ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

ΤΜΗΜΑ ΔΙΔΑΚΤΙΚΗΣ ΤΗΣ ΤΕΧΝΟΛΟΓΙΑΣ ΚΑΙ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΠΜΣ – Κατεύθυνση:
"Ψηφιακές Επικοινωνίες & Δίκτυα"

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Μελέτη και ανάλυση των

ΣΥΣΤΗΜΑΤΩΝ ΑΝΙΧΝΕΥΣΗΣ ΕΙΣΒΟΛΩΝ
INTRUSION DETECTION SYSTEMS

ΟΙΚΟΝΟΜΟΥ ΕΥΘΥΜΙΟΣ

Α.Μ. ΜΕ/0549

ΠΕΙΡΑΙΑΣ 2008

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

Τμήμα Διδακτικής της Τεχνολογίας και Ψηφιακών Συστημάτων

Κατεύθυνση

Ψηφιακές επικοινωνίες και δίκτυα

<u>Διπλωματική εργασία:</u>

Μελέτη και ανάλυση των ΣΥΣΤΗΜΑΤΩΝ ΑΝΙΧΝΕΥΣΗΣ ΕΙΣΒΟΛΩΝ INTRUSION DETECTION SYSTEMS

Οικονόμου Ευθύμιος

Α.Μ. ΜΕ/0549

ΕΠΙΒΛΕΨΗ: Λέκτορας Ξενάκης Χρήστος

ΠΕΙΡΑΙΑΣ 2008

Αφιερώνεται στους γονείς μου

Ταξιάρχη και Γεωργία

ΠΡΟΛΟΓΟΣ

Το πρόβλημα της ασφάλειας στα δίκτυα και τα υπολογιστικά συστήματα έχει απασχολήσει, απασχολεί και θα απασχολεί όλους εκείνους που εμπλέκονται και διακυβεύονται τα συμφέροντά τους από την χρήση των δικτύων των υπολογιστών.

Η διακίνηση των δεδομένων μέσω τηλεπικοινωνιακών δικτύων δημιουργεί προβλήματα καθώς αυτά καθίστανται ευπρόσβλητα σε κακόβουλες ενέργειες. Επίσης η σύνδεση των ιδιωτικών δικτύων με το Internet ή η διασύνδεσή τους μέσω αυτού δίνει τη δυνατότητα επιθέσεων προς τους υπολογιστές των ιδιωτικών δικτύων.

Η μελέτη και ανάλυση των Συστημάτων Ανίχνευσης Εισβολών (Intrusion Detection Systems - IDSs), αποτελεί το θέμα της παρούσας Διπλωματικής Εργασίας.

Στόχος και αντικείμενο αυτής, είναι η παρουσίαση των IDS συστημάτων δίνοντας έμφαση:

- στην Ανίχνευση Εισβολών (Intrusion Detection)
- στην Αρχιτεκτονική και Οργάνωση των IDSs συστημάτων (Arhitecture and Organization of IDSs)
- στα Τεχνικές Ανάλυσης-Μοντέλα εισβολών (Models of Intrusion)
- στο Χειρισμό και Πρόληψη περιστατικών των Εισβολών (Intrusion Handling and Incident Prevention)

Η συγκεκριμένη Διπλωματική Εργασία φιλοδοξεί να συμβάλλει, όσο το δυνατόν καλύτερα, στην κάλυψη των παραπάνω στόχων και να αναδείξει ότι με την φαινομενικά αλματώδη ανάπτυξη των Τηλεπικοινωνιών, της Πληροφορικής και γενικότερα της Τεχνολογίας τίθεται το θέμα της Ασφάλειας.

Κλείνοντας τον πρόλογο αυτό, θα ήθελα να εκφράσω τις ευχαριστίες μου στον καθηγητή μου, κύριο *Χρήστο Ξενάκη*, που με την πολύτιμη συμβολή του βοήθησε ουσιαστικά στην πραγμάτωση της παρούσας Διπλωματικής Εργασίας.

Μάιος 2008

Πειραιάς

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

ΚΑΤΑΛΟΓΟΣ ΕΙΚΟΝΩΝ

ΚΑΤΑΛΟΓΟΣ ΠΙΝΑΚΩΝ

ΚΕΦΑΛΑΙΟ 1^{ο}

ΕΙΣΑΓΩΓΗ

1. Τι σημαίνει "Ασφάλεια" στα Δίκτυα Υπολογιστών

Το πρόβλημα της ασφάλειας των πληροφοριών είναι ιδιαίτερα σημαντικό στα σύγχρονα δίκτυα υπολογιστών. Η χρησιμοποίηση όλο και πιο προχωρημένων τεχνικών και τεχνολογιών όπως για παράδειγμα οι σύγχρονες βάσεις δεδομένων και τα σύγχρονα δίκτυα, προσφέρει αναμφισβήτητα σημαντικά πλεονεκτήματα και δυνατότητες, αυξάνει όμως ταυτόχρονα σημαντικά τα προβλήματα τα σχετικά με την προστασία και τη διαθεσιμότητα των πληροφοριών.

Η ασφάλεια αποτελεί αναγκαία συνθήκη και είναι απαραίτητη, σε συνδυασμό με τις άλλες βασικές προϋποθέσεις λειτουργίας όπως η ποιότητα και η απόδοση, για την εξασφάλιση της εύρυθμης λειτουργίας μιας επιχείρησης ή ενός οργανισμού. Αυτό είναι ιδιαίτερα σημαντικό σήμερα όπου πολύ συχνά το σύνολο των παρεχομένων υπηρεσιών μιας επιχείρησης στηρίζεται στην πληροφορική (π.χ. πάνω από το 80% των υπηρεσιών μιας τράπεζας).

Η έννοια της ασφάλειας ενός Δικτύου Υπολογιστών σχετίζεται με την ικανότητα μιας επιχείρησης ή ενός οργανισμού να προστατεύει τις πληροφορίες του από τυχόν αλλοιώσεις και καταστροφές, καθώς και από μη εξουσιοδοτημένη χρήση των πόρων του. Σχετίζεται επίσης με την ικανότητά του να παρέχει ορθές και αξιόπιστες πληροφορίες, οι οποίες είναι διαθέσιμες στους εξουσιοδοτημένους χρήστες κάθε φορά που τις αναζητούν. Η ικανότητα αυτή στηρίζεται στη λήψη μέτρων τα οποία διασφαλίζουν την ακεραιότητα και την εμπιστευτικότητα των δεδομένων, καθώς και την αδιάλειπτη λειτουργία του δικτύου.

Σύμφωνα με τον προηγούμενο ορισμό της ασφάλειας, η ασφάλεια στα δίκτυα υπολογιστών έχει να κάνει με την πρόληψη και ανίχνευση μη εξουσιοδοτημένων ενεργειών των χρηστών του δικτύου καθώς και την λήψη μέτρων. Ποιο συγκεκριμένα η ασφάλεια στα δίκτυα υπολογιστών σχετίζεται με:

- ***Πρόληψη (Prevention)***: Την λήψη δηλαδή μέτρων για να προληφθούν φθορές των μονάδων ενός δικτύου υπολογιστών.
- ***Ανίχνευση (Detection)***: Την λήψη μέτρων για την ανίχνευση του πότε, πώς και από ποιον προκλήθηκε φθορά σε μία από τις παραπάνω μονάδες.
- ***Αντίδραση (Reaction)***: Την λήψη δηλαδή μέτρων για την αποκατάσταση ή ανάκτηση των συστατικών ενός δικτύου.

Η ασφάλεια δικτύων και πληροφοριών μπορεί ακόμη να οριστεί ως η δυνατότητα ενός δικτύου ή συστήματος πληροφοριών να αντισταθεί, σε δεδομένο επίπεδο αξιοπιστίας, σε τυχαία συμβάντα ή κακόβουλες ενέργειες που θέτουν σε κίνδυνο τη διάθεση, την επαλήθευση ταυτότητας, την ακεραιότητα και την τήρηση του απορρήτου των δεδομένων που έχουν αποθηκευτεί ή μεταδοθεί καθώς και τις συναφείς υπηρεσίες που παρέχονται είτε είναι προσβάσιμες μέσω των δικτύων και συστημάτων αυτών.

Η προστασία ενός δικτύου το οποίο συνδέεται και με το Internet είναι ένα θέμα που καλούνται να αντιμετωπίσουν οι σύγχρονες επιχειρήσεις και οργανισμοί. Είναι γενικά αποδεκτό σήμερα ότι η έννοια της ασφάλειας των δικτύων υπολογιστών αλλά και των πληροφοριακών συστημάτων γενικότερα, συνδέεται στενά με τρεις βασικές έννοιες:

- ***Διαθεσιμότητα (Availability)***
- ***Εμπιστευτικότητα (Confidentiality)***
- ***Ακεραιότητα (Integrity)***

Οι γενικές απαιτήσεις ασφάλειας δικτύων και συστημάτων πληροφοριών μπορούν να διατυπωθούν με τα εξής τρία, αλληλένδετα χαρακτηριστικά:

i. <u>Διαθεσιμότητα</u>

Διαθεσιμότητα ονομάζεται η ιδιότητα του να είναι προσπελάσιμες και χωρίς αδικαιολόγητη καθυστέρηση οι υπηρεσίες ενός δικτύου υπολογιστών όταν τις χρειάζεται μια εξουσιοδοτημένη οντότητα. Με τον όρο διαθεσιμότητα εννοούμε ότι δηλαδή ότι τα δεδομένα είναι προσβάσιμα (accessible) και οι υπηρεσίες λειτουργούν, παρά τις όποιες τυχόν διαταραχές, όπως διακοπή τροφοδοσίας, φυσικές καταστροφές, ατυχήματα ή επιθέσεις. Αυτό σημαίνει ότι οι εξουσιοδοτημένοι χρήστες των υπολογιστικών συστημάτων και των υπολογιστών του δικτύου δεν αντιμετωπίζουν προβλήματα άρνησης εξυπηρέτησης (**D**enial **o**f **S**ervice - **DoS**) όταν επιθυμούν να προσπελάσουν τους πόρους του δικτύου.

Για τους σκοπούς της ασφάλειας, μας απασχολεί βασικά η παρεμπόδιση κακόβουλων επιθέσεων που αποσκοπούν στο να παρακωλύσουν την πρόσβαση των νόμιμων χρηστών σε ένα πληροφοριακό σύστημα. Αυτές οι επιθέσεις ονομάζονται επιθέσεις άρνησης παροχής υπηρεσιών. Η άρνηση παροχής υπηρεσιών σημαίνει παρεμπόδιση της εξουσιοδοτημένης προσπέλασης πληροφοριών και πόρων ή πρόκληση καθυστέρησης των λειτουργιών που είναι κρίσιμες στο χρόνο. Η αντιμετώπισή τους αποσκοπεί στο να υπερνικήσει την σκόπιμη, που προκαλείται από κακόβουλα μέρη, παρά τυχαία απώλεια της διαθεσιμότητας. Ένα παράδειγμα επίθεσης άρνησης παροχής υπηρεσιών είναι οι επιθέσεις «πλημμύρας» στο διαδίκτυο, όπου ο επιτιθέμενος κατακλύζει έναν εξυπηρετητή στέλνοντάς του έναν τεράστιο αριθμό αιτήσεων σύνδεσης.

Παρόλο που η διαθεσιμότητα συχνά αναδεικνύεται στο πλέον σημαντικό χαρακτηριστικό της ασφάλειας, εντούτοις λίγοι μηχανισμοί υπάρχουν για να βοηθήσουν στην υποστήριξή της.

ii. Εμπιστευτικότητα

Σε πολλές περιπτώσεις της καθημερινής ζωής οι έννοιες της ασφάλειας και της εμπιστευτικότητας σχεδόν ταυτίζονται, όπως για παράδειγμα στα στρατιωτικά περιβάλλοντα όπου η ασφάλεια έχει τη σημασία του να κρατούνται μυστικές οι πληροφορίες.

Η εμπιστευτικότητα σημαίνει πρόληψη μη εξουσιοδοτημένης αποκάλυψης πληροφοριών, δηλαδή, πρόληψη από μη εξουσιοδοτημένη ανάγνωση. Επομένως, σημαίνει ότι τα δεδομένα που διακινούνται μεταξύ των υπολογιστών ενός δικτύου, αποκαλύπτονται μόνο σε εξουσιοδοτημένα άτομα. Αυτό αφορά όχι μόνο την προστασία από μη εξουσιοδοτημένη αποκάλυψη των δεδομένων αυτών καθαυτών αλλά ακόμη και από το γεγονός ότι τα δεδομένα απλώς υπάρχουν. Έτσι για παράδειγμα, το γεγονός ότι κανείς έχει φάκελο εγκληματία είναι συχνά το ίδιο σημαντικό όπως και οι λεπτομέρειες για το έγκλημα που διαπράχθηκε.

Άλλες εκφάνσεις της εμπιστευτικότητας είναι:

- Η **ιδιωτικότητα (secrecy)**: προστασία των δεδομένων προσωπικού χαρακτήρα, δηλαδή αυτών που αφορούν συγκεκριμένα πρόσωπα και
- Η **μυστικότητα (privacy)**: προστασία των δεδομένων που ανήκουν σε έναν οργανισμό ή μια επιχείρηση.

iii. Ακεραιότητα

Πρόκειται για την επιβεβαίωση ότι τα δεδομένα που έχουν αποσταλεί, παραληφθεί ή αποθηκευτεί είναι πλήρη και δεν έχουν υποστεί αλλοίωση. Η ακεραιότητα μπορεί να οριστεί γενικότερα ως η απαίτηση να είναι τα πράγματα όπως πρέπει να είναι. Στην πληροφορική, ακεραιότητα σημαίνει πρόληψη μη εξουσιοδοτημένης μεταβολής πληροφοριών, δηλαδή, πρόληψη από μη εξουσιοδοτημένη εγγραφή ή διαγραφή, συμπεριλαμβανομένης και της μη εξουσιοδοτημένης δημιουργίας δεδομένων.

Επομένως, σημαίνει ότι η μετατροπή, διαγραφή και δημιουργία των δεδομένων ενός υπολογιστικού συστήματος, γίνεται μόνο από εξουσιοδοτημένα μέρη.

2. Προβλήματα Ασφαλείας Δικτύων

Ένα δικτυωμένο σύστημα είναι επιρρεπές σε ένα αριθμό απειλών που προέρχονται και από νόμιμους χρήστες του συστήματος αλλά και κυρίως από επίδοξους εισβολείς. Κάθε κόμβος του δικτύου είναι ένα υπολογιστικό σύστημα με όλα τα γνωστά προβλήματα ασφάλειας. Σε αυτά, έρχεται το δίκτυο να προσθέσει το πρόβλημα της επικοινωνίας μέσω ενός πολύ εκτεθειμένου μέσου και της προσπέλασης από μακρινές τοποθεσίες μέσω πιθανώς μη-έμπιστων υπολογιστικών συστημάτων. Μερικοί λόγοι για τους οποίους αποκτούν ιδιαίτερη σημασία τα θέματα ασφάλειας δικτύων υπολογιστών είναι οι εξής:

- Η αυξημένη περιπλοκότητα περιορίζει το αίσθημα εμπιστοσύνης για την ασφάλεια των δικτύων.
- Υπάρχει αύξηση στον αριθμό των διαύλων επικοινωνίας και άρα των πιθανών σημείων επίθεσης, τα οποία πρέπει να οχυρωθούν κατάλληλα.
- Έχουν γίνει ασαφή τα όρια των δικτύων και οι διακρίσεις μεταξύ των τμημάτων μιας επιχείρησης. Κάθε κόμβος οφείλει να είναι ικανός να αντιδράσει σωστά στη παρουσία ενός νέου και μη-έμπιστου κόμβου. Από την άλλη, κάθε κόμβος μπορεί να ανήκει ταυτόχρονα σε περισσότερα από ένα δίκτυα, με αποτέλεσμα να μην είναι ξεκάθαρη η εικόνα των νομίμων χρηστών του κάθε δικτύου.
- Η δυνατότητα ανωνυμίας ενός χρήστη απαιτεί ισχυρούς μηχανισμούς πιστοποίησης μεταξύ των υπολογιστών, που συνήθως είναι διαφορετικοί από αυτούς που πιστοποιούν τους χρήστες στα υπολογιστικά συστήματα.

Υπάρχει αδυναμία ελέγχου της δρομολόγησης των δεδομένων που διακινούνται μέσω των δικτύων.

3. Αναγκαιότητα και Σκοπιμότητα της Ασφάλειας

Είναι γεγονός ότι, παρά την προφανή της χρησιμότητα, η λήψη των απαραίτητων μέτρων ασφάλειας δημιουργεί πολλές φορές κάποια πρόσθετη επιβάρυνση στην απόδοση και το κόστος λειτουργίας του δικτύου υπολογιστών μιας επιχείρησης. Θα πρέπει ακόμη να αποδεχτούμε το κόστος της ασφάλειας και ως κόστος χρόνου και ως κόστος χρήματος. Συνεπώς, μπορεί να θεωρηθεί ότι η ασφάλεια βρίσκεται σε σχέση αντιστρόφως ανάλογη με την αποδοτικότητα του δικτύου υπολογιστών μιας επιχείρησης. Αυτό όμως δεν είναι σωστό γιατί η ασφάλεια είναι κόστος αναγκαίο για την ομαλή και εύρυθμη λειτουργία του.

Το συγκεκριμένο κόστος για την ασφάλεια των δικτύων μιας επιχείρησης εξαρτάται και προκύπτει από την εκάστοτε ακολουθούμενη πολιτική ασφάλειας. Απαιτείται συνεπώς μια πολιτική ασφαλείας η οποία θα πρέπει να εξισορροπεί το κόστος εισαγωγής ασφάλειας από την μία πλευρά και το κόστος ζημιών από πιθανολογούμενο κίνδυνο από την άλλη. Επίσης, θα πρέπει να δημιουργούνται τέτοιες συνθήκες ασφάλειας ώστε να μη παρεμποδίζεται η ευελιξία και η ανάπτυξη της επιχείρησης.

Η αναγκαία πολιτική ασφάλειας καθορίζεται από μία δυναμική εκτίμηση του κόστους των μέτρων ασφάλειας σε σχέση με τις συνέπειες που θα έχει για τον οργανισμό οποιαδήποτε πρόκληση δυσλειτουργίας. Ο βασικός αυτός κανόνας ισχύει για όλους τους τομείς και όλα τα επίπεδα ασφάλειας. Έτσι, σε κάθε περίπτωση όπου απαιτείται η λήψη κάποιου μέτρου ασφάλειας, πρέπει να εξετάζεται η πιθανότητα να συμβεί κάποιο πρόβλημα ασφάλειας, σε σχέση με τις συνέπειες που αυτό θα δημιουργήσει. Εάν η τιμή των δύο αυτών παραμέτρων είναι υψηλή, τότε πρέπει απαραίτητα να ληφθούν μέτρα, ανεξάρτητα από το κόστος πρόληψης.

Τέλος, πρέπει να σημειωθεί ότι η ασφάλεια χαρακτηρίζεται από την φύση της ως δυναμική παράμετρος και όχι στατική, καθώς η τεχνολογία, ο ανταγωνισμός, η πολυπλοκότητα των πληροφοριακών συστημάτων και η ολοένα βελτιούμενη επιτηδειότητα των 'επιτιθέμενων', απαιτούν τη λήψη νέων και συνεχώς αυστηρότερων μέτρων ασφάλειας. Συνεπώς, η ακολουθούμενη πολιτική ασφαλείας θα πρέπει να επανεξετάζεται τακτικά και να διορθώνεται όπου αυτό κρίνεται απαραίτητο.

4. Προτεινόμενη Μεθοδολογία Βελτίωσης της Ασφάλειας

Η ύπαρξη ασφάλειας στο intranet και το extranet απαιτεί την δημιουργία εμποδίων στην φυσική προσπέλαση του εξοπλισμού, το δίκτυο, αλλά και τις εφαρμογές. Τι είναι όμως

αυτό που θέλουμε να διαφυλάξουμε; Μία γενική απάντηση της μορφής «τον οργανισμό ή εταιρία μου από αυτούς που θέλουν να χρησιμοποιήσουν την τεχνολογία για να κάνουν κακό», αφήνει περιθώρια για μία μόνο λύση στο πρόβλημα: μην χρησιμοποιείτε υπολογιστές. Αυτή την στιγμή δεν υπάρχει 100% ασφαλές σύστημα προστασίας ενός intranet ή extranet. Μάλιστα όσο πλησιάζουμε προς την απόλυτη ασφάλεια το ίδιο ασυμπτωτικά διογκώνεται το κόστος για την δημιουργία ενός τέτοιου συστήματος ασφάλειας.

Για να είναι εφικτή μια υλοποίηση, δηλαδή το κόστος υλοποίησης του συστήματος ασφάλειας να είναι μικρότερο από το κόστος μιας επίθεσης, πρέπει να γίνουν μία σειρά από ενέργειες που έχουν σκοπό την ανάλυση, τον σχεδιασμό, την υλοποίηση και την λειτουργία του συστήματος μας. για την αντιμετώπιση περιστατικών επιθέσεων.

Έτσι χρειάζεται:

- Να γίνει ανάλυση των κινδύνων που έχουμε να αντιμετωπίσουμε και καταγραφή των πόρων που πρέπει να διαφυλάξουμε,
- να προσδιοριστεί η πολιτική ασφάλειας που θα εφαρμόσουμε,
- να σχεδιάσουμε την αρχιτεκτονική του υπολογιστικού και πληροφοριακού συστήματος που θα αναπτύξουμε,
- να αποφασίσουμε για τις υπηρεσίες ασφάλειας που θα υιοθετήσουμε για την προστασία του intranet/extranet,
- να γνωρίζουμε τα εργαλεία και τις μεθόδους επιθέσεων καθώς και τα αντίμετρα που πρέπει να εφαρμόζονται,
- να έχουμε σχεδιάσει τον τρόπο αντιμετώπισης ενός περιστατικού επίθεσης,
- να ενημερώνουμε τους χρήστες μας,
- να είμαστε πάντα ενήμεροι για τα τελευταία νέα σε θέματα ασφάλειας παρακολουθώντας λίστες και ανακοινώσεις κατασκευαστών υπολογιστικών συστημάτων, οργανισμών ασφάλειας, χρηστών, ακόμα και hackers.

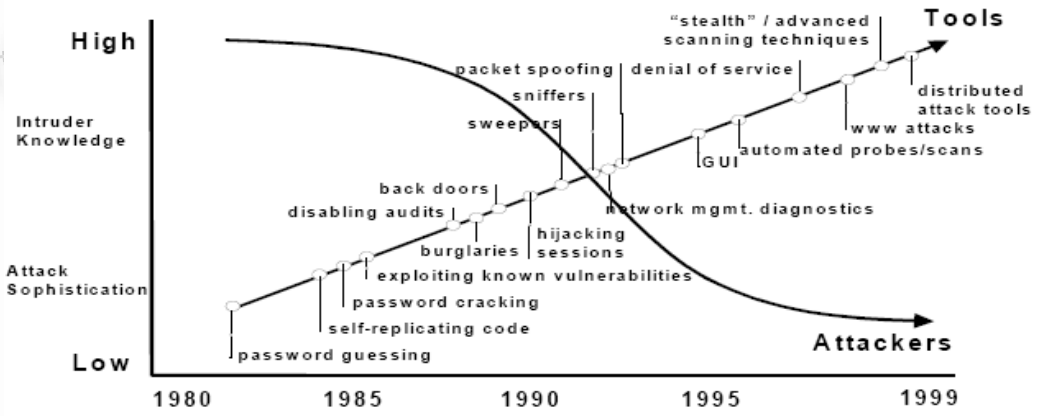
Για να έχουμε ένα ικανοποιητικό επίπεδο ασφάλειας πρέπει να αναλύσουμε τα παραπάνω χαρακτηριστικά με σκοπό την ικανοποίηση των γενικών απαιτήσεων της ασφάλειας ***(Διαθεσιμότητα-Availability, Εμπιστευτικότητα-Confidentiality, Ακεραιότητα-Integrity)*** που αναλύσαμε παραπάνω.

ΚΕΦΑΛΑΙΟ 2ο

ΑΝΙΧΝΕΥΣΗ ΕΙΣΒΟΛΩΝ

Τα τελευταία χρόνια έχει δοθεί ιδιαίτερη σημασία στο πεδίο της ανίχνευσης εισβολών σε δίκτυα κυρίως λόγω της τεράστιας επέκτασης και ανάπτυξης του Διαδικτύου καθώς και του μεγάλου αριθμού δικτυωμένων συστημάτων που υπάρχουν. Ο αυξανόμενος αριθμός δικτυωμένων υπολογιστικών συστημάτων έχει οδηγήσει σε μια αύξηση των παράνομων δραστηριοτήτων, όχι μόνο από εξωτερικούς «εισβολείς» αλλά και από το εσωτερικό των δικτύων, από υπαλλήλους που καταχρώνται τις δυνατότητες και τα δικαιώματα που τους δίνονται για προσωπικό όφελος.

Με την αύξηση των παράνομων δραστηριοτήτων και των εισβολών, υπήρξε παράλληλη ανάπτυξη και στα συστήματα ανίχνευσης εισβολών, τόσο στον εμπορικό όσο και στον ερευνητικό τομέα. Αυτά τα συστήματα προσπαθούν με διαφορετικές μεθόδους να ανιχνεύσουν την όποια παράνομη δραστηριότητα. Τα συστήματα αυτά συνήθως ανιχνεύουν ένα περιορισμένο εύρος εισβολών αλλά αποτυγχάνουν πέραν αυτού. Στη δεκαετία του '80, οι εισβολείς ήταν οι system experts. Είχαν ένα υψηλό επίπεδο εμπειρίας και κατασκεύασαν προσωπικά τις μεθόδους για να "σπάνε" τα συστήματα. Σήμερα, η απαιτούμενη γνώση για την πραγματοποίηση μιας επίθεσης ολοένα και μειώνεται, λόγω της διαδεδομένης και εύκολης χρήσης των εργαλείων ανίχνευσης εισβολών και των διαφόρων προγραμμάτων που αναπαράγουν τις γνωστές μεθόδους επίθεσης (Εικόνα 1).



Εικόνα 1: Attack sophistication vs. Intruder technical knowledge

Με τον όρο ***Ανίχνευση Εισβολών – Intrusion Detection*** αναφερόμαστε στην παρακολούθηση και ανάλυση των συμβάντων που λαμβάνουν χώρα σε υπολογιστές ή δίκτυα, με σκοπό να εντοπισθούν ενδείξεις προσπαθειών εισβολής. Οι «προσπάθειες εισβολής» περιλαμβάνουν ίχνη από απόπειρες για παραβίαση της ακεραιότητας, εμπιστευτικότητας ή διαθεσιμότητας των πληροφοριακών πόρων, καθώς επίσης και προσπάθειες για παράκαμψη των μηχανισμών ασφάλειας. Μία τέτοια εισβολή μπορεί να προέρχεται:

i. από «*εξωτερικούς*» προς το εταιρικό δίκτυο χρήστες, οι οποίοι κανονικά δεν έχουν δικαίωμα πρόσβασης στο πληροφοριακό σύστημα, αλλά προσπαθούν να το προσπελάσουν.

ii. από «*εσωτερικούς*» χρήστες που έχουν περιορισμένα δικαιώματα πρόσβασης αλλά επιχειρούν ενέργειες που η πολιτική ασφάλειας τους απαγορεύει.

iii. από «*εσωτερικούς*» χρήστες, οι οποίοι έχουν κατάλληλα δικαιώματα πρόσβασης για τις πράξεις στις οποίες προβαίνουν, αλλά ασκούν τα δικαιώματα αυτά με καταχρηστικό τρόπο. Για παράδειγμα, ένας υπάλληλος της μισθοδοσίας έχει δικαίωμα να τροποποιεί τους μισθούς των υπαλλήλων, αλλά η παροχή στον εαυτό του αύξησης 80% χωρίς τη σχετική εντολή από τη διοίκηση είναι μία περίπτωση καταχρηστικής άσκησης του δικαιώματός του.

Τα συστήματα ανίχνευσης εισβολών (***I**ntrusion **D**etection **S**ystems-**IDS***) είναι συστήματα που συντίθενται από υλικό και λογισμικό και έχουν ως στόχο την αυτοματοποίηση της ανίχνευσης εισβολών.

Ως εργαλείο επίθεσης (attack tool) χαρακτηρίζεται ένα αυτοματοποιημένο πρόγραμμα, το οποίο είναι σχεδιασμένο με σκοπό την παραβίαση της πολιτικής της ασφάλειας ενός συστήματος.

1. Λόγοι εισαγωγής των Συστημάτων Ανίχνευσης Εισβολών

Υπάρχουν πολυάριθμοι λόγοι για τους οποίους ένας οργανισμός θα επιθυμούσε να εγκαταστήσει και να θέσει σε λειτουργία ένα σύστημα ανίχνευσης εισβολών. Οι πιο σημαντικοί παρατίθενται στη συνέχεια.

i. ***Πρόληψη προβλημάτων***. Τα συστήματα ανίχνευσης εισβολών συνεισφέρουν στην πρόληψη προβλημάτων κατά δύο τρόπους: αφ’ ενός είναι πιθανόν να επισημάνουν τις προσπάθειες εισβολής σε ένα πρώιμο στάδιο, οπότε και θα ληφθούν τα κατάλληλα μέτρα

για την αντιμετώπισή τους πριν γίνει κάποια σημαντική ζημιά. Αφ' ετέρου, γνωρίζοντας οι επίδοξοι εισβολείς ότι υφίσταται κάποιο τέτοιο σύστημα, ξέρουν ότι η πιθανότητα αποκάλυψης και τιμωρίας τους είναι σαφώς μεγαλύτερη, και κατά συνέπεια ενδέχεται να μην εκδηλώσουν συνολικά την επίθεσή τους.

ii. ***Ανίχνευση επιθέσεων και παραβιάσεων που δεν ανιχνεύονται με άλλα μέσα***. Επί παραδείγματι, οι καταχρήσεις δικαιωμάτων από εσωτερικούς χρήστες δεν είναι δυνατόν να αντιμετωπισθούν με σχήματα διακρίβωσης ταυτότητας και ελέγχου πρόσβασης, διότι τα σχήματα αυτά δεν είναι σχεδιασμένα για να αντιμετωπίζουν τέτοιου είδους ζητήματα.

iii. ***Εντοπισμός και αντιμετώπιση προσπαθειών ανίχνευσης***. Ένα τυπικό σχήμα επίθεσης σε πληροφοριακά συστήματα χωρίζεται σε τρεις φάσεις: αρχικά ανιχνεύεται το πληροφοριακό σύστημα για να διαπιστωθεί η διαμόρφωσή του και οι προσφερόμενες από αυτό υπηρεσίες. Στη συνέχεια, ανασύρονται από «βιβλιοθήκες» οι τεχνικές που είναι δυνατόν να χρησιμοποιηθούν για να παραβιαστεί η ασφάλεια του συστήματος και, τέλος, οι τεχνικές αυτές χρησιμοποιούνται. Ενώ τα υπόλοιπα μέτρα ασφάλειας (firewalls, προγράμματα επιδιόρθωσης, έλεγχος πρόσβασης κ.ά.) εστιάζονται στην αντιμετώπιση της τελευταίας φάσης, τα συστήματα ανίχνευσης εισβολών μπορούν να ανιχνεύσουν τις προσπάθειες ανίχνευσης και να τις αναχαιτίσουν ή να ενημερώσουν σχετικά τους διαχειριστές για λήψη μέτρων. Η άμεση αντίδραση σε τέτοια ενδεχόμενα θωρακίζει το σύστημα και αποθαρρύνει τους επίδοξους εισβολείς.

iv. ***Τεκμηρίωση υπαρκτών απειλών***. Τα συστήματα ανίχνευσης εισβολών μπορούν να αποδείξουν το γεγονός ότι ένα πληροφοριακό σύστημα αντιμετωπίζει απειλές, πριν κάποια από αυτές δημιουργήσει σημαντικές ζημιές. Μία τέτοια τεκμηρίωση είναι πολλαπλώς χρήσιμη, καθώς α) πείθει τη διοίκηση του οργανισμού-εταιρίας για κατανομή πόρων στα συστήματα ασφάλειας β) βοηθά στον προσδιορισμό των μέτρων ασφάλειας που είναι πιο κατάλληλα για το σύστημα, καθώς η φύση των απειλών προσδιορίζει σε μεγάλο βαθμό και τα αντίμετρα που πρέπει να εφαρμοσθούν γ) βοηθά στην πιο αποτελεσματική κατανομή των πόρων ασφάλειας στα διάφορα τμήματα του πληροφοριακού συστήματος, ανάλογα με τις απειλές που το καθένα αντιμετωπίζει και την αξία του για τον οργανισμό.

v. ***Έλεγχος ποιότητας για το σχεδιασμό ασφάλειας και τη διαχείριση***. Τόσο το σχέδιο ασφάλειας του οργανισμού όσο και η υλοποίησή του από τους διαχειριστές ασφάλειας και συστημάτων είναι πιθανόν να παρουσιάζουν ατέλειες. Τα συστήματα ανίχνευσης εισβολών μπορούν να καταδείξουν τις ατέλειες, βοηθώντας έτσι στη διόρθωσή τους, πριν

αυτές γίνουν αντικείμενο εκμετάλλευσης.

vi. Τα συστήματα ανίχνευσης εισβολών μπορούν να παράσχουν πληροφορίες για ***επιτυχείς επιθέσεις***, συνεισφέροντας στην αποτίμηση του μεγέθους της ζημιάς, στη διαμόρφωση της λίστας ενεργειών για την ανάκαμψη και στον σχεδιασμό και εφαρμογή προληπτικών μέτρων για μελλοντική αποφυγή αντίστοιχων περιστατικών.

vii. ***Θωράκιση παλαιών συστημάτων***. Σε αρκετές περιπτώσεις είναι απαραίτητη η διατήρηση σε λειτουργία παλαιών συστημάτων τα οποία δεν υποστηρίζονται πια από τους κατασκευαστές τους και που, ως εκ τούτου, είναι πιο ευάλωτα σε επιθέσεις. Τα πεπαλαιωμένα συστήματα μπορούν να προστατευθούν με τη χρήση συστημάτων ανίχνευσης εισβολών.

viii. ***Συμπλήρωση των διαδικασιών εγκατάστασης επιδιορθωτικών προγραμμάτων***. Ακόμη και στην περίπτωση που τα συστήματα του οργανισμού υποστηρίζονται από τους κατασκευαστές και έτσι υπάρχουν τα σχετικά επιδιορθωτικά προγράμματα, η διαθεσιμότητα των προγραμμάτων αυτών δεν είναι πάντα άμεση, ενώ για πολύπλοκα περιβάλλοντα η εγκατάστασή τους μπορεί να καθυστερεί για διάφορους λόγους.

ix. ***Αναγκαιότητα ύπαρξης ευπαθών υπηρεσιών***. Μολονότι για μερικές υπηρεσίες είναι γνωστό ότι είναι επισφαλείς από την πλευρά της ασφάλειας, οι χρήστες ή η διοίκηση οργανισμών απαιτούν μερικές φορές τη διατήρησή τους διότι θεωρούνται πιο εύχρηστες και άρα πιο παραγωγικές. Τυπικό παράδειγμα είναι η υπηρεσία FTP που σαφώς είναι προβληματική καθώς διακινεί μη κρυπτογραφημένα συνθηματικά, ωστόσο το ασφαλέστερο αντίστοιχο, το ασφαλές πρωτόκολλο μεταφοράς αρχείων, είναι σημαντικά πιο δύσχρηστο. Τα συστήματα ανίχνευσης εισβολών μπορούν να ελέγχουν τις επισφαλείς υπηρεσίες, εντοπίζοντας περιστατικά προξενούν αυξημένους κινδύνους.

x. ***Αξιολόγηση των ενεργειών των χρηστών ή των διαχειριστών***. Οι μηχανισμοί ασφάλειας που παρέχονται από το σύστημα είναι δυνατόν να μην χρησιμοποιούνται σωστά ή αποτελεσματικά από τους χρήστες και τους διαχειριστές. Το σύστημα ανίχνευσης εισβολών μπορεί να επισημαίνει τις σχετικές δυνατότητες βελτίωσης.

xi. ***Έλεγχος συνέπειας μεταξύ πολιτικής ασφάλειας και κανόνων πρόσβασης***. Η πολιτική ασφάλειας που ισχύει στα πλαίσια του οργανισμού είναι δυνατόν να μην απεικονίζεται πιστά στους κανόνες πρόσβασης που έχουν θεσπίσει οι διαχειριστές . Μέσω αρχείων καταγραφών που τηρούνται από τα συστήματα ανίχνευσης εισβολών είναι δυνατόν να εντοπισθούν οι ασυνέπειες και να διορθωθούν.

2. Στόχοι των Συστημάτων Ανίχνευσης Εισβολών

Τα επιθυμητά χαρακτηριστικά-στόχοι των πραγματικών συστημάτων ανίχνευσης εισβολών παρατίθενται παρακάτω:

i. ***Ανίχνευση μεγάλου εύρους εισβολών***: Οι εισβολές, τόσο αυτές που προέρχονται από το εσωτερικό του δικτύου, όσο και από το εξωτερικό, παρουσιάζουν ιδιαίτερο ενδιαφέρον. Με τα IDS μπορούν να εντοπιστούν γνωστές και άγνωστες επιθέσεις. Η δυνατότητα αυτή προϋποθέτει την ύπαρξη ενός μηχανισμού εκμάθησης ή προσαρμογής στους νέους τύπους επίθεσης και στις αλλαγές της συνήθους δραστηριότητας των χρηστών.

ii. ***Έγκαιρη ανίχνευση εισβολών***: Ο όρος έγκαιρη δεν αναφέρεται κυριολεκτικά σε πραγματικό χρόνο (real time), αφού η ανίχνευση της εισβολής σε πραγματικό χρόνο εισάγει σημαντικά ζητήματα ανταπόκρισης. Συχνά, όμως, απαιτείται η ανακάλυψη μίας εισβολής σε εύλογο χρονικό διάστημα. Και αυτό γιατί στις περισσότερες περιπτώσεις, ο προσδιορισμός μιας εισβολής που πραγματοποιήθηκε πριν από σημαντικό χρονικό διάστημα φαίνεται να μην παρουσιάζει ιδιαίτερη χρησιμότητα.

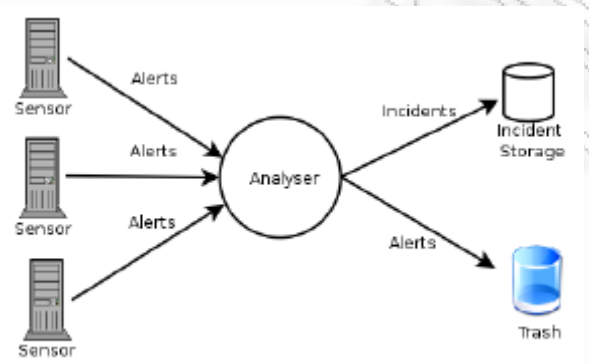
iii. ***Παρουσίαση της ανάλυσης με απλή και εύκολα αντιληπτή μορφή***: Θα ήταν επιθυμητό τα αποτελέσματα ανίχνευσης μιας εισβολής να προκύπτουν, τελικά, από την τιμή μιας δίτιμης μεταβλητής. Συνήθως, όμως, αυτό δεν μπορεί να συμβεί αφού οι εισβολές δεν είναι λειτουργικά τόσο σαφείς. Για το λόγο αυτό, ο μηχανισμός ανίχνευσης εισβολών παρουσιάζει περισσότερο σύνθετα δεδομένα στον υπεύθυνο ασφάλειας του συστήματος. Εκείνος, με τη σειρά του, πρέπει να συνάγει αν πρέπει να ληφθούν κάποια μέτρα και ποια ακριβώς πρέπει να είναι αυτά. Επειδή οι μηχανισμοί ανίχνευσης εισβολών μπορεί να παρακολουθούν περισσότερα από ένα συστήματα, ιδιαίτερη κρισιμότητα παρουσιάζει η διεπαφή τους με το χρήστη.

xii. ***Να είναι ακριβή***: Ένα *ψευδές θετικό* σήμα (*false positive*) προκύπτει όταν ένα σύστημα εντοπισμού εισβολών αναφέρει μία επίθεση, ενώ στην πραγματικότητα δεν υπάρχει σχετική επίθεση σε εξέλιξη. Τα ψευδώς θετικά σήματα μειώνουν την αξιοπιστία του συστήματος και αυξάνουν αναιτίως την απαιτούμενη εργασία. Τα *ψευδώς αρνητικά* σήματα (*false negative*) παράγονται όταν ένα σύστημα ανίχνευσης εισβολών αποτυγχάνει να αναφέρει μια πραγματική επίθεση που βρίσκεται σε εξέλιξη. Αυτά είναι ιδιαίτερα αρνητικά, αφού ο σκοπός των συστημάτων εντοπισμού εισβολών είναι ακριβώς να αναφέρουν τις πραγματικές επιθέσεις. Γενικός σκοπός ενός συστήματος ανίχνευσης εισβολών είναι να ελαχιστοποιήσει τις εσφαλμένες ενδείξεις από αμφότερες τις κατηγορίες σφαλμάτων.

3. Συναγερμοί και Γεγονότα

Στα συστήματα ανίχνευσης εισβολών, οι όροι *"**Συναγερμοί**"*, ***Alerts*** και τα *"**Γεγονότα**"*, ***Incidents***, διαδραματίζουν έναν σημαντικό ρόλο.

Η εισαγωγή ενός IDS παρέχεται από έναν ή περισσότερους αισθητήρες (sensors), οι οποίοι είναι σημεία παρατήρησης στο δίκτυο. Αυτοί οι αισθητήρες παράγουν συνήθως πολλά alerts. Ωστόσο, πολλά από αυτά τα alerts δεν είναι σχετικά-έγκυρα. Όλα τα alerts αναλύονται, και μόνο τα σχετικά-έγκυρα alerts αναφέρονται ως incidents. Η επισκόπηση της διαδικασίας αυτής απεικονίζεται στην παρακάτω Εικόνα. Η είσοδος της προαναφερθείσας διεργασίας, που αποτελείται από τα alerts, παρέχεται από τους αισθητήρες.



Εικόνα 2: Διαδικασία ανάλυσης των alerts, σε alerts και incidents

3.1. Alerts

Τα **alerts**, μερικές φορές καλούμενα ως **γεγονότα** (**indicators**) ή **συμβάντα** (**events**), ορίζονται ως οι αισθητές ή ευδιάκριτες ενέργειες που επιβεβαιώνουν ή αρνούνται τις εχθρικές προθέσεις. Όπως παρουσιάζεται στην Εικόνα 2, τα alerts είναι οι είσοδοι (inputs) των γεννητριών των γεγονότων.

Τα alerts προφανώς προέρχονται από τη δικτυακή κυκλοφορία (traffic) που ελήφθησαν από τους **IDS sensors**. Ένα κανονικό IDS δεν έχει κανένα πρόσθετο χαρακτηριστικό γνώρισμα. Είναι ακριβώς ένα σύστημα ηλεκτρονικών υπολογιστών ή ένα τμήμα δικτύου, χωρίς τα πρόσθετα συστήματα που τρέχουν σε αυτό. Δεδομένου ότι ένα IDS δεν προσφέρει καμία χρήσιμη υπηρεσία στους χρήστες Internet και επιπλέον του γεγονότος ότι οι διευθύνσεις του Internet του IDS δεν είναι δημοσίως γνωστές, θεωρητικά δεν πρέπει να υπάρξει καμία κυκλοφορία σε ή από το IDS και επομένως η επί το πλείστον κυκλοφορία στο IDS είναι ύποπτη.

3.2. Incidents

Όλα τα alerts έχουν μια συγκεκριμένη τιμή κινδύνου, αλλά μερικές έχουν μεγαλύτερη τιμή από άλλες. Το alert που έχει μια αρκετά υψηλή τιμή, και που θεωρείται ένα "**security-relevant system event**" στο οποίο η πολιτική ασφάλειας του συστήματος δεν πέτυχε ή αλλιώς παραβιάστηκε θεωρείται ως ένα incident (γεγονός). Εντούτοις υπάρχουν μερικά προβλήματα στη διάκριση των incidents από τα alerts.

Καταρχήν, τα γεγονότα είναι τα αποτελέσματα της ερμηνείας ενός αναλυτή των δεικτών. Οι αναλυτές παρατηρούν τα alerts που παράγονται από τις γεννήτριες γεγονότων. Ο ανθρώπινος εγκέφαλος είναι αυτός που αποφασίζει σχετικά με την τιμή. Η αναγνώριση-προσδιορισμός ενός incident είναι μια χειροκίνητη (manual) διαδικασία όπου ειδικευμένοι αναλυτές ασφάλειας πρέπει να παρατηρήσουν και να αναλύσουν την ασυνήθιστη δραστηριότητα. Το λογισμικό ανίχνευσης εισβολών "χτίζει" σχέδια μιας κανονικής χρήσης συστημάτων, που προκαλεί έναν συναγερμό (alert) οποτεδήποτε η χρήση φαίνεται ως ανώμαλη.

Επιπρόσθετα, καθώς το ποσό της κυκλοφορίας (traffic) σε ένα δίκτυο αυξάνεται, ο έλεγχος-παρακολούθηση (monitoring) της κυκλοφορίας και η απομόνωση των απειλών από την ομαλή δραστηριότητα γίνονται όλο και περισσότερο δύσκολα επιτεύξιμο.

Λόγω των προαναφερθέντων δυσκολιών, τα συστήματα ανίχνευσης εισβολών ενδεχομένως να επιστρέψουν το λανθασμένο αποτέλεσμα. Οι δύο ακόλουθοι τύποι λανθασμένων-ψευδών (false) αποτελεσμάτων μπορούν να εμφανιστούν.

Type I	False positive	An alarm is raised for something that is not really an attack.
Type II	False negative	Not raising an alarm for a real attack.

Πίνακας 1:Τύποι λαθών που μπορούν να εμφανιστούν, χρησιμοποιώντας ένα IDS

Οι **βαθμοί** (**degrees**) των false positives (ψευδώς θετικά) και των false negatives (ψευδώς αρνητικά) μαζί, αντιπροσωπεύουν την ***ευαισθησία του συστήματος***. Οι περισσότερες IDS εφαρμογές επιτρέπουν το συντονισμό της ευαισθησίας του συστήματος, είτε προς τη μια είτε προς την άλλη ευαισθησία. Οι τιμές αυτές των false positives και των false negatives, είναι στενά συνδεδεμένες με τους όρους ανάκληση (recall) και ακρίβεια (precision) αντίστοιχα. Ένας υψηλότερος βαθμός των false positives σημαίνει μια χαμηλότερη ακρίβεια, και αντίστροφα. Ένας υψηλότερος βαθμός των false negatives σημαίνει ότι η ανάκληση του IDS είναι χαμηλότερη.

Οι όροι, false positives και false negatives έχουν οριστεί-αναλυθεί και πιο πάνω στους στόχους των IDS (ακρίβεια).

4. Γενικό μοντέλο για την Ανίχνευση Εισβολών

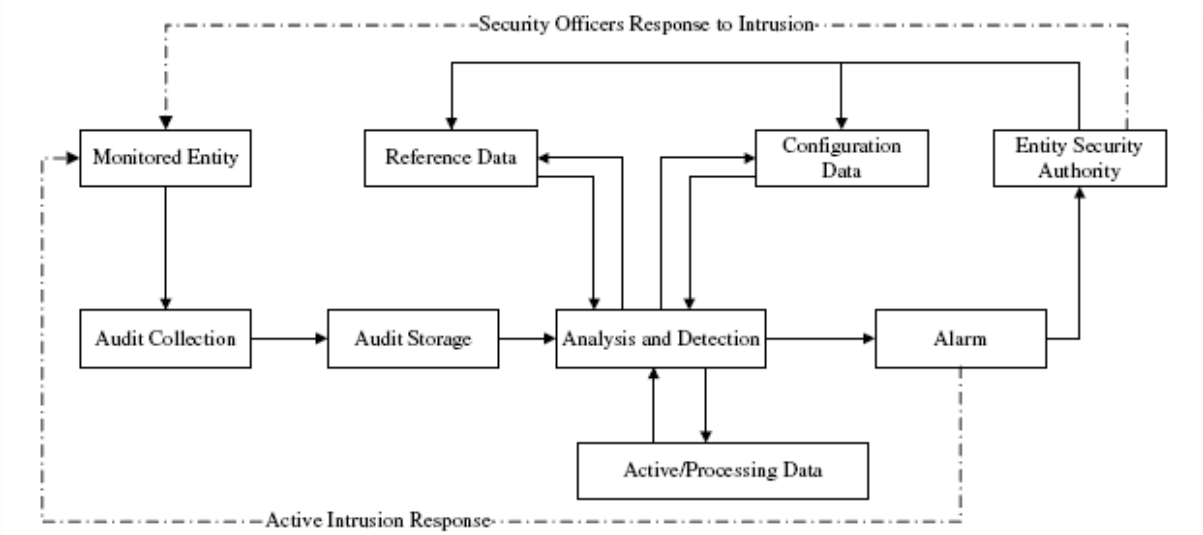
Προκειμένου να δράσει ένα σχήμα ανίχνευσης εισβολών σε οποιοδήποτε σύστημα, απαιτείται να καθορισθούν οι εξής γενικές παράμετροι:

i. ***Πηγές πληροφοριών / Information Sources***. Όπως αναφέρθηκε, τα συστήματα ανίχνευσης εισβολών παρακολουθούν και αναλύουν συμβάντα που λαμβάνουν χώρα στο πληροφοριακό σύστημα, προκειμένου να εντοπίσουν τις προσπάθειες εισβολής. Θα πρέπει έτσι να ορισθούν τα συμβάντα που θα παρακολουθούνται και τα αντίστοιχα συστήματα από τα οποία θα αντλούνται οι πληροφορίες αυτές. Οι πηγές πληροφοριών συνολικά κατατάσσονται σε τρεις κατηγορίες: α) *τα δίκτυα και δικτυακά στοιχεία / Network-based information gathering* β) *τους υπολογιστές / Host-based information gathering* και γ) *τις εφαρμογές / Application-based information gathering*.

ii. ***Τρόποι ανάλυσης πληροφοριών / Analysis***. Έχοντας συλλέξει τις σχετικές πληροφορίες από τις καθορισθείσες πηγές, το σύστημα ανίχνευσης εισβολών θα πρέπει να τις αξιολογήσει για να συμπεράνει αν τα καταγραφέντα συμβάντα συνιστούν επίθεση. Υπάρχουν τέσσερις τρόποι ανάλυσης των πληροφοριών: α) η *ανίχνευση κακής χρήσης-συμπεριφοράς / Signature or Misuse Detection*, που προσπαθεί να εντοπίσει συμβάντα τα οποία είναι γνωστό ότι εντάσσονται σε διαδικασίες επίθεσης, β) η *ανίχνευση διαταραχών-ανωμαλιών / Anomaly Detection*, που επιχειρεί να εντοπίσει συμπεριφορές συστημάτων που αποκλίνουν από το «φυσιολογικό», γ) η *ανίχνευση που βασίζεται στο μοντέλο προδιαγραφών / Specification-based detection*, όπου καθορίζει αν μια ακολουθία οδηγιών παραβιάζει ή όχι μια προδιαγραφή σχετικά με τον τρόπο τον οποίο πρέπει να εκτελείται ένα πρόγραμμα, ή ένα σύστημα με αποτέλεσμα να αναφέρει μια εισβολή και δ) το *υβριδικό μοντέλο / Hybrid or compound detection* όπου συνδυάζει τις παραπάνω προσεγγίσεις.

iii. ***Αντίδραση / Response***. Η παράμετρος αυτή καθορίζει το πώς θα αντιδράσει το σύστημα όταν διαπιστώσει ότι κάποια προσπάθεια εισβολής είναι εν εξελίξει ή ότι έχει ήδη πραγματοποιηθεί. Δύο διακριτές κατευθύνσεις είναι η παθητική αντίδραση, που κυρίως συνίσταται στην ενημέρωση των αρμοδίων και η ενεργός αντίδραση, η οποία ορίζει ότι το ίδιο το σύστημα ανίχνευσης εισβολών θα προσπαθήσει να αναχαιτίσει την επίθεση.

Στην παρακάτω εικόνα παρουσιάζεται ένα γενικευμένο μοντέλο ενός τυπικού Intrusion Detection System (***C**ommon **I**ntrusion **D**etection **F**ramework-**CIDF***).



Εικόνα 3: Γενικό μοντέλο τυπικού Intrusion Detection System

Συγκεκριμένα στην εικόνα αυτή τα ενιαία βέλη υποδηλώνουν το data/control flow ενώ τα βέλη με κουκίδες την απόκριση σε μια δράση εισβολής. Ένα τέτοιο μοντέλο περιλαμβάνει τα παρακάτω δομικά στοιχεία:

- ***Audit data collection:*** Αυτή η ενότητα χρησιμοποιείται στη φάση συλλογής δεδομένων ελέγχου (audit data collection). Τα δεδομένα που συλλέγονται σε αυτήν την φάση αναλύονται από τον αλγόριθμο ανίχνευσης εισβολών για να βρουν τα ίχνη ύποπτης δραστηριότητας. Η πηγή των στοιχείων μπορεί να είναι host/network activity logs, command-based logs, application-based logs, κλπ.

- ***Audit data storage:*** Τα τυπικά συστήματα ανίχνευσης εισβολών αποθηκεύουν τα δεδομένα ελέγχου (audit data) είτε κατά τρόπο αόριστο είτε για αρκετά μεγάλο χρονικό διάστημα για μετέπειτα αναφορά. Ο όγκος των δεδομένων είναι συχνά υπερβολικά μεγάλος. Ως εκ τούτου, το πρόβλημα της μείωσης δεδομένων ελέγχου είναι ένα σημαντικό ερευνητικό ζήτημα στο σχέδιο των συστημάτων ανίχνευσης εισβολών.

- ***Analysis and detection:*** Η επεξεργασία είναι η καρδιά ενός συστήματος ανίχνευσης εισβολών. Εδώ είναι που οι αλγόριθμοι ανιχνεύουν τις ύποπτες δραστηριότητες οι οποίες εφαρμόζονται. Οι αλγόριθμοι για την ανάλυση και την ανίχνευση (analysis and detection) των εισβολών έχουν ταξινομηθεί παραδοσιακά σε τρεις ευρείες κατηγορίες: ανίχνευση υπογραφών (ή κακής χρήσης)/signature (or misuse) detection, ανίχνευση ανωμαλιών/anomaly detection και υβριδική ανίχνευση/hybrid (or compound) detection.

- ***Configuration data:*** Τα δεδομένα διαμόρφωσης αποτελούν το πιο ευαίσθητο μέρος ενός συστήματος ανίχνευσης εισβολών. Περιέχει πληροφορίες που είναι σχετικές με τη λειτουργία του ίδιου του συστήματος ανίχνευσης εισβολών όπως πληροφορίες για πώς και πότε να συλλέξουν τα δεδομένα ελέγχου, πώς να αποκριθούν στις εισβολές, κλπ.
- ***Reference data:*** Η ενότητα αποθήκευσης δεδομένων αναφοράς (reference data) αποθηκεύει πληροφορίες για γνωστές υπογραφές εισβολών (στην περίπτωση της ανίχνευσης υπογραφών/signature detection) ή τα προφίλ κανονικής συμπεριφοράς (στην περίπτωση της ανίχνευσης ανωμαλιών/anomaly detection). Στην τελευταία περίπτωση, τα προφίλ ενημερώνονται όταν νέα γνώση για τη συμπεριφορά του συστήματος είναι διαθέσιμη.
- ***Active/processing data:*** Το στοιχείο επεξεργασίας πρέπει να αποθηκεύει συχνά ενδιάμεσα αποτελέσματα όπως πληροφορίες σχετικές με τις μερικώς εκπληρωμένες υπογραφές εισβολών.
- ***Alarm:*** Αυτό το μέρος του συστήματος χειρίζεται την έξοδο-παραγωγή (output) από το σύστημα ανίχνευσης εισβολών. Η έξοδος μπορεί να είναι είτε μια αυτοματοποιημένη απάντηση (response) σε μια εισβολή είτε ένας συναγερμός (alert) μιας ύποπτης δραστηριότητας για έναν υπάλληλο ασφάλειας συστημάτων.

ΚΕΦΑΛΑΙΟ 3ο

ΑΡΧΙΤΕΚΤΟΝΙΚΗ ΣΥΣΤΗΜΑΤΩΝ ΑΝΙΧΝΕΥΣΗΣ ΕΙΣΒΟΛΩΝ

Ένα ιδιαίτερα σημαντικό ζήτημα σε σχέση με την αρχιτεκτονική είναι το αν θα «**συστεγάζεται**» η παρακολουθούμενη οντότητα και το σύστημα ανίχνευσης εισβολών στην ίδια υπολογιστική πλατφόρμα ή θα χρησιμοποιούνται διακριτά συστήματα. Για παράδειγμα, προκειμένου να παρακολουθούμε ένα σύστημα βάσης δεδομένων θα μπορούσαμε να εγκαταστήσουμε το σύστημα ανίχνευσης εισβολών στον ίδιο τον εξυπηρετητή βάσεων δεδομένων ή σε ένα ξεχωριστό σύστημα. Η συστέγαση παρουσιάζει το ιδιαίτερα σημαντικό πλεονέκτημα ότι έχει σαφώς μικρότερο κόστος, καθώς δεν απαιτεί την αγορά πρόσθετου εξοπλισμού. Αυτό είναι ιδιαίτερα σημαντικό στις περιπτώσεις όπου έχουμε εγκαταστάσεις με μεγάλους υπολογιστές, οι οποίοι είναι εξαιρετικά δαπανηροί. Από την άλλη πλευρά, εγκαθιστώντας το σύστημα ανίχνευσης εισβολών στην ίδια πλατφόρμα με το υπό παρακολούθηση σύστημα μειώνεται η παρεχόμενη ασφάλεια, καθώς αν ο εισβολέας κατορθώσει να «*σπάσει*» το σύστημα έχει τη δυνατότητα να απενεργοποιήσει συνολικά το σύστημα ανίχνευσης εισβολών. Αντίθετα, αν το σύστημα ανίχνευσης εισβολών είναι εγκατεστημένο σε διακριτό υπολογιστικό σύστημα, ο εισβολέας μπορεί να μην γνωρίζει καν την ύπαρξή του.

1. Στρατηγική Ελέγχου

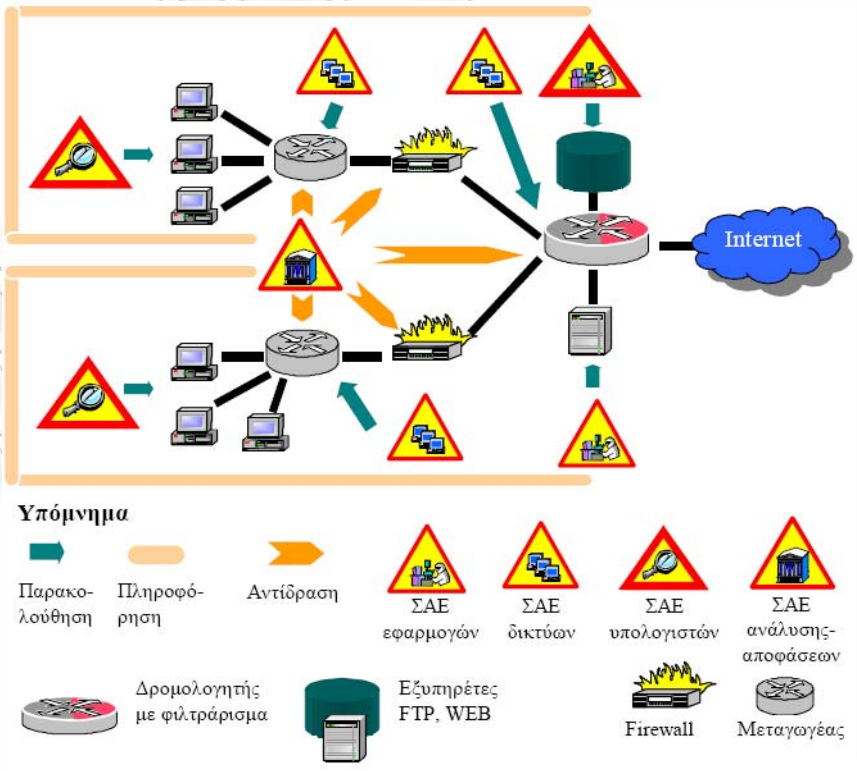
Πέραν του ζητήματος της συστέγασης ή όχι παρακολουθούμενου και συστήματος ανίχνευσης εισβολών, μία ακόμη βασική παράμετρος της αρχιτεκτονικής είναι η ***στρατηγική ελέγχου*** **(*Control Strategy*)**, δηλαδή η τοποθέτηση του σημείου όπου αναλύονται τα συμβάντα και λαμβάνονται οι αποφάσεις για τις πιθανές αντιδράσεις.

Η ***πρώτη προσέγγιση*** σχετικά με τη στρατηγική ελέγχου είναι η *συγκεντρωτική στρατηγική ελέγχου* ***(Centralized)***. Σύμφωνα με τη στρατηγική αυτή, τα συμβάντα που συλλέγονται από την παρακολούθηση προωθούνται σε έναν κεντρικό κόμβο του συστήματος

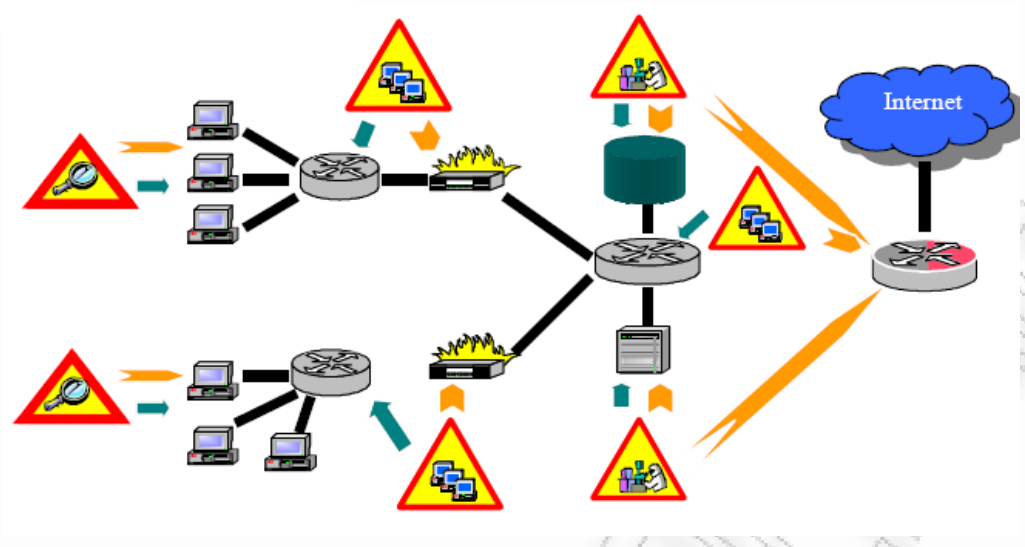
ανίχνευσης εισβολών, ο οποίος μεριμνά για την ανάλυσή τους και την τυχόν λήψη μέτρων. Κατά προτίμηση, η διακίνηση των στοιχείων για τα συμβάντα πρέπει να γίνεται από ξεχωριστό επικοινωνιακό κανάλι από αυτό που διακινούνται τα λειτουργικά δεδομένα του πληροφοριακού συστήματος, ή, αν αυτό κριθεί ιδιαίτερα δαπανηρό, η διακίνηση των στοιχείων για τα συμβάντα πρέπει να είναι κρυπτογραφημένη (Εικόνα 3).

Η ***δεύτερη προσέγγιση*** σε σχέση με τη στρατηγική ελέγχου είναι ο *πλήρως αποκεντρωμένος έλεγχος* ***(Fully Distributed)***. Στην προσέγγιση αυτή δεν υπάρχει Σύστημα Ανίχνευσης Εισβολών ανάλυσης-αποφάσεων, αλλά το κάθε Σύστημα Ανίχνευσης Εισβολών που συλλέγει τις πληροφορίες είναι επίσης υπεύθυνο για την ανάλυσή τους και τα διαμόρφωση των αντιδράσεων (Εικόνα 4).

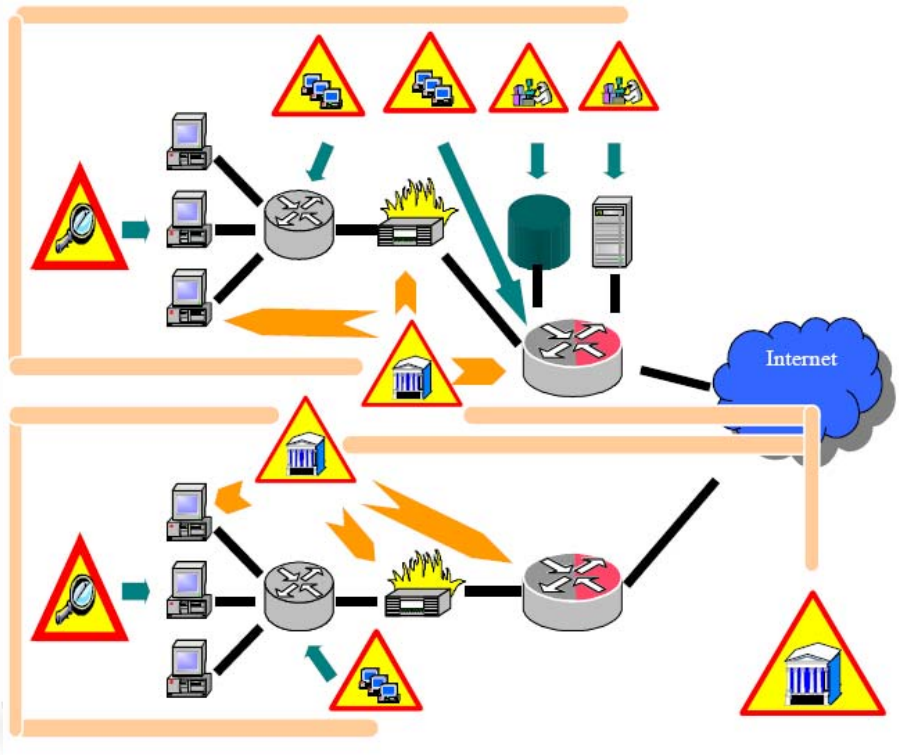
Η ***τρίτη προσέγγιση*** στη στρατηγική ελέγχου είναι ο *ημιαποκεντρωμένος έλεγχος* ***(Partially Distributed)***. Σύμφωνα με την προσέγγιση αυτή, τα παρακολουθούμενα συστήματα κατατμώνται σε διάφορες ζώνες, και σε κάθε ζώνη τοποθετείται ένα σύστημα ανίχνευσης εισβολών ανάλυσης-αποφάσεων, το οποίο πληροφορείται σχετικά με τα συμβάντα της ζώνης αυτής, αναλύει τις πληροφορίες και λαμβάνει τις σχετικές αποφάσεις. Είναι επίσης δυνατόν να υπάρχει και ένα «κεντρικό» σύστημα ανίχνευσης εισβολών, το οποίο πληροφορείται από τα συστήματα ανίχνευσης εισβολών ανάλυσης-αποφάσεων των διαφόρων ζωνών σχετικά με τα πιο αξιοσημείωτα συμβάντα ή για συμβάντα τα οποία πρέπει να αναλυθούν συνδυαστικά για όλες τις ζώνες (Εικόνα 5).



Εικόνα 4: Συγκεντρωτική στρατηγική ελέγχου



Εικόνα 5: Πλήρως αποκεντρωμένη στρατηγική ελέγχου



Εικόνα 6: Ημιαποκεντρωμένη στρατηγική ελέγχου

2. Χρονισμός της Ανάλυσης

Σε σχέση με το ***πότε*** αναλύονται οι πληροφορίες που συλλέγονται από ένα σύστημα ανίχνευσης εισβολών ακολουθούνται γενικά οι εξής δύο πρακτικές:

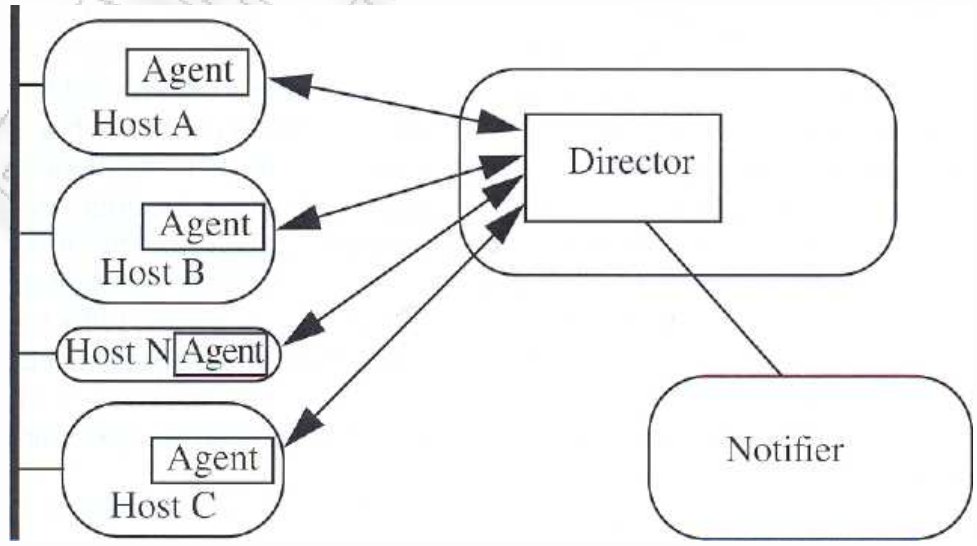
i. ***Ανάλυση σε πραγματικό χρόνο (real time-continuous)***. Οι συλλεγόμενες πληροφορίες αναλύονται αμέσως μόλις παραληφθούν. Προϋπόθεση για μία τέτοια προσέγγιση είναι δίκτυα με μεγάλες ταχύτητες και ισχυροί υπολογιστές, καθώς η ταχύτητα διακίνησης και

ανάλυσης των σχετικών πληροφοριών πρέπει να είναι μεγαλύτερη από την ταχύτητα γέννησής τους. Η προσέγγιση αυτή παρέχει δυνατότητα για άμεση αντίδραση.

ii. ***Περιοδική ή μαζική ανάλυση (interval based-batch mode)***. Οι συλλεγόμενες πληροφορίες αποθηκεύονται σε αρχεία καταγραφής, τα οποία αναλύονται μαζικά σε περιόδους που κρίνονται πιο κατάλληλες, π.χ. περιόδους ελαττωμένου υπολογιστικού ή δικτυακού φορτίου. Η προσέγγιση αυτή είναι ιδιαίτερα βολική όταν η παρακολουθούμενη οντότητα και το σύστημα ανίχνευσης εισβολών φιλοξενούνται στην ίδια υπολογιστική πλατφόρμα, καθώς η ανάλυση σε πραγματικό χρόνο θα είχε επιπτώσεις στις επιδόσεις του συστήματος, από την άλλη πλευρά όμως η προσέγγιση αυτή στερεί τη δυνατότητα άμεσης αντίδρασης.

3. Αρχιτεκτονική-Μηχανισμοί Ελεγκτικής Παρακολούθησης

Ένα σύστημα ανίχνευσης εισβολών αποτελεί ταυτόχρονα και ένα *αυτοματοποιημένο μηχανισμό παρακολούθησης και ελέγχου* (*auditing*). Όπως όλοι οι μηχανισμοί ελεγκτικής παρακολούθησης, αποτελείται από τρία μέρη (Εικόνα 7). Ο ***αντιπρόσωπος*** **(*agent*)** αντιστοιχεί στον logger: αποκτά πληροφορίες από ένα στόχο, όπως ένα υπολογιστικό σύστημα. Ο ***διευθυντής*** (***director***) αντιστοιχεί στον αναλυτή: αναλύει τα δεδομένα που προέρχονται από τους αντιπροσώπους όπως απαιτείται, με σκοπό να προσδιορίσει εάν μία επίθεση είναι σε εξέλιξη ή έχει ήδη συμβεί. Ο διευθυντής μεταδίδει την πληροφορία στον ***αγγελιοφόρο*** **(*notifier*),** ο οποίος αποφασίζει πότε και πώς να ειδοποιήσει την αναγκαία οντότητα. Ο αγγελιοφόρος μπορεί να επικοινωνήσει με τους αντιπροσώπους για να ρυθμίσει θέματα εισαγωγής στοιχείων, αν αυτό κριθεί απαραίτητο.



Εικόνα 7: Μηχανισμοί ελεγκτικής παρακολούθησης

Οι Hosts A, B, and C είναι γενικής χρήσης υπολογιστές, και οι Agents παρακολουθούν (monitor) τη δραστηριότητα σε αυτούς. Ο Host N έχει σχεδιαστεί για την παρακολούθηση των δικτύων, και ο Agent αναφέρει τα δεδομένα που συλλέγονται από το δίκτυο στον Director

3.1. Ο Αντιπρόσωπος – Agent

Ένας αντιπρόσωπος αποκτά πληροφορίες από μία πηγή δεδομένων, ή ένα σύνολο πηγών δεδομένων (data source or set of data source). Η πηγή αυτή μπορεί να είναι ένα ***αρχείο καταγραφής*** (***log file***), κάποια άλλη ***διεργασία*** ή ένα ***δίκτυο υπολογιστών***. Όταν ζητηθεί η πληροφορία, αυτή μπορεί να σταλεί απευθείας στο διευθυντή. Συνήθως, όμως η πληροφορία επεξεργάζεται σε κάποια συγκεκριμένη μορφοποίηση ώστε να απαλλάξει το διευθυντή από τη δραστηριότητα αυτή. Επίσης, ο αντιπρόσωπος μπορεί να απορρίψει πληροφορίες που θεωρεί μη σχετικές.

Ο διευθυντής μπορεί να θεωρήσει ότι χρειάζεται περισσότερη πληροφορία από κάποια συγκεκριμένη πηγή (information source). Σε αυτή την περίπτωση, μπορεί να καθοδηγήσει τον αντιπρόσωπο να συλλέξει πρόσθετα στοιχεία ή να επεξεργαστεί με διαφορετικό τρόπο τα στοιχεία που συλλέγει. Ο διευθυντής μπορεί να λάβει σχετική απόφαση για να ελαττώσει την απαιτούμενη επεξεργασία, αλλά μπορεί επίσης και να ζητήσει αύξηση του επιπέδου της πληροφορίας που λαμβάνεται όταν υποψιάζεται ότι υπάρχει επίθεση.

Ένας αντιπρόσωπος μπορεί να συλλέξει πληροφορίες από ένα μοναδικό υπολογιστή, από ένα σύνολο υπολογιστών, ή από ένα δίκτυο (single host, set of hosts or network). Στις επόμενες παραγράφους εξετάζονται τα είδη της πληροφορίας που είναι διαθέσιμα στην καθεμία περίπτωση, καθώς και ο τρόπος που αυτά μπορούν να συλλεχθούν.

Παρακάτω κατατάσσουμε τα ***Συστήματα Ανίχνευσης Εισβολών βάση της πηγής πληροφορίας (data source)*** *που μπορούν να συλλέξουν*.

3.1.1 Συλλογή Πληροφοριών Βασισμένη στον Υπολογιστή (Host-based Information Gathering)

Οι βασισμένοι στον υπολογιστή αντιπρόσωποι συνήθως χρησιμοποιούν τα αρχεία καταγραφής (logs) συστήματος και εφαρμογής για να αντλήσουν εγγραφές γεγονότων και να τις αναλύσουν ώστε να καθορίσουν τα στοιχεία που πρέπει να μεταβιβάσουν στο διευθυντή.

Ουσιαστικά, τα ***host-based συστήματα*** ψάχνουν για ίχνη εισβολής στο τοπικό σύστημα του host. Χρησιμοποιούν συχνά το μηχανισμό ελέγχου και **καταγραφή**ς (**auditing**) του host σαν πηγή πληροφοριών για ανάλυση. Πιο συγκεκριμένα ψάχνουν για ασυνήθη δραστηριότητα που περιορίζεται στον τοπικό host, όπως **logins**, παράξενη πρόσβαση σε αρχεία, μη εγκεκριμένη αύξηση δικαιωμάτων ή μετατροπές σε δικαιώματα του συστήματος. Η συγκεκριμένη αρχιτεκτονική χρησιμοποιεί μηχανισμούς βασισμένους σε κανόνες για την ανάλυση της δραστηριότητας. Για παράδειγμα, ένας τέτοιος κανόνας μπορεί να είναι ο εξής: δυνατότητα για πρόσβαση στο λογαριασμό root (διαχειριστή) είναι δυνατή μόνο μέσω της εντολής su. Συνεπώς, επιτυχημένες προσπάθειες πρόσβασης στο λογαριασμό root θα μπορούσαν να θεωρηθούν ως επίθεση.

Μία παραλλαγή της συλλογής πληροφοριών βασισμένης στον υπολογιστή εμφανίζεται όταν ο αντιπρόσωπος παράγει μόνος του τις πληροφορίες. Η διαδικασία αυτή πραγματοποιείται από τους ελεγκτές της πολιτικής (policy checkers). Οι ελεγκτές πολιτικής αναλύουν την κατάσταση του συστήματος ή την κατάσταση κάποιων συγκεκριμένων αντικειμένων του συστήματος και μεταχειρίζονται τα αποτελέσματα ως να είναι αρχεία καταγραφής για να τα μειώσουν και ακολούθως να τα διαβιβάσουν.

Όσον αφορά την εγκατάσταση ενός host-based IDS, θα πρέπει να σημειώσουμε ότι δεν είναι απαραίτητη η εκτέλεσή του πάνω στο παρακολουθούμενο υπολογιστικό σύστημα αλλά το IDS μπορεί να είναι εγκατεστημένο σε άλλο σύστημα και να προσπελαύνει τις πληροφορίες π.χ. μέσω αρχείων που προσαρτά με το πρωτόκολλο NFS, ή να τις λαμβάνει από το δίκτυο μέσω του πρωτοκόλλου SNMP.

Αν μία εταιρία επιλέξει την τεχνική των IDS συλλογής πληροφοριών από υπολογιστές για την προστασία του εταιρικού της υπολογιστικού περιβάλλοντος είναι σκόπιμο να ξεκινήσει την εγκατάσταση πρώτα από τους κρίσιμους εξυπηρέτες της και κατόπιν να προχωρήσει στους υπόλοιπους υπολογιστές. Αυτό θα δώσει και στο προσωπικό ασφάλειας τη δυνατότητα να εξοικειωθεί με το σύστημα όταν θα έχει εγκατασταθεί σε λίγους υπολογιστές, πριν κληθεί να διαχειρισθεί το σύστημα σε μεγάλη κλίμακα. Όταν IDS συλλογής πληροφοριών από υπολογιστές πρόκειται να εγκατασταθούν σε μεγάλο αριθμό υπολογιστών, αφ' ενός θα πρέπει να είναι της ίδιας τεχνολογίας, αφ΄ ετέρου δε θα πρέπει να χρησιμοποιηθεί IDS με αναφορά σε ένα κεντρικό σύστημα ανάλυσης-αποφάσεων, καθώς είναι πρακτικώς αδύνατο οι διαχειριστές να επισκέπτονται ξεχωριστά τα μηχανήματα και να ελέγχουν αν υπάρχει κάποιο πρόβλημα.

Πλεονεκτήματα

i. Τα host-based συστήματα μπορούν συχνά να λειτουργήσουν σε περιβάλλοντα όπου η δικτυακή κυκλοφορία είναι κρυπτογραφημένη, όταν παράγονται οι host-based πηγές πληροφοριών πριν την κρυπτογράφηση των δεδομένων ή/και αφότου γίνεται η αποκρυπτογράφηση των δεδομένων στον host του προορισμού

ii. Ένα host-based IDS μπορεί να αποτελέσει πολύ δυνατό εργαλείο ανάλυσης πιθανών επιθέσεων. Για παράδειγμα, είναι σε θέση μερικές φορές να πει τι ακριβώς έκανε ο εισβολέας, ποιες εντολές εκτέλεσε, ποια αρχεία έτρεξε και ποιες ρουτίνες του συστήματος κάλεσε αντί για μια αόριστη υπόθεση ότι προσπάθησε να εκτελέσει μια επικίνδυνη εντολή. Άρα τα host-based IDS συνήθως παρέχουν πολύ πιο λεπτομερείς και σχετικές πληροφορίες από ότι τα network-based IDS.

iii. Η χρήση τεχνικών μεταγωγής σε δικτυακό επίπεδο δεν επηρεάζει την κατηγορία αυτή των IDS, ενώ με ανάλυση των αρχείων καταγραφής ενεργειών μπορούν να αποκαλύψουν δούρειους ίππους ή άλλες προσπάθειες παραβίασης της ασφάλειας.

iv. Η δυνατότητά τους να ελέγξουν τα γεγονότα τοπικά σε έναν host, τα καθιστά ικανά να ανιχνεύουν τις επιθέσεις που δεν μπορούν να δουν τα network-based IDS.

v. Έχουν μικρότερους false positive ρυθμούς από ότι τα network-based. Αυτό συμβαίνει γιατί το εύρος των εντολών που εκτελούνται σε ένα συγκεκριμένο host είναι πολύ πιο εστιασμένο, παρά τα είδη της κίνησης πακέτων που ρέουν σε ένα δίκτυο. Αυτή η ιδιότητα μπορεί να μειώσει την πολυπλοκότητα των host-based μηχανισμών.

vi. Μπορούν να χρησιμοποιηθούν σε περιβάλλοντα όπου δεν χρειάζεται πλήρης ανίχνευση εισβολών ή όταν δεν υπάρχει διαθέσιμο bandwidth για επικοινωνία αισθητήρα–σταθμού ανάλυσης. Τα host-based IDS είναι πλήρως αυτοσυντηρούμενα, κάτι που τους επιτρέπει, σε κάποιες περιπτώσεις, να εκτελούνται από read-only μέσα. Έτσι, οι εισβολείς δύσκολα μπορούν να εξουδετερώσουν το IDS.

vii. Τέλος, σε ένα host-based σύστημα είναι ευκολότερο να σχηματιστεί μία ενεργή αντίδραση σε περίπτωση επίθεσης, όπως ο τερματισμός μιας υπηρεσίας ή το logging off ενός επιτιθέμενου χρήστη.

Μειονεκτήματα

i. Αυτά τα συστήματα είναι πολύ δυσκολότερα στη διαχείριση τους, δεδομένου ότι οι πληροφορίες πρέπει να διαμορφωθούν και να ρυθμιστούν για κάθε ελεγχόμενο host.

ii. Έχοντας μεμονωμένη εικόνα του κάθε υπολογιστή, είναι δύσκολο να εντοπισθούν επιθέσεις ή προσπάθειες ανίχνευσης σε ένα εταιρικό δίκτυο. Για παράδειγμα, η πραγματοποίηση αιτήσεων σύνδεσης στη θύρα 80 κάθε υπολογιστή ενός εταιρικού δικτύου είναι μία προφανής απόπειρα να εντοπισθούν οι υπολογιστές του εταιρικού δικτύου που προσφέρουν υπηρεσίες Web, παρ' όλα αυτά ένα IDS συλλογής πληροφοριών από υπολογιστές θα έχει εικόνα για έναν μόνο υπολογιστή και έτσι δεν θα μπορέσει να εντοπίσει την προσπάθεια ανίχνευσης.

iii. Τα host-based συστήματα απαιτούν εγκατάσταση στην συγκεκριμένη συσκευή που θέλουμε να προστατεύσουμε. Αν, για παράδειγμα έχουμε ένα server που πρέπει να τον προστατέψουμε θα πρέπει να εγκατασταθεί το IDS στον server αυτόν με ενδεχόμενα προβλήματα χωρητικότητας. Σε κάποιες περιπτώσεις, αυτό μπορεί να προκαλέσει και προβλήματα ασφαλείας μιας και το υπεύθυνο προσωπικό για την ασφάλεια του συστήματος ίσως να μην έχει πρόσβαση στον server όταν χρειαστεί.

iv. Ένα άλλο πρόβλημα είναι ότι έχουν την τάση να εξαρτώνται από το υπάρχον σύστημα καταγραφής (logging system) και ελέγχου του server. Εάν ο server δεν λειτουργεί έτσι ώστε η καταγραφή και ο έλεγχος να είναι σε ικανοποιητικό επίπεδο, θα πρέπει να γίνει αλλαγή στο configuration. Αυτό αποτελεί τεράστιο πρόβλημα αλλαγής στη διαχείριση του server.

v. Ακόμη, ένα τέτοιο σύστημα μπορεί να τεθεί εκτός λειτουργίας από ορισμένες επιθέσεις άρνησης υπηρεσιών, DoS (denial-of-service).

vi. Αυτά τα συστήματα είναι σχετικά ακριβά. Πολλοί οργανισμοί δεν έχουν την οικονομική δυνατότητα να προστατέψουν ολόκληρα δικτυακά τμήματα με τη χρήση network-based IDS. Αντίθετα, θα πρέπει να επιλέξουν ποια συστήματα θα προστατέψουν και ποια όχι. Αυτό το γεγονός αφήνει μεγάλα κενά στην κάλυψη της ανίχνευσης εισβολών στο δίκτυο, αφού ένας εισβολέας σε ένα γειτονικό, αλλά απροστάτευτο σύστημα μπορεί να υποκλέψει authentication πληροφορίες ή άλλο πολύτιμο υλικό από το δίκτυο.

Τέλος, τα host based IDS είναι πιο ευάλωτα, σε μεγαλύτερο ακόμα βαθμό από τοπικούς περιορισμούς. Αγνοούν εντελώς το περιβάλλον του δικτύου, άρα ο χρόνος ανάλυσης που απαιτείται για την εκτίμηση ζημιών από πιθανή εισβολή αυξάνει γραμμικά με τον αριθμό των host που προστατεύονται. Για παράδειγμα αν ένας άνθρωπος χρειάζεται τον χρόνο για να ερευνήσει ένα περιστατικό σε ένα σύστημα, θα χρειαστεί 2t για δύο συστήματα, 3t για τρία κοκ.

3.1.2 Συλλογή Πληροφοριών Βασισμένη στο Δίκτυο (Network-based Information Gathering)

Οι αντιπρόσωποι που προσανατολίζονται σε δίκτυα χρησιμοποιούν πληθώρα συσκευών και λογισμικού για να **καταγράψουν-παρακολουθήσουν (monitor)** την κυκλοφορία στο δίκτυο. Αυτή η τεχνική παρέχει πληροφορίες διαφορετικής μορφής σε σχέση με αυτές που παρέχει ο έλεγχος που βασίζεται στον υπολογιστή (host-based monitoring). Είναι δυνατή η ανίχνευση επιθέσεων προσανατολισμένων στο δίκτυο (network-oriented), όπως μια επίθεση άρνησης παροχής υπηρεσίας που προκαλείται από υπερφόρτωση δικτύου. Επίσης, η τεχνική αυτή μπορεί να ελέγξει την κυκλοφορία για ένα μεγάλο αριθμό υπολογιστών και να εξετάσει το περιεχόμενο της ίδιας της κυκλοφορίας, ενεργώντας παρακολούθηση περιεχομένου (content monitoring).

Οι αντιπρόσωποι που προσανατολίζονται σε δίκτυα (***network-based agents***) αξιοποιούν τεχνικές ***παρακολούθησης δικτύου*** (***network sniffing***) με σκοπό να μελετήσουν την κυκλοφορία στο δίκτυο. Στην περίπτωση αυτή, ένα σύστημα παρέχει στον αντιπρόσωπο πρόσβαση σε όλη την κυκλοφορία του δικτύου που διέρχεται από αυτόν τον υπολογιστή. Η κατανομή των αντιπροσώπων ελέγχου, με τρόπον ώστε να ελαχιστοποιείται ο αριθμός που απαιτείται για την παροχή πλήρους κάλυψης του δικτύου, αποτελεί ένα δύσκολο προς επίλυση πρόβλημα. Γενικά, η πολιτική ασφάλειας εστιάζει περισσότερο στους εισβολείς που εισέρχονται στο δίκτυο παρά στα εσωτερικά μέλη του δικτύου.

Τα δικτυακά IDS αποτελούν την πλειοψηφία των εμπορικών συστημάτων ανίχνευσης εισβολών. Τα συγκεκριμένα IDS ανιχνεύουν τις επιθέσεις με τη σύλληψη και την ανάλυση των δικτυακών πακέτων.

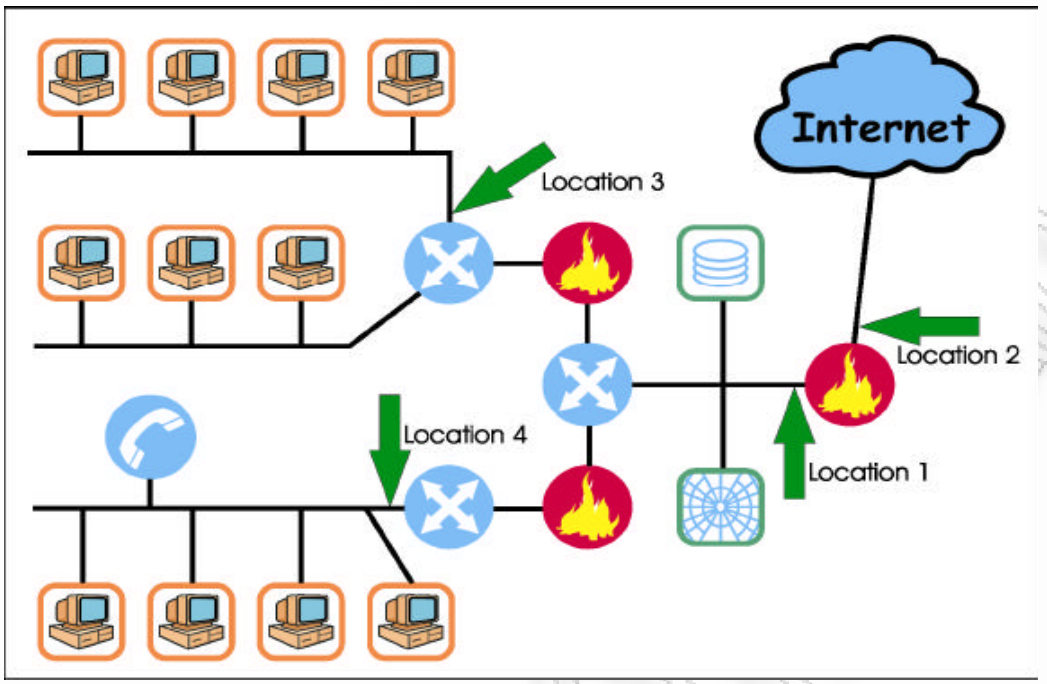
Το δικτυακό IDS συνήθως αποτελείται από δύο μέρη: τους ***αισθητήρες*** (***sensors***) και τον ***σταθμό διαχείρισης/ανάλυσης*** (***analysis and detection station)***. Ο αισθητήρας βρίσκεται σε ένα τομέα του δικτύου και παρακολουθεί για ύποπτη κίνηση. Ο σταθμός διαχείρισης λαμβάνει τις ενδείξεις κινδύνου από τους αισθητήρες και τις μεταβιβάζει στον administrator του συστήματος.

Οι αισθητήρες είναι συνήθως συστήματα που υπάρχουν μόνο για να παρακολουθούν το δίκτυο. Έχουν ένα δικτυακό interface που αναλύει τα πάντα, δηλαδή λαμβάνουν όλη την δικτυακή κίνηση, όχι μόνο ότι προορίζεται για τη δικιά τους IP διεύθυνση, αλλά και το διερχόμενο από αυτούς traffic με σκοπό την περαιτέρω ανάλυση. Αν ανιχνεύσουν κάτι ύποπτο το μεταβιβάζουν στον σταθμό διαχείρισης/ανάλυσης.

Ο σταθμός διαχείρισης/ανάλυσης μπορεί να δείξει τα σήματα κινδύνου, που έλαβε από τους αισθητήρες ή να πραγματοποιήσει επιπλέον ανάλυση.

Ένα επιπρόσθετο θέμα που αφορά την αρχιτεκτονική των συστημάτων ανίχνευσης εισβολών σχετικά με την πληροφορία που συλλέγουν από το δίκτυο είναι το ***που θα τοποθετηθούν*** *(Εικόνα 8)*, εντός της δικτυακής αρχιτεκτονικής ενός εταιρικού δικτύου. Έτσι, οι πιο διαδεδομένες πρακτικές παρουσιάζονται παρακάτω:

- *Πίσω από το εξωτερικό firewall (**Location 1**)*. Θεωρώντας δεδομένη την ύπαρξη ενός firewall που παρεμβαίνει μεταξύ του εταιρικού δικτύου και του διαδικτύου, η πρώτη επιλογή είναι να τοποθετείται το σύστημα ανίχνευσης εισβολών μεταξύ του firewall και του εταιρικού δικτύου. Η τοποθέτησή του στη θέση αυτή του δίνει τη δυνατότητα να ανιχνεύει επιθέσεις που ξεπερνούν την περιμετρική άμυνα (δηλαδή το firewall) και να αποκαλύπτει προβλήματα στη διαμόρφωση του firewall (π.χ. πακέτα που τελικά διέρχονται από το firewall ενώ δεν θα έπρεπε). Η συγκεκριμένη τοποθέτηση επιτρέπει επίσης την ανίχνευση επιθέσεων που στοχεύουν στους εξυπηρέτες δημόσιας πρόσβασης του εταιρικού δικτύου, όπως εξυπηρέτες Web και FTP, ενώ μπορεί επίσης να αποκαλύψει και την ύπαρξη επιθέσεων που επέτυχαν, καθώς πιθανότατα θα υπάρξει "εξερχόμενη" κυκλοφορία από το "θύμα" της επίθεσης, η οποία θα ανιχνευθεί από το σύστημα ανίχνευσης εισβολών.
- *Μπροστά από το εξωτερικό firewall (**Location 2**)*. Στην προσέγγιση αυτή το σύστημα ανίχνευσης εισβολών τοποθετείται πριν το εξωτερικό firewall με στόχο να ανιχνεύσει και να τεκμηριώσει το σύνολο των επιθέσεων που θα δεχθεί το εταιρικό δίκτυο από το διαδίκτυο. Η δυνατότητα αυτή δεν υπάρχει στην περίπτωση τοποθέτησης πίσω από το firewall, καθώς το firewall θα έχει ήδη "φιλτράρει" αρκετούς τύπους επιθέσεων.
- *Σε μεγάλους δικτυακούς κόμβους στο εσωτερικό του εταιρικού δικτύου (**Location 3**)*. Η τοποθέτηση αυτή υιοθετείται όταν κύριος στόχος είναι να ελεγχθούν όσο το δυνατόν περισσότεροι υπολογιστές του εσωτερικού δικτύου. Εποπτεύοντας μεγάλο μέρος της δικτυακής κυκλοφορίας είναι δυνατόν να ανιχνευθεί μεγάλο ποσοστό των πραγματοποιούμενων επιθέσεων, ενώ επίσης υπάρχει και η δυνατότητα ανίχνευσης επιθέσεων που πραγματοποιούνται από εσωτερικούς χρήστες.
- *Σε υποδίκτυα μεγάλης σημασίας (**Location 4**)*. Η επιλογή αυτή υιοθετείται συνήθως όταν υπάρχουν υποδίκτυα με μεγάλο βαθμό κρισιμότητας, π.χ. ένα υποδίκτυο που συγκεντρώνει τους εξυπηρέτες εφαρμογών, βάσεων δεδομένων και αρχείων μιας εταιρίας. Με τον τρόπο αυτό προστατεύονται οι πιο πολύτιμοι πόροι, και η προσέγγιση αυτή αποτελεί την πρώτη επιλογή όταν οι οικονομικοί πόροι για αγορά και χρήση IDS είναι περιορισμένοι.



Εικόνα 8: Τοπολογίες των Network-Based IDS αισθητήρων

Location 1: *Outside an external firewall,* ***Location 2:*** *Behind each external firewall, in the network DMZ,* ***Location 3:*** *On major network backbones,* ***Location 4:*** *On critical subnets*

Πλεονεκτήματα

i. Μερικά καλά τοποθετημένα δικτυακά συστήματα ανίχνευσης εισβολών μπορούν να ελέγχουν (monitor) ένα μεγάλο δίκτυο και να ανιχνεύουν κάποιες από τις επιθέσεις που χρησιμοποιούν αυτό το δίκτυο.

ii. Τα network-based συστήματα έχουν την τάση να είναι καλύτερα αυτοδιατηρούμενα από ότι τα host-based. Τρέχουν σε ένα συγκεκριμένο σύστημα και η εγκατάσταση τους είναι απλή σε μια τοποθεσία στο δίκτυο που δίνει τη δυνατότητα παρακολούθησης ευαίσθητης κίνησης δεδομένων, χωρίς εξουσιοδότηση ή κάποιων ειδών πρόσβασης με κατάχρηση προνομίων εξουσιοδότησης.

iii. Η υλοποίηση των network-based IDS επηρεάζουν σε μικρό βαθμό το ήδη υπάρχον δίκτυο, μιας και αυτά είναι συνήθως παθητικές συσκευές. Έτσι ένα δικτυακό IDS δεν απαιτεί μετατροπές στους server μιας επιχείρησης ή στους hosts για να εγκατασταθεί. Αυτό είναι μεγάλο όφελος, γιατί συνήθως οι servers έχουν μικρές ανοχές όσον αφορά τη CPU, το I/O και την χωρητικότητα του δίσκου. Η εγκατάσταση επιπλέον λογισμικού ίσως να δημιουργήσει προβλήματα λειτουργικότητας.

iv. Το IDS δεν αποτελεί κρίσιμο παράγοντα για την λειτουργικότητα του δικτύου, γιατί δεν λειτουργεί ως router ή κάποια άλλη κρίσιμη συσκευή. Άρα, τυχόν αποτυχία στο σύστημα

του IDS δε θα έχει σημαντική επίδραση στην επιχείρηση. Ένα επιπλέον όφελος είναι ότι πιθανότατα θα συναντήσουμε λιγότερη αντίδραση από ανθρώπους εντός του εργασιακού περιβάλλοντος. Ο κίνδυνος για τις υπάρχουσες κρίσιμες.

v. Τέλος, τα δικτυακά συστήματα ανίχνευσης εισβολών μπορούν να είναι αρκετά ασφαλή απέναντι στις επιθέσεις και ακόμη περισσότερο, αόρατα στους επιτιθέμενους-εισβολείς.

Μειονεκτήματα

i. Ένα network-based IDS απλά εξετάζει τη δικτυακή σύνδεση στον τομέα που είναι συνδεδεμένο και μόνο. Δεν μπορεί να ανιχνεύσει μία επίθεση που γίνεται σε διαφορετικό τμήμα του δικτύου. Το πρόβλημα αυτό γίνεται μεγαλύτερο σε ένα περιβάλλον με πολλαπλές δικτυώσεις Ethernet. Για να καλύψει τις ανάγκες του σε δικτυακή κάλυψη, ένας μεγάλος οργανισμός θα πρέπει να αγοράσει πολλούς αισθητήρες κάτι που σημαίνει επιπλέον κόστος.

ii. Ένα network-based IDS δεν μπορεί να αναλύσει κρυπτογραφημένες πληροφορίες. Το πρόβλημα αυτό γίνεται εντονότερο σε πολλές περιπτώσεις οργανισμών (και επιτιθέμενων) που χρησιμοποιούν τα εικονικά ιδιωτικά δίκτυα, **VPNs** (virtual private networks).

vi. Με την παρακολούθηση μόνο των δικτυακών πακέτων είναι εξαιρετικά δύσκολο να υπάρξει συμπέρασμα για το αν η επίθεση πέτυχε το στόχο της.

iii. Αν η δικτυακή επικοινωνία βασίζεται στη μεταγωγή, τότε η συλλογή του συνόλου της δικτυακής κυκλοφορίας είναι δύσκολη. Υπάρχουν ενεργά στοιχεία που παρέχουν μία θύρα παρακολούθησης (monitoring port), η οποία αναμεταδίδει όλα τα πακέτα που διέρχονται μέσα από το ενεργό στοιχείο, αλλά τα συγκεκριμένα μοντέλα είναι σαφώς πιο ακριβά από τα αντίστοιχα που δεν διαθέτουν τέτοια θύρα.

iv. Ένα σύστημα ανίχνευσης επιθέσεων μπορεί να χρειαστεί να μεταδώσει μεγάλες ποσότητες δεδομένων στο κεντρικό σύστημα ανάλυσης. Κάποιες φορές αυτό σημαίνει ότι οποιοδήποτε εξεταζόμενο πακέτο παράγει μία μεγαλύτερη ποσότητα κίνησης δεδομένων. Πολλά τέτοια συστήματα χρησιμοποιούν επιθετικές μεθόδους ελάττωσης δεδομένων για να μειώσουν την παραγόμενη κίνηση (traffic) επικοινωνίας. Επίσης, προωθούν αρκετές από τις διαδικασίες επιλογής ενέργειας στον αισθητήρα μόνο και χρησιμοποιούν το σύστημα ανάλυσης ως οθόνη της κατάστασης του δικτύου ή ως κέντρο επικοινωνίας, παρά για πραγματική ανάλυση. Το μειονέκτημα εδώ είναι ότι

παρέχεται ελάχιστος συντονισμός μεταξύ των αισθητήρων, δηλαδή οποιοσδήποτε αισθητήρας δεν γνωρίζει αν κάποιος άλλος έχει ανιχνεύσει μια επίθεση. Ένα τέτοιο σύστημα δεν μπορεί συνήθως να ανιχνεύσει συνεργατικές ή πολύπλοκες επιθέσεις.

v. Τα network-based IDS συνήθως χρησιμοποιούν ανάλυση signatures για να καλύψουν τις προδιαγραφές απόδοσης. Έτσι, ανιχνεύονται κοινές προγραμματισμένες επιθέσεις από εξωτερικές πηγές, αλλά αυτή η μέθοδος δεν είναι επαρκής για πιο πολύπλοκα είδη επιθέσεων. Αυτές απαιτούν καλύτερη ικανότητα για ανάλυση του περιβάλλοντος.

Τέλος, μερικά network-based IDS αντιμετωπίζουν προβλήματα όταν εμπλέκονται με network-based επιθέσεις που εμπλέκουν κατακερματισμένα πακέτα. Αυτά τα "κακοφτιαγμένα-malformed" πακέτα προκαλούν στα IDS αστάθεια και κατάρρευση.

3.1.3 Συλλογή Πληροφοριών Βασισμένη στις Πηγές Πληροφοριών-Εφαρμογές (Application-based Information Gathering)

Σκοπός του αντιπροσώπου είναι η παροχή πληροφοριών στο διευθυντή, ώστε εκείνος να είναι σε θέση να αναφέρει επιθέσεις, δηλαδή πιθανές παραβιάσεις της πολιτικής ασφάλειας (security policy). Κατά συνέπεια είναι απαραίτητη η συγκέντρωση της πληροφορίας. Ωστόσο, η πληροφορία μπορεί να μελετηθεί σε διάφορα επίπεδα.

Η διαφορά μεταξύ των όψεων επίπεδου εφαρμογής και συστήματος, ζήτημα το οποίο ουσιαστικά αποτελεί πρόβλημα επιπέδων αφαίρεσης, επηρεάζει το περιεχόμενο των πληροφοριών που θα στείλει ο αντιπρόσωπος στο διευθυντή και το συμπέρασμα που θα συνάγει ο διευθυντής μετά από την ανάλυση των πληροφοριών. Ο αντιπρόσωπος ή ο διευθυντής πρέπει είτε να λαμβάνουν την πληροφορία στο επίπεδο αφαίρεσης στο οποίο αναζητούν προβλήματα ασφάλειας, είτε να είναι σε θέση να αντιστοιχίζουν την πληροφορία στο κατάλληλο για αυτούς επίπεδο.

Τα IDS που είναι ***βασισμένα σε πηγές πληροφοριών και εφαρμογές***, αποτελούν υποσύνολο των host-based IDS τα οποία αναλύουν τα γεγονότα που συμβαίνουν μέσα σε μια εφαρμογή λογισμικού. Οι πιο κοινές πηγές πληροφοριών που χρησιμοποιούνται στην περίπτωση αυτή συνήθως είναι η παρακολούθηση αρχείων καταγραφής, ημερολογίων δοσοληψιών ή επικοινωνίας της εφαρμογής.

Η δυνατότητα της άμεσης διασύνδεσης της εφαρμογή, με τη σημαντική περιοχή ή την οριζόμενη από application-specific γνώση που περιλαμβάνεται στη μηχανή ανάλυσης, επιτρέπει στα ***application-based IDS*** να ανιχνεύσουν ύποπτες συμπεριφορές λόγω των

εξουσιοδοτημένων χρηστών όταν γίνεται υπέρβαση στην **εξουσιοδότησή (authorization)** τους. Αυτό συμβαίνει διότι τέτοια προβλήματα είναι πιθανότερο να εμφανιστούν στην αλληλεπίδραση μεταξύ του χρήστη, των δεδομένων στοιχείων, και της εφαρμογής.

Πλεονεκτήματα

i. Έχοντας αυξημένη γνώση για τη συγκεκριμένη εφαρμογή, μπορούν να διαγνώσουν μεγάλο πλήθος παραβιάσεων που θα ήταν αδύνατο από τα λιγότερο "εξειδικευμένα" IDS.

ii. Τέτοιου είδους IDS μπορούν να διαγνώσουν αρκετά αποτελεσματικά περιπτώσεις κατάχρησης δικαιωμάτων.

iii. Η λειτουργία τους δεν επηρεάζεται από τη χρήση κρυπτογράφησης στην επικοινωνία, καθώς είναι τοποθετημένα σε σημείο όπου και η μη κρυπτογραφημένη μορφή των πληροφοριών είναι διαθέσιμη.

Μειονεκτήματα

i. Από την άλλη πλευρά, μιας και τα application-based IDS ελέγχουν-παρατηρούν γεγονότα στο επίπεδο αφαίρεσης χρηστών, δεν μπορούν συνήθως να ανιχνεύσουν Δούρειους Ίππους (Trojan Horses) ή άλλα τέτοια κακόβουλα λογισμικά επιθέσεων. Επομένως, πρέπει οπωσδήποτε να συμπληρώνονται από πιο γενικά IDS (network or host-based), προκειμένου να προφυλάσσεται και το υπολογιστικό σύστημα που φιλοξενεί την εφαρμογή, πέρα από την ίδια την εφαρμογή.

Επίσης οι διαχειριστές πρέπει να ρυθμίσουν σωστά την ασφάλεια του περιβάλλοντος, καθώς τα αρχεία καταγραφής των εφαρμογών είναι συνήθως πλημμελέστερα προστατευμένα, σε σχέση με αυτά του Λειτουργικού Συστήματος και έτσι οι επιτιθέμενοι μπορεί να τα αλλοιώσουν πριν το IDS αξιοποιήσει τις πληροφορίες που κατεγράφησαν σε αυτά.

3.2. Ο Διευθυντής – Director

Ο διευθυντής έχει τη δυνατότητα περιορισμού των εισερχόμενων εγγραφών από το αρχείο καταγραφής για να εξαλείψει τις περιττές εγγραφές (redundant records), είτε αυτές είναι μη αναγκαίες, είτε είναι επικαλυπτόμενες με άλλες. Με τη χρήση μιας μηχανής ανάλυσης (analysis engine) καθορίζει εάν μια επίθεση (attack), ή ο πρόδρομος μιας επίθεσης (precursor of an attack), βρίσκεται σε εξέλιξη. Η μηχανή ανάλυσης μπορεί να χρησιμοποιήσει οποιαδήποτε τεχνική ή σύνολο τεχνικών για να εξάγει τα συμπεράσματα της.

Επειδή ο ρόλος του διευθυντή είναι κρίσιμος για την αποτελεσματικότητα του συστήματος ανίχνευσης εισβολών, το πρόγραμμα αυτό εκτελείται συνήθως σε ένα ξεχωριστό σύστημα. Αυτό επιτρέπει στο σύστημα να αφιερωθεί στη δραστηριότητα του διευθυντή. Παράπλευρο αποτέλεσμα αποτελεί το γεγονός ότι δεν είναι διαθέσιμοι στους απλούς χρήστες οι ειδικοί κανόνες και οι ***κατατομές*** τους (***profiles***). Επιπλέον, οι επιτιθέμενοι στερούνται τη γνώση που απαιτείται για να ξεφύγουν από το σύστημα ανίχνευσης εισβολών με την προσαρμογή στις γνωστές κατατομές ή τη χρησιμοποίηση μόνο των τεχνικών που οι κανόνες δεν περιλαμβάνουν. Επίσης, ο διευθυντής πρέπει να συσχετίζει πληροφορίες από πολλαπλά αρχεία (multiple logs).

Πολλοί τύποι διευθυντών τροποποιούν το σύνολο κανόνων που χρησιμοποιούν για τη λήψη αποφάσεων. Αυτοί οι αποκαλούμενοι ***προσαρμοστικοί διευθυντές*** (***adaptive directors***) αλλάζουν τις κατατομές, προσθέτουν ή αφαιρούν κανόνες, ή προσαρμόζονται στις αλλαγές των συστημάτων που παρακολουθούν. Οι τυπικοί προσαρμοστικοί διευθυντές ενσωματώνουν διάφορες θεωρητικές προσεγγίσεις μάθησης, με σκοπό να καθορίσουν τον τρόπο προσαρμογής της συμπεριφοράς τους.

Οι διευθυντές σπανίως χρησιμοποιούν μία μόνο τεχνική ανάλυσης, γιατί διαφορετικές τεχνικές τονίζουν διαφορετικές όψεις των εισβολών. Τα αποτελέσματα κάθε τεχνικής συνδυάζονται, αναλύονται και ακολούθως χρησιμοποιούνται.

3.3. Ο Αγγελιοφόρος – Notifier

Ο αγγελιοφόρος λαμβάνει την πληροφορία από το διευθυντή και δρομολογεί τις κατάλληλες ενέργειες. Σε κάποιες περιπτώσεις αποστέλλει απλώς μία ειδοποίηση προς τον υπεύθυνο ασφάλειας ότι μία επίθεση βρίσκεται σε εξέλιξη. Σε άλλες περιπτώσεις ο αγγελιοφόρος μπορεί να εκτελέσει κάποιες ενέργειες για να απαντήσει στις επιθέσεις.

Πολλά συστήματα ανίχνευσης εισβολών χρησιμοποιούν γραφικό περιβάλλον. Μία καλά σχεδιασμένη εικόνα γραφικών επιτρέπει στο σύστημα ανίχνευσης εισβολών να μεταβιβάσει την πληροφορία με μία σαφή εικόνα ή ένα σύνολο εικόνων. Η παραγόμενη εικόνα πρέπει να επιτρέπει στους χρήστες να προσδιορίζουν ποιες επιθέσεις βρίσκονται σε εξέλιξη. Στην ιδανική μορφή, θα πρέπει να παρέχεται κάποια σαφής ένδειξη για το πόσο πιθανό είναι να μην αποτελεί ψευδή συναγερμό, είτε θετικό είτε αρνητικό. Οι προαναφερθείσες απαιτήσεις οδηγούν στην αναγκαιότητα σχεδίασης ενός GUI με λιτότητα και σαφήνεια.

Ο αγγελιοφόρος μπορεί είτε να στείλει ένα ηλεκτρονικό μήνυμα στην κατάλληλη οντότητα, είτε να δημιουργήσει εγγραφές στα κατάλληλα αρχεία καταγραφής.

ΚΕΦΑΛΑΙΟ 4ο

ΤΕΧΝΙΚΕΣ ΑΝΑΛΥΣΗΣ ΣΥΜΒΑΝΤΩΝ-ΕΙΣΒΟΛΩΝ

Μία άλλη κατηγοριοποίηση των IDS γίνεται αντίστοιχα με την τεχνική που ανιχνεύονται και αναλύονται οι εισβολές.

Υπάρχουν 6 κατηγορίες εισβολών που απειλούν την ασφάλεια των πληροφοριακών συστημάτων ανεξάρτητα από την πηγή και είναι οι παρακάτω:

i. ***Προσπάθεια εισόδου (attempted break-ins)*** στο σύστημα, που ανιχνεύεται από τυπικά προφίλ συμπεριφοράς ή παραβιάσεις περιορισμών ασφαλείας.

ii. ***Κρυφή επίθεση (masquerade attacks)***, που ανιχνεύεται επίσης από τα τυπικά προφίλ συμπεριφοράς.

iii. ***Διείσδυση (penetration)*** στο σύστημα ελέγχου ασφαλείας, οι οποία ανιχνεύεται με συνεχή παρακολούθηση συγκεκριμένων προτύπων δραστηριότητας.

iv. ***Διαρροή (leakage)***, που γίνεται αντιληπτή με μια τυπική χρήση των πόρων του συστήματος.

v. ***DoS, Denial of Service (άρνηση της υπηρεσίας)***, που επίσης γίνεται αντιληπτή από χρήση πόρων του συστήματος.

vi. ***Κακόβουλη χρήση (malicious use)***, που ανιχνεύεται μέσω τυπικής συμπεριφοράς προφίλ, παραβιάσεων κανόνων ασφαλείας, ή με χρήση ειδικών προνομίων.

Τα συστήματα ανίχνευσης εισβολών προσδιορίζουν εάν κάποιες ενέργειες αποτελούν εισβολές, με βάση ένα ή περισσότερα μοντέλα εισβολών (models of intrusion). Ένα μοντέλο ταξινομεί μία ακολουθία καταστάσεων ή ενεργειών, ή χαρακτηρίζει καταστάσεις ή ενέργειες ως "καλές" (δηλαδή δεν υπάρχει εισβολή) ή "κακές" (δηλαδή υπάρχουν πιθανές εισβολές).

Τα μοντέλα ***κακής συμπεριφοράς*** (***misuse***) συγκρίνουν ενέργειες ή καταστάσεις με ακολουθίες που είναι ήδη γνωστό ότι αποτελούν εισβολές, ή με ακολουθίες που θεωρείται ότι αποτελούν εισβολές και τις ταξινομούν ως "κακές". Τα μοντέλα ***ανίχνευσης διαταραχών***

(***anomaly detection***) αποφαίνονται με βάση στατιστικά στοιχεία και ταξινομούν τις ενέργειες ή καταστάσεις που είναι στατιστικά ασυνήθιστες ως "κακές". Τα μοντέλα που ***βασίζονται στις προδιαγραφές*** (***specification-based***) ταξινομούν τις καταστάσεις που παραβιάζουν τις προδιαγραφές ως "κακές". Στην πράξη, συχνά τα μοντέλα είναι ένας ***συνδυασμός*** των παραπάνω μοντέλων (***compound-hybrid***) και τα συστήματα ανίχνευσης εισβολών χρησιμοποιούν συνδυασμό δύο ή τριών διαφορετικών τύπων μοντέλων. Τα μοντέλα μπορεί να είναι είτε *προσαρμοστικά* (*adaptive*) δηλαδή μοντέλα που αλλάζουν τη συμπεριφορά τους με βάση τις καταστάσεις και τις ενέργειες των συστημάτων, είτε *στατικά* (*static*) δηλαδή μοντέλα που αρχικοποιούνται από δεδομένα που έχουν συλλέγει και δεν τροποποιούνται κατά τη διάρκεια εκτέλεσης του συστήματος.

1. Μοντέλο Ανίχνευσης Κακής Συμπεριφοράς

Σε μερικά περιβάλλοντα, ο όρος ***κακή συμπεριφορά (misuse)*** αναφέρεται σε μια επίθεση από έναν εσωτερικό ή έναν εξουσιοδοτημένο χρήστη. Στα συστήματα ανίχνευσης εισβολών, ο όρος κακή συμπεριφορά αναφέρεται στη *βασισμένη-σε-κανόνες ανίχνευση*.

Η ανίχνευση κακής συμπεριφοράς (Signature or Misuse Detection, Knowledge-based Detection) προσδιορίζει εάν μία ακολουθία εντολών που εκτελείται παραβιάζει την πολιτική ασφάλειας των περιοχών στις οποίες εκτελείται. Σε αυτή την περίπτωση, περιγράφεται μία πιθανή εισβολή.

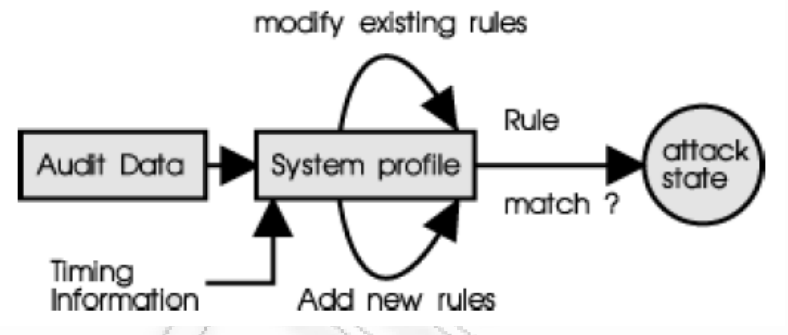
Η ανίχνευση κακής συμπεριφοράς απαιτεί γνώση όλων των ευπαθειών των συστημάτων ή των δυνητικών ευπαθειών που οι επιτιθέμενοι προσπαθούν να εκμεταλλευτούν. Το σύστημα ανίχνευσης εισβολών ενσωματώνει αυτή τη γνώση σε ένα σύνολο κανόνων (rule set). Όταν τα στοιχεία παρέχονται στο σύστημα ανίχνευσης εισβολών, αυτό εφαρμόζει το σύνολο κανόνων στα στοιχεία αυτά, ώστε να καθορίσει εάν κάποιες ακολουθίες στοιχείων ταιριάζουν με κάποιους από τους κανόνες. Σε καταφατική περίπτωση, συνάγεται ότι βρίσκεται σε εξέλιξη μια πιθανή εισβολή.

Η ιδέα πίσω από την misuse detection είναι ότι υπάρχουν τρόποι αναπαράστασης επιθέσεων με τη μορφή ενός προτύπου ή signature, ώστε ακόμα και παραλλαγές της επίθεσης να μπορούν να ανιχνευτούν. Άρα τα συστήματα αυτά μοιάζουν πολύ με τα antivirus προγράμματα, μπορούν να ανιχνεύσουν πολλά ή όλα τα γνωστά πρότυπα εισβολής, αλλά δεν είναι αποτελεσματικά σε άγνωστες τεχνικές επίθεσης.

Σημαντικό είναι να τονίσουμε πως τα anomaly detection συστήματα προσπαθούν να μαντέψουν το συμπλήρωμα της "κακής" συμπεριφοράς, ενώ τα misuse detection συστήματα

προσπαθούν να αναγνωρίσουν γνωστές "κακές" συμπεριφορές. Το σημαντικότερο ζήτημα στα misuse detection συστήματα είναι το πώς θα δημιουργήσουμε ένα signature που περιγράφουν όλες τις πιθανές παραλλαγές μιας σχετικής επίθεσης και πώς θα δημιουργήσουμε signatures που αγνοούν την μη επιθετική δραστηριότητα. Ένα σχηματικό παράδειγμα ενός τυπικού misuse detection συστήματος παρουσιάζεται στην παρακάτω .

Τα συστήματα ανίχνευσης εισβολών που βασίζονται σε κακή συμπεριφορά χρησιμοποιούν συνήθως έμπειρα συστήματα για να αναλύσουν τα στοιχεία και να εφαρμόσουν το σύνολο κανόνων. Τα συστήματα αυτά δεν μπορούν να ανιχνεύσουν επιθέσεις που είναι άγνωστες στους δημιουργούς του συνόλου κανόνων. Οι άγνωστες επιθέσεις που έχουν διεξαχθεί, ή και οι παραλλαγές γνωστών επιθέσεων, δύσκολα ανιχνεύονται. Πρόσφατα συστήματα ανίχνευσης εισβολών χρησιμοποίησαν προσαρμοστικές μεθόδους, περιλαμβάνοντας νευρωνικά δίκτυα (neural networks) και δίκτυα Petri (Petri nets) για να βελτιώσουν τις δυνατότητες ανίχνευσης.



Εικόνα 9: Ένα τυπικό σύστημα ανίχνευσης κακής συμπεριφοράς

Το σύστημα **IDIOT** (**I**ntrusion **D**etection **I**n **O**ur **T**ime) παρακολουθεί τα αρχεία καταγραφής (audit logs) ερευνώντας για κάποια ακολουθία γεγονότων που αντιστοιχεί σε μια επίθεση. Εναλλακτική προσέγγιση θα ήταν να αγνοηθούν οι καταστάσεις και το σύστημα να εστιάσει στις εντολές που τροποποιούν τις καταστάσεις αυτές. Οι ερευνητές στο University of California, Santa Barbara, έχουν σχεδιάσει διάφορα συστήματα που αναλύουν τα αποτελέσματα των εντολών που χρησιμοποιούνται για να παραβιάσουν μία πολιτική ασφάλειας.

Ένα σημαντικό χαρακτηριστικό γνώρισμα για τα συστήματα ανίχνευσης εισβολών είναι μια διεπαφή, από την οποία οι νέοι χρήστες ή συντηρητές του συστήματος μπορούν να προσθέσουν νέους κανόνες ή δεδομένα. Το **NFR** (**N**etwork **F**light **R**ecorder) αποτελεί κλασικό παράδειγμα.

Αξιολογώντας την τεχνική αυτή μπορούμε να πούμε τα παρακάτω:

- ☞ Η τεχνική της ανίχνευσης κακής συμπεριφοράς είναι πολύ αποτελεσματική τεχνική για ανίχνευση επιθέσεων, η οποία μάλιστα δεν παράγει πολλές ψευδείς αναφορές επιθέσεων.

- ☞ Έχει τη δυνατότητα να ανιχνεύσει έγκαιρα συγκεκριμένες επιθέσεις, ενδεχομένως και τα εργαλεία που χρησιμοποιούνται σ'αυτές, ώστε να θωρακιστεί το σύστημα, ενώ είναι κατάλληλη και για διαχειριστές χωρίς ιδιαίτερες τεχνικές γνώσεις.
- ☞ Από την άλλη πλευρά, τα εργαλεία που βασίζονται στην τεχνική της ανίχνευσης κακής συμπεριφοράς ανιχνεύουν μόνο τις επιθέσεις για τις οποίες γνωρίζουν (δηλαδή υπάρχουν στοιχεία στη βάση δεδομένων τους που αφορά τις γνωστές επιθέσεις), καθιστώντας έτσι απαραίτητη την τακτική ενημέρωση της βάσης δεδομένων αυτής με στοιχεία για νέες επιθέσεις.

Επίσης, τα περισσότερα εργαλεία δεν ανιχνεύουν παραλλαγές γνωστών επιθέσεων, κάτι που έχει σαφείς επιπτώσεις στην αποτελεσματικότητά τους.

2. Μοντέλο Ανίχνευσης Διαταραχών

Η ***Ανίχνευση Διαταραχών (Anomaly Detection, Behavior-based Detection)*** χρησιμοποιεί τη θεώρηση ότι η *απροσδόκητη συμπεριφορά (unexpected behavior)* αποτελεί τεκμήριο εισβολής. Προφανώς υπονοείται η ύπαρξη κάποιου μέτρου για το χαρακτηρισμό της συμπεριφοράς ενός χρήστη ή μιας διεργασίας (process) ως αναμενόμενης. Κάθε τέτοιο μέτρο αναφέρεται σε ένα υποκείμενο (subject) και ένα αντικείμενο (object).

Η τεχνική της ανίχνευσης διαταραχών (anomaly detection technique) αναλύει ένα σύνολο χαρακτηριστικών του συστήματος και συγκρίνει τη συμπεριφορά τους με ένα σύνολο αναμενόμενων τιμών (expected values). Ως αποτέλεσμα παρέχει πληροφορία κατά πόσο οι τιμές που υπολογίστηκαν (computed statistics) ταιριάζουν με τις αναμενόμενες μετρήσεις (expected measurements).

Μια προσέγγιση ανίχνευσης διαταραχών αποτελείται συνήθως από δύο φάσεις: τη ***φάση εκπαίδευσης*** (***training phase***) και τη ***φάση δοκιμασίας-ελέγχου*** (***testing phase***). Στην πρώτη φάση, καθορίζεται η κανονική κατατομή κυκλοφορίας (traffic profile) και στην δεύτερη, η γνωστή κατατομή (learned profile) εφαρμόζεται στα νέα δεδομένα.

2.1. Προϋπόθεση της ανίχνευσης διαταραχών

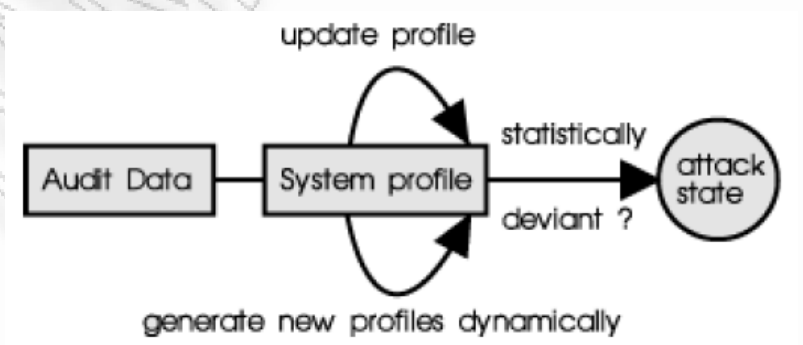
Η βασική ιδέα της ανίχνευσης διαταραχών είναι ότι η δραστηριότητα εισβολής (intrusive activity) είναι ένα υποσύνολο της ανώμαλης δραστηριότητας (anomalous activity). Εάν υποθέσουμε ότι ένας εισβολέας, ο οποίος δεν γνωρίζει το προφίλ της δραστηριότητας του νόμιμου χρήστη, εισβάλει host σύστημα, υπάρχει μια μεγάλη πιθανότητα η δραστηριότητα του

εισβολέα θα ανιχνευθεί ως ανώμαλη. Στην ιδανική περίπτωση, το σύνολο ανώμαλων δραστηριοτήτων θα είναι το ίδιο με το σύνολο δραστηριοτήτων εισβολής. Σε μια τέτοια περίπτωση, όλες οι ανώμαλες δραστηριότητες επισημαίνονται-σηματοδοτούνται (flagging) ως εισβολές οι οποίες οδηγούν σε μη ψευδώς θετικά (no false positives) και μη ψευδώς αρνητικά (no false negatives) σήματα. Εντούτοις, η δραστηριότητα εισβολής δεν συμπίπτει πάντα με την ανώμαλη δραστηριότητα. Έτσι έχουν προταθεί τέσσερις δυνατές πιθανότητες, κάθε μια με μια διαφορετική από το μηδέν πιθανότητα (non-zero probability):

- *Intrusive but not anomalous*: Εδώ μιλάμε για τα ***ψευδώς αρνητικά*** σήματα (***false negatives***) Ένα σύστημα ανίχνευσης εισβολών αποτυγχάνει να ανιχνεύσει αυτόν τον τύπο δραστηριότητας δεδομένου ότι η δραστηριότητα δεν είναι ανώμαλη.
- *Not intrusive but anomalous*: Αυτά είναι ***ψευδώς θετικά*** (***false positives***). Με άλλα λόγια, η δραστηριότητα δεν είναι παρεισφρητική, αλλά επειδή είναι ανώμαλη, ένα σύστημα ανίχνευσης εισβολών το εκθέτει όπως εισβολή.
- *Not intrusive and not anomalous*: Εδώ αναφερόμαστε στα ***αληθώς αρνητικά*** (***true negatives***). Η δραστηριότητα δεν είναι εισβολή και δεν αναφέρεται ως εισβολή.
- *Intrusive and anomalous*: Αυτά είναι ***αληθώς θετικά*** (***true positives***). Η δραστηριότητα είναι εισβολή και αναφέρεται ως τέτοια.

Όταν τα false negatives πρέπει να ελαχιστοποιηθούν, τα κατώτατα όρια που καθορίζουν μια διαταραχή θέτονται χαμηλά. Αυτό οδηγεί σε πολλά false positives και μειώνει την αποτελεσματικότητα των αυτοματοποιημένων μηχανισμών για την ανίχνευση εισβολών. Επιπλέον δημιουργεί πρόσθετο φόρτο εργασίας για το διαχειριστή της ασφάλειας, ο οποίος πρέπει να ερευνήσει κάθε γεγονός (incident) και να απορρίψει τις false positive περιπτώσεις.

Ένα σχηματικό παράδειγμα ενός τυπικού anomaly detection συστήματος είναι το παρακάτω:



Εικόνα 10: Ένα τυπικό σύστημα ανίχνευσης διαταραχών

Το κυριότερο στην ανίχνευση διαταραχών σε συστήματα ανίχνευσης επιθέσεων, είναι να γίνονται οι επιλογές στα επίπεδα των ορίων έτσι, ώστε κανένα από τα δύο προβλήματα (false

positives και false negatives) να μη μεγιστοποιείται. Σημαντική είναι, επίσης και η επιλογή των χαρακτηριστικών στην παρακολούθηση δεδομένων. Τα συστήματα ανίχνευσης διαταραχών είναι υπολογιστικά ακριβά, λόγω του κόστους του ελέγχου και της συνεχούς ανανέωσης (updating) των μετρικών του προφίλ ενός συστήματος.

Αποτιμώντας την τεχνική της ανίχνευσης ανωμαλιών, μπορούμε να σημειώσουμε ότι έχει τη δυνατότητα να ανιχνεύσει νέους τύπους επιθέσεων, στο βαθμό που αυτές θα προκαλέσουν αποκλίσεις τις κωδικοποιήσεις "κανονικής" συμπεριφοράς, ενώ έχουν επίσης τη δυνατότητα να παράγουν κανόνες που θα τροφοδοτούν τα συστήματα ανίχνευσης καταχρήσεων. Από την άλλη πλευρά όμως τείνουν να δημιουργούν ψευδείς αναφορές εισβολής, ενώ για τη δημιουργία των κωδικοποιήσεων "κανονικής συμπεριφοράς" απαιτούνται εκτεταμένα στοιχεία, συλλεγμένα από μακρά περίοδο λειτουργίας του συστήματος.

2.2. Τεχνικές που χρησιμοποιούνται στην ανίχνευση διαταραχών

Παρακάτω παρουσιάζονται μερικές αρχιτεκτονικές και μέθοδοι οι οποίες έχουν προταθεί για την ανίχνευση διαταραχών. Αυτές περιλαμβάνουν την στατιστική ανίχνευση (statistical anomaly detection), μέθοδοι βασισμένες στην πρόβλεψη προτύπων (predictive pattern generation) και τεχνικές βασισμένες στη χρήση των νευρωνικών δικτύων (neural networks).

2.1.1 Στατιστική Ανίχνευση

Στις στατιστικές μεθόδους για την ανίχνευση ανωμαλιών, το σύστημα παρατηρεί τη δραστηριότητα των υποκειμένων (subjects) και παράγει κατατομές (profiles) που αντιπροσωπεύουν τη συμπεριφορά τους (behavior). Το profile αυτό περιλαμβάνει χαρακτηριστικά μέτρα (measures) όπως το *μέτρο έντασης δραστηριότητας* (*activity intensity measure*), το *μέτρο κατανομής δεδομένων ελέγχου* (*audit record distribution measure*), τα *κατηγορικά μέτρα* (*categorical measures*), η κατανομή μιας δραστηριότητας πέρα από τις κατηγορίες, και *τακτικά μέτρα* (*ordinal measures*), όπως η χρήση της CPU. Τυπικά, δύο profiles διατηρούνται για το κάθε υποκείμενο: το τρέχον και το αποθηκευμένο. Όσο τα γεγονότα του συστήματος/δικτύου (audit log records, εισερχόμενα πακέτα, κ.α.) υποβάλλονται σε επεξεργασία (process), το σύστημα ανίχνευσης εισβολών αναβαθμίζει (update) το τρέχον profile και υπολογίζει περιοδικά ένα αποτέλεσμα διαταραχής (που δείχνει το βαθμό παρατυπίας/διαταραχής για το συγκεκριμένο γεγονός) συγκρίνοντάς το με το αποθηκευμένο, χρησιμοποιώντας μια συνάρτηση σχετική με την διαταραχή (function of abnormality) όλων των μέτρων μέσα στο profile. Εάν το αποτέλεσμα διαταραχής είναι υψηλότερο από ένα ορισμένο

κατώτατο όριο (threashold), το σύστημα ανίχνευσης εισβολών παράγει ένα συναγερμό (alert).

Στις ***στατιστικές μεθόδους*** για την ***ανίχνευση ανωμαλιών*** αναφέρονται ***τρία μοντέλα***:

i. Το *πρώτο μοντέλο* χρησιμοποιεί το ***Μετρικό Σύστημα Τιμών Κατωφλίου (Threshold Metric)***. Σύμφωνα με αυτό, αναμένεται να εμφανιστούν γεγονότα κατ' ελάχιστο m και κατά μέγιστο n, για κάποιο γεγονός και κάποιες τιμές m και n. Εάν κατά τη διάρκεια μιας συγκεκριμένης χρονικής περιόδου εμφανίζονται λιγότερα από m ή περισσότερα από n γεγονότα, τότε η συμπεριφορά θεωρείται ***διαταραγμένη (anomalous)***.

Ο καθορισμός των τιμών κατωφλίου αυξάνει την πολυπλοκότητα και συνεπώς τη χρήση του μοντέλου. Οι τιμές κατωφλίου πρέπει να λάβουν υπόψη τα χαρακτηριστικά των χρηστών και τα διαφορετικά επίπεδα εξειδίκευσης τους. Εάν για το παραπάνω παράδειγμα το n τεθεί στη τιμή 3 για ένα σύστημα στη Γαλλία και οι αρχικοί χρήστες αυτού του συστήματος ήταν στις ΗΠΑ, η διαφορά στα πληκτρολόγια θα προκαλούσε σημαντικό αριθμό αδικαιολόγητων συναγερμών (false alarms). Αν όμως το σύστημα βρισκόταν στις ΗΠΑ, θέτοντας το n ίσο με 3 η τιμή κατωφλίου θα ήταν απολύτως λογική. Μία λύση θα ήταν να συνδυαστεί αυτή η προσέγγιση με τα άλλα δύο μοντέλα, ώστε να προσαρμοστούν οι τιμές κατωφλίου στην παρατηρούμενη ή προβλεπόμενη συμπεριφορά των χρηστών.

ii. Το *δεύτερο μοντέλο* χρησιμοποιεί ***Στατιστικές Ροπές (Statistical Moments)***. Ο αναλυτής γνωρίζει το μέσο και την τυπική απόκλιση (οι δύο πρώτες ροπές) και πιθανότατα άλλα μέτρα συσχέτισης (ροπές υψηλότερης τάξης). Αν οι τιμές βρίσκονται εκτός του αναμενόμενου διαστήματος γι' αυτήν τη ροπή, η συμπεριφορά που αντιπροσωπεύουν οι τιμές θεωρείται διαταραγμένη (anomalous). Επειδή η κατατομή (profile) της περιγραφής του συστήματος μπορεί να εμπεριέχει καθυστερήσεις, τα μοντέλα ανίχνευσης διαταραχών (anomaly-based IDS) συνυπολογίζουν αυτές τις αλλαγές σταθμίζοντας (weighting) τα δεδομένα ή τροποποιώντας τους στατιστικούς κανόνες με βάση τους οποίους λαμβάνονται οι αποφάσεις.

Τα μοντέλα στατιστικών ροπών παρέχουν περισσότερη ευελιξία από τα μοντέλα τιμών κατωφλίου. Οι διαχειριστές μπορούν να τα ρυθμίσουν καλύτερα, ώστε να επιτυγχάνεται μεγαλύτερη διακριτότητα από τα μοντέλα τιμών κατωφλίου. Με την ευελιξία, όμως, που επιτυγχάνεται εμφανίζονται και προβλήματα πολυπλοκότητας. Συγκεκριμένα, μία υπόθεση εργασίας είναι ότι η συμπεριφορά τόσο των διεργασιών όσο και των χρηστών μπορούν να μοντελοποιηθούν στατιστικά. Αν αυτή η συμπεριφορά ταιριάζει με κάποια στατιστική κατανομή, όπως η κατανομή Gauss ή η κανονική κατανομή (Gaussian or normal distribution), ο προσδιορισμός των παραμέτρων απαιτεί πειραματικά δεδομένα που

μπορούν να ληφθούν από το σύστημα. Στην περίπτωση που δεν ταιριάζει, η ανάλυση πρέπει να χρησιμοποιήσει άλλες τεχνικές, όπως τη συστοιχία (clustering), ώστε να προσδιοριστούν τα χαρακτηριστικά, οι ροπές και οι τιμές που υποδεικνύουν μη κανονική συμπεριφορά. Ένα επιπλέον πρόβλημα είναι η δυσκολία του υπολογισμού αυτών των ροπών σε πραγματικό χρόνο.

iii. Το <u>*τρίτο μοντέλο*</u> είναι το ***Μαρκοβιανό μοντέλο (Markov model)***. Σύμφωνα με το μοντέλο αυτό ένα σύστημα εξετάζεται σε μία συγκεκριμένη χρονική στιγμή. Τα γεγονότα (events) που προηγήθηκαν χρονικά έχουν θέσει το σύστημα σε μια συγκεκριμένη κατάσταση. Όταν συμβεί το επόμενο γεγονός, το σύστημα μεταβαίνει σε μία νέα κατάσταση. Με την πάροδο του χρόνου μπορεί να αναπτυχθεί ένα σύνολο πιθανοτήτων μετάβασης. Όταν συμβεί ένα γεγονός που προκαλεί μία μετάβαση με μικρή πιθανότητα (low probability), το γεγονός κρίνεται διαταραγμένο (anomalous). Το μοντέλο προτείνει τη χρήση κάποιας κατάστασης (state), ή προϊστορίας (past history) για τον εντοπισμό των διαταραχών. Οι διαταραχές δεν είναι πλέον βασισμένες σε στατιστικά των περιστατικών μεμονωμένων γεγονότων, αλλά σε ακολουθίες γεγονότων. Αυτή η προσέγγιση δηλώνει εντοπισμό κακής συμπεριφοράς (misuse detection) και χρησιμοποιήθηκε για την ανάπτυξη αποτελεσματικών μηχανισμών εντοπισμού διαταραχών.

Η προσέγγιση αυτή ακολουθήθηκε στο σύστημα TIM της **DEC** (**D**igital **E**quipment **C**orporation's). Το σχήμα αυτό χρησιμοποιούσε μία τεχνική τεχνητής νοημοσύνης (artificial intelligence technique) αποκαλούμενη *επαγωγική εκμάθηση βασισμένη στο χρόνο* (*time-based inductive learning*). Στο σύστημα εισάγεται ένα γεγονός κάποιου τύπου για να προβλεφθεί. Το σύστημα αναπτύσσει ένα σύνολο προσωρινά συσχετισμένων συνθηκών που προβλέπει τη στιγμή κατά την οποία θα συμβεί το γεγονός στα πλαίσια ενός συνόλου.

Η αποτελεσματικότητα των Μαρκοβιανών μοντέλων εξαρτάται από την εγκυρότητα των δεδομένων που χρησιμοποιούνται, για την εγκατάσταση του μοντέλου. Αυτά τα δεδομένα, αποκαλούμενα συνήθως *δεδομένα εκμάθησης* (*training data*), αποκτώνται πειραματικά, συνήθως από πληθυσμούς που θεωρούνται κανονικής συμπεριφοράς (normal). Για παράδειγμα, το TIM μπορεί να αποκτήσει δεδομένα με την απλή παρατήρηση (monitoring) ενός εταιρικού συστήματος για την εγκατάσταση των σχετικών γεγονότων και των ακολουθιών τους. Οι Hofmeyer, Somayaji και Forest (οι οποίοι προσδιόρισαν την "κανονική συμπεριφορά" με όρους ακολουθιών κλήσεων συστήματος διαφορετικού μήκους, με την ονομασία "ίχνη") απέκτησαν ίχνη (traces) κλήσεων συστήματος από διεργασίες που εκτελούνταν σε κανονικό περιβάλλον. Αν αυτά τα δεδομένα εκμάθησης αντανακλούν με ακρίβεια στο περιβάλλον όπου θα εκτελεστεί το σύστημα ανίχνευσης

εισβολών και καλύπτουν όλες τις πιθανές κανονικές χρήσεις του συστήματος, τότε το μοντέλο θα λειτουργήσει αποδοτικά. Στην περίπτωση που τα δεδομένα εκμάθησης δεν ανταποκρίνονται στο συγκεκριμένο περιβάλλον, τα μοντέλα Markov θα παράγουν αδικαιολόγητες και άστοχες αναφορές (false reports) για διαταραγμένες συμπεριφορές.

Ένα θέμα ανοιχτό προς συζήτηση στη στατιστική προσέγγιση ειδικά, αλλά και στα συστήματα ανίχνευσης επιθέσεων γενικότερα, είναι η επιλογή των μετρικών-παραγόντων που θα παρακολουθούνται. Δεν είναι γνωστό ακόμη ποιο υποσύνολο των παραγόντων αυτών είναι σε θέση να προβλέψει ακριβώς τις δραστηριότητες εισβολής.

Στατικές μέθοδοι απόφασης συνήθως οδηγούν σε λάθος αποτέλεσμα λόγω της μοναδικότητας κάθε συστήματος.

Αυτός που φαίνεται πιο αποτελεσματικός είναι ο στατικός και δυναμικός, μαζί, συνδυασμός των μετρικών-παραγόντων. Προβλήματα που προκύπτουν από τη χρήση αυτής της τεχνικής λύνονται με χρήση άλλων μεθόδων όπως είναι η γενετική πρόβλεψη προτύπων, η οποία λαμβάνει υπόψη προηγούμενα γεγονότα κατά την ανάλυση των δεδομένων.

2.1.2 Πρόβλεψη προτύπων

Αυτή η μέθοδος ανίχνευσης εισβολών (***predictive pattern generation***) προσπαθεί να ***προβλέψει μελλοντικά γεγονότα*** με χρήση γεγονότων που ήδη έχουν συμβεί. Παραδείγματος χάριν, μπορούμε να θέσουμε τον εξής κανόνα:

$$E1 - E2 \rightarrow (E3 = 80\%, E4 = 15\%, E5 = 5\%)$$

Αυτό σημαίνει ότι με δεδομένα τα γεγονότα E1 και E2 και με το E2 να ακολουθεί το E1 στο χρόνο, υπάρχει 80% πιθανότητα να ακολουθήσει το γεγονός E3, 15 % να ακολουθήσει το E4 και 5% να ακολουθήσει το E5. Το πρόβλημα είναι ότι μερικά επιθετικά σενάρια που δεν έχουν προβλεφθεί από το σύστημα δε θα χαρακτηριστούν ως εισβολή. Δηλαδή, αν μια ακολουθία γεγονότων A-B-C υπάρχει και είναι εισβολή, αλλά δεν βρίσκεται στη βάση των κανόνων, θα καταχωρηθεί απλά ως άγνωστη. Αυτό το πρόβλημα μπορεί να λυθεί μερικώς με τον χαρακτηρισμό οποιοδήποτε αγνώστου γεγονότος ως εισβολή (αυξάνοντας έτσι τον αριθμό των false negatives). Στην φυσιολογική περίπτωση, ένα γεγονός χαρακτηρίζεται ως εισβολή εάν ταιριάζει με το αριστερό μέρος του κανόνα ανάλυσης και το δεξί μέρος είναι πολύ διαφορετικό από το αποτέλεσμα της πρόβλεψης.

Υπάρχουν πολλά πλεονεκτήματα σε αυτήν την προσέγγιση. Πρώτον, ακολουθιακά πρότυπα βασισμένα σε κανόνες μπορούν να ανιχνεύσουν ανώμαλες δραστηριότητες πολύ πιο εύκολα

από τις παραδοσιακές μεθόδους. Δεύτερο, τα συστήματα που κατασκευάζονται χρησιμοποιώντας αυτό το μοντέλο είναι ιδιαίτερα προσαρμόσιμα σε αλλαγές. Αυτό συμβαίνει γιατί τα λιγότερο καλά και αποτελεσματικά πρότυπα συνεχώς εξαλείφονται, ενώ παραμένουν μόνο τα πολύ ποιοτικά πρότυπα. Τρίτο, είναι πιο εύκολο να εντοπιστούν χρήστες που προσπαθούν να επηρεάσουν και να κατευθύνουν το σύστημα κατά τη διάρκεια που αυτό μαθαίνει. Τέταρτο και τελευταίο, οι ανώμαλες δραστηριότητες εντοπίζονται και αναφέρονται μέσα σε λίγα δευτερόλεπτα από τη στιγμή της λήψης της κρίσιμης πληροφορίας.

2.1.3 Νευρωνικά Δίκτυα

Μια διαφορετική προσέγγιση στα συστήματα εντοπισμού εισβολής είναι η χρήση ***νευρωνικών δικτύων (neural networks)***. Η ιδέα εδώ είναι να "εκπαιδεύσουμε" ένα νευρωνικό δίκτυο με τέτοιο τρόπο, ώστε να μπορεί να προβλέψει την επόμενη εντολή ή ενέργεια ενός χρήστη, με βάση προηγούμενες εντολές και ενέργειες. Το δίκτυο λειτουργεί με βάση ενός συνόλου εντολών, αντιπροσωπευτικών του χρήστη. Μετά την περίοδο εκμάθησης το δίκτυο προσπαθεί να ταιριάξει πραγματικές εντολές με το πραγματικό προφίλ του χρήστη, που ήδη υπάρχει στο δίκτυο. Όσα γεγονότα προβλεφθούν λάθος στην πραγματικότητα απεικονίζουν την διαφοροποίηση του χρήστη από το προφίλ του.

<u>*Κάποια πλεονεκτήματα των νευρωνικών δικτύων*</u> είναι ότι τα καταφέρνουν καλά με πολύπλοκα δεδομένα, η επιτυχία τους δεν εξαρτάται από καμία στατιστική υπόθεση για την φύση των δεδομένων και είναι πιο εύκολο να μετατραπούν για διαφορετικές ομάδες χρηστών. Όμως υπάρχουν και προβλήματα. Πρώτα, ένα μικρό σύνολο πληροφοριών θα οδηγήσει σε πολλά false positives, ενώ ένα μεγάλο σύνολο θα οδηγήσει σε άσχετα δεδομένα και στην αύξηση των false negatives. Δεύτερο, η τοπολογία του δικτύου αποφασίζεται μετά από πολλές διαδοχικές δοκιμές και λάθη. Τρίτο, ο εισβολέας μπορεί να "εκπαιδεύσει" το δίκτυο κατά την φάση εκμάθησης.

3. Μοντέλο βασισμένο στις Προδιαγραφές

Η ανίχνευση διαταραχών περιγράφηκε ως η τεχνική για την αναζήτηση ασυνήθιστων καταστάσεων. Η ανίχνευση κακής συμπεριφοράς αναφέρθηκε ως η τεχνική για την αναζήτηση των καταστάσεων που είναι γνωστό ότι είναι ανεπιθύμητες. Η ανίχνευση προδιαγραφών αναζητά καταστάσεις που είναι γνωστό ότι δεν είναι επιθυμητές και όταν το σύστημα

εισέρχεται σε μία τέτοια κατάσταση αναφέρει μία πιθανή εισβολή.

Η ανίχνευση που βασίζεται στις προδιαγραφές (Specification-based detection) καθορίζει εάν μια ακολουθία οδηγιών παραβιάζει ή όχι μια προδιαγραφή σχετικά με τον τρόπο με τον οποίο πρέπει να εκτελείται ένα πρόγραμμα, ή ένα σύστημα. Σε αυτή την περίπτωση, αναφέρει μια πιθανή εισβολή.

Για λόγους ασφάλειας πρέπει να προσδιοριστούν και να ελεγχθούν μόνον τα προγράμματα που αλλάζουν με κάποιον τρόπο την κατάσταση προστασίας των συστημάτων. Για παράδειγμα, επειδή ο συντάκτης πολιτικής (policy editor) των Windows NT αλλάζει τις ρυθμίσεις που σχετίζονται με την ασφάλεια, πρέπει να υπάρχει σχετική προδιαγραφή.

Η ανίχνευση εισβολών που βασίζεται στις προδιαγραφές βρίσκεται ακόμη στα αρχικά της στάδια. Μεταξύ των θετικών χαρακτηριστικών περιλαμβάνεται ο φορμαλισμός, σε ένα σχετικά χαμηλό επίπεδο, του γεγονότος το οποίο θα μπορούσε να συμβεί. Αυτό ακριβώς σημαίνει ότι οι εισβολές που χρησιμοποιούν άγνωστες επιθέσεις θα μπορούσαν να ανιχνευθούν. Απαιτείται, όμως, πρόσθετη προσπάθεια για τον εντοπισμό και την ανάλυση των προγραμμάτων που μπορούν να προκαλέσουν προβλήματα ασφάλειας.

4. Υβριδικό Μοντέλο

Έχει προταθεί ότι η ικανότητα ελέγχου (monitoring) των τρεχόντων συστημάτων ανίχνευσης εισβολών μπορεί να βελτιωθεί με την υιοθέτηση μια υβριδικής μεθόδου που αποτελείται ταυτόχρονα και από τις στρατηγικές ανίχνευσης διαταραχών καθώς επίσης και των υπογραφών. Ένα υβριδικό ή σύνθετο (hybrid or compound) σύστημα ανίχνευσης συνδυάζει και τις δύο παραπάνω προσεγγίσεις.

Στην ουσία, ***ένα υβριδικό σύστημα ανίχνευσης είναι ένα κατά υπογραφή εμπνευσμένο (signature inspired) σύστημα ανίχνευσης εισβολών που λαμβάνει μια απόφαση χρησιμοποιώντας ένα "υβριδικό πρότυπο" που είναι βασισμένο και στην κανονική συμπεριφορά (normal behavior) του συστήματος και στην παρεισφρητική συμπεριφορά (intrusive behavior) των εισβολέων.***

Σε ένα υβριδικό σύστημα, η τεχνική ανίχνευσης διαταραχών ενισχύει την ανίχνευση νέων ή άγνωστων επιθέσεων ενώ η τεχνική ανίχνευσης κακής συμπεριφοράς ανιχνεύει τις γνωστές επιθέσεις. Επιπλέον, η τεχνική ανίχνευσης υπογραφών είναι σε θέση να ανιχνεύσει τις επιθέσεις που προωθούνται από έναν επίμονο επιτιθέμενο που προσπαθεί να αλλάξει τη συμπεριφορά των σχεδίων-προτύπων (patterns) με στόχο την επανεκπαίδευση της ενότητας (module) της

ανίχνευσης διαταραχών έτσι ώστε θα δεχτεί τη συμπεριφορά της επίθεσης ως κανονική.

Αν και είναι αλήθεια ότι ο συνδυασμός των πολλαπλών τεχνολογιών ανίχνευσης εισβολών σε ένα ενιαίο σύστημα μπορεί θεωρητικά να παραγάγει ένα πολύ ισχυρότερο σύστημα ανίχνευσης εισβολών, τα προκύπτοντα υβριδικά συστήματα δεν είναι πάντα καλύτερα. Οι διαφορετικές τεχνολογίες ανίχνευσης εισβολών εξετάζουν την κυκλοφορία των συστημάτων ή/και των δικτύων και ψάχνουν την παρεισφρητική δραστηριότητα (intrusive activity) με διαφορετικούς τρόπους. Επομένως, η σημαντικότερη πρόκληση στην οικοδόμηση ενός λειτουργικού υβριδικού συστήματος ανίχνευσης εισβολών είναι το να παίρνει και να αξιοποιεί αυτές τις διαφορετικές τεχνολογίες για αποτελεσματικότερη και αποδοτικότερη επικοινωνία διαλειτουργικότητα (interoperation).

ΚΕΦΑΛΑΙΟ 5^{0}

ΟΡΓΑΝΩΣΗ ΣΥΣΤΗΜΑΤΩΝ ΑΝΙΧΝΕΥΣΗΣ ΕΙΣΒΟΛΩΝ

Ένα σύστημα ανίχνευσης εισβολών μπορεί να οργανωθεί με διάφορους τρόπους. Παρακάτω μελετώνται ενδεικτικά τρία παραδείγματα οργάνωσης, χρησιμοποιώντας αντίστοιχα συστήματα ανίχνευσης εισβολών που έχουν αναπτυχθεί ερευνητικά. Το πρώτο σύστημα εξετάζει απλώς την κυκλοφορία στο δίκτυο. Το δεύτερο ερευνά τον τρόπο με τον οποίο μπορούν να διασυνδεθούν οι πηγές από το δίκτυο και τα συνδεδεμένα συστήματα. Το τρίτο σύστημα κατανέμει το διευθυντή σε πολλά συστήματα, με σκοπό την ενίσχυση της ασφάλειας και της αξιοπιστίας.

1. Παρακολούθηση της Κυκλοφορίας στο Δίκτυο για εισβολές-NSM

Το σύστημα *Network Security Monitor (NSM)* διαμορφώνει αρχικά μία **κατατομή (profile)** για την αναμενόμενη χρήση ενός δικτύου και ακολούθως συγκρίνει την τρέχουσα χρήση με εκείνη της κατατομής. Επίσης, επιτρέπει τον καθορισμό ενός συνόλου υπογραφών (signatures), προκειμένου να ανιχνεύσει συγκεκριμένες ακολουθίες δικτυακής κίνησης, οι οποίες καταδεικνύουν επιθέσεις. Το σύστημα NSM εκτελείται σε ένα τοπικό δίκτυο. Το σύστημα παρακολούθησης (monitor) υπολογίζει το βαθμό αξιοποίησης (utilization) του δικτύου και άλλα χαρακτηριστικά, ενώ υπάρχει η δυνατότητα ρύθμισης του ώστε να εξετάζει τη δραστηριότητα ενός χρήστη, μιας ομάδας χρηστών ή μιας υπηρεσίας και να καταγράφει ενδεχόμενη διαταραγμένη συμπεριφορά.

Το NSM παρακολουθεί την πηγή της κίνησης του δικτύου, τον προορισμό και την παρεχόμενη υπηρεσία. Ορίζει μια μοναδική ταυτότητα σύνδεσης (connection ID) για κάθε σύνδεση. Η πηγή, ο προορισμός και η υπηρεσία χρησιμοποιούνται ως άξονες για έναν τρισδιάστατο πίνακα. Κάθε στοιχείο του πίνακα περιέχει τον αριθμό των πακέτων που στάλθηκαν μέσω εκείνης της σύνδεσης κατά τη διάρκεια μιας καθορισμένης χρονικής περιόδου, καθώς και το σύνολο των δεδομένων εκείνων των πακέτων. Επιπλέον, το NSM υπολογίζει τα

αναμενόμενα δεδομένα της σύνδεσης με το δίκτυο. Τα δεδομένα του πίνακα συγκρίνονται με τα αναμενόμενα δεδομένα της σύνδεσης και οποιοδήποτε δεδομένο εκτός του αναμενόμενου εύρους ερμηνεύεται ως διαταραχή.

Οι υπεύθυνοι για την ανάπτυξη του NSM διαπίστωσαν ότι παραγόταν μεγάλος αριθμός δεδομένων κατά τη διάρκεια της ανάλυσης ενός δικτύου. Για να μειωθεί το σχετικό κόστος (overhead), διαμόρφωσαν μία ιεραρχία για τα δεδομένα του πίνακα και τα παραγόμενα αναμενόμενα δεδομένα σύνδεσης για τα δεδομένα αυτά. Εάν οποιαδήποτε ομάδα στην ιεραρχία παρουσιάσει διαταραγμένα δεδομένα, ο υπεύθυνος του συστήματος ασφάλειας μπορεί να ζητήσει από το NSM να τα αναλύσει στα υποκείμενα στοιχεία. Οι ομάδες διαμορφώνονταν διαιρώντας τους άξονες του πίνακα. Για παράδειγμα, μια ομάδα θα αποτελούνταν από το σύνολο της κίνησης μεταξύ δύο συστημάτων για κάθε υπηρεσία. Θα περιείχε τα δεδομένα {(A, B, SMTP), (A, B, FTP),...}, όπου τα A και B θα ήταν τα ονόματα των συστημάτων (host names). Η επόμενη ομάδα θα εμφάνιζε τα ονόματα των υπηρεσιών και θα ομαδοποιούσε όλη την κίνηση σε ζεύγη πηγής-προορισμού (source-destination pairs). Στο υψηλότερο επίπεδο, η κίνηση θα ομαδοποιούνταν στο επίπεδο της πηγής και το NSM θα ανέλυε τα δεδομένα στο επίπεδο της πηγής. Εάν παρουσιαζόταν κάποια διαταραχή, ο υπεύθυνος του συστήματος ασφάλειας θα μπορούσε να ζητήσει από το NSM να εξετάσει κάθε στοιχείο της υποκείμενης ομάδας και να προσδιορίσει ποιο συγκεκριμένο ζεύγος πηγής-προορισμού παρουσίασε τη διαταραχή.

Το γεγονός ότι το NSM χρησιμοποιεί πίνακα, επέτρεψε την ανάπτυξη ενός απλού σχήματος, βασισμένου σε υπογραφή, για την αναζήτηση γνωστών υποδειγμάτων κακής συμπεριφοράς. Για παράδειγμα, επαναλαμβανόμενες συνδέσεις telnet που διαρκούσαν μόνον όσο ο τυπικός χρόνος πρόσβασης (normal setup time) θα υποδείκνυε αποτυχημένη προσπάθεια σύνδεσης. Ένας συγκεκριμένος κανόνας θα μπορούσε να αναζητήσει το περιστατικό αυτό στον πίνακα, αν και όπως επισημαίνουν οι σχεδιαστές του NSM, τα πρότυπα αυτά θα μπορούσαν να κρυφτούν όσο κάποιος οδηγείται προς την κορυφή της ιεραρχίας.

Η υλοποίηση του NSM επέτρεψε, επίσης, στον αναλυτή να καταγράψει συγκεκριμένους κανόνες, με βάση τους οποίους θα συγκρινόταν η κίνηση του δικτύου. Οι κανόνες που χρησιμοποιήθηκαν αρχικά, αφορούσαν τον έλεγχο για τυχόν υπερβολικό αριθμό προσπαθειών σύνδεσης (logins), για τυχόν επικοινωνία ενός υπολογιστικού συστήματος με δέκα πέντε ή περισσότερα συστήματα ή για οποιαδήποτε προσπάθεια επικοινωνίας με ανύπαρκτο σύστημα (host).

Το NSM παρείχε μια γραφική διεπαφή στο χρήστη, ώστε να παρέχεται η δυνατότητα στον υπεύθυνο του συστήματος ασφάλειας να διαπιστώνει εύκολα την κατάσταση στην οποία

βρίσκεται το δίκτυο. Επιπλέον, η διαχείριση της απεικόνισης ήταν ανεξάρτητη από τον αναλυτή πινάκων του NSM, έτσι ώστε ο τελευταίος να είναι σε θέση να αφιερώσει το χρόνο του αποκλειστικά στην ανάλυση των δεδομένων. Το πρωτότυπο σύστημα που αναπτύχθηκε στο University of California at Davis, εντόπιζε πολλές επιθέσεις. Όπως συμβαίνει σε όλα τα συστήματα ανίχνευσης εισβολών, το NSM κατέγραφε λανθασμένα θετικά επεισόδια (false positives), όπως την πρόσβαση αποφοίτων του Πανεπιστημίου σε λογαριασμούς (accounts) οι οποίοι είχαν παραμείνει ανενεργοί για αρκετά μεγάλο χρονικό διάστημα.

Το NSM είναι σημαντικό για δύο λόγους. Απετέλεσε τη βάση για ένα μεγάλο αριθμό συστημάτων ανίχνευσης εισβολών. Μάλιστα, έντεκα χρόνια μετά από τη δημιουργία του χρησιμοποιούνταν σε πολλά συστήματα. Επιπλέον απέδειξε ότι η ανίχνευση εισβολών σε δίκτυο ήταν εφικτή σε πρακτικό επίπεδο. Καθώς η κίνηση στο δικτύου χαρακτηρίζεται ολοένα και περισσότερο από κρυπτογραφημένη ροή μηνυμάτων, η δυνατότητα ανάλυσης των περιεχομένων των πακέτων μειώνεται, αλλά το NSM δεν εξέταζε τα περιεχόμενα (contents) της κίνησης, αλλά πραγματοποιούσε ανάλυση της ίδιας της κίνησης. Επομένως, η μεθοδολογία αυτή θα εξακολουθήσει να είναι αποτελεσματική.

2. Συνδυασμένη προσέγγιση-DIDS

Το σύστημα ***D**istributed **I**ntrusion **D**etection **S**ystem (DIDS)* συνδύαζε τις δυνατότητες του NSM, με τη δυνατότητα παρακολούθησης εισβολών σε μεμονωμένα συστήματα. Η αναγκαιότητα του ήταν αποτέλεσμα της διαπίστωσης της μη επάρκειας των παρακολουθήσεων που βασίζονταν αποκλειστικά στο δίκτυο και των παρακολουθήσεων που βασίζονταν αποκλειστικά στον υπολογιστή. Ένας εισβολέας που προσπαθούσε να συνδεθεί με ένα σύστημα μέσω ενός λογαριασμού που δεν απαιτούσε χρήση συνθηματικού (password) δε θα ανιχνευόταν ως κακόβουλος από ένα σύστημα παρακολούθησης του δικτύου (network monitor). Παρόλα αυτά, οι μετέπειτα ενέργειες του ενδέχεται να προκαλούσαν ένα σύστημα παρακολούθησης βασισμένο σε υπολογιστή (host-based monitor) να συνάγει την παρουσία ενός εισβολέα. Ομοίως, εάν ένας εισβολέας επιχειρούσε να συνδεθεί παραπάνω από μία φορές μέσω telnet με ένα σύστημα χρησιμοποιώντας κάθε φορά διαφορετικό όνομα σύνδεσης, ο μηχανισμός παρακολούθησης εισβολής βασισμένος στον υπολογιστή δε θα ανέφερε κάποιο πρόβλημα, αντίθετα, όμως, το βασισμένο στο δίκτυο σύστημα παρακολούθησης (network-based monitor) θα μπορούσε να ανιχνεύσει τις επαναλαμβανόμενες αποτυχημένες προσπάθειες σύνδεσης.

Το DIDS, αφενός χρησιμοποιούσε μηχανή ανάλυσης κεντρικοποιημένης λειτουργίας (centralized analysis engine), ουσιαστικά το διευθυντή DIDS (DIDS director), αφετέρου

απαιτούσε την τοποθέτηση αντιπροσώπων (agents) στο σύστημα που παρακολουθούνταν, καθώς και σε ένα σημείο όπου θα πραγματοποιούνταν η παρακολούθηση της κίνησης του δικτύου. Οι αντιπρόσωποι έλεγχαν τα αρχεία καταγραφής (logs) για ύποπτα περιστατικά και τα ανέφεραν στο διευθυντή DIDS. Ακολούθως, ο διευθυντής DJDS ενεργοποιούσε ένα έμπειρο σύστημα (expert system) που πραγματοποιούσε την ανάλυση των δεδομένων. Το έμπειρο σύστημα ήταν σύστημα βασισμένο σε εντολές (rule-based system) και ήταν σε θέση να εξάγει συμπεράσματα, τόσο για μεμονωμένα συστήματα, όσο και για ολόκληρο το σύστημα που συμπεριλάμβανε υπολογιστές και δίκτυο. Στη συνέχεια, τα αποτελέσματα προωθούνταν προς το περιβάλλον του χρήστη και παρουσιάζονταν με εύκολα αντιληπτό τρόπο διαμέσου φιλικής διεπαφής στον υπεύθυνο του συστήματος ασφάλειας.

Ένα πρόβλημα αποτελεί η αλλαγή **ταυτότητας (identity)**, καθώς ένας εισβολέας κινείται από σύστημα σε σύστημα. Για παράδειγμα, ένας εισβολέας θα μπορούσε να αποκτήσει πρόσβαση στο πρώτο σύστημα ως χρήστης alice και έπειτα στο δεύτερο σύστημα ως χρήστης bob. Οι μηχανισμοί βασισμένοι στον υπολογιστή δεν είναι σε θέση να γνωρίζουν ότι η alice και ο bob είναι στην πραγματικότητα ο ίδιος χρήστης και έτσι δεν μπορούν να συσχετίσουν τις ενέργειες αυτές. Όμως, ο διευθυντής DIDS θα κατέγραφε ότι η alice συνδέθηκε με το μακρινό σύστημα και ότι ο bob συνδέθηκε μέσω της ίδιας σύνδεσης. Το έμπειρο σύστημα, με τη σειρά του, θα συμπέραινε ότι πρόκειται για τον ίδιο χρήστη. Για να επιτραπεί, όμως, αυτός ο τύπος συσχετισμού έπρεπε κάθε χρήστης να αναγνωριζόταν από ένα μοναδικό αριθμό ταυτότητας δικτύου (***Network Identification Number-NID***). Στο παράδειγμα που αναφέρθηκε, επειδή η alice και ο bob ήταν στην πραγματικότητα ο ίδιος χρήστης και, οι δύο θα μοιράζονταν ένα κοινό NID.

Οι αντιπρόσωποι υπολογιστών και ο αντιπρόσωπος δικτύου υποστηρίζουν την επίλυση των προβλημάτων που εμφανίζονται κατά την κατανεμημένη ανίχνευση εισβολών (distributed intrusion detection). Τα αρχεία καταγραφής των υπολογιστών αναλύονται προκειμένου να εξαχθούν ύποπτες εγγραφές. Σε μερικές περιπτώσεις εκτελούνται απλές ενέργειες προκειμένου να καθοριστεί εάν οι καταχωρίσεις θα πρέπει να προωθηθούν. Για παράδειγμα, οι αντιπρόσωποι υπολογιστών παρακολουθούν το σύστημα για τυχόν επιθέσεις χρησιμοποιώντας τις υπογραφές. Οι περιλήψεις των αποτελεσμάτων παρακολούθησης αποστέλλονται στο διευθυντή. Άλλα γεγονότα προωθούνται άμεσα. Για το λόγο αυτό, το μοντέλο DIDS ζητά από τους αντιπροσώπους των υπολογιστών να αναφέρουν τα συμβάντα ή γεγονότα (events), που είναι πληροφορίες που περιλαμβάνονται στις καταχωρίσεις των αρχείων, την ενέργεια (action) και το πεδίο (domain) (Πίνακας 2). Τα υποκείμενα, όπως είναι οι ενεργές διεργασίες (active processes), εκτελούν ενέργειες και τα πεδία χαρακτηρίζουν τις παθητικές οντότητες. Για

παράδειγμα, μία διεργασία μπορεί να είναι, είτε ένα υποκείμενο όταν αλλάζει την κατάσταση προστασίας ενός αρχείου, είτε ένα αντικείμενο όταν τερματίζεται. Ένα αντικείμενο αντιστοιχίζεται στο υψηλότερης προτεραιότητας πεδίο που ανήκει.

session_start	*create*	*tagged*	*sys_info*
session_end	*delete*	*authentication*	*user_info*
read	*move*	*audit*	*utility*
write	*change_rights*	*network*	*owned*
execute	*change_user_id*	*system*	*not_owned*
terminate			

Πίνακας 2:Οι εντολές του DIDS και τα τμήματα. Οι δύο αριστερά στήλες περιλαμβάνουν τους τύπους των ενεργειών και οι δυο δεξιά τους τύπους των τμημάτων

Για παράδειγμα, ένα αρχείο μπορεί να χαρακτηριστεί ως σημαντικό. Εάν το αρχείο περιέχει *δεδομένα αυθεντικοποίησης (authentication data)* και έχει χαρακτηριστεί και ως σημαντικό, θα αναφερθεί ως χαρακτηρισμένο αντικείμενο (tagged object). Ένας πίνακας, ο οποίος παράγεται μη αυτοματοποιημένα, υπαγορεύει τα περιστατικά που αποστέλλονται στο διευθυντή DIDS με κριτήριο τις ενέργειες και τα πεδία που συνδέονται με τα γεγονότα. Γεγονότα που συνδέονται με το NID είναι εκείνα που περιλαμβάνουν ενέργειες τύπου session_start, ενώ εκτελούν ενέργειες σε πεδία του δικτύου. Αυτές οι πράξεις προωθούνται, ώστε ο διευθυντής DIDS να μπορεί να ενημερώνει αναλόγως το σύστημα.

Ο αντιπρόσωπος δικτύου αποτελεί μία απλουστευμένη έκδοση του NSM και παρέχει τις πληροφορίες που προαναφέρθηκαν.

Το έμπειρο σύστημα, ένα βασικό συστατικό στη λειτουργία του διευθυντή DIDS, εξάγει υψηλού επιπέδου πληροφορίες σχετικές με μια εισβολή από τα χαμηλού επιπέδου δεδομένα που λαμβάνει. Οι κανόνες αναφοράς προέρχονται από ένα ιεραρχικό μοντέλο ανίχνευσης εισβολής. Αυτό το μοντέλο περιλαμβάνει έξι επίπεδα στη διαδικασία εξαγωγής συμπερασμάτων:

i. Στο χαμηλότερο επίπεδο, όλες οι εγγραφές των αρχείων καταγραφής είναι ορατές. Προέρχονται από τον αντιπρόσωπο του υπολογιστή, από τον αντιπρόσωπο του δικτύου, καθώς και από άλλες πηγές που μπορεί να διαθέτει ο διευθυντής DIDS.

ii. Στο επίπεδο αυτό τα γεγονότα λαμβάνουν πληροφορίες από τις καταχωρίσεις των αρχείων συμβάντων (log entries).

iii. Στο επίπεδο αυτό ορίζεται ένα υποκείμενο που συγκεντρώνει όλα τα γεγονότα που σχετίζονται με ένα και μοναδικό χρήστη. Το NID αντιστοιχίζεται σε αυτό το υποκείμενο. Στο επίπεδο αυτό ορίζεται το όριο μεταξύ των πληροφοριών που εξαρτώνται από τη μηχανή, καθώς επίσης και το επίπεδο αφαίρεσης του χρήστη ως υποκειμένου και των σχετικών γεγονότων.

iv. Το επίπεδο αυτό προσθέτει διάφορες συναφείς πληροφορίες. Για παράδειγμα, προσωρινά χρονικά δεδομένα, όπως ο χρόνος χρήσης του επεξεργαστή και χωρικά δεδομένα όπως η εγγύτητα σε άλλα γεγονότα. Εάν ο χρήστης προσπαθήσει να συνδεθεί κάποια ώρα κατά την οποία δεν είχε προσπαθήσει ποτέ πριν να συνδεθεί, ή εάν μία σειρά από αποτυχημένες προσπάθειες σύνδεσης ακολουθεί εντολές ανίχνευσης προκειμένου να διαπιστωθεί ποιος χρησιμοποιεί ένα σύστημα, το συμπέρασμα που συνάγεται είναι ότι αναφερόμαστε σε ύποπτα γεγονότα.

v. Το επίπεδο αυτό ασχολείται με τις απειλές προς το δίκτυο (network threats), οι οποίες είναι συνδυασμοί διαφόρων γεγονότων. Μια απειλή είναι εξαπάτηση-κακομεταχείριση (abuse) εάν μεταβάλλεται η κατάσταση προστασίας του συστήματος. Παράδειγμα αποτελεί η μεταβολή ενός προστατευμένου από εγγραφή αρχείου, σε αρχείο το οποίο μπορεί να τροποποιηθεί από τον καθένα. Μία απειλή θεωρείται κακή συμπεριφορά (misuse) εάν παραβιάζει την πολιτική, χωρίς όμως να μεταβάλλει την κατάσταση του συστήματος. Παράδειγμα αποτελεί η απαγορευμένη αντιγραφή ενός αρχείου εργασίας, που μπορούσε όμως να αναγνωστεί από τον καθένα. Μία απειλή είναι μία ύποπτη πράξη (suspicious act) αν δεν παραβιάζει την πολιτική, αλλά μπορεί να θεωρηθεί ότι είναι εντός του πεδίου ενεργειών για την προετοιμασία μιας επίθεσης. Για παράδειγμα, μια εντολή finger μπορεί να αποτελεί προοίμιο μιας επίθεσης.

vi. Το επίπεδο αυτό βαθμολογεί, σε κλίμακα 1-100, την κατάσταση ασφάλειας του δικτύου. Αυτή η βαθμολογία προέρχεται από τις απειλές προς το σύστημα που αναπτύσσονται στο επίπεδο 5. Αποτελεί ευκολία για τους χρήστες, διότι επιτρέπει στον υπεύθυνο ασφάλειας των συστημάτων να εντοπίσει γρήγορα τα προβλήματα. Επειδή τα μη επεξεργασμένα δεδομένα που χρησιμοποιούνται για τον υπολογισμό αυτής της βαθμολογίας είναι διαθέσιμα, τα συμπεράσματα μπορούν να προκύψουν χωρίς καθυστερήσεις.

Στο έμπειρο σύστημα κάθε κανόνας έχει μία σχετική αξία κανόνα (rule value). Η αξία κανόνα χρησιμοποιείται προκειμένου να υπολογιστεί η βαθμολογία. Ο υπεύθυνος ασφάλειας των συστημάτων ανατροφοδοτεί (feedbacks) το έμπειρο σύστημα, ενώ σε περίπτωση εμφάνισης ψευδών συναγερμών (false alarms) το έμπειρο σύστημα μειώνει την αξία που συνδέεται με τους κανόνες που οδήγησαν στον ψευδή συναγερμό.

3. Αυτόνομοι Αντιπρόσωποι-AAFID

Το 1995 οι Crosbie και Spafford, εξέτασαν διάφορα συστήματα ανίχνευσης εισβολών υπό την σκοπιά της ανοχής που παρουσιάζουν σε σφάλματα (fault tolerance). Το γενικό συμπέρασμά τους ήταν ότι, ένα τυπικό σύστημα ανίχνευσης εισβολών, που λαμβάνει πληροφορίες παρακολουθώντας συστήματα και δίκτυα, αποτελεί δυνητικό σημείο αποτυχίας (single point failure), αφού στην περίπτωση που ο διευθυντής αποτύχει το IDS δε θα λειτουργήσει. Η πρόταση τους ήταν να διαχωριστεί το σύστημα ανίχνευσης εισβολών σε πολλαπλά συστατικά, τα οποία θα λειτουργούν μεν ανεξάρτητα μεταξύ τους, αλλά θα επικοινωνούν προκειμένου να συσχετίσουν τις ληφθείσες πληροφορίες.

Ένας αυτόνομος αντιπρόσωπος είναι μια διεργασία που μπορεί να ενεργεί ανεξάρτητα από το σύστημα του οποίου αποτελεί μέρος.

Έτσι, οι M. Crosbie και E. Spafford πρότειναν την ανάπτυξη ***αυτόνομων αντιπροσώπων Autonomous Agents for Intrusion Detection (AAFID)*** καθένας από τους οποίους θα εκτελούσε μία συγκεκριμένη λειτουργία παρακολούθησης. Κάθε αντιπρόσωπος θα είχε το δικό του εσωτερικό μοντέλο και όταν ο αντιπρόσωπος ανίχνευε είτε μια απόκλιση (deviation) από την αναμενόμενη συμπεριφορά (expected behavior), είτε ταύτιση με ένα πρότυπο στα πλαίσια ενός συγκεκριμένου κανόνα, είτε μία παραβίαση μιας προδιαγραφής, τότε θα ειδοποιούσε σχετικά τους άλλους αντιπροσώπους. Οι αντιπρόσωποι, με τη σειρά τους, θα καθόριζαν από κοινού εάν το σύνολο των ειδοποιήσεων ήταν επαρκές ώστε να μπορεί να αποτελέσει μία δυνητική εισβολή.

Το <u>πλεονέκτημα</u> σε αυτή την οργάνωση βασίζεται στη συνεργασία των αντιπροσώπων: δεν υπάρχει πλέον ένα δυνητικό σημείο αποτυχίας. Εάν ένας αντιπρόσωπος τεθεί εκτός λειτουργίας, οι υπόλοιποι είναι σε θέση να συνεχίσουν τη λειτουργία τους. Επιπλέον, εάν ένας εισβολέας καταστείλει έναν αντιπρόσωπο, δε γνωρίζει τίποτα για τους υπόλοιπους αντιπροσώπους στο σύστημα ή για αυτούς που ελέγχουν το δίκτυο. Ο ίδιος ο διευθυντής κατανέμεται (distributed) μεταξύ των αντιπροσώπων, έτσι ώστε να μην μπορεί να υποστεί επίθεση κατά τον τρόπο που συμβαίνει σε ένα σύστημα ανίχνευσης εισβολών με ένα διευθυντή σε ένα μοναδικό υπολογιστή.

Άλλα πλεονεκτήματα περιλαμβάνουν την εξειδίκευση του κάθε αντιπροσώπου. Ο αντιπρόσωπος μπορεί να αναπτυχθεί με τρόπον ώστε να ελέγχει έναν πόρο (resource), παραμένοντας μικρός και απλός, ικανοποιώντας τη βασική αρχή της οικονομίας μηχανισμών (economy of mechanisms). Οι αντιπρόσωποι θα μπορούσαν επίσης να μεταναστεύσουν (migrate) μέσω των τοπικών δικτύων και να επεξεργαστούν δεδομένα σε πολλαπλά συστήματα. Η προσέγγιση αυτή μπορεί να εφαρμοστεί για επίτευξη κλιμάκωσης και σε μεγαλύτερα δίκτυα εξαιτίας της κατανεμημένης φύσης του διευθυντή.

Τα συνήθη *μειονεκτήματα* των αυτόνομων αντιπροσώπων εντοπίζονται στο αυξημένο *υπολογιστικό κόστος (overhead)* των απαιτούμενων επικοινωνιών, καθώς μειώνεται η λειτουργικότητα του κάθε αντιπροσώπου, απαιτούνται περισσότεροι αντιπρόσωποι για τη συνολική παρακολούθηση του συστήματος, με επακόλουθο την αύξηση στο κόστος επικοινωνίας. Επιπλέον, θα πρέπει να διασφαλίζονται οι επικοινωνίες, όπως βεβαίως και οι κατανεμημένοι υπολογισμοί.

ΚΕΦΑΛΑΙΟ 6^{ο}

ΑΠΟΚΡΙΣΗ ΣΤΙΣ ΕΙΣΒΟΛΕΣ

Μετά την ανίχνευση μιας εισβολής, το επόμενο ζήτημα που τίθεται είναι ο τρόπος με τον οποίο μπορεί να προστατευθεί ένα σύστημα. Ο τομέας της ***απόκρισης στην εισβολή (intrusion response)*** μελετά το πρόβλημα αυτό. Στόχος είναι να αντιμετωπιστεί η αποπειραθείσα επίθεση με τρόπο ώστε να ελαχιστοποιείται η ζημιά, όπως προσδιορίζεται από την ισχύουσα πολιτική ασφάλειας. Μερικοί μηχανισμοί ανίχνευσης εισβολών μπορούν να βελτιωθούν προκειμένου να αποτρέψουν τους εισβολείς. Σε αντίθετη περίπτωση, οι υπεύθυνοι ασφάλειας πρέπει να αποκριθούν στην επίθεση και να αποκαταστήσουν οποιαδήποτε ζημιά προκλήθηκε.

1. Πρόληψη Περιστατικών

Το βέλτιστο θα ήταν να είναι δυνατό να ανιχνευτούν και να διακοπούν οι προσπάθειες εισβολής, πριν την επίτευξη του στόχου τους. Αυτό τυπικά περιλαμβάνει επιμελή παρακολούθηση του συστήματος, συνήθως με ένα μηχανισμό ανίχνευσης εισβολών και τη λήψη μέτρων για την αντιμετώπιση της επίθεσης.

Στα πλαίσια της απόκρισης, η ***πρόληψη περιστατικών (incident prevention)*** απαιτεί τον εντοπισμό της επίθεσης πριν από την ολοκλήρωση της. Ακολούθως, λαμβάνονται μέτρα προκειμένου να αποτραπεί η ολοκλήρωση της επίθεσης. Αυτό μπορεί να πραγματοποιηθεί είτε αυτοματοποιημένα είτε μη αυτοματοποιημένα.

Τα συστήματα ασφάλειας πολλαπλών επιπέδων είναι εξαιρετικά περιβάλλοντα για υλοποίηση των "jails", επειδή παρέχουν μεγαλύτερο βαθμό περιορισμού από τα συνηθισμένα συστήματα. Ο επιτιθέμενος τοποθετείται σε ένα περιβάλλον ασφάλειας που είναι απομονωμένο από τα υπόλοιπα. Οι ενσωματωμένοι μηχανισμοί ασφάλειας είναι σχεδιασμένοι ώστε να περιορίζουν την πρόσβαση στα αντικείμενα μέσα στο απομονωμένο περιβάλλον, περιορίζοντας με τον τρόπο αυτό τον επιτιθέμενο. Πιο περίπλοκες προσεγγίσεις βασισμένες στον υπολογιστή μπορούν να ενσωματωθούν στους μηχανισμούς ανίχνευσης εισβολών. Οι μέθοδοι που βασίζονται στην υπογραφή (signature-based) καθιστούν δυνατή την παρακολούθηση των

μεταβάσεων για πιθανές επιθέσεις. Οι μέθοδοι που βασίζονται στη διαταραχή (anomaly-based) καθιστούν εφικτή την παρακολούθηση σχετικών χαρακτηριστικών του συστήματος για τυχόν διαταραχές και την άμεση αντίδραση όταν οι διαταραχές εντοπίζονται σε πραγματικό χρόνο.

2. Χειρισμός των Εισβολών

Όταν λαμβάνει χώρα μία εισβολή, η πολιτική ασφάλειας του συστήματος έχει παραβιαστεί. Ο ***χειρισμός των εισβολών (intrusion handling)*** περιλαμβάνει την εκ νέου συμμόρφωση του συστήματος με την πολιτική ασφάλειας και τη λήψη μέτρων κατά του επιτιθέμενου, όπως αυτά καθορίζονται από την ισχύουσα πολιτική. Ο χειρισμός των εισβολών περιλαμβάνει έξι φάσεις:

i. ***Προετοιμασία (preparation)*** για μία επίθεση: Αυτό το βήμα εμφανίζεται πριν ανιχνευθούν οποιεσδήποτε επιθέσεις. Στα πλαίσια του βήματος αυτού εγκαθίστανται οι διαδικασίες και οι μηχανισμοί για την ανίχνευση και την απόκριση στις επιθέσεις.

ii. ***Ταυτοποίηση (identification)*** μιας επίθεσης: Το βήμα αυτό διαμορφώνει τις υπόλοιπες φάσεις.

iii. ***Περιορισμός (containment)*** της επίθεσης: Το βήμα αυτό περιορίζει σε όσο το δυνατό μεγαλύτερο βαθμό τη ζημιά στο σύστημα.

iv. ***Εξουδετέρωση (eradication)*** της επίθεσης: Από το βήμα αυτό σταματά η επίθεση και παρεμποδίζονται περαιτέρω παρόμοιες επιθέσεις.

v. ***Αποκατάσταση (recovery)*** από την επίθεση: Στο βήμα αυτό αποκαθίσταται η ασφαλής κατάσταση στο σύστημα, σύμφωνα με τις επιταγές της ισχύουσας πολιτικής ασφάλειας.

vi. ***Συνεχής παρακολούθηση (follow-up***) της επίθεσης: Αυτό το βήμα περιλαμβάνει τη λήψη μέτρων κατά του επιτιθέμενου, τον προσδιορισμό των προβλημάτων κατά το χειρισμό του γεγονότος και καταγραφή των σχετικών εμπειριών που αποκτήθηκαν.

3. Αντιδράσεις των συστημάτων ανίχνευσης εισβολών

Οι αντιδράσεις των συστημάτων ανίχνευσης εισβολών διακρίνονται γενικά σε δύο κατηγορίες, τις ***ενεργές (active responses)*** και τις ***παθητικές (passive responses)***.

3.1. Ενεργές αντιδράσεις

Στις ***ενεργές αντιδράσεις*** το σύστημα προσπαθεί να λάβει κάποια μέτρα για να τεκμηριώσει

καλύτερα ή να αναχαιτίσει την επίθεση. Προς την κατεύθυνση αυτή το σύστημα ανίχνευσης εισβολών μπορεί να προβεί σε μία ή περισσότερες από τις ακόλουθες ενέργειες:

i. ***Συλλογή περισσοτέρων πληροφοριών***, με κύριο στόχο την καλύτερη αξιολόγηση της επίθεσης ή/και τη συλλογή στοιχείων για νομικές ενέργειες. Προς την κατεύθυνση αυτή μπορεί να αυξηθεί η ευαισθησία των αισθητήρων π.χ. αρχείων καταγραφής, πακέτων δικτύου που αναλύονται κ.λ.π. ή να υπάρξουν "ερωτήσεις" προς το σύστημα από το οποίο εκπορεύεται η επίθεση για να διαπιστωθεί ποιοι χρήστες είναι συνδεδεμένοι κ.α.

ii. ***Τροποποίηση περιβάλλοντος***. Η κατεύθυνση αυτή αποσκοπεί στο να οδηγήσει την επίθεση σε αποτυχία. Αυτό μπορεί να επιτευχθεί με αποστολή προς τον επιτιθέμενο πακέτων τερματισμού σύνδεσης που να φαίνεται ότι προέρχονται από το υπό επίθεση σύστημα, με επαναρύθμιση firewalls και δρομολογητών και υπηρεσιών εισάγοντας απαγορεύσεις για διευθύνσεις IP, θυρών, δικτυακών πρωτοκόλλων, υπηρεσιών ή φυσικών συνδέσεων.

Αντεπίθεση, η οποία συνίσταται σε χρήση τεχνικών για αδρανοποίηση του επιτιθέμενου ή συλλογή πληροφοριών για αυτόν. Θα μπορούσε έτσι να υπάρξει καταιγισμός δικτυακών πακέτων προς το σύστημα απ' όπου φαίνεται να ξεκινά η επίθεση, ή εξαπόλυση επιθέσεων προς υπηρεσίες που αυτός προσφέρει. Η αντεπίθεση δεν είναι πρακτική που πρέπει να εφαρμόζεται στη γενική περίπτωση, καθώς μπορεί να έχει νομικές επιπτώσεις (η αυτοδικία δεν θεωρείται νόμιμη ενέργεια) και μπορεί επίσης να "θυμώσει" τους εισβολείς, με συνέπεια να εξαπολύσουν πιο "σκληρές" επιθέσεις. Είναι τέλος πιθανόν μία αντεπίθεση να έχει ως αποτέλεσμα να "χτυπηθούν" αθώοι, καθώς σε δημόσια δίκτυα (π.χ. δίκτυα IP) δεν υπάρχει ισχυρή διακρίβωση της ταυτότητας προέλευσης των δικτυακών πακέτων, και έτσι αυτή μπορεί να έχει πλαστογραφηθεί. Σε μία περίπτωση πλαστογραφίας της ταυτότητας προέλευσης, στη διάρκεια της αντεπίθεσης θα "χτυπηθεί" το σύστημα που φαίνεται στην ταυτότητα προέλευσης των δικτυακών πακέτων, το οποίο όμως δεν θα είναι το σύστημα από το οποίο προέρχεται η επίθεση. Αν πρόκειται σε οποιαδήποτε περίπτωση να χρησιμοποιηθεί τεχνική αντεπίθεσης, αυτή πρέπει να γίνει υπό την εποπτεία ειδικών.

3.2. Παθητικές αντιδράσεις

Οι παθητικές αντιδράσεις ***συνίστανται κυρίως σε ειδοποιήσεις και συναγερμούς*** για το προσωπικό ασφάλειας. Οι ειδοποιήσεις αυτές μπορούν να έχουν κυμαινόμενο βαθμό λεπτομέρειας και μπορούν να εμφανίζονται σε ειδικό χώρο του συστήματος ανίχνευσης εισβολών, σε παράθυρο μηνύματος, σε συσκευές τηλεειδοποίησης, με μηνύματα σε κινητά κ.α. Μολονότι και το ηλεκτρονικό ταχυδρομείο θα μπορούσε να χρησιμοποιηθεί για τέτοιου

ειδοποιήσεις αυτής της μορφής, είναι επισφαλές να βασισθεί κανείς σ' αυτό καθώς ο εισβολέας ενδέχεται να "μπλοκάρει" την αποστολή μηνυμάτων.

Για την αναφορά των προβλημάτων μπορεί να χρησιμοποιηθεί και το πρωτόκολλο SNMP, το οποίο είναι ένα ευρέως διαδεδομένο στάνταρ. Η προσέγγιση αυτή έχει το πλεονέκτημα ότι παρέχει τη δυνατότητα ολοκλήρωσης με συστήματα διαχείρισης δικτύου, αξιοποιώντας περαιτέρω μια δαπανηρή υποδομή (λογισμικού και επικοινωνίας), και ολοκληρώνοντας τις λειτουργίες διαχείρισης. Συνολικά, η παθητικές αντιδράσεις είναι λιγότερο απαιτητικές σε πόρους από τις ενεργές αντιδράσεις.

4. Η "αυτοάμυνα" των συστημάτων ανίχνευσης εισβολών

Σε πολλές περιστάσεις το ίδιο το IDS μπορεί να αποτελέσει στόχο επιθέσεων με στόχο την ανίχνευση, την παράκαμψη ή την αχρήστευσή του. Θα πρέπει έτσι να λαμβάνονται μέτρα ώστε το ίδιο το σύστημα ανίχνευσης εισβολών να μην γίνεται στόχος ή/και να μπορεί να αποκρούει τέτοιου είδους επιθέσεις. Στα μέτρα αυτά μπορούν να εντάσσονται:

i. Η αποφυγή της κοινοποίησης της παρουσίας του IDS με δικτυακά μηνύματα, ακόμη και σε περιπτώσεις συναγερμού. Αν είναι απολύτως απαραίτητο να εκπεμφθεί μήνυμα, είναι σκόπιμο να εκπέμπεται με πλαστή δικτυακή διεύθυνση.

ii. Συνολικά είναι καλό τα στοιχεία που συλλέγονται από το IDS να διακινούνται από ξεχωριστά κανάλια επικοινωνίας, προκειμένου να μην εντοπίζεται η κυκλοφορία αυτή από τους πιθανούς εισβολείς. Αν αυτό είναι αδύνατον, επιβάλλεται η χρήση κρυπτογράφησης και ισχυρών μηχανισμών διακρίβωσης ταυτότητας. Η κρυπτογράφηση προστατεύει τα διακινούμενα στοιχεία από το να αποκαλυφθούν στους εισβολείς, ενώ η ισχυρή διακρίβωση ταυτότητας αποτρέπει τους εισβολείς από το να αποστείλουν πλαστογραφημένα στοιχεία στο σύστημα ανίχνευσης εισβολών με στόχο την παραπλάνησή του.

Το ίδιο το σύστημα ανίχνευσης εισβολών δεν πρέπει να παρέχει δικτυακώς προσπελάσιμες υπηρεσίες, όπως απομακρυσμένης σύνδεσης, ηλεκτρονικού ταχυδρομείου κ.λ.π., καθώς αυτές αφ' ενός θα αποκαλύψουν την ύπαρξή του, αφ' ετέρου μπορούν να αξιοποιηθούν από τους εισβολείς σε επιθέσεις εναντίον του συστήματος ανίχνευσης εισβολών.

ΚΕΦΑΛΑΙΟ 7^{ο}

ΣΥΝΟΨΗ-ΣΥΜΠΕΡΑΣΜΑΤΑ

Στην παρούσα εργασία αναπτύχθηκαν θέματα που σχετίζονται με την ***ανίχνευση εισβολών***. Αυτά αφορούν, τις αιτίες καθώς και τους στόχους για την εισαγωγή των διαφόρων συστημάτων ασφάλειας και πιο συγκεκριμένα στα Συστήματα Ανίχνευσης Εισβολών.

Τα συστήματα ανίχνευσης εισβολών αποτελούνται από τρία λειτουργικά τμήματα, τις *πηγές πληροφοριών*, την *ανάλυση*, και την *απόκριση*. Το σύστημα λαμβάνει τις πληροφορίες γεγονότων από μια ή περισσότερες πηγές πληροφοριών, εκτελεί μια συντονισμένη ανάλυση των δεδομένων γεγονότων (event data), και έπειτα παράγει τις απαραίτητες αποκρίσεις, που μπορεί να είναι εκθέσεις ή ενεργές επεμβάσεις όταν ανιχνεύονται οι εισβολές.

Τα συστήματα ανίχνευσης εισβολών αποτελούν ουσιαστικά *μηχανές εποπτείας* και *ελέγχου*, κατά συνέπεια μπορούν να ακολουθηθούν τα υπάρχοντα μοντέλα για την περιγραφή των αρχιτεκτονικών. Ο *διευθυντής* μπορεί να έχει είτε *κεντρικοποιημένη* δομή είτε *κατανεμημένη*, ενώ μπορεί να είναι είτε *ιεραρχικός* είτε *τμηματοποιημένος*. Κάθε οργάνωση έχει πλεονεκτήματα και μειονεκτήματα, αλλά για τα δίκτυα ευρείας περιοχής, ένας κατανεμημένος διευθυντής παρέχει τη μέγιστη ευελιξία και ρωμαλεότητα. Οι *πληροφορίες* μπορούν να *συγκεντρωθούν* είτε από τους *υπολογιστές*, είτε από το *δίκτυο*, είτε από *αμφότερα*, είτε από *άλλους διευθυντές*.

Για την ανίχνευση εισβολών σε ένα σύστημα έχουν προταθεί τρία βασικά μοντέλα καθώς επίσης και συνδυασμός αυτών.

Η *ανίχνευση διαταραχών* αναζητά κάποια ασυνήθη συμπεριφορά. Αναπτύσσεται αρχικά ένα βασικό πλαίσιο αναμενόμενων γεγονότων ή χαρακτηριστικών των διεργασιών, των χρηστών, ή των ομάδων χρηστών. Σε όποια περίπτωση καταγράφεται παρέκκλιση, αυτή θεωρείται πιθανή εισβολή. Επειδή στις περισσότερες περιπτώσεις οι συμπεριφορές χρηστών και συστημάτων μεταβάλλονται προϊόντος του χρόνου, θα πρέπει να υπάρχει έξυπνος, διαρκής και αποτελεσματικός μηχανισμός ενημέρωσης των κατατομών αυτών.

Η *ανίχνευση κακής συμπεριφοράς* αναζητά ακολουθίες γεγονότων που είναι γνωστό ότι παρουσιάζουν οι επιθέσεις. Πρέπει να υπάρχει ένα σύνολο κανόνων ή μία βάση δεδομένων των επιθέσεων, όπου να περιλαμβάνονται οι απαραίτητες πληροφορίες. Στην ιδεατή περίπτωση, ένα έμπειρο σύστημα θα χρησιμοποιήσει το σύνολο κανόνων για να ανιχνεύσει τις προηγούμενες άγνωστες επιθέσεις. Οι τεχνικές που βασίζονται στην κατάσταση και οι τεχνικές που βασίζονται στη μετάβαση καταστάσεων θεωρούνται σχετικά αποτελεσματικές.

Η *ανίχνευση που βασίζεται στις προδιαγραφές* αναζητά ενέργειες εκτός των προδιαγραφών των βασικών προγραμμάτων. Κάθε πρόγραμμα διαθέτει ένα σύνολο κανόνων που διευκρινίζει τις επιτρεπτές ενέργειες. Εάν το πρόγραμμα προσπαθεί να προβεί σε οποιαδήποτε άλλη ενέργεια, ο μηχανισμός ανίχνευσης εισβολής αναφέρει μία πιθανή εισβολή. Αυτή η μέθοδος απαιτεί στο αρχικό στάδιο τη συλλογή των προδιαγραφών για τα προγράμματα.

Η *ανίχνευση μέσω του υβριδικού μοντέλου* αποτελείται ταυτόχρονα και από τις στρατηγικές ανίχνευσης διαταραχών καθώς επίσης και των υπογραφών. Εδώ η τεχνική ανίχνευσης διαταραχών ενισχύει την ανίχνευση νέων ή άγνωστων επιθέσεων ενώ η τεχνική ανίχνευσης κακής συμπεριφοράς ανιχνεύει τις γνωστές επιθέσεις.

Οι κατηγορίες *χρονισμού* είναι η *περιοδική ή μαζική ανάλυση* (interval-based or batch mode) και *πραγματικός χρόνος* (real-time). Τα πιο κοινά εμπορικά IDSs είναι πραγματικού χρόνου, βασισμένα σε δίκτυο συστήματα.

Όταν εμφανίζεται μία εισβολή, είναι απαραίτητη κάποια *απόκριση*. Εάν η προσπάθεια εισβολής ανιχνευτεί προτού η επίθεση τελεσφορήσει, το σύστημα μπορεί να λάβει μέτρα για να αποτρέψει την επιτυχία της επίθεσης. Σε αντίθετη περίπτωση πρέπει να αντιμετωπιστεί η εισβολή. Στα βήματα που ακολουθούνται περιλαμβάνεται ο περιορισμός της επίθεσης, η εξουδετέρωση για να εξαλειφθούν οι διεργασίες ή οι συνδέσεις που έχουν επιτευχθεί, καθώς και η παρακολούθηση της εξέλιξης των γεγονότων ώστε αφενός να ληφθούν μέτρα κατά του επιτιθέμενου, αφετέρου να εξαχθούν χρήσιμα συμπεράσματα από την επίθεση.

ΑΝΟΙΧΤΕΣ ΠΡΟΚΛΗΣΕΙΣ-ΣΥΜΠΕΡΑΣΜΑΤΙΚΑ

Τα τελευταία είκοσι χρόνια, τα συστήματα ανίχνευσης εισβολών έχουν εξελιχθεί αργά από host -και λειτουργικά συστήματα- specific applications σε distributed συστήματα που περιλαμβάνουν μια ευρεία γκάμα λειτουργικών συστημάτων. Οι προκλήσεις που ανακύπτουν για την νέα γενιά των συστημάτων ανίχνευσης εισβολών είναι πολλές. Πρώτα απ' όλα, τα παραδοσιακά συστήματα ανίχνευσης εισβολών δεν έχουν προσαρμοστεί επαρκώς στα νέα πρότυπα δικτύωσης όπως τα ασύρματα και κινητά δίκτυα, ούτε έχουν

εξελιχθεί για να καλύψουν τις απαιτήσεις που τίθενται από μεγάλα (gigabit και terabit) δίκτυα.

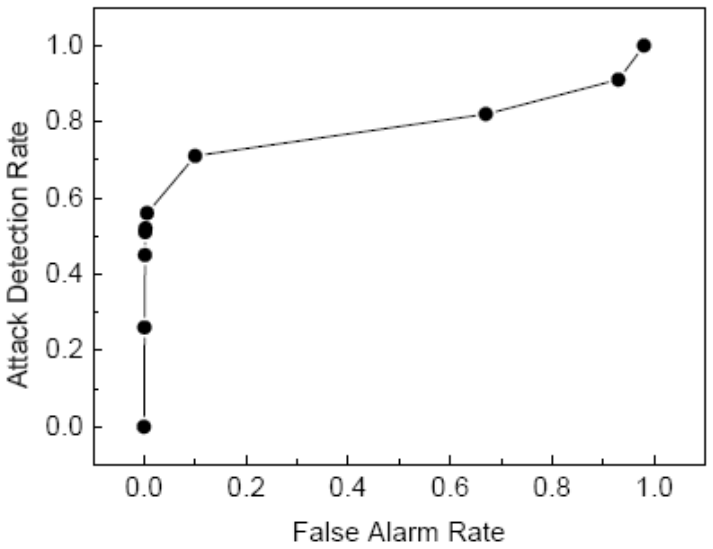
Παράγοντες όπως θόρυβος στα δεδομένα ελέγχου (audit data), αλλάζουν διαρκώς τα traffic profiles, και η μεγάλη ποσότητα δικτυακής κυκλοφορίας καθιστούν δύσκολο να χτιστεί ένα κανονικό profile κυκλοφορίας ενός δικτύου με σκοπό την ανίχνευση εισβολών. Η επίπτωση είναι ότι, ελλείψει κάποιου θεμελιώδους επανασχεδιασμού, οι σημερινές προσεγγίσεις ανίχνευσης εισβολών δεν θα είναι σε θέση να προστατεύσουν επαρκώς τα αυριανά δίκτυα από τις εισβολές και τις επιθέσεις. *Επομένως, η μεθοδολογία σχεδιασμού των συστημάτων ανίχνευσης εισβολών πρέπει να ακολουθήσει στενά τις αλλαγές στις τεχνολογίες συστημάτων και δικτύωσης.*

Ένα χρόνιο πρόβλημα που αποτρέπει τη ευρεία ανάπτυξη των συστημάτων ανίχνευσης εισβολών είναι η *ανικανότητά* τους *να καταστείλουν τους ψεύτικους συναγερμούς* (false alarms). Έχει παρουσιαστεί σε δοκιμή εργαστηρίων ότι υψηλής τεχνολογίας συστήματα ανίχνευσης εισβολών συχνά "καταρρέουν" (crash) κάτω από το φόρτο των ψεύτικων συναγερμών που παράγουν. Όταν εμφανίζονται οι πραγματικές επιθέσεις, είτε δεν ανιχνεύονται από το σύστημα ανίχνευσης εισβολών είτε τα ίχνη που αφήνει ο εισβολέας ή/και τα ίχνη που δείχνουν την πραγματική επίθεση χάνονται μέσα στο μεγάλο αριθμό των ψεύτικων συναγερμών κατά την καταγραφή των γεγονότων (log events).

Τα πράγματα γίνονται χειρότερα, διότι η αποτελεσματικότητα ενός συστήματος ανίχνευσης εισβολών αυξάνεται όσο μειώνεται ο αριθμός ψεύτικων συναγερμών. Στην έρευνά του, ο Axelsson πρότεινε ότι ένας ψεύτικος συναγερμός σε 100.000 γεγονότα ήταν η ελάχιστη απαίτηση για ένα σύστημα ανίχνευσης εισβολών έτσι ώστε να είναι αποτελεσματικό. Επομένως, η αρχική και πιθανώς η σημαντικότερη πρόκληση που πρέπει να αντιμετωπιστεί είναι η ανάπτυξη των αποτελεσματικών στρατηγικών για να μειωθεί το υψηλό ποσοστό ψεύτικων συναγερμών.

Κατά τη διάρκεια των ετών, πολυάριθμες τεχνικές, πρότυπα, και ολοκληρωμένα συστήματα ανίχνευσης εισβολών έχουν προταθεί και έχουν χτιστεί σε εμπορικούς και ερευνητικούς τομείς. Εντούτοις, δεν υπάρχει κανένα συνολικά αποδεκτό πρότυπο/μετρικό σύστημα για την αξιολόγηση ενός συστήματος ανίχνευσης εισβολών. Αν και η **R**eceiver **O**perating **C**haracteristic (**ROC**) **καμπύλη** (**curve**) έχει χρησιμοποιηθεί ευρέως για να αξιολογήσει την ακρίβεια των συστημάτων ανίχνευσης εισβολών και να αναλύσει την ανταλλαγή μεταξύ του ποσοστού ψευδών θετικών (false positives rate) και του ποσοστού

ανίχνευσης (detection rate), οι αξιολογήσεις βασισμένες στην ROC καμπύλη είναι συχνά παραπλανητικές ή/και ελλιπείς.



Εικόνα 11: Καμπύλη ROC που περιγράφει το ποσοστό επιθέσεων που ανιχνεύονται σε σχέση με το ποσοστό των ψεύτικων συναγερμών – Detection Performance.

Πρόσφατα, έχουν προταθεί διάφορες μέθοδοι για να αντιμετωπίσουν το ζήτημα αυτό. Εντούτοις, οι περισσότεροι, εάν όχι όλες, των προτεινόμενων λύσεων στηρίζονται στις *τιμές παραμέτρων (parameters values)* (όπως το κόστος που σχετίζεται με κάθε ψεύτικο συναγερμό ή τη χαμένη περίπτωση επίθεσης) που είναι δύσκολο να ληφθούν και είναι υποκειμενικές σε ένα συγκεκριμένο δίκτυο ή σύστημα. Κατά συνέπεια, τέτοιες μετρικές μπορούν να στερούνται την αντικειμενικότητα που απαιτείται για να πραγματοποιήσουν μια δίκαιη αξιολόγηση ενός δεδομένου συστήματος. Επομένως, μια από τις ανοικτές προκλήσεις είναι η ανάπτυξη μιας γενικής συστηματικής μεθοδολογίας ή/και ένα σύνολο μετρικών που μπορεί να χρησιμοποιηθεί με σκοπό την ορθή αξιολόγηση των IDS συστημάτων.

Υπάρχει μια έλλειψη ενός τυποποιημένου συνόλου δεδομένων αξιολόγησης που μπορεί να *εξομοιώσει (simulate)* τα ρεαλιστικά περιβάλλοντα δικτύων. Ενώ οι αξιολογήσεις ανίχνευσης εισβολών του 1998 και του 1999 από τα εργαστήρια DARPA/MIT Lincoln έχουν χρησιμοποιηθεί για να αξιολογήσουν έναν μεγάλο αριθμό συστημάτων ανίχνευσης εισβολών, η μεθοδολογία που χρησιμοποιείται για να παράγει τα δεδομένα αυτά είναι ακατάλληλη για τη εξομοίωση των πραγματικών περιβαλλόντων δικτύων. Επομένως, υπάρχει μια μεγάλη ανάγκη να χτιστεί ένα πιο κατάλληλο dataset αξιολόγησης. Η μεθοδολογία για την παραγωγή του dataset αξιολόγησης πρέπει όχι μόνο να εξομοιώσει τις ρεαλιστικές συνθήκες δικτύων αλλά και να είναι σε θέση να παράγει τα datasets που διαπλέκουν την κανονική (normal) με την ανώμαλη κυκλοφορία (anomalous traffic).

Μια σημαντική διάσταση της ανίχνευσης εισβολών, που έχει επίσης προταθεί ως "*evaluation metric"*, είναι η δυνατότητα ενός συστήματος ανίχνευσης εισβολών να αυτοπροστατευθεί από τις επιθέσεις. Οι επιθέσεις στα συστήματα ανίχνευσης εισβολών μπορούν να λάβουν διάφορες μορφές. Για παράδειγμα, αν θεωρήσουμε έναν επιτιθέμενο που στέλνει έναν μεγάλο όγκο από non-attack packets τα οποία είναι ειδικά φτιαγμένα για να προκαλούν πολλούς συναγερμούς μέσα σε ένα σύστημα ανίχνευσης εισβολών, κατακλύζει τον ανθρώπινο χειριστή με false positives ή καταρρέει (crash) τα εργαλεία επεξεργασίας ή παρουσίασης. Ο Axelsson, διαπίστωσε ότι μια πλειοψηφία των τότε διαθέσιμων συστημάτων ανίχνευσης εισβολών, λειτουργούσαν ανεπαρκώς όταν προσπαθούσαν να αυτοπροστατευθούν από τις επιθέσεις. Από τότε, η δυνατότητα των συστημάτων ανίχνευσης εισβολών στην αυτοάμυνα από τις επιθέσεις έχει βελτιωθεί οριακά.

Ένα άλλο πρόβλημα που θέτει ακόμα μια σημαντική πρόκληση είναι η προσπάθεια να καθοριστεί αυτό που είναι "*κανονικό-normal*" σε ένα δίκτυο. Για το λόγο αυτό, υπάρχει μια ανάγκη για την ανακάλυψη της σταθεράς των χαρακτηριστικών γνωρισμάτων μιας επίθεσης, "attack invariant". Η attack invariant θα ήταν ένα χαρακτηριστικό γνώρισμα του δικτύου/του συστήματος που μπορεί πάντα να επιβεβαιώνεται, εκτός από παρουσία μια επίθεσης. Τα παραδείγματα περιλαμβάνουν τον όγκο της κυκλοφορίας, τον αριθμό συνδέσεων στις μη κοινές πόρτες, κα. Προκειμένου να καθοριστούν τέτοιες σταθερές επίθεσης, είναι επιτακτική μια καλύτερη κατανόηση της φύσης των ανωμαλιών στο δίκτυο ή/και τον host.

Παραδοσιακά, η *κρυπτογράφηση (encryption)* είναι μια προτιμημένη μεθοδολογία για την διασφάλιση των δεδομένων και την παρεμπόδιση των κακόβουλων χρηστών από την πρόσβαση σε προνομιούχες/ιδιωτικές πληροφορίες. Εντούτοις, η διαδεδομένη χρήση της κρυπτογράφησης συνεπάγεται ότι οι διαχειριστές των δικτύων έχουν μια περιορισμένη άποψη του δικτύου δεδομένου ότι τα παραδοσιακά συστήματα ανίχνευσης εισβολών δεν έχουν τη δυνατότητα να αποκρυπτογραφούν τα κρυπτογραφημένα πακέτα τα οποία αναχαιτίζονται/παρεμποδίζονται (intercepted). Όταν ένα σύστημα ανίχνευσης εισβολών παρεμποδίζει ένα κρυπτογραφημένο πακέτο, τυπικά το απορρίπτει, το οποίο οδηγεί σε αυξημένη μείωση του ποσού της κυκλοφορίας που είναι σε θέση να εξετάσει. Επομένως, η πρόκληση για τους ερευνητές ασφάλειας είναι η ανάπτυξη μηχανισμών ασφάλειας που παρέχουν την ασφάλεια δεδομένων χωρίς να περιορίζουν τις λειτουργίες των συστημάτων ανίχνευσης εισβολών.

Ένα *αυξανόμενο πρόβλημα* στα σημερινά εταιρικά δίκτυα είναι οι *απειλές* που τίθενται από τα *μέλη (insiders)*, δηλαδή, τους δυσαρεστημένους υπαλλήλους. Σε μια έρευνα που διενεργήθηκε από United States Secret Service και CERT of Carnegie Mellon University, το

71% των ερωτηθέντων από τους 500 συμμετέχοντες ανέφερε ότι το 29% των επιθέσεων που γνώριζαν προκλήθηκαν εκ των έσω. Οι ερωτηθέντες ανέφεραν τους τρέχοντες ή προηγούμενους υπαλλήλους καθώς και τους αναδόχους/εργολάβους (contractors) ως τη δεύτερη μεγαλύτερη απειλή δικτυακής ασφάλειας, με τους χάκερ να προηγούνται. Η **σύνθεση** (**configuration**) ενός συστήματος ανίχνευσης εισβολών με σκοπό την ανίχνευση εσωτερικών επιθέσεων είναι πολύ δύσκολη. Η μέγιστη πρόκληση βρίσκεται στη δημιουργία ενός καλού **κανόνα** (**rule set**) που τίθεται για την ανίχνευση των εσωτερικών (internal) επιθέσεων ή των ανωμαλιών. Διαφορετικοί χρήστες δικτύων απαιτούν διαφορετικούς **βαθμούς πρόσβασης** (**degrees of access**) σε διαφορετικές υπηρεσίες, servers, και συστήματα για την εργασία τους, καθιστώντας το εξαιρετικά δύσκολο να καθορίσουν και να δημιουργήσουν τα συγκεκριμένα profiles των χρηστών και συστημάτων.

Ο βαθμός της απαιτούμενης ασφάλειας κρίνεται από το σκοπό της επεξεργασίας/εφαρμογής, τη φύση των δεδομένων που θα αποτελέσουν αντικείμενο της επεξεργασίας, τους κινδύνους που εγκυμονεί η συγκεκριμένη επεξεργασία και οι οποίοι πρέπει να προσδιοριστούν με σχετική ***Αποτίμηση Επικινδυνότητας (Risk Assessment)****, καθώς και από την εξέλιξη της τεχνολογίας και το κόστος των μέτρων.*

Παρόλο που τα συστήματα ανίχνευσης εισβολών είναι μια πολύτιμη προσθήκη στην υποδομή ασφάλειας ενός οργανισμού δεν πρέπει να τα θεωρούμε "πανάκεια". Κατά τη διάρκεια του σχεδιασμού της στρατηγικής ασφάλειας για τα συστήματα ενός οργανισμού, είναι σημαντικό να γνωρίζουμε ποια IDSs πρέπει και μπορούν να χρησιμοποιηθούν (δυνατότητες και περιορισμοί αυτών) καθώς και ποιοι στόχοι μπορούν να εξυπηρετηθούν καλύτερα από άλλους τύπους μηχανισμών ασφάλειας. Με την τρέχουσα μορφή τους τα IDSs παρέχουν σημαντική υποστήριξη στα ήδη υπάρχοντα μέτρα προστασίας ενός δικτύου και σε συνδυασμό με άλλους μηχανισμούς ασφάλειας, αποτελούν ένα σημαντικό εργαλείο για την παρακολούθηση και την αποτροπή δικτυακών επιθέσεων.

Η απειλή και η επικαιρότητα των εισβολών αποτελούν προδήλως μια πραγματικότητα. Τις περισσότερες φορές, οι οργανισμοί δεν είναι έτοιμοι να προστατευθούν από τις εισβολές. Εντούτοις, κάθε οργανισμός πρέπει να έχει μια πολιτική ασφάλειας και μια στρατηγική για να καταπολεμήσει την εισβολή, αποδοτικά και αποτελεσματικά. Η στρατηγική πρέπει να περιλάβει την προετοιμασία, τον έλεγχο, την ανίχνευση, την αποκατάσταση και την απάντηση. Εάν αυτό εφαρμόζεται, οι οργανισμοί θα είναι σε θέση να προστατεύσουν τα συστήματά τους, τα δίκτυα και τα ευαίσθητα στοιχεία τους.

ΠΑΡΑΡΤΗΜΑ Ι

Πίνακας 3: Ταξινόμηση των ερευνημένων συστημάτων σύμφωνα με τα χαρακτηριστικά του συστήματος

Name of system	Publ. year	Time of detection	Granularity	Audit source	Type of response	Data-processing	Data-collection	Security	Inter-oper.
Haystack [Sma88]	1988	non-real	batch	host	passive	centralised	centralised	low	low
MIDAS [SSHW88]	1988	real	continuous	host	passive	centralised	centralised	low	low
IDES [LJL+88]	1988	real	continuous	host	passive	centralised	distributed	low	low
W&S [VL89]	1989	real	continuous	host	passive	centralised	centralised	low	low
Comp-Watch [DR90]	1990	non-real	batch	host	passive	centralised	centralised	low	low
NSM [HDL+90]	1990	real	continuous	network	passive	centralised	centralised	low	low
NADIR [JDS91]	1991	non-real	continuous	host	passive	centralised	distributed	low	low
Hyperview [DBS92]	1992	real	continuous	host	passive	centralised	centralised	low	low
DIDS [SSTG92]	1992	real	continuous	both	passive	distributed	distributed	low	low
ASAX [HCMM92]	1992	real	continuous	host	passive	centralised	centralised	low	higher
USTAT [Ilg93]	1993	real	continuous	host	passive	centralised	centralised	low	low
DPEM [KFL94]	1994	real	batch	host	passive	distributed	distributed	low	low
IDIOT [KS94b]	1994	real	continuous	host	passive	centralised	centralised	low	higher
NIDES [AFV95]	1995	real	continuous	host	passive	centralised	distributed	low	higher
GrIDS [rCCF+96]	1996	non-real	batch	both	passive	distributed	distributed	low	low
CSM [WP96]	1996	real	continuous	host	active	distributed	distributed	low	low
Janus [GWTB96]	1996	real	continuous	host	active*	centralised	centralised	low	low
JiNao [JGS+97]	1997	real	batch	host	passive	distributed	distributed	low	low
EMERALD [PN97]	1997	real	continuous	both	active	distributed	distributed	moderate	high
Bro [Pax88]	1998	real	continuous	network	passive	centralised	centralised	higher	low

Η Ιστορία του IDS

Το 1980, ο *James Anderson* αρχικά πρότεινε ότι οι *διαδρομές ελέγχου (audit trails)* πρέπει να χρησιμοποιηθούν για να ελέγξουν (monitor) τις απειλές. Η σημασία τέτοιων δεδομένων δεν ήταν αντιληπτή εκείνη τη στιγμή και όλες οι διαθέσιμες διαδικασίες ασφάλειας συστημάτων στράφηκαν στην άρνηση της πρόσβασης στα ευαίσθητα δεδομένα από μια αναρμόδια πηγή. Το 1987, η *Dorothy Denning* παρουσίασε ένα *αφηρημένο πρότυπο (abstract model)* ενός συστήματος ανίχνευσης εισβολών. Αυτή η εργασία ήταν η πρώτη για να προτείνει την έννοια της ανίχνευσης εισβολών ως λύση στο πρόβλημα παρέχοντας μια αίσθηση της ασφάλειας στα δίκτυα των ηλεκτρονικών υπολογιστών. Ήταν περισσότερο μια αναδρομική προσέγγιση, σε σύγκριση με τις παραδοσιακές δυναμικές μεθόδους κρυπτογράφησης και ελέγχου πρόσβασης. Το 1988, το *Δικτυακό σκουλήκι (Internet worm)* ,επίσης γνωστό ως σκουλήκι Morris, κατέστησε το Διαδίκτυο να είναι μη διαθέσιμο για περίπου πέντε ημέρες. Αυτό το γεγονός έφερε την ανάγκη για την ασφάλεια υπολογιστών στο προσκήνιο.

Το ίδιο έτος η *Teresa Lunt και άλλοι* τελειοποίησαν το πρότυπο ανίχνευσης εισβολών που προτάθηκε από την *Denning* και δημιούργησαν το ***IDES (Intrusion Detection Expert System)***. Αυτό το σύστημα σχεδιάστηκε για να ανιχνεύσει τις προσπάθειες εισβολών ενάντια σε έναν υπολογιστή (host). Μια βελτιωμένη έκδοση αναπτύχθηκε το 1995, το ***NIDES (Next-generation Intrusion Detection Expert System)***. Επίσης το 1988, το σύστημα ***Haystack*** αναπτύχθηκε προκειμένου να βοηθηθούν οι Air Force Security Officers να ανιχνεύσουν την κακή χρήση των κεντρικών υπολογιστών (mainframes) που χρησιμοποιήθηκαν στις βάσεις της Πολεμικής Αεροπορίας, και ο ***MIDAS (Multics Intrusion Detection and Alerting System)*** δημιουργήθηκε για τους ίδιους λόγους, αλλά για τον National Computer Security Center's Multics κεντρικό υπολογιστή. Το 1989, είχαμε το ***Wisdom and Sense*** από το εθνικό εργαστήριο Los Alamos, και το ***Information Security Officer's Assistant (ISOA)*** από την Planning Research Corporation.

Μια νέα ιδέα εισήχθη το 1990, με ***NSM (Network Security Monitor***, αποκαλούμενο σήμερα ***Network Intrusion Detector*** ή ***NID***) όπου, αντί της εξέτασης των audit trails ενός host συστήματος υπολογιστών, η ύποπτη συμπεριφορά ανιχνεύθηκε παθητικά ελέγχοντας τη δικτυακή κυκλοφορία στο LAN. Το 1991, μια διαφορετική ιδέα εισήχθη με το ***NADIR (Network Anomaly Detection and Intrusion Reporter)*** και το ***DIDS (Distributed Intrusion Detection System)***. Εδώ τα audit data από διαφορετικούς hosts συλλέχθηκαν προκειμένου να ανιχνευθούν οι συντονισμένες επιθέσεις ενάντια σε ένα σύνολο από hosts. Το 1994, οι *Mark*

Crosbie και Gene Spafford πρότειναν τη χρήση των *αυτόνομων αντιπροσώπων (autonomous agents)* προκειμένου να βελτιωθεί η εξελιξιμότητα, η συντήρηση, η αποδοτικότητα και η ανοχή σε σφάλματα ενός IDS.

Μια άλλη προσέγγιση για να εξετάσει τις ανεπάρκειες εξελιξιμότητας στα περισσότερα σύγχρονα συστήματα ανίχνευσης εισβολών προτάθηκε το 1996, με το σχεδιασμό και την πραγματοποίηση του ***GrIDS (Graph-Based Intrusion Detection System).*** Αυτό το σύστημα διευκολύνει την ανίχνευση των μεγάλης-κλίμακας αυτοματοποιημένων ή συντονισμένων επιθέσεων, οι οποίες μπορούν ακόμη και να εκταθούν σε πολλαπλές διοικητικές περιοχές. Το 1998, οι *Ross Anderson και Abida Khattak* πρόσφεραν μια καινοτόμο προσέγγιση στην ανίχνευση εισβολών, με την ενσωμάτωση των *τεχνικών ανάκτησης πληροφοριών (informational retrieval techniques)* στα εργαλεία ανίχνευσης εισβολών. Και καθώς η έρευνα στον τομέα αυτό συνεχίζεται, βλέπουμε ότι αυτό το πρότυπο προτείνεται ως απάντηση στις απαιτήσεις ασφάλειας άλλων τεχνολογικών περιοχών, όπως τα *κινητά δίκτυα (mobile networks)*.

ΠΑΡΑΡΤΗΜΑ ΙΙ

Το Snort 2.0

1. Γενική περιγραφή του Snort 2.0

Το Snort είναι ένα Open Source και lightweight NIDS που μέχρι την έκδοση 1.9.1 το χρησιμοποιούσαν σε δίκτυα μικρού σχετικά μεγέθους και με μικρό σχετικά bandwidth μέχρι ***100Mbps***. Όμως από την έκδοση 2.0 και μετά άλλαξε ριζικά ο μηχανισμός εντοπισμού (Detection engine) με την νέα "Hi-performance Multi-Rule Inspection engine" και έτσι το snort μπορεί να χρησιμοποιηθεί και σε δίκτυα με ***Gigabit*** Bandwidth.Ο δημιουργός του είναι ο *Martin Roesch* και ο κώδικας του είναι γραμμένος σε C. Το Snort εκτός από την λειτουργία του σαν NIDS μπορεί να δουλέψει και σαν ένας απλός sniffer ή σαν ένας sniffer που καταγράφει (logging) τα πακέτα που λαμβάνει σε log αρχεία σε μορφή απλού κειμένου ASCII. Έχει λοιπόν τρία modes λειτουργίας που περιγράφονται παρακάτω είναι:

i. **Sniffer** mode.
ii. **Packet logger** mode.
iii. **NIDS** mode.

1.1. Sniffer Mode

Σε αυτό το mode λειτουργίας το Snort έχει την ικανότητα να διαβάζει τα πακέτα που περνάνε από το δίκτυο, να τα αποκωδικοποιεί και να τα εμφανίζει στην οθόνη σε φιλική μορφή για τον χρήστη.

Ο χρήστης με διάφορα BPF (Berkley Packet Filter) φίλτρα που μπορεί να χρησιμοποιήσει, έχει την δυνατότητα να ορίσει το είδος των πακέτων που θα εμφανίζονται όσο αναφορά το πρωτόκολλο, τον αποστολέα, τον παραλήπτη και διάφορα άλλα χαρακτηριστικά ενός πακέτου. Για παράδειγμα αν γράψει την λέξη κλειδί **icmp** στο snort τότε αυτό θα δείχνει μόνο τα πακέτα που είναι τύπου ICMP. Η λειτουργία αυτή του Snort είναι παρόμοια με αυτή του γνωστού εργαλείου tcpdump, το οποίο διατίθεται κυρίως με τα περισσότερα *λειτουργικά συστήματα* της οικογένειας του **Unix**.

1.2. Packet Logger Mode

Σε αυτό το mode λειτουργίας το Snort αποθηκεύει στο δίσκο τα πακέτα που διαβάζει από το δίκτυο, αντί απλά να τα εμφανίζει στην οθόνη. Η διαδικασία αυτή είναι αρκετά σημαντική στην περίπτωση που απαιτείται τα πακέτα αυτά να εξεταστούν με λεπτομέρεια σε επόμενο στάδιο.

Το Snort μπορεί να αποθηκεύσει τα πακέτα αυτά σε διάφορα formats, ανάλογα με τις ανάγκες του χρήστη. Για παράδειγμα μπορεί να αποθηκεύσει τα πακέτα σε binary μορφή (tcpdump format), με την οποία μπορούν να χρησιμοποιηθούν σαν είσοδο σε διάφορα άλλα προγράμματα ανάλυσης πακέτων και πρωτοκόλλων, σε ASCII μορφή ώστε να είναι δυνατή η ανάγνωσή τους, σε XML μορφή ή και να οργανωθούν σε βάσεις δεδομένων.

Είναι σημαντικό να σημειωθεί εδώ ότι αυτό το mode μπορεί να λειτουργεί παράλληλα με το *sniffer mode* ή το *NIDS mode* και δεν λειτουργεί υποχρεωτικά ανεξάρτητα από τα αλλά mode.

1.3. NIDS Mode

Αυτή είναι η κύρια λειτουργία του Snort. Όπως αναφέρθηκε προηγουμένως, το Snort είναι ένα IDS το οποίο ενεργεί σε επίπεδο δικτύου, δηλαδή τα γεγονότα που παρακολουθεί και εξετάζει για την εμφάνιση μίας πιθανής επίθεσης, αφορούν την δραστηριότητα που παρατηρείται σε ένα δίκτυο. Το Snort έχει την ικανότητα να ανιχνεύει ένα μεγάλο φάσμα από γνωστές δικτυακές επιθέσεις, όπως *portscans, buffer overflows, OS fingerprints* και πολλά άλλα.

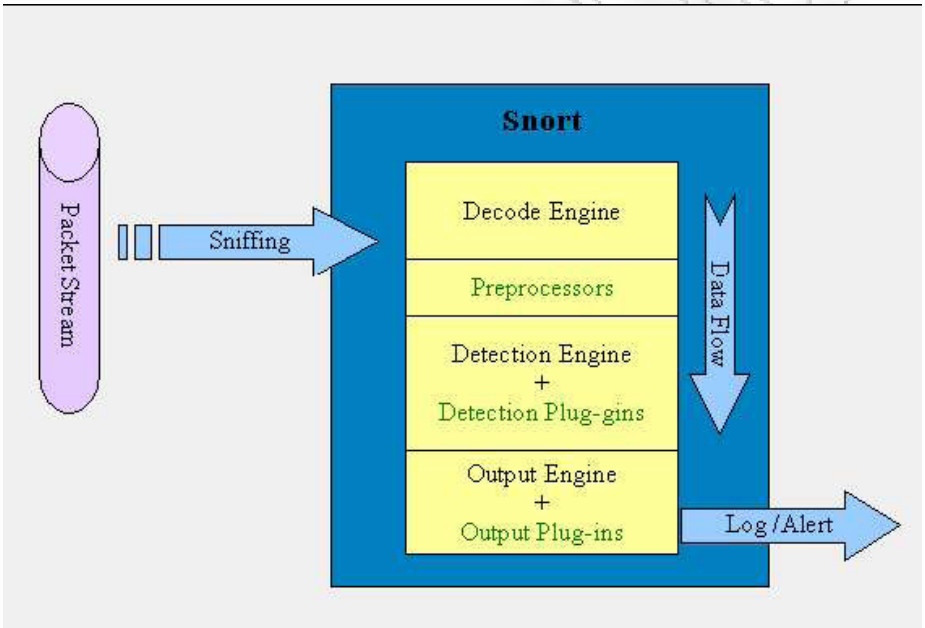
Η τεχνική που χρησιμοποιεί το Snort για την διαδικασία αυτή είναι κατά κύριο λόγο η *Misuse Detection* με την χρήση των *Signatures* ενός βλαβερού (malicious) πακέτου. Το Snort όμως ειδικά μετά την έκδοση 2.0 συνδυάζει την λειτουργία της ανάλυσης των γεγονότων με κάποιες από τις μεθόδους του ***Protocol Anomaly Detection*** και του ***Anomaly Detection*** για την ανίχνευση πιθανών επιθέσεων. Οι μηχανισμοί αυτοί υλοποιούνται κατά κύριο λόγο από τους preprocessors αλλά και από το νέο μηχανισμό του snort 2.0 να συντάσσει τα rules.

2. Η Μηχανή του Snort2.0

Το Snort αποτελείται από τέσσερα υποσυστήματα λειτουργίας. Κάθε πακέτο που επεξεργάζεται το Snort, θα περάσει από κάθε ένα από αυτά τα υποσυστήματα :

- Packets capturing και decoding engine.
- Rules parsing και detection engine που αντικαταστάθηκε με την Hi-performance Multi-Rule Inspection engine.
- Logging ή Output engine.
- Detection plugins, Output plugins and Preprocessors handling engine.

Το σχήμα που ακολουθεί παρουσιάζει την δομή του Snort, όσο αναφορά τα υποσυστήματα από τα οποία αποτελείται και αναπαριστά την διαδρομή που ακολουθεί κάθε πακέτο κατά την επεξεργασία του από το Snort.



Εικόνα 12: Δομή του Snort.

3. Snort Signatures και Alerts

Το Snort χρησιμοποιεί αρχεία με υπογραφές που ταιριάζουν κάποια χαρακτηριστικά μιας συγκεκριμένης επικοινωνίας. Τα ***Signatures*** του ***Snort*** ονομάζονται και ***Rules***, καθώς είναι κανόνες οι οποίοι περιγράφουν τα χαρακτηριστικά ενός πακέτου που μπορεί να είναι μέρος μίας γνωστής επίθεσης, καθώς και την ενέργεια που θα εκτελεστεί κατά τον εντοπισμό του. Κάθε πακέτο που εντοπίζεται από το Snort, ελέγχεται για το αν έχει τα ίδια χαρακτηριστικά με αυτά που περιγράφονται από κάποιο Rule. Τα Rules του Snort μπορούν να γραφτούν σε απλή περιγραφική γλώσσα σε ASCII μορφή και κάθε ένα από αυτά αποτελείται από δύο λογικά μέρη, τον *Rule Header* και τα *Rule Options*.

Παράδειγμα υπογραφής του Snort είναι το εξής:

alert tcp $EXTERNAL_NET 27374 -> $HOME_NET any (msg:"BACKDOOR subseven

22";flow:to_server,established;content:"|

0d0a5b52504c5d3030320d0a|";reference:arachnids,485; reference:url,

www.hackfix.org/subseven/; classtype:misc-activity; sid:103; rev:5;)

Ο κανόνας αυτός θα δημιουργήσει ένα ***Alert*** όταν εντοπίσει το backdoor subseven. Η υπογραφή ταιριάζει τα πακέτα που περιέχουν το string 0d0a5b52504c5d3030320d0a, το οποίο είναι χαρακτηριστικό του subseven.

Ο επόμενος κανόνας εντοπίζει το *buffer overflow* στον iis με webdav που ανακαλύφθηκε το 2003:

alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"WEB-

IIS WEBDAV exploit attempt"; flow:to_server,established;
content:"HTTP/1.1|0a|Content-

type|3a| text/xml|0a|HOST|3a|"; content:"Accept|3a| |2a|/|2a0a|Translate|3a|

f|0a|Contentlength| 3a| 5276|0a0a|"; distance:1; reference:cve,CAN-2003-0109;

reference:bugtraq,7716; classtype:attempted-admin; sid:2090; rev:2;)

Ανάλυση και ταίριασμα υπογραφών εκτός από το Snort κάνουν και τα υπόλοιπα intrusion detection συστήματα, αλλά ακόμα και το iptables, το πολύ διάσημο open source packet filter/firewall.

Το Snort διανέμεται με πάνω από 2500 έτοιμα *Signatures*, για χρήση τους στην ανίχνευση γνωστών επιθέσεων, ενώ για την δημιουργία νέων *Rules* προσφέρει μία μεγάλη γκάμα από options που μπορεί ο χρήστης να χρησιμοποιήσει, τα οποία του δίνουν την ευελιξία να εκτελεί λεπτομερής και σε βάθος περιγραφή των χαρακτηριστικών του κάθε πακέτου, για το οποίο θέλει να γίνει έλεγχος για τον εντοπισμό μίας επίθεσης. Επίσης υπάρχει και το site bleeding snort rules στο οποίο δημοσιεύονται πειραματικά *rules*, τα οποία μετά από λίγο καιρό ενσωματώνονται σαν επίσημα *rules* για το Snort. Όταν το Snort ανιχνεύσει μία επίθεση έχει την δυνατότητα να γνωστοποιήσει τα αποτελέσματά του με διάφορους τρόπους, με την μορφή *alerts*. Κάποιοι από αυτούς είναι, σε πραγματικό χρόνο με την χρήση αναδυόμενων παραθύρων στην οθόνη, σε ASCII μορφή στην κονσόλα, να τα

αποθηκεύσει σε αρχεία σε ASCII μορφή για μετέπειτα ανάγνωση ή και να τα οργανώσει σε βάσεις δεδομένων όπως MySQL, PostgreSQL,Oracle, unixODBC, κ.α. Ένα *alert* μπορεί να δώσει πληροφορίες για μια επίθεση, όπως το είδος της, τον επιτιθέμενο και το στόχο, αν είναι υψηλής προτεραιότητας ή όχι και φυσικά ποια πακέτα οδήγησαν στην ανίχνευση της επίθεσης.

Στο παρακάτω σχήμα παρουσιάζεται ένα *alert* του Snort.

[**] [1:553:4] POLICY FTP anonymous login attempt [**] [Classification: Misc activity] [Priority: 3] 03/11-12:23:37.280737 192.168.0.9:1245 -> 192.168.100.25:21 TCP TTL:128 TOS:0x0 ID:13318 IpLen:20 DgmLen:56 DF ***AP* Seq: 0x74603DEF Ack: 0x7B16BDCC Win: 0xFAB2 TcpLen: 20**

Το alert αυτό δημιουργήθηκε από το Snort καθώς εντόπισε μία προσπάθεια για σύνδεση ενός χρήστη σαν anonymous, στον ftp server με την IP διεύθυνση 192.168.100.25. Κάποιοι ftp servers επιτρέπουν την χρήση τους από χρήστες που δεν έχουν έναν εξουσιοδοτημένο λογαριασμό, αν αυτοί συνδεθούν με το username anonymous και δώσουν για password την mail διεύθυνσή τους. Αυτό όμως μπορεί να δημιουργήσει τρύπες ασφάλειας σε έναν ftp server και για αυτό κάποιοι δεν επιτρέπουν την χρήση του κοινού λογαριασμού anonymous. Στην περίπτωση που ο συγκεκριμένος ftp server δεν επιτρέπει σε χρήστες χωρίς κάποιο εξουσιοδοτημένο προσωπικό λογαριασμό να συνδεθούν σε αυτόν, τότε αυτό το alert μπορεί να είναι μία ένδειξη για προσπάθεια παραβίασης του συστήματος. Στο δείγμα του alert που παρουσιάζεται αναφέρεται η ώρα που ανιχνεύτηκε το γεγονός καθώς και το είδος της επίθεσης που εντοπίστηκε, ενώ ακολουθεί περιγραφή των χαρακτηριστικών του πακέτου που οδήγησε στην δημιουργία του alert.

ΠΑΡΑΡΤΗΜΑ ΙΙΙ

Παρουσίαση δημοφιλών Συστημάτων Ανίχνευσης Εισβολών

1. RealSecure (Internet Security Systems)

Προϊον	**RealSecure**
Κατασκευαστής	Internet Security Systems (ISS)
Υποστηριζόμενες πλατφόρμες	Solaris (Sparc and x86), Windows NT
Πηγή δεδομένων	Δικτυακή & Τερματική
Μοντέλο ανίχνευσης	Μοντέλο ανίχνευσης βασισμένο σε κανόνες
Συμπεριφορά	Ανίχνευση & Απόκριση

1.1. Εισαγωγή

Ο ανιχνευτής RealSecure λειτουργεί με δικτυακή και τερματική λογική και έχει σύστημα απόκρισης που λειτουργεί σε πραγματικό χρόνο (real time response). Χρησιμοποιεί προκαθορισμένα σχήματα επιθέσεων ή εσφαλμένων χρήσεων, για να ανιχνεύσει ενέργειες που παραβιάζουν την δεδηλωμένη πολίτικη ασφάλεια της επιχείρησης.

1.2. Αρχιτεκτονική

Η αρχιτεκτονική του RealSecure αποτελείτε από τρεις βασικές λειτουργικές μονάδες:

- Μηχανή του RealSecure (RealSecure Engines)
- Εντολοδόχους του RealSecure (RealSecure Agents)
- Γενικός διαχειριστής (RealSecure Manager)

Οι μηχανές του RealSecure «τρέχουν» σε αποκλειστικά για αυτήν την εργασία τερματικά και παγιδεύουν και στην συνέχεια αναλύουν τα πακέτα που κυκλοφορούν στο υπό παρακολούθηση δίκτυο. Τα πακέτα αυτά που παγιδεύονται συγκρίνονται με γνωστά σενάρια επιθέσεων που είναι καταχωρημένα στις βάσεις δεδομένων, ελπίζοντας ότι μπορεί να διαχωρίσει μεταξύ τους επιθέσεις που τυχών να συμβαίνουν ταυτόχρονα.

Η εσωτερική αρχιτεκτονική της μηχανής του RealSecure αποτελείτε από πέντε βασικές μονάδες:

i. Interface δικτύου

ii. Μονάδα παγίδευσης πακέτων

iii. Μονάδα φιλτραρίσματος

iv. Μονάδα αναγνώρισης επίθεσης

v. Μονάδα απόκρισης

Οι εντολοδόχοι (agents) είναι οι ομόλογοι της μηχανής του RealSecure βασιζόμενοι όμως σε τερματική λογική (δηλ. τρέχουν σε αυτόνομα τερματικά στοιχεία του δικτύου). Οι εντολοδόχοι αναλύουν τα αρχεία ημερολογίου των τερματικών με παρόμοιο τρόπο με αυτόν που χρησιμοποιεί η μηχανή του RealSecure για την ανάλυση των πακέτων του δικτύου. Εφόσον έχει ανιχνευτεί επίθεση ο εντολοδόχος έχει την δυνατότητα να τερματίσει διεργασίες του συστήματος ή να απενεργοποιήσει λογαριασμούς χρηστών. Οι εντολοδόχοι του RealSecure έχουν ακόμα την δυνατότητα να αναδιαμορφώσουν τόσο την μηχανή όσο και τους firewalls, έτσι ώστε να εμποδίσουν/μπλοκάρουν πιθανές μελλοντικές επιθέσεις/εισβολές από συγκεριμένες πηγές. Προς το παρών, το λογισμικό τω εντολοδόχων διατίθεται μόνο για πλατφόρμες Windows NT.

Ο γενικός διαχειριστής του RealSecure είναι μια κονσόλα διαχείρισης που δίνει την δυνατότητα συνολικής παρακολούθησης με γραφικό περιβάλλον όλου του συστήματος καθώς και της μηχανής και των εντολοδόχων που προαναφέρθηκαν. Η κονσόλα υποστηρίζει τρεις βασικές υπηρεσίες:

- ☞ Κεντρική παρουσίαση συναγερμών σε πραγματικό χρόνο
- ☞ Κεντρική διαχείριση δεδομένων
- ☞ Κεντρική ρύθμιση (configuration) της μηχανής του RealSecure

2. Intruder Alert (Axent Technologies)

Προϊον	**Intruder Alert**
Κατασκευαστής	Axent Technologies Inc.
Υποστηριζόμενες πλατφόρμες	Solaris (Sparc), SunOS, Windows 98/NT, NetWare, AIX, Digital Unix, HP-UX, IRIX, SVR4 (Motorolla 88000), AT&T GIS (NCR), OpenVMS
Πηγή δεδομένων	Δικτυακή & Τερματική
Μοντέλο ανίχνευσης	Μοντέλο ανίχνευσης βασισμένο σε κανόνες
Συμπεριφορά	Ανίχνευση & Απόκριση

2.1. Εισαγωγή

Το Intruder Alert είναι ένα πραγματικού χρόνου, βασισμένο σε κανόνες σύστημα ανίχνευσης ηλεκτρονικών εισβολών. Παρακολουθεί τα ακολουθιακά δεδομένα ελέγχου των τερματικών μέσα σε ένα κατανεμημένο περιβάλλον. Η ανίχνευση των προσπαθειών εισβολών βασίζεται σε κανόνες ή απρόβλεπτα λάθη του συστήματος (exceptions). Η μηχανή που βασίζεται σε κανόνες αναζητά συγκεκριμένες και προκαθορισμένες ακολουθίες δεδομένων. Οι ακολουθίες αυτές ονομάζονται «χνάρια» (footprints) και αναγνωρίζουν μονοσήμαντα ανώμαλες συμπεριφορές/πλάνα μέσα στα ακολουθιακά δεδομένα ελέγχου των τερματικών (audit trails).

2.2. Αρχιτεκτονική

Το Intruder Alert αποτελείτε από τρεις βασικές λειτουργικές μονάδες:

- Interface κονσόλας (interface concole)
- Γενικός διαχειριστής (Manager)
- Εντολοδόχοι (Agent)

Το interface κονσόλας καθώς και ο γενικός διαχειριστής επιτρέπουν την ρύθμιση των κανόνων σύμφωνα με την πολίτικη ασφάλειας της επιχείρησης. Παρότι οι *διαχειριστές συναγερμού* και οι *εντολοδόχοι του Intruder Alert* υποστηρίζονται από πληθώρα λειτουργικών συστημάτων (συμπεριλαμβανομένου του UNIX), η κονσόλα και ο γενικός διαχειριστής υποστηρίζονται μόνο από τα Windows NT.

Οι εντολοδόχοι είναι διεργασίες και δαίμονες (daemons) που «τρέχουν» στα τερματικά που είναι υπό παρακολούθηση. Οι εντολοδόχοι συλλέγουν δεδομένα ελέγχου και εφαρμόζουν το

σύνολο κανόνων όπως αυτό έχει ρυθμιστεί από τον administrator του συστήματος. Όλοι οι *εντολοδόχοι* πρέπει να έχουν καταχωρηθεί στον *γενικό διαχειριστή*, για να γίνει εφικτή η ρύθμισή τους. Στην φάση της καταχώρησης αυτής, δημιουργείται ένα ασφαλές κανάλι επικοινωνίας με σκοπό να προστατεύσει τα δεδομένα που ανταλλάσσονται μεταξύ των συμμετεχόντων στοιχείων του δικτύου.

Πρόσθετα Χαρακτηριστικά

Net Prowler

Εκτός από την ανάλυση δεδομένων σε τερματική βάση το Intruder Alert έχει την δυνατότητα να αναλύσει και τα πακέτα του συστήματος δικτυακά. Η διεργασία αυτή πραγματοποιείται στην ουσία από ξεχωριστό προϊόν. Αυτό συλλέγει δεδομένα από τα interface των καρτών δικτύου, γεγονός που επιτρέπει στον εντολοδόχο να παγιδεύσει πακέτα που προορίζονται σε άλλες διευθύνσεις εκτός από την δική του. Η Axent Technologies αποκαλεί την παραπάνω διεργασία «**Τεχνολογία Net Prowler**». Το Net Prowler υποστηρίζεται μόνο από πλατφόρμα Windows NT.

Μονάδα Περίπολου (PATROL module)

Οι οργανισμοί που έχουν στην διάθεσή τους μεγάλα δίκτυα και σημαντικό αριθμό τερματικών, χρησιμοποιούν συνήθως κάποια εφαρμογή διαχείρισης δικτύου/τερματικών έτσι ώστε να μειώσει το κόστος συντήρησης και εποπτείας. Διαχείριση Ασφάλειας σημαίνει ότι αυτές καθαυτές οι διαδικασίες διαχείρισης πρέπει να είναι ασφαλισμένες και ότι μόνο οι εξουσιοδοτημένοι χρήστες έχουν την δυνατότητα να εκτελέσουν τέτοιες διαδικασίες. Διαχείριση Ασφάλειας σημαίνει ότι οι παράμετροι του συστήματος ασφαλείας μπορούν να ρυθμιστούν με την ίδια ευκολία που ρυθμίζεται οποιαδήποτε άλλη παράμετρος του δικτύου ή των τερματικών.

Η Μονάδα Περίπολου από την BMC Software είναι ένα ολοκληρωμένο πακέτο προγραμμάτων που μπορεί να χρησιμοποιηθεί στην διαχείριση πολύπλοκων δικτυακών δομών μέσα σε ένα κατανεμημένο περιβάλλον.

3. NetRanger (Cisco Systems, Inc)

Προϊον	**NetRanger**
Κατασκευαστής	Cisco Systems, Inc
Υποστηριζόμενες πλατφόρμες	Εξειδικευμένο hardware και Solaris x86 v.2.6
Πηγή δεδομένων	Δικτυακή
Μοντέλο ανίχνευσης	Μοντέλο ανίχνευσης βασισμένο σε κανόνες
Συμπεριφορά	Ανίχνευση & Απόκριση

3.1. Εισαγωγή

Το NetRanger είναι ένα πραγματικού χρόνου σύστημα ανίχνευσης ηλεκτρονικών εισβολών σχεδιασμένο έτσι ώστε να εντοπίζει επιθέσεις μέσα στην δικτυακή υποδομή των επιχειρήσεων. Είναι αμιγώς σύστημα με δικτυακή λογική και αναλύει διεξοδικά τα πακέτα που κυκλοφορούν στο δίκτυο. Το μοντέλο ανίχνευσης «εσφαλμένης χρήσης» χρησιμοποιείται στον εντοπισμό παραβιάσεων της πολιτικής ασφάλειας της επιχείρησης. Ακόμα το NetRanger έχει δυνατότητες απόκρισης σε πραγματικό χρόνο με ενέργειες όπως ο τερματισμός συγκεκριμένων συνδέσεων και το μπλοκάρισμα αναμενόμενων προσπαθειών εισβολής.

3.2. Αρχιτεκτονική

Το NetRanger αποτελείτε από τρεις βασικές λειτουργικές μονάδες:

- Αισθητήρες (Sensors)
- Οδηγό (Director)
- Διαδικασίες Post Office

Η αρχιτεκτονική συστήματος του NetRanger είναι από τα πολύ δυνατά σημεία του. Οι αισθητήρες σε συνδυασμό με τους οδηγούς μπορούν να σχηματίσουν ιεραρχικές δομές, που επιτρέπουν την παρακολούθηση μεγάλου αριθμού δικτυακών τμημάτων (network segments).

Οι αισθητήρες του συστήματος είναι αυτές που παρακολουθούν την κίνηση στο δίκτυο και συλλέγουν σχετικές πληροφορίες. Υπό φυσιολογικές συνθήκες, ένας αισθητήρας παρακολουθεί την κίνηση σε ένα και μόνο τμήμα του δικτύου. Ένα εξειδικευμένο σύστημα χρησιμοποιείται για να μειώσει την κίνηση στο δίκτυο. Η ύποπτες συμπεριφορές ανιχνεύονται με τον εντοπισμό συγκεκριμένων ακολουθιών δυαδικών δεδομένων. Επιπρόσθετα το NetRanger ελέγχει και τα αρχεία συστήματος των δρομολογητών της Cisco, για πιθανές παραβιάσεις.

Στην σημερινή έκδοση του προϊόντος οι αισθητήρες διατίθενται για Ethernet, Fast Ethernet, Token Ring και FDDI.

Το NetRanger αποκρίνεται σε πιθανές παραβιάσεις της πολιτικής ασφάλειας με τον τερματισμό ενεργών TCP συνδέσεων ή την ενημέρωση των καταλόγων ελέγχου πρόσβασης(ACL) των δρομολογητών ή των firewall.

Ο *Οδηγός* παρέχει την δυνατότητα κεντρικής διαχείρισης των αισθητήρων που είναι κατανεμημένοι μέσα στο δίκτυο. Από τον Οδηγό ο διαχειριστής του συστήματος μπορεί να ρυθμίσει τους αισθητήρες και να αναλύσει τα ενδεχόμενα κενά ασφαλείας στο σύστημα. Ο Οδηγός χρησιμοποιείται ακόμα για την εξαγωγή δεδομένων σε συστήματα αναφορών (reporting systems) και το download/δημιουργία νέων σχεδίων επίθεσης.

Οι διαδικασίες Post Office χειρίζονται την επικοινωνία μεταξύ του Οδηγού και των *Αισθητήρων*. Οι διαδικασίες αυτές χρησιμοποιούν ένα πρωτόκολλο εφαρμογής βασισμένο στο UDP με χαρακτηριστικά για εξουσιοδότηση και μηχανισμούς ελέγχου δυσλειτουργιών (fault tolerance).

4. POLYCENTER (Compaq)

Προϊον	**POLYCENTER**
Κατασκευαστής	Compaq (former Digital Equiment Corp.)
Υποστηριζόμενες πλατφόρμες	SunOS, Open VMS
Πηγή δεδομένων	Τερματική
Μοντέλο ανίχνευσης	Μοντέλο ανίχνευσης βασισμένο σε κανόνες και σε ευρεση ανωμαλιών
Συμπεριφορά	Ανίχνευση & Απόκριση

4.1. Εισαγωγή

Το POLYCENTER είναι ανιχνευτής ηλεκτρονικών εισβολών που λειτουργεί βασισμένο σε τερματική λογική που σημαίνει ότι είναι εγκατεστημένο στα τερματικά που είναι κατανεμημένα μέσα στο δίκτυο. Εντοπίζει εισβολές και προσπάθειες εισβολής εξετάζοντας τα αρχεία ελέγχου στα επιμέρους τερματικά.

Το POLYCENTER μπορεί να ρυθμιστεί έτσι ώστε να ανιχνεύει πολλαπλές κατηγορίες εισβολών όπως:

- Προσπάθειες εκτέλεσης προγραμμάτων χωρίς εξουσιοδότηση
- Ύποπτες μεταφορές αρχείων μέσα στο δίκτυο
- Ύποπτες ενέργειες προς κάποιο τερματικό, χρήστη ή αρχείο
- Δραστηριότητες εκτός του κανονικού ωραρίου εργασίας

Η ανάλυση των δεδομένων ελέγχου χρησιμοποιεί διαδικασίες τεχνητής νοημοσύνης (AI) που σχεδιάστηκαν στα πλαίσια έρευνας από την Digital Equipment Corp. Οι πληροφορίες που υπάρχουν σε σχέση με τα γνωστά σενάρια επίθεσης χρησιμοποιούνται από το POLYCENTER, για να εντοπιστούν ύποπτες δραστηριότητες που θα μπορούσαν να υποδείξουν επίθεση προς κάποιο τερματικό στοιχείο του δικτύου. Ένα μοντέλο «περιπτώσεων» (case model) χρησιμοποιείται για να αναθέσει σε συγκεκριμένους εικονικούς εντολοδόχους του συστήματος ανίχνευσης (agents) την παρακολούθηση ύποπτων συμπεριφορών. Ο εικονικός εντολοδόχος παρακολουθεί τον ύποπτο και τα αποδεικτικά στοιχεία (log files) της υπόθεσης. Με την ανάλυση των γεγονότων ασφάλειας (security events) ανά υπόθεση/περίπτωση, το POLYCENTER είναι σε θέση να διακρίνει τις πραγματικές απειλές από τις απλές λανθασμένες συμπεριφορές.

5. Network Flight Recorder (Network Flight Recorder, Inc.)

Προϊον	**Network Flight Recorder**
Κατασκευαστής	Network Flight Recorder, Inc.)
Υποστηριζόμενες πλατφόρμες	Windows NT, Solaris (Sparc)
Πηγή δεδομένων	Δικτυακή
Μοντέλο ανίχνευσης	Μοντέλο ανίχνευσης βασισμένο σε κανόνες
Συμπεριφορά	Ανίχνευση & Απόκριση

5.1. Εισαγωγή

Το Network Flight Recorder (**NFR**) δεν μπορεί να χαρακτηριστεί ως ένα αμιγές σύστημα ανίχνευσης ηλεκτρονικών εισβολών, παρότι έχει αρκετά χαρακτηριστικά ενός IDS. Όπως καταδεικνύει και το όνομα του προϊόντος το Network Flight Recorder σχεδιάστηκε με πρωταρχικό στόχο την επίτευξη μιας μεταμοντέρνας ανάλυσης των γεγονότων που συμβαίνουν σε ένα δίκτυο, όπως για παράδειγμα όταν ένας administrator θέλει να διαπιστώσει τι πραγματικά έγινε στο δίκτυο κατά την εισβολή ή κάποια άλλη ανωμαλία του συστήματος.

Το Network Flight Recorder παρέχει δυνατότητες *καταγραφής* και *φιλτραρίσματος* της κίνησης στο δίκτυο με σκοπό την καταχώρηση σε αρχεία ή την στατιστική ανάλυση και μπορεί να ρυθμιστεί έτσι ώστε να πυροδοτεί (trigger) συναγερμό σε συγκεκριμένα γεγονότα. Σύμφωνα με την ομάδα που το ανάπτυξε, το Network Flight Recorder σχεδιάστηκε για να συμπληρώνει ένα σύστημα ανίχνευσης ηλεκτρονικών εισβολών. Χρησιμοποιεί μια «σκούπα πακέτων» για να συλλέξει όλα τα πακέτα από το δίκτυο. Τα πακέτα αυτά τροφοδοτούνται σε μια μηχανή απόφασης, όπου γίνεται η εκτίμηση μέσω ειδικών φίλτρων γραμμένων σε N-code, μια γλώσσα που αναπτύχθηκε αποκλειστικά για το NFR. Με ένα τέτοιο φίλτρο, είναι δυνατό να καταγραφούν οι επιλεγμένες πληροφορίες από τα φιλτραρισμένα πακέτα σε δίσκους και να πυροδοτήσουν συναγερμό. Οι πληροφορίες που καταγράφονται στον δίσκο μπορούν να γίνουν προσπελάσιμες μέσω ενός υποστηρικτικού υποσυστήματος υποβολής ερωτημάτων (queries), το οποίο είναι σαφώς διαχωρισμένο με το υποσύστημα καταγραφής. Οι χρήστες μπορούν μέσω ενός Web browser να συνδεθούν με τον HTTP διακομιστή που επικοινωνεί με το NFR, με σκοπό την υποβολή των ερωτημάτων. Ο browser κατεβάζει και εκτελεί Java Applets που εξυπηρετούν το user interface του NFR. Τα αποτελέσματα των ερωτημάτων αυτών οπτικοποιούνται στον χρήστη με τη βοήθεια της Java και με τη μορφή διαφορετικών τύπων λιστών ή διαγραμμάτων.

6. CyberCorp (Network Associates, Inc.)

Προϊον	**CyberCorp**
Κατασκευαστής	Network Associates, Inc.
Υποστηριζόμενες πλατφόρμες	Windows NT, Solaris (Sparc)
Πηγή δεδομένων	Δικτυακή & Τερματική
Μοντέλο ανίχνευσης	Μοντέλο ανίχνευσης βασισμένο σε κανόνες
Συμπεριφορά	Ανίχνευση & Απόκριση

6.1. Εισαγωγή

Η Network Associates παρέχει μια σειρά από προϊόντα ανίχνευσης ηλεκτρονικών εισβολών υπό την ονομασία CyberCorp. Τα CyberCorp Network και CyberCorp Server είναι τμήματα του συνόλου προγραμμάτωντης Network Associates με την ονομασία Net Tools Secure.

Το CyberCorp Network (**CCN**) παρέχει ανίχνευση εισβολών σε πραγματικό χρόνο αξιοποιώντας πληροφορίες από το τοπικό δίκτυο. Το CyberCorp Server (**CCS**) εστίαζει στην προστασία των servers και των άλλων τερματικών μέσα στο δικτυακό περιβάλλον.

Αισθητήρες τοποθετούνται σε στρατηγικές θέσεις στο δίκτυο με σκοπό να εντοπίσουν ύποπτες συμπεριφορές. Οι αισθητήρες λειτουργούν σε συνεργασία με ένα διακομιστή διαχείρισης (management server) ο οποίος καταγράφει σε αρχεία ύποπτα γεγονότα και στέλνει ειδοποιήσεις συναγερμού στις κονσόλες διαχείρισης (management consoles). Στην συνέχεια ενεργοποιούνται αυτοματοποιημένες διαδικασίες απόκρισης, για να τερματίσουν διεργασίες του συστήματος ή να ειδοποιήσουν τους administrators μέσω email. Ακόμα το CCN είναι εξοπλισμένο με μια ζωτικής σημασίας λειτουργία που προστατεύει τους αισθητήρες από εξωτερικές παρεμβάσεις.

Το CyberCorp Network βασίζεται στην τεχνολογία ανίχνευσης της Wheelgroup, Inc (είναι πλέον αγορασμένη από την Cisco). Για την ακρίβεια το NetRanger της Cisco και το CyberCorp Network χρησιμοποιούν παρόμοιες τακτικές για την ανίχνευση των επιθέσεων. Η βασική διαφορά ανάμεσα σε αυτά τα δυο προϊόντα είναι ότι το NetRanger εστιάζει στην προστασία της περιμέτρου του δικτύου χρησιμοποιώντας firewalls ή δρομολογητές (routers) για να μπλοκάρει τις εισβολές, ενώ το CyberCorp εστιάζει στην προστασία του δικτύου από εσωτερικές επιθέσεις.

Τα αντικείμενα στα οποία το CyberCorp ανιχνεύει επιθέσεις περιλαμβάνουν:

- Unix & Windows/Windows NT τερματικά
- Δικτυακές Υπηρεσίες (Network Services)
- Web Servers & browsers
- Διάφορες εφαρμογές
- Σωρούς πρωτοκόλλων (Protocol stacks)

6.2. Αρχιτεκτονική

Το CyberCorp έχει δυο βασικές λειτουργικές μονάδες:

i. Τους αισθητήρες CyberCorp (sensors)

ii. Τον διακομιστή διαχείρισης CyberCorp (management server)

Οι αισθητήρες κατανέμονται μέσα στο δίκτυο και ρυθμίζονται έτσι ώστε να ανιχνεύουν εισβολές, βασιζόμενοι στις πληροφορίες που συλλέγουν στο τμήμα δικτύου (network segment) όπου είναι συνδεδεμένοι. Η Network Associates συνιστά την τοποθέτηση των αισθητήρων σε σημεία υψηλής επικινδυνότητας όπως:

- Wide Area Links
- Dial-in συνδέσεις
- Server clusters
- Σε άλλα κρίσιμα τμήματα του δικτύου

Ο διακομιστής διαχείρισης (management server) συλλέγει τα δεδομένα ελέγχου από τους αισθητήρες και παρέχει καταγραφή τους σε αρχεία και αντίστοιχες ειδοποιήσεις συναγερμού. Στην συνέχεια χρησιμοποιείται μια εφαρμογή βασισμένη σε τεχνολογίες web (web-based interface) η οποία επιτρέπει στον γενικό διαχειριστή να επιβλέψει το σύστημα από οποιαδήποτε τοποθεσία. Η ασφάλεια του συστήματος βελτιώνεται με την χρήση διαδικασιών κρυπτογράφησης με σκοπό να προστατεύσουν τα κανάλια επικοινωνίας ανάμεσα στους αισθητήρες/διαχειριστές και την web εφαρμογή που προαναφέρθηκε.

7. Tripwire

Το **Tripwire** κυκλοφόρησε για πρώτη φορά το 1992 από τον *Gene Kim* (Tripwire's CTO) και τον *Dr. Eugene Spafford* (από το εργαστήριο COAST του πανεπιστημίου Perdue). Ο σκοπός του λογισμικού Tripwire είναι η εξακρίβωση της ακεραιότητας των συστημάτων αρχείων (file-systems), καταλόγων ή κλειδιών μητρώου σε προστατευόμενα μηχανήματα. Παρέχει ένα θεμελιώδες επίπεδο ασφάλειας για κάθε οργανισμό που ενδιαφέρεται για την ακεραιότητα του συστήματος δεδομένων του. Αυτό επιτυγχάνεται από το Tripwire με την ανίχνευση οποιωνδήποτε μεταβολών, είτε από εσωτερικές ή εξωτερικές επιθέσεις στην ακεραιότητα των δεδομένων.

Το Tripwire είναι το πλέον ευρέως διαδεδομένο εργαλείο ανάλυσης ακεραιότητας αρχείων σε πλατφόρμες UNIX, χρησιμοποιούμενο από χιλιάδες εμπορικές εταιρείες, κυβερνητικούς και εκπαιδευτικούς οργανισμούς παγκοσμίως.

Η τεχνολογία ανάλυσης ακεραιότητας που χρησιμοποιεί το Tripwire επιτρέπει στο χρήστη να ελέγξει επακριβώς τι έχει αλλάξει σε ένα σύστημα μέσα στο χρόνο. Το Tripwire σαν ανιχνευτής εισβολών σε συγκεκριμένες μηχανές-στόχους, μπορεί να προστατεύσει αποτελεσματικά από απειλές τους εξυπηρετητές και τους σταθμούς εργασίας που αποτελούν ένα εταιρικό δίκτυο. Μπορεί επίσης να καθοριστεί ένα μοναδικό αρχείο πολιτικής για την ασφάλεια μίας ομάδας μηχανημάτων επιτρέποντας έτσι την ανάπτυξη διοίκησης σε κλιμακωτά επίπεδα.

Παραδείγματα συγκεκριμένων εφαρμογών για τις οποίες μπορεί να χρησιμοποιηθεί το Tripwire είναι τα ακόλουθα :

- *Ανίχνευση Εισβολών* – Το Tripwire σχεδιάστηκε ως το πλέον αξιόπιστο εργαλείο Ανίχνευσης Εισβολών σε υπολογιστικά συστήματα. Το Tripwire ανιχνεύει εισβολείς ή μη εξουσιοδοτημένες αλλαγές σε βασικά αρχεία του συστήματος και κατάλογους.
- *Συμμόρφωση Συστήματος και πολιτικής* – Το Tripwire επιβεβαιώνει ότι το Σύστημα είναι σύμφωνο με τα πρότυπα της Τεχνολογίας Πληροφορικής παρακολουθώντας τα αρχεία του συστήματος για αλλαγές. Βοηθά τον διαχειριστή να δημιουργήσει μια baseline βάση δεδομένων του ιδανικού συστήματος για λόγους σύγκρισης με αλλά συστήματα που πρέπει να βρίσκονται στην ίδια κατάσταση.
- *Κλείδωμα Συστήματος* – Το Tripwire μπορεί επίσης να χρησιμοποιηθεί για την εξασφάλιση ότι δεν έχει εγκατασταθεί νέο μη-εξουσιοδοτημένο λογισμικό στο Σύστημα. Εφόσον το Σύστημα έχει κλειδωθεί, το Tripwire ελέγχει οποιαδήποτε

εγκατάσταση μη-εξουσιοδοτημένου λογισμικού ή εφαρμογών.

- *Εκτίμηση Ζημίας και Ανάνηψη* – Το Tripwire μπορεί να χρησιμοποιηθεί επίσης και μετά από μια επίθεση για να προσδιορισθεί το μέγεθος της Ζημίας και ποια αρχεία πρέπει να επιδιορθωθούν ή να αντικατασταθούν.
- *Ιατροδικαστική (Forensics)* – Οι αναφορές του Tripwire μπορούν να χρησιμοποιηθούν για τη συλλογή ντοκουμέντων που στοιχειοθετούν μια εισβολή.

8. COPS

Το πακέτο λογισμικού **COPS (C**omputer **O**racle and **P**assword **S**ystem**)** προέρχεται από το Πανεπιστήμιο του Perdue, όπως εξάλλου και το Tripwire. Εξετάζει ένα σύστημα για έναν αριθμό γνωστών αδυναμιών του συστήματος και τις κοινοποιεί στον διαχειριστή του συστήματος (σε ορισμένες περιπτώσεις μπορεί να διορθώσει αυτόματα τα προβλήματα αυτά).

Το COPS είναι ένα ελεύθερα διαθέσιμο σύνολο προγραμμάτων τα οποία ελέγχουν ποικίλες προβληματικές περιοχές της ασφάλειας ενός συστήματος UNIX. Το COPS δεν διορθώνει αλλά απλά αναφέρει πιθανά ρήγματα ασφαλείας (security holes). Το COPS μπορεί να χρησιμοποιηθεί για να επιτελέσει έλεγχο στις παρακάτω περιοχές, μεταξύ άλλων :

- Άδειες και τρόποι λειτουργίας (modes) αρχείων, καταλόγων, συσκευών.
- Αδύναμα συνθηματικά (passwords).
- Περιεχόμενο, μορφότυπο και ασφάλεια των αρχείων των συνθηματικών και της πολιτικής (policy) του συστήματος.
- Τα προγράμματα και τα αρχεία που τρέχουν στο /etc/rc* και τα αρχεία cron(tab).
- Ύπαρξη των αρχείων root-SUID (Set User ID), το δικαίωμα επανεγγραφής τους και το αν είναι ή όχι shell-scripts.
- Έναν έλεγχο CRC σε σημαντικά δυαδικά (binary) αρχεία για την αναφορά τυχόν αλλαγών σε αυτά.
- Δυνατότητα έγγραφης στους αρχικούς καταλόγους των χρηστών και στα αρχεία εκκίνησης (.profile, .cshrc κλπ.).
- Ρύθμιση ανώνυμου ftp.

9. SATAN

Το **SATAN** (**S**ecurity **A**nalysis **T**ool for **A**uditing **N**etworks) σχεδιάστηκε και κατασκευάστηκε το 1995 από τους *Dan Farmer και Wietse Venema*. Η διάφορα του από το COPS είναι ότι το COPS είναι ένα host-based Unix εργαλείο έλεγχου ασφάλειας, δηλαδή τρέχει πάνω στον υπολογιστή του οποίου εξετάζεται η ασφάλεια. Το SATAN είναι ένα εργαλείο έλεγχου ασφάλειας απομακρυσμένου δικτύου (remote network), δηλαδή μπορεί να κάνει αναφορά για την ασφάλεια οποιουδήποτε υπολογιστή ή δικτύου στον οποίο έχει IP πρόσβαση το μηχάνημα στο οποίο εκτελείται το SATAN. Δεν χρειάζεται κάποιος λογαριασμός ή δικαιώματα στις απομακρυσμένες μηχανές στις οποίες γίνεται έλεγχος.

Στην πιο απλή (και default) μορφή του το SATAN συλλέγει όσες το δυνατόν περισσότερες πληροφορίες για απομακρυσμένους υπολογιστές και δίκτυα εξετάζοντας υπηρεσίες δικτύων όπως είναι οι finger, NFS, NIS, ftp και tftp, rexd κλπ. Η πληροφορία που συγκεντρώνεται περιέχει την παρουσία διάφορων υπηρεσιών πληροφοριών για δίκτυα καθώς και πιθανά ελαττώματα στην ασφάλεια – συνήθως λανθασμένη εγκατάσταση ή διαρρύθμιση υπηρεσιών δικτύου, γνωστά bugs σε utilities του συστήματος ή του δικτύου, ή φτωχές και αδύναμες αποφάσεις πολιτικής του συστήματος.

Μπορεί κατόπιν είτε να αναφέρει τα δεδομένα αυτά ή να χρησιμοποιήσει ένα rule-based σύστημα για να ανακαλύψει πιθανά προβλήματα ασφάλειας. Οι χρήστες μπορούν να εξετάσουν, να ερευνήσουν και να αναλύσουν τα την έξοδο του προγράμματος μέσα από κάποιον HTML browser, όπως τον Mosaic, Netscape, ή Lynx.

Ενώ το πρόγραμμα είναι κυρίως προσανατολισμένο προς την ανάλυση των θεμάτων ασφάλειας μέσω των αποτελεσμάτων, ένα μεγάλο ποσό γενικής πληροφορίας για το δίκτυο μπορεί να αντληθεί με την χρήση του εργαλείου – όπως τοπολογία δικτύου, ποιες υπηρεσίες δικτύου τρέχουν, τύπος λογισμικού και υλικού που χρησιμοποιείται στο δίκτυο κλπ.

Το SATAN είναι πλέον χρήσιμο όταν χρησιμοποιείται από τους διαχειριστές συστήματος η ασφάλειας που είναι υπεύθυνοι για την ασφάλεια του συγκεκριμένου συστήματος. Πάντως, καθώς είναι ελευθέρα διαθέσιμο μέσα στο Διαδίκτυο, μπορεί να χρησιμοποιηθεί από οποιονδήποτε ανησυχεί για την ασφάλεια του συστήματος του, αφού πιθανοί εισβολείς θα μπορούν να έχουν πρόσβαση στις ίδιες πληροφορίες αδυναμίας του συστήματος και εφόσον είναι πιθανόν να αποκαλυφθούν προβλήματα ασφάλειας που πρώτα ήταν άγνωστα.

10. Crack

Το **Crack** έχει αναπτυχθεί από τον *Alec D.E. Muffett* και η πιο πρόσφατη έκδοση του ελευθέρα διαθέσιμη στο Διαδίκτυο είναι η 4.1, με ημερομηνία κυκλοφορίας 3/3/1992. Το Crack είναι ένας αναλυτής συνθηματικών για συστήματα UNIX. Είναι σχεδιασμένο να βρίσκει συνθηματικά 8-χαρακτηρων κρυπτογραφημένα σε DES χρησιμοποιώντας ορισμένες τεχνικές πρόβλεψης. Έχει γραφτεί έτσι ώστε να είναι ευέλικτο, διαμορφώσιμο, και γρήγορο.

11. Bro

Το **Bro** είναι ένα IDS που αναπτύχθηκε στο Lawrence Berkley National Laboratory. Ο πηγαίος κώδικάς του είναι ελεύθερα διαθέσιμος και είναι βασισμένο σε μια modular αρχιτεκτονική. Η μηχανή γεγονότος (event engine) είναι χωρισμένη από το διερμηνέα πολιτικής σεναρίων (policy script interpreter), η οποία υπαγορεύει την πολιτική που εφαρμόζεται μέσω μιας ιδιόκτητης γλώσσας. Η μηχανή γεγονότος σχεδιάζεται έτσι ώστε να είναι ικανή να ελέγχει τις συνδέσεις δικτύων για πάνω από 100 Mbps, δείχνοντας ότι έχει δοθεί έμφαση στην απόδοση του συστήματος.

12. NID

Το **NID** (**N**etwork **I**ntrusion **D**etector) είναι ένα άλλο ελεύθερα διαθέσιμο IDS. Εγκαθίσταται σε ένα αφιερωμένο σύστημα από όπου ελέγχει την δικτυακή κυκλοφορία. Ψάχνει για τις γνωστές υπογραφές επίθεσης, καθώς επίσης και για τις αποκλίσεις από την κανονική συμπεριφορά μέσα στο δίκτυο. Σε περίπτωση που μια εισβολή ανιχνεύεται ο διευθυντής ασφάλειας ειδοποιείται.

13. Άλλα εμπορικά IDS

- ✓ ***Stake Out I.D.*** (Harris Communications, Inc.)
- ✓ ***Kane Security Monitor*** (Security Dynamics)
- ✓ ***Session Wall-3*** (AbirNet)
- ✓ ***Entrax*** (Centrax Corporation)
- ✓ ***CMDS*** (Science Application International Corporation)
- ✓ ***SecureNet Pro*** (MimeStar, Inc.)
- ✓ ***INTOUCH INSA*** (Touch Technologies, Inc.)
- ✓ ***T-Sight*** (EnGarde Systems, Inc.)
- ✓ ***NIDES*** (SRI International)
- ✓ ***ID-Trak*** (Internet Tools, Inc.)
- ✓ ***SecureCom Suite*** (ODS Networks)

ΑΝΑΦΟΡΕΣ

[1] Denning, D. “An Intrusion Detection Model.” IEEE Transactions on Software Engineering, 13.2 (1987) 222

[2] S. Axelsson, Intrusion Detection Systems: A Survey and Taxonomy, Chalmers University, Technical Report 99-15, March 2000

[3] S. Axelsson, Research in intrusion-detection systems: a survey, Department of Computer Engineering, Chalmers University of Technology, Goteborg, Sweden, Technical Report 98 17, December 1998

[4] "An overview of anomaly detection techniques: Existing solutions and latest technological trends", Patcha A., Park J. Computer Networks: The International Journal of Computer and Telecommunications Networking, 2007

[5] Intrusion detection: systems and models, Sherif, J.S. Dearmond, T.G. Jet Propulsion Lab., California Inst. of Technol., Pasadena, CA

[6] Cyber Security Challenges: Designing Efficient Intrusion Detection Systems and Antivirus Tools Srinivas Mukkamala, Andrew Sung and Ajith Abraham* Department of Computer Science, New Mexico Tech, USA *School of Computer Science and Engineering, Chung-Ang University, Korea

[7] Cisco Systems, Inc., Deploying Network-Based Intrusion Detection, March, 2004

[8] Guide to Intrusion Detection and Prevention Systems (IDPS) - NIST Special Publication 800-34- Feb 2007

[9] NIST Special Publication on Intrusion Detection Systems, Rebecca Bace1 and Peter Mell2

[10] Host-based Intrusion Detection Systems, Pieter de Boer & Martin Pels, Revision 1.10 – February 4, 2005

[11] Smaha, S.E., Haystack: An intrusion detection system, in Proceedings of the 4th: Aerospace Computer Security Applications Conference, 1988

[12] JE. Gaffney, JW. Ulvila, Evaluation of intrusion detectors: a decision theory approach, in: Proceedings of the 2001 IEEE Symposium on Security and Privacy, Oakland, CA, USA, 2001, pp. 50–61.

[13] Feature deduction and ensemble design of intrusion detection systems, Srilatha, Chebrol, Abraham, Ajith, Thomas, Johnson P, Computers & Security. Vol. 24, no. 4, pp. 295-307. June 2005

[14] Introduction to COMPUTER SECURITY, Addison-Wisley, Matt Bishop, University of California – Davis, 2005

[15] Ασφάλεια δικτύων υπολογιστών, Κάτσικας, Σωκράτης Κ., Γκρίτζαλης, Δημήτρης Α., Γκρίτζαλης, Στέφανος, Παπασωτηρίου 2003

[16] ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΩΝ ΚΑΙ ΥΠΟΛΟΓΙΣΤΙΚΩΝ ΣΥΣΤΗΜΑΤΩΝ ΑΝΑΧΑΙΤΙΣΤΕ ΤΟΥΣ ΕΙΣΒΟΛΕΙΣ, Κομνηνός Θόδωρος, Σπυράκης Παύλος, 2002

[17] http://www.acm.org/crossroads/xrds2-4/intrus.html

[18] http://www.softpanorama.org/Security/intrusion_detection.shtml#News

[19] http://www.linuxfocus.org/English/May2003/article292.shtml#292lfindex0

[20] http://toivo.talikka.com/internet-security/intrusion-detection-systems.html#introduction

[21] http://en.wikipedia.org/wiki/Intrusion_detection_system

[22] http://www.sans.org/resources/idfaq/index.php?portal=5bce0c66818d808d318d6d62bd

[23] http://www.snort.org

[24] http://ezine.daemonnews.org/199905/ids.html#Ref3#Ref3