ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

ΤΜΗΜΑ ΔΙΔΑΚΤΙΚΗΣ ΤΗΣ ΤΕΧΝΟΛΟΓΙΑΣ ΚΑΙ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΠΜΣ – Κατεύθυνση: "Ψηφιακές Επικοινωνίες & Δίκτυα"

Δ Ι Π Λ Ω Μ Α Τ Ι Κ Η Ε Ρ Γ Α Σ Ι Α

ΜΕΛΕΤΗ ΤΩΝ ΣΥΝΕΡΓΑΤΙΚΩΝ ΑΡΧΙΤΕΚΤΟΝΙΚΩΝ ΣΥΣΤΗΜΑΤΩΝ ΑΝΙΧΝΕΥΣΗΣ ΕΙΣΒΟΛΩΝ

Ανδρεάδης Σωτήριος

ΜΕ 08041

ΠΕΙΡΑΙΑΣ 2010

Επιβλέπων : Λαμπρινουδάκης Κώστας

Επίκουρος Καθηγητής

ΠΡΟΛΟΓΟΣ

Τα τελευταία χρόνια η ανίχνευση εισβολών σε δίκτυα υπολογιστών έχει αναδειχθεί σε ένα δημοφιλές και διαρκώς εξελισσόμενο επιστημονικό πεδίο εφαρμογής. Ένας από τους κύριους λόγους είναι η εξάπλωση του Διαδικτύου καθώς και ο μεγάλος αριθμός δικτυωμένων συστημάτων που υπάρχουν σε οργανισμούς, εταιρείες, φορείς κα. Ο συνεχώς αυξανόμενος αριθμός των υπολογιστικών συστημάτων από επιχειρήσεις και ιδιώτες είχε σαν συνέπεια την εμφάνιση και ανάπτυξη παράνομων δραστηριοτήτων από διάφορους εισβολείς. Αναπόφευκτα η εμφάνιση των παράνομων δραστηριοτήτων, προκάλεσε την μελέτη και ανάπτυξη συστημάτων ανίχνευσης εισβολών τόσο στον ερευνητικό - επιστημονικό τομέα όσο και σε πρακτικό επίπεδο.

Στην Διπλωματική αυτή εργασία, αφού γίνει αναφορά στις βασικές αρχές της ασφάλειας, της αναγκαιότητας της πολιτικής ασφάλειας από τους χρήστες των πληροφοριακών συστημάτων και των διαφόρων απειλών που τα συστήματα αντιμετωπίζουν γίνεται προσπάθεια περιγραφής και λειτουργίας των ΣΥΣΤΗΜΑΤΩΝ ΑΝΙΧΝΕΥΣΗΣ ΕΙΣΒΟΛΩΝ (INTRUSION DETECTION SYSTEMS - IDS).

Σκοπός της εργασίας αυτής είναι να γνωρίσουμε τους λόγους χρήσης των συστημάτων ανίχνευσης εισβολών, την αρχιτεκτονική τους, την εξέλιξή τους και τα επιθυμητά χαρακτηριστικά τους.

Επίσης γίνεται προσπάθεια ταξινόμησής τους ανάλογα με τον τρόπο που το κάθε ένα σύστημα ανίχνευσης εισβολών υλοποιεί την διαδικασία της παρακολούθησης και της ανάλυσης των δεδομένων με στόχο την ανίχνευση εισβολών.

Παράλληλα με την ανάπτυξη των ασύρματων δικτύων στα συστήματα υπολογιστών παρατηρήθηκε η εμφάνιση παράνομων δραστηριοτήτων και σε αυτά. Έτσι επιτακτική ήταν η ανάγκη να προστατευτούν και τα δίκτυα αυτά από κατάλληλα συστήματα ανίχνευσης εισβολών. Για τον λόγο αυτό η εργασία αυτή κάνει λόγο για τους κινδύνους που αντιμετωπίζουν τα ασύρματα ad hoc δίκτυα και τις διάφορες αρχιτεκτονικές που χρησιμοποιούνται για να προστατευτούν.

Τέλος ακολουθεί αναφορά στην αρχιτεκτονική, στα χαρακτηρίστηκα και στην λειτουργία προϊόντων IDS.

Για την εξεύρεση βιβλιογραφίας και ειδικών αναφορών ανέτρεξα στην βιβλιοθήκη του Εθνικού Μετσόβειου Πολυτεχνείου (Ε.Μ.Π), στο διαδίκτυο και σε επιστημονικά συγγράμματα.

Τέλος θα ήθελα να ευχαριστήσω τον καθηγητή μου κ. Λαμπρινουδάκη Κώστα, ο οποίος απετέλεσε τον γνώμονα των κινήσεών μου για την εκπόνηση της παρούσας Διπλωματικής Εργασίας.

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

ΠΕΡΙΕΧΟΜΕΝΑ

ΣΧΗΜΑΤΑ

ΚΕΦΑΛΑΙΟ 1

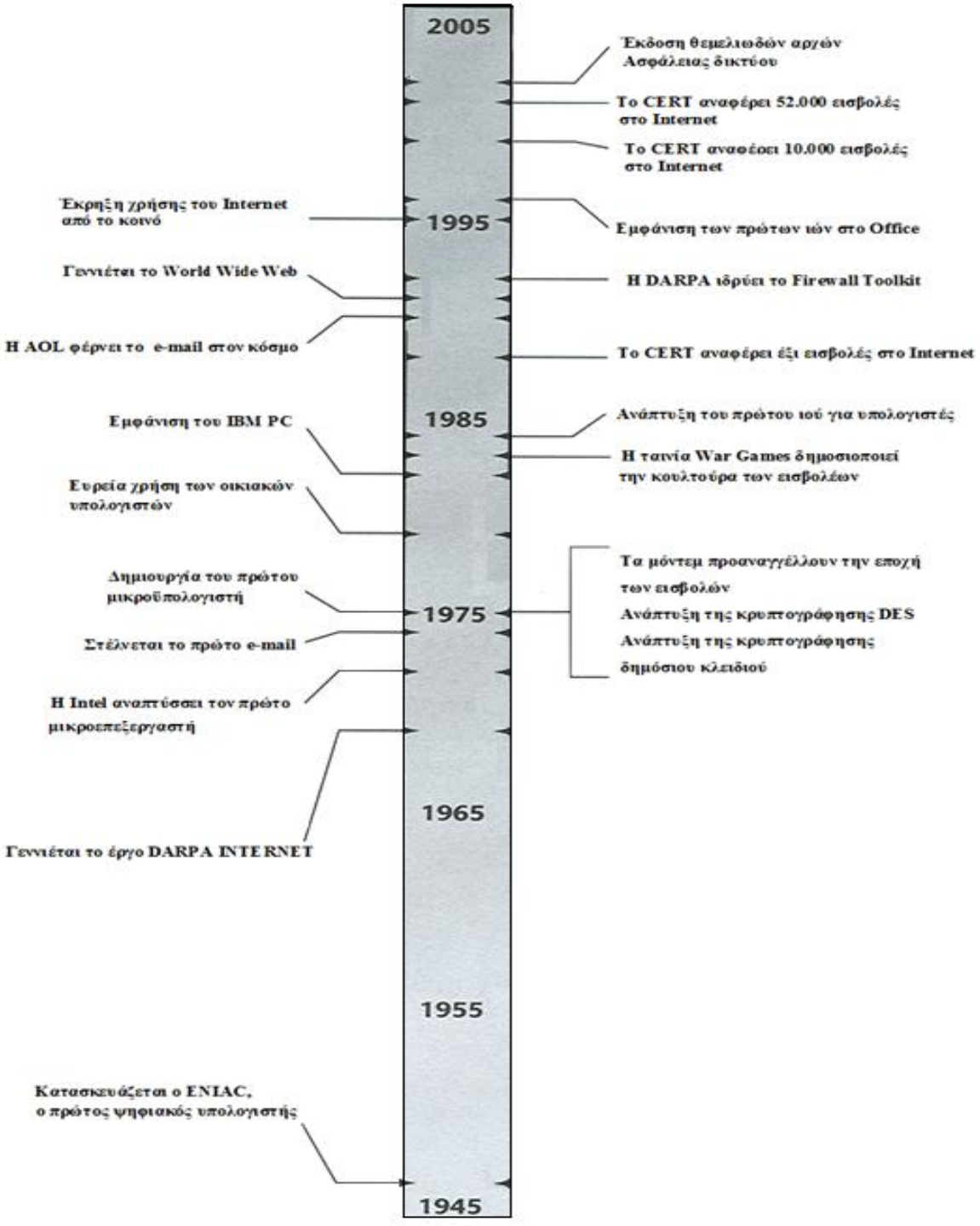
ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΩΝ

Ο κόσμος της πληροφορικής εξελίσσεται ραγδαία τόσο σε επίπεδο λογισμικού όσο και σε επίπεδο δυνατοτήτων των χρηστών. Παράλληλα, εξ' ίσου ραγδαία είναι και η ανάπτυξη εισβολών – απειλών που αντιμετωπίζουν τα πληροφοριακά συστήματα και οι χρήστες τους.
Έτσι οι υπολογιστές αποτελούν ταυτόχρονα μέσα και στόχους επιθέσεων. Η αντιμετώπιση των επιθέσεων αυτών επιτυγχάνεται με την εφαρμογή ορισμένων σταθερών και θεμελιωδών αρχών οι οποίες ορίζουν την ασφάλειά τους.

1.1 ΟΡΙΣΜΟΣ ΚΑΙ ΙΣΤΟΡΙΚΗ ΑΝΑΔΡΟΜΗ ΑΣΦΑΛΕΙΑΣ ΥΠΟΛΟΓΙΣΤΩΝ ΚΑΙ ΔΙΚΤΥΩΝ

Με τον όρο **Ασφάλεια Δικτύων και Υπολογιστών** εννοούμε το σύνολο των μέτρων που λαμβάνονται για την αποτροπή απωλειών που προέρχονται από επιθέσεις οι οποίες αποσκοπούν στην μη εξουσιοδοτημένη εκμετάλλευση υπολογιστικών και δικτυακών πόρων και δεδομένων.
Οι απώλειες μπορεί να συμβούν λόγω σφάλματος χρήστη, προβλημάτων στον κώδικα, κακόβουλων ενεργειών, αποτυχιών υλικού και ενεργειών της φύσης.
Η ασφάλεια ενός δικτύου υπολογιστών είναι απαραίτητη τόσο σε επίπεδο αλλοίωσης όσο και σε επίπεδο ορθότητας και αξιοπιστίας. 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).
Ανατρέχοντας στην ιστορία ασφάλειας υπολογιστών εύκολα αντιλαμβάνεται κανείς, ότι οι υπολογιστές δεν είναι ασφαλείς λόγω εισβολών σχεδόν καταστροφικών. Για παράδειγμα το 2001 ήταν ένα κακό έτος για την ασφάλεια στο internet λόγω της διάχυσης του σκουληκιού (worm) με το όνομα Code Red. Αμέσως μετά εμφανίστηκε και ο ιός (virus) Nimbda. Οι

δεκαετίες σταθμοί στην ιστορία των υπολογιστών από την γέννησή τους απεικονίζονται στο παρακάτω σχήμα 1 και είναι : 1945-1955, 1955 - 1965, 1965 – 1975, 1975 – 1985, 1985 – 1995, 1995 – 2005, 2005 και μετά.



Σχήμα 1. Οι δεκαετίες σταθμοί στην ιστορία των υπολογιστών.

1.2 ΒΑΣΙΚΕΣ ΑΡΧΕΣ ΑΣΦΑΛΕΙΑΣ ΚΑΙ ΑΠΑΙΤΗΣΕΙΣ

Σήμερα το σύνολο των ατομικών και επιχειρηματικών δραστηριοτήτων εκτελούνται κυρίως ηλεκτρονικά. Η ποιότητα αλλά και η ποσότητα της διακινούμενης πληροφορίας αυξήθηκε κατακόρυφα. Αναπόφευκτο ήταν, να εμφανιστούν κρούσματα ηλεκτρονικού εγκλήματος. Το πλεονέκτημα του διαδικτύου, δηλαδή της πολλαπλής διασύνδεσης των υπολογιστών, ταυτόχρονα αποτελεί και το σοβαρότερο μειονέκτημα. Σε αυτό συνδράμει και η ανωνυμία που επικρατεί. Οποιοσδήποτε μπορεί να δεχθεί επίθεση και κυρίως κομβικά συστήματα που είτε διαχειρίζονται ευαίσθητα δεδομένα είτε οικονομικής φύσεως πληροφορίες. Από την άλλη, η υπάρχουσα διαδικτυακή τεχνολογική υποδομή παρουσιάζει ενσωματωμένα τρωτά σημεία. Η γνώση και εκμετάλλευση αυτών των αδυναμιών είναι η απαρχή μιας επίθεσης. Έχει αποδειχθεί ότι οι οικονομικές συνέπειες μιας επιτυχημένης επίθεσης μπορεί να είναι υψηλότατες σε σχέση με το κόστος της. Οι πιθανοί εισβολείς προέρχονται είτε από το εξωτερικό δίκτυο του στόχου, όπως είναι οι ανταγωνιστές, ξένες υπηρεσίες πληροφοριών κ.α., είτε από το εσωτερικό δίκτυο του στόχου, όπως δυσαρεστημένοι υπάλληλοι, ελλιπής εκπαίδευση προσωπικού κ.α. Τα διαδικτυακά εγκλήματα εκτείνονται από απλές απάτες με κλοπή πιστωτικών καρτών έως προσεκτικές επιθέσεις για πρόσβαση σε ευαίσθητες πληροφορίες. Σκοπός των αρχών ασφαλείας είναι να προστατευτούν τόσο όσοι χρησιμοποιούν δίκτυα υπολογιστών όσο και οι απλοί χρήστες από το λεγόμενο κακόβουλο λογισμικό και κατ' επέκταση από τους κακόβουλους χρήστες. Δεν αποκλείονται βέβαια και τυχαία συμβάντα. Θα πρέπει όμως οποιοσδήποτε χρησιμοποιεί δίκτυα υπολογιστών να έχει την ικανότητα να προστατεύει τις πληροφορίες του από τυχόν αλλοιώσεις ή καταστροφές και να παρέχει ορθές και αξιόπιστες πληροφορίες σε εξουσιοδοτημένους χρήστες. Επομένως 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. 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.

Προκειμένου ένα δίκτυο να μην είναι διαβλητό πρέπει να πληροί τις παρακάτω απαιτήσεις ασφαλείας :

- **Εμπιστευτικότητα (Confidentiality).** Η αρχή της εμπιστευτικότητας προστατεύει ευαίσθητη πληροφορία από μη εξουσιοδοτημένη πρόσβαση ή υποκλοπή της. Η πληροφορία πρέπει να είναι εμφανής μόνο μεταξύ των νόμιμων άκρων μιας επικοινωνίας και όχι και σε αυτούς που πιθανά «ακούνε» το κανάλι της επικοινωνίας και περιλαμβάνει τις παρακάτω τέσσερις περιπτώσεις :
  - Εμπιστευτικότητα σύνδεσης (Connection).
  - Εμπιστευτικότητα μη-σύνδεσης (Connectionless).
  - Εμπιστευτικότητα επιλεκτικού πεδίου (Selective field).
  - Εμπιστευτικότητα ροής πληροφοριών (Traffic flow).

  Τα λειτουργικά συστήματα διαθέτουν συνήθως ενσωματωμένους μηχανισμούς για την προστασία των αρχείων. Οι μηχανισμοί αυτοί δίνουν τη δυνατότητα σε ένα διαχειριστή να ελέγχει ποιος θα έχει πρόσβαση στα περιεχόμενα των αρχείων αυτών. Η εμπιστευτικότητα μπορεί να επιτευχθεί και με την κρυπτογράφηση. Η κρυπτογράφηση επιτυγχάνεται με την παρεμβολή χαρακτήρων στα δεδομένα, έτσι ώστε να είναι δύσκολη και χρονοβόρα η εύρεση της αρχικής πληροφορίας για οποιονδήποτε άλλο έκτος από τους εξουσιοδοτημένους παραλήπτες. Οι εξουσιοδοτημένοι παραλήπτες και οι ιδιοκτήτες της πληροφορίας κατέχουν τα κλειδιά για την αποκρυπτογράφηση της πληροφορίας.

- **Διαθεσιμότητα (Availability).** Η αρχή της διαθεσιμότητας εξασφαλίζει ότι η πληροφορία ή οι υπηρεσίες είναι προσπελάσιμες και λειτουργικές, όταν ζητηθούν από κάποιον ο οποίος είναι εξουσιοδοτημένος για πρόσβαση σε αυτές. Με την αρχή αυτή σχετίζεται και η έννοια της εμπιστοσύνης. Η διαθεσιμότητα είναι ένας από τους πιο σημαντικούς παράγοντες της καλής λειτουργίας ενός συστήματος και μάλιστα τα τελευταία χρόνια η ιδιότητα αυτή αποτελεί στόχο πολλών επιθέσεων DoS (Denial of Service) και DDoS (Distributed Denial of Service).

- **Ακεραιότητα (Integrity).** Η αρχή της ακεραιότητας εξασφαλίζει ότι η πληροφορία ή το λογισμικό είναι πλήρες, σωστό και αυθεντικό, δηλαδή ότι δεν έχει υποστεί κάποια αλλαγή με κάποιον παράνομο τρόπο. Έτσι εξασφαλίζουμε την ύπαρξη κατάλληλων μηχανισμών στα σωστά σημεία, οι οποίοι μας προστατεύουν από τυχαία ή κακόβουλη τροποποίηση της αρχικής πληροφορίας βοηθώντας στην επίτευξη της καλής λειτουργίας της ασφάλειας ενός λειτουργικού συστήματος.

1.3 ΓΙΑΤΙ ΟΙ ΥΠΟΛΟΓΙΣΤΕΣ ΔΕΝ ΕΙΝΑΙ ΑΣΦΑΛΕΙΣ

Από τότε που ξεκίνησαν να χρησιμοποιούνται οι υπολογιστές μέχρι και σήμερα οι χρήστες τους διαπιστώνουν ότι υπάρχουν τρωτά σημεία στην λειτουργία τους τα οποία αποτελούν αιτία επιθέσεων και εισβολών. Η πλειοψηφία των περισσότερων εισβολών έχει σχέση με ένα από τα παρακάτω προβλήματα :

- Η ασφάλεια είναι ενοχλητική : Οι διαχειριστές συχνά δεν υλοποιούν χαρακτηριστικά ασφάλειας μέσα σε λειτουργικά συστήματα, για να μην δημιουργούν προβλήματα στους χρήστες. Οι χρήστες, συχνά παρακάμπτουν την ασφάλεια, επιλέγοντας εύχρηστους κωδικούς πρόσβασης, μην αλλάζοντας τους κωδικούς τους και αποκαλύπτοντάς τους σε συνεργάτες τους. Οι προμηθευτές παραδίδουν το λογισμικό τους, έτσι ώστε να μπορεί να εγκατασταθεί με τα περισσότερα χαρακτηριστικά του και με ανενεργά τα χαρακτηριστικά ασφάλειάς του. Αυτό σημαίνει ότι η πλειοψηφία των εγκαταστάσεων δεν είναι ποτέ σωστά ασφαλισμένη.

- Το λογισμικό παραδίδεται βιαστικά στην αγορά : Οι προμηθευτές επικεντρώνουν την προσοχή τους στην προσθήκη χαρακτηριστικών, που κάνουν το λογισμικό τους πιο χρήσιμο και ταχύτερα εξελισσόμενο χωρίς να δίνουν ιδιαίτερη σημασία στην ασφάλεια που παρέχει, διότι αν ξόδευαν το χρόνο τους με την ασφάλεια θα επισκιάζονταν από τον ανταγωνισμό γιατί οι πελάτες δεν δίνουν την πρέπουσα αξία στην ασφάλεια του λογισμικού και τα λιγότερο ασφαλή προϊόντα φτάνουν πάντα πρώτα στην αγορά και γίνονται πρότυπα της αγοράς. Επίσης οι προμηθευτές για να αποφύγουν προβλήματα με τους πελάτες τους προσπαθούν να κρύψουν τα προβλήματα των λειτουργικών συστημάτων τους.

- Οι υπολογιστές και το λογισμικό εξελίσσονται πολύ γρήγορα. Οι υπολογιστές και η τεχνολογία δικτύωσης εξελίσσονται πολύ γρήγορα. Εταιρείες και προγραμματιστές δεν μπορούν να προβλέψουν τα προβλήματα και τι θα πάει στραβά.

Η συσσώρευση όλων αυτών των προβλημάτων ασφαλείας μας κάνει να αναρωτιόμαστε αν το πρόβλημα της ασφάλειας θα λυθεί ποτέ. Η μέχρι σήμερα πείρα μας λέει ότι τα προβλήματα πάντα θα υπάρχουν.

Με την πρόοδο της τεχνολογίας ανακαλύπτονται και τρόποι αντιμετώπισης των εισβολών όπως : ασφαλή πρωτόκολλα που μπορεί να τοποθετηθούν πάνω στα ανασφαλή ή και να τα αντικαταστήσουν. Οι γενικοί μηχανισμοί ασφαλείας είναι απλοί ενώ οι εφαρμογές απαιτούν πλούσια χαρακτηριστικά ασφάλειας. Το δίλημμα, λοιπόν που παρουσιάζεται εδώ είναι πως από την μια πλευρά οι απλοί γενικοί μηχανισμοί μπορεί να μην καλύπτουν συγκεκριμένες απαιτήσεις ασφάλειας ενώ από την άλλη πλευρά, η επιλογή των σωστών χαρακτηριστικών και λειτουργιών από ένα πλούσιο σε επιλογές μηχανισμό, απαιτεί την εμπειρία του χρήστη στην ασφάλεια. Υπάρχει μια προφανής εξισορρόπηση των χαρακτηριστικών που διέπουν τους μηχανισμούς ασφάλειας καθώς, όσο μεγαλύτερη θέλουμε να είναι η διαβεβαίωση για την ασφαλή λειτουργία ενός μηχανισμού, τόσο πιο απλός πρέπει να είναι στη λειτουργία του, οπότε συμπεραίνουμε ότι πλούσια σε επιλογές συστήματα και υψηλή διαβεβαίωση δεν συμπορεύονται εύκολα. Όσο οι απαιτήσεις από ένα λειτουργικό σύστημα αυξάνουν τόσο η ισορροπία θα μετατοπίζεται προς την μεριά του χρήστη (πολυπλοκότητα) απ' ό,τι τη μεριά του συστήματος. Επομένως σύμφωνα με όλα τα παραπάνω που αφορούν την ασφάλεια των υπολογιστών, γεννιώνται οι εξής προβληματισμοί : που θα πρέπει να εστιαστούν οι έλεγχοι της ασφάλειας ; Στα δεδομένα, στις λειτουργίες ή στους χρήστες ; Απλότητα ή διαβεβαίωση ; Όμως όσο ταχύτατη κι αν είναι η πρόοδος σε επίπεδο υλικού και λογισμικού με άλλο τόσο ταχύτατη πρόοδο κατασκευάζουν τα εργαλεία τους και οι εισβολείς με αποτέλεσμα κατασκευαστές, χρήστες και εισβολείς να βρίσκονται σε ένα συνεχή ανταγωνισμό.

1.4 ΠΟΛΙΤΙΚΗ ΑΣΦΑΛΕΙΑΣ

Η πολιτική ασφάλειας είναι το σύνολο των κανόνων που ρυθμίζουν την πρόσβαση που έχει κάθε χρήστης στα πληροφοριακά συστήματα ενός οργανισμού. Χωρίς την ύπαρξη πολιτικής ασφάλειας δεν υπάρχει ένα γενικό πλαίσιο για την ασφάλεια. Με την πολιτική ορίζουμε ποια συμπεριφορά είναι επιτρεπόμενη μέσα στον οργανισμό ως προς την χρήση των προσφερόμενων υπηρεσιών, μέσα από διαδικασίες που πρέπει να ακολουθηθούν από όλους. Η πολιτική ασφάλειας είναι μία καλή μέθοδος για την δημιουργία αυτοαντίληψης ανάμεσα στα στελέχη του οργανισμού. Οι χρήστες αντιμετωπίζουν τις πολιτικές σαν ένα φρένο της

παραγωγικότητας ή ένα τρόπο να ελέγχεται η συμπεριφορά των εργαζομένων. Οι αποφάσεις που λαμβάνονται για την ασφάλεια ενός δικτύου από τον διαχειριστή του, καθορίζουν το πόσο ασφαλές είναι ένα δίκτυο καθώς και την ευκολία στη χρήση του. Καταρχήν θα πρέπει να αποφασιστεί τι είναι σκόπιμο να διαφυλαχτεί. Όταν γίνει αυτό θα πρέπει να οριστούν οι περιορισμοί που θα πρέπει να τεθούν ώστε να έχουμε το επιθυμητό αποτέλεσμα.

Οι στόχοι της πολιτική ασφάλειας καθορίζονται από παράγοντες όπως :

1. Προσφερόμενες υπηρεσίες σε σχέση με την ασφάλεια του δικτύου. Η χρήση κάποιων υπηρεσιών αυξάνει τον κίνδυνο για την άρση της ασφάλειας ενός δικτύου, με αποτέλεσμα το κόστος των υπηρεσιών αυτών να είναι μεγαλύτερο από τα οφέλη τους. Σε τέτοιες περιπτώσεις είναι προτιμότερη η κατάργηση της υπηρεσίας.
2. Ευκολία χρήσης σε σχέση με τη προσφερόμενη ασφάλεια. Το ευκολότερο σύστημα στη χρήση είναι αυτό που προσφέρει άμεση πρόσβαση χωρίς την ύπαρξη συνθηματικών. Όμως ένα τέτοιο σύστημα δεν προσφέρει καμία απολύτως ασφάλεια. Με την χρήση συνθηματικών (password) το σύστημα γίνεται λίγο πιο δύσκολο αφού κάθε χρήστης θα πρέπει να θυμάται τον κωδικό του, αλλά ταυτόχρονα γίνεται και πιο ασφαλές.
3. Κόστος ασφάλειας ενάντια στον κίνδυνο απώλειας. Υπάρχουν διάφορα είδη που προσδιορίζουν το κόστος της ασφάλειας όπως :

- Κόστος αγοράς υλικού ή λογισμικού, όπως firewalls, IDS και on-time password generators.
- Απόδοση η οποία εξαρτάται από την σχέση χρόνου και ευκολίας στην χρήση (κωδικοποίηση - αποκωδικοποίηση).

Υπάρχουν επίσης διάφορα επίπεδα κινδύνου όπως :

- Άρση του απορρήτου (π.χ. ανάγνωση πληροφορίας από τρίτους).
- Απώλεια δεδομένων (διαγραφή δεδομένων).
- Απώλεια υπηρεσιών (χρήση των πηγών του δικτύου, άρνηση πρόσβασης στο δίκτυο κ.α.).

Μια πολιτική ασφάλειας για να είναι κατάλληλη για τον οργανισμό θα πρέπει να είναι αποδεκτή από όλους τους εργαζομένους και από τη διεύθυνση του οργανισμού ώστε να επιτύχει στους στόχους της. Οι ομάδες εργαζομένων που εμπλέκονται σε μια πολιτική ασφάλειας είναι :

- Απλοί χρήστες - η πολιτική ασφάλειας αφορά αυτούς ως επί το πλείστον.
- Προσωπικό υποστήριξης - είναι αυτοί που θα υλοποιήσουν και θα υποστηρίξουν την πολιτική ασφάλειας.
- Διοικητικό προσωπικό - καθορίζουν το βαθμό προστασίας των περισσότερων δεδομένων και αναλαμβάνουν το οικονομικό κόστος της πολιτικής που θα υλοποιηθεί.

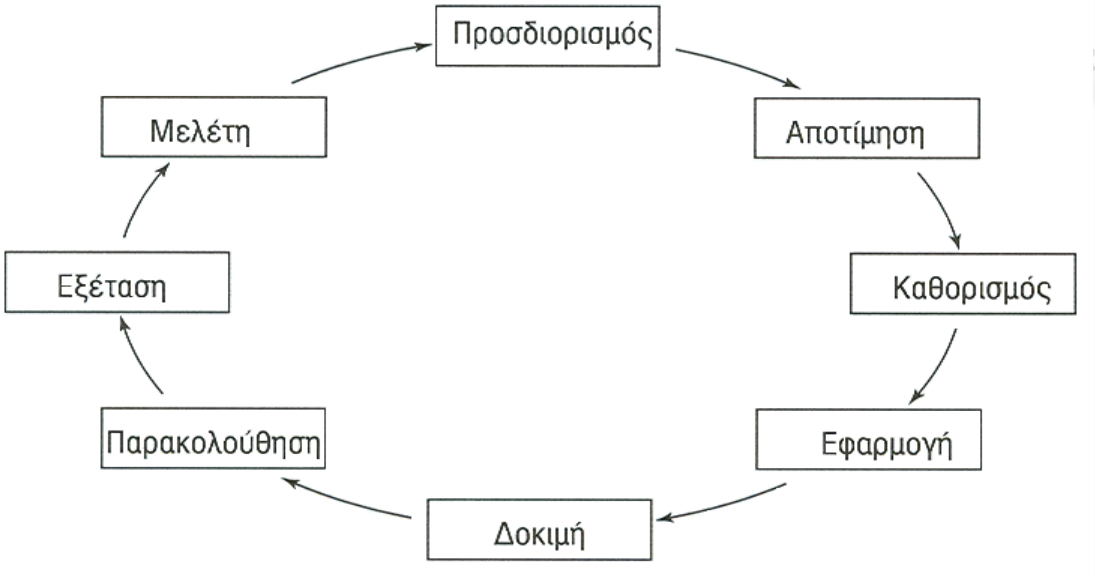
- Νομικοί σύμβουλοι - που ενδιαφέρονται για την φήμη και την νομική κάλυψη του οργανισμού.

1.5 Ο ΚΥΚΛΟΣ ΔΙΑΧΕΙΡΙΣΗ ΤΗΣ ΑΣΦΑΛΕΙΑΣ

Η διαχείριση της ασφάλειας είναι μια εργασία που πρέπει να γίνεται συνεχώς προκειμένου να διατηρείται το σύστημα όσο το δυνατό ασφαλέστερο. Δουλειά του διαχειριστή ασφάλειας είναι να καθορίζει ποια μέτρα ασφάλειας πρέπει να λαμβάνονται και αν αυτά τα μέτρα ασφάλειας εκτελούνται σωστά. Η όλη διαδικασία μπορεί να διαιρεθεί και σε διακριτά βήματα, τα οποία μπορούν να εκτελεστούν μεθοδικά. Ο κύκλος της διαχείρισης της ασφάλειας περιλαμβάνει τα παρακάτω βήματα :

- Προσδιορισμός των πιθανών τρωτών σημείων.
- Αποτίμηση των τρωτών σημείων για να καθοριστεί το πώς μπορούν να επιδιορθωθούν αποτελεσματικά.
- Καθορισμός αντιμέτρων που μπορούν να εφαρμοστούν αποτελεσματικά, ώστε να επιδιορθωθούν τα τρωτά σημεία.
- Εφαρμογή των αντιμέτρων.
- Δοκιμή των αντιμέτρων για έλεγχο της αποτελεσματικότητά τους, προσομοιώνοντας μια επίθεση.
- Παρακολούθηση των αρχείων καταγραφών του διακομιστή, των IDS και των firewalls για απόδειξη των παραβιάσεων της ασφάλειας.
- Εξέταση όλων των ενδείξεων παραβίασης για τον καθορισμό της εξέλιξης της παραβίασης και τον προσδιορισμό νέων πιθανών τρωτών σημείων.
- Μελέτη δημοσίων πηγών ασφάλειας για ειδήσεις και νέες ανακαλύψεις τρωτών σημείων ασφάλειας.
- Επανάληψη του κύκλου διαχείρισης της ασφάλειας.

Η όλη διαδικασία της διαχείρισης της ασφάλειας απεικονίζεται στο παρακάτω σχήμα 2.



Σχήμα 2. Διαχείριση της ασφάλειας.

Συνοψίζοντας η κυκλική φύση της ασφάλειας είναι κάτι το ιδιαίτερα σημαντικό. Σε αντίθεση με μια κατασκευή, η οποία είναι στατική και έχει μόνο μερικά γνωστά τρωτά σημεία, τα δίκτυα υπολογιστών δεν είναι στατικά – αλλάζουν συνεχώς. Κάθε νέα προσθήκη, λογισμικού ή υλικού, πρέπει να αποτιμηθεί μέσα στο περιβάλλον της ασφάλειας, ώστε να καθοριστεί αν θα προσθέσει ένα νέο τρωτό σημείο στο σύστημα. Οι μέθοδοι που χρησιμοποιούνται από εισβολείς για να προσπελάσουν ένα σύστημα πρέπει να μελετούνται συνεχώς και το λογισμικό του συστήματος πρέπει να ενημερώνεται, όταν εκδίδονται νέες διορθώσεις ασφάλειας.

ΚΕΦΑΛΑΙΟ 2

ΕΙΣΒΟΛΕΣ – ΑΠΕΙΛΕΣ

Μέσω των υπολογιστικών συστημάτων και των δικτύων διακινείται πλέον τεράστιος όγκος και μεγάλη ποικιλία πληροφοριών, καθιστώντας τα σημαντικό παράγοντα της καθημερινής δραστηριότητας. Η φύση αυτή των υπολογιστικών συστημάτων και των δικτύων έχει δημιουργήσει μία διαρκώς αυξανόμενη ανάγκη προστασίας των δεδομένων, λόγω του ότι υπολογιστικά συστήματα και δίκτυα είναι εκτεθειμένα σε ένα μεγάλο αριθμό απειλών αφού είναι δυνατή η μη εξουσιοδοτημένη πρόσβαση στις διακινούμενες πληροφορίες που δύσκολα ανιχνεύονται έχοντας πιθανά, καταστρεπτικές συνέπειες για τη προσωπική ζωή των πολιτών, την εύρυθμη λειτουργία οργανισμών (οικονομικών, στρατιωτικών, πολιτικών) και κατ' επέκταση κρατών.

Οι επίδοξοι εισβολείς είναι κακόβουλοι χρήστες που προσπαθούν για την καταστροφή ή υποκλοπή πληροφοριών που διαχειρίζονται τα υπολογιστικά συστήματα. Προκειμένου να υλοποιηθούν οι αρχές ασφάλειας και η σωστή άμυνα ενάντια στους εισβολείς απαιτείται πλήρης γνώση του αντιπάλου.

Γνωρίζοντας τα κίνητρα ενός εισβολέα, μπορούμε να προβλέψουμε τον κίνδυνο και να προσαρμόσουμε την άμυνά μας έτσι, ώστε να προστατευτούμε από τον τύπο εισβολέων που αναμένεται να επιτεθούν στο δίκτυό μας, διατηρώντας την ευελιξία του συστήματος, ώστε να μπορεί να χρησιμοποιείται από τους νόμιμους χρήστες.

Τα δυσάρεστα αποτελέσματα των εισβολών απασχόλησαν και συνεχίζουν να απασχολούν τόσο την επιστημονική κοινότητα όσο και τους κατασκευαστές λογισμικού και υλικού προς την κατεύθυνση ανεύρεσης μεθόδων ανίχνευσης και αντιμετώπισής τους.

2.1 ΤΙ ΕΙΝΑΙ ΕΙΣΒΟΛΗ ΚΑΙ ΤΥΠΟΙ ΕΙΣΒΟΛΕΩΝ

Με τον όρο εισβολή θα μπορούσαμε να χαρακτηρίσουμε την προσπάθεια προσπέλασης ενός συστήματος υπολογιστών, χωρίς εξουσιοδότηση με σκοπό την υποκλοπή ή την καταστροφή πληροφοριών. Είναι δηλαδή το σύνολο ενεργειών που προσπαθούν να διαβάλλουν την ακεραιότητα, την εμπιστευτικότητα ή τη διαθεσιμότητα ενός υπολογιστικού πόρου.
Ο χαρακτηρισμός εισβολέας αποδίδεται σε κάθε άτομο που επιχειρεί την εισβολή χωρίς να έχει εξουσιοδότηση για την ενέργειά του αυτή. Αρχικά ο όρος εισβολέας αναφερόταν στους πεπειραμένους χρήστες υπολογιστών. Όταν όμως η εισβολή στα συστήματα υπολογιστών έγινε δημοφιλής (σπάσιμο – cracking) ο όρος εισβολέας συνδέθηκε με διάφορες κατηγορίες χρηστών. Έτσι λοιπόν, ένας εισβολέας μπορεί να είναι ένας έφηβος που αναρωτιέται τι μπορεί να κάνει στο διαδίκτυο ή ένας φοιτητής που κατασκεύασε ένα νέο εργαλείο. Μπορεί να είναι κάποιος που προσπαθεί να έχει ίδιο όφελος ή ένας πληρωμένος κατάσκοπος που προσπαθεί να κλέψει πληροφορίες για ανταγωνιστές από εταιρίες ακόμα και από κράτη. Μπορεί ακόμα να είναι ένας απολυμένος ή δυσαρεστημένος υπάλληλος. Πιθανά κίνητρά του είναι η διασκέδαση, ο διανοητικός ανταγωνισμός, η αίσθηση της ισχύος ή το χρηματικό όφελος. Τους επιτιθέμενους εισβολείς μπορούμε να τους ταξινομήσουμε σε δύο τύπους : τους **εξωτερικούς επιτιθέμενους** οι οποίοι είναι μη-εξουσιοδοτημένοι χρήστες των μηχανημάτων στα οποία πραγματοποιούν επίθεση, και τους **εσωτερικούς επιτιθέμενους**, οι οποίοι είναι εξουσιοδοτημένοι χρήστες του συστήματος και υπερβαίνουν τα νόμιμα δικαιώματα πρόσβασης που έχουν. Οι επιτιθέμενοι αυτής της κατηγορίας διαχωρίζονται σε **μεταμφιεσμένους** (masqueraders) οι οποίοι χρησιμοποιούν τα πιστοποιητικά ταυτότητας και πιστοποίησης νόμιμων χρηστών, και σε **κρυφούς** (clandestine) επιτιθέμενους οι οποίοι ξεφεύγουν με επιτυχία από τα μέτρα παρακολούθησης και καταγραφής. Ανάλογα με τη σειρά αυξανόμενης απειλής οι εισβολείς κατατάσσονται στις παρακάτω κατηγορίες :

Ειδικοί ασφάλειας είναι σε θέση να κάνουν εισβολές, αλλά δεν το κάνουν για ηθικούς ή για οικονομικούς λόγους. Οι ειδικοί ασφάλειας υπολογιστών έχουν δει ότι βγάζουν περισσότερα χρήματα αν αποτρέπουν τις εισβολές, παρά αν τις κάνουν, οπότε ξοδεύουν το χρόνο τους παρακολουθώντας τις κοινότητες των εισβολέων και τις τρέχουσες τεχνικές προκειμένου να γίνουν πιο αποτελεσματικοί στη μάχη εναντίον των εισβολέων. Συχνά είναι οι πρώτοι που βρίσκουν νέες μεθόδους εισβολής και συχνά γράφουν λογισμικό για να ελέγχουν ή για να προκαλούν μια κατάσταση.

Έφηβοι εισβολείς είναι σπουδαστές που κάνουν εισβολές, ενώ βρίσκονται σε κάποια βαθμίδα της εκπαίδευσης - γυμνάσιο, λύκειο ή πανεπιστήμιο. Αυτοί οι εισβολείς μπορούν να χρησιμοποιούν τους δικούς τους υπολογιστές ή μπορούν να χρησιμοποιούν τους ισχυρούς πόρους της σχολής τους για να κάνουν τις εισβολές τους. Ενδιαφέρονται να εντυπωσιάσουν τους φίλους τους και κάνουν εισβολές κυρίως για να πάρουν δωρεάν πράγματα, όπως λογισμικό και μουσική. Αυτοί οι εισβολείς αποτελούν το 90% περίπου του συνολικού αριθμού δραστηριότητας εισβολών στο Internet.

Εισβολείς από ιδεολογία είναι εκείνοι που κάνουν εισβολές για να προωθήσουν κάποιο πολιτικό σκοπό. Από το 2000, η εισβολή από ιδεολογία έχει ξεφύγει από την εμφάνιση μερικών μόνο επεισοδίων και έχει φτάσει σε επίπεδο πλήρους πολέμου πληροφοριών. Στην προσπάθειά τους να διαδηλώσουν τις ιδέες τους, αυτοί οι εισβολείς (συνήθως) καταστρέφουν ιστοθέσεις ή κάνουν επιθέσεις άρνησης παροχής υπηρεσίας, εναντίον των ιδεολογικών τους αντιπάλων. Αν και σχεδόν ποτέ δεν κατευθύνουν τις επιθέσεις τους εναντίον στόχων που δεν είναι εχθροί τους, αθώοι χρήστες συχνά βρίσκονται στο μέσο των πυρών. Παραδείγματα εισβολών από ιδεολογία είναι η καταστροφή ιστοθέσεων εφημερίδων, κυβερνητικών υπηρεσιών και το σκουλήκι Code Red, το οποίο προέρχεται από την Κίνα (το οποίο κατέστρεψε ιστοθέσεις με ένα μήνυμα που δυσφημεί την κυβέρνηση των Η.ΠΑ). Αυτό το είδος εισβολής εμφανίζεται κατά κύματα, όταν συμβαίνουν μεγάλα γεγονότα στον πολιτικό στίβο και αποτελούν μικρό κίνδυνο, επειδή στην ουσία απλώς γράφουν τα συνθήματά τους στον κυβερνοχώρο, χωρίς να προκαλούν άλλα προβλήματα.

Εγκληματίες εισβολείς είναι εκείνοι που κάνουν εισβολές είτε για εκδίκηση, για να διαπράξουν κλοπές ή για να προκαλέσουν καταστροφές. Είναι αυτοί που έχουν εισβάλει σε διακομιστές Internet για να κλέψουν αριθμούς πιστωτικών καρτών ή έχουν εισβάλει στο μηχανισμό τραπεζικών συναλλαγών του Internet για να κλέψουν χρήματα. Είναι παρόμοιοι με κάθε άλλο εγκληματία και προσπαθούν να κάνουν ζημιά, αδιαφορώντας για το ποιος είναι το θύμα. Απειλούν ότι θα κάνουν επιθέσεις άρνησης παροχής υπηρεσιών, για να ζητήσουν χρήματα από εταιρείες τα έσοδα των οποίων προέρχονται από μια δημόσια ιστοθέση. Επειδή οι επιθέσεις άρνησης παροχής υπηρεσιών δεν μπορούν να αποτραπούν εύκολα (μπορούν να εμφανιστούν σαν μια μεγάλη ποσότητα νόμιμων αιτήσεων), τα θύματα συχνά αισθάνονται ότι δεν έχουν καμία άλλη επιλογή παρά να πληρώσουν.

Δυσαρεστημένοι υπάλληλοι είναι οι πιο επικίνδυνοι - και μπορούν να δημιουργήσουν τα περισσότερα προβλήματα από όλους τους εισβολείς. Μπορούν να προκαλέσουν σοβαρές καταστροφές στο δίκτυο της εταιρείας ή του οργανισμού που εργάζονται και δύσκολα ανιχνεύονται πριν να συμβούν. Οι επιθέσεις τους μπορεί να είναι από περίπλοκες (π.χ. ένας διαχειριστής δικτύου που διαβάζει τα e-mail άλλων ανθρώπων) μέχρι απλές (π.χ. ένας υπάλληλος που κάνει καταστροφές στο διακομιστή της βάσης δεδομένων). Ένας αποδοτικός τρόπος αποτροπής τέτοιων προβλημάτων είναι η γνωστοποίηση σε όλους τους υπαλλήλους μιας εταιρίας ή οργανισμού ότι το τμήμα πληροφορικής καταγράφει όλες τις δραστηριότητες των υπαλλήλων κατά την χρήση του δικτύου.

2.2 ΤΡΟΠΟΙ ΔΡΑΣΗΣ ΕΙΣΒΟΛΕΩΝ

Ο αριθμός των τρόπων δράσης των εισβολέων είναι μικρός αλλά ικανός για να επιτύχει το σκοπό του. Οι τρόποι με τους οποίους ένας εισβολέας μπορεί να προσπελάσει το δίκτυο είναι οι παρακάτω τέσσερις :

- **Συνδεόμενος μέσω του Internet :** Η εισβολή μέσω του Internet είναι η περισσότερο διαθέσιμη, ευκολότερα εκμεταλλεύσιμη και η πιο προβληματική περιοχή για εισβολή στο δίκτυο. Επιλύεται με την χρήση firewalls και IDS όπως θα αναλυθεί στην συνέχεια της εργασίας μας.

- **Χρησιμοποιώντας έναν υπολογιστή του δικτύου :** Επιτυγχάνεται με την προσωπική διείσδυση του εισβολέα μέσα στην επιχείρηση ή τον οργανισμό. Κάθεται σε ένα τερματικό και αρχίζει να διαμορφώνει την κατάσταση για περαιτέρω απομακρυσμένη διείσδυση μέσα στα υπολογιστικά συστήματα. Σε μεγάλες εταιρείες και οργανισμούς, όπου ο αριθμός των εργαζομένων είναι μεγάλος και οι περισσότεροι δεν γνωρίζονται μεταξύ τους και δεν χρησιμοποιούν κάρτες εισόδου ή δεν υπάρχει έλεγχος κατά την είσοδο, η διείσδυση είναι σχετικά εύκολη. Έτσι ο εισβολέας φτάνει στην αίθουσα του διακομιστή και σε ελάχιστο χρόνο μπορεί να συνδέσει ένα μικρό εξωτερικό μόντεμ ή ένα ασύρματο σημείο προσπέλασης, χωρίς καν να χρειαστεί η επανεκκίνηση του διακομιστή. Η αντιμετώπιση της απευθείας εισβολής μπορεί να επιτευχθεί με ισχυρή φυσική ασφάλεια στις εγκαταστάσεις των πληροφοριακών συστημάτων. Με την

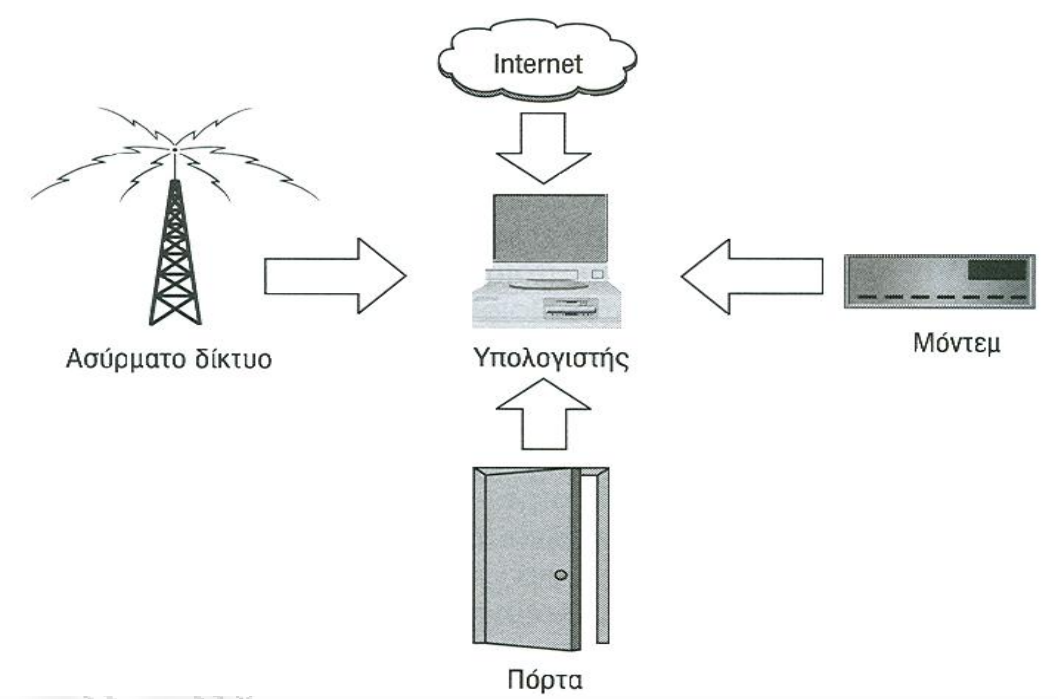
τοποθέτηση firewalls ανάμεσα στην σύνδεση WAN και στο εσωτερικό δίκτυο ή πίσω από ασύρματες συνδέσεις. Έτσι παρακολουθείται κάθε σύνδεση που βγαίνει από το κτήριο.

- **Καλώντας μέσω ενός διακομιστή απομακρυσμένης προσπέλασης (Remote Access Service, RAS) :** Η εισβολή μέσω τηλεφωνικής κλήσης, μέσω μόντεμ, ήταν παλιότερα ο μόνος τρόπος εισβολής, αλλά γρήγορα πήρε τη δεύτερη θέση, μετά από την εισβολή μέσω του Internet.Αυτό δεν σημαίνει ότι η εισβολή μέσω τηλεφωνικής κλήσης έχει εξαλειφθεί διότι οι εισβολείς που έχουν συγκεκριμένο στόχο, θα εφαρμόσουν κάθε διαθέσιμο μέσο για να τον προσπελάσουν. Η εισβολή μέσω τηλεφωνικής κλήσης σημαίνει συνήθως εκμετάλλευση ενός μόντεμ που είναι συνδεδεμένο σε ένα διακομιστή υπηρεσίας απομακρυσμένης προσπέλασης (RAS) και περιλαμβάνει κλήσεις προς διακριτούς υπολογιστές. Κάθε μόντεμ που έχει διαμορφωθεί, ώστε να απαντά για να επιτρέπει απομακρυσμένη προσπέλαση ή απομακρυσμένο έλεγχο από κάθε υπάλληλο που χρησιμοποιεί τον υπολογιστή, αποτελεί ένα πρόβλημα ασφάλειας. Η λύση του προβλήματος της εισβολής μέσω τηλεφωνικής κλήσης είναι σχετικά εύκολη με την τοποθέτηση των διακομιστών RAS έξω από τα firewalls μέσα στη δημόσια ζώνη ασφάλειας και με την επιβολή στους νόμιμους χρήστες να πιστοποιούνται πρώτα στο firewall για να εισέλθουν στους πόρους του δικτύου. Έτσι δεν θα πρέπει να επιτρέπεται σε καμία συσκευή να απαντά σε μια τηλεφωνική κλήση πίσω από αυτό το firewall. Αυτή η μέθοδος εξαλείφει το πρόβλημα της εισβολής μέσω τηλεφωνικής κλήσης, κάνοντας τις τηλεφωνικές κλήσεις να λειτουργούν ως μια σύνδεση Internet.

- **Συνδεόμενος μέσω ενός ανασφαλούς ασύρματου δικτύου :** Η ασύρματη επικοινωνία, που στηρίζεται στο δημοφιλές πρωτόκολλο 802. 11 b που λειτουργεί στα 11 Mbps, είναι φθηνή και έχει αρχίσει να χρησιμοποιείται ευρέως στον χώρο των δικτύων. Το πρωτόκολλο 802.11 επιτρέπει σε διαχειριστές να συνδέουν σημεία ασύρματης προσπέλασης (WAP) στα δίκτυά τους και να επιτρέπουν σε χρήστες (συνήθως με φορητούς υπολογιστές) να προσπελαύνουν το δίκτυό τους. Δύο σημεία ασύρματης προσπέλασης WAP μπορούν να συνδεθούν μεταξύ τους για να δημιουργήσουν μια ασύρματη γέφυρα ανάμεσα σε κτήρια, κάτι που μπορεί να εξοικονομήσει δεκάδες χιλιάδες ευρώ από μια εταιρεία, σε κόστος κατασκευής ή κόστος κυκλωμάτων. Το 802.11 b δινόταν με ένα πολυδιαφημισμένο σχήμα

κρυπτογράφησης, που ονομαζόταν Διασφάλιση Απορρήτου Ισοδύναμη της Ενσύρματης Επικοινωνίας (WEP), το οποίο υποσχόταν ότι θα επιτρέπει τη δικτύωση με την ίδια ασφάλεια που παρέχουν τα ενσύρματα δίκτυα. Η ιδέα ήταν σπουδαία. Οι ειδικοί της ασφάλειας χρειάστηκαν όμως λιγότερο από 11 ώρες για να παραβιάσουν το σύστημα. Αρχικά κανένας δεν έδωσε σημασία, οπότε αυτοί οι ειδικοί εξέδωσαν ένα λογισμικό που επέτρεπε την αυτόματη εισβολή. Το WEP έχει παραβιαστεί τόσο πολύ πλέον, που πρέπει να θεωρείται σαν ανασφαλής σύνδεση μέσω του Internet. Όλες οι ασύρματες συσκευές πρέπει να τοποθετηθούν στη δημόσια πλευρά του Internet, και οι χρήστες πρέπει να πιστοποιούνται με το firewall τους. Η νεότερη υπηρεσία 128-bit WEP είναι περισσότερο ασφαλής, αλλά δεν πρέπει επίσης να θεωρείται ισοδύναμη της ενσύρματης ασφάλειας.

Όλοι οι παραπάνω τρόποι δράσεις των εισβολέων απεικονίζοντα στο παρακάτω σχήμα.



Σχήμα 3. Τρόποι δράσης εισβολέων.

2.3 ΤΕΧΝΙΚΕΣ ΕΙΣΒΟΛΗΣ

Οι επιθέσεις εισβολής προχωρούν σε μια σειρά φάσεων, χρησιμοποιώντας διάφορα εργαλεία και τεχνικές. Ο εισβολέας προκειμένου να επιτύχει την εισβολή του σε ένα σύστημα εφαρμόζει τις παρακάτω φάσεις :

- Επιλογή στόχου.
- Συλλογή πληροφοριών.
- Επίθεση

Ο εισβολέας αφού επιλέξει τον στόχο του θα προσπαθήσει να μάθει στοιχεία για το δίκτυο στόχο μέσω διαδοχικών επιθέσεων, οπότε αυτές οι φάσεις παρέχουν στοιχεία στον εισβολέα, ώστε να μπορεί να συλλέξει πληροφορίες από επιθέσεις που απέτυχαν.

2.3.1 Επιλογή Στόχου

Κατά την φάση αυτή ο εισβολέας προσδιορίζει ένα συγκεκριμένο υπολογιστή για να του επιτεθεί. Για να περάσει από αυτήν την φάση, πρέπει να είναι διαθέσιμος κάποιος τρόπος επίθεσης, οπότε το μηχάνημα πρέπει είτε να έχει διαφημίσει την παρουσία του ή να έχει βρεθεί μέσω μιας ενέργειας αναζήτησης. Προκειμένου ο εισβολέας να επιλέξει το στόχο του εφαρμόζει διάφορες μεθόδους οι οποίες αναλύονται παρακάτω.

- Αναζήτηση DNS (Domain Main System)

Οι εισβολείς που ψάχνουν για ένα συγκεκριμένο στόχο χρησιμοποιούν την ίδια μέθοδο που χρησιμοποιούν τα προγράμματα περιήγησης στο Web για να βρουν ένα ξενιστή (host). Ψάχνουν το όνομα τομέα χρησιμοποιώντας ένα Σύστημα Ονομάτων Τομέων (DNS, υπηρεσία καταλόγου ονόματος ξενιστή προς διεύθυνση IP του Internet). Η συγκεκριμένη ενέργεια είναι εύκολη και από τεχνικής σκοπιάς δεν θεωρείται επίθεση. Για να προστατεύσει κάποιος το δίκτυό του από αυτήν την τεχνική επιλογής στόχου, αρκεί να μην καταχωρίσει δημόσια ονόματα τομέων για τους ξενιστές του, εκτός των διακομιστών ταχυδρομείου και Web. Έτσι περιορίζεται το πρόβλημα των επιθέσεων σε αυτούς μόνο τους διακομιστές. Για το εσωτερικό του δικτύου του πρέπει να χρησιμοποίηση εσωτερικούς διακομιστές DNS, που

δεν είναι διαθέσιμοι στο Internet και οι οποίοι δεν εκτελούν μεταφορές ζώνης DNS με δημόσιους διακομιστές DNS. Αυτό επιτυγχάνεται εύκολα καταχωρώντας το όνομά του ".com" στον ISP του και χρησιμοποιώντας το Windows Active Directory ή το Bind στο Unix στον εσωτερικό του διακομιστή, που δεν προσπελαύνεται από το Internet, προκειμένου να διαχειριστεί το εσωτερικό του όνομα.

- Σάρωση Διευθύνσεων Δικτύου

Οι εισβολείς που ψάχνουν για ευκαιριακούς στόχους χρησιμοποιούν μια μέθοδο που καλείται σάρωση διευθύνσεων δικτύου για να τους βρουν. Οι εισβολείς θα καθορίσουν διευθύνσεις αρχής και τέλους για σάρωση και μετά το πρόγραμμά τους θα στείλει ένα μήνυμα ηχούς ICMP σε καθεμία από αυτές τις διευθύνσεις δικτύου. Αν ένας υπολογιστής απαντήσει σε μια από αυτές τις διευθύνσεις, τότε οι εισβολείς έχουν βρει ένα στόχο. Σαρώσεις διευθύνσεων γίνονται συνεχώς στο Internet. Στατιστικά ένας υπολογιστής συνδεδεμένος στο Internet, πιθανότητα η διεύθυνσή του να σαρώνεται τουλάχιστον μια φορά την ώρα. Ο καλύτερος τρόπος για να ματαιωθεί αυτό το είδος επίθεσης είναι να διαμορφώνει κάθε χρήστης τα μηχανήματά του, ώστε να απαντούν σε μηνύματα ηχούς ICMP. Αυτό θα δυσκολέψει τους εισβολείς να καταλάβουν ότι τα μηχανήματά του υπάρχουν.

- Σάρωση θύρας.

Εφαρμόζοντας αυτή την μέθοδο ο εισβολέας, αφού επιλέξει έναν υπολογιστή στόχου, θα προσπαθήσει να καθορίσει ποιο λειτουργικό σύστημα εκτελεί και ποιες υπηρεσίες παρέχει στους πελάτες του δικτύου. Σε ένα δίκτυο TCP/IP (όπως το Internet), οι υπηρεσίες παρέχονται σε αριθμημένες συνδέσεις, που καλούνται θύρες. Οι θύρες στις οποίες αποκρίνεται ένας υπολογιστής καθορίζουν συνήθως το λειτουργικό σύστημα και τις παρεχόμενες υπηρεσίες του υπολογιστή στόχου. Υπάρχουν αρκετά εργαλεία στο Internet, τα οποία μπορεί να χρησιμοποιήσει ένας εισβολέας για να καθορίσει ποιες θύρες αποκρίνονται σε αιτήσεις συνδέσεων δικτύου. Αυτά τα εργαλεία δοκιμάζουν κάθε θύρα με τη σειρά και αναφέρουν στον εισβολέα ποιες θύρες αρνούνται τις συνδέσεις και ποιες όχι. Ο εισβολέας μπορεί κατόπιν να επικεντρώσει την προσοχή του στις θύρες που αποκρίνονται σε υπηρεσίες, οι οποίες συχνά μένουν ανασφάλιστες ή έχουν προβλήματα ασφάλειας. Η σάρωση θυρών μπορεί να αποκαλύψει ποιο λειτουργικό σύστημα χρησιμοποιεί ο υπολογιστής, επειδή κάθε λειτουργικό σύστημα έχει ένα διαφορετικό σύνολο προεπιλεγμένων υπηρεσιών. Για παράδειγμα, αν κάνει σάρωση στις θύρες TCP 0 ως 150, ένας εισβολέας μπορεί να διακρίνει ξενιστές Windows (από την παρουσία της θύρας 139 στη λίστα σάρωσης) και διάφορους

ξενιστές Unix (από την παρουσία απλών υπηρεσιών TCP/IP όπως τη θύρα 23 [Telnet], την οποία τα Windows δεν εγκαθιστούν προεπιλεγμένα). Αυτές οι πληροφορίες "λένε" στον εισβολέα ποια εργαλεία πρέπει να χρησιμοποιήσει για να εισβάλει στο δίκτυο στόχο. Οι σαρώσεις θυρών αποτελούν άμεση απόδειξη ότι ένας εισβολέας έχει βάλει στόχο ένα δίκτυο. Γι' αυτόν το λόγο πρέπει κάθε χρήστης να μελετά σοβαρά όλες τις σαρώσεις θυρών.

- Σάρωση Υπηρεσίας

Τα σκουλήκια του Internet, τα οποία είναι αυτοματοποιημένες επιθέσεις εισβολής, που διαπράττονται από προγράμματα, τα οποία εκτελούνται σε προσβεβλημένους υπολογιστές, λειτουργούν υλοποιώντας μια επίθεση και μετά ψάχνοντας για υπολογιστές που είναι ευπρόσβλητοι σε αυτή. Αυτή η αναζήτηση παίρνει τη μορφή μιας σάρωσης θύρας προς τη συγκεκριμένη θύρα που εξετάζει η επίθεση. Επειδή το σκουλήκι κάνει σάρωση σε μια θύρα, δεν θα εμφανιστεί ούτε ως σάρωση διεύθυνσης (επειδή δεν είναι μια ICMP), ούτε ως σάρωση θύρας (επειδή κτυπά μόνο μια θύρα). Στην πραγματικότητα, δεν υπάρχει τρόπος να καταλάβετε αν μια σάρωση υπηρεσίας είναι μια νόμιμη προσπάθεια σύνδεσης ή μια κακόβουλη σάρωση υπηρεσίας.

Συνήθως μια σάρωση υπηρεσίας ακολουθείται είτε από μια ανίχνευση αρχιτεκτονικής (αν το σκουλήκι είναι ευφυές) ή απλώς από μια προσπάθεια επίθεσης στην συγκεκριμένη υπηρεσία, όπως είναι μια υπερχείλιση καταχωρητή (buffer overrun). Με τον όρο υπερχείλιση καταχωρητή εννοούμε μια ενέργεια εισβολής που στέλνει συγκεκριμένες λάθος μορφοποιημένες πληροφορίες σε μια υπηρεσία, για να εκτελέσει κώδικα της επιλογής του εισβολέα στον υπολογιστή στόχου. Έτσι δημιουργεί μια διαδρομή για μελλοντική εκμετάλλευση.

2.3.2 Συλλογή Πληροφοριών

Η συλλογή πληροφοριών είναι η φάση κατά την οποία ο εισβολέας καθορίζει τα χαρακτηριστικά του στόχου, πριν να του επιτεθεί. Αυτή μπορεί να γίνει είτε μέσω δημόσια διαθέσιμων πληροφοριών, που εκδίδονται για το στόχο ή ερευνώντας το στόχο, χρησιμοποιώντας μη επιθετικές μεθόδους, για να πάρει πληροφορίες από αυτόν. Η φάση αυτή επιτυγχάνεται με τους παρακάτω τρόπους.

- Συλλογή Δεδομένων SNMP

Το πρωτόκολλο Simple Network Management Protocol (SNMP) είναι ένα βασικό εργαλείο για διαχείριση μεγάλων δικτύων TCP/IP αλλά χωρίς ενσωματωμένη ασφάλεια. Το SNMP επιτρέπει στο διαχειριστή να υποβάλει ερωτήματα απομακρυσμένα για την κατάσταση συσκευών δικτύου, για την τροποποίηση της διαμόρφωσής τους και να ελέγξει τις λειτουργίες τους. Δυστυχώς, οι εισβολείς μπορούν επίσης να χρησιμοποιήσουν το SNMP για να συλλέξουν δεδομένα για ένα δίκτυο ή να επέμβουν στην λειτουργία του.

Όπως είπαμε παραπάνω το πρωτόκολλο SNMP έχει σχεδιαστεί έτσι, ώστε να παρέχει αυτόματα τις λεπτομέρειες διαμόρφωσης συσκευών δικτύου. Έτσι, "τρύπιες" συσκευές στην δημόσια πλευρά ενός δικτύου, μπορούν να δώσουν πάρα πολλές πληροφορίες για το εσωτερικό του.

Σχεδόν κάθε τύπος συσκευής δικτύου, από συγκεντρωτές μέχρι μεταγωγείς και μέχρι δρομολογητές προς διακομιστές, μπορεί να διαμορφωθεί ώστε να παρέχει πληροφορίες διαμόρφωσης και διαχείρισης SNMP. Διασυνδέσεις όπως τα καλωδιακά μόντεμ και πολλά firewalls συχνά διαμορφώνονται μέσω SNMP. Λόγω της πανταχού παρουσίας του SNMP συχνά αγνοείται σε συσκευές που βρίσκονται έξω από το δημόσιο firewall,και αποτελεί μια πηγή πληροφοριών για το δίκτυο και επίσης παρέχει την δυνατότητα σε έναν εισβολέα να διαχειριστεί μια συσκευή απομακρυσμένα.

- Ανίχνευση Αρχιτεκτονικής

Οι ανιχνεύσεις αρχιτεκτονικής εργάζονται μελετώντας τα μηνύματα σφάλματος με τα οποία αποκρίνονται οι υπολογιστές, όταν προκύπτουν προβλήματα. Αντί να προσπαθήσουν να κάνουν μια επίθεση, οι ανιχνεύσεις : προσπαθούν απλώς να πάρουν μια απόκριση από ένα σύστημα και να την εξετάσουν. Οι εισβολείς είναι σε θέση να προσδιορίσουν το λειτουργικό σύστημα που εκτελείται στον υπολογιστή στόχου, με βάση την ακριβή φύση του μηνύματος σφάλματος, επειδή κάθε τύπος λειτουργικού συστήματος αποκρίνεται κάπως διαφορετικά.

Οι εισβολείς εξετάζουν τις αποκρίσεις σε λανθασμένες μεταδόσεις πακέτων από έναν ξενιστή στόχου, χρησιμοποιώντας ένα αυτοματοποιημένο εργαλείο, το οποίο περιέχει μια βάση δεδομένων με γνωστούς τύπους αποκρίσεων. Επειδή δεν υπάρχει πρότυπος ορισμός αποκρίσεων, κάθε λειτουργικό σύστημα απαντά με ένα μοναδικό τρόπο. Συγκρίνοντας τις μοναδικές αποκρίσεις με μια βάση δεδομένων γνωστών αποκρίσεων, οι εισβολείς μπορούν να καθορίσουν ποιο λειτουργικό σύστημα εκτελεί ο ξενιστής στόχου. Για να αμυνθούμε σε αυτό τον τρόπο εισβολής δεν αρκεί να έχουμε μπλοκάρει μόνο τις θύρες αλλά να έχουμε

λάβει όλα τα μέτρα ασφάλειας που διασφαλίζουν το λειτουργικό σας σύστημα, ακόμη και αν πιστεύουμε ότι ο εισβολέας δεν γνωρίζει ποιο λειτουργικό σύστημα έχουμε.

- Αναζητήσεις Υπηρεσιών Καταλόγου

Το πρωτόκολλο Lightweight Directory Access Protocol (LDAP) χρησιμοποιείται για να διαβάσει, να τροποποίηση ή να γράψει πληροφορίες για χρήστες, υπολογιστές και άλλους πόρους ενός δικτύου, σε μια υπηρεσία καταλόγου. Είναι μια υπηρεσία από την οποία μπορούν να εξαχθούν πληροφορίες. Οι χρήστες παρέχοντας πληροφορίες LDAP στο κοινό, δίνουν πάρα πολλές πληροφορίες, οι οποίες μπορεί να περιλαμβάνουν πολύτιμες ενδείξεις για τη φύση του δικτύου τους και τους ίδιους. Οι εισβολείς χρησιμοποιούν το LDAP, καθώς και παλιότερες υπηρεσίες καταλόγου, όπως τις Finger και Who is, προκειμένου να συλλέξουν τις πληροφορίες για τα συστήματα μέσα στο δίκτυο στόχο και τους χρήστες του.

- Μύρισμα (sniffing)

Μύρισμα είναι η συλλογή όλων των πακέτων που ρέουν επάνω σε ένα δίκτυο και η εξέταση των περιεχομένων τους, μπορεί να χρησιμοποιηθεί για να καθορίσει σχεδόν όλα τα στοιχεία για ένα δίκτυο. Το μύρισμα μπορεί να θεωρηθεί υποκλοπή σε έναν υπολογιστή. Αν και κρυπτογραφημένα πακέτα μπορούν να συλλεχτούν μέσω μυρίσματος, είναι άχρηστα, εκτός και αν ο συλλέκτης έχει κάποιο τρόπο να τα αποκρυπτογραφήσει.

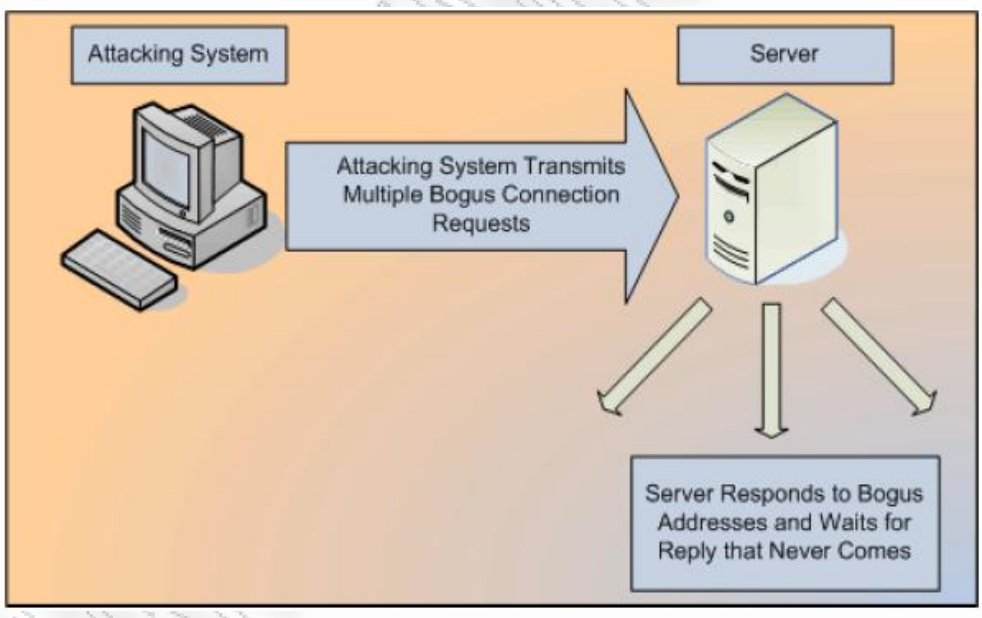
Το μύρισμα είναι από τεχνικής σκοπιάς μια επίθεση συλλογής πληροφοριών, αλλά δεν μπορεί να γίνει χωρίς να έχει κάποιος φυσική πρόσβαση στο δίκτυο ή να έχει ήδη παραβιάσει έναν υπολογιστή μέσα στο δίκτυο. Δεν είναι δυνατό να υποκλαπεί απομακρυσμένα μια σύνδεση, παρά μόνο αν γίνει μια επίθεση ενδιαμέσου εναντίον του υπολογιστή. Γι' αυτόν το λόγο, τέτοιες επιθέσεις είναι πολύ σπάνιες.

2.3.3 Επιθέσεις

Οι εισβολείς χρησιμοποιούν διάφορα είδη επιθέσεων εναντίον των υπολογιστών. Οι περισσότερες από τις επιθέσεις είναι εξειδικευμένες ώστε να εκμεταλλεύονται μια συγκεκριμένη υπηρεσία δικτύου. Παρακάτω αναφέρουμε τους συνηθέστερους και περισσότερο εφαρμόσιμους τύπους επιθέσεων ανάλογα με τη σειρά δυσκολίας διάπραξής τους.

- Άρνηση Παροχής Υπηρεσίας (Denial of Service, DoS)

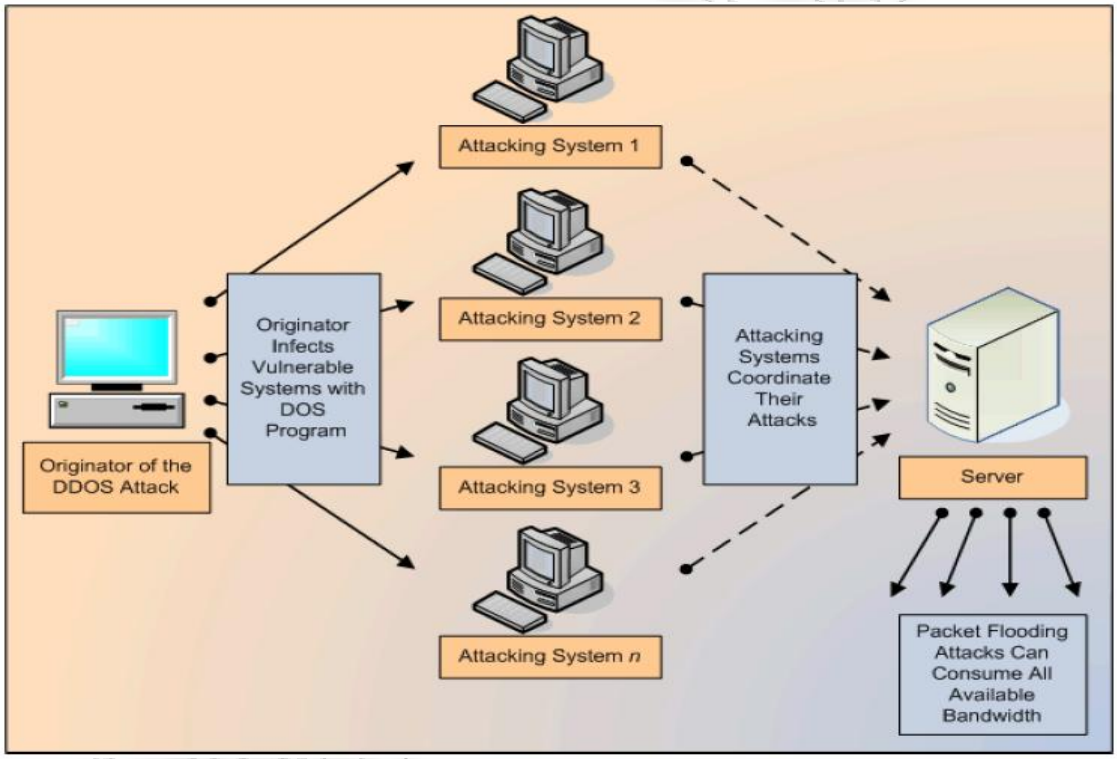
Οι δικτυωμένοι υπολογιστές υλοποιούν ένα συγκεκριμένο πρωτόκολλο για μετάδοση δεδομένων και αναμένουν αυτό το πρωτόκολλο να μεταδώσει πληροφορίες που έχουν κάποια σημασία. Όταν το πρωτόκολλο υλοποιείται λανθασμένα και δεν γίνεται αρκετός έλεγχος σφαλμάτων για ανίχνευση του σφάλματος, είναι πιθανό να συμβεί μια επίθεση άρνησης παροχής υπηρεσίας (DoS) . Οι DoS επιθέσεις (σχήμα 4) συντρίβουν τους κεντρικούς υπολογιστές με ψευδή κυκλοφορία και αιτήματα για συνδέσεις, εξαντλώντας τελικά τους πόρους ενός κεντρικού υπολογιστή. Όταν χιλιάδες από αυτά τα ψευδή αιτήματα υποβάλλονται, ο κεντρικός υπολογιστής εξαντλεί την ομάδα συνδέσεών του, η οποία αποτρέπει την πρόσβαση στους χρήστες. Έτσι σε ορισμένες περιπτώσεις, ο υπολογιστής που υφίσταται την επίθεση θα καταρρεύσει ή θα κρεμάσει. Σε άλλες περιπτώσεις, η υπηρεσία που υφίσταται την επίθεση θα αποτύχει χωρίς να προκαλέσει κατάρρευση του υπολογιστή.



Σχήμα 4. Επίθεση τύπου DoS.

Μια άλλη μορφή DoS επίθεσης είναι η κατανεμημένη επίθεση Άρνησης Παροχής Υπηρεσίας (Distributed Denial of Service, DDoS) η οποία χρησιμοποιεί πολλούς υπολογιστές για να πραγματοποιήσει μία κατευθυνόμενη επίθεση Άρνησης Παροχής Υπηρεσίας (DoS) ενάντια ενός ή περισσότερων στόχων (σχήμα 5). Χρησιμοποιώντας την τεχνολογία πελάτη - εξυπηρετητή, ο επιτιθέμενος μπορεί να πολλαπλασιάσει σημαντικά την αποτελεσματικότητα

της επίθεσης DoS θέτοντας υπό τον έλεγχό του, τους πόρους πολλαπλών ακούσιων συνεργών υπολογιστών, οι οποίοι χρησιμοποιούνται σαν πλατφόρμες επίθεσης. Η επίθεση DDoS είναι η πιο εξελιγμένη μορφή των επιθέσεων DoS. Διαχωρίζεται από τις άλλες επιθέσεις, από την ικανότητά της να αναπτύσσει τα όπλα της με ένα κατανεμημένο τρόπο στο Διαδίκτυο και να αθροίζει αυτές τις δυνάμεις ώστε να δημιουργηθεί πολύ επικίνδυνη κυκλοφορία. Οι επιθέσεις DDoS ποτέ δεν προσπαθούν να μπουν στο σύστημα του θύματος, καθιστώντας κατά αυτό τον τρόπο κάθε παραδοσιακό μηχανισμό προστασίας ασφάλειας μη αποτελεσματικό. Όσο πιο περίπλοκη είναι μια υπηρεσία, τόσο πιθανότερο είναι να υποστεί μια επίθεση άρνησης παροχής υπηρεσίας.



Σχήμα 5. Επίθεση τύπου DDoS.

- Πλημμύρες (flood)

Με τον όρο πλημμύρα χαρακτηρίζουμε μια επίθεση που προσπαθεί να κατακλύσει έναν πόρο μεταδίδοντας μεγάλους όγκους κίνησης. Οι πλημμύρες είναι απλές επιθέσεις άρνησης παροχής υπηρεσιών, που εργάζονται χρησιμοποιώντας σπάνιους πόρους, όπως είναι το εύρος ζώνης δικτύου ή την υπολογιστική ισχύ ενός υπολογιστή. Ένας από τους πιο γνωστούς τύπους πλημμύρας, η πλημμύρα SYN, περιγράφεται παρακάτω.

Η πλημμύρα SYN εκμεταλλεύεται το μηχανισμό σύνδεσης του TCP (Transmission Control Protocol). Όταν ξεκινάει μια σύνδεση TCP/IP, ο αιτών μεταδίδει ένα μήνυμα SYN στην αιτούσα υπηρεσία του ξενιστή και ο παραλήπτης διακομιστής αποκρίνεται με ένα μήνυμα SYN-ACK που δέχεται τη σύνδεση. Ο εισβολέας αποκρίνεται με ένα μήνυμα ACK και έτσι η κίνηση μπορεί να αρχίσει να ρέει επάνω στην αμφίδρομη σύνδεση TCP. Όταν ένας διακομιστής δέχεται το αρχικό μήνυμα SYN, συνήθως δημιουργεί μια σειρά βημάτων, για να χειριστεί τις αιτήσεις σύνδεσης. Αυτή η σειρά βημάτων απαιτεί χρόνο ΚΜΕ και δεσμεύει μια ποσότητα μνήμης. Πλημμυρίζοντας ένα δημόσιο διακομιστή με πακέτα SYN, τα οποία δεν ακολουθούνται ποτέ από ένα ACK, οι εισβολείς μπορούν να κάνουν το δημόσιο διακομιστή να δεσμεύσει μνήμη και χρόνο επεξεργαστή για να τα χειριστεί και έτσι να απαγορεύει σε νόμιμους χρήστες να χρησιμοποιούν τους ίδιους πόρους. Το πρακτικό αποτέλεσμα μιας πλημμύρας SYN είναι ότι ο διακομιστής που δέχεται την επίθεση γίνεται πολύ αργός και οι νόμιμοι χρήστες δεν μπορούν να συνδεθούν. Αυτό το είδος πλημμύρας SYN δεν μπορεί να διακριθεί από τον απλό μεγάλο όγκο κίνησης και έτσι να μπορέσει να ξεπεράσει τα φίλτρα πλημμύρας SYN.

- Πλαστογραφημένο E-mail.

Οι εισβολείς μπορούν να δημιουργήσουν e-mail που φαίνεται να προέρχεται από οποιονδήποτε θέλουν. Επίσης μπορούν να αλλάξουν την απάντηση στον αποστολέα κι έτσι η πλαστογράφηση γίνεται μη ανιχνεύσιμη. Τα πλαστογραφημένα e-mail περιλαμβάνουν έναν εγκαταστάσιμο Δούρειο Ίππο ή μια σύνδεση προς μια κακόβουλη ιστοθέση. Είναι μια μορφή ψυχολογικής επίθεσης, που παρακινούν τον αποδέκτη να απαντήσει σε αυτά με αποτέλεσμα χρήσιμες πληροφορίες να έρθουν στη διάθεση του εισβολέα. Αυτός είναι ο ευκολότερος τρόπος προσπέλασης ενός συγκεκριμένου δικτύου στόχου.

- Δούρειοι Ίπποι (Trojan Horse)

Οι Δούρειοι ίπποι είναι προγράμματα, τα οποία εγκαθίστανται κρυφά σε ένα σύστημα στόχου, απευθείας από ένα εισβολέα, μέσω ενός ιού ή σκουληκιού σε έναν ανυποψίαστο χρήστη και προσποιούνται ότι έχουν άλλες λειτουργίες από αυτές που πραγματικά υλοποιούν. Αφού εγκατασταθεί, ο Δούρειος ίππος είτε επιστρέφει πληροφορίες στον εισβολέα ή του παρέχει άμεση πρόσβαση στον υπολογιστή του θύματος. Οι πιο χρήσιμοι Δούρειοι ίπποι ονομάζονται πίσω πόρτες. Αυτά τα προγράμματα παρέχουν ένα μηχανισμό με βάση τον οποίο ο εισβολέας μπορεί να ελέγξει απευθείας τον υπολογιστή. Τα ιδανικά προγράμματα πίσω πόρτας είναι μικρά και γρήγορα εγκαθιστάμενα. Οι Δούρειοι ίπποι

συνήθως μεταφέρονται μέσω ιών που παράγονται από e-mail ή στέλνονται ως συνημμένα σε e-mail.

- Phishing

Ο όρος phishing αναφέρεται στη διαδικασία "ψαρέματος" για λογαριασμούς και κωδικούς πρόσβασης. Ο εισβολέας δημιουργεί μια ιστοθέση που μιμείται την εμφάνιση μιας έγκυρης ιστοθέσης και στέλνοντας ένα μήνυμα e-mail, που φαίνεται ότι είναι έγκυρο, προσκαλεί ανθρώπους να συνδεθούν σε αυτή. Το θύμα συνδέεται σε αυτήν την ιστοθέση και προσπαθώντας να χρησιμοποιήσει κάποια υπηρεσία της πληκτρολογεί όνομα λογαριασμού και κωδικό πρόσβασης. Έτσι τα στοιχεία του θύματος είναι πλέον στη διάθεση του εισβολέα. Μια καλή διαδικασία ψαρέματος μπορεί να ψαρέψει χιλιάδες έγκυρους συνδυασμούς λογαριασμών και κωδικών πρόσβασης για ηλεκτρονικές ιστοθέσεις τραπεζών, ιστοθέσεις χρηματιστηριακών συναλλαγών ή κάθε τύπου ιστοθέσεις όπου διεξάγονται οικονομικές συναλλαγές. Επομένως, θα πρέπει πάντα να επιβεβαιώνουμε τη διεύθυνση των ιστοθέσεων στις οποίες συνδεόμαστε και μας ζητούν οποιεσδήποτε πληροφορίες του λογαριασμού μας.

- Υπερχειλίσεις Καταχωρητή

Οι υπερχειλίσεις καταχωρητή είναι μια κλάση επιθέσεων που εκμεταλλεύονται μια συγκεκριμένη αδυναμία που παρουσιάζεται σε λογισμικό. Οι υπερχειλίσεις καταχωρητή εκμεταλλεύονται το γεγονός ότι τα περισσότερα προγράμματα δεσμεύουν μπλοκ της μνήμης σε τμήματα σταθερού μεγέθους για να δημιουργήσουν μια πρόχειρη περιοχή, που καλείται καταχωρητής (buffer), μέσα στην οποία επεξεργάζονται εσωτερικές πληροφορίες δικτύου. Αυτοί οι καταχωρητές προγραμματίζονται ώστε να έχουν σταθερό μέγιστο μέγεθος ή να εμπιστεύονται το μήνυμα που δηλώνει το μέγεθός τους. Οι υπερχειλίσεις καταχωρητή προκαλούνται όταν ένα μήνυμα "λέει" ψέματα για το μέγεθός του ή είναι ηθελημένα μεγαλύτερο από το επιτρεπόμενο μέγιστο μέγεθος. Για παράδειγμα, αν ένα μήνυμα "λέει" ότι έχει μήκος 240 bytes, αλλά στην πραγματικότητα έχει μήκος 256 bytes, η υπηρεσία που το λαμβάνει μπορεί να δεσμεύσει ένα καταχωρητή μήκους 240 bytes αλλά να αντιγράψει 256 bytes πληροφοριών σε αυτόν τον καταχωρητή. Τα 16 bytes μνήμης πέρα από το τέλος του καταχωρητή θα αντικατασταθούν από οτιδήποτε περιέχουν τα τελευταία 16 bytes του μηνύματος. Οι εισβολείς εκμεταλλεύονται αυτά τα προβλήματα εισάγοντας κώδικα γλώσσας μηχανής στο τμήμα του μηνύματος που βρίσκεται μετά από το τέλος του καταχωρητή. Ακόμη πιο προβληματικό είναι το γεγονός ότι το λογισμικό γράφεται συνήθως με τέτοιον τρόπο ώστε η εκτέλεση του κώδικα να αρχίζει μετά το τέλος της θέσης του καταχωρητή και

έτσι να επιτρέπει στον εισβολέα να εκτελεί κώδικα μέσα στο περιβάλλον ασφαλείας της εκτελούμενης υπηρεσίας. Γράφοντας ένα μικρό πρόγραμμα για να ανοίξουν μια τρύπα ασφάλειας και τοποθετώντας αυτόν τον κώδικα στο ωφέλιμο τμήμα του καταχωρητή, οι εισβολείς μπορούν να πάρουν τον έλεγχο του συστήματος. Συνεχώς ανακαλύπτονται νέες επιθέσεις υπερχείλισης καταχωρητή και είναι από τις πιο σοβαρές απειλές επιθέσεων σήμερα. Για να προστατευθούν οι χρήστες από αυτές θα πρέπει να ενημερώνονται συνεχώς για θέματα ασφάλειας για το λειτουργικό τους σύστημα ή να χρησιμοποιούν πληρεξούσιους (proxies) ασφάλειας, οι οποίοι μπορούν να απορρίψουν ύποπτες ή λάθος διαμορφωμένες συνδέσεις πριν αυτές να φτάσουν στο διακομιστή τους.

- Δρομολόγηση Προέλευσης (source routing)

Η οικογένεια πρωτοκόλλων TCP/IP περιλαμβάνει μια σπάνια χρησιμοποιούμενη επιλογή για καθορισμό του ακριβούς δρόμου που πρέπει να ακολουθήσει ένα πακέτο, καθώς διασχίζει ένα δίκτυο που βασίζεται στο πρωτόκολλο TCP/IP (σαν το Internet). Αυτή η επιλογή ονομάζεται δρομολόγηση προέλευσης και επιτρέπει σε έναν εισβολέα να στείλει δεδομένα από έναν υπολογιστή και να κάνει να φαίνεται ότι προέρχονται από έναν άλλο (συνήθως περισσότερο έμπιστο) υπολογιστή. Η δρομολόγηση προέλευσης είναι ένα χρήσιμο εργαλείο για διάγνωση αποτυχιών δικτύου και για επίλυση προβλημάτων δικτύου, αλλά μπορεί να χρησιμοποιηθεί και από εισβολείς. Προς αποφυγή προσπέλασης ενός δικτύου από εισβολείς με την μέθοδο δρομολόγηση προέλευσης πρέπει οι χρήστες να διαμορφώνουν τα firewalls των δικτύων τους έτσι ώστε να απορρίπτουν όλα τα πακέτα TCP/I P με δρομολόγηση προέλευσης που προέρχονται από το Internet.

- Κλοπή Συνόδου (hijack)

Οι εισβολείς μπορούν μερικές φορές να κλέψουν μια ήδη καθορισμένη και πιστοποιημένη σύνδεση δικτύου. Για να κλέψει μια υπάρχουσα σύνδεση TCP, ένας εισβολέας πρέπει να είναι σε θέση να προβλέψει αριθμούς ακολουθίας TCP/IP, τους οποίους χρησιμοποιούν οι δύο επικοινωνούντες υπολογιστές για να κρατούν σε σωστή σειρά πακέτα IP και για να σιγουρεύουν ότι όλα φτάνουν στον προορισμό τους. Αυτό είναι σχετικά εύκολο επειδή οι περισσότερες υλοποιήσεις TCP/IP χρησιμοποιούν γεννήτριες ψευδοτυχαίων αριθμών οι οποίες παράγουν προβλεπτούς αριθμούς ακολουθίας. Ο εισβολέας πρέπει να είναι επίσης σε θέση να ανακατευθύνει τη σύνδεση TCP/IP στον υπολογιστή του εισβολέα και να εκκινήσει μια επίθεση άρνησης παροχής υπηρεσίας εναντίον του υπολογιστή του θύματος έτσι ώστε ο υπολογιστής θύμα να μην δηλώνει στον υπολογιστή διακομιστή ότι κάτι δεν πάει καλά. Το

TCP/IP δεν είναι το μόνο πρωτόκολλο που μπορεί να υποστεί κλοπή συνόδου - τα περισσότερα πρωτόκολλα, περιλαμβανομένου και του ασύρματου πρωτοκόλλου 802.11 b και του πρωτοκόλλου ψηφιακών κινητών τηλεφώνων είναι επίσης πιθανώς ύποπτα για κλοπή συνόδου.

- Επιθέσεις παρακολούθησης (sniffing)

Έτσι ονομάζονται τα προγράμματα που μπορούν να παρακολουθούν (μυρίζουν,sniff) και είναι ικανά να υποκλέπτουν δεδομένα που ταξιδεύουν σε ένα δίκτυο επιπέδου IP πακέτων. Τα προγράμματα αυτά με κατάλληλες τεχνικές έχουν τη δυνατότητα να αναλύουν την συμπεριφορά συστημάτων, να ανακατασκευάζουν τα μηνύματα, να εντοπίζουν πιθανά προβλήματα και να κάνουν αναγνώριση των πρωτοκόλλων που διέπουν τα δίκτυα. Οι sniffer τρέχουν σε τοπικά δίκτυα και κλέβουν κωδικούς πρόσβασης ή παρακολουθούν τις πληκτρολογήσεις από συγκεκριμένους υπολογιστές στόχους. Με την χρήση κατάλληλων μηχανισμών ανασυνθέτουν τα πακέτα που μπορεί να έχουν χρήσιμη πληροφορία χωρίς όμως να επηρεάζουν το περιεχόμενό τους. Τα βήματα μιας επίθεσης τέτοιου τύπου είναι κλιμακωτά. Αρχικά ανιχνεύουν το στόχο και εντοπίζουν παραλείψεις στην ασφάλεια. Στην συνέχεια εισβάλλουν σβήνουν τα ίχνη τους, αποδυναμώνουν την άμυνα του συστήματος και εγκαθιστούν Trojans Horses για την εξάπλωσή τους.

- Επιθέσεις Ενδιαμέσου (man in the middle)

Οι επιθέσεις ενδιαμέσου είναι σπάνιες και δύσκολο να διαπραχθούν, αλλά είναι ιδιαίτερα αποδοτικές όταν δουλέψουν. Σε μια επίθεση ενδιαμέσου, ο εισβολέας λειτουργεί ανάμεσα σε δύο υπολογιστές του δικτύου. Κατά τις επιθέσεις αυτές οι εισβολείς εξαπατούν τους χρήστες – θύματα τα οποία επικοινωνούν μεταξύ τους. Δηλαδή ο επιτιθέμενος παρεμποδίζει την κυκλοφορία της επικοινωνίας μεταξύ των νόμιμων χρηστών και αλλοιώνει τις πληροφορίες που στέλνονται σε κάθε χρήστη χωρίς αυτό να γίνεται αντιληπτό από τους χρήστες. Επειδή με αυτό τον τρόπο δεν γίνεται αντιληπτός από τον αρχικό αποστολέα ή τον παραλήπτη, ένας επιτιθέμενος μπορεί να ξεγελάσει το θύμα, ώστε να του αποκαλύψει εμπιστευτικές πληροφορίες. Ο επιτιθέμενος υποκρίνεται πως είναι ο αρχικός αποστολέας, τον οποίο πιθανώς εμπιστεύεται ο παραλήπτης.

2.4 ΧΕΙΡΙΣΜΟΣ ΤΩΝ ΕΙΣΒΟΛΩΝ

Κατά την διάρκεια μιας εισβολής η πολιτική ασφαλείας του συστήματος παραβιάζεται. Τότε είναι η στιγμή για την εκ νέου συμμόρφωση του συστήματος με την πολιτική ασφάλειας και τη λήψη μέτρων κατά του επιτιθέμενου, όπως αυτά καθορίζονται από την ισχύουσα πολιτική. Η ενέργεια αυτή ονομάζεται **χειρισμός εισβολών (intrusion handling)** και περιλαμβάνει τις παρακάτω έξι φάσεις :

- **Προετοιμασία (preparation)** για μία επίθεση : Αυτή η φάση εμφανίζεται πριν ανιχνευθούν οποιεσδήποτε επιθέσεις. Στα πλαίσια της φάσης αυτής εγκαθίστανται οι διαδικασίες και οι μηχανισμοί για την ανίχνευση και την απόκριση στις επιθέσεις.

- **Ταυτοποίηση (identification)** μιας επίθεσης : Η φάση αυτή διαμορφώνει τις υπόλοιπες φάσεις.

- **Περιορισμός (containment)** της επίθεσης : Η φάση αυτή περιορίζει σε όσο το δυνατό μεγαλύτερο βαθμό τη ζημία στο σύστημα.

- **Εξουδετέρωση (eradication)** της επίθεσης : Από τη φάση αυτή σταματά η επίθεση και παρεμποδίζονται περαιτέρω παρόμοιες επιθέσεις.

- **Αποκατάσταση (recovery)** από την επίθεση : Στη φάση αυτή αποκαθίσταται η ασφαλής κατάσταση στο σύστημα, σύμφωνα με τις επιταγές της ισχύουσας πολιτικής ασφάλειας.

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

ΚΕΦΑΛΑΙΟ 3

ΣΥΣΤΗΜΑΤΑ ΑΝΙΧΝΕΥΣΗΣ ΕΙΣΒΟΛΩΝ (INTRUSION DETECTION SYSTEMS - IDS)

Τα τελευταία χρόνια παρατηρείται αλματώδης ανάπτυξη εφαρμογών και δικτυακών υπηρεσιών των υπολογιστικών συστημάτων.

Παράλληλα όμως με την αύξηση των διαδικτυακών και πληροφοριακών συστημάτων, έχει προκύψει με ταχείς ρυθμούς ανάπτυξης η αύξηση παράνομων εφαρμογών και δραστηριοτήτων που απειλούν και προσβάλλουν την ασφαλή λειτουργία τους.

Συγχρόνως έχει αυξηθεί και το πλήθος των κακόβουλων χρηστών – εισβολέων, οι οποίοι επιχειρούν με όπλο τους ολοένα και πιο έξυπνες, πολύπλοκες και επιζήμιες δικτυακές επιθέσεις.

Εξ αιτίας αυτής της εξέλιξης, τα κλασικά μέτρα ασφάλειας δεν φαίνεται να επαρκούν για την προστασία των συστημάτων και των πληροφοριών που περιέχουν αυτά και συνεχώς γίνεται προσπάθεια για ανάπτυξη νέων μηχανισμών ασφάλειας, που θα παρέχουν την επιθυμητή προστασία από δικτυακές επιθέσεις.

Μία σχετικά νέα και συνεχώς αναπτυσσόμενη μέθοδος προστασίας που ήταν μια εναλλακτική αυτοματοποιημένη προσέγγιση του προβλήματος, έκανε την εμφάνισή της στα μέσα της δεκαετίας του ‘80 και ονομάστηκε Ανίχνευση Επιθέσεων (Intrusion Detection).

Ο όρος **Intrusion Detection** σημαίνει **Ανίχνευση Επιθέσεων** και έχει να κάνει με την παρακολούθηση των γεγονότων που συμβαίνουν σε ένα σύστημα ή δίκτυο και την ανάλυσή τους για σημάδια επιθέσεων. Στόχος της είναι η αποτροπή παραβίασης της εμπιστευτικότητας, ακεραιότητας, διαθεσιμότητας και των μηχανισμών ασφάλειας ενός συστήματος ή ενός δικτύου και ο προσδιορισμός, κατά προτίμηση σε πραγματικό χρόνο, της κακής χρήσης και της κατάχρησης των συστημάτων τόσο από τα ίδια τα εσωτερικά μέλη τους τα οποία χωρίζονται σε αυτούς που ενώ έχουν περιορισμένα δικαιώματα πρόσβασης στο σύστημα, επιχειρούν εφαρμόζοντας απαγορευμένες ενέργειες για διατάραξη της ασφάλειάς τους και σε αυτούς που ναι μεν έχουν το δικαίωμα πρόσβασης αλλά το εκμεταλλεύονται καταχρηστικά, χωρίς την σύμφωνη γνώμη του διαχειριστή ασφαλείας του συστήματος, όσο

και από τους εξωτερικούς χρήστες οι οποίοι προσπαθούν να προσπελάσουν το δίκτυο χωρίς να έχουν δικαίωμα πρόσβασης σε αυτό.

Οι πιο γνωστοί εισβολείς, με υψηλό επίπεδο εμπειρίας, που πέτυχαν να κατασκευάσουν οι ίδιοι τις μεθόδους – εργαλεία τους για να σπάνε τα συστήματα, ήταν οι system experts. Με την πάροδο του χρόνου, οι απαιτούμενες γνώσεις για υλοποίηση των επιθέσεων όλο και μειώνονται. Αυτό οφείλεται στα πολλά και εύχρηστα εργαλεία εισβολής που έχουν εφευρεθεί.

Προκειμένου λοιπόν να διασφαλίζονται τα δίκτυα από επιθέσεις και να ενισχύεται η άμυνά τους στην παράνομη πρόσβαση, χρησιμοποιήθηκαν τα **Συστήματα Ανίχνευσης Εισβολής (Intrusion Detection Systems - IDS)**.

Αυτά είναι εργαλεία με μορφή λογισμικού ή και υλικού τα οποία αυτοματοποιούν τη διαδικασία ελέγχου, ανάλυσης, αναγνώρισης και αντίδρασης σε ύποπτες δραστηριότητες, οι οποίες στοχεύουν σε δικτυακούς και υπολογιστικούς πόρους. Συλλέγουν πληροφορίες από μια πληθώρα δικτυακών πηγών και συστημάτων, στην συνέχεια τις αναλύουν και τις παρουσιάζουν στον διαχειριστή ασφαλείας για να προβεί σε κατάλληλες ενέργειες αντιμετώπισής τους.

Για να αντιμετωπιστούν σωστά οι επιθέσεις πρέπει η ανίχνευσή τους να στηρίζεται σε κάποιο σχέδιο δράσης που θα επιτρέπει στο σύστημα να αντιδρά όταν βρίσκεται υπό επίθεση.

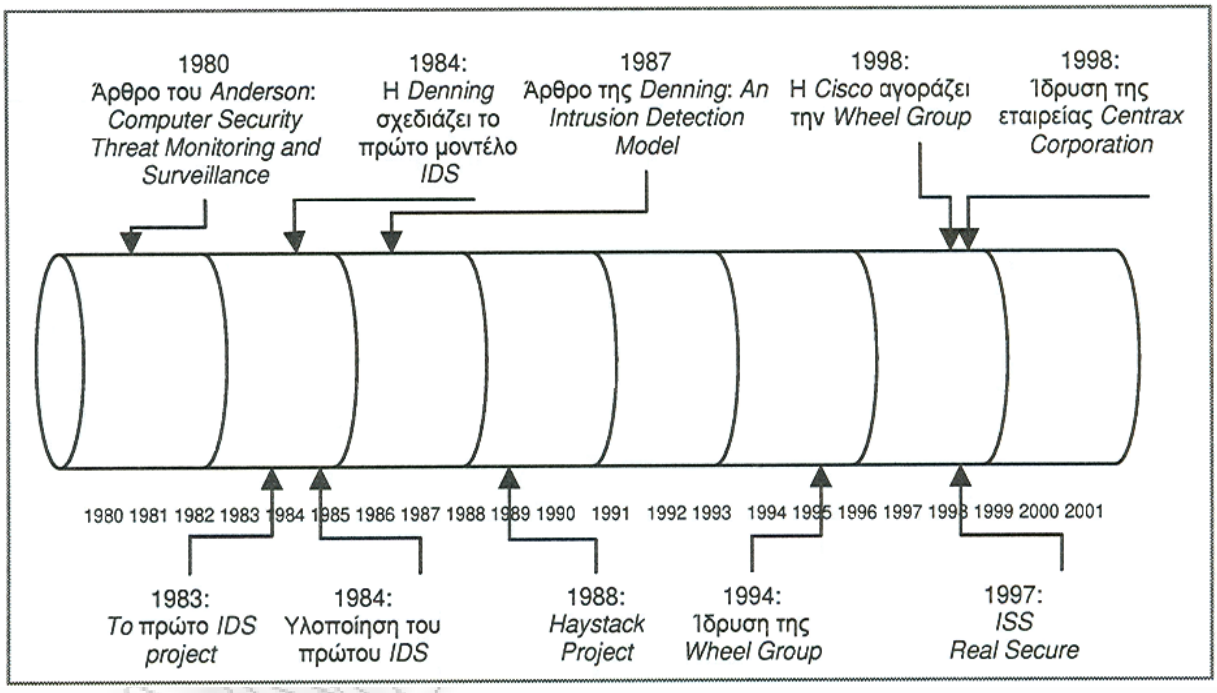
3.1 Η ΕΞΕΛΙΞΗ ΤΩΝ ΣΥΣΤΗΜΑΤΩΝ ΑΝΙΧΝΕΥΣΗΣ ΕΙΣΒΟΛΩΝ (IDS)

Όσο αυξανόταν η χρήση υπολογιστών τόσο μεγάλωνε και ο προβληματισμός των αρμοδίων κατά πόσο τα συστήματα είναι ασφαλή. Ο προβληματισμός αυτός απετέλεσε την αφετηρία για παρακολούθηση και ανάλυση συμβάντων σε δίκτυα υπολογιστών με σκοπό την αναγνώριση προσπαθειών που στοχεύουν στην παραβίαση των μηχανισμών ασφάλειας.

Η ιδέα για την δημιουργία και χρήση ενός συστήματος που θα αποτελούσε μια γραμμή άμυνας και θα συνέβαλε στην προστασία ενός συστήματος ξεκινά στη δεκαετία του '80, με ένα κείμενο του James Anderson, ο οποίος είχε εξαγάγει το συμπέρασμα ότι τα αρχεία καταγραφής (audit files) ενός συστήματος μπορεί να είναι μια πολύ καλή πηγή για το τι έχει συμβεί στο σύστημα, καθώς και για τον τρόπο με τον οποίο ο χρήστης λειτουργεί πάνω του. Έτσι, θα μπορούσαν να ανιχνευτούν πιθανές αλλαγές οι οποίες υποδηλώνουν επίθεση ή και κακή χρήση του συστήματος. Πάνω σ' αυτή την ιδέα άρχισαν σιγά-σιγά να ξεπηδούν τα πρώτα «πρωτόγονα» IDS συστήματα, τα οποία αρχικά ταξινομούσαν και παρουσίαζαν τα

αρχεία καταγραφής στον διαχειριστή με τρόπο τέτοιο ώστε να μπορεί αφενός να καταλάβει το περιεχόμενό τους και αφετέρου να μπορεί να συνθέσει την χρονική ροή των γεγονότων. Ήταν το 1987, όταν η Dorothy Denning πρότεινε ένα σύστημα ανίχνευσης εισβολών, στηρίζοντας την προσπάθειά της πάνω σε ένα αφηρημένο πρότυπο που σκοπό είχε να παρέχει στοιχειώδες αίσθημα ασφάλειας στα υπολογιστικά συστήματα.

Αργότερα, οι σύνθετες ανάγκες για την προστασία του αμερικανικού στρατού, άρχισαν να κάνουν τις δυνατότητες αυτών των συστημάτων περισσότερο σύνθετες και δυναμικές, ενώ περίπου στο 1995 άρχισαν οι πρώτες εμπορικές εκδόσεις των IDS, από ομάδες ανθρώπων που είχαν φύγει από κυβερνητικά έργα και δημιούργησαν εμπορικές εταιρίες. Στο παρακάτω σχήμα 6 μπορούμε να δούμε -εν συντομία- τα πιο σημαντικά γεγονότα στη δημιουργία των IDS :



Σχήμα 6. Εξέλιξη των IDS.

3.2 ΛΟΓΟΙ ΧΡΗΣΗΣ ΣΥΣΤΗΜΑΤΩΝ ΑΝΙΧΝΕΥΣΗΣ ΕΙΣΒΟΛΩΝ

Υπάρχουν διάφοροι λόγοι για τους οποίους είναι απαραίτητη η χρήση των Συστημάτων Ανίχνευσης Εισβολών. Οι σημαντικότεροι από αυτούς είναι :

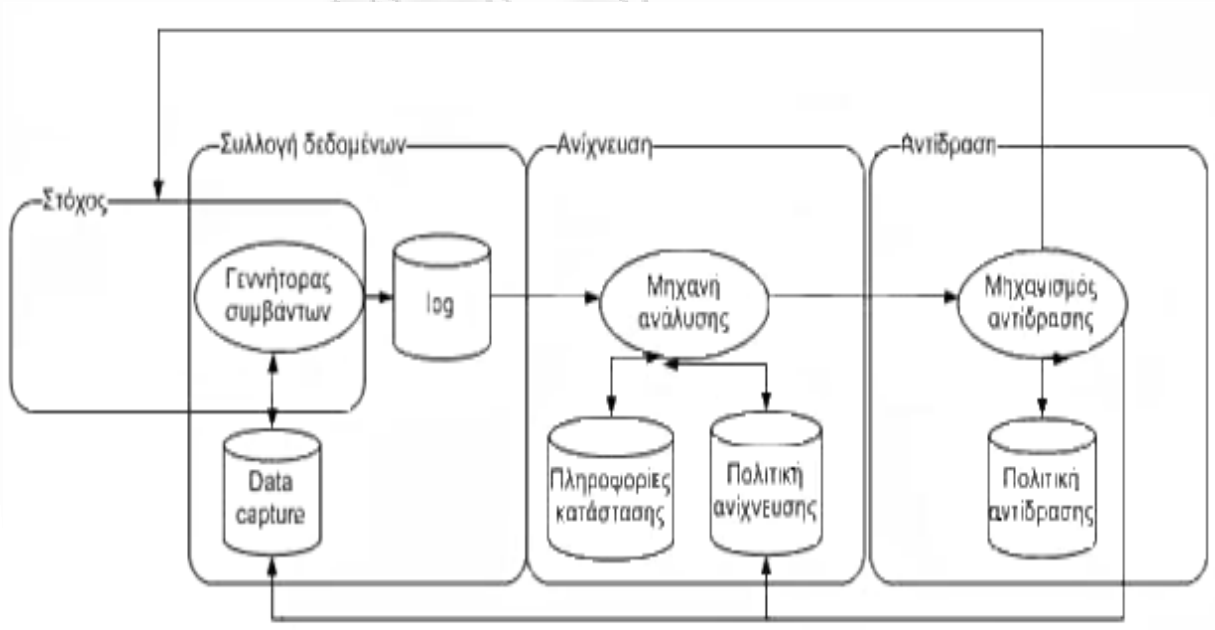
- Για ανίχνευση επιθέσεων και παραβίαση κανόνων ασφαλείας που μπορεί να προκαλέσουν ανεπανόρθωτες ζημιές σε ένα σύστημα και να προσβάλλουν τα συμφέροντα ενός οργανισμού ή μιας επιχείρησης. Στην περίπτωση αυτή πρέπει η ανίχνευση της εισβολής να γίνεται αντιληπτή έγκαιρα, σε πρώιμο στάδιο προς αποτροπή ανεπιθύμητων επιπτώσεων. Άρα η πρόληψη του προβλήματος αποτελεί τη βάση επιτυχών αποτελεσμάτων απόκρουσης μιας επίθεσης και αφορά εσωτερικούς και εξωτερικούς επιτιθέμενους.
- Για ανίχνευση και εντοπισμό ενεργειών που προηγούνται μιας επίθεσης. Εδώ, συνήθως προηγούνται κάποια στάδια, που ακολουθεί ο εισβολέας πριν πραγματοποιήσει μια επίθεση. Αρχικά ο εισβολέας προσπαθεί να ανιχνεύσει την δομή των πληροφοριακών συστημάτων, να συγκεντρώσει πληροφορίες που αφορούν το λογισμικό τους, να εντοπίσει τυχόν αδυναμίες ασφάλειας του συστήματος και την μη έγκαιρη διόρθωση λαθών των χρηστών. Στην συνέχεια, μελετά τις ατέλειες ή τις πληροφορίες που απέκτησε για το δίκτυο – στόχο, προκειμένου να βρει τον πιο αποτελεσματικό τρόπο προσπέλασης τόσο σε χρόνο όσο και σε κόστος. Τέλος χρησιμοποιεί τη γνώση του σαν εργαλείο για να πετύχει το στόχο του.
- Δίχως την ύπαρξη ενός Συστήματος Ανίχνευσης Εισβολής ο επιτιθέμενος είναι πολύ πιθανό να πραγματοποιήσει τις αναγνωριστικές του κινήσεις ανενόχλητος και χωρίς να γίνει αντιληπτός. Το Σύστημα Ανίχνευσης Εισβολής έχει τη δυνατότητα να εντοπίσει τις κινήσεις αυτές του επιτιθέμενου, να τις τεκμηριώσει, να καταγράψει το γεγονός και ή να εμποδίσει τον επιτιθέμενο να τις ολοκληρώσει ή και να ειδοποιήσει τους υπεύθυνους ασφαλείας, οπότε η κατάσταση να τεθεί άμεσα υπό έλεγχο. Εδώ πολύ σημαντικό είναι κάθε πληροφορία που δίνει το Σύστημα Ανίχνευσης, να είναι καθαρή, σύντομη και σαφής, ώστε οι διαχειριστές ασφαλείας να επεμβαίνουν πριν προλάβουν οι εισβολείς και εκμεταλλευτούν τις ατέλειες του συστήματος. Η καταγραφή μιας παραβίασης από το Σύστημα Ανίχνευσης βοηθά στην εκτίμηση της τυχόν προκληθείσας ζημιάς και παρέχει τεκμήρια σε περίπτωση δικαστικής διένεξης.
- Υπάρχουν περιπτώσεις όπου η λειτουργία παλαιών πληροφοριακών συστημάτων με επισφαλή προσφορά υπηρεσιών για λόγους οικονομίας ή εύκολης χρήσης είναι απαραίτητη. Εδώ τα συστήματα αυτά δεν υποστηρίζονται με μέτρα ασφαλείας από τους κατασκευαστές τους. Άλλες φορές πάλι, τα πληροφοριακά συστήματα υποστηρίζονται μεν από τους κατασκευαστές τους, αλλά χρειάζονται και περαιτέρω υποστήριξη για λόγους όπως μειωμένη ή ελαττωματική ασφάλεια λογισμικού. Έτσι

με την υποστήριξη αυτών των συστημάτων αποτρέπονται οι επίδοξοι επιτιθέμενοι να συνεχίσουν την προσπάθειά τους, επειδή φοβούνται ότι θα εντοπιστούν και θα τιμωρηθούν.

- Για την συγκέντρωση πληροφοριών οι οποίες θα βοηθήσουν στην αποκατάσταση των συστημάτων που παραβιάστηκαν και στη διόρθωση αδυναμιών και παραλήψεων, οι οποίες οφείλονται πολλές φορές στους ίδιους τους διαχειριστές ασφαλείας ή και τους χρήστες ενός συστήματος λόγω ελλιπούς εκπαίδευσης και γνώσης. Έτσι το Σύστημα Ανίχνευσης βοηθά στην βελτίωση των ενεργειών των διαχειριστών ασφαλείας ώστε να εφαρμόζουν την σωστή πολιτική ασφαλείας.

3.3 ΓΕΝΙΚΟ ΜΟΝΤΕΛΟ ΕΝΟΣ ΣΥΣΤΗΜΑΤΟΣ ΑΝΙΧΝΕΥΣΗΣ ΕΠΙΘΕΣΕΩΝ

Το πρώτο μοντέλο για ανίχνευση επιθέσεων υλοποιήθηκε από την Dorothy Denning στο εργαστήριο του Stanford (SRI International). Ένα γενικό μοντέλο ενός IDS μπορεί να καθοριστεί σαν μια ομάδα από διάφορα αλληλοεξαρτώμενα μέρη. Τα μέρη αυτά απαρτίζουν ένα αρχιτεκτονικό πλαίσιο, το οποίο καθορίζεται από τις παρακάτω παραμέτρους και απεικονίζεται στο παρακάτω σχήμα 7.



Σχήμα 7. Γενικό Μοντέλο IDS.

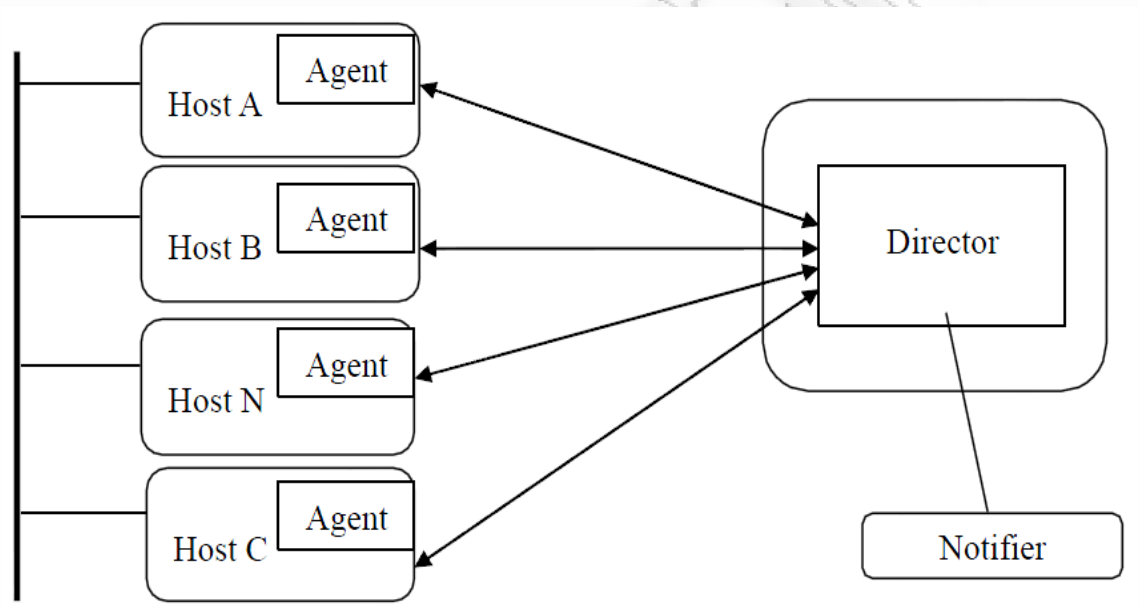
Συλλογή δεδομένων από κατάλληλους αισθητήρες (Data Collection Unit). Στο υποσύστημα συλλογής δεδομένων γίνεται η συλλογή των πληροφοριών που αφορά συγκεκριμένα γεγονότα, όπως είναι τα δεδομένα που κινούνται στο δίκτυο (data capture), τα αρχεία καταγραφής (log files) του λειτουργικού συστήματος και τα logs αρχεία των εφαρμογών. Στην συνέχεια, μέσω του γεννήτορα συμβάντων, γίνεται η προώθηση αυτών των πληροφοριών στα υπόλοιπα μέρη και συγκεκριμένα στο υποσύστημα ανάλυσης, αφού γίνει το σχετικό φιλτράρισμα από περιττά στοιχεία, μειώνοντας έτσι τον όγκο τους.

Υποσύστημα Ανίχνευσης (Analysis Engine). Στο υποσύστημα αυτό, μέσω της μηχανής ανάλυσης (Analysis Engine), γίνεται πιο διεξοδική η ανάλυση των στοιχείων που παρέχονται από την προηγούμενη λειτουργία της συλλογής (χωρίς περιττά στοιχεία πλέον), καθώς και η εξαγωγή συμπερασμάτων για την απόπειρα ή πραγματοποίηση μιας επίθεσης. Αυτή η εξαγωγή γίνεται με την υλοποίηση του αλγόριθμου ανίχνευσης. Η πολιτική ανίχνευσης είναι ένα σύνολο κανόνων, που έχει στη διάθεσή του το Intrusion Detection System έτσι ώστε να ανιχνεύει επιθέσεις. Υπάρχουν διάφορες τεχνικές ανίχνευσης. Μια από αυτές είναι η αναζήτηση στα δεδομένα, κάποιας γνωστής υπογραφής (signature) επίθεσης, ώστε να ταυτοποιηθεί αυτή η επίθεση. Στη περίπτωση αυτή θα πρέπει το IDS να είναι ενημερωμένο με υπογραφές ήδη γνωστών επιθέσεων. Μια άλλη τεχνική για ταυτοποίηση επίθεσης, αφορά τη μη συνηθισμένη χρήση ή δραστηριότητα του συστήματος, την οποία το IDS κρίνει ως παραβίαση του προφίλ χρήσης του. Η μηχανή ανάλυσης μπορεί να συνδυάζει περισσότερες από μια τεχνικές για μεγαλύτερη αποτελεσματικότητα. Τέλος στο υποσύστημα αυτό, το IDS κρατά «πληροφορίες κατάστασης», όπως είναι πληροφορίες για επίθεση που δεν έχει ολοκληρωθεί ή η τρέχουσα κατάσταση του συστήματος, ώστε να μπορούν αργότερα να χρησιμοποιηθούν από τους διαχειριστές ασφαλείας για περαιτέρω ανάλυση.

Υποσύστημα Αντίδρασης (Response Unit). Στο υποσύστημα αυτό αποστέλλονται όλες οι πληροφορίες από τη μηχανή ανάλυσης. Έτσι καθορίζεται η πολιτική αντίδρασης του IDS. Η πολιτική αντίδρασης χαρακτηρίζεται παθητική στην περίπτωση που ενημερώνει τους διαχειριστές για την παραβίαση του συστήματος, προκειμένου να προβούν εκείνοι στις κατάλληλες ενέργειες ή ενεργός στην περίπτωση που το ίδιο το σύστημα δρα δυναμικά με το κλείσιμο συνδέσεων ή ports, ώστε να προστατευτεί το δίκτυο και τα συστήματα από περαιτέρω επιθέσεις, μέχρι να γίνει ανάλυση των γεγονότων.

3.4 ΓΕΝΙΚΗ ΑΡΧΙΤΕΚΤΟΝΙΚΗ ΕΝΟΣ IDS

Κάθε Σύστημα Ανίχνευσης Εισβολών αποτελεί έναν αυτοματοποιημένο μηχανισμό παρακολούθησης και ελέγχου. Ο μηχανισμός αυτός, όπως απεικονίζεται στο παρακάτω σχήμα 8, αποτελείται από τρία μέρη : **Αντιπρόσωπος (Agent)**, **Διευθυντής (Director)**, **Αγγελιοφόρος (Notifier)**.



Σχήμα 8. Αρχιτεκτονική ενός IDS.

- Αντιπρόσωπος (Agent)

Στόχος του Αντιπροσώπου είναι να αποκτά πληροφορίες οι οποίες συνήθως επεξεργάζονται, μορφοποιούνται και μεταδίδονται στον Διευθυντή. Επίσης μεταδίδει τον χρόνο και τον τόπο μιας αποτυχημένης εισαγωγής. Ο Αντιπρόσωπος μπορεί και να απορρίψει κάποιες πληροφορίες τις οποίες θεωρεί άχρηστες. Πηγή προέλευσης των πληροφοριών μπορεί να είναι ένα αρχείο καταγραφής (log file), ένα δίκτυο υπολογιστών ή κάποια άλλη διεργασία.

- Διευθυντής (Director)

Στόχος του Διευθυντή είναι να αναλύει τα συγκεντρωθέντα δεδομένα και να αποφασίζει αν θα αυξήσει ή θα ελαττώσει την επεξεργασία αυτών των δεδομένων στην περίπτωση που υποψιάζεται ότι κάποια επίθεση βρίσκεται σε εξέλιξη. Δίνει οδηγίες στον αντιπρόσωπο είτε για να συλλέξει περισσότερες πληροφορίες είτε για να τις επεξεργαστεί με διαφορετικό τρόπο. Επειδή ο ρόλος του Διευθυντή είναι κρίσιμος για την αποτελεσματικότητα του Συστήματος Ανίχνευσης Εισβολών χρησιμοποιεί περισσότερες από μία τεχνικές ανάλυσης και συσχετίζει πληροφορίες από πολλαπλά αρχεία (multiple logs), με σκοπό το καθορισμό του τρόπου συμπεριφοράς του συστήματος.

- Αγγελιοφόρος (Notifier)

Αυτός λαμβάνει την πληροφορία από τον Διευθυντή και αποφασίζει για τον χρόνο και τον τρόπο που θα ενεργήσει. Άλλοτε απαντά αυτόνομα στις επιθέσεις και άλλοτε απλά ειδοποιεί τον υπεύθυνο ασφαλείας του συστήματος.

3.5 ALERTS - ΤΥΠΟΙ ΣΥΝΑΓΕΡΜΩΝ ΕΝΟΣ IDS

Σκοπός των Συστημάτων Ανίχνευσης Εισβολών είναι η ανίχνευση επιθέσεων μέσα από τη συλλογή και ανάλυση διαφόρων δεδομένων. Η διαδικασία της συλλογής δεδομένων γίνεται μέσω αισθητήρων (sensors), οι οποίοι παρατηρούν συνεχώς την δικτυακή κίνηση. Κάθε επισήμανση για την ανίχνευση μιας επίθεσης από τους αισθητήρες που προωθείται για περαιτέρω ανάλυση ονομάζεται Alert. Οι αισθητήρες παράγουν πολλά Alert όμως κάποια από αυτά δεν είναι έγκυρα αλλά έχουν δημιουργηθεί από νόμιμες ενέργειες που πραγματοποιούνται στο δίκτυο. Αυτό συμβαίνει διότι όσο το ποσοστό της νόμιμης δικτυακής κίνησης αυξάνει, ο έλεγχος της κυκλοφορίας και ο διαχωρισμός των απειλών από τη φυσιολογική δραστηριότητα γίνεται όλο και πιο δύσκολος. Έτσι πολλές από τις επισημάνσεις Alert μπορεί να είναι ένας ψευδής συναγερμός. Οι τύποι αυτοί των λανθασμένων συναγερμών είναι δύο :

- False Positives είναι οι λανθασμένες επισημάνσεις που παράγει ένα IDS όταν ανιχνεύσει κάποιο γεγονός σαν περίπτωση πιθανής επίθεσης ενώ δεν είναι. Συνήθως προκύπτουν από

κακή ρύθμιση του IDS ή από περιπτώσεις γεγονότων που δεν μπορούν να διαχωριστούν σαφώς από μία επίθεση.

- False Negatives είναι οι περιπτώσεις επιθέσεων τις οποίες το IDS δεν κατάφερε μετά από την εξέτασή τους να τις επισημάνει. Συνήθως προκύπτουν από κακή ρύθμιση του IDS ή από την εμφάνιση μιας νέας επίθεσης για την οποία δεν υπάρχει προηγούμενη γνώση.

Το ποσοστό των False Positives και False Negatives μαζί καθορίζουν την ευαισθησία του συστήματος. Στόχος του IDS θα πρέπει να είναι η διάκριση της μη φυσιολογικής συμπεριφοράς από την φυσιολογική συμπεριφορά του συστήματος.

Οι διαχειριστές ασφάλειας έχουν την δυνατότητα να καθορίζουν το βαθμό τις ευαισθησίας του συστήματος ανάλογα με τις ρυθμίσεις που πραγματοποιούν στο IDS και συνεχώς θα πρέπει να γίνονται προσπάθειες οι οποίες θα βελτιώσουν το IDS κυρίως στον τομέα των συμπτωμάτων των ψευδών συναγερμών.

3.6 ΕΠΙΘΥΜΗΤΑ ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ ΕΝΟΣ ΣΥΣΤΗΜΑΤΟΣ ΑΝΙΧΝΕΥΣΗΣ ΕΠΙΘΕΣΕΩΝ (IDS)

Τα χαρακτηριστικά του ιδανικού Συστήματος Ανίχνευσης Επιθέσεων είναι τα παρακάτω :

- Πρέπει να τρέχει συνεχώς με ελάχιστη ανθρώπινη παρακολούθηση.
- Πρέπει να μπορεί, αφού αντιμετωπίσει πιθανά σφάλματα που προέρχονται από λάθος ή από σκοπιμότητα, να επανέλθει ακριβώς στην προηγούμενη κατάστασή του, σαν να μην είχε συμβεί τίποτε.
- Πρέπει να είναι σχεδόν αδύνατο να τροποποιήσει ή να αχρηστεύσει κάποιος το Σύστημα Ανίχνευσης Επιθέσεων και να μπορεί να ελέγχει τον εαυτό του αν πραγματικά δέχεται επίθεση.
- Πρέπει να επηρεάζει ελάχιστα την απόδοση των υπολογιστών στους οποίους τρέχει, ώστε να μην παρεμποδίζει την κανονική τους λειτουργία.
- Πρέπει να είναι διαμορφώσιμο ώστε να προσαρμόζεται με ακρίβεια στο δίκτυο και στο υπολογιστικό σύστημα που παρακολουθεί.
- Πρέπει να είναι ανεξάρτητο του λειτουργικού συστήματος, ώστε να ανιχνεύει επιθέσεις σε οποιοδήποτε λειτουργικό σύστημα.

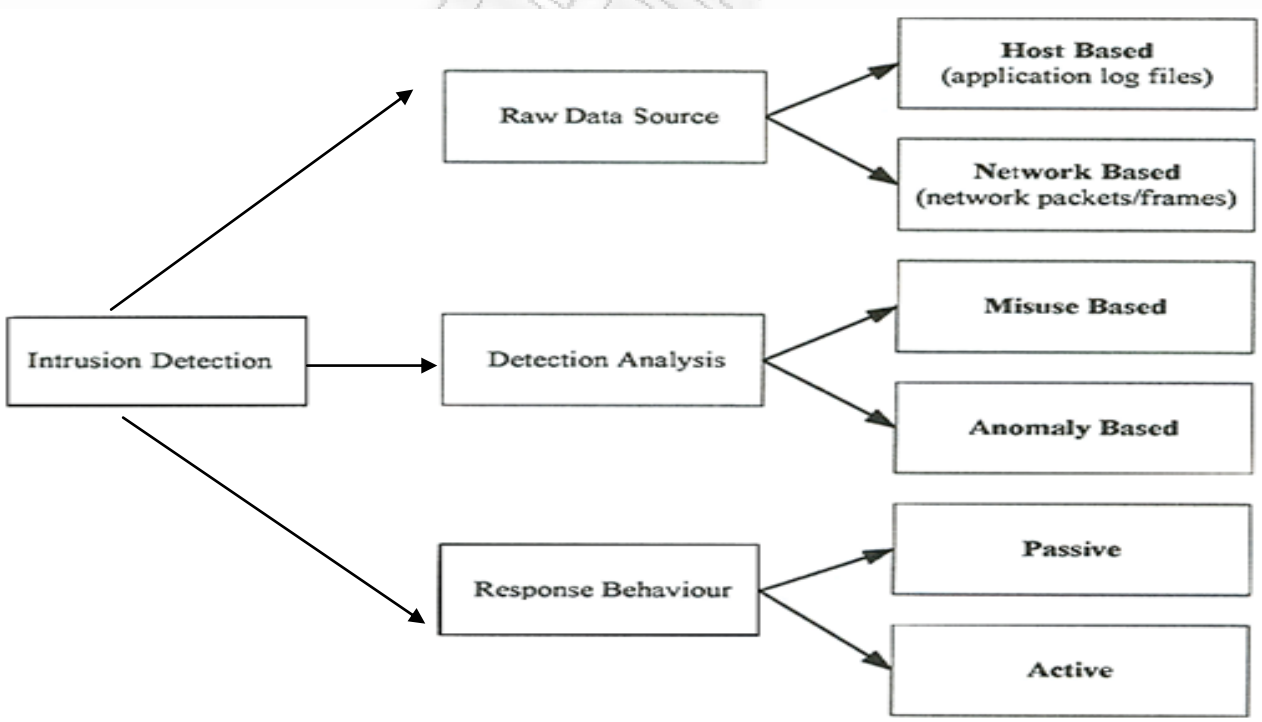
- Πρέπει να μπορεί να προσαρμοστεί σε αλλαγές στο δίκτυο και στο υπολογιστικό σύστημα που παρακολουθεί.
- Πρέπει να μπορεί να ανιχνεύσει επιθέσεις και δεν πρέπει να χαρακτηρίζει, σαν επίθεση, περιπτώσεις καλής λειτουργίας του δικτύου (false positive).
- Πρέπει να ανιχνεύει και να αναφέρει τις επιθέσεις όσο πιο γρήγορα γίνεται και να είναι αρκετά γενικό ώστε να ανιχνεύει πολλούς διαφορετικούς τύπους επιθέσεων, ακόμα και άγνωστους.

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

ΚΕΦΑΛΑΙΟ 4

ΤΑΞΙΝΟΜΗΣΗ ΚΑΙ ΕΙΔΗ ΣΥΣΤΗΜΑΤΩΝ ΑΝΙΧΝΕΥΣΗΣ ΕΙΣΒΟΛΩΝ

Η Ανίχνευση Εισβολών περιλαμβάνει την συλλογή δεδομένων και την ανάλυσή τους προκειμένου να καθορίσει αν το σύστημα είναι υπό απειλή. Τα στάδια της ανίχνευσης εισβολών σχηματίζουν τις κατηγορίες των Συστημάτων Ανίχνευσης Εισβολών. Οι κατηγορίες εξαρτώνται από τον τρόπο που το κάθε ένα σύστημα ανίχνευσης εισβολών υλοποιεί την διαδικασία της παρακολούθησης και της ανάλυσης των δεδομένων με στόχο την ανίχνευση εισβολής. Τα IDS συντίθεται από διάφορα λειτουργικά μέρη, τα οποία εκτελούν συγκεκριμένες λειτουργίες.



Σχήμα 9. Κατηγορίες Συστημάτων IDS.

Κάθε μέρος περιγράφεται και κατηγοριοποιείται από διαφορετικές προσεγγίσεις. Αυτές βασίζονται στον χαρακτήρα, τον σκοπό, την λειτουργία και την μέθοδο εργασίας τους. Το παραπάνω σχήμα 9 παρουσιάζει τις κυριότερες κατηγορίες συστημάτων IDS. Τα περισσότερα IDS επιτελούν τρείς θεμελιώδεις λειτουργίες οι οποίες σχετίζονται με την **Πηγή Πληροφοριών (Information Sources)**, την **Ανάλυση (Analysis)** και την **Απόκριση (Response).** Ανάλογα με το πώς το κάθε ένα IDS υλοποιεί αυτές τις λειτουργίες προκύπτουν και οι κατηγορίες των IDS. Με τον τρόπο αυτό θα ταξινομήσουμε και εμείς τα Συστήματα Ανίχνευσης Εισβολών στην συνέχεια του κεφαλαίου μας.

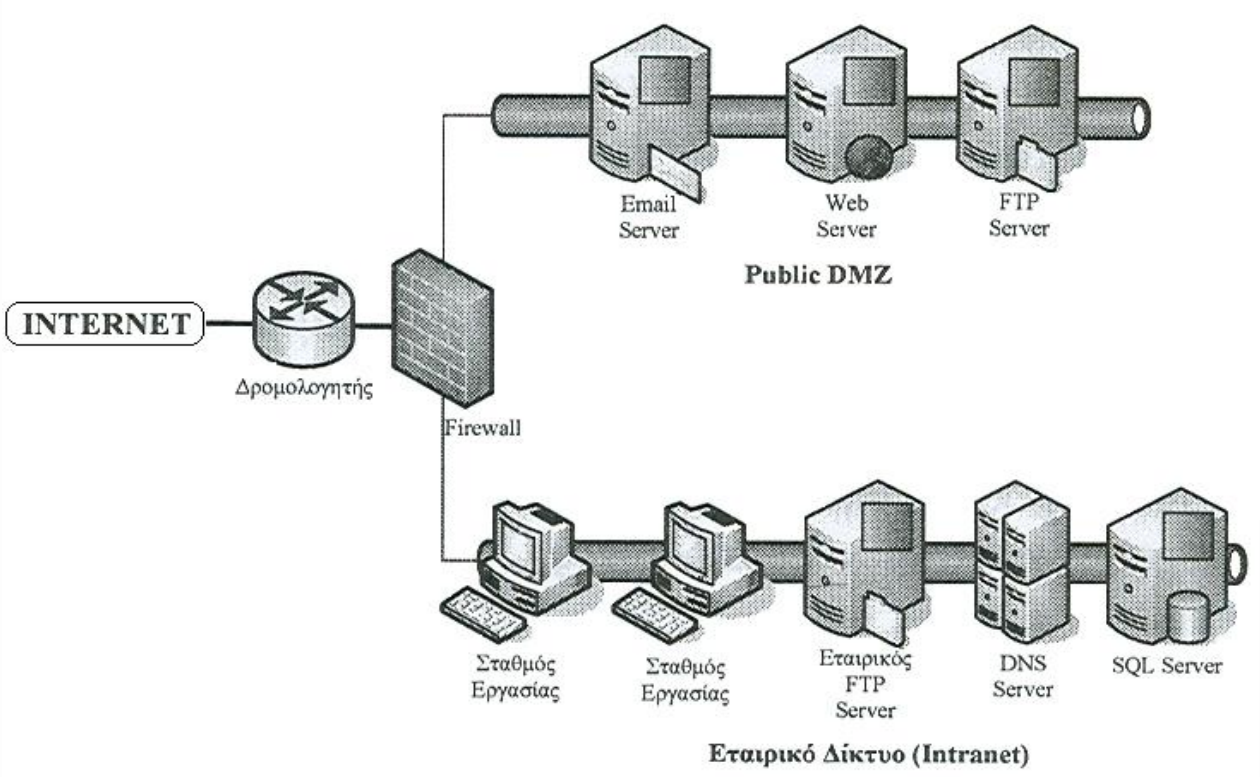
4.1 ΚΑΤΗΓΟΡΟΙΟΠΟΙΗΣΗ ΜΕ ΒΑΣΗ ΤΙΣ ΠΗΓΕΣ ΠΛΗΡΟΦΟΡΙΑΣ

Πηγές Πληροφορίας είναι αυτές που χρησιμοποιεί ένα Σύστημα Ανίχνευσης Εισβολών με σκοπό να συλλέξει την κατάλληλη πληροφορία, την οποία θα αναλύσει προκειμένου να καθορίσει αν έχει πραγματοποιηθεί μία επίθεση. Αυτές οι πληροφορίες μπορεί να προέρχονται από αρχεία καταγραφής του συστήματος, από τα δικτυακά πακέτα που ανήκουν στο traffic ενός δικτύου, το οποίο μπορεί να είναι ένα δίκτυο κορμού (Backbone) ή ένα τμήμα (segment) ενός τοπικού δικτύου (LAN). Επίσης μπορεί να προέρχονται από αρχεία καταγραφής εφαρμογών, από δικτυακή κίνηση σε ασύρματο δίκτυο ή από αισθητήρες κατανεμημένους σε κάποιο δίκτυο. Κάποια άλλα Συστήματα Ανίχνευσης Εισβολών παρακολουθούν και αναλύουν πληροφορίες που εξάγονται από το Λειτουργικό Σύστημα (Λ.Σ) ή από τις εφαρμογές ενός συστήματος. Έτσι οι πιο συνήθεις πηγές πληροφορίας μπορεί να είναι σε επίπεδο παρακολούθησης συστήματος (Host) και δικτύου (Network) δημιουργώντας τις αντίστοιχες κατηγορίες των IDSs με τα δικά τους πλεονεκτήματα και μειονεκτήματα η κάθε μία.

4.1.1 IDS Μεμονωμένου Συστήματος
Host – based Intrusion Detection Systems

Η κατηγορία Μεμονωμένου Συστήματος (Host – based Intrusion Detection Systems, HIDS) ελέγχει τη δραστηριότητα του χρήστη ή των process για ‘ ‘υπογραφές επιθέσεων’’. Τα HIDS ψάχνουν για ίχνη εισβολής, ασυνήθιστες δραστηριότητες, που περιορίζονται στο τοπικό

σύστημα Host όπως απεικονίζεται στο παρακάτω σχήμα 10. Στην συγκεκριμένη αρχιτεκτονική χρησιμοποιείται ο μηχανισμός ελέγχου και καταγραφής του Host σαν πηγή πληροφοριών για ανάλυση των δραστηριοτήτων.



Σχήμα 10. Τοποθέτηση HIDS.

Ελέγχει τα κρίσιμα αρχεία του λειτουργικού συστήματος (system files), ερευνώντας για παράξενη πρόσβαση στα αρχεία. Επίσης ελέγχει τα γεγονότα συστήματος (system events) και τα αρχεία ελέγχου και καταγραφής ασφαλείας (audit log files) ψάχνοντας για μη εγκεκριμένη αύξηση δικαιωμάτων ή μετατροπές δικαιωμάτων του συστήματος. Τα αρχεία του λειτουργικού συστήματος ελέγχονται με τη χρήση ‘‘ετικετών αθροισμάτων’’ (checksum tags), οι οποίες επισυνάπτονται στα αρχεία αυτά από το IDS όταν γίνεται η αρχική του εγκατάσταση και ελέγχονται σε τακτά χρονικά διαστήματα για περίεργες και μη προγραμματισμένες αλλαγές. Το IDS χρησιμοποιεί δυναμικές μαθηματικές εκφράσεις για να καθορίσει τις ‘‘ετικέτες’’. Επιπλέον, ορισμένα προϊόντα ερευνούν τις ‘‘πόρτες’’ (ports) του συστήματος και ενημερώνουν τον διαχειριστή ασφαλείας του συστήματος όταν ζητείται πρόσβαση σε κάποιες (συγκεκριμένες) από αυτές. Η εγκατάσταση ενός HIDS είναι δυνατόν

να μη πραγματοποιηθεί πάνω στο παρακολουθούμενο σύστημα αλλά να εγκατασταθεί σε ένα άλλο και να προσπελαύνει τις πληροφορίες από εκεί μέσω του πρωτοκόλλου SNMP. Έτσι κάποια HIDS προσφέρουν την δυνατότητα χρήσης μιας κοινής κονσόλας διαχείρισης και ελέγχου πολλών συστημάτων με αποτέλεσμα την ευκολότερη χρήση τους.

4.1.1.1 Πλεονεκτήματα και Μειονεκτήματα των HIDS

Τα hostbased συστήματα ανίχνευσης εισβολών χαρακτηρίζονται από ορισμένα πλεονεκτήματα τα οποία τα καθιστούν αρκετά αποτελεσματικά στην λειτουργία τους. Θα μπορούσαμε να συνοψίσουμε τα πλεονεκτήματά τους ως εξής :

- Επειδή λειτουργούν τοπικά σε ένα σύστημα host που προστατεύουν έχουν την δυνατότητα να ανιχνεύουν επιθέσεις που δεν ανιχνεύονται από τα NIDS.
- Μπορούν να επαληθεύσουν την επιτυχία ή την αποτυχία μιας επίθεσης με τον έλεγχο των αρχείων ελέγχου και καταγραφής (logfiles).
- Ελέγχουν τις κύριες δραστηριότητες στην χρήση του συστήματος, όπως την πρόσβαση σε συγκεκριμένα αρχεία (critical files), την δραστηριότητα logon-logoff των χρηστών, πιθανές αλλαγές στους λογαριασμούς των χρηστών και αλλαγές στις πολιτικές του συστήματος.
- Είναι ευκολότερο να σχηματιστεί μια ενεργή αντίδραση σε περίπτωση επίθεσης, όπως ο τερματισμός μιας υπηρεσίας ή το logging off ενός επιτιθέμενου χρήστη.
- Προσφέρουν ανίχνευση και αντίδραση σε επιθέσεις σε (σχεδόν) πραγματικό χρόνο, ενώ δεν απαιτούν την χρήση ειδικευμένου υλικού (hardware), μια και η μορφή τους είναι μόνο λογισμική (software), ενώ ενσωματώνονται χωρίς επιπλέον έξοδα στην υπάρχουσα υποδομή του δικτύου.
- Μπορούν να χρησιμοποιηθούν σε κρυπτογραφημένα ή και switched περιβάλλοντα δικτύου, καθώς τα δεδομένα αποκρυπτογραφούνται μόλις εισάγονται στο σύστημα, ενώ η αποτελεσματικότητά τους δεν περιορίζεται από σύνθετες αρχιτεκτονικές δικτύων Π.χ. Network partitioning, Virtual LANs, switched environment, internαl firewalling κλπ.
- Μπορούν να ανιχνεύσουν επιθέσεις οι οποίες μπορεί να ξεφύγουν από τα IDS δικτύου, όπως τοπικές επιθέσεις (locαl ή keyboard attacks), μετατροπές σε αρχεία συστήματος

(π.χ. μέσω ενός Trojan Horse), προσπάθειες απόκτησης πρόσβασης στο σύστημα με την τεχνική brute force κλπ.

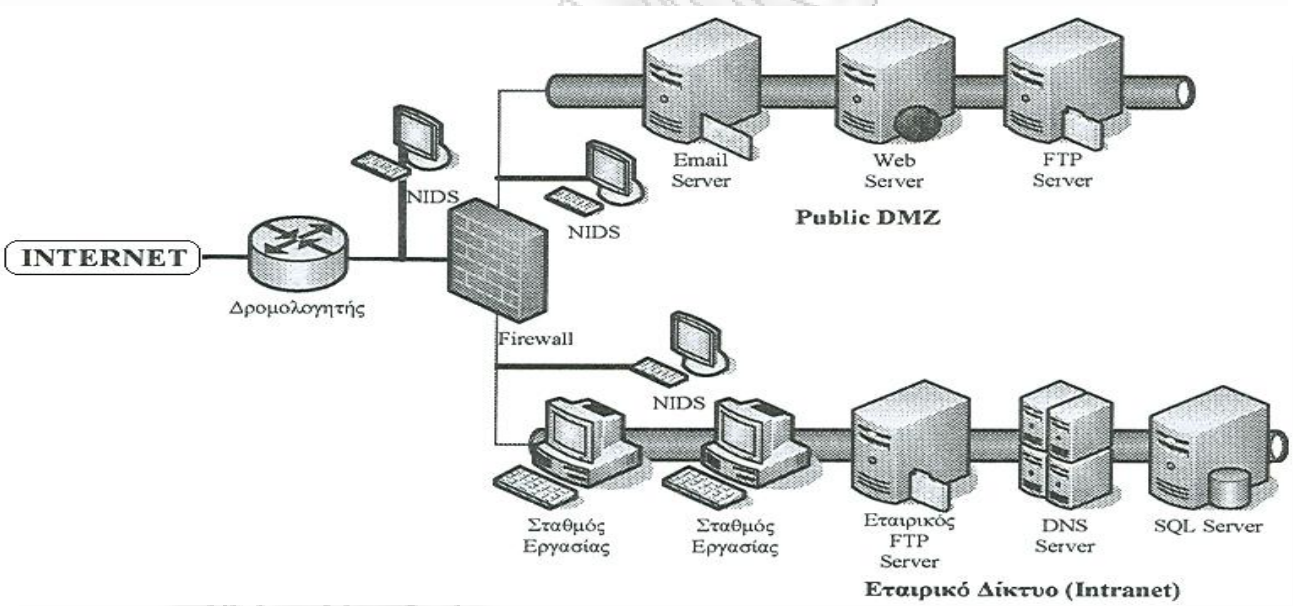
- Έχουν μικρότερους false positive ρυθμούς από ότι τα network. Αυτό συμβαίνει γιατί το εύρος των εντολών που εκτελούνται σε ένα συγκεκριμένο host είναι πολύ πιο εστιασμένο, παρά τα είδη της κίνησης πακέτων που ρέουν σε ένα δίκτυο. Αυτή η ιδιότητα μπορεί να μειώσει την πολυπλοκότητα των host-based μηχανισμών.

Τα HIDS εκτός από τα παραπάνω πλεονεκτήματα παρουσιάζουν και κάποιες αδυναμίες στο τρόπο ανίχνευσης εισβολών. Λόγω αυτών των αδυναμιών παρουσιάζουν μειονεκτήματα τα οποία αναφέρονται παρακάτω :

- Τα HIDS είναι δυσκολότερο να τα διαχειριστούμε μαζικά (mass administration), επειδή πρέπει να διαμορφώνονται και να ρυθμίζονται ξεχωριστά για κάθε σύστημα στο οποίο εγκαθίστανται για πρώτη φορά, κάτι που δημιουργεί πρόβλημα στο προσωπικό που τα διαχειρίζεται και γενικότερα στη διαχείρισή τους, ειδικά σε μεγάλα και κατανεμημένα περιβάλλοντα.
- Τα HIDS απαιτούν εγκατάσταση στην συγκεκριμένη συσκευή που θέλουμε να προστατεύσουμε. Αν έχουμε ένα server που πρέπει να τον προστατέψουμε θα πρέπει να εγκατασταθεί το σύστημα ανίχνευσης στον server αυτόν με ενδεχόμενα προβλήματα χωρητικότητας.
- 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.
- Τα HIDS είναι επιρρεπή σε κάποιες Denial of Service (DoS) επιθέσεις, οι οποίες μπορεί να προκαλέσουν την διακοπή της λειτουργίας τους.
- Τα HIDS χρησιμοποιούν τους πόρους του συστήματος στο οποίο είναι εγκατεστημένα, γεγονός το οποίο προσδίδει ένα επιπλέον κόστος στην απόδοση του συστήματος, ειδικότερα αν χρησιμοποιείται μια ‘‘σφιχτή’’ πολιτική.

4.1.2 IDS Δικτυακού Συστήματος
Network–based Intrusion Detection Systems

Η κατηγορία Δικτυακού Συστήματος (Network – based Intrusion Detection Systems, NIDS) είναι η πιο συνηθισμένη και ελέγχει τη δικτυακή δραστηριότητα. Τα NIDS παρακολουθούν και αναλύουν, σε πραγματικό χρόνο, κάθε πακέτο που κυκλοφορεί στο traffic ενός δικτύου. Αυτή η τεχνική παρέχει πληροφορίες διαφορετικής μορφής σε σχέση με αυτές που παρέχει ο έλεγχος που βασίζεται στον υπολογιστή (host–based monitoring). Τα πακέτα αυτά είναι η κύρια πηγή πληροφοριών τους. Αποτελούνται από δύο λογικά τμήματα : το σταθμό παρακολούθησης δικτύου (IDS sensor) και τον σταθμό διαχείρισης – ανάλυσης όπως απεικονίζεται και στο παρακάτω σχήμα 11. Ο σταθμός παρακολούθησης είναι συνδεδεμένος με το δίκτυο, ο αισθητήρας δηλαδή βρίσκεται σε έναν τομέα του δικτύου και παρακολουθεί για ύποπτη κίνηση.



Σχήμα 11. Τοποθέτηση NIDS.

Οι αισθητήρες (Sensors) παρακολουθούν την δικτυακή κίνηση (traffic), αναλύουν τοπικά τα πακέτα σε πραγματικό χρόνο και καταγράφουν τα αποτελέσματά τους τοπικά ή και απομακρυσμένα σε ένα κεντρικό σύστημα. Επίσης οι αισθητήρες έχουν την δυνατότητα να κάνουν κρυφή την παρουσία τους (Stealth Mode), έτσι ώστε να μην είναι δυνατό για τον επιτιθέμενο να αντιληφθεί την θέση τους ή και την ύπαρξή τους. Στην περίπτωση που ο σταθμός παρακολούθησης διαπιστώνει ύποπτη δραστηριότητα, ενημερώνει το σταθμό

διαχείρισης. Αυτό που πραγματικά συμβαίνει, είναι η χρήση μίας κάρτας δικτύου η οποία λειτουργεί σε κατάσταση ‘‘promiscuous mode’’. Συνήθως μια κάρτα Ethernet διαβάζει όλες τις πληροφορίες που διακινούνται σε ένα δίκτυο και δέχεται πακέτα που προορίζονται αποκλειστικά για εκείνη. Αν μια τέτοια κάρτα τεθεί σε promiscuous mode δέχεται όλες τις πληροφορίες (sniffer) ανεξάρτητα του προορισμού τους με σκοπό την ανάλυσή τους. Αν κατά την ανάλυση της δραστηριότητας του δικτύου ανιχνεύσει ότι υπάρχει ‘‘υπογραφή’’ κάποιας επίθεσης, τότε ενημερώνει και μεταβιβάζει το ύποπτο συμβάν στο σταθμό διαχείρισης. Ο σταθμός διαχείρισης – ανάλυσης έχει την δυνατότητα, να εμφανίσει στην οθόνη του διαχειριστή, τα σήματα κινδύνου που έλαβε από τους αισθητήρες με κάποιο alarm ή να πραγματοποιήσει επιπλέον ανάλυση. Ο σταθμός διαχείρισης μπορεί να διαθέτει λογισμικό Network Management ή δικό του GUI (Γραφικό Περιβάλλον Χρήστη, Graphical User Interface) ώστε να βοηθήσει το διαχειριστή να αναλύσει καλύτερα μια επίθεση.

4.1.2.1 Πλεονεκτήματα και Μειονεκτήματα των NIDS

Ιδιαίτερη απήχηση παρουσιάζουν τα NIDS επειδή χαρακτηρίζονται από ορισμένα προτερήματα, τα οποία τα καθιστούν πολύ αποτελεσματικά στην λειτουργία τους. Λόγω του τρόπου λειτουργίας τους είναι δυνατόν να μην εγκαταστήσουμε πρωτόκολλο επικοινωνίας στην κάρτα διασύνδεσης δικτύου. Θα μπορούσαμε να συνοψίσουμε τα πλεονεκτήματά τους ως εξής :

- Όταν είναι σωστά τοποθετημένα μπορούν να ελέγχουν ένα μεγάλο δίκτυο και να ανιχνεύουν επιθέσεις που εκδηλώνονται μέσω αυτού. Προκειμένου να εγκατασταθεί ένα NIDS δεν είναι απαραίτητη η τροποποίηση των εξυπηρετητών παραγωγής (production servers) ή των hosts.
- Επειδή η εγκατάστασή τους είναι απλή, έχουν την δυνατότητα παρακολούθησης δεδομένων χωρίς εξουσιοδότηση.
- Έχουν χαμηλό συνολικό κόστος. Σε κάθε δίκτυο αντιστοιχεί ένα IDS το οποίο ελέγχει όλη τη κίνηση, σε αντίθεση με το host–based οπού αντιστοιχεί ένα IDS ανά υπολογιστή.
- Για να λειτουργήσει αποτελεσματικά ένα τέτοιο σύστημα χρειάζονται λίγοι μόνο αισθητήρες (sensors), καθώς εάν τοποθετηθούν σε στρατηγικά σημεία (π.χ. Span

πόρτες σε ένα switch) του δικτύου μπορούν να προσφέρουν πλήρη εικόνα του, δίνοντας παράλληλα τη δυνατότητα ευκολότερης διαχείρισης, ενώ τόσο η αρχιτεκτονική όσο και η φύση της λειτουργίας τους κάνει δύσκολη την εκδήλωση επίθεσης.

- Το δικτυακό σύστημα ανίχνευσης εισβολών δεν αποτελεί κρίσιμο παράγοντα για τη λειτουργικότητα του δικτύου, γιατί δε λειτουργεί ως δρομολογητής ή ως κάποια άλλη κρίσιμη συσκευή. Άρα τυχόν αποτυχία στο σύστημα ανίχνευσης εισβολών δε θα έχει σημαντική επίδραση στην επιχείρηση.
- Τα Δικτυακά συστήματα ανίχνευσης εισβολών ανιχνεύουν επιθέσεις που τα host-based συστήματα δεν μπορούν να ανιχνεύσουν, όπως π.χ. επιθέσεις DoS που βασίζονται στα περιεχόμενα των IP πακέτων.
- Τα NIDS ανιχνεύουν επιθέσεις σε (σχεδόν) πραγματικό χρόνο, οπότε προσφέρουν ταχύτατη ενημέρωση για την εξέλιξη μιας επίθεσης, ενώ μπορούν να προστατέψουν αυτόματα το δίκτυο πριν ακόμα γίνει ζημιά (π.χ. δυναμική ρύθμιση του firewall έτσι ώστε να σταματήσει τη σύνδεση με τη συγκεκριμένη IP από την οποία γίνεται η επίθεση).
- Τα συστήματα αυτά κάνουν ιδιαίτερα δύσκολο το έργο της διαγραφής των στοιχείων μιας επίθεσης από έναν επιτιθέμενο, αφού λειτουργούν σε (σχεδόν) πραγματικό χρόνο και μπορούν να αποθηκεύσουν τα στοιχεία αυτά σε ειδικούς χώρους, π.χ. σε ένα σύστημα μακριά από το κυρίως δίκτυο. Με την τεχνική αυτή δεν επιτρέπουν στον επιτιθέμενο να φτάσει σε σημείο ώστε να μπορεί να διαγράψει τις αποδείξεις της επίθεσής του.
- Μπορούν να δουν επιθέσεις που προορίζονταν για το δίκτυο αλλά αποτράπηκαν από το firewall και, γενικότερα, μπορούν να βοηθήσουν στη σημαντική συλλογή πληροφοριών για το τι είδους προσπάθειες επίθεσης γίνονται στο δίκτυο (και πότε), έτσι ώστε να υπάρξει η δυνατότητα καλύτερης διαμόρφωσης της πολιτικής ασφάλειας του δικτύου, καθώς και της αρχιτεκτονικής του.
- Δρουν ανεξάρτητα από κάθε λειτουργικό σύστημα, οπότε και δεν χρειάζονται πληροφορίες από εκείνο, ενώ παράλληλα δεν επηρεάζονται από προβλήματα και bugs που μπορεί να υπάρχουν και τα οποία διακινδυνεύουν την καλή τους λειτουργία.
- Δεν χρειάζεται να περιμένουν να ανιχνεύσουν μία επίθεση όταν εκείνη καταχωρηθεί στα αρχεία καταγραφής για να αντιδράσουν και δεν έχουν επίδραση στην απόδοση

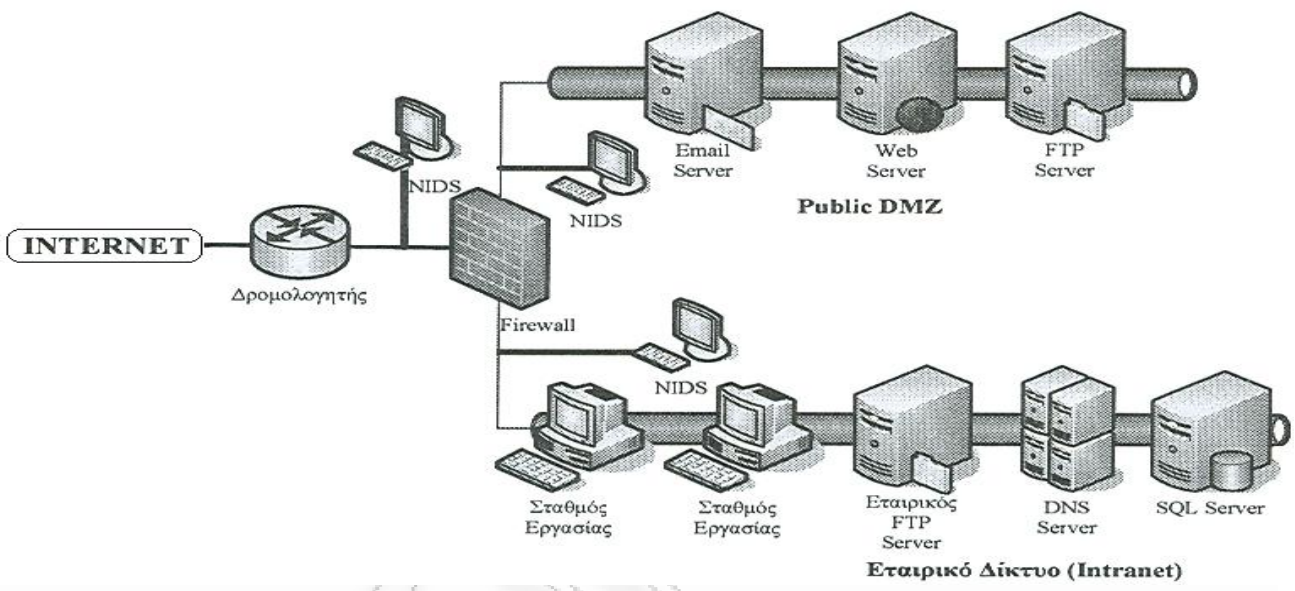
κανενός συστήματος (μια και δρουν αυτόνομα και με δικούς τους υπολογιστικούς πόρους).

Τα Δικτυακά συστήματα ανίχνευσης εισβολών παρουσιάζουν και αδυναμίες όταν έχουν να αντιμετωπίσουν network-based επιθέσεις που εμπλέκουν κατακερματισμένα πακέτα. Κάποια από αυτά που προκαλούν αστάθεια και κατάρρευση των NIDS είναι :

- Τα Δικτυακά συστήματα ανίχνευσης εισβολών συνήθως χρησιμοποιούν ανάλυση signatures. Έτσι μπορούν να ανιχνεύσουν κοινές προγραμματισμένες επιθέσεις από εξωτερικές πηγές, αλλά αδυνατούν να ανιχνεύσουν πιο πολύπλοκες επιθέσεις. Αυτές απαιτούν καλύτερη ικανότητα για ανάλυση του περιβάλλοντος.
- Ένα NIDS πιθανόν να αντιμετωπίσει δυσκολίες στο χειρισμό επιθέσεων στην διάρκεια κρυπτογραφημένων συνόδων. Το πρόβλημα αυτό γίνεται εντονότερο όταν χρησιμοποιούνται εικονικά ιδιωτικά δίκτυα (VPNs, virtual private networks).
- Τα περισσότερα NIDS δεν μπορούν να καθορίσουν αν μία επίθεση ήταν επιτυχής. Αυτό που κάνουν είναι απλά να επισημάνουν το γεγονός της εμφάνισης μίας επίθεσης και των συστημάτων που είχε στόχο. Στην συνέχεια ο υπεύθυνος ασφαλείας του δικτύου είναι υπεύθυνος να εξετάσει κάθε ένα από αυτά τα συστήματα για να εντοπίσει αν η επίθεση πέτυχε.
- Τα NIDS μπορούν να παρουσιάσουν προβλήματα σε δίκτυα όπου υπάρχει μεγάλη δικτυακή κίνηση. Στην περίπτωση αυτή τα NIDS δεν έχουν τους πόρους να επεξεργαστούν όλα τα πακέτα, με αποτέλεσμα να αγνοήσει κάποια από αυτά, κάτι που μπορεί να οδηγήσει στην αποτυχία αναγνώρισης μίας επίθεσης.
- Ένα NIDS μπορεί να αναλύσει τις πληροφορίες που συλλέγει από το segment στο οποίο είναι συνδεδεμένο, δηλαδή δεν έχει την δυνατότητα να συλλέξει πληροφορίες από άλλα segment του δικτύου ώστε να εντοπίσει επιθέσεις σε οποιοδήποτε σημείο του δικτύου. Για να ξεπεραστεί αυτό το πρόβλημα θα πρέπει να αγοραστούν πολλοί αισθητήρες και να τοποθετηθούν σε διαφορετικά τμήματα του δικτύου κάτι που σημαίνει επιπλέον κόστος

4.1.3 Συνδυασμένη Λύση Δικτυακού και Μεμονωμένου Συστήματος IDS

Για την καλύτερη και αποτελεσματικότερη ασφάλεια των δικτύων από τις διαφόρων μορφών επιθέσεις, είναι αναγκαία μια συνδυασμένη και ολοκληρωμένη λύση τόσο από NIDS όσο και από HIDS, η οποία θα καλύπτει τις λειτουργικές ανάγκες κάθε δικτύου. Μια τυπική συνδυασμένη λύση των δύο αυτών συστημάτων απεικονίζεται στο παρακάτω σχήμα 12.



Σχήμα 12. Συνδυασμένη λύση IDS.

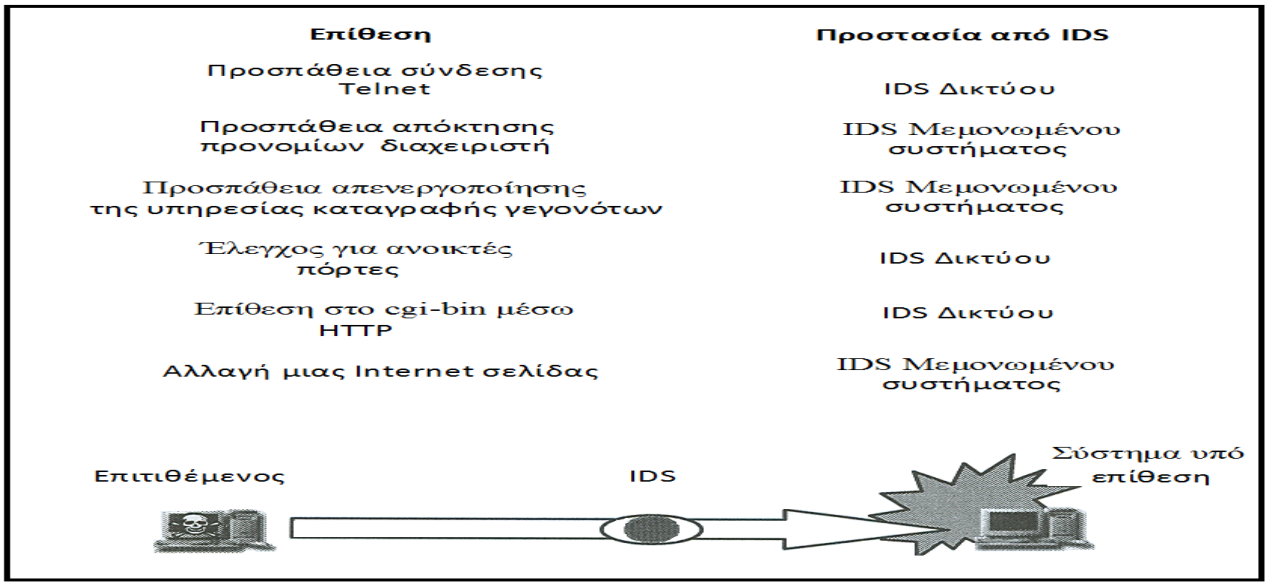
Η συνδυασμένη αυτή λύση παρουσιάζει προτερήματα όπως :

- Κάνει πλέον δυνατή την ανίχνευση σε όλα τα επίπεδα ενός δικτύου δηλαδή από το σημείο εισόδου στο δίκτυο μέχρι το κάθε σύστημα ξεχωριστά, με αρκετά καλή απόδοση.
- Είναι πολύ εύκολο έτσι να δει κανείς ‘‘μοτίβα επιθέσεων’’ τα οποία εξελίσσονται σε μια χρονική ροή, καθώς τα συστήματα αυτά προσφέρουν την ικανότητα της παρουσίασης της εξέλιξης μιας επίθεσης. Αυτή η δυνατότητα είναι ιδιαίτερα χρήσιμη όταν έχει πραγματοποιηθεί μια επίθεση και χρειάζονται στοιχεία για την ανάλυσή της.

Παρουσιάζει όμως και μειονεκτήματα όπως :

- Δεν υπάρχει ακόμα η δυνατότητα χρήσης και ανάμειξης των προϊόντων διαφορετικών κατασκευαστών λόγω του ότι η εμπορική τους επιβίωση επιτάσσει την ανάγκη κατασκευής των προϊόντων τους με μοναδικό τρόπο και χωρίς ιδιαίτερα περιθώρια διαλειτουργικότητας. Τα τελευταία χρόνια γίνονται προσπάθειες για κάτι τέτοιο με πιο σημαντικές τις προτάσεις του IETF καθώς και το ‘‘Κοινό Πλαίσιο Συστημάτων Ανίχνευσης εισβολής’’ (Common Intrusion Detection Framework-CIDF) .
- Μια συνδυασμένη λύση έχει ιδιαίτερο φόρτο εγκατάστασης και διαχείρισης, ιδιαίτερα σε πολύπλοκα και ετερογενή δίκτυα και συστήματα.

Τα περισσότερα σύγχρονα IDS συνδυάζουν τόσο host όσο network λύσεις προσπαθώντας με αυτό τον τρόπο να λύσουν τα μεμονωμένα προβλήματα ανίχνευσης που έχει η κάθε μια τεχνολογία χωριστά όταν ένα δίκτυο ή σύστημα δέχεται κάποιο τύπο επίθεσης. Στο παρακάτω σχήμα 13 απεικονίζονται παραδείγματα επιθέσεων και ο τύπος IDS που χρησιμοποιείται για την αντιμετώπισή τους.



Σχήμα 13. Παραδείγματα επιθέσεων και προστασία.

4.1.4 Παρακολούθηση της Κυκλοφορίας στο Δίκτυο Network Security Monitor – NSM

Το Network Security Monitor – NSM είναι ένα σύστημα εντοπισμού εισβολών και εξετάζει απλώς την κυκλοφορία στο δίκτυο. Αποτελεί ένα network based σύστημα ανίχνευσης εισβολών. Δε χρησιμοποιεί τα στοιχεία ελέγχου από το host μηχάνημα, αλλά αντίθετα παρακολουθεί τη δικτυακή κίνηση για να εντοπίσει εισβολές. Από τη στιγμή που οι βασισμένες στο δίκτυο επιθέσεις είναι πλέον οι πιο διαδεδομένες, λόγω της εξάπλωσης του διαδικτύου, το NSM αποτελεί πολύτιμο εργαλείο στην ανίχνευση επιθέσεων.

Το NSM διαμορφώνει αρχικά μια κατανομή (profile) για την αναμενόμενη χρήση του δικτύου. Ακολούθως συγκρίνει την τρέχουσα χρήση του δικτύου με εκείνη της κατανομής. Αν η τρέχουσα χρήση διαφέρει από την αναμενόμενη, ερμηνεύεται ως διαταραχή. Δηλαδή το σύστημα αυτό ανιχνεύει επιθέσεις με βάση το μοντέλο ανίχνευσης διαταραχών, αφού οτιδήποτε αποκλίνει από το αναμενόμενο θεωρείται εισβολή. Συγκεκριμένα το NSM παρακολουθεί τη πηγή κίνησης του δικτύου, τον προορισμό και την παρεχόμενη υπηρεσία. Ορίζει μια μοναδική ταυτότητα σύνδεσης (connection ID) για κάθε σύνδεση. Τα παρακολουθούμενα στοιχεία σχηματίζουν ένα πίνακα. Κάθε στοιχείο του πίνακα περιέχει έναν αριθμό πακέτων τα οποία στάλθηκαν κατά την διάρκεια μιας καθορισμένης χρονικής περιόδου. Συγκρίνει τα δεδομένα της κάθε σύνδεσης με τα αναμενόμενα δεδομένα της σύνδεσης. Οποιοδήποτε δεδομένο εκτός του αναμενόμενου εύρους θεωρείται διαταραχή. Το NSM κρίθηκε δαπανηρό λόγω του μεγάλου αριθμού δεδομένων που παράγονταν κατά την ανάλυση του δικτύου. Προκειμένου να μειωθεί το κόστος, οι υπεύθυνοι ομαδοποίησαν και ιεράρχησαν τα δεδομένα. Με αυτόν τον τρόπο ζητούσαν από το σύστημα να αναλύσει τα στοιχεία που περιείχε η ομάδα που παρουσίαζε διαταραχή. Ένα σύστημα NSM καθορίζει ένα σύνολο ενεργειών, οι οποίες καταδεικνύουν επιθέσεις. Αν μια ενέργεια που πραγματοποιείται στο δίκτυο ταυτίζεται με μια ενέργεια του συνόλου, τότε το σύστημα αναφέρει επίθεση. Δηλαδή το σύστημα χρησιμοποιεί και το μοντέλο ανίχνευσης κακής συμπεριφοράς για ανίχνευση εισβολών στο δίκτυο. Συγκεκριμένα, ο αναλυτής του συστήματος NSM καταγράφει συγκεκριμένους κανόνες, με βάση τους οποίους συγκρίνεται η κίνηση του δικτύου. Οι κανόνες που χρησιμοποιήθηκαν αρχικά αφορούσαν τον έλεγχο για τυχόν υπερβολικό αριθμό προσπαθειών σύνδεσης, για τυχόν επικοινωνία ενός υπολογιστικού συστήματος με δεκαπέντε ή περισσότερα συστήματα ή για οποιαδήποτε προσπάθεια επικοινωνίας με ανύπαρκτο σύστημα. Το πρωτότυπο σύστημα NSM αναπτύχθηκε στο

University of California at Davis και εντόπιζε πολλές επιθέσεις. Όπως συμβαίνει σε όλα τα συστήματα ανίχνευσης εισβολών, το NSM κατέγραφε λανθασμένους συναγερμούς, όπως την πρόσβαση αποφοίτων του Πανεπιστημίου σε λογαριασμούς οι οποίοι είχαν παραμείνει ανενεργοί για μεγάλο χρονικό διάστημα. Το σύστημα NSM είναι σημαντικό για τους παρακάτω λόγους :

- Απετέλεσε τη βάση για ένα μεγάλο αριθμό συστημάτων ανίχνευσης εισβολών. Μάλιστα, έντεκα χρόνια από τη δημιουργία του χρησιμοποιούνταν σε πολλά συστήματα. Επιπλέον απέδειξε ότι η ανίχνευση εισβολών σε δίκτυο ήταν εφικτή σε πρακτικό επίπεδο.
- Το NSM δεν είναι φανερό στον εισβολέα αφού παρακολουθεί παθητικά τη δικτυακή κίνηση. Επομένως δε μπορεί να τεθεί εκτός λειτουργίας ή να κινδυνέψουν τα δεδομένα του.
- Η κίνηση στο δίκτυο χαρακτηρίζεται ολοένα και περισσότερο από κρυπτογραφημένη ροή μηνυμάτων με αποτέλεσμα η δυνατότητα ανάλυσης των περιεχομένων των πακέτων να μειώνεται. Όμως το NSM εξακολουθεί να είναι αποτελεσματικό διότι δεν εξετάζει τα περιεχόμενα της κίνησης αλλά πραγματοποιεί ανάλυση της ίδιας της κίνησης.
- Το NSM μπορεί να χρησιμοποιηθεί σε οποιοδήποτε σύστημα, γιατί παρακολουθεί δικτυακή κίνηση με χρήση πρωτοκόλλων TCP, UDP, ICMP τα οποία είναι καθιερωμένα.

4.1.5 Συνδυασμένη Προσέγγιση (DIDS)
Distributed Instruction Detection System – DIDS

Το σύστημα Distributed Instruction Detection System – DIDS συνδυάζει τις δυνατότητες του NSM, με τη δυνατότητα παρακολούθησης εισβολών σε μεμονωμένα συστήματα. Δηλαδή χρησιμοποιεί τόσο την τεχνολογία network based IDS, την οποία χρησιμοποιεί και το NSM, όσο και την τεχνολογία host based IDS. Το DIDS χρησιμοποιεί το συνδυασμό αυτό λόγω της διαπίστωσης της μη επάρκειας των παρακολουθήσεων που βασίζονταν αποκλειστικά στο δίκτυο και των παρακολουθήσεων που βασίζονταν αποκλειστικά στον υπολογιστή. Ένας εισβολέας που προσπαθεί να συνδεθεί με ένα σύστημα μέσω ενός λογαριασμού που δεν

απαιτεί χρήση συνθηματικού (password) δε θα ανιχνευόταν ως κακόβουλος από ένα σύστημα παρακολούθησης δικτύου. Ενδεχομένως οι μετέπειτα ενέργειές του να προκαλούσαν ένα σύστημα παρακολούθησης βασισμένο σε υπολογιστή να σημάνει συναγερμό εισβολής. Από την άλλη πλευρά ένα σύστημα ανίχνευσης βασισμένο σε υπολογιστή δε θα μπορούσε να ανιχνεύσει έναν εισβολέα ο οποίος επιχειρεί να συνδεθεί με ένα σύστημα παραπάνω από μια φορές μέσω telnet χρησιμοποιώντας κάθε φορά διαφορετικό όνομα σύνδεσης. Αντίθετα το βασισμένο στο δίκτυο σύστημα ανίχνευσης θα μπορούσε να ανιχνεύσει τις επαναλαμβανόμενες αποτυχημένες προσπάθειες σύνδεσης. Το σύστημα DIDS χρησιμοποιεί ένα έμπειρο σύστημα το οποίο πραγματοποιεί την ανάλυση των δεδομένων. Το έμπειρο σύστημα είναι βασισμένο σε εντολές και είναι σε θέση να εξάγει συμπεράσματα, τόσο για μεμονωμένα συστήματα, όσο και για ολόκληρο το σύστημα που συμπεριλαμβάνει υπολογιστές και δίκτυο. Στη συνέχεια τα αποτελέσματα παρουσιάζονται στον υπεύθυνο ασφάλειας του συστήματος. Πρόβλημα αποτελεί καθώς ένας εισβολέας κινείται από σύστημα σε σύστημα αλλάζοντας ταυτότητα. Για παράδειγμα ένας εισβολέας εισέρχεται στο πρώτο σύστημα ως χρήστης A και στο δεύτερο σύστημα ως χρήστης B. Οι μηχανισμοί βασισμένοι στον υπολογιστή δεν μπορούν να γνωρίζουν ότι ο χρήστης A και ο χρήστης B είναι ένας και έτσι δεν μπορούν να συσχετίσουν τις ενέργειες αυτές. Όμως το έμπειρο σύστημα μπορεί να συμπεράνει ότι πρόκειται για τον ίδιο χρήστη. Για να είναι όμως δυνατή η συσχέτιση πρέπει κάθε χρήστης να έχει ένα μοναδικό αριθμό ταυτότητας δικτύου (Network Identification Number – NID). Έτσι ο χρήστης A και B που είναι στην πραγματικότητα ο ίδιος χρήστης θα μοιράζονταν ένα κοινό NID.

Το έμπειρο σύστημα, ένα βασικό συστατικό στη λειτουργία του συστήματος DIDS, εξάγει πληροφορίες σχετικά με μια εισβολή από τα δεδομένα που λαμβάνει, με τη χρήση κάποιων κανόνων ενός μοντέλου ανίχνευσης εισβολών. Αυτό το μοντέλο περιλαμβάνει τα παρακάτω πέντε επίπεδα :

1. Αρχικά συγκεντρώνει όλα τα δεδομένα για το δίκτυο και όλες τις πληροφορίες για τη δραστηριότητα των χρηστών.
2. Ορίζει ένα υποκείμενο που συγκεντρώνει όλα τα γεγονότα που σχετίζονται με ένα και μοναδικό χρήστη. Το NID αντιστοιχίζεται σε αυτό το υποκείμενο.
3. Προσθέτει διάφορες συναφείς πληροφορίες. Για παράδειγμα χρονικά δεδομένα όπως ο χρόνος χρήσης του επεξεργαστή και χωρικά δεδομένα όπως η ομοιότητα με άλλα γεγονότα. Εάν ο χρήστης προσπαθήσει να συνδεθεί κάποια ώρα κατά την οποία δεν είχε προσπαθήσει

ποτέ πριν να συνδεθεί συνάγεται το συμπέρασμα ότι πιθανό να αναφερόμαστε σε ύποπτο γεγονός.

4. Ασχολείται με τις απειλές προς το δίκτυο (network threats), οι οποίες είναι συνδυασμοί διαφόρων γεγονότων. Μια απειλή είναι εξαπάτηση (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. Μια απειλή θεωρείται κακή συμπεριφορά (misuse) εάν παραβιάζει την πολιτική, χωρίς όμως να μεταβάλλει την κατάσταση του συστήματος. Παράδειγμα αποτελεί η αντιγραφή ενός απαγορευμένου αρχείου, που όμως το αντίγραφο αρχείο είναι προσιτό στον καθένα. Μια απειλή είναι ύποπτη πράξη (suspicious act) αν δεν παραβιάζει την πολιτική, αλλά μπορεί να θεωρηθεί ότι είναι εντός του πεδίου ενεργειών για την προετοιμασία μιας επίθεσης.

5. Βαθμολογεί την κατάσταση ασφάλειας του δικτύου, με βάση τις απειλές προς το σύστημα που αναπτύσσονται στο προηγούμενο επίπεδο. Έτσι δίνεται η δυνατότητα στον υπεύθυνο ασφάλειας του συστήματος να εντοπίσει γρήγορα τα προβλήματα και να εξάγει συμπεράσματα χωρίς καθυστέρηση.

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

4.2 ΚΑΤΗΓΟΡΟΙΟΠΟΙΗΣΗ ΜΕ ΒΑΣΗ ΤΙΣ ΤΕΧΝΙΚΕΣ ΑΝΑΛΥΣΗΣ

Τα συστήματα ανίχνευσης εισβολών προσδιορίζουν, αν κάποιες ενέργειες αποτελούν εισβολές, με κριτήριο ένα ή περισσότερα μοντέλα εισβολών (models of intrusion). Ο ρόλος του μοντέλου είναι να ταξινομήσει τις ενέργειες ή τις καταστάσεις σε ένα σύστημα και να τις χαρακτηρίσει ‘‘καλές’’ ή ‘‘κακές’’. Υπάρχουν κυρίως τρεις προσεγγίσεις για την ανάλυση των συμβάντων προς ανίχνευση των επιθέσεων. Η πρώτη είναι η τεχνική του **Μοντέλου Κακής Συμπεριφοράς (Misuse Detection**), η δεύτερη είναι η τεχνική του **Μοντέλου Ανίχνευσης Διαταραχών (Anomaly Detection)** και η τρίτη του **Μοντέλου Ανίχνευσης Διαταραχών Πρωτοκόλλων (Protocol Anomaly Detection).**

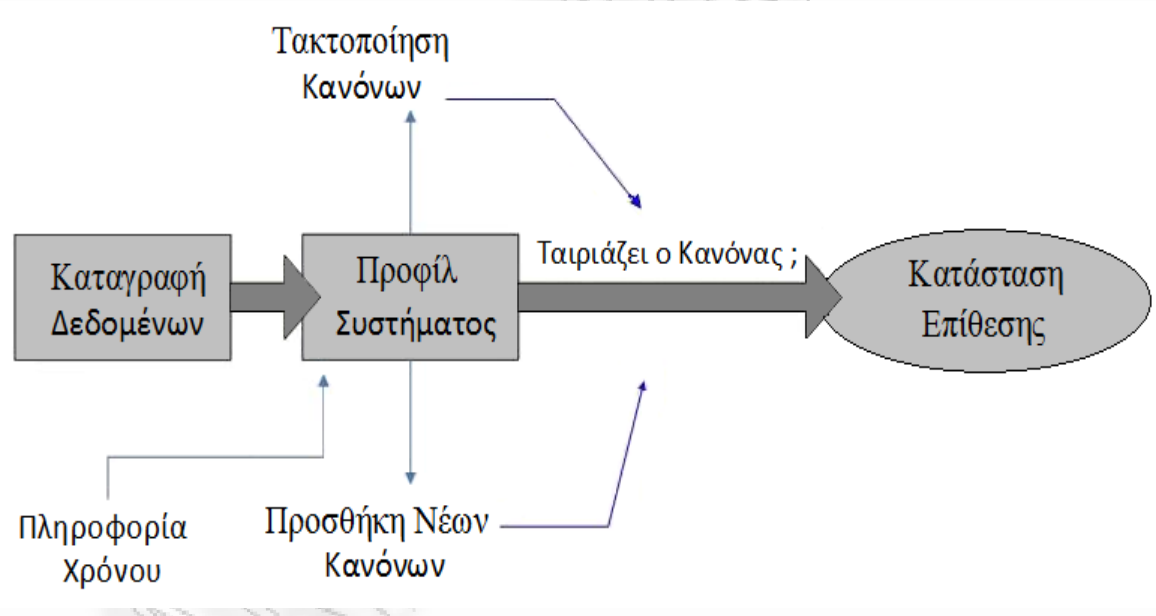
Πολλές φορές τα συστήματα ανίχνευσης εισβολών χρησιμοποιούν συνδυασμό διαφορετικών τύπων μοντέλων (compound hybrid). Τα μοντέλα μπορεί να είναι προσαρμοστικά (adaptive) δηλαδή μοντέλα που αλλάζουν τη συμπεριφορά τους με βάση τις καταστάσεις και τις ενέργειες των συστημάτων ή στατικά (static) δηλαδή μοντέλα που αρχικοποιούνται από δεδομένα που έχουν συλλέξει και δεν τροποποιούνται κατά την διάρκεια εκτέλεσης του συστήματος. Κάθε μία από αυτές τις τεχνικές έχει τα πλεονεκτήματα και τα μειονεκτήματά της, ενώ η καλύτερη προσέγγιση είναι αυτή στην οποία χρησιμοποιείται κατά κύριο λόγο η τεχνική του Misuse Detection, η οποία συνδυάζεται με τα αποτελέσματα του Protocol Anomaly Detection και κάποιες έξυπνες μεθόδους του Anomaly Detection.

4.2.1 Μοντέλου Κακής Συμπεριφοράς Misuse Detection

Χρησιμοποιείται από τα περισσότερα IDS και προσπαθεί να εντοπίσει κάτι που θεωρείται ‘‘ύποπτο’’. Με την τεχνική του Misuse Detection ελέγχεται η δραστηριότητα ενός δικτύου για να εντοπιστούν γεγονότα που μπορεί να ταιριάζουν με κάποια προκαθορισμένα πρότυπα γεγονότων που περιγράφουν μία γνωστή επίθεση. Τα πρότυπα αυτά ονομάζονται Signatures (υπογραφές) και για αυτό το λόγο η τεχνική αυτή ονομάζεται και Ανίχνευση βασιζόμενη σε υπογραφές (Signatures-based detection). Ένα signature μπορεί για παράδειγμα να περιγράφει κάποια χαρακτηριστικά ενός πακέτου, όπως η εμφάνιση στα data του, ενός συγκεκριμένου λεκτικού που χρησιμοποιείται για μία επίθεση. Συνήθως για κάθε επίθεση ορίζεται και ξεχωριστό signature, αλλά υπάρχουν και προσεγγίσεις όπου ένα signature μπορεί να περιγράφει μία ομάδα από επιθέσεις. Η τεχνική αυτή ονομάζεται Statebased detection. Εφαρμόζεται για συγκεκριμένες εφαρμογές – πρωτόκολλα όπως HTTP, IRC.

Η ανίχνευση κακής συμπεριφοράς απαιτεί τη γνώση όλων των ευπαθειών των συστημάτων που οι επιτιθέμενοι προσπαθούν να εκμεταλλευτούν. Το σύστημα ανίχνευσης εισβολών ενσωματώνει αυτή τη γνώση σε ένα σύνολο κανόνων. Ουσιαστικά το σύνολο αυτό περιέχει πρότυπα εισβολής. Οι κανόνες του συνόλου εφαρμόζονται στα γεγονότα που συμβαίνουν στο δίκτυο, ώστε να καθοριστεί εάν κάποια γεγονότα ταιριάζουν με κάποιους από τους κανόνες. Σε καταφατική περίπτωση συνάγεται το συμπέρασμα ότι βρίσκεται σε εξέλιξη μια πιθανή εισβολή. Τα συστήματα ανίχνευσης εισβολών που βασίζονται στο μοντέλο κακής συμπεριφοράς μοιάζουν πολύ με τα antivirus προγράμματα. Μπορούν να ανιχνεύσουν πολλά γνωστά πρότυπα εισβολής, αλλά δεν μπορούν να ανιχνεύσουν επιθέσεις που είναι άγνωστες

στους δημιουργούς του συνόλου των κανόνων. Οι άγνωστες επιθέσεις που έχουν διεξαχθεί, ή ακόμη και οι παραλλαγές γνωστών επιθέσεων, είναι δύσκολο να ανιχνευθούν. Με άλλα λόγια, τα μοντέλα κακής συμπεριφοράς προσπαθούν να αναγνωρίσουν γνωστές ‘‘κακές’’ συμπεριφορές. Τα συστήματα ανίχνευσης εισβολών που βασίζονται στο μοντέλο κακής συμπεριφοράς χρησιμοποιούν συνήθως έμπειρα συστήματα για να αναλύσουν τα γεγονότα που συμβαίνουν στο δίκτυο και να εφαρμόσουν το σύνολο κανόνων σ’ αυτά. 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 οι πιθανές παραλλαγές μιας σχετικής επίθεσης και πώς θα δημιουργήσουμε Signatures που αγνοούν την μη επιθετική δραστηριότητα. Στο παρακάτω σχήμα 14 απεικονίζεται ένα τυπικό Misuse detection σύστημα.



Σχήμα 14. Παράδειγμα συστήματος ανίχνευσης κακής συμπεριφοράς.

Η εφαρμογή ενός τέτοιου IDS περιλαμβάνει συνήθως ένα έμπειρο σύστημα που εκτελεί τη σύγκριση με κανόνες αποθηκευμένους σε μια βάση δεδομένων. Μια προφανής δυσκολία σε αυτή την αρχιτεκτονική είναι η ανάγκη για τη σταθερή ενημέρωση της βάσης με καινούριες υπογραφές επιθέσεων, καθώς νέες μέθοδοι επιθέσεων γίνονται γνωστές καθημερινά. Δεδομένου ότι το πρότυπο αυτό λειτουργεί με την έρευνα για δείγματα που είναι

αντιπροσωπευτικά διαφόρων επιθέσεων, αναφέρεται στη βιβλιογραφία ως πρότυπο ανίχνευσης κακής χρήσης.

Αξιολογώντας την τεχνική Misuse Detection καταλήγουμε στο συμπέρασμα ότι παρουσιάζει τα παρακάτω πλεονεκτήματα :

- Έχει την ικανότητα να ανιχνεύει επιθέσεις χωρίς να παράγει πολύ μεγάλο αριθμό από False Positives.
- Έχει την δυνατότητα να ανιχνεύει γρήγορα και αρκετά αξιόπιστα το εργαλείο που χρησιμοποιήθηκε για να υλοποιηθεί μια επίθεση, ώστε να προστατευτεί καλύτερα το σύστημα.

Επίσης παρουσιάζει και κάποια μειονεκτήματα όπως :

- Με την τεχνική του Misuse Detection μπορούν να ανιχνευτούν μόνο γνωστές επιθέσεις και για αυτό το λόγο πρέπει τα signatures να ανανεώνονται τακτικά ώστε να καλύπτουν νέες επιθέσεις που εμφανίζονται.

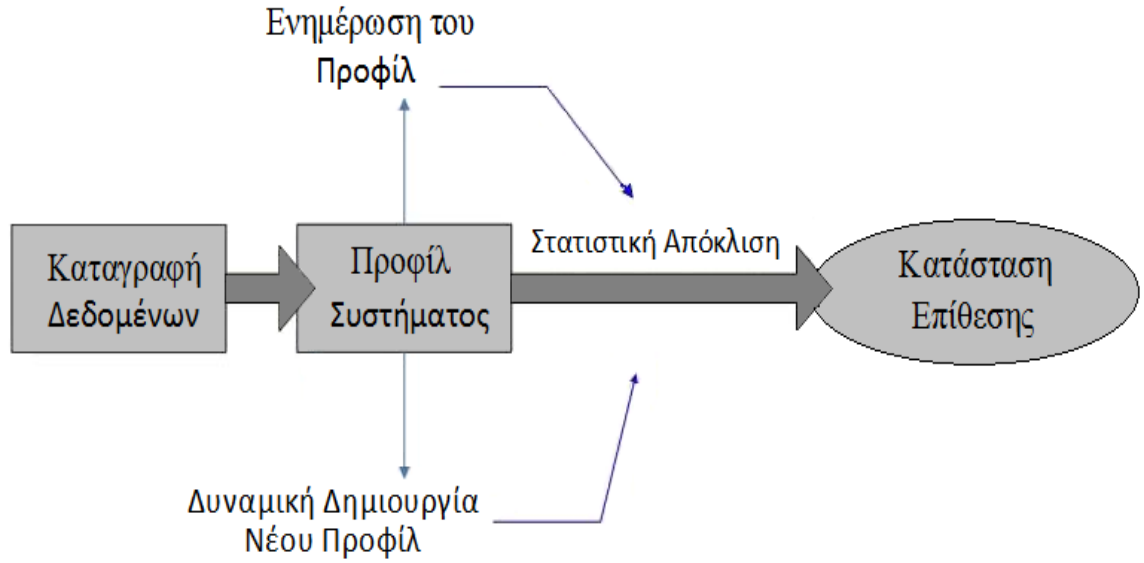
- Η αξιοπιστία της Misuse Detection τεχνικής στηρίζεται στην ποιότητα και την σωστή δημιουργία των Signatures που χρησιμοποιεί. Πολλά IDSs χρησιμοποιούν signatures που περιγράφουν αυστηρά μία συγκεκριμένη επίθεση και δεν έχουν την δυνατότητα να ανιχνεύουν διάφορες παραλλαγές αυτής. Η state-based τεχνική σε πολλές περιπτώσεις καταφέρνει να ξεπεράσει αυτό το πρόβλημα.

4.2.2 Μοντέλο Ανίχνευσης Διαταραχών
Anomaly Detection

Η τεχνική του Anomaly Detection προσπαθεί να εντοπίσει μη φυσιολογική, ασυνήθιστη συμπεριφορά ενός δικτύου ή ενός συστήματος. Επειδή η μέθοδος αυτή έχει σαν βάση τις ασυνήθιστες συμπεριφορές ονομάζεται και behavior-based. Λειτουργεί με την υπόθεση ότι η δραστηριότητα που παράγεται με την εμφάνιση μίας επίθεσης, παρουσιάζει διαφορές από την φυσιολογική (νόμιμη) δραστηριότητα και για αυτό υπάρχει η δυνατότητα να ανιχνευτούν τυχόν επιθέσεις, από συστήματα που μπορούν να εντοπίσουν αυτές τις διαφορές.

Αρχικά με την μέθοδο του Anomaly Detection δημιουργούνται πρότυπα (patterns) που αντιπροσωπεύουν την φυσιολογική συμπεριφορά των χρηστών ή των συστημάτων ή του traffic ενός δικτύου. Τα πρότυπα αυτά χτίζονται από δεδομένα που συλλέγονται κατά την κανονική λειτουργία και αποτελούν το δείγμα φυσιολογικής δραστηριότητας. Το Μοντέλο Ανίχνευσης Διαταραχών χρησιμοποιεί ένα σύνολο στατιστικών στοιχείων που διαμορφώνουν τη συμπεριφορά μιας οντότητας. Οντότητα μπορεί να είναι ένας χρήστης, μια ομάδα χρηστών ή ένας υπολογιστής. Το προφίλ μιας οντότητας χρηστών, μπορεί να περιλάβει πληροφορίες όπως η μέση διάρκεια των συνόδων του Telnet και FTP, το ποσό των bytes που μεταδίδονται και προς τις δύο κατευθύνσεις, τις ώρες της ημέρας ή τα τερματικά από τα οποία συνδέεται ο χρήστης. Το προφίλ ενός υπολογιστή μπορεί να περιλαμβάνει τη μέση χρησιμοποίηση της CPU, το μέσο αριθμό συνδεδεμένων χρηστών, κ.α.

Η δημιουργία των patterns είναι το πιο δύσκολο κομμάτι της τεχνικής του Anomaly Detection καθώς η δραστηριότητα ενός δικτύου ή ενός συστήματος παρουσιάζει πολλές διακυμάνσεις και δεν είναι εύκολο να μοντελοποιηθεί. Στη συνέχεια συλλέγονται δεδομένα από τα γεγονότα που συμβαίνουν και με διάφορες μεθόδους εξετάζεται κατά πόσο αυτά διαφέρουν από τα patterns της φυσιολογικής δραστηριότητας. Ένα IDS ελέγχει τη λειτουργία ενός υπολογιστικού συστήματος και συγκρίνει συνεχώς το τρέχον προφίλ ενός συστήματος, με το προφίλ που είναι αποθηκευμένο στη βάση δεδομένων του. Σε περίπτωση που ανιχνεύσει μια μεγάλη απόκλιση από την κανονική συμπεριφορά στέλνει μία ειδοποίηση στο διαχειριστή ασφάλειας των υπολογιστικών συστημάτων. Το μέγεθος μιας μεγάλης απόκλισης ορίζεται ως ένα κατώτατο όριο που τίθεται από το IDS ή τον διαχειριστή ασφάλειας των συστημάτων. Συνήθως τα αποθηκευμένα προφίλ ενημερώνονται συνεχώς προκειμένου να απεικονιστούν οι αλλαγές στη συμπεριφορά των χρηστών ή του συστήματος. Τα IDS αυτά στηρίζονται σε μεγάλο ποσοστό στα αρχεία καταγραφής (log files) που παρέχονται από το λειτουργικό σύστημα του υπολογιστή, το οποίο τα καθιστά αρχιτεκτονικά εξαρτώμενα και πιο ευάλωτα σε επιθέσεις DoS (Denial of Service) ενάντια σε αυτά, δεδομένου ότι ένας εισβολέας μπορεί να κατορθώσει να καθυστερήσει το μηχανισμό καταγραφής ή ακόμα και να τον σταματήσει τελείως. Ένα παράδειγμα συστήματος ανίχνευσης διαταραχών απεικονίζεται στο παρακάτω σχήμα 15.



Σχήμα 15. Παράδειγμα συστήματος ανίχνευσης διαταραχών.

Με τον τρόπο που δουλεύουν τα μοντέλα αυτά παρουσιάζουν δύο προβλήματα :

1. Ασυνήθεις δραστηριότητες, που δεν έχουν χαρακτήρα εισβολής τις χαρακτηρίζουν ως επιθετικές (false positive).

2. Επιθετικές δραστηριότητες που δεν είναι ασυνήθεις, δεν τις χαρακτηρίζουν ως επιθέσεις (false negative).

Το δεύτερο πρόβλημα είναι ιδιαίτερα επικίνδυνο και πιο σοβαρό από το πρώτο πρόβλημα, αφού σκοπός των συστημάτων ανίχνευσης εισβολών είναι η ανίχνευση επιθέσεων. 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 positive και false negatives) να μη μεγιστοποιείται. Σημαντική είναι, επίσης και η επιλογή των χαρακτηριστικών στην παρακολούθηση δεδομένων. Ένα αρνητικό στοιχείο είναι ότι τα συστήματα ανίχνευσης διαταραχών είναι ακριβά, λόγω του κόστους του ελέγχου και της συνεχούς ανανέωσης του προφίλ δραστηριότητας του συστήματος. Επίσης για να δημιουργηθούν τα patterns της φυσιολογικής δραστηριότητας συνήθως απαιτούνται εκτεταμένα εκπαιδευτικά σύνολα που θα χρησιμοποιηθούν ως παράδειγμα. Συμπερασματικά θα πρέπει να σημειώσουμε το πιο σημαντικό πλεονέκτημα των μεθόδων αυτών είναι η ικανότητά τους να ανιχνεύουν νέες επιθέσεις ενάντια στα υπολογιστικά συστήματα. Αυτό είναι πιθανό γιατί οι τεχνικές ανίχνευσης ανωμαλιών δεν αναλύουν τη δικτυακή κίνηση για να εντοπίσουν συγκεκριμένα πρότυπα, αλλά αντίθετα συγκρίνουν την τρέχουσα

δραστηριότητα με μοντέλα προηγούμενης συμπεριφοράς. Το Anomaly Detection αποτελεί ένα καθαρά ερευνητικό αντικείμενο με πολλά ελπιδοφόρα μηνύματα για το μέλλον. Μερικές από τις μεθόδους που χρησιμοποιούνται στην τεχνική του Anomaly Detection για να γίνει η δημιουργία των patterns και η σύγκριση των γεγονότων με αυτά αναπτύσσονται παρακάτω.

4.2.2.1 Στατιστική προσέγγιση (Statistical Anomaly Detection)

Στις στατιστικές μεθόδους για την ανίχνευση ανωμαλιών, το σύστημα παρατηρεί τη δραστηριότητα των διαφόρων οντοτήτων και παράγει τα κατάλληλα προφίλ για να περιγράψει τη συμπεριφορά τους. Τυπικά, διατηρούνται δύο προφίλ για κάθε οντότητα : το τρέχον προφίλ και το αποθηκευμένο προφίλ. Καθώς τα γεγονότα του δικτύου (δηλαδή αρχεία καταγραφής, εισερχόμενα πακέτα, κ.λπ.) υποβάλλονται σε επεξεργασία, το σύστημα ανίχνευσης εισβολής ενημερώνει το τρέχον προφίλ και υπολογίζεται περιοδικά ένας βαθμός ανωμαλίας (Anomaly score), που δείχνει το βαθμό παρατυπίας για το συγκεκριμένο γεγονός, συγκρίνοντας το τρέχον προφίλ με το αποθηκευμένο. Υπάρχουν πολλοί παράγοντες που επηρεάζουν το προφίλ συμπεριφοράς όπως ο χρόνος χρήσης του επεξεργαστή, ο αριθμός των δικτυακών συνδέσεων στην μονάδα του χρόνου κ.λπ. Σε μερικά συστήματα το παρόν προφίλ και το προηγούμενο συνενώνονται ανά διαστήματα, ενώ σε άλλα η παραγωγή προφίλ γίνεται σε μια χρονική περίοδο. Εάν ο βαθμός ανωμαλίας είναι υψηλότερος από ένα ορισμένο κατώτατο όριο (threshold), το σύστημα ανίχνευσης εισβολών παράγει ένα προειδοποιητικό μήνυμα (alert). Οι στατιστικές προσεγγίσεις στο πεδίο της ανίχνευσης ανωμαλιών έχουν αρκετά πλεονεκτήματα. Αρχικά, αυτά τα συστήματα, όπως τα περισσότερα συστήματα ανίχνευσης ανωμαλιών, δεν απαιτούν προγενέστερη γνώση των προβλημάτων ασφαλείας ή/και των επιθέσεων που έχουν προηγηθεί. Κατά συνέπεια, τέτοια συστήματα έχουν την ικανότητα της ανίχνευσης επιθέσεων τύπου ‘‘μηδενικής μέρας’’ (zero day) ή επιθέσεων που δεν είναι ευρέως γνωστές. Επιπλέον, οι στατιστικές προσεγγίσεις μπορούν να παρέχουν μία ακριβή προειδοποίηση των κακόβουλων δραστηριοτήτων όπου αυτές εμφανίζονται σε παρατεταμένες χρονικά περιόδους. Ένα πολύ κοινό παράδειγμα μιας τέτοιας δραστηριότητας είναι μια δραστηριότητα σάρωσης θυρών (portscan). Χαρακτηριστικά, η κατανομή των πακέτων από δραστηριότητα portscan είναι ιδιαίτερα ανώμαλη σε σύγκριση με τη συνηθισμένη κατανομή κίνησης. Έχοντας αυτό υπόψη, τα portscans ακόμα και όταν

κατανέμονται σε ένα μεγάλο χρονικό διάστημα θα γίνουν αντιληπτά από τις στατιστικές μεθόδους επειδή θα προκαλέσουν ανώμαλη δραστηριότητα.

Όμως οι στατιστικές τεχνικές ανίχνευσης ανωμαλιών έχουν και κάποια μειονεκτήματα. Οι επιτιθέμενοι μπορούν να εκπαιδεύσουν ένα σύστημα ανίχνευσης ανωμαλιών που χρησιμοποιεί στατιστική ανάλυση να δεχτεί μία ανώμαλη συμπεριφορά σαν κανονική. Μπορεί επίσης να είναι δύσκολο να καθοριστούν τα κατώτατα όρια που ελαχιστοποιούν τις πιθανότητες ψευδών θετικών και ψευδών αρνητικών περιστατικών. Επιπλέον, οι στατιστικές μέθοδοι χρειάζονται τις ακριβείς στατιστικές κατανομές των διαφόρων μετρικών του δικτύου, αλλά αυτές πάντοτε δεν μπορούν να διαμορφωθούν κατάλληλα με βάση τις συμπεριφορές των διαφόρων οντοτήτων μέσα στο δίκτυο. Στις στατιστικές μεθόδους ανίχνευσης ανωμαλιών περιλαμβάνονται τρία μοντέλα :

- **Μετρικό Σύστημα Τιμών Κατωφλίου (Threshold Metric)**

Με αυτή την μέθοδο καταμετρούνται κάποια χαρακτηριστικά της συμπεριφοράς του χρήστη και του συστήματος και ελέγχεται το πλήθος τους, σε σχέση με κάποιο ανώτατο όριο που θεωρείται το επιτρεπτό. Τέτοιου είδους χαρακτηριστικά συμπεριφοράς μπορεί να είναι ο αριθμός των αρχείων στα οποία είχε πρόσβαση ένας χρήστης μέσα σε συγκεκριμένη χρονική περίοδο, το πλήθος των αποτυχημένων προσπαθειών κάποιου χρήστη να κάνει login σε ένα σύστημα, το ποσοστό της CPU που κάνει χρήση ένα process κ.α. Το ανώτατο επιτρεπτό όριο μπορεί να έχει μία στατική τιμή ή να μεταλλάσσεται δυναμικά, προσαρμόζοντας την τιμή του, σύμφωνα με τις τιμές που παρατηρούνται στη διάρκεια του χρόνου και θεωρούνται φυσιολογικές. Το μοντέλο αυτό χαρακτηρίζει τις δραστηριότητες που γίνονται στο σύστημα ως επιθετικές ή μη, με βάση κάποιες καθορισμένες τιμές κατωφλίου (threshold metric). Το μοντέλο λειτουργεί ως εξής : Κάποιο συγκεκριμένο γεγονός αναμένεται να εμφανιστεί, σε δεδομένη χρονική περίοδο, κατ' ελάχιστο m και κατά μέγιστο n, όπου m και n συγκεκριμένες τιμές. Εάν κατά τη διάρκεια της συγκεκριμένης χρονικής περιόδου, το συγκεκριμένο γεγονός εμφανίζεται λιγότερο από m ή περισσότερο από n, τότε η συμπεριφορά θεωρείται διαταραγμένη. Για παράδειγμα στο λειτουργικό σύστημα MS-Windows NT 4.0 επιτρέπεται η αποτροπή της εισαγωγής ενός χρήστη, μετά από κάποιο αριθμό n αποτυχημένων προσπαθειών εισαγωγής. Αυτό αποτελεί ενέργεια ενός συστήματος ανίχνευσης εισβολών που χρησιμοποιεί το μοντέλο τιμών κατωφλίου, με κατώτατο όριο

το 0 και ανώτατο όριο το n. Οι προσπάθειες για εισαγωγή στο σύστημα θεωρούνται ασυνήθεις ή διαταραγμένες μετά από n αποτυχημένες προσπάθειες για εισαγωγή. Ο καθορισμός των τιμών κατωφλίου αυξάνει την πολυπλοκότητα του μοντέλου.

- **Στατιστικές Ροπές (Statistical Moments).**

Το μοντέλο αυτό χρησιμοποιεί στατιστικές ροπές. 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' αυτή τη ροπή, η συμπεριφορά που αντιπροσωπεύουν οι τιμές θεωρείται διαταραγμένη. Επειδή η κατανομή (profile) της περιγραφής του συστήματος μπορεί να εμπεριέχει καθυστερήσεις, τα μοντέλα ανίχνευσης διαταραχών συνυπολογίζουν αυτές τις αλλαγές τροποποιώντας τους στατιστικούς κανόνες με βάση τους οποίους λαμβάνονται οι αποφάσεις. Επιπλέον η περιγραφή της κατανομής κάθε συστήματος ενημερώνεται σε τακτά χρονικά διαστήματα (π.χ. κάθε μέρα), με βάση τη συμπεριφορά που έχει παρατηρηθεί. Τα μοντέλα στατιστικών ροπών παρέχουν μεγαλύτερη ευελιξία από τα μοντέλα τιμών κατωφλίου. Με την ευελιξία, όμως, εμφανίζονται και προβλήματα πολυπλοκότητας. Η συμπεριφορά τόσο των χρηστών, όσο και των διεργασιών μπορεί να μοντελοποιηθεί στατιστικά. Αν αυτή η συμπεριφορά ταιριάζει με κάποια στατιστική κατανομή, όπως η κατανομή Causs ή η κανονική κατανομή, ο προσδιορισμός των παραμέτρων απαιτεί πειραματικά δεδομένα που μπορούν να ληφθούν από το σύστημα. Σε περίπτωση που δεν ταιριάζει, η ανάλυση πρέπει να χρησιμοποιήσει άλλες τεχνικές, όπως τη συστοιχία. Η τεχνική της συστοιχίας απαιτεί να είναι διαθέσιμο κάποιο σύνολο δεδομένων, το οποίο προκύπτει από την παρακολούθηση του συστήματος για κάποια χρονική περίοδο. Ακολούθως τα δεδομένα ομαδοποιούνται σε συστοιχίες, με βάση κάποια ιδιότητα που αποκαλείται χαρακτηριστικό γνώρισμα. Με αυτή την τεχνική μπορούν 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.

- **Μαρκοβιανό μοντέλο (Markov model)**.

Αυτό το μοντέλο εξετάζει ένα σύστημα σε μια συγκεκριμένη χρονική στιγμή. Το σύνολο των προηγηθέντων χρονικά γεγονότων θέτει το σύστημα σε μια συγκεκριμένη κατάσταση. Μόλις λάβει χώρα ένα νέο γεγονός τότε το σύστημα μεταβαίνει σε μια νέα κατάσταση. Έτσι με τη πάροδο του χρόνου δημιουργείται ένα σύνολο πιθανοτήτων μετάβασης του συστήματος από την μία κατάσταση στις επόμενες. Κάθε γεγονός που προκαλεί μετάβαση από την υπάρχουσα κατάσταση σε άλλη και δεν ανήκει στο σύνολο πιθανοτήτων που έχει αναπτυχθεί ή έχει μικρή πιθανότητα θεωρείται διαταραγμένο. Το Μαρκοβιανό μοντέλο για την ανίχνευση των διαταραχών προτείνει τη χρήση κάποιας κατάστασης και οι διαταραχές βασίζονται σε ακολουθίες γεγονότων που μεταβάλλουν την κατάσταση του συστήματος

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 μετρικών-παραγόντων.

4.2.2.2 Πρόβλεψη προτύπων (Predictive pattern generation)

Αυτό το μοντέλο ανίχνευσης εισβολών προσπαθεί να προβλέψει μελλοντικά γεγονότα με χρήση γεγονότων που έχουν ήδη συμβεί. Τα γεγονότα που προηγήθηκαν χρονικά έχουν θέσει το σύστημα σε μια συγκεκριμένη κατάσταση. Όταν συμβεί το επόμενο γεγονός, το σύστημα μεταβαίνει σε μια νέα κατάσταση. Προϊόντος του χρόνου μπορεί να αναπτυχθεί ένα σύνολο πιθανοτήτων μετάβασης. Όταν συμβεί ένα γεγονός που προκαλεί μια μετάβαση με μικρή πιθανότητα, το γεγονός κρίνεται διαταραγμένο. Οι διαταραχές δεν είναι πλέον βασισμένες σε στατιστικά των περιστατικών μεμονωμένων γεγονότων, αλλά σε ακολουθίες γεγονότων. Για παράδειγμα υπάρχει σε ένα σύστημα ο εξής κανόνας :

$$E1 - E2 \rightarrow (E3 = 86\%, E4 = 14\%).$$

Αυτό σημαίνει ότι με δεδομένα τα γεγονότα E1 και E2 και με το E2 να ακολουθεί το E1 στο χρόνο, υπάρχει 86% πιθανότητα να ακολουθήσει το γεγονός E3 και 14% πιθανότητα να ακολουθήσει το γεγονός E4. Αν συμβεί η ακολουθία E1-E2-E5 τότε θα ενεργοποιηθεί η κατάσταση συναγερμού, διότι η ακολουθία E1-E2 πρέπει να ακολουθείται από το E3 ή E4 γεγονός. Το πρόβλημα στο μοντέλο αυτό είναι ότι διάφορα επιθετικά σενάρια που δεν έχουν

προβλεφθεί από το σύστημα δε θα χαρακτηριστούν ως εισβολή. Δηλαδή αν μια ακολουθία γεγονότων A-B-E υπάρχει και είναι εισβολή, αλλά δε βρίσκεται στη βάση κανόνων, θα καταχωρηθεί απλά ως άγνωστη. Αυτό το πρόβλημα μπορεί να λυθεί μερικώς με το χαρακτηρισμό οποιουδήποτε άγνωστου γεγονότος ως εισβολή (αυξάνοντας έτσι τον αριθμό 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 και πολλά πλεονεκτήματα σε αυτό το μοντέλο. Τα ακολουθιακά πρότυπα βασισμένα σε κανόνες μπορούν να ανιχνεύσουν ανώμαλες δραστηριότητες πολύ πιο εύκολα από άλλα μοντέλα. Επιπλέον τα συστήματα που κατασκευάζονται χρησιμοποιώντας αυτό το μοντέλο είναι ιδιαίτερα προσαρμόσιμα σε αλλαγές. Αυτό συμβαίνει γιατί τα λιγότερα καλά και αποτελεσματικά πρότυπα συνεχώς εξαλείφονται, ενώ παραμένουν μόνο τα πολύ ποιοτικά πρότυπα. Τέλος, οι ανώμαλες δραστηριότητες εντοπίζονται και αναφέρονται μέσα σε λίγα δευτερόλεπτα από τη στιγμή της λήψης της κρίσιμης πληροφορίας.

4.2.2.3 Νευρωνικά Δίκτυα (Neural Networks)

Τα Νευρωνικά Δίκτυα αποτελούν μια διαφορετική προσέγγιση εντοπισμού εισβολής στα πληροφοριακά συστήματα. Ένα νευρωνικό δίκτυο λειτουργεί με βάση το σύνολο των εντολών που αντιπροσωπεύουν ένα χρήστη. Αυτά τα συστήματα μαθαίνουν να προβλέπουν την επόμενη εντολή ή ενέργεια βασισμένα σε μια ακολουθία από προηγούμενες εντολές ή ενέργειες ενός συγκεκριμένου χρήστη. Η κατασκευή ενός IDS με νευρωνικά δίκτυα αποτελείται από 3 φάσεις :

1. Η συλλογή του συνόλου δεδομένων εκπαίδευσης (**training set**) χρησιμοποιώντας τα αρχεία ελέγχου (**audit logs**) για κάθε χρήστη για μια δεδομένη χρονική περίοδο. Με αυτόν τον τρόπο σχηματίζεται ένα διάνυσμα για κάθε μέρα και για κάθε χρήστη, το οποίο δείχνει πόσο συχνά ο χρήστης εκτέλεσε κάθε εντολή - ενέργεια.

2. Η εκπαίδευση του νευρωνικού δικτύου ώστε να αναγνωρίζει το χρήστη βάσει των διανυσμάτων κατανομής των εντολών (**command distributionvectors**).

3. Αναγνώριση του χρήστη βάσει του προαναφερθέντος διανύσματος. Εάν το δίκτυο αποφαίνεται ότι δεν πρόκειται για τον πραγματικό χρήστη, σημαίνει συναγερμός.

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.

Μερικά πλεονεκτήματα της χρήσης νευρωνικών δικτύων είναι ότι αντιμετωπίζουν ικανοποιητικά πολύπλοκα δεδομένα που περιέχουν θόρυβο, η επιτυχία τους δε εξαρτάται από οποιαδήποτε στατιστική υπόθεση σχετικά με τη φύση των υπό εξέταση δεδομένων και είναι ευκολότερη η τροποποίησή τους για νέες κοινότητες χρηστών.

Παρουσιάζουν όμως και κάποιες αδυναμίες : ένα μικρό παράθυρο θα καταλήξει σε false Positives ενώ ένα μεγάλο παράθυρο θα καταλήξει σε άσχετα δεδομένα καθώς επίσης και σε αύξηση των false negatives. Επιπλέον, η τοπολογία δικτύου καθορίζεται μόνον μετά από σημαντικό αριθμό δοκιμών και λαθών (**trial and error**) και τέλος ένας εισβολέας μπορεί να εκπαιδεύσει το δίκτυο κατά τη φάση της μάθησης.

4.2.3 Σύγκριση των μεθόδων Anomaly και Misuse Detection

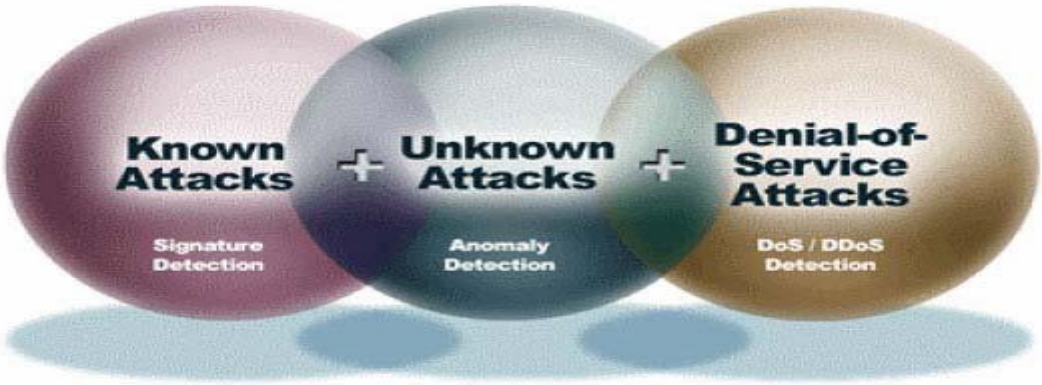
Τα συστήματα ανίχνευσης ανωμαλιών προσπαθούν να εντοπίσουν το συμπλήρωμα της κακής συμπεριφοράς, ενώ τα συστήματα ανίχνευσης κατάχρησης προσπαθούν να αναγνωρίσουν την κακή συμπεριφορά. Το κύριο μειονέκτημα των προσεγγίσεων της misuse detection είναι ότι μπορούν να ανιχνεύουν μόνο τις επιθέσεις τις οποίες έχουν εκπαιδευτεί να ανιχνεύουν. Νέες ή άγνωστες επιθέσεις ή ακόμα και παραλλαγές γνωστών επιθέσεων δε θα εντοπίζονται. Σε μια εποχή που ελαττώματα ασφάλειας στο λογισμικό ανακαλύπτονται και αξιοποιούνται από αναρμόδιους χρήστες καθημερινά, η αντίδραση που προσφέρουν οι μέθοδοι της misuse detection δεν είναι ικανή να αποτρέψει κακόβουλες ενέργειες. Το κύριο πλεονέκτημα των προσεγγίσεων της anomaly detection είναι η ικανότητα να εντοπίζει καινούριες ή άγνωστες επιθέσεις, παραλλαγές γνωστών επιθέσεων, ακόμα και αποκλίσεις από την κανονική χρήση των προγραμμάτων ανεξάρτητα από το αν η πηγή είναι ένας εξουσιοδοτημένος εσωτερικός χρήστης ή ένας μη εξουσιοδοτημένος εξωτερικός χρήστης. Ωστόσο, το μειονέκτημα των μεθόδων αυτών είναι ότι πολύ γνωστές επιθέσεις πιθανόν να μην ανιχνεύονται, ειδικά αν ταιριάζουν με το καθιερωμένο προφίλ του χρήστη. Από τη στιγμή που θα ανιχνευτεί, συχνά είναι δύσκολο να χαρακτηριστεί η φύση της επίθεσης. Ένα άλλο μειονέκτημα αρκετών

τεχνικών της anomaly detection είναι ότι ένας κακόβουλος χρήστης, που γνωρίζει ότι παρακολουθείται με σκοπό τη δημιουργία του προφίλ του, μπορεί σταδιακά σε μεγάλο βάθος χρόνου να αλλάξει τη συμπεριφορά του προκειμένου να εκπαιδεύσει το σύστημα ανίχνευσης να αναγνωρίζει την κακόβουλη συμπεριφορά ως φυσιολογική. Τέλος, σημαντική αδυναμία τους είναι το υψηλό ποσοστό εσφαλμένων συναγερμών (**false alarm rate**). Αυτό οφείλεται στο γεγονός ότι συμπεριφορές που δεν έχουν παρατηρηθεί παλαιότερα, αν και νόμιμες και φυσιολογικές, μπορούν να αναγνωριστούν ως ανωμαλίες. Τα πλεονεκτήματα και τα μειονεκτήματα των προαναφερθέντων προσεγγίσεων συνοψίζονται στο παρακάτω σχήμα 16.

	Anomaly Detection	**Misuse Detection**
Πλεονεκτήματα	Καινούριες επιθέσεις μπορούν να ανιχνευτούν	Χαμηλότερος ρυθμός false positive
Μειονεκτήματα	Υψηλότερος ρυθμός false positive	Καινούριες επιθέσεις δεν μπορούν να ανιχνευτούν
		Η βάση δεδομένων των επιθέσεων πρέπει να ενημερώνεται σε τακτική βάση

Σχήμα 16. Anomaly και Misuse Detection.

Για κάθε τεχνική υπάρχουν διαφορετικές προσεγγίσεις. Ο διαχειριστής ασφάλειας του δικτύου έχει να αντιμετωπίσει το πρόβλημα της επιλογής ενός κατάλληλου IDS για το συγκεκριμένο υπολογιστικό σύστημα. Η επιλογή αυτή περιπλέκεται από τη διαθεσιμότητα πολλών διαφορετικών προσεγγίσεων. Προκειμένου τα υπολογιστικά συστήματα και δίκτυα, κυβερνητικά ή επιχειρησιακά, να καταστούν στο μέγιστο βαθμό ασφαλή και ανθεκτικά ενάντια στο τεράστιο φάσμα απειλών και ευπαθειών, πρέπει οι δύο παραπάνω μεθοδολογίες να συνδυάζονται και να υλοποιούνται παράλληλα με μηχανισμούς πρόληψης επιθέσεων DoS όπως φαίνεται στο παρακάτω σχήμα 17.



Σχήμα 17. Συνδυασμός τεχνικών για μεγαλύτερη ασφάλεια.

4.2.4 Μοντέλου Ανίχνευσης Διαταραχών Πρωτοκόλλων (Protocol Anomaly Detection)

Η τεχνική αυτή έχει εμφανιστεί τα τελευταία χρόνια στο χώρο των IDSs και στην ουσία είναι μία παραλλαγή της τεχνικής του Anomaly Detection. Η διαφορά τους βρίσκεται στο ότι η Protocol Anomaly Detection ελέγχει την δραστηριότητα του δικτύου όσο αναφορά την σωστή χρήση των πρωτοκόλλων επικοινωνίας και κυρίως εκείνων που ανήκουν στην οικογένεια του TCP/IP. Τα πρωτόκολλα επικοινωνίας είναι σύνολα από αρχές και κανόνες που ορίζουν τον τρόπο με τον οποίο επιτυγχάνεται η επικοινωνία μεταξύ δύο διασυνδεδεμένων συστημάτων. Είναι γεγονός ότι ένα πολύ μεγάλο ποσοστό των επιθέσεων που λαμβάνουν χώρα στο Internet υλοποιούνται με την μη φυσιολογική χρήση των πρωτοκόλλων επικοινωνίας. Η θεωρητική χρήση των πρωτοκόλλων ορίζεται σε επίσημα, ευρέως αποδεκτά έγγραφα τα RFCs (Request For Comments) τα οποία περιγράφουν τα standards, που κάθε πρωτόκολλο πρέπει να ακολουθεί κατά την υλοποίησή του. Οι επιθέσεις που στηρίζονται στην μη φυσιολογική χρήση των πρωτοκόλλων, αποβλέπουν στο γεγονός ότι τέτοιου είδους ενέργειες έχουν παραβλεφθεί από τα RFCs ή στην κακή υλοποίηση και εφαρμογή των κανόνων που περιγράφονται στα RFCs, από διάφορους κατασκευαστές λειτουργικών συστημάτων και λογισμικών γενικότερα. Με την τεχνική του Protocol Anomaly Detection παρακολουθείται και αναλύεται η δραστηριότητα που έχει σχέση με την χρήση των πρωτοκόλλων και ελέγχεται για το αν αυτή συμφωνεί με κάποια patterns τα οποία περιγράφουν την φυσιολογική, νόμιμη χρήση των πρωτοκόλλων. Η δημιουργία των patterns είναι πιο εύκολη υπόθεση σε σχέση με την τεχνική του Anomaly Detection, καθώς σε αυτήν

την περίπτωση τα patterns αποτελούνται από τους προκαθορισμένους κανόνες που περιγράφονται από τα RFCs και όχι από κανόνες που περιγράφουν την φυσιολογική δραστηριότητα ενός δικτύου ή ενός συστήματος που μπορεί να παρουσιάζει πολλές διακυμάνσεις.

Το Protocol Anomaly Detection παρουσιάζει πλεονεκτήματα όπως :

- Μπορεί να εντοπίσει κάποια ασυνήθιστη δραστηριότητα που αφορά μη φυσιολογική χρήση κάποιου πρωτοκόλλου και για αυτό το λόγο μπορεί να ανιχνεύσει συμπτώματα μίας επίθεσης χωρίς να απαιτείται η γνώση λεπτομερειών για αυτή.
- Μπορεί να ανιχνεύσει επιθέσεις που δεν έχουν επαναληφθεί και γενικότερα δεν υπάρχει προηγούμενη γνώση για αυτές.
- Μπορεί να εξάγει πληροφορίες οι οποίες στην συνέχεια να χρησιμοποιηθούν σαν είσοδο σε IDSs που κάνουν χρήση της τεχνικής του Misuse Detection.

Το Protocol Anomaly Detection παρουσιάζει και κάποια μειονεκτήματα όπως :

- Η δημιουργία των patterns δεν μπορεί πάντα να ακολουθεί πιστά στους κανόνες που ορίζονται από τα RFCs, καθώς δεν συμβαίνει το ίδιο και από τα λειτουργικά συστήματα και τα άλλα λογισμικά που κάνουν χρήση των πρωτοκόλλων. Τα patterns που δημιουργούνται πρέπει να λαμβάνουν το γεγονός αυτό υπόψη τους.
- Δεν μπορούν να ανιχνεύσουν επιθέσεις που δεν στηρίζονται στην μη φυσιολογική χρήση των πρωτοκόλλων.
- Όταν ανιχνευτεί μία επίθεση με την τεχνική αυτή, συνήθως δεν προσφέρονται πληροφορίες που να περιγράφουν επαρκώς το είδος της και απαιτείται η συμμετοχή εξειδικευμένων ατόμων που να μπορούν να ερμηνεύσουν τα αποτελέσματα που παράγονται.

4.3 ΚΑΤΗΓΟΡΟΙΟΠΟΙΗΣΗ ΜΕ ΒΑΣΗ ΤΗΝ ΑΠΟΚΡΙΣΗ – ΑΝΤΙΔΡΑΣΗ RESPONSES

Μετά το στάδιο της συλλογής των δεδομένων και της επεξεργασίας τους, τα IDSs πρέπει με κάποιο τρόπο να γνωστοποιήσουν τα αποτελέσματά τους, αναφέροντας τα γεγονότα που υποδεικνύουν πιθανές περιπτώσεις επιθέσεων ή και να δράσουν προς αντιμετώπιση αυτών.
Η λειτουργία αυτή των IDSs είναι πολύ σημαντική, καθώς αυτή θα αποτελέσει την βάση για να ληφθούν τα κατάλληλα μέτρα προστασίας γρήγορα και αποτελεσματικά. Τα είδη των Responses μπορούν να διαχωριστούν σε Active Responses και Passive Responses.

4.3.1 Ενεργές Αντιδράσεις – Active Responses

Τα Active Responses είναι αυτοματοποιημένες ενέργειες που εκτελούνται από τα IDS, όταν ανιχνεύσουν συγκεκριμένους τύπους εισβολών, προκειμένου να τις αντιμετωπίσουν με τον αποτελεσματικότερο τρόπο. Για την αποτελεσματική αντιμετώπιση αυτών των επιθέσεων τα IDS προβαίνουν στις παρακάτω ενέργειες :

- Συλλογή επιπρόσθετων πληροφοριών. Αυτή είναι ίσως η λιγότερο ενεργητική αντίδραση αλλά σε ορισμένες περιπτώσεις η πιο παραγωγική. Η λειτουργία της είναι να συλλεχτούν περισσότερες πληροφορίες για μία πιθανή επίθεση που εντοπίστηκε, οι οποίες θα ξεκαθαρίσουν περισσότερο την κατάσταση, ώστε να ληφθεί η κατάλληλη απόφαση για το αν πρέπει να παρθούν κάποια παραπέρα μέτρα προστασίας. Έτσι κάποιο IDS όταν εντοπίσει μία πιθανή επίθεση, μπορεί για παράδειγμα να αυξήσει το επίπεδο ευαισθησίας των Information Sources που χρησιμοποιεί (πχ. να ρυθμίσει κάποιον Sensor να καταγράφει όλα τα πακέτα ενός δικτύου και όχι αυτά που αφορούν συγκεκριμένα συστήματα ή πόρτες) ή να υπάρξουν "ερωτήσεις" προς το σύστημα από το οποίο εκπορεύεται η επίθεση για να διαπιστωθεί ποιοι χρήστες είναι συνδεδεμένοι κ.α. Με την συλλογή της επιπρόσθετης πληροφορίας γίνεται δυνατό να συλλεχθούν περισσότερα στοιχεία για μία πιθανή επίθεση, τα οποία εξυπηρετούν τόσο στην αποφυγή λανθασμένων συμπερασμάτων

που μπορεί να προκύψουν, όσο και στον εντοπισμό και την ποινική δίωξη του επιτιθέμενου.

- Παρεμπόδιση του επιτιθέμενου. Ένας άλλος τύπος του Active Response, είναι η αναχαίτιση της επίθεσης την ώρα που πραγματοποιείται και στη συνέχεια ή παρεμπόδιση της παραπέρα πρόσβασης του επιτιθέμενου στο προστατευόμενο σύστημα ή δίκτυο ώστε η προσπάθεια του εισβολέα να αποτύχει. Στην ουσία το IDS εμποδίζει τα πακέτα που έχουν IP διεύθυνση, από την οποία φαίνεται ότι προέρχεται ο επιτιθέμενος και όχι τον ίδιο τον επιτιθέμενο προσωπικά. Πολλές φορές αυτό δεν αποτελεί αξιόπιστη λύση, καθώς οι πιο έμπειροι επιτιθέμενοι χρησιμοποιούν ψεύτικες IP διευθύνσεις. Παρόλα αυτά με τέτοιου είδους ενέργειες είναι δυνατό να εμποδιστούν οι πιο αρχάριοι και να αποθαρρυνθούν οι πιο έμπειροι, που υλοποιούν μία επίθεση. Τέτοιες ενέργειες περιλαμβάνουν : την αποστολή πακέτων (με ενεργοποιημένο το RST flag στον TCP header) τα οποία θα τερματίσουν οποιαδήποτε σύνδεση του επιτιθέμενου με το σύστημα – στόχο.

  Την ρύθμιση των routers και των firewall του δικτύου, ώστε να μην επιτρέπουν την διέλευση οποιουδήποτε πακέτου, το οποίο έχει διεύθυνση αποστολέα ή παραλήπτη, την IP διεύθυνση την οποία χρησιμοποιεί ο επιτιθέμενος στα πακέτα που στέλνει.

  Την ρύθμιση των routers και των firewall του δικτύου, ώστε να μην είναι δυνατή η πρόσβαση σε πόρτες, υπηρεσίες και πρωτόκολλα που κάνει χρήση ο επιτιθέμενος.

- Δράση εναντίον του επιτιθέμενου. Υπάρχουν πολλές σκέψεις για το αν είναι σωστό κατά την ανίχνευση μίας επίθεσης να παρθούν μέτρα που συμπεριλαμβάνουν την δράση εναντίον του επιτιθέμενου. Στην πιο ακραία μορφή της αυτή η δράση θα μπορούσε να είναι η υλοποίηση επίθεσης με στόχο τον επιτιθέμενο ή η συλλογή πληροφοριών για το δίκτυό του. Παρόλο που αυτή η αντιμετώπιση μοιάζει αρκετά αποτελεσματική και δίκαιη, κρύβει πολλούς κινδύνους. Κατά πρώτο λόγο αυτού του είδους η δράση μπορεί να είναι παράνομη. Επιπρόσθετα καθώς πολλοί επιτιθέμενοι χρησιμοποιούν ψεύτικες IP διευθύνσεις όταν εξαπολύουν μία επίθεση, τέτοιου είδους δράση θα μπορούσε να προκαλέσει ζημιές σε λάθος χρήστες ή και δίκτυα. Τέλος κάτι τέτοιο θα μπορούσε να προκαλέσει περισσότερο τον επιτιθέμενο και αυτός να αντιδράσει εξαπολύοντας μία επίθεση που θα μπορούσε να έχει καταστροφικά αποτελέσματα. Τέτοιου είδους δράση εναντίον του επιτιθέμενου πρέπει να γίνεται με

πολύ προσοχή και πριν κάποιος αποφασίσει να υιοθετήσει αυτήν την τεχνική, καλό είναι να έχει συμβουλευτεί κάποιον ειδικό για τα νομικά θέματα που προκύπτουν.

4.3.2 Παθητικές Αντιδράσεις – Passive Responses

Τα Passive Responses είναι η μέθοδος με την οποία το IDS απλά προμηθεύει τους αρμόδιους χρήστες, με τις πληροφορίες που αφορούν την ανίχνευση μίας επίθεσης. Στη συνέχεια είναι στην ευθύνη των αρμοδίων να δράσουν κατάλληλα, εκμεταλλευόμενοι τις πληροφορίες αυτές. Αυτού του είδους η αντίδραση είναι και η πιο συνήθης από τα περισσότερα IDSs. Οι παθητικές αντιδράσεις αφορούν ειδοποιήσεις και συναγερμούς. Υπάρχουν διάφοροι τρόποι με τους οποίους μπορεί ένα IDS να γνωστοποιήσει τα αποτελέσματα του στους αρμόδιους χρήστες. Οι κυριότεροι από τους τρόπους αυτούς είναι η ανακοίνωση των Alerts (συναγερμοί) και η χρήση του πρωτοκόλλου SNMP (Simple Network Management Protocol).

- Ανακοίνωση των Alert. Αυτή η τεχνική έχει να κάνει με τον τρόπο που ένα IDS ανακοινώνει και παρουσιάζει στους αρμόδιους χρήστες, τις επισημάνσεις του για μία επίθεση. Μία επισήμανση για την ανίχνευση κάποιας επίθεσης, συνήθως ονομάζεται alert. Τα περισσότερα IDSs δίνουν την δυνατότητα στον χρήστη να καθορίσει με σχετική ευχέρεια, την στιγμή και την μορφή που θα παράγονται τα Alerts και σε ποιους χρήστες θα παρουσιάζονται. Ένα IDS είναι δυνατόν να ρυθμιστεί ώστε τα alerts να εμφανίζονται σε πραγματικό χρόνο, την ώρα που εντοπίζεται μία επίθεση, όπως για παράδειγμα με αναδυόμενα παράθυρα στην οθόνη ή μπορεί να ρυθμιστεί ώστε να καταγράφει τα alerts σε κάποιο αρχείο για μετέπειτα εξέταση. Η μορφή που θα παράγεται ένα alert από το IDS, μπορεί να είναι από μία απλή αναφορά στο είδος της επίθεσης με έναν τίτλο, στον επιτιθέμενο και στο θύμα αυτής, μέχρι και αναλυτική αναφορά που θα περιέχει και πληροφορίες για το πακέτο που οδήγησε στον εντοπισμό της επίθεσης, κάνοντας λεπτομερή περιγραφή του ή αναφορά στο εργαλείο που χρησιμοποιήθηκε για την υλοποίησή της. Επίσης κάποια IDSs έχουν την δυνατότητα να πληροφορούν με alerts απομακρυσμένα τους εξουσιοδοτημένους χρήστες, είτε με αποστολή e-mail σε αυτούς, είτε ακόμα μέσω κλήσεων ή αποστολή γραπτών μηνυμάτων σε κινητά τηλέφωνα που ανήκουν σε αυτούς.

- SNMP και SNMP Traps. Κάποια IDSs έχουν την δυνατότητα να αναφέρουν τα alerts που παράγουν, σε ένα κεντρικό σύστημα διαχείρισης του δικτύου με την χρήση του πρωτοκόλλου SNMP (Simple Network Management Protocol) και των SNMP Traps. Το αρχιτεκτονικό μοντέλο του SNMP βασίζεται σε ένα σταθμό διαχείρισης δικτύου (Network Management Station), ένα σύστημα στο οποίο εκτελείται το SNMP με κατάλληλο λογισμικό διαχείρισης και διάφορα άλλα στοιχεία του δικτύου, όπως εξυπηρετητές (servers), δρομολογητές (routers), σταθμοί εργασίας (hosts), δικτυακές πύλες (gateways), κ.α. Στην βάση πληροφοριών του σταθμού διαχείρισης συγκεντρώνονται όλες οι πληροφορίες που βρίσκονται στις αντίστοιχες βάσεις των δικτυακών συσκευών που αυτός διαχειρίζεται. Αντίστοιχα, σε μια δικτυακή συσκευή το SNMP υλοποιείται από έναν κατάλληλο αντιπρόσωπο διαχείρισης ο οποίος παρέχει πρόσβαση στη βάση διαχείρισης πληροφοριών της συγκεκριμένης συσκευής. Για να υλοποιηθούν οι θεμελιώδεις λειτουργίες του SNMP χρησιμοποιούνται παγίδες (Traps) οι οποίες επιτρέπουν σε έναν agent να αναφέρει ένα γεγονός στο σταθμό διαχείρισης. Έτσι με τον τρόπο αυτό γίνεται η αποστολή σε ένα κεντρικό σύστημα, των alerts που παράγονται από διάφορα IDSs ενός δικτύου, καθώς και άλλων πληροφοριών που εξάγονται από άλλους μηχανισμούς ασφάλειας, όπως Firewalls και είναι δυνατό να γίνει ευκολότερα συσχετισμός μεταξύ των αποτελεσμάτων που έχουν προκύψει από διαφορετικές πηγές και να σχηματιστεί μία πιο σαφής και λεπτομερής εικόνα των γεγονότων.

ΚΕΦΑΛΑΙΟ 5

ΑΣΥΡΜΑΤΑ ΔΙΚΤΥΑ ΚΑΙ ΣΥΣΤΗΜΑΤΑ ΑΝΙΧΝΕΥΣΗΣ ΕΙΣΒΟΛΩΝ

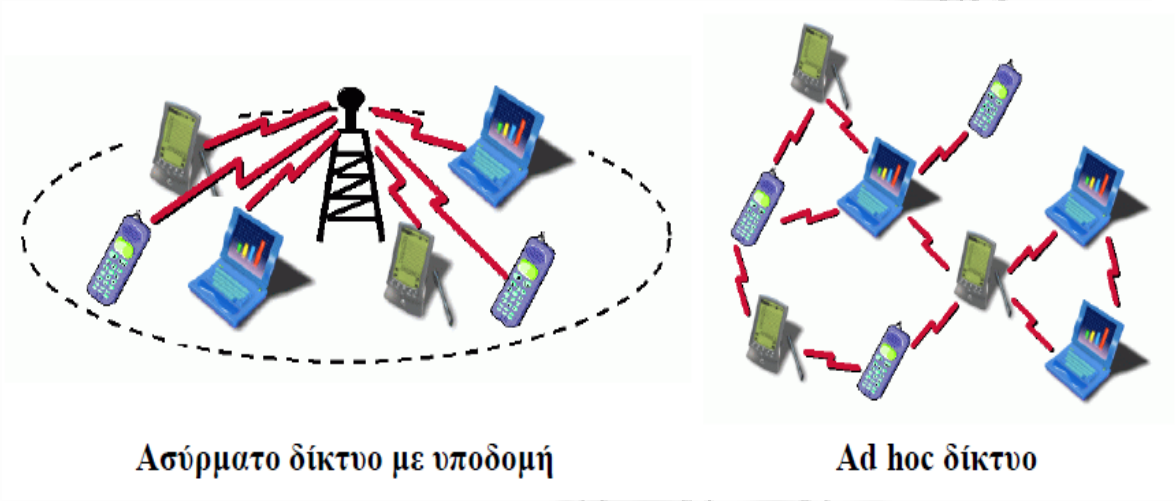
Στα τέλη του 19ου αιώνα, ο G. Marconi υλοποίησε για πρώτη φορά ένα σύστημα ασύρματης μετάδοσης, βασιζόμενος στην θεωρία που είχε διατυπώσει ο Maxwell. Μέχρι το 1940 χρησιμοποιούνταν συνήθως συχνότητες UHF. Από την δεκαετία του ’40 και έπειτα, η αλματώδης ανάπτυξη της πληροφορικής και της ηλεκτρονικής σε συνδυασμό με την αύξηση του όγκου πληροφορίας, έχουν οδηγήσει στην ανάπτυξη νέων τεχνολογιών. Με τον καιρό αναπτύχθηκε ένας μεγάλος αριθμός ασύρματων δικτύων ανάλογα με το σκοπό και τα αντίστοιχα μέσα που διατίθενται για τη δημιουργία τους.

Η ασύρματη τεχνολογία για την δικτύωση υπολογιστών αλλά και άλλων συσκευών αποτελεί μία από τις περισσότερο υποσχόμενες υπάρχουσες τεχνολογίες που είναι σήμερα διαθέσιμες. Το συγκεκριμένο μέσο διασύνδεσης έχει γίνει ιδιαίτερα δημοφιλές και με την υποστήριξη την οποία δέχεται, ίσως αποτελέσει την πιο σημαντική τεχνολογία που αφορά τους ηλεκτρονικούς υπολογιστές στο προσεχές μέλλον. Δυστυχώς, όπως και άλλες νέες τεχνολογίες, έτσι και η ασύρματη δικτύωση αντιμετωπίζει πολλές προκλήσεις, όσον αφορά τον τομέα της ασφάλειας.

5.1 ΠΕΡΙΓΡΑΦΗ ΤΩΝ ΑΣΥΡΜΑΤΩΝ AD HOC ΔΙΚΤΥΩΝ

Η ασύρματη επικοινωνία επιτρέπει τη μεταφορά πληροφοριών μεταξύ ενός δικτύου αποσυνδεδεμένων και συχνά κινητών χρηστών. Τα δημοφιλή ασύρματα δίκτυα, όπως τα δίκτυα κινητής τηλεφωνίας και τα ασύρματα LANs είναι παραδοσιακά βασισμένα σε υποδομή, δηλ. οι σταθμοί βάσεως, τα σημεία πρόσβασης και οι κεντρικοί υπολογιστές (servers) αναπτύσσονται (παίρνουν συγκεκριμένες θέσεις) προτού να μπορέσει να χρησιμοποιηθεί το δίκτυο. Αντίθετα, τα ad hoc δίκτυα, είναι δίκτυα τυχαία διαμορφωμένα

και διαμορφώνονται δυναμικά μεταξύ μιας ομάδας ασύρματων χρηστών χωρίς να απαιτούν καμία υπάρχουσα υποδομή ή προ-διαμόρφωση, όπως φαίνεται στο παρακάτω σχήμα 18.



Σχήμα 18. Ασύρματο δίκτυο με υποδομή και ad hoc δίκτυο.

Αναλυτικά ένα ασύρματο **ad hoc δίκτυο**, είναι ένα ασύρματο δίκτυο όπου οι ασύρματες μονάδες που το αποτελούν (οι οποίες συνήθως είναι και κινητές) δεν χρησιμοποιούν απαραίτητα κάποια προϋπάρχουσα υποδομή (όπως επικοινωνία όλων των συσκευών με κάποιο συγκεκριμένο σημείο πρόσβασης) για την συμμετοχή τους σε αυτό. Οι διασυνδέσεις μεταξύ των κόμβων δεν είναι επίσης σταθερές και μπορεί να αλλάζουν, αφού οι κόμβοι του δικτύου είναι συνήθως κινητοί και όχι σταθεροί. Κάθε κόμβος του δικτύου διαδραματίζει ενεργό ρόλο στην δρομολόγηση των δεδομένων που ανταλλάσσονται, μεταδίδοντας δεδομένα σε άλλους κόμβους του δικτύου, αναλόγως συνήθως με την ποιότητα και την εφικτότητα της σύνδεσης κάθε φορά. Έτσι για παράδειγμα αν κάποιος κόμβος Α θέλει να επικοινωνήσει με κάποιον κόμβο Β, τότε αυτό συνήθως γίνεται με την μεσολάβηση άλλων κόμβων του δικτύου, οι οποίοι δρομολογούν κατάλληλα τα απαιτούμενα δεδομένα.

Η δυναμική και αυτό-οργανωτική φύση των δικτύων ad hoc τα καθιστά ιδιαίτερα χρήσιμα σε καταστάσεις όπου απαιτούνται γρήγορες επεκτάσεις δικτύων ή η επέκταση και διαχείριση της υποδομής των δικτύων είναι απαγορευτικά δαπανηρές. Οι εφαρμογές των ad hoc δικτύων, διαφέρουν ανάλογα με το είδος και την δομή τους. Για παράδειγμα, ίσως τα περισσότερο γνωστά ασύρματα ad hoc δίκτυα είναι τα ασύρματα δίκτυα αισθητήρων (Wireless Sensor Networks – WSN), τα οποία βρίσκουν εφαρμογές σε στρατιωτικές διαδικασίες, σε παρακολούθηση πληθυσμών άγριων ζώων με την τοποθέτηση μικρών συσκευών αισθητήρων, σε νοσοκομειακές εγκαταστάσεις για την παρακολούθηση ασθενών,

κτλ. Όπως ήδη αναφέρθηκε, θεωρούμε ότι οι κόμβοι στα ασύρματα ad hoc δίκτυα είναι κινητοί (mobile) και μπορούν να αλλάζουν θέση κατά την παρουσία τους στο δίκτυο. Τα ασύρματα ad hoc δίκτυα αυτού του είδους ονομάζονται **MANETs (Mobile Ad Hoc Networks)** και είναι αυτά που βρίσκουν τις περισσότερες εφαρμογές και τα οποία κινούν το μεγαλύτερο επιστημονικό ενδιαφέρον σήμερα. Η φύση των ασύρματων ad hoc δικτύων τα καθιστά ελκυστικά αλλά και ιδιαίτερα ευάλωτα σε επιθέσεις. Αυτό συμβαίνει διότι τα MANETs δε διαθέτουν συσκευές όπως δρομολογητές, μεταγωγείς ή πύλες, στις οποίες η εφαρμογή ενός συστήματος ανίχνευσης εισβολών γίνεται εύκολα.

5.2 ΠΡΟΒΛΗΜΑΤΑ ΑΣΦΑΛΕΙΑΣ ΣΤΑ AD HOC ΔΙΚΤΥΑ

Λόγω της ασύρματης φύσης των συνδέσεων, μεταξύ των κόμβων του δικτύου οι επιθέσεις μπορεί να ποικίλουν από υποκλοπή μεταδιδόμενων δεδομένων, μέχρι ενεργό αποστολή (κακόβουλων) δεδομένων στο δίκτυο. Σε αντίθεση με τα ενσύρματα δίκτυα, όπου σε πολλά από αυτά ο επιτιθέμενος ίσως είναι αναγκαίο να έχει μία φυσική παρουσία στον χώρο όπου το δίκτυο είναι εγκατεστημένο, στα ασύρματα δίκτυα η επίθεση μπορεί να γίνει από απόσταση, στοχεύοντας σε οποιονδήποτε από τους κόμβους που το αποτελούν. Αυτό πρακτικά σημαίνει ότι ένα ασύρματο ad hoc δίκτυο δεν έχει μία ξεκάθαρη γραμμή ασφαλείας (όπως π.χ. ένα firewall) αλλά κάθε κόμβος αποτελεί έναν εν δυνάμει στόχο και θα πρέπει να διαθέτει τα μέσα έτσι ώστε να ανταπεξέλθει στις κάθε φορά συνθήκες.

Οι (φορητοί) κόμβοι του δικτύου είναι αυτόνομες οντότητες, οι οποίες έχουν την δυνατότητα να λειτουργούν ανεξάρτητα από τις υπόλοιπες, χωρίς να τις ειδοποιούν για την λειτουργία τους, παρά μόνο κατά την αποστολή μηνυμάτων. Έτσι, αν ο επιτιθέμενος έχει φυσική πρόσβαση στους κόμβους του δικτύου, μπορεί να αντικαταστήσει κάποιον από αυτούς ή ακόμη και να προσθέσει κάποιον παραπάνω. Συνεπώς όλοι οι κόμβοι του δικτύου θα πρέπει να είναι προετοιμασμένοι να λειτουργήσουν σε κάποια λειτουργία όπου δεν μπορούν να εμπιστευθούν έναν ή περισσότερους κόμβους του ασύρματου δικτύου.

Οι αλγόριθμοι δρομολόγησης των μηνυμάτων που χρησιμοποιούνται στα ασύρματα ad hoc δίκτυα είναι αποκεντρωτικοί και στηρίζονται στην συνεργασία μεταξύ των κόμβων του δικτύου. Έτσι η επίθεση σε έναν κόμβο και η ενδεχόμενη μεταβολή του, ίσως παραλύσει ολόκληρο το δίκτυο, αν ο κόμβος αυτός μεταδίδει λάθος μηνύματα δρομολόγησης.

Φυσικά διάφορες τεχνικές κρυπτογράφησης θα μπορούσαν να αντιμετωπίσουν το εν λόγω πρόβλημα (ως ένα μέρος του τουλάχιστον) καθώς και κάποια από τα παραπάνω, αλλά δεν

μπορεί να εξαλείψει το πρόβλημα της ασφάλειας στην ολότητά του. Όπως σε κάθε ασύρματο και ενσύρματο δίκτυο, η κυκλοφορία σε ένα ad hoc δίκτυο είναι ευαίσθητη σε επιθέσεις που αφορούν την ασφάλεια. Για τον λόγο αυτό, με σκοπό να ασφαλίσουμε ένα ad hoc δίκτυο, πρέπει να λάβουμε υπ' όψιν μας όχι μόνο χαρακτηριστικά όπως είναι η διαθεσιμότητα, η εμπιστευτικότητα, η ακεραιότητα και η πιστοποίηση αλλά και τις απειλές τις οποίες επεκτείνονται ακόμη και στην βασική δομή των δικτύων. Τα αξιοπρόσεκτα χαρακτηριστικά των ad hoc δικτύων προσφέρουν τόσο τις προκλήσεις όσο και τις ευκαιρίες στην επίτευξη αυτών των σκοπών. Από την στιγμή που ένα ad hoc δίκτυο κάνει χρήση ασύρματων συνδέσμων γίνεται επιρρεπές σε επιθέσεις μέσω συνδέσμων. Υπάρχουν δύο ειδών επιθέσεις. Οι παθητικές επιθέσεις που αρκούνται στην υποκλοπή των μηνυμάτων και οι ενεργητικές που τροποποιούν και καταστρέφουν μηνύματα, δημιουργούν παρεμβολές και προκαλούν κατάρρευση του συστήματος.

Η ιστορία των δικτύων έχει δείξει ότι τεχνικές πρόληψης επιθέσεων όπως η κρυπτογράφηση (encryption) και η αυθεντικοποίηση (authentication), όπου θεωρούνται συνήθως ως η πρώτη γραμμή άμυνας, από μόνες τους δεν επαρκούν για την αντιμετώπιση των προβλημάτων ασφαλείας που υπάρχουν. Όσο περισσότερο αυξάνεται η πολυπλοκότητα ενός συστήματος, τόσο περισσότερο αυξάνονται και τα κενά ασφαλείας του, γεγονός που το καθιστά περισσότερο ευάλωτο σε επιθέσεις.

Προσφάτως έχουν εξετασθεί οι αδυναμίες και το κατά πόσο είναι ευάλωτο ένα δίκτυο ad hoc. Σύμφωνα με την προσέγγιση των δύο ερευνητών Zhang και Lee, κάθε κόμβος θεωρείται υπεύθυνος για την αναζήτηση σημάτων για τοπικές εισβολές ανεξαρτήτως, αλλά οι γείτονες κόμβοι έχουν την δυνατότητα της συνεργασίας και εξιχνίασης σε ευρύτερο φάσμα. Ιδιαίτεροι παράγοντες συστημάτων ανίχνευσης εισβολών βρίσκονται σε κάθε κόμβο ξεχωριστά. Κάθε τέτοιος παράγοντας συστήματος υπάρχει ανεξάρτητα και παρακολουθεί τοπικές δραστηριότητες, όπως δραστηριότητες συστήματος-χρηστών,δραστηριότητες επικοινωνίας κλπ. Αυτοί οι παράγοντες των συστημάτων αναπτύσσονται συλλεκτικά από το σύστημα, με σκοπό την προστασία του δικτύου ad hoc από εχθρικές επιθέσεις. Αν ένας παράγοντας ενός συστήματος εξιχνίασης εισβολών, διαπιστώσει μια εισβολή από τοπικά σε αυτόν δεδομένα, τότε οι γειτονικοί παράγοντες θα συνεργαστούν για την ανεύρεση ενεργειών εισβολών στην ευρύτερη, του συγκεκριμένου κόμβου, περιοχή. Οι ανταποκρίσεις ανίχνευσης εισβολών προωθούνται, τόσο από το τοπικό σύστημα ανταπόκρισης του παράγοντα του συγκεκριμένου κόμβου, όσο και από ολόκληρο το συνεργαζόμενο σύστημα ανταπόκρισης. Ο τύπος της αντίδρασης, στις εισβολές, εξαρτάται από τον τύπο των πρωτοκόλλων και των εφαρμογών του δικτύου, αλλά και από την πιστότητα των ενδείξεων. Η ασφάλεια για κάθε ad hoc δίκτυο

αποτελεί ένα δύσκολο πρόβλημα που έχουμε να αντιμετωπίσουμε και είναι στενά συνδεδεμένη με πρωτόκολλα διανομής κωδικών κλειδιών τα οποία θα δημιουργήσουν αξιοπιστία σε ένα σύστημα. Για παράδειγμα ένας παράγοντας, κάποιου συστήματος ανίχνευσης εισβολών μπορεί να αποστείλει ένα αίτημα άρσης της πιστοποίησης σε όλους τους κόμβους του δικτύου και να ζητήσει από τους πιο πρόσφατους χρήστες να πιστοποιήσουν για ακόμη μία φορά τους εαυτούς τους. Στην συνέχεια κάνοντας χρήση διαφόρων μηχανισμών εκτός των ορίων, όπως είναι η οπτική επαφή, ζητά από τους πιο πρόσφατους χρήστες να πιστοποιήσουν τους κόμβους με τους οποίους σχετίζονται. Μόνο οι κόμβοι οι οποίοι έχουν επαναπιστοποιηθεί έχουν την δυνατότητα να διαπραγματεύονται καινούρια κανάλια επικοινωνίας, τα οποία στην συνέχεια αναγνωρίζουν κάθε επόμενο σαν γνήσιο. Για τον λόγο αυτό, οι δεσμευμένοι εχθρικοί κόμβοι μπορούν να αποκλειστούν και να γίνουν ακίνδυνοι. Τέλος οι διαχειριστές χρησιμοποιούν μια υπομονάδα ασφαλούς επικοινωνίας στα δικά τους συστήματα ανίχνευσης εισβολών και προωθούν ένα υψηλής πιστότητας κανάλι επικοινωνίας μεταξύ των παραγόντων του συστήματος. Η σχεδίαση ασφαλών κωδικών κλειδιών στα δίκτυα ad hoc αποτελεί ένα μείζον ζήτημα και πρόβλημα συγχρόνως. Η ανταλλαγή των απαραίτητων κλειδιών μπορεί πράγματι να βοηθήσει στην ανάπτυξη κάποιας προσωρινής ασφάλειας μεταξύ των επικοινωνούντων σημείων. Ωστόσο είναι ακόμη ευαίσθητα στις ανθρωποκεντρικές (man in the middle) επιθέσεις οι οποίες είναι πολύ δύσκολο να καταπολεμηθούν σε ένα δίκτυο ad hoc. Προσφάτως οι Zhang και Lee ερμήνευσαν τα ευρισκόμενα δεδομένα ώστε να περιγράψουν για τον κάθε κόμβο τις φυσικές ενημερώσεις πληροφόρησης για την δρομολόγηση. Από την στιγμή που μία δικαιολογημένη αλλαγή στα περί δρομολόγησης, μπορεί βασικά να οφείλεται στις φυσικές κινήσεις των κόμβων ή τις αλλαγές των περιεχομένων του δικτύου, κάθε κινητός κόμβος πρέπει να χρησιμοποιείται με αξιοπιστία πληροφορίας, η οποία πρέπει να είναι έμπιστη. Έχει συμφωνηθεί να γίνεται χρήση της πληροφορίας στις φυσικές κινήσεις των κόμβων και στην αλλαγή ανταπόκρισης στο πλάνο δρομολόγησης σαν βάση της ευρισκόμενης πληροφορίας. Ένα φυσικό προφίλ της ευρισκόμενης αυτής πληροφορίας, συντελεί στον αποτελεσματικό καθορισμό της συσχέτισης των φυσικών κινήσεων των κόμβων και εντοπίζει τις αλλαγές στο σχέδιο δρομολόγησης. Ένας αλγόριθμος ταξινόμησης, χρησιμοποιείται για να ταξινομηθεί και να περιγραφεί η εκτίμηση των αλλαγών που προέρχονται από το κέρδος των αλλαγών στην δρομολόγηση και από το κέρδος των αλλαγών στο πλήθος των αναπηδήσεων (hops) όλων των διαδρομών. Τα πρωτόκολλα δημοσίων κλειδιών και μεθόδων συμμετρικών κλειδιών, είναι επίσης δύσκολα και δίχως υποδομή και έτσι είναι πολύ δύσκολο να καταλάβουμε την χρήση των πρωτοκόλλων που βασίζονται στην πιστοποίηση. Η μεγάλη

συνάθροιση των διανεμόμενων πληροφοριών σε ένα ad hoc δίκτυο επιφέρει άλλους νέους τύπους προβλημάτων ασφαλείας. Πάντως δεν πρέπει να ξεχνάμε ότι πάντα θα υπάρχουν πολλοί διάφοροι τύποι έμπιστων σχέσεων , οι οποίοι είναι δύσκολο να διατηρηθούν μεταξύ των γειτονικών κόμβων σε μια μεγάλη κοινωνία. Η ποιότητα του ελέγχου των υπηρεσιών, πρέπει να χρησιμοποιείται για να προωθεί μια λογική λύση στην διανομή του μεγάλου πλήθους των πληροφοριών σε ένα ad hoc δίκτυο.

Συνοψίζοντας, μπορούμε να πούμε ότι τα ασύρματα ad hoc δίκτυα έχουν κενά ασφαλείας τα οποία δεν μπορούν να προληφθούν εύκολα ή ρεαλιστικά. Έτσι λοιπόν, η χρήση Συστημάτων Εντοπισμού Εισβολέων (Intrusion Detection Systems – IDS) αποτελεί μία ικανοποιητική λύση, η οποία μπορεί να βελτιώσει την ασφάλειά τους έως έναν βαθμό.

5.3 ΚΑΤΗΓΟΡΙΕΣ ΤΩΝ IDS ΣΤΑ ΑΣΥΡΜΑΤΑ AD HOC ΔΙΚΤΥΑ

Η εγκατάσταση ενός IDS λειτουργεί εν δυνάμει ως ένα δεύτερο τείχος ασφαλείας για την προστασία του δικτύου. Ένα Σύστημα Εντοπισμού Εισβολέων (Intrusion Detection System – IDS) είναι ένα λογισμικό το οποίο παρακολουθεί τις δραστηριότητες ενός δικτύου και καταγράφει αυτές που πιθανώς αποτελούν εισβολή για το δίκτυο αυτό. Η χρήση των IDS είναι διαφορετική από αυτή των τειχών ασφαλείας (firewalls). Ένα firewall περιορίζει την πρόσβαση στις συνδέσεις του δικτύου, έτσι ώστε να αποτρέψει μία επίθεση. Ένα IDS ενεργοποιείται όταν μία πιθανή επίθεση έχει ήδη επιτύχει (εάν κάποιος έχει δηλαδή ήδη αποκτήσει πρόσβαση στο δίκτυο) και εκτελεί ενέργειες για να ειδοποιήσει τους υπεύθυνους του δικτύου ή να περιορίσει την επίθεση όσο κατά το δυνατόν περισσότερο. Σε γενικές γραμμές τα IDS χωρίζονται με βάση την λειτουργία τους σε τρεις κατηγορίες :

- **Συστήματα εντοπισμού ανωμαλιών.** Τα συστήματα αυτά αποθηκεύουν, συνήθως με την χρήση κάποιας μεθόδου στατιστικής ανάλυσης, τα προφίλ των χρηστών του συστήματος ή των δραστηριοτήτων που λαμβάνουν χώρο στο σύστημα αυτό. Κατά τακτά χρονικά διαστήματα, το IDS εξετάζει αν κάποιο προφίλ παρεκλίνει πολύ από τα κανονικά. Αν αυτό συμβεί, τότε ίσως κάποια εισβολή είναι σε εξέλιξη. Το μειονέκτημα της συγκεκριμένης τεχνικής είναι ότι τα προφίλ των χρηστών ή δραστηριοτήτων του συστήματος θα πρέπει να ελέγχονται σε περιοδική βάση, κάτι που ίσως έχει επιπρόσθετο κόστος σε μεγάλα και πολύπλοκα συστήματα.

- **Συστήματα εντοπισμού ήδη γνωστών επιθέσεων.** Τα συστήματα αυτά λειτουργούν με τρόπο παρόμοιο αυτού των συστημάτων προστασίας έναντι των ιών (antivirus). Το IDS διατηρεί πρότυπα δεδομένων ήδη γνωστών επιθέσεων και συγκρίνει τα δεδομένα τα οποία συλλέγει από το δίκτυο με τα πρότυπα αυτά. Σε περίπτωση που τα δεδομένα είναι παρόμοια, τότε θεωρεί ότι πραγματοποιείται κάποια επίθεση. Το μειονέκτημα των συστημάτων αυτών είναι ότι δεν μπορούν να εντοπίσουν νέα είδη επιθέσεων, τα οποία δεν είναι ήδη καταγεγραμμένα.

- **Συστήματα βασισμένα σε προδιαγραφές.** Στα συστήματα αυτά ο διαχειριστής εισάγει ένα σύνολο περιορισμών που περιγράφουν την σωστή λειτουργία ενός προγράμματος ή ενός πρωτοκόλλου. Αν κατά την λειτουργία του δικτύου κάποιος από τους περιορισμούς καταρριφθεί ή αρθεί, τότε το σύστημα θεωρεί ότι πραγματοποιείται κάποια επίθεση. Τα συγκεκριμένα συστήματα είναι σε θέση να αντιληφθούν και να καταγράψουν νέα είδη επιθέσεων.

Τα IDS τα οποία προορίζονται για εγκατάσταση και λειτουργία σε ασύρματα δίκτυα, ονομάζονται **WIDS (Wireless Intrusion Detection Systems)**. Σε γενικές γραμμές κάθε WIDS σύστημα το οποίο προορίζεται για χρήση σε ένα ασύρματο ad hoc δίκτυο, θα πρέπει να διαθέτει (ή τουλάχιστον να ικανοποιεί σε έναν ικανοποιητικό βαθμό) δύο χαρακτηριστικά. Τα χαρακτηριστικά αυτά είναι η **αποτελεσματικότητα (effectiveness)** – δηλαδή ο σωστός διαχωρισμός των επιθέσεων από τις κανονικές δραστηριότητες του συστήματος – και η **αποδοτικότητα (efficiency)** – δηλαδή η λειτουργία του με όσο το δυνατό λιγότερο κόστος, δεδομένης της φύσης των κόμβων των ad hoc δικτύων. Οι προδιαγραφές ενός ιδανικού WIDS είναι σε γενικές γραμμές οι παρακάτω :

- Το WIDS δεν θα πρέπει να εισάγει κάποιο νέο κενό ασφαλείας στο ασύρματο δίκτυο. Στην ουσία δηλαδή δεν θα πρέπει να κάνει έναν οποιοδήποτε κόμβο του δικτύου περισσότερο ευάλωτο απ’ ότι είναι ήδη.

- Το WIDS θα πρέπει να λειτουργεί συνεχώς, παράλληλα με την λειτουργία του ασύρματου δικτύου και να μην είναι ορατό στους χρήστες του δικτύου ή στις δραστηριότητές του.

- Το WIDS θα πρέπει να αντιδρά κατάλληλα σε περίπτωση επίθεσης. Αυτό πρακτικά σημαίνει ότι δεν θα πρέπει απλά να αναγνωρίζει την επίθεση αλλά είναι επιθυμητό και να προβαίνει σε κατάλληλες ενέργειες, προσπαθώντας ενδεχομένως να την αποτρέψει ή να την περιορίσει χωρίς την μεσολάβηση του χρήστη.

- Το WIDS θα πρέπει να είναι αυτόνομο, να μην σπαταλά πολλούς από τους πόρους των κόμβων στους οποίους εκτελείται και να μπορεί να προστατεύεται από ενδεχόμενες επιθέσεις σε αυτό.

Ενώ στα ενσύρματα δίκτυα τα IDS μπορούν να εγκατασταθούν σε κεντρικές συσκευές του δικτύου, όπως οι δρομολογητές ή οι μεταγωγείς, στα ασύρματα ad hoc δίκτυα δεν υπάρχει η εν λόγω δυνατότητα, αφού αυτά έχουν αποκεντρωτικό χαρακτήρα. Επίσης δεν υπάρχει κάποιος σαφής διαχωρισμός για την συνηθισμένη ή μη συμπεριφορά μιας δραστηριότητας, αφού λόγω της φύσης του δικτύου, κάποιος κόμβος μπορεί να αντιμετωπίσει κάποιο πρόβλημα, το οποίο δεν έχει καμία σχέση με κάποια επίθεση (π.χ. να βγει εκτός εύρους επικοινωνίας με κάποιους από τους γειτονικούς του κόμβους) και να μεταβιβάζει λανθασμένες πληροφορίες δρομολόγησης στους κόμβους που επικοινωνεί. Πολλά είναι τα WIDS τα οποία έχουν προταθεί κατά καιρούς, έτσι ώστε να ταιριάζουν καλύτερα στα διαφορετικά χαρακτηριστικά των ασύρματων ad hoc δικτύων. Θα εξετάσουμε τις περισσότερο σημαντικές αρχιτεκτονικές αυτών στην επόμενη ενότητα.

5.4 ΒΑΣΙΚΕΣ ΑΡΧΙΤΕΚΤΟΝΙΚΕΣ ΤΩΝ WIDS ΣΤΑ ΑΣΥΡΜΑΤΑ AD HOC ΔΙΚΤΥΑ

Οι αρχιτεκτονικές των ασύρματων ad hoc δικτύων είναι δυνατό να ποικίλουν από επίπεδες αρχιτεκτονικές (flat) μέχρι αρχιτεκτονικές πολλών επιπέδων (multi-layered). Έτσι λοιπόν η βέλτιστη αρχιτεκτονική ενός WIDS για την εφαρμογή του σε ένα τέτοιο δίκτυο, ίσως εξαρτάται σε μεγάλο βαθμό από την αρχιτεκτονική του ίδιου του δικτύου. Σε ένα επίπεδο ασύρματο δίκτυο, όλοι οι κόμβοι του δικτύου θεωρούνται ίσοι και η συγκεκριμένη αρχιτεκτονική ίσως είναι κατάλληλη για εφαρμογές εικονικών αιθουσών και εξ αποστάσεως εκπαίδευσης. Σε αντίθεση, σε ένα δίκτυο αρχιτεκτονικής πολλών επιπέδων, κάποιοι κόμβοι θεωρούνται διαφορετικοί από κάποιους άλλους. Έτσι για παράδειγμα οι κόμβοι μπορεί να

χωρίζονται σε **συστάδες (clusters)** κι ένας κόμβος έχει τον ρόλο του κόμβου - διαχειριστή (clusterhead) για την κάθε συστάδα. Η επικοινωνία μεταξύ των κόμβων της ίδιας συστάδας μπορεί να γίνεται ελεύθερα, αλλά η επικοινωνία μεταξύ κόμβων διαφορετικών συστάδων γίνεται μεταξύ των κόμβων - διαχειριστών. Η αρχιτεκτονική αυτή είναι ιδιαίτερα χρήσιμη σε στρατιωτικού τύπου εφαρμογές.

Οι βασικότερες αρχιτεκτονικές των WIDS για τα ασύρματα ad hoc δίκτυα, είναι σε γενικές γραμμές οι παρακάτω :

- **Απομονωμένα IDS (Stand-Alone IDS):** το σύστημα εγκαθίσταται σε κάθε κόμβο του δικτύου και οι κόμβοι δεν ανταλλάσουν πληροφορίες μεταξύ τους.

- **Συνεργατικά IDS (Cooperative IDS):** το σύστημα εγκαθίσταται σε όλους τους κόμβους του δικτύου. Οι κόμβοι συνεργάζονται μεταξύ τους στην περίπτωση μιας εκτεταμένης επίθεσης στο δίκτυο.

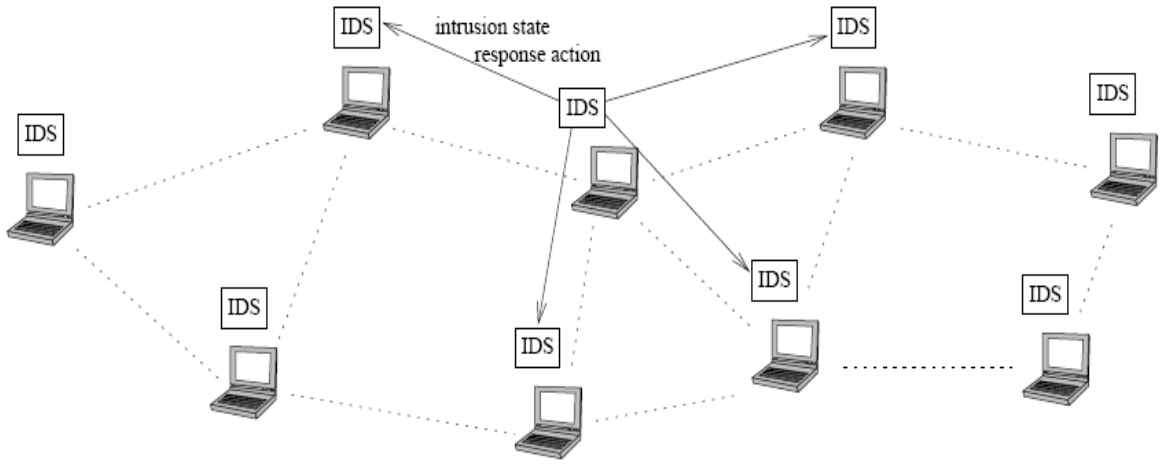
- **Ιεραρχικά IDS (Hierarchical IDS):** αποτελεί γενίκευση των συνεργατικών IDS και εφαρμόζονται σε ασύρματα ad hoc δίκτυα που ακολουθούν την αρχιτεκτονική των συστάδων.

- **IDS Κινητών Πρακτόρων (Mobile Agent IDS):** σύμφωνα με την αρχιτεκτονική αυτή, κινητοί πράκτορες (δηλαδή λογισμικό που έχει την δυνατότητα μεταφοράς από έναν κόμβο του δικτύου σε άλλον) τοποθετούνται αρχικά σε έναν ή περισσότερους κόμβους του δικτύου και στην συνέχεια συγκεντρώνουν τις πληροφορίες που μάζεψαν για την εξαγωγή κάποιου συμπεράσματος.

Από τις παραπάνω αρχιτεκτονικές, οι περισσότερο σημαντικές είναι αυτές των συνεργατικών και των ιεραρχικών IDS.

5.4.1 Συνεργατικά IDS (Cooperative IDS)

Τα συνεργατικά IDS είναι ίσως η αρχιτεκτονική η οποία ταιριάζει καλύτερα στην επίπεδη δομή των ασύρματων ad hoc δικτύων. Σε ένα συνεργατικό IDS, ο κάθε κόμβος του ασύρματου δικτύου συμμετέχει ενεργά στην όλη διαδικασία εντοπισμού μιας επίθεσης, αφού το IDS εγκαθίσταται σε κάθε κόμβο, όπως παρουσιάζεται και στο παρακάτω σχήμα 19.



Σχήμα 19. Δομή ενός συνεργατικού IDS.

Αφού ο κάθε κόμβος του δικτύου θεωρείται ισότιμος, στις περισσότερες περιπτώσεις, το λογισμικό το οποίο εγκαθίσταται σε κάθε κόμβο, πραγματοποιεί ακριβώς την ίδια λειτουργία. Το IDS σε κάθε κόμβο είναι υπεύθυνο για την συλλογή δεδομένων που είναι απαραίτητα για τον εντοπισμό τοπικών επιθέσεων (δηλαδή επιθέσεων στον εν λόγω κόμβο ή σε γειτονικούς του) που πιθανώς να συμβούν. Αν είναι απαραίτητες περισσότερες πληροφορίες για τον εντοπισμό μιας επίθεσης, τότε οι γειτονικοί κόμβοι συμμετέχουν κι αυτοί συνεργατικά για την εξαγωγή κάποιου συμπεράσματος. Η σημαντικότερη πρόκληση για τέτοιου είδους IDS, είναι η ασφαλής μεταφορά των δεδομένων μεταξύ των κόμβων του δικτύου. Μία από τις πιο σημαντικές μελέτες πάνω στον τομέα των συνεργατικών IDS, είναι αυτή των Zhang και Lee, όπου κάθε κόμβος είναι βέβαιος ότι έχει πραγματοποιηθεί κάποια επίθεση, βάση κάποιου ποσοστού (πιθανότητας). Αν το ποσοστό αυτό γίνει αρκετά υψηλό σε έναν κόμβο, τότε αυτός ειδοποιεί τους γειτονικούς του, οι οποίοι με την σειρά τους ελέγχουν το δικό τους ποσοστό και η διαδικασία αυτή επεκτείνεται σε όλους τους κόμβους του ασύρματου ad hoc δικτύου, έτσι ώστε να εξαχθεί ένα τελικό συμπέρασμα και να πραγματοποιηθούν οι κατάλληλες ενέργειες σε περίπτωση επίθεσης.

Τα πλεονεκτήματα των συνεργατικών IDS έγκεινται κυρίως στην ομοιότητα της λειτουργίας τους με την λειτουργία του ασύρματου ad hoc δικτύου. Η συγκεκριμένη αρχιτεκτονική είναι σε θέση να αντιμετωπίσει μεμονωμένες τοπικές επιθέσεις, χωρίς να απασχολήσει όλους τους κόμβους του δικτύου, καθώς και γενικευμένες επιθέσεις, ενεργοποιώντας διαδοχικά ολόκληρο το δίκτυο. Από την άλλη, η συγκεκριμένη αρχιτεκτονική παρουσιάζει κι ορισμένα μειονεκτήματα.

Ένα από τα μειονεκτήματα αυτά, είναι ότι θεωρεί ότι όλοι οι κόμβοι του ασύρματου ad hoc δικτύου είναι ισότιμοι και συνεπώς έχουν τις ίδιες υπολογιστικές ικανότητες. Αυτό φυσικά δεν είναι πάντοτε εφικτό, αφού η ανάλυση των δεδομένων που συλλέγονται μπορεί να έχει μεγαλύτερο κόστος σε κάποιους κόμβους απ' ότι σε κάποιους άλλους. Έτσι για παράδειγμα κάποιος επιτιθέμενος που γνωρίζει εκ των προτέρων την αρχιτεκτονική του δικτύου, ίσως επιλέξει να επιτεθεί αρχικά σε κάποιον από τους λιγότερο υπολογιστικά ικανούς κόμβους του δικτύου, κερδίζοντας έτσι πολύτιμο χρόνο για την εκδήλωση της επίθεσης. Ένα άλλο επίσης σημαντικό μειονέκτημα, είναι η πιθανή δυσκολία διάδοσης της απειλής, όταν το δίκτυο είναι μεγάλο σε μέγεθος. Αν το δίκτυο αποτελείται από πολλούς (π.χ. εκατοντάδες κόμβους), η επικοινωνία μεταξύ των γειτονικών κόμβων ίσως είναι περιορισμένη σε ταχύτητα, είτε για λόγους περιορισμένης υπολογιστικής δύναμης ορισμένων κόμβων, είτε γιατί ο επιτιθέμενος έχει θέσει κάποιους κόμβους εκτός λειτουργίας, είτε επειδή οι ασύρματες συνδέσεις μεταξύ των κόμβων δεν είναι γρήγορες ή αξιόπιστες, κτλ.

5.4.2 Ιεραρχικά IDS (Hierarchical IDS)

Οι ιεραρχικές αρχιτεκτονικές των IDS επεκτείνουν τις συνεργατικές αρχιτεκτονικές και έχουν προταθεί κυρίως για ασύρματα ad hoc δίκτυα πολλών επιπέδων. Σε ένα τέτοιο σύστημα, συνήθως οι κόμβοι - διαχειριστές (clusterheads) της κάθε συστάδας (cluster), αναλαμβάνουν περισσότερες λειτουργίες από τις λειτουργίες των υπόλοιπων κόμβων της συστάδας. Μπορούμε να πούμε ότι οι κόμβοι - διαχειριστές διαδραματίζουν λειτουργία παρόμοια με αυτή των δρομολογητών και των μεταγωγέων σε ένα ενσύρματο δίκτυο.

Η λειτουργία ενός ιεραρχικού IDS είναι η εξής : αρχικά το IDS εγκαθίσταται σε κάθε κόμβο του δικτύου, αλλά με διαφορετική λειτουργικότητα στους κόμβους - διαχειριστές από τους απλούς κόμβους μιας συστάδας. Οι απλοί κόμβοι μιας συστάδας είναι υπεύθυνοι για την συλλογή τοπικών πληροφοριών. Σε περίπτωση που αντιληφθούν πιθανή επίθεση, προσπαθούν να την αντιμετωπίσουν, ενώ ταυτόχρονα ειδοποιούν τον κόμβο - διαχειριστή της

συστάδας τους. Οι κόμβοι - διαχειριστές των συστάδων, είναι καταρχάς υπεύθυνοι για την συλλογή τοπικών πληροφοριών, αλλά και για την ειδοποίηση των κόμβων της συστάδας τους στην περίπτωση μιας επίθεσης μεγάλης κλίμακας, την οποία μπορούν να αντιληφθούν, είτε επικοινωνώντας με τους κόμβους - διαχειριστές άλλων συστάδων, είτε λαμβάνοντας πολλές πληροφορίες για επιθέσεις από τους κόμβους της συστάδας τους. Φυσικά, οι συστάδες θα μπορούσαν να διαχωριστούν και σε μικρότερες υπό-συστάδες, οι οποίες θα είχαν μία παρόμοια ιεραρχία με αυτή που παρουσιάστηκε. Έτσι λοιπόν, με την θεώρηση αυτή, δημιουργείται ένα νοητό δέντρο ιεραρχίας, όπου εκτός των φύλλων, κάθε κόμβος αποτελεί τον κόμβο - διαχειριστή των οποίων είναι πρόγονος.

Το κύριο πλεονέκτημα των ιεραρχικών IDS είναι ότι μπορούν να εφαρμοστούν σε ασύρματα δίκτυα μεγάλου μεγέθους και εύρους. Τα ιεραρχικά IDS επίσης αξιοποιούν όσο είναι δυνατόν καλύτερα τους κόμβους του δικτύου, αφού σε γενικές γραμμές οι κόμβοι που βρίσκονται σε χαμηλότερα επίπεδα πραγματοποιούν λιγότερες υπολογιστικές ενέργειες από τους κόμβους που βρίσκονται σε υψηλότερα. Με τον τρόπο αυτό, οι κόμβοι - διαχειριστές της κάθε συστάδας αναλαμβάνουν συνήθως την ανάλυση των δεδομένων (π.χ. υλοποιώντας κάποιον αλγόριθμο εντοπισμού ανωμαλιών), απορροφώντας έτσι το μεγαλύτερο μέρος της υπολογιστικής διαδικασίας.

Όσον αφορά τα μειονεκτήματα των ιεραρχικών IDS, αυτά οφείλονται κυρίως στην ίδια την ιεραρχική δομή του συστήματος. Αν ο επιτιθέμενος καταφέρει και θέσει εκτός λειτουργίας τον κόμβο - διαχειριστή μιας συστάδας, τότε στην ουσία έχει αποσυντονίσει την όλη διαδικασία αναγνώρισης και αντιμετώπισης της επίθεσης. Ένα επίσης σημαντικό μειονέκτημα, το οποίο οφείλεται κι αυτό στην ιεραρχική δομή του IDS, είναι ότι η επίθεση ακόμη και σε ορισμένους κόμβους που δεν είναι σημαντικοί ίσως δημιουργήσει προβλήματα στην μετάδοση των πληροφοριών προς τους κόμβους των παραπάνω επιπέδων, οι οποίοι είναι και οι περισσότερο σημαντικοί για την λήψη αποφάσεων και τον καθορισμό της γενικής στρατηγικής για την αντιμετώπιση της επίθεσης.

ΚΕΦΑΛΑΙΟ 6

ΑΝΑΦΟΡΑ ΣΕ ΠΡΟΙΟΝΤΑ - ΕΡΓΑΛΕΙΑ ΑΝΙΧΝΕΥΣΗΣ ΕΙΣΒΟΛΩΝ

Παράλληλα με την ραγδαία ανάπτυξη των πληροφοριακών συστημάτων σε διάφορους τομείς ραγδαία ήταν και η ανάπτυξη τρόπων και μεθόδων από κακόβουλους χρήστες με σκοπό να πλήξουν συστήματα – στόχους. Έτσι γρήγορα έγινε αντιληπτό ότι τα υπολογιστικά σύστημα παρουσιάζουν και τρωτά σημεία τα οποία έπρεπε να διορθωθούν. Τα τελευταία 20 χρόνια η έρευνα για την ανάπτυξη συστημάτων ανίχνευσης εισβολών είχε σαν αποτέλεσμα την δημιουργία αρκετών τέτοιων βιώσιμων συστημάτων. Αρκετά από αυτά υπήρξαν και προσοδοφόρα εμπορικά εγχειρήματα αφού εταιρείες - χρήστες υπολογιστικών συστημάτων κατάλαβαν την ανάγκη για θωράκιση των συστημάτων τους από διάφορες απειλές. Κάποια από αυτά τα εργαλεία που κυκλοφορούν στην αγορά αναφέρονται παρακάτω.

6.1 TRPIPWIRE

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). Σήμερα συνεχίζει να αναπτύσσεται ως ένα πακέτο από την εταιρεία Tripwire Security Systems. 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 των δεδομένων του συστήματος. 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. 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 άλλα 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.

Το Tripwire διαφέρει από άλλα Συστήματα Ανίχνευσης Εισβολών (Intrusion Detection Systems) στο ότι δεν βασίζεται στην διαρκή ενημέρωσή του με τις ‘‘γνωστές’’ μεθόδους (υπογραφές επίθεσης) των Εισβολών, αλλά επικεντρώνεται στην παρακολούθηση του προσδιορισμένου συστήματος. Δεν ενδιαφέρεται για το ‘‘πώς’’ συνέβη μια συγκεκριμένη επίθεση, αλλά για το ότι πραγματικά έλαβε χώρα. Ανιχνεύει όλους τους τύπους των ανωμαλιών, από κακοήθεις εξωτερικές επιθέσεις έως την καταστροφή αρχείων. Έτσι , εφόσον το Tripwire ανιχνεύει κάθε μετατροπή σε αρχείο, κατάλογο, κλειδί μητρώου, θα αναγνωρίσει και νέες άγνωστες επιθέσεις ή ιούς και τεχνολογία που δεν ανιχνεύονται από Firewalls ή αλλά συστήματα ανίχνευσης εισβολών. Μεριμνά επίσης για την προστασία των δικών του αρχείων. Πιο συγκεκριμένα κωδικοποιεί και υπογράφει τα αρχεία πολιτικής, διαρρύθμισης, βάσης δεδομένων και προαιρετικά αρχεία αναφορών χρησιμοποιώντας τον συμμετρικό κρυπτογραφικό αλγόριθμο El Gamal με 1024-bit κλειδιά. Υπογράφοντας έτσι

ένα αρχείο κατά αυτό τον τρόπο το κάνει υπολογιστικά ανέφικτο για έναν εισβολέα να μεταβάλλει το αρχείο χωρίς να αναγνωρισθεί το αρχείο ως άκυρο από το Tripwire.

Το Tripwire πρώτα εξετάζει (scans) τον υπολογιστή και κατόπιν δημιουργεί μια baseline βάση δεδομένων του συστήματος αρχείων, ένα δηλαδή περιεκτικό ψηφιακό στιγμιότυπο του συστήματος σε μια γνωστή ασφαλή κατάσταση. Ο χρήστης μπορεί να κάνει μια πολύ ακριβή διαρρύθμιση του εργαλείου, υποδεικνύοντας μεμονωμένα αρχεία και καταλόγους προς παρακολούθηση σε συγκεκριμένα μηχανήματα. Το Tripwire μπορεί εν συνεχεία να καθορίσει χωρίς αμφιβολία εάν ένα προστατευμένο αρχείο έχει μεταβληθεί κατά τρόπο που παραβιάζει την πολιτική ασφάλειας που έχει καταστρωθεί από τον διαχειριστή του συστήματος. Το Tripwire έρχεται με ένα default αρχείο πολιτικής (policy file) για κάθε συγκεκριμένη λειτουργική πλατφόρμα. Αυτό το αρχείο πολιτικής είναι σχεδιασμένο να παρακολουθεί συγκεκριμένα αρχεία ανάλογα με το λειτουργικό σύστημα. Παρόλα αυτά ο χρήστης μπορεί εύκολα να επιλέξει αυτός ποια αρχεία θέλει να παρακολουθεί στον συγκεκριμένο υπολογιστή. Μετά από ένα έλεγχο ακεραιότητας, το Tripwire θα συγκρίνει τα ευρήματα του με την baseline βάση δεδομένων που έχει ήδη δημιουργήσει, και αν τυχόν υπάρχουν διαφορές, παράγεται μια αναφορά παραβίασης (violation report) που αναλύει λεπτομερειακά τις συγκεκριμένες αλλαγές που επιφέρει κάθε παραβίαση. Αυτές οι αναφορές μπορούν να σταλούν με e-mail στο διαχειριστή του συστήματος για επισκόπηση ή μπορούν να παρατηρηθούν τοπικά στη μηχανή-στόχο. Εάν όμως η παραβίαση στην ουσία ήταν μια εξουσιοδοτημένη αλλαγή, όπως η εγκατάσταση μίας νέας εφαρμογής ή μίας αναβάθμισης, τότε το Tripwire ενημερώνει τις αλλαγές στην βάση δεδομένων έτσι ώστε να μην εμφανίζονται στις αναφορές ως παραβιάσεις. Οι χρήστες έχουν επιλογή να εκτελούν το πρόγραμμα μια φορά την ημέρα σε ώρες μη αιχμής για να ολοκληρώσουν ένα πλήρη έλεγχο ακεραιότητας, ή μπορούν να το εκτελούν σε επιλεγμένα σημαντικά αρχεία κάθε λίγες ώρες για επιβεβαίωση της ακεραιότητας των δεδομένων και κατόπιν να εκτελέσουν ένα πλήρη έλεγχο του αρχείου συστήματος μια φορά την ημέρα.

Οι περιορισμοί από την χρήση του Tripwire σε ένα σύστημα είναι κυρίως ότι δεν μπορεί να γίνει οποιαδήποτε εγκατάσταση νέου λογισμικού ή αναβάθμιση υπάρχοντος λογισμικού, ή μεταβολή σε κάποιο κρίσιμο αρχείο του συστήματος χωρίς εξουσιοδότηση από τον διαχειριστή του συστήματος.

6.2 COPS

Το πακέτο λογισμικού COPS (Computer Oracle and Password System) προέρχεται από το Πανεπιστήμιο του Perdue. 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.

Είναι ένα ελεύθερα διαθέσιμο σύνολο προγραμμάτων τα οποία ελέγχουν ποικίλες προβληματικές περιοχές της ασφάλειας ενός συστήματος UNIX.

Δεν διορθώνει αλλά απλά αναφέρει πιθανά ρήγματα ασφαλείας (security holes). 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
- Δυνατότητα έγγραφης στους αρχικούς καταλόγους των χρηστών και στα αρχεία εκκίνησης (.profile, .cshrc κλπ.)
- Ρύθμιση ανώνυμου ftp

Τα προγράμματα που συνιστούν το COPS ήταν αρχικά γραμμένα σε φλοιό Bourne (με την χρήση awk, sed, grep, κτλ) για μέγιστη μεταφερσιμότητα σε αλλά συστήματα, ευελιξία και αναγνωσιμότητα, με λίγες γραμμές κώδικα σε γλώσσα C για μεγαλύτερη ταχύτητα. Το ολόκληρο σύστημα τρέχει πάντως στις περισσότερες, μηχανές με BSD και System V. Επιπρόσθετα, περιλαμβάνεται και μια έκδοση σε Perl, η οποία μπορεί να μην είναι τόσο φορητή όσο η έκδοση Bourne/C, αλλά έχει κάποια πλεονεκτήματα. Το COPS κατασκευάστηκε με τέτοιο τρόπο ώστε νέα εργαλεία να μπορούν να προστεθούν ή υπάρχοντα εργαλεία να μεταβληθούν ώστε να ανταποκρίνονται στις ανάγκες ασφάλειας του συστήματος στο οποίο έχει εγκατασταθεί. Το COPS περιλαμβάνει επίσης κάποια προγράμματα υποστήριξης. Το κυριότερο είναι το CARP (COPS Analysis and Report Program). Το CARP είναι ένας διερμηνευτής αποτελεσμάτων που είναι σχεδιασμένος να αναλύει και να παράγει μια περίληψη για τις διάφορες αναφορές του COPS από ένα πλήρες δίκτυο ή σύνολο υπολογιστών. Είναι έτσι σχεδιασμένο ώστε να μην μπορεί να χρησιμοποιηθεί από κακόβουλους χρήστες και εισβολείς με σκοπό να εκμεταλλευθούν (exploit) τις αδυναμίες του συστήματος. Για αυτό τον σκοπό δεν προχωρά στην εκτέλεση μετατροπών στο σύστημα προσπαθώντας να διορθώσει προβλήματα, ούτε περιγράφει την πιθανή αιτία των αδυναμιών του συστήματος και τις πληροφορίες οι οποίες θα μπορούσαν να

χρησιμοποιηθούν για κάποια επίθεση στο σύστημα. Επίσης, δεν περιλαμβάνει εργαλεία τα οποία θα μπορούσαν να δώσουν κάποιο στρατηγικό πλεονέκτημα σε επίδοξους εισβολείς. Το εργαλείο έλεγχου συνθηματικών που διαθέτει π.χ. έχει έναν τόσο απλό αλγόριθμο, ο οποίος ήδη βρίσκεται στις βιβλιοθήκες του συστήματος.

Το COPS είναι δομημένο σαν μια συλλογή από υποπρογράμματα τα οποία καλούνται από κάποιο script του φλοιού. Το script του ανώτερου επιπέδου (toplevel script) συλλέγει τις εξόδους από τα υποπρογράμματα και είτε στέλνει ένα mail με τις σχετικές πληροφορίες στον διαχειριστή του συστήματος είτε δημιουργεί ένα αρχείο (επιλεγμένο από τον χρήστη) με τα προβλήματα που βρήκε κατά την λειτουργία του στο σύστημα. Όλα τα προγράμματα του COPS μονάχα ενημερώνουν τον χρήστη για κάποιο πιθανό πρόβλημα. Δεν προσπαθούν να διορθώσουν και σε καμία περίπτωση να εκμεταλλευτούν οποιοδήποτε από τα προβλήματα που ανιχνεύουν. Επειδή το COPS δεν διορθώνει πιθανούς κινδύνους που βρίσκει, δεν χρειάζεται να εκτελεστεί από κάποιον λογαριασμό με αυξημένα δικαιώματα (privileges), όπως από τον root. Ο μόνος έλεγχος ασφάλειας που πρέπει να γίνεται από το root για βέλτιστα αποτελέσματα και επειδή απαιτεί αρκετό χρόνο, είναι ο έλεγχος των αρχείων SUID, προκειμένου να βρεθούν όλα τα παρόμοια αρχεία στο σύστημα.

Το COPS δεν μπορεί να χρησιμοποιηθεί ώστε να ελέγχει έναν υπολογιστή από μακριά, καθώς όλα τα τεστ και οι έλεγχοι που γίνονται απαιτούν ένα φλοιό που πρέπει να βρίσκεται πάνω στον υπολογιστή που εξετάζεται. Δεν διορθώνει τα λάθη και τα προβλήματα που ανιχνεύει στην ασφάλεια του συστήματος για διάφορους λόγους, ο κυριότερος εκ των οποίων είναι ότι η ασφάλεια των υπολογιστικών συστημάτων δεν είναι κάτι σταθερό.

6.3 SATAN

Το SATAN (Security Analysis Tool for Auditing Networks) σχεδιάστηκε και κατασκευάστηκε το 1995 από τους Dan Farmer και Wietse Venema. Η διαφορά 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 ελέγχου 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. Μπορεί κατόπιν είτε να αναφέρει τα δεδομένα αυτά ή να χρησιμοποιήσει ένα rule-based σύστημα για να ανακαλύψει πιθανά προβλήματα ασφάλειας. 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 συστήματός 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.

Το SATAN έχει μια έκτατη αρχιτεκτονική. Στο κέντρο βρίσκεται ένας σχετικά μικρός γενικός πυρήνας ο οποίος γνωρίζει ελάχιστα έως καθόλου για τύπους συστημάτων, ονόματα υπηρεσιών δικτύου, αδυναμίες ή άλλες λεπτομέρειες. Η γνώση για τις λεπτομέρειες των υπηρεσιών δικτύου, των τύπων συστημάτων κτλ. είναι δομημένη σε μικρά αφιερωμένα εργαλεία συλλογής δεδομένων και βάσεις κανόνων (rule bases). Η συμπεριφορά του SATAN ελέγχεται από ένα configuration file. Οι ρυθμίσεις μπορούν να αλλάξουν είτε μέσω επιλογών της γραμμής εντολών είτε μέσα από ένα hypertext-type σύστημα διεπαφής με τον χρήστη.

Το SATAN έχει ένα πρόγραμμα απόκτησης πληροφοριών για ένα στόχο (target) το οποίο χρησιμοποιεί την εντολή fping για να προσδιορίσει εάν ένας υπολογιστής ή ένα σύνολο υπολογιστών σε ένα υπό-δίκτυο είναι ζωντανοί (alive). Κατόπιν περνάει την λίστα με τους υπολογιστές σε μια μηχανή η οποία οδηγεί την συλλογή δεδομένων και τον κύριο βρόγχο επανατροφοδότησης. Κάθε υπολογιστής εξετάζεται εάν έχει ελεγχθεί νωρίτερα, και αν όχι, ένα σύνολο από τεστ τρέχει πάνω του (το σετ των τεστ εξαρτάται από την απόσταση στην οποία βρίσκεται ο υπολογιστής από την αρχική μηχανή και το επίπεδο εξέτασης που έχει ορισθεί). Τα τεστ δημιουργούν μια εγγραφή δεδομένων που περιλαμβάνει το όνομα του υπολογιστή, τα τεστ που έτρεξαν σε αυτόν, και τα αποτελέσματα που προέκυψαν από τον έλεγχο. Τα δεδομένα αυτά κατόπιν σώζονται σε ένα αρχείο για περαιτέρω ανάλυση. Το υποσύστημα της διεπαφής με τον χρήστη χρησιμοποιεί HTML για να συνδέσει και να

παρουσιάσει με τρόπο κατανοητό και ευανάγνωστο προς τον χρήστη τα τεράστια ποσά δεδομένων σαν αποτελέσματα. Οι hacker συστημάτων, πιθανοί εισβολείς ή οποιοιδήποτε τυχαίοι χρήστες του Διαδικτύου θα μπορούσαν να τρέξουν το SATAN εναντίον υπολογιστών στους οποίους δεν έχουν καμία εξουσιοδότηση. Αυτό είναι ένα πρόβλημα από την στιγμή που μερικά από τα τεστ που εκτελεί το SATAN είναι παρόμοια με τεχνικές επίθεσης που χρησιμοποιούν οι crackers συστημάτων. Ο πιο ασφαλής τρόπος για να τρέξει το SATAN είναι πίσω από ένα firewall, εφόσον σε αυτήν την περίπτωση το SATAN θα εξετάσει μόνο συστήματα στα οποία έχει πρόσβαση μέσω της IP διεύθυνσης, και δεν θα ξεπεράσει τον υπολογιστή στον οποίο είναι εγκατεστημένος ο firewall.

6.4 SHADOW (US Navy Naval Surface Warfare Center)

Το Shadow (Secondary Heuristics for Defensive Online Warfare) είναι ένα δωρεάν network-based σύστημα ανίχνευσης κατάχρησης που τρέχει σε Unix. Πραγματοποιεί ανάλυση TCP/IP κυκλοφορίας και αποτελείται από 2 συστατικά : έναν αισθητήρα και ένα σταθμό ανάλυσης. Ο αισθητήρας ‘‘κάθεται’’ στο υπό ανάλυση δίκτυο και καταγράφει όλη την κυκλοφορία. Τα ακατέργαστα αρχεία δεδομένων από τον αισθητήρα στέλλονται μέσω ασφαλούς καναλιού στο σταθμό ανάλυσης για αναγνώριση προτύπων. Το Shadow απαιτεί εκτεταμένη χειροκίνητη ανάλυση και απόκριση σε γεγονότα. Σε αντίθεση με άλλα εμπορικά συστήματα, που αυτοματοποιούν τουλάχιστον ένα μέρος της ανάλυσης, αυτές οι εργασίες αφήνονται στα χέρια ειδικών ασφάλειας και απαιτούν πολλή εμπειρία και επιδεξιότητα.

6.5 REALSECURE

Το RealSecure της εταιρείας είναι ένα real time intrusion detection system και ανήκει στις κατηγορίες host-based και network-based IDS. Έχει την δυνατότητα να παρακολουθεί πλήρως το δίκτυο και τα συστήματα μιας επιχείρησης σε real time ώστε εάν ανιχνεύσει ύποπτη δραστηριότητα να ενημερώσει τον διαχειριστή ασφαλείας και να διακοπεί η επικείμενη επίθεση.

Το RealSecure αποτελείται από τρία διαφορετικά λειτουργικά τμήματα που συνεργάζονται μεταξύ τους για την μεγαλύτερη δυνατή προστασία. Αυτά είναι :

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

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 συγκεκριμένες πηγές. 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 :

1. Κεντρική παρουσίαση συναγερμών σε πραγματικό χρόνο
2. Κεντρική διαχείριση δεδομένων
3. Κεντρική ρύθμιση (configuration) της μηχανής του RealSecure

6.6 POLYCENTER (Compaq)

Το POLYCENTER είναι ανιχνευτής 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). 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.

6.7 SNORT

Το Snort είναι ένα δωρεάν ανοιχτού κώδικα λογισμικό που λειτουργεί ως ολοκληρωμένο σύστημα ανίχνευσης εισβολών (Intrusion Detection System – IDS) αλλά και ως σύστημα παρεμπόδισης εισβολών (Intrusion Prevention System – IPS). Ο δημιουργός του είναι ο Martin Roesch και ο κώδικας του είναι γραμμένος στη γλώσσα C.

Μπορεί να κάνει καταγραφή πακέτων και ανάλυση κίνησης σε πραγματικό χρόνο σε δίκτυα IP. Μπορεί να εκτελεί ανάλυση πρωτοκόλλων, εύρεση και ταίριασμα (matching) περιεχομένου και συνήθως χρησιμοποιείται για να ανιχνεύσει παθητικά ή να μπλοκάρει ενεργά μια ποικιλία δικτυακών επιθέσεων και διερευνήσεων (probes), όπως υπερχειλίσεις buffer, κρυφή σάρωση πορτών (stealth scan), διερευνήσεις πρωτοκόλλου SMB (Server Message Block) και προσπάθειες αναγνώρισης (fingerprinting) του λειτουργικού συστήματος ανάμεσα σε πολλά άλλα χαρακτηριστικά. Το Snort χαρακτηρίζεται ως μια ‘‘ελαφριά’’ (lightweight) τεχνολογία ανίχνευσης εισβολών σε σύγκριση με τα εμπορικώς διαθέσιμα αντίστοιχα συστήματα και είναι η πιο ευρέως αναπτυγμένη τεχνολογία ανίχνευσης και παρεμπόδισης εισβολών παγκοσμίως.

Αναλυτικότερα το Snort, χρησιμοποιεί για την ανίχνευση μια γλώσσα καθοδηγούμενη από κανόνες (rule-driven) η οποία συνδυάζει τα πλεονεκτήματα των μεθόδων ανίχνευσης βασιζόμενων στις υπογραφές (signatures), στην ανάλυση των πρωτοκόλλων για εύρεση ανωμαλιών, αλλά και γενικότερα στην ανώμαλη συμπεριφορά ως νεότερη τεχνική. Οι μηχανισμοί για τον εντοπισμό ανώμαλης συμπεριφοράς υλοποιούνται κατά κύριο λόγο από κάποιες μονάδες που ονομάζονται preprocessors, παρόλο που δίνεται η δυνατότητα να εκφραστεί η ανώμαλη συμπεριφορά και μέσα από ένα κανόνα για την ανάλυση ενός πακέτου ή μιας ροής. Οι preprocessors είναι σαν μία συμπληρωματική μηχανή του Snort όπου χωρίς

αυτούς ορισμένα είδη επιθέσεων δεν θα μπορούσαν να εντοπιστούν και προσφέρουν την δυνατότητα στο Snort να εντοπίζει κάποιες επιθέσεις που δεν έχουν γίνει ακόμα κανόνες. Οι κανόνες (rules) περιγράφουν τα χαρακτηριστικά ενός πακέτου που μπορεί να είναι μέρος μιας γνωστής επίθεσης. Κάθε ένας από τους κανόνες ουσιαστικά περιγράφει ποια είναι η ‘‘εικόνα’’ ενός βλαβερού πακέτου και επίσης πως πρέπει το Snort να αντιδράσει όταν εντοπίσει κάποια υπογραφή σε κάποιο πακέτο. Το Snort περιλαμβάνει πάνω από 6.000 κανόνες. Οι κανόνες και οι υπογραφές συχνά χρησιμοποιούνται σαν συνώνυμες λέξεις. Οι διαφορές τους είναι οι εξής : Οι υπογραφές είναι τα ειδικά χαρακτηριστικά του πακέτου που το χαρακτηρίζουν σαν ύποπτο ή βλαβερό (malicious). Τα χαρακτηριστικά αυτά βρίσκονται στο payload ή στο header του πακέτου και είναι μοτίβα από συμβολοσειρές (string patterns) που χαρακτηρίζονται σαν υπογραφή (signature) ενός «κακού» πακέτου. Γενικά η περιγραφή ενός πακέτου που είναι «κακό», όταν γίνεται με μια υπογραφή είναι στατική. Δηλαδή μια υπογραφή περιγράφει κάποιο υπαρκτό χαρακτηριστικό στο payload ή στο header του πακέτου. Οι κανόνες περιγράφουν στο Snort ή άλλο IDS τα χαρακτηριστικά ενός πακέτου που μπορεί να είναι μέρος μίας γνωστής επίθεσης καθώς και την ενέργεια που θα εκτελεστεί κατά τον εντοπισμό του. Η περιγραφή ενός πακέτου με ένα κανόνα είναι αρκετά πιο δυναμική. Αφενός, σε ένα κανόνα μπορεί να περιγράφονται περισσότερα του ενός υπαρκτά χαρακτηριστικά στο payload, αφετέρου, μπορούν να περιγράφονται χαρακτηριστικά που δεν πρέπει να έχει ένα πακέτο για να θεωρηθεί ύποπτο. Τέλος, ένας κανόνας μπορεί να περιγράφει μια ολόκληρη ροή και όχι ένα πακέτο, στις περιπτώσεις που γίνεται ανίχνευση εισβολών κρατώντας την ‘‘κατάσταση’’ (state) των συνδέσεων.

6.8 WIDS

Όσον αφορά τα πραγματικά συστήματα λογισμικού, τα οποία υλοποιούν ένα WIDS, αυτά έχουν εξελιχθεί αρκετά τα τελευταία χρονιά και διατίθενται τόσο σε δωρεάν (open source) όσο και συνδρομητική χρήση. Κάποια από τα περισσότερο σημαντικά λογισμικά, παρουσιάζονται συνοπτικά παρακάτω.

Το περισσότερο γνωστό WIDS είναι το SNORT το οποίο είναι ένα λογισμικό ανοιχτού πηγαίου κώδικα (open source) και διατίθεται δωρεάν. Το SNORT αποτελεί ένα δημοφιλές IDS, το οποίο με την χρήση ειδικού plug-in (SNORT wireless) (http://www.snort.org), μπορεί να χρησιμοποιηθεί και για τα ασύρματα ad hoc δίκτυα. Το συγκεκριμένο plug-in

επιτρέπει την δημιουργία κανόνων ανίχνευσης επιθέσεων, οι οποίοι μπορούν να προσαρμοστούν αναλόγως με το δίκτυο στο οποίο χρησιμοποιείται.

Ένα άλλο επίσης αρκετά γνωστό WIDS ανοικτού πηγαίου κώδικα, είναι το WIDZ (http://freshmeat.net/projects/widz/?topic_id=43,245,151,152), το οποίο εξειδικεύεται στην ανίχνευση των ραδιοσυχνοτήτων που χρησιμοποιούνται για την μεταφορά μηνυμάτων μεταξύ των κόμβων του δικτύου. Το WIDS μπορεί να ενσωματωθεί στο SNORT, έτσι ώστε να λειτουργεί παράλληλα μαζί του. Τέλος, ένα αρκετά δημοφιλές WIDS είναι και το Kismet (http://www.kismetwireless.net/), το οποίο εξειδικεύεται στην ανακάλυψη αναλυτών πακέτων (packet analyzers ή sniffers), τους οποίους τυχόν χρησιμοποιούν επίδοξοι εισβολείς για την πρόσβαση σε ένα (όχι απαραίτητα μόνο ασύρματο) δίκτυο. Το Kismet αποτελεί κι αυτό ένα λογισμικό ανοικτού κώδικα και διατίθεται δωρεάν.

ΚΕΦΑΛΑΙΟ 7

ΠΑΡΑΤΗΡΗΣΕΙΣ – ΣΥΜΠΕΡΑΣΜΑΤΑ

Η ασφάλεια έχει γίνει κρίσιμο συστατικό της σχεδίασης συστημάτων και δικτύων σήμερα. Στη πραγματικότητα πρόκειται για ένα αγώνα χωρίς τέλος ανάμεσα στους κακόβουλους επιτιθέμενους και τους υπεύθυνους ασφαλείας των συστημάτων. Οι επιτιθέμενοι χρησιμοποιούν ολοένα και εξυπνότερους τρόπους εκμετάλλευσης των αδυναμιών των συστημάτων, έτσι θα υπάρχει πάντα η ανάγκη για εξυπνότερες και καλύτερες λύσεις ασφαλείας. Η δυσκολία της διασφάλισης πληροφοριών οφείλεται στην έλλειψη γνώσης σε βάθος και συνειδητοποίησης των απειλών. Όσο καλύτερα αναλύσει, κατανοήσει και κατηγοριοποιήσει κανείς τις απειλές τόσο πιο αποτελεσματικές τεχνικές μπορεί να εφαρμόσει για να τις αντιμετωπίσει.

Προκειμένου να διασαφηνιστεί ο όρος ασφάλεια είναι αναγκαίο να οριστούν ποιοί πόροι πρέπει να προστατεύονται και απέναντι σε ποιές απειλές. Το ζητούμενο στις τεχνικές ασφάλειας των δικτύων είναι η επιτυχής εξουδετέρωση απειλών όπως κλοπή, απάτη, κατασκοπία. Κύριο πρόβλημα που πρέπει να αντιμετωπιστεί είναι ο έγκαιρος προσδιορισμός των τρωτών και η βελτίωση της ασφάλειας των συστημάτων πριν από την δράση των εισβολέων.

Ιστορικά γεγονότα μαρτυρούν πως η πρόληψη από μόνη της (όπως για παράδειγμα με τεχνικές κρυπτογραφίας και αυθεντικοποίησης) δεν επαρκεί. Για το λόγο αυτό, στα μέσα της δεκαετίας του ‘80 μία εναλλακτική προσέγγιση που ονομαζόταν ανίχνευση εισβολής (intrusion detection) έκανε την εμφάνισή της. Η νέα αυτή προσέγγιση της ασφάλειας, δεν είχε σκοπό να αλλάξει την υπάρχουσα υποδομή των πιθανά ανασφαλών συστημάτων με καινούρια συστήματα που θα ήταν ασφαλή, αλλά επιδιώκει να δράσει συμπληρωματικά προς αυτά. Η ανίχνευση εισβολών λειτουργεί έχοντας ως βάση την αρχή ότι οποιαδήποτε προσπάθεια διείσδυσης σε ένα σύστημα μπορεί να ανιχνευθεί και ο διαχειριστής να ειδοποιηθεί, παρά να εμποδιστεί στην πραγματικότητα η απόπειρα πραγματοποίησής της. Έτσι τα συστήματα ανίχνευσης εισβολών έρχονται στο προσκήνιο. Η ανίχνευση εισβολών είναι το λογικό συμπλήρωμα των Firewalls των δικτύων, επεκτείνοντας τις ικανότητες διαχείρισης της ασφάλειας των διαχειριστών ασφαλείας των συστημάτων, να συμπεριλάβουν

μεθόδους επίβλεψης (auditing), αναγνώρισης επιθέσεων και ανάδρασης. Είναι πολύ δύσκολο αν όχι ακατόρθωτο να σχεδιάσει κανείς ένα σύστημα που θα είναι εύχρηστο και συγχρόνως ασφαλές. Τα συστήματα ανίχνευσης επιθέσεων θα ήταν βασισμένα σε μια τεχνολογία που θα επέτρεπε να ανιχνεύει επιθέσεις σε υπολογιστές και σε δίκτυα, κατά προτίμηση σε πραγματικό χρόνο, και να ειδοποιούν για αυτές το διαχειριστή ασφαλείας.

Επίσης, δεν μπορεί κανείς να αποκλείσει από ένα θεωρητικά ασφαλές σύστημα κάποιο λάθος στην παραμετροποίηση από τον διαχειριστή το οποίο θα οδηγήσει σε πρόβλημα ασφαλείας. Τα προϊόντα ανίχνευσης εισβολών κερδίζουν παγκόσμια αναγνώριση ως σημαντικά εργαλεία που βελτιώνουν την ασφάλεια των δικτύων και των πληροφοριακών συστημάτων και η προσέγγιση αυτή με το πέρασμα του χρόνου κέρδισε όλο και περισσότερο έδαφος στο χώρο της ασφάλειας με αποτέλεσμα ένας μεγάλος αριθμός από πρωτότυπα τέτοια συστήματα να έχουν δημιουργηθεί σήμερα σε πολλά ερευνητικά κέντρα και μερικά από αυτά να έχουν εγκατασταθεί σε παραγωγικά συστήματα.

Παράλληλα με την εξέλιξη των ενσύρματων δικτύων άρχισαν να αναπτύσσονται και τα ασύρματα δίκτυα προκειμένου να ικανοποιηθούν οι τεχνολογικές ανάγκες της κοινωνίας. Όπως τα ενσύρματα έτσι και τα ασύρματα αντιμετώπισαν το θέμα της ασφάλειας. Στα ασύρματα δίκτυα, τυπικά η επικοινωνία λαμβάνει χώρα μόνο ανάμεσα σε ασύρματους κόμβους και σημεία πρόσβασης, αλλά όχι απ' ευθείας ανάμεσα σε ασύρματους κόμβους (nodes). Ωστόσο τα ad hoc ασύρματα δίκτυα δεν χρειάζονται καμία υποδομή για να τεθούν σε λειτουργία. Ο κάθε κόμβος έχει την δυνατότητα να επικοινωνεί με κάποιον άλλο κόμβο, χωρίς την παρεμβολή κάποιου σημείου πρόσβασης μεταξύ των κόμβων να είναι απαραίτητη. Η κινητικότητα των κόμβων σε ένα ad hoc δίκτυο προκαλεί πολύ συχνές αλλαγές όσον αφορά την τοπολογία του εν λόγου δικτύου. Επομένως οι μηχανισμοί ασφαλείας γίνονται αναγκαία για τα ad hoc δίκτυα και αναπόσπαστα μέρη αυτών. Πραγματοποιώντας μία σύγκριση, μεταξύ των ενσύρματων και των ασύρματων ad hoc δικτύων, στα οποία η κυκλοφορία που παρακολουθείται, συνηθίζεται να γίνεται σε διάφορους μεταγωγούς (switches), δρομολογητές (routers) και ανοίγματα θυρών, συμπεραίνουμε ότι ένα ασύρματο ad hoc δίκτυο δεν έχει σημεία συγκέντρωσης διακίνησης στα οποία ένα σύστημα ανίχνευσης εισβολών να μπορεί να συλλέγει πληροφορίες για ολόκληρο το δίκτυο. Έτσι λοιπόν η βέλτιστη αρχιτεκτονική ενός ασύρματου συστήματος ανίχνευσης εισβολών (WIDS) για την εφαρμογή του σε ένα τέτοιο δίκτυο εξαρτάται σε μεγάλο βαθμό από την αρχιτεκτονική του ίδιου του δικτύου και κάθε κόμβος θεωρείται υπεύθυνος για την αναζήτηση σημάτων για τοπικές εισβολές ανεξαρτήτως.

Τόσο τα IDS και τα WIDS βρίσκονται υπό συνεχή εξέλιξη που κυρίως έχει να κάνει με την βελτίωση της αποδοτικότητάς τους και την εξάλειψη των συμπτωμάτων από False Positives και False Negatives που παρουσιάζουν.

Κάθε IDS υλοποιεί τρεις θεμελιώδεις λειτουργίες, που έχουν να κάνουν με τις Πηγές της Πληροφορίας από τις οποίες συλλέγει τα γεγονότα που θα εξετάσει για την ανίχνευση μίας επίθεσης, τις Τεχνικές Ανάλυσης που χρησιμοποιεί για να εξετάσει τα γεγονότα αυτά και τον τρόπο που αντιδρά (Responses) όταν ανιχνεύσει μία πιθανή επίθεση. Τα IDSs που κυρίως χρησιμοποιούνται σήμερα, είναι αυτά που λειτουργούν σε επίπεδο δικτύου (NIDS) και χρησιμοποιούν για την ανάλυση των γεγονότων που εξετάζουν την τεχνική του Misuse Detection, η οποία συνήθως συνδυάζεται κατά κύριο λόγο με την τεχνική του Protocol Anomaly Detection και ίσως με κάποια αποτελέσματα της Anomaly Detection. Η προτεινόμενη πρακτική χρήσης IDSs σε ένα δίκτυο, περιλαμβάνει την εφαρμογή NIDSs σε ζωτικά σημεία του δικτύου και την εφαρμογή HIDSs στα σημαντικότερα συστήματα του.

Συμπερασματικά οι κυριότεροι παράμετροι αποτίμησης της ποιότητας των συστημάτων ανίχνευσης εισβολών είναι η Ακρίβεια δηλαδή τι συχνότητα εμφάνισης έχουν οι εσφαλμένα θετικές ανιχνεύσεις (false positives), η Απόδοση δηλαδή πόσο γρήγορα μπορεί να συλλέξει στοιχεία και να επεξεργαστεί αναφορές, η Πληρότητα Ανίχνευσης δηλαδή το ποσοστό επιθέσεων που θα καταφέρει να ανιχνεύσει, η Αντοχή σε επιθέσεις προς το ίδιο το σύστημα IDS και η Ταχύτητα κατάληξης σε συμπεράσματα. Σήμερα διατίθενται αρκετά και διάφορα IDSs, υλοποιημένα τόσο σε Hardware ή Software, όσο και με την μορφή εμπορικών ή Open Source εφαρμογών. Το πιο επιθυμητό χαρακτηριστικό όμως ενός συστήματος ανίχνευσης εισβολών είναι η ικανότητά του να βρίσκεται ένα βήμα πιο μπροστά από τον επιτιθέμενο, η δυναμική του δηλαδή να ανιχνεύει νέες επιθέσεις και η σωστή επιλογή ενός τέτοιου εργαλείου, εξαρτάται από τους στόχους και τις ανάγκες προστασίας κάθε δικτύου.

ΒΙΒΛΙΟΓΡΑΦΙΚΕΣ ΑΝΑΦΟΡΕΣ

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

[2] Denning, D. "An Intrusion Detection Model." IEEE Transactions on Software Engineering, 1987

[3] Sundaram A., '' An Introduction to Intrusion detection'', 1996

[4] A. Mishra, K. Nadkarni, A. Patcha, "Intrusion Detection in Wireless Ad Hoc Networks",

[5] Satria Mandala, Md. Asri Ngadi, A. Hanan Abdullah, "A Survey on MANET Intrusion Detection", 2004

[6] Yongguang Zhang, Wenke Lee, "Intrusion Detection in Wireless AdHoc Networks", 2000 Krishna Gorantala, "Routing Protocols in Mobile Ad-hoc Networks"

[7] T.W. Anderson, "An introduction to multivariate statistical analysis" (Second ed., John Wiley & Sons, 1994)

[8] Asaka M., Onabuta T., Inoue T., Okazawa S., Goto S., "A New Intrusion Detection Method Based on Discriminant Analysis" (IEEE Transactions On Information & Systems, Vol. E84-D, No. 5, 2001)

[9] T D Garvey, Lunt T.F., "Model based intrusion detection" (In Proceedings of the 14th National Computer Security Conference, 1991)

[10] Biermann E., Cloete E., Venter L.M., "Comparison of intrusion detection systems" (Computers & Security, No 20, 2001)

[11] R. Heady, G. Luger, A. Maccabe, M. Servilla, "The architecture of a network level intrusion detection system" (Technical report, 1990)

[12] "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

[13]Wenke Lee Salvatore J. Stolfo : Data Mining Approaches for Intrusion Detection

[14] Gaia Maselli , Luca Deri ,Stefano Suin : Design and Implementation of an Anomaly Detection System : an Empirical Approach

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

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

[17] Θ. Κομνηνός, Π. Σπυράκης : ''Ασφάλεια Δικτύων & Υπολογιστικών Συστημάτων'', 2002 Ελληνικά Γράμματα

[18] Πάγκαλος Γ., Μαυρίδης Ι., "Ασφάλεια Πληροφοριακών Συστημάτων και Δικτύων", Εκδόσεις Ανικούλα, 2002

[19] Matthew Strebe : Ασφάλεια Δικτύων – Εισαγωγή στην σύγχρονη τεχνολογία, Εκδόσεις Μ. Γκιούρδας 2005

[20] Γ. Λεκάτης, Ν. Κλαδάκης : Ασφάλεια Δικτύων και Συστημάτων, Εκδόσεις Παπασωτηρίου 2001

[21] Α. Σουρής, Δ. Πατσός, Ν. Γρηγοριάδης : Ασφάλεια της πληροφορίας, Εκδόσεις Νέων Τεχνολογιών 2004

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