Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Μεταπτυχιακή Διατριβή
στα Πληροφοριακά και Επικοινωνιακά Συστήματα

Συστήματα Ανίχνευσης και Πρόληψης Επιθέσεων: Μια Επισκόπηση

Πάτροκλος Ιωαννίδης

Επιβλέπων Καθηγητής
Στέφανος Γκρίτζαλης

Αύγουστος 2014

Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Συστήματα Ανίχνευσης και Πρόληψης Επιθέσεων: Μια Επισκόπηση

Πάτροκλος Ιωαννίδης

Επιβλέπων Καθηγητής
Στέφανος Γκρίτζαλης

Η παρούσα μεταπτυχιακή διατριβή υποβλήθηκε
προς μερική εκπλήρωση των απαιτήσεων για απόκτηση

μεταπτυχιακού τίτλου σπουδών
στα Πληροφοριακά Συστήματα

από τη Σχολή Θετικών και Εφαρμοσμένων Επιστημών
του Ανοικτού Πανεπιστημίου Κύπρου

Αύγουστος 2014

Περίληψη

Η Ανίχνευση και Πρόληψη Επιθέσεων αποτελεί ένα από τα σημαντικότερα μέσα για τη διασφάλιση και προστασία των υπολογιστικών συστημάτων από κακόβουλους επιτιθέμενους, καθώς επιτυγχάνει την ανίχνευση επιθέσεων, περιορίζει την επίδρασή τους και είναι απαραίτητη προκειμένου να επιτύχουμε μεγάλη επιβιωσιμότητα σε ένα δίκτυο. Η αντιμετώπιση των επιθέσεων σε υπολογιστικά συστήματα, με χαρακτήρα κυρίως προληπτικό, αλλά και με δυνατότητες ολοκληρωμένης καταγραφής των επιτυχών και ανεπιτυχών προσπαθειών παραβίασης, παρέχει προστασία σε περιβάλλοντα κρίσιμων υπολογιστικών υποδομών (critical infrastructure protection).

Σκοπός της διπλωματικής είναι να γνωρίσουμε τους λόγους χρήσης των συστημάτων Ανίχνευσης και Πρόληψης επιθέσεών, την αρχιτεκτονική τους , την εξέλιξη τους και τα επιθυμητά χαρακτηριστικά τους. Αρχικά θα μελετηθούν διεξοδικά τα σύγχρονα συστήματα Ανίχνευσης και Πρόληψης Επιθέσεων, με βάση μοντέλα εισβολών (models of intrusion), όπως το μοντέλο ανίχνευσης διαταραχών (anomaly model), το μοντέλο κακής συμπεριφοράς (misuse model), το μοντέλο που βασίζεται στις προδιαγραφές (specification-based model), μοντέλα τα οποία ενδέχεται να είναι προσαρμοστικά (adaptive) ή στατικά (static). Επιπλέον, θα περιγραφούν σύγχρονες αρχιτεκτονικές συστημάτων Ανίχνευσης και Πρόληψης Εισβολών. Στη συνέχεια θα μελετηθεί η οργάνωσή τους και η αποτελεσματικότητά τους σε γνωστές και άγνωστες επιθέσεις. Τέλος θα δοθεί ιδιαίτερη έμφαση στα ευρύτερα αξιοποιούμενα σχετικά συστήματα, για την προστασία περιβαλλόντων κρίσιμων υπολογιστικών υποδομών.

Λέξεις κλειδιά: Συστήματα Ανίχνευσης και Πρόληψης Επιθέσεων, Μοντέλα εισβολών, Μοντέλο ανίχνευσης διαταραχών, Μοντέλο κακής συμπεριφοράς, Μοντέλο που βασίζεται στις προδιαγραφές, Αρχιτεκτονικές συστημάτων Ανίχνευσης και Πρόληψης Εισβολών.

Summary

The detection and prevention of attacks is one of the most important means to safeguard and protect computer systems from malicious attackers, as it achieves the detection of attacks, limits their impact and is necessary to attain survivability within a large network. The encountering of attacks on computer systems in a preventative manner, but also with capabilities that can comprehensively record the successful and unsuccessful breaching attempts, provides protection in critical infrastructure protection environments.

The purpose of the thesis is to become acquainted with the reasons that detection and prevention systems are necessary, their architecture, their development and their desired characteristics. Initially, modern detection and prevention systems will be studied in detail, with the use of models of intrusion, such as the anomaly model, the misuse model, the specification - based model, as well as the adaptive or static models. Furthermore, modern architectures of detection and prevention systems will be described. Thereinafter, their organization and effectiveness to known and unknown attacks will be studied. Finally, particular emphasis will be given to the relevant systems that are more widely used, for the protection of critical infrastructure protection environments.

Keywords: Detection and prevention systems, models of intrusion, anomaly model, misuse model, specification - based model, System architectures for detection and prevention.

Ευχαριστίες

Στο σημείο αυτό θα ήθελα να ευχαριστήσω τον κύριο Γκρίτζαλη Στέφανο, πρύτανη του Πανεπιστημίου Αιγαίου, για τις πολύτιμες συμβουλές και χρήσιμες διορθώσεις του. Χωρίς την ουσιαστική βοήθεια του θα ήταν αδύνατη η περάτωση της διπλωματικής αυτής εργασίας.

Επίσης θα ήθελα να ευχαριστήσω την οικογένεια μου, που είναι πάντα δίπλα μου δείχνοντας έμπρακτα την υποστήριξη και την εμπιστοσύνη τους για την εκπλήρωση των στόχων μου. Τέλος τους φίλους μου για την συμπαράσταση που μου προσφέρανε σε όλη τη διάρκεια εκπόνησης της εργασίας αυτής.

Περιεχόμενα

Περιεχόμενα Εικόνων

Κεφάλαιο 1
Εισαγωγή

Η κοινότητα της Τεχνολογίας Πληροφοριών και Επικοινωνιών (ΤΠΕ) αποτελεί ένα περίπλοκο επιστημονικό πεδίο, που περιέχει ταυτόχρονα τεχνολογίες του παρελθόντος και μια συνεχή αύξηση σε τεχνολογίες νέων συστημάτων, δικτύων, λογισμικού και πρωτοκόλλων. Η διασφάλιση των σημερινών δικτύων περιλαμβάνει όχι μόνο σωστή διαχείριση, τείχη προστασίας (firewalls) και εκπαίδευση των χρηστών του, αλλά και συχνό έλεγχο πραγματικών συνθηκών και επαλήθευση για το τι είναι ασφαλές και τι όχι [1]. Παρόλα αυτά υπάρχει περίπτωση παρά την ορθή λειτουργία του firewall κάποιος από αυτούς να κυριευτεί από κάποια απειλή επειδή ήταν ευάλωτος σε μια ασυνήθιστη αίτηση. Εκτός από firewall πιθανά να υπάρχουν και άλλα στοιχεία που να χρησιμοποιούνται ως πρώτη γραμμή άμυνας, όπως οι Λίστες Ελέγχου Πρόσβασης (Access Control Lists – ACLs). Αν και όλα αυτά συμβάλουν στην βελτίωση του επιπέδου ασφάλειας, ωστόσο δεν μπορούμε ποτέ να είμαστε σίγουροι ότι ακολουθήθηκαν οι βέλτιστες λύσεις που θα προσφέρουν την καλύτερη δυνατή προστασία. Για τον λόγο αυτό θεωρείται καλύτερα η ύπαρξη μιας δεύτερης γραμμή άμυνας. Η τακτική αυτή, δηλαδή η χρήση πολλών επιπέδων άμυνας στο δίκτυο, είναι γνωστή με τον όρο «Defence in Depth» (Άμυνα σε Βάθος). Ενισχύουμε όσο μπορούμε την πρώτη γραμμή άμυνας ώστε να μην επιτρέπεται η παράνομη πρόσβαση στο εσωτερικό μας δίκτυο, αλλά αν αυτό αποτύχει, τότε έχουμε και εναλλακτικό σχέδιο. Ένας ανιχνευτικός μηχανισμός είναι πολύ καλή λύση για το δεύτερο επίπεδο

προστασίας. Για αυτό το λόγο, αναπτύχθηκαν συστήματα λογισμικού και εφαρμογές δικτυακής ασφάλειας που παρακολουθούν το δίκτυο και τις δραστηριότητές του για κακόβουλη χρήση. Τα σημαντικότερα συστήματα που το επιτυγχάνουν αυτό είναι τα Συστήματα Ανίχνευσης και Πρόληψης Επιθέσεων (Intrusion Detection and Prevention Systems). Η σημασία του έγκειται πως σε ένα ρεαλιστικό υπολογιστικό και δικτυακό περιβάλλον του οποίου η ανίχνευση εισβολής είναι δυσκολότερη γιατί ο παράγοντας που μειώνει την αποδοτικότητα ενός IDPS δεν είναι η ικανότητά του να αναγνωρίσει σωστά την εισβολή, αλλά η ικανότητά του να σταματά τους λάθος συναγερμούς. Η μελέτη και χρησιμοποίηση των συστημάτων αυτών τόσο στον ερευνητικό – επιστημονικό τομέα όσο και σε πρακτικό επίπεδο θα βοηθήσει στην αντιμετώπιση της πρόθεσης ενός κακόβουλου χρήστη να αποκτήσει παράνομα πρόσβαση σε μέρη και στοιχεία μιας κρίσιμης υπολογιστικής υποδομής (πχ. Στρατιωτικά Δίκτυα) ή σε πόρους και αρχεία ενός αυτόνομου υπολογιστή.

1.1 Δομή Εργασίας

Μέχρι το σημείο αυτό έγινε μια γενική εισαγωγή στο θέμα που θα μας απασχολήσει. Στη συνέχεια του πρώτου μέρους θα γίνει ανάλυση του σκοπού της έρευνας αυτής.

Στο **κεφάλαιο 2** περιγράφεται η σημασία και η σπουδαιότητα της ασφάλειας σε περιβάλλον κρίσιμων υπολογιστικών υποδομών, οι βασικές αρχές της Ασφάλειας αλλά και η Πολιτική Ασφαλείας που επιλέγεται για την προστασία αυτού. Τέλος γίνεται αναφορά στο κύκλο διαχείρισης για την αντιμετώπιση των απειλών αυτών .

Στο **Κεφάλαιο 3** περιγράφονται οι γνωστές και άγνωστες επιθέσεις των υποδομών αυτών καθώς και οι τρόποι αντιμετώπισης αυτών.

Στο **Κεφάλαιο 4** γίνεται αναλυτική περιγραφή των Συστημάτων Ανίχνευσης και Πρόληψης Επιθέσεων με απώτερο σκοπό την ταξινόμηση τους, τους στόχους αλλά και την παρουσίαση ενός Γενικού Μοντέλου. Επιπλέον αναλύονται τα μοντέλα εισβολών βάση των οποίων θα γίνει μελέτη σύγχρονων συστημάτων Ανίχνευσης και Πρόληψης Επιθέσεων. Θα αναλυθούν το μοντέλο ανίχνευσης διαταραχών (anomaly model), το μοντέλο κακής συμπεριφοράς (misuse model), το μοντέλο που βασίζεται στις προδιαγραφές (specification-based model), καθώς και μοντέλα τα οποία ενδέχεται να είναι προσαρμοστικά (adaptive) ή στατικά (static).

Το **Κεφάλαιο 5** περιγράφονται η δομή αλλά και η αρχιτεκτονική των Συστημάτων Ανίχνευσης και Πρόληψης Επιθέσεων. Επίσης θα εξεταστούν τα είδη της πληροφορίας που είναι διαθέσιμα στην καθεμία περίπτωση, καθώς και ο τρόπος που αυτά μπορούν να συλλεχθούν. θα μελετηθεί ο τομέας της απόκρισης στην εισβολή. Θα καθοριστούν διαδικασίες και ενέργειες που ουσιαστικά θα αποτελούν και την πολιτική ασφαλείας προκειμένου να αντιμετωπίζεται η αποπειραθείσα επίθεση με τρόπο ώστε να ελαχιστοποιείται η ζημιά.

Στο **Κεφάλαιο 6** γίνεται αναλυτική περιγραφή των ευρύτερων αξιοποιούμενων συστημάτων Ανίχνευσης και Πρόληψης Επιθέσεων. Συγκεκριμένα θα γίνει ανάλυση της οργάνωση, των δυνατοτήτων αλλά και της αποτελεσματικότητας του καθενός. Επιπλέον θα γίνει μια διαδικασία περιγραφής και σύγκρισης των συστημάτων αυτών σε περιβάλλοντα κρίσιμων υπολογιστικών υποδομών.

Το **Κεφάλαιο 7** ολοκληρώνει την εργασία με κάποια συμπεράσματα.

1.2 Σκοπός της εργασίας.

Μέσα από την έρευνα αυτή θα επιδιώξουμε να διατυπώσουμε το επίπεδο που διαδραματίζουν τα συστήματα αυτά στην ασφάλεια μιας υπολογιστικής υποδομής. Επιπλέον θα μελετήσουμε και παρουσιάσουμε στο ποια πρέπει να είναι τα επιθυμητά χαρακτηριστικά ενός συστήματος Ανίχνευσης και Πρόληψης Επιθέσεων, με σκοπό την προστασία κρίσιμων υπολογιστικών υποδομών. Τέλος θα γίνει μια ταξινόμηση-μελέτη των συστημάτων Ανίχνευσης και Πρόληψης Επιθέσεων λαμβάνοντας υπόψη την εκπλήρωση των αρχών Ανίχνευσης και Πρόληψης αλλά και την αποτελεσματικότητας τους.

Η μελέτη και ανάλυση των συστημάτων Ανίχνευσης και Πρόληψης Επιθέσεων θα οδηγήσει στην σύγκριση των μελετών που έγιναν και της προσπάθειας που θα αναπτυχθεί και παρουσιαστεί για καινούργια ευρήματα (εξελίξεις και αδυναμίες) των συστημάτων αυτών. Επιπλέον θα γίνει μια προσπάθεια να δοθούν λύσεις στα διάφορα ερωτήματα που τέθηκαν και αποτελούν στόχο στην εν λόγω μελέτη. Επιπλέον θα συνοψιστούν σημαντικά συμπεράσματα καθώς και προτάσεις κατευθύνσεων για μελλοντική έρευνα.

Γενικότερα παρατηρούνται αναπτύξεις νέων μηχανισμών υποστήριξης των συστημάτων Ανίχνευσης και Πρόληψης Επιθέσεων για καλύτερη απόδοση, γεγονός που αποτελεί σημαντική

εξέλιξη [1]. Επιπλέον μέσα από τις αδυναμίες που παρατηρούνται στα διάφορα συστήματα θα πρέπει να προταθούν αντίστοιχες λύσεις και βελτιώσεις τους. Θα γίνει μια προσπάθεια ανάλυσης και επιλογής των ευρέως αξιοποιούμενων συστημάτων ταξινομώντας τα ανάλογα με την εκπλήρωση των αρχών ανίχνευσης και πρόληψης των συστημάτων. Τέλος θα γίνει μια προσέγγιση και μελέτη στις αρχιτεκτονικές των συστημάτων αυτών κατανοώντας την λειτουργία τους .

Κεφάλαιο 2

Ασφάλεια Σε Περιβάλλον Κρίσιμων Υπολογιστικών Υποδομών (critical infrastructure protection)

Στις μέρες μας οι κρίσιμες υπολογιστικές υποδομές χρησιμοποιούνται από όλο και μεγαλύτερα τμήματα του πληθυσμού παγκοσμίως, ενώ και οι ανάγκες που εξυπηρετούν ολοένα και διευρύνονται. Από τις μεγάλες εταιρείες, οργανισμούς που τα χρησιμοποιούν για την οργάνωση και διοίκηση των κατά τόπους παραρτημάτων τους και τα ανά τον κόσμο πανεπιστήμια που με τη βοήθειά τους συνδέονται και συνεργάζονται μεταξύ τους, μέχρι τον απλό πολίτη που κάνει αγορές μέσω Διαδικτύου, όλοι, λίγο-πολύ, τώρα πια χρειάζονται την δικτύωση αυτή. Γίνεται επομένως αντιληπτό, ότι η ασφάλεια στην εκ των ων ουκ άνευ, όπως φαίνεται, χρήση των κρίσιμων υπολογιστικών υποδομών είναι ζήτημα καίριας σημασίας.

2.1. Έννοια Ασφάλειας Πληροφοριακών Συστημάτων

Η ασφάλεια στα υπολογιστικά συστήματα και δίκτυα μπορεί να θεωρηθεί ως η δυνατότητα ενός υπολογιστικού συστήματος ή δικτύου να αντισταθεί, με δεδομένο επίπεδο αξιοπιστίας, σε τυχαία συμβάντα ή κακόβουλες ενέργειες που θέτουν σε κίνδυνο την επαλήθευση ταυτότητας, την ακεραιότητα τη διάθεση και την τήρηση της εμπιστευτικότητας των δεδομένων που έχουν αποθηκευτεί ή μεταδοθεί ή επεξεργαστεί, καθώς και τις συναφείς υπηρεσίες που παρέχονται ή είναι προσβάσιμες μέσω των δικτύων και συστημάτων αυτών.

2.1.1. Βασικές Αρχές Ασφάλειας Πληροφοριακών Συστημάτων

Η προστασία των κρίσιμων υπολογιστικών υποδομών αποτελεί θέμα που θα πρέπει να αντιμετωπίσουν όλοι οι εμπλεκόμενοι φορείς. Είναι γενικά αποδεκτό ότι η ασφάλεια των υποδομών αυτών συνδέεται στενά με τρεις βασικές έννοιες [8].

- **Διαθεσιμότητα (Availability)**

Διαθεσιμότητα ονομάζεται η ιδιότητα του να είναι προσπελάσιμες και χωρίς αδικαιολόγητη καθυστέρηση οι υπηρεσίες ενός δικτύου όταν τις χρειάζεται μια εξουσιοδοτημένη οντότητα. Για τους σκοπούς της ασφάλειας, μας απασχολεί βασικά η παρεμπόδιση κακόβουλων επιθέσεων που αποσκοπούν στο να παρακωλύσουν την πρόσβαση των νόμιμων χρηστών σε ένα πληροφοριακό σύστημα. Αυτές οι επιθέσεις ονομάζονται επιθέσεις άρνησης παροχής υπηρεσιών (DoS). Η άρνηση παροχής υπηρεσιών σημαίνει παρεμπόδιση της εξουσιοδοτημένης προσπέλασης πληροφοριών και πόρων ή πρόκλησης καθυστέρησης των λειτουργιών που είναι κρίσιμες στο χρόνο. Ένα παράδειγμα άρνησης παροχής υπηρεσιών είναι οι επιθέσεις <<πλημύρας>> όπου ο επιτιθέμενος κατακλύζει ένα εξυπηρετητή στέλνοντας του ένα μεγάλο αριθμό αιτήσεων.

Μια επίθεση DoS μπορεί να διαπραχτεί με διάφορους τρόπους. Υπάρχουν τρεις βασικοί τύποι επιθέσεων:

1. Κατανάλωση υπολογιστικών πόρων, όπως εύρος ζώνης, διάστημα δίσκων, ή ΚΜΕ χρόνος.

2. Διάσπαση των πληροφοριών διαμόρφωσης, όπως δρομολόγηση πληροφορίες.

3. Διάσπαση των φυσικών τμημάτων δικτύων.

- **Εμπιστευτικότητα (Confidentiality)**

Εμπιστευτικότητα σημαίνει πρόληψη μη εξουσιοδοτημένης αποκάλυψης πληροφοριών, δηλαδή, πρόληψη από μη εξουσιοδοτημένη ανάγνωση. Επομένως, τα δεδομένα που διακινούνται μεταξύ των υπολογιστών ενός δικτύου, αποκαλύπτονται μόνο σε εξουσιοδοτημένα άτομα.

Άλλες εκφάνσεις της εμπιστευτικότητας είναι:

1. Η ιδιωτικότητα, προστασία των δεδομένων προσωπικού χαρακτήρα, δηλαδή αυτών που αφορούν συγκεκριμένα πρόσωπα και

2. Η μυστικότητα, προστασία των δεδομένων που ανήκουν σε έναν οργανισμό ή μια επιχείρηση.

Εμπιστευτικότητα είναι έννοια που πολλές φορές ταυτίζεται με την έννοια της ασφάλειας και ειδικότερα σε κρίσιμες υπολογιστικές υποδομές όπως είναι και οι στρατιωτικές όπου θα πρέπει να κρατούνται μυστικές οι πληροφορίες.

- **Ακεραιότητα (Integrity)**

Η ακεραιότητα μπορεί να οριστεί γενικότερα ως η απαίτηση να είναι τα πράγματα όπως πρέπει να είναι. Στην πληροφορική, ακεραιότητα σημαίνει πρόληψη μη εξουσιοδοτημένης μεταβολής πληροφοριών, δηλαδή πρόληψη από μη εξουσιοδοτημένη εγγραφή ή διαγραφή, συμπεριλαμβανομένης και της μη εξουσιοδοτημένης δημιουργίας δεδομένων.

2.1.2 Δράσεις Ασφάλειας Πληροφοριακών Συστημάτων

Οι δράσεις ασφάλειας στις κρίσιμες υπολογιστικές υποδομές σχετίζονται με:

- Ανίχνευση (Detection): Τη λήψη μέτρων για την ανίχνευση του χρόνου, του τρόπου και της ταυτότητας εκείνου που προκάλεσε φθορά σε μία από τις προαναφερόμενες συνιστώσες.

- Αντίδραση (Reaction): Τη λήψη μέτρων για την αποκατάσταση ή ανάκτηση των συστατικών ενός υπολογιστικού συστήματος και δικτύου.

- Πρόληψη (Prevention): Τη λήψη μέτρων για την αποφυγή ζημίας στις επιμέρους συνιστώσες ενός υπολογιστικού συστήματος και δικτύου.

2.2 Πολιτική Ασφαλείας

Το πρώτο βήμα για την υλοποίηση μιας ολοκληρωμένης λύσης για τα ζητήματα δικτυακής ασφάλειας μιας κρίσιμης υπολογιστικής υποδομής είναι η χάραξη μιας συγκεκριμένης πολιτικής που θα καθορίζει τον τρόπο που αυτός ή αυτή θα λειτουργεί. Η πολιτική αυτή συνήθως παίρνει την μορφή επίσημου εγγράφου το οποίο φτάνει στα χέρια κάθε υπαλλήλου ή μέλους του οργανισμού και ουσιαστικά αντιπροσωπεύει το πρωτόκολλο με βάση το οποίο θα λειτουργεί ο καθένας. Με τον τρόπο αυτό, όλοι λαμβάνουν γνώση των ευθυνών τους, συνειδητοποιούν την κρισιμότητα του ρόλου που έχει να παίξει ο καθένας ξεχωριστά αλλά και τις συνέπειες που μπορεί να έχει η μη τήρηση των κανόνων αυτών. Αν και κάτι τέτοιο δεν εξαλείφει τους κινδύνους για την ασφάλεια από αμελή ή λανθασμένη συμπεριφορά μεμονωμένων μελών του ανθρώπινου δυναμικού, τους μειώνει σημαντικά κάνοντας το όλο οικοδόμημα πιο στέρεο και συμπαγές.

Η παραπάνω διαδικασία που περιγράψαμε της κατάστρωσης πολιτικής ασφάλειας για τον οργανισμό ή την εταιρεία έχει πλέον διεθνώς προτυποποιηθεί, στο πρότυπο ISO 17799, που αναφέρει λεπτομερώς τις διάφορες πτυχές που πρέπει να καλυφθούν, από τις οποίες μερικές από τις πιο κυρίαρχες ακολουθούν παρακάτω [8].

- Έλεγχος ασφαλούς λειτουργίας τόσο σε επίπεδο δικτύου όσο και σε επίπεδο υπολογιστών που το απαρτίζουν (host). Είναι σημαντικό να υπάρχει τέτοια μέριμνα, αφού κάτι τέτοιο ουσιαστικά θα λειτουργεί σαν δεύτερο τμήμα άμυνας, προστατεύοντας από κάποια επίθεση ακόμα και αν αυτή επιτύχει να ξεπεράσει τα όποια μέτρα ασφάλειας στα όρια του δικτύου.

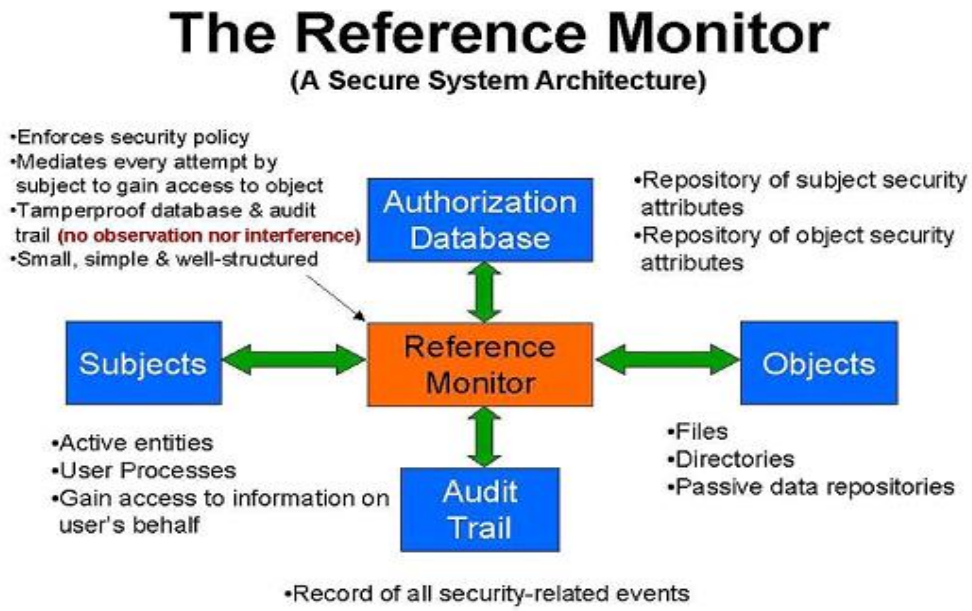
- Άρτια οργανωμένο σύστημα ανίχνευσης και πρόληψης επιθέσεων (Intrusion Detection and Prevention Systems) το οποίο έγκαιρα, επακριβώς και αποτελεσματικά θα ενημερώνει για την ύπαρξη επιθέσεων στο σύστημα και θα λαμβάνει τα κατάλληλα μέτρα για την καταρχήν αποτροπή τους.

- Σωστά καταρτισμένα συστήματα εξουσιοδότησης (authorization) και ελέγχου πρόσβασης (access control) που αξιόπιστα θα τσεκάρουν καθέναν που προσπαθεί να μπει στο δίκτυο και τις όποιες υπηρεσίες αυτό παρέχει.

- Πλήρη εφεδρικά (backup) συστήματα αποθήκευσης και αποκατάστασης σε περίπτωση επιτυχούς επίθεσης από την οποία μπορεί να καταρρεύσει το δίκτυο.

- Σύγχρονη και αξιόπιστη τεχνολογία κρυπτογράφησης που μπορεί να καταστήσει σαφώς ασφαλέστερες τις επικοινωνίες ανάμεσα σε κόμβους του εσωτερικού δικτύου αλλά και σε αυτές που πραγματοποιούνται μέσω του Internet.

- Αποτελεσματική φυσική φύλαξη του χώρου καθώς όσο άρτια και αν είναι η δικτυακή ασφάλεια, σε περίπτωση που δεν συνδυάζεται από εξίσου ισχυρή φυσική ασφάλεια, είναι σαφές ότι δεν θα έχει καμία αξία.



Εικόνα 2.2: Αρχιτεκτονική ασφαλούς συστήματος

2.3. Συνιστώσες Ασφαλείας

Οι παράγοντες που καθορίζουν τις διαφορετικές συνιστώσες, υλικό (hardware) ή λογισμικό (software), για την ασφάλεια ενός οργανισμού είναι πάρα πολλές αφού όπως έχει γίνει φανερό το εύρος που πρέπει να καλύψουν είναι αρκετά μεγάλο. Παρακάτω παρουσιάζονται ορισμένες από τις κυριότερες συνιστώσες ασφαλείας.

Η κρυπτογραφία είναι ένα εξαιρετικής σημασίας μέσο που μπορεί να χρησιμοποιηθεί προκειμένου να υπάρξει ασφάλεια. Με τη χρήση της κρυπτογραφίας, οι επικοινωνίες μπορεί να γίνουν ασφαλέστερες αφού η δυνατότητα υποκλοπής τους γίνεται ασύγκριτα δυσκολότερη. Πολλές φορές μάλιστα, κάτι τέτοιο είναι πρακτικά αδύνατον. Η κρυπτογραφία είναι δυνατόν να εφαρμοστεί σε πολλά επίπεδα: στο επίπεδο εφαρμογής, στο επίπεδο δικτύου, μεταξύ πελάτη-εξυπηρετητή, πελάτη-πελάτη, εξυπηρετητή - εξυπηρετητή κ.α. ενώ χωρίζεται σε δυο βασικές κατηγορίες. Τις μεθόδους κρυφού κλειδιού (secret key) με σημαντικότερο εκπρόσωπο την 3DES και δημόσιου κλειδιού (public key) με κυριότερες τις SSL και RSA.

Ο πυρότοιχος (firewall) αποτελεί συστατικό απαραίτητο για την ασφάλεια. Γενικά ένα firewall είναι μια συσκευή που ελέγχει τον τρόπο επικοινωνίας ανάμεσα σε δυο δίκτυα. Τυπικά αυτό που κάνει είναι να ελέγχει τα πακέτα που ανταλλάσσουν τα δυο δίκτυα φροντίζοντας να αποκόπτει όποια από αυτά είναι ύποπτα για κάποιου είδους επίθεση. Οι υλοποιήσεις πυρότοιχων που είναι διαθέσιμες σήμερα ποικίλλουν σε μέγεθος και πολυπλοκότητα λειτουργώντας σε διαφορετικά επίπεδα και εξυπηρετώντας πολλές φορές και επιπλέον σκοπούς. Ο συνδυασμός του με επιμέρους μέσα ασφαλείας επιφέρει τα απαιτούμενα αποτελέσματα.

Όλα τα παραπάνω αποτελούν την παθητική ασφάλεια ενός δικτύου και είναι αναγκαία η ύπαρξη κάποιου συστήματος που ενεργά και σε πραγματικό χρόνο θα ανιχνεύει και θα αποτρέπει επιθέσεις στο δίκτυο. Αυτού του είδους τα συστήματα είναι τα συστήματα που προαναφέραμε και θα ασχοληθούμε στην συγκεκριμένη εργασία και τα οποία καλούνται Ανίχνευσης και Πρόληψης Επιθέσεων (Intrusion Detection and Prevention Systems) και λειτουργούν εξετάζοντας το δίκτυο για ύποπτη ή πέρα από τα συνηθισμένα δραστηριότητα, καταγράφοντας και τερματίζοντας την πριν γίνει ζημιά όπου αυτό είναι δυνατόν [12].

Κεφάλαιο 3

Γνωστές και Άγνωστες Επιθέσεις

Στις μέρες μας οι επιθέσεις εναντίον κρίσιμων υπολογιστικών υποδομών έχουν πάρει μεγάλη έκταση και προκαλούν σοβαρά προβλήματα σε οργανισμούς, εταιρείες και χρήστες. Συνήθως στόχος ενός κακόβουλου είναι η κατάργηση της κανονικής λειτουργίας ενός συστήματος και η υποκλοπή απορρήτων δεδομένων προς όφελός του.

3.1. Επιθέσεις

Με τον όρο επίθεση εννοούμε την προσπάθεια να εισέλθουμε σε ένα σύστημα χωρίς να έχουμε την αντίστοιχη εξουσιοδότηση ώστε να αποσπάσουμε ή να τροποποιήσουμε πληροφορίες. Πιο κάτω αναλύονται οι κατηγορίες των πιθανών επιθέσεων που μπορεί να δεχθεί ένα δίκτυο αλλά

και οι κακόβουλοι χρήστες ή χάκερς που μπορεί να δράσουν. Τέλος γίνεται αναφορά στους πιθανούς στόχους πού είναι τα θύματα.

3.1.1 Κατηγοριοποίηση Επιθέσεων

Οι επιθέσεις μπορούν να κατηγοριοποιηθούν ανάλογα με το προφίλ που ακολουθούν και με το οποίο τις ανιχνεύουμε. Σε αυτή την παράγραφο ορίζουμε τους διαφορετικούς τύπους επιθέσεων και τις κατηγοριοποιούμε ανάλογα με τα χαρακτηριστικά τους και την συμπεριφορά που ακολουθούν, ως εξής [1, 19]:

- Απόπειρα διάρρηξης (attempted break-in): κάποιος που προσπαθεί να εισέλθει είτε σε ένα λογαριασμό χρήστη είτε στο ίδιο το σύστημα και μπορεί να εμφανίσει μεγάλα ποσοστά λανθασμένων κωδικών.

- Μεταμφιεσμένες επιθέσεις ή επιτυχής διάρρηξη (masquerading or successful break-in): κάποιος που προσπαθεί να εισέλθει παράνομα σε ένα σύστημα μέσω ενός λογαριασμού νόμιμου χρήστη που όμως δεν του ανήκει και για τον οποίον δεν έχει αντίστοιχη εξουσιοδότηση, μπορεί να έχει διαφορετική ώρα και τόπο εισόδου απ' ότι ο νόμιμος χρήστης και κάτοχος του λογαριασμού. Επιπρόσθετα, ο επιτιθέμενος μπορεί να έχει σημαντικές διαφορές στην συμπεριφορά/χρήση του συστήματος από τον κανονικό χρήστη. Μπορεί, για παράδειγμα, να περνάει πολύ χρόνο στην εξερεύνηση φακέλων και αρχείων.

- Εισβολή από νόμιμο χρήστη (penetration by legitimate user): ένας νόμιμος χρήστης που προσπαθεί να διασπάσει τους μηχανισμούς ασφάλειας του λειτουργικού συστήματος μπορεί να εκτελεί διαφορετικά προγράμματα και εντολές ώστε να κερδίσει πρόσβαση σε αρχεία και προγράμματα στα οποία δεν έχει το δικαίωμα.

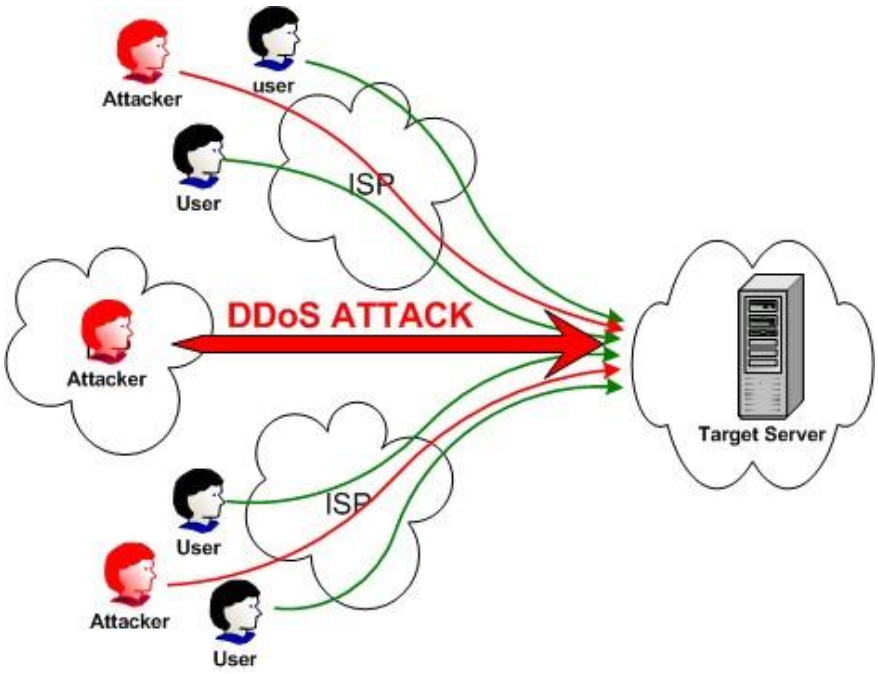
- Διαρροή από νόμιμο χρήστη (leakage by legitimate user): ένας χρήστης που θα εισέλθει στο σύστημα σε ασυνήθιστες χρονικές στιγμές και προσπαθεί να αποσπάσει ευαίσθητες πληροφορίες-έγγραφα, στέλνοντας π.χ. δεδομένα προς εκτύπωση σε μακρινούς και μη-χρησιμοποιούμενους εκτυπωτές.

- Δούρειος ίππος (Trojan horse): τύπος κακόβουλου λογισμικού που ενώ φαίνεται ότι εκτελεί επιθυμητές λειτουργίες καταφέρνει να αποκτήσει παράνομα πρόσβαση στο

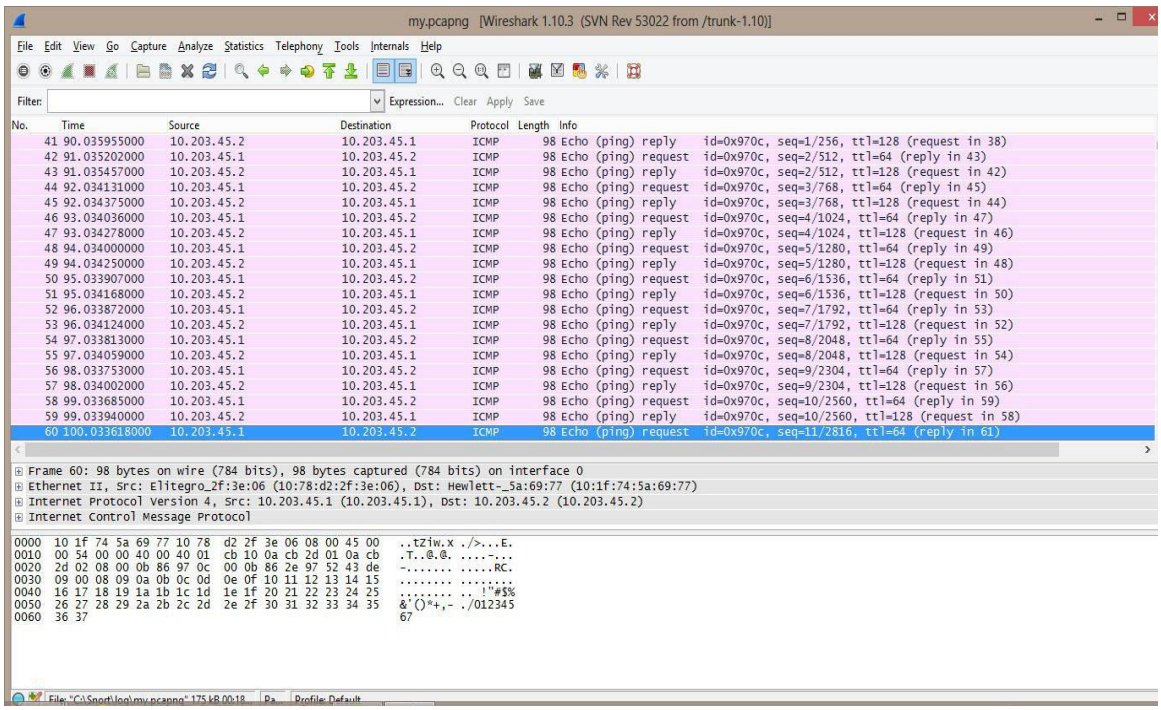
σύστημα. Δεν αναπαράγεται μόνο του (αντίθετα με τους ιούς), αλλά χρειάζεται την εκτέλεσή του από το χρήστη. Η συμπεριφορά ενός προγράμματος με εγκατεστημένο Trojan διαφέρει ως προς την φυσιολογική χρήση πόρων (συσκευές εισόδου-εξόδου, χρήση CPU) του κανονικού προγράμματος.

- Ιός (virus): ο ιός είναι λογισμικό που, αφού εκτελεστεί από έναν χρήστη του συστήματος, μπορεί και αναπαράγεται μόνο του σε ένα λειτουργικό σύστημα μολύνοντας τα αρχεία του. Ένας ιός αυξάνει σημαντικά την αντιγραφή-αναπαραγωγή εκτελέσιμων αρχείων, τη χωρητικότητα που καταλαμβάνουν ή την ίδια την εκτέλεσή τους.

- Άρνηση Υπηρεσίας (Denial-of-Service, DoS): ένας επιτιθέμενος που μονοπωλεί ένα πόρο του συστήματος (συνήθως σε δίκτυο) με ασυνήθιστα υψηλή δραστηριότητα. Συνήθως η επίθεση γίνεται αντιληπτή όταν ο χρήστης δεν μπορεί να έχει πρόσβαση στον πόρο ενώ το δικαιούται. Όταν, για τον ίδιο σκοπό, χρησιμοποιούνται περισσότερα από ένα συστήματα-επιτιθέμενοι, η επίθεση μετατρέπεται σε Διανεμημένη Άρνηση Υπηρεσίας (Distributed Denial-of-Service, DDoS).



Εικόνα 3.1.1.1: Άρνηση Υπηρεσίας (Denial-of-Service, DoS)



Εικόνα 3.1.1.2 : Η ping επίθεσης που φαίνεται, οδηγεί σε Denial of Service. Η διεύθυνση IP του μηχανήματος που έχει 10.203.45.1 δημιουργεί μία ping επίθεση στο μηχάνημα που έχει τη διεύθυνση IP 10.203.45.2.[3]

- Σκουλήκι (worm): το σκουλήκι είναι ένα αυτοαναπαραγόμενο και κακόβουλο πρόγραμμα υπολογιστή, το οποίο χρησιμοποιεί δίκτυο υπολογιστών για να στείλει αντίγραφα του εαυτού του σε άλλους κόμβους (υπολογιστές του δικτύου) και μπορεί να το πράξει χωρίς την παρέμβαση του χρήστη. Το γεγονός αυτό οφείλεται σε κενά ασφαλείας του υπολογιστή προορισμού [10]. Η διαφορά του με τον ιό έγκειται στο γεγονός ότι ο τελευταίος χρειάζεται για την εκτέλεσή του την παρέμβαση κάποιου χρήστη, μολύνει αρχεία στατικά και δεν διαδίδεται σε ένα δίκτυο χωρίς την παρέμβαση κάποιου χρήστη.

3.1.2 Κακόβουλοι Χρήστες, Hackers και Crackers

Η συσχέτιση αυτών των εννοιών με την πάροδο του χρόνου βάση των ενεργειών και δραστηριοτήτων τους, οδήγησε τους οργανισμούς /εταιρείες αλλά και τα μέσα ενημέρωσης να τους αντιμετωπίζουν σαν κοινό στόχο.

Θα επικεντρωθούμε περισσότερο με την έννοια του hacker η οποία είναι και η ποιο πολύ διαδεδομένη. Ξεκίνησε από μία τηλεφωνική εταιρεία την Packard Bell. Τότε περίπου υπήρξαν οι πρώτοι hackers που δεν ξεπερνούσαν τα όρια της φάρσας, μέχρι τη δεκαετία του ’60. Οι σπουδαστές του πανεπιστημίου MIT, είχαν τη φυσική περιέργεια για τον τρόπο λειτουργίας κάθε συσκευής που υπήρχε. Οι υπολογιστές τότε ήταν mainframes, μηχανήματα κλειδωμένα σε δωμάτια με ελεγχόμενη θερμοκρασία. Το κόστος λειτουργίας τους ήταν απαγορευτικό και οι ερευνητές είχαν στη διάθεσή τους περιορισμένο χρόνο εργασίας. Τότε, οι πιο έξυπνοι από αυτούς, δημιούργησαν τα πρώτα hacks, προγράμματα που βοηθούσαν στη γρηγορότερη εκτέλεση υπολογισμών. Αρκετές φορές τα hacks ήταν καλύτερα προγράμματα από τα αρχικά. Ίσως το καλύτερο hack της ιστορίας έγινε το 1969, όταν δύο υπάλληλοι της Bell συνέθεσαν κάποιες εντολές για να αυξήσουν την ταχύτητα των υπολογιστών, και το hack το ονόμασαν UNIX. Τη δεκαετία του ’70 το hacking ήταν εξερεύνηση και κατανόηση του τρόπου λειτουργίας του νέου κόσμου. Γύρω στο 1971, ένας βετεράνος του Βιετνάμ ανακάλυψε ότι η σφυρίχτρα που έδιναν δώρο τα δημητριακά Cap ‘n’ Crunch παρήγαγε ήχο συχνότητας 2600 mhz. Απλά σφύριζε στην τηλεφωνική συσκευή και έκανε τηλεφωνήματα χωρίς χρέωση. Το μόνο που έλειπε από τη σκηνή της δεκαετίας του ’70 ήταν ένα εικονικό μαγαζί συγκέντρωσης των hackers. Το 1978, οι Randy Sousa και Ward Christiansen δημιούργησαν το πρώτο BBS (Bulletin Board System) που λειτουργεί μέχρι και σήμερα [11].

Σήμερα με τον όρο hacker χαρακτηρίζεται το άτομο που έχει πολλές τεχνικές γνώσεις για τους υπολογιστές αλλά και προχωρημένες γνώσεις προγραμματισμού, μπορεί να εντοπίσει αδυναμίες σε συστήματα υπολογιστών, να λύνει τεχνικά προβλήματα, να βελτιώνει εφαρμογές αλλά και που συνεργάζεται μ’ άλλους ομοίους για την επίλυση των προβλημάτων των υπολογιστών, χωρίς όμως να προξενεί κάποια ζημιά. Σε όλες τις περιπτώσεις οι hackers είναι άτομα με αυξημένο δείκτη νοημοσύνης [5].

Οι κατηγορίες στις οποίες διακρίνονται οι hackers είναι:

- White hat hackers

Άτομα που τους αρέσει να “σπάνε” την ασφάλεια συστημάτων για μη κακόβουλους σκοπούς. Τους αρέσει η γνώση, το να κατανοούν πώς λειτουργεί κάποιο πρόγραμμα ή μηχανισμός.

- Crackers ή Black hat hackers

Οι **crackers** (*criminal hackers*) θεωρούνται ως οι κακόβουλοι hackers και έχουν ως στόχο την πρόκληση ζημιάς σε δίκτυα υπολογιστών, την εισβολή σε υπολογιστές χρηστών χωρίς εξουσιοδότηση, την δημιουργία ιών, την παραβίαση κωδικών ασφαλείας, την καταστροφή ή και την αλλοίωση δικτυακών τόπων (Web sites) όπου αφήνουν περήφανα την δικτυακή τους σφραγίδα με το ψευδώνυμό τους, την δημιουργία πειρατικών αντιγράφων προγραμμάτων ή τραγουδιών ή βίντεο κ.ά.

- Script kiddie

Είναι άτομα χωρίς πολλές γνώσεις, που χρησιμοποιούν έτοιμα προγράμματα για να κάνουν επιθέσεις ή φιγούρα στους φίλους τους. Είναι άτομα που, καλά καλά, δε χαρακτηρίζονται hackers.

- Hacktivists ή νέο-hackers

Είναι άτομα που χρησιμοποιούν τις γνώσεις τους με σκοπό να πουν ή προωθήσουν μια κοινωνική, ιδεολογική, θρησκευτική ή πολιτική γνώμη. Στις περισσότερες περιπτώσεις καταστρέφουν την κεντρική σελίδα από γνωστά site ή το αλλάζουν με σκοπό να γελοιοποιήσουν τον ιδιοκτήτη. Σπάνια, χρησιμοποιούν τις γνώσεις τους στο όνομα της internet - τρομοκρατίας.

3.1.3 Θύματα

Πρόκειται για υπολογιστές και γενικότερα για ΠΣ ή δικτυακούς πόρους. Αρχικά, ένας υπολογιστής όπου υπάρχει πιθανότητα να γίνει μέσο εκμετάλλευσης από έναν επιτιθέμενο είναι ένας *στόχος* (target). Αν υπάρξει συμβάν που παραβιάζει την ασφάλεια του στόχου τότε έχουμε έναν *υπολογιστή-θύμα* (victim) [1].

Κεφάλαιο 4
Συστήματα Ανίχνευσης και Πρόληψης Επιθέσεων

Στο κεφάλαιο αυτό θα γίνει μια επισκόπηση των συστημάτων ανίχνευσης και πρόληψης επιθέσεων (IDPS), καθώς και πώς μπορούν να χρησιμοποιηθούν. Έπειτα, περιγράφονται οι βασικές λειτουργίες που τα συστήματα αυτά εκτελούν αλλά και οι μεθοδολογίες ανίχνευσης που χρησιμοποιούν.

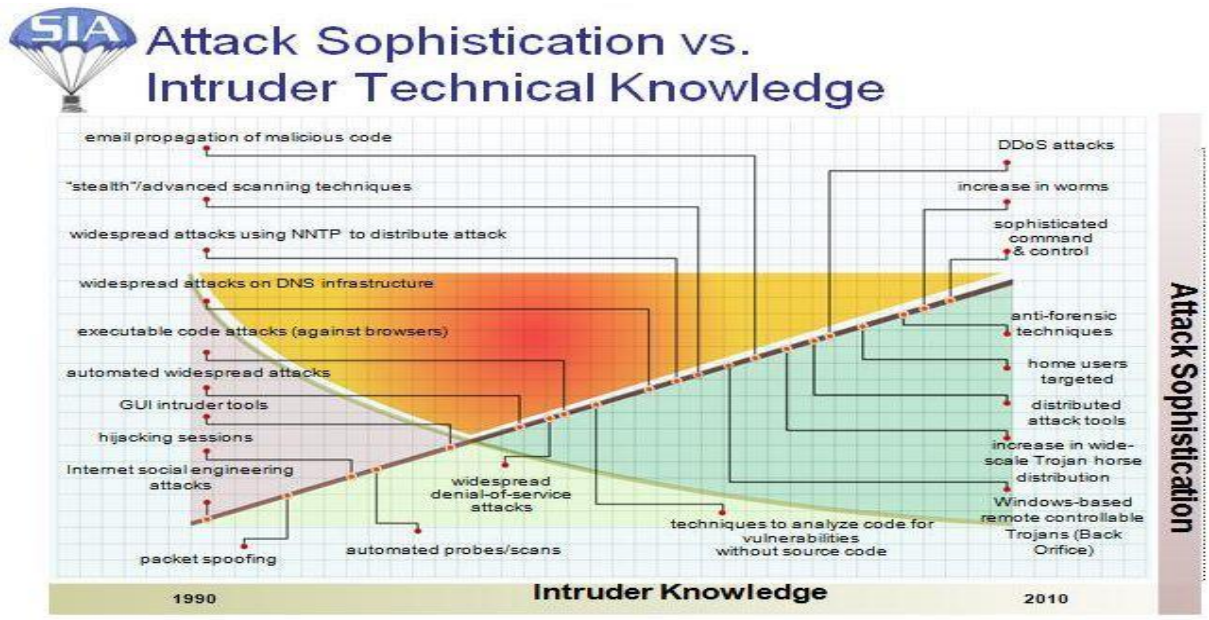
4.1 Ορισμός IDPS

Ανίχνευση επιθέσεων είναι η διαδικασία παρακολούθησης γεγονότων-συμβάντων που συμβαίνουν σε ένα ΠΣ ή δίκτυο και η ανάλυσή τους για πιθανές απειλές. Το λογισμικό/σύστημα που υλοποιεί αυτή την διαδικασία ονομάζεται *Σύστημα Ανίχνευσης Εισβολών* (IDS) [41]. Ένα

σύστημα πρόληψης εισβολής (IPS) είναι λογισμικό που έχει όλες τις ικανότητες ενός συστήματος ανίχνευσης εισβολής και μπορεί επίσης να προσπαθήσει να σταματήσει τα πιθανά γεγονότα.

Τα συστήματα IDS και IPS παρουσιάζουν τις ίδιες ικανότητες, και οι διαχειριστές μπορούν συνήθως να θέσουν εκτός λειτουργίας τα χαρακτηριστικά γνωρίσματα πρόληψης IPS στα προϊόντα, αναγκάζοντας τα για να λειτουργήσουν ως IDS. Συνεπώς, για τη συντομία τα συστήματα ανίχνευσης και πρόληψης επιθέσεων όρου (IDPS) χρησιμοποιούνται σε όλο το υπόλοιπο της εργασίας για να αναφερθούν και σε IDS και IPS συστήματα.

Το IDPS στρέφεται πρώτιστα στον προσδιορισμό των πιθανών γεγονότων. Παραδείγματος χάριν, ένα IDPS θα μπορούσε να ανιχνεύσει πότε ένας επιτιθέμενος έχει συμβάλει επιτυχώς ένα σύστημα με την εκμετάλλευση μιας ευπάθειας του συστήματος. Το IDPS θα μπορούσε έπειτα να εκθέσει το γεγονός στους διαχειριστές ασφάλειας, οι οποίοι θα μπορούσαν γρήγορα να αρχίσουν τις συναφείς ενέργειες για να ελαχιστοποιήσουν τη ζημία που προκλήθηκε από την επίθεση. Το IDPS θα μπορούσε επίσης να καταγράψει τις πληροφορίες που θα μπορούσαν να χρησιμοποιηθούν έναντι των επιθέσεων. Επιπλέον το IDPS μπορεί να διαμορφωθεί για να αναγνωρίσει τις παραβιάσεις των πολιτικών ασφάλειας. Χαρακτηριστικά αναφέρεται και η εξής έκφραση ότι << an IDPS catches the threats the firewall misses >>. Επίσης, κάποιο IDPS μπορεί να ελέγξει τις μεταφορές αρχείων και να προσδιορίσει αυτούς που η κίνηση τους είναι ύποπτη, όπως η αντιγραφή μιας μεγάλης βάσης δεδομένων επάνω στο laptop ενός χρήστη. Τέλος πολλά IDPSs μπορούν να προσδιορίσουν τη δραστηριότητα αναγνώρισης, η οποία μπορεί να δείξει ότι μια επίθεση είναι επικείμενη [41].



Εικόνα 4.1 : Ανάλυση δυνατοτήτων IDPS

4.2 Στόχοι IDPS

Οι στόχοι των πραγματικών συστημάτων ανίχνευσης και πρόληψης επιθέσεων είναι [4]:

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

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

3. *Παρουσίαση της ανάλυσης με απλή και εύκολα αντιληπτή μορφή:* Θα ήταν επιθυμητό τα αποτελέσματα ανίχνευσης μιας επίθεσης να προκύπτουν, τελικά, από την τιμή μιας

δίτιμης μεταβλητής. Συνήθως, όμως, αυτό δεν μπορεί να συμβεί αφού οι επιθέσεις δεν είναι λειτουργικά τόσο σαφείς. Για το λόγο αυτό, ο μηχανισμός ανίχνευσης επιθέσεων παρουσιάζει περισσότερο σύνθετα δεδομένα στον υπεύθυνο ασφάλειας του συστήματος. Εκείνος, με τη σειρά του, πρέπει να συνάγει αν πρέπει να ληφθούν κάποια μέτρα και ποια ακριβώς πρέπει να είναι αυτά. Επειδή οι μηχανισμοί ανίχνευσης επιθέσεων μπορεί να παρακολουθούν περισσότερα από ένα συστήματα, ιδιαίτερη κρισιμότητα παρουσιάζει η διεπαφή τους με το χρήστη.

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

4.3. Χαρακτηριστικά Ενός Καλού Συστήματος IDPS

Τα συστήματα IDPS παρουσιάζουν σήμερα τρομερή εξέλιξη και αποτέλεσμα αυτού είναι να υπάρχουν πάρα πολλά διαθέσιμα. Προκειμένου να επιλέξουμε κάποιο, θα πρέπει να λάβουμε υπόψη μας, εκτός φυσικά από το κόστος του, και τα παρακάτω χαρακτηριστικά [6]:

- Ένα καλό IDPS λειτουργεί διαρκώς, χωρίς να χρειάζεται ανθρώπινη παρουσία παρά μόνο την παρακολούθηση του και την συλλογή των αποτελεσμάτων ελέγχου. Τα αποδοτικά συστήματα επεξεργάζονται πληροφορίες του συστήματος που επιτηρούν και προσφεύγουν στο διαχειριστή ασφάλειας μόνο όταν ανιχνευτεί με βεβαιότητα κάποια επίθεση ή υπάρξει υποψία μιας νέας επίθεσης, για την οποία δεν υπάρχουν γνωστοί τρόποι αντιμετώπισης.

- Ένα καλό IDPS πρέπει επίσης να είναι ανεκτικό σε παραβιάσεις του συστήματος το οποίο επιτηρεί. Μετά την προσβολή από κάποιον εισβολέα, είναι απαραίτητη η επαναφορά του

συστήματος στην προηγούμενη κατάστασή του. Η επανάκτηση των συστημάτων αρχείων που πιθανόν καταστράφηκαν και η απομάκρυνση μορφών που πιθανόν προσέβαλαν το σύστημα αποτελούν βασικές λειτουργίες ενός αποτελεσματικού IDPS. Από την άλλη μεριά, το ίδιο το IDPS πρέπει να μπορεί να επανέλθει σε κανονική λειτουργία μετά από μια διακοπή του επιτηρούμενου συστήματος.

- Ένα καλό IDPS είναι ανεκτικό σε παραβιάσεις των ίδιων του των στοιχείων. Κοινό χαρακτηριστικό της τακτικής που ακολουθούν πολλοί εισβολείς είναι η διαγραφή κάθε στοιχείου που μπορεί να προδώσει την παρουσία τους στο σύστημα. Τα ίχνη ελέγχου, λοιπόν, που αποτελούν ζωτική είσοδο στο IDPS, πρέπει να φυλάσσονται σε ασφαλή μέρη. Επιπλέον, το IDPS πρέπει να αντιλαμβάνεται απόπειρες τροποποίησης των στοιχείων αυτών. Πρέπει, επίσης, να ανθίσταται σε απόπειρες παραποίησης των βάσεων γνώσης του, των κανόνων που χρησιμοποιεί, των στατιστικών προφίλ, των μετρικών και των ορίων ευαισθησίας του.

- Ένα καλό IDPS είναι οικονομικό. Στόχος του είναι η αποδοτικότερη και αδιάλειπτη λειτουργία του συστήματος που επιτηρεί και όχι η παρεμπόδιση και μείωση της αποτελεσματικότητάς του. Πρέπει, συνεπώς, το IDPS να απασχολεί όσο το δυνατόν λιγότερους από τους πόρους του συστήματος.

- Ένα καλό IDPS είναι γρήγορο. Η ανακάλυψη μιας εισβολής μετά από μεγάλο χρονικό διάστημα αφ' ότου αυτή ολοκληρώθηκε, αποτελεί μεν επιτυχία του IDPS, αλλά η ζημιά μπορεί ήδη να έχει γίνει.

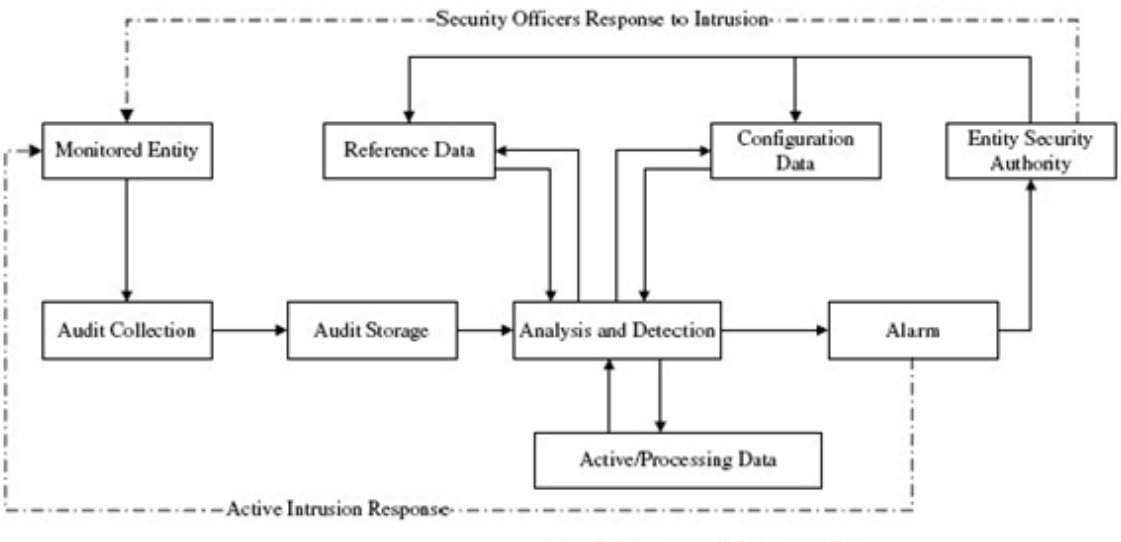
- Ένα καλό IDPS είναι προσαρμόσιμο. Παρ' όλο που τα περισσότερα από τα σημερινά δικτυωμένα υπολογιστικά συστήματα βασίζονται σε πλατφόρμες Unix, καθένα τους έχει τις δικές του διαφορετικές πολιτικές ασφάλειας, που πηγάζουν από διαφορετικές απαιτήσεις ασφάλειας. Συνεπώς, ένα αποτελεσματικό IDPS πρέπει να μπορεί να προσαρμόζεται εύκολα σε διαφορετικά υπολογιστικά περιβάλλοντα.

- Ένα καλό IDPS είναι αναβαθμίσιμο. Πρέπει όχι μόνο να υπάρχει δυνατότητα εισαγωγής νέων τεχνικών ανίχνευσης και αντιμετώπισης απειλών, αλλά και συνύπαρξης αυτών των τεχνικών και αποδοτικής διαλειτουργίας τους με τις υπάρχουσες.

- Ένα καλό IDPS είναι συντηρήσιμο. Η συντήρηση της βάσης γνώσης των IDPS που χρησιμοποιούν έμπειρα συστήματα δεν είναι και τόσο εύκολη υπόθεση, επειδή απαιτεί γνώσεις διατήρησης και δημιουργίας βάσεων γνώσης, έμπειρων συστημάτων και κανόνων. Το υποσύστημα λήψης απόφασης του IDPS πρέπει να μπορεί να ενημερώνεται εύκολα, χωρίς να απαιτούνται ειδικές γνώσεις, τις οποίες ένας διαχειριστής συστήματος συνήθως δεν έχει. Η ικανότητα μάθησης και καλής αξιοποίησης και διαχείρισης της ήδη αποκτηθείσας γνώσης αποτελεί αναγκαίο χαρακτηριστικό ενός καλού IDPS, αν σκεφτούμε το μέγεθος που μπορεί να αποκτήσει μια συνεχώς ενημερωμένη βάση γνώσης. Τέλος, ένα καλό IDPS ελαχιστοποιεί τις λαθεμένες αρνητικές αποφάσεις (false negatives). Αναλυτικότερα, ένα καλό IDPS έχει την ικανότητα να μη χαρακτηρίζει μια ενέργεια ως φυσιολογική, ενώ στην πραγματικότητα αυτή είναι απειλητική. Η συμπεριφορά αυτή είναι προτιμότερη από αυτήν που χαρακτηρίζει μια πράξη ως απειλητική, ενώ στην πραγματικότητα είναι φυσιολογική (false positive).

4.4 Γενικό Μοντέλο IDPS

Σήμερα για να δράσει ένα IDPS σε οποιοδήποτε σύστημα θα πρέπει να έχει τα παρακάτω χαρακτηριστικά και να παρουσιάζει την μορφή του πιο κάτω μοντέλου (Εικόνα 4.4):



Εικόνα 4.4 : Γενικό μοντέλο IDPS

4.5. Μοντέλα Εισβολών και Τρόποι Ανάλυσης Πληροφοριών

Όπως αναφέρθηκε και προηγουμένως τα συστήματα ανίχνευσης εισβολών προσδιορίζουν εάν κάποιες ενέργειες αποτελούν εισβολές, με βάση ένα ή περισσότερα μοντέλα εισβολών (models of intrusion). Στη παράγραφο αυτή θα γίνει μία προσέγγιση αλλά και ανάλυση διάφορων μοντέλων που ανάλογα με τον τρόπο που δρουν κατατάσσονται σε διάφορες κατηγορίες. Τα σημαντικότερα είναι τα μοντέλα ανίχνευσης διαταραχών (anomaly models) τα οποία με βάση στατιστικά στοιχεία ταξινομούν τις ενέργειες ή καταστάσεις που είναι στατιστικά ασυνήθιστες ως «κακές», τα μοντέλα κακής συμπεριφοράς (misuse models) τα οποία συγκρίνουν ενέργειες ή καταστάσεις με ακολουθίες που είναι ήδη γνωστές ότι αποτελούν εισβολές, ή με ακολουθίες που θεωρείται ότι αποτελούν εισβολές και τις ταξινομούν ως «κακές» και τα μοντέλα που βασίζονται στις προδιαγραφές (specification-based models) τα οποία ταξινομούν τις καταστάσεις που παραβιάζουν τις προδιαγραφές ως «κακές». Τα μοντέλα μπορεί να είναι είτε προσαρμοστικά (adaptive) δηλαδή μοντέλα που αλλάζουν τη συμπεριφορά τους με βάση τις καταστάσεις και τις ενέργειες των συστημάτων, είτε στατικά (static) δηλαδή μοντέλα που αρχικοποιούνται από δεδομένα που έχουν συλλεγεί και δεν τροποποιούνται κατά τη διάρκεια εκτέλεσης του συστήματος. Τέλος αναφέρεται ότι τα μοντέλα αυτά μπορούν να συνδυαστούν μεταξύ τους παρέχοντας μεγαλύτερο επίπεδο ασφάλειας αλλά και απόδοσης.

4.5.1 Μοντέλο Ανίχνευσης Διαταραχών.

Το 1993 ο Steven Bellovin δημοσίευσε μία εργασία με τίτλο "Packets Found on an Internet", στην οποία περιγράφει την ανώμαλη δικτυακή κυκλοφορία. Και προσδιορίζει μια ανώμαλη μετάδοση κυκλοφορίας (broadcast traffic). Ο Bellovin συμπεραίνει: «για μερικούς, τα ευρήματα μπορούν να περιγράφουν λακωνικά με τη φράση «λάθη συμβαίνουν» ("bugs happen").

Οι τεχνικές ανίχνευσης διαταραχών καταλήγουν στο συμπέρασμα ότι όλες οι επιθετικές δραστηριότητες είναι αναγκαστικά ανωμαλίες. Αυτό σημαίνει ότι αν μπορούσαμε να καθιερώσουμε ένα "σύνηθες προφίλ δραστηριότητας" για ένα σύστημα, θα ήμασταν σε θέση, θεωρητικά, να σημαδέψουμε όλες τις καταστάσεις του συστήματος που αποκλίνουν από το καθιερωμένο προφίλ. Αυτό μπορεί να γίνει με βάση ένα, στατιστικά, σημαντικό νούμερο προσπαθειών εισβολής. Παρόλα αυτά αν συλλογιστούμε ότι το σύνολο των επιθετικών

δραστηριοτήτων αλλάζει την κατάσταση του συστήματος από την αρχική του μορφή, βγάζουμε κάποιες ενδιαφέρουσες εκδοχές [7] :

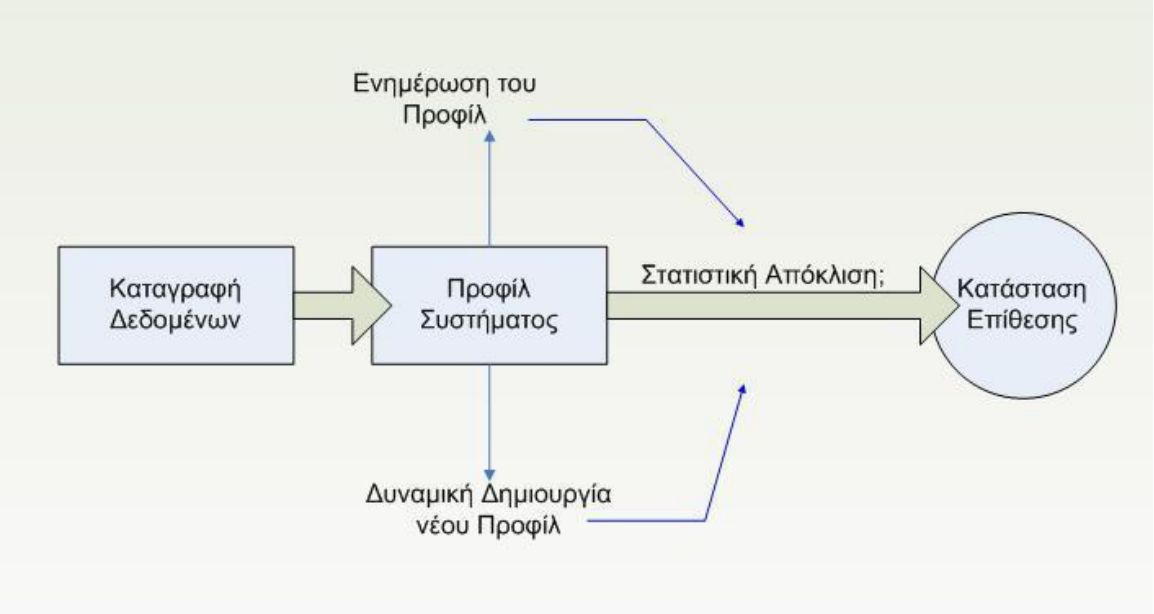
- Ασυνήθεις δραστηριότητες που δεν έχουν χαρακτήρα εισβολής χαρακτηρίζονται ως επιθετικές.

- Επιθετικές δραστηριότητες που δεν είναι ασυνήθεις, καταλήγουν σε false negatives (γεγονότα δεν χαρακτηρίζονται ως επιθέσεις, ενώ στην πραγματικότητα είναι).

Αυτό είναι ένα ιδιαίτερα επικίνδυνο πρόβλημα και μάλιστα σοβαρότερο από το πρόβλημα των false positive (γεγονότα χαρακτηρίζονται ως επιθέσεις, ενώ δεν είναι στην πραγματικότητα).

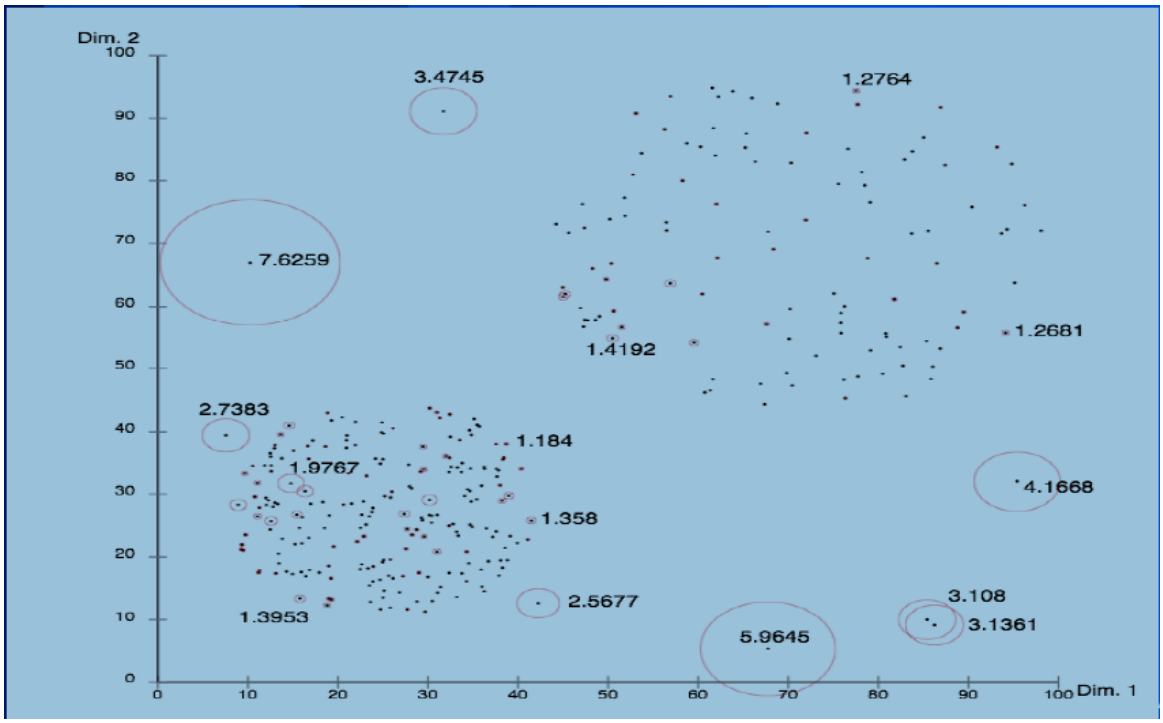
Τα κυριότερα θύματα λοιπόν, στην ανίχνευση διαταραχή σε συστήματα ανιχνεύσεις επικλήσεων, είναι να γίνονται οι επιλογές μέσα στα επίπεδα των ορίων, ώστε κανένα από τα δύο παραπάνω προβλήματα να μην μεγιστοποιείται. Σημαντική είναι, επίσης και η επιλογή των χαρακτηριστικών στην παρακολούθηση δεδομένων. Τα συστήματα ανίχνευσης διαταραχής είναι υπολογιστικά ακριβά, λόγω του κόστους του ελέγχου και της συνεχούς ανανέωσης (updating) των μετρικών του προφίλ ενός συστήματος.

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



Εικόνα 4.5.1.1 : Μοντέλο ανίχνευσης διαταραχών

Γραφική αναπαράσταση μιας κατατομής:



Εικόνα 4.5.1.2 : Γραφική αναπαράσταση μιας κατατομής με μοντέλο ανίχνευσης διαταραχών

Μερικές από τις σημαντικές προσεγγίσεις στα συστήματα ανίχνευσης διαταραχής αναλύονται παρακάτω.

4.5.1.1 Νευρωνικά Δίκτυα

Μια σημαντική μέθοδος που χρησιμοποιείται στα συστήματα εντοπισμού εισβολών είναι τα νευρωνικά δίκτυα. Η ιδέα εδώ είναι να «εκπαιδεύσουμε» ένα νευρωνικό δίκτυο με τέτοιο τρόπο, ώστε να μπορεί να προβλέψει την επόμενη εντολή σε ενέργεια ενός χρήστη, με βάση προηγούμενες εντολές και ενέργειες. Το δίκτυο λειτουργεί με βάση ένα σύνολο εντολών, αντιπροσωπευτικών του χρήστη. Μετά την περίοδο εκμάθησης το δίκτυο προσπαθεί να ταιριάξει πραγματικές εντολές με το πραγματικό προφίλ του χρήστη, που ήδη υπάρχει στο δίκτυο. Όσα γεγονότα προβλεφθούν λάθος στην πραγματικότητα απεικονίζουν την διαφοροποίηση του χρήστη από το προφίλ του.

Κάποια πλεονεκτήματα των νευρωνικών δικτύων είναι ότι τα καταφέρνουν καλά με πολύπλοκα δεδομένα, η επιτυχία τους δεν εξαρτάται από καμία στατιστική υπόθεση για την φύση των δεδομένων και είναι πιο εύκολο να μετατραπούν για διαφορετικές ομάδες χρηστών. Όμως υπάρχουν και προβλήματα. Πρώτα ένα μικρό σύνολο πληροφοριών θα επιφέρει πολλά false positives, ενώ ένα άλλο θα επιφέρει άσχετα δεδομένα. Επίσης η τοπολογία του δικτύου δημιουργείται μετά από πολλά λάθη και τέλος ο εισβολέας μπορεί να «εκπαιδεύσει» το δίκτυο κατά την φάση εκμάθησης [12].

4.5.1.2 Γενετική Πρόβλεψη Προτύπων

Με αυτή την μέθοδο θέλουμε να προβλέψουμε μελλοντικά γεγονότα στηριζόμενη σε γεγονότα τα οποία έχουν συμβεί και καταγραφεί [25]. Οπότε ισχύει ο εξής κανόνας: E1 - E2 (E3 = 80%, E4 = 15%, E5 = 5%) Αυτό σημαίνει ότι με δεδομένα τα γεγονότα E1 και E2 και με το E2 να ακολουθεί το E1 στο χρόνο, υπάρχει 80% πιθανότητα να ακολουθήσει το γεγονός E3, 15 % να ακολουθήσει το E4 και 5% να ακολουθήσει το E5. Το πρόβλημα είναι ότι μερικά επιθετικά σενάρια που δεν έχουν προβλεφτεί από το σύστημα θα χαρακτηριστούν σαν εισβολή. Δηλαδή, αν μια ακολουθία γεγονότων A-B-C υπάρχει και είναι εισβολή, αλλά δεν βρίσκεται στη βάση των κανόνων, θα καταχωρηθεί απλά ως άγνωστη. Αυτό το πρόβλημα μπορεί να λυθεί μερικώς με τον χαρακτηρισμό οποιουδήποτε αγνώστου γεγονότα ως εισβολή .

Υπάρχουν πολλά πλεονεκτήματα σε αυτήν την προσέγγιση [25]. Πρώτο στηριζόμενος σε πρότυπα και κανόνες μπορείς να ανιχνεύσεις εισβολές ποιο εύκολα από τις παραδοσιακές μεθόδους. Επίσης τα συστήματα που κατασκευάζονται χρησιμοποιώντας αυτό το μοντέλο είναι ιδιαίτερα προσαρμοστικά σε αλλαγές. Αυτό συμβαίνει γιατί τα λιγότερο καλά και αποτελεσματικά πρότυπα συνεχώς εξαλείφονται, ενώ παραμένουν τα πολύ ποιοτικά μόνο πρότυπα. Εξίσου σημαντικό , είναι το γεγονός ότι είναι πιο εύκολο να εντοπιστούν χρήστες που προσπαθούν να εκπαιδεύσουν το σύστημα κατά τον τρόπο που τους βολεύει και κυρίως κατά την διάρκεια που μαθαίνει. Τέλος οι ανώμαλες δραστηριότητες εντοπίζονται και ανακόπτονται μέσα σε λίγα δευτερόλεπτα από τη στιγμή της λήψης της κρίσιμης πληροφορίας.

4.5.1.3 Στατιστική Προσέγγιση

Στην μέθοδο αυτή, αρχικά δημιουργούνται τα πρότυπα συμπεριφοράς για τα υπό εξέταση αντικείμενα. Καθώς το σύστημα συνεχίζει να τρέχει , ο ανιχνευτής διαταραχών συνεχώς παράγει

την διακύμανση του παρόντος προφίλ σε σχέση με την αρχική κατάσταση [32]. Σε μερικά συστήματα το παρόν προφίλ και το προηγούμενο συνενώνονται ανά διαστήματα, ενώ σε άλλα η παραγωγή προφίλ γίνεται σε μια χρονική περίοδο. Το κυριότερο πλεονέκτημα των στατιστικών συστημάτων είναι ότι συνεχώς προσαρμόζονται καλύτερα στην παρακολούθηση της συμπεριφοράς των χρηστών. Συνεπώς είναι πιο ευαίσθητα από τον ανθρώπινο παράγοντα. Πάντως, υπάρχουν μερικά προβλήματα με αυτά τα συστήματα, γιατί μπορούν σταδιακά να κατευθυνθούν με τέτοιο τρόπο από εισβολείς, ώστε να οδηγούνται σε λάθος εκτιμήσεις. Για παράδειγμα, γεγονότα εισβολής να εκτιμηθούν ως φυσιολογικά, false negatives ή false positives να παράγονται ανάλογα με το όριο ύπαρξης ή με ύπαρξης διαταραχής (threshold) είναι πολύ μικρό ή μεγάλο αντίστοιχα και σχέσεις μεταξύ γεγονότων να μην αναφερθούν λόγω της μικρής ευαισθησίας των στατιστικών παραγόντων που χρησιμοποιούνται [32].

Παραδείγματα στατιστικών μοντέλων είναι το μοντέλο τιμών κατωφλίου, το μοντέλο στατιστικών ροπών και το μοντέλο Markov. Αναλυτικότερα παρουσιάζονται ως εξής [22]:

- **Μοντέλο Τιμών Κατωφλίου:**

Το μοντέλο αυτό χρησιμοποιεί μία μετρική σχετιζόμενη με τιμές κατωφλίου (threshold metric). Αναμένεται να εμφανιστούν γεγονότα κατ' ελάχιστο m και κατά μέγιστο n, για κάποιο γεγονός και κάποιες τιμές m και n. Εάν κατά τη διάρκεια μιας συγκεκριμένης χρονικής περιόδου εμφανίζονται λιγότερα από m γεγονότα ή περισσότερα από n, τότε η συμπεριφορά θεωρείται διαταραγμένη. Ο καθορισμός των τιμών κατωφλίου αυξάνει την πολυπλοκότητα του μοντέλου. Οι τιμές κατωφλίου πρέπει να λάβουν υπόψη τα χαρακτηριστικά των χρηστών και τα διαφορετικά επίπεδα εξειδίκευσής τους.

- **Μοντέλο Στατιστικών Ροπών:**

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

αποφάσεις. Τα μοντέλα στατιστικών ροπών παρέχουν περισσότερη ευελιξία από τα μοντέλα τιμών κατωφλίου.

- **Μοντέλο Markov:**

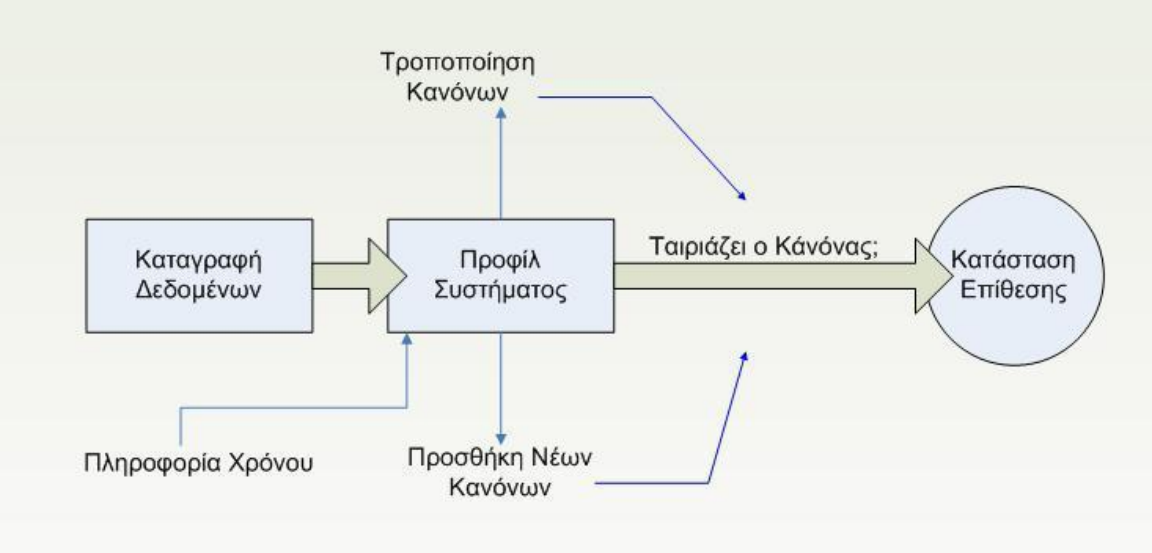
Το μοντέλο αυτό εξετάζει ένα σύστημα σε μία συγκεκριμένη χρονική στιγμή. Τα γεγονότα που προηγήθηκαν χρονικά έχουν θέσει το σύστημα σε μια συγκεκριμένη κατάσταση. Όταν συμβεί το επόμενο γεγονός, το σύστημα μεταβαίνει σε μία νέα κατάσταση. Προϊόντος του χρόνου μπορεί να αναπτυχθεί ένα σύνολο πιθανοτήτων μετάβασης. Όταν συμβεί ένα γεγονός που προκαλεί μία μετάβαση με μικρή πιθανότητα, το γεγονός κρίνεται διαταραγμένο. Το μοντέλο προτείνει τη χρήση κάποιας κατάστασης (state), ή προϊστορίας για τον εντοπισμό των διαταραχών. Οι διαταραχές δεν είναι πλέον βασισμένες σε στατιστικά των περιστατικών μεμονωμένων γεγονότων, αλλά σε ακολουθίες γεγονότων. Αυτή η προσέγγιση δηλώνει εντοπισμό κακής συμπεριφοράς (misuse detection) και χρησιμοποιήθηκε για την ανάπτυξη αποτελεσματικών μηχανισμών εντοπισμού διαταραχών.

4.5.2. Μοντέλο Κακής Συμπεριφοράς

Αναλύοντας αρχικά τον όρο κακή συμπεριφορά (misuse) σε κρίσιμα υπολογιστικά περιβάλλοντα καταλήγουμε ότι αναφέρεται σε μια επίθεση από έναν εσωτερικό ή έναν εξουσιοδοτημένο χρήστη. Στα συστήματα ανίχνευσης και πρόληψης επιθέσεων, ο όρος κακή συμπεριφορά αναφέρεται στη βασισμένη-σε-κανόνες ανίχνευση. Η ανίχνευση κακής συμπεριφοράς (Signature or Misuse Detection, Knowledge - based Detection) προσδιορίζει εάν μία ακολουθία εντολών που εκτελείται παραβιάζει την πολιτική ασφάλειας των περιοχών στις οποίες εκτελείται. Σε αυτή την περίπτωση, περιγράφεται μία πιθανή εισβολή [4].

Βασιζόμενη στα ποιο πάνω καταλήγουμε ότι το misuse detection είναι ότι υπάρχουν τρόποι αναπαράστασης επιθέσεων με τη μορφή ενός αποτυπώματος ή signature, ώστε ακόμα και παραλλαγές της επίθεσης να μπορούν να ανιχνευτούν [7]. Άρα τα συστήματα αυτά μοιάζουν πολύ με τα antivirus προγράμματα, και μπορούν να ανιχνεύσουν πολλά ή όλα τα γνωστά πρότυπα εισβολής, αλλά δεν είναι αποτελεσματικά σε άγνωστες τεχνικές επιθέσεις.. Το σημαντικότερο στα misuse detection συστήματα είναι το πώς θα δημιουργήσουμε signatures που να περιγράφουν όλες τις παραλλαγές μιας σχετικής επίθεσης και πώς θα δημιουργήσουμε signatures που αγνοούν την μη επιθετική δραστηριότητα.

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



Εικόνα 4.5.2 : Μοντέλο κακής συμπεριφοράς

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

Η τεχνική της ανίχνευσης κακής συμπεριφοράς είναι πολύ αποτελεσματική τεχνική για ανίχνευση επιθέσεων, η οποία μάλιστα δεν παράγει πολλές ψευδείς αναφορές επιθέσεων. 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 [7].

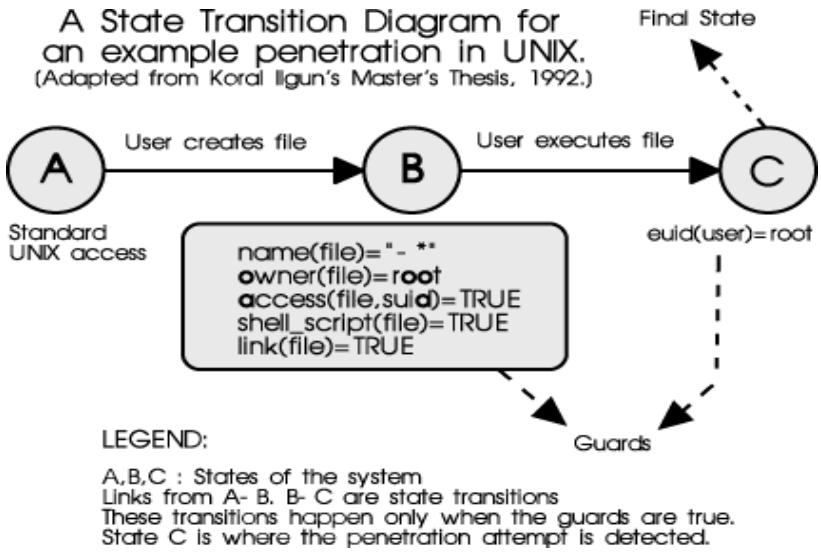
Μερικά συστήματα που σχεδιάστηκαν για την ανίχνευση της εισβολής στηριζόμενη στη φιλοσοφία του misuse detection φαίνονται και αναλύονται στις ποιο κάτω υποπαραγράφους.

4.5.2.1 Παρακολούθηση Πληκτρολόγησης

Είναι μια απλή τεχνική η οποία παρακολουθεί χτυπήματα πλήκτρων για πρότυπα επίθεσης. Δυστυχώς το σύστημα αυτό έχει πολλά ελαττώματα. Δυνατότητες των shells, όπως bash, ksh, tcsh στις οποίες ο χρήστης χρησιμοποιεί aliases, ξεπερνούν την τεχνική αυτή εύκολα. Επίσης, η μέθοδος δεν αναλύει την εκτέλεση της εντολής, αλλά μόνο την πληκτρολόγηση. Αυτό σημαίνει ότι ένα κακόβουλο πρόγραμμα δεν μπορεί να χαρακτηριστεί ως επιθετική δραστηριότητα. Τα λειτουργικά συστήματα δεν προσφέρουν πολλές δυνατότητες για παρακολούθηση χτυπημάτων πλήκτρων, επομένως ο αισθητήρας πρέπει να μπορεί να καταγράφει τα χτυπήματα πριν τα στείλει στον σταθμό ανάλυσης. Μια βελτίωση σε αυτό θα ήταν να παρακολουθούμε τις κλίσεις των εφαρμογών, έτσι ώστε να είναι δυνατή και η ανάλυση της εκτέλεσης του προγράμματος [7].

4.5.2.2 Ανάλυσης Μετάβασης Καταστάσεων

Στην τεχνική αυτή το σύστημα παρακολούθησης αναπαρίσταται σαν ένα διάγραμμα μετάβασης καταστάσεων. Κακώς τα δεδομένα αναλύονται το σύστημα πραγματοποιεί μεταβάσεις από μία κατάσταση σε άλλη. Η μετάβαση γίνεται αν κάποια Boolean κατάσταση είναι αληθής. Η προσέγγιση αυτή δίνει αποτελέσματα όταν έχουμε μεταβάσεις από ασφαλείς σε μη ασφαλείς καταστάσεις σύμφωνα με γνωστά πρότυπα επιθέσεων [7]. Το παρακάτω παράδειγμα δείχνει τη λειτουργία του μοντέλου:



Εικόνα 4.5.2.2: Μοντέλο ανάλυσης μετάβασης κατάστασης

- επιτιθέμενος δημιουργεί ένα σύνδεσμο ξεκινώντας με "-" (ας πούμε –x) στο setuid shell του root που περιέχει τον μηχανισμό #!/bin/sh.

- επιτιθέμενος εκτελεί –x.

Για να φτάσουμε στην τελική κατάσταση εισβολής, πρέπει να προϋπάρχουν κάποιες καταστάσεις. Αν αυτές οι καταστάσεις προστασίας είναι αληθείς, τότε έχουμε εισβολή σχεδόν σίγουρα. Αν κάποια από αυτές τις καταστάσεις δεν είναι αληθείς, η πιθανότητα εισβολής μειώνεται. Παρατηρούμε ότι αυτές οι καταστάσεις προστασίας υπάρχουν για να φιλτράρουν τις δραστηριότητες εισβολής από τις φυσιολογικές δραστηριότητες. Μερικά πλεονεκτήματα αυτής τις προσέγγισης είναι: μπορεί να ανιχνεύσει συνεργατικές επιθέσεις, μπορεί να εντοπίσει επιθέσεις που γεννούνται σε πολλές συνόδους χρηστών και μπορεί να προβλέψει επικίνδυνες καταστάσεις σύμφωνα με την παρούσα κατάσταση του συστήματος και να λάβει προληπτικά μέτρα.

Παρόλα αυτά υπάρχουν και μερικά προβλήματα με τα συστήματα μετάβασης καταστάσεων. Τα πρότυπα επιθέσεων μπορούν να ορίσουν μόνο μια αλληλουχία γεγονότων, παρά περισσότερο πολύπλοκες φόρμουλες. Δεν μπορούν να ανιχνεύσουν επιθέσεις τύπου denial of service, failed logins, διαφοροποιήσεις από την φυσιολογική χρήση και παθητική παρακολούθηση. Αυτό γίνεται, γιατί τα αντικείμενα αυτά δεν καταγράφονται από μηχανισμό ανίχνευσης ή δεν μπορούν να αναπαρασταθούν με διαγράμματα μετάβασης καταστάσεων [7].

4.5.2.3 Βασισμένα σε Σενάρια Εισβολής

Η ιδέα είναι ότι συγκεκριμένα σενάρια συμπεραίνονται από άλλες συγκεκριμένες φανερές δραστηριότητες. Αν αυτές οι δραστηριότητες παρακολουθούνται, είναι δυνατό να εντοπίσουμε προσπάθειες εισβολής με εξέταση των δραστηριοτήτων που εξάγονται από συγκεκριμένα σενάρια εισβολής [8]. Το βασικό μοντέλο του συστήματος αποτελείται από τρία modules.

Ο προβλεπτής χρησιμοποιεί ενεργά μοντέλα και μοντέλα σεναρίων και προσπαθεί να προβλέψει το επόμενο βήμα σε ένα σενάριο που αναμένεται να συμβεί. Ένα μοντέλο σεναρίου είναι μια βάση δεδομένων με προδιαγραφές επιθετικών σεναρίων. Ο σχεδιαστής στη συνέχεια, μεταφράζει αυτήν την υπόθεση σε μία ένδειξη της συμπεριφοράς, όπως κα πρέπει να συμβεί

μετά. Χρησιμοποιεί την πληροφορία πρόβλεψης για να σχεδιάσει το επόμενο βήμα. Ο διερμηνέας χρησιμοποιεί την πληροφορία από τον σχεδιαστή και ψάχνει για αυτήν στα δεδομένα που έρχονται. Το σύστημα προχωρά με αυτόν τον τρόπο, συγκεντρώνοντας όλο και περισσότερες αποδείξεις για μια προσπάθεια εισβολής μέχρι να συναντήσει ένα όριο (threshold). Σε αυτό το σημείο στέλνει alert για προσπάθεια εισβολής.

Η προσέγγιση αυτή είναι πολύ καλή. Επειδή ο σχεδιαστής και ο διερμηνέας γνωρίζουν τι πρέπει να αναζητήσουν σε κάθε βήμα, οι άχρηστες πληροφορίες φιλτράρονται και οδηγούμαστε σε εξαιρετικά αποτελέσματα. Επιπλέον, το σύστημα μπορεί να προβλέψει την επόμενη κίνηση του επιτιθέμενου, σύμφωνα με το μοντέλο εισβολής. Αυτές οι προβλέψεις χρησιμοποιούνται για να επαληθεύουμε μια υποψία εισβολής, για να πάρουμε προληπτικά μέτρα ή για να αποφασίσουμε ποια δεδομένα να αναζητήσουμε στη συνέχεια.

Όμως, υπάρχουν κάποια κρίσιμα θέματα σχετικά με το παραπάνω σύστημα. Πρώτα, τα πρότυπα για τα σενάρια εισβολής πρέπει να αναγνωρίζονται εύκολα. Δεύτερο, τα πρότυπα πρέπει πάντα να συμβαίνουν σύμφωνα με το μοντέλο συμπεριφοράς για την οποία αναθέτονται. Τρίτο τα πρότυπα πρέπει να είναι μοναδικά και να μην συνδυάζονται με καμία άλλη φυσιολογική συμπεριφορά [7].

4.5.3 Μοντέλο Βάση Προδιαγραφών

Η ανίχνευση διαταραχών περιγράφηκε ως η τεχνική για την αναζήτηση ασυνήθιστων καταστάσεων. Η ανίχνευση κακής συμπεριφοράς αναφέρθηκε ως η τεχνική για την αναζήτηση των καταστάσεων που είναι γνωστό ότι είναι ανεπιθύμητες. Η ανίχνευση προδιαγραφών αναζητά καταστάσεις που είναι γνωστό ότι δεν είναι επιθυμητές και όταν το σύστημα εισέρχεται σε μία τέτοια κατάσταση αναφέρει μία πιθανή εισβολή. Η *ανίχνευση που βασίζεται στις προδιαγραφές* (specification-based detection) καθορίζει εάν μια ακολουθία οδηγιών παραβιάζει ή όχι μια προδιαγραφή σχετικά με τον τρόπο με τον οποίο πρέπει να εκτελείται ένα πρόγραμμα, ή ένα σύστημα. Σε αυτή την περίπτωση, αναφέρει μια πιθανή εισβολή [22].

Κεφάλαιο 5
Δομή Και Αρχιτεκτονική IDPS

Προκειμένου να επιτευχθούν οι στόχοι που θέλει να επιτύχει ένα σύστημα IDPS θα πρέπει να συνδυάσει όλα εκείνα τα πλεονεκτήματα που παρουσιάζουν τα διάφορα μοντέλα αλλά και οι διάφορες κατηγορίες των συστημάτων αυτών. Αρχικά θα γίνει μια προσπάθεια παρουσίασης ενός γενικότερου μοντέλου που αναφέρεται στα περισσότερα IDPS. Στην συνέχεια θα αναλυθούν τα χαρακτηριστικά των Δικτυακών (Network-Based - NIDS) και των Εξυπηρετητών (Host-Based - HIDS) από τα οποία θα μπορούσαμε να αναφέρουμε ότι ο συνδυασμός τους θα αποτελούσε την βέλτιστη λύση για ένα αποτελεσματικό IDPS. Τέλος αναλύεται ο τομέας της απόκρισης στην εισβολή ο οποίος μελετά τις ενέργειες οι οποίες γίνονται μετά την ανίχνευση της εισβολής για να προστατευθεί το σύστημα.

5.1 Αρχιτεκτονική IDPS

Αρκετά σύγχρονα IDPS, χρησιμοποιούν τεχνικές όπως νευρωνικά δίκτυα, αυτόνομους πράκτορες, γράφους, αλλά και γλώσσες αναγνώρισης χρηστών. Ένα γενικότερο, αρχιτεκτονικό,

μοντέλο (Εικόνα 5.1.1) που περιγράφει τα περισσότερα IDPS διακρίνει οκτώ βασικά δομικά στοιχεία ενός IDPS [6].

1. Το υποσύστημα **συλλογής στοιχείων**, που είναι υπεύθυνο για τη συλλογή δεδομένων από το σύστημα υπό παρακολούθηση και τη μετάφρασή τους σε μια εσωτερική, κοινή γλώσσα. Τα δεδομένα αυτά περιλαμβάνουν εγγραφές του ίχνους ελέγχου, στοιχεία κίνησης του δικτύου κ.λπ.

2. Το υποσύστημα **ερμηνείας πληροφοριών**, που έχει την ευθύνη της ερμηνείας των δεδομένων που συλλέγει το υποσύστημα συλλογής στοιχείων, προκειμένου να αποφασίσει αν τα δεδομένα συνιστούν καταστάσεις ύποπτες για εισβολή.

3. Το υποσύστημα **λήψης απόφασης**, που είναι υπεύθυνο για τη λήψη της τελικής απόφασης για το αν πράγματι πρόκειται για εισβολή ή όχι.

4. Το υποσύστημα **επιλογής και εφαρμογής αντιμέτρων**, που, αν το υποσύστημα λήψης απόφασης αποφασίσει ότι συντρέχει εισβολή, έχει την ευθύνη επιλογής και ίσως εφαρμογής κατάλληλων αντιμέτρων.

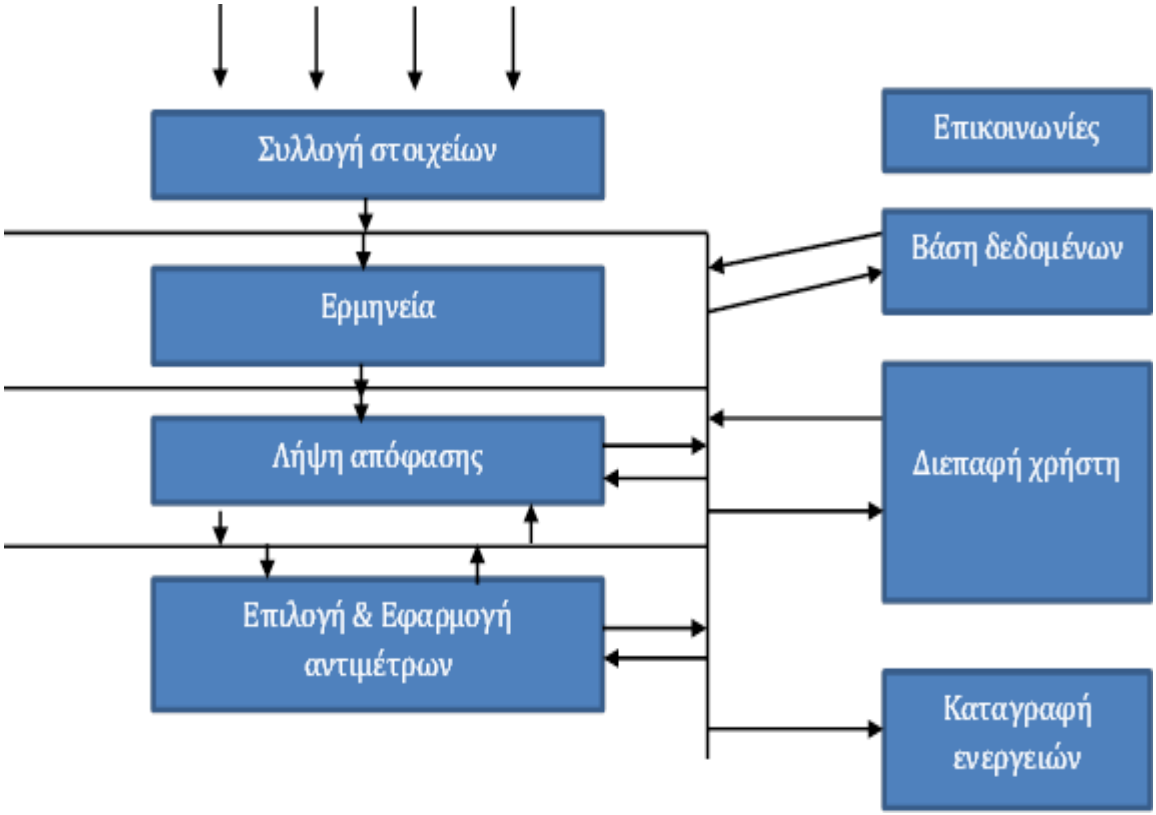
5. Το υποσύστημα **διεπαφής με το χρήστη**, που έχει την ευθύνη παρουσίασης στο διαχειριστή ασφάλειας των ευρημάτων του συστήματος και επίσης της αποδοχής των εντολών του.

6. Το υποσύστημα **επικοινωνιών**, που επιτρέπει την επικοινωνία μεταξύ των υποσυστημάτων.

7. Το υποσύστημα **καταγραφής ενεργειών**, που αποτελεί το ίχνος ελέγχου του ίδιου του συστήματος.

8. Το υποσύστημα **βάσης δεδομένων ασφάλειας**, στην οποία καταγράφονται όλες οι παράμετροι ασφάλειας του συστήματος.

Αυτονόητο είναι ότι κάποια από τα υποσυστήματα αυτά είναι δυνατόν να απουσιάζουν σε συγκεκριμένα IDPS ή κάποια υποσυστήματα να είναι ενσωματωμένα σε κάποια άλλα. Οι τεχνολογίες που μπορούν να χρησιμοποιηθούν για την υλοποίηση των υποσυστημάτων αυτών ποικίλλουν ανάλογα με το υποσύστημα.



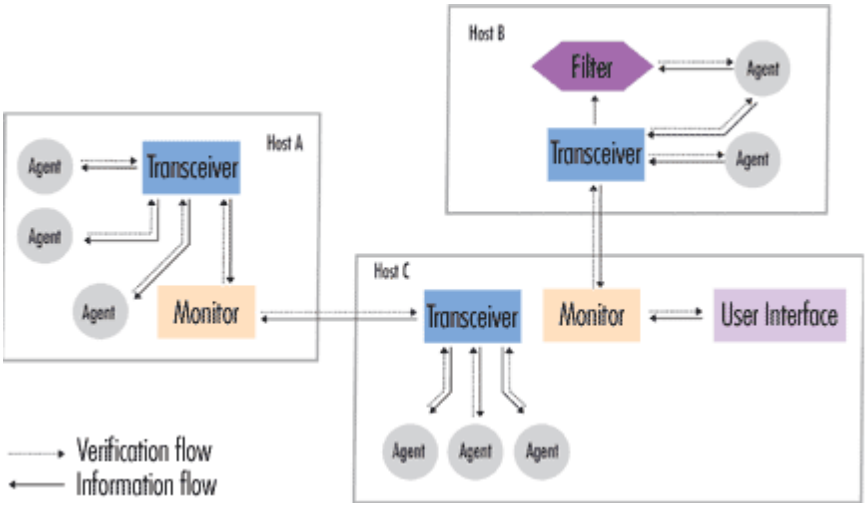
Εικόνα 5.1.1 : Αρχιτεκτονικό μοντέλο IDPS

Τα συστήματα ανίχνευσης και πρόληψης επιθέσεων μπορούν να οργανωθούν είτε κεντρικά (για παράδειγμα, φυσικά ολοκληρωμένα μέσα σε ένα τείχος προστασίας) είτε να διανεμηθούν. Ένα κατανεμημένο σύστημα ανίχνευσης και πρόληψης επιθέσεων αποτελείται από πολλαπλά συστήματα ανίχνευσης και πρόληψης επιθέσεων σε ένα μεγάλο δίκτυο, τα οποία επικοινωνούν μεταξύ τους. Πιο εξελιγμένα συστήματα ακολουθούν μια αρχή δομής πράκτορα, όπου μικρές αυτόνομες ενότητες οργανώνονται σε μια βάση ανά-ξενιστή (per-host) σε όλο το προστατευόμενο δίκτυο. Ο ρόλος του πράκτορα είναι να παρακολουθεί και να φιλτράρει όλες τις δραστηριότητες εντός της προστατευόμενης περιοχής και - ανάλογα με την προσέγγιση που υιοθετείται - προβαίνει σε μια πρώτη ανάλυση, έχοντας ακόμα και τη δυνατότητα να αναλάβει δράση αποκρίνοντας. Το δίκτυο των συνεργαζόμενων πρακτόρων που στέλνουν αναφορές στον κεντρικό εξυπηρέτη ανάλυσης είναι ένα από τα πιο σημαντικά εργαλεία των συστημάτων ανίχνευσης εισβολών.

Τα κατανεμημένα συστήματα ανίχνευσης και πρόληψης επιθέσεων μπορούν να χρησιμοποιούν πιο εξελιγμένα εργαλεία ανάλυσης, τα οποία συνδέονται κυρίως με την ανίχνευση των κατανεμημένων επιθέσεων. Ένας άλλος ξεχωριστός ρόλος του πράκτορα συνδέεται με την κινητικότητα του και την περιαγωγή του σε πολλαπλές φυσικές τοποθεσίες. Επιπλέον, οι πράκτορες μπορούν να είναι ειδικά αφιερωμένοι στην ανίχνευση ορισμένων γνωστών επιθέσεων υπογραφής. Αυτό αποτελεί αποφασιστικό παράγοντα κατά την εισαγωγή μέσων προστασίας που συνδέονται με νέους τύπους επιθέσεων. Τα συστήματα ανίχνευσης και πρόληψης επιθέσεων που είναι βασιζόμενα σε πράκτορες χρησιμοποιούν λιγότερο απαιτητικούς μηχανισμούς για την πολιτική ενημέρωσης απόκρισης.

Μία λύση πολύ πρακτορικής αρχιτεκτονικής, η οποία προήλθε το 1994 είναι η AAFID (Αυτόνομοι Πράκτορες για Ανίχνευση Εισβολής- Autonomous Agents for Intrusion Detection) – (Εικόνα 5.1.2). Χρησιμοποιεί πράκτορες που παρακολουθούν μια συγκεκριμένη πτυχή της συμπεριφοράς του συστήματος που διαμένουν, σε εκείνο το χρονικό διάστημα. Για παράδειγμα, ένας πράκτορας μπορεί να δει έναν ανώμαλο αριθμό από telnet συνεδρίες στο πλαίσιο του συστήματος που ελέγχει. Ένας πράκτορας έχει την ικανότητα να προβεί σε ειδοποίηση, όταν ανιχνεύει ένα ύποπτο συμβάν.

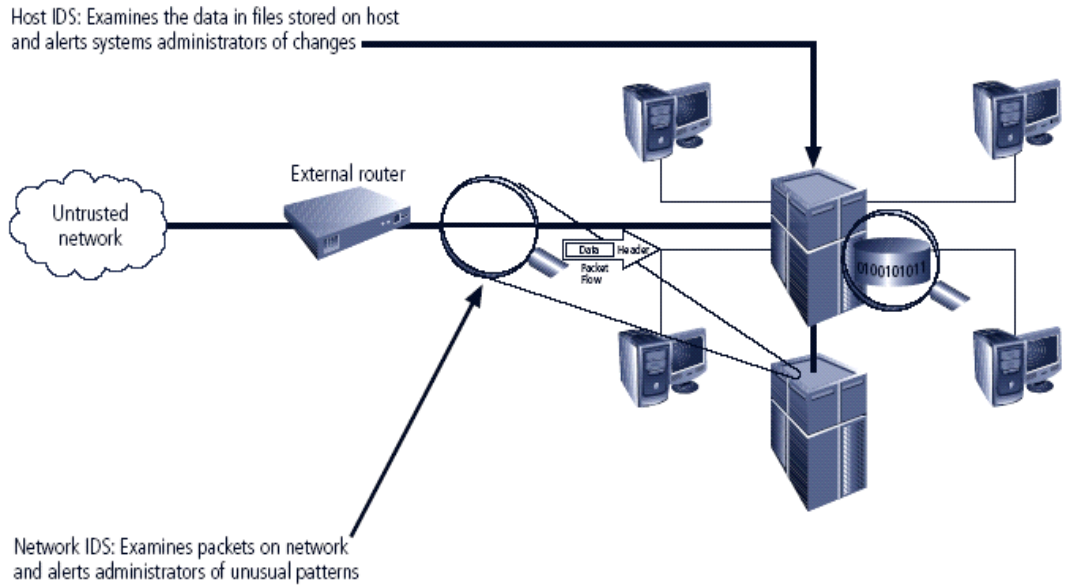
Οι πράκτορες μπορούν να κλωνοποιηθούν και να στραφούν σε άλλα συστήματα. Εκτός από τους πράκτορες, το σύστημα μπορεί να έχει πομποδέκτες, για να παρακολουθούν όλες τις εργασίες που πραγματοποιούνται από τους πράκτορες σε ένα συγκεκριμένο εξυπηρέτη. Οι πομποδέκτες εκπέμπουν πάντοτε τα αποτελέσματα των πράξεών τους σε ένα μοναδικό ελεγκτή εκπομπών. Οι ελεγκτές εκπομπών λαμβάνουν πληροφορίες από μια συγκεκριμένη περιοχή του δικτύου (όχι μόνο από έναν εξυπηρέτη), κάτι που σημαίνει ότι μπορούν να συσχετίζονται με κατανεμημένες πληροφορίες. Επιπλέον, ορισμένα φίλτρα μπορούν να χρησιμοποιηθούν για την επιλογή και την ομαδοποίηση των δεδομένων.



Εικόνα 5.1.2 : Μία παρουσίαση ενός συστήματος ανίχνευσης και πρόληψης επιθέσεων που χρησιμοποιεί αυτόνομους πράκτορες (AAFID)

5.2 Κατηγοριοποίηση IDPS Αναλόγως Τοπολογίας

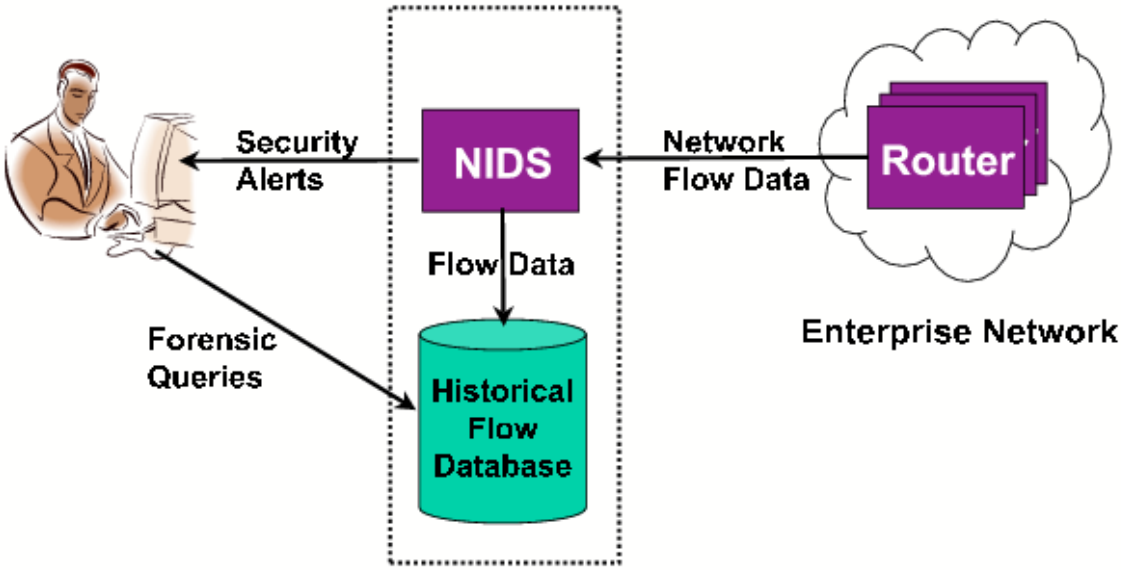
Η κατηγοριοποίηση των συστημάτων ανίχνευσης και πρόληψης επιθέσεων αναλόγως της τοπολογίας τους είναι σε Δικτυακά (Network-Based - NIDS) και εξυπηρετητών (Host-Based - HIDS) (Εικόνα 5.2). Στα ποιο κάτω υποκεφάλαια θα αναλυθούν τα πλεονεκτήματα και μειονεκτήματα που παρουσιάζουν καθώς και η χρησιμοποίηση τους σε περιβάλλον κρίσιμων υπολογιστικών υποδομών.



Εικόνα 5.2: Κατηγοριοποίηση IDPS αναλόγως τοπολογίας

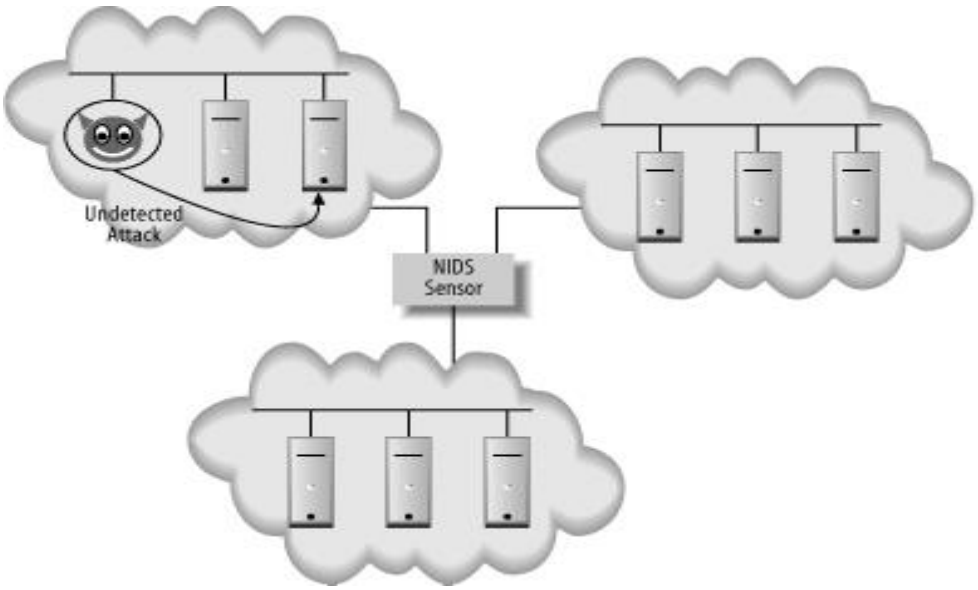
5.2.1 Δικτυακά (Network-Based - NIDS)

Η γενικότερη μορφή παρουσίασης λειτουργιάς ενός συστήματος ανίχνευσης και πρόληψης επιθέσεων βασιζόμενο στο δίκτυο (NIDS) φαίνεται παρακάτω (Εικόνα 5.2.1.1). Τα συστήματα αυτά τοποθετούνται σε στρατηγικά σημεία μέσα στα δίκτυα προκειμένου να παρακολουθούν την κίνηση από και προς όλες τις συσκευές του δικτύου. Ιδανικό σενάριο είναι να ελέγχονται όλες οι εξερχόμενες και εισερχόμενες κινήσεις έτσι ώστε να εντοπίζονται οι εισβολές εκείνες που θα ήθελαν με οποιαδήποτε τρόπο να βλάψουν το δίκτυο. Σαν εισβολές ή κακόβουλες δραστηριότητες, που θα μπορούσε να εντοπίσει ένα τέτοιο σύστημα ανίχνευσης και πρόληψης επιθέσεων είναι οι επιθέσεις άρνησης υπηρεσίας (DoS attack), σαρώσεις πυλών ή ακόμη και προσπάθειες «ραγίσματος» (cracking) σε υπολογιστές χρησιμοποιώντας την Παρακολούθηση Ασφάλειας Δικτύου (Network Security Monitoring - NSM) της κίνησης του δικτύου.



Εικόνα 5.2.1.1: Λειτουργία ενός συστήματος ανίχνευσης επιθέσεων βασιζόμενο στο δίκτυο (NIDS)

Εάν γινόταν μια προσπάθεια να μελετηθεί το NIDS θα λέγαμε ότι αποτελείται από δύο τμήματα: τους **αισθητήρες** και τον **σταθμό διαχείρισης / ανάλυσης**. Ο αισθητήρας βρίσκεται σε ένα τομέα του δικτύου και παρακολουθεί για ύποπτες κινήσεις. Ο σταθμός διαχείρισης λαμβάνει τις ενδείξεις κινδύνου από τους αισθητήρες και τις μεταβιβάζει στον διαχειριστή του συστήματος, δηλαδή στον διαχειριστή ασφαλείας του δικτύου. Οι αισθητήρες είναι συστήματα που υπάρχουν μόνο για να παρακολουθούν το δίκτυο. Έχουν ένα δικτυακό interface που αναλύει τα πάντα. Αν ανιχνεύσουν κάτι ύποπτο το μεταβιβάζουν στον σταθμό διαχείρισης / ανάλυσης. Ο σταθμός διαχείρισης / ανάλυσης μπορεί να δείξει τα σήματα κινδύνου, που έλαβε από τους αισθητήρες ι να πραγματοποιήσει επιπλέον ανάλυση. Στο σχήμα ποιο κάτω φαίνεται η ανάπτυξη NIDS αισθητήρα. Συχνά, τα συστήματα ανίχνευσης εισβολής βασισμένα στο δίκτυο συντονίζονται με άλλα συστήματα. Μπορούν, για παράδειγμα, να ενημερώσουν τη «μαύρη λίστα» ορισμένων τειχών προστασίας με τις διευθύνσεις IP των υπολογιστών που χρησιμοποιούνται από τον (ύποπτο) εισβολέα.



Εικόνα 5.2.1.2: Λειτουργία ενός συστήματος ανίχνευσης επιθέσεων βασιζόμενο σε NIDS αισθητήρα

5.2.1.1 Πλεονεκτήματα των NIDS

Μερικά από τα πλεονεκτήματα που παρουσιάζει ένα σύστημα ανίχνευσης και πρόληψης επιθέσεων στο δίκτυο είναι τα παρακάτω [7]:

- Μπορούν να ανιχνεύσουν κάποιες από τις επιθέσεις που χρησιμοποιούν το δίκτυο. Είναι επαρκή για την ανίχνευση πρόσβασης.

- Έχουν την τάση να είναι καλύτερα αυτό-διατηρούμενα από ότι τα host–based. Τρέχουν σε ένα συγκεκριμένο σύστημα και η εγκατάσταση τους είναι απλή και πραγματοποιείται σε μια τοποθεσία στο δίκτυο που δίνει τη δυνατότητα παρακολούθησης ευαίσθητης κίνησης δεδομένων, η προσπέλαση χωρίς εξουσιοδότηση ή κάποιου είδους πρόσβαση με κατάχρηση προνομίων εξουσιοδότησης.

- Δεν απαιτεί μετατροπές στους servers ενός υπολογιστικού κέντρου ή στους κόμβους για να εγκατασταθεί. Αυτό είναι μεγάλο όφελος, γιατί συνήθως οι servers έχουν μικρές ανοχές όσο αφορά τη CPU, το I/O και την χωρητικότητα του δίσκου. Η εγκατάσταση επιπλέον λογισμικού μπορεί να δημιουργήσει προβλήματα λειτουργικότητας.

- Δεν αποτελεί κρίσιμο παράγοντα για την λειτουργικότητα του δικτύου. Άρα, τυχόν αποτυχία στο σύστημα του IDS δε θα έχει σημαντική επίδραση στην λειτουργία του λοιπού εξοπλισμού.

- Θα συναντήσουμε λιγότερη αντίδραση από εργαζόμενους του περιβάλλοντος καθώς δεν θα απαιτηθεί να εγκαταστήσουν λογισμικό στα συστήματά τους.

5.2.1.2 Μειονεκτήματα των NIDS

Μερικά από τα μειονεκτήματα που παρουσιάζει ένα σύστημα ανίχνευσης και πρόληψης επιθέσεων στο δίκτυο είναι τα παρακάτω [7]:

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

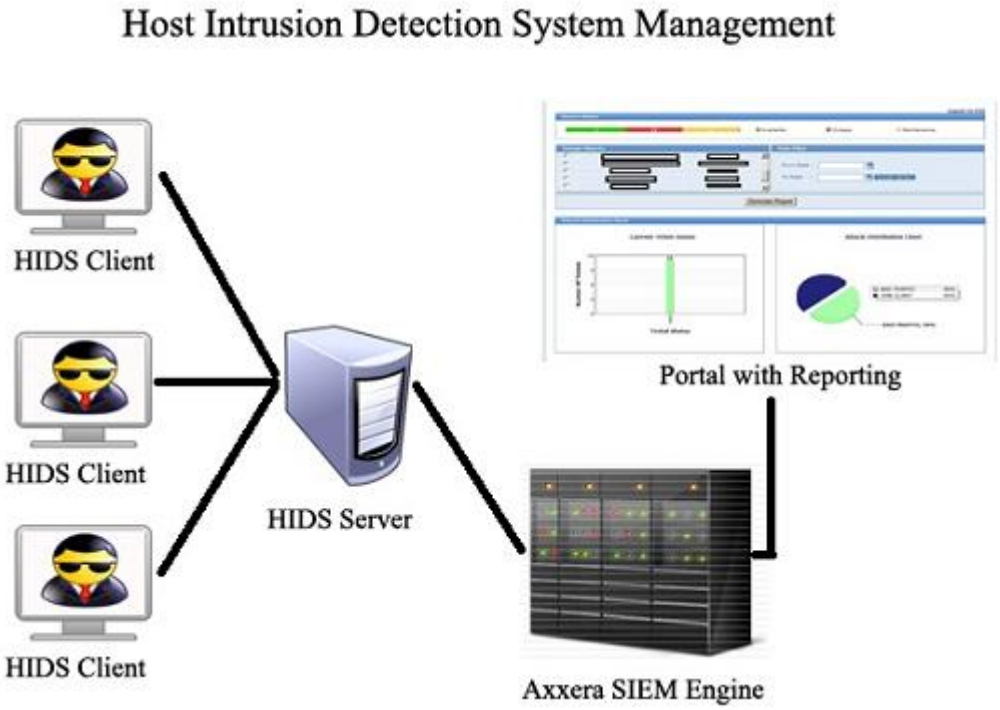
- Χρησιμοποιούν ανάλυση αποτυπωμάτων/signatures για να καλύψουν τις προδιαγραφές απόδοσης. Έτσι ανιχνεύονται γνωστές προγραμματισμένες επιθέσεις από εξωτερικές πηγές, αλλά αυτή η μέθοδος δεν είναι επαρκής για πιο πολύπλοκα είδη επιθέσεων.

- Ένα σύστημα ανίχνευσης επιθέσεων NIDS μπορεί να χρειαστεί να μεταδώσει μεγάλες ποσότητες δεδομένων στο κεντρικό σύστημα ανάλυσης. Πολλά τέτοια συστήματα χρησιμοποιούν επιθετικές μεθόδους ελάττωσης δεδομένων για να μειώσουν το παραγόμενο traffic επικοινωνίας. Το μειονέκτημα εδώ είναι ότι παρέχεται ελάχιστος συντονισμός μεταξύ των αισθητήρων. Ένα τέτοιο σύστημα δεν μπορεί να ανιχνεύσει συνεργατικές πολύπλοκες επιθέσεις.

- Υπάρχει πιθανότητα να αντιμετωπίσει δυσκολίες στο χειρισμό επιθέσεων στη διάρκεια κρυπτογραφημένων συνόδων. Ευτυχώς, είναι πολύ λίγες οι επιθέσεις που πραγματοποιούνται εντός μιας κρυπτογραφημένης συνόδου, εκτός από τις επιθέσεις εναντίον ευπαθών Web Servers. Αυτό το γεγονός θα γίνει περισσότερο εμφανής με την μετάβαση στο IPv6.

5.2.2 Εξυπηρετητών (Host-Based - HIDS).

Ένα σύστημα ανίχνευσης και πρόληψης επιθέσεων που βασίζεται στον εξυπηρετητή (HIDS) λειτουργεί ως συσκευή του δικτύου. Ουσιαστικά ελέγχει τόσο τα εξερχόμενα όσο και τα εισερχόμενα πακέτα τα οποία διέρχονται από την συσκευή. Όταν αντιληφθεί κακόβουλη δραστηριότητα τότε ενημερώνει το διαχειριστή του δικτύου ειδεμή παραμένει στην ενημέρωση του χρήστη. Χρησιμοποιούν συχνά το μηχανισμό έλεγχου και καταγραφής του κόμβου σαν πηγή πληροφοριών για ανάλυση. Πιο συγκεκριμένα ψάχνουν για ασυνήθη δραστηριότητα που περιορίζεται στον τοπικό κόμβο, όπως logins, παράξενη πρόσβαση σε αρχεία, μη εγκεκριμένη άφιξη δικαιωμάτων η μετατροπές σε δικαιώματα του συστήματος. Η συγκεκριμένη αρχιτεκτονική χρησιμοποιεί μηχανισμούς βασισμένους σε κανόνες για την ανάλυση της δραστηριότητας. Παράδειγμα της αρχιτεκτονικής αυτής φαίνεται στην πιο κάτω εικόνα.



Εικόνα 5.2.2 : Σύστημα ανίχνευσης επιθέσεων βασιζόμενο στον Εξυπηρετητή.

5.2.2.1 Πλεονεκτήματα των HIDS

Μερικά από τα πλεονεκτήματα που παρουσιάζει ένα σύστημα ανίχνευσης και πρόληψης επιθέσεων στον εξυπηρετητή είναι τα παρακάτω [7]:

- Μπορεί να αποτελέσει πολύ δυνατό εργαλείο ανάλυσης πιθανών επιθέσεων. Για παράδειγμα, είναι σε θέση μερικές φορές να καταγράψει τι ακριβώς κάνει ο εισβολέας, ποιες εντολές εκτέλεσε, ποια αρχεία έτρεξε και ποιές ρουτίνες του συστήματος κάλεσε**.**

- Έχουν μικρότερους false positive ρυθμούς από ότι τα network based. Αυτό συμβαίνει γιατί το εύρος των εντολών που εκτελούνται σε ένα συγκεκριμένο κόμβο 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.

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

- Τέλος, σε ένα Host – Based σύστημα είναι ευκολότερο να σχηματιστεί μία ενεργή αντίδραση σε περίπτωση επίθεση, όπως ο τερματισμός μιας υπηρεσίας ή το logging off ενός επιτιθέμενου χρήστη.

5.2.2.2 Μειονεκτήματα των HIDS

Μερικά από τα μειονεκτήματα που παρουσιάζει ένα σύστημα ανίχνευσης και πρόληψης επιθέσεων στον εξυπηρετητή είναι τα παρακάτω [7]:

- Απαιτούν εγκατάσταση στο σύστημα που θέλουμε να προστατεύσουμε. Αν, για παράδειγμα, έχουμε έναν server που πρέπει να τον προστατέψουμε θα πρέπει να εγκατασταθεί το IDS στον server αυτόν.

- "Έχουν την τάση να εξαρτώνται από το υπάρχον σύστημα καταγραφής (logging system) και έλεγχου του server. Εάν ο server δεν λειτουργεί έτσι ώστε η καταγραφή και ο έλεγχος να είναι σε ικανοποιητικό επίπεδο, κα πρέπει να γίνει αλλαγή στις ρυθμίσεις του. Αυτό αποτελεί τεράστιο πρόβλημα αλλαγής στη διαχείριση του server.

- Αυτά τα συστήματα είναι σχετικά ακριβά. Πολλοί οργανισμοί δεν έχουν την οικονομική δυνατότητα να προστατέψουν ολόκληρα δικτυακά τμήματα με τη χρήση Host – 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.

- Αγνοούν εντελώς το περιβάλλον του δικτύου, άρα ο χρόνος ανάλυσης που απαιτείται για την εκτίμηση ζημιών από πιθανή εισβολή αυξάνει γραμμικά με τον αριθμό των κόμβων που προστατεύονται.

5.3 Απόκριση Εισβολών

Μετά την ανίχνευση της εισβολής θα πρέπει να τεθεί σαν στόχος να αντιμετωπιστεί η αποπειραθείσα επίθεση με τρόπο ώστε να ελαχιστοποιείται η ζημιά, όπως προσδιορίζεται από την ισχύουσα πολιτική ασφάλειας. Μερικοί μηχανισμοί ανίχνευσης εισβολών μπορούν να βελτιωθούν προκειμένου να αποτρέψουν τους εισβολείς. Σε αντίθετη περίπτωση, οι υπεύθυνοι ασφάλειας πρέπει να αποκριθούν στην επίθεση και να προσπαθήσουν να αποκαταστήσουν οποιαδήποτε ζημιά προκλήθηκε. Παραδειγματικά μια αρχιτεκτονική μιας Μηχανής Απόκρισης Εισβολών φαίνεται στη ποιο κάτω εικόνα.

Εικόνα 5.3 : Αρχιτεκτονική μηχανής απόκρισης επιθέσεων.

Η διαλειτουργία των Μονάδων Καθολικής Απόκρισης, της Μονάδας Τοπικής Απόκρισης αλλά και της Μονάδας Επικοινωνίας συνθέτουν την Μηχανή Απόκρισης Εισβολών. Είναι προφανές για να επιτευχθούν οι στόχοι της απόκρισης των επιθέσεων θα πρέπει να εκτελεστούν οι εξής ενέργειες που αναλύονται λεπτομερέστατα στα παρακάτω κεφάλαια. Δηλαδή θα πρέπει να παρθούν αλλά και να λειτουργήσουν τα μέτρα πρόληψης για την προστασία των συστημάτων αυτών καθώς και επίσης και οι μηχανισμοί αντίδρασης σε περίπτωση που εντοπιστεί η επίθεση. Τέλος σημαντικό αποτελεί και το τμήμα χειρισμού των επιθέσεων που απώτερο σκοπό έχει να αναχαιτίσει και εξουδετέρωση την επίθεση.

5.3.1 Προστασία με Συστήματα Πρόληψης Επιθέσεων (IPS)

Όπως αναφέρθηκε και στην αρχή της εργασίας ένα IPS (Intrusion Prevention System) αποτελεί μέρος ενός IDS και δεν αποτελούν ξεχωριστές οντότητες. Για αυτό και οι παραπάνω μας αναφορές γίνονται σε ένα σύστημα IDPS. Επιπρόσθετα αναφέρεται ότι αυτό συμβαίνει επειδή το IDS είναι αυτό που ανιχνεύει μια επίθεση, οπότε αυτό πρέπει να πάρει και την πρωτοβουλία για να την σταματήσει.

Στην ουσία ένα IPS, συνδυάζει τα χαρακτηριστικά ενός Firewall και ενός IDS, καθώς μπορεί και μπλοκάρει την ανεπιθύμητη κίνηση έχοντας την βοήθεια της ανίχνευσης των κακόβουλων πακέτων που προσφέρει ένα IDS [7]. Η διαφορά του από το firewall είναι ότι έχει καλύτερη και πιο ολοκληρωμένη πληροφορία. Αυτό οφείλεται στην ύπαρξη του IDS, το οποίο και

παρακολουθεί όλη την δικτυακή κίνηση. Τα συστήματα αποτροπής επιθέσεων συναντώνται στους παρακάτω τύπους [46]:

- **Host-Based (HIPSs),** βρίσκονται σε ένα συγκεκριμένο μηχάνημα και παρακολουθούν την κίνηση και κάποια άλλα στοιχεία προκειμένου να αποτρέψουν επιθέσεις.

- **Network-based (NIPSs),** όπου η εφαρμογή IPS ή το υλικό που παίζει το ρόλο του IPS βρίσκεται στο δίκτυο και έχει IP αυτού του δικτύου. Τα συστήματα αυτά αναλύουν, βρίσκουν, και αναφέρουν συμβάντα που έχουν να κάνουν με συστήματα ασφαλείας. Είναι σχεδιασμένα ώστε να ελέγχουν τη δικτυακή κίνηση.

- **Content-based (CBIPSs),** είναι τα συστήματα εκείνα που παρακολουθούν το περιεχόμενο των πακέτων για μοναδικές ακολουθίες, τις οποίες ονομάζουμε υπογραφές, με σκοπό να αναγνωρίσουν και να αποτρέψουν γνωστούς τύπους επιθέσεων.

- **Rate-based (RBIPSs),** είναι τα συστήματα εκείνα που στόχο έχουν να αποτρέψουν επιθέσεις τύπου άρνησης εξυπηρέτησης. Η λειτουργία τους βασίζεται στο γεγονός ότι παρακολουθούν και μαθαίνουν φυσιολογικές δικτυακές συμπεριφορές. Με βάση λοιπόν την πραγματικού χρόνου παρακολούθησης του δικτύου και κάποια στατιστικά στοιχεία μπορούν να αναγνωρίσουν κάποια με αποδεκτά όρια για συγκεκριμένους τύπους κίνησης, π.χ TCP, UDP. Οι επιθέσεις αναγνωρίζονται όταν ξεπεραστούν κάποια φράγματα. Όταν θ επίθεση αναγνωριστεί, τότε εφαρμόζονται διάφοροι μηχανισμοί αποτροπής όπως είναι για παράδειγμα το port/protocol filtering (black-listing, white-listing).

5.3.2 Μηχανισμοί Αντίδρασης

Οι αντιδράσεις ανίχνευσης επιθέσεων διακρίνονται σε δύο κατηγορίες:

- **Παθητικός Μηχανισμός Αντίδρασης** (passive response mechanism). Στόχος του είναι να ειδοποιήσει το διαχειριστή για το συμβάν (email, sms, pop-up παράθυρο) και να καταγράψει το συμβάν που προηγήθηκε. Βασικό χαρακτηριστικό των μηχανισμών αυτών είναι ότι οι παθητικές αντιδράσεις συνίστανται κυρίως σε ειδοποιήσεις και συναγερμούς προς το προσωπικό ασφάλειας καθώς και οι ειδοποιήσεις αυτές μπορούν να έχουν κυμαινόμενο βαθμό λεπτομέρειας και μπορούν να εμφανίζονται σε ειδικό χώρο

του συστήματος ανίχνευσης εισβολών, σε παράθυρο μηνύματος, σε συσκευές τηλεειδοποίησης, με μηνύματα σε κινητά τηλέφωνα.*

- **Ενεργητικός Μηχανισμός Αντίδρασης** (active response mechanism). Στόχος του είναι το ίδιο το σύστημα να λάβει κάποια αναγκαία μέτρα προκειμένου να αντιμετωπιστεί το συμβάν ή ακόμα καλύτερα να αναχαιτιστεί. Όσον αφορά τον ενεργητικό παρουσιάζει χαρακτηριστικά όπως τον Τερματισμό της επίθεσης, την Συλλογή περισσότερης πληροφορίας, των Εντοπισμός της πηγής, την Καταγραφή των σταδίων της επίθεσης, την Αποθήκευση σημαντικής πληροφορίας καθώς και την Περιορισμένη πρόσβαση σε ύποπτους χρήστες ή διεργασίες ή διευθύνσεις. Πέραν όμως των πλεονεκτημάτων που παρουσιάζει ο μηχανισμός αυτός, εμφανίζει τα μειονεκτήματα που αφορούν το γεγονός ότι σε περίπτωση λάθους μπορεί να επηρεαστεί ένας νόμιμος χρήστης, επίσης μπορεί να χρησιμοποιηθεί ως εργαλείο επίθεσης και τέλος μπορεί να υποδηλώσει τη μέχρι εκείνη τη στιγμή μη ορατή παρουσία του.

5.3.3 Χειρισμός Επιθέσεων

Όταν λαμβάνει χώρα μία εισβολή, η πολιτική ασφάλειας του συστήματος έχει παραβιαστεί. Ο χειρισμός των εισβολών περιλαμβάνει την εκ νέου συμμόρφωση του συστήματος με την πολιτική ασφάλειας και τη λήψη μέτρων κατά του επιτιθέμενου, όπως αυτά καθορίζονται από την ισχύουσα πολιτική. Ο χειρισμός των εισβολών περιλαμβάνει έξι φάσεις [32].

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

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

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

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

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

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

Κεφάλαιο 6
Ευρύτερα Αξιοποιούμενα Συστήματα IDPS

6.1 Εξέλιξη των IDPS

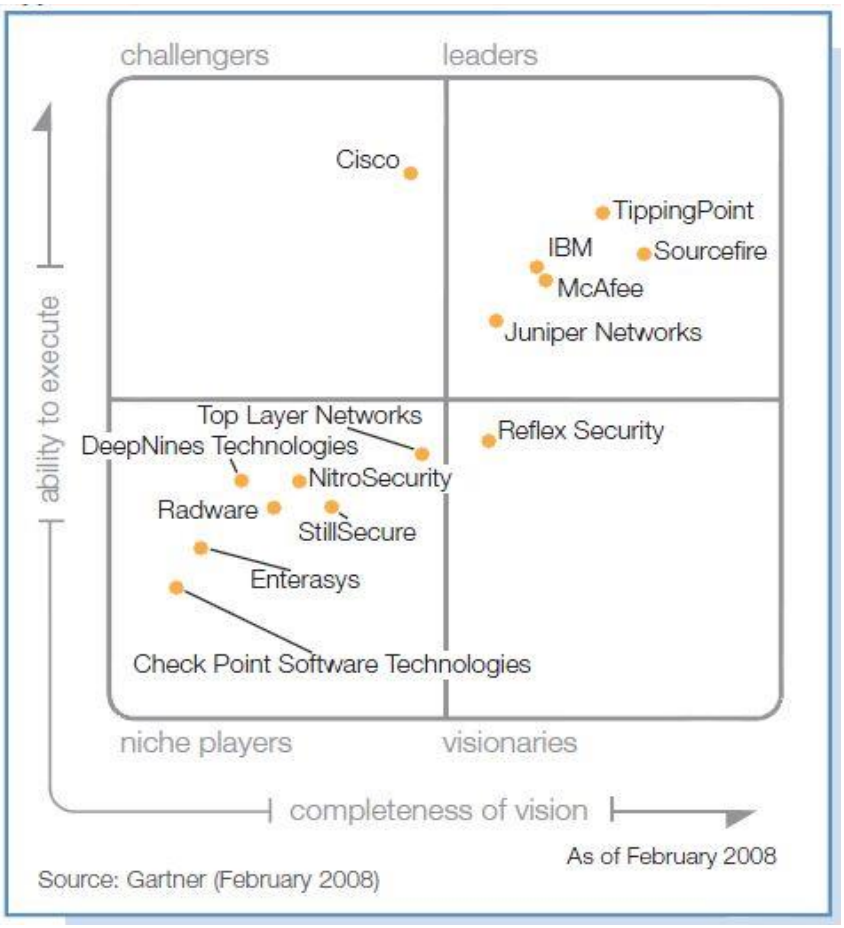
Η σημαντικότερη εξέλιξη της τεχνολογίας ανίχνευσης επιθέσεων είναι ότι από τα παθητικά IDS που απλά παρακολουθούσαν και ανέλυαν τις επιθέσεις που δεχόταν το σύστημα μεταφερθήκαμε στα ενεργά, προληπτικά IDPS. Μπορούμε πλέον να έχουμε περιμετρικά του δικτύου μας μια ασπίδα, και εσωτερικά αυτού να προστατεύουμε κάθε κόμβο ξεχωριστά. Επίσης, τα σημερινά IDPS μπορούν και λειτουργούν σε μεγαλύτερες ταχύτητες και

περιλαμβάνουν για την αναγνώριση των επιθέσεων και άλλους μηχανισμούς πέρα από τη χρήση απλών κανόνων υπογραφής, χωρίς να χρειάζεται να διακόψουν συνδέσεις για την αντιμετώπισή τους [1]. Οι έξι μεγαλύτεροι προμηθευτές IDPS, σύμφωνα με έρευνα του 2009 [29], είναι οι Cisco, McAfee, Juniper, IBM, Sourcefire και TippingPoint, βάσει διαφόρων κριτηρίων (σχέση τιμής-απόδοσης, μελλοντικό πλάνο, κ.α.) που τέθηκαν από μεγάλους οργανισμούς (Εικόνα 6.1.1). Από άποψη αποδοτικότητας, στην κορυφή βρίσκεται η Cisco .

	Product			Vendor		
	Features	Usability	Affordability	Viability	Strategy	Support
Check Point	○	◕	○	◑	◑	◑
Cisco	◑	◑	●	◕	◔	◑
HP	●	◕	◑	◕	◔	●
IBM	◑	○	◕	●	○	●
Juniper	◑	◑	●	◑	○	○
McAfee	●	●	○	◑	◑	◕
Radware	◔	○	○	◔	●	◕
Sourcefire	◑	◑	◕	◔	●	◕
Top Layer	◑	○	◕	○	●	○

Εικόνα 6.1.1 : Κριτήρια επιλογής IDPS

Στη ποιο κάτω εικόνα παρουσιάζεται το επίπεδο στο οποίο βρίσκονται οι προμηθευτές αναλόγως της δυνατότητας τους να φέρουν εις πέρας μια αποστολή.



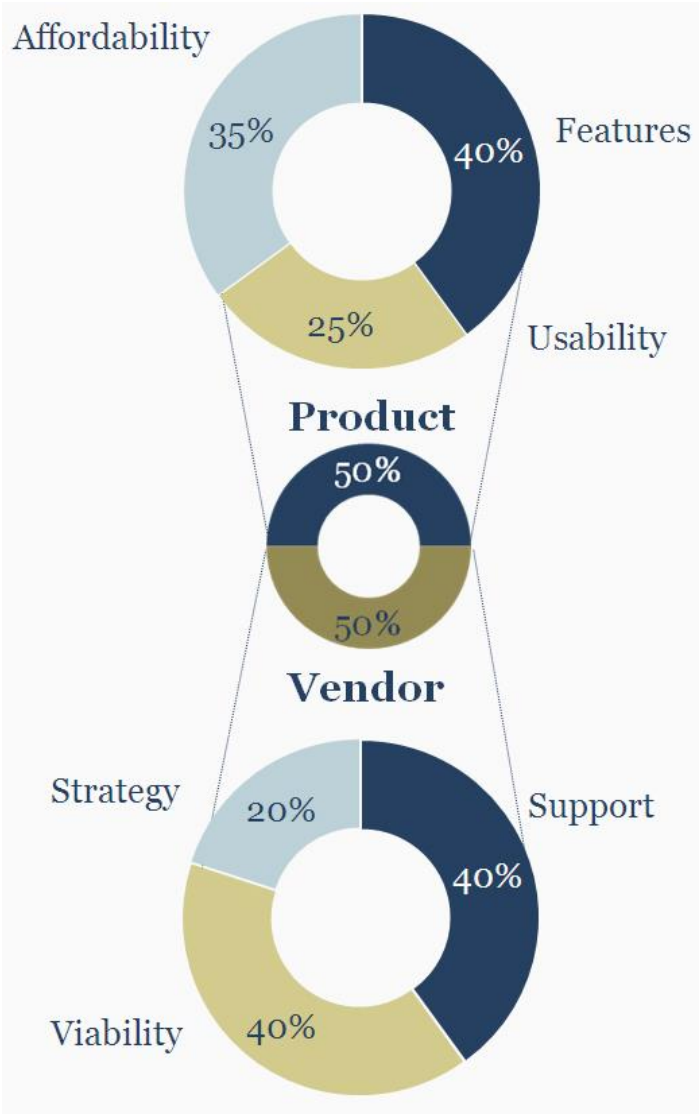
Εικόνα 6.1.2 : Οι μεγαλύτεροι προμηθευτές IDPS[29]

6.2 Μέτρηση Αποτελεσματικότητας IDPS

Για την επιλογή ενός συστήματος IDPS θα πρέπει να καθοριστούν παράμετροι που να καθορίζουν την αποτελεσματικότητα του συστήματος. Συγκεκριμένα θα πρέπει τα IDPSs να αξιολογούνται χρησιμοποιώντας τις ποιο κάτω τέσσερις κυρίαρχες μετρήσεις: Τα κατώτατα όρια (thresholds), μαύρες λίστες και λευκές λίστες (blacklists and whitelists), τις ρυθμίσεις ειδοποιήσεων (alert settings) και τον κωδικό προβολής καθώς και την επεξεργασία του (code viewing and editing). Επιπλέον στην αξιολόγηση των συστημάτων αυτών θα πρέπει να μπορούν να διαβάσουν για παράδειγμα: σε 100 Mb / s, ένα IDPS να ήταν σε θέση να εντοπίσει το 97% των επιθέσεων που πραγματοποιούνται. Τέλος πολύ σημαντικό είναι να αναφερθεί ότι θα πρέπει κατά την ανάπτυξη ενός συστήματος να υπάρχουν οι αντίστοιχοι μηχανισμοί ελέγχου που να επαληθεύου αν τα συστήματα αυτά εκτελούν τις λειτουργίες τους όπως αναμενόταν καθώς και κριτήρια επιλογής των συστημάτων αυτών τα οποία θα δίνουν μια μεγαλύτερη βαρύτητα.

Μερικές από αυτές τις διαδικασίες δοκιμών που θα επιτρέψου στο διαχειριστή να ελέγξει το σύστημα του είναι οι παρακάτω:

- Καταγραφή και επανεκπομπής των πακέτων σε συνθήκες πραγματικού αλλά και υπαρκτού ιού ή σκουληκιού σάρωσης.
- Καταγραφή και επανεκπομπής των πακέτων σε συνθήκες πραγματικού αλλά και υπαρκτού ιού ή σκουληκιού σάρωσης καθώς και με ελλιπή συνδέσεις σε TCP / IP (λείπουν πακέτα SYN)
- Διεξαγωγή ενός πραγματικού ιού ή σκουληκιού σάρωσης σε ένα άτρωτο σύστημα



Εικόνα 6.2 : Αποτελεσματικότητα ενός IDPS

6.3 Ευρύτερα Αξιοποιούμενα Συστήματα IDPS.

Ένα IDPS μπορεί να είναι ένα μεγάλο εργαλείο για την προληπτική παρακολούθηση και την προστασία του δικτύου από κακόβουλη δραστηριότητα, ωστόσο είναι επίσης επιρρεπής σε ψευδείς συναγερμούς. Οποιαδήποτε λύση IDPS εφαρμοστεί, θα πρέπει να "συντονιστεί" τη στιγμή που θα γίνει η εγκατάσταση για πρώτη φορά. Χρειάζεται το IDPS να είναι σωστά ρυθμισμένο ώστε να αναγνωρίσει τι είναι κανονική κυκλοφορία στο δίκτυο έναντι αυτού που θα μπορούσε να είναι κακόβουλη κυκλοφορία. Οι διαχειριστές ή χρήστες είναι υπεύθυνοι για την αντιμετώπιση των IDPS ειδοποιήσεων, πρέπει να καταλάβουν τι σημαίνουν τα σήματα και πώς θα ανταποκριθούν αποτελεσματικά. Αποτέλεσμα αυτού είναι να υπάρχουν διάφορα συστήματα IDPS αναλόγως της αποστολής τους. Ποιο κάτω μελετάμε τα ευρύτερα αξιοποιούμενα σε μια κρίσιμη υπολογιστική υποδομή [28]. Επιπλέον παραθέτουμε ένα συγκριτικό πίνακα μεταξύ των ευρύτερων αξιοποιούμενων όπως την παρακάτω εικόνα.

Intrusion Detection Technique	Network Usage	Throughput	Speed	Large User Community	IPS Capability	Open Source	Installation/ Deployment	Analysis GUI	Operating system	Parameters
Anomaly Based	Less	Maximum	Faster	No	No	Yes	Typical	Less	Unix	Bro
Signature based	Medium	Moderate	Fast	Yes	Yes	Yes	Easy	Many	Win/ Unix/ Mac	Snort
Signature based	Less	Moderate	Medium	-	No	Yes	Easy	Less	Unix	NFR
Signature based	Very Less	Maximum	Faster	No (Emerging)	Yes	Yes	Intermediate	Many	Win/Unix/ Mac/BSD	Suricata
Host based	Medium	Maximum	Fast	Less	No	No	Easy	Standalone	Unix	Dragon Squire

Εικόνα 6.3 : Συγκριτικός Πίνακας με γνωστά IDPS

6.3.1 Snort

Εικόνα 6.3.1 : Snort

6.3.1.1 Λίγα λόγια για το Snort

Το Snort είναι ένα ελαφρύ, ανοιχτού κώδικα σύστημα ανίχνευσης και πρόληψης εισβολών. Έχει την ικανότητα να αναλύει δικτυακή κίνηση σε πραγματικό χρόνο, να ειδοποιεί για πιθανές επιθέσεις, να μπλοκάρει και να καταγράφει πακέτα σε δίκτυα πρωτοκόλλου IP (Internet Protocol). Χρησιμοποιεί ένα συνδυασμό μηχανισμών ανάλυσης των διαφόρων πρωτοκόλλων επικοινωνίας και αναγνώρισης προτύπων με σκοπό να ανιχνεύσει ανωμαλίες, επιθέσεις και άλλες περιπτώσεις κατά τις οποίες γίνεται κακή χρήση του δικτύου. Επιπλέον, χρησιμοποιεί μια ευέλικτη γλώσσα κανόνων για να περιγράψει τις δραστηριότητες που μπορούν να θεωρηθούν κακόβουλες. Η μηχανή ανάλυσης και ανίχνευσης του Snort αποτελείται από ένα σύνολο διαφορετικών υποσυστημάτων (plugins) που, όπως θα δούμε παρακάτω, ενσωματώνονται σε μια ενιαία αρχιτεκτονική.

Το Snort αποτελεί μια από τις πιο μοντέρνες εφαρμογές στον τομέα της αναγνώρισης εισβολών, προσφέροντας 3 βασικές λειτουργίες. Μπορεί να λειτουργήσει: α) ως παρατηρητής πακέτων δικτύου (network packet sniffer), β) ως καταγραφέας δικτυακών πακέτων ή γ) ως ένα Network-based IDS. Υπάρχουν, επίσης, πάρα πολλά προγράμματα που μπορούν να προστεθούν στο Snort τα οποία προσφέρουν επιπλέον τρόπους διαχείρισης των αρχείων καταγραφών του (logfiles) και μπορούν να ανανεώνουν το σετ των υπογραφών/κανόνων της μηχανής ανίχνευσης. Με αυτό τον τρόπο, δίνεται η δυνατότητα στους διαχειριστές των δικτύων να ελέγξουν με πιο αποδοτικό τρόπο την πιθανότητα ύπαρξης κακόβουλης κίνησης και να μπορούν να ειδοποιηθούν σε αντίστοιχη περίπτωση [1, 9].

Τα βασικότερα στοιχεία που διατηρεί το Snort από την αρχή της υλοποίησής του (από τον Martin Roesch) μέχρι και σήμερα είναι ότι μπορεί να λειτουργήσει σε διάφορα λειτουργικά συστήματα και ότι πρόκειται για μια φορητή εφαρμογή . Τέλος, έχει έξοδο και σε δεκαεξαδική αλλά και σε ASCII μορφή, ενώ όλων των ειδών τα πακέτα μπορούν να αποτυπωθούν με μια πλήρη, σταθερή και συνεπή μορφή.

6.3.1.2 Συστατικά Snort- Αρχιτεκτονική

Το Snort στηρίζεται στα παρακάτω στάδια τα οποία αντιστοίχως εκτελούν τις λειτουργίες τους με σκοπό να επιτευχτεί η ανίχνευση του κακόβουλου προγράμματος [1]:

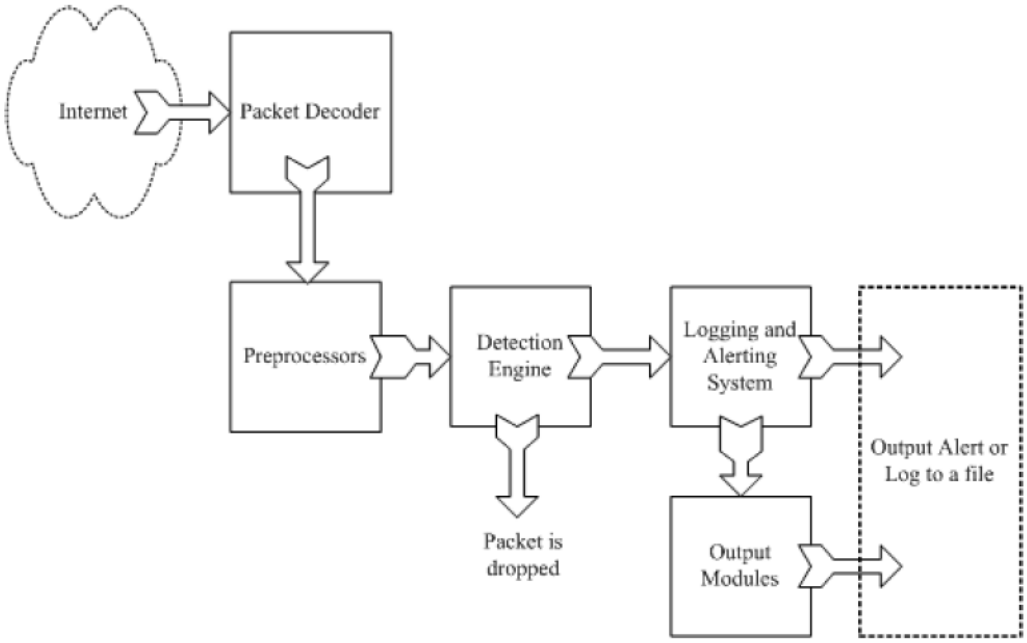
- Αποκωδικοποιητής πακέτων (Packet Decoder): παίρνει πακέτα από διαφορετικούς τύπους των διεπαφών δικτύου (Ethernet, SLIP, PPP κ.ά.) και ετοιμάζει τα πακέτα για επεξεργασία.

- Προεπεξεργαστής (Preprocessor): προετοιμάζει τα δεδομένα για την μηχανή ανίχνευσης, ανιχνεύει ανωμαλίες στις επικεφαλίδες των πακέτων, ανασυγκροτεί τα πακέτα κάνει αποκωδικοποίηση HTTP URI επανασυναρμολογεί τα TCP ρεύματα (streams).

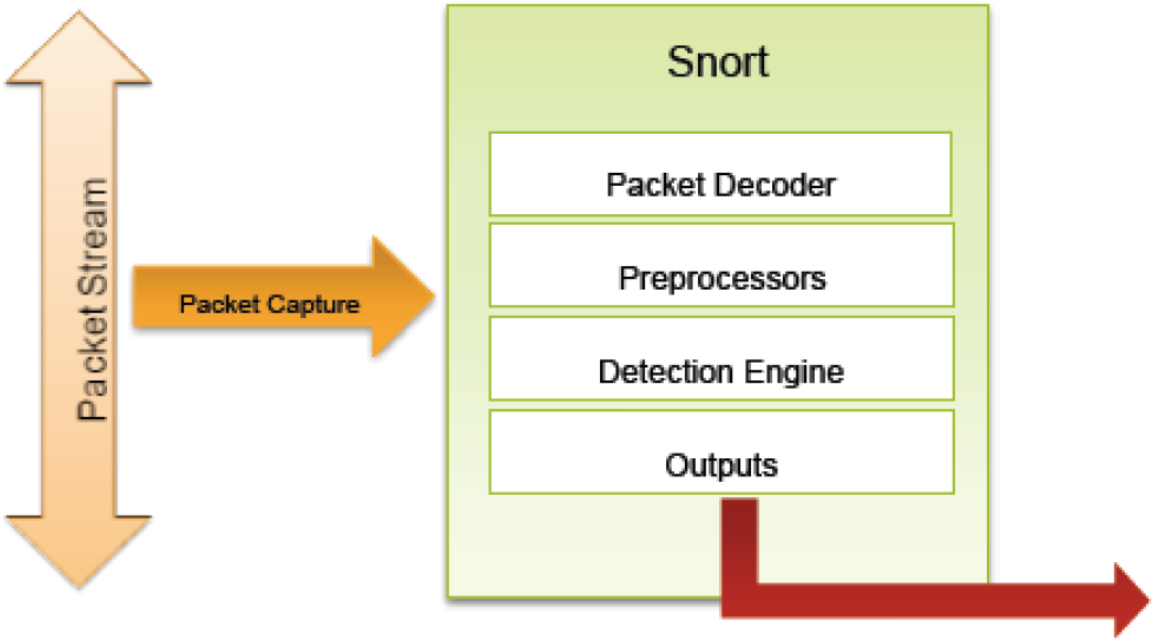
- Μηχανή ανίχνευσης: το πιο σημαντικό μέρος, εφαρμόζει τους κανόνες για τα πακέτα

- Καταγραφή και σύστημα συναγερμού.

- Μονάδες Εξόδου: επεξεργάζονται τις ειδοποιήσεις και τις καταγράφουν για να παράγουν το τελικό αποτέλεσμα (Εικόνα 6.3.1.2.2).



Εικόνα 6.3.1.2.1: Συστατικά του Snort



Εικόνα 6.3.1.2.2 : Αρχιτεκτονική του Snort IDS και πορεία πληροφορίας.

6.3.1.3 Προκλήσεις Snort

Πέραν των δυνατοτήτων που παρουσιάστηκαν καλό είναι να αναφερθούμε και σε κάποιες σημαντικές προκλήσεις που καλείται να αντιμετωπίσει το Snort. Αναλυτικότερα είναι οι παρακάτω:

- Κατάχρηση ανίχνευσης - αποφυγή γνωστών εισβολών
- Η βάση δεδομένων των κανόνων είναι όλο και μεγαλύτερη και αυξάνεται συνεχώς
- Στη snort έκδοση 2.3.2, υπάρχουν 2,600 κανόνες 80% από αυτούς είναι υπογραφές
- Το Snort δαπανά το 80% του χρόνου εργασίας για να κάνει αντιστοίχηση strings
- Ανίχνευση με βάση την ανωμαλία - εντοπισμός νέων επιθέσεων: Η πιθανότητα ανίχνευσης είναι χαμηλή.

6.3.2 Suricata

Εικόνα 6.3.2 : Suricata

6.3.2.1 Λίγα λόγια για το Suricata

Το Suricata είναι ένα δίκτυο υψηλής απόδοσης IDPS για την Ασφάλεια Δικτύων Παρακολούθησης. Είναι ένα Open Source σύστημα και ανήκει σε μια κοινότητα που εργάζεται για μη κερδοσκοπικό ίδρυμα, το Ίδρυμα Open Information Security (OISF). Συγκεκριμένα το Suricata έχει αναπτυχθεί από την OISF και υποστηρίζεται από τους υποστηρικτές της. Αποτελεί σύστημα επόμενης γενιάς και δεν πρόκειται απλώς να αντικαταστήσει ή να μιμηθεί τα υφιστάμενα εργαλεία στον κλάδο, αλλά θα φέρει νέες ιδέες και τεχνολογίες στον τομέα

Το Suricata ξεχωρίζει για τα 3 ποιο κάτω δεδομένα:

1. Multi-threading

Το Suricata είναι μια πολυνηματική (multi-threaded) μηχανή. Αυτό σημαίνει ότι μπορεί να εκτελέσει αυξημένη ταχύτητα και αποτελεσματικότητα στην ανάλυση της κίνησης δικτύου και παράλληλα να εξισορροπήσει το φορτίο της επεξεργασίας . Αυτό έχει σαν αποτέλεσμα να μπορεί να επιτύχει ταχύτητες 10 gigabit.

2. Πρωτόκολλο αναγνώρισης

Τα πιο κοινά πρωτόκολλα αναγνωρίζονται αυτόματα από το Suricata. Αυτό καθιστά το Suricata το πιο αποτελεσματικό στα Malware εμπόδια. Επιπλέον, διαθέτει εύρος λέξεων - κλειδιών που μπορούν να ταιριάξουν σε διάφορα πρωτόκολλα.

3. Φάκελος αναγνώρισης, MD5 Checksums και Εξαγωγή αρχείων

Το Suricata μπορεί να εντοπίσει χιλιάδες είδη αρχείων κατά τη διέλευση του από ένα δίκτυο. Όχι μόνο να το εντοπίσει, αλλά μπορεί να το εξετάσει και περαιτέρω, μέχρι και στο επίπεδο εξαγωγής του.

6.3.2.2 Χαρακτηριστικά Suricata

Ο στόχος του σχεδιασμού του Suricata σε πρώτη φάση ήταν να υπάρχει μια λειτουργική και διανεμητέα μηχανή IDPS . Η αρχική έκδοση (beta version) ήταν διαθέσιμη από την 1η Ιανουαρίου 2010. Η μηχανή υποστηρίζει ή παρέχει τις ακόλουθες λειτουργίες: το τελευταίο SnortVRT, την Snort υλοτομία, τις επιλογές βασικής γλώσσας, multithreading, την επιτάχυνση υλικού (με

εξαρτήσεις / περιορισμούς της κάρτας δικτύου και υλικού), ενιαία έξοδο που επιτρέπει την αλληλεπίδραση με εξωτερικά συστήματα διαχείρισης καταγραφής, IPv6, την βασισμένη σε κανόνες «φήμη» IP, βιβλιοθήκη με την ικανότητα αλληλεπίδρασης με άλλες εφαρμογές, έξοδο για στατιστικά απόδοσης και ένα απλό και αποτελεσματικό εγχειρίδιο χρήσης.

Με τη συνεργασία της κοινότητας ανοιχτού λογισμικού(open source) και τον ηγετικό ID / PS σετ κανόνων που διατίθενται, η OISF έχει κατασκευάσει τη μηχανή Suricata για να απλοποιηθεί η διαδικασία της διατήρησης των βέλτιστων επιπέδων ασφαλείας. Μέσω στρατηγικών συνεργασιών, η OISF αξιοποιεί την εμπειρία των νέων απειλών (www.emergingthreats.net) και άλλους επιφανείς πόρους στη βιομηχανία έτσι ώστε να παρέχει το πιο σύγχρονο και ολοκληρωμένο σετ κανόνων .

Η HTP βιβλιοθήκη είναι ένας κανονικοποιητής (normalizer) και μεταφραστής HTTP που γράφτηκε από τον Ιβάν Ρίστιτς του Mod Security fame για την OISF. Η βιβλιοθήκη αυτή ενσωματώνει και παρέχει πολύ προηγμένη επεξεργασία των ροών HTTP για το Suricata. Η βιβλιοθήκη HTP απαιτείται από την μηχανή, αλλά μπορεί επίσης να χρησιμοποιηθεί ανεξάρτητα σε ένα ευρύ φάσμα εφαρμογών και εργαλείων [48].

.
Επιπλέον χαρακτηριστικά του Suricata είναι [28] :

- Υποστήριξη όλων των λειτουργικών συστημάτων
- Παράλληλη λειτουργία με IPS συστήματα
- Αυτόματη ανίχνευση πρωτοκόλλων με υψηλή απόδοση
- Αποτελεί ένα δίκτυο παρακολούθησης της ασφάλειας
- Φιλτράρισμα των συναγερμών και των συμβάντων
- Εξωτερική υποστήριξη άλλων εργαλείων για την ανάλυση δεδομένων

Επιπλέον, μέσα από τη μορφή εξόδου Unified2 και του εργαλείου Barnyard2, το Suricata μπορεί να χρησιμοποιηθεί με BASE, Snorby, Sguil, SQueRT και άλλα εργαλεία με άριστη διαλειτουργικότητα αλλά και επιφέροντας επιτυχή αποτελέσματα (Εικόνα 6.3.2.2) [33].

Εικόνα 6.3.2.2 : Το Suricata με συνδυασμό άλλων εργαλείων

6.3.2.3 Σύγκριση με άλλα IDPS

Σκόπιμο θα ήταν να παρουσιάσουμε τις διάφορες λειτουργίες που διαθέτει το σύστημα μας αυτό και πάντα συγκρινόμενο με άλλα συστήματα (Εικόνα 6.3.2.3). Από αυτό διαφαίνεται η υψηλή απόδοση του αλλά και η αποτελεσματικότητα του γεγονός που το κατατάσσει στα ευρύτερα αξιοποιούμενα.

Features	Existing IDS/IPS Engines (Open and Commercial)	Suricata (by the OISF)
Multi - Threaded Processing	No	Yes
Complete IPv6 Support	Some	Complete
IP Reputation	Cisco Only	Yes (soon)
Automated Protocol Detection	No	Yes
GPU Acceleration	No	Yes
Multi - Platform Native Hard- ware Acceleration Support	No	Yes

Global Variables/Flowbits	No	Yes (soon)
Full Windows Support	Some	Yes
Inline Windows Support	No	Yes
GeoIP Lookups	No	Yes (soon)
Advanced HTTP Parsing	No	Yes
HTTP Access Logging	No	Yes
SMB Acces Logging	No	Yes (soon)
HTTP Blocklist Lookups	No	Yes (soon)
Free	Some	Yes

Εικόνα 6.3.2.3 : Λειτουργίες που διαθέτει το Suricata σε σύγκριση με τα υπόλοιπα IDPS που είναι διαθέσιμα στην αγορά.

6.3.3 Bro

Εικόνα 6.3.3: Bro

6.3.3.1 Λίγα λόγια για το Bro

Το Bro είναι ένα open-source σύστημα, το οποίο είναι Unix-based Network Intrusion Detection System (NIDS) και παρακολουθεί παθητικά την κυκλοφορία του δικτύου ψάχνοντας για ύποπτη δραστηριότητα. Το Bro ανιχνεύει εισβολές από την πρώτη κυκλοφορία του δικτύου ανάλυσης και στη συνέχεια εξαγάγει σε επίπεδο εφαρμογής τη σημασιολογία ενώ στη συνέχεια εκτελεί εκδήλωση προσανατολισμένη σε αναλυτές που συγκρίνουν τη δραστηριότητα με πρότυπα που την κρίνουν ως ενοχλητική (Richard, 2005). Η ανάλυσή περιλαμβάνει την ανίχνευση των

συγκεκριμένων επιθέσεων, συμπεριλαμβανομένου εκείνων που ορίζονται από τις υπογραφές , αλλά επίσης και εκείνα που ορίζονται από ασυνήθιστες δραστηριότητες [43].

Το Bro χρησιμοποιεί μια εξειδικευμένη πολιτική που επιτρέπει σε ένα site να προσαρμόσει τη λειτουργία του, καθώς και πολιτικές που βοηθούν σε εξελισσόμενες νέες επιθέσεις που ανακαλύφθηκαν. Αν το Bro εντοπίσει κάτι ύποπτο, μπορεί να προχώρηση στην καταχώρηση του στο μητρώο, επίσης στην προειδοποίηση του χειριστή σε πραγματικό χρόνο , καθώς και στην εκτέλεση μιας εντολής του λειτουργικού συστήματος (π.χ για να τερματίσει μια σύνδεση ή ένα μπλοκ κακόβουλο υποδοχής). Επιπλέον , λεπτομερή αρχεία καταγραφής του Bro μπορεί να είναι ιδιαίτερα χρήσιμα για την εγκληματολογία.

6.3.3.2 Δυνατότητες Bro

Το Bro σαν σύστημα πέραν των βασικών του χαρακτηριστικών, παρουσιάζει και κάποιες δυνατότητες που το καθιστούν στα ισχυρά IDS και αναλύονται μέσα από τις παρακάτω εικόνες [19]. Συγκεκριμένα η εικόνα 6.3.3.2.1 μας δίνει πληροφορίες μέσα από ανάλυση που γίνεται σε χρονική περίοδο μίας μέρας. Παρατηρούμε αποτελέσματα από δέκα σαρώσεις καθώς επίσης και μια επιτυχημένης καταστολής μιας επίθεσης. Επιπλέον το τμήμα στατιστικής κυκλοφορίας εμφανίζει τον συνολικό αριθμό των πακέτων που διήλθαν. Η εικόνα 6.3.3.2.3 μας αναλύει συνοπτικά τις πληροφορίες και δίνει μια πιο λεπτομερή παρουσίαση του επιθετικού περιστατικού. Παρατηρούνται αναλυτικά η διεύθυνση IP του εισβολέα, ο στόχος που είχε αλλά και οι συναγερμοί και επιθέσεις που χρησιμοποιήθηκαν. Όσον αφορά την εικόνα 6.3.3.2.2 δίδονται οι διάφορες πληροφορίες που αφορούν το ιστορικό των επιθέσεων και συγκεκριμένα ότι είχαμε 14 επιτυχείς συνδέσεις σε βάρος του απομακρυσμένου υπολογιστή, ενώ 10 από αυτές ήταν ανεπιτυχής. Επιπλέον μας παρουσιάζει ενδείξεις της ημερομηνίας, της υποδοχής, καθώς και της πραγματικής θύρας που σαρώθηκε. Τέλος στις εκθέσεις παρατηρείται ότι δεν απεικονίζεται το χρονικό διάστημα του περιστατικού στο οποίο γίνονται προσπάθειές παραβιάσεις παρόλο που το Bro μας προσφέρει ένα διάστημα εμπιστοσύνης και μας παρουσιάζει την πιθανότητα επιτυχημένων επιθέσεων σε χρονοδιάγραμμα.

```
Bro Report                                                    Organization Name
=============================================================================
Summary                          July 28, 2004 17:01 to July 29, 2004 17:00
=============================================================================
 Incident       Likely Successful          1
 Summary        Unknown                    0
                Likely Unsuccessful        0
                Scans                     10

 System         Bro disk space:   <% at time of report generation>
 Statistics     Bro Process cpu:  <time>
                Bro restarts:     <date/time>
                System reboots:   <date/time>

 Traffic        Number of packets:       <count>
 Statistics     Number of valid packets: <count>  <% of total>
                Protocol summary
                Http: <count>   <% of total>
                SSH : <count>   <% of total>
                SMTP: <count>   <% of total>
                Etc.
                Average bandwidth:
                Peak bandwidth:
=============================================================================
```

Εικόνα 6.3.3.2.1: Έκθεση περιστατικού με τη χρήση του Bro για χρονικό διάστημα 1 ημέρας

```
Remote Host Connection History (all successful/unsuccessful to site)
      24 hrs     |      3 days      |      7 days      |      30 days
-----------------------------------------------------------------------------
       14/10     |        0/0       |        0/0       |        0/0
-----------------------------------------------------------------------------
  Total since remote host first seen on 07/29/04: 14/10

=============================================================================
Scans
=============================================================================
==
Date Dropped            Host                                    Port Scanned
-----------------------------------------------------------------------------
Jul 29 13:14 n219077002119.netvigator.com                        (3128/tcp)
Jul 29 13:23 node1.lbnl.nodes.planet-lab.org                     (49702/tcp)
Jul 29 13:30 213-145-189-50.dd.nextgentel.com                    (4899/tcp)
Jul 29 13:32 211.55.52.67                                        (1034/tcp)
Jul 29 13:52 user-69-1-11-116.knology.net                        (3128/tcp)

*****************************************************************************
```

Εικόνα 6.3.3.2.2: Ιστορικό συνδέσεων σε απομακρυσμένο υπολογιστή

```
Incident     ORGCODE-000002                                  LIKELY SUCCESSFUL
---------------------
Remote Host: 84.136.138.21   p54877614.dip.hacker.net
 Local Host: 124.333.183.162 pooroljoe.dhcp.org.com

Alarm(s) 1 MS-SQL xp_cmdshell - program execution
           Jul 29 12:43 84.135.118.20 -> 128.3.183.62
         2 TFTP Get Runtime.exe
           Jul 29 12:43 128.3.183.62 -> 84.135.118.20

Connections (only first 25 after alarm are listed)
-----------
                  time      byte   remote       local    byte
 date    time   duration  transfer  port  type   port  transfer  protocol
----- -------- -------- --------- -----  ---- ------ --------- ----------
07/29 12:43:31        ?     566 b  4634  1  >  1433      467 b  tcp/MSSQL
07/29 12:43:31        0         ?  2318  2 <     69       20 b  udp/tftp
07/29 12:43:32    265.7       4 b  4638  * <   2318      3.0kb  udp
07/29 12:48:56        ?         ?  4640    >  2362          ?  tcp
07/29 12:50:05        ?    11.4kb  4639  * <   3333      8.6kb  tcp
07/29 12:53:00        0         ?  4684  *  >  2362          ?  tcp
07/29 12:53:07        ?         ?  4685  *  >  2362          ?  tcp
07/29 12:53:59        ?         ?  4689  *  >  2362          ?  tcp
07/29 12:54:14      6.1         0  4693  * <   2380     94.2kb  tcp
07/29 12:54:21       .5      50 b  4694    >  2381          0  tcp
07/29 12:54:23       .7         ?  4695   <   2382          0  tcp
07/29 12:54:25       .5      51 b  4696  *  >  2383          0  tcp
07/29 12:54:27       .5      61 b  4697  *  >  2384          0  tcp
07/29 12:54:28       .7      39 b  4698    >  2385          0  tcp
07/29 12:54:31       .5      41 b  4699  *  >  2386          0  tcp
07/29 12:54:33      1.2    4.9 kb  4700    >  2387          0  tcp
07/29 12:54:35     12.8  195.0 kb  4701  * <   2388          0  tcp
07/29 12:54:53       .2         ?  4703   <   2390          0  tcp
07/29 12:54:54       .5      37 b  4704    >  2391          0  tcp
07/29 12:54:56      3.4      23 b  4705  *  >  2392          0  tcp
07/29 12:55:04     21.4  308.7 kb  4706    >  2393          0  tcp
07/29 12:55:27     50.7         ?  4707    >  2394          ?  tcp
07/29 12:59:23        ?         ?  4775    >  1433          ?  tcp
07/29 12:59:25        ?         ?  4774  *  >  3333          ?  tcp
```

Εικόνα 6.3.3.2.3: Έκθεση Συμβάντος μέσω του Bro με συναγερμούς και συνδέσεις που τέθηκαν

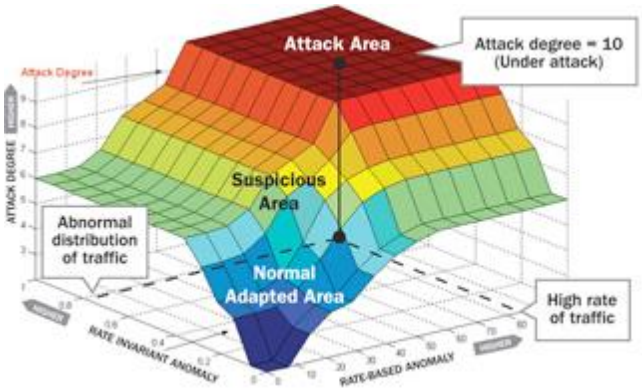
6.3.4 Radware

Εικόνα 6.3.4: Radware

6.3.4.1 Λίγα λόγια για το Radware

Το Radware αποτελεί ένα IPS (Intrusion Prevention System) σύστημα με ένα μοναδικό και ξεχωριστό τρόπο καθώς αναλύει πολλαπλούς τύπους κυκλοφορίας σε ένα δίκτυο προκειμένου να ανιχνεύσει και να αντιμετωπίσει πιθανές επιθέσεις προτού αυτές αναγνωριστούν και καταχωρηθούν σαν επίσημες επιθέσεις [19] . Το ποιο πάνω επιτυγχάνεται από το σύστημα αυτό

αναλύοντας τόσο το δίκτυο ,όσο και τις κινήσεις των servers και clients που διέρχονται από το δίκτυο αυτό. Τα πρότυπα που χρησιμοποιούνται στην περίπτωση αυτή είναι το "rate-based anomalies" (μεγάλος αριθμός κυκλοφορίας), το "rate invariant anomalies" (μη φυσιολογική κίνηση) και το "attack degree" (ανίχνευση πραγματικής επιβλαβής επίθεσης). Όλα αυτά τα πρότυπα μας καθορίζουν τις διάφορες περιοχές επίθεσης από τις οποίες διακρίνεται η επικινδυνότητα της περιοχής επίθεσης κατατάσσοντας τις παράλληλα με βαθμό επικινδυνότητας όπως φαίνεται και στην εικόνα 6.3.4.1. Αποτέλεσμα αυτού είναι να μπορούμε να πάρουμε τα αναγκαία μέτρα για την προστασία από τις πιθανές επιθέσεις.



Εικόνα 6.3.4.1: Ιστορικό συνδέσεων σε απομακρυσμένο υπολογιστή

Έτσι μόλις εντοπιστεί μια επιβλαβής επίθεση, τα Radware IPS συστήματα δημιουργούν ένα κανόνα αποκλεισμού για την συγκεκριμένη επίθεση. Αν η επίθεση αργότερα μεταλλαχθεί τότε το Radware IPS είναι σε θέση δυναμικά να τροποποίηση τα χαρακτηριστικά του και να αντιμετωπίσει εκ νέου την νέα επίθεση. Το γεγονός ότι έχει την δυνατότητα να αντιληφθεί μια καινούργια επίθεση η οποία δεν είναι καταχωρημένη και να την αντιμετώπιση αποτελεί μοναδικό χαρακτηριστικό για ένα IPS σύστημα και για αυτό το λόγο το Radware IPS ξεχωρίζει.

6.3.4.2 Βασικά χαρακτηριστικά Radware

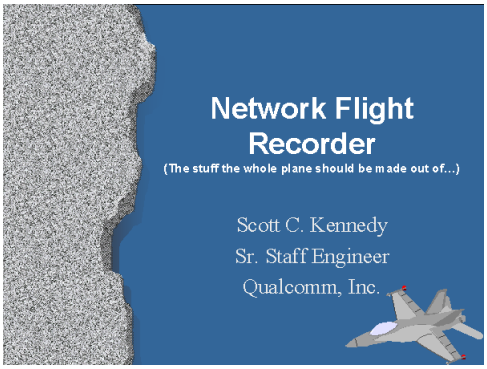
Τα Radware IPS συστήματα βασιζόμενα στην τεχνολογία ανίχνευσης υπογραφών με την οποία επιτυγχάνεται η πρόληψη και αντιμετώπιση των γνωστών τρωτών σημείων, μπορεί να

ανιχνεύσει και μετριάζει τις αναδυόμενες επιθέσεις του δικτύου σε πραγματικό χρόνο, όπως τις επιθέσεις zero-λεπτό, τις επιθέσεις DoS / DDoS. Όλα αυτά γίνονται μάλιστα χωρίς την ανάγκη για ανθρώπινη παρέμβαση αλλά και χωρίς να εμποδίζεται η κίνηση του δικτύου γεγονός που αποτελεί σημαντικό χαρακτηριστικό στις δυνατότητες του συστήματος.

Το Radware διαθέτει τα παρακάτω χαρακτηριστικά [23]:

- Διατήρηση επιχειρησιακής κατάστασης και συνέχιση των εργασιών του ανεξάρτητα του αν το δίκτυο βρίσκεται υπό επίθεση
- Παροχή λύσεων ασφαλείας για κέντρα δεδομένων
- Υψηλές δυνατότητες παρακολούθησης και πληροφόρησης για παροχή λύσεων
- Επιτυγχάνεται μείωση συνολικού κόστους στην Διαχείριση Ασφάλειας
- Διατήρηση επιχειρησιακής συνέχειας και παραγωγικότητας ενώ παράλληλα επιτυγχάνεται και η προστασία από τις DDoS απειλές.
- Ακριβής Πρόληψη Επιθέσεων
- Υψηλή απόδοση
- "Pay-As-You-Grow" για μείωση CAPEX
- Ευκολία Διαχείρισης Ασφάλειας για μείωση OPEX

6.3.5 Network Flight Recorder (NFR)



Εικόνα 6.3.5: Network Flight Recorder (NFR)

6.3.5.1 Λίγα λόγια για το NFR

Το Network Flight Recorder (NFR) αποτελεί ένα ξεχωριστό σύστημα, που πέραν των χαρακτηριστικών IDPS που παρουσιάζει διαθέτει και επιπλέον δυνατότητες αξιοποιήσεις σε περιβάλλον κρίσιμων υποδομών. Όπως καταδεικνύει και το όνομα του προϊόντος το NFR σχεδιάστηκε με πρωταρχικό στόχο την επίτευξη μιας μεταμοντέρνας ανάλυσης των γεγονότων που συμβαίνουν σε ένα δίκτυο, όπως για παράδειγμα όταν ένας administrator θέλει να διαπιστώσει τι πραγματικά έγινε στο δίκτυο κατά την εισβολή ή κάποια άλλη ανωμαλία του συστήματος. Γενικότερα σχεδιάστηκε με απώτερο σκοπό να υποστηρίζει τα συστήματα IDPS [4].

Το NFR παρέχει δυνατότητες καταγραφής και φιλτραρίσματος της κίνησης στο δίκτυο με σκοπό την καταχώρηση σε αρχεία ή την στατιστική ανάλυση και μπορεί να ρυθμιστεί έτσι ώστε να πυροδοτεί (trigger) συναγερμό σε συγκεκριμένα γεγονότα. Το βασικότερο χαρακτηριστικό του NFR είναι ο λιτός σχεδιασμός του και η προσαρμοστικότητά του στις ανάγκες των χρηστών. Ως συνήθως, αυτό μπορεί να αποτελέσει και τη μέγιστη αδυναμία του, αφού ένας χρήστης πρέπει να γνωρίζει σαφώς τι ακριβώς αναζητά.

Επιμέρους χαρακτηριστικά του NFR είναι [31]:

- Διαθέτει ενσωματωμένα μέσα τα οποία υποβοηθούν την επέκταση καθώς και την προσαρμογή του.

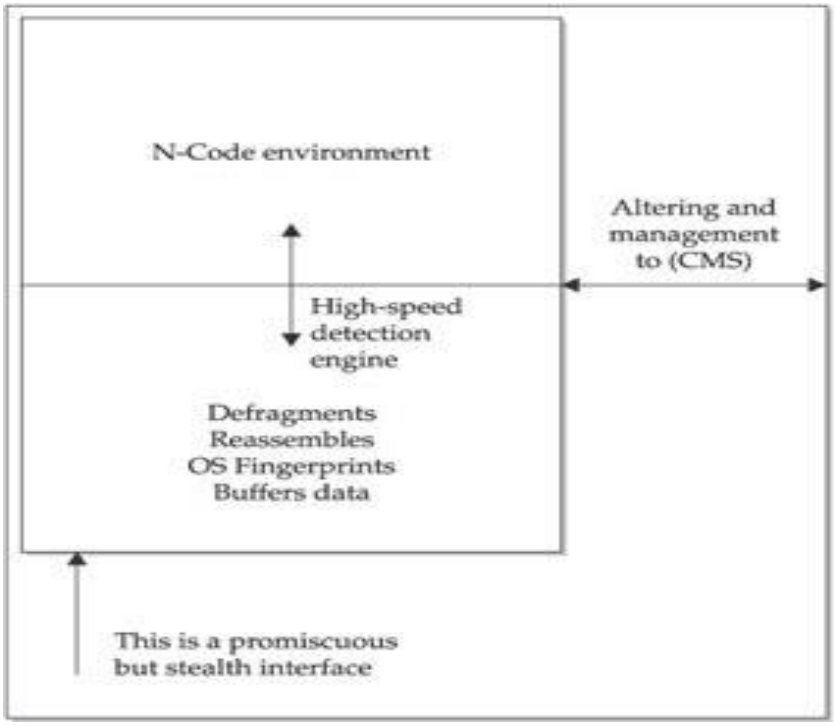
- Χρησιμοποιεί γλώσσα που είναι ευέλικτη σε δίκτυο υψηλής κυκλοφορίας.

- Δεν εμποδίζει τη δραστηριότητα του δικτύου

- Διαθέτει δυνατότητα δυναμικής ειδοποίησης.

6.3.5.2 Αρχιτεκτονική NFR

Το εργαλείο ανίχνευσης εισβολών Network Flight Recorder (NFR) αποτελείται από τρία συστατικά [22]. Το πρώτο, γνωστό ως **packet sucker**, διαβάζει τα πακέτα από το δίκτυο. Τα πακέτα δρομολογούνται προς μία μηχανή απόφασης, η οποία χρησιμοποιεί ορισμένα φίλτρα που είναι γραμμένα σε γλώσσα N-code για να εξάγει πληροφορίες. Το NFR παρέχει δύο επίπεδα μηχανισμών ανίχνευσης όπως φαίνεται και από την εικόνα 6.3.5.2.1. Όταν απαιτείται, τα πακέτα θα ελεγχθούν με βάση έναν πίνακα καταστάσεων για να επιτρέψουν την επανασυναρμολόγηση των τεμαχισμένων πακέτων. Τα φίλτρα είναι συνδεδεμένα με γεγονότα, όπως για παράδειγμα με αφίξεις πακέτων. Το δεύτερο συστατικό, γνωστό ως **backend**, γράφει στο δίσκο τα δεδομένα που παράγονται από τα φίλτρα και ακολούθως το ίδιο το πακέτο απορρίπτεται. Το τρίτο συστατικό, το **query backend**, επιτρέπει στους διαχειριστές να εξάγουν μη επεξεργάσιμα και επεξεργάσιμα δεδομένα από το δίσκο. Το query backend μπορεί να υπολογίσει σειρά στατιστικών στοιχείων των δεδομένων, όπως το χρονικό διάστημα ανάμεσα στις αφίξεις δύο πακέτων για ένα συγκεκριμένο διακομιστή και να παρουσιάσει τα στοιχεία με ποικίλες μορφές. Ο διαχωρισμός του μηχανισμού υποβολής ερωτημάτων από τη ροή εισαγωγής πακέτων επιτρέπει στους διαχειριστές να υποβάλλουν ερωτήματα στο NFR, χωρίς αυτό να επιδρά αρνητικά στη δυνατότητά του να χειριστεί τα εισερχόμενα πακέτα.



Εικόνα 6.3.5.2.1: NFR - Μηχανισμός ανίχνευσης

Αν και υπάρχουν ορισμένα έτοιμα φίλτρα, οι χρήστες μπορούν να γράψουν δικά τους χρησιμοποιώντας τη γλώσσα N-code. Αυτή η γλώσσα είναι προσανατολισμένη σε στοίβα και υπάρχει διερμηνευτής ενσωματωμένος στο εργαλείο NFR. Περιλαμβάνει όλα τα συνηθισμένα χαρακτηριστικά γνωρίσματα γλώσσας υψηλού επιπέδου (βρόχους, συνθήκες ελέγχου κλπ.), όπως και ένα σύνολο από τύπους δεδομένων για μετρητές και διευθύνσεις IP. Τα πακέτα θεωρούνται δομές και τα πεδία είναι ενσωματωμένα στη γλώσσα. Για παράδειγμα, στον κώδικα που ακολουθεί, το φίλτρο αγνοεί όλη την κυκλοφορία που δεν προορίζεται για ένα σύνολο εξυπηρετών παγκόσμιο ιστού [22]:

 # list of my web servers

my_ web _servers - [10.237.100.189 10.237.55.93] ;

 # we assume all HTTP traffic is on port 80 filter watch tcp (client, dport:80)

{

if (ip. dest != my _web _servers)

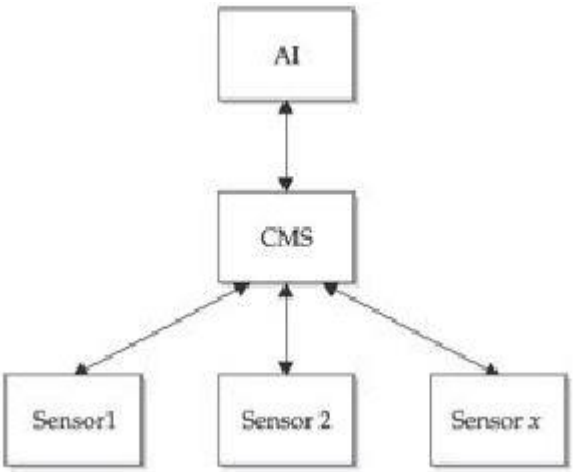
return;

 # now process the packet; we just write out packet info

record system.time, ip.src,- ip.dest to www._list;

}
www_list = recorder("log")

Μία προσέγγιση αρχιτεκτονικής του NFR φαίνεται στην παρακάτω εικόνα στην οποία διαφαίνονται οι αισθητήρες που βρίσκονται στο πρώτο επίπεδο, από το οποίο γίνεται η συλλογή των πληροφοριών. Στην συνέχεια στο δεύτερο επίπεδο όλες αυτές οι πληροφορίες καταλήγουν στο κεντρικό σύστημα διαχείρισης όπου αποθηκεύει και επεξεργάζεται τις πληροφορίες αυτές σε ένα ενιαίο και κεντρικό σημείο. Τέλος στο επίπεδο AI γίνεται η όλη επεξεργασία του περιβάλλοντος του IDPS [31].



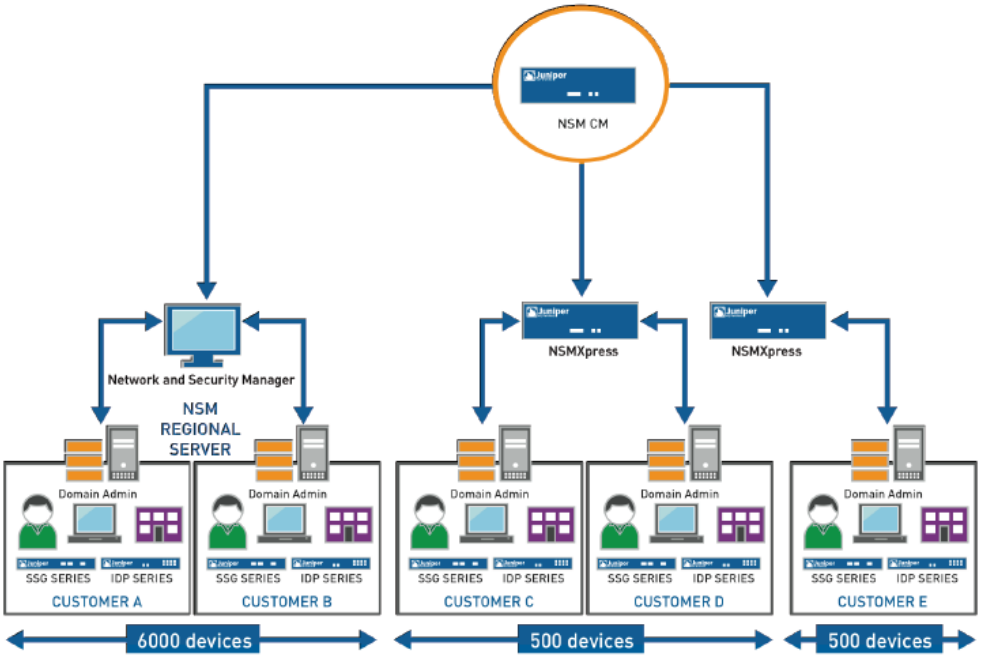
Εικόνα 6.3.5.2.2: NFR – Επίπεδα αρχιτεκτονικής

6.3.6 Juniper

Εικόνα 6.3.6 : Juniper

6.3.6.1 Λίγα λόγια για το Juniper

Η Juniper Networks βρίσκεται σε υψηλό επίπεδο έχοντας σχεδιάσει ένα IPS που μπορεί να προσφέρει ασφάλεια είτε σε αυτόνομα συστήματα είτε σε ολόκληρα δίκτυα, συνδυάζοντας τη λειτουργικότητα των HIDS με αυτή των NIDS. Το Juniper IPS μπορεί να συνυπάρξει και με άλλα λογισμικά ασφαλείας. Υλοποιείται ως μια εφαρμογή που μπορεί να ομαδοποιηθεί με άλλες λειτουργίες περιμέτρου όπως τα firewalls. Η εξέλιξη δε των συστημάτων που αγόρασε από την Netscreen Technologies στην ανάπτυξη της πλατφόρμας JUNOS της επέτρεψε να παραμείνει σε υψηλό επίπεδο στην αγορά των IDPS. Το IPS είναι σε θέση να κατανοήσει τις εφαρμογές των κανόνων δικτύου αλλά και του συστήματος ελέγχου πρόσβασης. Η εικόνα 6.3.6.1 απεικονίζει τις αλληλεπιδράσεις μεταξύ των κόμβων αλλά και τη πρόσβαση στο σύστημα ελέγχου από την οποία μπορούν να συλλέγουν πληροφορίες που αφορούν την πολιτική ασφαλείας του δικτύου [19, 38].



Εικόνα 6.3.6.1 : Πρόσβαση στο σύστημα ελέγχου των Juniper IPS κόμβων

6.3.6.2 Χαρακτηριστικά Juniper

Το Juniper IPS χειρίζεται τις αναφορές στόχων πάρα πολύ καλά και έχει την ικανότητα να παρέχει αναφορές που αφορούν τις συσκευές του διαχειριστή ασφαλείας. Η εικόνα 6.3.6.2 δείχνει μια λίστα με τις τυποποιημένες αναφορές. Επιπλέον, το IPS προσφέρει μεγάλη λειτουργικότητα στο χειρισμό ελέγχου πρόσβασης των χρηστών . Για παράδειγμα , εάν ένας διαχειριστής θέλει να εμποδίσει την ανταλλαγή άμεσων μηνυμάτων (IM) για ένα ορισμένο σύνολο των εργαζομένων , αλλά και να επιτρέψει σε συγκεκριμένους πελάτες θα πρέπει να δημιουργηθούν κανόνες που να κάνουν δεκτές τις αιτήσεις από το Google Chat για τους χρήστες του X , Y , Z και όχι για άλλους χρήστες [19, 38].

Report	Description
Top 100 Attacks (last 24 hours)	Those attacks that are detected most frequently within the last 24 hours
Top 100 Attacks Prevented (last 24 hours)	Those attacks that are prevented most frequently within the last 24 hours
Top 20 Attackers (All Attacks - Last 24 hours)	IP addresses that have most frequently been the source of an attack during the last 24 hours

Top 20 Attackers Prevented(All Attacks - Last 24 hours)	IP addresses that have most frequently been prevented from attacking the network during the last 24 hours
Top 20 Targets (last 24 hours)	IP addresses that have most frequently been target of an attack during the last 24 hours
Top 20 Targets Prevented (last 24 hours)	IP addresses that have most frequently prevented attacks during the last 24 hours
All Attacks by Severity (last 24 hours)	Number of attacks by severity level (set in attack objects)
All Attacks Prevented by Severity (last 24 hours)	Number of attacks prevented by severity level (set in attack objects)
All Attacks Over Time (last 7 days)	All attacks detected during the last 7 days
All Attacks Prevented Over Time (last 7 days)	All attacks prevented during the last 7 days

Εικόνα 6.3.6.2 : Λίστα τυποποιημένων αναφορών

Τα σημαντικότερα χαρακτηριστικά του συγκεκριμένου IPS είναι:

- Η δυνατότητα υψηλού ελέγχου από το διαχειριστή του συστήματος
- Η ικανότητα για επικύρωση πρωτοκόλλων επικοινωνίας
- Η επιλεκτική παρακολούθηση της κίνησης του δικτύου

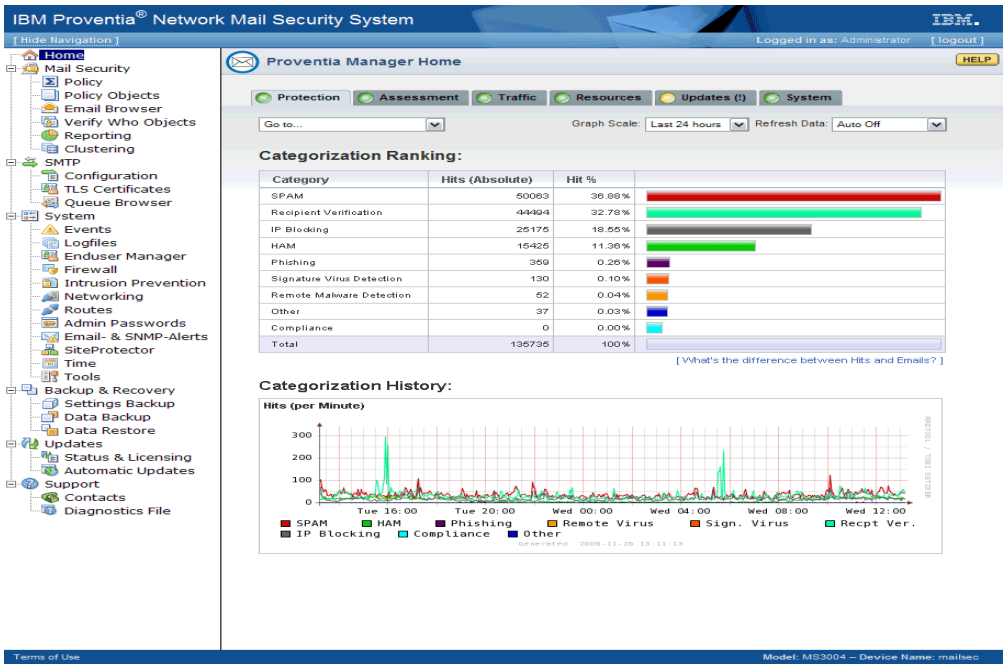
6.3.7 Proventia

Εικόνα 6.3.7: Proventia

6.3.7.1 Λίγα λόγια για το Proventia

Το κλειδί στην απόδοση του Proventia IPS της IBM είναι το IBM Protocol Analysis Module που υποστηρίζει ανάλυση πακέτων δικτύου σε βάθος [1]. Προστατεύει από απειλές όπως επιθέσεις Ιστού, επιθέσεις εντός του συστήματος (insider threats) και από κακόβουλο λογισμικό (malware). Σημαντικό είναι ότι παρέχει προστασία και στα τρία στρώματα του δικτύου που είναι ο πυρήνας, περιμετρικά αλλά και στα απομακρυσμένα τμήματα. Κύριο πλεονέκτημα είναι η συνεχόμενη, 24/7 ανανέωσή του για νέες απειλές από την ομάδα ανάπτυξης X-Force. Η ομάδα X-Force είναι ένας παγκοσμίου φήμης οργανισμός που πραγματοποιεί έρευνα γύρω από την ασφάλεια και εξειδικεύεται στην εξέταση των απειλών αλλά και στον εντοπισμό των τρωτών σημείων ενός λογισμικού.

Αποτέλεσμα αυτού είναι ότι το Proventia μπορεί να σταματήσει ολόκληρες κατηγορίες επιθέσεων, συμπεριλαμβανομένων των νέων και άγνωστων απειλών και μάλιστα χωρίς αναβαθμίσεις. Σε αντίθεση με άλλα IPS που απλά ελπίζουν να ταιριάζουν οι υπογραφές προστασίας τους γεγονός που αποτελεί μία διαδικασία που είναι πολύ αργή να σταματήσει εξελισσόμενες απειλές. Παρακάτω φαίνεται μία εικόνα καταγραφής αποτελεσμάτων και αναφορών από το Proventia IPS της IBM.



Εικόνα 6.3.7.1 : Καταγραφή αποτελεσμάτων και αναφορών από το Proventia IPS

6.3.7.2 Δυνατότητες του Proventia σε γνωστές απειλές

Το Proventia IPS παρουσιάζει την δυνατότητα πρόληψης των ακόλουθων κατηγοριών απειλών ενός δικτύου που καλό είναι να προσεγγίζονται αναλυτικά προκειμένου να αντιμετωπίζονται πρόωρα και αποτελεσματικότερα. Οι σημαντικότερες απειλές που επιτυγχάνεται η πρόληψη τους από το Proventia IPS είναι [37]:

- Backdoors

Είναι μια μέθοδος που παρακάμπτει την κανονική ταυτότητα και εξασφαλίζει την παράνομη απομακρυσμένη πρόσβαση σε έναν υπολογιστή.

- Botnets

Είναι μια συλλογή από προγράμματα σύνδεσης στο Internet επικοινωνία με άλλα παρόμοια προγράμματα, προκειμένου να εκτελέσουν επιθέσεις. Η λέξη botnet είναι ένας συνδυασμός των λέξεων ρομπότ και του δικτύου.

- Cross-site scripting (XSS)

Αναφέρεται στην εκμετάλλευση διάφορων ευπαθειών (vulnerabilities) υπολογιστικών συστημάτων με εισαγωγή κώδικα HTML ή Javascript σε κάποιο ιστοχώρο.

- Distributed Denial of service (DDoS)

Ονομάζονται γενικά οι επιθέσεις εναντίον ενός υπολογιστή, ή μιας υπηρεσίας που παρέχεται, οι οποίες έχουν ως σκοπό να καταστήσουν τον υπολογιστή ή την υπηρεσία ανίκανη να δεχτεί άλλες συνδέσεις και έτσι να μην μπορεί να εξυπηρετήσει άλλους πιθανούς πελάτες.

- Insider threats

Είναι μια κακόβουλη απειλή για μια οργάνωση που προέρχεται από ανθρώπους μέσα στον οργανισμό, όπως είναι οι εργαζόμενοι, πρώην εργαζόμενοι, οι εργολάβοι ή συνεργάτες, οι οποίοι έχουν εμπιστευτικές πληροφορίες σχετικά με τις πρακτικές ασφαλείας του οργανισμού, δεδομένων και συστήματα ηλεκτρονικών υπολογιστών.

- Instant messaging- Trojans

Μπορεί να χρησιμοποιηθεί για να εισαγάγει Trojans, ιούς και άλλα κακόβουλα λογισμικά στο δίκτυο.

- Peer-to-peer (P2P) networks - Viruses

Διευκολύνει τη μεταφορά των αρχείων που έχουν μολυνθεί με Trojans και ιούς.

- Rootkits

Είναι λογισμικό που επιτρέπει την συνεχή πρόσβαση σε έναν υπολογιστή με προνόμια υπερχρήστη, ενώ κρύβει ενεργά την παρουσία του από τους διαχειριστές με το να ενσωματώνεται σε βασικά αρχεία του λειτουργικού συστήματος ή άλλων εφαρμογών.

- Spam

Ονομάζεται η μαζική αποστολή ηλεκτρονικών μηνυμάτων ή άλλων, σε μια προσπάθεια προώθησης προϊόντων ή ιδεών

- Spyware

Αναφέρεται σε ένα είδος κακόβουλου λογισμικού το οποίο φορτώνεται κρυφά (με ύπουλο τρόπο) σε έναν υπολογιστή χωρίς να το ξέρει ο χρήστης και εκτελείται στο παρασκήνιο κάνοντας διάφορα πράγματα πίσω από την πλάτη του χρήστη.

- Worms

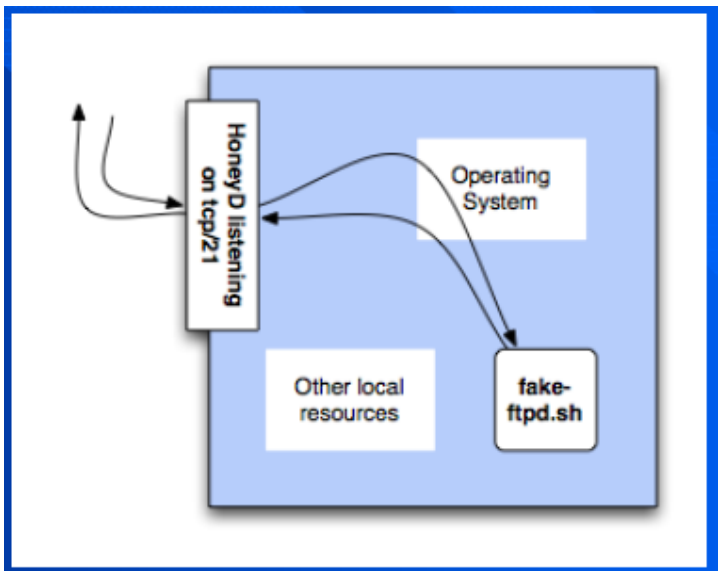
Είναι ένα αυτοαναπαραγόμενο και κακόβουλο πρόγραμμα υπολογιστή, το οποίο χρησιμοποιεί δίκτυο υπολογιστών για να στείλει αντίγραφα του εαυτού του σε άλλους κόμβους (υπολογιστές του δικτύου) και μπορεί να το πράξει χωρίς την παρέμβαση του χρήστη.

6.4 Εναλλακτικά Συστήματα Ανίχνευσης Επιθέσεων.

Μετά από την μελέτη αλλά κυρίως τη κατανόηση των IDPS συστημάτων καλό θα ήταν να αναφερθούμε σε εναλλακτικά συστήματα ανίχνευσης επιθέσεων τα οποία είναι:

6.4.1 Honeypots.

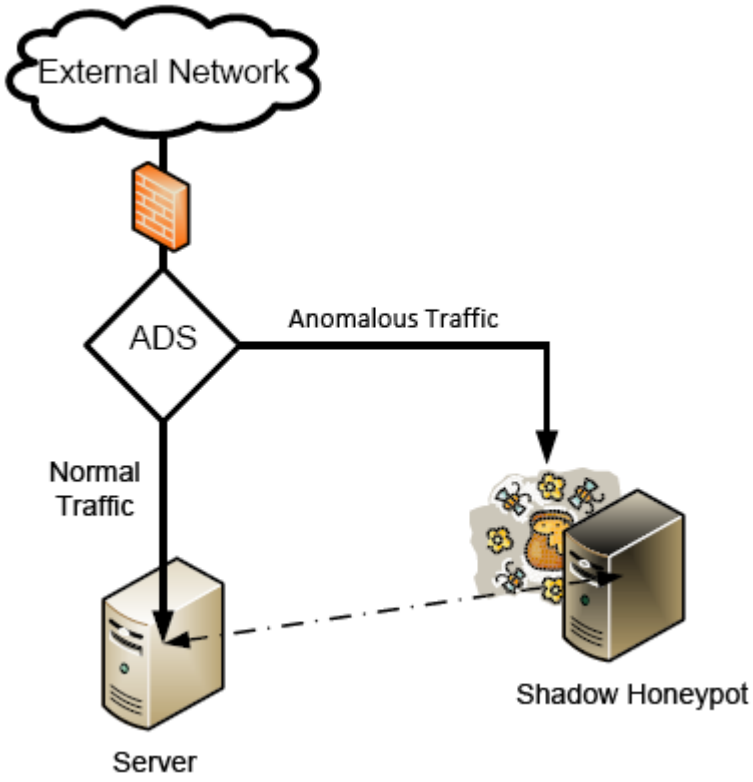
Ουσιαστικά αποτελούν μια παγίδα που χρησιμοποιείται για τον εντοπισμό, την αποτροπή και, σε κάποιο βαθμό, την εξουδετέρωση μιας επίθεσης. Συγκεκριμένα μοιάζει να αποτελεί μέρος του δικτύου, αλλά είναι απομονωμένο και παρακολουθείται συλλέγοντας χρήσιμες πληροφορίες. Σκοπός του είναι να αποτελεί εύκολο στόχο, και αυτό το επιτυγχάνει αφού διαφημίζει ενδιαφέρουσες και ελκυστικές υπηρεσίες.



Εικόνα 6.4.1.1: Σκοπός των Honeypots

Σε γενικές γραμμές, υπάρχουν δύο δημοφιλείς λόγοι ή στόχοι πίσω από τη δημιουργία ενός Honeypot [2]:

- Γνώση πως οι επιτιθέμενοι προσπαθούν να αποκτήσουν πρόσβαση στα συστήματα. Η γενική ιδέα είναι ότι από μια καταγραφή των δραστηριοτήτων του επιτιθέμενου, μπορούμε να αποκτήσουμε εικόνα για τις μεθοδολογίες επίθεσης του αλλά και για την καλύτερη προστασία του συστήματος μας.
- Συγκέντρωση εγκληματολογικών πληροφοριών που απαιτούνται για να βοηθήσουν στην σύλληψη ή δίωξη του επιτιθέμενου. Αυτό είναι το είδος των πληροφοριών που απαιτούνται συχνά για να παρέχουν στους υπαλλήλους επιβολής του νόμου, με τα στοιχεία που απαιτούνται για την άσκηση δίωξης.



Εικόνα 6.4.1.2: Τα Honeypots στο δίκτυο

- **Πλεονεκτήματα**

1. Εντοπίζει μόνο ότι είναι ύποπτο και κακόβουλο
2. Απαιτεί λιγότερα δεδομένα για ανάλυση, από ότι τα IDS ο eypo
3. Προσφέρει πληροφορίες για τον εισβολέα
4. Εντοπίζει νέους τύπους κακόβουλου λογισμικού

- **Μειονεκτήματα**

1. Οι εισβολείς πρέπει να αλληλεπιδράσουν με το honeypot
2. Δυνητικός κίνδυνος για το δίκτυο

3. Χρειάζεται διαρκή επέκταση

6.4.2 Darknet

Το Darknet ή Network Telescope ή Black Hole συλλέγει και παρατηρεί γεγονότα τα οποία συμβαίνουν στο Διαδίκτυο. Ουσιαστικά η βασική ιδέα είναι να παρατηρεί την κυκλοφορία της πληροφορίας σε σκοτεινές-αχρησιμοποίητες διευθύνσεις του Δικτύου. Δεδομένου ότι η κίνηση σε αυτές τις διευθύνσεις είναι de-facto ύποπτη, μπορεί να αντλήσει πληροφορίες για πιθανή επίθεση κατανεμημένης άρνησης παροχής υπηρεσίας (DDoS) ή για τυχαία σάρωση αναπαραγωγών (worms) [4].

Εικόνα 6.4.2: Βασική ιδέα Darknet

Κεφάλαιο 7

Γενικότερα Συμπεράσματα

7.1 Συμπέρασμα

Η ασφάλεια έχει γίνει κρίσιμο συστατικό της σχεδίασης συστημάτων και δικτύων σήμερα. Στη πραγματικότητα είναι ένας αγώνας χωρίς τέλους 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. Για την καλύτερη διασφάλιση των πληροφοριών αυτών θα πρέπει να υπάρξει καλύτερη κατανόηση και ανάλυση των απειλών. Με αποτέλεσμα να δημιουργηθούν και εξελιχθούν τεχνικές που να επιφέρουν καλύτερα αποτελέσματα όπως διαπιστώθηκε πιο πάνω για τα IDPS συστήματα που αποτελούν ουσιαστικά μηχανές εποπτείας και ελέγχου, αλλά και εντοπισμού των απειλών αυτών.

Είναι γενικότερα αποδεκτό ότι η σημερινή γενιά των IDPS συστημάτων παρουσιάζει μεγάλες δυνατότητες στην ανάλυση , την ανίχνευση και την πρόληψη των επιθέσεων . Στην προσπάθεια μας να κατανοήσουμε την λειτουργία των συστημάτων αυτών, διαπιστώσαμε τον τρόπο με τον οποίο ένα IDPS σύστημα αναλύει, επεξεργάζεται, εκθέτει και απεικονίζει το σύνολο των πληροφοριών προς τους διαχειριστές των δικτύων προκειμένου να επιτυγχάνεται η καλύτερη και αποδοτικότερη ασφάλεια του δικτύου.

Επιπλέον μελετήθηκαν τα ευρύτερα αξιοποιούμενα IDPS συστήματα και παρουσιάστηκαν τα χαρακτηριστικά τους, οι αρχιτεκτονικές τους καθώς και συγκρίσεις μεταξύ τους. Αποτέλεσμα είναι το γεγονός ότι υπάρχουν διάφορα συστήματα IDPS αναλόγως της αποστολής τους και εναπόκειται στους αντίστοιχους διαχειριστές στο να καταλάβουν τις απειλές αλλά και των σημάτων που μπορούν να χαρακτηριστούν ως κακόβουλα.

Τέλος θα μπορούσαμε να αναφέρουμε ότι υπάρχουν πάρα πολλά διαθέσιμα IDPS συστήματα ανοικτού κώδικα, αλλά αν έπρεπε να επιλέξουμε κάποιο τότε το Snort είναι το καλύτερο εναλλακτικό σύστημα για την εξασφάλιση της ασφάλειας ενός δικτύου. Το γεγονός ότι είναι ελαφρύ εργαλείο για TCP/IP δίκτυα, το βοηθά στο να μην χρειάζεται εγκατάσταση επιπρόσθετων εμπορικών αισθητήρων (μείωση κόστους). Το Snort είναι μια μηχανή ανίχνευσης και πρόληψης ανοιχτού κώδικα και για αυτό το λόγο βρίσκει μεγάλη αποδοχή από την φοιτητική και την επιστημονική κοινότητα. Είναι ιδιαίτερα προσαρμόσιμο και οι κανόνες που χρησιμοποιεί μπορούν να προσαρμοστούν στο είδος δικτύου που προστατεύει σε κάθε περίπτωση. Σημαντικό πλεονέκτημα του Snort είναι η συνεισφορά που δέχεται από τις κοινότητες ανοικτού κώδικα, οι οποίες το προμηθεύουν συνεχώς με ενημερώσεις. Το Snort είναι από τα πλέον επεκτάσιμα IDPS με βιβλιοθήκη 14.000 κανόνων και αυτό το καθιστά μοναδικό.

7.2 Μελλοντική Έρευνα

Στη εργασία αυτή ερευνήσαμε το πρόβλημα της διασφάλισης κρίσιμών υπολογιστικών και δικτυακών υποδομών επικεντρώνοντας την έρευνά μας στην ανίχνευση και πρόληψη επιθέσεων προτείνοντας αποτελεσματικές προσεγγίσεις καθώς τα ευρύτερα αξιοποιούμενα IDPS συστήματα. Υπάρχουν όμως δυνατότητες βελτίωσης αλλά και νέοι δρόμοι εξερεύνησης χρησιμοποιώντας νέες μεθοδολογίες όπως:

- Η ποικιλία και πολυπλοκότητα των δικτυακών επιθέσεων περιλαμβανομένων των επιθέσεων άρνησης εξυπηρέτησης (Denial of Service (DoS)) είναι πολύ πιθανό να αυξηθεί. Ανεξάρτητα από τα μέτρα προστασίας που μπορούν να χρησιμοποιηθούν τώρα, χρειάζεται να αντιμετωπίσουμε τις δικτυακές επιθέσεις σαν ένα πρόβλημα που απαιτεί μακροχρόνια προσπάθεια προκειμένου να ορίσουμε και να υλοποιήσουμε αποτελεσματικές λύσεις.

- Είναι σημαντικό να μελετηθούν τα εργαλεία επίθεσης καθώς και οι στρατηγικές των επιτιθέμενων προκειμένου να γίνουν πιο κατανοητή και προσιτοί οι τρόποι αντιμετώπισης τους.

- Θα πρέπει να επιδιωχθεί η βελτίωση της απόδοσης των συστημάτων ανίχνευσης και πρόληψης επιθέσεων καθώς και ο περιορισμός των λανθασμένων συναγερμών.

- Επιπλέον σημαντική είναι η πιθανή επέκταση των συστημάτων ανίχνευσης επιθέσεων με ευαισθησία στο κόστος.

- Εξίσου σημαντικό είναι να επιτευχθεί η συσχέτιση πολλών IDPS σε μία υποδομή επιτυγχάνοντας την εκμετάλλευση του πλήθους των δυνατοτήτων των συστημάτων αυτών.

- Τέλος υπάρχει ακόμα περιθώριο αύξησης της φιλικότητας κατά την αξιολόγηση γεγονότων

Βιβλιογραφία

[01] Αδάμου Αλέξανδρου, Σχεδίαση και ανάπτυξη μηχανισμού για τη δυναμική ανίχνευση αργών επιθέσεων σε Συστήματα Ανίχνευσης Εισβολής (IDS), Θεσσαλονίκη 2013. http://vivliothmmy.ee.auth.gr/2024/1/Adamos_Thesis.pdf

[02] Αικατερίνη Β. Μητροκώτσα, << Ανίχνευση Εισβολών σε Δίκτυα Υπολογιστών με Αλγόριθμούς Μηχανικής Μάθησης>>, Πειραιάς 2007.

[03] Ανδρεάδης Σωτήριος, Μελέτη των Συνεργατικών Αρχιτεκτονικής Συστημάτων Ανίχνευσης εισβολών, Πειραιάς 2010. http://digilib.lib.unipi.gr/dspace/bitstream/unipi/4048/1/Andreadis.pdf

[04] Γκρίτζαλης Σ., Γκρίτζαλης Δ., Κάτσικας Σ., « Ασφάλεια Δικτύων Υπολογιστών.» Εκδόσεις Παπασωτηρίου, 2004.

[05] Κακόβουλοι Χρήστες, Hacker και Cracker. http://el.wikipedia.org/wiki/%CE%A7%CE%AC%CE%BA%CE%B5%CF%81

[06] Κάτσικας Σ., Προστασία και Ασφάλεια Συστημάτων Υπολογιστών: Ασφάλεια Δικτύων, Ελληνικό Ανοικτό Πανεπιστήμιο, Πάτρα, 2001. http://psifiakoskosmos.files.wordpress.com/2009/12/katsikas-22.pdf

[07] Κομνηνός Θ., «Μοντέλα ασυνήθους δικτυακής κυκλοφορίας σε TCP/IP δικτυακά υπολογιστικά περιβάλλοντα.» Πάτρα, Νοέμβριος 2008.

[08] Οικονόμου Ευθύμιος, «Μελέτη και ανάλυση των Συστημάτων Ανίχνευσης εισβολών.», Πειραιάς 2008.

[09] Π. Κυριακή. «Εργαλείο Ανίχνευσης Εισβολών» Θεσσαλονίκη, 2012.

[10] Σκουλήκι Υπολογιστή (worm).

http://el.wikipedia.org/wiki/%CE%A3%CE%BA%CE%BF%CF%85%CE%BB%CE%AE%CE%BA%CE%B9_%CF%85%CF%80%CE%BF%CE%BB%CE%BF%CE%B3%CE%B9%CF%83%CF%84%CE%AE

[11] Τι σημαίνει hacker.

http://iguru.gr/2012/08/09/what-it-means-hacker/

[12] Χρήστος Π., «Ασφάλεια δικτύων – Συστήματα ανίχνευσης εισβολών (Intrusion detection systems – IDS). Μελέτη των προβλημάτων ασφαλείας που παρουσιάζονται σε δίκτυα και υπολογιστικά συστήματα συνδεδεμένα με το Διαδίκτυο. Παρουσίαση των λύσεων που προσφέρει ένα IDS. Υλοποίηση και δοκιμή IDS.» Πάτρα, 2002.

[13] Abraham A., Thomas J., 2005, Distributed Intrusion Detection Systems: A Computational Intelligence Approach.

http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.59.7322&rep=rep1&type=pdf

[14] Anthony Kelley. NETWORK FLIGHT RECORDER – A NEW TOOL FOR THE WAR» 2000.

[15] Axelsson Stefan, 2000, Intrusion Detection Systems: A Survey and Taxonomy.

[16] Axelsson Stefan, 2000, Intrusion Detection Systems: A Survey and Taxonomy. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.1.6603&rep=rep1&type=pdf

[17] Bace R., Intrusion Detection, Macmillan Technical Publishing, Indianapolis, 2000.

[18] Bierman E., Cloete E., Venter L. M., Comparison of Intrusion detection Systems, Computer & Security, No 20, 2001.

[19] Bro. https://www.bro.org/

[20] Denning D., 1987, An Intrusion-Detection Model.

[21] Denning D., 1996, Protection and Defence of Intrusion. http://faculty.nps.edu/dedennin/publications/Protection%20and%20Defense%20of%20Intrusion.htm

[22] Feng, H., J. Giffin, Y. Huang, S. Jha, W. Lee, και B. Miller. «Formalizing sensitivity in static analysis for intrusion detection». Proceedings of the IEEE Symposium on Security and Privacy. IEEE, 2004.

[23] Ganesh Kumar Varadarajan, «Web Application Attack Analysis Using Bro IDS», 2012.

http://www.sans.org/reading-room/whitepapers/detection/web-application-attack-analysis-bro-ids-34042

[24] Ghosh A., Schwartzbard A., 1999, A study in using neural networks for anomaly and misuse detection, In Proceedings of the Eighth USENIX Security Symposium. https://www.usenix.org/legacy/publications/library/proceedings/sec99/full_papers/ghosh/ghosh.pdf

[25] Han, Sang-Jun, Sung-Bae Cho. «Evolutionary neural networks for anomaly detection XE "anomaly detection" based on the behavior of a program». Transactions on Systems, Man, and Cybernetics, 2005.

[26] Honeypot, http://www.sans.org/security-resources/idfaq/honeypot3.php

[27] IBM Global Technology Services. «The Proventia Network Intrusion Prevention System Protection Engine».

[28] Juniper Network Security Products.

http://www.juniper.net/us/en/products-services/security/

[29] Kibirkstis A., 2009, Intrusion Detection FAQ: What Are The Top Selling IDS/IPS and What Differentiates Them from Each Other?

http://www.sans.org/security-resources/idfaq/top-selling-ids-ips.php

[30] Koutsoutos S., Christou I., Efremidis S., 2006, An Intrusion Detection System for Network-Initiated Attacks Using a Hybrid Neural Network.

[31] Kumar A., Chandak S., Dewanjee R. «Recent Advances in Intrusion Detection Systems: An Analytical Evaluation and Comparative Study» 2014.

[32] Leon Elizabeth, Olfa Nasraoui, Jonatan Gomez. «Network Intrusion Detection Using Genetic Clustering». Στο Genetic and Evolutionary Computation – GECCO 2004, 1312-1313. Berlin / Heidelberg: Springer, 2004.

[33] Martin Roesch, 2001, Snort README. http://www.snort.org

[34] Network Flight Recorder (NFR), http://www.nfr.net

[35] Network Security, 2011, Volume 2011 Issue 12, DDoS: Threats and Mitigation http://www.sciencedirect.com/science/article/pii/S1353485811701283

[36] Papadaki M., Advanced Intrusion Detection Systems, Network Research Group, University of Plymouth, UK, 2008.

[37] Proventia,

http://www-935.ibm.com/services/us/en/it-services/proventia-web-application-security.html

[38] Radware. http://www.radware.com/

[39] Raghuram Ponnaganti. « Comparative study of three IDS systems (NFR, EMELAND, SNORT) » 2014.

[40] R-U-Dead-Yet, 2011, HTTP POST Denial of Service tool.

https://code.google.com/p/r-u-dead-yet/

[41] Scarfone K., Mell P., 2007, Guide to Intrusion Detection and Prevention Systems (IDPS), National Institute of Standards and Technology.

[42] Shameli A., Dagenais M., Jabbarifar Real M., 2012, Time Intrusion Prediction based on Optimized Alerts with Hidden Markov Model. http://ojs.academypublisher.com/index.php/jnw/article/view/jnw0702311321/4365

[43] Sig Myers, John Musacchio, Ning Bao, «UCSC-SOE-10-12: Intrusion Detection Systems: A Feature and Capability Analysis», 2010.

http://www.soe.ucsc.edu/research/technical-reports/UCSC-SOE-10-12

http://www.radware.com/Solutions/Security/

[44] Suricata. http://suricata-ids.org/

[45] Tung B., 1999, The Common Intrusion Detection Framework. http://gost.isi.edu/cidf/

[46] Ulrich, Flegel. «Models of Misuse Scenarios». *Privacy-Respecting Intrusion Detection*, 203-228. Springer, 2007.

[47] Wolthusen D., Intrusion Detection and Prevention Systems, Information Security Group, Department of Mathematics, Royal Holloway, University of London, UK, 2010.

[48] Young, Greg, Prescatore John. «Magic Quadrant for Network Intrusion Prevention System Appliances, 1H08». IBM COM. 2008.

http://www-935.ibm.com/services/us/iss/pdf/esr_magic-quadrant-for-network-intrusion-prevention-system-appliances-1h08.pdf