ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΛΟΠΟΝΝΗΣΟΥ
ΣΧΟΛΗ ΜΗΧΑΝΙΚΩΝ
ΤΜΗΜΑ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ
ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ
(Τμήμα Μηχανικών Πληροφορικής Τ.Ε., ΤΕΙ Δυτικής Ελλάδας)

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Συστήματα πρόληψης και ανίχνευσης εισβολών «Intrusion Prevention & Detection Systems»

Κόρακας Ιωάννης ΑΜ:2144

Επιβλέπων Καθηγητής: Δρ. Βασίλειος Τριανταφύλλου

Πάτρα, Νοέμβριος 2022

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή

Πάτρα, 28/11/2022

ΕΠΙΤΡΟΠΗ ΑΞΙΟΛΟΓΗΣΗΣ

1. Γεώργιος Ασημακόπουλος

2. Σωτήρης Χριστοδούλου

3. Βασίλειος Τριανταφύλλου

Υπεύθυνη Δήλωση Φοιτητή

Βεβαιώνω ότι είμαι συγγραφέας αυτής της εργασίας και ότι κάθε βοήθεια την οποία είχα για την προετοιμασίατης είναι πλήρως αναγνωρισμένη και αναφέρεται στην εργασία. Επίσης έχω αναφέρει τις όποιες πηγές από τις οποίες έκανα χρήση δεδομένων, ιδεών ή λέξεων, είτε αυτές αναφέρονται ακριβώς είτε παραφρασμένες. Επίσης βεβαιώνω ότι αυτή η εργασία προετοιμάστηκε από εμένα προσωπικά ειδικά για τη συγκεκριμένη εργασία. Η έγκριση της διπλωματικής εργασίας από το Τμήμα Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών του Πανεπιστημίου Πελοποννήσου δεν υποδηλώνει απαραιτήτως και αποδοχή των απόψεων του συγγραφέα εκ μέρους του Τμήματος. Η παρούσα εργασία αποτελεί πνευματική ιδιοκτησία του φοιτητή Κόρακα Ιωάννη που την εκπόνησε. Στο πλαίσιο της πολιτικής ανοικτής πρόσβασης ο συγγραφέας/δημιουργός εκχωρεί στο Πανεπιστήμιο Πελοποννήσου, μη αποκλειστική άδεια χρήσης του δικαιώματος αναπαραγωγής, προσαρμογής, δημόσιου δανεισμού, παρουσίασης στο κοινό και ψηφιακής διάχυσής τους διεθνώς, σε ηλεκτρονική μορφή και σε οποιοδήποτε μέσο, για διδακτικούς και ερευνητικούς σκοπούς, άνευ ανταλλάγματος και για όλο το χρόνο διάρκειας των δικαιωμάτων πνευματικής ιδιοκτησίας. Η ανοικτή πρόσβαση στο πλήρες κείμενο για μελέτη και ανάγνωση δεν σημαίνει καθ’ οιονδήποτε τρόπο παραχώρηση δικαιωμάτων διανοητικής ιδιοκτησίας του συγγραφέα/δημιουργού ούτε επιτρέπει την αναπαραγωγή, αναδημοσίευση, αντιγραφή, αποθήκευση, πώληση, εμπορική χρήση, μετάδοση, διανομή, έκδοση, εκτέλεση, «μεταφόρτωση» (downloading), «ανάρτηση»(uploading), μετάφραση, τροποποίηση με οποιονδήποτε τρόπο, τμηματικά ή περιληπτικά της εργασίας, χωρίς τη ρητή προηγούμενη έγγραφη συναίνεση του συγγραφέα/δημιουργού. Ο συγγραφέας/δημιουργός διατηρεί το σύνολο των ηθικών και περιουσιακών του δικαιωμάτων.

Πίνακας περιεχομένων

Περίληψη 6

Εισαγωγή 8

Κεφάλαιο 1ο 10

1.1.Εισαγωγή 10

1.2. Το Μοντέλο OSI 11

1.3. IPsec ασφάλεια στο internet 11

1.4. Εφαρμογές του IPsec 12

1.5. Ιστορική Αναδρομή των Firewall 13

1.6. Ανάπτυξη τεχνολογιών τείχους προστασίας «filter firewalls» 14

Κεφάλαιο 2ο: «Ασφάλεια Δικτύων» 20

2.1. Πολιτικές Ασφάλειας Δικτύων 20

2.2. Τύποι προστασίας ασφάλειας δικτύου 21

2.3. Τύποι επιθέσεων 24

2.4. Μέθοδοι επιθέσεων 25

2.5. Κακόβουλοι χρηστες «hackers» 30

2.5.1. Γιατί οι άνθρωποι χακάρουν 32

2.5.2. Τύποι των hacks 33

2.5.3. Πως οι οργανισμοί μετριάζουν τις εισβολές 35

2.5.4 Τι συμβαίνει όταν οι οργανισμοί δεν προστατεύουν σωστά τα δεδομένα τους; 35

2.6. Σάρωση θυρών «Port scanning» 36

2.7. Ασφάλιση δικτύου με το σημείο ελέγχου 37

Κεφάλαιο 3ο: «Συστήματα Ανίχνευσης Εισβολών» 38

3.1. Εισαγωγή στα Συστήματα Ανίχνευσης Εισβολών (IDS) 38

3.2. Αναγνωριστικά που βασίζονται στον κεντρικό υπολογιστή «host-based identifiers» 39

3.3. Αναγνωριστικά που βασίζονται στο δίκτυο «network-based identifiers» 43

3.3.1. Τεχνικές εντοπισμού ύποπτης συμπεριφοράς 45

3.3.2 Αντιδραση του NID σε ύποπτη συμπεριφορά 45

3.4. Σύγκριση των Συστημάτων Ανίχνευσης Εισβολών 46

Κεφάλαιο 4ο: «Συστήματα Αποφυγής Εισβολών» 50

4.1. Εισαγωγή 50

4.2. Ανάπτυξη 50

4.3. Πώς λειτουργεί το IPS 52

4.4. Ζητήματα γύρω από το σύστημα IPS 56

4.5. Περαιτέρω εξελίξεις 57

Κεφάλαιο 5ο: «Προφύλαξη από εισβολές δικτύου» 59

5.1. Προληπτικά μέτρα 59

5.2. Παρακολούθηση και ανίχνευση εισβολών 63

5.2.1.Παρακολούθηση με βάση τον κεντρικό υπολογιστή «host-based Monitoring» 64

5.2.2. Παρακολούθηση της κυκλοφορίας «Traffic Monitoring» 65

5.2.3. Ανίχνευση βάση υπογραφής «Signature-Based Detection» 66

5.2.4. Ανωμαλίες συμπεριφοράς «Behavior Anomalies» 66

5.2.5. Συστήματα πρόληψης εισβολών «Intrusion Prevention Systems» 67

5.3. Αντιδραστικά μέτρα «Reactive Measures» 67

5.3.1. Καραντίνα «Quarantine» 68
5.3.2. Ανίχνευση ίχνους «Traceback» 68
Κεφάλαιο 6ο: «Δημιουργία νέας στρατηγικής επίθεσης» 70
6.1. Εισαγωγή 70
6.2. Υπολογισμός μήκους συμβολοσειράς 71
Μήκος του buffer 72
6.3. Εισαγωγή της εντολής που πρόκειται να εκτελεστεί 73
Κάνοντας μια εκμετάλλευση Beta 73
Χρήση του κατασκευασμένου κώδικα εκμετάλλευσης 73
6.4. Συμπέρασμα 74
Επίλογος 75
Βιβλιογραφία 76

Πίνακας Συντομογραφιών

AD - Anomaly Detection

ASR - Attack Signature Recognition

RTID - Real-time intrusion detection

CIAC - Computer Incident Advisory Capability

CMDS - Computer Misuse Detection System

COM - Common Operation Models

CSTC - Cyber Solution Tools Centre

DDoS - Distributed Denial of Service

DEC - Digital Equipment Corporation

DIDS - Distributed Intrusion Detection System

DNS - Domain Name Service

DoS - Denial of Service

FDDI - Fiber Distributed Data Interface

FTP - File Transfer Protocol

HTTP - Hypertext Transfer Protocol

ICMP - Internet Control Message Protocol

IDES - Intrusion Detection Expert System

IDS- Intrusion Detection Systems

IEEE - Institute of Electrical and Electronics Engineers

IP - Internet Protocol

IPS - Intrusion Prevention Systems

LDAP - Lightweight Directory Address Protocol

MDC - Microsoft Download Centre

MRSE - Multi-Rule Search Engine

MSRC - Microsoft Security Response Centre

IETF - Internet Engineering Task Force

DMZ - De-Militarized Zone

Πινακας Ορολογίας

Cyberspace (Κυβερνοχώρος): Με τον όρο κυβερνοχώρος υποδηλώνεται το περιβάλλον που έχει δημιουργηθεί από δίκτυα επικοινωνιών που χρησιμοποιούν ηλεκτρονικούς υπολογιστές.

Exploit: Είναι ένας τύπος κακόβουλου λογισμικού που εκμεταλλεύεται σφάλματα ή ευπάθειες, τα οποία χρησιμοποιούν οι εγκληματίες του κυβερνοχώρου για να αποκτήσουν παράνομη πρόσβαση σε ένα σύστημα.

Patch: διορθοτικος κωδικας

Signature files: Τα αρχεία υπογραφών αποτελούν σημαντικό μέρος του τρόπου λειτουργίας των λογισμικών antivirus και antimalware. Αυτά τα αρχεία περιέχουν πληροφορίες σχετικά με διάφορους ιούς και κακόβουλο λογισμικό, οι οποίες χρησιμοποιούνται από το λογισμικό για την ανίχνευση, τον καθαρισμό και την αφαίρεση των απειλών που εντοπίστηκαν.

Signature: Στην ορολογία της ασφάλειας υπολογιστών, η υπογραφή(signature) είναι ένα τυπικό αποτύπωμα ή μοτίβο που σχετίζεται με μια κακόβουλη επίθεση σε ένα δίκτυο ή σύστημα υπολογιστών. Αυτό το μοτίβο μπορεί να είναι μια σειρά από bytes στο αρχείο (ακολουθία byte) στην κυκλοφορία δικτύου. Μπορεί επίσης να λάβει τη μορφή μη εξουσιοδοτημένης εκτέλεσης λογισμικού, μη εξουσιοδοτημένης πρόσβασης στο δίκτυο, μη εξουσιοδοτημένης πρόσβασης στον κατάλογο ή ανωμαλιών στη χρήση των προνομίων του δικτύου.

Backdoor: Το backdoor είναι ένας τύπος κακόβουλου λογισμικού που αναιρεί τις συνηθείς διαδικασίες ελέγχου ταυτότητας για την πρόσβαση σε ένα σύστημα. Ως αποτέλεσμα, παρέχεται απομακρυσμένη πρόσβαση σε πόρους μιας εφαρμογής, όπως βάσεις δεδομένων και διακομιστές αρχείων, δίνοντας στους δράστες τη δυνατότητα να εκδίδουν εξ αποστάσεως εντολές συστήματος και να ενημερώνουν κακόβουλο λογισμικό.

DMZ: Στα δίκτυα υπολογιστών, η DMZ ή αποστρατιωτικοποιημένη ζώνη είναι ένα φυσικό ή λογικό υποδίκτυο που διαχωρίζει ένα τοπικό δίκτυο (LAN) από άλλα μη αξιόπιστα δίκτυα συνήθως το δημόσιο διαδίκτυο. Τα DMZ είναι επίσης γνωστά ως περιμετρικά δίκτυα ή προστατευμένα υποδίκτυα.

Host: είναι ένας κεντρικός υπολογιστής δικτύου ή άλλη συσκευή συνδεδεμένη σε δίκτυο υπολογιστών. Ένας κεντρικός υπολογιστής μπορεί να λειτουργεί ως διακομιστής που προσφέρει πόρους πληροφοριών, υπηρεσίες και εφαρμογές σε χρήστες ή άλλους κεντρικούς υπολογιστές στο δίκτυο.

Proxies: Είναι οι διακομιστές μεσολάβησης που έχουν στόχο να βελτιώσουν την ταχύτητα πλοήγησης στο Διαδίκτυο και παράλληλα να μειώσουν την κίνηση του δικτύου προς το Διαδίκτυο. Τοποθετούνται ενδιάμεσα των χρηστών και του Διαδικτύου.

Snort: Το Snort είναι το κορυφαίο Σύστημα Πρόληψης Εισβολών Ανοιχτού Κώδικα (IPS) στον κόσμο. Το Snort IPS χρησιμοποιεί μια σειρά από κανόνες που βοηθούν στον ορισμό της κακόβουλης δραστηριότητας δικτύου και χρησιμοποιεί αυτούς τους κανόνες για να βρει πακέτα που ταιριάζουν με αυτούς και να δημιουργήσει ειδοποιήσεις για τους χρήστες.

Root: Είναι όταν λειτουγούμε ως διαχειριστής, ο root είναι ένας λογαριασμός υπερ-χρήστη (**super user**) σε έναν υπολογιστή ή ένα δίκτυο και έχει πλήρη έλεγχο.

Buffer: Είναι μια περιοχή της μνήμης που χρησιμοποιείται για την προσωρινή συγκράτηση δεδομένων κατά τη μετακίνησή τους από ένα μέρος σε άλλο. Ένας buffer χρησιμοποιείται κατά τη μετακίνηση δεδομένων μεταξύ διεργασιών σε έναν υπολογιστή**.**

Phishing: Το "ψάρεμα" είναι μια δημοφιλής μορφή εγκλήματος στον κυβερνοχώρο λόγω της αποτελεσματικότητάς του. Οι εγκληματίες του κυβερνοχώρου έχουν επιτύχει να χρησιμοποιούν μηνύματα ηλεκτρονικού ταχυδρομείου, μηνύματα κειμένου, άμεσα μηνύματα στα μέσα κοινωνικής δικτύωσης ή σε βιντεοπαιχνίδια, για να κάνουν τους ανθρώπους να απαντήσουν με τα προσωπικά τους στοιχεία.

social engineering: Η κοινωνική μηχανική είναι ο όρος που χρησιμοποιείται για ένα ευρύ φάσμα κακόβουλων δραστηριοτήτων που επιτυγχάνονται μέσω ανθρώπινων αλληλεπιδράσεων. Χρησιμοποιεί ψυχολογική χειραγώγηση για να εξαπατήσει τους χρήστες ώστε να κάνουν λάθη ασφαλείας ή να δώσουν ευαίσθητες πληροφορίες.

Pastebin: Το pastebin είναι μια διαδικτυακή εφαρμογή που επιτρέπει στους χρήστες να ανεβάζουν και να μοιράζονται κείμενο στο διαδίκτυο. Η πιο συνηθισμένη χρήση είναι η κοινή χρήση πηγαίου κώδικα ή πληροφοριών διαμόρφωσης.

Dark web: Το σκοτεινό διαδίκτυο, είναι ένας ανώνυμος διαδικτυακός ιστός, στον οποίο ανώνυμοι χρήστες έχουν πρόσβαση σε κρυφές υπηρεσίες.

Περίληψη

Τις τελευταίες δεκαετίες τα δίκτυα υπολογιστών εχουν εξελιχτεί πάρα πολύ και αυτό μπορεί να ειναι επικύνδινο. Το διαδύκτιο είναι ένας δίαυλος επικοινωνίας για εκατομμύρια κόσμο με την ανάγκη της επικοινωνίας εξ αποστάσεως μέχρι και εταιρείες και επαγγελματίες με σκοπούς όπως εμπόριο, ανταλλαγή δεδομένων, όμως πίσω απ΄ολα αυτά κρύβονται πολλοί κίνδυνοι.

Στην παρούσα εργασία θα αναλύσουμε αυτούς τους κίνδυνους και θα δούμε τεχνικές και τρόπους ασφαλείας.Αρχικά, θα αναπτύξουμε την αρχιτεκτονική των firewalls και θα δούμε ειδικότερα και το IPsec, τι ασφάλεια παρέχει αλλά και πως εφαρμόζεται στο διαδίκτυο. Στη συνέχεια θα μιλήσουμε για τις πολίτικες ασφαλείας και θα αναπτύξουμε μεθόδους και συστήματα ασφαλείας που μπορούν να εφαρμοστούν στο διαδίκτυο για την προστασία των δεδομένων. Θα δούμε τρόπους επιθέσεων σε ένα δίκτυο υπολογιστών και τρόπους προστασίας. Στόχος αυτής της έργασίας είναι να εντοπιστούν τα λεπτά και αβίαστα σημάδια ενός δικτύου που δέχεται επίθεση. Για την επίτευξη αυτού του στόχου θα χρησημοποιήσουμε τεχνικές, όπως η παρακολούθηση των στοιχείων του δικτύου για τον εντοπισμό ανώμαλης συμπεριφοράς και κατάχρησης. Αυτή η τεχνική ανέπτυξε το σύστημα Ανίχνευσης Εισβολής (IDS). Αυτή η εργασία αξιολογεί τις απόψεις σχετικά με το τι κάνει έναν χάκερ. Πώς ένας χάκερ θα έπιανε κανονικά ένα δίκτυο και πώς κατασκευάζονται νέες στρατηγικές επίθεσης. Στη συνεχεια θα δουμε πως μια IPS εμποδίζει την εισβολή; Για να απαντηθεί αυτή η ερώτηση, η διατριβή θα προχωρήσει ως εξής:

- Εξέταση των αντιμετρημάτων που μπορούν να εφαρμόσουν οι οργανισμοί για να συμπληρώσουν ένα IPS.
- Ανάλυση των τύπων των ατόμων που προσπαθούν να παρακάμψουν την εφαρμοζόμενη IPS.

Τέλος στο κεφάλαιο έξι εξετάζουμε τις μεθόδους που θα χρησιμοποιούσαν αυτοί οι άνθρωποι και πώς δημιουργείται μια νέα στρατηγική επίθεσης. Στη συνέχεια, διεξάγεται ένα πείραμα για την προβολή μεθόδων hacking, ακολουθούμενο από αντίμετρα που αν εφαρμόζονταν θα μπορούσαν να μειώσουν τις επιπτώσεις της επίθεσης.

Λέξεις-Κλειδιά: Συστήματα Ανίχνευσης Εισβολών, Πληροφορική, Τείχος Προστασίας, Εισβολή, Δεδομένα.

Abstract

In the last few decades computer networks have evolved enormously and this can be dangerous. The Internet is a communication channel for millions of people with the need to communicate at a distance, up to companies and professionals for purposes such as trade, data exchange, but behind all this there are many risks.

In this paper we will analyze these risks and we will look at security techniques and ways of security. First, we will develop the architecture of firewalls and we will look in particular at IPsec, what security it provides and how it is applied on the internet. We will then talk about security policies and develop security methods and systems that can be applied on the internet to protect data. We will look at ways of attacking a computer network and ways of protecting it. The goal of this work is to identify the subtle and effortless signs of a network under attack. To achieve this goal, we will use techniques such as monitoring network elements to detect abnormal behavior and abuse. This technique developed the Intrusion Detection System (IDS). This paper evaluates views on what makes a hacker. How a hacker would normally capture a network and how new attack strategies are constructed. With the continued release of insecure operating systems and software, protecting these products is a persistent problem. Then we will see how an IPS prevents invasion? To answer this question, the thesis will proceed as follows:

- Examination of the countermeasures that organizations can apply to complete an IPS.
- Analysis of the types of people who try to bypass the applied IPS.

Finally in chapter six we look at the methods these people would use and how a new attack strategy is created. An experiment is then conducted to demonstrate hacking methods, followed by countermeasures that, if implemented, could reduce the impact of the attack.

Keywords: Intrusion Detection Systems, Information Technology, Firewall, Intrusion, Data.

Εισαγωγή

Τα έργα διαδικτύου που συνδέουν πολλούς οργανισμούς δημιουργούν πιθανά προβλήματα ασφαλείας τα οποία δεν μπορούν να επιλυθούν απλά με εσωτερικές διοικητικές διαδικασίες. Οι οργανισμοί θα ήθελαν να περιορίσουν την πρόσβαση μεταξύ των οργανώσεων σε συγκεκριμένους περιορισμένους φορείς και εφαρμογές, προκειμένου να περιορίσουν τις πιθανότητες ζημιών και να μειώσουν τον αριθμό των συστημάτων που πρέπει να διασφαλίζονται κατά των επιθέσεων. Ένας τρόπος περιορισμού της πρόσβασης είναι να αποτρέπεται η είσοδος ή η έξοδος ορισμένων πακέτων από έναν οργανισμό μέσω των θυρών του. Αυτό το έγγραφο περιγράφει απλούς, ευέλικτους και μετρίως αποτελεσματικούς μηχανισμούς για τον έλεγχο των πακέτων που ρέουν μέσω μιας πύλης που βασίζεται στο Unix. [32]

Η προηγούμενη παράγραφος ήταν η περίληψη του πρώτου αναγνωρισμένου εγγράφου σχετικά με τα τείχη προστασίας και τα ζητήματα ασφάλειας που τα περιβάλλουν. Παρουσιάστηκε από τον Jeffery C. Mogul στην καλοκαιρινή διάσκεψη USENIX που πραγματοποιήθηκε στη Βαλτιμόρη το 1989. Πριν από την εμφάνιση των υπολογιστών και τη δικτύωση ο όρος «Firewall» χρησιμοποιήθηκε σε ένα κτίριο ως αλεξίπυρο τείχος που χρησιμοποιείται ως εμπόδιο για την πρόληψη της εξάπλωσης της φωτιάς. [26]

Καθώς το Διαδίκτυο αναπτύχθηκε από αναχαίτηση πόρων σε μια ανοιχτή κοινότητα, προέκυψε η ανάγκη να σταματήσουν οι ανεπιθύμητες επιθέσεις σε δίκτυα υπολογιστών. Η ανησυχητική ταχύτητα ακόμη και των πρώτων επιθέσεων θεωρήθηκε καταστροφική**.**

Η πρώτη τεκμηριωμένη «επίθεση» του διαδικτύου κυκλοφόρησε στις 3 Νοεμβρίου 1988. Αυτή η επίθεση έδειξε την ανάγκη για κάποιο βαθμό άμυνας του δικτύου. Τα Συστήματα Πρόληψης Εισβολής (IPS) είναι η τελευταία βοήθεια για την προστασία των δικτύων από επιθέσεις με τη βοήθεια υπολογιστή. Η προηγούμενη ανάπτυξη συστημάτων υπήρξε ένα σημαντικό βήμα καθώς τα τείχη προστασίας και τα συστήματα ανίχνευσης εισβολής (IDS) έθεσαν ισχυρά θεμέλια για το IPS. Ένα σημαντικό μέρος της έρευνας σε αυτόν τον τομέα έχει αφιερωθεί στην ανάπτυξη και την πρόοδο των τειχών προστασίας και IDS. Αυτή η έρευνα δείχνει ότι η ανάπτυξη ανταποκρινόταν στην ανάγκη να διορθωθούν τα προβλήματα σε προηγούμενες αρχιτεκτονικές και όχι μια θεμελιώδης επιθυμία για τη βελτίωση ενός προτεινόμενου προϊόντος χωρίς προβλήματα. [54]

Ένα IPS έχει σχεδιαστεί για την προστασία ενός δικτύου. Είναι συνδεδεμένο στο ενσωματωμένο δίκτυο, ώστε να μπορεί να παρακολουθεί όλη την κυκλοφορία του δικτύου που αποστέλλεται και λαμβάνεται. Ένα IPS έχει τη δυνατότητα να επιτρέπει ή να αποτρέπει την κυκλοφορία του δικτύου. Ένα IPS είναι μια εφαρμογή στις τεχνολογίες τείχους προστασίας και στο IDS, καθώς συνδυάζει και τα δύο σε μία συσκευή.[51]

Κεφάλαιο 1ο

1.1.Εισαγωγή

Η ανάπτυξη των δικτύων στους υπολογιστές ήταν ραγδαία της τελευταίες δεκαετίες παγκοσμίως, για την κάλυψη αναγκών μεγάλων εταιριών, την συνεργασία πανεπιστημίων, άλλων φορέων, ακόμα και του απλού πολίτη. Αυτό έχει σαν αποτέλεσμα την προσπάθεια και την δημιουργία μίας αρχιτεκτονικής ασφάλειας δικτύων, όσο το δυνατόν πιο επιτυχημένα. Με την έννοια ασφάλεια δικτύων, αναφερόμαστε σ' ένα πολυσύνθετο κομμάτι, το οποίο αποτελείται από διάφορους κανόνες, πολιτικές ασφάλειας, ενέργειες αλλά και εξοπλισμό (software/hardware). [10]

Με τον όρο «ασφάλεια», υποδηλώνονται ένα πλήθος εννοιών, όπως είναι η εμπιστευτικότητα (Confidentiality), δηλαδή η προστασία της πληροφορίας από μη εξουσιοδοτημένη πρόσβαση, η ακεραιότητα (Integrity), δηλαδή η προστασία της πληροφορίας από μη εξουσιοδοτημένη τροποποίηση και τέλος η διαθεσιμότητα (Availability), όπου τα δεδομένα υπάρχουν στη θέση, στον χρόνο και στην μορφή που ο χρήστης τα χρειάζεται. Άλλες μορφές της εμπιστευτικότητας είναι: η ιδιωτικοποίηση (privacy), δηλαδή η προστασία των προσωπικών δεδομένων καθώς και η μυστικότητα (secrecy), δηλαδή η προστασία δεδομένων που ανήκουν σε μία εταιρεία. Δίνοντας λοιπόν, μεγάλη βαρύτητα στην ασφάλεια των δικτύων αποτρέπουμε τυχόν επιθέσεις που έχουν ως αντίκτυπο οικονομικές απώλειες, πιθανή σπατάλη πολύτιμου χρόνου για την αποκατάσταση του συστήματος που δέχτηκε επίθεση, όπως και την αποφυγή ενδεχόμενου καίριου πλήγματος στο κύρος και την αξιοπιστία του συστήματος.[58]

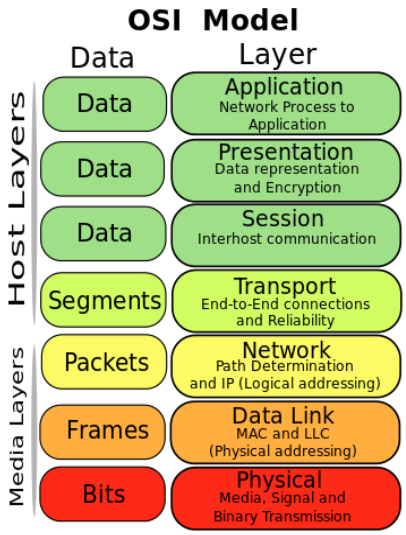
Η Ασφάλεια Δικτύου είναι ζωτικής σημασίας για την προστασία των δεδομένων και των πληροφοριών των πελατών, για τη διατήρηση της ασφάλειας των κοινών δεδομένων και για την εξασφάλιση αξιόπιστης πρόσβασης και απόδοσης δικτύου, καθώς και για την προστασία από απειλές στον κυβερνοχώρο. Μια καλά σχεδιασμένη λύση ασφάλειας δικτύου μειώνει τα γενικά έξοδα και προστατεύει τους οργανισμούς από δαπανηρές απώλειες που προκύπτουν από παραβίαση δεδομένων ή άλλο περιστατικό ασφάλειας. Η διασφάλιση νόμιμης πρόσβασης σε συστήματα, εφαρμογές και δεδομένα επιτρέπει τη λειτουργία των επιχειρήσεων και την παράδοση υπηρεσιών και προϊόντων στους πελάτες. [17]

1.2. Το Μοντέλο OSI

Το μοντελο OSI βασιζεται σε μια πρόταση που αναπτύχθηκε από τον Διεθνή Οργανισμό Πρωτύπων (International Standards Organization/ ISO)για την τυποποίηση των πρωτοκόλλων που χρησιμοποιούνται στα διάφορα επίπεδα των δικτύων. OSI σημαίνει Διασύνδεση Ανοικτών Συστημάτων (Open System Interconnection), λόγω του ότι ασχολείται με τη διασύνδεση ανοικτών συστημάτων, δηλαδή συστήματα που ειναι ανοιχτά στην επικοινωνία με άλλα συστήματα.[56]

Το μοντέλο OSI αποτελείται απο επτά επίπεδα:

1) Φυσικό Επίπεδο
2) Επίπεδο Ζεύξης Δεδομένων
3) Επίπεδο Δικτύου
4) Επίπεδο Μεταφοράς
5) Επίπεδο Συνόδου
6) Επίπεδο Παρουσίασης
7) Επίπεδο Εφαρμογής



Εικονα 1.1: το μοντελο OSI

1.3. IPsec ασφάλεια στο internet

Για την παροχή ασφάλειας σε ένα πακέτο στο επίπεδο IP, το IETF (Internet Engineering Task Force), σχεδίασε μια συλλογή πρωτοκόλλων, την ασφάλεια IP (IPsec). Δεν εφαρμόζεται συγκεκριμένη μέθοδος αυθεντικοποίησης από το IPsec. Το IPsec αφήνει την επιλογή των μεθόδων κρυπτογράφησης, αυθεντικοποίησης και κατακερματισμού στην οντότητα, παρέχοντας ένα περιβάλλον εργασίας και έναν μηχανισμό. Τα μετρά που λαμβάνονται για την ασφάλεια εφαρμόζονται στο επίπεδο μεταφοράς, το επίπεδο εφαρμογής και το επίπεδο δικτύου. Στο επίπεδο IP πρέπει κάθε συσκευή να ενεργοποιηθεί. Για αυτόν τον λόγο, η υλοποίηση των στοιχείων ασφάλειας είναι πολύπλοκη. Το IP πέρα από τις υπηρεσίες που παρέχει σε εφαρμογές χρηστών, παρέχει υπηρεσίες και σε πρωτόκολλα όπως ICMP, IGMP και OSPF. Για τον λόγο αυτό, δεν είναι ιδιαίτερα αποτελεσματική η ασφάλεια σε αυτό το επίπεδο, με εξαίρεση τις συσκευές που έχουν εξοπλιστεί έτσι, ώστε να την χρησιμοποιούν. [55]

1.4. Εφαρμογές του IPsec

Το IPSec παρέχει τη δυνατότητα να ασφαλίζει τις επικοινωνίες κατά μήκος ενός τοπικού δικτύου(LAN), κατά μήκος ιδιωτικών και δημοσίων δικτύων ευρείας περιοχής(WAN) και κατά μήκος του Διαδικτύου.

Παραδείγματα της χρήσης του:

- Ασφάλεια στην συνδεσιμότητας υποκαταστημάτων μέσω του Διαδικτυου: Μια εταιρεία μπορεί να δημιουργήσει ασφαλή εικονικά ιδιωτικά δίκτυα (Virtual Private Networks, VPN) μέσω του Διαδικτύου ή μέσω ενός δημοσίου WAN. Αυτό επιτρέπει σε μια επιχείρηση να βασίζεται στο διαδίκτυο μειώνοντας την ανάγκ της για ιδιωτικά δίκτυα, εξοικονομώντας χρήματα και μειώνοντας το διαχειριστικό κόστος

- Ασφάλεια στην τηλεπρόσβαση μέσω του Διαδικτύου: Ένας τερματικός χρήστης του οποίου το σύστημα είναι εφοδιασμένο με πρωτοκολλά ασφάλειας IP μπορεί να κάνει μια τοπική κλήση σε έναν παροχέα υπηρεσιών Διαδικτύου (ISP) και να επιτύχει ασφαλή πρόσβαση σε ένα εταιρικό δίκτυο. Με τον τρόπο αυτό μειώνεται το κόστος για την μετακίνηση ή τη σύνδεση των εργαζομένων.

- Εγκατάσταση συνδεσιμότητας υπερενδοδικτύου (extranet) και ενδοδικτύου (intranet) με συνεταίρους: Το IPSec μπορεί να χρησιμοποιηθεί για να ασφαλίσει την επικοινωνία με άλλους οργανισμούς, εξασφαλίζοντας πιστοποίηση αυθεντικότητας και την εμπιστευτικότητα και παρέχοντας μηχανισμούς ανταλλάγης κλειδιού.

- Βελτίωση ασφάλειας ηλεκτρονικού εμπορίου : Έστω και αν κάποιες εφαρμογές του ηλεκτρονικού εμπορίου και συναλλαγών μέσω του Διαδικτύου έχουν ενσωματωμένα πρωτόκολλα ασφάλειας , η χρήση του IPSec αυξάνει την υπάρχουσα ασφάλεια.

Το βασικό χαρακτηριστικό του IPSec που του επιτρέπει να υποστηρίζει αυτές τις ποικίλες εφαρμογές είναι ότι μπορεί να κρυπτογραφήσει και να πιστοποίησει όλη την κίνηση δεδομένων στο επίπεδο IP. Με τον τρόπο αυτό μπορούν να χρησιμοποιούν κρυπτογραφία όλες οι κατανεμημένες εφαρμογές, όπως η τηλεσύνδεση, οι εφαρμογές πελάτη διακομιστή, το ηλεκτρονικό ταχυδρομείο, η μεταφορά αρχείων, η πρόσβαση στον Παγκοσμιο ιστό, κ.λπ. [55]

1.5. Ιστορική Αναδρομή των Firewall

Ακολουθεί ένα χρονοδιάγραμμα των εξελισσόμενων τεχνολογιών τείχους προστασίας και του τρόπου με τον οποίο εξελίχθηκαν. Δείχνει μια σαφή σταθερή τάση να βελτιώνεται συνεχώς σε προηγούμενες μεθόδους και fixfaults στην προηγούμενη τεχνολογία. Οι ιδέες που περιγράφονται σε αυτή την ενότητα συζητούνται με μεγαλύτερο βάθος. Η πρώτη γενιά αρχιτεκτονικών τείχους προστασίας έχει χρησιμοποιηθεί σχεδόν όσο οι δρομολογητές και πρωτοεμφανίστηκε γύρω στο 1985. Ωστόσο, η πρώτη έντυπη εγγραφή της διαδικασίας διαλογής που χρησιμοποιήθηκε από τα τείχη προστασίας φίλτρων πακέτων δεν εμφανίστηκε παρά μόνον το έτος 1988, όταν ο Jeff Mogul από την Digital Equipment Corporation δημοσίευσε τις μελέτες του. [24,28]

Κατά την περίοδο περίπου 1989-1990, ο Dave Presotto και ο Howard Trickey της AT&T Bell Laboratories ανέλαβαν τη δεύτερη γενιά αρχιτεκτονικών τείχους προστασίας με την έρευνά τους σε ηλεκτρονόμους κυκλωμάτων, οι οποίοι ήταν γνωστοί ως τείχη προστασίας επιπέδου κυκλώματος. Εφάρμοσαν επίσης το πρώτο μοντέλο εργασίας της τρίτης γενιάς αρχιτεκτονικών τείχους προστασίας, γνωστό ως τείχος προστασίας επιπέδου εφαρμογών. Ωστόσο, ούτε δημοσίευσαν οποιαδήποτε εργασία που περιγράφει αυτή την αρχιτεκτονική ούτε κυκλοφόρησαν ένα προϊόν με βάση το έργο τους. Όπως συμβαίνει συχνά στην έρευνα και την ανάπτυξη, η τρίτη γενιά αρχιτεκτονικών τείχους προστασίας ερευνήθηκε και αναπτύχθηκε ανεξάρτητα από αρκετούς ανθρώπους στις Ηνωμένες Πολιτείες κατά τη διάρκεια της δεκαετίας του 1980 και των αρχών της δεκαετίας του 1990. [23]

Οι δημοσιεύσεις από τον Gene Spafford του Πανεπιστημίου Purdue, τον Bill Cheswick των εργαστηρίωνAT&T Bell και τον Marcus Ranum που περιγράφουν τα τείχη προστασίας των επιπέδων εφαρμογών εμφανίστηκαν για πρώτη φορά το 1990 και το 1991. Το έργο του Marcus Ranum έλαβε τη μεγαλύτερη προσοχή το 1991 και πήρε τη μορφή των οικοδεσποτών προμαχώνα που εκτελούν υπηρεσίες μεσολάβησης. Το έργο του Ranum εξελίχθηκε γρήγορα στο πρώτο σε πωλήσεις προϊόν: Το προϊόν ασφαλούς εξωτερικής πρόσβασης (SEAL) της Digital Equipment Corporation. Γύρω στο 1991, ο Bill Cheswick και ο Steve Bellovin άρχισαν να ερευνούν το δυναμικό φιλτράρισμα πακέτων επίσης γνωστό ως κρατική επιθεώρηση και έφτασε στο σημείο να βοηθήσει στην ανάπτυξη ενός εσωτερικού προϊόντος στο BellLaboratories με βάση αυτή την αρχιτεκτονική. [22] Ωστόσο, αυτό το προϊόν δεν κυκλοφόρησε ποτέ. Το 1992, ο BobBraden και η Annette DeSchon στο Ινστιτούτο Επιστημών Πληροφοριών του USC άρχισαν να αναζητούν ανεξάρτητα δυναμικά τείχη προστασίας φίλτρων πακέτων. Η Check PointSoftware κυκλοφόρησε το πρώτο εμπορικό προϊόν με βάση

αυτή την αρχιτεκτονική τέταρτης γενιάς το 1994. Κατά τη διάρκεια του 1996, Scott Wiegel, Επικεφαλής Επιστήμονας στην Παγκόσμια Ομάδα Λογισμικού Διαδικτύου, Inc., άρχισε να καθορίζει τα σχέδια για την αρχιτεκτονική τείχους προστασίας πέμπτης γενιάς, την αρχιτεκτονική διακομιστή μεσολάβησης πυρήνα. Το CiscoCentri Firewall, που κυκλοφόρησε το 1997, ήταν το πρώτο εμπορικό προϊόν που βασίστηκε σε αυτή την αρχιτεκτονική. [19]

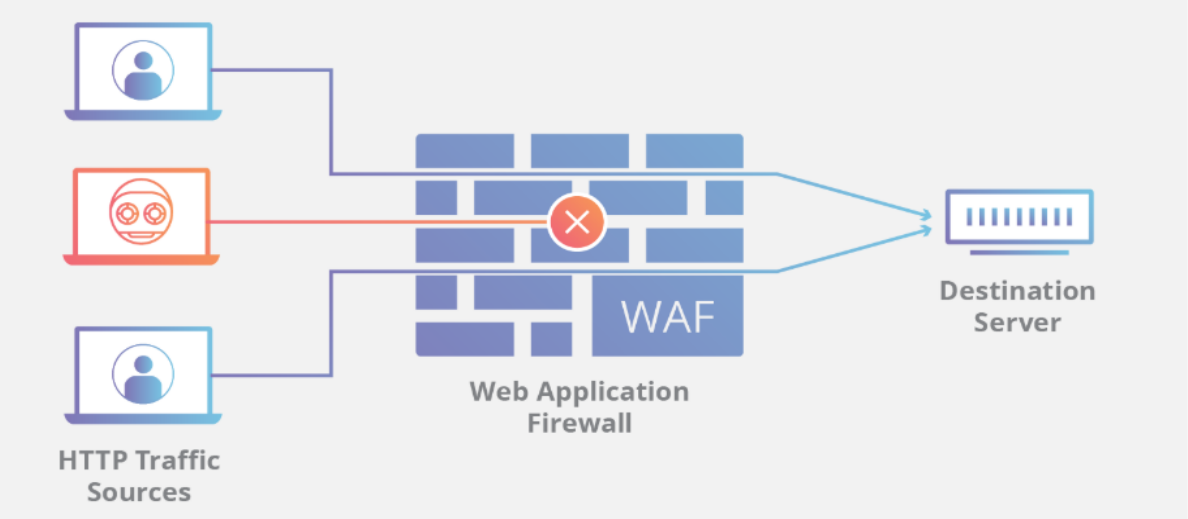
1.6. Ανάπτυξη τεχνολογιών τείχους προστασίας «filter firewalls»

Τα πρώτα τείχη προστασίας χρησιμοποίησαν την τεχνολογία δρομολογητή πρωτοκόλλου Internet (IP), το επίπεδο δικτύου και τα φίλτρα για να καθορίσουν εάν επιτραπεί η πρόσβαση στο δίκτυο. Τα πακέτα filter firewalls θα μπορούσαν μόνο να επιτρέψουν ή να απορρίψουν την επικοινωνία δικτύου. Οι κανόνες φιλτραρίσματος έπρεπε να αναλυθούν με μη αυτόματο τρόπο από το διαχειριστή του τείχους προστασίας. Οι κανόνες φιλτραρίσματος εξετάζουν εισερχόμενα ή εξερχόμενα πακέτα, επιτρέποντας ή απωθώντας τη μετάδοσή τους. Η βάση για αυτούς τους κανόνες ήταν συχνά η προέλευση IPaddress, η θύρα προορισμού και το πρωτόκολλο που χρησιμοποιήθηκε. Ένα πρόβλημα του πρώτου τείχους προστασίας filter firewalls ήταν ότι επειδή χρησιμοποιούσε τεχνολογία δρομολογητή IP που διέσχιζε την κυκλοφορία μέσω της σύνδεσης, επέτρεπε άμεσες συνδέσεις μεταξύ δικτύων μέσω εξουσιοδότησης(authorization). Για να διορθωθεί αυτό το πρόβλημα, αναπτύχθηκε μια περαιτέρω σειρά τειχών προστασίας μεταξύ 1989 και 1990 χρησιμοποιώντας πύλες τείχους προστασίας επιπέδου κυκλώματος. [18]

Οι πύλες σε επίπεδο κυκλώματος βασίζονται σε κεντρικούς υπολογιστές και βρίσκονται σε μεμονωμένους πελάτες και διακομιστές εντός του δικτύου. Οι πύλες σε επίπεδο κυκλώματος εξετάζουν τα εισερχόμενα πακέτα πρωτοκόλλου Διαδικτύου (IP) σε επίπεδο συνεδρίας Πρωτόκολλο Ελέγχου Μετάδοσης (TCP) ή Πρωτόκολλο Δεδομένων Χρήστη (UDP) για να βεβαιωθεί ότι ο αποστολέας επιτρέπεται να μεταβεί στον παραλήπτη και ότι ο παραλήπτης επιτρέπεται να λάβει από τον αποστολέα.

Η επόμενη πρόοδος στην τεχνολογία τείχους προστασίας πραγματοποιήθηκε το 1991 με την πρώτη εμπορική κυκλοφορία του firewall από την Digital Equipment Corporation (DEC) με τη νέα ανάπτυξη ενός τείχους προστασίας στοιβάδων που ονομάζεται SEAL. [17]Η νέα γενιά τειχών προστασίας χρησιμοποιεί φίλτρα και πύλες εφαρμογών ή proxies για τον έλεγχο της κυκλοφοριακής ρύθμισης ή την έξοδο από τα δίκτυά τους. Το τείχος προστασίας επιπέδου εφαρμογής είναι ένας μεσάζων μεταξύ του δικτύου και του Διαδικτύου όπως φαίνεται παρακάτω στην εικόνα 1.2. Το τείχος προστασίας επιπέδου εφαρμογής έχει δύο κύριες

λειτουργίες, για να ενεργεί ως διακομιστής μεσολάβησης ή ως proxy client. Αυτό σημαίνει ότι το τείχος προστασίας είναι το ενδιάμεσο για κάθε επικοινωνία που διασχίζει τα δύο δίκτυα (εσωτερικό δίκτυο και Internet). Όταν ένας υπολογιστής Α θέλει να επικοινωνήσει με τον υπολογιστή Β που είναι συνδεδεμένος στον παγκόσμιο ιστό, το τείχος προστασίας C λειτουργεί ως μεσάζων μεταξύ των υπολογιστών Α και Β. Το τείχος προστασίας C παίρνει την προβλεπόμενη επικοινωνία από τον υπολογιστή Α και την κατευθύνει στον υπολογιστή Β, όταν ο υπολογιστής Β απαντά, απαντά στο τείχος προστασίας C νομίζοντας ότι είναι ο υπολογιστής Α. Όταν ο υπολογιστής Α επικοινωνεί πίσω στον υπολογιστή Β, στην πραγματικότητα μεταβιβάζει δεδομένα μόνο στο τείχος προστασίας C. [13]



Εικόνα 1.2 τείχος προστασίας σε επίπεδο εφαρμογής

Οι συνδέσεις Inbound πραγματοποιούνται πάντα με το πρόγραμμα-πελάτη μεσολάβησης, ενώ οι εξερχόμενες συνδέσεις γίνονται με το διακομιστή μεσολάβησης. Δεν υπάρχει άμεση σύνδεση μεταξύ του εσωτερικού δικτύου και ενός ανασφαλούς δικτύου. Ένα τυπικό τείχος προστασίας επιπέδου εφαρμογής μπορεί να παρέχει υπηρεσίες μεσολάβησης για εφαρμογές και πρωτόκολλα όπως είναι το πρωτόκολλο μεταφοράς αρχείων (FTP), το πρωτόκολλο μεταφοράς υπερκειμένου (HTTP) και το πρωτόκολλο απλής μεταφοράς αλληλογραφίας (SMTP). [11] Πλέον όπως έχει σημειωθεί πρέπει να εγκατασταθεί ένας ξεχωριστός διακομιστής μεσολάβησης για κάθε υπηρεσία επιπέδου εφαρμογής. Όταν το τείχος προστασίας επιπέδου εφαρμογής μεταβιβάζει την κυκλοφορία από δίκτυο σε δίκτυο, το τείχος προστασίας έχει την ευκαιρία να αναλύσει τα δεδομένα και τις κεφαλίδες μέσα στην κυκλοφορία. Όταν η κυκλοφορία φτάσει στην εσωτερική σύνδεση, το τείχος προστασίας αξιολογεί τις διευθύνσεις IP. Εξετάζει τα δεδομένα μέσα στο πακέτο για να τοποθετήσει σε ένα εξωτερικό αρχείο

προέλευσης πληροφορίες απόκρυψης και χρησιμοποιεί τυχόν φίλτρα ή πολιτικές που υπάρχουν για να καθορίσει εάν η κυκλοφορία είναι νόμιμη ή όχι και αν επιτρέπεται να εισέλθει στο εσωτερικό δίκτυο. [8]

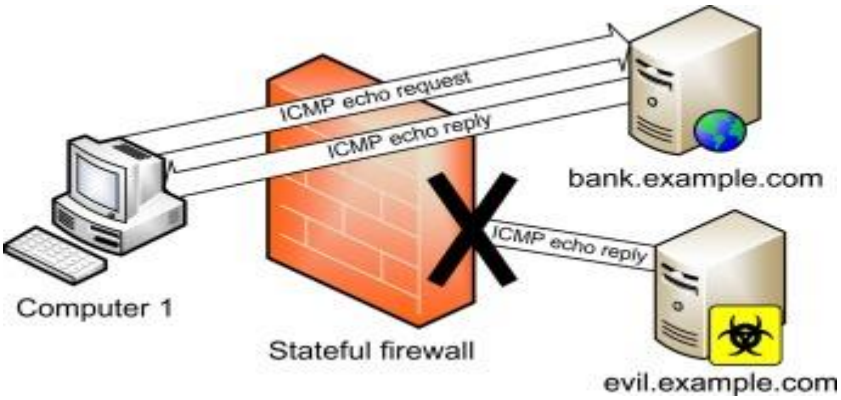
Τα πλεονεκτήματα αυτής της τεχνικής είναι ότι επειδή ενεργούν ως διακομιστής μεσολάβησης, όλη η επικοινωνία μεταβιβάζει το τείχος προστασίας. Μπορεί επίσης να ελέγξει ποια πρωτόκολλα χρησιμοποιούνται, όπως HTTP και FTP, αλλά μπορεί να διασαφηνίσει ομότιμους υπολογιστές (P2P) και άλλα πρωτόκολλα που δεν χρησιμοποιούνται. Ένα τείχος προστασίας επιπέδου εφαρμογής μπορεί να περιορίσει την πρόσβαση σε ορισμένες υπηρεσίες δικτύου και ιστότοπους που δεν σχετίζονται με την επιχείρηση, όπως ιστότοπους web ή πορνογραφία. [6]

Το τείχος προστασίας επιπέδου εφαρμογής μπορεί επίσης να χρησιμοποιήσει τον έλεγχο ταυτότητας και τον έλεγχο ταυτότητας του αντικειμένου HTTP. Καθώς όλη η κυκλοφορία ρέει μέσα από αυτό, το τείχος προστασίας επιπέδου εφαρμογής έχει όλες τις πληροφορίες που απαιτούνται για τη δημιουργία ολοκληρωμένων αναφορών ελέγχου. Όπως και με πολλές πτυχές της Επιστήμης των Πληροφοριών, υπάρχουν μειονεκτήματα όπως:

- Καθώς όλη η κυκλοφορία ρέει μέσα από αυτό, ο διακομιστής μεσολάβησης εισάγει καθυστερήσεις στην επικοινωνία.
- Ένας νέος διακομιστής μεσολάβησης πρέπει να γραφτεί για κάθε νέο πρωτόκολλο που πρέπει να περάσει μέσω του τείχους προστασίας, συχνά λόγω καθυστερήσεων.
- Καθώς το τείχος προστασίας εκτελείται χρησιμοποιώντας αρχιτεκτονική λειτουργικού συστήματος τρίτου μέρους, είναι ευάλωτη σε σφάλματα λειτουργικού συστήματος (OS) και επιπέδου εφαρμογής. [5]

Λόγω των μειονεκτημάτων με το κόστος και την απόδοση των τειχών προστασίας επιπέδου εφαρμογής και την ασφάλεια του φιλτραρίσματος πακέτων, αναπτύχθηκε μια νέα μέθοδος. Αντί να εξετάσει τα περιεχόμενα κάθε πακέτου, οι πληροφορίες κεφαλίδας του πακέτου συγκρίνονται με πακέτα που είναι γνωστό ότι είναι αξιόπιστα. Ένα νέο χαρακτηριστικό του τείχους προστασίας επιθεώρησης ήταν η δημιουργία ενός κρατικού πίνακα. Αυτός ο πίνακας διατήρησε μια λίστα ανοιχτών συνδέσεων. Όταν ένας χρήστης είχε πρόσβαση σε μια εξωτερική υπηρεσία, το κρατικό τείχος προστασίας επιθεώρησης θυμήθηκε λεπτομέρειες σχετικά με την αρχική αίτηση, όπως ο αριθμός θύρας, η προέλευση και η διεύθυνση προορισμού. Αυτή η «ανάμνηση» καλείται «διάσωση του κράτους». Όταν το εξωτερικό σύστημα ανταποκρίθηκε σε μια αίτηση, το τείχος προστασίας συνέκρινε τα πακέτα που ελήφθησαν με την αποθηκευμένη κατάσταση για να καθορίσει εάν το περιεχόμενο τους είναι

νόμιμο. Το αποτέλεσμα ενός κρατικού πίνακα σήμαινε ότι ένα πακέτο μπορεί να δημιουργηθεί από ένα τρίτο μέρος για να μοιάζει με άτυπη νόμιμη απόκριση. Όταν το τείχος προστασίας έλεγξε τον πίνακα κατάστασης, δεν θα υπήρχε καταχώρηση σύνδεσης για την απόκριση, απαγορεύοντας έτσι την πρόσβαση στο εσωτερικό δίκτυο.



Εικόνα 1.3 Κρατικό τείχος προστασίας

Ένα κρατικό τείχος προστασίας επιθεώρησης θα μπορούσε να διαβάσει και τα επτά επίπεδα διασύνδεσης ανοικτών συστημάτων (OSI), επιτρέποντάς του να φιλτράρει πακέτα σε επίπεδο κεφαλίδας, καθώς και να παρέχει τη δυνατότητα ανάλυσης των εφαρμογών, ξεπερνώντας τις αδυναμίες των συσκευών φιλτραρίσματος IP. Η ίδια η κρατική επιθεώρηση έχει αποδειχθεί ένας πολύ αποτελεσματικός μηχανισμός ελέγχου πρόσβασης. Ωστόσο, με τη χρήση οποιασδήποτε νέας τεχνολογίας, η κρατική επιθεώρηση είχε τα μειονεκτήματά της. Χαρακτηριστικό παράδειγμα αποτελεί η εγγενής αδυναμία του UDP η οποία οφειλόταν στην έλλειψη κρατικής σύνδεσης. Το UDP δεν διαθέτει έλεγχο διόρθωσης σφαλμάτων ή ακεραιότητας. Εάν σταλεί ένα πακέτο UDP, μια απόκριση ενός πακέτου μπορεί ενδεχομένως να κάνει κλικ σε έναν χάκερ. [49]

Ένα άλλο μειονέκτημα ήταν ότι ένα κρατικό τείχος προστασίας επιθεώρησης δεν ήταν πληρεξούσιος πάροχος. Επιτρέπει στα εσωτερικά πακέτα να κατευθύνουν το δρόμο τους προς το εξωτερικό δίκτυο, εκθέτοντας έτσι εσωτερικές διευθύνσεις IP σε πιθανούς χάκερ. Ορισμένοι προμηθευτές τείχους προστασίας χρησιμοποιούν κρατικούς ελέγχους και proxies μαζί για πρόσθετη ασφάλεια.[31] Όπως και να έχει, ένα πλεονέκτημα είναι ότι το πιο κοινό πρωτόκολλο επικοινωνίας που χρησιμοποιείται μέσω του Internet είναι το TCP και το TCP διατηρεί την κατάσταση. Αυτό σημαίνει ότι πρέπει να χρησιμοποιηθούν αριθμοί ακολουθίας. Προκειμένου να ανατραπεί η ασφάλεια που παρέχει το TCP, όχι μόνο πρέπει να

πλαστογραφηθεί η διεύθυνση IP προέλευσης, αλλά πρέπει επίσης κάποιος να είναι σε θέση να γνωρίζει τον αριθμό ακολουθίας που πρέπει να χρησιμοποιηθεί. Ένα παράδειγμα εφαρμογής κρατικού ελέγχου είναι το τείχος προστασίας freeware IPTables που είναι κατάλληλο με πολλές διανομές Linux. Οι ipTables ελέγχουν και φιλτράρουν κάθε πακέτο ξεχωριστά. Το τείχος προστασίας επιθεώρησης χρησιμοποιεί επίσης φίλτρα. Για παράδειγμα, μπορεί να κάνει διάκριση μεταξύ πακέτων που αναζητούν μια σύνδεση και εκείνων που είναι ήδη συνδεδεμένα σε μια περίοδο λειτουργίας, ελέγχοντας αν έχει οριστεί το SYNflag στην κεφαλίδα του πακέτου (καθώς και αν έχουν οριστεί σημαίες FIN και ACK). [48]

Μεταξύ του επιπέδου εφαρμογής και των κρατικών τειχών επιθεώρησης, πρέπει να λαμβάνονται υπόψη οι πολιτικές και οι διαδικασίες ενός οργανισμού. Οι πύλες εφαρμογής παρέχουν καλύτερο έλεγχο και καταγραφή, ενώ η κρατική επιθεώρηση έχει τόσο το πλεονέκτημα στην απόδοση όσο και πολύ μεγαλύτερη ευελιξία, αλλά με τη σειρά μιας λανθασμένης διαμόρφωσης.

Η επόμενη ανάπτυξη τεχνολογιών τείχους προστασίας ήταν η εισαγωγή δυναμικών πακέτων φιλτραρίσματος. Ήταν στενά συνδεδεμένα με τα κρατικά τείχη προστασίας επιθεώρησης. Πολλοί ορισμοί τους κατατάσσουν ως την ίδια τεχνολογία. Η πρόοδος στα δυναμικά τείχη προστασίας φιλτραρίσματος πακέτων ήταν παρόμοια με τον κρατικό πίνακα καθώς εξετάζει κάθε πακέτο σε αντίθεση με τη σύνδεση στο σύνολό της. Η ασφάλεια γύρω από την επικοινωνία αυξήθηκε έτσι ώστε οι πιθανοί επιτιθέμενοι να μην μπορούν να προσαρμόσουν ένα πακέτο που κρατιέται μέσα στην κανονική επικοινωνία. Η μέθοδος του τείχους προστασίας φιλτραρίσματος δυναμικών πακέτων είχε αρνητική απόδοση, αλλά με την πρόοδο στην τεχνολογία microchip, δεν ήταν μια σημαντική ανησυχία. [47]

Η ανάπτυξη με δυναμικά τείχη προστασίας φιλτραρίσματος πακέτων ήταν η εμπορική έκδοση του Firewall-1 από την Check Point Technologies το 1994. Αυτό το τείχος προστασίας ήταν το πρώτο φιλικό προς το χρήστη προϊόν με εικονίδια και απλοποιημένη εγκατάσταση και διαχείριση. Επιπλέον, το Firewall-1 δεν απάντησε σε καμία επεξεργασία αρχείων, η οποία ήταν απαραίτητη σε άλλα εμπορικά προϊόντα. Η γραφική διεπαφή διαμόρφωσης και διαχείρισης απλοποίησε σε μεγάλο βαθμό την εγκατάσταση και τη διαχείριση.

Η τρέχουσα τεχνολογία που χρησιμοποιείται για τείχη προστασίας ταξινομείται ως τείχη προστασίας διακομιστή μεσολάβησης πυρήνα. [46] Αυτή η τεχνολογία καθορίζει πακέτα σε πολλαπλά επίπεδα της στοίβας πρωτοκόλλου στο διακομιστή μεσολάβησης και είναι παρόμοια με το επίπεδο εφαρμογής στη χρήση διακομιστών μεσολάβησης. Η Cisco έχει εφαρμόσει

αυτήν την τεχνολογία στην ανάπτυξη ενός προϊόντος που ονομάζεται Τείχος προστασίας Centri. Αυτή η εφαρμογή χρησιμοποιεί το Στέλεχος των Windows NT, το οποίο είναι ο πυρήνας των Windows NT, 2000, 2003 και αποτελείται από τρία στοιχεία: Το πρώτο στοιχείο καταγράφει πακέτα που φθάνουν στο διακομιστή τείχους προστασίας. Στη συνέχεια, το πακέτο αναλύεται διαβάζοντας τις πληροφορίες κεφαλίδας και τα δεδομένα υπογραφής. Τόσο τα δεδομένα σχετικά με το πακέτο όσο και το ίδιο το πακέτο περνούν στο δεύτερο στάδιο. Αυτό το δεύτερο στάδιο λαμβάνει τα δεδομένα σχετικά με το πακέτο και αποφασίζει αν θα αποθέσει το πακέτο, θα αντιστοιχίσει σε μια υπάρχουσα περίοδο λειτουργίας ή θα δημιουργήσει μια νέα περίοδο λειτουργίας χρησιμοποιώντας τα δεδομένα που λαμβάνονται σχετικά με το πακέτο. [45] Εάν υπάρχει μια περιοδική περίοδος λειτουργίας, το πακέτο μεταβιβάζεται μέσω μιας προσαρμοσμένης στοίβας πρωτοκόλλου που δημιουργήθηκε ειδικά για αυτήν την περίοδο λειτουργίας, η οποία είναι μια προσαρμοσμένη εφαρμογή της προσέγγισης που γνωρίζει ευρέως μια μετάφραση διεύθυνσης δικτύου. Αυτό το τελευταίο στάδιο επιβάλλει την πολιτική ασφαλείας όπως έχει ρυθμιστεί στο αρχείο στο τελικό στάδιο, το διακομιστή μεσολάβησης πυρήνα, καθώς επιθεωρεί κάθε πακέτο. Ο διακομιστής μεσολάβησης πυρήνα αποτελείται από διακομιστές μεσολάβησης για πρωτόκολλα επιπέδου εφαρμογής όπως HTTP, FTP, Telnet και SMTP, πρωτόκολλα επιπέδου μεταφοράς όπως πρωτόκολλο μηνυμάτων ελέγχου Internet (ICMP) TCP και πρωτόκολλα UDP και επιπέδου δικτύου, όπως IP. Αυτοί οι διακομιστές μεσολάβησης μπορούν να ρυθμιστούν έτσι ώστε το δεύτερο στάδιο να καθορίζει ποια απόφαση θα λάβει σχετικά με το πακέτο. [7]

Τα τείχη προστασίας ως προϊόντα εξακολουθούν να είναι μια έγκυρη μέθοδος για την πρόληψη βασικών εισβολών. Μπορούν να αξιολογήσουν τη θέση μιας σύνδεσης, μπορούν να εμποδίσουν την επικοινωνία μεταξύ συστημάτων εάν η επικοινωνία δεν είναι δυνατή ή είναι αυτόκλητη και μπορούν να απομονώσουν συστήματα που δεν πρέπει να συνδεθούν με ένα μη ασφαλές δίκτυο. Ωστόσο, η έρευνα και η ανάπτυξη στράφηκαν σε μια νέα τεχνολογία που ονομάζεται IDS. [44]

Κεφάλαιο 2ο: «Ασφάλεια Δικτύων»

2.1. Πολιτικές Ασφάλειας Δικτύων

Βασικός παράγοντας για την σωστή ασφάλεια οποιουδήποτε δικτύου είναι η χάραξη μίας προκαθορισμένης πολιτικής που θα καθορίζει τον τρόπο με τον οποίο θα λειτουργεί αυτή. Η πολιτική αυτή (policy Security) στις μέρες μας είναι πλέον διεθνών προδιαγραφών. Υπάρχουν δηλαδή πρότυπα που μπορεί μία εταιρία ή ένας οργανισμός ν' ακολουθήσει εφαρμόζοντας στο δίκτυό του, όπως είναι το ISO 27002(update 17799) πρότυπο, που αναφέρει λεπτομερώς τα σημεία που πρέπει να καλυφθούν ώστε να πιστοποιείται η ασφάλεια δικτύου του. Κρίσιμα σημεία που χρήζουν προσοχής είναι τα ακόλουθα: [64]

- Πρώτον, ο 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.
- Δεύτερον, το άρτια οργανωμένο σύστημα ανίχνευσης επιθέσεων (Intrusion Detection System). Αυτό επιδιώκει έγκαιρα, επακριβώς και αποτελεσματικά να 8 ενημερώνει για την ύπαρξη επιθέσεων στο σύστημα και να λαμβάνει τα κατάλληλα μέτρα για, την καταρχήν, αποτροπή τους.
- Τρίτον, τα 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.
- Τέταρτον, τα πλήρη εφεδρικά (backup) συστήματα αποθήκευσης και αποκατάστασης. Αυτά λειτουργούν σε περίπτωση επιτυχούς επίθεσης από την οποία μπορεί να καταρρεύσει το δίκτυο.
- Πέμπτον, η σύγχρονη και αξιόπιστη τεχνολογία κρυπτογράφησης. Σκοπός της είναι να καταστήσει σαφώς ασφαλέστερες τις επικοινωνίες ανάμεσα σε κόμβους του εσωτερικού δικτύου, αλλά και σε αυτές που πραγματοποιούνται μέσω του διαδικτύου(Internet).[63]

2.2. Τύποι προστασίας ασφάλειας δικτύου

Οι τυποι προστασίας ασφάλειας δικτύου είναι οι εξής:

1. Τείχος προστασίας

Τα τείχη προστασίας ελέγχουν την εισερχόμενη και εξερχόμενη κίνηση στα δίκτυα, με προκαθορισμένους κανόνες ασφαλείας. Τα τείχη προστασίας εμποδίζουν την μη φιλική κίνηση και είναι απαραίτητο μέρος του καθημερινού υπολογισμού. Η Ασφάλεια Δικτύου βασίζεται σε μεγάλο βαθμό στα Τείχη προστασίας, και ιδιαίτερα στα Τείχη προστασίας επόμενης γενιάς , τα οποία επικεντρώνονται στον αποκλεισμό επιθέσεων κακόβουλου λογισμικού και επιπέδου εφαρμογής. [37]

2. Τμηματοποίηση Δικτύου

Η τμηματοποίηση δικτύου ορίζει τα όρια μεταξύ τμημάτων δικτύου όπου τα περιουσιακά στοιχεία εντός της ομάδας έχουν μια κοινή λειτουργία, κίνδυνο ή ρόλο μέσα σε έναν οργανισμό. Για παράδειγμα, η περιμετρική πύλη τμηματοποιεί ένα εταιρικό δίκτυο από το Διαδίκτυο. Οι πιθανές απειλές εκτός του δικτύου αποτρέπονται, διασφαλίζοντας ότι τα ευαίσθητα δεδομένα ενός οργανισμού παραμένουν εντός. Οι οργανισμοί μπορούν να προχωρήσουν περαιτέρω ορίζοντας πρόσθετα εσωτερικά όρια στο δίκτυό τους, τα οποία μπορούν να παρέχουν βελτιωμένη ασφάλεια και έλεγχο πρόσβασης. [35]

3. Έλεγχος Πρόσβασης

Ο έλεγχος πρόσβασης καθορίζει τα άτομα ή τις ομάδες και τις συσκευές που έχουν πρόσβαση σε εφαρμογές και συστήματα δικτύου, απορρίπτοντας έτσι την αυθαίρετη πρόσβαση και ίσως απειλές. Οι ενσωματώσεις με προϊόντα διαχείρισης ταυτότητας και πρόσβασης (IAM) μπορούν να προσδιορίσουν με σαφήνεια τις πολιτικές χρήστη και ελέγχου πρόσβασης βάσει ρόλων (RBAC) που διασφαλίζουν ότι το άτομο και η συσκευή έχουν εξουσιοδότηση πρόσβασης στο στοιχείο. [51]

4. Απομακρυσμένη πρόσβαση VPN

Το VPN παρέχει απομακρυσμένη και ασφαλή πρόσβαση σε ένα εταιρικό δίκτυο σε μεμονωμένους κεντρικούς υπολογιστές ή πελάτες, όπως τηλεργαζόμενους, χρήστες κινητής τηλεφωνίας και καταναλωτές εκτός δικτύου. Κάθε κεντρικός υπολογιστής έχει συνήθως φορτωμένο λογισμικό πελάτη VPN ή χρησιμοποιεί έναν πελάτη που βασίζεται στο web. Το απόρρητο και η ακεραιότητα των ευαίσθητων πληροφοριών διασφαλίζεται μέσω του ελέγχου

ταυτότητας πολλαπλών παραγόντων, της σάρωσης συμμόρφωσης στο τελικό σημείο και της κρυπτογράφησης όλων των μεταδιδόμενων δεδομένων. [35]

5. Πρόσβαση στο δίκτυο μηδενικής εμπιστοσύνης (ZTNA)

Το μοντέλο ασφάλειας μηδενικής εμπιστοσύνης δηλώνει ότι ένας χρήστης πρέπει να έχει μόνο την πρόσβαση και τα δικαιώματα που απαιτούνται για να εκπληρώσει τον ρόλο του. Αυτή είναι μια πολύ διαφορετική προσέγγιση από αυτή που παρέχουν οι παραδοσιακές λύσεις ασφάλειας, όπως τα VPN, που παρέχουν σε έναν χρήστη πλήρη πρόσβαση στο δίκτυο προορισμού. Η πρόσβαση στο δίκτυο μηδενικής εμπιστοσύνης (ZTNA) γνωστή και ως λύσεις περιμετρικής καθορισμένης από λογισμικό (SDP) επιτρέπει την λεπτομερή πρόσβαση στις εφαρμογές ενός οργανισμού από χρήστες που απαιτούν αυτήν την πρόσβαση για την εκτέλεση των καθηκόντων τους. [34]

6. Ασφάλεια email

Η ασφάλεια email αναφέρεται σε οποιεσδήποτε διαδικασίες, προϊόντα και υπηρεσίες που έχουν σχεδιαστεί για την προστασία των λογαριασμών και των περιεχομένων του email από εξωτερικές απειλές. Οι περισσότεροι πάροχοι υπηρεσιών email έχουν ενσωματωμένες λειτουργίες ασφαλείας email που έχουν σχεδιαστεί για να σας κρατούν ασφαλείς, αλλά αυτές μπορεί να μην είναι αρκετές για να εμποδίσουν τους εγκληματίες του κυβερνοχώρου να έχουν πρόσβαση στις πληροφορίες σας. [33]

7. Πρόληψη απώλειας δεδομένων (DLP)

Η πρόληψη απώλειας δεδομένων (DLP) είναι μια μεθοδολογία κυβερνοασφάλειας που συνδυάζει τεχνολογία και βέλτιστες πρακτικές για την πρόληψη της έκθεσης ευαίσθητων πληροφοριών εκτός ενός οργανισμού, ειδικά ρυθμιζόμενων δεδομένων όπως προσωπικά αναγνωρίσιμες πληροφορίες (PII) και δεδομένα σχετικά με τη συμμόρφωση: HIPAA, SOX, PCI DSS , και τα λοιπά.

8. Συστήματα αποτροπής εισβολής (IPS)

Οι τεχνολογίες IPS μπορούν να ανιχνεύσουν ή να αποτρέψουν επιθέσεις ασφάλειας δικτύου, όπως επιθέσεις ωμής βίας, επιθέσεις άρνησης υπηρεσίας (DoS) και εκμεταλλεύσεις γνωστών τρωτών σημείων. [50] Μια ευπάθεια είναι μια αδυναμία, για παράδειγμα, σε ένα σύστημα λογισμικού και μια εκμετάλλευση είναι μια επίθεση που αξιοποιεί αυτήν την ευπάθεια για να αποκτήσει τον έλεγχο αυτού του συστήματος. Όταν ανακοινώνεται ένα exploit, υπάρχει συχνά

ένα παράθυρο ευκαιρίας για τους εισβολείς να εκμεταλλευτούν αυτήν την ευπάθεια πριν από την εφαρμογή της ενημέρωσης κώδικα ασφαλείας. Σε αυτές τις περιπτώσεις μπορεί να χρησιμοποιηθεί ένα σύστημα αποτροπής εισβολής για να αποκλείσει γρήγορα αυτές τις επιθέσεις. [36]

9. Sandboxing

Το Sandboxing είναι μια πρακτική ασφάλειας στον κυβερνοχώρο όπου εκτελείτε κώδικας ή ανοίγεται από αρχεία σε ένα ασφαλές, απομονωμένο περιβάλλον σε μια μηχανή υποδοχής που μιμείται τα λειτουργικά περιβάλλοντα τελικού χρήστη. Το Sandboxing παρατηρεί τα αρχεία ή τον κώδικα καθώς ανοίγονται και αναζητά κακόβουλη συμπεριφορά για να αποτρέψει την είσοδο απειλών στο δίκτυο. Για παράδειγμα, κακόβουλο λογισμικό σε αρχεία όπως PDF, Microsoft Word, Excel και PowerPoint μπορεί να εντοπιστεί και να αποκλειστεί με ασφάλεια πριν τα αρχεία φτάσουν σε έναν ανυποψίαστο τελικό χρήστη.

10. Υπερκλίμακα Ασφάλεια Δικτύου

Υπερκλίμακα είναι η ικανότητα μιας αρχιτεκτονικής να κλιμακώνεται κατάλληλα, καθώς προστίθεται αυξημένη ζήτηση στο σύστημα. Αυτή η λύση περιλαμβάνει ταχεία ανάπτυξη και κλιμάκωση προς τα πάνω ή προς τα κάτω για την κάλυψη των αλλαγών στις απαιτήσεις ασφάλειας δικτύου. Με την αυστηρή ενσωμάτωση πόρων δικτύωσης και υπολογισμού σε ένα σύστημα που καθορίζεται από λογισμικό, είναι δυνατό να αξιοποιηθούν πλήρως όλοι οι διαθέσιμοι πόροι υλικού σε μια λύση ομαδοποίησης. [38]

11. Cloud Network Security

Οι εφαρμογές και ο φόρτος εργασίας δεν φιλοξενούνται πλέον αποκλειστικά εντός των εγκαταστάσεων σε ένα τοπικό κέντρο δεδομένων. Η προστασία του σύγχρονου κέντρου δεδομένων απαιτεί μεγαλύτερη ευελιξία και καινοτομία για να συμβαδίζει με τη μετάβαση του φόρτου εργασίας των εφαρμογών στο cloud. Οι λύσεις δικτύωσης που καθορίζονται από λογισμικό (SDN) και SD-WAN καθορίζονται από λογισμικό επιτρέπουν λύσεις ασφάλειας δικτύου σε ιδιωτικές, δημόσιες, υβριδικές και φιλοξενούμενες σε cloud εγκαταστάσεις Firewall-as-a-Service (FWaaS). [40]

2.3. Τύποι επιθέσεων

- Virous – Ιός : Ένας ιός είναι ένα κακόβουλο αρχείο με δυνατότητα λήψης που μπορεί να παραμείνει αδρανές και αναπαράγεται χρησιμοποιώντας προγράμματα υπολογιστή με τον δικό του κώδικα. Μόλις διαδοθεί, αυτά τα αρχεία μολύνονται και μπορούν να εξαπλωθούν από τον έναν υπολογιστή στον άλλο και να καταστρέψουν δεδομένα δικτύου.

- Worms – σκουλήκια: είναι ένα πολύ επικίνδυνο είδος εχθρικού κώδικα. Αυτά αναπαράγονται με ανεξάρτητες ευπάθειες εκμετάλλευσης στα δίκτυα. Μπορεί να επιβραδύνει τα δίκτυα υπολογιστών καταναλώνοντας το εύρος ζώνης καθώς και να επιβραδύνει την αποτελεσματικότητα του υπολογιστή σας στην επεξεργασία δεδομένων. Ένα worm είναι ένα αυτόνομο κακόβουλο λογισμικό που μπορεί να διαδοθεί και να λειτουργήσει ανεξάρτητα από άλλα αρχεία, ενώ ένας ιός χρειάζεται ένα πρόγραμμα υποδοχής για να εξαπλωθεί. [41]

- Trojan Horses – Δούρειοι ίπποι: Ο trojan είναι ένα πρόγραμμα backdoor που δημιουργεί μια είσοδο για κακόβουλους χρήστες εξασφαλίζοντας πρόσβαση στο σύστημα του υπολογιστή χρησιμοποιώντας κάτι που μοιάζει με πραγματικό πρόγραμμα, αλλά γρήγορα αποδεικνύεται επιβλαβές. Ένας ιός trojan μπορεί να διαγράψει αρχεία, να ενεργοποιήσει άλλο κακόβουλο λογισμικό που είναι κρυμμένο στο δίκτυο του υπολογιστή σας, όπως έναν ιό και να κλέψει πολύτιμα δεδομένα. Οι Δούρειοι Ίπποι κατατάσσονται σε διάφορες κατηγορίες ανάλογα με τη ζημιά που προκαλούν ή με τον τρόπο που παραβιάζουν ένα σύστημα:

    1) Δούρειος Ίππος απομακρυσμένης πρόσβασης: επιτρέπει τη μη εξουσιοδοτημένη απομακρυσμένη πρόσβαση.
    2) Καταστροφικός Δούρειος Ίππος: καταστρέφει ή διαγράφει τα αρχεία.
    3) Δούρειος Ίππος απενεργοποίησης λογισμικού ασφαλείας: σταματά ολα τα προγράμματα προστασίας από ιούς και τα τείχη προστασίας.
    4) Επιθέσεις άρνησης υπηρεσίων (Denial of Service,DoS).
    5) Αποστολή e-mail
    6) URL Trojan: Εεπιτρέπει στον υπολογιστή να συνδεθεί στο διαδίκτυο μόνο μέσω μίας πολυ ακριβής σύνδεσης. [40]

- Λογισμικό κατασκοπείας: Όπως προδίδει το όνομά του, το λογισμικό κατασκοπείας είναι ένας ιός υπολογιστή που συλλέγει πληροφορίες για ένα άτομο ή οργανισμό χωρίς τη ρητή γνώση τους και μπορεί να στείλει τις πληροφορίες που συλλέγονται σε τρίτους χωρίς τη συγκατάθεση του καταναλωτή.
- Adware: Μπορεί να ανακατευθύνει τα αιτήματα αναζήτησής σας σε ιστότοπους διαφήμισης και να συλλέγει δεδομένα μάρκετινγκ σχετικά με εσάς, έτσι ώστε να εμφανίζονται προσαρμοσμένες διαφημίσεις με βάση το ιστορικό αναζήτησης και αγορών σας.
- Ransomware: Αυτός είναι ένας τύπος trojan cyberware που έχει σχεδιαστεί για να κερδίζει χρήματα από τον υπολογιστή του ατόμου ή του οργανισμού στον οποίο είναι εγκατεστημένο κρυπτογραφώντας δεδομένα έτσι ώστε να μην μπορούν να χρησιμοποιηθούν, εμποδίζοντας την πρόσβαση στο σύστημα του χρήστη.

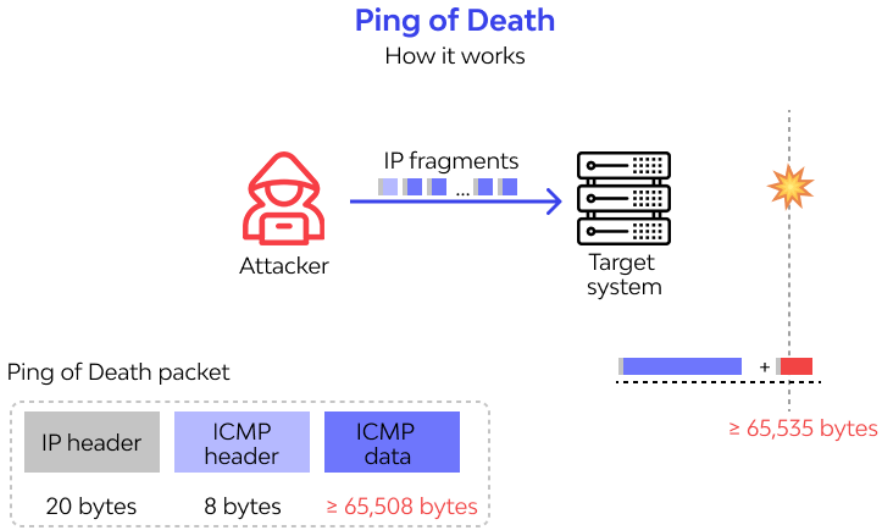
2.4. Μέθοδοι επιθέσεων

Denial of Service: Επιθέσεις άρνησης υπηρεσιών (DOS), είναι ένας συνεχής κίνδυνος για τον ιστοτοπο. Το DoS έχει λάβει αυξημένη προσοχή καθώς μπορεί να οδηγήσει σε σοβαρή απώλεια εσόδων, εάν ένας ιστότοπος αποσυνδεθεί για μεγάλο χρονικό διάστημα. Ο υπολογιστής – θύμα για ένα χρονικό διάστημα δεν είναι σε θέση να εξυπηρετεί αιτήσεις πελατών(clients) εξαιτίας του τεράστιου πλήθους εικονικών αιτήσεων που δέχεται από τον επιτιθέμενο. Υπάρχουν πολλά είδη DoS , πολλά από τα όποια εκμεταλλεύονται εγγενείς αδυναμίες του TCP/IP.

Παρακάτω θα δούμε 5 απο τα πιο γνωστά είδη επιθέσεων (DoS):

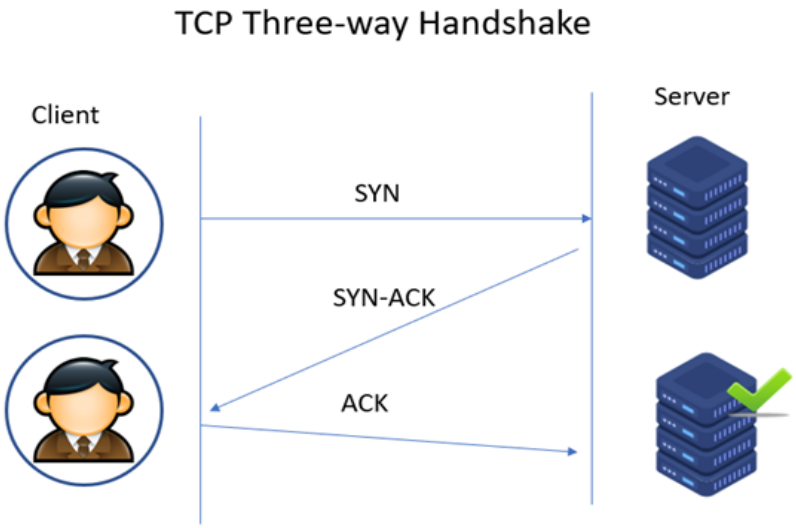
1) Ping of Death: Μια επίθεση ping of death ("POD") περιλαμβάνει την αποστολή πολλαπλών εσφαλμένων ή κακόβουλων ping σε έναν υπολογιστή. Το μέγιστο μήκος πακέτου ενός πακέτου IP (συμπεριλαμβανομένης της κεφαλίδας) είναι 65.535 byte. Ωστόσο, το επίπεδο σύνδεσης συνήθως θέτει όρια στο μέγιστο μέγεθος πλαισίου - για παράδειγμα 1500 byte σε ένα δίκτυο Ethernet. Σε αυτήν την περίπτωση, ένα μεγάλο πακέτο IP χωρίζεται σε πολλαπλά πακέτα IP (γνωστά ως fragments) και στον κεντρικό υπολογιστή του παραλήπτη επανασυναρμολογεί τα τμήματα IP σε ολόκληρο το πακέτο. Σε σενάριο Ping of Death, μετά από κακόβουλο χειρισμό του περιεχομένου του τμήματος, ο παραλήπτης καταλήγει με ένα πακέτο IP που είναι μεγαλύτερο από 65.535 byte όταν επανασυναρμολογηθεί. Αυτό μπορεί να υπερχειλίσει τη μνήμη buffer που

έχει εκχωρηθεί για το πακέτο, προκαλώντας άρνηση υπηρεσίας για νόμιμα πακέτα.[59]



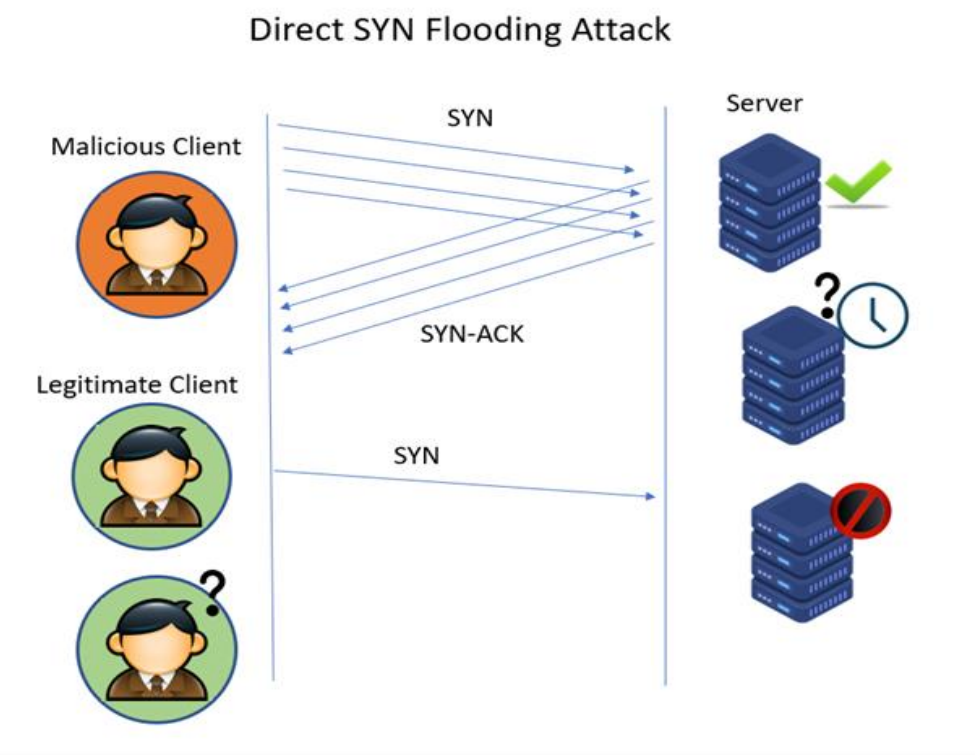
Εικόνα 2.1 Πως λειτουργεί το Ping of Death

2) SYN flood Attack: Μια επίθεση DDoS SYN flood εκμεταλλεύεται μια γνωστή αδυναμία στην ακολουθία σύνδεσης TCP (την "τριμερή χειραψία"), όπου ένα αίτημα SYN για την εκκίνηση μιας σύνδεσης TCP με έναν κεντρικό υπολογιστή πρέπει να απαντηθεί με απαντήσεις SYN-ACK από αυτόν τον κεντρικό υπολογιστή και στη συνέχεια επιβεβαιώνεται από μια απάντηση ACK από τον αιτούντα.



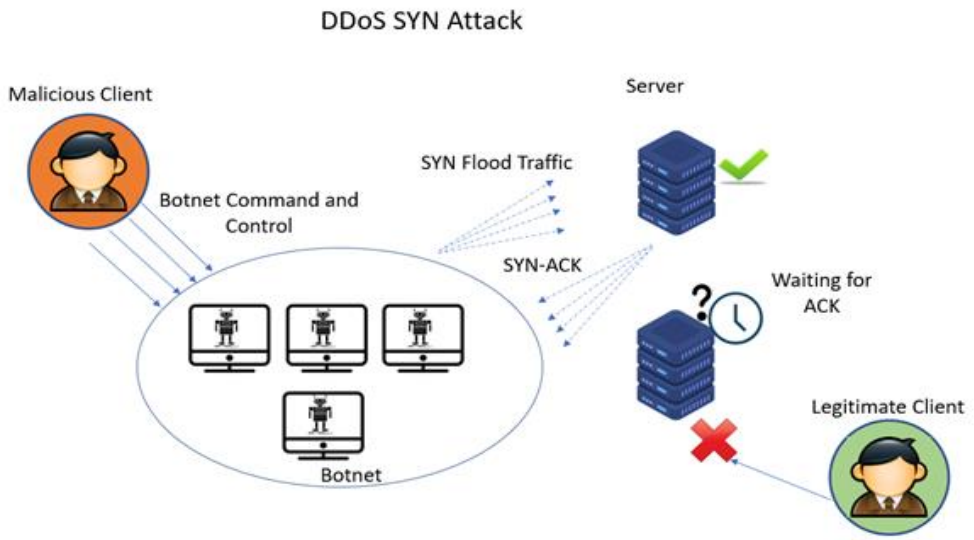
Εικόνα 2.2 Τριμερή χειραψία TCP

Σε ένα σενάριο SYN flood, ο αιτών στέλνει πολλαπλά αιτήματα SYN, αλλά είτε δεν ανταποκρίνεται στην απόκριση SYN-ACK του κεντρικού υπολογιστή είτε στέλνει τα αιτήματα SYN από μια πλαστογραφημένη διεύθυνση IP. Είτε έτσι είτε αλλιώς, το σύστημα κεντρικού υπολογιστή συνεχίζει να περιμένει για επιβεβαίωση για κάθε ένα από τα αιτήματα, δεσμεύοντας πόρους έως ότου δεν μπορούν να πραγματοποιηθούν νέες συνδέσεις και τελικά οδηγεί σε άρνηση υπηρεσίας.[59]



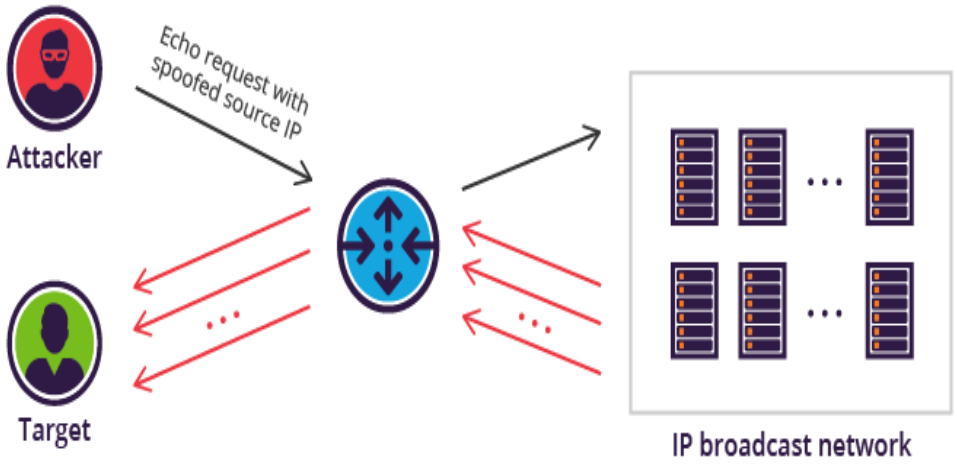
Εικόνα 2.3 Άμεση επίθεση SYN flood

3) DDoS (Distributed Denial of Service) SYN attack: Σε αυτή την παραλλαγή της επίθεσης SYN flood, ο διακομιστής-θύμα λαμβάνει ταυτόχρονα πακέτα SYN από πολλούς μολυσμένους υπολογιστές υπό τον έλεγχο του επιτιθέμενου. Αυτός ο συνδυασμός των υποκλοπή μηχανημάτων ονομάζεται botnet.Οπως βλεπουμε στην εικόνα 2.4.



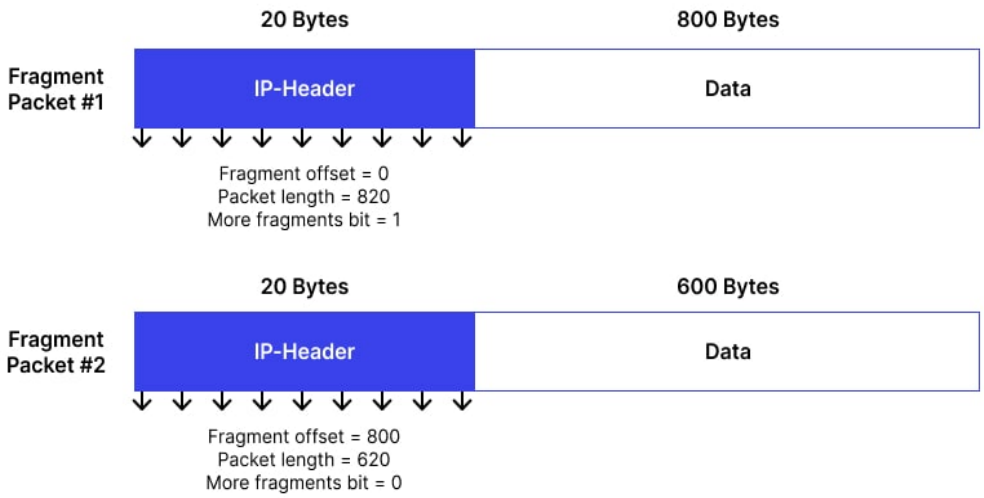
Εικόνα 2.4 DDOS SYN Attack

4) Smurf Attack: Η επίθεση smurf πραγματοποιείται με τη χρήση του πρωτοκόλλου ICMP. Σε κανονικές συνθήκες, ο κεντρικός υπολογιστής A στέλνει ένα μήνυμα αίτησης echo στον κεντρικό υπολογιστή B και τότε ο B στέλνει ένα μήνυμα απάντησης echo στον A. Όταν συμβαίνει μια επίθεση smurf, ο κεντρικός υπολογιστής A παραποιεί τη διεύθυνση IP χρησιμοποιώντας τον κεντρικό υπολογιστή C και στη συνέχεια στέλνει ένα μήνυμα αίτησης echo σε μια διεύθυνση εκπομπής, έτσι ώστε ο κεντρικός υπολογιστής C να λαμβάνει όλα τα μηνύματα απάντησης echo. Ως αποτέλεσμα, οι συνδέσεις και οι δρομολογητές προς τον υποδοχέα C μπορεί να φρακάρουν από την μεγάλη κυκλοφορία και ο C δεν μπορεί να λάβει αιτήματα από άλλους χρήστες. Η επίθεση smurf μπορεί να ανιχνευθεί εύκολα παρατηρώντας μια συμπεριφορά κίνησης κατά την οποία αποστέλλεται μεγάλος αριθμός απαντήσεων echo σε ένα συγκεκριμένο σύστημα χωρίς αίτημα echo από το σύστημα-θύμα.[59]



Εικόνα 2.5 Smurf Attack

5) Teardrop Attack: Ο επιτιθέμενος εκμεταλλεύεται αδυναμίες στην ανασυγκρότηση των πακέτων IP. Όταν ένα τέτοιο πακέτο αποστέλλεται στο διαδίκτυο, ενδέχεται να ταξιδεύει τεμαχισμένο σε επιμέρους μικρότερα τμήματα. Κάθε τμήμα περιλαμβάνει στην κεφαλή του ένα πεδίο, όπου περιγράφεται η θέση του στο αρχικό, πακέτο IP. Ο θύτης χρησιμοποιεί ένα πρόγραμμα, που ονομάζεται " Teardrop", το οποίο τεμαχίζει πακέτα IP σε τμήματα με λανθασμένες πληροφορίες στο πεδίο αυτό. Όταν ο υπολογιστής – στόχος προσπαθήσει να συναρμολογήσει τα "παραπλανητικά" αυτά τμήματα, θα κολλήσει ή θα επανεκκινήσει, εκτός και αν ο διαχειριστής συστήματος έχει φροντίσει να αναβαθμίσει το λειτουργικό με το κατάλληλο patch που διορθώνει το πρόβλημα.[60]



Εικόνα 2.6 teardrop attack

2.5. Κακόβουλοι χρηστες «hackers»

Είναι ασφαλές να υποθέσουμε ότι, στην εποχή του Διαδικτύου, όλοι οι οργανισμοί και οι υπηρεσίες θα στοχοποιηθούν από κακόβουλους χάκερ αργά ή γρήγορα. Το θέμα δεν είναι αν, αλλά το πότε. Πώς θα μπορούσε να οριστεί εννοιολογικά το Hacking, τέλος πάντων; [44]

Το «hacking», που προέρχεται από μια γερμανική λέξη που σημαίνει «κόβω σε κομμάτια», είναι η διαδικασία συλλογής πληροφοριών (ή οτιδήποτε, πραγματικά) μαζί με έναν νέο τρόπο που οδηγεί σε κάτι ενδιαφέρον ή χρήσιμο. Σε ένα πλαίσιο υπολογιστή, η λέξη προήλθε με μια θετική χροιά - για παράδειγμα, ο Steve Wozniak, ένας από τους αρχικούς ιδρυτές της Apple, ήταν ένας εξαιρετικός χάκερ.

Σήμερα, ο όρος «χάκερ» χρησιμοποιείται πιο συχνά για να περιγράψει κάποιον που ανακαλύπτει και εκμεταλλεύεται μια αδυναμία ή ευπάθεια του συστήματος υπολογιστή. Οι χάκερ χρησιμοποιούν τρωτά σημεία για να αποκλείσουν την πρόσβαση στο σύστημα, να συλλέξουν πληροφορίες ή να αποκτήσουν πρόσβαση σε περισσότερους υπολογιστές σε ένα δίκτυο.

Εικόνα 2.7 κακόβουλοι χρήστες (hackers)

Αυτό δεν σημαίνει ότι οι χάκερ είναι όλοι «κακοί». Στην πραγματικότητα, υπάρχει ένα ηθικό επάγγελμα hacking γνωστό ως δοκιμή διείσδυσης .Δεν είναι όλοι οι χάκερ το ίδιο. Υπάρχουν διάφοροι τύποι χάκερ. Ακολουθούν μερικοί από τους πιο συνηθισμένους όρους που χρησιμοποιούνται για να περιγράψουν τους χάκερ και τι κάνουν: [46]

- Άσπρο καπέλο

Οι χάκερ λευκού καπέλου λειτουργούν ηθικά ως ελεγκτές διείσδυσης. Έχουν πλήρη, συμβατική άδεια να προσπαθήσουν να παραβιάσουν ένα σύστημα και να λειτουργήσουν νόμιμα. Στόχος τους είναι να βρουν τρωτά σημεία του συστήματος και να βελτιώσουν την ασφάλεια του συστήματος.

- Μαύρο καπέλο

Αυτοί οι χάκερ είναι οι τυπικοί χάκερ που φορούν κουκούλα τα μεσάνυχτα που απεικονίζονται στα μέσα ενημέρωσης. Λειτουργούν παράνομα και εκμεταλλεύονται τα συστήματα για κάποιο προσωπικό όφελος.

- Γκρι καπέλο

Χάκερ γκρι καπέλων λειτουργούν στον φράχτη. Τις περισσότερες φορές, χακάρουν με καλές προθέσεις, αλλά μπορεί να μην είχαν προσεγγίσει το hack με έναν εντελώς ηθικό ή νόμιμο τρόπο.

Εικόνα 2.8 black vs grey vs white hat hackers

2.5.1. Γιατί οι άνθρωποι χακάρουν

Το hacking έχει ως επί το πλείστον μια κακή χροιά, αλλά τα κίνητρα των χάκερ ποικίλλουν σε όλο το μαύρο, λευκό και γκρι φάσμα. Εδώ είναι τα πιο κοινά κίνητρα πίσω από τους χάκερ.

- Γρήγορα χρήματα

Οι χάκερ συχνά παρακινούνται από την απόκτηση κλεμμένων στοιχείων πιστωτικής κάρτας ή την πώληση παραβιασμένων πληροφοριών στο διαδίκτυο. [35]

- Χακτιβισμός

Χακτιβισμός είναι η χρήση τεχνικών πειρατείας για την αξιοποίηση του πολιτικού ακτιβισμού. Οι hacktivists συχνά χειραγωγούν ιστότοπους και δίκτυα ως μορφή διαμαρτυρίας. Αυτό συνήθως μοιάζει με επίθεση κατανεμημένης άρνησης υπηρεσίας (DDoS), η οποία διακόπτει την πρόσβαση στο δίκτυο. Οι Anonymous είναι μια διάσημη ομάδα χακτιβιστών.

- Εθνική Ασφάλεια/Κυβερνοπόλεμος

Το Stuxnet είναι ένα ευρέως γνωστό παράδειγμα στρατηγικής hacking που υποστηρίζεται από την εθνική ασφάλεια. Το Stuxnet είναι ένα worm υπολογιστή που επιτέθηκε σε πυρηνικές εγκαταστάσεις του Ιράν. Το worm αυτό εικάζεται ότι είναι μια κοινή προσπάθεια μεταξύ αμερικανικών και ισραηλινών υπηρεσιών πληροφοριών. Τα εθνικά διαδικτυακά hacks τείνουν να είναι εξαιρετικά επιτυχημένα, καθώς οι ομάδες τους έχουν τους πόρους και την υπομονή να βρουν τρωτά σημεία και να τα εκμεταλλευτούν.

- Βελτίωση Συστημάτων Ασφαλείας

Όπως αναφέρθηκε προηγουμένως, οι ελεγκτές διείσδυσης ή τα λευκά καπέλα παραβιάζουν συστήματα για να δοκιμάσουν τα τρωτά σημεία για να βελτιώσουν την ασφάλεια. [48]

- Άλλοι λόγοι

Πολλοί χάκερ χακάρουν απλώς επειδή μπορούν. Για μερικούς ανθρώπους, το hacking είναι σαν ένα χόμπι - όπως συμβαίνει με τις περισσότερες επιδιώξεις, είναι ένας άλλος λόγος για να συνδεθείτε με μια κοινότητα ομοϊδεατών ατόμων.

2.5.2. Τύποι των hacks

Οι στρατηγικές hacking κατατασσόνται σε δύο κατηγορίες, ανεξάρτητα από το τι απόχρωση είναι το καπέλο ενός χάκερ.

- Κατηγορία 1: Zero-Day

Αυτή η κατηγορία hacks είναι ευπάθειες που δεν είχαν ξαναδεί, γνωστές και ως τρωτά σημεία zero-day. Είναι τα πιο επιζήμια γιατί δεν έχουν μπαλώσει. Οι ομάδες ασφαλείας δεν ξέρουν πώς να αμυνθούν εναντίον τους και συχνά δεν συνειδητοποιούν καν ότι ένα σύστημα έχει παραβιαστεί. Οι χάκερ πίσω από αυτές τις επιθέσεις είναι πολύ εξειδικευμένοι, τρομακτικοί και έξυπνοι χάκερ.

Κυρίως, οι χάκερ «σώζουν» αυτές τις επιθέσεις για κάτι που έχει τεράστια οικονομική απόδοση. Οι επιθέσεις Zero-day συνήθως πραγματοποιούνται σε πολυεθνικές επιχειρήσεις ή εθνικά συστήματα ασφαλείας. [49]

Το Heartbleed ήταν ένα μηδενικό exploit που δημοσιοποιήθηκε το 2014 εναντίον διακομιστών Linux. Συγκλονιστικά, δεν υπάρχει τρόπος να γνωρίζουμε πόσοι άνθρωποι γνώριζαν και χρησιμοποίησαν το exploit πριν δημοσιοποιηθεί. Ο κώδικας που εκμεταλλεύτηκε η Heartbleed εισήχθη τρία χρόνια πριν δημοσιοποιηθούν τα τρωτά σημεία του.

- Κατηγορία 2: Όλα τα άλλα

Η πλειοψηφία των σημερινών hacks χρησιμοποιούν κώδικα που έχει γραφτεί από κάποιον άλλο και έχει κυκλοφορήσει στη φύση. Αυτό το είδος χάκερ αποκαλείται συχνά script kiddie, δηλαδή χρησιμοποιούν προϋπάρχον λογισμικό για να εξαπολύσουν επιθέσεις και δεν έχουν μεγάλη, εώς καμία, εξειδίκευση στον προγραμματισμό. [13]

Μια διαδικασία σεναρίου kiddie μοιάζει με αυτό:

- Πραγματοποιεί λήψη ενός κακόβουλου κώδικα ή σεναρίου
- Το στοχεύει σε κάποιον ή κάτι στο διαδίκτυο που δεν του αρέσει

Αυτά τα hacks είναι αρκετά εύκολο να αμυνθούν, εάν ένας υπολογιστής ενημερωθεί.

Ένας από τους πιο συνηθισμένους τρόπους δημιουργίας επιθέσεων είναι, παρακολουθώντας τις ενημερώσεις ασφαλείας για τα Windows, παρατηρώντας τα τρωτά σημεία που έκλεισαν και εισβάλλοντας σε αυτά τα τρωτά σημεία σε διακομιστές που δεν έχουν ενημερωθεί εγκαίρως. [14]

Οι οργανισμοί ασφαλείας είναι πολύ καλοί στο να προωθούν ενημερώσεις ασφαλείας μόλις ανακαλυφθούν οι εισβολές και κυκλοφορήσει ο κώδικας. Εάν ένα παιδί μπορεί να βρει ένα σενάριο στο Διαδίκτυο, το ίδιο μπορεί να κάνει και ένας επαγγελματίας ασφαλείας.

Η κοινωνική μηχανική , η πρακτική της χειραγώγησης των ανθρώπων για την αποκάλυψη πληροφοριών, είναι μακράν η ευκολότερη μέθοδος απόκτησης πρόσβασης σε ένα σύστημα υπολογιστή. Οι χρήστες μπορεί να μην δίνουν σκόπιμα τον κωδικό πρόσβασής τους, αλλά κάποιες γνώσεις ψυχολογίας και ένα άγγιγμα τεχνασμάτων είναι υπεραρκετά για τους χάκερ για να αποκτήσουν αυτό που θέλουν. Αυτό μπορεί να φαίνεται υπερβολή αλλά ένας εκπληκτικός αριθμός ατόμων δίνει πρόθυμα τις πληροφορίες τους αφού δουν ένα καλά διαμορφωμένο email. [12]

Πριν από μερικά χρόνια, ένας χάκερ έκλεψε το αναγνωριστικό Twitter @N (το οποίο προφανώς εκτιμάται στα 50.000 $) μέσω κάποιων έξυπνων τηλεφωνημάτων. Βασικά, ο χάκερ κάλεσε το Paypal και χρησιμοποίησε τακτικές κοινωνικής μηχανικής για να αποκτήσει τα τέσσερα τελευταία ψηφία της πιστωτικής κάρτας του θύματος. Στη συνέχεια τηλεφώνησε στην εταιρεία φιλοξενίας ιστοσελίδων του θύματος, GoDaddy, και χρησιμοποίησε τα στοιχεία της πιστωτικής κάρτας για να επαναφέρει τους κωδικούς πρόσβασης. Στη συνέχεια, ο χάκερ κράτησε όμηρο τον επιχειρηματικό ιστότοπο του θύματος έως ότου το θύμα αναγκάστηκε να εγκαταλείψει το @N.

Η πειρατεία που βασίζεται σε προγραμματισμό είναι σημαντικά πιο δύσκολη, καθώς απαιτεί μεγάλη προσπάθεια για την εύρεση εκτεθειμένων τρωτών σημείων. Οι χάκερ εκμεταλλεύονται ευάλωτο κώδικα για να αποκτήσουν πλήρη δικαιώματα διαχείρισης του συστήματος.

2.5.3. Πως οι οργανισμοί μετριάζουν τις εισβολές

Οι οργανισμοί που εφαρμόζουν καλή ασφάλεια αποθηκεύουν σημαντικές πληροφορίες χρηστών σε διαφορετικά σημεία κάτω από διαφορετικά πρωτόκολλα ασφαλείας. Με αυτόν τον τρόπο, όταν οι χάκερ μπαίνουν σε έναν υπολογιστή με λίστα ονομάτων χρήστη, δεν λαμβάνουν απαραίτητα άλλα προσωπικά στοιχεία, όπως πιστωτικές κάρτες. Τα τείχη προστασίας βοηθούν επίσης στην προστασία ενός δικτύου από κυβερνοεπιθέσεις. [15]

Οι οργανισμοί μπορούν να δημιουργήσουν συστήματα παρακολούθησης δικτύου για να συλλάβουν μια εισβολή σε εξέλιξη. Το σύστημα μπορεί να παραβλέπει τις πρώτες κινήσεις, αλλά μπορεί να συλλάβει τους χάκερ να κατεβάζουν πληροφορίες ή να διαπράττουν άλλες κακόβουλες δραστηριότητες. Η ομάδα ασφαλείας της εταιρείας μπορεί στη συνέχεια να επέμβει και να μετριάσει τις ζημιές. Οι οργανισμοί μπορούν επίσης να χρησιμοποιήσουν εργαλεία ανακάλυψης δεδομένων για να βρουν αποδεικτικά στοιχεία πρώιμης παραβίασης δεδομένων ή πειρατείας σε ιστότοπους όπως το Pastebin και ο Dark Web.

Οι ασφαλείς εταιρείες εκπαιδεύουν επίσης το προσωπικό τους σχετικά με τις βέλτιστες πρακτικές ασφάλειας , όπως πρακτικές κωδικών πρόσβασης, έλεγχο ταυτότητας 2 παραγόντων και πώς να αναγνωρίζουν μηνύματα phishing ή social engineering. Εκδίδουν επίσης συμβουλές σε περίπτωση ύποπτης δραστηριότητας.

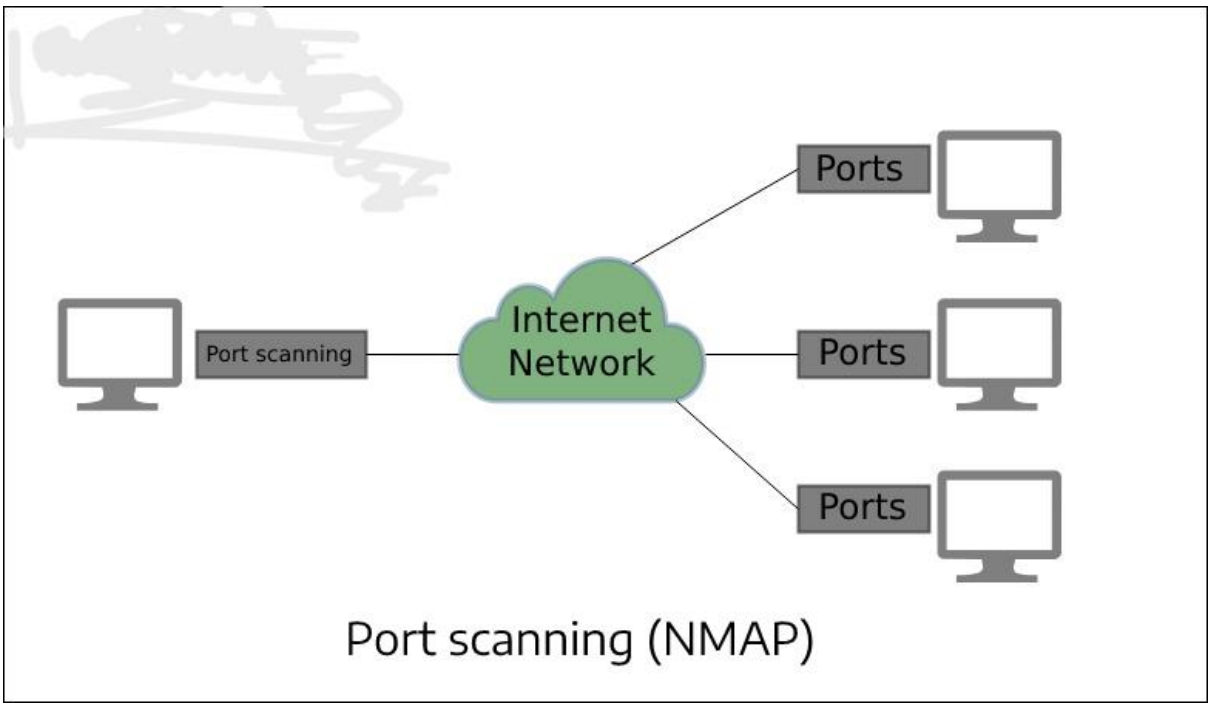
2.5.4 Τι συμβαίνει όταν οι οργανισμοί δεν προστατεύουν σωστά τα δεδομένα τους;

Η Adobe και η Sony είναι καλά παραδείγματα μεγάλων εταιρειών που παραβιάστηκαν λόγω έλλειψης στρατηγικών ασφαλείας. Η Adobe αμέλησε να κρυπτογραφήσει και να αποθηκεύσει σωστά τις πληροφορίες των χρηστών. Όταν το σύστημά τους παραβιάστηκε, χρειάστηκε πολύ λίγη προσπάθεια για τους χάκερ να αντιστρέψουν τους κωδικούς πρόσβασης. Ερευνητές ασφαλείας είπαν ότι η εταιρεία «θα πρέπει να κρεμάσει το κεφάλι της από ντροπή», σχετικά με τα συστήματα ασφαλείας της. Η Sony απέτυχε επίσης να δημιουργήσει επαρκή ασφάλεια του συστήματος, αποτυγχάνοντας να ανιχνεύσει περισσότερα από 100 terabytes απώλειας πληροφοριών από τους διακομιστές της. [11]

Οι χάκερ αναζητούν οποιαδήποτε πολύτιμα δεδομένα. Αυτό μπορεί να είναι μια ποικιλία πραγμάτων όπως στοιχεία προσωπικής ταυτοποίησης, οικονομικές πληροφορίες, κωδικός, διαβαθμισμένα έγγραφα και πολλά άλλα. Αυτές οι πληροφορίες συχνά πωλούνται, χρησιμοποιούνται για εκβιασμό ή χρησιμοποιούνται για παρενόχληση και εκφοβισμό ατόμων. [13]

2.6. Σάρωση θυρών «Port scanning»

Σάρωση θυρών είναι το όνομα της τεχνικής που χρησιμοποιείται για τον εντοπισμό των διαθέσιμων θυρών και υπηρεσιών σε κεντρικούς υπολογιστές σε ένα δίκτυο. Οι μηχανικοί ασφαλείας το χρησιμοποιούν μερικές φορές για να σαρώνουν υπολογιστές για ευπάθειες και οι χάκερ το χρησιμοποιούν επίσης για να στοχεύουν θύματα. Μπορεί να χρησιμοποιηθεί για την αποστολή αιτημάτων σύνδεσης σε υπολογιστές-στόχους και στη συνέχεια για την παρακολούθηση των θυρών. Οι σαρωτές δικτύου δεν βλάπτουν στην πραγματικότητα τους υπολογιστές, αλλά υποβάλλουν αιτήματα παρόμοια με αυτά που αποστέλλουν οι ανθρώπινοι χρήστες που επισκέπτονται ιστότοπους ή συνδέονται σε άλλους υπολογιστές χρησιμοποιώντας εφαρμογές όπως το πρωτόκολλο απομακρυσμένης επιφάνειας εργασίας (RDP) και το Telnet. Η σάρωση θύρας πραγματοποιείται με την αποστολή πακέτων ICMP echo-request με συγκεκριμένες σημαίες που έχουν οριστεί στις επικεφαλίδες των πακέτων και υποδεικνύουν τον τύπο του μηνύματος που μεταδίδεται: ο τύπος 8 υποδεικνύει ότι το αίτημα είναι ένα πακέτο echo-reply με τη διεύθυνση IP προέλευσης ως τον αποκρινόμενο υπολογιστή, ενώ ο τύπος 0 υποδεικνύει ότι δεν αναμένεται απάντηση από τον αποκρινόμενο υπολογιστή. Ένα δημοφιλές εργαλείο port scanning ανοιχτού κώδικα είναι το Nmap.[35]



Εικόνα 2.9 Σάρωση θυρών

Για να προστατεύσετε το δίκτυό σας από σαρώσεις θυρών, είναι σημαντικό να κατανοήσετε τους διαφορετικούς τύπους σαρώσεων θυρών που χρησιμοποιούνται από τους χάκερ.

Τύποι σαρώσεων θυρών:

- Vanilla: Ο σαρωτής προσπαθεί να συνδεθεί και στις 65. 535 θύρες). Ο σαρωτής αναζητά ανοικτές θύρες UDP
- Sweep: Ο σαρωτής εντοπίζει μια πανομοιότυπη θύρα σε πάνω από έναν υπολογιστή για να διαπιστώσει ποιος υπολογιστής είναι ενεργός
- FTP Bounce: Ο σαρωτής περνάει από έναν διακομιστή FTP για να αποκρύψει την πηγή
- Stealth: Ο σαρωτής κλειδώνει τα αρχεία του σαρωμένου υπολογιστή

2.7. Ασφάλιση δικτύου με το σημείο ελέγχου

Η Ασφάλεια Δικτύου είναι ζωτικής σημασίας για την προστασία των δεδομένων και των πληροφοριών των πελατών. Διατηρεί ασφαλή τα κοινά δεδομένα, προστατεύει από ιούς και βοηθά στην απόδοση του δικτύου μειώνοντας τα γενικά έξοδα και τις δαπανηρές απώλειες από παραβιάσεις δεδομένων. Επιπλέον μπορεί να εξοικονομήσει χρήματα για τις επιχειρήσεις μακροπρόθεσμα, καθώς υπάρχει λιγότερος χρόνος διακοπής λειτουργίας από κακόβουλους χρήστες ή ιούς. [41]

Κεφάλαιο 3ο: «Συστήματα Ανίχνευσης Εισβολών»

3.1. Εισαγωγή στα Συστήματα Ανίχνευσης Εισβολών (IDS)

Στόχος του Συστήματος Ανίχνευσης Εισβολής (IDS) είναι η παρακολούθηση των στοιχείων του δικτύου για τον εντοπισμό ανώμαλης συμπεριφοράς και κατάχρησης. Ένας τέτοιος στόχος έχει αναγνωριστεί ως σημαντικός εδώ και σχεδόν είκοσι χρόνια, αλλά μόνο πρόσφατα σημειώθηκε δραματική αύξηση της δημοτικότητας και της ενσωμάτωσης στις συνολικές υποδομές ασφάλειας των νέων.

Η πρώτη αναγνωρισμένη εργασία IDS δημοσιεύθηκε το 1980 από τον James Anderson, με τίτλο *«παρακολούθηση απειλών ασφάλειας υπολογιστών»*. Γράφτηκε για έναν κυβερνητικό οργανισμό των ΗΠΑ και εισήγαγε την ιδέα ότι τα μονοπάτια ελέγχου περιείχαν ζωτικής σημασίας πληροφορίες που θα μπορούσαν να χρησιμοποιηθούν για την παρακολούθηση και την κατανόηση της συμπεριφοράς των χρηστών. Αυτή η εικόνα των δεδομένων ελέγχου και η σημασία τους οδήγησαν σε έντονες βελτιώσεις στα υποσυστήματα ελέγχου σχεδόν κάθε λειτουργικού συστήματος. Το έργο του ήταν η αρχή του IDS. Το έτος 1983, η Dr. Dorothy Denning, που εργάζεται ως μέρος του *Stanford Research Institute International*, άρχισε να εργάζεται σε ένα έγγραφο παρακολούθησης, αργότερα με τίτλο *«Ένα μοντέλο ανίχνευσης εισβολής»*. [34]

Η μελέτη ανέλυσε τα ελεγκτικά εργαλεία από κυβερνητικούς υπολογιστές κεντρικού υπολογιστή και δημιούργησε προφίλ χρηστών με βάση τις δραστηριότητες που καταγράφηκαν. Αργότερα, ο *Dr.Denning* βοήθησε στην ανάπτυξη του συστήματος εμπειρογνωμόνων ανίχνευσης εισβολής *(IDES)* που χρησιμοποιήθηκε ως θεμέλιο για την ανάπτυξη τεχνολογίας *IDS*. Στο πλαίσιο της μελέτης, το Stanford Research Institute ανέπτυξε επίσης ένα μέσο παρακολούθησης και ανάλυσης δεδομένων ελέγχου από χρήστες στο ARPANET (σύντομα θα μετονομαστεί σε Διαδίκτυο). Χρησιμοποιώντας το ερευνητικό και αναπτυξιακό της έργο στο Stanford Research Institute, η *Dr. Denning* δημοσίευσε το αποφασιστικό έργο, *«Ένα μοντέλο ανίχνευσης εισβολής»*, το οποίο αποκάλυψε την παραπληροφόρηση για την ανάπτυξη του εμπορικού συστήματος ανίχνευσης εισβολής. Η εργασία της ήταν η βάση για το μεγαλύτερο μέρος της εργασίας στο IDS που ακολούθησε. Η εργασία δημοσιεύθηκε το 1987 από το Ινστιτούτο Ηλεκτρολόγων μηχανικών και Ηλεκτρονικών Μηχανικών (IEEE). [43]

Η πρώτη εφαρμογή του μοντέλου ανίχνευσης εισβολής ταξινομήθηκε ως κεντρικός υπολογιστής IDS. Το IDS που βασίζεται στον κεντρικό υπολογιστή παρακολουθεί απευθείας τους υπολογιστές στους οποίους εκτελούνται, συχνά μέσω στενής επανένταξης με το λειτουργικό σύστημα. Αυτή η ενοποίηση έχει ένα κόστος, καθώς το σύστημα παρακολουθεί τους χρήστες ακριβώς όπως παρακολουθούν εξωτερικούς χρήστες και ο αριθμός των υπολογιστών συχνά καθιστά δυνατή την προστασία κάθε υπολογιστή στο δίκτυο χρησιμοποιώντας ένα αναγνωριστικό που βασίζεται στον κεντρικό υπολογιστή.

Μια άλλη διάκριση στην υλοποίηση ids που βασίζεται στον κεντρικό υπολογιστή είναι ότι επειδή η κυκλοφορία δικτύου παρακολουθείται συνεχώς, η απαιτούμενη ισχύς επεξεργασίας έχει συχνά αρνητικό αντίκτυπο στη λειτουργική απόδοση του υπολογιστή.

3.2. Αναγνωριστικά που βασίζονται στον κεντρικό υπολογιστή «host-based identifiers»

Ένα IDS θα πρέπει να ανιχνεύσει μη φυσιολογική χρήση του συστήματος. Επομένως, οι παραβιάσεις ασφαλείας θα μπορούσαν να εντοπιστούν από μη φυσιολογικά πρότυπα χρήσης του συστήματος.

Ακολουθούν παραδείγματα παραβιάσεων ασφαλείας που θα ήταν στα μοτίβα μη φυσιολογικής χρήσης.

• Απόπειρα διάρρηξης: Κάποιος που προσπαθεί να εισέλθει σε ένα σύστημα μπορεί να δημιουργήσει ένα ασυνήθιστα υψηλό ποσοστό παραβιάσεων κωδικού πρόσβασης σε σχέση με έναν μόνο λογαριασμό ή το σύστημα στο σύνολό του.

• Μεταμφιεσμένη ή επιτυχής διάρρηξη: Κάποιος που συνδέεται σε ένα σύστημα μέσω μη εξουσιοδοτημένου λογαριασμού και κωδικού πρόσβασης μπορεί να έχει αδιάφορο χρόνο σύνδεσης, ή τον τύπο σύνδεσης με αυτόν του νόμιμου χρήστη του λογαριασμού. Η συμπεριφορά του μη εξουσιοδοτημένου χρήστη μπορεί να διαφέρει σημαντικά από εκείνη του νόμιμου χρήστη. Συγκεκριμένα, μπορεί να περάσει το μεγαλύτερο μέρος του χρόνου του περιηγούμενος σε καταλόγους και να εκτελέσει εντολές κατάστασης συστήματος, όπου ως νόμιμος χρήστης μπορεί να επικεντρωθεί στην επεξεργασία ή τη συγκέντρωση και τη σύνδεση προγραμμάτων. Πολλές διαρρήξεις έχουν ανακαλυφθεί από αξιωματικούς ασφαλείας ή άλλους χρήστες στο σύστημα που έχουν παρατηρήσει τον υποτιθέμενο χρήστη να συμπεριφέρεται παράξενα.[36]

• Διείσδυση από νόμιμο χρήστη: Ένας χρήστης που προσπαθεί να διεισδύσει στους μηχανισμούς ασφαλείας του λειτουργικού συστήματος μπορεί να εκτελέσει διαφορετικά προγράμματα ή να προκαλέσει περισσότερες παραβιάσεις προστασίας από προσπάθειες πρόσβασης σε μη εξουσιοδοτημένα προγράμματα αρχείων. Εάν η προσπάθειά του επιτύχει, θα έχει πρόσβαση σε εντολές και αρχεία που κανονικά δεν χρησιμοποιούνται σε αυτόν. [21]

• Διαρροή από νόμιμο χρήστη: Ένας χρήστης που προσπαθεί να διαρρεύσει ευαίσθητα έγγραφα μπορεί να συνδεθεί στο σύστημα σε ασυνήθιστες χρονικές στιγμές ή να δρομολογήσει δεδομένα σε απομακρυσμένους εκτυπωτές που κανονικά δεν χρησιμοποιούνται.

• Μεταφορά από νόμιμο χρήστη: Ένας χρήστης που προσπαθεί να αποκτήσει μη εξουσιοδοτημένα δεδομένα από μια βάση δεδομένων μέσω συνάθροισης και συμπεράσματος ανακτά περισσότερες εγγραφές από το συνηθισμένο.

• Δούρειος ίππος: Η συμπεριφορά ενός δούρειου ίππου που φυτεύεται ή αντικαθίσταται από ένα πρόγραμμα μπορεί να διαφέρει από το πρόγραμμα από την άποψη του χρόνου CPU.

• Ιός: Ένας ιός που εισβάλει σε ένα σύστημα μπορεί να προκαλέσει αύξηση της συχνότητας των εκτελέσιμων αρχείων που ξαναγράφονται, αποθήκευση που χρησιμοποιείται από εκτελέσιμα αρχεία ή ένα συγκεκριμένο πρόγραμμα που εκτελείται καθώς εξαπλώνεται ο ιός.

• Άρνηση υπηρεσίας: Ένας εισβολέας ικανός να μονοπωλήσει έναν πόρο (π.χ. δίκτυο) μπορεί να έχει ασυνήθιστα υψηλή δραστηριότητα σε σχέση με τον πόρο, ενώ η δραστηριότητα για όλους τους άλλους χρήστες είναι ασυνήθιστα χαμηλή.

Ένα παράδειγμα ευρέως χρησιμοποιούμενου IDS είναι το Snort. Ενώ το Snort διατίθεται στην αγορά ως σύστημα εισβολής δικτύου, για τους σκοπούς αυτής της επίδειξης μπορεί να χρησιμοποιηθεί ως ids που βασίζεται στον κεντρικό υπολογιστή. Το Snort είναι σε θέση να εκτελεί ανάλυση κυκλοφορίας σε πραγματικό χρόνο και καταγραφή πακέτων σε δίκτυα IP και ανάλυση πρωτοκόλλου canperform, αναζήτηση/αντιστοίχιση περιεχομένου και μπορεί να χρησιμοποιηθεί για τον εντοπισμό μιας ποικιλίας επιθέσεων και ανιχνευτών, όπως υπερχειλίσεις buffer, σαρώσεις θύρας stealth, επιθέσεις CGI, ανιχνευτές SMB και πολλά άλλα. [39]

Το Snort χρησιμοποιεί μια ευέλικτη γλώσσα κανόνων για να περιγράψει την κυκλοφορία που πρέπει να συλλέγει ή να περνάει, καθώς και τον κινητήρα που χρησιμοποιεί αρθρωτή αρχιτεκτονική plug-in. Το Snort διαθέτει δυνατότητα ειδοποίησης σε πραγματικό χρόνο, ενσωματώνοντας μηχανισμούς ειδοποίησης για syslog, ένα καθορισμένο από το χρήστη αρχείο, μια υποδοχή Unix ή μηνύματα Win Pop up σε υπολογιστές-πελάτες windows που χρησιμοποιούν το επιδέξιο samba.

Το Snort κυκλοφόρησε για πρώτη φορά στις 22 Δεκεμβρίου 1998 ως Snort 0.96. Η τελευταία εκδοχή είναι το Snort 2.4.3που ενημερώθηκε τελευταία φορά στις 17 Οκτωβρίου 2005. Αυτή η τελευταία έκδοση ενσωματώνει έναν νέο αναλυτή ροής πρωτοκόλλου HTTP (PFA) και τον μηχανισμό ανίχνευσης. Το PFA ταξινομεί τα πρωτόκολλα εφαρμογών δικτύου σε ροές δεδομένων υπολογιστή-πελάτη και διακομιστή. Αυτές οι ροές είναι η επικοινωνία μεταξύ του υπολογιστή-πελάτη και του διακομιστή. Η επικοινωνία υπολογιστή-πελάτη προς διακομιστή είναι ξεχωριστή από το διακομιστή στην επικοινωνία του υπολογιστή-πελάτη. Η ανάλυση αυτής της επικοινωνίας πραγματοποιείται σε υψηλό επίπεδο και ελέγχει μόνο τις σημαντικές πληροφορίες του πρωτοκόλλου, όπως κωδικούς απόκρισης διακομιστή ή κωδικό αίτησης πελάτη. Αυτή η ανάλυση πρωτοκόλλου δεν είναι απόλυτη. Αντίθετα, χρησιμοποιείται σε συνδυασμό με μεθόδους γενικής ανάλυσης που χρησιμοποιούνται ήδη. Το κύριο όφελος της PFA είναι ο μειωμένος χρόνος επεξεργασίας και η μείωση του αριθμού των ψευδών. Μόλις συναχθούν οι ροές πρωτοκόλλου, ο μηχανισμός ανίχνευσης χρησιμοποιεί τις ροές δεδομένων για να αναζητήσει πιθανές παραβιάσεις πολιτικής. [23]

Ο μηχανισμός ανίχνευσης έχει τρία κύρια στοιχεία, το Rule Optimiser (RO), τον μηχανισμό Search Engine (MRSE) και τον εκλογέα συμβάντων.Το RO χρησιμοποιεί μια καθορισμένη μεθοδολογία για τη διαχείριση των κανόνων Snort και τους εφαρμόζει στο network traffic. Στη συνέχεια, σχηματίζονται υποσύνολα κανόνων με βάση μοναδικά κριτήρια κανόνα και πακέτων. [41] Η βάση της ταξινόμησης των υποσύνολα είναι μοναδικές παράμετροι, όπως η θύρα προέλευσης, η θύρα προορισμού και τα περιεχόμενα των κανόνων. Κάθε υποσύνολο αποτελείται από ένα πλήρες σύνολο κανόνων που ισχύουν για κάθε πακέτο. Αυτό εγγυάται ότι κάθε πακέτο θα δοκιμαστεί και, ως εκ τούτου, διασφαλίζει ότι οι κανόνες που δεν μπορούν ποτέ να ταιριάξουν με τα πακέτα δεν δοκιμάζονται. Όταν το Snort αρχίσει να εκτελείται, το πρόγραμμα διαβάζει και αναλύει όλους τους ενεργοποιημένους κανόνες και, στη συνέχεια, ταξινομεί τους κανόνες σε υποσύνολα. Όταν οι κανόνες έχουν διαιρεθεί, κάθε εισερχόμενο πακέτο αντιστοιχίζεται σε ένα σύνολο κανόνων που πληροί τις μοναδικές παραμέτρους του πακέτου. Για παράδειγμα, το Snort εκτελείται με 1500 κανόνες να χωρίζονται σε μικρότερα

υποσύνολα με βάση πρωτόκολλα επιπέδου μεταφοράς και εφαρμογής. Αυτό συνεχίζεται μέχρι να καλυφθούν όλοι οι κανόνες και τα πρωτόκολλα. Μόλις βελτιστοποιηθούν οι κανόνες, επιλέγεται το σύνολο κανόνων και αρχίζει η διαδικασία MRSE. Το MRSE έχει τρεις ξεχωριστές αναζητήσεις: το πεδίο πρωτοκόλλου, το γενικό περιεχόμενο και την ανωμαλία πακέτων. Η αναζήτηση πεδίου πρωτοκόλλου επιτρέπει σε έναν κανόνα να καθορίσει ένα συγκεκριμένο πεδίο σε ένα πρωτόκολλο προς αναζήτηση. [38]

Για παράδειγμα, το Snort χρησιμοποιεί τη λέξη-κλειδί *«uricontent»* για να αναζητήσει πεδία αιτήσεων HTTP.uri. Η γενική αναζήτηση περιεχομένου επιτρέπει σε έναν κανόνα να καθορίσει μια σειρά byte που θα ταιριάζουν με το πακέτο. Για παράδειγμα, αυτή η λειτουργία χρησιμοποιείται για την αναζήτηση υπερχειλίσεων buffer σε όλα τα πακέτα και μπορεί επίσης να χρησιμοποιηθεί από χρήστες Snort για την αναζήτηση οποιωνδήποτε συνόλων ASCII ή δυαδικών byte που μπορεί να σημαίνει επίθεση στο δίκτυο τους. Η αναζήτηση ανωμαλίας πακέτου επιτρέπει σε έναν κανόνα να καθορίσει τα χαρακτηριστικά μιας κεφαλίδας πακέτου ή πακέτου που είναι αιτία ανησυχίας.

Η αναζήτηση ανωμαλίας πακέτου δεν αναζητά περιεχόμενο στο πακέτο, επικεντρώνεται στα πακέτα άλλα χαρακτηριστικά. Αυτός είναι ένας συγκεκριμένος τύπος ανίχνευσης. Ένα παράδειγμα κανόνα τέτοιου κανόνα είναι ένας κανόνας που αναζητά ένα πακέτο ICMP πάνω από 800 byte. Εάν βρεθεί αντιστοιχία χρησιμοποιώντας οποιονδήποτε από αυτούς τους τρεις τύπους αναζήτησης, όλη η επεξεργαστική ισχύς χρησιμοποιείται για την επικύρωση του συγκεκριμένου κανόνα. [37]

Η μηχανή αναζήτησης συνεχίζει την έρευνα από εκεί που ήταν αμέσως μετά τον εντοπισμό του σπίρτου. Όταν η μηχανή αναζήτησης έχει επεξεργαστεί το πακέτο, ο επιλογέας συμβάντων επεξεργάζεται την ουρά άφιξης. Ο επιλογέας συμβάντων επιτρέπει στον Snort να ταξινομεί κάθε εμφάνιση κάθε αντιστοίχισης κανόνα μέσα σε ένα πακέτο. Ο επιλογέας δίνει προτεραιότητα σε συμβάντα από την ουρά συμβάντων και επιλέγει συμβάντα με βάση την εκχωρημένη τιμή. Αυτό το συμβάν αποστέλλεται στη συνέχεια στο σύστημα εξόδου Snort.31. Με αυτήν την κατευθυντήρια γραμμή παραβιάσεων ασφαλείας και τις εσωτερικές εργασίες του Snort ως παράδειγμα, ένα IDSs θα πρέπει να είναι σε θέση να παρακολουθεί τις ενέργειες ενός ύποπτου εισβολέα. Ο διαχειριστής του συστήματος μπορεί επίσης να χρησιμοποιήσει τα αρχεία καταγραφής συστήματος και άλλες πηγές πληροφοριών για να εντοπίσει τον παραβάτη χρήστη και στη συνέχεια να το κάνει σύμφωνα με την πολιτική του οργανισμού. Αυτό θα μπορούσε να είναι οτιδήποτε από την απαγόρευση του χρήστη, τη συμμετοχή σε περαιτέρω

έρευνα ή απλώς την ειδοποίηση των αρμόδιων αρχών. Οι τελευταίες εξελίξεις στο IDS που βασίζεται σε κεντρικούς υπολογιστές αποσκοπούν στη χρήση του πλεονεκτήματος της άμεσης πρόσβασης στο σύστημα σε συνδυασμό με μια διαδικασία που απαιτεί πολύ λιγότερη επεξεργαστική ισχύ. [36]

Περαιτέρω, η ιδέα των αισθητήρων IDS σε άλλους υπολογιστές οδήγησε στην εισαγωγή του IDS.3.5 που βασίζεται στο δίκτυο. Η επόμενη ανάπτυξη του IDS, του Κατανεμημένου Συστήματος Ανίχνευσης Εισβολής (DIDS), αναπτύχθηκε από τον Haystack. Το σύστημα DIDS χρησιμοποίησε την προηγούμενη έρευνα, αλλά και ιχνηλάτησε τα μηχανήματα-πελάτες, καθώς και τους φύλακες στους οποίους είχε επικεντρωθεί προηγούμενη έρευνα. Το 1990 ο Todd Heberlein εισήγαγε την ιδέα της ανίχνευσης εισβολής δικτύου. Ο Heberlein ήταν ο πρώτος συγγραφέας και προγραμματιστής του Network Security Monitor (NSM), το οποίο ήταν το πρώτο εξάγωνο ενός συστήματος ανίχνευσης εισβολής δικτύου. Η υλοποίηση αυτή αναπτύχθηκε σε μεγάλες εγκαταστάσεις της κυβέρνησης των ΗΠΑ που απαιτούν μαζική ανάλυση δικτύου. Αυτό οδήγησε στο συνδυασμό NSM με το DIDS για να δημιουργήσει την ιδέα του υβριδικού IDS.

Η εξέλιξη αυτή είχε αυξημένο ενδιαφέρον και, κατά τη διάρκεια των επενδύσεων, στην αγορά IDS, φέρνοντάς την στον εμπορικό κόσμο. Μετά την εμπορική κυκλοφορία συστημάτων όπως το Haystack Labs Stalker, πολλά προϊόντα κυκλοφόρησαν αργότερα. Για παράδειγμα, η Science Applications International Corporation (SAIC) ανέπτυξε μια ανίχνευση εισβολής που βασίζεται στον κεντρικό υπολογιστή και ονομάζεται Σύστημα Ανίχνευσης Κατάχρησης Υπολογιστών (CMDS) και η Πολεμική Αεροπορία των ΗΠΑ ανέπτυξε ταυτόχρονα το Αυτοματοποιημένο Σύστημα Μέτρησης Ασφαλείας (ASIM) για την παρακολούθηση της κυκλοφορίας δικτύου στο δίκτυο USAF. Το ASIM εξακολουθεί να χρησιμοποιείται σήμερα. [34]

3.3. Αναγνωριστικά που βασίζονται στο δίκτυο «network-based identifiers»

Το IDS που βασίζεται στο Δίκτυο παρακολουθεί την κυκλοφορία δικτύου μεταξύ κεντρικών υπολογιστών. Σε αντίθεση με το IDS που βασίζεται στον κεντρικό υπολογιστή, το οποίο ανιχνεύει εντελώς τη συμπεριφορά, αυτά τα συστήματα προκαλούν συμπεριφορά με βάση το περιεχόμενο και τη μορφή των πακέτων δεδομένων στο δίκτυο. Μεταξύ άλλων, αναλύουν απτά αιτήματα για ευαίσθητες πληροφορίες και επανειλημμένες αποτυχημένες προσπάθειες παραβίασης της πολιτικής ασφάλειας. Πολλά τρέχοντα IDS που βασίζονται στο δίκτυο είναι αρκετά πρωτόγονα, παρακολουθώντας μόνο τις λέξεις και τις εντολές του λεξιλογίου ενός

χάκερ. Μερικές είναι πιο εξελιγμένες και αναλυμένες πληροφορίες για το πρωτόκολλο. Εάν το IDS που βασίζεται στον κεντρικό υπολογιστή είναι ανάλογο με ένα σκυλί φρουράς για κάθε υπολογιστή, το IDS που βασίζεται στο δίκτυο είναι σαν περιπολίες της αστυνομίας. [10]

Ένα παράδειγμα λειτουργίας ενός IDS που βασίζεται στο δίκτυο είναι ένα προϊόν που ονομάζεται απλώς NID. Το NID είναι μια σειρά εργαλείων λογισμικού που βοηθά στον εντοπισμό, την ανάλυση και τη συλλογή αποδεικτικών στοιχείων ύποπτης συμπεριφοράς που συμβαίνουν σε δίκτυο Διασύνδεσης Δεδομένων Ethernet ή Fibre Distributed Data Interface (FDDI) χρησιμοποιώντας IP. Το NID αναπτύχθηκε για το Υπουργείο Ενέργειας των ΗΠΑ ως μέρος του Κέντρου Εργαλείων Cyber Solution Συμβουλευτικής Ικανότητας Περιστατικών Υπολογιστών (CIAC CSTC) και κατά τη στιγμή της σύνταξης εφαρμόζεται επί του παρόντος ως Version 2.6.NID λειτουργεί παθητικά σε έναν αυτόνομο κεντρικό υπολογιστή (αντί να κατοικεί στους οικοδεσπότες που παρακολουθεί), και είναι υπεύθυνο για τη συλλογή δεδομένων ή / και στατιστικών στοιχείων σχετικά με την κυκλοφορία του δικτύου. Το NID λειτουργεί εντός ενός καθορισμένου τομέα ασφαλείας κεντρικών υπολογιστών ή ενός υπο-δικτύου. Ένας τομέας ασφαλείας αποτελείται είτε από ένα υποδίκτυο ενός δικτύου είτε από ολόκληρο το δίκτυο με το οποίο συνδέεται απευθείας το NID. Ο τομέας ασφαλείας μπορεί να βελτιωθεί εξετάζοντας την κυκλοφορία από συγκεκριμένες υπηρεσίες Internet. [33]

Το NID έχει μοναδικά χαρακτηριστικά:

- Είναι παθητικό, αυτό σημαίνει ότι οι εισβολείς δεν γνωρίζουν ότι είναι εκεί.
- Δεν απαιτεί τροποποίηση κεντρικού υπολογιστή.
- Μπορεί να αναλύσει δεδομένα καθώς φτάνει ή σε μεταγενέστερο χρόνο.
- Παρέχει ειδοποιήσεις σε πραγματικό χρόνο για ύποπτη συμπεριφορά.
- Μπορεί να ξεκινήσει συλλογή δεδομένων κατά τον εντοπισμό ύποπτης συμπεριφοράς. Αυτό μπορεί να σταματήσει κατά την κρίση της ύποπτης συμπεριφοράς.
- Παρέχει μια πλήρη σειρά αναλυτικών εργαλείων.
- Είναι προσαρμόσιμη.

3.3.1. Τεχνικές εντοπισμού ύποπτης συμπεριφοράς

Το NID χρησιμοποιεί τρεις τεχνικές για τον εντοπισμό ύποπτης συμπεριφοράς. [32]

1) Αναγνώριση υπογραφής επίθεσης (ASR).

   Η τεχνική ASR εξετάζει πακέτα δεδομένων για σειρές byte που σχετίζονται με γνωστές επιθέσεις και η εμφάνιση υποδηλώνει την πιθανότητα ύποπτης συμπεριφοράς. Ειδικοί μη εκτυπώσιμοι χαρακτήρες ελέγχου μπορούν επίσης να συμπεριληφθούν στους ορισμούς των μοτίβων. Εάν βρεθεί ένα ύποπτο μοτίβο, το NID μπορεί να σηματοδοτήσει συναγερμό, να εμφανίσει το περιβάλλον στο οποίο βρίσκεται το μοτίβο και να αρχίσει να αποθηκεύσει τα network packets της περιόδου λειτουργίας σε ένα αρχείο εξόδου. Στη συνέχεια, οι φάκελοι αυτοί μπορούν να εξεταστούν σε μεταγενέστερη ημερομηνία για να διαπιστωθεί αν έχει επέλθει έγκαιρη συμπεριφορά.

2) Μοντέλο κινδύνου ευπάθειας (VRM)

   Το NID διαθέτει ένα VRM που υπολογίζει μια τιμή προειδοποίησης με βάση το επίπεδο ασφαλείας ενός κεντρικού υπολογιστή, κάθε έλεγχο ταυτότητας που απαιτείται για την υπηρεσία που χρησιμοποιείται και τυχόν πρόσφατες συναλλαγές του κεντρικού υπολογιστή. Αυτή η τιμή προειδοποίησης χρησιμοποιείται για την επικοινωνία.

3) Ανίχνευση ανωμαλιών (AD)

   Το (AD) παρακολουθεί και αναφέρει ανωμαλίες καθώς συμβαίνουν. Τα δύο κύρια σύνολα ανωμαλιών που μπορεί να έχει το NID είναι δραστηριότητες που σχετίζονται με μη αξιόπιστους ή απροσδόκητους κεντρικούς υπολογιστές και γνωστές επιθέσεις δικτύου, όπως σαρώσεις θύρας ή πλημμύρες SYN.

3.3.2 Αντιδραση του NID σε ύποπτη συμπεριφορά

Όταν εντοπιστεί ύποπτη συμπεριφορά, το NID μπορεί να αντιδράσει σε αυτό με τρεις διαφορετικούς τρόπους: [31]

1) Με Αναδρομική ανάλυση εισβολής (RIA)

   Το RIA χρησιμοποιείται για την ανάλυση της κυκλοφορίας για ενδείξεις ύποπτης συμπεριφοράς. Μόλις η ανάλυση είναι επιτυχής, οποιαδήποτε ύποπτη επικοινωνία μπορεί να επαναληφθεί, ώστε ένας ανθρώπινος αναλυτής να μπορεί να ανακαλύψει νέες τεχνικές εισβολής. Αυτή η τεχνική είναι περισσότερο μια τεχνική παρακολούθησης καθώς εξετάζει προηγούμενα αρχεία επικοινωνίας.

2) Την ανίχνευση εισβολής σε πραγματικό χρόνο (RTID)

   Το RTID χρησιμοποιείται για την επεξεργασία ύποπτης συμπεριφοράς όταν συμβαίνει. Τα πακέτα δικτύου που σχετίζονται ευνοϊκή με συμπεριφορά συλλέγονται συνεχώς μέχρι να τερματιστεί η περίοδος λειτουργίας. Αυτό το σύστημα μοιάζει περισσότερο με συναγερμό, καθώς συλλέγει δεδομένα σχετικά με ύποπτη συμπεριφορά καθώς συμβαίνει.

3) Τη συλλογή στατιστικών (SG)

   Το SG χρησιμοποιείται για τη συλλογή πληροφοριών σχετικά με τα πακέτα, όπως δεδομένα κεφαλίδας, τον αποστολέα και τον παραλήπτη και τα πρωτόκολλα που χρησιμοποιούνται.

Όλες αυτές οι πληροφορίες χρησιμοποιούνται για την εκτέλεση στατιστικής ανάλυσης σχετικά με την κυκλοφορία. Αυτό το παράδειγμα ενός αναγνωριστικού δικτύου που λειτουργεί δείχνει ότι τα προβλήματα που αντιμετωπίζει το IDS που βασίζεται στον κεντρικό υπολογιστή μπορούν να ξεπεραστούν χρησιμοποιώντας έναν παθητικό κεντρικό υπολογιστή ακρόασης στο δίκτυο. Η σύγκριση των δύο διαφορετικών μέτρων είναι δύσκολη, επειδή είναι διαφορετικές τεχνολογίες που κάνουν διαφορετικές εργασίες στο πλαίσιο των ίδιων παραμέτρων. [30]

3.4. Σύγκριση των Συστημάτων Ανίχνευσης Εισβολών

Τα οφέλη του IDS που βασίζεται σε δίκτυο έναντι κεντρικού υπολογιστή πρέπει να προβάλλονται στο πλαίσιο. Τα ακόλουθα είναι ορισμένα πλεονεκτήματα και περιορισμοί του αντίστοιχου αναγνωριστικού δελτίου και θα πρέπει να εξετάζονται εάν πρόκειται να εφαρμοστεί ένα IDS.

Πλεονεκτήματα των IDS που βασίζονται στο δίκτυο:

• Μπορεί να αναπτυχθεί στρατηγικά σε κρίσιμα σημεία πρόσβασης για την προβολή δικτύου κυκλοφορία που προορίζεται για αμέτρητα συστήματα που πρέπει να προστατεύονται.

• Είναι ανεξάρτητα από το λειτουργικό σύστημα και δεν απαιτούν λογισμικό για φόρτωση και διαχείριση σε διάφορους κεντρικούς υπολογιστές, όπως συμβαίνει με την προσέγγιση που βασίζεται στον κεντρικό υπολογιστή. [28]

• Απαιτούν λιγότερα σημεία ανίχνευσης, ώστε το κόστος ιδιοκτησίας να είναι συνήθως χαμηλότερο για μια επιχείρηση.

• Εάν απαιτείται, μπορεί να τοποθετηθεί εκτός δικτύου για τη συλλογή πληροφοριών σχετικά με προσπάθειες εισβολής, καθώς ενδέχεται να μην περάσει από το τείχος προστασίας.

Πλεονεκτήματα των IDS που βασίζεται σε κεντρικό υπολογιστή:

•Είναι πιο κοντά στο χρήστη, και έτσι είναι σε θέση να διακρίνουν επιθέσεις και κακή χρήση που θα ήταν πολύ δύσκολο να παρατηρήσει ο οιοσδήποτε από το δίκτυο.

• Μπορεί να παρακολουθεί τη δραστηριότητα που αφορά το σύστημα, όπως η σύνδεση και αποσύνδεση χρηστών, η πρόσβαση σε αρχεία, οι αλλαγές στα δικαιώματα προμήθειας, οι προσπάθειες εγκατάστασης νέων εκτελέσιμων αρχείων και η πρόσβαση σε προνομιακές υπηρεσίες.

• Μπορεί επίσης να βοηθήσει να ξεπεραστούν ορισμένες από τις προκλήσεις που προκύπτουν από κρυπτογραφημένες επικοινωνίες και δίκτυα μεταγωγής. Το πρόβλημα είναι ότι η κρυπτογράφηση απαιτεί πολλή επεξεργαστική ισχύ και τα δίκτυα μεταγωγής προκαλούν προβλήματα σχετικά με το πού να εντοπίζονται τα ids. [27]

• Έχουν επεκτείνει τις δυνατότητες καταγραφής στο επίπεδο εφαρμογής επιτρέποντας στον παράγοντα συστήματος IDS να προστατεύει εφαρμογές όπως διακομιστές web ή βάσης δεδομένων.

Περιορισμοί και αναγνωριστικά που βασίζονται στο δίκτυο:

• Έχουν όρια που προέρχονται από τεχνικούς περιορισμούς υλικού. Η ταχύτητα του επεξεργαστή και ο χρόνος παρακολούθησης της μνήμης υπαγορεύουν την απόδοση των μηχανών παρακολούθησης δικτύου.

Το περιθώριο βελτίωσης θα μπορούσε να προέλθει από τρεις τομείς:

1)Καλύτεροι αλγόριθμοι

2)Ταχύτερο υλικό

3)Βελτιωμένη αλληλεπίδραση μεταξύ λογισμικού και υλικού

• Είναι μια σχετικά νέα πειθαρχία όπου η εμπειρία αποκτάται και μοιράζεται καθημερινά. Οι τεχνικές μηχανικής Modernsoftware, όπως οι αναζητήσεις hash-table, χρησιμοποιούνται για την αντιμετώπιση του προβλήματος απόδοσης από την πλευρά του λογισμικού.

• Η παρακολούθηση κρυπτογραφημένων πακέτων είναι, αν και θεωρητικά δυνατή, δύσκολο να γίνει στην πράξη. Όχι μόνο το σύστημα παρακολούθησης πρέπει να γνωρίζει τα σχετικά κλειδιά, αλλά η αποκρυπτογράφηση πρέπει επίσης να συμβεί σε πραγματικό χρόνο.

• Έχει περιορισμένη δυνατότητα εντοπισμού ενός εισβολέα που κάθεται στην κονσόλα του σταθμού εργασίας. Τα αναγνωριστικά που βασίζονται στον κεντρικό υπολογιστή και βρίσκονται πιο κοντά στην πλευρά του τελικού χρήστη μπορούν να παρέχουν πρόσθετη υποστήριξη για τον εντοπισμό αυτού του τύπου παραβίασης ασφαλείας.

Περιορισμοί και αναγνωριστηκά που βασίζονται σε κεντρικό υπολογιστή:

• Τα αναγνωριστικά που βασίζονται σε κεντρικούς υπολογιστές είναι συνήθως πιο κοντά σε επιχειρηματικές κρίσιμες εφαρμογές, είναι επίσης πιο κατάλληλοι για να ανταποκριθούν. Πλέον συγκεκριμένα, όταν υπάρχουν ανησυχίες σχετικά με τις επιθέσεις (DoS), θα πρέπει να υπάρχει ένα αναγνωριστικό που βασίζεται στο δίκτυο. [26]

• Για να παρέχεται πλήρης προστασία, οι παράγοντες του συστήματος πρέπει να εγκαθίστανται σε ένα σύστημα ανά σύστημα σε ολόκληρο τον οργανισμό.

• Είναι επίσης σημαντικό να σημειωθεί ότι ο όγκος των γενικών εξόδων διαχείρισης που συνδέονται με την ρύθμιση των πρακτόρων και των κινητήρων και την αντιμετώπιση συμβάντων είναι ανάλογος με την εγκατεστημένη βάση των συστημάτων ανίχνευσης εισβολής και οι ικανότητες των υπαλλήλων ασφαλείας να ανταποκρίνονται στις ειδοποιήσεις της κονσόλας.

Από την άποψη αυτή, οι τεχνικοί περιορισμοί των προϊόντων ενδέχεται να υπερβαίνουν κατά πολύ την ανθρώπινη ικανότητα και η αποτελεσματικότητα του συστήματος ασφαλείας που εφαρμόζεται θα εξαρτηθεί τόσο από τη διαμόρφωση των πολιτικών ασφαλείας, και πώς έχει επιλέξει κανείς να χειρίζεται τις αντιδράσεις σε περιστατικά σε πραγματικό χρόνο με την οργάνωση. Τα όρια IDS που βασίζονται σε κεντρικούς υπολογιστές μικραινούν από τα πλεονεκτήματα μιας λύσης που βασίζεται στο δίκτυο και αντίστροφα. Αυτό δείχνει ότι το IDS

που βασίζεται στο δίκτυο και τον κεντρικό υπολογιστή θα λειτουργούσε καλύτερα όταν συνδυάζονταν για να δημιουργήσουν μια ολοκληρωμένη στρατηγική ασφάλειας. Με αυτόν τον τρόπο ξεκίνησε η ανάπτυξη συστημάτων πρόληψης της εισβολής (IPS). [25]

Κεφάλαιο 4ο: «Συστήματα Αποφυγής Εισβολών»

4.1. Εισαγωγή

Έχει προταθεί ότι το IPS είναι μια επαναστατική νέα τεχνολογία ασφάλειας. Για να περιγραφεί το IPS ως επαναστατική μέθοδος τεχνολογίας, θα πρέπει κανείς να έχει περιορισμένη άποψη για την αγορά προϊόντων ασφαλείας. Το IPS συνθέτει πτυχές πολλών γνωστών, υπαρχουσών τεχνολογιών ασφαλείας, συμπεριλαμβανομένων των anti-virus, του λογισμικού, του εντοπισμού εισβολής και των τειχών προστασίας. Η εξέλιξη και όχι η επανάσταση είναι σαφώς η πιο επιφανής διαδικασία αλλαγής. Στο μοντέλο IPS, αντί να αναπτύσσει αντιδραστικές πολιτικές ασφάλειας, η πολιτική ασφάλειας γίνεται ένα δραστικό εργαλείο για την προστασία ενός οργανισμού. Αυτό επιτρέπει στον οργανισμό να γίνει «αυτο-προσδιοριστικός». Για να επιτευχθεί το ιδανικό της αυτοπροστασίας, όλες οι επιθέσεις εναντίον οποιουδήποτε μέρους του προστατευμένου περιβάλλοντος εκτρέπονται από το IPS. [35]

Επειδή το IPS είναι ασφαλές, μπορούν να πάρουν οποιαδήποτε ροή πακέτων δικτύου και να καθορίσουν την πρόθεση - είτε πρόκειται για επίθεση είτε για νόμιμη χρήση - και στη συνέχεια να λάβουν την κατάλληλη απάντηση με πλήρη τελειότητα. Το τελικό αποτέλεσμα θα ήταν μόνο μια περιορισμένη ανάγκη για λύσεις IDS ή παρακολούθηση, καθώς όλα όσα αντιπροσωπεύουν μια απειλή αποκλείονται. Ενώ ένας αξιοθαύμαστος στόχος, στην πραγματικότητα είναι απίστευτα δύσκολος επειδή οι νέες στρατηγικές επιθέσεων εξελίσσονται συνεχώς. Προκειμένου δέ να αντιμετωπίσει νέες επιθέσεις, το IPS πρέπει να ενημερώνει συνεχώς τη βιβλιοθήκη επίθεσης τους με παρόμοιο τρόπο με τους anti-virus scanners. Αυτό σημαίνει δέ ότι ένα IPS είναι τόσο ασφαλές όσο η τελευταία ενημέρωση.

Ως αποτέλεσμα της δυσκολίας εφαρμογής ενός πραγματικά ασφαλούς IPS, οι περισσότερες υλοποιήσεις σήμερα χρησιμοποιούν ένα συριγμό ανωμαλίας ή ανίχνευσης και IDS που βασίζεται στη συμπεριφορά για την ταχεία ανίχνευση μιας επίθεσης. Τα περισσότερα προϊόντα IPS βασίζονται στο δίκτυο και αναπτύσσονται με τη μορφή συσκευών υψηλής απόδοσης με λειτουργικά συστήματα και υλικολογισμικό. [25]

4.2. Ανάπτυξη

Οι ανεπάρκειες που είναι εγγενείς στις τρέχουσες άμυνες, όπως το IDS (τόσο με βάση τον κεντρικό υπολογιστή όσο και με βάση το δίκτυο) έχουν οδηγήσει στην ανάπτυξη του IPS. Επιφανειακά, το IDS και το IPS φαίνεται να είναι εξίσου αποτελεσματικά. Μετά από όλα, μοιράζονται μια μακρά λίστα των παρόμοιων λειτουργιών, όπως η επιθεώρηση πακέτων, η

ανάλυση κατάστασης, η επανασυναρμολόγηση τμήματος, η τμηματική συναρμογές TCP, η επιθεώρηση πακέτων βάθους, η επικύρωση πρωτοκόλλου και η αντιστοίχιση υπογραφών. [24]

Ένα IPS λειτουργεί ως ένας επί της ουσίας φύλακας ασφαλείας στην πύλη μιας ιδιωτικής κοινότητας, επιτρέποντας και αποτρέποντας την πρόσβαση με βάση τα αξιόπιστα και ορισμένα προκαθορισμένα πρωτόκολλα ασφαλείας. Όπως περιγράφεται σε προηγούμενες ενότητες, σκοπός του IDS είναι η παροχή παρακολούθησης, λογιστικού ελέγχου και αναφοράς της δραστηριότητας του δικτύου. Λειτουργεί στα πακέτα που επιτρέπονται μέσω ενός στοιχείου ελέγχου πρόσβασης συσκευή, όπως ένα τείχος προστασίας.

Περαιτέρω, σημειώνεται ότι οι λύσεις IDS είναι φορτωμένες με νοημοσύνη, χρησιμοποιώντας πολλές διαφορετικές τεχνικές για τον εντοπισμό πιθανών επιθέσεων, εισβολών, εκμεταλλεύσεων και καταχρήσεων. Η κύρια προσδοκία της IPS είναι ότι θα μειώσει την απειλή επίθεσης εξαλείφοντας την κυκλοφορία του δικτύου και το κακόβουλο λογισμικό, ενώ θα συνεχίσει να επιτρέπει τη συνέχιση της νόμιμης δραστηριότητας. Οι λύσεις IPS πρέπει να έχουν ντετερμινιστικό χαρακτήρα. Οι ντετερμινιστικές δυνατότητες ενσταλάζουν την εμπιστοσύνη που απαιτείται για μια απόλυτη απόφαση, όπως η άρνηση της κυκλοφορίας στο δίκτυο. Αυτό σημαίνει ότι το IPS είναι ιδανικά σε θέση να αντιμετωπίσει: [16]

• Ανεπιθύμητες επιθέσεις εφαρμογών εναντίον ιδιωτικών δικτύων και εφαρμογών.

• Πακέτα επίθεσης (όπως επί παραδείγματι είναι το WinNuke) χρησιμοποιώντας φίλτρα πακέτων υψηλής ταχύτητας.

• Κατάχρηση πρωτοκόλλου και ενέργειες αποφυγής - χειρισμοί πρωτοκόλλου δικτύου όπως fragroute και TCPoverlap exploits.

• Επιθέσεις DoS όπως πλημμύρες SYN και ICMP.

• Κατάχρηση εφαρμογών και χειρισμοί πρωτοκόλλου

• Γνωστές και άγνωστες επιθέσεις κατά http, FTP, DNS, SMTP.

• Υπερφόρτωση εφαρμογών ή επιθέσεις κατάχρησης. [3]

Όλες αυτές οι επιθέσεις και η ευάλωτη κατάσταση που τους επιτρέπει να συμβούν είναι καλά τεκμηριωμένες. Η παράνοια, οι ανωμαλίες στα πρωτόκολλα επικοινωνίας από το δίκτυο μέσω του επιπέδου εφαρμογής δεν έχουν καμία θέση σε οποιοδήποτε είδος νόμιμης κυκλοφορίας. Η διαφορά μεταξύ IDS και IPS είναι ότι το IDS χρησιμοποιεί ιστορική κυκλοφορία για να καθορίσει εάν υπάρχει δυνατότητα απειλής, συμπεριλαμβανομένης της εκτέλεσης στατιστικής

ανάλυσης του όγκου κυκλοφορίας, των μοτίβων κυκλοφορίας και των δραστηριοτήτων. Το IPS πρέπει να είναι ντετερμινιστικό σε όλες τις αποφάσεις του προκειμένου να εκτελεί τη λειτουργία του scrubbingtraffic. Ένα IPS υποτίθεται ότι λειτουργεί όλη την ώρα και λαμβάνει αποφάσεις ελέγχου πρόσβασης στο δίκτυο. Τα τείχη προστασίας παρείχαν την πρώτη ντετερμινιστική προσέγγιση για τον έλεγχο πρόσβασης στο δίκτυο, παρέχοντας βασική δυνατότητα IPS. [1]

Οι συσκευές IPS προσθέτουν δυνατότητα επόμενης γενιάς σε αυτά τα τείχη προστασίας - εξακολουθούν να παρέχουν τον τύπο της ντετερμινιστικής άνεσης που απαιτείται από μια ενσωματωμένη συσκευή που εκδίδει αποφάσεις ελέγχου πρόσβασης. Τα IPS έχουν αναπτύξει, έχουν ξεπεράσει τους περιορισμούς που αντιμετώπισαν οι προηγούμενες τεχνολογίες και βρήκαν νέα ζητήματα που πρέπει ακόμα να αντιμετωπιστούν. Το σύστημα IPS έχει γενικά βελτιωθεί σε σχέση με προηγούμενες τεχνικές, εάν εφαρμοστεί σωστά και σχεδιαστεί όπως περιγράφεται παραπάνω.

4.3. Πώς λειτουργεί το IPS

Με την ανάπτυξη που περιγράφηκε προηγουμένως δείχνοντας νέες και καλύτερες λύσεις ασφάλειας, το σύστημα IPS πρέπει να ενσωματώσει νέες ιδέες και μεθόδους για την πρόοδο. Το σύστημα IPS είναι συσκευές δικτύου που μπορούν να δεχτούν ή να αρνηθούν την κυκλοφορία με βάση διευθύνσεις IP, πρωτόκολλο / υπηρεσία, ανάλυση επιπέδου εφαρμογής και επαλήθευση. Το IPS λαμβάνει κυκλοφορία από το δίκτυο, συναρμολογεί εκ νέου τις ροές κυκλοφορίας και εξετάζει πρωτόκολλα και εντολές εφαρμογής για τον εντοπισμό ύποπτων πεδίων που δικαιολογούν κάποια προκαθορισμένη ενέργεια. Αυτές οι ενέργειες ποικίλλουν από την καταγραφή ύποπτων συμβάντων έως την πλήρη κατάργηση της σύνδεσης. Ένα IPS ελέγχει όλα τα επίπεδα πληροφοριών πακέτων που ταξιδεύουν στο δίκτυο (εκτός από το φυσικό στρώμα), και όχι μόνο τα πρώτα 4 επίπεδα που ελέγχονται από ένα τείχος προστασίας. Μια μέθοδος έξι επιπέδων, που συνήθως ονομάζεται επιθεώρηση *«βαθύ πακέτο»*, επιτρέπει σε ένα IPS να εκτελεί πακέτα υπογραφής μέχρι ένα επίπεδο εφαρμογής. [29]

Το αποτέλεσμα είναι μια εξαιρετικά ακριβής συσκευή φιλτραρίσματος που, σε αντίθεση με ένα NIDS, έχει ελάχιστα ψευδώς θετικά αποτελέσματα. Αυτή είναι μια ουσιαστική βελτίωση σε σχέση με τα ψευδή στοιχεία που συνήθως κυριαρχούν στο περιεχόμενο των περισσότερων καθημερινών αναφορών που βρίσκονται στα τυπικά αρχεία καταγραφής NIDS.[54] Όπως και με ένα τυπικό τείχος προστασίας, το IPS διαθέτει τουλάχιστον δύο διεπαφές δικτύου. Ένα που ορίζεται ως εσωτερικό και ένα ως εξωτερικό. Καθώς τα πακέτα εμφανίζονται σε οποιαδήποτε

διεπαφή, μεταβιβάζονται στον μηχανισμό ανίχνευσης. Ωστόσο, εάν εντοπίσει ένα κακόβουλο πακέτο, εκτός από την αύξηση μιας ειδοποίησης, θα απορρίψει το πακέτο και θα επισημάνει αυτή τη ροή ως *«κακή»*. Καθώς τα υπόλοιπα πακέτα που συνθέτουν τη συγκεκριμένη TCP session φτάνουν στη συσκευή IPS, απορρίπτονται αμέσως. Τα νόμιμα πακέτα περνούν στη δεύτερη διασύνδεση και στον προορισμό που προορίζονται. Μια χρήσιμη παρενέργεια ορισμένων προϊόντων IPS είναι ότι, φυσικά, θα παρέχουν μια λειτουργία *«packetscrubbing»* για την κατάργηση ασυνεπειών πρωτοκόλλου που προκύπτουν από διαφορετικές ερμηνείες των προδιαγραφών TCP/IP. Τυχόν κατακερματισμένα πακέτα, πακέτα εκτός παραγγελίας ή πακέτα με επικαλυπτόμενα θραύσματα IP θα παραγγελθούν και θα *«καθαριστούν»* πριν μεταφερθούν στον κεντρικό υπολογιστή προορισμού και τα παράνομα πακέτα μπορούν να μεταφερθούν εντελώς. Το στοιχείο υλικού ενός IPS βασίζεται σε τεχνολογία επεξεργαστή πολλαπλών διακομιστών, ώστε η συσκευή να μπορεί να κάθεται σχεδόν αόρατα μέσα σε ένα δίκτυο. Αυτοί οι επεξεργαστές επεξεργάζονται εκατομμύρια οδηγίες κάθε δευτερόλεπτο, προκειμένου να χειριστούν έναν πολύ μεγαλύτερο όγκο κυκλοφορίας από έναν μόνο επεξεργαστή. Στην πραγματικότητα, τα περισσότερα IPS επιτυγχάνουν ελάχιστη έως μη αισθητή λανθάνουσα κατάσταση καθισμένοι στη γραμμή σε ένα δίκτυο, καθώς μπορούν να αναλύσουν την κυκλοφορία σε ταχύτητες έως gigabit. Όλα τα IPS χρησιμοποιούν επίσης την *«κρατική επιθεώρηση»* για να διατηρήσουν τη διαφάνεια χαμηλή. Χρησιμοποιώντας την κρατική επιθεώρηση, οι συσκευές πρέπει μόνο να αναλύσουν τα μέρη μιας συνεδρίας που ταιριάζουν με μια υπογραφή επίθεσης. Οι περισσότεροι οργανισμοί απαιτούν αυτόν τον τύπο λειτουργικότητας, ειδικά για μια συσκευή που πρέπει πραγματικά να καθίσει στη γραμμή σε ένα δίκτυο που πρέπει να εκτελεί σε υψηλές ταχύτητες για πολλούς χρηστές. [27,28]

Οι συσκευές IPS υποχρεούνται να εκτελούν τις ακόλουθες εργασίες, προκειμένου να αποφευχθούν τα ίδια προβλήματα που αντιμετωπίζουν τα αναγνωριστικά:

• Οι λειτουργίες σε απευθείας σύνδεση: Μόνο με τη λειτουργία σε απευθείας σύνδεση μπορεί μια συσκευή IPS να εκτελέσει πραγματική προστασία, απορρίπτοντας όλα τα ύποπτα πακέτα αμέσως και εμποδίζοντας το υπόλοιπο αυτής της ροής.

• Αδιαμφισβήτητη ακρίβεια ανίχνευσης: Είναι επιτακτική ανάγκη η ποιότητα των υπογραφών να είναι αναμφισβήτητη, δεδομένου ότι τα ψευδώς θετικά μπορούν να οδηγήσουν σε μια κατάσταση DoS. Ο χρήστης πρέπει να είναι σε θέση να είναι

σίγουρος ότι το IPS εμποδίζει μόνο κακόβουλη κυκλοφορία. Οι νέες υπογραφές θα πρέπει να διατίθενται σε τακτική βάση και η εφαρμογή τους θα πρέπει να είναι γρήγορη (να εφαρμόζεται σε όλους τους αισθητήρες σε μία λειτουργία μέσω κεντρικής κονσόλας) και απρόσκοπτη (χωρίς επανεκκίνηση αισθητήρα).

• Προηγμένες δυνατότητες χειρισμού ειδοποιήσεων και εγκληματολογικής ανάλυσης: Μόλις οι ειδοποιήσεις έχουν ανυψωθεί στον αισθητήρα και περάσουν σε μια κεντρική κονσόλα, κάποιος πρέπει: να τα εξετάσουμε, να συσχετίσουμε όπου είναι απαραίτητο, να διερευνήσουμε και, τελικά, να αποφασίσουμε για μια ενέργεια. Οι ανακεφαλαιώσεις που προσφέρει η κονσόλα όσον αφορά την προβολή σε κατάσταση συναγερμού (σε πραγματικό χρόνο και ιστορική) και την υποβολή εκθέσεων είναι το κλειδί για τον προσδιορισμό της αποτελεσματικότητας του IPS.
[25]

• Αξιοπιστία και διαθεσιμότητα: Σε περίπτωση αποτυχίας μιας ενσωματωμένης συσκευής, έχει τη δυνατότητα να κλείσει μια ζωτική διαδρομή δικτύου. Ένα εξαιρετικά χαμηλό ποσοστό αποτυχίας είναι πολύ σημαντικό για τη μεγιστοποίηση του χρόνου. Εάν συμβεί αυτό, η συσκευή θα πρέπει να παρέχει την επιλογή αποτυχίας ανοίγματος ή υποστήριξης αποτυχίας που λειτουργεί σε μια ομάδα ανακατεύθυνσης. Επιπλέον, για να μειωθεί ο χρόνος διακοπής λειτουργίας για ενημερώσεις υπογραφής και πρωτοκόλλου, ένα IPS πρέπει να υποστηρίζει τη δυνατότητα λήψης αυτών των ενημερώσεων χωρίς να απαιτείται επανεκκίνηση του μηχανήματος-συσκευής. Όταν λειτουργούν σε απευθείας σύνδεση, οι αισθητήρες που επανεκκινούν σε όλη την επιχείρηση μεταφράζουν αποτελεσματικά το χρόνο διακοπής λειτουργίας του δικτύου κατά τη διάρκεια της επανεκκίνησης.

• Υψηλή απόδοση: Τα ποσοστά επεξεργασίας πακέτων πρέπει να είναι σε ταχύτητα καλωδίου υπό πραγματικές συνθήκες κυκλοφορίας. Η συσκευή πρέπει να βελτιώσει την αναφερόμενη απόδοση με όλες τις υπογραφές ενεργοποιημένες. Το περιθώριο θα πρέπει να είναι ενσωματωμένο στις δυνατότητες απόδοσης για να μπορεί η συσκευή να χειρίζεται τυχόν αυξήσεις στο μέγεθος των πακέτων υπογραφής που μπορεί να προκύψουν κατά τη διάρκεια των λίγων ετών.

• Χαμηλή λανθάνουσα κατάσταση: Όταν μια συσκευή τοποθετείται σε σειρά, είναι σημαντικό ο αντίκτυπός της στη συνολική απόδοση του δικτύου να είναι σημαντικός. Τα πακέτα θα πρέπει να υποβάλλονται σε επεξεργασία αρκετά γρήγορα, έτσι ώστε ο συνολικός λανθάνων χρόνος της συσκευής να είναι όσο το δυνατόν πιο κοντά σε αυτόν που προσφέρεται από μια συσκευή επιπέδου τέσσερα, όπως ένα τείχος προστασίας. Το IPS υποστηρίζει ένα ευρύ φάσμα πρωτοκόλλων και εφαρμογών, συμπεριλαμβανομένων εκείνων που απαιτούνται για την προστασία του δικτύου από επιθέσεις από το Διαδίκτυο. [24] Οι νέες εφαρμογές μπορούν να επιτραπούν μέσω IPS χωρίς να απαιτούνται αλλαγές στους σταθμούς εργασίας χρήστη. Οι συσκευές IPS είναι πιο διαφανείς στο δίκτυο. Στην ιδανική περίπτωση, ένα IPS θα πρέπει να εντοπίζει και να σταματά γρήγορα τέσσερις σημαντικούς τύπους επιθέσεων και ενοχλητικών δραστηριοτήτων που μαστίζουν τα σημερινά δίκτυα δεδομένων.

1)Θα πρέπει να μπλοκάρει τις έρευνες και τις σαρώσεις πριν από την επίθεση για να αρνηθεί στους επιτιθέμενους πολύτιμες πληροφορίες σχετικά με τις υπηρεσίες του δικτύου και τις πιθανές ευπάθειες.

2)Θα πρέπει να είναι μια ουσιαστική πρώτη γραμμή άμυνας για τον μετριασμό των επιθέσεων DoS και κατανεμημένης άρνησης υπηρεσίας.

3)Θα πρέπει να εντοπίζει και να αποκλείει επιθέσεις λεξικών, επιθέσεις ωμής βίας και προσπάθειες Πρόσβασης σε διακομιστές protected web.

4)Θα πρέπει να είναι σωστά διαμορφωμένο και σε θέση να σταματήσει εντελώς τη διανομή των server-to-server worms όπως SQL Slammer, Code Red και Nimda.

Αυτές οι τέσσερις λειτουργίες θα πρέπει να θεωρούνται ελάχιστη απαίτηση. Εάν ένα IPS εφαρμόσει όλα τα προαναφερθέντα στοιχεία και ολοκληρώσει τις απαιτούμενες λειτουργίες, θα είναι μια υπηρεσία ποιοτική. Ωστόσο, εάν το IPS δεν πληροί αυτές τις προϋποθέσεις, ενδέχεται να τεθούν τα ακόλουθα προβλήματα και πρέπει να αντιμετωπιστούν. [23]

4.4. Ζητήματα γύρω από το σύστημα IPS

Με οποιαδήποτε πρόοδο στην τεχνολογία υπάρχουν σφάλματα για την επιδιόρθωση και η ταχύτητα του δικτύου θα υποφέρει ως αποτέλεσμα. Τα ακόλουθα είναι ορισμένα προβλήματα με τον κακό σχεδιασμό ή την εφαρμογή ενός προϊόντος IPS. υπάρχει αριθμός περιοχών προκλήσεων για την εφαρμογή μιας συσκευής IPS που δεν χρειάζεται να αντιμετωπίζουν κατά την εκτέλεση προϊόντων IDS παθητικής λειτουργίας. Όλες αυτές οι προκλήσεις προέρχονται από το γεγονός ότι η συσκευή IPS έχει σχεδιαστεί για να λειτουργεί σε σειρά, παρουσιάζοντας ένα πιθανό σημείο εμπλοκής και ένα μόνο σημείο αποτυχίας. Εάν αποτύχει ένα παθητικό IDS, το χειρότερο που μπορεί να συμβεί είναι ότι ορισμένες απόπειρες επιθέσεων ενδέχεται να περάσουν απαρατήρητες. [22, 50]

Εάν μια συσκευή IPS σε σειρά αποτύχει, μπορεί να επηρεάσει σοβαρά την απόδοση του δικτύου. Ο λανθάνων χρόνος μπορεί να οδηγήσει σε απαράδεκτες τιμές, ή ίσως εάν η συσκευή αποτύχει, θα κλείσει, στην οποία περίπτωση προκύπτει η κατάσταση μιας αυτοπροκαλούμενης κατάστασης DoS. Ακόμη και αν η συσκευή IPS δεν αποτύχει εντελώς, εξακολουθεί να έχει τη δυνατότητα να λειτουργήσει ως συμφόρηση, αυξάνοντας τον λανθάνοντα χρόνο και μειώνοντας την απόδοση καθώς αγωνίζεται να συμβληθεί με δυνητικά ένα gigabit ή περισσότερη κυκλοφορία δικτύου, ειδικά εάν υπάρχει ένα σημαντικό σύνολο που φορτώνεται. [21]

Τα πακέτα που απορρίπτονται είναι επίσης προβληματικά: εάν ακόμη και ένα από αυτά τα πακέτα που έπεσαν είναι ένα πακέτο που χρησιμοποιείται στη ροή δεδομένων exploit, είναι πιθανό να χαθεί ολόκληρη η εκμετάλλευση. Ένα άλλο πιθανό πρόβλημα είναι το ψευδώς θετικό. Το ψευδώς θετικό συμβαίνει όταν μια εκμετάλλευση δεν κατασκευάζεται αρκετά προσεκτικά, έτσι ώστε η νόμιμη κυκλοφορία να μπορεί να την αναγκάσει να πυροβολήσει τυχαία. Αν και απλώς ενοχλητικό σε μια παθητική συσκευή IDS, τα αποτελέσματα μπορεί να είναι πολύ πιο σοβαρά και εκτεταμένα σε μια συσκευή IPS σε σειρά. Και πάλι, το αποτέλεσμα είναι μια αυτοπροκαλούμενη κατάσταση DoS, Από ορισμένες απόψεις, οι δυνατότητες απόδοσης και ανίχνευσης είναι το μικρότερο από τα προβλήματα. Το πρόβλημα με ένα προϊόν Gigabit IPS είναι, από τη φύση και τις δυνατότητές του, ο όγκος των δεδομένων προειδοποίησης που είναι πιθανό να δημιουργήσει. Σε ένα πολυσύχναστο δίκτυο, πολλές τέτοιες ειδοποιήσεις θα δημιουργηθούν σε μία εργάσιμη ημέρα. [20]

4.5. Περαιτέρω εξελίξεις

Τα υφιστάμενο προϊόν, το IPS αναπτύσσεται και ενισχύεται πάντα. Η συνεχής ανάπτυξη των υφιστάμενων IPS ελπίζουμε ότι θα ενσωματώσει συστατικά στοιχεία που βασίζονται στη συμπεριφορά. Σε αντίθεση με τα εργαλεία ids ή ανίχνευσης ιών, η IPS που βασίζεται στη συμπεριφορά δεν ανταποκρίνεται σε καθιερωμένες κυκλοφοριακές πτώσεις ή σε εξέταση συνημμένων.

Οι παραδοσιακές προσεγγίσεις στις επιθέσεις του Κόκκινου Κώδικα ή της Νίμδας ήταν να αναζητήσουν μοτίβα κώδικα και μετά να αναλάβουν δράση. [15] Μέχρι να αναπτυχθεί μια υπογραφή επίθεσης, ήταν πολύ αργά για να αποφευχθεί μια επίθεση. [53] Θα μπορούσε να ειπωθεί ότι το IPS που βασίζεται στη συμπεριφορά απλά σκιαγραφεί διαφορετικά σημάδια επίθεσης. Με την κατάρτιση προφίλ των κλήσεων αντί για μεμονωμένα μοτίβα επίθεσης, το IPS που βασίζεται στη συμπεριφορά εφαρμόζει μια χαμηλότερη κοινή προσέγγιση του ατόμου στο πρόβλημα. Το μειονέκτημα αυτού θα ήταν η δημιουργία ψευδώς θετικών αποτελεσμάτων, με αποτέλεσμα το IPS να απαγορεύσει τη νόμιμη κυκλοφορία. Αυτή η προσέγγιση απλοποιεί τη συντήρηση για τον τελικό χρήστη, επειδή οι ενημερώσεις ευπάθειας ως απάντηση σε συγκεκριμένες απειλές δεν χρειάζεται να είναι σε ισχύ για να αποφευχθεί η επιτυχία μιας συγκεκριμένης επίθεσης. Εάν συμβεί επίθεση και η πολιτική δεν επιτρέπει τη συμπεριφορά της, η επίθεση δεν είναι επιτυχής. Το IPS που βασίζεται στη συμπεριφορά αντιπροσωπεύει την αναδυόμενη γενιά τεχνολογίας ασφάλειας. Αντί να επικεντρώνει στην αντιδραστική διόρθωση, η προληπτική συμπεριφορά που βασίζεται στο IPS εξετάζει τη δραστηριότητα του δικτύου όπως συμβαίνει και λαμβάνει άμεσα μέτρα για την πρόληψη της εκτέλεσης κακόβουλων συμπεριφορών. [14]

Εν κατακλείδι, το σύστημα IPS δεν είναι το μόνο στοιχείο που είναι απαραίτητο για την ασφάλεια του δικτύου, είναι κάτι περισσότερο από μια *«αδιέξοδη»* λύση ασφαλείας. Η ιδέα του IPS ξεκίνησε με την έναρξη του τείχους προστασίας και αυτά τα νέα συστήματα είναι απλώς μια άλλη βελτίωση σε σχέση με την τεχνολογία τείχους προστασίας. Είναι *«ευφυή»* τείχη προστασίας, καθώς οι δυνατότητες επιθεώρησης τους είναι ισχυρότερες, πιο εξελιγμένες, πιο αποτελεσματικές και πιο αποτελεσματικές στην εφαρμογή τους. [52] Ωστόσο, παρά την πρόοδό τους, τα συστήματα αυτά δεν είναι αλάνθαστα και δεν θα πρέπει να είναι η μόνη τεχνολογία που χρησιμοποιείται σε ένα εις βάθος αμυντικό μοντέλο. Κατά κανόνα, μια IPS θα πρέπει να είναι μια πύλη ή μια συσκευή περιγράμματος για να αποκλείσει επιθέσεις πριν φτάσουν στο εταιρικό τείχος προστασίας ή εισέλθουν στο δίκτυο. Ένα IPS δεν θα αντικαταστήσει ένα τείχος προστασίας, αλλά θα πρέπει στην πραγματικότητα να κάνει το

τείχος προστασίας πιο αποτελεσματικό με τον έλεγχο και τον αποκλεισμό της πλειοψηφίας των προβλημάτων στην άκρη του δικτύου.[19] Πολλές επιχειρήσεις αναπτύσσουν προϊόντα IPS σε συνδυασμό με ids ή IPS που βασίζονται σε κεντρικούς υπολογιστή για μια «*πολυεπίπεδη*» άμυνα. Ένας μικρός αριθμός επιχειρήσεων που επιθυμούν να μειώσουν τα γενικά έξοδα πειραματίζονται με ένα διαχειριζόμενο IPS που παρέχεται από ένα αξιόπιστο τρίτο μέρος. Το IPS είναι μια τεχνολογία που θα βοηθήσει ολόκληρη την κοινότητα ασφάλειας δικτύων στην ανάπτυξη μιας συνολικής στρατηγικής. Είναι ένα μέρος μιας ολόκληρης στρατηγικής, η οποία, μπορεί να διασφαλιστεί, θα συνεχίσει να εξελίσσεται με την πάροδο του χρόνου και θα εξελιχθεί σε κάτι που χρησιμοποιείται από τους επαγγελματίες ασφαλείας παντού. [18]

Κεφάλαιο 5ο: «Προφύλαξη από εισβολές δικτύου»

5.1. Προληπτικά μέτρα

Οι περισσότεροι χρήστες υπολογιστών γνωρίζουν ότι η χρήση του Διαδικτύου ενέχει κινδύνους για την ασφάλεια. Θα ήταν λογικό να λαμβάνουν προφυλάξεις για την ελαχιστοποίηση της έκθεσης τους σε επιθέσεις. Ευτυχώς, υπάρχουν διάφορες επιλογές στους χρήστες υπολογιστών να ενισχύσουν τα συστήματά τους με μέτρα ασφαλείας ώστε να μειώσουν τους κινδύνους.[65]

- Έλενχος πρόσβασης «Access Control»: Στην ασφάλεια υπολογιστών, ο έλεγχος πρόσβασης αναφέρεται σε μηχανισμούς που επιτρέπουν στους χρήστες να εκτελούν λειτουργίες μέχρι το εξουσιοδοτημένο επίπεδό τους και περιορίζουν τους χρήστες από την εκτέλεση μη εξουσιοδοτημένων λειτουργιών.

  Ο έλεγχος πρόσβασης περιλαμβάνει:

  - Αυθεντικοποίηση χρηστών
  - Εξουσιοδότηση των προνομίων τους
  - Έλεγχος για την παρακολούθηση και καταγραφή των ενεργειών των χρηστών.

  Όλοι οι χρήστες υπολογιστών είναι εξοικειωμένοι με κάποιο είδος ελέγχου πρόσβασης.

Εικόνα 5.1 Access Control

Αυθεντικοποίηση είναι η διαδικασία επαλήθευσης της ταυτότητας ενός χρήστη. Η αυθεντικοποίηση βασίζεται συνήθως σε έναν ή περισσότερους από αυτούς τους παράγοντες:

- Κάτι που γνωρίζει ο χρήστης, όπως κωδικός πρόσβασης ή PIN
- Κάτι που έχει ο χρήστης, όπως μια έξυπνη κάρτα ή ένα κουπόνι
- Κάτι προσωπικό σχετικά με τον χρήστη, όπως ένα δακτυλικό αποτύπωμα, μοτίβο αμφιβληστροειδούς (retinal pattern) ή αναγνώρηση προσώπου.

Η χρήση ενός μόνο παράγοντα, ακόμη και αν προσφέρονται πολλαπλά αποδεικτικά στοιχεία, θεωρείται αδύναμη αυθεντικοποίηση. Ένας συνδυασμός δύο παραγόντων, όπως ένας κωδικός πρόσβασης και ένα δακτυλικό αποτύπωμα, που είναι γνωστός ως έλεγχος ταυτότητας δύο παραγόντων (ή πολλαπλών παραγόντων), θεωρείται ισχυρός έλεγχος ταυτότητας.[65]

Εξουσιοδότηση είναι η διαδικασία καθορισμού του τι μπορεί να κάνει ένας χρήστης που έχει πιστοποιηθεί. Τα περισσότερα λειτουργικά συστήματα έχουν ένα καθιερωμένο σύνολο δικαιωμάτων που σχετίζονται με την ανάγνωση, την εγγραφή ή την εκτέλεση πρόσβασης. Για παράδειγμα, ένας συνηθισμένος χρήστης μπορεί να έχει δικαίωμα ανάγνωσης ενός συγκεκριμένου αρχείου αλλά όχι να γράψει σε αυτό, ενώ ένας root ή superuser θα έχει πλήρη προνόμια για να κάνει οτιδήποτε.

Ο έλεγχος είναι απαραίτητος για να διασφαλιστεί ότι οι χρήστες είναι υπόλογοι. Τα συστήματα ηλεκτρονικών υπολογιστών καταγράφουν ενέργειες στο σύστημα σε αρχεία καταγραφής. Για λόγους ασφαλείας, είναι ανεκτίμητα εγκληματολογικά εργαλεία για την αναδημιουργία και την ανάλυση περιστατικών. Για παράδειγμα, ένας χρήστης που επιχειρεί πολλές αποτυχημένες συνδέσεις μπορεί να θεωρηθεί ως εισβολέας.

- Κλείσιμο θυρών «Closing Ports»: Πρωτόκολλα επιπέδου μεταφοράς, δηλαδή το πρωτόκολλο ελέγχου μετάδοσης (TCP) και το αρχείο δεδομένων χρήστη (User Datagram) Πρωτόκολλο (UDP), αναγνωρίζουν εφαρμογές που επικοινωνούν μεταξύ τους μέσω αριθμών θυρών. Οι αριθμοί θύρας 1 έως 1023 είναι γνωστοί και εκχωρούνται από το Internet Assigned Numbers Authority (IANA) σε τυποποιημένες

υπηρεσίες που εκτελούνται με δικαιώματα root. Για παράδειγμα, οι διακομιστές Web ακούνε στη θύρα TCP 80 για αιτήσεις πελατών. Αριθμοί θυρών 1024 έως 49151 χρησιμοποιούνται από διάφορες εφαρμογές με συνηθισμένα προνόμια χρήστη. Οι αριθμοί θύρας πάνω από 49151 χρησιμοποιούνται δυναμικά από τις εφαρμογές.

Είναι καλή πρακτική να κλείνετε τις θύρες που είναι περιττές, επειδή οι επιτιθέμενοι μπορούν να χρησιμοποιήσουν ανοικτές θύρες, ιδίως εκείνες που βρίσκονται σε υψηλότερο εύρος. Για παράδειγμα, το δούρειο ίππο είναι γνωστό ότι χρησιμοποιεί τη θύρα 27374 από προεπιλογή, ενώ το Netbus χρησιμοποιεί τη θύρα 12345. Ωστόσο, το κλείσιμο των θυρών δεν εγγυάται από μόνο του την ασφάλεια ενός κεντρικού υπολογιστή. Ορισμένοι κεντρικοί υπολογιστές πρέπει να διατηρούν τη θύρα TCP 80 ανοιχτή για το πρωτόκολλο μεταφοράς υπερκειμένου (HTTP), αλλά οι επιθέσεις μπορούν να πραγματοποιηθούν μέσω αυτής της θύρας.[63]

- Έλεγχος ευπάθειας και επιδιόρθωση «Vulnerability Testing and Patching»:

  Όπως αναφέρθηκε προηγουμένως, τα τρωτά σημεία είναι αδυναμίες του λογισμικού που μπορούν να χρησιμοποιηθούν για την παραβίαση ενός υπολογιστή. Το ευάλωτο λογισμικό περιλαμβάνει όλους τους τύπους λειτουργικών συστημάτων και προγραμμάτων εφαρμογών. Νέα τρωτά σημεία ανακαλύπτονται συνεχώς με διάφορους τρόπους. Οι νέες ευπάθειες που ανακαλύπτονται από ερευνητές ασφαλείας συνήθως αναφέρονται εμπιστευτικά στον προμηθευτή, στον οποίο δίνεται χρόνος για να μελετήσει την ευπάθεια και να αναπτύξει μια λύση. Από όλες τις ευπάθειες που αποκαλύφθηκαν το 2007, το 50% μπορούσε να διορθωθεί μέσω διορθώσεων από τους προμηθευτές . Όταν είναι έτοιμο, ο πωλητής θα δημοσιεύσει την ευπάθεια, ελπίζουμε μαζί με ένα patch. Έχει υποστηριχθεί ότι η δημοσίευση των ευπαθειών θα βοηθήσει τους επιτιθέμενους. Αν και αυτό μπορεί να είναι αλήθεια, η δημοσίευση προάγει επίσης την ευαισθητοποίηση ολόκληρης της κοινότητας. Οι διαχειριστές συστημάτων θα είναι σε θέση να αξιολογούν τα συστήματά τους και να λαμβάνουν τις κατάλληλες προφυλάξεις. Θα περίμενε κανείς ότι οι διαχειριστές συστημάτων θα γνώριζαν τις ρυθμίσεις παραμέτρων των υπολογιστών στο δίκτυό τους, αλλά σε μεγάλους οργανισμούς θα ήταν δύσκολο να παρακολουθούν τις πιθανές αλλαγές παραμέτρων που πραγματοποιούνται από τους χρήστες. Ο έλεγχος ευπάθειας προσφέρει έναν απλό τρόπο για να μάθουμε για τη διαμόρφωση των υπολογιστών σε ένα δίκτυο. Ο έλεγχος τρωτότητας είναι μια άσκηση διερεύνησης των συστημάτων για γνωστές ευπάθειες. Απαιτεί μια βάση δεδομένων με γνωστές ευπάθειες, μια γεννήτρια πακέτων και

ρουτίνες δοκιμής για τη δημιουργία μιας ακολουθίας πακέτων για τον έλεγχο μιας συγκεκριμένης ευπάθειας. Εάν βρεθεί μια ευπάθεια και υπάρχει διαθέσιμη ενημέρωση λογισμικού, ο εν λόγω κεντρικός υπολογιστής θα πρέπει να ενημερωθεί. [61]

- Antivirus and Antispyware εργαλεία: Ο πολλαπλασιασμός του κακόβουλου λογισμικού προκαλεί την ανάγκη για λογισμικό προστασίας από ιούς. Το λογισμικό Antivirus έχει αναπτυχθεί για να ανιχνεύει την παρουσία κακόβουλου λογισμικού, να αφαιρεί το κακόβουλο λογισμικό και να προστατεύει τον χρήστη από μελλοντικές μολύνσεις. Η ανίχνευση θα πρέπει ιδανικά να ελαχιστοποιεί ταυτόχρονα τα ψευδώς θετικά αποτελέσματα (ψευδείς συναγερμοί) και τα ψευδώς αρνητικά αποτελέσματα (μη εντοπισμένο κακόβουλο λογισμικό). Το λογισμικό antivirus αντιμετωπίζει μια σειρά από δύσκολες προκλήσεις:
  - Οι τακτικές του κακόβουλου λογισμικού είναι εξελιγμένες και εξελίσσονται συνεχώς.
  - Ακόμη και το λειτουργικό σύστημα στους μολυσμένους υπολογιστές δεν είναι αξιόπιστο.
  - Το κακόβουλο λογισμικό μπορεί να υπάρχει εξ ολοκλήρου στη μνήμη χωρίς να επηρεάζει τα αρχεία.
  - Το κακόβουλο λογισμικό μπορεί να επιτεθεί σε διαδικασίες προστασίας από ιούς.
  - Το φορτίο επεξεργασίας για το λογισμικό προστασίας από ιούς δεν μπορεί να υποβαθμίσει την απόδοση του υπολογιστή ώστε οι χρήστες να ενοχλούνται και να απενεργοποιούν το λογισμικό προστασίας από ιούς.

  Μία από τις απλούστερες εργασίες που εκτελεί το λογισμικό προστασίας από ιούς είναι η σάρωση αρχείων. Αυτή η διαδικασία συγκρίνει τα bytes στα αρχεία με γνωστές υπογραφές(signature files) που ειναι μοτίβα bytes ενδεικτικά ενός γνωστού κακόβουλου λογισμικού. Αντιπροσωπεύει τη γενική προσέγγιση της ανίχνευσης με βάση την υπογραφή. Όταν συλλαμβάνεται νέο κακόβουλο λογισμικό, αναλύεται για μοναδικά χαρακτηριστικά που μπορούν να περιγραφούν σε μια υπογραφή.
  Η νέα υπογραφή διανέμεται ως ενημερώσεις σε προγράμματα προστασίας από ιούς. Το Antivirus αναζητά την υπογραφή κατά τη σάρωση αρχείων, και εάν βρεθεί ταύτιση, η υπογραφή προσδιορίζει συγκεκριμένα το κακόβουλο λογισμικό. Ωστόσο, η μέθοδος αυτή έχει σημαντικά μειονεκτήματα: η ανάπτυξη και η δοκιμή νέων υπογραφών απαιτεί χρόνο. Οι χρήστες πρέπει να διατηρούν τα αρχεία υπογραφών τους

ενημερωμένα. Ενα νέο κακόβουλο λογισμικό χωρίς γνωστή υπογραφή μπορεί να διαφύγει της ανίχνευσης.

- Έλεγχος πρόσβασης δικτύου «Network Access Control»:

  Ένας ευάλωτος host μπορεί να θέσει σε κίνδυνο όχι μόνο τον εαυτό του αλλά και μια ολόκληρη κοινότητα. Πρώτον, ένας ευάλωτος κεντρικός υπολογιστής μπορεί να προσελκύσει επιθέσεις. Εάν παραβιαστεί, ο κεντρικός υπολογιστής θα μπορούσε να χρησιμοποιηθεί για την εξαπόλυση επιθέσεων σε άλλους κεντρικούς υπολογιστές. Ο εκτεθειμένος κεντρικός υπολογιστής μπορεί να δώσει πληροφορίες στον επιτιθέμενο ή μπορεί να υπάρχουν σχέσεις εμπιστοσύνης μεταξύ των κεντρικών υπολογιστών που θα μπορούσαν να βοηθήσουν τον επιτιθέμενο. Σε κάθε περίπτωση, δεν είναι επιθυμητό να έχετε στο δίκτυό σας έναν υποδοχέα με αδύναμη προστασία. Η γενική ιδέα του ελέγχου πρόσβασης στο δίκτυο (NAC), είναι να περιοριστεί η πρόσβαση ενός κεντρικού υπολογιστή σε ένα δίκτυο, εκτός εάν ο κεντρικός υπολογιστής μπορεί να αποδείξει ότι διαθέτει ισχυρή ασφάλεια. Η διαδικασία NAC περιλαμβάνει τον κεντρικό υπολογιστή, το δίκτυο (συνήθως δρομολογητές ή μεταγωγείς και διακομιστές) και μια πολιτική ασφαλείας. Η κατάσταση ασφαλείας ενός κεντρικού υπολογιστή περιλαμβάνει τη διεύθυνση IP, το λειτουργικό σύστημα, το λογισμικό προστασίας από ιούς, το προσωπικό τείχος προστασίας και το σύστημα ανίχνευσης εισβολών του κεντρικού υπολογιστή.

5.2. Παρακολούθηση και ανίχνευση εισβολών

Τα προληπτικά μέτρα είναι πολύ σημαντικά γιατί συμβάλλουν στη μείωση των κινδύνων από διάφορες επιθέσεις, ομως είναι πρακτικά αδύνατο να αποτραπούν όλες οι επιθέσεις. Γι' αυτό η ανίχνευση εισβολών είναι επίσης απαραίτητη για την ανίχνευση και διάγνωση κακόβουλων δραστηριοτήτων, π.χ. έναν συναγερμό διάρρηξης. Η ανίχνευση εισβολών είναι ουσιαστικά ένας συνδυασμός παρακολούθησης, ανάλυσης και απόκρισης. Συνήθως ένα IDS υποστηρίζει μια κονσόλα για ανθρώπινη διεπαφή και εμφάνιση. Η παρακολούθηση και η ανάλυση θεωρούνται συνήθως παθητικές τεχνικές, επειδή δεν παρεμβαίνουν στις τρέχουσες δραστηριότητες. Η τυπική αντίδραση του IDS είναι μια ειδοποίηση προς τους διαχειριστές συστημάτων, οι οποίοι μπορεί να επιλέξουν να συνεχίσουν την περαιτέρω διερεύνηση ή όχι. Συνοψίζοντας, τα παραδοσιακά IDS δεν προσφέρουν μεγάλη ανταπόκριση πέραν των ειδοποιήσεων, με την παραδοχή ότι τα περιστατικά ασφαλείας χρειάζονται ανθρώπινη εμπειρία και κρίση για την παρακολούθηση.[50]

Η ακρίβεια ανίχνευσης είναι το κρίσιμο πρόβλημα για την ανίχνευση εισβολών. Η ανίχνευση εισβολών θα πρέπει ιδανικά να ελαχιστοποιεί τα ψευδώς θετικά (φυσιολογικά περιστατικά που εκλαμβάνονται λανθασμένα ως ύποπτα) και τα ψευδώς αρνητικά (κακόβουλα περιστατικά που διαφεύγουν της ανίχνευσης). Φυσικά, τα ψευδώς αρνητικά αποτελέσματα είναι αντίθετα με τον ουσιαστικό σκοπό της ανίχνευσης εισβολών. Τα ψευδώς θετικά αποτελέσματα είναι επίσης επιβλαβή, επειδή είναι ενοχλητικά για τους διαχειριστές συστημάτων, οι οποίοι πρέπει να σπαταλούν χρόνο για τη διερεύνηση ψευδών συναγερμών. Η ανίχνευση εισβολών θα πρέπει επίσης να επιδιώκει κάτι περισσότερο από τον εντοπισμό περιστατικών ασφαλείας. Εκτός από την αναφορά των γεγονότων ενός περιστατικού, η ανίχνευση εισβολής θα πρέπει να εξακριβώνει τη φύση του περιστατικού, τον δράστη, τη σοβαρότητα (κακόβουλο έναντι ύποπτου), την έκταση και τις πιθανές συνέπειες (όπως η μετάβαση από έναν στόχο σε περισσότερους στόχους).

Οι προσεγγίσεις IDS μπορούν να κατηγοριοποιηθούν με δύο τρόπους. Ένας τρόπος είναι να διακρίνουμε τα IDS που βασίζονται στον κεντρικό υπολογιστή και τα IDS που βασίζονται στο δίκτυο, ανάλογα με το πού γίνεται η ανίχνευση. Ένα IDS με βάση τον κεντρικό υπολογιστή παρακολουθεί έναν μεμονωμένο κεντρικό υπολογιστή, ενώ ένα IDS με βάση το δίκτυο λειτουργεί σε πακέτα δικτύου. Ένας άλλος τρόπος για να δείτε τα IDS είναι η προσέγγισή τους στην ανάλυση. Οι δύο προσεγγίσεις ανάλυσης είναι η ανίχνευση κατάχρησης (με βάση την υπογραφή) και η ανίχνευση ανωμαλίας (με βάση τη συμπεριφορά). Οι δύο αυτές απόψεις είναι συμπληρωματικές και συχνά χρησιμοποιούνται σε συνδυασμό.[50]

5.2.1.Παρακολούθηση με βάση τον κεντρικό υπολογιστή «host-based Monitoring»

Το IDS που βασίζεται σε κεντρικό υπολογιστή εκτελείται σε έναν κεντρικό υπολογιστή και παρακολουθεί τις δραστηριότητες του συστήματος για ενδείξεις ύποπτης συμπεριφοράς. Παραδείγματα θα μπορούσαν να είναι αλλαγές στο μητρώο του συστήματος, επανειλημμένες αποτυχημένες προσπάθειες σύνδεσης, ή εγκατάσταση μιας κερκόπορτας. Τα IDS με βάση τον κεντρικό υπολογιστή συνήθως παρακολουθούν αντικείμενα του συστήματος, διεργασίες και περιοχές μνήμης. Για κάθε αντικείμενο του συστήματος, το IDS συνήθως παρακολουθεί χαρακτηριστικά όπως δικαιώματα, μέγεθος, ημερομηνίες τροποποίησης και κατακερματισμένα περιεχόμενα, για να αναγνωρίζει τις αλλαγές. Ένα πρόβλημα που αντιμετωπίζει ενα IDS με βάση τον κεντρικό υπολογιστή (host-based IDS) είναι η πιθανή παραποίηση από έναν εισβολέα. Για παράδειγμα εάν ένας επιτιθέμενος αποκτήσει τον έλεγχο ενός συστήματος, το IDS δεν μπορεί να είναι αξιόπιστο. Έτσι, η ειδική προστασία του IDS από την παραποίηση θα

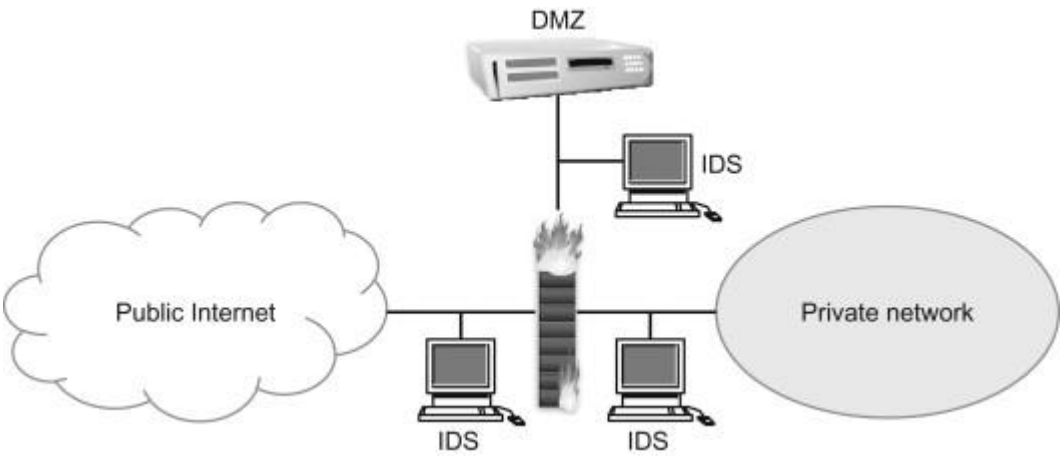
πρέπει να ενσωματωθεί σε έναν κεντρικό υπολογιστή. Ένα IDS με βάση τον κεντρικό υπολογιστή δεν αποτελεί από μόνο του μια ολοκληρωμένη λύση. Αν και η παρακολούθηση του κεντρικού υπολογιστή είναι λογική, έχει τρία σημαντικά μειονεκτήματα:

- Η ορατότητα περιορίζεται σε έναν μόνο κεντρικό υπολογιστή.
- Η διαδικασία IDS καταναλώνει πόρους, επηρεάζοντας ενδεχομένως την απόδοση του κεντρικού υπολογιστή.
- Οι επιθέσεις δεν θα γίνουν αντιληπτές μέχρι να φτάσουν ήδη στον host.

Τα IDS με βάση τον κεντρικό υπολογιστή και τα IDS με βάση το δίκτυο χρησιμοποιούνται συχνά μαζί για να συνδυάσουν τις δυνάμεις τους.

5.2.2. Παρακολούθηση της κυκλοφορίας «Traffic Monitoring»

Τα IDS που βασίζονται στο δίκτυο συνήθως παρακολουθούν τα πακέτα δικτύου για ενδείξεις αναγνώρισης, εκμεταλλεύσεων, επιθέσεων DoS και κακόβουλου λογισμικού. Τα IDS που βασίζονται στο δίκτυο μπορούν να δουν την κυκλοφορία για έναν πληθυσμό κεντρικών υπολογιστών, μπορούν να αναγνωρίσουν μοτίβα που μοιράζονται πολλοί κεντρικοί υπολογιστές και έχουν τη δυνατότητα να δουν επιθέσεις πριν φτάσουν στους κεντρικούς υπολογιστές. Τα IDS τοποθετούνται σε διάφορες θέσεις για διαφορετικές προβολές, όπως φαίνεται στο Σχήμα 5.2. Ένα IDS εκτός τείχους προστασίας είναι χρήσιμο για την εκμάθηση κακόβουλων δραστηριοτήτων στο Διαδίκτυο. Ένα IDS στην DMZ θα βλέπει τις επιθέσεις που προέρχονται από το Διαδίκτυο και μπορούν να περάσουν από το εξωτερικό τείχος προστασίας στους δημόσιους διακομιστές. Τέλος, ένα IDS στο ιδιωτικό δίκτυο είναι απαραίτητο για τον εντοπισμό τυχόν επιθέσεων που είναι σε θέση να εισβάλουν επιτυχώς στην περιμετρική ασφάλεια.



Σχήμα 5.2: IDS που παρακολουθούν διάφορες ζώνες δικτύου.

5.2.3. Ανίχνευση βάση υπογραφής «Signature-Based Detection»

Η ανίχνευση εισβολών με βάση την υπογραφή εξαρτάται από μοτίβα που προσδιορίζουν μοναδικά μια επίθεση. Εάν ένα περιστατικό ταιριάζει με μια γνωστή υπογραφή, η υπογραφή προσδιορίζει τη συγκεκριμένη επίθεση. Το κεντρικό ζήτημα είναι ο τρόπος ορισμού υπογραφών ή μοντέλων επιθέσεων. Εάν οι υπογραφές είναι πολύ συγκεκριμένες, μια αλλαγή στην τακτική επίθεσης θα μπορούσε να οδηγήσει σε ψευδώς αρνητικό (χαμένο συναγερμό). Μια υπογραφή επίθεσης πρέπει να είναι αρκετά ευρεία ώστε να καλύπτει μια ολόκληρη κατηγορία επιθέσεων. Από την άλλη πλευρά, εάν οι υπογραφές είναι πολύ γενικές, μπορεί να προκύψουν ψευδώς θετικά αποτελέσματα.[59]

Οι προσεγγίσεις που βασίζονται σε υπογραφές έχουν τρία εγγενή μειονεκτήματα:

- Οι υπογραφές απαιτούν χρόνο για να αναπτυχθούν για νέες επιθέσεις.
- Οι νέες υπογραφές πρέπει να διανέμονται συνεχώς.
- Οι νέες επιθέσεις μπορεί να μην γίνουν αντιληπτές εάν δεν είναι γνωστή η αντίστοιχη υπογραφή.

Το Snort είναι ένα δημοφιλές παράδειγμα ενός IDS με βάση την υπογραφή (www. snort. org). Οι υπογραφές του Snort είναι κανόνες που ορίζουν πεδία που ταιριάζουν με πακέτα πληροφοριών σχετικά με την αναπαριστώμενη επίθεση. Το Snort είναι εφοδιασμένο με περισσότερους από 1800 κανόνες που καλύπτουν ένα ευρύ φάσμα επιθέσεων, ενώ συνεχώς γράφονται νέοι κανόνες.

5.2.4. Ανωμαλίες συμπεριφοράς «Behavior Anomalies»

Ένα IDS βασισμένο στη συμπεριφορά είναι ελκυστικό για τη δυνατότητά του να αναγνωρίζει νέες επιθέσεις χωρίς γνωστή υπογραφή. Προϋποθέτει ότι οι επιθέσεις θα είναι διαφορετικές από την κανονική συμπεριφορά. Έτσι, το κρίσιμο ζήτημα είναι πώς να οριστεί η φυσιολογική συμπεριφορά, και οτιδήποτε εκτός του φυσιολογικού (ανώμαλο) χαρακτηρίζεται ως ύποπτο. Μια συνήθης προσέγγιση είναι ο ορισμός της κανονικής συμπεριφοράς με στατιστικούς όρους, οι οποίοι επιτρέπουν αποκλίσεις εντός ενός εύρους.[62]

Οι προσεγγίσεις που βασίζονται στη συμπεριφορά έχουν σημαντικές προκλήσεις. Πρώτον, η φυσιολογική συμπεριφορά βασίζεται στη συμπεριφορά του παρελθόντος. Συνεπώς, για την

εκπαίδευση του IDS πρέπει να είναι διαθέσιμα δεδομένα σχετικά με την προηγούμενη συμπεριφορά. Δεύτερον, η συμπεριφορά μπορεί και αλλάζει με την πάροδο του χρόνου, οπότε κάθε προσέγγιση IDS πρέπει να είναι προσαρμοστική. Τρίτον, οι ανωμαλίες είναι απλώς ασυνήθιστα γεγονότα, όχι απαραίτητα κακόβουλα. Ένα IDS βασισμένο στη συμπεριφορά μπορεί να υποδείξει περιστατικά προς περαιτέρω διερεύνηση, αλλά δεν είναι καλό στο να διακρίνει την ακριβή φύση των επιθέσεων.

5.2.5. Συστήματα πρόληψης εισβολών «Intrusion Prevention Systems»

Τα IDS είναι παθητικές τεχνικές. Συνήθως ειδοποιούν τον διαχειριστή συστημάτων για να διερευνήσει περαιτέρω και να λάβει τα κατάλληλα μέτρα. Η ανταπόκριση μπορεί να είναι αργή εάν ο διαχειριστής συστημάτων είναι απασχολημένος ή εάν η διερεύνηση του περιστατικού είναι χρονοβόρα.

Μια παραλλαγή που ονομάζεται σύστημα πρόληψης εισβολών (IPS) επιδιώκει να συνδυάσει τις λειτουργίες παρακολούθησης και ανάλυσης ενός IDS με πιο ενεργές αυτοματοποιημένες αντιδράσεις, όπως την αυτόματη αναδιαμόρφωση των τειχών προστασίας για τον αποκλεισμό μιας επίθεσης. Ένα IPS στοχεύει σε ταχύτερη απόκριση από ό,τι μπορεί να επιτύχει ο άνθρωπος, αλλά η ακρίβειά του εξαρτάται από τις ίδιες τεχνικές με το IDS. Η απάντηση δεν πρέπει να βλάψει τη νόμιμη κυκλοφορία, επομένως η ακρίβεια είναι κρίσιμη.[41]

5.3. Αντιδραστικά μέτρα «Reactive Measures»

Όταν ανιχνεύεται και αναλύεται μια επίθεση, οι διαχειριστές συστημάτων πρέπει να προβούν στην κατάλληλη αντίδραση της επίθεσης. Ένα από τα πιο βασικά στο θέμα της ασφάλειας είναι ότι η αντίδραση πρέπει να είναι ανάλογη της απειλής. Προφανώς, η απάντηση εξαρτάται από τις περιστάσεις, αλλά υπάρχουν διάφορες επιλογές. Γενικά, είναι δυνατό να μπλοκάρετε, να επιβραδύνετε, να τροποποιήσετε ή να ανακατευθύνετε οποιαδήποτε κακόβουλη κυκλοφορία. Δεν είναι δυνατόν να περιγραφεί κάθε πιθανή απάντηση. Εδώ περιγράφουμε μόνο δύο απαντήσεις: καραντίνα και εντοπισμός.

5.3.1. Καραντίνα «Quarantine»

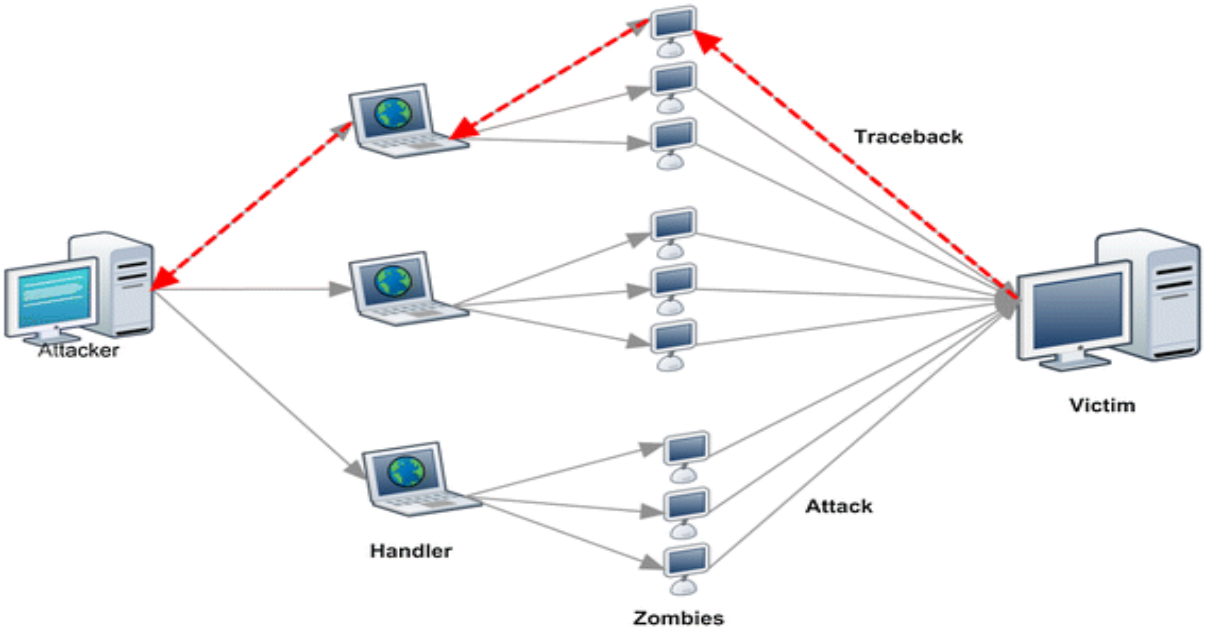
Η δυναμική καραντίνα στην ασφάλεια υπολογιστών είναι ανάλογη με την καραντίνα για τις μολυσματικές ασθένειες. Είναι μια κατάλληλη αντίδραση, ιδίως στο πλαίσιο του κακόβουλου λογισμικού, για να αποτρέψει έναν μολυσμένο υπολογιστή από το να μολύνει άλλους υπολογιστές. Το μολυσμένο αυτό κακόβουλο λογισμικό απαιτεί συνδεσιμότητα μεταξύ ενός μολυσμένου κεντρικού υπολογιστή και ενός νέου στόχου, οπότε είναι λογικό να διακόπτεται η συνδεσιμότητα μεταξύ κεντρικών υπολογιστών ή δικτύων ως μέσο παρεμπόδισης της περαιτέρω εξάπλωσης του κακόβουλου λογισμικού.

Εντός του δικτύου, η κυκλοφορία μπορεί να αποκλειστεί από τείχη προστασίας ή δρομολογητές με λίστες ελέγχου πρόσβασης. Οι λίστες ελέγχου πρόσβασης(ACLs) είναι παρόμοιες με τους κανόνες τείχους προστασίας, επιτρέποντας στους δρομολογητές να απορρίπτουν επιλεκτικά πακέτα.

5.3.2. Ανίχνευση ίχνους «Traceback»

Μία από τις κρίσιμες προοπτικές μιας επίθεσης είναι η ταυτότητα ή η τοποθεσία του δράστη. Δυστυχώς, ο εντοπισμός ενός επιτιθέμενου σε δίκτυα IP είναι σχεδόν αδύνατος διότι:

- Η διεύθυνση προέλευσης στα πακέτα IP μπορεί εύκολα να παραποιηθεί (πλαστογραφηθεί).
- Οι δρομολογητές είναι από τη σχεδίασή τους κενοί, χωρίς κατάσταση και δεν διατηρούν αρχεία των προωθούμενων πακέτων.
- Οι επιτιθέμενοι μπορούν να χρησιμοποιήσουν μια σειρά ενδιάμεσων υπολογιστών (που ονομάζονται " *stepping stones* " ή "zombies") για να πραγματοποιούν τις επιθέσεις τους.



Εικόνα 5.3 IP traceback mechanism

Οι ενδιάμεσοι υπολογιστές είναι συνήθως αθώοι και καταλαμβάνονται από ένα exploit ή κακόβουλο λογισμικό και τίθενται υπό τον έλεγχο του επιτιθέμενου. Στην πράξη, μπορεί να είναι δυνατόν να εντοπιστεί μια επίθεση μέχρι τον πλησιέστερο ενδιάμεσο host, αλλά ίσως είναι υπερβολικό να περιμένουμε να εντοπίσουμε μια επίθεση μέχρι τον πραγματικό επιτιθέμενο.

Για να εντοπιστεί η διαδρομή ενός πακέτου, κάποιες πληροφορίες παρακολούθησης πρέπει είτε να αποθηκεύονται στους δρομολογητές κατά την προώθηση του πακέτου είτε να μεταφέρονται στο πακέτο. Ένα παράδειγμα της πρώτης προσέγγισης είναι η αποθήκευση ενός κατακερματισμού ενός πακέτου για κάποιο χρονικό διάστημα. Εάν πραγματοποιηθεί επίθεση, ο κεντρικός υπολογιστής-στόχος θα ζητήσει από τους δρομολογητές ένα hash του πακέτου επίθεσης. Εάν ένας δρομολογητής έχει το hash, αυτό αποτελεί απόδειξη ότι το πακέτο προωθήθηκε από τον εν λόγω δρομολογητή. Για να μειωθεί η κατανάλωση μνήμης, αποθηκεύεται ο κατακερματισμός αντί για την αποθήκευση ολόκληρου του πακέτου. Η αποθήκευση είναι προσωρινή αντί για μόνιμη, ώστε οι δρομολογητές να μην ξεμένουν από μνήμη.

Κεφάλαιο 6ο: «Δημιουργία νέας στρατηγικής επίθεσης»

6.1. Εισαγωγή

Στον κατασκευαστικό τομέα, νέα προϊόντα αναπτύσσονται και πωλούνται συνεχώς ως το επόμενο καλύτερο πράγμα. Το ίδιο συμβαίνει στον κόσμο των εκμεταλλεύσεων υπολογιστών και των τρωτών σημείων. Όταν κυκλοφορήσει το πιο πρόσφατο θέμα ευπάθειας, υπάρχει ένας αγώνας δρόμου για τη δημιουργία ενός exploit που μπορεί να χρησιμοποιήσει αυτό το θέμα ευπάθειας προς όφελος του εισβολέα. Το ακόλουθο κεφάλαιο εξετάζει τη διαδικασία κατασκευής μιας τέτοιας εκμετάλλευσης.

Μια επίθεση σε ένα σύστημα υπολογιστή είναι συνήθως μια προσπάθεια παράκαμψης ή ανατροπής της ασφάλειας ενός συστήματος. Υπάρχουν δύο διαφορετικοί τύποι επίθεσης: ενεργητικοί και παθητικοί. Οι παθητικές επιθέσεις μπορούν να θεωρηθούν ως επιθέσεις που δεν έχουν πολλά ορατά σημάδια ότι συμβαίνουν. [8]

Για παράδειγμα, μια παθητική επίθεση θα μπορούσε να είναι η υποκλοπή και η ανάγνωση δεδομένων χωρίς να αλλάξουν τα δεδομένα. Οι ενεργές επιθέσεις είναι προσπάθειες τροποποίησης ή καταστροφής δεδομένων. Αυτό μπορεί να κυμαίνεται από το να κάνετε τα συστήματα εκτός λειτουργίας έως την αλλαγή εγγραφών ή ακόμη και τη διαγραφή τους. Οι ενεργές επιθέσεις είναι συνήθως οι πιο δημόσιες και επιζήμιες για τη φήμη του στόχου. Οι παθητικές επιθέσεις συχνά κοστίζουν το μεγαλύτερο χρηματικό ποσό στα θύματα, καθώς είναι συνήθως πράξεις βιομηχανικής κατασκοπείας. Μια στρατηγική επίθεσης είναι η ακολουθία των σαρώσεων (port scanning) για την αναγνώριση των αδυναμιών ενός συστήματος και η χρήση εργαλείων που απαιτούνται για την πραγματοποίηση της επίθεσης. Αυτό μπορεί να κυμαίνεται από μια τυχαία μετάδοση IP που στέλνει ένα exploit έως την εκτέλεση μιας σάρωσης για τον εντοπισμό ευάλωτων υπολογιστών πριν από την αποστολή της εκμετάλλευσης. Το κύριο συστατικό κάθε επιθετικής στρατηγικής είναι ο κώδικας εκμετάλλευσης στον οποίο θα επικεντρωθεί αυτό το κεφάλαιο.

Το μεγαλύτερο μέρος της αναγνώρισης ευπάθειας γίνεται ιδιωτικά. Ωστόσο, όταν αναφέρεται ένας, οι ακόλουθοι τέσσερις ιστότοποι είναι οι κύριοι διεθνείς οργανισμοί που αναφέρουν και δημοσιεύουν ευπάθειες. Αυτές οι τοποθεσίες έχουν πόρους σχετικά με τον προσδιορισμό του κώδικα εκμετάλλευσης που είναι ήδη διαθέσιμος και άλλων πόρων ασφαλείας: [9]

- http://www.cert.org/nav/index_red.html
- http://www.us-cert.gov/cas/techalerts/

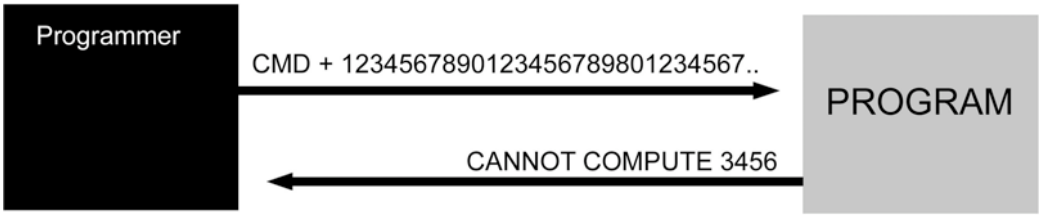
- http://www.sans.org/top20/
- http://cve.mitre.org/cve/

Άλλες τοποθεσίες που είναι αφιερωμένες στον εντοπισμό και τη δημοσίευση ευπαθειών είναι:

- http://www.securityfocus.com/bid

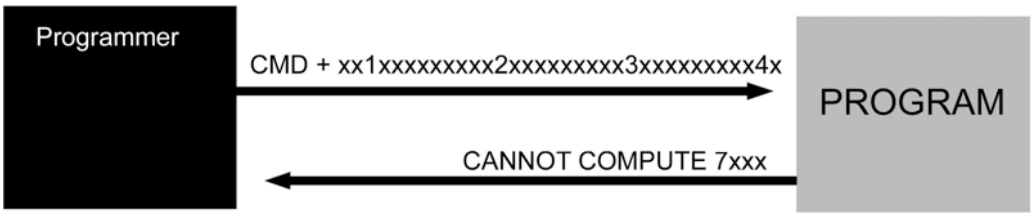
6.2. Υπολογισμός μήκους συμβολοσειράς

Μόλις ανακαλυφθεί το σφάλμα, θα γίνει μια σειρά δοκιμών για να ανακαλύψετε το μήκος του buffer. Αυτό είναι απαραίτητο επειδή το μήκος του buffer καθορίζει σε ποιο στάδιο θα τοποθετηθεί ο κώδικας που πρόκειται να γραφτεί στο πρόγραμμα στη συμβολοσειρά επίθεσης. Η πρώτη συμβολοσειρά που δοκιμάστηκε θα ήταν μια ακολουθία ψηφίων όπως 123456789012345678901 2... Σε αυτό το παράδειγμα, ο αριθμός 3 επιλέχθηκε για να επιστραφεί ως εξαίρεση (που σημαίνει ότι το πρόγραμμα δεν μπορούσε να υπολογίσει την τιμή).



Εικόνα 6.1 Υπολογισμός Συμβολοσειράς

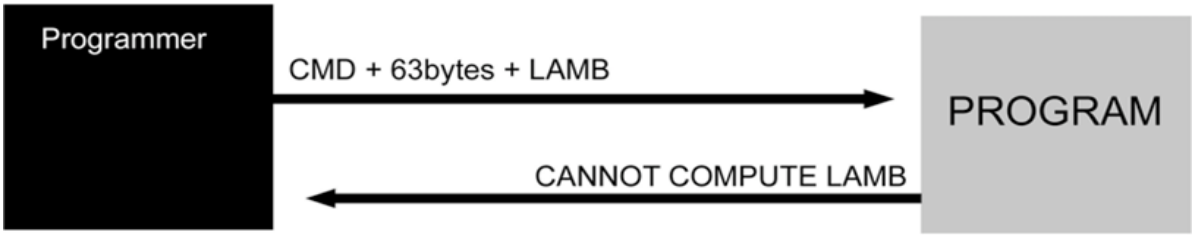
Η επόμενη ακολουθία που θα δοκιμαστεί θα είναι xx1xxxxxxxxxxxxxxxxxxxxx3xxx... κλπ. Αυτό συμβαίνει επειδή ο αριθμός 3 αντικαθίσταται με μια διαδοχική συμβολοσειρά αριθμών και όλοι οι άλλοι χαρακτήρες αντικαθίστανται με έναν τυχαίο χαρακτήρα. Στη συνέχεια, αν ο αριθμός 7 ήταν η εξαίρεση που επιστράφηκε, θα γνωρίζαμε τώρα ότι το μήκος του buffer ήταν 63. Είναι 63, όχι 73, επειδή η ακολουθία ξεκίνησε με 1 όχι 0.



Εικόνα 6.2 Υπολογισμός Συμβολοσειράς

Μήκος του buffer

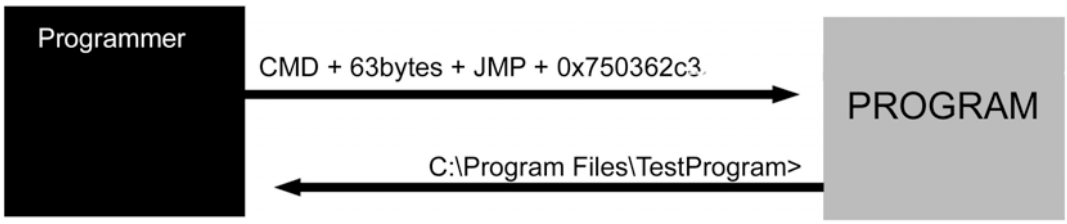
Τώρα που το μήκος έχει αποδειχθεί, ένας κώδικας μπορεί να εισαχθεί στο τέλος του buffer και θα εκτελεστεί από το πρόγραμμα. Εάν στάλθηκε το ακόλουθο buffer : CMD + 63 τυχαία byte + LAMB και η εξαίρεση που επιστράφηκε ήταν LAMB, τότε έχουμε αποδείξει ότι το buffer έχει μήκος 63 byte. [7]



Εικονα 6.3 Υπολογισμος μηκους buffer

6.3. Εισαγωγή της εντολής που πρόκειται να εκτελεστεί

Τώρα που έχει αποδειχθεί το μήκος του buffer, πρέπει να εισαχθεί μια εντολή προς εκτέλεση στο τέλος του buffer. Για παράδειγμα, εάν θέλαμε να εκτελεστεί ένα κέλυφος εντολών, τότε η σχετική εντολή συναρμολογητή με τη σχετική διεύθυνση μητρώου θα πρέπει να συνενωθεί στο τέλος της συμβολοσειράς. Για παράδειγμα, εάν θέλαμε το πρόγραμμα να μεταβεί στο κέλυφος εντολών, πρέπει να βρεθεί το μητρώο που περιέχει το κέλυφος εντολών. Υποθετικά, εάν το μητρώο ήταν 0x750362c3 τότε η εντολή θα είχε την εξής εμφάνιση: CMD + 63byte + μετάβαση στην εντολή + 0x750362c3



Εικόνα 6.4 Εισαγωγή εντολής

Κάνοντας μια εκμετάλλευση Beta

Τώρα που η εκμετάλλευση έχει δοκιμαστεί και λειτουργεί, ειναι στην κρίση του προγραμματιστή να αποφασίσει τι θα κάνει με την εκμετάλλευση. [5]

Χρήση του κατασκευασμένου κώδικα εκμετάλλευσης

Τώρα ο χάκερ έχει κωδικοποιήσει ένα exploit που θα χρησιμοποιήσουν για την ευπάθεια. Μπορεί να το κρατήσουν για την ιδιωτική τους συλλογή, αλλά πιθανότατα θα το προβάλλουν στη γενική κοινότητα. Αυτό παρέχει μια σαφή απεικόνιση του τρόπου με τον οποίο μεταβιβάζεται η γνώση του τρόπου γραφής ενός κατορθωτικού. Καθώς αναπτύσσονται νέοι τύποι εκμεταλλεύσεων, η μέθοδος για τη γραφή τους θα γίνει επίσης ευρύτερα γνωστή. Η καλύτερη άμυνα ενάντια σε αυτού του είδους τα

προβλήματα είναι η συνεχής παρακολούθηση της έγκαιρης ανίχνευσης και η συνεχής ενημέρωση των βιβλιοθηκών των ορισμών κατά των ιών και άλλων αντιμεγμάτων.

6.4. Συμπέρασμα

Ο στόχος αυτού του πειράματος ήταν να παρατηρήσει ένα δίκτυο υπό επίθεση, να καταγράψει ποιες ενέργειες έκαναν οι επιτιθέμενοι και να δώσει προτάσεις σχετικά με τους αμυντικούς μηχανισμούς που μπορούν να χρησιμοποιηθούν για την αντιμετώπιση επιθέσεων. [3]

Η συμπεριφορά του μαθητή σε αυτό το πείραμα έμοιαζε με τη συμπεριφορά των χάκερ λευκών καπελών. Οι μαθητές μιμήθηκαν τους χάκερ με λευκά καπέλα επειδή δεν κατέστρεψαν τις πληροφορίες του συστήματος. Οι μέθοδοι που χρησιμοποίησαν οι μαθητές μοντελοποιούσαν τις ενέργειες ενός τυπικού χάκερ. Οι μαθητές ολοκλήρωσαν την εκτύπωση , τη σάρωση, την απαρίθμηση, την απόκτηση πρόσβασης και την πειρατεία. [4]

Κατά τη δεύτερη φάση του πειράματος, όταν το λογισμικό IPS εισήχθη σε υπολογιστές του δικτύου, οι μαθητές δεν μπορούσαν να αποκτήσουν πρόσβαση στους υπολογιστές του δικτύου.

Τα αποτελέσματα δείχνουν ότι το πιο πρόσφατο λογισμικό είναι ικανοποιητικό, καθώς εμποδίζει τους φοιτητές της επιστήμης των πληροφοριών του τέταρτου έτους να αποκτήσουν πρόσβαση. Ωστόσο, πολλοί χάκερ στον πραγματικό κόσμο έχουν ανώτερες ικανότητες hacking και μπορεί να έχουν παρακάμψει τα προϊόντα IPS.

Ένας ικανός χάκερ μπορεί να ήταν σε θέση να παρακάμψει τα προϊόντα IPS χρησιμοποιώντας τα κατορθώματα υπερχείλισης buffer ή τις νέες στρατηγικές που η IPS δεν αναγνωρίζει. Αυτό το πρόβλημα των νέων στρατηγικών επίθεσης βρίσκεται σε εξέλιξη και όταν αναπτυχθούν νέα προϊόντα, θα πρέπει να επιλύσουν αυτήν τη δύσκολη θέση. [3]

Επίλογος

Αυτή η έρευνα ξεκίνησε για να ανακαλύψει πώς ένα IPS αποτρέπει την εισβολή. Η έρευνα σχεδίαζε να εντοπίσει τα λεπτά και προφανή σημάδια ενός δικτύου που δέχεται επίθεση. Η κίνηση δικτύου που χρησιμοποιείται για την ανίχνευση και την επίθεση στους ευάλωτους υπολογιστές. Κατά τη διάρκεια του πειράματος, εντοπίστηκαν συγκεκριμένες συμπεριφορές κατά τη διάρκεια της επίθεσης. Αυτοί οι σωτήρες καταγράφηκαν ως ο επιτιθέμενος που σαρώνει το δίκτυο, απαριθμεί το σύστημα-στόχο και αποκτά πρόσβαση στο σύστημα. Οι επιτιθέμενοι κατάφεραν να αποκτήσουν πρόσβαση, κάτι που ήταν θετικό αποτέλεσμα. Επειδή η συμπεριφορά των χάκερ μπορεί να προβλεφθεί, υπάρχουν μετρήσιμες ενέργειες που μπορεί να λάβει ένας διαχειριστής συστημάτων για να ελαχιστοποιήσει τις επιπτώσεις των επιθέσεων. [2] Παρά τα προβλήματα που σχετίζονται με τους τεχνικούς περιορισμούς των επιτιθέμενων, απτά οφέλη από το αποτέλεσμα αυτού του πειράματος. Το πείραμα ήταν ευεργετικό ολιστικά. Τα αποτελέσματα περιγράφουν τον τρόπο με τον οποίο μπορεί κανείς να εντοπίσει την κυκλοφορία σάρωσης θύρας και τη συμπεριφορά ενός δημοφιλούς σαρωτή απαρίθμησης. Αυτή η διατριβή παρέχει μια πολύτιμη συμβολή στον τομέα IPS. Έχει επιδείξει μια σαφή τάση στην εξέλιξη του συστήματος πυρόσβεσης και εισβολής, έχει δώσει μια εικόνα για την ψυχή ενός χάκερ, παρέχει ένα στερεό παράδειγμα της ανάπτυξης μιας εκμετάλλευσης υπερχείλισης buffer και δείχνει τα βήματα ή τις κρίσεις μιας πραγματικής επίθεσης σε ένα δίκτυο. Περαιτέρω έρευνα στον τομέα αυτό θα μπορούσε να είναι η ανάπτυξη ενός δικτύου με κενά ασφαλείας που εκτίθενται σε ένα ανασφαλές δίκτυο όπως το Διαδίκτυο. Μια άλλη γραμμή έρευνας θα μπορούσε να είναι η ανάπλαση ενός IPS που θα ενσωματώνει τις πτυχές που απαριθμούνταν προηγουμένως στο κεφάλαιο τέσσερα. Δεδομένου περισσότερου χρόνου, θα ήταν επωφελές να ανακατασκευαστεί το ασφαλές δίκτυο και να εμπλακούν ανώτεροι επιτιθέμενοι, έτσι ώστε να παρατηρηθούν όλες οι πτυχές μιας επίθεσης. Αυτό θα παρείχε μια καλύτερη πιθανότητα μιας επίθεσης. Αν το IPS αναπτυχθεί στο μέλλον, τα ζητήματα που αφορούν τις τρέχουσες υλοποιήσεις θα πρέπει να ξεπεραστούν. Στη συνέχεια, η βιομηχανία θα ήταν καλύτερα εξοπλισμένη για να αντιμετωπίσει νέες επιθέσεις που θα εξοικονομούσαν χρήματα και απώλεια φήμης, και γενικά, τα δίκτυα υπολογιστών θα υπέφεραν λιγότερο. [1]

Βιβλιογραφία

[1] Adomavicius, Gedas, 2003, *Information Security, University of Minnesota*, Website accessed 28 April 2022. http://ids.csom.umn.edu/faculty/gedas/6452/slides/IT5-6pp.pdf.

[2] Al-Shaer, Ehab, 2003, *Why Network Security*, DePaul University, Website accessed 28 April 2022, http://www.mnlab.cs.depaul.edu/~ehab/Courses/TDC572/PDF/1-motive&attack.pdf.

[3] Alvarez, Sergio, 2004, *Intro to Win32 Exploits*, Hack3rs.org, Website accessed 28 April 2022 http://hack3rs.org/~shadown/Twister/papers/Intro%20to%20Win32%20Exploits.pdf

[4] Anderson, James P, 1980, *Computer Security Threat Monitoring and Surveillance*, Website accessed 23 April 2022, http://csrc.nist.gov/publications/history/ande80.pdf.

[5] Anon, 1997, *IT security policies dated Computer Fraud & Security*, 12, December p. 3.

[6] Anon, 2001, *Microsoft make anti-hacker film Network Security*, 6, 1st June, p.2.

[7] Anon, 2002, Where do all the hackers come from? *Computer Fraud & Security*, *3*, 1st March, p. 2.

[8] Anon, 2002a, Italian police arrest hacker group *Computer Fraud & Security*, *2*, 1st February, p.4.

[9] Anon, 2002c, Microsoft calls on hacker expert *Computer Fraud & Security, 3,* 1st March, pp. 3-4.

[10] Anon, 2003a, Computer security, and operating system updates *Information and Software Technology, 45* (8), pp. 461-467.

[11] Anon, 2003b, Hacker breaches 8 million credit card accounts *Computer Fraud & Security, 3,* March, p.1.

[12] Anon, 2003c, *Hacker group - cracked Network Security*, 2, February, p.3.

[13] Anon, 2003d, Hackers control 3 million servers *Network Security, 7*, July, pp. 1-2.

[14] Anon, 2003e, Black Hat Conference: Not Just Hackers, *Network Security*, *9*, September, pp. 5-6.

[15] Anon, *A Hacker's Ethics and Hacking Methods*, Virginia Tech, Website accessed 28 April 2022,http://courses.cs.vt.edu/~cs3604/support/Assignments/Final.Assmt.F99/Hacking

/handout1.html.
[16] Anti-Hack, 2001, History of Firewalls, Website accessed 2 May 2022. http://dmsweb.badm.sc.edu/mgsc890/firewalls/fire2.htm.
[17] Argus Systems Group, 2004, Data Sheet, Website accessed 28 April 2022, http://www.argus-systems.com/product/overview/lx/#PitBull_LX
[18] Austen, J. 1997, Can the laws really cut down hacking? *Information Security Technical Report, 2*, (1), p.5.
[19] Boran, Sean, 2003, IT Security Cookbook, boran.com, Website accessed 3 May 2022. http://www.boran.com/security/index.html.
[20] Caswell, Brian, and Marty Roesch, 2004, What is Snort? Snort.org. Website. Accessed 28 April 2022. http://www.snort.org/about.html
[21] Cisco Systems, 2002, Evolution of the Firewall, Cisco Systems (28 September 2002), Website accessed 11 May 2022. http://www.cisco.com/univercd/cc/td/doc/product/iaabu/centri4/user/scf4ch3.htm.
[22] Citadel Security, 2003, Data Sheet, Citadel Security, Website accessed 20 July 2004, http://www.citadel.com/Downloads/Hercules_Datasheet.pdf
[23] Clark, Mark H. 2003, Hacker Culture. Isis, *Philadelphia, 4*, Dec, (4), pp. 776 - 7.
Collett, Stacy, 2002, Manage Those Patches!, ComputerWorld Inc, Website accessed 28 April 2022 http://www.stbernard.com/products/updateexpert/reviews/CompWorld-Jul02.pdf
[24] Computer Advisory Incident Capability, 2004, NID Introduction, US Department of Energy, Website accessed 28 April 2022, http://ciac.llnl.gov/cstc/nid/intro.html
[25] Connolly, P. J., 2002, Why we hack, *InfoWorld, 12, Aug. 24* (32); p. 28.
[26] Conway, Maura, 2003, Hackers as terrorists? Why it does not compute, *Computer Fraud & Security, 12* December, pp 10-13.
[27] Corbitt, Terry, 2003, Tracking the hacker, *Management Services, 47*, April, (4); pp. 20 – 21.
[28] Crosbie, Mark J., and Benjamin A. Kuperman, 2001, A Building Block Approach to Intrusion Detection, Recent Advances in Intrusion Detection. Website accessed 9 May 2022. http://www.raidsymposium.org/raid2001/papers/crosbie_kuperman_raid2001.pdf.
[29]David, Jon, 2001, The Ins and Outs of Intrusion Detection, *Network Security, 10*,

31st October, pp. 13-15.
[30] David, Jon, 2002, Policy enforcement in the workplace, *Computers & Security, 21*, (6), 1 October, pp. 506-513.
[31] Denning, Dorothy, E. 1987, An Intrusion Detection Model, *IEEE Transactions on Software Engineering, Number 2*, February, p. 222
[32] Dictionary.com, 2005, Dictionary.com/patch, Lexico Publishing, Website accessed 6 April 2022, http://dictionary.reference.com/search?q=patch
[33] Dictionary.com, 2005, Dictionary.com/policy, Lexico Publishing, Website accessed 28 April 2022, http://dictionary.reference.com/search?q=policy
[34] Durst, Robert, Terrence Champion, Brian Witten, Eric Miller, and Luigi Spagnuolo, 1999, Testing and evaluating computer intrusion detection systems, *Communications of the ACM, 42* (7), July, pp. 53- 61.
[35] Entercept Security, 2001, Attackers And Their Tools: How Entercept Protects Servers, Entecept Security, Website accessed 13 April 2022, http://www.nai.com/us/_tier2/products/_media/mcafee/wp_attackerstools.pdf
[36] Fitzgerald, Michael, 2004, *Hackers, Crackers and Script Kiddies*, ExtremeTech.com, January 8, p. 1.
[37] Furnell, S. M., and M. J. Warren, 1999, Computer hacking and cyber terrorism: the real threats in the new millennium? *Computers & Security, 18* (1), pp. 28-34.
[38] Gordon, Lawrence A, Martin P. Loeb, *William Lucyshyn and Robert Richardson,* 2004, CSI/FBI Computer Crime and Security Survey, Computer Security Institute. Website accessed 13 April 2022, http://www.usdoj.gov/criminal/cybercrime/CSI_FBI.htm
[39] Govinda, S., 2002, Hacking and Intrusion Detection Management, University of Montana, Website accessed 17 April 2022, ncb.intnet.mu/ncb/events/cyber/pres4.ppt
[40] Grover, Sandeep, 2003, *Buffer Overflow Attacks and Their Countermeasures*, SSC Publications, Website accessed 12 April 2022, http://www.linuxjournal.com/article.php?sid=6701
[41] Hagopian, Stephanie, 2004, Network-Based Intrusion Prevention System Technology, SANS Institute, Website accessed 7 April 2022, www.giac.org/practical/GSEC/Stephanie_Hagopian_GSEC.pdf
[42] Hancock, Bill, 1999, A unique Canadian approach — Invite the hacker to nail your networks, *Computers & Security, 18* (2), pp. 103-104.

[43] Hancock, Bill, 1999, Hackers attack US Government web sites in protest of Chinese embassy bombing, *Computers & Security*, *18* (4), p.279.
[44] Hancock, Bill, 2000, NASA Hacker Pleads Guilty, *Computers & Security*, *19* (8), 1 December, pp. 668-669.
[45] Henning, Ronda, and Richard Caliari, 2003, *Behavior-Based Intrusion Prevention*, Harris Corporation, Website accessed 7 May 2022, http://www.stat.harris.com/solutions/bbip.asp
[46] Hunt, R. and T. Verwoerd, 2003, Reactive firewalls—a new technique, *Computer Communications*, *26*, pp.1302–1317.
[47] Hunter, Philip, 2003, Distributed Intrusion Detection Systems (DIDS) can make security more adaptive, *Network Security*, *3*, March, pp. 16-18.
[48] Kovacich, Geald, L., 1995, Local Area Networks Security: Establishing Policies and Procedures, *Network Security*, *1*, January, pp. 13-16.
[49] Krull, Joseph E., 2003, *What to expect from your IPS*, Communications News, 40, October, (10), p. 19.
[50] Lim, Jeanee, 2003, *Intrusion detection & prevention systems*, Asia Computer Weekly June 30th, p. 1.
[51] Lindstrom, Pete, 2004, Intrusion Prevention Systems (IPS): Next Generation Firewalls, Website accessed 2 May 2022, www.forumintrusion.com/Spire_IPS_Whitepaper.pdf
[52] McHugh, John, Christie, A., and Allen, J., 2000, The Role of Intrusion Detection Systems, IEEE Software, October 2000, Website accessed 8 May 2022. http://www.computer.org/software/so2000/pdf/s5042.pdf.
[53] Meyer, Helen, 1997, A History of Firewall Technology, *Computers & Security*, *16* (4), p. 331.
[54] Meyer, Helen, 1998, Is network intrusion detection software being used

[55] N. Doraswamy, D. Karkins, IPSec: The New Security Standard for the Internet, Intranets and Virtual Private Networks, Prentice Hall PTR Internet Infrastructure Series, New York, 1999

[56] Εκδόσεις κλειδάριθμος. Πέμπτη Αμερικανική Έκδοση. Δίκτυα Υπολογιστών. Συγγραφείς: Tatenbaum – Wetherall.

[57] Frankel, S., Kent, K., Lewkowski, R., Orebaugh, A.D., Ritchey, R.W. and Sharma, S.R (2005). Guide to IPsec VPNs. National Institute of Standards and Technology Special Publication 800-77.

[58] Γ. Πάγκαλος- Ι. Μαυρίδης, Ασφάλεια Πληροφοριακών συστημάτων και δικτύων, Εκδόσεις ΑΝΙΚΟΥΛΑ ΘΕΣΣΑΛΟΝΙΚΗ 2002. ISBN: 960-516-018-8.

[59] Krushang Sonar, Hardik Upadhyay, A Survey: DDOS Attack on Internet of Things.International Journal of Engineering Research and Development e-ISSN: 2278-067X, p-ISSN: 2278-800X, www.ijerd.com Volume 10, Issue 11 (November 2014), PP.58-63

[60] A. Saied, R. E. Overill, and T. Radzik, ‘‘Detection of known and unknown DDoS attacks using artificial neural networks,’’ Neurocomputing, vol. 172, pp. 385–393, Jan. 2016.

[61] Peris-Lopez P, Hernandez-Castro JC, Estevez-Tapiador J, Ribagorda A. RFID systems: a survey on security threats and proposed solutions. In: 11th IFIP International Conference on Personal Wireless Communications – PWC06, Vol. 4217 of Lecture Notes in Computer Science. Springer-Verlag; 2006.p. 159–70.

[62] Haehnel D, Burgard W, Fox D, Fishkin K, Philipose M. Mapping and localization with WID technology, International Conference on Robotics & Automation 2004.

[63] Στέφανος Γκρίτζαλης- Σωκράτης Κ. Κάτσικας- Δημήτρης Γκρίτζαλης, Ασφάλεια Δικτύων Υπολογιστών, Εκδόσεις Παπασωτηρίου Αθήνα 2003. ISBN: 960-7530-45-4

[64] Γ. Πάγκαλος- Ι. Μαυρίδης, Ασφάλεια Πληροφοριακών συστημάτων και δικτύων, Εκδόσεις ΑΝΙΚΟΥΛΑ ΘΕΣΣΑΛΟΝΙΚΗ 2002. ISBN: 960-516-018-8

[65] Vacca, John R. Network and system security Elsevier, Syngress is an imprint of Elsevier Inc. 2009. ISBN: 978-1-59749-535-6