2021-01

þÿ œ - ¸ ¿ ´ ¿ ¹ ± Í ¾ · Ã · Â µ À ¹ À - ´ ¿ Å

þÿ ± Ã Æ ¬ » µ ¹ ± Â Ã µ µ Ä ± ¹ Á ¹ º ¬ ´ ¯ º Ä Å

þÿ ‘ » µ ¾ ¹ ¬ ´ · Â , ± ½ ± ³ ¹ Î Ä · Â

þÿ œ µ Ä ± À Ä Å Ç ¹ ± º Ì Á Ì ³ Á ± ¼ ¼ ± Ã Ä ± » · Á ¿ Æ ¿ Á ¹ ± º ¬ £ Å Ã Ä ® ¼ ± Ä ± º ± ¹ Ä · ½ ¨ · Æ ¹ ± º
þÿ £ Ç ¿ » ® ” ¹ ¿ ¯ º · Ã · Â Ÿ ¹ º ¿ ½ ¿ ¼ ¯ ± Â º ± ¹ • À ¹ Ã Ä ® ¼ · Â ¥ À ¿ » ¿ ³ ¹ Ã Ä Î ½ , ± ½ µ À ¹ Ã Ä ® ¼

ΙΑΝΟΥΑΡΙΟΣ 2021

Τμήμα Πληροφορικής

«Μέθοδοι αύξησης επιπέδου ασφάλειας σε εταιρικά δίκτυα»

ΑΛΕΞΙΑΔΗΣ ΠΑΝΑΓΙΩΤΗΣ

ΙΑΝΟΥΑΡΙΟΣ 2021

Τμήμα Πληροφορικής

«Μέθοδοι αύξησης επιπέδου ασφάλειας σε εταιρικά δίκτυα»

Διατριβή η οποία υποβλήθηκε προς απόκτηση εξ αποστάσεως μεταπτυχιακού τίτλου σπουδών στα Πληροφοριακά Συστήματα και την Ψηφιακή Καινοτομία στο Πανεπιστήμιο Νεάπολις

ΑΛΕΞΙΑΔΗΣ ΠΑΝΑΓΙΩΤΗΣ

ΙΑΝΟΥΑΡΙΟΣ 2021

Πνευματικά δικαιώματα

Ονοματεπώνυμο Φοιτητή/Φοιτήτριας: ……..

Τίτλος Μεταπτυχιακής Διατριβής: …….

Η παρούσα Μεταπτυχιακή Διατριβή εκπονήθηκε στο πλαίσιο των σπουδών για την απόκτηση εξ αποστάσεως μεταπτυχιακού τίτλου στο Πανεπιστήμιο Νεάπολις και εγκρίθηκε στις …..…… [ημερομηνία έγκρισης] από τα μέλη της Εξεταστικής Επιτροπής.

Εξεταστική Επιτροπή:

Πρώτος επιβλέπων (Πανεπιστήμιο Νεάπολις Πάφος)……[ονοματεπώνυμο, βαθμίδα, υπογραφή]

Μέλος Εξεταστικής Επιτροπής: ……[ονοματεπώνυμο, βαθμίδα, υπογραφή]

Μέλος Εξεταστικής Επιτροπής: ……[ονοματεπώνυμο, βαθμίδα, υπογραφή]

Περίληψη στα Ελληνικά (έκτασης 500 λέξεων)

Για τους οργανισμούς τα Πληροφοριακά Συστήματα αποτελούν τον πυρήνα των παρεχόμενων υπηρεσιών που προσφέρονται στα μέλη, στους εξωτερικούς συνεργάτες και στους πελάτες. Ταυτόχρονα διατηρούν σημαντικά πνευματικά περιουσιακά στοιχεία που αποφέρουν το στρατηγικό πλεονέκτημα απέναντι στον ανταγωνισμό. Καθώς τα παγκόσμια δίκτυα αναπτύσσουν τη διασύνδεση των πληροφοριακών συστημάτων η απρόσκοπτη λειτουργία των υπηρεσιών επικοινωνίας και πληροφορικής αποτελεί ζωτικό παράγοντα.
Ένα Πληροφοριακό Σύστημα για να λειτουργεί με ασφάλεια πρέπει να ικανοποιεί τις αρχές του τρίπτυχου Εμπιστευτικότητα, Ακεραιότητα και Διαθεσιμότητα. Οι διαχειριστές τους συχνά βρίσκονται αντιμέτωποι με απειλές οι οποίες έχουν σαν στόχο να αποκτήσουν μη εξουσιοδοτημένη πρόσβαση στις πληροφορίες, να τις αποκαλύψουν ή να τις αλλοιώσουν και να τεθούν οι παρεχόμενες υπηρεσίες εκτός λειτουργίας. Οι κακόβουλοι χρήστες εκμεταλλεύονται γνωστές ή και άγνωστες ευπάθειες των συστημάτων για να εκτελέσουν μεταξύ άλλων επιθέσεις malware, phishing και Denial of Service. Από την πλευρά τους οι διαχειριστές διαθέτουν μία παλέτα εργαλείων για να ασφαλίσουν το Πληροφοριακό Σύστημα, να αποτρέψουν μία επίθεση ή να περιορίσουν την έκτασής της και τη ζημιά που θα επιφέρει. Ακρογωνιαίος λίθος της ασφάλειας είναι τα τείχη προστασίας τα οποία ανάλογα με τον τύπο και την τοπολογία που θα επιλεγεί είναι σε θέση να προστατεύσουν ολόκληρο το σύστημα καθώς και επιμέρους μέρη του που απαιτούν αυστηρότερους κανόνες πρόσβασης. Για την παροχή υπηρεσιών σε απομακρυσμένους χρήστες αναπτύσσονται τα ιδιωτικά εικονικά δίκτυα που προσφέρουν ασφαλή σύνδεση. Στον τομέα της ανίχνευσης και του εντοπισμού επιθέσεων κομβικό ρόλο παίζουν τα Συστήματα ανίχνευσης εισβολών (IDS) τα οποία είναι σε θέση να εντοπίζουν πληθώρα εισβολών σε εύλογο χρονικό διάστημα με ακρίβεια και να παρουσιάζουν με κατανοητό τρόπο την ανάλυση της κίνησης του δικτύου. Τα συστήματα πρόληψης εισβολών προχωρούν ένα βήμα παραπέρα προσφέροντας και τη δυνατότητα αποτροπής ή περιορισμού της κακόβουλης δραστηριότητας. Για την ανίχνευση εισβολών χρήσιμο εργαλείο είναι τα honey pots τα οποία όχι μόνο μπορούν να προσελκύσουν έναν εισβολέα απομακρύνοντάς τον από τα κρίσιμα μέρη του συστήματος αλλά χάρη στους καταγραφείς συμβάντων που διαθέτουν προσφέρονται για την ανάλυση των μεθόδων επιθέσεων που λαμβάνουν χώρα. Οι αλγόριθμοι κρυπτογράφησης διατηρούν τη μυστικότητα των κρυπτογραφημένων πληροφοριών με τη βοήθεια των αλγόριθμων κρυπτογράφησης την ακεραιότητα και την προέλευσή τους. Για τον όσο το δυνατό έγκαιρο εντοπισμό των επερχόμενων επιθέσεων έχει αναπτυχθεί τον λογισμικό ανοιχτού κώδικα Snort. Ανάμεσα στα χαρακτηριστικά του είναι η εύκολη εγκατάσταση στους κόμβους του δικτύου, οι χαμηλές απαιτήσεις σε μνήμη και επεξεργαστική ισχύ και η απλή διαμόρφωσή του. Η αρχιτεκτονική του Snort περιλαμβάνει την αποκωδικοποίηση των πακέτων, τη μηχανή ανίχνευσης εισβολών, τον καταγραφέα των συμβάντων και την παραγωγή των ειδοποιήσεων. Τέλος χρησιμοποιεί μια απλή και ευέλικτη γλώσσα για τη δημιουργία των κανόνων που χρησιμοποιεί η μηχανή ανίχνευσης. Στα πλαίσια της παρούσας διατριβής ζητήθηκε η συγγραφή μίας πρώιμης εφαρμογής που θα χρησιμοποιείται παράλληλα με το Snort. Η γλώσσα προγραμματισμού που επιλέχθηκε είναι η Python 3 η οποία μία ισχυρή γλώσσα που είναι δημοφιλής τόσο στους αρχάριους όσο και στους προχωρημένους προγραμματιστές. Επίσης παρέχει μια μεγάλη βιβλιοθήκη που περιλαμβάνει πολλούς τομείς μειώνοντας σημαντικά το μέγεθος του κώδικα που πρέπει να γραφθεί. Λειτουργία της πρώιμης εφαρμογής είναι να απενεργοποιεί συγκεκριμένες υπηρεσίες του συστήματος εφόσον το κρίνει απαραίτητο ο διαχειριστής αξιολογώντας τα ευρήματα που του παρουσιάζει το Snort.

Περίληψη σε μία Διεθνή Γλώσσα (έκτασης 500 λέξεων)

Organizations around the world provide a variety of services to their members, associates as well as their clients. In the core of this process stand the Information Systems. They preserve crucial intellectual assets that add important value to the company especially against competition. As global networks expand, Information Systems interconnectivity follow offering new services and great potential. It's vital for the systems to operate smoothly. An Information System must comply with the 3 principles of security hence Confidentiality, Integrity and Availability. Administrators often face threats that their main target is to gain unauthorized access, to reveal, steal or manipulate information and to set off crucial system services. Malicious users tend to exploit known or unknow vulnerabilities in order to perform various attacks like malware, phishing and Denial of Service. From their part, administrators can use a collection of tools in order to secure their systems against such attempts or at least try to manage the damage. Firewalls play crucial part in this effort. Depending on the type or the selected topology, they can protect the entire system as well as specific sectors which demand strict access policy. Remote users can access services of the Information System using Virtual Private network. which provide secure connection. Concerning detection of incoming attacks, Intrusion Detection Systems are capable of detecting possible intrusions relatively fast, with accuracy, providing the network traffic data in an understandable way. Taking a step further, Intrusion Prevention Systems add the ability to stop or isolate an ongoing attack. Honey pots are a useful tool to detect attacks. They attract the intruder away from the vital parts of the system while at the same time by logging his actions, the administrator can study their techniques. Cryptographic algorithms keep the integrity and the source of the information intact. Snort is an open-source software that its main goal is to alert accurately and on time for an incoming attack. Among its main characteristics are: easy installation on the majority of the network's nodes, low demands for memory and cpu and the simplicity of the configuration process. Snort's architecture is consisted by four elements. The packet decoder, the detection engine, the logger and the alerter. Also, it uses a simple language in order to create the rules that the detection engine uses. In the framework of this essay a preliminary application was developed with the aimed purpose to work in parallel with Snort. The chosen programming language is Python 3, a powerful and popular language among both novice and experienced programmers. It provides an extensive library the use of which reduces the size of code. This preliminary application allows the administrator to deactivate specific system services based on the data that are provided by Snort.

Ευχαριστίες

Μετά το πέρας της διαδικασίας συγγραφής της παρούσας διατριβής νιώθω την ανάγκη να ευχαριστήσω όλους τους καθηγητές που μας πρόσφεραν όχι μόνο τη γνώση αλλά τον τρόπο σκέψης και τις αρχές για να την αξιοποιήσουμε. Επίσης θα ήθελα να ευχαριστήσω τον επιβλέποντα καθηγητή κύριο Ζαχαριουδάκη Ελευθέριο για την έμπνευση, τη βοήθεια, την υπομονή και την καθοδήγηση στις πολυάριθμες τηλεδιασκέψεις. Αποτελεί για μένα παράδειγμα προς μίμηση. Τέλος οφείλω και ένα μεγάλο ευχαριστώ στη σύζυγό μου για την πίστη και την υποστήριξη καθ' όλη τη διάρκεια του υπέροχου αυτού ταξιδιού.

Αφιέρωση

Στη μνήμη των γονιών μου.

Περιεχόμενα

Κεφάλαιο 1

1.1 Εισαγωγή - Τεχνολογία πληροφοριών

Η πληροφορία είναι ένα σημαντικό κεφάλαιο για κάθε επιχείρηση. Όσο περισσότερες πληροφορίες έχει στη διάθεση της τόσο καλύτερα μπορεί να προσαρμοστεί στο επιχειρηματικό περιβάλλον. Οι πληροφορίες είναι συχνά ένα από τα πιο σημαντικά στοιχεία που διαθέτει μία εταιρεία. Διαφοροποιούν τις εταιρείες και παράγουν μόχλευση η οποία παίζει καθοριστικό ρόλο στον ανταγωνισμό. Η πληροφορία ταξινομείται σε διάφορες κατηγορίες. Αυτό γίνεται με σκοπό να ελεγχθεί η πρόσβαση με βάση συγκεκριμένα κριτήρια, ανάλογα με τη σημασία, την ευαισθησία και την πιθανότητα κλοπής ή κατάχρησης. Οι οργανισμοί συνήθως επιλέγουν να χρησιμοποιήσουν περισσότερους πόρους για τον έλεγχο ευαίσθητων πληροφοριών.
Οι οργανισμοί ταξινομούν την πληροφορία με διαφορετικό τρόπο προκυμμένου να διαχειριστούν τις πτυχές του χειρισμού. Έτσι χρησιμοποιούν την επισήμανση (υδατογραφήματα σε κεφαλίδες και υποσέλιδα), διανομή (ποιος μπορεί να έχει πρόσβαση), αναπαραγωγή (δημιουργία αντιγράφων), δημοσιοποίηση (πως παρέχεται στους εξωτερικούς συνεργάτες), αποθήκευση (που φυλάσσεται), κρυπτογράφηση, διάθεση και μέθοδοι μετάδοσης (ηλεκτρονική αλληλογραφία, εκτύπωση, φαξ και συμβατική αλληλογραφία). Οι λεπτομέρειες περιγράφονται στην πολιτική ταξινόμησης και διαχείρισης πληροφοριών ενός οργανισμού, η οποία αντιπροσωπεύει ένα πολύ σημαντικό στοιχείο της συνολικής πολιτικής ασφάλειας ενός οργανισμού.
Οι πληροφορίες που προορίζονται μόνο για εσωτερική χρήση συνήθως έχουν πρόσβαση μόνο οι υπάλληλοι, οι εργολάβοι και οι πάροχοι υπηρεσιών αλλά όχι το ευρύ κοινό. Τέτοιες είναι τα εσωτερικά σημειώματα, αλληλογραφία, συζητήσεις μέσω email, εταιρικές ανακοινώσεις και γενικό υλικό παρουσίασης. Αυτός ο τύπος πληροφοριών είναι συνήθως ο λιγότερο περιορισμένος διότι το κόστος προστασίας τους είναι δυσανάλογο με την αξία της πληροφορίας ή τον κίνδυνο αποκάλυψης της.
Οι εταιρείες ενδέχεται να έχουν εμπιστευτικές πληροφορίες όπως σχέδια έρευνας και ανάπτυξης, διαδικασίες κατασκευής, στρατηγικές εταιρικές πληροφορίες, χάρτες πορείας προϊόντων, περιγραφές διεργασιών, λίστες πελατών και στοιχεία επικοινωνίας, οικονομικές προβλέψεις και ανακοινώσεις κερδών, στοιχεία τα οποία προορίζονται για εσωτερική χρήση όταν αυτό κρίνεται απαραίτητο. Τυχόν απώλεια ή κλοπή εμπιστευτικών πληροφοριών θα μπορούσε να παραβιάσει την ιδιωτικότητα των ατόμων, να μειώσει το ανταγωνιστικό πλεονέκτημα της εταιρείας ή να προκαλέσει ζημιά στην εταιρεία. Αυτός ο τύπος πληροφοριών είναι διαθέσιμος σε εξωτερικούς συνεργάτες μόνο για εταιρικούς σκοπούς και μόνο μετά τη σύναψη συμφωνίας εμπιστευτικότητας.
Οι εξειδικευμένες ή εμπιστευτικές πληροφορίες περιλαμβάνουν εμπορικά μυστικά, όπως φόρμουλες, λεπτομέρειες παραγωγής και άλλη πνευματική ιδιοκτησία, ιδιόκτητες μεθοδολογίες και πρακτικές που περιγράφουν τον τρόπο παροχής υπηρεσιών, ερευνητικά σχέδια, ηλεκτρονικούς κώδικες, κωδικούς πρόσβασης και κλειδιά κρυπτογράφησης. Εάν αποκαλυφθούν τέτοιου είδους πληροφορίες αυτό μπορεί να βλάψει σοβαρά το ανταγωνιστικό πλεονέκτημα της εταιρείας. Συνήθως περιορίζεται σε λίγα μόνο άτομα ή τμήματα εντός της εταιρείας και σπάνια αποκαλύπτεται εκτός αυτής.
Όσο προηγμένοι είναι οι έλεγχοι ασφαλείας που προστατεύουν τους διαφορετικούς τύπους δεδομένων, τόσο μεγαλύτερο είναι το επίπεδο πρόσβασης που μπορεί να παρέχεται με ασφάλεια σε εξουσιοδοτημένα μέρη που πρέπει να χρησιμοποιούν αυτά τα

δεδομένα. Ομοίως, τρίτα μέρη μπορούν να προσφέρουν πρόσβαση στα δικά τους δεδομένα εφόσον είναι ασφαλή. Όσο υψηλότερη είναι η αμοιβαία εμπιστοσύνη, τόσο περισσότερη πρόσβαση μπορεί να παρέχει ένας οργανισμός με ασφάλεια σε εξωτερικά μέρη όπως οι πελάτες, οι προμηθευτές, οι επιχειρηματικοί συνεργάτες, οι σύμβουλοι κ.α.. Σε αυτή τη παγκόσμια αναπτυσσόμενη ψηφιακή εποχή η δυνατότητα παροχής αυτής της ασφαλούς και αξιόπιστης πρόσβασης δεν είναι πλέον παράγοντας διαφοροποίησης αλλά επιχειρησιακή ανάγκη. (Rhodes-Ousley, 2013)

1.2 Περιγραφή εταιρικού δικτύου

Η αξία των πληροφοριών προέρχεται από τα χαρακτηριστικά που περιέχει. Όταν αλλάζει ένα χαρακτηριστικό της πληροφορίας, η αξία της είτε αυξάνεται, είτε συνηθέστερα μειώνεται. Κάποια χαρακτηριστικά επηρεάζουν την αξία της πληροφορίας με διαφορετικό τρόπο για τους χρήστες ανάλογα με τις περιστάσεις. Για παράδειγμα οι επικαιροποιημένες πληροφορίες μπορεί να είναι κρίσιμος παράγοντας διότι οι πληροφορίες χάνουν μέρος ή όλη την αξία τους όταν παραδίδονται καθυστερημένα. (Whitman & Mattord, 2014)
Οι περισσότεροι συμφωνούν ότι οι ιδιωτικές πληροφορίες πρέπει να είναι ασφαλείς. Για να θεωρηθούν οι πληροφορίες ασφαλείς πρέπει να ικανοποιούν τις τρεις βασικές αρχές των πληροφοριών. Όταν ένας οργανισμός διασφαλίζει αυτές τις τρεις αρχές, τότε ικανοποιεί τις απαιτήσεις των ασφαλών πληροφοριών. Οι τρεις αρχές είναι οι εξής:
Εμπιστευτικότητα (Confidentiality): Μόνο εξουσιοδοτημένοι χρήστες έχουν πρόσβαση στις πληροφορίες.
Ακεραιότητα (Integrity): Μόνο εξουσιοδοτημένοι χρήστες μπορούν να αλλάξουν τις πληροφορίες.
Διαθεσιμότητα (Availability): Οι πληροφορίες είναι προσβάσιμες από εξουσιοδοτημένους χρήστες όποτε τις ζητούν.
Το παραπάνω τρίπτυχο είναι γνωστό ως C.I.A. και αποτελεί τη βάση της ασφάλειας των πληροφοριακών συστημάτων. (Kim & Solomon, 2018)
Εμπιστευτικότητα: Η εμπιστευτικότητα αφορά τη διατήρηση εξουσιοδοτημένων περιορισμών στην πρόσβαση και αποκάλυψη πληροφοριών, συμπεριλαμβανομένων των μέσων για την προστασία του προσωπικού απορρήτου και της ιδιοκτησίας. Η απώλεια της εμπιστευτικότητας είναι η μη εξουσιοδοτημένη αποκάλυψη πληροφοριών. (Stallings, Brown, Bauer & Bhattacharjee, 2015)
Η εμπιστευτικότητα αναφέρεται στον περιορισμό της πρόσβασης σε δεδομένα μόνο σε εκείνους που έχουν την εξουσιοδότηση να τα χρησιμοποιούν. Σε γενικές γραμμές, αυτό σημαίνει ότι ένα μόνο σύνολο δεδομένων είναι προσβάσιμο σε ένα ή περισσότερα εξουσιοδοτημένα άτομα ή συστήματα και κανείς άλλος δεν μπορεί να έχει πρόσβαση σε αυτά. Η εμπιστευτικότητα είναι όρος διακριτός από το απόρρητο με την έννοια ότι το «εμπιστευτικό» συνεπάγεται πρόσβαση σε ένα σύνολο δεδομένων από πολλές πηγές, ενώ το «απόρρητο» συνήθως σημαίνει ότι τα δεδομένα είναι προσβάσιμα μόνο σε μία μόνο πηγή. Έτσι, ένας κωδικός πρόσβασης θεωρείται ιδιωτικός επειδή μόνο ένα άτομο θα πρέπει να τον γνωρίζει, ενώ το αρχείο ενός ασθενούς θεωρείται εμπιστευτικό επειδή επιτρέπεται σε πολλά μέλη του ιατρικού προσωπικού του ασθενούς να τον μελετήσουν. (Rhodes-Ousley, 2013)
Από τη στιγμή που ευαίσθητες πληροφορίες αποθηκεύονται σε υπολογιστικά συστήματα που ανήκουν στην κυβέρνηση, στο στρατό ή σε βιομηχανικά συγκροτήματα, δημιουργείται η ανάγκη να διατηρηθούν κρυφά. Σκοπός είναι η απόκρυψη πληροφοριών ή πόρων. Για παράδειγμα στρατιωτικά και πολιτικά κρατικά ιδρύματα συχνά περιορίζουν την πρόσβαση σε πληροφορίες σε ανθρώπους που την χρειάζονται. Η πρώτη επίσημη

εργασία στον τομέα της ασφάλειας των υπολογιστών ανατέθηκε από το στρατό των ΗΠΑ προκυμμένου να εφαρμοστούν έλεγχοι στη διάδοση των πληροφοριών. Η ίδια αρχή επίσης εφαρμόζεται και από τις βιομηχανίες οι οποίες κρατούν τα ιδιόκτητα σχέδιά τους ασφαλή από τυχόν απόπειρες των ανταγωνιστών να τα υποκλέψουν.
Μηχανισμοί ελέγχου πρόσβασης υποστηρίζουν την εμπιστευτικότητα. Ένας από αυτούς είναι η κρυπτογραφία η οποία μετατρέπει τα δεδομένα σε μία ακατανόητη μορφή. Ένα κρυπτογραφικό κλειδί ελέγχει τη πρόσβαση στα δεδομένα οπότε το ίδιο το κλειδί αποτελεί πλέον το στοιχείο που πρέπει να προστατευτεί.
Η εμπιστευτικότητα επίσης εφαρμόζεται και στην ύπαρξη των δεδομένων η οποία μερικές φορές είναι πιο αποκαλυπτική από τα ίδια τα δεδομένα. Για παράδειγμα ο ακριβής αριθμός των ατόμων που δυσπιστούν απέναντι στην πολιτική της κυβέρνησης πάνω σε ένα φλέγον ζήτημα είναι λιγότερο σημαντικός από το γεγονός ότι η ίδια η κυβέρνηση ζήτησε τη διεξαγωγή μίας δημοσκόπησης πάνω σε αυτό το θέμα. Έτσι το πώς δυσαρέστησε μία κυβερνητική πολιτική τους πολίτες μπορεί να είναι λιγότερο σημαντικό από το να ξέρουμε ότι η ενόχληση αυτή όντως έλαβε χώρα. Οι μηχανισμοί ελέγχου πρόσβασης ορισμένες φορές κρύβουν την ίδια την ύπαρξη των δεδομένων στη προσπάθεια τους να προστατευτούν οι πληροφορίες που περιέχονται.
Η απόκρυψη πόρων είναι άλλη μία σημαντική πτυχή της εμπιστευτικότητας. Οι οργανισμοί συχνά κρύβουν τη διαμόρφωση του δικτύου τους όπως επίσης και τα συστήματα που χρησιμοποιούν. Αυτό δείχνει ότι δεν επιθυμούν να γίνει γνωστός ο εξοπλισμός που χρησιμοποιούν ούτως ώστε να αποφύγουν τη χρήση του δίχως εξουσιοδότηση. (Bishop, 2002)
Ακεραιότητα: Η ακεραιότητα αφορά τη προστασία από ακατάλληλη τροποποίηση ή καταστροφή πληροφοριών συμπεριλαμβανομένης της διασφάλισης μη απόρριψης πληροφοριών και αυθεντικότητας. Η απώλεια ακεραιότητας είναι η μη εξουσιοδοτημένη τροποποίηση ή καταστροφή πληροφοριών. (Stallings, Brown, Bauer & Bhattacharjee, 2015)
Η ακεραιότητα σχετίζεται ιδιαίτερα με τα δεδομένα και αναφέρεται στη διασφάλιση ότι τα δεδομένα δεν έχουν τροποποιηθεί με μη εξουσιοδοτημένο τρόπο. Τα στοιχεία ελέγχου ακεραιότητας έχουν σκοπό να διασφαλίσουν ότι ένα σύνολο δεδομένων δεν μπορεί να τροποποιηθεί (ή να διαγραφεί εξ ολοκλήρου) από μη εξουσιοδοτημένο χρήστη. Μέρος του στόχου των ελέγχων ακεραιότητας είναι να αποτρέψει μη εξουσιοδοτημένα άτομα να κάνουν αλλαγές στα δεδομένα και ένα άλλο μέρος είναι να παρέχει ένα μέσο αποκατάστασης δεδομένων σε μια γνωστή καλή κατάσταση (όπως στα αντίγραφα ασφαλείας). (Rhodes-Ousley, 2013)
Η ακεραιότητα αναφέρεται στην αξιοπιστία των δεδομένων ή των πόρων και συνήθως διατυπώνεται ως η αποτροπή ακατάλληλης ή μη εξουσιοδοτημένης αλλαγής. Η ακεραιότητα περιλαμβάνει την ακεραιότητα των δεδομένων (το περιεχόμενο των πληροφοριών) και την ακεραιότητα της προέλευσης (η πηγή των δεδομένων που συχνά ονομάζεται έλεγχος ταυτότητας). Η πηγή των πληροφοριών μπορεί να βασίζεται στην ακρίβεια και την αξιοπιστία της και στην εμπιστοσύνη που δείχνουν οι άνθρωποι στις πληροφορίες. Αυτή η διχοτομία δείχνει την αρχή ότι η πτυχή της ακεραιότητας που είναι γνωστή ως αξιοπιστία αποτελεί κεντρικό πυλώνα για την ορθή λειτουργία ενός συστήματος.
Οι μηχανισμοί της ακεραιότητας χωρίζονται σε δύο κατηγορίες: οι μηχανισμοί αποτροπής και οι μηχανισμοί εντοπισμού.
Οι μηχανισμοί αποτροπής επιδιώκουν να διατηρήσουν την ακεραιότητα των δεδομένων αποκλείοντας τυχόν μη εξουσιοδοτημένες προσπάθειες αλλαγής των δεδομένων ή τυχόν προσπάθειες αλλαγής δεδομένων με μη εξουσιοδοτημένους τρόπους. Η διάκριση αυτών

των δύο είναι σημαντική. Η πρώτη περίπτωση συμβαίνει όταν ένας χρήστης προσπαθεί να αλλάξει τα δεδομένα δίχως να έχει την κατάλληλη εξουσιοδότηση ενώ η δεύτερη όταν ένας εξουσιοδοτημένος χρήστης προσπαθεί να αλλάξει τα δεδομένα με άλλους τρόπους.
Οι μηχανισμοί εντοπισμού δεν προσπαθούν να αποτρέψουν τις παραβιάσεις της ακεραιότητας. Απλώς αναφέρουν ότι η ακεραιότητα των δεδομένων δεν είναι πλέον αξιόπιστη. Οι μηχανισμοί ανίχνευσης μπορούν να λύσουν τα συμβάντα του συστήματος (ενέργειες χρήστη ή συστήματος) για να εντοπίσουν προβλήματα ή πιο συχνά μπορούν να αναλύσουν τα ίδια τα δεδομένα για να δουν αν απαιτούνται ή είναι αποτελεσματικοί οι περιορισμοί. Οι μηχανισμοί αναφέρουν τον πραγματικό λόγο της παραβίασης της ακεραιότητας.
Η διαφορά της ακεραιότητας με την εμπιστευτικότητα είναι σημαντική. Με την εμπιστευτικότητα τα δεδομένα είτε έχουν εκτεθεί είτε όχι ενώ η ακεραιότητα περιλαμβάνει την ορθότητα αλλά και την αξιοπιστία των δεδομένων. Η προέλευση των δεδομένων (πώς και από ποιόν αποκτήθηκαν), πόσο καλά τα δεδομένα ήταν προστατευμένα προτού έρθουν και πόσο καλά τα δεδομένα είναι προστατευμένα τώρα επηρεάζουν την ακεραιότητα τους. (Bishop, 2002)
Διαθεσιμότητα: Η διαθεσιμότητα αφορά την εξασφάλιση έγκυρης και αξιόπιστης πρόσβασης και χρήσης των πληροφοριών. Ως απώλεια διαθεσιμότητας ορίζεται η διακοπή της πρόσβασης ή της χρήσης πληροφοριών ή ενός πληροφοριακού συστήματος. (Stallings, Brown, Bauer & Bhattacharjee, 2015)
Σε αντίθεση με την εμπιστευτικότητα και την ακεραιότητα, οι οποίες έχουν άμεση σχέση με τα δεδομένα που περιέχονται στα συστήματα υπολογιστών, η διαθεσιμότητα αναφέρεται στον «χρόνο λειτουργίας» των υπηρεσιών που παρέχονται από τα υπολογιστικά συστήματα – αποτελεί τη διαβεβαίωση ότι η υπηρεσία θα είναι διαθέσιμη όταν χρειαστεί. Η διαθεσιμότητα των υπηρεσιών προστατεύεται συνήθως με την εφαρμογή ελέγχων υψηλής διαθεσιμότητας (ή συνεχούς υπηρεσίας) σε υπολογιστές, δίκτυα και αποθηκευτικά μέσα. Ζεύγη υψηλής διαθεσιμότητας (HA) ή ομάδες υπολογιστών, επιπρόσθετες συνδέσεις δικτύου και δίσκοι σε διάταξη RAID είναι ορισμένοι από τους μηχανισμούς για την προστασία της διαθεσιμότητας. (Rhodes-Ousley, 2013)
Η διαθεσιμότητα είναι η δυνατότητα να χρησιμοποιηθούν οι πληροφορίες και οι πόροι. Είναι μια σημαντική πτυχή της αξιοπιστίας καθώς και του σχεδιασμού του συστήματος διότι ένα μη διαθέσιμο σύστημα αντιστοιχεί σε ένα μη υπάρχον. Η πτυχή της διαθεσιμότητας που έχει σχέση με την ασφάλεια είναι ότι κάποιος μπορεί σκόπιμα να ενεργήσει ώστε να υπάρχει άρνηση στη πρόσβαση δεδομένων ή σε μια υπηρεσία καθιστώντας τα μη διαθέσιμα. Οι σχεδιασμοί συστημάτων συνήθως προϋποθέτουν ένα στατιστικό μοντέλο για την ανάλυση των αναμενόμενων προτύπων χρήσης και οι μηχανισμοί διασφαλίζουν τη διαθεσιμότητα όταν ισχύει αυτό το μοντέλο. Όταν κάποιος είναι σε θέση να χειραγωγήσει τη χρήση ή κάποιες παραμέτρους οι οποίες ελέγχουν τη χρήση όπως είναι η κίνηση του δικτύου τότε οι υποθέσεις του στατιστικού μοντέλου δεν ισχύουν. Αυτό σημαίνει ότι οι μηχανισμοί που είναι επιφορτισμένοι με το να κρατούν διαθέσιμους τους πόρους ή τα δεδομένα εργάζονται σε ένα περιβάλλον για το οποίο δεν έχουν σχεδιαστεί. Αυτό έχει ως αποτέλεσμα ότι συχνά θα αποτύχουν στη λειτουργία τους.
Η προσπάθεια για τον αποκλεισμό της διαθεσιμότητας ονομάζεται επίθεση άρνησης υπηρεσίας (Denial of Service – DoS). Τέτοιες επιθέσεις είναι δύσκολο να εντοπιστούν διότι ο αναλυτής πρέπει να καθορίσει εάν τα ασυνήθιστα πρότυπα πρόσβασης οφείλονται σε σκόπιμη χειραγώγηση πόρων ή από το περιβάλλον. Ο πολύπλοκος αυτός προσδιορισμός αποτελεί τη φύση των στατιστικών μοντέλων. Ακόμα και αν το μοντέλο περιγράφει με ακρίβεια το περιβάλλον άτυπα συμβάντα απλά συμβάλλουν στη φύση των στατιστικών.

Μία εσκεμμένη προσπάθεια να καταστεί ένας πόρος μη διαθέσιμος μπορεί να μοιάζει ή να είναι ένα άτυπο – μη αναμενόμενο συμβάν. Σε ορισμένα όμως περιβάλλοντα μπορεί να μην φαίνεται καν ως άτυπο. (Bishop, 2002)
Παρόλο που η χρήση του τρίπτυχου C.I.A. για τον καθορισμό των στόχων ασφαλείας είναι λεπτομερώς καθορισμένη, οι ειδικοί στο τομέα της ασφάλειας ορίζουν πρόσθετες έννοιες για την παρουσίαση της πλήρους εικόνας. Δύο από τις πιο συχνά αναφερόμενες είναι οι εξής:
Αυθεντικότητα: Η ιδιότητα – ικανότητα του συστήματος να επαληθεύει τη ταυτότητα του χρήστη ώστε να διασφαλίζεται η εμπιστοσύνη. Εμπιστοσύνη στην εγκυρότητα μίας μετάδοσης, ενός μηνύματος ή ενός δημιουργού μηνυμάτων. Αυτό πρακτικά σημαίνει την επαλήθευση της ταυτότητας των χρηστών και ότι κάθε είσοδος που φτάνει στο σύστημα προήλθε από μία αξιόπιστη πηγή. Ευθύνη: Ο στόχος ασφαλείας που δημιουργεί την απαίτηση να εντοπίζονται οι ενέργειες μιας οντότητας. Έτσι υποστηρίζεται η αποτροπή, η απομόνωση σφαλμάτων, ο εντοπισμός και η πρόληψη εισβολών ακόμα και η αποκατάσταση μετά την εισβολή και οι νομικές συνέπειες. Επειδή απολύτως ασφαλή συστήματα δεν είναι ακόμη εφικτά οι οργανισμοί πρέπει να είναι σε θέση να εντοπίζουν την πηγή της παραβίασης ασφαλείας. Τα συστήματα πρέπει να τηρούν τα αρχεία των δραστηριοτήτων τους ώστε να είναι δυνατές μεταγενέστερες αναλύσεις για τον εντοπισμό παραβιάσεων ασφαλείας ή να βοηθήσουν σε περίπτωση διαφορών που αφορούν τις συναλλαγές. (Stallings, Brown, Bauer & Bhattacharjee, 2015)
Για να γίνει κατανοητός ο ρόλος των τριών αρχών στην ασφάλεια ενός πληροφοριακού συστήματος θα πρέπει πρώτα να παρουσιαστεί η τυπική υποδομή. Είτε πρόκειται για μία μικρή επιχείρηση, είτε για ένα μεγάλο κυβερνητικό φορέα ή μια δημόσια εταιρεία οι περισσότερες υποδομές πληροφορικής αποτελούνται από τους ακόλουθους εφτά τομείς: User, Workstation, LAN, LAN-to-WAN, WAN, Remote Access, και System/Application Domains. Μια τυπική υποδομή πληροφορικής έχει συνήθως αυτούς τους εφτά τομείς. Καθένας απαιτεί κατάλληλους ελέγχους ασφαλείας. Οι έλεγχοι αυτοί πρέπει να πληρούν τις απαιτήσεις του τρίπτυχου C.I.A..

1.2.1 User Domain (Τομέας Χρήστη)

Ο Τομέας Χρήστη καθορίζει τα άτομα που έχουν πρόσβαση στο πληροφοριακό σύστημα ενός οργανισμού. Ο Τομέας Χρήστη περιλαμβάνει τα εξής χαρακτηριστικά:
Ρόλοι και Εργασίες: Οι χρήστες μπορούν να έχουν πρόσβαση σε συστήματα, εφαρμογές και δεδομένα ανάλογα με τα καθορισμένα δικαιώματα πρόσβασης. Οι εργαζόμενοι οφείλουν να συμμορφώνονται με τις πολιτικές της επιχείρησης. Χαρακτηριστικό του τομέα χρήστη είναι η πολιτική χρήσης. Αυτή καθορίζει την ορθή χρήση των συστημάτων της πληροφορικής. Με απλά λόγια είναι ένα βιβλίο κανόνων που πρέπει να ακολουθούν οι εργαζόμενοι. Η παραβίαση αυτών των κανόνων μπορεί να αποτελέσει λόγο απόλυσης. Αυτό είναι το σημείο από όπου ξεκινά το πρώτο επίπεδο ασφάλειας σε μία πολυεπίπεδη στρατηγική ασφαλείας.
Υπευθυνότητα: Οι εργαζόμενοι είναι υπεύθυνοι για τη χρήση των συστημάτων πληροφορικής.
Ευθύνη: Η σημασία της πρόσβασης στο πληροφοριακό σύστημα μιας επιχείρησης είναι τόσο μεγάλη που το τμήμα ανθρωπίνων πόρων έχει την ευθύνη για τον έλεγχο του ιστορικού των υπαλλήλων που έχουν πρόσβαση σε ευαίσθητα δεδομένα.
Ο τομέας χρήστη είναι ο ασθενέστερος κρίκος σε ένα πληροφοριακό σύστημα. Οι υπεύθυνοι της ασφάλειας οφείλουν να κατανοήσουν τί μπορεί να παρακινήσει κάποιον ώστε να θέσει σε κίνδυνο το σύστημα, τις εφαρμογές ή τα δεδομένα ενός οργανισμού.

Workstation Domain (Σταθμός Εργασίας)
Σταθμός Εργασίας μπορεί να είναι ένας επιτραπέζιος υπολογιστής, ένας φορητός υπολογιστής, ένα τερματικό ή οποιαδήποτε άλλη συσκευή που συνδέεται στο δίκτυο. Οι υπολογιστές των σταθμών εργασίας μπορεί να είναι είτε λογισμικό είτε ένας πραγματικός υπολογιστής χωρίς σκληρό δίσκο που λειτουργεί σε δίκτυο και βασίζεται στο διακομιστή για την παροχή εφαρμογών, δεδομένων και όλες της επεξεργασίας. Τέτοιου είδους τερματικά χρησιμοποιούνται συνήθως σε μεγάλους οργανισμούς, βιβλιοθήκες και σχολεία. Αντιθέτως τα έξυπνα τερματικά είναι πλήρως εξοπλισμένα και περιέχουν σκληρό δίσκο, εφαρμογές και δυνατότητα επεξεργασίας τοπικά και κάνουν χρήση του διακομιστή κυρίως για την αποθήκευση αρχείων. Ένας συνηθισμένος υπολογιστής αποτελεί τέτοιο παράδειγμα. Άλλες συσκευές που μπορεί να θεωρηθούν σταθμοί εργασίας είναι τα έξυπνα τηλέφωνα και τα tablet.
Το προσωπικό ενός οργανισμού πρέπει να έχει την απαραίτητη πρόσβαση για λόγους παραγωγικότητας. Οι εργασίες περιλαμβάνουν τη παραμετροποίηση του υλικού, τη διαδικασία ελέγχου του συστήματος και την επαλήθευση των αρχείων προστασίας από ιούς. Οι έλεγχοι του συστήματος είναι η διαδικασία εξασφάλισης από τυχόν γνωστές απειλές. Περιλαμβάνουν τη διασφάλιση ότι οι υπολογιστές έχουν εγκατεστημένες τις πιο πρόσφατες εκδόσεις λογισμικού, ενημερώσεις ασφαλείας και διαμορφώσεις συστήματος. Ο σταθμός εργασίας χρειάζεται επίσης επιπλέον επίπεδα ασφάλειας, μια τακτική που αναφέρεται ως ασφάλεια σε βάθος. Ένα άλλο κοινό επίπεδο ασφαλείας είναι η εφαρμογή αναγνωριστικών σύνδεσης και κωδικών πρόσβασης για την προστασία της εισόδου στο πληροφοριακό σύστημα. Η ομάδα υποστήριξης ενός οργανισμού είναι υπεύθυνη για τον τομέα εργασίας. Η επιβολή καθορισμένων προτύπων είναι ζωτικής σημασίας για τη διασφάλιση της ακεραιότητας των σταθμών εργασίας και των δεδομένων των χρηστών. Ο τομέας αυτός απαιτεί αυστηρούς ελέγχους ασφαλείας και πρόσβασης διότι οι χρήστες έχουν πρόσβαση σε συστήματα, εφαρμογές και δεδομένα.

1.2.2 LAN Domain (Τομέας Τοπικού Δικτύου)

Το τοπικό δίκτυο είναι ένα σύνολο υπολογιστών που συνδέονται μεταξύ τους ή πάνω σε ένα κοινό μέσο σύνδεσης. Τα μέσα σύνδεσης δικτύου μπορούν να περιλαμβάνουν καλώδια, οπτικές ίνες ή ραδιοκύματα ενώ οργανώνονται ανά λειτουργία ή ανά τμήμα. Μόλις συνδεθεί ο υπολογιστής μπορεί να έχει πρόσβαση σε συστήματα, εφαρμογές, στο διαδίκτυο και σε δεδομένα. Το υλικό μέρος του τοπικού δικτύου περιλαμβάνει τις κάρτες δικτύου, τα καλώδια, switch, τους διακομιστές αρχείων και εκτύπωσης καθώς και σημεία ασύρματης πρόσβασης. Στο λογικό μέρος συναντάμε τη διαχείριση του συστήματος, το σχεδιασμό των υπηρεσιών καταλόγου και αρχείων, τη διαμόρφωση λογισμικού των σταθμών επεξεργασίας και του διακομιστή TCP/IP καθώς και των πρωτοκόλλων επικοινωνίας. Επίσης περιλαμβάνει το σχεδιασμό του διακομιστή αποθήκευσης δεδομένων και τη σχεδίαση των εικονικών τοπικών δικτύων (Virtual LANs).
Ο τομέας του LAN περιλαμβάνει τόσο το φυσικό όσο και το λογικό μέρος του τοπικού δικτύου. Στο φυσικό μέρος περιλαμβάνεται το απαραίτητο υλικό (συσκευές και καλωδιώσεις) ενώ στο λογικό ο σχεδιασμός, οι ρυθμίσεις και η συντήρηση του συστήματος.

1.2.3 LAN to WAN Domain (Τομέας Σύνδεσης Τοπικού Δικτύου με το Διαδίκτυο)

Είναι το σημείο όπου το πληροφοριακό σύστημα συνδέεται με ένα δίκτυο ευρείας περιοχής και το διαδίκτυο. Δυστυχώς η σύνδεση στο διαδίκτυο ισοδυναμεί με πρόσκληση

προς τους πιθανούς εισβολείς. Αυτό συμβαίνει διότι το διαδίκτυο είναι ανοιχτό, δημόσιο και εύκολα προσβάσιμο από οποιονδήποτε. Το μεγαλύτερο μέρος της κίνησης στο διαδίκτυο είναι καθαρό κείμενο. Αυτό σημαίνει ότι είναι ορατό και όχι ιδιωτικό. Οι εφαρμογές δικτύου χρησιμοποιούν δύο κοινά πρωτόκολλα μεταφοράς: το Transmission Control Protocol (TCP) και το User Datagram Protocol (UDP). Τόσο το TCP όσο και το UDP χρησιμοποιούν θύρες για να προσδιορίσουν την εφαρμογή ή τη λειτουργία. Οι θύρες αυτές με απλά λόγια λειτουργούν σαν κανάλια σε μια τηλεόραση δείχνοντας ποιο σταθμό εκπέμπουν. Όταν ένα πακέτο αποστέλλεται μέσω TCP ή UDP ο αριθμός της θύρας εμφανίζεται στην κεφαλίδα του πακέτου. Επειδή πολλές υπηρεσίες σχετίζονται με μία κοινή θύρα η γνώση του αριθμού της αποκαλύπτει ουσιαστικά τι είδους πακέτο είναι. Αυτό ισοδυναμεί με το να διαφημίζεις τον κόσμο τί μεταδίδεις. Απλά παραδείγματα θυρών που χρησιμοποιούν τα πρωτόκολλα TCP και UDP είναι η θύρα 80 (HTTP-πρωτόκολλο επικοινωνίας μεταξύ των πλοηγών και των ιστοσελίδων), θύρα 20 (FTP-πρωτόκολλο για τη μεταφορά αρχείων), θύρα 23 (Telnet – δικτυακό πρωτόκολλο για την απομακρυσμένη διαχείριση συσκευών) και θύρα 22 (SSH – δικτυακό πρωτόκολλο για την απομακρυσμένη διαχείριση συσκευών που υποστηρίζει κρυπτογράφηση δεδομένων).
Ο τομέας LAN to WAN περιλαμβάνει τόσο το υλικό μέρος όσο και το λογικό σχεδιασμό των συσκευών ασφαλείας. Είναι ένας από τους πιο πολύπλοκους τομείς όπου πρέπει να διασφαλιστεί το πληροφοριακό σύστημα. Πρέπει να διατηρηθούν τα επίπεδα ασφαλείας ενώ ταυτόχρονα να δίνεται στους χρήστες όσο το δυνατόν περισσότερη πρόσβαση. Το υλικό πρέπει να διαχειρίζεται με τέτοιο τρόπο ώστε να παρέχει εύκολη πρόσβαση στις υπηρεσίες. Οι συσκευές ασφαλείας πρέπει να είναι διαμορφωμένες με τέτοιο τρόπο ώστε να συμμορφώνονται με την πολιτική του οργανισμού. Αυτό θα αξιοποιήσει στο έπακρο τη διαθεσιμότητα, θα διασφαλίσει την ακεραιότητα των δεδομένων και θα διατηρήσει την εμπιστευτικότητα. Οι ρόλοι και οι εργασίες που απαιτούνται στο τομέα LAN to WAN περιλαμβάνουν τη διαχείριση και παραμετροποίηση συσκευών και οντοτήτων όπως δρομολογητές, firewall, DMZ (Demilitarized zone), συστήματα ανίχνευσης εισβολής (IDS-Intrusion detection system), συστήματα πρόληψης εισβολής (IPS- Intrusion prevention system), διακομιστές μεσολάβησης (Proxy servers) και τέλος φίλτρα περιεχομένου για την ηλεκτρονική αλληλογραφία και την πλοήγηση στο διαδίκτυο. Όλες αυτές οι οντότητες προϋποθέτουν συνεχή παρακολούθηση ούτως ώστε σε περίπτωση συμβάντων ασφαλείας ή ειδοποιήσεων να λαμβάνονται τα απαραίτητα μέτρα.

1.2.4 Τομέας Δικτύου Ευρείας Περιοχής (Wide Area Network)

Ο τομέας WAN συνδέει απομακρυσμένες τοποθεσίες. Καθώς το κόστος δικτύου μειώνεται, οι οργανισμοί είναι σε θέση να επενδύσουν σε ταχύτερες συνδέσεις στο διαδίκτυο και σε δίκτυα ευρείας περιοχής. Σήμερα οι πάροχοι τηλεπικοινωνιακών υπηρεσιών παρέχουν κορμούς οπτικών ινών σε εθνικό επίπεδο για την δημιουργία ιδιωτικών δικτύων, επικοινωνία IP από άκρο σε άκρο για την παροχή υπηρεσιών IP και επικοινωνίας χρησιμοποιώντας την υποδομή του παρόχου. Επίσης παρέχονται υπηρεσίες cloud στο διαδίκτυο, υπηρεσίες Ethernet σε επίπεδο μητροπολιτικής περιοχής και αποκλειστική πρόσβαση στο δίκτυο.

1.2.5 Τομέας Απομακρυσμένης Πρόσβασης (Remote Access Domain)

Ο τομέας απομακρυσμένης πρόσβασης συνδέει απομακρυσμένους χρήστες με την υποδομή πληροφορικής του οργανισμού. Η απομακρυσμένη πρόσβαση είναι ζωτικής σημασίας για τους εργαζόμενους που δραστηριοποιούνται στο πεδίο εφαρμογής ή από

το σπίτι. Για παράδειγμα εξωτερικοί αντιπρόσωποι πωλήσεων, ειδικοί τεχνικής υποστήριξης ή επαγγελματίες υγείας. Η παγκόσμια πρόσβαση καθιστά εύκολη τη σύνδεση στο διαδίκτυο, το ηλεκτρονικό ταχυδρομείο ή άλλες εταιρικές εφαρμογές οπουδήποτε υπάρχει σημείο πρόσβασης σε ασύρματη σύνδεση. Ο τομέας απομακρυσμένης πρόσβασης είναι πολύ σημαντικός αλλά κρύβει και κινδύνους στη χρήση του. Στις μέρες μας ένας εργαζόμενος που το πεδίο δράσης του βρίσκεται εκτός των εταιρικών εγκαταστάσεων κάνει χρήση συσκευών και υπηρεσιών όπως τα έξυπνα τηλέφωνα και το δίκτυο κινητής τηλεφωνίας, εφαρμογές άμεσων μηνυμάτων, έχει πρόσβαση στο ηλεκτρονικό ταχυδρομείο μέσω φορητών συσκευών και έχει πρόσβαση στο διαδίκτυο από τοπικά ασύρματα σημεία πρόσβασης. Τέλος κάνει χρήση VPN (Virtual Private Network) συνδέσεων ώστε να αποκτήσει ασφαλή απομακρυσμένη πρόσβαση στο πληροφοριακό σύστημα της εταιρείας.
Το πεδίο αυτού του τομέα περιορίζεται στην απομακρυσμένη πρόσβαση μέσω διαδικτύου και επικοινωνιών IP. Η διαμόρφωση του τομέα απαιτεί μηχανική των δικτύων και λύσεις VPN. Ο τομέας αυτός αφορά τόσο στην απομακρυσμένη σύνδεση μεμονωμένων χρηστών όσο και στην πρόσβαση πολλών χρηστών. Ο τομέας απομακρυσμένης πρόσβασης αποτελεί το έκτο επίπεδο ασφαλείας σε ένα τυπικό πληροφοριακό σύστημα. Περιλαμβάνει υλικό όπως έξυπνα τηλέφωνα, ταμπλέτες, δρομολογητές και Firewall VPN καθώς επίσης και λογισμικό πελάτη VPN για laptop, ασφαλείς πλοηγούς στο διαδίκτυο, SSL (Secure Sockets Layer) / VPN web server και διακομιστές αυθεντικοποίησης των απομακρυσμένων χρηστών.
Η απομακρυσμένη πρόσβαση είναι επικίνδυνη αλλά και απαραίτητη για τους υπαλλήλους που μετακινούνται. Αυτό ισχύει για οργανισμούς των οποίων το προσωπικό μετακινείται όπως πωλητές, σύμβουλοι, και προσωπικό υποστήριξης. Καθώς οι εταιρείες προσπαθούν να μειώσουν τα κόστη λειτουργίας, αρκετές παροτρύνουν το προσωπικό να εργαστεί από το σπίτι. Η εξασφάλιση ασφαλών συνδέσεων είναι κορυφαία προτεραιότητα. Για την επαλήθευση των χρηστών και την κρυπτογράφηση των δεδομένων γίνεται χρήση του προτύπου ταξινόμησης δεδομένων. Οι έλεγχοι ασφαλείας των απομακρυσμένων χρηστών ακολουθούν την αναγνώριση (παροχή ονόματος χρήστη ή αναγνωριστικού σύνδεσης), τον έλεγχο ταυτότητας (παροχή κωδικού πρόσβασης και σε δεύτερο επίπεδο βιομετρικά χαρακτηριστικά ή έξυπνες κάρτες) και τέλος εξουσιοδότηση (η διαδικασία παραχώρησης δικαιωμάτων χρήσης του εταιρικού πληροφοριακού συστήματος).

1.2.6 Τομέας συστήματος / εφαρμογών (System/ Application Domain)

Ο τομέας συστήματος / εφαρμογών διατηρεί όλα τα κρίσιμα συστήματα, τις εφαρμογές και τα δεδομένα. Οι εξουσιοδοτημένοι χρήστες ενδέχεται να έχουν πρόσβαση σε πολλά στοιχεία αυτού του τομέα. Η ασφαλής πρόσβαση ενδέχεται να απαιτεί ελέγχους ταυτότητας δευτέρου επιπέδου. Τμήματα της επιχείρησης όπως οι ανθρώπινοι πόροι και η μισθοδοσία (το προσωπικό του τμήματος διαχειρίζεται προσωπικά δεδομένα και εμπιστευτικές πληροφορίες), το τμήμα λογιστικής και οικονομικών (τα εκτελεστικά στελέχη έχουν πρόσβαση σε δεδομένα για να λάβουν ορθές επιχειρηματικές αποφάσεις, απαιτούνται μοναδικοί έλεγχοι ασφαλείας που παρέχουν περιορισμένη πρόσβαση σε όσους τα χρειάζονται) και το τμήμα διαχείρισης πελατών (οι πωλητές έχουν πρόσβαση σε πραγματικό χρόνο σε πληροφορίες που περιλαμβάνουν μεταξύ άλλων το ιστορικό αγορών των πελατών και ευαίσθητα ιδιωτικά εταιρικά δεδομένα).
Ο τομέας συστήματος / εφαρμογών αποτελείται από το υλικό, λειτουργικά συστήματα, εφαρμογές και δεδομένα. Επίσης περιλαμβάνει τον λογικό σχεδιασμό του υλικού. Εδώ

επίσης βρίσκονται οι κρίσιμες εφαρμογές της επιχείρησης και τα στοιχεία πνευματικής ιδιοκτησίας. Πρέπει να ασφαλίζεται τόσο φυσικά όσο και λογικά.
Η διασφάλιση του τομέα συστήματος / εφαρμογών πρέπει να προστατεύει τόσο το υλικό όσο και το λογισμικό. Όσον αφορά το υλικό είναι απαραίτητο να διασφαλίζεται ότι μόνο το εξουσιοδοτημένο προσωπικό θα έχει πρόσβαση στο χώρο ενώ παράλληλα ο εξοπλισμός θα προστατεύεται από φυσικές καταστροφές. Σχετικά με το λογισμικό πρέπει να εφαρμόζονται όλες οι αναβαθμίσεις ασφαλείας και να λαμβάνονται συχνά αντίγραφα δεδομένων. Τα αντίγραφα αυτά πρέπει να βρίσκονται σε διαφορετικό χώρο από τον τομέα. Απαραίτητα είναι επίσης τα διαγνωστικά τεστ ασφαλείας όπως διαγνωστικές επιθέσεις ώστε να εντοπίζονται κενά ασφαλείας και αδυναμίες του λογισμικού.
(Kim & Solomon, 2018)

1.3 ΑΠΕΙΛΕΣ

Απειλή είναι η πιθανή παραβίαση της ασφάλειας ενός πληροφοριακού συστήματος. Δεν είναι απαραίτητο η παραβίαση να λάβει χώρα ώστε να θεωρήσουμε ότι υπάρχει απειλή. Το γεγονός ότι ενδέχεται να συμβεί μία παραβίαση σημαίνει ότι πρέπει να ληφθούν τα απαραίτητα μέτρα για την αποτροπή της. (Bishop, 2002)
Οι κίνδυνοι, οι απειλές και οι ευπάθειες συμβαδίζουν. Κίνδυνο ονομάζουμε την πιθανότητα να συμβεί κάτι κακό. Απειλή είναι οποιαδήποτε ενέργεια μπορεί να βλάψει ή να θέσει σε κίνδυνο ένα στοιχείο του ΠΣ. Τέλος ευπάθεια είναι μία πιθανή αδυναμία στον ίδιο το σχεδιασμό ή στο κώδικα του λογισμικού. Μία ευπάθεια που μπορεί να αξιοποιηθεί αποτελεί απειλή. Εάν υπάρχει μία ευπάθεια στο σύστημα τότε υπάρχει και η πιθανότητα μίας απειλής. Οποιαδήποτε απειλή εκμεταλλεύεται μία ευπάθεια δημιουργεί τον κίνδυνο να προκύψει ένα αρνητικό συμβάν. Είναι αδύνατο να εξαλειφθούν οι απειλές, αλλά είναι εφικτό να προστατευθεί το ΠΣ από τις ευπάθειες. Με αυτόν τον τρόπο, παρόλο που υπάρχει η απειλή, δεν μπορεί να εκμεταλλευτεί την ευπάθεια. Το κλειδί για τη προστασία των στοιχείων του ΠΣ από τον κίνδυνο επίθεσης είναι η εξάλειψη ή η αντιμετώπιση όσο το δυνατόν περισσότερων τρωτών σημείων.
(Kim & Solomon, 2018)
Η αξιολόγηση των απειλών είναι ένα σημαντικό μέρος της ανάλυσης κινδύνου. Προσδιορίζοντας τις απειλές, βοηθά στο να εστιαστεί η στρατηγική ασφαλείας και να μειωθεί η πιθανότητα να παραβλεφθούν σημαντικοί τομείς κινδύνου που διαφορετικά θα παραμέναν απροστάτευτοι. Οι απειλές μπορούν να λάβουν πολλές μορφές και για να είναι επιτυχής μια στρατηγική ασφαλείας πρέπει να είναι αρκετά ολοκληρωμένη ώστε να διαχειρίζεται τις πιο σημαντικές απειλές. (Rhodes-Ousley, 2013)
Οι απειλές μπορεί να προέρχονται από ένα άτομο, μία ομάδα ατόμων ή από ένα οργανισμό. Η απειλή εναντίων μιας υπολογιστικής συσκευής μπορεί να είναι μία οποιαδήποτε ενέργεια, τυχαία ή κακόβουλη, που δύναται να έχει αρνητική επίδραση στα στοιχεία και τους πόρους ενός ατόμου ή ενός οργανισμού. Στοιχείο μπορεί να είναι το υλικό, το λογισμικό, βάσεις δεδομένων, αρχεία, πληροφορίες ή το ίδιο το δίκτυο. Η απειλή είναι σημαντική από τη σκοπιά της ασφάλειας. Στόχος της είναι να παρέχει πληροφορίες, μεθοδολογίες και τεχνικές που αντιμετωπίζουν τις απειλές. Ο στόχος αυτός μπορεί να επιτευχθεί αναπτύσσοντας πολιτικές που βοηθούν τους διαχειριστές ΠΣ και δικτύων, τους σχεδιαστές, τους προγραμματιστές και τους χρήστες να αποφεύγουν ανεπιθύμητα χαρακτηριστικά και αδυναμίες του συστήματος. Οι απειλές μπορούν να εντοπιστούν και να ταξινομηθούν ανάλογα με τη σημασία και τα αποτελέσματα τους. Έτσι μπορούν να ταξινομηθούν ανάλογα με τις πιθανότητες οικονομικής ζημιάς, αρνητικής φήμης που ενδέχεται να δημιουργήσουν, ή τη συχνότητα που ενδέχεται να συμβούν. Κάθε

οργανισμός μπορεί να κατατάξει μία απειλή σε ανώτερο ή κατώτερο επίπεδο σε σχέση με κάποιον άλλο βάση της επίδρασης που μπορεί να επιφέρει.
Οι πιο συνηθισμένες απειλές χωρίς απαραίτητα να είναι σε συγκεκριμένη σειρά επικινδυνότητας περιλαμβάνουν τα εξής:

- Βιομηχανική κατασκοπία
- Τρομοκρατία
- Εσωτερικός εισβολέας
- Κακόβουλο λογισμικό
- Αποτυχία υλικού ή λογισμικού
- Κλοπή εξοπλισμού
- Εξωτερικός εισβολέας
- Φυσική καταστροφή

Δεν είναι όλες οι απειλές κακόβουλες. Αν και ορισμένες απειλές μπορεί να είναι σκόπιμες, άλλες μπορεί να είναι τυχαίες. Οι τυχαίες απειλές μπορεί να περιλαμβάνουν αποτυχία υλικού ή πρόβλημα λογισμικού που προκαλείται από την έλλειψη ελέγχων. Ωστόσο, τα αποτελέσματα τυχαίων απειλών μπορεί να είναι εξίσου επιβλαβή με τις κακόβουλες απειλές. Είναι σημαντικό να καταβληθεί κάθε δυνατή προσπάθεια ώστε να ελαχιστοποιηθούν όλες οι παραβιάσεις ασφαλείας είτε είναι κακόβουλες είτε είναι τυχαίες. Στόχος είναι η προστασία του δικτύου και του ΠΣ από οποιαδήποτε επίθεση και η πρόληψη της κλοπής, της καταστροφής και της φθοράς των στοιχείων ενός ατόμου ή ενός οργανισμού. (Kim & Solomon, 2018)

1.3.1 Βασικοί τύποι απειλών πληροφορίας

Οι τρείς δομές ασφαλείας – CIA – αντιμετωπίζουν απειλές για την ασφάλεια ενός συστήματος. Οι απειλές αυτές χωρίζονται σε τέσσερις γενικές κατηγορίες: αποκάλυψη ή μη εξουσιοδοτημένη πρόσβαση στις πληροφορίες, εξαπάτηση ή αποδοχή ψευδών δεδομένων, διαταραχή ή διακοπή (παρεμπόδιση) της εύρυθμης λειτουργίας και σφετερισμός ή μη εξουσιοδοτημένος έλεγχος κάποιου μέρους του συστήματος. Οι τέσσερις αυτές γενικές κατηγορίες περιλαμβάνουν πολλές κοινές απειλές.
Παρακολούθηση ή υποκλοπή, είναι η μη εξουσιοδοτημένη παρακολούθηση πληροφοριών και αποτελεί μία μορφή αποκάλυψης. Είναι μία παθητική ενέργεια που φανερώνει ότι μία οντότητα ακούει ή διαβάζει τις επικοινωνίες ή ακόμα πλοηγείται στα αρχεία και στις πληροφορίες του συστήματος. Η παθητική σύνδεση με την υποδομή του δικτύου αποτελεί μία μορφή κατασκοπίας κατά την οποία ένα δίκτυο παρακολουθείται. Οι υπηρεσίες της εμπιστευτικότητας επιδιώκουν να αντιμετωπίσουν αυτή την απειλή.
Η τροποποίηση ή αλλαγή, είναι η μη εξουσιοδοτημένη επέμβαση στην πληροφορία και καλύπτει τρεις κατηγορίες απειλών. Ο κύριος στόχος μπορεί να είναι η εξαπάτηση κατά την οποία μια οντότητα επαφίεται στα τροποποιημένα δεδομένα για να καθορίσει τις ενέργειες που θα ακολουθήσει ή ποια λανθασμένη πληροφορία θα γίνει αποδεκτή ως ορθή και θα δημοσιευθεί. Εάν τα τροποποιημένα δεδομένα ελέγχουν τη λειτουργία του συστήματος τότε οι απειλές της διαταραχής και του σφετερισμού προκύπτουν. Σε αντίθεση με την παρακολούθηση, η τροποποίηση είναι ενεργή απειλή και έχει ως αποτέλεσμα την αλλαγή των πληροφοριών. Η ενεργητική σύνδεση με την υποδομή του δικτύου είναι μια μορφή τροποποίησης κατά την οποία τα δεδομένα που κυκλοφορούν στο δίκτυο τροποποιούνται, νέα δεδομένα εισάγονται και μέρη των δεδομένων

σβήνονται. Οι υπηρεσίες της ακεραιότητας επιδιώκουν να αντιμετωπίσουν αυτή την απειλή.

Η μεταμφίεση ή πλαστογράφηση είναι η πλαστοπροσωπία μιας οντότητας από μία άλλη και αποτελεί μία μορφή τόσο εξαπάτησης όσο και σφετερισμού. Παραπλανεί ένα θύμα ώστε να πιστεύει ότι η οντότητα με την οποία επικοινωνεί είναι κάποια άλλη. Για παράδειγμα ένας χρήστης προσπαθεί να συνδεθεί με ένα υπολογιστή μέσω διαδικτύου και αντ' αυτού συνδέεται σε κάποιον άλλο. Παρόλο που η μεταμφίεση είναι κυρίως εξαπάτηση συχνά χρησιμοποιείται από τον επιτιθέμενο για την απόκτηση ελέγχου του συστήματος πλαστοπροσωπώντας την ταυτότητα ενός εξουσιοδοτημένου χρήστη. Οι υπηρεσίες ακεραιότητας (υπηρεσίες αυθεντικοποίησης) επιδιώκουν να αντιμετωπίσουν αυτή την απειλή.

Αποκήρυξη της προέλευσης είναι μία ψευδής άρνηση κατά την οποία μία οντότητα έστειλε ή δημιούργησε κάτι, είναι μία μορφή εξαπάτησης. Περίπτωση τέτοιας τακτικής αποτελεί όταν ένας πελάτης αποστέλλει μία επιστολή σε έναν έμπορο στην οποία συμφωνεί να πληρώσει ένα σημαντικό ποσό για ένα προϊόν. Ο έμπορος αποστέλλει το προϊόν και μετά απαιτεί τη πληρωμή. Ο πελάτης αρνείται ότι παρήγγειλε το προϊόν και σύμφωνα με την νομοθεσία δικαιούται να το κρατήσει δίχως να το πληρώσει. Ο πελάτης αποκήρυξε την προέλευση της επιστολής. Εάν ο έμπορος δεν είναι σε θέση να αποδείξει ότι η επιστολή προήλθε από τον πελάτη τότε η επίθεση είναι επιτυχής. Μία παραλλαγή αυτού είναι η άρνηση του χρήστη ότι δημιούργησε συγκεκριμένες πληροφορίες ή οντότητες όπως αρχεία. Οι μηχανισμοί ακεραιότητας προσπαθούν να αντιμετωπίσουν αυτή την απειλή.

Άρνηση παραλαβής είναι η ψευδής άρνηση ότι μία οντότητα έλαβε πληροφορίες ή μηνύματα και αποτελεί μορφή εξαπάτησης. Υποθετικά ένας πελάτης παραγγέλνει ένα ακριβό προϊόν αλλά ο έμπορος απαιτεί εξόφληση πριν την αποστολή. Ο πελάτης πληρώνει και ο έμπορος αποστέλλει το προϊόν. Ο πελάτης ρωτά τον έμπορο πότε θα παραλάβει το προϊόν. Εάν ο πελάτης έχει ήδη παραλάβει το προϊόν, τότε η ερώτηση αποτελεί επίθεση άρνηση παραλαβής. Ο έμπορος μπορεί να αμυνθεί αποδεικνύοντας ότι ο πελάτης παρέλαβε το προϊόν παρά τις αρνήσεις του. Οι μηχανισμοί ακεραιότητας και διαθεσιμότητας προσπαθούν να διαφυλάξουν το σύστημα από αυτές τις απειλές.

Καθυστέρηση είναι η προσωρινή αναστολή μιας υπηρεσίας και αποτελεί μορφή σφετερισμού, παρόλο που μπορεί να παίξει υποστηρικτικό ρόλο στην εξαπάτηση. Στην ουσία επηρεάζει το χρόνο παράδοσης ενός μηνύματος επιμηκύνοντας τον. Αυτό απαιτεί τη χειραγώγηση των δομών ελέγχου του συστήματος όπως στοιχεία του δικτύου ή του διακομιστή και ως εκ τούτου αποτελεί μία μορφή σφετερισμού. Αν μια οντότητα αναμένει ένα μήνυμα εξουσιοδότησης το οποίο καθυστερεί ενδέχεται να υποβάλει ερώτημα σε ένα δευτερεύοντα διακομιστή για την εξουσιοδότηση. Παρόλο που ο επιτιθέμενος μπορεί να μην είναι σε θέση να παρουσιαστεί ως ο κύριος διακομιστής μπορεί να είναι σε θέση ως ο δευτερεύον και να παρέχει λανθασμένες πληροφορίες. Οι μηχανισμοί διαθεσιμότητας μπορούν συχνά να αποτρέψουν αυτή την απειλή.

Επίθεση άρνησης υπηρεσίας (DoS) είναι η μακροχρόνια αναστολή παροχής μίας υπηρεσίας και αποτελεί μορφή σφετερισμού. Συχνά χρησιμοποιείται μαζί με άλλους μηχανισμούς για εξαπάτηση. Ο επιτιθέμενος εμποδίζει ένα διακομιστή να παρέχει μία υπηρεσία. Η άρνηση μπορεί να λάβει χώρα στη πηγή εμποδίζοντας το διακομιστή να αποκτήσει τους πόρους που απαιτούνται για την εκτέλεση της λειτουργίας του, στον προορισμό αποκλείοντας την επικοινωνία με τον διακομιστή ή κατά μήκος της ενδιάμεσης διαδρομής απορρίπτοντας μηνύματα μεταξύ του πελάτη και του διακομιστή. Η επίθεση άρνησης υπηρεσίας αποτελεί την ίδια απειλή με μια μακρόχρονη καθυστέρηση. Οι μηχανισμοί διαθεσιμότητας επιδιώκουν να αντιμετωπίσουν αυτή την απειλή.

Η άρνηση ή η καθυστέρηση παροχής μίας υπηρεσίας μπορεί να προκύψει από άμεσες επιθέσεις ή από προβλήματα που δεν σχετίζονται με την ασφάλεια. Τα αίτια και το αποτέλεσμα αυτής της κατάστασης είναι σημαντικά ενώ η πρόθεση τους δεν είναι. Εάν η καθυστέρηση ή άρνηση υπηρεσίας θέτει σε κίνδυνο την ασφάλεια του συστήματος ή είναι μέρος μιας ακολουθίας συμβάντων που οδηγούν στη δυσλειτουργία του συστήματος τότε θεωρούνται ως μία απόπειρα παραβίασης της ασφάλειας του συστήματος. Υπάρχει πιθανότητα να οφείλονται σε ένα σφάλμα χρήστη ή να είναι αποτέλεσμα των χαρακτηριστικών του περιβάλλοντος παρά από συγκεκριμένες ενέργειες ενός επιτιθέμενου. (Bishop, 2002)

1.3.2 Απειλές παραβίασης της ιδιωτικότητας

Η ιδιωτικότητα στο διαδίκτυο ορίζεται το δικαίωμα των χρηστών να ελέγχουν την αποθήκευση, την επαναφορά, την παροχή σε τρίτους και την προβολή προσωπικών στοιχείων τους μέσω του διαδικτύου. Το απόρρητο του διαδικτύου είναι ένα υποσύνολο του απορρήτου δεδομένων. Οι ανησυχίες περί του απορρήτου έχουν διατυπωθεί από την αρχή της χρήσης σε μεγάλη κλίμακα των διασυνδεδεμένων υπολογιστικών συστημάτων. (David, Fano 1965)
Το απόρρητο μπορεί να περιλαμβάνει είτε πληροφορίες προσωπικής ταυτοποίησης είτε τη συμπεριφορά των χρηστών όταν επισκέπτονται έναν ιστότοπο. Οι πληροφορίες προσωπικής ταυτοποίησης αναφέρονται σε κάθε πληροφορία που μπορεί να χρησιμοποιηθεί για την ταυτοποίηση ενός ατόμου. Έτσι η ηλικία και η διεύθυνση από μόνες τους μπορούν να προσδιορίσουν την ταυτότητα ενός ατόμου δίχως να αποκαλυφθεί ρητά το όνομα του διότι αυτά τα δύο στοιχεία είναι αρκετά για να το προσδιορίσουν. Άλλες μορφές των πληροφοριών προσωπικής ταυτοποίησης ενδέχεται να περιλαμβάνουν δεδομένα παρακολούθησης GPS που χρησιμοποιούνται από εφαρμογές έξυπνων τηλεφώνων και οι οποίες καταγράφουν τις καθημερινές μετακινήσεις, πληροφορίες οι οποίες είναι και αυτές αρκετές για να αναγνωριστεί ένα άτομο. Ο Bruce Schneier αναφέρει χαρακτηριστικά «Η ιδιωτικότητα προστατεύει τους πολίτες από την κατάχρηση εξουσίας των κυβερνώντων ακόμα και αν οι πολίτες δεν παρανομούν τη στιγμή της επιτήρησης». (DeVries, Singer, Keller, Michael, Krolik 2018)
Το διαδίκτυο και η ψηφιακή ιδιωτικότητα αντιμετωπίζονται διαφορετικά από τους πολίτες σε σύγκριση με τις παραδοσιακές προσδοκίες της ιδιωτικής ζωής. Στη δεύτερη η απαίτηση είναι οι φυσικοί χώροι όπως τα σπίτια και τα αυτοκίνητα να μην παραβιάζονται ενώ το απόρρητο του διαδικτύου ασχολείται κυρίως με την προστασία των πληροφοριών των χρηστών. (Kang, 1998) Είναι φανερό ότι οι χρήστες δίνουν βαρύτητα στην ιδιωτικότητα της φυσικής καθημερινότητας αμελώντας σε μεγάλο βαθμό τη ψηφιακή. Υπάρχουν άτομα με μέτριες ανησυχίες για το διαδικτυακό απόρρητο και δεν επιθυμούν να διατηρούν πλήρη ανωνυμία. Οι χρήστες του διαδικτύου μπορούν να προστατεύσουν το απόρρητο τους μέσω ελεγχόμενης αποκάλυψης προσωπικών στοιχείων. Η αποκάλυψη της διεύθυνσης IP, πληροφοριών που δεν μπορούν να οδηγήσουν σε ταυτοποίηση θα μπορούσαν να γίνουν αποδεκτές παραχωρήσεις με αντάλλαγμα υπηρεσίες πιο προσαρμοσμένες στις ανάγκες τους. Από την άλλη πλευρά όμως υπάρχουν και αυτοί οι οποίοι επιθυμούν ισχυρότερη προστασία της ιδιωτικότητας. Σε αυτή τη περίπτωση ενδέχεται να προσπαθήσουν να επιτύχουν ανωνυμία στο διαδίκτυο ώστε να διασφαλίσουν το απόρρητο τους απαγορεύοντας σε τρίτους να συνδέσουν τις δραστηριότητες τους με πληροφορίες προσωπικής ταυτοποίησης. Για να διατηρήσουν το απόρρητο των πληροφοριών οι χρήστες πρέπει να είναι προσεκτικοί με το τι υποβάλλουν ακόμα και το τι βλέπουν στο διαδίκτυο. Έτσι κατά την συμπλήρωση στοιχείων και την

αγορά προϊόντων, οι πληροφορίες αυτές παρακολουθούνται και επειδή δεν είναι ιδιωτικές, ορισμένες εταιρείες αποστέλλουν ανεπιθύμητη αλληλογραφία διαφημίζοντας παρόμοια προϊόντα.
Οι δημοσιεύσεις στο διαδίκτυο μπορεί να είναι επιβλαβείς και να εκθέσουν τα άτομα σε κακόβουλες επιθέσεις. Ορισμένες πληροφορίες παραμένουν δημοσιευμένες για δεκαετίες, ανάλογα με τους όρους υπηρεσίας και τις πολιτικές απορρήτου συγκεκριμένων υπηρεσιών που προσφέρονται στο διαδίκτυο. Αυτό μπορεί να περιλαμβάνει σχόλια γραμμένα σε ιστολόγια, φωτογραφίες και ιστότοπους όπως το Facebook, το twitter και το Instagram. Οι πληροφορίες αυτές απορροφούνται στον κυβερνοχώρο και μόλις δημοσιευθούν, ο οποιοσδήποτε μπορεί να τις ανακαλύψει και να αποκτήσει πρόσβαση. Ορισμένοι εργοδότες ερευνούν τους υποψήφιους εργαζόμενους αναζητώντας στο διαδίκτυο λεπτομέρειες της προσωπικής τους ζωής επηρεάζοντας ενδεχομένως το αποτέλεσμα της αξιολόγησης.

1.3.3 Internet Protocol (IP) Addresses

Όλοι οι Ιστότοποι λαμβάνουν και πολλοί από αυτούς παρακολουθούν ποια διεύθυνση IP χρησιμοποιείται από τον υπολογιστή του επισκέπτη. Οι εταιρείες αντιστοιχούν τα δεδομένα με την πάροδο του χρόνου με σκοπό να συσχετίσουν το όνομα, τη διεύθυνση και άλλες πληροφορίες με την IP του χρήστη. (Cyphers, Bennett 2019)
Υπάρχει αμφιβολία για το πόσο ιδιωτικές πρέπει να είναι οι διευθύνσεις IP. Το δικαστήριο της Ευρωπαϊκής Ένωσης έχει αποφανθεί ότι πρέπει να αντιμετωπίζονται ως προσωπικά αναγνωρίσιμες πληροφορίες εάν ο ιστότοπος που τις παρακολουθεί ή κάποιος τρίτος όπως ένας πάροχος υπηρεσιών, γνωρίζει το όνομα ή τη διεύθυνση του κατόχου της διεύθυνσης IP κάτι που θα ήταν αληθές για στατικές και όχι δυναμικές διευθύνσεις. Οι κανονισμοί της πολιτείας της Καλιφόρνια αναφέρουν ότι οι διευθύνσεις IP οφείλουν να αντιμετωπίζονται ως προσωπικά στοιχεία αφού μία επιχείρηση και όχι κάποιος τρίτος μπορεί να τις συνδέσει με το όνομα και την διεύθυνση του χρήστη. Έτσι για να μπορέσει η αστυνομία του Κάλγκαρι να εντοπίσει τις διευθύνσεις χρηστών οι οποίοι υπέπεσαν σε διαδικτυακές παρανομίες αναγκάστηκε να ζητήσει τη συνδρομή του δικαστηρίου της Αλμπέρτα. Η απόφαση υποχρέωνε τον πάροχο τηλεπικοινωνιακών υπηρεσιών να ενημερώσει για τα στοιχεία των χρηστών στους ανήκαν οι συγκεκριμένες διευθύνσεις IP. (Canadian Lawyer Magazine, 2020)

1.3.3.1 HTTP COOKIES

Ένα cookie HTTP είναι δεδομένα που αποθηκεύονται στον υπολογιστή του χρήστη και βοηθούν στην αυτοματοποιημένη πρόσβαση, σε λειτουργίες ιστού ή αναφέρονται σε πληροφορίες που είναι απαραίτητες για να λειτουργήσουν σωστά σύνθετοι ιστότοποι. Μπορούν όμως να χρησιμοποιηθούν και για την παρακολούθηση των χρηστών αποθηκεύοντας ειδικά δεδομένα ιστορικού χρήσης τα οποία ονομάζονται tracking cookies. Τα cookies αποτελούν κοινή ανησυχία στο τομέα της ιδιωτικότητας στο διαδίκτυο. Αν και οι προγραμματιστές ιστοτόπων χρησιμοποιούν συνήθως τα cookies για νόμιμους τεχνικούς σκοπούς, εμφανίζονται και περιπτώσεις κατάχρησης. Το 2009, δύο ερευνητές αναφέρουν ότι τα προφίλ κοινωνικής δικτύωσης θα μπορούσαν να συνδεθούν με cookies επιτρέποντας στο δίκτυο να συσχετιστεί με συνήθειες περιήγησης. (Krishnamurthy, Wills, 2009)
Στο παρελθόν, οι ιστότοποι δεν ενημέρωναν ρητά το χρήστη για την αποθήκευση των cookies, ωστόσο τα cookies παρακολούθησης και ειδικά αυτά των τρίτων

χρησιμοποιούνται συνήθως ως τρόποι συλλογής μακροπρόθεσμων αρχείων ιστορικού περιήγησης των χρηστών. Το γεγονός αυτό ώθησε τόσο την Ευρωπαϊκή Ένωση όσο και τις ΗΠΑ να αναλάβουν δράση το 2011. (Lee, 2011) Τα cookies μπορούν επίσης να έχουν επιπτώσεις και στην εγκληματολογία των υπολογιστών. Τα τελευταία χρόνια οι χρήστες έχουν αρχίσει να συνειδητοποιούν τις επιζήμιες επιπτώσεις τους με αποτέλεσμα να τα διαγράφουν σε τακτά χρονικά διαστήματα. (Pew Internet & American Life Project, 2000) Δεδομένου όμως ότι είναι ο κύριος τρόπος στόχευσης δυνητικών πελατών οι διαφημιστές άρχισαν να χρησιμοποιούν επίμονα flash και zombie cookies αλλά τα σύγχρονα προγράμματα περιήγησης και το λογισμικό προστασίας από κακόβουλο λογισμικό μπορούν πλέον να τα αποκλείσουν ή να τα εντοπίσουν και να τα αφαιρέσουν. (Dent, 2014)
Οι αρχικοί προγραμματιστές των cookies τα δημιούργησαν με σκοπό μόνο ο ιστότοπος που τα διέθετε αρχικά στους χρήστες να έχει την δυνατότητα να τα ανακτήσει. Στη πράξη όμως αυτό μπορεί να παρακαμφθεί. Πιθανές συνέπειες περιλαμβάνουν την τοποθέτηση μίας ετικέτας προσωπικής ταυτοποίησης του χρήστη σε ένα πρόγραμμα περιήγησης για την διευκόλυνση της διαδικασίας δημιουργίας του προφίλ ιστού ή τη χρήση ειδικών scripts μεταξύ ιστοτόπων και άλλων τεχνικών για την κλοπή πολύτιμων πληροφοριών από τα cookies του χρήστη.
Τα cookies ως τεχνολογία προσφέρουν οφέλη. Για τους ιστοτόπους που επισκέπτεται συχνά ο χρήστης και απαιτείται κωδικός πρόσβασης, τα cookies ενδέχεται να επιτρέπουν τη χρήση τους δίχως την ανάγκη ταυτοποίησης. Μπορεί επίσης να παρακολουθεί τις προτιμήσεις για να υποδεικνύει ιστοτόπους ενδιαφέροντος. Τα cookies καθιστούν δωρεάν τη χρήση των περισσότερων ιστοτόπων χωρίς την απαίτηση καμίας πληρωμής. Μερικά από αυτά τα οφέλη όμως μπορεί να θεωρηθούν και αρνητικά. Έτσι ένας από τους ποιο συνηθισμένους τρόπους κλοπής είναι οι hackers που χρησιμοποιούν το όνομα χρήστη και το κωδικό πρόσβασης που αποθηκεύει ένα cookie. Ενώ πολλοί ιστότοποι είναι δωρεάν, πωλούν το χώρο τους σε διαφημιζόμενους. Αυτές οι διαφημίσεις, οι οποίες είναι εξατομικευμένες ως προς τις προτιμήσεις του κάθε χρήστη, μπορεί μερικές φορές να παγώσουν τον Η/Υ ή να προκαλέσουν ενόχληση. Τα cookies είναι επί των πλείστων αβλαβή εκτός από αυτά των τρίτων. Αυτά τα cookie δεν δημιουργούνται από τον ίδιο τον ιστότοπο αλλά από διαφημιστικές εταιρείες της κατηγορίας web banner. Αυτά είναι επικίνδυνα διότι λαμβάνουν τις ίδιες πληροφορίες όπως και τα κανονικά, δηλαδή συνήθειες περιήγησης και ιστότοπους που επισκέπτονται συχνά, αλλά στη συνέχεια κοινοποιούν αυτές τις πληροφορίες σε άλλες εταιρείες.
Τα cookies συνδέονται συχνά με αναδυόμενα παράθυρα, επειδή αυτά τα παράθυρα είναι συχνά αλλά όχι πάντα προσαρμοσμένα στις προτιμήσεις του χρήστη. Αυτά τα παράθυρα είναι ενοχλητικά επειδή το κουμπί κλεισίματος μπορεί να είναι κρυμμένο στρατηγικά δυσχεραίνοντας τη λειτουργία. Στις χειρότερες περιπτώσεις αυτές οι αναδυόμενες διαφημίσεις μπορούν να καταλάβουν ολόκληρη την οθόνη και στη προσπάθεια του ο χρήστης να τις κλείσει μπορεί να μεταφερθεί σε κάποιο ανεπιθύμητο ιστότοπο.
Τα cookies θεωρούνται αρνητικά διότι η πλειοψηφία των χρηστών δεν είναι σε θέση να κατανοήσει επακριβώς τον τρόπο λειτουργίας τους και δρουν στο παρασκήνιο όταν ο χρήστης πλοηγείται στο διαδίκτυο. Η ιδέα ότι κάθε κίνηση στο διαδίκτυο παρακολουθείται προκαλεί ανησυχίες στους χρήστες.
Ορισμένοι χρήστες επιλέγουν την απενεργοποίηση των cookies μία ενέργεια που μπορεί να μειώσει ορισμένους κινδύνους της ιδιωτικότητας αλλά δύναται να περιορίσει σημαντικά ή να αποτρέψει τη λειτουργικότητα πολλών ιστότοπων.
Η διαδικασία δημιουργίας προφίλ η οποία είναι γνωστή και ως παρακολούθηση συγκεντρώνει και αναλύει διάφορα γεγονότα τα οποία το καθένα αποδίδεται σε μία μεμονωμένη αρχική οντότητα. Προκυμμένου να συγκεντρώσει πληροφορίες και ειδικά

πρότυπα δραστηριότητας σχετικά με την αρχική οντότητα. Ορισμένοι οργανισμοί ασχολούνται με τη δημιουργία του προφίλ περιήγησης των χρηστών συλλέγοντας διευθύνσεις ιστοτόπων που επισκέπτονται.
Ορισμένοι διαδικτυακοί οργανισμοί που διεξάγουν έρευνες marketing μπορούν να χρησιμοποιήσουν αυτή τη πρακτική νόμιμα προκυμμένου μεταξύ άλλων να δημιουργήσουν προφίλ τυπικών χρηστών του διαδικτύου. Τέτοια προφίλ, περιγράφουν τις μέσες τάσεις μεγάλων ομάδων χρηστών του διαδικτύου και όχι των πραγματικών ατόμων, μπορούν στη συνέχεια να αποδειχτούν χρήσιμα για την ανάλυση της αγοράς. Αν και τα συγκεντρωτικά δεδομένα δεν αποτελούν παραβίαση της ιδιωτικότητας, ορισμένοι πιστεύουν ότι η δημιουργία του αρχικού προφίλ αποτελεί.
Η δημιουργία προφίλ γίνεται ακόμα πιο αμφιλεγόμενο ζήτημα ιδιωτικότητας όταν η αντιστοίχιση δεδομένων συσχετίζει το προφίλ ενός ατόμου με τις πληροφορίες προσωπικής ταυτοποίησης του.
Οι κυβερνήσεις και οι οργανισμοί είναι σε θέση να δημιουργήσουν ιστότοπους honeypot οι οποίοι περιέχουν αμφιλεγόμενα θέματα με σκοπό την προσέλκυση και παρακολούθηση χρηστών. Αυτό αποτελεί ένα πιθανό κίνδυνο για τους χρήστες.

1.3.4 Μηχανές αναζήτησης και ιδιωτικότητα

Η ιδιωτικότητα κατά τη χρήση των μηχανών αναζήτησης είναι ένα υποσύνολο της ιδιωτικότητας στο διαδίκτυο που επικεντρώνεται στα δεδομένα των χρηστών που συλλέγονται από τις μηχανές αναζήτησης. Και οι δύο περιπτώσεις ιδιωτικότητας εμπίπτουν στην κατηγορία της ιδιωτικότητας των πληροφοριών. Οι ανησυχίες επικεντρώνονται στην ικανότητα των μηχανών αναζήτησης, στο ιστορικό περιήγησης, στις διευθύνσεις IP και στα cookies των χρηστών με απώτερο στόχο τη δημιουργία προφίλ χρήστη. Η συλλογή πληροφοριών προσωπικής ταυτοποίησης από τις μηχανές αναζήτησης συνιστά παρακολούθηση. (Pekala, Shayna. 2017)
Αυτή η κατάσταση είναι αμφιλεγόμενη διότι οι μηχανές αναζήτησης ισχυρίζονται ότι συλλέγουν τα δεδομένα ενός χρήστη για να είναι σε θέση να βελτιώσουν τα αποτελέσματα και να παρέχουν στο χρήστη καλύτερη εμπειρία αναζήτησης. Ωστόσο, μηχανές αναζήτησης είναι σε θέση να κάνουν κατάχρηση και να θέσουν σε κίνδυνο το απόρρητο των χρηστών τους πωλώντας τα δεδομένα τους σε διαφημιστικές εταιρείες με σκοπό το κέρδος. Λόγω της έλλειψης κανονισμών οι χρήστες πρέπει να αποφασίσουν τί είναι πιο σημαντικό: η συνάφεια και η ταχύτητα των αποτελεσμάτων ή ιδιωτικότητα τους και να επιλέξουν ανάλογα μία μηχανή αναζήτησης. (Lenard, Thomas, Rubin. 2010)
Το νομικό πλαίσιο που αναφέρεται στη προστασία της ιδιωτικότητας των χρηστών δεν είναι πολύ σταθερό. Οι πιο δημοφιλείς μηχανές αναζήτησης συλλέγουν προσωπικά στοιχεία παράλληλα όμως έχουν εμφανιστεί πρόσφατα και κάποιες οι οποίες επικεντρώνονται στην ιδιωτικότητα. (Ridgway, Renee, 2017)

1.3.5 Πολιτικές απορρήτου

Αποτελεί πρακτική των μηχανών αναζήτησης η δημοσίευση των πολιτικών απορρήτων που ακολουθούν ώστε να ενημερωθούν οι χρήστες σχετικά με τα δεδομένα που συλλέγονται και για ποιους σκοπούς χρησιμοποιούνται. Παρόλο που αυτή η πολιτική αποτελεί μία προσπάθεια διαφάνειας από μέρους των μηχανών αναζήτησης, πολλοί

χρήστες δεν τις διαβάζουν ποτέ και ως εκ τούτου δεν γνωρίζουν πόσες από τις ιδιωτικές τους πληροφορίες όπως κωδικοί πρόσβασης και αποθηκευμένα αρχεία συλλέγονται από τα cookies και ενδέχεται να καταγράφονται και να διατηρούνται από τη μηχανή αναζήτησης. Αυτό συνδέεται με το φαινόμενο της γνωστοποίησης και συγκατάθεσης που ακολουθούν οι πολιτικές απορρήτου. (Dolin, Ron, 2010)
Οι πολιτικές αυτές ουσιαστικά λειτουργούν γνωστοποιώντας στο χρήστη τους όρους ιδιωτικότητας από τον οποίο ζητούν να συμφωνήσει. Αυτό έχει ως στόχο να δώσει τη δυνατότητα στο χρήστη να αποφασίσει ελεύθερα εάν θα κάνει χρήση της υπηρεσίας ή όχι. Ωστόσο αυτή η απόφαση δεν μπορεί να ληφθεί τόσο ελεύθερα επειδή το κόστος της άρνησης χρήσης της υπηρεσίας μπορεί να είναι πολύ υψηλό. Ένα άλλο μεγάλο ζήτημα αποτελεί η κατανόηση αυτών των όρων ακόμη και στην απίθανη περίπτωση που ένας χρήστης αποφασίσει να τους διαβάσει. Οι μηχανές αναζήτησης που λειτουργούν με γνώμονα την ιδιωτικότητα, όπως το DuckDuckGo, δηλώνουν στις πολιτικές απορρήτου ότι συλλέγουν πολύ λιγότερα δεδομένα σε σχέση με την Google ή τη Yahoo. (https://duckduckgo.com/privacy)

1.3.6 Τύποι δεδομένων που συλλέγονται από τις μηχανές αναζήτησης

Οι περισσότερες μηχανές αναζήτησης έχουν τη δυνατότητα και συλλέγουν προσωπικά στοιχεία των χρηστών σύμφωνα με τις πολιτικές απορρήτου που ακολουθούν. Αυτά τα δεδομένα χρήστη μπορούν να είναι οτιδήποτε, από πληροφορίες τοποθεσίας έως cookies, διευθύνσεις IP, το ιστορικό ερωτημάτων αναζήτησης, το ιστορικό κλικ και τα διαδικτυακά ίχνη. (Strahilevitz, Jacob,Kugler, 2016) Αυτά τα δεδομένα αποθηκεύονται συχνά σε μεγάλες βάσεις δεδομένων και για λόγους ανωνυμίας ενδέχεται στους χρήστες να εκχωρηθούν αριθμοί.
Τα δεδομένα που συλλέγονται μπορούν να αποθηκευτούν για μεγάλο χρονικό διάστημα. Στην περίπτωση της Google αυτά διατηρούνται για έως και εννέα μήνες. Ορισμένες μελέτες όμως αναφέρουν ότι αυτός ο αριθμός είναι στη πραγματικότητα δεκαοχτώ μήνες. Τα δεδομένα αυτά χρησιμοποιούνται για διάφορους λόγους όπως η βελτιστοποίηση και η εξατομίκευση των αποτελεσμάτων αναζήτησης, η στοχευμένη διαφήμιση και η προσπάθεια προστασίας των χρηστών από απάτες και επιθέσεις ηλεκτρονικού ψαρέματος. Τέτοια δεδομένα μπορούν να συλλεχθούν ακόμη και όταν ο χρήστης δεν είναι συνδεδεμένος στο λογαριασμό του ή χρησιμοποιεί διαφορετική διεύθυνση IP, με την βοήθεια των cookies. (Tene, 2008)

1.3.7 Προφίλ χρήστη και εξατομίκευση

Αυτό που κάνουν συχνά οι μηχανές αναζήτησης μόλις συλλέξουν πληροφορίες σχετικά με τις συνήθειες ενός χρήστη είναι να δημιουργηθεί ένα προφίλ το οποίο βοηθά τη μηχανή αναζήτησης να αποφασίσει ποιοι σύνδεσμοι θα εμφανίζονται για διαφορετικά ερωτήματα που υποβάλλονται ή με ποιες διαφημίσεις θα στοχεύσουν. (Wicker, Jörg & Stefan Kramer, 2017) Μια ενδιαφέρουσα εξέλιξη σε αυτό το τομέα είναι η αυτόματη μάθηση. Η χρήση της βοηθά τις μηχανές αναζήτησης να βελτιώσουν τα μοντέλα προφίλ ώστε να είναι σε θέση να προβλέψουν με μεγαλύτερη ακρίβεια σε ποιο σύνδεσμο θα πατήσει κλικ ένας συγκεκριμένος χρήστης κάνοντας δοκιμές μεταξύ δύο διαφορετικών αποτελεσμάτων που του προσφέρονται και μετρώντας τις αντιδράσεις του. (van Otterlo, Martijn, 2014)

1.4 Τεχνολογία αναγνώρισης προσώπου

Η τεχνολογία αναγνώρισης προσώπου χρησιμοποιείται κυρίως για την ταυτοποίηση ατόμων. Είναι μία από τις πολλές τεχνολογίες βιομετρικού ελέγχου ταυτότητας όπως τα δαχτυλικά αποτυπώματα, η ανάλυση των φλεβών της παλάμης, η αλληλουχία DNA, η εκτύπωση παλάμης και η αναγνώριση της ίριδας.
Οι περισσότερες σύγχρονες τεχνολογίες αναγνώρισης προσώπου όπως και οι υπόλοιποι βιομετρικοί έλεγχοι αποτελούνται από δύο διαδικασίες την εγγραφή και την αντιστοίχιση. Στη περίπτωση της αντιστοίχισης προσώπου αυτές οι δύο διαδικασίες μπορούν να χωριστούν περαιτέρω σε τέσσερα κύρια συστατικά: (Naker & Greenbaum, 2017)
1 Λήψη: Η εικόνα λαμβάνεται μέσω κάμερας ή αποκτάται από μία βάση δεδομένων εικόνων.
2 Αποδόμηση: Είναι η δημιουργία ψηφιακής και αναζητήσιμης αναπαράστασης του προσώπου μέσω σύνθετων αλγόριθμων οι οποίοι μεταξύ άλλων χωρίζουν το πρόσωπο σε κομβικά σημεία τα οποία δεν αλλάζουν πολύ με την πάροδο της ηλικίας τέτοια είναι οι κόγχες των οφθαλμών ή το σχήμα της μύτης. Εκτός από αυτή τη γεωμετρική προσέγγιση όπου το σύστημα καθορίζει τη γύρω περιοχή και τη χωρική σχέση μεταξύ των κομβικών σημείων άλλοι αλγόριθμοι προσπαθούν να αποδομήσουν το πρόσωπο. Τέτοιες προσπάθειες περιλαμβάνουν την ανάλυση της υφής του δέρματος δηλαδή τη θέση των γραμμών, των κηλίδων και των πόρων του δέρματος. Επίσης ακολουθείται φωτομετρική προσέγγιση όπου διεξάγεται αλγοριθμική ερμηνεία ενός προσώπου, ουσιαστικά γίνεται ένας σταθμισμένος συνδυασμός τυποποιημένων προσώπων.
3 Αποθήκευση: Λαμβάνει χώρα με έξυπνο τρόπο και περιλαμβάνει την αποδομημένη ψηφιακή αναπαράσταση και σε ορισμένες περιπτώσεις το πρωτότυπο, σε τεράστιες βάσεις δεδομένων με δυνατότητα αναζήτησης. Σε ορισμένα συστήματα, μετά την αρχική ανάλυση, το σύστημα εφαρμόζει μία διαδικασία τυποποίησης στη φωτογραφία και την αποθηκεύει καθώς και όλες τις άλλες φωτογραφίες στη βάση δεδομένων χρησιμοποιώντας μη συνεπή μορφή. Αυτή η αποθηκευμένη φωτογραφία αποτελεί τη βάση για το τελικό αποτύπωμα του προσώπου εξάγοντας τα χαρακτηριστικά του από τη φωτογραφία.
4 Σύγκριση: Η χρήση αλγορίθμων για τη σύγκριση μίας ληφθήσας εικόνας ή μιας ψηφιακής αναπαράστασης με τις εικόνες που συλλέγονται και αποθηκεύονται στη βάση δεδομένων.
Σε αντίθεση με τα άλλα συστήματα βιομετρικής αναγνώρισης όπως η αναγνώριση της ίριδας και τα δακτυλικά αποτυπώματα, η αναγνώριση προσώπου έχει σχεδιαστεί για να λειτουργεί από απόσταση χωρίς τη γνώση ή τη συγκατάθεση του ατόμου που αναγνωρίζεται. Παρά τους σημερινούς περιορισμούς η τεχνολογία αναγνώρισης προσώπου έχει ήδη εφαρμοστεί σε πολλούς τομείς όπως η ασφάλεια, το εμπόριο, τα κοινωνικά μέσα δικτύωσης, η προσωπική χρήση ακόμη και για θρησκευτικούς σκοπούς. (Wenyi, 2003)

1.5 Απειλές κατά της ακεραιότητας

Οι απειλές κατά της ακεραιότητας επηρεάζουν τόσο την εγκυρότητα των πληροφοριών όσο και τη διασφάλιση ότι οι πληροφορίες είναι σωστές. Εάν οι πληροφορίες αλλάξουν δίχως προειδοποίηση, εξουσιοδότηση ή διαδικασία ελέγχου, η ακεραιότητά τους δεν μπορεί να διασφαλιστεί.
Δυσλειτουργίες

Σημαντική πηγή κινδύνων παραβίασης της ακεραιότητας των δεδομένων αποτελεί η αποτυχία του υλικού και των αποθηκευτικών μέσων ενός πληροφοριακού συστήματος που οδηγεί στη καταστροφή των δεδομένων.

Διαγραφή και απώλεια δεδομένων

Τα δεδομένα μπορεί να καταστραφούν κατά λάθος η σκόπιμα λόγω βλαβών του υλικού ή λανθασμένου χειρισμού. Τα δεδομένα αυτά μπορεί να περιλαμβάνουν οικονομικές, οργανωτικές, προσωπικές και ελεγκτικές πληροφορίες.

Αλλοίωση και παραβίαση δεδομένων

Αλλαγές σε δεδομένα που προκαλούνται από δυσλειτουργία του υλικού ή των συστημάτων αποθήκευσης ή από κακόβουλους χρήστες ή από κακόβουλο λογισμικό. Αυτά μπορεί να βλάψουν την ακεραιότητα των δεδομένων. Η ακεραιότητα μπορεί επίσης να παραβιαστεί από χρήστες που τροποποιούν δεδομένα με πρόθεση να εξαπατήσουν.

Τυχαία τροποποίηση

Είναι ίσως η πιο κοινή αιτία απώλειας της ακεραιότητας των δεδομένων. Η τυχαία τροποποίηση συμβαίνει είτε όταν ένας χρήστης κάνει σκόπιμα αλλαγές στα δεδομένα, αλλά κάνει τις αλλαγές σε λάθος δεδομένα είτε όταν ένας χρήστης εισάγει δεδομένα λανθασμένα. (Rhodes-Ousley, 2013)

Η ακεραιότητα των δεδομένων είναι η διασφάλιση ότι οι πληροφορίες μπορούν να είναι προσβάσιμες ή να τροποποιηθούν μόνο από εκείνους που έχουν την απαραίτητη εξουσιοδότηση στο σύστημα. Τα μέτρα που λαμβάνονται για την εξασφάλιση της ακεραιότητας περιλαμβάνουν τον έλεγχο του φυσικού περιβάλλοντος, των τερματικών και των διακομιστών, τον περιορισμό της πρόσβασης σε δεδομένα και τη διατήρηση αυστηρών πρακτικών ελέγχου ταυτότητας. Η ακεραιότητα των δεδομένων μπορεί επίσης να απειληθεί από περιβαλλοντικούς κινδύνους, όπως θερμότητα, σκόνη και ηλεκτρικές υπερτάσεις.

Οι περισσότεροι οργανισμοί σήμερα προσπαθούν να βελτιώσουν την ανταλλαγή αγαθών, υπηρεσιών, πληροφοριών και γνώσεων χρησιμοποιώντας τεχνολογίες δικτύου. Σε αυτές τις επιχειρηματικές δραστηριότητες, η σωστή επιλογή και ενσωμάτωση υλικού και λογισμικού είναι απαραίτητη για την επίτευξη των επιθυμητών οφελών και τον περιορισμό των σχετικών κινδύνων. Αυτοί οι κίνδυνοι ισχύουν για κάθε πτυχή ενός πληροφοριακού συστήματος που χρησιμοποιείται για την υποστήριξη μιας επιχειρηματικής διαδικασίας και υπάρχουν σε πολλά σημεία και πολλές φορές σε όλα τα συστήματα εφαρμογών. Ωστόσο, κίνδυνοι εμφανίζονται κυρίως στα ακόλουθα στοιχεία ενός συστήματος:

Διεπαφή χρήστη: Οι κίνδυνοι σε αυτόν τον τομέα γενικά σχετίζονται με το εάν υπάρχουν επαρκείς περιορισμοί ως προς τα άτομα σε έναν οργανισμό είναι εξουσιοδοτημένα να εκτελούν επιχειρήσεις ή λειτουργίες συστήματος βάσει των αναγκών εργασίας τους, καθώς και την ανάγκη επιβολής εύλογου διαχωρισμού καθηκόντων.

Επεξεργασία: Οι κίνδυνοι σε αυτόν τον τομέα σχετίζονται γενικά με το εάν υπάρχουν επαρκείς έλεγχοι για να διασφαλιστεί ότι η επεξεργασία δεδομένων έχει ολοκληρωθεί και είναι έγκαιρη. Αυτός ο κίνδυνος περιλαμβάνει επίσης κινδύνους που σχετίζονται με την ακρίβεια και την ακεραιότητα των αναφορών που χρησιμοποιούνται για τη σύνοψη αποτελεσμάτων και τη λήψη επιχειρηματικών αποφάσεων.

Επεξεργασία σφαλμάτων: Οι κίνδυνοι σε αυτόν τον τομέα σχετίζονται γενικά με το κατά πόσον υπάρχουν επαρκείς διαδικασίες και άλλες μέθοδοι συστήματος για να διασφαλιστεί ότι τυχόν εξαιρέσεις εισαγωγής δεδομένων ή επεξεργασίας που καταγράφονται διορθώνονται επαρκώς και επεξεργάζονται με ακρίβεια, ολοκληρωμένα και εγκαίρως.

Διεπαφή: Οι κίνδυνοι σε αυτόν τον τομέα σχετίζονται γενικά με το εάν υπάρχουν επαρκείς προληπτικοί ή έλεγχοι εντοπισμού για να διασφαλιστεί ότι τα δεδομένα που έχουν υποβληθεί σε επεξεργασία, συνοψίζονται και μεταδίδονται επαρκώς και πλήρως από ένα άλλο σύστημα εφαρμογής το οποίο τροφοδοτείτε με δεδομένα ή πληροφορίες.
Διαχείριση αλλαγών: Οι κίνδυνοι σε αυτόν τον τομέα μπορεί γενικά να θεωρούνται μέρος του κινδύνου υποδομής, αλλά επηρεάζουν σημαντικά τα πληροφοριακά συστήματα. Αυτοί οι κίνδυνοι σχετίζονται με την ανεπαρκή διαχείριση αλλαγών και με διαδικασίες που περιλαμβάνουν τη συμμετοχή των χρηστών και την εκπαίδευση τους, καθώς και με τις διαδικασίες με τις οποίες οι αλλαγές σε οποιαδήποτε πτυχή ενός πληροφοριακού συστήματος κοινοποιούνται και εφαρμόζονται.
Δεδομένα: Οι κίνδυνοι σε αυτόν τον τομέα γενικά θεωρούνται ότι αποτελούν μέρος των κινδύνων υποδομής, αλλά επηρεάζουν σημαντικά τα πληροφοριακά συστήματα. Αυτοί οι κίνδυνοι σχετίζονται με τον ανεπαρκή έλεγχο διαχείρισης δεδομένων, συμπεριλαμβανομένης τόσο της ασφάλειας / ακεραιότητας των επεξεργασμένων δεδομένων όσο και της αποτελεσματικής διαχείρισης των βάσεων δεδομένων και των δομών δεδομένων.
Η ακεραιότητα των δεδομένων μπορεί να χαθεί λόγω σφαλμάτων προγραμματισμού, λόγω σφάλματων επεξεργασίας ή σφάλματα διαχείρισης / διαδικασίας. (Protiviti KnowledgeLeader,2020)

1.6 Απειλές κατά της προσβασιμότητας

Όπως συμβαίνει με οποιαδήποτε υπηρεσία ασφαλείας, ο έλεγχος ταυτότητας του χρήστη και ιδίως η απομακρυσμένη πιστοποίηση χρηστών, υπόκεινται σε διάφορες επιθέσεις.
Οι επιθέσεις πελατών λαμβάνουν χώρα όταν ένας κακόβουλος χρήστης προσπαθεί να επιτύχει έλεγχο ταυτότητας χρήστη χωρίς πρόσβαση στον απομακρυσμένο κεντρικό υπολογιστή ή στη διαδρομή της παρεμβαίνουσας επικοινωνίας. Έτσι προσπαθεί να μεταμφιεστεί ως νόμιμος χρήστης. Για ένα σύστημα που η ασφάλεια του βασίζεται σε κωδικούς πρόσβασης, ο αντίπαλος μπορεί να επιχειρήσει να μαντέψει τον πιθανό κωδικό πρόσβασης χρήστη. Μπορεί να γίνουν πολλαπλές προσπάθειες. Στην ακραία περίπτωση, εκτελεί μία διαδικασία δοκιμής όλων των πιθανών κωδικών πρόσβασης σε μια εξαντλητική προσπάθεια να πετύχει τον σκοπό του. Ένας τρόπος να αποτραπεί μια τέτοια επίθεση είναι να επιλεγεί ένας κωδικός πρόσβασης που να είναι και μεγάλος και μη προβλέψιμος. Στην πραγματικότητα, ένας τέτοιος κωδικός πρόσβασης έχει μεγάλη εντροπία. Δηλαδή, απαιτούνται πολλά bits για την αναπαράσταση του κωδικού πρόσβασης. Ένα άλλο αντίμετρο είναι ο περιορισμός του αριθμού των προσπαθειών που μπορούν να γίνουν σε μια δεδομένη χρονική περίοδο από μια δεδομένη πηγή. Ένα token μπορεί να δημιουργήσει έναν κωδικό πρόσβασης υψηλής εντροπίας από ένα PIN χαμηλής εντροπίας ή μια λέξη-κλειδί, αποτρέποντας τις εξαντλητικές αναζητήσεις. Ο αντίπαλος μπορεί να είναι σε θέση να μαντέψει ή να αποκτήσει τον κωδικό PIN ή τον κωδικό πρόσβασης, αλλά πρέπει επιπλέον να αποκτήσει το φυσικό token για να πετύχει. Οι επιθέσεις στον κεντρικό υπολογιστή κατευθύνονται στο αρχείο χρήστη όπου αποθηκεύονται οι κωδικοί πρόσβασης, οι κωδικοί των token και τα βιομετρικά πρότυπα.
Η υποκλοπή στο πλαίσιο των κωδικών πρόσβασης αναφέρεται στην προσπάθεια ενός αντιπάλου να μάθει τον κωδικό πρόσβασης παρατηρώντας τον χρήστη, βρίσκοντας ένα γραπτό αντίγραφο του κωδικού πρόσβασης ή κάποια παρόμοια επίθεση που περιλαμβάνει τη φυσική εγγύτητα του χρήστη και του αντιπάλου. Μια άλλη μορφή υποκλοπής είναι η καταγραφή πλήκτρων (keylogging), στην οποία έχει εγκατασταθεί κακόβουλο υλικό ή λογισμικό, έτσι ώστε ο εισβολέας να μπορεί να υποκλέψει τις

πληκτρολογήσεις του χρήστη για μελλοντική ανάλυση. Ένα σύστημα που βασίζεται σε πολλούς παράγοντες (συνδυασμός κωδικού πρόσβασης και token ή κωδικού πρόσβασης και βιομετρικού) είναι ανθεκτικό σε αυτόν τον τύπο επίθεσης. Για ένα token, ανάλογη απειλή είναι η κλοπή του ή η φυσική αντιγραφή του. Και σε αυτή τη περίπτωση, ένα πρωτόκολλο πολλαπλών παραγόντων είναι σε θέση να αντισταθεί απέναντι σε αυτόν τον επίθεσης καλύτερα από ένα πρωτόκολλο που βασίζεται αμιγώς στο token. Η αντίστοιχη απειλή για ένα βιομετρικό πρωτόκολλο είναι η αντιγραφή ή η μίμηση της βιομετρικής παραμέτρου έτσι ώστε να δημιουργηθεί το επιθυμητό πρότυπο. Τα δυναμικά βιομετρικά είναι λιγότερο ευαίσθητα σε τέτοιες επιθέσεις. Για τα στατικά βιομετρικά στοιχεία, ο έλεγχος ταυτότητας συσκευής είναι ένα χρήσιμο αντίμετρο.
Οι επιθέσεις επανάληψης περιλαμβάνουν έναν αντίπαλο που επαναλαμβάνει μια απόκριση χρήστη που είχε ήδη καταγραφεί. Το πιο συνηθισμένο αντίμετρο για τέτοιες επιθέσεις είναι το πρωτόκολλο αντιμετώπισης πρόκλησης.
Σε μια επίθεση όπου γίνεται χρήση της μεθόδου των Δούρειων ίππων, μια εφαρμογή ή μια φυσική συσκευή μεταμφιέζεται ως αυθεντική με σκοπό την υποκλοπή του κωδικού πρόσβασης του χρήστη, του κωδικού token ή των βιομετρικών. Ο επιτιθέμενος μπορεί στη συνέχεια να χρησιμοποιήσει τις υποκλαπείσες πληροφορίες για να μεταμφιεστεί ως νόμιμος χρήστης.
Μια επίθεση άρνησης υπηρεσίας προσπαθεί να απενεργοποιήσει μια υπηρεσία ελέγχου ταυτότητας χρήστη πλημμυρίζοντας την με πολλές προσπάθειες ελέγχου ταυτότητας. Μια πιο επιλεκτική επίθεση αρνείται την υπηρεσία σε έναν συγκεκριμένο χρήστη προσπαθώντας να συνδεθεί έως ότου επιτευχθεί το όριο που προκαλεί κλείδωμα σε αυτόν τον χρήστη λόγω πάρα πολλών προσπαθειών σύνδεσης. Ένα πρωτόκολλο ελέγχου ταυτότητας πολλαπλών φαινομένων που περιλαμβάνει ένα token αποτρέπει αυτήν την επίθεση, επειδή ο αντίπαλος πρέπει πρώτα να αποκτήσει το διακριτικό. (Stallings, Brown, Bauer & Bhattacharjee, 2015)

1.7 Απειλές κατά της αυθεντικότητας

Η αυθεντικότητα των δεδομένων είναι η ιδιότητα να είναι γνήσια και να μπορούν να επαληθεύονται άρα να υπάρχει εμπιστοσύνη. Εμπιστοσύνη στην εγκυρότητα μιας μετάδοσης, ενός μηνύματος ή ενός δημιουργού μηνυμάτων. Αυτό σημαίνει την επαλήθευση ότι οι χρήστες είναι αυτοί που λένε ότι είναι και ότι κάθε είσοδος που φτάνει στο σύστημα προέρχεται από μια αξιόπιστη πηγή. (Stallings, Brown, Bauer & Bhattacharjee, 2015)
Στο μυαλό των περισσότερων ανθρώπων, το απόρρητο είναι ο στόχος που σχετίζεται περισσότερο με την κρυπτογραφία. Αλλά ο έλεγχος ταυτότητας μηνυμάτων είναι αναμφισβήτητα ακόμη πιο σημαντικός. Πράγματι, ίσως ή να μην είναι τόσο σημαντικό εάν κάποιο συγκεκριμένο μήνυμα που αποστέλλεται παραμένει ιδιωτικό, αλλά σχεδόν σίγουρα πρέπει να υπάρχει βεβαιότητα για τον δημιουργό του κάθε μηνύματος το οποίο φθάνει στο Πληροφοριακό Σύστημα. Ο έλεγχος ταυτότητας μηνυμάτων είναι αυτό που σας προσφέρει αυτή την εγγύηση
Ο έλεγχος ταυτότητας μηνύματος επιτρέπει στο ένα μέρος - τον αποστολέα - να στείλει ένα μήνυμα στο άλλο μέρος - στον παραλήπτη - με τέτοιο τρόπο ώστε εάν το μήνυμα τροποποιηθεί καθ' οδόν, τότε ο παραλήπτης να το εντοπίσει σχεδόν σίγουρα. Ο έλεγχος ταυτότητας μηνύματος ονομάζεται επίσης έλεγχος ταυτότητας προέλευσης δεδομένων Ο έλεγχος ταυτότητας μηνυμάτων λέγεται ότι προστατεύει την ακεραιότητα ενός μηνύματος, διασφαλίζοντας ότι κάθε μήνυμα που λαμβάνεται και θεωρείται αποδεκτό

φτάνει στην ίδια κατάσταση στην οποία στάλθηκε – δίχως να έχει εισαχθεί, τροποποιηθεί ή να λείπει ούτε ένα bit.
Είναι συχνά ζωτικής σημασίας για έναν χρήστη που λαμβάνει ένα μήνυμα να είναι σίγουρος ποιος το έστειλε. Εάν ένας κακόβουλος χρήστης μπορεί να καλέσει στον κεντρικό υπολογιστή της τράπεζάς του και να πραγματοποιήσει συναλλαγές κατάθεσης με τέτοιον τρόπο ώστε να φαίνεται ότι προέρχονται από ένα υποκατάστημα, τότε το τραπεζικό σύστημα είναι ευάλωτο. Εάν ένας χρήστης δίχως προνόμια χρήσης μπορεί να αλληλεπιδράσει μέσω του δικτύου με τον κεντρικό υπολογιστή της εταιρείας του με τέτοιο τρόπο ώστε το μηχάνημα να πιστεύει ότι τα πακέτα που λαμβάνει προέρχονται από το διαχειριστή του συστήματος, τότε όλοι οι μηχανισμοί ελέγχου πρόσβασης του μηχανήματος είναι άχρηστοι. Σε τέτοιες περιπτώσεις ο κίνδυνος είναι ότι ένας αντίπαλος Α, ο πλαστογράφος, θα δημιουργήσει μηνύματα που μοιάζουν να προέρχονται από κάποιο άλλο μέρος, τον S, τον (νόμιμο) αποστολέα. Ο εισβολέας θα στείλει ένα μήνυμα Μ στον R, τον παραλήπτη (orverifier), με την ταυτότητα του S. Ο δέκτης R θα εξαπατηθεί να πιστέψει ότι ο Μ προέρχεται από τον S. Λόγω αυτής της λανθασμένης πεποίθησης, ο R μπορεί να ενεργήσει ακατάλληλα στον Μ. (Bellare, 2012)

1.8 Απειλές παραβίασης - Παρακολούθησης.

Η υποκλοπή – παρακολούθηση (eavesdropping ή sniffing) συμβαίνει όταν ένας κεντρικός υπολογιστής ορίζει τη διεπαφή δικτύου του σε κατάσταση λειτουργίας «promiscuous mode» και αντιγράφει τα πακέτα που περνούν με σκοπό να τα αναλύσει σε δεύτερο χρόνο. Η λειτουργία αυτή επιτρέπει σε μια συσκευή δικτύου να παρακολουθεί και να διαβάζει κάθε πακέτο δεδομένων του δικτύου, ακόμη και αν η διεύθυνση του πακέτου δεν ταιριάζει με τη συσκευή δικτύου. Είναι μέθοδος αυτή δίνει τη δυνατότητα να συνδεθεί υλικό και λογισμικό για την παρακολούθηση και ανάλυση όλων των πακέτων σε αυτό το τμήμα του μέσου μετάδοσης χωρίς να γίνει αντιληπτό από τους άλλους χρήστες. Στόχοι για τέτοιου είδους υποκλοπές μπορούν να είναι δορυφορικές, ασύρματες, κινητές και άλλες μέθοδοι μετάδοσης. (Kim & Solomon, 2018)
Το Sniffing πιο συγκεκριμένα λαμβάνει χώρα όταν ένα μη εξουσιοδοτημένο τρίτο μέρος καταγράφει πακέτα δικτύου που προορίζονται για άλλους υπολογιστές. Το sniffing πακέτων επιτρέπει στον εισβολέα να κοιτάξει το μεταδιδόμενο περιεχόμενο και να αποπειραθεί να αποκαλύψει κωδικούς πρόσβασης και εμπιστευτικά δεδομένα. Προκειμένου να χρησιμοποιήσει λογισμικό παρακολούθησης, ένας εισβολέας πρέπει να έχει μια promiscuous κάρτα δικτύου και ένα εξειδικευμένο οδηγούς λογισμικού για πακέτα δικτύων, πρέπει να είναι συνδεδεμένο με το τμήμα του δικτύου που θέλει να παρακολουθήσει και πρέπει να χρησιμοποιεί λογισμικό sniffer. Από προεπιλογή, μια κάρτα δικτύου (NIC) σε έναν υπολογιστή συνήθως απορρίπτει την κίνηση που δεν προορίζεται για αυτήν. Βάζοντας το NIC σε λειτουργία promiscuous, θα διαβάσει οποιοδήποτε πακέτο περνάει από το συγκεκριμένο καλώδιο δικτύου. Σημαντική παράμετρος αποτελεί το γεγονός ότι για να καταγράψει την κυκλοφορία ένα sniffer, πρέπει να είναι σε θέση να το συλλάβει. Σε δίκτυα που περιέχουν switch, κάθε τομέας έχει ξεχωριστό collision και η παρακολούθηση των πακέτων από έναν εισβολέα μπορεί να είναι δύσκολη, αλλά όχι αδύνατη. Οι επιθέσεις παρακολούθησης πακέτων συναντώνται συχνότερα σε δημόσια δίκτυα είτε ασύρματα είτε ενσύρματα τα οποία ανήκουν στον ίδιο τομέα collision ή μέσω του Διαδικτύου όπου ο εισβολέας μπορεί να εισάγει ένα sniffer στη διαδρομή μεταξύ της πηγής και του προορισμού . Έτσι, σε ένα LAN, ένας χρήστης με περιορισμένα δικαιώματα μπορεί να παρακολουθήσει την κίνηση που προέρχεται από έναν λογαριασμό διαχειριστή, ελπίζοντας να υποκλέψει τον κωδικό πρόσβασης.

Οι εισβολείς που χρησιμοποιούν τη μέθοδο sniffing ελπίζουν να υποκλέψουν κωδικούς πρόσβασης ή άλλες εμπιστευτικές πληροφορίες. Παρόλο που πολλά πρωτόκολλα κρυπτογραφούν την κυκλοφορία στο δίκτυο, πολλά πρωτόκολλα αποστέλλουν δεδομένα χωρίς κρυπτογράφηση σε μορφή απλού κειμένου. Δημοφιλή πρωτόκολλα όπως το HTTP, το FTP και το Telnet είναι διάσημα για τη διαρροή κωδικών πρόσβασης και εμπιστευτικών πληροφοριών με τη χρήση εργαλείων sniffing. (Rhodes-Ousley, 2013)

Κεφάλαιο 2 - ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

2.1 Εισαγωγή

Οι οργανισμοί αξιοποιούν τη δύναμη του Διαδικτύου για να συνδεθούν με όλους τους τύπους εξωτερικών οντοτήτων – τέτοιες είναι οι πελάτες, ομότιμοι οργανισμοί και προμηθευτές. Η δημιουργία αυτής της διασύνδεσης σκοπό έχει να διαμορφώσει έναν απλό και ομαλό μηχανισμό διάδοσης πληροφοριών, να διευκολύνει τις επιχειρηματικών λειτουργείες και να παρέχει απομακρυσμένη πρόσβαση σε συστήματα και δεδομένα.
Για τις επιχειρήσεις είναι σημαντικό να μπορούν να έχουν διαθέσιμες υπηρεσίες και δεδομένα από απόσταση τόσο για τους δικούς τους υπαλλήλους όσο και για τους εξωτερικούς συνεργάτες τους. Ταυτόχρονα όμως με την εύρυθμη παροχή υπηρεσιών και πληροφοριών, οι επιχειρήσεις οφείλουν να διασφαλίζουν την ασφάλεια των πόρων που τις παρέχουν. Ο σχεδιασμός του δικτύου παίζει αναπόσπαστο ρόλο στην ικανότητα ενός οργανισμού να διαχειρίζεται αποτελεσματικά και να διασφαλίζει την πρόσβαση στα δεδομένα του. (Rhodes-Ousley, 2013)

2.2 Τείχος Προστασίας (Firewall)

Τα firewalls είναι ένα από τα πιο δημοφιλή και σημαντικά εργαλεία που χρησιμοποιούνται για την ασφάλεια δικτύων από τα πρώτα χρόνια των διασυνδεδεμένων υπολογιστών. Η βασική λειτουργία ενός τείχους προστασίας είναι η παρακολούθηση της κυκλοφορίας του δικτύου με σκοπό την αποτροπή μη εξουσιοδοτημένης πρόσβασης μεταξύ των δικτύων των υπολογιστών. Πιο συγκεκριμένα είναι η πρώτη γραμμή άμυνας μεταξύ του εσωτερικού δικτύου και των μη αξιόπιστων δικτύων όπως το Διαδίκτυο. (Rhodes-Ousley, 2013)
Το τείχος προστασίας ελέγχει τη ροή της κυκλοφορίας εμποδίζοντας την είσοδο ή την έξοδο από ένα συγκεκριμένο τμήμα του δικτύου τη μη εξουσιοδοτημένη κίνηση. Μπορεί να τοποθετηθεί μεταξύ ενός εσωτερικού δικτύου και του εξωτερικού κόσμου ή εντός του εσωτερικού δικτύου για ελέγχει τη πρόσβαση σε συγκεκριμένα εταιρικά στοιχεία ώστε αυτή να πραγματοποιείται μόνο από εξουσιοδοτημένους χρήστες. Τα firewalls είναι κρίσιμα στοιχεία της ασφάλειας ενός δικτύου. Από μόνα τους όμως δεν είναι σε θέση να επιλύσουν όλα τα προβλήματα ασφαλείας, αλλά αποτελούν μεταξύ άλλων ένα πολύ απαραίτητο αποτρεπτικό μέσο. (Kim & Solomon, 2018)
Τα τείχη προστασίας μπορούν να φιλτράρουν σε διάφορα επίπεδα της στοίβας πρωτοκόλλου των δικτύων. Υπάρχουν τρεις κύριες κατηγορίες: packet filtering, circuit gateways και application gateways. Κάθε ένα από αυτά παίρνει το όνομά του από το επίπεδο πρωτοκόλλου που ελέγχει, από το χαμηλότερο στο υψηλότερο επίπεδο. (Cheswick, Bellovin & Rubin, 2003)

2.2.1 Packet Filters

Ένα τείχος προστασίας φιλτραρίσματος πακέτων είναι μία πολύ βασική επιλογή. Συγκρίνει την εισερχόμενη/εξερχόμενη κίνηση με ένα σύνολο κανόνων που ορίζουν ποια κίνηση θα επιτρέψει να περάσει. Λαμβάνει αυτήν την απόφαση για κάθε πακέτο που φτάνει στο τείχος προστασίας ενώ δεν «θυμάται» ποια πακέτα έλεγξε στο παρελθόν. (Kim

& Solomon, 2018) Πιο συγκεκριμένα εκτελεί έλεγχο πρόσβασης με βάση τα χαρακτηριστικά των κεφαλίδων των πακέτων, όπως τις διευθύνσεις προορισμού, τις διευθύνσεις προέλευσης και τις θύρες. (Bishop, 2002)

Το φιλτράρισμα μπορεί να γίνει στην εισερχόμενη κίνηση, στην εξερχόμενη κίνηση ή και στα δύο. Ο διαχειριστής συντάσσει μια λίστα με τα αποδεκτά μηχανήματα και υπηρεσίες και μια λίστα με μη αποδεκτές μηχανές ή υπηρεσίες. Ένα packet filter firewall μπορεί εύκολα να επιτρέψει ή να αρνηθεί την πρόσβαση σε επίπεδο κεντρικού υπολογιστή ή δικτύου. Έτσι ο διαχειριστής μπορεί να επιτρέψει την πρόσβαση IP μεταξύ δύο κεντρικών υπολογιστών A και B ή να αρνηθεί οποιαδήποτε πρόσβαση στο B εκτός εξαιρόντας από τον κανόνα τον υπολογιστή A. Τα firewalls αυτής της κατηγορίας λειτουργούν καλά για τον αποκλεισμό των πλαστών πακέτων, είτε εισερχόμενων είτε εξερχόμενων. (Cheswick, Bellovin & Rubin, 2003)

Τα τείχη προστασίας φιλτραρίσματος πακέτων ανιχνεύουν πακέτα δεδομένων δικτύου και ελέγχουν εάν είναι σύμφωνα με τους κανόνες της βάσης δεδομένων του τείχους προστασίας ή τους παραβιάζουν. Το φιλτράρισμα του τείχους προστασίας επιθεωρεί τα πακέτα στο επίπεδο δικτύου ή στο επίπεδο 3 του μοντέλου Open Systems Interconnect (OSI). Εάν η συσκευή εντοπίσει ένα πακέτο που ταιριάζει με έναν περιορισμό τότε απαγορεύει στο πακέτο να περάσει από το ένα δίκτυο στο άλλο. Οι περιορισμοί που εφαρμόζονται πιο συχνά στα τείχη προστασίας φιλτραρίσματος πακέτων βασίζονται στον παρακάτω συνδυασμό:

- Πηγή IP και διεύθυνση προορισμού
- Κατεύθυνση (εισερχόμενη ή εξερχόμενη)
- Πρωτόκολλο, για τείχη προστασίας ικανά να εξετάσουν το επίπεδο πρωτοκόλλου IP
- Αιτήματα προέλευσης πρωτοκόλλου ελέγχου μετάδοσης (TCP) ή User Datagram Protocol (UDP) και προορισμού θύρας, για τείχη προστασίας ικανά να εξετάσουν το επίπεδο TCP / UPD

Η δομή πακέτων ποικίλλει ανάλογα με τη φύση του πακέτου. Οι δύο κύριοι τύποι υπηρεσιών που φιλτράρονται είναι TCP και UDP.

Τα απλά μοντέλα εξετάζουν δύο πτυχές της κεφαλίδας πακέτου: τον προορισμό και τη διεύθυνση πηγής. Επιβάλλουν περιορισμούς διευθύνσεων μέσω ACL, οι οποίοι δημιουργούνται και τροποποιούνται από τους διαχειριστές.

Τα τρία υποσύνολα αυτής της κατηγορίας είναι το στατικό φιλτράρισμα(static filtering), το δυναμικό φιλτράρισμα (dynamic filtering) και ο έλεγχος πακέτων (stateful packet inspection - SPI). Επιβάλλουν περιορισμούς διευθύνσεων, κανόνες που έχουν σχεδιαστεί για να απαγορεύουν τη διέλευση πακέτων με συγκεκριμένες διευθύνσεις ή μερικές διευθύνσεις μέσω της συσκευής. Το στατικό φιλτράρισμα απαιτεί την ανάπτυξη και εγκατάσταση των κανόνων φιλτραρίσματος στο τείχος προστασίας. Οι κανόνες δημιουργούνται και από ένα άτομο που είτε επεξεργάζεται άμεσα το σύνολο των κανόνων είτε χρησιμοποιεί μια διεπαφή προγραμματισμού για να καθορίσει τους κανόνες και την ακολουθία. Οποιεσδήποτε αλλαγές στους κανόνες απαιτούν ανθρώπινη παρέμβαση. Αυτός ο τύπος φιλτραρίσματος είναι κοινός σε δρομολογητές δικτύου και πύλες.

Ένα dynamic filtering firewall μπορεί να αντιδράσει σε ένα επερχόμενο συμβάν και να ενημερώσει ή να δημιουργήσει κανόνες για την αντιμετώπιση αυτού του συμβάντος. Αυτή η αντίδραση θα μπορούσε να είναι θετική, επιτρέποντας σε έναν εσωτερικό χρήστη να συμμετάσχει σε μια συγκεκριμένη δραστηριότητα κατόπιν αιτήματος ή αρνητική προχωρώντας στην απόρριψη όλων των πακέτων από μια συγκεκριμένη διεύθυνση όταν ανιχνεύεται αυξημένη παρουσία ενός συγκεκριμένου τύπου πακέτου με λανθασμένη μορφή. Ενώ τα τείχη προστασίας στατικού φιλτραρίσματος επιτρέπουν την είσοδο ολόκληρων σετ ενός τύπου πακέτου αποκρινόμενα σε εξουσιοδοτημένα αιτήματα, το

δυναμικό φιλτράρισμα πακέτων επιτρέπει την είσοδο μόνο ενός συγκεκριμένου πακέτου με μια συγκεκριμένη πηγή, προορισμό και διεύθυνση θύρας. Αυτό το φιλτράρισμα λειτουργεί ανοίγοντας και κλείνοντας "πόρτες" στο τείχος προστασίας βάσει των πληροφοριών που περιλαμβάνονται στην κεφαλίδα του πακέτου. Η λειτουργία αυτή καθιστά τα δυναμικά φίλτρα πακέτων μια ενδιάμεση μορφή μεταξύ των παραδοσιακών στατικών φίλτρων πακέτων και των διακομιστών μεσολάβησης εφαρμογών.
Τα τείχη προστασίας SPI, που ονομάζονται επίσης και firewall επιθεώρησης, παρακολουθούν κάθε σύνδεση δικτύου μεταξύ εσωτερικών και εξωτερικών συστημάτων χρησιμοποιώντας έναν πίνακα κατάστασης. Έτσι παρακολουθείται η κατάσταση και το πλαίσιο κάθε πακέτου στη συνομιλία καταγράφοντας ποιος σταθμός έστειλε ποιο πακέτο και πότε. Όπως τα packet filters, τα SPI εκτελούν φιλτράρισμα πακέτων, αλλά προχωρούν και ένα βήμα παραπέρα. Ενώ τα απλά τείχη προστασίας φιλτραρίσματος πακέτων επιτρέπουν ή απορρίπτουν συγκεκριμένα πακέτα με βάση τη διεύθυνσή τους, ένα SPI μπορεί να επισπεύσει τα εισερχόμενα πακέτα που είναι απαντήσεις σε εσωτερικά αιτήματα. Εάν όμως λάβει ένα εισερχόμενο πακέτο που δεν μπορεί να ταιριάξει στον πίνακα κατάστασής του, αναφέρεται στο ACL για να καθορίσει εάν θα επιτρέψει στο πακέτο να περάσει. (Whitman & Mattord, 2014) Αυτό σημαίνει ότι θυμάται πληροφορίες σχετικά με την κατάσταση μιας επικοινωνίας δικτύου. Μόλις το τείχος προστασίας λάβει το πρώτο πακέτο μιας νέας επικοινωνίας, το τείχος προστασίας θυμάται αυτήν την περίοδο της επικοινωνίας μέχρι αυτή να τερματιστεί. Έτσι δεν χρειάζεται να ελέγχει τους κανόνες του κάθε φορά που λαμβάνει ένα πακέτο. Αυτό συμβαίνει μόνο όταν ξεκινά μια νέα συνεδρία επικοινωνίας. (Kim & Solomon, 2018)

2.2.2 Application Level Filtering

Τα application level firewall προχωρούν ένα βήμα παραπέρα από τα stateful packet inspection (SPI). Δεν επιτρέπουν στην πραγματικότητα τα πακέτα να ταξιδεύουν απευθείας μεταξύ των συστημάτων που βρίσκονται στις αντίθετες πλευρές του τείχους προστασίας. Το τείχος προστασίας ανοίγει ξεχωριστές συνδέσεις επικοινωνίας με καθένα από τα δύο συστήματα και στη συνέχεια ενεργεί ως ενδιάμεσος (proxy) μεταξύ των δύο. Αυτό προσθέτει έναν πρόσθετο βαθμό προστασίας, επειδή το firewall κατά τη λήψη της απόφασης μπορεί να αναλύσει πληροφορίες σχετικά με την εφαρμογή που χρησιμοποιείται και έτσι να αποφασίσει αν θα επιτρέψει ή θα αρνηθεί την κυκλοφορία. (Kim & Solomon, 2018)
Τα φίλτρα πακέτων δεν χρειάζονται να καταλάβουν πολλά για την κίνηση που περιορίζουν, ενώ τα φίλτρα σε επίπεδο εφαρμογής ασχολούνται με τις λεπτομέρειες της συγκεκριμένης υπηρεσίας που ελέγχουν και είναι συνήθως πιο περίπλοκα από τα πρώτα. Αντί να χρησιμοποιούν έναν μηχανισμό γενικής χρήσης για να επιτρέπουν τη ροή πολλών διαφορετικών ειδών κυκλοφορίας, μπορούν να χρησιμοποιούν κωδικούς ειδικού σκοπού για κάθε επιθυμητή εφαρμογή. (Cheswick, Bellovin & Rubin, 2003) Συχνά εγκαθίσταται σε έναν ειδικό υπολογιστή ξεχωριστό από το τείχος προστασίας φιλτραρίσματος πακέτων, αλλά χρησιμοποιείται συνήθως σε συνδυασμό με αυτό. (Whitman & Mattord, 2014)

2.2.3 Circuit Level Gateway

Ένας άλλος τύπος τείχους προστασίας είναι η πύλη κυκλώματος ή αλλιώς ένας διακομιστής μεσολάβησης επιπέδου κυκλώματος. Αυτό μπορεί να είναι ένα αυτόνομο σύστημα ή μπορεί να είναι μια εξειδικευμένη λειτουργία που εκτελείται από ένα application level firewall για ορισμένες εφαρμογές. Όπως με μια πύλη εφαρμογών, μια

πύλη επιπέδου κυκλώματος δεν επιτρέπει την απευθείας σύνδεση TCP από άκρο σε άκρο. Αντίθετα, η πύλη δημιουργεί δύο συνδέσεις TCP, μία με τον εσωτερικό κόμβο και μία με τον εξωτερικό κόμβο. Μόλις δημιουργηθούν οι δύο συνδέσεις, η πύλη μεταδίδει συνήθως τμήματα TCP από τη μία σύνδεση στην άλλη χωρίς να εξετάσει το περιεχόμενο. Η λειτουργία ασφαλείας συνίσταται στον καθορισμό των συνδέσεων που θα επιτρέπονται. (Stallings, Brown, Bauer & Bhattacharjee, 2015) Γενικά, αυτές οι υπηρεσίες αναμετάδοσης δεν εξετάζουν τα bytes καθώς διατρέχουν. Μπορεί να καταγράψουν τον αριθμό των bytes και τον προορισμό TCP και αυτά τα αρχεία καταγραφής (logs) μπορεί να είναι χρήσιμα. (Cheswick, Bellovin & Rubin, 2003)

2.3 Τεχνικές Τοπολογίας Firewall

Ένα τείχος προστασίας βρίσκεται συνήθως στην περίμετρο του δικτύου, μεταξύ του εσωτερικού δικτύου και των εξωτερικών συνδέσεων. Ωστόσο, πρόσθετα συστήματα τείχους προστασίας μπορούν να τοποθετηθούν εντός της περιμέτρου του δικτύου για να παρέχουν πιο εξειδικευμένη προστασία σε κεντρικούς υπολογιστές με υψηλότερες απαιτήσεις ασφαλείας. (Rhodes-Ousley, 2013)

2.3.1 Border Firewall

Η τοπολογία του Border Firewall αποτελεί την πιο βασική προσέγγιση. Διαχωρίζει απλώς το προστατευμένο δίκτυο από το Διαδίκτυο. Η θέση του βρίσκεται συνήθως πίσω από το δρομολογητή και λαμβάνει όλες τις επικοινωνίες που περνούν από το δρομολογητή προς το τοπικό δίκτυο. Καθώς επίσης και όλες τις εξερχόμενες. Στη συγκεκριμένη τοπολογία χρησιμοποιούνται συνήθως είτε packet filtering είτε stateful packet inspection firewalls. Η τοπολογία του Border Firewall συναντάται πιο συχνά σε οργανισμούς που δεν φιλοξενούν δημόσιες υπηρεσίες. Στην περίπτωση που ένας οργανισμός έχει αναθέσει σε εξωτερικούς συνεργάτες να τρέχουν τις υπηρεσίες web και email τότε η ανάγκη εξωτερικών συνδέσεων προς το πληροφοριακό σύστημα είναι εκ των πραγμάτων περιορισμένη. Σε αυτήν την περίπτωση, αποτελεί κοινή πρακτική ο αποκλεισμός του μεγαλύτερου μέρους της εισερχόμενης κίνησης (αν όχι όλου). Η συγκεκριμένη τοπολογία υπερέχει σε αυτό το σενάριο. (Kim & Solomon, 2018)

2.3.2 Demilitarized Zone (DMZ)

Συχνά ένας οργανισμός δεν είναι δυνατό να αποκλείσει όλη την κυκλοφορία στο δίκτυό του. Στην περίπτωση που φιλοξενεί έναν δημόσιο ιστότοπο ή τον δικό σας διακομιστή email, πρέπει να επιτρέψει τις εισερχόμενες συνδέσεις σε περιορισμένη βάση. Το DMZ είναι η καλύτερη προσέγγιση για αυτόν τον τύπο απαιτήσεων. Σε αυτήν την περίπτωση το firewall έχει τρεις κάρτες δικτύου. Οι δύο έχουν ρυθμιστεί πανομοιότυπα με ένα Border Firewall, με τη μία να είναι συνδεδεμένη στο Διαδίκτυο και τη δεύτερη στο εσωτερικό δίκτυο. Η τρίτη κάρτα συνδέεται με ένα ειδικό δίκτυο που είναι γνωστό ως screened subnet ή η αποστρατικοποιημένη ζώνη (DMZ). (Kim & Solomon, 2018) Σε μια παραλλαγή αυτής της τοπολογίας η δεύτερη κάρτα του εξωτερικού τείχους προστασίας συνδέεται με ένα εσωτερικό τείχος το οποίο με τη σειρά του προστατεύει το ιδιωτικό δίκτυο με αυστηρότερους κανόνες.
Συνήθως, τα συστήματα που βρίσκονται στο DMZ απαιτούν ή ενισχύουν εξωτερική συνδεσιμότητα του οργανισμού, όπως εταιρική ιστοσελίδα, τον διακομιστή e-mail ή τον διακομιστή DNS. Το εξωτερικό τείχος προστασίας παρέχει ένα μέτρο ελέγχου πρόσβασης

και προστασίας για τα συστήματα DMZ σύμφωνα με την ανάγκη τους για εξωτερική συνδεσιμότητα. Το εξωτερικό τείχος προστασίας παρέχει επίσης ένα βασικό επίπεδο προστασίας για το υπόλοιπο του εταιρικού δικτύου. Σε αυτόν τον τύπο διαμόρφωσης, τα εσωτερικά τείχη προστασίας εξυπηρετούν τρεις σκοπούς:
1. Το εσωτερικό τείχος προστασίας παρέχει τη δυνατότητα πιο αυστηρού φιλτραρίσματος, σε σύγκριση με το εξωτερικό τείχος προστασίας, προκειμένου να προστατεύσει τους διακομιστές και τους σταθμούς εργασίας από εξωτερικές επιθέσεις.
2. Το εσωτερικό τείχος προστασίας παρέχει αμφίδρομη προστασία σε σχέση με το DMZ. Πρώτον, το εσωτερικό τείχος προστασίας προστατεύει το υπόλοιπο δίκτυο από επιθέσεις που μπορούν να ξεκινήσουν από τα συστήματα του DMZ. Τέτοιες επιθέσεις μπορεί να προέρχονται από worms, rootkit, bots ή άλλα κακόβουλα προγράμματα που έχουν μολύνει ή διακινούνται μέσω ενός συστήματος του DMZ. Δεύτερον, ένα εσωτερικό τείχος προστασίας μπορεί να προστατεύσει τα συστήματα DMZ από μία επίθεση που μπορεί να προέρχεται από το εσωτερικό προστατευμένο δίκτυο.
3. Πολλαπλά εσωτερικά τείχη προστασίας μπορούν να χρησιμοποιηθούν για την προστασία τμημάτων του εσωτερικού δικτύου. (Stallings, Brown, Bauer & Bhattacharjee, 2015)

2.3.3 Multilayered Firewalls (Πολυεπίπεδα τείχη προστασίας)

Σε μεγάλα ή (και) εξαιρετικά ασφαλή περιβάλλοντα, οι οργανισμοί χρησιμοποιούν συχνά πολλαπλά τείχη προστασίας για να χωρίσουν το δίκτυό τους σε τομείς. Έτσι σε ένα πληροφοριακό σύστημα δύο εσωτερικά τείχη προστασίας μπορούν να χωρίζει το εσωτερικό δίκτυο σε δύο τομείς Α και Β προστατεύοντας τον έναν από τον άλλον. Ταυτόχρονα υπάρχει και ένα τρίτο firewall το οποίο λειτουργεί ως border firewallκαι προστατεύει όλο το δίκτυο από το internet.
Τα πολλαπλά τείχη προστασίας είναι χρήσιμα όταν υπάρχουν δίκτυα με διαφορετικά επίπεδα ασφαλείας. Στην παραπάνω περίπτωση, οι γενικοί χρήστες ενδέχεται να συνδεθούν στο υποδίκτυο Α ακριβώς πίσω από το εξωτερικό firewall. Οι χρήστες που εργάζονται σε ένα μυστικό ερευνητικό έργο ενδέχεται να συνδεθούν στο υποδίκτυο Β. Τα στελέχη του οργανισμού ενδέχεται να συνδεθούν στο υποδίκτυο C. Αυτή η δομή παρέχει στο μυστικό έργο και στα στελέχη προστασία από γενική ομάδα χρηστών.

2.4 Unified Threat Management (Ενοποιημένη διαχείριση απειλών)

Τα τείχη προστασίας είναι τόσο σημαντικά για την ασφάλεια του δικτύου που έχουν εξελιχθεί σε συσκευές που κάνουν πολύ περισσότερα από μια απλή επιθεώρηση πακέτων. Στην πραγματικότητα, τα τείχη προστασίας πολλαπλών χρήσεων αναφέρονται πιο συχνά ως συσκευές ενοποιημένης διαχείρισης απειλών (UTM). Οι συσκευές UTM παρέχουν φιλτράρισμα καθώς και πολλές άλλες υπηρεσίες ασφαλείας. Ορισμένες από τις υπηρεσίες που παρέχουν οι συσκευές UTM περιλαμβάνουν:
• Φίλτρο διεύθυνσης URL - Αυτή η δυνατότητα φιλτράρει την κυκλοφορία ιστού εξετάζοντας τη διεύθυνση URL σε αντίθεση με τη διεύθυνση IP.
• Έλεγχος περιεχομένου - Η συσκευή εξετάζει μέρος ή ολόκληρο το περιεχόμενο πακέτων δικτύου για να προσδιορίσει εάν πρέπει να επιτραπεί να περάσει το πακέτο. Αυτός ο τύπος επιθεώρησης μπορεί να συντελέσει στον εντοπισμό κακόβουλου περιεχομένου από αξιόπιστες πηγές. Αυτό είναι δυνατόν να συμβεί εάν παραβιαστεί μια αξιόπιστη πηγή.

• Έλεγχος κακόβουλου λογισμικού - Μια εξειδικευμένη μορφή επιθεώρησης περιεχομένου, η συσκευή εξετάζει το περιεχόμενο των πακέτων για ενδείξεις κακόβουλου λογισμικού.

Αυτές οι ενοποιημένες υπηρεσίες καθιστούν δυνατή τη μείωση του αριθμού των συσκευών που πρέπει να αναλύουν πακέτα δικτύου. Λιγότερες συσκευές UTM μπορούν να παρέχουν το ίδιο επίπεδο ασφάλειας με πολλές αλλά παλαιότερες συσκευές. Ωστόσο, ακόμη και όταν γίνεται χρήση λιγότερων συσκευών που επιθεωρούν πακέτα, η εγκατάσταση συσκευών UTM επιβραδύνει συχνά ένα δίκτυο λόγω του μεγάλου όγκου εργασίας που πρέπει να επιτελέσουν οι συσκευές. Χρειάζεται χρόνος για τον έλεγχο και την ανάλυση κάθε πακέτου δικτύου σε πολλαπλά επίπεδα της στοίβας δικτύου. Για το λόγο αυτό, ορισμένοι οργανισμοί έχουν επιλέξει μια προσέγγιση «μεσαίου δρόμου». Μια πύλη ασφάλειας ιστού επιτυγχάνει μερικά από αυτά που κάνει μια συσκευή UTM, δίχως τις καθυστερήσεις που προκαλούν. Εν ολίγοις, μια πύλη ασφαλείας ιστού εκτελεί φιλτράρισμα διευθύνσεων URL, αλλά δεν εξετάζει το περιεχόμενο των πακέτων. (Kim & Solomon, 2018)

2.5 Virtual Private Networks (Ιδιωτικά Εικονικά Δίκτυα)

Με την έλευση της τηλεργασίας, η απομακρυσμένη πρόσβαση έχει βρει εφαρμογή σε πολλά εταιρικά δίκτυα. Σήμερα πολλές εταιρείες έχουν υπαλλήλους οι οποίοι σπάνια έρχονται ποτέ στο χώρο εργασίας. Αυτοί οι χρήστες εργάζονται στο σπίτι ή στο δρόμο. Ωστόσο, χρειάζονται πρόσβαση σε πόρους και υπηρεσίες. Αυτό σημαίνει ότι για να μπορέσουν να αποκτήσουν πρόσβαση στα συστήματα και τις υπηρεσίας της εταιρείας πρέπει να γίνει χρήση του Διαδικτύου με ότι και αν σημαίνει αυτό όσον αφορά την ασφάλεια. Στόχος είναι οι υπάλληλοι να αποκτήσουν την πρόσβαση που χρειάζονται, δίχως να καταστεί το πληροφοριακό σύστημα ευάλωτο σε εξωτερικές επιθέσεις.

Τα εικονικά ιδιωτικά δίκτυα (VPN) είναι ένας καλός τρόπος για να αυξηθεί το επίπεδο ασφάλειας των δεδομένων που μεταδίδονται μέσω ενός δημόσιου δικτύου δεδομένων. Συνήθως χρησιμοποιούν κρυπτογράφηση για να προστατεύσουν όλα τα δεδομένα που ανταλλάσσονται μεταξύ ενός χρήστη και του δικτύου του οργανισμού. Η χρήση ενός VPN για απομακρυσμένη πρόσβαση παρέχει ασφάλεια και είναι οικονομικά αποδοτική. Η διαφορά κόστους της χρήσης ενός VPN έναντι του κόστους μιας αποκλειστικής σύνδεσης είναι σημαντική. (Kim & Solomon, 2018)

Ο στόχος ενός VPN είναι να παρέχει ένα ασφαλές κανάλι επικοινωνίας μέσω ενός δικτύου, συνήθως ένα ιδιωτικό tunnel μέσω του Διαδικτύου. Για να γίνει αυτό, ενσωματώνεται μια κεφαλίδα που παρέχει πληροφορίες δρομολόγησης ώστε τα πακέτα να φτάσουν στον προορισμό. Επιπρόσθετα εφαρμόζεται κρυπτογράφηση και στα πακέτα και με τον τρόπο αυτό εξασφαλίζονται η ακεραιότητα, η εμπιστευτικότητα και η αυθεντικότητα.

Οι περισσότερες συνδέσεις VPN επιτρέπουν την ενθυλάκωση όλων των κοινών τύπων κίνησης δικτύου. Οι συνδέσεις IPv6 μπορούν επίσης να μεταφερθούν σε δίκτυα IPv4 χρησιμοποιώντας tunnel, αλλά αυτοί οι τύποι δεν είναι απαραίτητα κρυπτογραφημένοι και από μόνοι τους δεν είναι VPN (αναφέρονται ως σήραγγες διπλής στοίβας και υπάρχουν μερικές διαφορετικές μέθοδοι ως προς τη χρήση τους). Ο απώτερος στόχος της υπηρεσίας VPN είναι να επιτρέψει στους πελάτες να έχουν τις ίδιες λειτουργικές δυνατότητες μέσω του tunnel που θα είχαν αν ήταν τοπικά συνδεδεμένοι με το εταιρικό τους δίκτυο δηλαδή παρέχει μια ασφαλή απομακρυσμένη πρόσβαση. (Rhodes-Ousley, 2013)

Τα εικονικά ιδιωτικά δίκτυα (VPN) αποτελούν εφαρμογή της κρυπτογραφίας. Το Virtual Private Network Consortium (VPNC, στο www.vpnc.org) ορίζει το VPN ως «ένα ιδιωτικό

δίκτυο δεδομένων που χρησιμοποιεί τη δημόσια υποδομή τηλεπικοινωνιών, διατηρώντας ταυτόχρονα το απόρρητο μέσω της χρήσης ενός πρωτοκόλλου tunnelling και διαδικασιών ασφαλείας. Τα VPN χρησιμοποιούνται συνήθως για την ασφαλή επέκταση των εσωτερικών συνδέσεων του δικτύου ενός οργανισμού σε απομακρυσμένες τοποθεσίες. Το VPNC ορίζει τρεις τεχνολογίες VPN: τα αξιόπιστα-Trusted VPN, τα ασφαλή-Secure VPN και τα υβριδικά-Hybrid VPN. Ένα Trusted VPN, γνωστό και ως παλαιό VPN, βρίσκει εφαρμογή όταν ο οργανισμός χρησιμοποιεί μισθωμένα κυκλώματα από έναν πάροχο ISP και πραγματοποιεί την εναλλαγή πακέτων. Ο οργανισμός πρέπει να εμπιστεύεται τον πάροχο υπηρεσιών, ο οποίος παρέχει υπεύθυνη διαβεβαίωση ότι κανένας άλλος δεν επιτρέπεται να χρησιμοποιεί αυτά τα κυκλώματα και ότι τα κυκλώματα συντηρούνται και προστατεύονται σωστά - εξ ου και το όνομα αξιόπιστο VPN. Τα Secure VPN χρησιμοποιούν πρωτόκολλα ασφαλείας όπως το IPSec για να κρυπτογραφούν την κυκλοφορία που περνάει μέσα από μη ασφαλή δημόσια δίκτυα όπως το Διαδίκτυο. Ένα Hybrid VPN συνδυάζει και τις δύο τεχνολογίες παρέχοντας κρυπτογραφημένες μεταδόσεις (όπως σε ασφαλές VPN) μέσω κάποιου ασφαλούς ή μη δικτύου.

Για να μπορεί ένα VPN να είναι ασφαλές και αξιόπιστο ενώ βασίζεται σε δημόσια δίκτυα πρέπει να επιτύχει τα ακόλουθα, ανεξάρτητα από τις συγκεκριμένες τεχνολογίες και πρωτόκολλα που χρησιμοποιούνται:

● Ενθυλάκωση εισερχόμενων και εξερχόμενων δεδομένων, στην οποία το εγγενές πρωτόκολλο του πελάτη είναι ενσωματωμένο στα πλαίσια ενός πρωτοκόλλου που μπορεί να δρομολογηθεί μέσω του δημόσιου δικτύου και να χρησιμοποιηθεί από το περιβάλλον δικτύου διακομιστή.

● Κρυπτογράφηση των εισερχόμενων και των εξερχόμενων δεδομένων ώστε να διατηρηθεί η ιδιωτικότητα των δεδομένων κατά τη μεταφορά τους μέσω δημόσιου δικτύου, αλλά ταυτόχρονα να μπορούν να χρησιμοποιηθούν από τους υπολογιστές-πελάτες και τους διακομιστές στα τοπικά δίκτυα που βρίσκονται στα δύο άκρα της σύνδεσης VPN.

● Έλεγχος ταυτότητας του απομακρυσμένου υπολογιστή και ίσως και του απομακρυσμένου χρήστη. Ο έλεγχος ταυτότητας και η επακόλουθη εξουσιοδότηση χρήστη για την εκτέλεση συγκεκριμένων ενεργειών βασίζονται στην ακριβή και αξιόπιστη αναγνώριση του απομακρυσμένου συστήματος και του χρήστη. (Whitman & Mattord, 2014)

Τα VPN απαιτούν από τον εξοπλισμό πύλης (gateway) να έχει περίσσεια επεξεργαστικής ισχύς ώστε να είναι σε θέση να διαχειριστεί τους αλγόριθμους κρυπτογράφησης. Την εργασία αυτή, υπάρχει δυνατότητα να την αναλάβει κάποια εξειδικευμένη συσκευή VPN, αποφεύγοντας έτσι ανεπιθύμητους τερματισμούς συνδέσεων λόγω υπερφόρτωσης του router ή του firewall. Σημαντικό σημείο κατά την ανάπτυξη ενός VPN είναι η ασφάλεια των υπολογιστών των τελικών χρηστών. Μόλις οι χρήστες συνδεθούν στο εταιρικό δίκτυο, οι υπολογιστές τους θα μπορούσαν για έναν εισβολέα να λειτουργήσουν ως μια ανοιχτή πύλη προς τους εταιρικούς πόρους και να αποκτήσουν πρόσβαση. Για το λόγο αυτό, πολλοί οργανισμοί απαιτούν από τους υπαλλήλους να εγκαταστήσουν λογισμικό ασφαλείας στους οικιακούς υπολογιστές τους. Οι τρεις κύριες τεχνολογίες VPN που χρησιμοποιούνται σήμερα είναι οι εξής:

• Point-to-Point Tunneling Protocol (PPTP) - Το συγκεκριμένο πρωτόκολλο ήταν κάποτε το πιο διαδεδομένο. Για πολλά χρόνια, σχεδόν όλα τα VPN χρησιμοποίησαν PPTP. Ρυθμίζεται εύκολα υπολογιστές-πελάτες, επειδή τα περισσότερα λειτουργικά συστήματα το υποστηρίζουν.

• Secure Sockets Layer (SSL) - Το Secure Sockets Layer κρυπτογραφεί τις επικοινωνίες ιστού και πολλά VPN το χρησιμοποιούν για να παρέχουν κρυπτογραφημένη επικοινωνία. Οι

χρήστες συνδέονται σε μια ιστοσελίδα που προστατεύεται από SSL και συνδέονται. Στη συνέχεια, το πρόγραμμα περιήγησης ιστού πραγματοποιεί λήψη ειδικού λογισμικού που τα συνδέει με το VPN. Η μέθοδος αυτή δεν απαιτεί την εκ των προτέρων διαμόρφωση του συστήματος. Για αυτόν τον λόγο, τα SSL VPN γίνονται ολοένα και πιο δημοφιλή στους χρήστες.

• IPSec — Internet Protocol Security (IPSec) είναι μια σειρά πρωτοκόλλων που έχουν σχεδιαστεί για να συνδέονται τα μέρη με ασφάλεια. Παρόλο που ορισμένα IPSec VPN είναι διαθέσιμα για τελικούς τους χρήστες, συχνά απαιτούν την εγκατάσταση λογισμικού τρίτων στο σύστημα του χρήστη και για το λόγο αυτό δεν είναι δημοφιλή. Πολλοί οργανισμοί χρησιμοποιούν το IPSec για να συνδέσουν δύο σημεία με ασφάλεια μέσω του Διαδικτύου. Πολλοι δρομολογητές και τείχη προστασίας υποστηρίζουν το πρωτόκολλο IPSec το οποίο ενσωματώνουν στις επιλογές λειτουργίας τους προσφέροντας έτσι τη δυνατότητα να ρυθμιστούν εύκολα.

Τα ιδιωτικά εικονικά δίκτυα συνεισφέρουν στη λειτουργία ενός οργανισμού. Προσφέρουν μια οικονομική και ασφαλή εναλλακτική των μισθωμένων γραμμών μεταξύ δύο σημείων. Επιτρέπουν επίσης στους χρήστες να συνδέονται με ασφάλεια στο δίκτυο του οργανισμού από απομακρυσμένες τοποθεσίες. Αυτό βοηθάει στην αύξηση της παραγωγικότητας επειδή οι εργαζόμενοι μπορούν εύκολα να έχουν πρόσβαση στους πόρους που χρειάζονται ενώ βρίσκονται εν κινήσει. (Kim & Solomon, 2018)

2.6 Network access control (NAC) - Έλεγχος πρόσβασης στο σύστημα

Τα συστήματα NAC σας επιτρέπουν τον διαχειριστή να προσθέσει επιπλέον απαιτήσεις ασφαλείας πριν επιτραπεί σε μια συσκευή να συνδεθεί στο δίκτυό. Έτσι εκτελούνται δύο σημαντικές εργασίες: ο έλεγχος ταυτότητας και η στάση. Αν και το NAC είναι μια νέα τεχνολογία, η δημοτικότητά της αυξάνεται. Πολλοί οργανισμοί αναπτύσσουν Network access controls τόσο για εσωτερικούς χρήστες όσο και για τους επισκέπτες που χρησιμοποιούν το δίκτυό τους ενώ λειτουργεί το σε ενσύρματα όσο και σε ασύρματα δίκτυα. Το πρότυπο IEEE 802.1x περιγράφει την πιο κοινή τεχνολογία NAC. Συνήθως αναφέρεται ως απλά 802.1x ή 1x, αυτό το πρότυπο αναφέρει τη διαδικασία που πρέπει να ακολουθήσουν οι πελάτες ώστε να αλληλεπιδράσουν με μια συσκευή NAC και να αποκτήσουν πρόσβαση στο δίκτυο. Το λογισμικό που είναι εγκατεστημένο στους υπολογιστές των χρηστών απαιτεί την κατάθεση των διαπιστευτηρίων για να επιτρέψει τη σύνδεση με το δίκτυο.. Αφού τα επαληθεύσει, η συσκευή NAC δίνει εντολή στο switch (περίπτωση ενσύρματου δικτύου) ή στο access point (περίπτωση ασύρματου δικτύου) να επιτρέψει στον χρήστη την πρόσβαση στο δίκτυο. Αυτό είναι το στοιχείο ελέγχου ταυτότητας του NAC. Ο έλεγχος στάσης είναι μια προαιρετική δεύτερη χρήση της τεχνολογίας NAC. Όταν χρησιμοποιείται ο έλεγχος στάσης, η συσκευή NAC ελέγχει τη διαμόρφωση του υπολογιστή του χρήστη για να διασφαλίσει ότι πληροί τα πρότυπα ασφαλείας πριν του επιτρέψει την πρόσβαση στο δίκτυο. Ορισμένα στοιχεία που ελέγχονται συνήθως περιλαμβάνουν τα εξής:

• Ενημερωμένο λογισμικό προστασίας από ιούς
• Ενεργοποιημένο τείχος προστασίας
• Υποστηριζόμενο λειτουργικό σύστημα
• Ενημερωμένο λειτουργικό σύστημα

Εάν οι χρήστες προσπαθήσουν να συνδέσουν ένα μη συμμορφούμενο σύστημα σε ένα δίκτυο, η συσκευή NAC προσφέρει δύο επιλογές. Ο διαχειριστής μπορεί να αποφασίσει να αποκλείσει τέτοια συστήματα από το δίκτυο έως ότου επιδιορθωθούν. Εναλλακτικά,

το σύστημα μπορεί να συνδεθεί σε ένα ειδικό δίκτυο καραντίνας όπου παρέχεται η δυνατότητα να διορθωθεί το σύστημα πριν επιτραπεί η πρόσβαση στο κύριο δίκτυο. Το Extensible Authentication Protocol (EAP) είναι ένα πλαίσιο ελέγχου ταυτότητας που καθορίζει τη μεταφορά των κλειδιών και των διαπιστευτηρίων του ελέγχου ταυτότητας. Το EAP χρησιμοποιείται συνήθως στον έλεγχο ταυτότητας σε ένα ασύρματο δίκτυο. Το Protected Extensible Authentication Protocol (PEAP) είναι το EAP που εκτελείται σε ένα tunnel TLS. Το PEAP παρέχει περισσότερη ασφάλεια από το EAP για ανταλλαγές ελέγχου ταυτότητας. (Kim & Solomon, 2018)

2.7 Intrusion Detection Systems – Συστήματα ανίχνευσης εισβολών (IDS)

Ανίχνευση εισβολής καλείται η υπηρεσία ασφαλείας που παρακολουθεί και αναλύει τα συμβάντα του συστήματος με σκοπό την εύρεση και την έγκαιρη προειδοποίηση σε πραγματικό ή σχεδόν σε πραγματικό χρόνο, των προσπαθειών πρόσβασης σε πόρους του συστήματος με μη εξουσιοδοτημένο τρόπο. (Stallings, Brown, Bauer & Bhattacharjee, 2015)

Τα συστήματα IDS έχουν τέσσερεις κύριους σκοπούς:

Να εντοπίζουν μία πληθώρα από εισβολές, αυτές μπορούν να προέρχονται είτε από το εσωτερικό δίκτυο είτε από εξωτερικούς εισβολείς. Επιπλέον, πρέπει να είναι σε θέση να αναγνωρίζουν τόσο τις γνωστές επιθέσεις όσο και τις προηγουμένως άγνωστες. Αυτό υποδηλώνει την ύπαρξη ενός μηχανισμού εκμάθησης ή προσαρμογής σε νέους τύπους επιθέσεων ή σε αλλαγές της φυσιολογικής δραστηριότητας.

Να ανιχνεύουν τις εισβολές εγκαίρως. Ο όρος εγκαίρως δεν αναφέρεται στον εντοπισμό σε πραγματικό χρόνο αλλά σε ένα εύλογο σύντομο χρονικό διάστημα. Η ανάλυση της κίνησης του δικτύου σε πραγματικό χρόνο μπορεί να προκαλέσει προβλήματα στην ομαλή λειτουργία του, από την άλλη πλευρά όμως η ανάλυση πρέπει να ολοκληρωθεί εγκαίρως και οι διαχειριστές του ΠΣ να ενημερωθούν.

Να παρουσιάζουν με απλό και κατανοητό τρόπο την ανάλυση της κίνησης του δικτύου. Τα δεδομένα της κίνησης είναι πολύπλοκα ενώ συνήθως προέρχονται από παραπάνω από ένα συστήματα, η διεπαφή χρήστη του IDS έχει κομβικό ρόλο.

Να είναι ακριβή. Μία εσφαλμένη προειδοποίηση εισβολής λαμβάνει χώρα όταν το σύστημα αναφέρει επίθεση δίχως στην πραγματικότητα να υπάρχει. Οι εσφαλμένες ειδοποιήσεις αυξάνουν τον φόρτο εργασίας και μειώνουν την εμπιστοσύνη προς το σύστημα και τα αποτελέσματα που παρέχει. Παρόλα αυτά η αδυναμία εντοπισμού εισβολής θεωρείται μεγαλύτερος κίνδυνος διότι ο εντοπισμός τους είναι η κύρια εργασία αυτών των συστημάτων. (Bishop, 2002)

Ένα IDS περιλαμβάνει τρία λογικά στοιχεία:

• Αισθητήρες: Οι αισθητήρες είναι υπεύθυνοι για τη συλλογή δεδομένων. Η είσοδος για έναν αισθητήρα μπορεί να είναι οποιοδήποτε μέρος ενός συστήματος που θα μπορούσε να περιέχει ενδείξεις εισβολής. Οι τύποι εισόδου σε έναν αισθητήρα περιλαμβάνουν πακέτα δικτύου, αρχεία καταγραφής και ίχνη κλήσεων του συστήματος. Οι αισθητήρες συλλέγουν και προωθούν αυτές τις πληροφορίες στον αναλυτή.

• Αναλυτές: Οι αναλυτές λαμβάνουν ως είσοδο τα δεδομένα που έρχονται από έναν ή περισσότερους αισθητήρες ή από άλλους αναλυτές. Ο αναλυτής είναι υπεύθυνος να προσδιορίσει εάν έχει συμβεί εισβολή. Ως έξοδο δίνει την ένδειξη ότι έχει πραγματοποιηθεί εισβολή. Η έξοδος μπορεί να περιλαμβάνει αποδεικτικά στοιχεία που να υποστηρίζουν αυτό το συμπέρασμα. Ο αναλυτής μπορεί να παρέχει καθοδήγηση σχετικά με τις ενέργειες που πρέπει να ληφθούν ως αποτέλεσμα της εισβολής. Τα

δεδομένα εισόδου του αισθητήρα μπορούν επίσης να αποθηκευτούν για μελλοντική ανάλυση και αναθεώρηση σε μία μονάδα αποθήκευσης ή σε μία βάση δεδομένων.
• Διεπαφή χρήστη: Η διεπαφή χρήστη επιτρέπει στον χρήστη να βλέπει την έξοδο από το σύστημα ή να ελέγχει τη συμπεριφορά του συστήματος.
Ένα IDS μπορεί να χρησιμοποιεί έναν μόνο αισθητήρα και έναν αναλυτή, όπως ένα κλασικό HIDS σε έναν κεντρικό υπολογιστή ή ένα NIDS εγκατεστημένο σε ένα firewall. Τα πιο εξελιγμένα IDS μπορούν να χρησιμοποιούν πολλαπλούς αισθητήρες, σε μια σειρά συσκευών όπως κεντρικοί υπολογιστές και δικτυακές συσκευές, οι οποίοι στέλνουν πληροφορίες στον κεντρικό αναλυτή και στη διεπαφή χρήστη του συστήματος εφαρμόζοντας την αρχιτεκτονική των κατανεμημένων συστημάτων. Τα IDS ταξινομούνται συχνά με βάση την πηγή και τον τύπο των δεδομένων που αναλύονται:
• Host-based IDS (HIDS): Ο τύπος HIDS παρακολουθεί τα χαρακτηριστικά ενός μεμονωμένου κεντρικού υπολογιστή και τα συμβάντα που συμβαίνουν σε αυτόν. Τέτοια είναι τα αναγνωριστικά διεργασιών και οι κλήσεις συστήματος που πραγματοποιούν, ανιχνεύοντας ενδείξεις ύποπτης δραστηριότητας.
• Network based IDS (NIDS): Ο τύπος NIDS παρακολουθεί την κίνηση που πραγματοποιείται σε συγκεκριμένα τμήματα του δικτύου ή σε συσκευές του και αναλύει πρωτόκολλα δικτύου, μεταφορών και εφαρμογών για τον εντοπισμό ύποπτης δραστηριότητας.
• Κατανεμημένα ή υβριδικά IDS: Ο τύπος hybrid IDS συνδυάζει πληροφορίες που λαμβάνει από μία ομάδα αισθητήρων που είναι εγκατεστημένη τόσο σε κεντρικούς υπολογιστές όσο και σε συσκευές του δικτύου. Με αυτόν τον τρόπο ο κεντρικός αναλυτής είναι σε θέση να εντοπίζει και να ανταποκρίνεται καλύτερα σε περίπτωση εισβολής.
Τα IDS λειτουργούν συμπληρωματικά σε άλλα συστήματα προστασίας ενός πληροφοριακού συστήματος και αποτελούν μία ακόμα γραμμή άμυνας. Σε περίπτωση που μία εισβολή ανιχνευθεί αρκετά γρήγορα τότε ο εισβολέας είναι δυνατόν να αναγνωριστεί και να εξαχθεί από το σύστημα προτού γίνει οποιαδήποτε ζημιά ή κινδυνεύσουν τα δεδομένα. Ακόμα και στην περίπτωση που η εισβολή δεν ανιχνευθεί έγκαιρα, όσο πιο σύντομα συμβεί αυτό τόσο μικρότερη ζημιά θα γίνει και η ανάκτησης του συστήματος θα γίνει γρήγορα. Ακόμα, ένα αποτελεσματικό IDS μπορεί να χρησιμεύσει αποτρεπτικά αφού με τις ενέργειές του αποσοβεί τις εισβολές. Τέλος κατά τη διάρκεια μίας εισβολής, το σύστημα συλλέγει πληροφορίες για τις τεχνικές που χρησιμοποιήθηκαν ώστε να λάβει επιπρόσθετα μέτρα.
Η ανίχνευση εισβολών στηρίζεται στην υπόθεση ότι η συμπεριφορά του εισβολέα διαφέρει από αυτήν ενός νόμιμου χρήστη και αυτό μπορεί να ποσοτικοποιηθεί. Όπως είναι αναμενόμενο δεν υπάρχει σαφής διαχωρισμός μεταξύ της κανονικής χρήσης των πόρων που κάνει έναν εξουσιοδοτημένος χρήστης και της επίθεσης που κάνει ένας εισβολέας. Αντίθετα είναι αναμενόμενο να υπάρξει ως ένα σημείο αλληλεπικάλυψη. Αυτό σημαίνει ότι θα υπάρξουν περιπτώσεις που το IDS θα δώσει εσφαλμένες προειδοποιήσεις. Σε περίπτωση που διαχειριστής προσπαθήσει να μειώσει ένα τέτοιο ενδεχόμενο να συμβεί ελλοχεύει ο κίνδυνος το σύστημα να μην προειδοποιήσει και ο εισβολέας να μην αναγνωριστεί.
Τα Συστήματα ανίχνευσης εισβολών χρησιμοποιούν 2 εναλλακτικές μεθόδους για την ανάλυση των δεδομένων που λαμβάνουν από τους αισθητήρες. Η πρώτη είναι η ανίχνευση ανωμαλιών. Σύμφωνα με αυτήν την προσέγγιση, συλλέγονται τα δεδομένα που σχετίζονται με τη κίνηση που προκαλείται από τη χρήση του συστήματος από τους εξουσιοδοτημένους χρήστες. Στη συνέχεια η τρέχουσα κίνηση αναλύεται ώστε να προσδιοριστεί σε μεγάλο βαθμό εάν αυτή προέρχεται από έναν εισβολέα ή ένα νόμιμο χρήστη. Η δεύτερη μέθοδος ονομάζεται signature (ή heuristic) και βασίζεται σε ένα

σύνολο γνωστών μοτίβων κακόβουλων δεδομένων (υπογραφές-signatures) ή σε έναν σύνολο κανόνων επίθεσης (ευρετικές-heuristics). Τα στοιχεία αυτά συγκρίνονται με την τρέχουσα κίνηση του δικτύου ώστε να αποφασιστεί αν το σύστημα θα δώσει ως έξοδο το μήνυμα του συναγερμού. Αυτή η τεχνική αυτή είναι επίσης γνωστή ως ανίχνευση κακής χρήσης. Χαρακτηριστικό της είναι ότι μπορεί να αναγνωρίσει μόνο γνωστές επιθέσεις για τις οποίες έχει μοτίβα ή κανόνες. (Stallings, Brown, Bauer & Bhattacharjee, 2015)

2.7.1 Host-Based IDS (HIDS)

Ένα HIDS μπορεί να εγκατασταθεί σε έναν ηλεκτρονικό υπολογιστή το οποίο πρέπει να παρακολουθεί. Αυτός μπορεί να είναι έναν διακομιστής, ένας σταθμός εργασίας ή οποιαδήποτε δικτυακή συσκευή (εκτυπωτής, δρομολογητής ή πύλη εξόδου). Το HIDS μπορεί να εγκαθίσταται με πολλές μορφές όπως υπηρεσίας, daemon, τροποποίηση του πυρήνα ή ακόμα και ως εφαρμογή του υποκείμενου λειτουργικού συστήματος για να αποκτήσει δικαιώματα πρώτου ελέγχου. Παρόλο που το IDS μπορεί να εκτελέσει τη λειτουργία sniffing στην κίνηση του δικτύου, έχει εξαιρετικές επιδόσεις στην παρακολούθηση και την αναφορά των άμεσων αλληλεπιδράσεων που λαμβάνουν χώρα στο επίπεδο εφαρμογών. Οι επιθέσεις εφαρμογών μπορούν να περιλαμβάνουν τροποποιήσεις μνήμης, κακόβουλα αιτήματα εφαρμογών, υπερχείλιση buffer ή προσπάθειες τροποποίησης αρχείων. Ένα HIDS μπορεί να επιθεωρήσει κάθε εισερχόμενη εντολή, αναζητώντας σημάδια κακόβουλης λειτουργίας ή απλά να παρακολουθήσει μη εξουσιοδοτημένες αλλαγές αρχείων.
Ένα HIDS ακεραιότητας αρχείων (μερικές φορές ονομάζεται snapshot ή checksum HIDS) παίρνει ένα κρυπτογραφικό κατακερματισμό (hash) σημαντικών αρχείων ο οποίος είναι καθαρός, αργότερα επαναλαμβάνει τον έλεγχο για να τα συγκρίνει. Εάν παρατηρηθούν τυχόν αλλαγές, το HIDS ειδοποιεί τον διαχειριστή ότι ενδέχεται να υπήρξε αλλαγή στην ακεραιότητα.
Τα HIDS που παρακολουθούν τη συμπεριφορά (behavior- monitoring) εκτελούν παρακολούθηση σε πραγματικό χρόνο και ανακόπτουν ενδεχόμενη κακόβουλη συμπεριφορά. Έτσι, ένα Windows HIDS αναφέρει τις προσπάθειες τροποποίησης του μητρώου, τη μεταβολή των αρχείων, την πρόσβαση στο σύστημα, την αλλαγή κωδικών πρόσβασης, την αναβάθμιση των προνομίων δηλαδή την απευθείας τροποποίηση του κεντρικού υπολογιστή. Σε έναν κεντρικό υπολογιστή Unix, το HIDS που παρακολουθεί τη συμπεριφορά μπορεί να παρακολουθεί τις προσπάθειες πρόσβασης σε δυαδικά αρχεία συστήματος, τις απόπειρες λήψης των αρχείων που περιέχουν τους κωδικούς πρόσβασης, τις αλλαγές δικαιωμάτων και των προγραμματισμένων εργασιών. Ένα HIDS που παρακολουθεί τη συμπεριφορά σε έναν διακομιστή ιστού ενδέχεται να παρακολουθεί τα εισερχόμενα αιτήματα και να αναφέρει κακόβουλα επεξεργασμένες απαντήσεις HTML, επιθέσεις σεναρίων μεταξύ ιστότοπων ή έγχυση κώδικα SQL.

2.7.2 Network-Based IDS (NIDS)

Τα NIDS είναι τα πιο δημοφιλή από την οικογένεια των IDS και λειτουργούν συλλαμβάνοντας και αναλύοντας τα πακέτα δικτύου που διακινούνται μέσω του καλωδίου. Σε αντίθεση με το HIDS (το οποίο προστατεύει τη συσκευή στην οποία είναι εγκατεστημένο), το NIDS έχει σχεδιαστεί να προστατεύει περισσότερες από μία συσκευές. Μπορεί να προστατεύσει μια ομάδα κεντρικών υπολογιστών όπως είναι ένα σύμπλεγμα διακομιστών, ή να παρακολουθεί ένα ολόκληρο δίκτυο. Η κίνηση που καταγράφεται συγκρίνεται με τις προδιαγραφές πρωτοκόλλου και τη συμπεριφορά της κανονικής

κυκλοφορίας ή τα ωφέλιμα δεδομένα του πακέτου εξετάζονται για κακόβουλο περιεχόμενο. Εάν σημειωθεί απειλή ασφαλείας, καταγράφεται το συμβάν και δημιουργείται ειδοποίηση.

Ένα NIDS λειτουργεί εξετάζοντας την κυκλοφορία πακέτων δικτύου, συμπεριλαμβανομένης της κυκλοφορίας που δεν προορίζεται για τη συσκευή που φιλοξενεί το NIDS στο δίκτυο, για το λόγο αυτό η παραμετροποίηση είναι πιο σύνθετη από ένα HIDS. Έτσι ένα NIDS μπορεί να μην δημιουργήσει καθόλου ειδοποιήσεις διότι είτε δεν υπάρχει απειλή είτε δεν έχει ρυθμιστεί να ελέγχει τα πακέτα που κατευθύνονται σε άλλες συσκευές του Πληροφοριακού συστήματος. (Rhodes-Ousley, 2013)

Τα NIDS περιλαμβάνονται συνήθως στην περιμετρική υποδομή ασφαλείας ενός οργανισμού. Είναι είτε ενσωματωμένα είτε συνδεδεμένα με το τείχος προστασίας. Συνήθως επικεντρώνονται στην παρακολούθηση εξωτερικών προσπαθειών εισβολής, αναλύοντας για κακόβουλη δραστηριότητα τόσο τα πρότυπα κυκλοφορίας όσο και το περιεχόμενο της κυκλοφορίας. Ωστόσο, με την αυξανόμενη χρήση της κρυπτογράφησης, τα NIDS έχουν χάσει πλέον την πρόσβαση σε σημαντικό περιεχόμενο, μειώνοντας την απόδοσή τους. Έτσι, ενώ μπορούν ακόμα να διαδραματίσουν σημαντικό ρόλο, πλεόν αποτελούν ένα μόνο κομμάτι της λύσης. Μια τυπική εγκατάσταση NIDS περιλαμβάνει έναν αριθμό αισθητήρων για την παρακολούθηση της κυκλοφορίας των πακέτων, έναν ή περισσότερους διακομιστές για τις λειτουργίες διαχείρισης του NIDS και μία ή περισσότερες κονσόλες διαχείρισης για τη διεπαφή με τους χρήστες. Η ανάλυση των μοτίβων κυκλοφορίας για την ανίχνευση εισβολών μπορεί να γίνει στον αισθητήρα, στον διακομιστή διαχείρισης ή σε κάποιο συνδυασμό των δύο. (Stallings, Brown, Bauer & Bhattacharjee, 2015)

2.7.3 Distributed or Hybrid Intrusion Detection (Κατανεμημένα ή Υβριδικά Συστήματα Εντοπισμού Εισβολών) (Hybrid IDS)

Τα τελευταία χρόνια η έννοια των IDS που επικοινωνούν μεταξύ τους έχει εξελιχθεί σε σχεδιάσεις που περιλαμβάνουν κατανεμημένα συστήματα που συνεργάζονται για να εντοπίσουν εισβολές και να προσαρμοστούν στα νέα είδη επιθέσεων. Αυτά συνδυάζουν ένα κεντρικό IDS, με τις συμπληρωματικές πηγές πληροφορίων που χρησιμοποιούν τα HDIS οι οποίες περιλαμβάνουν τις λεπτομέρειες των διαδικασιών και των δεδομένων των υπολογιστών στους οποίους είναι εγκατεστημένα καθώς και με τα NIDS που συμβάλουν με τα συμβάντα και τα δεδομένα του δικτύου. Τα ανωτέρω οδηγούν στη διαχείριση και το συντονισμό του εντοπισμού και της ανταπόκρισης έναντι εισβολών στο πληροφοριακό σύστημα ενός οργανισμού. Τα IDS, τα firewall και τα υπόλοιπα συστήματα ασφαλείας αντιμετωπίζουν δύο σημαντικά θέματα. Το πρώτο συνίσταται στην αδυναμία του να αναγνωρίζουν μία απειλή είτε είναι νέα είτε προϋπάρχουσα που έχει όμως παραλλαχθεί σε μεγάλο βαθμό. Το δεύτερο περιλαμβάνει την αδυναμία έγκαιρης επικαιροποίησης του σχεδιασμού ώστε να αντιμετωπιστούν άμεσα οι επιθέσεις. Ξεχωριστό θέμα αποτελεί η περίμετρος ασφαλείας του συστήματος μιας και στις σύγχρονες επιχείρησης το σύνορο είναι μια αφηρημένη έννοια αφού ένας υπάλληλος μπορεί να συνδεθεί ασύρματα στο σύστημα είναι να αποκτήσει πρόσβαση με τη χρήση ενός φορητού υπολογιστή και ενός καλωδίου δικτύου. Η εκμετάλλευση αυτών των αδυναμιών έχει συμβεί συχνά. Οι επιτιθέμενοι αναπτύσσουν σκουλήκια (worms) και άλλο κακόβουλο λογισμικό το οποίο εξαπλώνεται πολύ γρήγορα και εξαπολύουν επιθέσεις που χτυπούν με σφοδρότητα προτού προλάβει να προετοιμαστεί η άμυνα. Αυτό το είδος επίθεσης εξακολουθεί να κυριαρχεί. Πρόσφατα όμως οι επιτιθέμενοι έχουν αναπτύξει μια τελείως διαφορετική προσέγγιση: Επιβραδύνουν τον ρυθμό εξάπλωσης της επίθεσης ώστε να καταστήσουν

εξαιρετικά δύσκολο τον εντοπισμό τους από τους συμβατικούς αλγόριθμους. (Anthes, 2007)
Ένας τρόπος για να αντιμετωπιστούν αυτές οι επιθέσεις είναι η ανάπτυξη συνεργαζόμενων συστημάτων τα οποία θα είναι σε θέση να αναγνωρίσουν αυτές τις επιθέσεις βασιζόμενα σε πιο ισχνές ενδείξεις και στη συνέχεια να προσαρμοστούν γρήγορα. Σύμφωνα με αυτήν την προσέγγιση, ανιχνευτές ανωμαλιών που είναι εγκατεστημένοι σε τοπικούς κόμβους αναζητούν ενδείξεις ασυνήθιστης δραστηριότητας. Έτσι εάν ένα μηχάνημα που συνήθως πραγματοποιεί λίγες συνδέσεις ξαφνικά τις αυξήσει κατακόρυφα τότε το σύστημα θα υποψιαστεί ότι βρίσκεται σε εξέλιξη μία επίθεση. Με αυτά μόνο τα στοιχεία η πιθανότητα λανθασμένης ειδοποίησης είναι αρκετά υψηλή οδηγώντας σε ενέργειες όπως την απομόνωση της συσκευής από το υπόλοιπο δίκτυο. Παράλληλα όμως εάν οι ενδείξεις είναι όντως αληθείς και το σύστημα τις αγνοήσει ή περιμένει περαιτέρω εξελίξεις τότε το δίκτυο θα εκτεθεί. Σε ένα προσαρμοστικό και συνεργατικό σύστημα, ο τοπικός κόμβος κάνει χρήση ενός πρωτοκόλλου peer to peer για να επικοινωνήσει με τους άλλους κόμβους και να τους ενημερώσει για τις υποψίες του ότι το δίκτυο δέχεται επίθεση. Όταν τα μηνύματα αυτά περάσουν ένα συγκεκριμένο όριο τότε λαμβάνονται μέτρα και σημαίνει ο κεντρικός συναγερμός ασφαλείας.
Κατά τα πρώτα στάδια της επίθεσης δεν λαμβάνονται μέτρα διότι ο κίνδυνος λανθασμένης ένδειξης είναι υψηλός. Εάν η επίθεση συνεχίσει τότε οι ενδείξεις ύπαρξής της γίνονται ισχυρότερες και ο κίνδυνος λάθους μειώνεται. Με αυτόν τον τρόπο όμως έχει χαθεί πολύτιμος χρόνος. Στην περίπτωση αυτή, τα υβριδικά συστήματα περιλαμβάνουν πολλούς συνεργαζόμενους τοπικούς αισθητήρες και ο καθένας από αυτούς υποπτεύεται ότι λαμβάνει χώρα μία επίθεση. Επειδή πολλά συστήματα βλέπουν τις ίδιες ενδείξεις μπορεί να δοθεί μήνυμα συναγερμού με μειωμένη πιθανότητα λάθους. Έτσι αντί να υπάρχει μεγάλη αναμονή για να βεβαιωθεί το σύστημα ότι όντως το σύστημα δέχεται επίθεση, η ύπαρξη μεγάλου αριθμού αισθητήρων μπορεί σε σύντομο χρονικό διάστημα να ανιχνεύσει επιτυχώς μία επίθεση. (Stallings, Brown, Bauer & Bhattacharjee, 2015)

2.8 Honeypots

Ένα άλλο στοιχείο της τεχνολογία ανίχνευσης εισβολών είναι το honeypot. Τα honeypots είναι δολώματα που έχουν σχεδιαστεί για να προσελκύσουν έναν πιθανό εισβολέα και να το απομακρύνουν από τα κρίσιμα συστήματα. Σκοπός τους είναι να συλλέξουν πληροφορίες σχετικά με τη δραστηριότητα του επιτιθέμενου και να τον ενθαρρύνουν να παραμείνει για αρκετό καιρό ώστε οι διαχειριστές να ανταποκριθούν στην απειλή. Αυτά τα συστήματα είναι γεμάτα από ψευδείς πληροφορίες που έχουν σχεδιαστεί ώστε να φαίνονται πολύτιμες, στις οποίες όμως ένας νόμιμος χρήστης του συστήματος δεν θα είχε πρόσβαση. Συνεπώς, οποιαδήποτε πρόσβαση στο honeypot είναι ύποπτη. Το σύστημα διαθέτει ευαίσθητους ανιχνευτές και καταγραφείς συμβάντων που εντοπίζουν αυτές τις προσβάσεις και συλλέγουν πληροφορίες σχετικά με τις δραστηριότητες του επιτιθέμενου. Επειδή οποιαδήποτε επίθεση εναντίον του honeypot φαίνεται να είναι επιτυχής, οι διαχειριστές έχουν χρόνο να κινητοποιηθούν, να καταγράψουν και να παρακολουθήσουν τον εισβολέα χωρίς να εκθέσουν ποτέ τα παραγωγικά συστήματα του οργανισμού.
Το honeypot είναι ένας πόρος που δεν έχει αξία στην παραγωγική διαδικασία ενός οργανισμού. Δεν υπάρχει κανένας λόγος για οποιονδήποτε εκτός του δικτύου να αλληλεπιδράσει μαζί του. Επομένως, κάθε προσπάθεια επικοινωνίας με το σύστημα είναι πιθανότατα μια έρευνα, σάρωση ή επίθεση. Αντίθετα, εάν ένα honeypot ξεκινά εξερχόμενη επικοινωνία, το σύστημα πιθανότατα έχει τεθεί σε κίνδυνο.

Τα Honeypots ταξινομούνται συνήθως σε δύο κατηγορίες, χαμηλής ή υψηλής αλληλεπίδρασης. Τα Honeypots χαμηλής αλληλεπίδρασης αποτελούνται από ένα πακέτο λογισμικού που μιμείται συγκεκριμένες υπηρεσίες ή συστήματα πληροφορικής αρκετά καλά ώστε να παρέχει μια ρεαλιστική αρχική αλληλεπίδραση, αλλά δεν τα προσομοιώνει πλήρως. Από την άλλη πλευρά τα Honeypots υψηλής αλληλεπίδρασης είναι ένα πραγματικό σύστημα, με πλήρες λειτουργικό σύστημα, υπηρεσίες και εφαρμογές, τα οποία είναι εξοπλισμένα και αναπτύσσονται όπου μπορούν να έχουν πρόσβαση οι εισβολείς.
Ένα honeypot υψηλής αλληλεπίδρασης αποτελεί έναν αληθοφανή στόχο που μπορεί να απασχολήσει έναν εισβολέα για μεγάλο χρονικό διάστημα. Ωστόσο, απαιτεί σημαντικά περισσότερους πόρους και, εάν παραβιαστεί τότε μπορεί να χρησιμοποιηθεί σε επιθέσεις εναντίον άλλων συστημάτων. Από τη άλλη ένα honeypot χαμηλής αλληλεπίδρασης παρέχει έναν λιγότερο αληθοφανή στόχο, ικανό όμως να εντοπίσει τους εισβολείς. Συνήθως χρησιμοποιείται ως συστατικό ενός hybrid IDS για την προειδοποίηση για επικείμενη επίθεση.
Οι αρχικές εκδόσεις περιλάμβαναν έναν υπολογιστή honeypot με διευθύνσεις IP σχεδιασμένες να προσελκύουν χάκερ. Η πρόσφατη έρευνα επικεντρώθηκε στη δημιουργία ολόκληρων δικτύων honeypot που μιμούνται μια επιχείρηση, πιθανώς με πραγματική ή προσομοιωμένη κίνηση και δεδομένα. Όταν οι χάκερ βρίσκονται μέσα στο δίκτυο, οι διαχειριστές μπορούν να παρατηρήσουν τη συμπεριφορά τους λεπτομερώς και να σχεδιάσουν τρόπους άμυνας. (Stallings, Brown, Bauer & Bhattacharjee, 2015)

2.9 Intrusion Prevention Systems – Συστήματα πρόληψης εισβολών (IPS)

Μια επιπλέον προσθήκη στη συλλογή των εργαλείων ασφάλειας πληροφοριακών συστημάτων είναι τα Συστήματα πρόληψης εισβολών (IDS). Πρόκειται για μια επέκταση των IDS που περιλαμβάνουν επιπρόσθετα τη δυνατότητα προσπάθειας αποκλεισμού ή αποτροπής της εντοπισμένης κακόβουλης δραστηριότητας. Όπως και στην περίπτωση των IDS, τα IPS ταξινομούνται στις ίδιες κατηγορίες, τα host based, τα network based και τέλος τα υβριδικά. Ομοίως, ο τρόπος ανίχνευσης των εισβολών μπορεί να βασίζεται είτε στον εντοπισμό ανωμαλιών στην κίνηση ώστε να προσδιοριστεί εάν η συμπεριφορά ανήκει σε κακόβουλο χρήστη ή όχι είτε στην ευρετική ανίχνευση για την αναγνώριση γνωστής κακόβουλης συμπεριφοράς.
Μόλις ένα IDS εντοπίσει κακόβουλη δραστηριότητα, μπορεί να ανταποκριθεί είτε τροποποιώντας ή αποκλείοντας πακέτα του δικτύου μέσα στην περίμετρο ή σε έναν κεντρικό υπολογιστή είτε τροποποιώντας ή αποκλείοντας τις κλήσεις συστήματος από προγράμματα που εκτελούνται σε έναν κεντρικό υπολογιστή. Έτσι, ένα network based IPS μπορεί να αποκλείσει την κυκλοφορία, όπως κάνει το τείχος προστασίας, χρησιμοποιώντας όμως ειδικούς αλγόριθμους για να μπορεί να προσδιορίσει πότε θα το κάνει.

2.9.1 Host-Based IPS

Ένα host based IPS (HIPS) μπορεί να χρησιμοποιήσει τεχνική ανίχνευσης υπογραφής και την τεχνική εντοπισμού ανωμαλιών για να αναγνωρίσει μία επίθεση. Στην πρώτη περίπτωση, το σύστημα εστιάζει στο περιεχόμενο της κίνησης στο επίπεδο εφαρμογών ή στις ακολουθίες κλήσεων συστήματος, αναζητώντας μοτίβα που έχουν αναγνωριστεί ως κακόβουλα. Σε περίπτωση ανίχνευσης ανωμαλιών, το IPS αναζητά μοτίβα συμπεριφοράς που υποδεικνύουν κακόβουλο λογισμικό. Επιθέσεις που αντιμετωπίζει ένα HIP είναι οι

απόπειρες τροποποίησης των πόρων του συστήματος (Rootkits, Trojan horses, και backdoors), αλλαγής δικαιωμάτων χρηστών, buffer – overflow, πρόσβασης στη λίστα διευθύνσεων email (worms).
Αυτού του είδους οι επιθέσεις παράγουν κίνηση η οποία αναλύεται και τα συστήματα μπορούν να προσαρμοστούν σε αυτές. Ορισμένα HIPS έχουν παραμετροποιηθεί ώστε να προστατεύουν συγκεκριμένα στοιχεία ενός πληροφοριακού συστήματος ανιχνεύοντας συγκεκριμένα είδη επιθέσεων που συχνά τα πλήττουν.
Εκτός από τις δύο προαναφερθείσες τεχνικές, τα HIPS κάνουν χρήση και της τεχνικής sandbox. Η συγκεκριμένη τεχνική είναι προσαρμοσμένη στα java applets και στις γλώσσες scripting γενικότερα. Το HIPS περιορίζει τον κώδικα σε μία απομονωμένη περιοχή (sandbox) και τον εκτελεί παρατηρώντας τη συμπεριφορά του. Σε περίπτωση που ο κώδικας παραβιάσει τους προκαθορισμένους κανόνες ή ταιριάξει με τις προκαθορισμένες υπογραφές συμπεριφοράς τότε διακόπτεται και αποτρέπεται η εκτέλεσή του στο κυρίως περιβάλλον του συστήματος.
Οι σταθεροί και φορητοί Η/Υ των επιχειρήσεων αποτελούν σε μεγαλύτερο βαθμό στόχοι επιθέσεων συγκριτικά με τις δικτυακές συσκευές. (Robb, 2006) Στη συγκεκριμένη κατηγορία, τα HIPS προσφέρουν μία ολοκληρωμένη προστασία τελικού σημείου συνδυάζονται πληθώρα εργαλείων που λειτουργούν συντονισμένα, πιο αποτελεσματικά και η διαχείρισή τους είναι ευκολότερη.

2.9.2 Network-Based IPS (NIPS)

Ένα NIPS είναι στην ουσία ένα IPS που έχει τη δυνατότητα να τροποποιεί ή να απορρίπτει πακέτα και να τερματίζει συνδέσεις TCP. Κάνει και αυτό χρήση των τεχνολογιών ανίχνευσης ανωμαλιών στην κίνηση του δικτύου και ανίχνευσης υπογραφών.
Μία από τις τεχνικές που εκμεταλλεύονται τα NIPS και δεν εφαρμόζονται από τα firewalls είναι η προστασία της ροής των δεδομένων. Η τεχνική αυτή απαιτεί την επανασυναρμολόγηση του ωφέλιμου φορτίου του επιπέδου εφαρμογών που περιέχεται στα πακέτα. Στη συνέχεια εφαρμόζονται φίλτρα σε όλη τη ροή κάθε φορά που καταφθάνει ένα νέο πακέτο της. Σε περίπτωση που η ροή κριθεί ότι είναι κακόβουλη, τα πιο πρόσφατα πακέτα καθώς και αυτά που ακολουθούν απορρίπτονται. Οι γενικές μέθοδοι που χρησιμοποιούνται από μια συσκευή NIPS για τον εντοπισμό κακόβουλων πακέτων περιλαμβάνουν την αντιστοίχιση μοτίβου (σαρώνει τα εισερχόμενα πακέτα για συγκεκριμένες ακολουθίες bytes και ελέγχει μέσα από μία βάση γνωστών επιθέσεων), την αντιστοίχιση κατάστασης (σαρώνει για υπογραφές επίθεσης στη ροή κυκλοφορίας και όχι στα μεμονωμένα πακέτα), την ανωμαλία πρωτοκόλλου (αναζητά αποκλίσεις από τα πρότυπα RFC), την ανωμαλία της κίνησης (ελέγχει για τυχών παρουσία ασυνήθιστης κίνησης ή κάποιας νέας υπηρεσίας) και την στατιστική ανωμαλία (αναπτύσσει βασικές γραμμές της κανονικής κίνησης και ειδοποιεί σε περίπτωση απόκλισης).

2.9.3 Distributed or Hybrid IPS - Κατανεμημένα ή Υβριδικά Συστήματα Πρόληψης Εισβολών (Hybrid IPS)

Η τελευταία κατηγορία των IPS είναι τα κατανεμημένα. Βασίζονται στη συλλογή δεδομένων από ένα μεγάλο αριθμό αισθητήρων οι οποίοι μεταφέρουν την πληροφορία σε ένα κεντρικό σύστημα ανάλυσης. Το σύστημα αυτό ικανό να συσχετίσει και να αναλύσει τα δεδομένα αυτά και στη συνέχεια να παραχθούν υπογραφές και πρότυπα συμπεριφοράς ώστε στη συνέχεια όλα τα συντονισμένα συστήματα να ενεργοποιηθούν

και να είναι σε θέση να αντιμετωπίσουν την κακόβουλη συμπεριφορά. (Stallings, Brown, Bauer & Bhattacharjee, 2015)

2.10 Κρυπτογραφία

Η λέξη κρυπτογραφία είναι σύνθετη και προέρχεται από δύο ελληνικές λέξεις που αποδίδουν την έννοια «μυστική γραφή». Η κρυπτογραφία είναι η τέχνη και η επιστήμη της απόκρυψης του νοήματος. Η κρυπτανάλυση είναι το σπάσιμο του κώδικα. Το βασικό συστατικό της κρυπτογραφίας είναι το κρυπτοσύστημα.
Ο πρωταρχικός στόχος της κρυπτογραφίας είναι η διατήρηση της μυστικότητας των κρυπτογραφημένων πληροφοριών αντιμετωπίζοντας έτσι την απειλή αποκάλυψης. Η κρυπτογραφία μπορεί επίσης να χρησιμοποιηθεί για την παροχή της ακεραιότητας τόσο των δεδομένων όσο και της προέλευσης τους, αντισταθμίζοντας έτσι τις απειλές της τροποποίησης και της μεταμφίεσης. Μπορεί επίσης να παρέχει μη απόρριψη, εξουδετερώνοντας την απειλή της άρνησης προέλευσης. Έτσι, είναι ένας εξαιρετικά ισχυρός μηχανισμός στον οποίο βασίζονται σε μεγάλο βαθμό οι τεχνικές ασφάλειας των υπολογιστικών συστημάτων.
Τα κρυπτοσυστήματα βασίζονται σε δύο τύπους μετασχηματισμών (Shannon,1948). Ο πρώτος τύπος ονομάζεται onfusion (έγχυση) και αντικαθιστά τμήματα του αρχικού μηνύματος με άλλα δεδομένα ώστε να αποκρύψει το αρχικό περιεχόμενο. Ο δεύτερος τύπος ονομάζεται diffusion (διάχυση) και βασίζεται στη διάχυση του αρχικού περιεχομένου σε όλη την έκταση του μηνύματος. Με αυτόν τον τρόπο αυξάνεται η δυσκολία αποκάλυψης του αρχικού κειμένου. (Bishop, 2002)
Η κρυπτογραφία είναι η τέχνη του μετασχηματισμού ενός αναγνώσιμου μηνύματος σε μια μορφή που είναι αναγνώσιμη μόνο από εξουσιοδοτημένους χρήστες:
• Μη κρυπτογραφημένες πληροφορίες - Πληροφορίες σε κατανοητή μορφή. Οι μη κρυπτογραφημένες πληροφορίες είναι απλό κείμενο, που ονομάζεται και cleartext.
• Κρυπτογραφημένες πληροφορίες - Πληροφορίες σε μη κατανοητή μορφή. Οι κρυπτογραφημένες πληροφορίες ονομάζονται ciphertext. Η κρυπτογράφηση είναι η διαδικασία μετατροπής του απλού κειμένου σε κρυπτοκείμενο.
Η αποκρυπτογράφηση είναι η διαδικασία μετατροπής του κρυπτογραφημένου κειμένου (ciphertext) σε απλό. Η κρυπτογράφηση χρησιμοποιεί γνωστές μαθηματικές διαδικασίες για την εκτέλεση των λειτουργιών της. Μια τέτοια διαδικασία είναι γνωστή ως αλγόριθμος. Ένας αλγόριθμος είναι μια επαναλαμβανόμενη διαδικασία που παράγει το ίδιο αποτέλεσμα όταν λαμβάνει την ίδια είσοδο. Το cipher είναι ένας αλγόριθμος για την κρυπτογράφηση ή την αποκρυπτογράφηση πληροφοριών. Αυτή η επαναληψιμότητα είναι σημαντική ώστε να επιβεβαιωθεί ότι οι πληροφορίες που κρυπτογραφήθηκαν μπορούν να αποκρυπτογραφηθούν.
Ο αλγόριθμος που χρησιμοποιείται για την κρυπτογράφηση δεν είναι πάντα απαραίτητο να χρησιμοποιηθεί και κατά την αποκρυπτογράφηση. Επιπλέον, ορισμένοι αλγόριθμοι κρυπτογράφησης δεν έχουν αντίστοιχους αποκρυπτογράφησης. Αυτοί ονομάζονται μονής κατεύθυνσης ή συναρτήσεις κατακερματισμού (hashing functions). Η έξοδος ενός τέτοιου αλγόριθμου ονομάζεται κατακερματισμός (hash). Οι συναρτήσεις κατακερματισμού χρησιμεύουν στο να προστατεύουν τα δεδομένα από μη εξουσιοδοτημένες αλλαγές.
Οι πιο διαδεδομένοι αλγόριθμοι κρυπτογράφησης (ciphers) απαιτούν ως είσοδο το αρχικό κείμενο σε μορφή plain text και ένα κλειδί. Ο αλγόριθμος στη συνέχεια χρησιμοποιεί το κλειδί για να διαφοροποιήσει την έξοδο έτσι ώστε οι πληροφορίες που περιέχονται στο κείμενο να προστατευτούν από οποιονδήποτε άλλο χρησιμοποιεί τον ίδιο αλγόριθμο.

Αλλάζοντας το κλειδί αλλάζει και η έξοδος ακόμα και αν το αρχικό κείμενο παραμείνει το ίδιο.

Οι αλγόριθμοι κρυπτογράφησης εμπίπτουν σε δύο γενικές κατηγορίες. Η πρώτη περιέχει αυτούς που κάνουν χρήση ιδιωτικού συμμετρικού κλειδιού και η δεύτερη αυτούς που χρησιμοποιούν ασύμμετρα δημόσια κλειδιά.

Γενικά δεν υπάρχει κάποιος αλγόριθμος που θα μπορούσε να χαρακτηριστεί τέλειος. Δοθέντος χρόνου και μέσων ένας επιτιθέμενος μπορεί να αποκρυπτογραφήσει οποιοδήποτε μήνυμα. Το θέμα είναι να καταστεί αυτή η διαδικασία ασύμφορη. Ο αριθμός των πιθανών κλειδιών ονομάζεται keyspace. Εφόσον ο επιτιθέμενος δεν διαθέτει καμία πληροφορία για το κλειδί, θα ξεκινήσει μια επίθεση brute force δοκιμάζοντας όλα τα πιθανά κλειδιά. Εφόσον ο αλγόριθμος δεν έχει μαθηματικές αδυναμίες ένα μεγάλο keyspace σημαίνει ότι ο επιτιθέμενος θα αφιερώσει περισσότερους πόρους και χρόνο αυξάνοντας το κόστος της διαδικασίας.

Υπάρχουν αλγόριθμοι κρυπτογράφησης ανοιχτού και κλειστού κώδικα. Οι ειδικοί μελετούν τους πρώτους για αδυναμίες και ανακαλύπτουν λάθη τα οποία μπορούν να εκθέσουν το αρχικό μήνυμα. Ο αλγόριθμος DES (Data Encryption Standard) ο οποίος δημιουργήθηκε το 1977 είναι ο πιο μελετημένος.

Στα σύγχρονα Πληροφοριακά Συστήματα η κρυπτογράφηση βρίσκει εφαρμογή τόσο στα δεδομένα που διακινούνται στο δίκτυο όσο και στα αποθηκευμένα. Διαφορετικές προσεγγίσεις ακολουθούνται για τις περιπτώσεις αυτές. Η ασφάλεια των μεταφερόμενων δεδομένων ονομάζεται ασφάλεια επικοινωνιών.

Στην ασφάλεια επικοινωνιών υπάρχουν δύο κύριες προσεγγίσεις. Σύμφωνα με την πρώτη λογισμικό αναλαμβάνει να κρυπτογραφήσει το μήνυμα πριν αυτό αποσταλεί στο δίκτυο. Η δεύτερη προσέγγιση αφήνει τις λειτουργίες των επικοινωνιών να διαχειριστούν την κρυπτογράφηση και την αποκρυπτογράφηση. Πιο συγκεκριμένα το λογισμικό των επικοινωνιών εκτελεί τη διαδικασία κατά τη διάρκεια της μετάδοσης ή της λήψης. Η δεύτερη προσέγγιση ονομάζεται κρυπτογράφηση σύνδεσης ή μεταφοράς διότι λαμβάνει χώρα στο επίπεδο του δικτύου. Κοινά πρωτόκολλα είναι το Secure Sockets Layer (SSL) και το Transport Layer Security (TLS) τα οποία χρησιμοποιούνται για τη δημιουργία ασφαλών συνδέσεων μεταξύ των Web Servers και των πλοηγών. Για τη σύνδεση σε απομακρυσμένους διακομιστές γίνεται χρήση του Secure Shell (SSH).

Η κρυπτογράφηση ικανοποιεί τις απαιτήσεις του τρίπτυχου CIA. Η εμπιστευτικότητα απαιτεί οι πληροφορίες να παραμένουν μυστικές στους μη εξουσιοδοτημένους χρήστες. Η κρυπτογράφηση μετασχηματίζει την πληροφορία σε μη κατανοητή μορφή για όποιον δεν έχει τον αλγόριθμο και το κλειδί να την αποκρυπτογραφήσει. Έτσι μόνο οι νόμιμοι χρήστες μπορούν να έχουν πρόσβαση. Η ακεραιότητα διασφαλίζει ότι κανείς (ούτε ο αποστολέας) μπορεί να αλλάξει το μήνυμα αφού αυτό αποσταλεί. Έτσι στην περίπτωση που ένα μήνυμα δεν έχει κρυπτογραφηθεί σωστά αυτό σημαίνει ότι έχει πιθανώς αλλαχθεί. Επιπρόσθετα υπάρχουν το hashs (συναρτήσεις κατακερματισμού) και το checksum (αθροίσματα ελέγχου). Το δεύτερο είναι ένας υπολογισμός των πληροφοριών που αποδίδει ένα αποτέλεσμα το οποίο είναι συνήθως πολύ μικρότερο από το αρχικό μήνυμα. Τέλος η αυθεντικότητα επιβεβαιώνει την ταυτότητα μιας οντότητας και η κρυπτογραφία αποτελεί ένα μέσο ταυτοποίησης οντοτήτων. Αυτό συμβαίνει είτε με τη χρήση συμμετρικού κλειδιού είτε με τη χρήση των μη συμμετρικών. Η κρυπτογραφία αποτελεί τον κεντρικό πυρήνα ενός πολυστρωματικού συστήματος ασφαλείας που καλύπτει σημαντικές εταιρικές λειτουργίες όπως το ηλεκτρονικό εμπόριο η απομακρυσμένη χρήση υπηρεσιών κ.α. (Kim & Solomon, 2018)

2.11 Network Monitors and Analyzers

Για τη διασφάλιση ότι τα μέτρα ασφαλείας που έχουν παρθεί παραμένουν αποτελεσματικά, οι διαχειριστές των Πληροφοριακών Συστημάτων παρακολουθούν το λογισμικό και τις συσκευές του δικτύου. Ταυτόχρονα αναλύουν την κυκλοφορία του που μεταφέρεται στο δίκτυο. Οι σαρωτές ευπαθειών (vulnerability scanners) σαρώνουν το Πληροφοριακό Σύστημα ενός οργανισμού με σκοπό την ανακάλυψη αδυναμιών. Έτσι μπορούν να ανακαλύψουν θύρες υπηρεσιών οι οποίες είναι άσκοπα ανοιχτές, λανθασμένες ρυθμίσεις στο λογισμικό, υπηρεσίες που δυσλειτουργούν προκαλώντας παράλληλα κινδύνους ασφαλείας κα.

Κεφάλαιο 3 – ΕΡΕΥΝΗΤΙΚΟ ΜΕΡΟΣ

3.1 Εισαγωγή

Ο πρωταρχικός σκοπός για την ασφάλεια ενός πληροφοριακού συστήματος είναι ο εντοπισμός και η αναφορά μίας εισβολής. Ανιχνεύοντας τα πρώτα σημάδια της, είναι δυνατόν να περιοριστεί η επίθεση και να αποτραπεί ή τουλάχιστον να μετριαστεί σε μεγάλο βαθμό η ζημιά και η απώλεια των πληροφοριών. Η διαδικασία της ειδοποίησης μιας εν εξελίξη επίθεση είναι κρίσιμη.
Για να μπορέσουν οι διαχειριστές του ΠΣ να προετοιμαστούν για μία επερχόμενη επίθεση, είναι πολύ σημαντικό να εντοπιστούν οι προπαρασκευαστικές κινήσεις των επιτιθέμενων. Οι περισσότερες επιθέσεις ξεκινούν με μία οργανωμένη και διεξοδική διερεύνηση του περιβάλλοντος δικτύου του οργανισμού και της άμυνας του. Αυτή η διαδικασία ονομάζεται αρχική ανίχνευση και επιτυγχάνεται μέσω δύο γενικών δραστηριοτήτων. Η πρώτη συλλέγει πληροφορίες σχετικά με τον οργανισμό, τις δραστηριότητες και τα στοιχεία του δικτύου ενώ η δεύτερη αναφέρεται στην ανίχνευση των τοπικών δικτυακών ρυθμίσεων, τα ενεργά συστήματα και των υπηρεσιών που προσφέρονται από τους κεντρικούς υπολογιστές. Ένα ΠΣ το οποίο είναι σε θέση να ανιχνεύσει τις προπαρασκευαστικές αυτές κινήσεις επιτρέπει στους διαχειριστές του να προετοιμαστούν για μία πιθανή επίθεση ή να ελαχιστοποιήσουν τις ενδεχόμενες απώλειες από αυτήν.
Είναι σημαντικό το ΠΣ του οργανισμού να προστατεύεται από γνωστές ευπάθειες και να είναι σε θέση να ανταποκρίνεται σε ένα ταχέως μεταβαλλόμενο περιβάλλον απειλών. Πολλοί παράγοντες μπορούν να καθυστερήσουν ή να υπονομεύσουν την ικανότητα ενός οργανισμού να προστατεύσει τα συστήματα του από επιθέσεις και τις επακόλουθες απώλειες. Έτσι παρόλο που οι γνωστές τεχνολογίες ασφάλειας πληροφοριών, όπως τα εργαλεία σάρωσης, επιτρέπουν στους διαχειριστές ασφάλειας να αξιολογήσουν την επάρκεια των συστημάτων τους, ενδέχεται να αποτύχουν να εντοπίσουν και να διορθώσουν μία γνωστή αδυναμία ή ακόμα και ο έλεγχος να λαμβάνει χώρα σπάνια. Επιπλέον ακόμη και όταν εντοπίζεται εγκαίρως μία ευπάθεια δεν μπορεί πάντα να διορθωθεί γρήγορα. Αυτό συμβαίνει διότι απαιτείται από το διαχειριστή να εγκαταστήσει ενημερώσεις και αναβαθμίσεις γεγονός που εξαρτάται από το φόρτο εργασίας του.
Πολλές φορές συμβαίνει οι ευπάθειες να είναι γνωστές σε ομάδες κακόβουλων χρηστών ενώ παράλληλα οι διαχειριστές να τις αγνοούν. Ο αριθμός και η πολυπλοκότητα των αναφερόμενων αδυναμιών συνεχίζουν να αυξάνονται οπότε εκ των πραγμάτων τα συστήματα είναι εξαιρετικά δύσκολο να είναι πάντα ενημερωμένα. Για το λόγο αυτό οι οργανισμοί αναθέτουν σε προγραμματιστές τον εντοπισμό των προβλημάτων και την ενημέρωση των συστημάτων. Παρόλα αυτά υπάρχει μία αναπόφευκτη καθυστέρηση κατά την διαδικασία του εντοπισμού της ευπάθειας και της ενημέρωσης του συστήματος. Κατά τον ίδιο τρόπο σημαντικές είναι οι καθυστερήσεις που παρατηρούνται κατά την ανίχνευση ενός ιού ή ενός worm και της διανομής της υπογραφής που επιτρέπει στις αντίστοιχες εφαρμογές ασφαλείας να εντοπίζουν και να περιορίζουν την απειλή.
Τέλος η κατάσταση περιπλέκεται περισσότερο όταν απαραίτητες υπηρεσίες για τη λειτουργία του ΠΣ παρουσιάζουν ευπάθειες αλλά δεν μπορούν να απενεργοποιηθούν ή να προστατευθούν επαρκώς διότι η παύση τους θα προκαλέσει πλήγμα στην εύρυθμη λειτουργία του οργανισμού. (Whitman & Mattord, 2014)

3.1.1 Virtual Box

Η εικονική μηχανή Virtual Box της Oracle είναι ένας υπερεπόπτης ανοιχτού κώδικα που αναπτύχθηκε για συστήματα x86 αρχιτεκτονικής. Το λογισμικό μπορεί να εγκατασταθεί σε πληθώρα λειτουργικών συστημάτων όπως τα Windows, macOS, Linux, Solaris, OpenSolaris κα. Υποστηρίζει τη δημιουργία και τη διαχείριση εικονικών μηχανών οι οποίες τρέχουν Windows, Linux, BSD, Solaris κα. Οι χρήστες του Virtual Box μπορούν να φορτώσουν πολλαπλά λειτουργικά συστήματα (guest) στο μηχάνημα που εκτελεί την εικονική μηχανή(host). Κάθε guest ΛΣ μπορεί να εκκινηθεί, να παυθεί προσωρινά ή να σταματήσει τελείως ανεξάρτητα εντός του πλαισίου της δικής του εικονικής μηχανής. Ο χρήστης έχει τη δυνατότητα να τις παραμετροποιήσει κάθε μία ξεχωριστά κάνοντας χρήση επιλογών που αφορούν τόσο το λογισμικό όσο και το υλικό. Το ΛΣ του host καθώς και οι εφαρμογές του μπορούν να επικοινωνήσουν με τα ΛΣ και τις εφαρμογές που τρέχουν στους guests μέσω ενός συνόλου μηχανισμών που μεταξύ άλλων περιλαμβάνουν κοινό πρόχειρο και εικονική δικτυακή εγκατάσταση. Τέλος οι εικονικές μηχανές μπορούν να επικοινωνήσουν απευθείας μεταξύ τους εφόσον παραμετροποιηθούν κατάλληλα. (VirtualBox.org/manual, 2013)

3.1.2 Linux Ubuntu

Το Ubuntu είναι μία διανομή του Linux βασισμένη στο Debian και αποτελείτε κυρίως από δωρεάν και ελεύθερο λογισμικό. Επίσημα εκδίδονται τρεις εκδόσεις: Desktop, Server και Core (Για συσκευές IoT) οι οποίες μπορούν να εγκατασταθούν είτε αυτόνομα σε έναν ηλεκτρονικό υπολογιστή είτε σε μία εικονική μηχανή. Η προεπιλεγμένη επιφάνεια εργασίας είναι το GNOME.

Το Ubuntu κυκλοφορεί νέα έκδοση κάθε έξι μήνες ενώ οι εκδόσεις που συνοδεύονται από μακρόχρονη υποστήριξη παρέχονται κάθε δύο χρόνια.

Τα πακέτα του Ubuntu βασίζονται σε αυτά της unstable branch του Debian και συγχρονίζονται μεταξύ τους κάθε έξι μήνες. Και οι δύο διανομές κάνουν χρήση των συστημάτων διαχείρισης πακέτων του Debian. Παρόλα αυτά δεν είναι απαραίτητο να είναι συμβατά μεταξύ τους πάντα.

Η προεπιλεγμένη εγκατάσταση του Linux Ubuntu περιλαμβάνει ένα ευρύ φάσμα λογισμικού όπως το Libre Office (Σουίτα Γραφείου), το Firefox, το Thunderbird, και το Transmission (λογισμικό BitTorrent) καθώς επίσης και απλά παιχνίδια. Επιπλέον πακέτα λογισμικού είναι προσβάσιμα μέσω της εφαρμογής Ubuntu Software καθώς επίσης των εργαλείων διαχείρισης πακέτων APT.

Το Linux Ubuntu στοχεύει να είναι ασφαλές χρησιμοποιώντας τις προεπιλεγμένες ρυθμίσεις. Τα προγράμματα χρήστη τρέχουν με περιορισμένα δικαιώματα και δεν μπορούν να προκαλέσουν αλλαγές στο λειτουργικό σύστημα ή στα αρχεία άλλων χρηστών. Για να αυξηθεί το επίπεδο ασφάλειας το εργαλείο sudo χρησιμοποιείται για να εκχωρήσει στο χρήστη προνόμια προσωρινά ώστε να εκτελέσει εργασίες διαχειριστή. Έτσι επιτρέπει τον λογαριασμό root να παραμείνει κλειδωμένος και το σύστημα να προστατευτεί από άπειρους χρήστες οι οποίοι είναι δυνατόν ακούσια να εκτελέσουν καταστροφικές αλλαγές ή να δημιουργήσουν κενά ασφαλείας.

Οι περισσότερες δικτυακές θύρες είναι κλειστές από προεπιλογή ώστε να αποφευχθούν πιθανές εισβολές. Το ενσωματωμένο τοίχος προστασίας επιτρέπει στους τελικούς χρήστες που εγκαθιστούν διακομιστές δικτύου να ελέγχουν την πρόσβαση.

3.1.3 Uncomplicated Firewall (UFW)

Ο πυρήνας του Linux Ubuntu παρέχει ένα σύστημα φιλτραρίσματος πακέτων που ονομάζεται netfilter ενώ η διεπαφή που το χειρίζεται είναι η σουίτα εντολών iptables. Η συγκεκριμένη παρέχει μία πλήρη λύση τείχους προστασίας που είναι παραμετροποιήσιμη και ευέλικτη. Το UFW είναι ένα frontend για τα iptables εξειδικευμένο για χρήση στα τείχη προστασίας που εγκαθίστανται σε κόμβους του δικτύου και παρέχει το πλαίσιο διαχείρισης του netfilter. Επίσης προσφέρει μία διεπαφή γραμμής εντολών για το χειρισμό του firewall. Στόχος του είναι η απλοποίηση της διαδικασίας παραμετροποίησης ώστε να γίνει προσιτή για τους χρήστες.

3.2 Snort

Το snort είναι ένα IDS ανοιχτού κώδικα εξαιρετικά παραμετροποιήσιμο το οποίο μπορεί να δουλέψει είτε ως Network Based IPS είτε ως Host Based IPS. Το snort έχει τα ακόλουθα χαρακτηριστικά :
Εύκολη εγκατάσταση στους περισσότερους κόμβους ενός δικτύου (κεντρικός υπολογιστής, διακομιστές, δρομολογητής).
Χαμηλές απαιτήσεις σε μνήμη και επεξεργαστική ισχύ προσφέροντας αποτελεσματική λειτουργία.
Διαμορφώνεται εύκολα από τους διαχειριστές του ΠΣ οι οποίοι μπορούν να εφαρμόσουν μία συγκεκριμένη λύση ασφαλείας σε σύντομο χρονικό διάστημα.
Το snort μπορεί να πραγματοποιήσει λήψη πακέτων σε πραγματικό χρόνο, ανάλυση πρωτοκόλλου όπως επίσης αναζήτηση και αντιστοίχιση περιεχομένου. Έχει σχεδιαστεί κυρίως για την ανάλυση των πρωτοκόλλων δικτύου TCP, UDP και ICMP και μπορεί να επεκταθεί με τα κατάλληλα πρόσθετα και σε άλλα πρωτόκολλα. Είναι σε θέση να εντοπίζει μία πλειάδα ανιχνεύσεων και επιθέσεων βασισμένο σε ένα σύνολο κανόνων που έχει διαμορφώσει ο διαχειριστής του συστήματος.

3.2.1 Η αρχιτεκτονική του Snort

Η εγκατάσταση του snort αποτελείται από τέσσερα λογικά μέρη:
Αποκωδικοποιητής πακέτων: Επεξεργάζεται κάθε πακέτο αναγνωρίζει και απομονώνει τις κεφαλίδες πρωτοκόλλου στα επίπεδα της σύνδεσης, δικτύου, μεταφοράς και εφαρμογής. Είναι σχεδιασμένος για να είναι αποτελεσματικός και η κύρια εργασία του αφορά τη ρύθμιση δεικτών ώστε οι διάφορες κεφαλίδες πρωτοκόλλου να μπορούν να εξαχθούν εύκολα.
Μηχανή ανίχνευσης: Εκτελεί την εργασία της ανίχνευσης εισβολών. Αυτή η ενότητα αναλύει κάθε πακέτο με βάση ένα σύνολο κανόνων που ορίζονται από τον διαχειριστή ασφαλείας. Στην ουσία κάθε πακέτο ελέγχεται με βάση αυτούς τους κανόνες για να προσδιοριστεί εάν τα χαρακτηριστικά ορίζονται από σε έναν από αυτούς. Ο πρώτος κανόνας που ταιριάζει με το αποκωδικοποιημένο πακέτο ενεργοποιεί τη δράση που καθορίζεται από τον κανόνα. Εάν κανένας κανόνας δεν ταιριάζει με το πακέτο τότε η μηχανή ανίχνευσης το απελευθερώνει.
Καταγραφέας (Logger): Για κάθε πακέτο που ταιριάζει με έναν κανόνα, αυτός καθορίζει ποιες επιλογές καταγραφής και ειδοποίησης πρέπει να ενεργοποιηθούν. Όταν έχει επιλεγεί η καταγραφή, ο Logger αποθηκεύει το πακέτο που ανιχνεύεται σε μορφή κατανοητή για τον άνθρωπο ή σε ποιο συμπαγή δυαδική μορφή σε ένα καθορισμένο αρχείο καταγραφής. Ο διαχειριστής ασφαλείας μπορεί στη συνέχεια να χρησιμοποιήσει το αρχείο καταγραφής για μελλοντική ανάλυση.
Ειδοποίηση (Alerter): Για κάθε πακέτο που εντοπίστηκε, μπορεί να σταλεί μία ειδοποίηση. Η επιλογή της ειδοποίησης στον αντίστοιχο κανόνα καθορίζει ποιες πληροφορίες θα περιληφθούν. Έτσι η ειδοποίηση συμβάντος μπορεί να σταλεί σε ένα αρχείο, σε ένα UNIX socket ή σε μία βάση δεδομένων. Ο Alerter μπορεί να απενεργοποιηθεί κατά την διάρκεια δοκιμών ή μελετών εισβολής.
Το snort χρησιμοποιεί μία απλή και ευέλικτη γλώσσα για να δημιουργήσει τους κανόνες που χρησιμοποιούνται από τη μηχανή ανίχνευσης. Παρόλο που οι κανόνες είναι απλοί και εύκολοι στη σύνταξη, είναι αρκετά ισχυροί και ανιχνεύουν μία μεγάλη ποικιλία εχθρικής

ή ύποπτης δικτυακής κίνησης. Κάθε κανόνας αποτελείται από μία σταθερή κεφαλίδα και καθόλου ή περισσότερες επιλογές. (Stallings, Brown, Bauer & Bhattacharjee, 2015)

3.3 Η χρήση της Python

Η γλώσσα Python είναι μία από τις πιο προσιτές γλώσσες προγραμματισμού που είναι διαθέσιμη διότι έχει απλή και όχι πολύπλοκη σύνταξη και δίνει μεγαλύτερη έμφαση στη φυσική γλώσσα. Λόγω της ευκολίας εκμάθησης και χρήσης ο κώδικας σε Python μπορεί να γραφτεί εύκολα και να εκτελεστεί πιο γρήγορα από άλλες γλώσσες προγραμματισμού. Η Python είναι εύκολη στη χρήση, ισχυρή και ευέλικτη καθιστώντας την μία εξαιρετική επιλογή τόσο για αρχάριους όσο και προχωρημένους. Η αναγνωσιμότητα της Python επιτρέπει στον χρήστη να σκέφτεται σαν προγραμματιστής και να μην χάνει χρόνο με περίπλοκους κανόνες σύνταξης. Η Python παρέχει μία μεγάλη βιβλιοθήκη που περιλαμβάνει τομείς όπως πρωτόκολλα διαδικτύου, λειτουργίες χαρακτήρων, εργαλεία υπηρεσιών Ιστού και διεπαφές λειτουργικού συστήματος. Πολλές προγραμματιστικές εργασίες που χρησιμοποιούνται συχνά έχουν ήδη γραφτεί στη βασική βιβλιοθήκη γεγονός που μειώνει το μέγεθος του κώδικα που πρέπει να αναπτυχθεί. Η Python αποτελεί την επιλογή πολλών διαχειριστών συστημάτων και διαχειριστών ασφαλείας. Έχει εύκολη διαχείριση μνήμης, συναντάται πάρα πολύ συχνά στη διαχείριση συστημάτων και αποτελεί μέρος του γνωστικού μου πεδίου.
Σκοπός του ερευνητικού μέρους του παρόντος πονήματος είναι η δημιουργία ενός γραφικού περιβάλλοντος στο οποίο θα εμφανίζονται συγκεκριμένα Alerts που παράγει το Snort και θα δίνεται η δυνατότητα εκτέλεσης συγκεκριμένων ενεργειών που αφορούν αυτές τις ειδοποιήσεις. Κατά την παρούσα περίοδο όλα τα γραφικά περιβάλλοντα διαχείρισης του Snort ανοιχτού κώδικα έχουν εγκαταλειφθεί και δεν παρέχεται πλέον υποστήριξη.

3.4 Το Πρόβλημα

Το Snort είναι ένα λογισμικό εντοπισμού και αποτροπής εισβολών ανοιχτού κώδικα το οποίο είναι πολύ ευέλικτο και παραμετροποιήσιμο. Σκοπός του είναι να ελέγχει την κίνηση του δικτύου με βάση ένα σύνολο κανόνων ώστε να εντοπίζει την ύποπτη και εν δυνάμει κακόβουλη κίνηση και να παράγει ειδοποιήσεις. Το Snort όμως δεν έχει τη δυνατότητα να σταματά υπηρεσίες ή να απομονώνει μέρη του συστήματος. Μέχρι την έκδοση Snort 2.9.2.x υπήρχε η επιλογή το λογισμικό να κάνει απευθείας εγγραφές των ειδοποιήσεων σε μία βάση δεδομένων MySQL ώστε ο διαχειριστής να μπορεί να εκμεταλλεύεται με τον μέγιστο δυνατό τρόπο τα αποτελέσματα του Output χρησιμοποιώντας τα κατάλληλα εργαλεία.
Από την έκδοση Snort 2.9.3 έπαψε να υποστηρίζεται αυτή η λειτουργία. (snort.org, 2012) Αντ' αυτής ακολουθήθηκε μία διαφορετική προσέγγιση. Τα παραγόμενα Alerts με τη χρήση του λογισμικού Unified 2 εγγράφονταν σε αρχεία Log. Στη συνέχεια το λογισμικό Barnyard 2 διάβαζε τα αρχεία καταγραφής που παρήγαγε το Unified 2 και τα εισήγαγε σε μία βάση δεδομένων MySQL. Το Barnyard 2 όπως και άλλα παρόμοια λογισμικά ανοιχτού κώδικα (ACID, BASE, Snorby) σταμάτησαν πλέον να υποστηρίζονται και να αναπτύσσονται. Έτσι δημιουργήθηκε κενό στην παλέτα εργαλείων ανοικτού κώδικα που προσφέρουν διαχείριση και εργαλειοποίηση των αποτελεσμάτων που παράγει το Snort. Στην ελεύθερη αγορά αναπτύχθηκε το λογισμικό SNOWL.
Το SNOWL είναι ένα γραφικό περιβάλλον για το Snort που σκοπό έχει να κάνει τη διαδικασία ρύθμισης του Snort αυτόματη και πιο κατανοητή. Ταυτόχρονα συντελεί ώστε

η ανάλυση των κινδύνων να καταστεί μία βολική διαδικασία. Με αυτό το τρόπο ο χρήστης αποφεύγει την εκμάθηση πολύπλοκων εντολών ενώ η ανάλυση γίνεται με γραφικό τρόπο. Μεταξύ άλλων το SNOWL προσφέρει γεωγραφικούς χάρτες προέλευσης των επιθέσεων σε πραγματικό χρόνο, διαγράμματα των επιθέσεων, διαγράμματα ομαδοποίησης των τύπων των επιθέσεων, λίστες διευθύνσεων IP από τις οποίες προέρχονται οι επιθέσεις και γραφήματα που παρουσιάζουν τους χρόνους διεξαγωγής των επιθέσεων. Τέλος το λογισμικό δίνει τη δυνατότητα στο διαχειριστή του πληροφοριακού συστήματος να δημιουργήσει φίλτρα αναζήτησης τα οποία είναι βασισμένα σε μια ποικιλία δεικτών και των συνδυασμών τους. Το λογισμικό SNOWL είναι ένα εξελιγμένο εργαλείο στη διάθεση των διαχειριστών και εκμεταλλεύεται τις πιο σύγχρονες τεχνολογίες. Σε αντίθεση με τα λογισμικά που συνόδευαν το Snort έως τώρα το SNOWL δεν είναι ανοιχτού κώδικα και η απόκτηση του απαιτεί την αγορά συνδρομής.

3.5 Η Μεθοδολογία

Στο πλαίσιο του ερευνητικού μέρους της παρούσας διπλωματικής εργασίας ζητήθηκε και ανέπτυξα ένα πρώιμο εργαλείο σε γλώσσα προγραμματισμού Python το οποίο να παρεμβαίνει στο σύστημα και να απενεργοποιεί συγκεκριμένες υπηρεσίες.
Για το σκοπό αυτό με τη χρήση του λογισμικού Virtual Machine VirtualBox της εταιρείας Oracle εγκαταστάθηκε σε μία εικονική μηχανή το λειτουργικό σύστημα Ubuntu 20.04 Desktop amd64. Στη συνέχεια εγκαταστάθηκε το λογισμικό Snort 3.0.3 (build6). Για να γίνει αυτό εφικτό προηγήθηκε η εγκατάσταση των απαραίτητων εργαλείων build καθώς και των dependencies. Στη συνέχεια εγκαταστάθηκε το OpenAppID το οποίο επιτρέπει στο Snort να αναγνωρίζει, να ελέγχει και να παρακολουθεί τις εφαρμογές που κάνουν χρήση του δικτύου. Το λογισμικό αποτελείται από ένα σύνολο packages (υπογραφές) τα οποία ταιριάζουν με συγκεκριμένους τύπους δεδομένων δικτύου που μεταξύ άλλων περιλαμβάνουν εφαρμογές επιπέδου 7.
Για τη δημιουργία του γραφικού περιβάλλοντος (GUI) του εργαλείου χρησιμοποιήθηκε το λογισμικό Qt Designer το οποίο αποτελεί μέρος της σουίτας PyQt έκδοση 5. Η τελευταία έχει αναπτυχθεί από τη βρετανική εταιρεία Riverbank Computing και είναι η πιο διαδεδομένη εργαλειοθήκη παραγωγής GUI. Διανέμεται δωρεάν μέσω της GNU General Public License και είναι διαθέσιμη για τις πλατφόρμες MS Windows, Linux και MacOS. Στην περίπτωση της Python λειτουργεί ως plugin. Για την ανάπτυξη του κύριου μέρους του κώδικα χρησιμοποιήθηκε το IDE PyCharm edu (δωρεάν έκδοση ανοιχτού κώδικα για εκπαιδευτικούς σκοπούς) με την Python έκδοση 3.8.5.
Οι ενέργειες που εκτελεί ο χρήστης μέσω του εργαλείου είναι εντολές που δίνονται προς το UFW. Το Uncomplicated Firewall είναι το προεπιλεγμένο εργαλείο διαχείρισης του τείχους προστασίας του Linux Ubuntu. Αναπτύχθηκε για να διευκολύνει τη ρύθμιση των iptables. Τα τελευταία είναι μία «βάση δεδομένων» των κανόνων που εφαρμόζει το firewall. Σκοπός του UFW είναι να παρέχει στο χρήστη ένα φιλικό περιβάλλον για να δημιουργήσει ένα IPv4 ή IPv6 host-based τείχος προστασίας.
Στόχος είναι ο χρήστης να λαμβάνει τα δεδομένα που παράγει ο Snort από την κονσόλα, να τα αξιολογεί και ανάλογα με τα ευρήματα να απενεργοποιεί συγκεκριμένες υπηρεσίες ή μέρη του συστήματος με τη βοήθεια της εφαρμογής.

3.6 Υλοποίηση

Το σύστημα στο οποίο στηρίχθηκε η εφαρμογή της υλοποίησης αποτελείται από έναν επεξεργαστή I7-9750H @2.60GHz με εγκατεστημένη μνήμη RAM 32GB, οδηγό NVME M2 1TB και κάρτα γραφικών ολοκληρωμένη με το chipset 1660ti της εταιρείας nvidia. Το εγκατεστημένο host λειτουργικό σύστημα είναι τα Windows 10 Home x64.
Αρχικά εγκαταστάθηκε το λογισμικό Oracle VM VirtualBox της έκδοσης 6.1 για συστήματα x64 καθώς επίσης και η επέκταση Extension Pack. Ακολούθησε η παραμετροποίηση. Στις γενικές ρυθμίσεις επιλέχθηκε η χρήση κοινού πρόχειρου και η δυνατότητα μεταφοράς και απόθεσης. Στις ρυθμίσεις του συστήματος δεσμεύτηκαν 8GB μνήμης RAM καθώς επίσης και 2 από τους 6 πυρήνες του επεξεργαστή. Στόχος ήταν η παροχή επαρκούς επεξεργαστικής ισχύς και μνήμης RAM στο guest ΛΣ χωρίς παράλληλα να επιβαρύνεται το host ΛΣ. Όσον αφορά τις ρυθμίσεις της οθόνης δεσμεύτηκαν 128MB μνήμης της κάρτας γραφικών ώστε να επιτυγχάνονται οι επιθυμητές αναλύσεις. Τέλος στις ρυθμίσεις δικτύου ενεργοποιήθηκε η κάρτα δικτύου με επιλεγμένη την λειτουργία γεφυρωμένης κάρτας ώστε το host και τα guest ΛΣ να βρίσκονται στο ίδιο δίκτυο.
Στη συνέχεια προχώρησε η εγκατάσταση του Linux Ubuntu x64 έκδοσης 20.4 LTS και σε δεύτερη εικονική μηχανή του Kali Linux έκδοσης 2020.4 amd64.

3.6.1 Εγκατάσταση του Snort 3

Για την προετοιμασία του συστήματος αποθηκεύτηκαν και εγκαταστάθηκαν οι πιο πρόσφατες λίστες πακέτων:

```
sudo apt-get update
sudo apt-get upgrade
```

Επίσης ελέγχθηκε ότι το ΛΣ έχει συγχρονίσει σωστά τη ζώνη ώρας. Στη συνέχεια δημιουργήθηκε ένας φάκελος στον οποίο θα αποθηκεύονται τα αρχεία πηγαίου κώδικα που θα χρησιμοποιηθούν στη συνέχεια.

```
mkdir ~/snort-source-files/
cd ~/snort-source-files/
```

Για να είναι εφικτή η εγκατάσταση του Snort έπρεπε να προηγηθεί η εγκατάσταση των προαπαιτούμενων πακέτων

```
sudo apt-get install -y build-essential autotools-dev
libdumbnet-dev \libluajit-5.1-dev libpcap-dev zlib1g-dev
pkg-config libhwloc-dev \cmake
```

Εγκαταστάθηκαν τα προαπαιτούμενα για τη βιβλιοθήκη απόκτησης δεδομένων του Snort

```
sudo apt-get install -y bison flex libcmocka-dev
```

Εγκαταστάθηκαν τα πακέτα Libnetfilter για να μπορεί ο Snort να χρησιμοποιηθεί σε λειτουργία IPS στα πλαίσια της έρευνας

```
sudo apt-get install -y libnetfilter-queue-dev libmnl-dev
```

Εγκαταστάθηκαν τα gperftools 2.7 που περιέχουν το εργαλείο Tcmalloc το οποίο διαχειρίζεται τη μνήμη κατά τη διάρκεια λειτουργίας του Snort

```
sudo apt-get install -y libunwind-dev

cd~/snort-source-files/

wget   https://github.com/gperftools/gperftools/releases/download/gperftools-2.7.90/gperftools-2.7.90.tar.gz

tar xzvf gperftools-2.7.90.tar.gz

cd gperftools-2.7.90

./configure

Make

sudo make install
```

Εγκαταστάθηκαν τα Ragel και Boost headers τα οποία χρησιμοποιεί ο Hyperscan κατά τη διαδικασία ταχείας ταυτοποίησης των κανόνων.

```
cd~/snort-source-files/

wget http://www.colm.net/files/ragel/ragel-6.10.tar.gz

tar -xzvf ragel-6.10.tar.gz

cd ragel-6.105

./configure

make

sudo make install
```

Εγκαταστάθηκαν οι βιβλιοθήκες C++ του Boost

```
cd~/snort-source-files/

wget https://dl.bintray.com/boostorg/release/1.72.0/source/boost_1_72_0.tar.gz

tar -xvzf boost_1_72_0.tar.gz
```

Εγκαταστάθηκε το Hyperscan 5.2.1

```
Cd ~/snort-source-files/

wget https://github.com/intel/hyperscan/archive/v5.2.1.tar.gz

tar -xvzf v5.2.1.tar.gz

mkdir  ~/snort_src/hyperscan-5.2.1-build
```

```
cd hyperscan-5.2.1-build/
cmake -DCMAKE_INSTALL_PREFIX=/usr/local-DBOOST_ROOT=~/ snort-source-files/boost_1_72_0/ ../hyperscan-5.2.1

make
sudo make install
```

Δοκιμάστηκε η λειτουργία του Hyperscan

```
cd~/snort-source-files/hyperscan-5.2.1-build/

./bin/unit-hyperscan
```

Εγκαταστάθηκε η βιβλιοθήκη απόκτησης δεδομένων (Data AcQuisition library -DAQ-)

```
cd ~/snort-source-files/

git clone https://github.com/snort3/libdaq.git

cd libdaq

./bootstrap

./configure

Make

sudo make install
```

Ενημερώθηκαν οι κοινές βιβλιοθήκες

```
sudo ldconfig
```

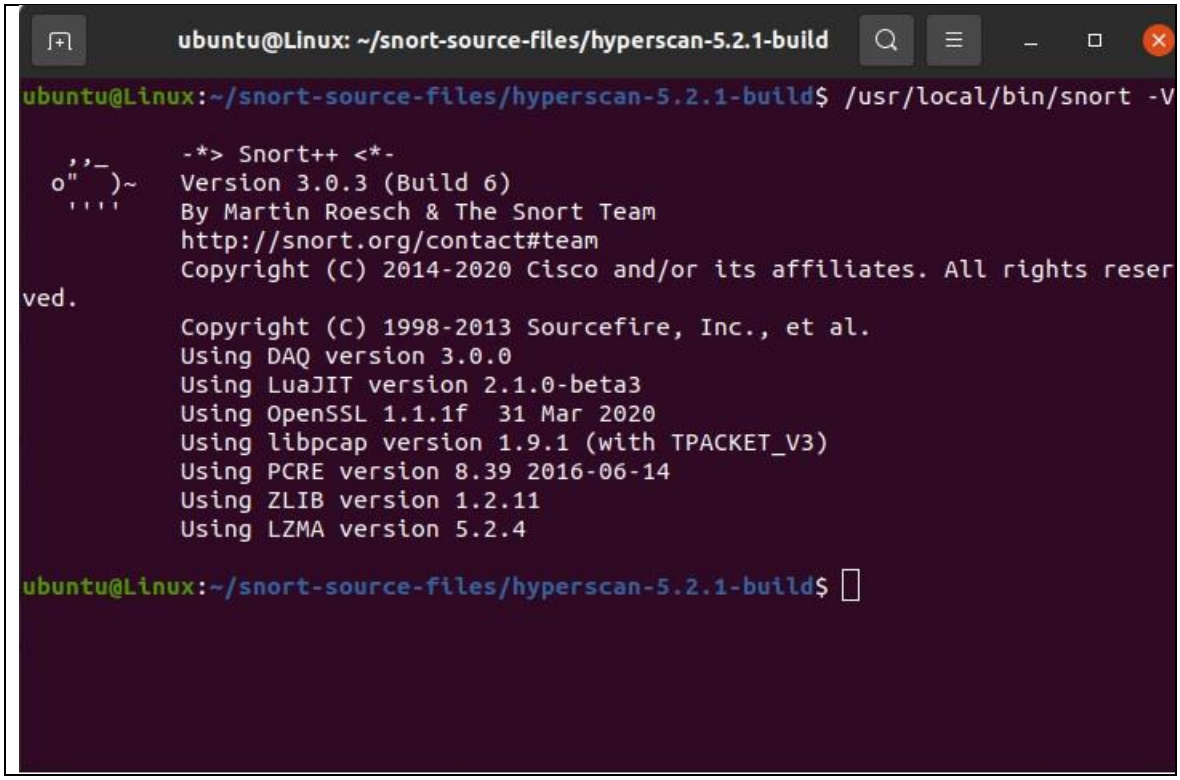
Στο σημείο αυτό το σύστημα ήταν προετοιμασμένο για την εγκατάσταση του Snort 3. Έγινε χρήση του αποθετήριου github:

```
cd ~/snort-source-files/

git clone git://github.com/snortadmin/snort3.git

cd snort3

./configure_cmake.sh --prefix=/usr/local--enable-tcmalloc

cd build

make

sudo make install
```

Το τελευταίο βήμα της εγκατάστασης η επιβεβαίωση ότι ο Snort ήταν σωστά εγκατεστημένος και μπορούσε να τρέχει χωρίς σφάλματα:

```
/usr/local/bin/snort -V
```

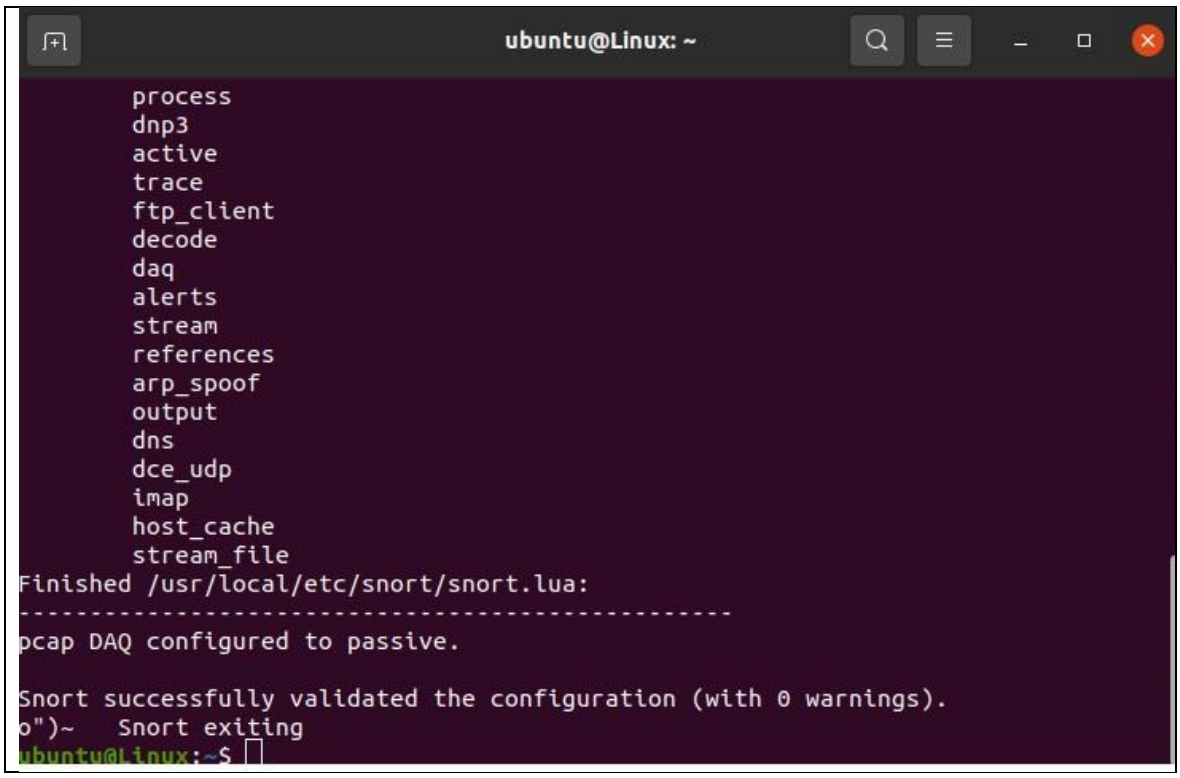
Το αποτέλεσμα στην έξοδο της οθόνης ήταν το παρακάτω:



Κατόπιν ο Snort δοκιμάστηκε με τη χρήση του προεπιλεγμένου αρχείου παραμετροποίησης:

```
snort -c /usr/local/etc/snort/snort.lua
```

Η έξοδος έδειξε τα ακόλουθα:



3.6.2 Παραμετροποίηση της κάρτας δικτύου

Οι σύγχρονες κάρτες δικτύου χρησιμοποιούν το υλικό για την επανένωση των πακέτων παράγοντας μεγαλύτερα σε μήκος πακέτα. Για το λόγο αυτό οι επιλογές LRO και GRO απενεργοποιήθηκαν δημιουργώντας την υπηρεσία systemD για να αλλάζει αυτές τις επιλογές. Πρώτα εντοπίστηκε το όνομα της διεπαφής την οποία χρησιμοποιεί ο Snort για να παρακολουθεί τα πακέτα χρησιμοποιώντας την εντολή:

```
ip address show
```

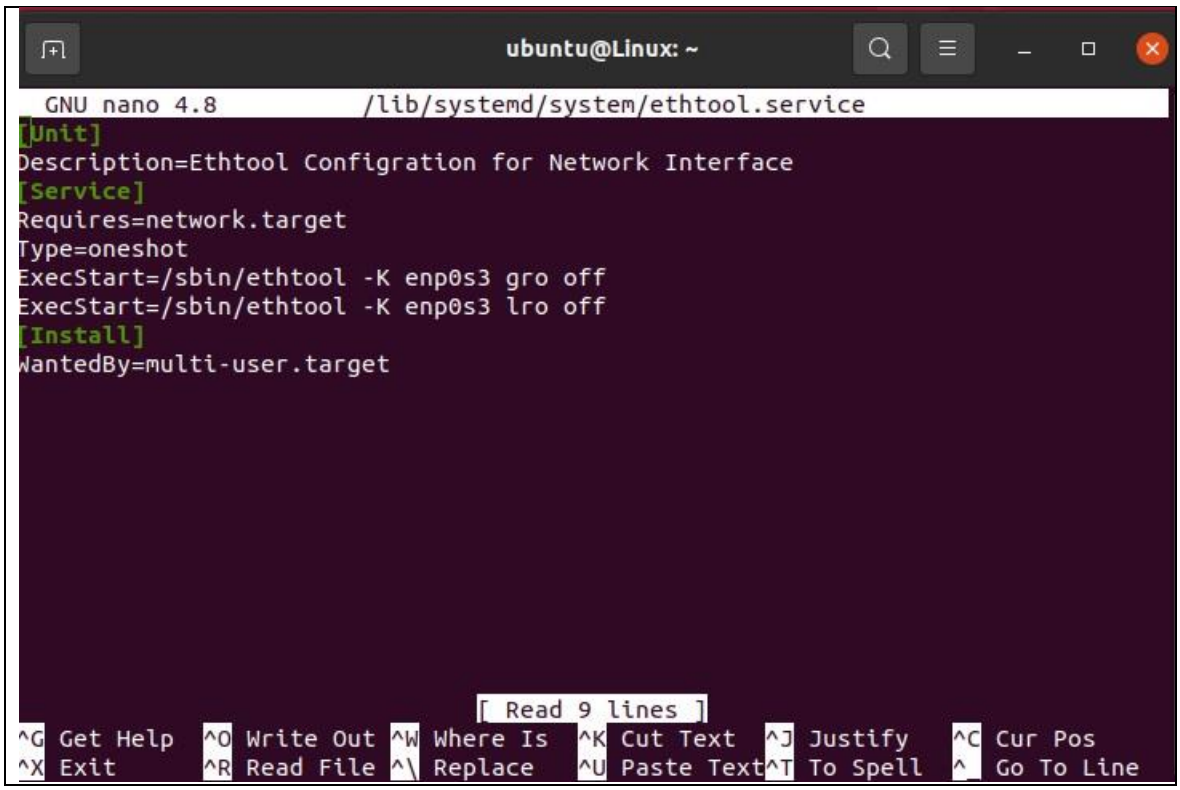
Αρχικά χρησιμοποιήθηκε η εντολή ethtool για να ελέγξουμε την κατάσταση:

```
ubuntu@linux: ~$ sudo ethtool -k enp0s3 | grep receive-
offload

generic-receive-offload: on

large-receive-offload: off [fixed]
```

Στη συνέχεια δημιουργήθηκε το script systemD:

```
sudo nano /lib/systemd/system/ethtool.service
```

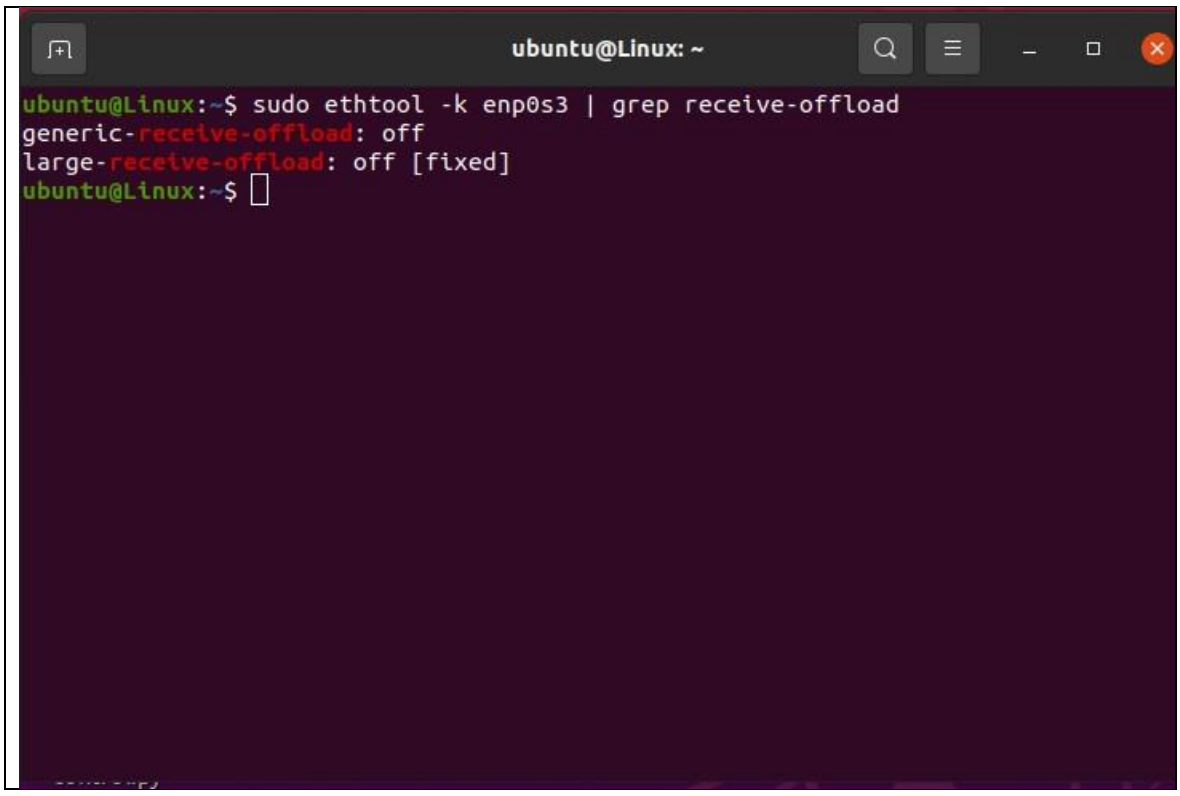
Έπειτα εισήχθησαν οι παρακάτω εντολές:



Όταν το αρχείο δημιουργήθηκε, ενεργοποιήθηκε και η υπηρεσία:

```
sudo systemctl enable ethtool

sudo service ethtool start
```

Το αποτέλεσμα είναι το παρακάτω:



3.6.3 Εγκατάσταση του OpenAppID

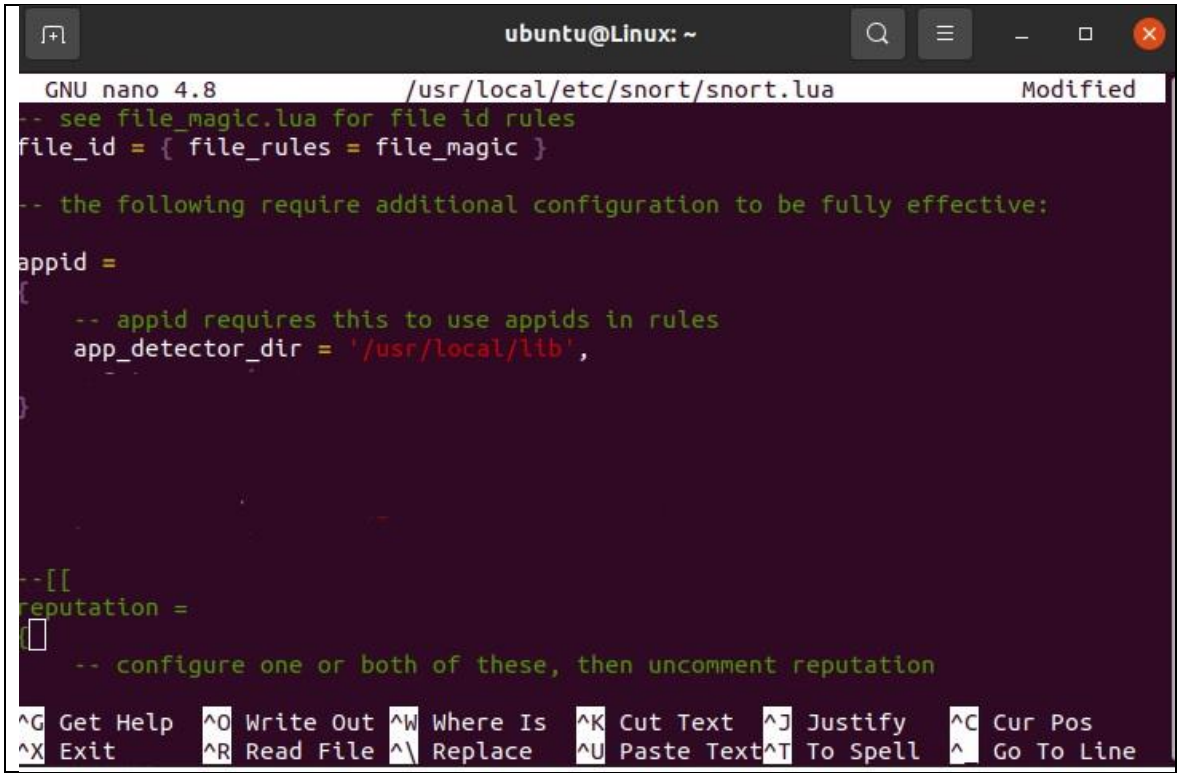
Το OpenAppID επιτρέπει την ταυτοποίηση στο επίπεδο εφαρμογής (επίπεδο 7 του μοντέλου OSI) της κίνησης. Δίνει τη δυνατότητα δημιουργίας κανόνων οι οποίοι λειτουργούν πάνω στη κίνηση του επιπέδου εφαρμογής και κρατάει αρχεία log για το κάθε τύπο της κίνησης που εντοπίστηκε.
Η ομάδα ανάπτυξης του Snort σε συνεργασία με την κοινότητα δημιούργησε ένα πακέτο ανιχνευτών (Application Detector Package):

```
cd~/snort-source-files/

wget https://snort.org/downloads/openappid/12159 -O
OpenAppId-12159.tgz

tar -xzvf OpenAppId-12159.tgz

sudo cp -R odp /usr/local/lib/
```

Μετά την ολοκλήρωση της αποθήκευσης των κανόνων επεξεργάστηκε το αρχείο παραμετροποίησης του Snort ώστε να μπορεί να τους φορτώσει:

```
sudo nano /usr/local/etc/snort/snort.lua
```

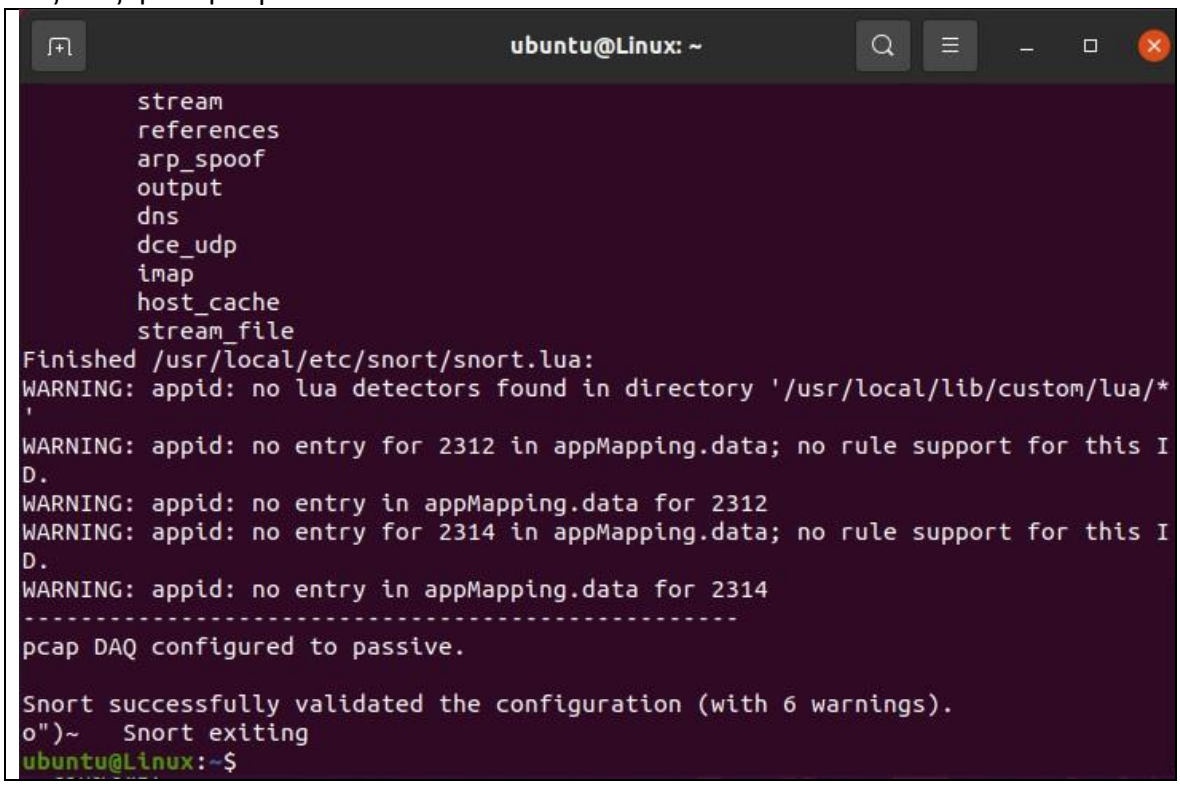
Στο αρχείο προστέθηκαν οι παρακάτω γραμμές:



Ακολούθησε ο έλεγχος της σωστής λειτουργίας:

```
snort -c /usr/local/etc/snort/snort.lua --warn-all
```

Η έξοδος ήταν η παρακάτω:



Στο αρχείο local.rules δημιουργήθηκαν δύο κανόνες, ο πρώτος ελέγχει τη χρήση του Facebook και ο δεύτερος την κίνηση ICMP. Η δημιουργία των παραπάνω έγινε με σκοπό τον έλεγχο των παραγόμενων ειδοποιήσεων.

```
sudo mkdir /usr/local/etc/rules
sudo touch /usr/local/etc/rules/local.rules
sudo nano /usr/local/etc/rules/local.rules
```

```
alert tcp any any -> any any ( msg:"Facebook Detected";
appids:"Facebook";sid:10000001; )2alert icmp any any ->
any any (msg:"ICMP Traffic Detected";sid:10000002;)
```

Η εκκίνηση του Snort με χρήση του αρχείου local.rules έγινε ως εξης:

```
snort -c /usr/local/etc/snort/snort.lua \
-R /usr/local/etc/rules/local.rules
```

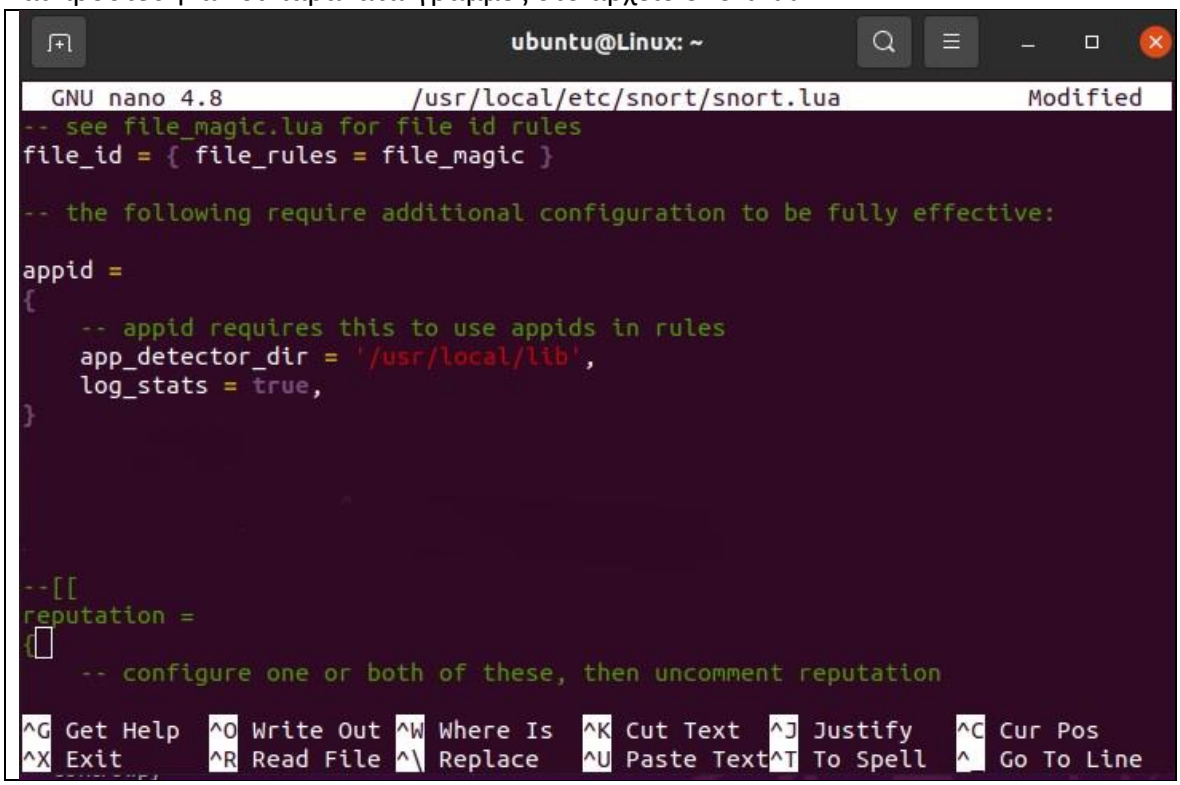
Στη συνέχεια δοκιμάστηκε να εκτελεστεί ο Snort σε λειτουργία IDS παρακολουθώντας τη διεπαφή του δικτύου:

```
sudo snort -c /usr/local/etc/snort/snort.lua -R
/usr/local/etc/rules/local.rules \2-i eth0 -A alert_fast
-s 65535 -k none
```

Για τη συλλογή στατιστικών του OpenAppID δημιουργήθηκε ένα αρχείο καταγραφής συμβάντων:

```
sudo mkdir /var/log/snort
```

Και προστέθηκαν οι παρακάτω γραμμές στο αρχείο Snort.lua:



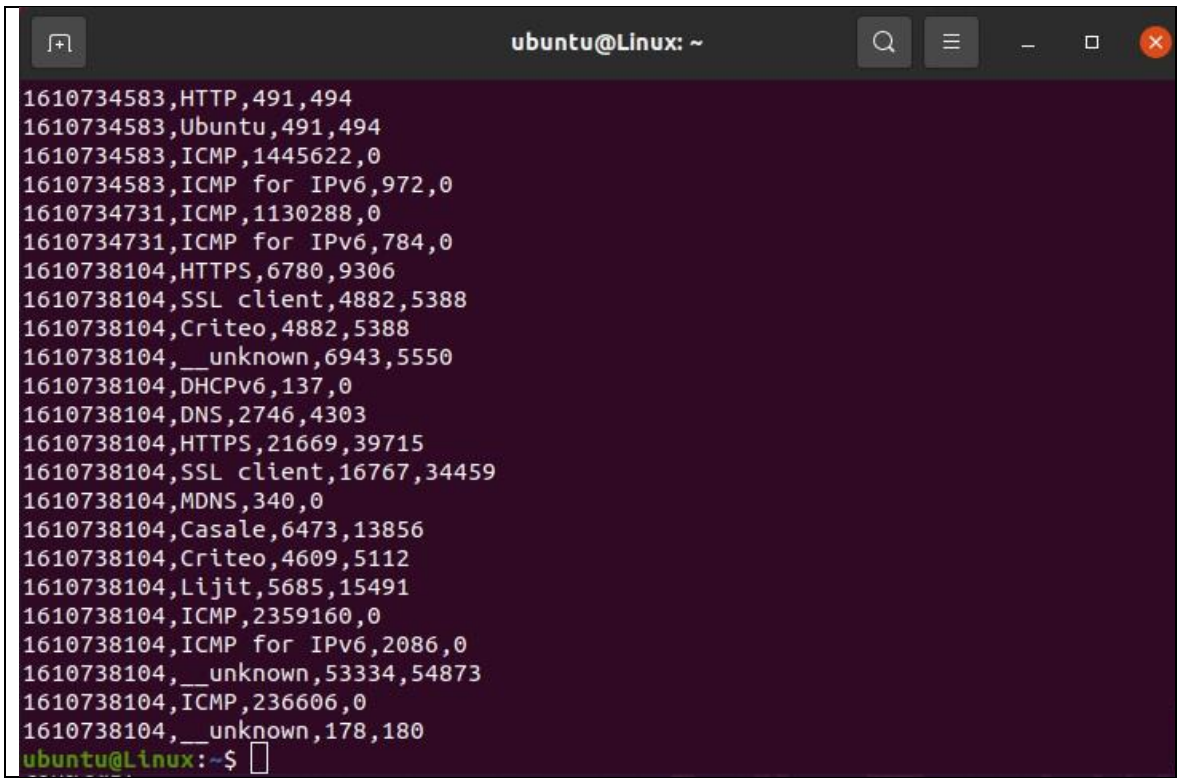
Εκτελέστηκε ο Snort με την επιλογή καταγραφής συμβάντων:

```
sudo snort -c /usr/local/etc/snort/snort.lua -R
/usr/local/etc/rules/local.rules \ -i enp0s3 -A
alert_fast -s 65535 -k none -l /var/log/snort
```

Το παραγόμενο αρχείο log ανήκει στο root οπότε αλλάχθηκαν τα δικαιώματα:

```
sudo chmod a+r /var/log/snort/appid_stats.log
```

Τα αποτελέσματα είναι τα παρακάτω:



3.6.4 Εγκατάσταση των κανόνων του Snort

Οι κανόνες της έκδοσης 3 του Snort περιλαμβάνουν περισσότερες επιλογές από τους αντίστοιχους της έκδοσης 2 και πρέπει στην παρούσα φάση να μεταφορτωθούν από το χρήστη.
Υπάρχουν τρία είδη κανόνων από όπου ο χρήστης μπορεί να επιλέξει. Οι κανόνες της κοινότητας οι οποίοι είναι δωρεάν, οι κανόνες των εγγεγραμμένων χρηστών οι οποίοι απαιτούν σύνδεση στο snort.org για να μεταφορτωθούν και τέλος οι κανόνες των συνδρομητών οι οποίοι παρέχονται κατόπιν συνδρομής. Για την παρούσα διατριβή επιλέχθηκε το σύνολο κανόνων των εγγεγραμμένων χρηστών το οποίο μεταφορτώθηκε στο φάκελο snort-src. Στη συνέχεια οι κανόνες αποσυμπιέστηκαν στην τοποθεσία /usr/local/etc/snort/. Στο φάκελο rules τοποθετήθηκαν οι κανόνες των εγγεγραμμένων χρηστών, στο φάκελο builtin_rules τοποθετήθηκε το αρχείο που περιέχει τις αναφορές και τις πληροφορίες για τους ενσωματωμένους κανόνες και ο φάκελος lists στον οποίο αποθηκεύτηκαν οι white και black lists. Η εφαρμογή έγινε ως εξής:

```
sudo mkdir /usr/local/etc/rules

sudo mkdir /usr/local/etc/builtin_rules

sudo mkdir /usr/local/etc/so_rules

sudo mkdir /usr/local/etc/lists
```

Η αντιγραφή των απαραίτητων αρχείων στις αντίστοιχες τοποθεσίες έγινε ως εξής:

```
cd~/snort-source-files

mkdir snortrules-3000

tar -xvzf snortrules-snapshot-3000.tar.gz -C
./snortrules-3000

cdsnortrules-3000

# αντιγραφή των μεμονωμένων αρχείων κανόνων
sudo cp ./rules/*.rules /usr/local/etc/rules/

# αντιγραφή του αρχείου των builtin κανόνων
sudo cp ./builtins/builtins.rules
/usr/local/etc/builtin_rules/

# αντιγραφή των νέων αρχείων παραμετροποίησης
# τα παλιά θα διαγραφούν
sudo cp ./etc/* /usr/local/etc/snort/
```

Τα τρία αρχεία που αντιγράφηκαν στο φάκελο etc είναι το file_magic.lua το οποίο δίνει οδηγίες στο Snort πως να αναγνωρίσει τους τύπους των αρχείων, το snort_defaults.lua το οποίο παραμετροποιεί τις επιλογές συστήματος του snort και τέλος το αρχείο snort.lua που αποτελεί το αρχείο παραμετροποίησης για μία συγκεκριμένη εκτέλεση του Snort. Κάθε φορά που εκτελείται ο Snort το αρχείο snort.lua περιγράφει πως θέλει ο διαχειριστής (με ποιες παραμέτρους) θέλει να το τρέξει. Το συγκεκριμένο αρχείο φορτώνει το αρχείο των προεπιλεγμένων ιδιοτήτων οι οποίες ισχύουν για όλο το σύστημα και εφαρμόζονται κάθε φορά που εκτελείται.
Το αρχείο snort.lua επεξεργάστηκε ως ακολούθως για να λειτουργεί σύμφωνα με τις ανάγκες του πονήματος:

```
sudo nano /usr/local/etc/snort/snort.lua
```

Προσδιορίστηκε το τοπικό υποδίκτυο που θα παρακολουθεί ο Snort:

```
HOME_NET ='192.168.0.0/32'
```

Στην επιλογή EXTERNAL_NET παρέμεινε η ιδιότητα any.
Για την παραμετροποιήση του πρόσθετου appid ακολουθήθηκε η μέθοδος που περιγράφηκε πιο πάνω. Η δοκιμή του Snort:

```
snort -c /usr/local/etc/snort/snort.lua
```

Έδωσε την παρακάτω έξοδο:

```
Snort successfully validated the configuration (with 0 warnings).
o")~   Snort exiting
ubuntu@Linux:~$
```

3.6.5 Ενεργοποίηση

Για να είναι σε θέση ο Snort να εντοπίσει κακόβουλη κίνηση η οποία δεν εντοπίζεται εύκολα από τους απλούς κανόνες ενεργοποιήθηκαν οι ενσωματωμένοι κανόνες από το αρχείο παραμετροποίησης snort.lua το οποίο βρίσκεται στη τοποθεσία /usr/local/etc/snort/. Επιπρόσθετα φορτώθηκε το αρχείο builtins.rules το οποίο περιέχει πληροφορίες για κάθε ειδοποίηση και οι οποίες θα τυπώνονται στην κονσόλα. Η εφαρμογή της ως άνω διαδικασίας έγινε ως εξής:

```
sudo nano /usr/local/etc/snort/snort.lua
```

```
ips =
{
  rules = [[
    include $BUILTIN_RULE_PATH/builtins.rules

    include $RULE_PATH/snort3-app-detect.rules
    include $RULE_PATH/snort3-browser-chrome.rules
}
```

Ακολούθησε ο έλεγχος:

```
snort -c /usr/local/etc/snort/snort.lua
```

Η έξοδος μας έδειξε τα παρακάτω:

```
Finished ips.rules:
Loading rule args:
Loading /usr/local/etc/rules/local.rules:
Finished /usr/local/etc/rules/local.rules:
Finished rule args:
-------------------------------------------------------------------------------
rule counts
           total rules loaded: 13108
```

Για να φορτωθούν οι κανόνες από το αρχείο local.rules θα πρέπει να προστεθούν οι παρακάτω γραμμές στο αρχείο snort.lua:

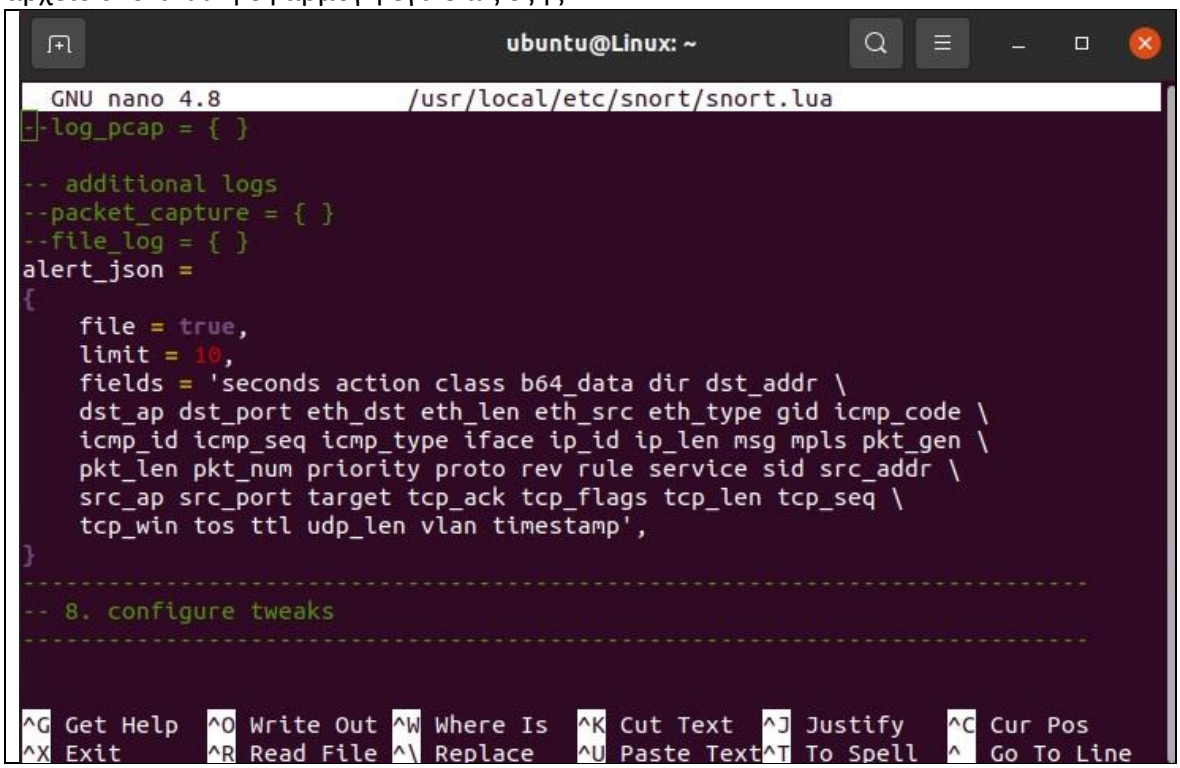
```
appid =
{
    app_detector_dir ='/usr/local/lib',
    log_stats =true,
}
```

Ακολούθησε ο έλεγχος:

```
sudo snort -c /usr/local/etc/snort/snort.lua \ -R
/usr/local/etc/rules/local.rules \ -i eth0 -A alert_fast
-s 65535 -k none -l /var/log/snort
```

3.6.6 Το πρόσθετο που παράγει ειδοποιήσεις σε αρχεία τύπου JSON

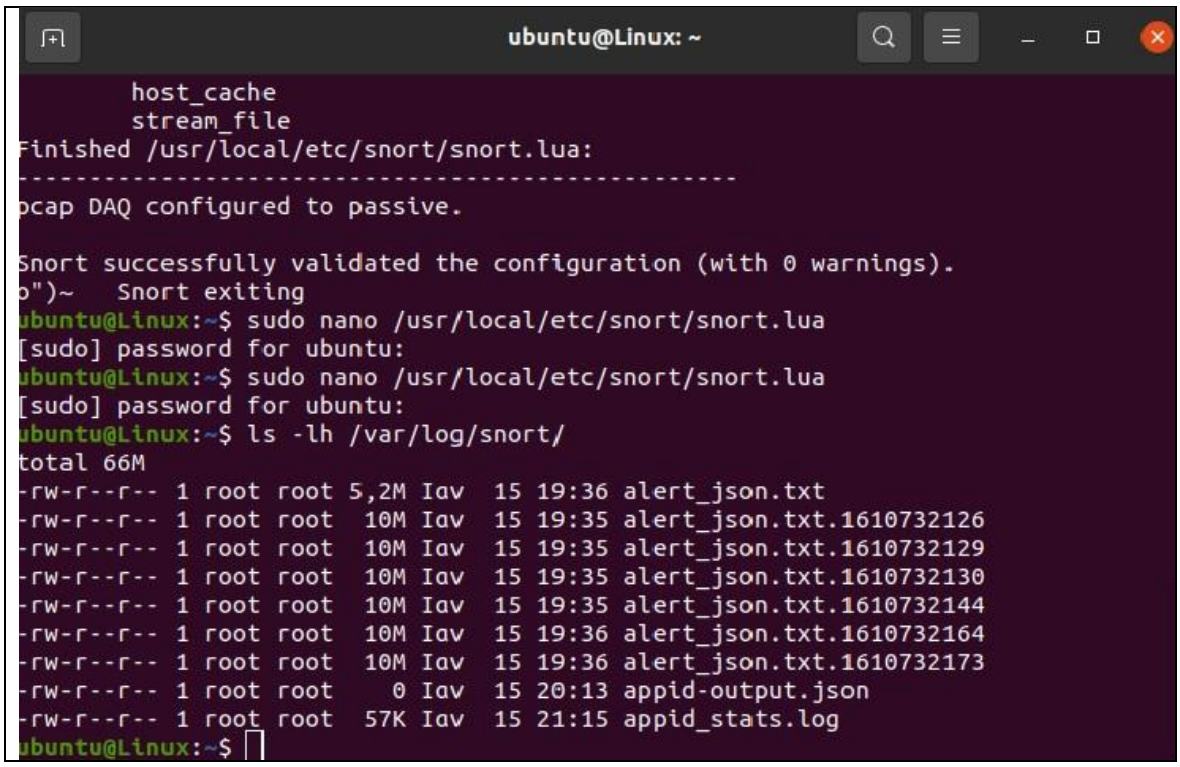
Ο Snort 3 περιέχει ένα σύνολο πρόσθετων εξόδου. Έως τώρα ενεργοποιήθηκε το πρόσθετο alert_fast το οποίο τυπώνει τις ειδοποιήσεις στην κονσόλα. Για να γίνει η εγγραφή των ειδοποιήσεων σε JSON αρχεία θα πρέπει να ενεργοποιηθεί το πρόσθετο alert_json από το αρχείο snort.lua η εφαρμογή έγινε ως εξής:



Στο πρόσθετο alert_json ορίστηκαν τρεις επιλογές:

- Ενεργοποιήθηκε η επιλογή εξόδου σε αρχείο αντί για την κονσόλα
- Ορίστηκε η επιλογή limit στο μέγεθος του αρχείου, δηλαδή όταν το αρχείο φτάσει τα 10MB ένα νέο θα δημιουργείται.
- Ορίστηκε στην επιλογή fields να περιλαμβάνονται στην εγγραφή του αρχείου όλα τα πεδία.

Το αποτέλεσμα της παραγωγής αρχείων εξόδου ήταν το παρακάτω:



Δημιουργία script για την εκτέλεση του Snort με την εκκίνηση του συστήματος. Δημιουργήθηκε το script systemD για να εκτελείται το Snort αυτόματα. Για λόγους ασφαλείας ο Snort εκτελείται ως απλός χρήστης. Πρώτα δημιουργήθηκε ο χρήστης και το group Snort:

```
sudo groupadd snort

sudo useradd snort -r -s /sbin/nologin -c SNORT_IDS -g
snort
```

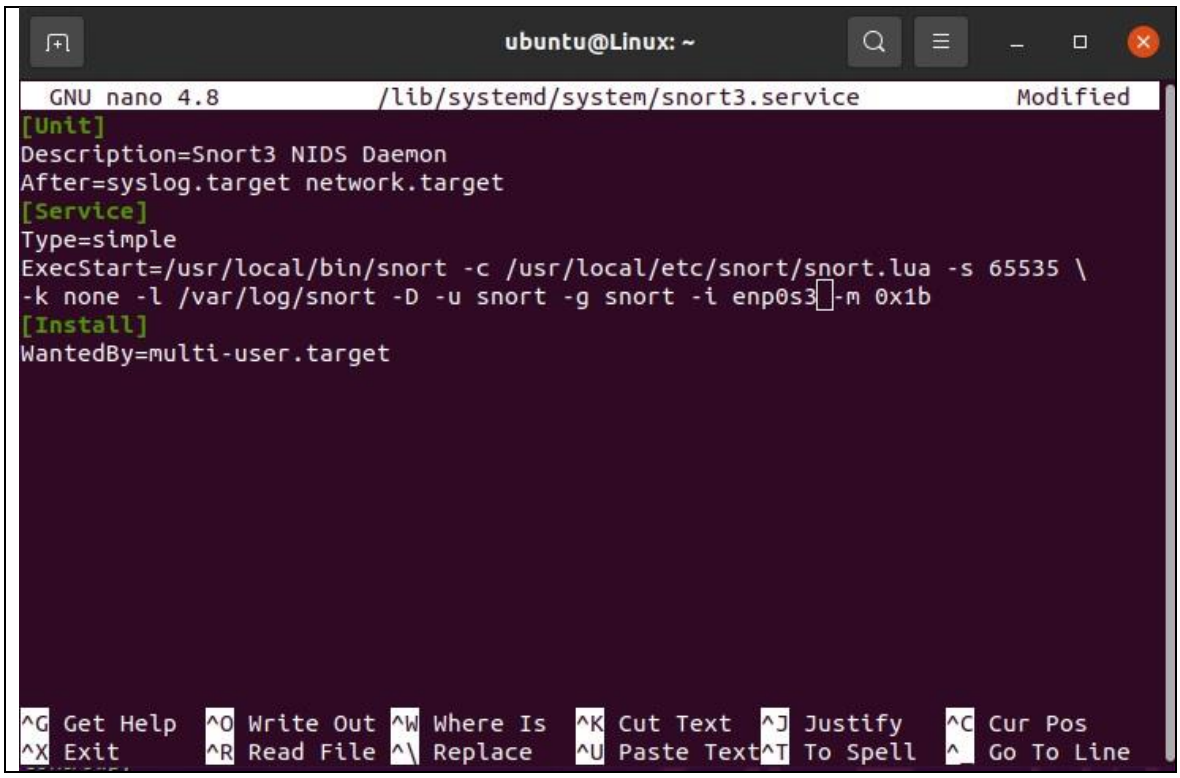
Στη συνέχεια δόθηκαν τα δικαιώματα του χρήστη Snort στο φάκελο log

```
sudo chmod -R 5775 /var/log/snort

sudo chown -R snort:snort /var/log/snort
```

Δημιουργήθηκε το αρχείο υπηρεσίας systemD:

```
sudo nano /lib/systemd/system/snort3.service
```

Και προστέθηκαν οι παρακάτω γραμμές:



Ενεργοποιήθηκε η υπηρεσία Snort systemD και εκκινήθηκε:

```
sudo systemctl enable snort3

sudo service snort3 start
```

Ακολούθησε ο έλεγχος της κατάστασης της υπηρεσίας:

```
service snort3 status
```

3.6.7 Εγκατάσταση της Python

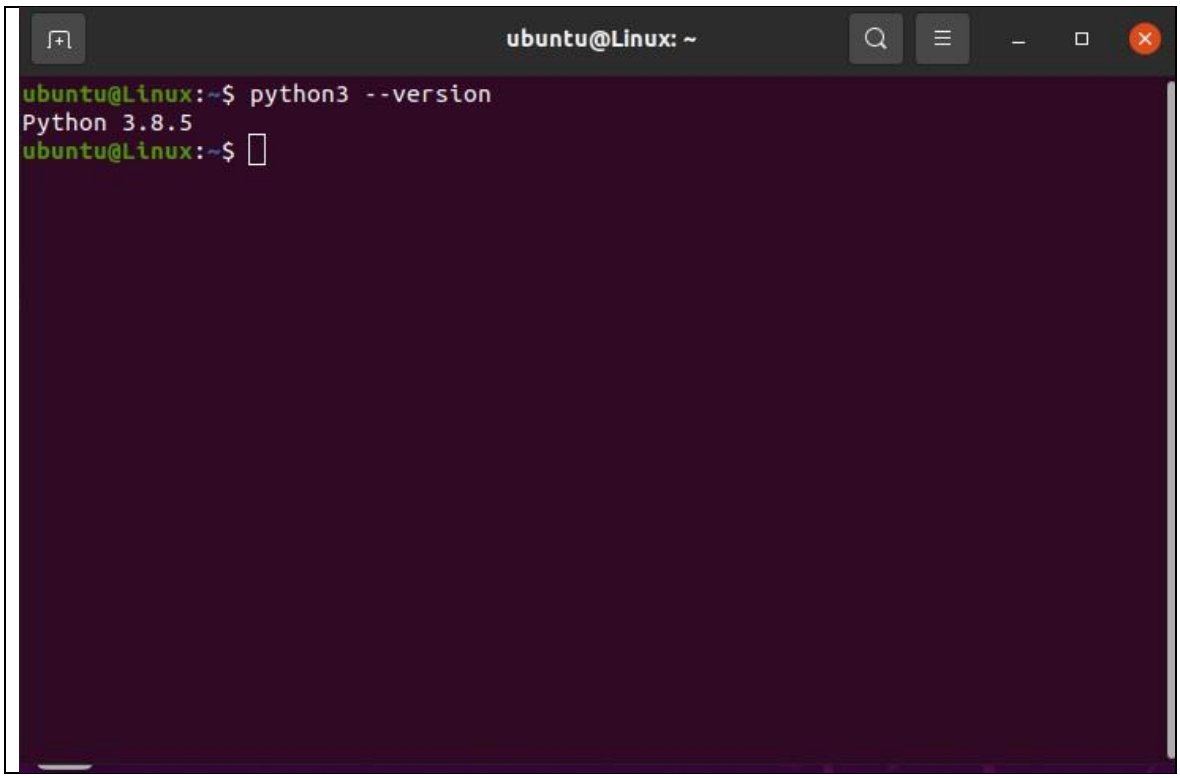
Από την έκδοση Ubuntu 20.04 η Python 3 περιλαμβάνεται στη βασική εγκατάσταση του συστήματος. Για να εγκατασταθεί η τελευταία έκδοση ακολουθήθηκαν τα παρακάτω βήματα:

```
sudo apt update
sudo apt install python3-pip
```

Η παραπάνω εντολή επίσης εγκατέστησε όλες τις απαραίτητες εξαρτήσεις. Ο έλεγχος της έκδοσης έγινε έτσι:

```
python3 --version
```

Το αποτέλεσμα ήταν το ακόλουθο:



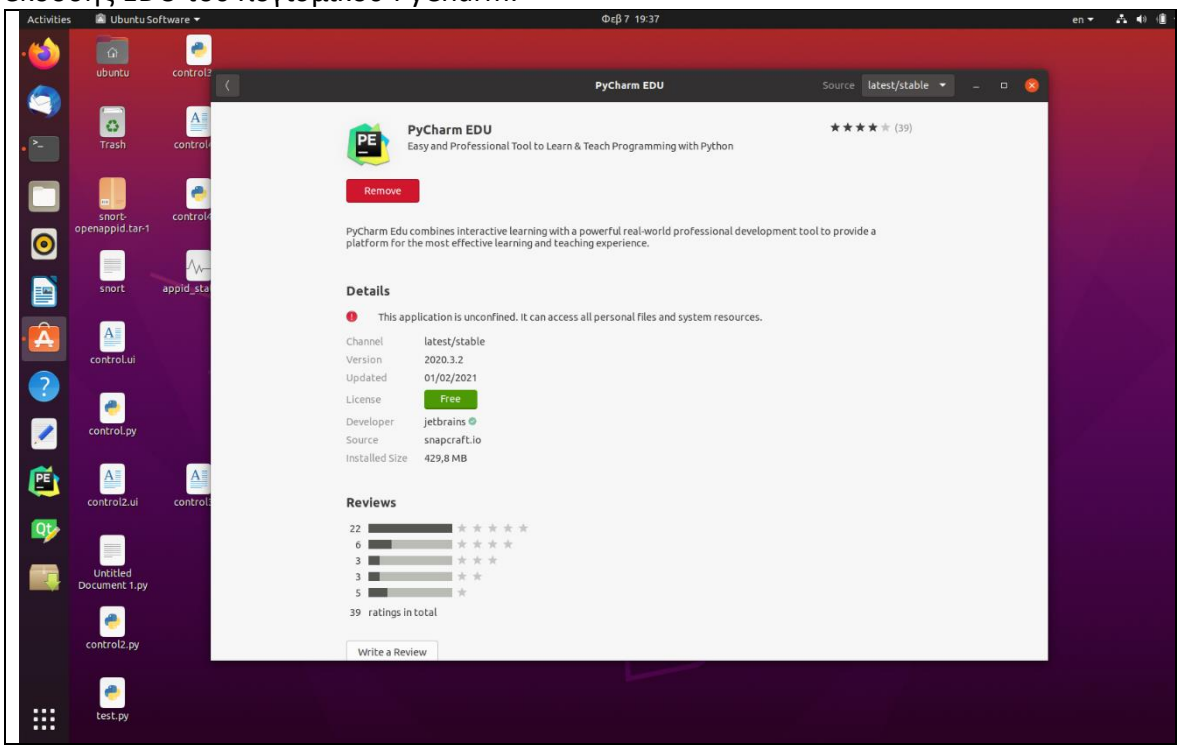
3.6.8 Εγκατάσταση του PyQt5

Εκτελέστηκαν οι παρακάτω εντολές για να εγκατασταθεί το PyQt5:

```
pip3 install --user pyqt5
sudo apt-get install python3-pyqt5
sudo apt-get install pyqt5-dev-tools
sudo apt-get install qttools5-dev-tools
```

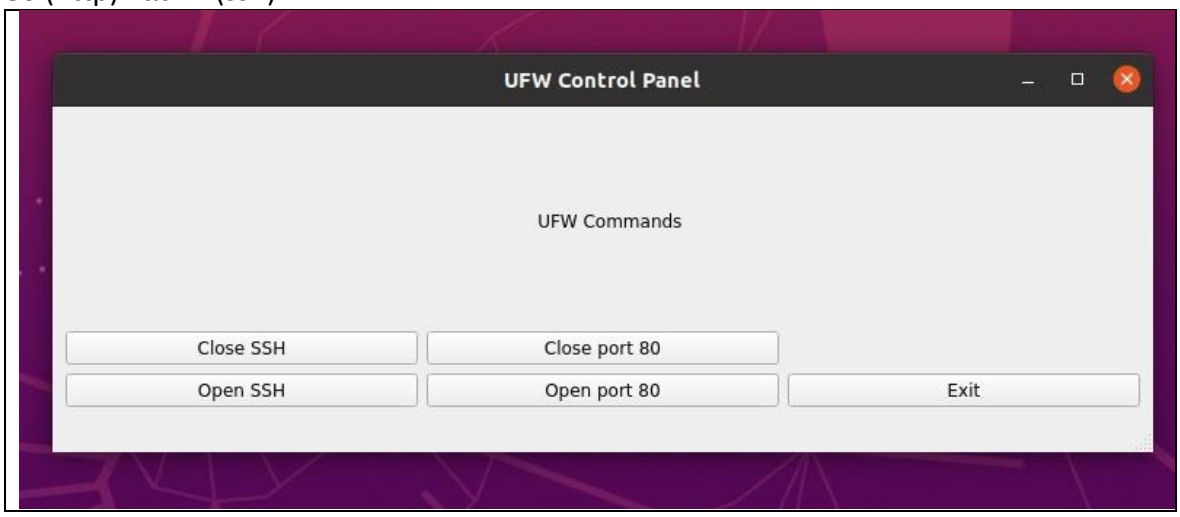
3.6.9 Εγκατάσταση του PyCharm

Χρησιμοποιήθηκε το εργαλείο Ubuntu Software για την εγκατάσταση της τελευταίας έκδοσης EDU του λογισμικού PyCharm.

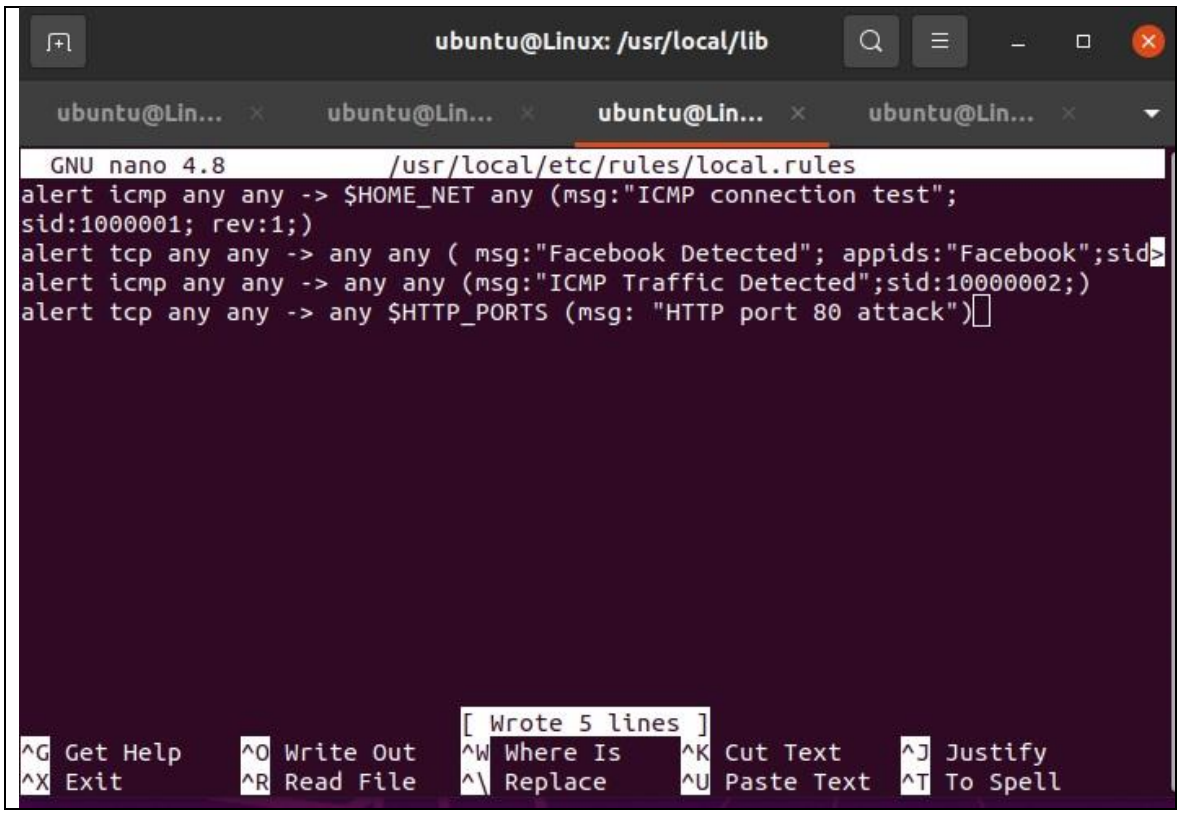


3.7 Εφαρμογή της υλοποίησης

Το πρώιμο εργαλείο δίνει τη δυνατότητα στο διαχειριστή να απενεργοποιήσει της θύρες 80 (http) και 22 (ssh).



Για τη δοκιμή της αποτελεσματικότητας εκτελέστηκαν οι παρακάτω ενέργειες:
Στο αρχείο /usr/local/etc/rules/local.rules προστέθηκε ένα νέο alert το οποίο ενεργοποιείται όταν υπάρχει κίνηση TCP προς τη θύρα 80 του συστήματος και τυπώνει το μήνυμα: HTTP port 80 attack.



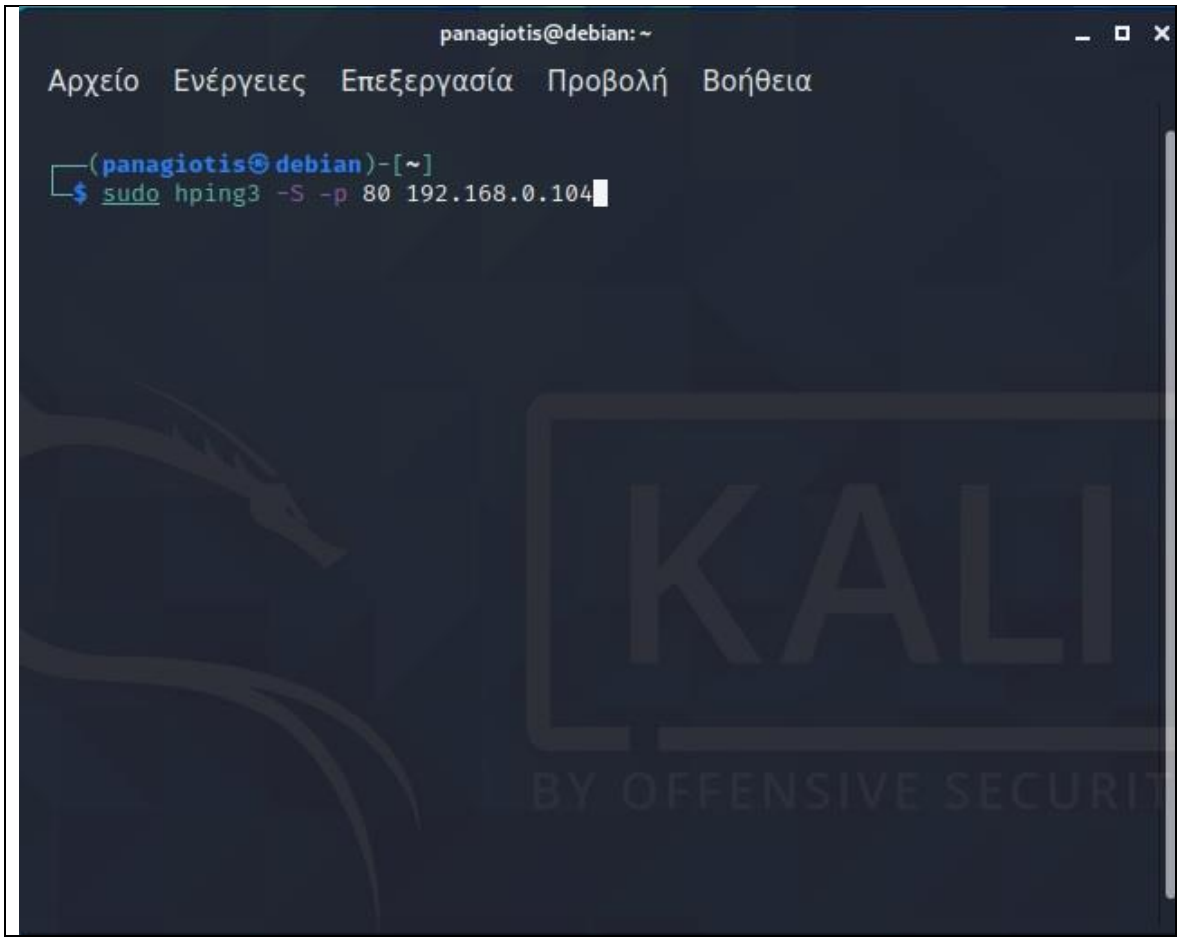
Στη συνέχεια εκτελέστηκε ο Snort3:

```
sudo snort -c /usr/local/etc/snort/snort.lua -R
/usr/local/etc/rules/local.rules \
-i enp0s3 -A alert_fast -s 65535 -k none
```

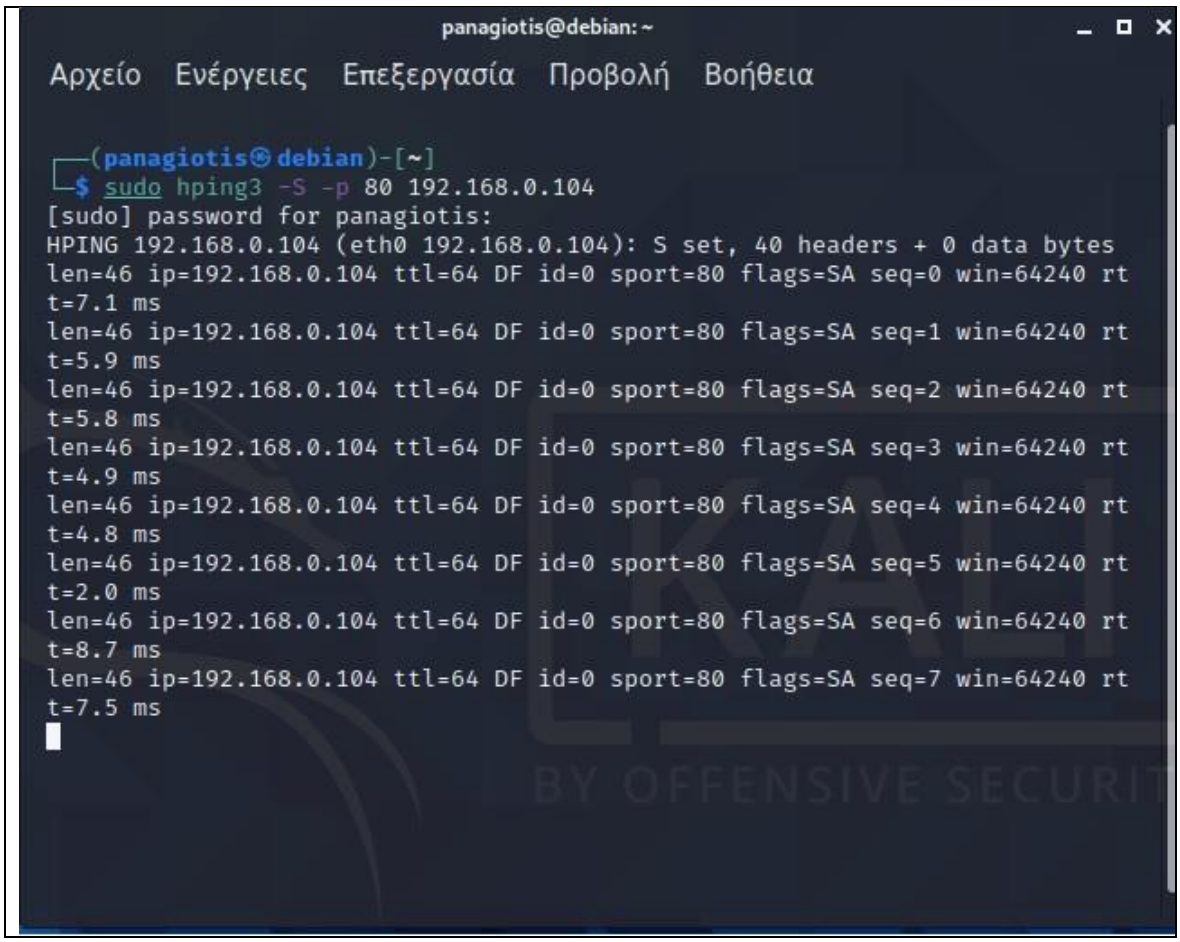
Σε δεύτερη εικονική μηχανή Kali Linux εκτελέστηκε η εντολή:

```
sudo hping3 -S -p 80 192.168.0.104
```

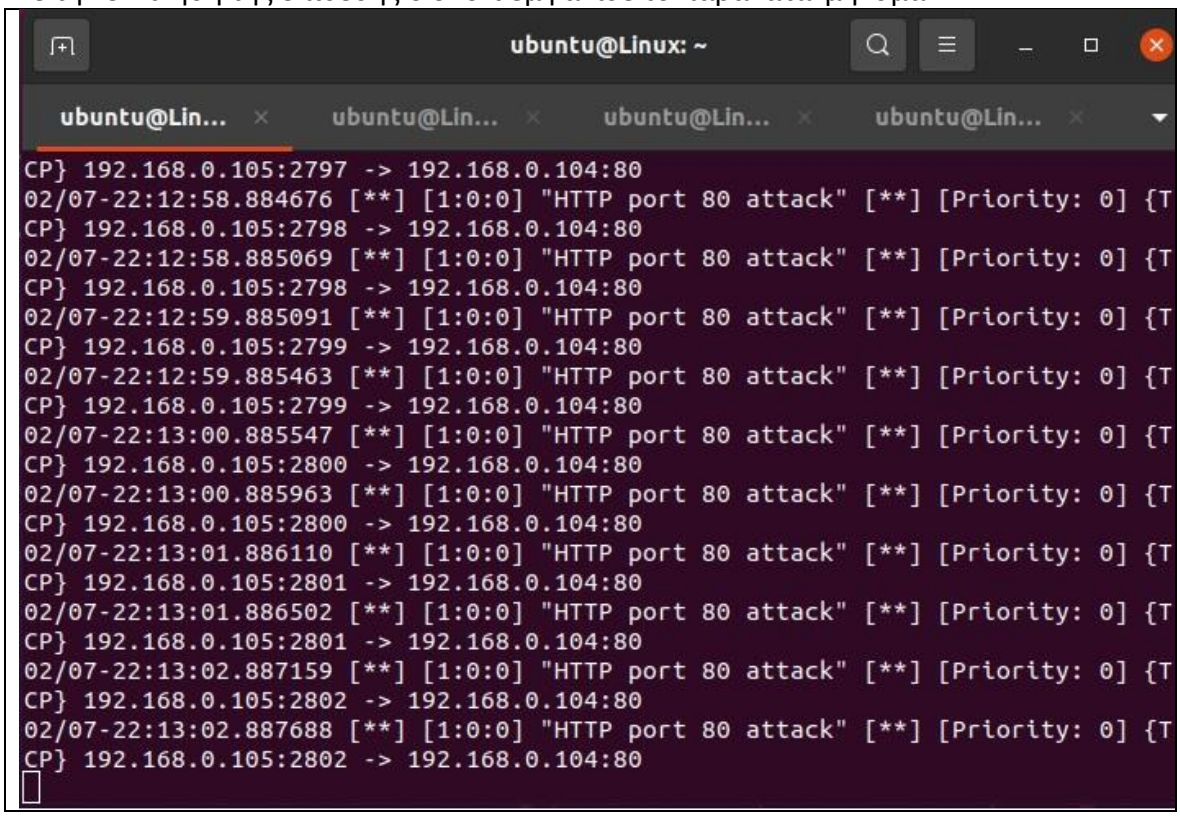
Το αποτέλεσμα είναι το παρακάτω:



Με την εκτέλεση της εντολής ξεκινά η επίθεση στη θύρα 80 του συστήματος. Για λόγους σταθερότητας του συστήματος δεν επιλέχθηκε η λειτουργεία flood του εργαλείου hping3.



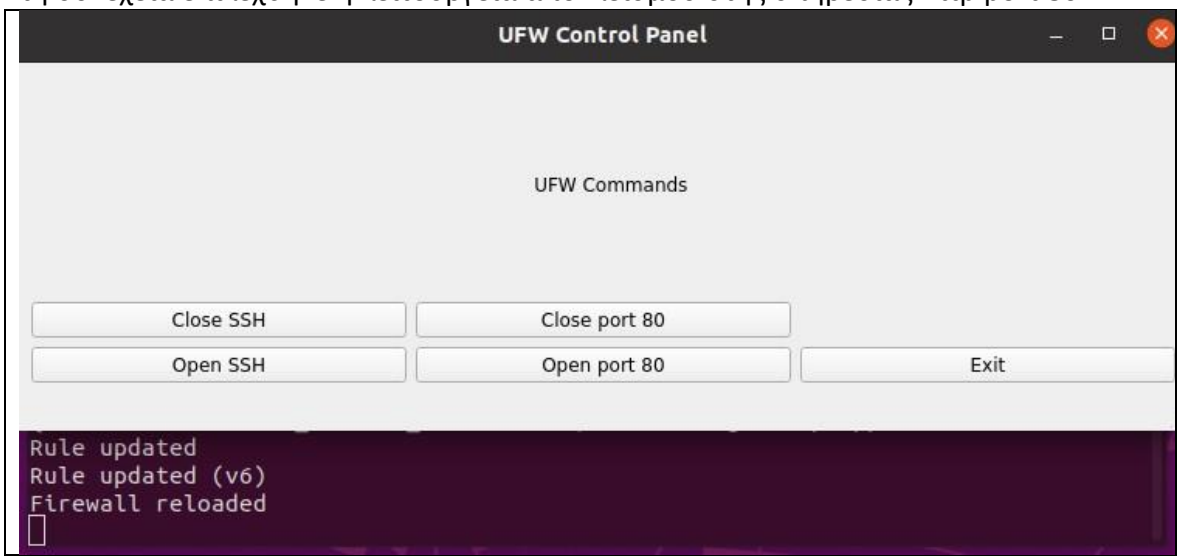
Με την εκκίνηση της επίθεσης ο Snort εμφάνισε το παρακάτω μήνυμα:



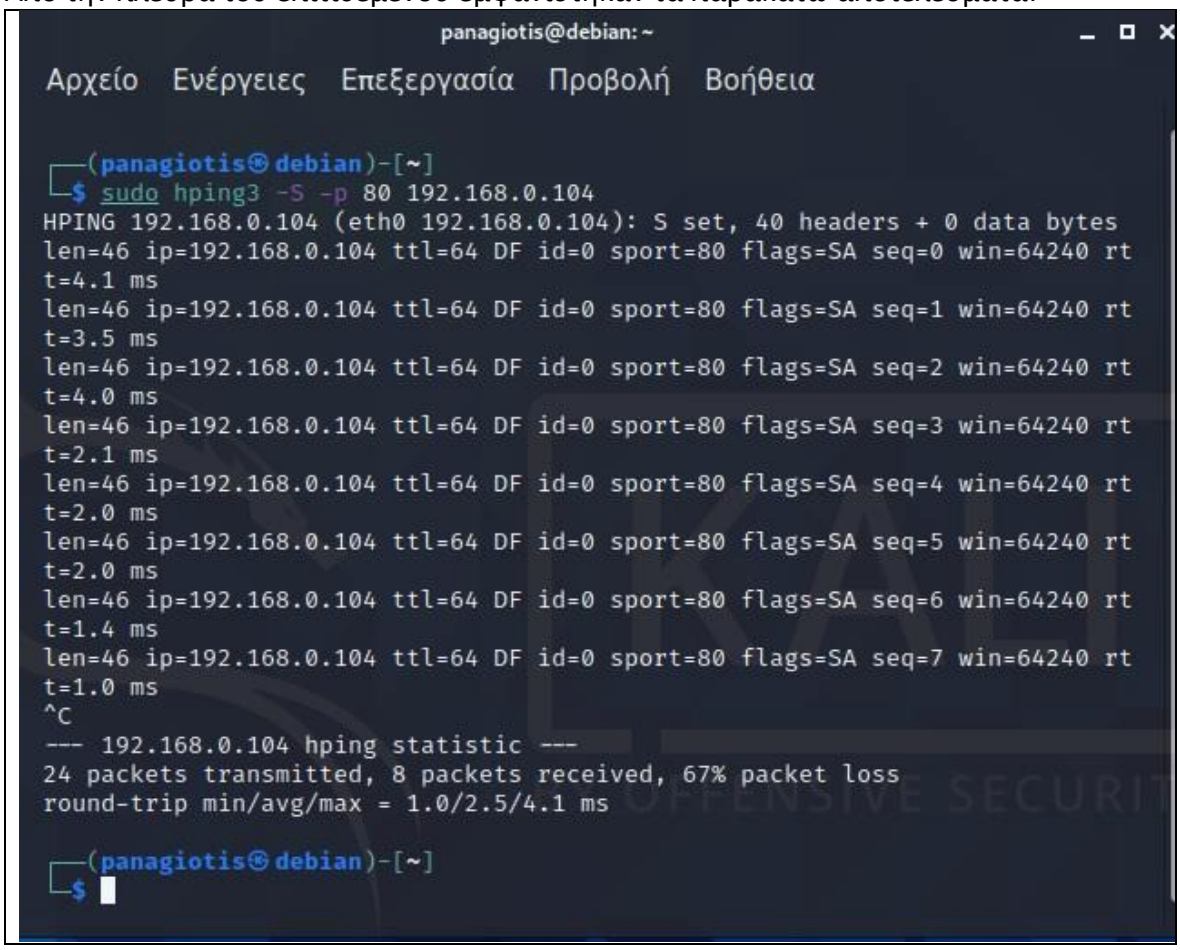
Για την αντιμετώπιση του κακόβουλου συμβάντος εκτελέστηκε το πρώιμο εργαλείο με δικαιώματα διαχειριστή ώστε να είναι σε θέση να δώσει εντολές στο UFW Firewall:

```
sudo python3 control.py
```

Στη συνέχεια επιλέχθηκε η λειτουργεία αποκλεισμού στης υπηρεσίας http port 80



Το πρώιμο εργαλείο εφάρμοσε την εντολή ufw deny 80 και κατόπιν επανακίνησε το UFW με την εντολή ufw reload.
Από την πλευρά του επιτιθέμενου εμφανίστηκαν τα παρακάτω αποτελέσματα:



Συνολικά αποστάλθηκαν 24 πακέτα στα πλαίσια της δοκιμής. Από αυτά απάντηση πήραν τα 8 πρώτα ενώ τα υπόλοιπα απορρίφθηκαν (packet loss) με την ενεργοποίηση του πρώιμου εργαλείου.

3.8 Συμπεράσματα

Σε έναν οργανισμό το Πληροφοριακό Σύστημα παίζει κομβικό ρόλο διότι διατηρεί πολύτιμα πνευματικά περιουσιακά στοιχεία καθώς και κρίσιμα δεδομένα από τη λειτουργία του που του αποδίδουν προστιθέμενη αξία. Ταυτόχρονα προσφέρει πληθώρα υπηρεσιών στα μέλη και στους εξωτερικούς συνεργάτες οι οποίες όχι μόνο συντελούν στην εύρυθμη λειτουργία αλλά προσδίδουν και συγκριτικό πλεονέκτημα απέναντι στον ανταγωνισμό. Για την ασφάλεια του Πληροφοριακού Συστήματος οι διαχειριστές έχουν πληθώρα εργαλείων. Κομβικό σημείο αποτελεί ο έγκαιρος εντοπισμός της επερχόμενης εισβολής και η απομόνωση των υπηρεσιών ή των μερών του συστήματος τα οποία παρουσιάζουν ευπάθειες και δέχονται την επίθεση. Το Snort είναι ένα εργαλείο ανοιχτού κώδικα το οποίο μπορεί να προσφέρει στη διαδικασία εντοπισμού μιας επερχόμενης επίθεσης ακόμα και αν αυτή βρίσκεται στα προκαταρκτικά στάδια εκδήλωσης της. Χάρη στην ανοιχτή αρχιτεκτονική, την πληθώρα πρόσθετων και στην ευελιξία παραμετροποίησης καθίσταται υπολογίσιμο όπλο εναντίων των κακόβουλων χρηστών. Το Snort αποτελεί τον πρώτο κρίκο μιας αλυσίδας εργαλείων που περιλαμβάνει τον εντοπισμό, την καταγραφή, την αξιολόγηση των ευρημάτων και τη λήψη αποφάσεων. Τα τελευταία χρόνια αυτή η νοητή αλυσίδα εργαλείων ανοιχτού κώδικα έχει διαταραχθεί διότι οι εφαρμογές καταγραφής και προώθησης των αποτελεσμάτων έχουν πάψει να υποστηρίζονται και να αναπτύσσονται από τους δημιουργούς τους. Τη θέση τους πήρε ένα εμπορικό προϊόν το οποίο απαιτεί συνδρομή για την εγκατάστασή του. Ακριβώς στο κενό αυτό της νοητής αλυσίδας τοποθετείται η πρώιμη εφαρμογή που αναπτύχθηκε στα πλαίσια της παρούσας μεταπτυχιακής διατριβής η οποία λαμβάνει το ρόλο να απομονώνει συγκεκριμένες υπηρεσίες ενός συστήματος όταν η αξιολόγηση των ευρημάτων δείξει ότι υπάρχει αυτή η ανάγκη.

Βιβλιογραφία

E. E. David; R. M. Fano (1965). "Some Thoughts About the Social Implications of Accessible Computing. Proceedings 1965 Fall Joint Computer Conference".
Valentino-DeVries, Jennifer; Singer, Natasha; Keller, Michael H.; Krolik, Aaron (2018-12-10). "Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret". The New York Times.
*Kang, Jerry (1998-01-01). "Information Privacy in Cyberspace Transactions". Stanford Law Review. **50** (4): 1193–1294*
Cyphers, Bennett (2019-12-02). "Behind the One-Way Mirror: A Deep Dive Into the Technology of Corporate Surveillance". Electronic Frontier Foundation
IP Addresses No Longer Protected in Alberta". Canadian Lawyer Magazine. 2020-02-11
Krishnamurthy B, Wills CE. (2009). "On the Leakage of Personally Identifiable Information Via Online Social Networks".
Edmond Lee (2011-05-06). "Sen. Rockefeller: Get Ready for a Real Do-Not-Track Bill for Online Advertising". Adage.com
"Trust and Privacy Online: Why Americans Want to Rewrite the Rules". Pew Internet & American Life Project. Released Aug. 20, 2000 Archived 2012-01-13 at the Wayback Machine
Six Common Internet Privacy Myths". Daniel Dent. 2014-10-23.
Pekala, Shayna. 2017. "Privacy and User Experience in 21st Century Library Discovery." *Information Technology and Libraries*36(2):48–58
Lenard, Thomas M. and Paul H. Rubin. 2010. "In Defense of Data: Information and the Costs of Privacy." *Policy & Internet*2(1):1–56
Ridgway, Renee. 2017. "Against a Personalisation of the Self." *Ephemera: Theory & Politics in Organization*17(2):377–97
Strahilevitz, Lior Jacob and Matthew B. Kugler. 2016. "Is Privacy Policy Language Irrelevant to Consumers?" *The Journal of Legal Studies*45(S2).
Dolin, Ron A. 2010. "Search Query Privacy: The Problem of Anonymization." *Hastings Science and Technology Law Journal*2(2):137–82.
Tene, Omer. 2008. "What Google Knows: Privacy and Internet Search Engines." *Utah Law Review*2008(4):1433–92
Duckduckgo privacy policy". https://duckduckgo.com/privacy
Wicker, Jörg and Stefan Kramer. 2017. "The Best Privacy Defense Is a Good Privacy Offense: Obfuscating a Search Engine User's Profile." *Data Mining and Knowledge Discovery*31(5):1419–43
Van Otterlo, Martijn. 2014. "Automated Experimentation in Walden 3.0. : The Next Step in Profiling, Predicting, Control and Surveillance." *Surveillance & Society* 12(2):255–72.
Naker, S., & Greenbaum, D. (2017). Now you see me: Now you still do: Facial recognition technology and the growing lack of privacy. *BUJ Sci. & Tech. L., 23*, 88
Wenyi Zhao et al., Face recognition: A literature survey. 35 ACMCOMPUTING SURVEYS(CSUR) 399 (2003)
Protiviti KnowledgeLeader, https://info.knowledgeleader.com/bid/161188/what-is-data-integrity-risk, 14/01/2020
Mihir Bellare. "Chapter 7: Message Authentication" (PDF). CSE 207: Modern Cryptography. Lecture notes for cryptography course.
"Data Origin Authentication". Web Service Security. Microsoft Developer Network.
Anthes, G. "Computer Security: Adapt or Die." ComputerWorld, January 8, 2007.
Robb, D. "Better Security Pill Gets Suite- r." Business Communications Review, October 2006

C. E. Shannon. “A Mathematical Theory of Communication,”Bell System Technical Journal27(3) pp. 379–423(July 1948).
Rhodes-Ousley, M., 2013. *Information security the complete reference*. McGraw Hill Professional.
Whitman, M.E. and Mattord, H.J., 2014. *Principles of information security*. Cengage Learning.
Kim, D. and Solomon, M.G., 2018. *Fundamentals of information systems security*. Jones & Bartlett Publishers.
Stallings, W., Brown, L., Bauer, M.D. and Bhattacharjee, A.K., 2015. *Computer security: principles and practice* (pp. 978-0). Upper Saddle River, NJ, USA: Pearson Education.
Bishop, M., 2002. Computer security: art and science.
Cheswick, W.R., Bellovin, S.M. and Rubin, A.D., 2003. *Firewalls and Internet security: repelling the wily hacker*. Addison-Wesley Professional.
Database output is dead. R.I.P., https://blog.snort.org/2012/07/database-output-is-dead-rip.html, 2012
I. Aad, J.-P. Hubaux, and E. W. Knightly. *“Denial of Service Resilience in Ad Hoc Networks,”Proceedings of theTenth Annual International Conference on Mobile Computing and Networking*pp. 202–215 (Sep. 2004)
Sample, C., and Schaffer, K. “An Overview of Anomaly Detection.” IT Pro, January/February 2013
National Institute of Standards and Technology. *Managing Information Secu-rity Risk: Organization, Mission, and Information System View*. Special Publica-tion 800-39, March 2011.
Ning, P., et al. “Techniques and Tools for Analyzing Intrusion Alerts.” *ACM Transactions on Information and System Security*, May 2004.
Andress, Jason and Steve Winterfeld. *Cyber Warfare*. Burlington, MA: Syngress Press, 2011
O’Toole, Darren. *Incident Management for IT Departments*. St. Albans, UK: Author, 2015.
Williams, Barry L. *Information Security Policy Development for Compliance*. Boca Raton, FL: CRC Press, 2013.

Παραρτήματα

```
from PyQt5 import QtCore, QtGui, QtWidgets
import sys, os

class Ui_MainWindow(object):
    def setupUi(self, MainWindow):
        MainWindow.setObjectName("MainWindow")
        MainWindow.resize(756, 237)
        self.centralwidget = QtWidgets.QWidget(MainWindow)
        self.centralwidget.setObjectName("centralwidget")
        self.gridLayout = QtWidgets.QGridLayout(self.centralwidget)
        self.gridLayout.setObjectName("gridLayout")
        self.openSSH = QtWidgets.QPushButton(self.centralwidget)
        self.openSSH.setObjectName("openSSH")
        self.gridLayout.addWidget(self.openSSH, 2, 0, 1, 1)
        self.closeSSH = QtWidgets.QPushButton(self.centralwidget)
        self.closeSSH.setObjectName("closeSSH")
        self.gridLayout.addWidget(self.closeSSH, 1, 0, 1, 1)
        self.exit = QtWidgets.QPushButton(self.centralwidget)
        self.exit.setObjectName("exit")
        self.gridLayout.addWidget(self.exit, 2, 3, 1, 1)
        self.label = QtWidgets.QLabel(self.centralwidget)
        self.label.setObjectName("label")
        self.gridLayout.addWidget(self.label, 0, 2, 1, 1)
        self.closePort80 = QtWidgets.QPushButton(self.centralwidget)
        self.closePort80.setObjectName("closePort80")
        self.gridLayout.addWidget(self.closePort80, 1, 2, 1, 1)
        self.openPort80 = QtWidgets.QPushButton(self.centralwidget)
        self.openPort80.setObjectName("openPort80")
        self.gridLayout.addWidget(self.openPort80, 2, 2, 1, 1)
        MainWindow.setCentralWidget(self.centralwidget)
        self.menubar = QtWidgets.QMenuBar(MainWindow)
        self.menubar.setGeometry(QtCore.QRect(0, 0, 756, 22))
        self.menubar.setObjectName("menubar")
        MainWindow.setMenuBar(self.menubar)
        self.statusbar = QtWidgets.QStatusBar(MainWindow)
        self.statusbar.setObjectName("statusbar")
        MainWindow.setStatusBar(self.statusbar)

        self.retranslateUi(MainWindow)
        QtCore.QMetaObject.connectSlotsByName(MainWindow)

        self.exit.clicked.connect(self.close_app)
        self.closeSSH.clicked.connect(self.closeSSH_app)
        self.openSSH.clicked.connect(self.openSSH_app)
        self.closePort80.clicked.connect(self.closePort80_app)
        self.openPort80.clicked.connect(self.openPort80_app)
```

```
    def closeSSH_app(self):
        os.system("ufw deny 22")
        os.system("ufw reload")
    def openSSH_app(self):
        os.system("ufw allow 22")
        os.system("ufw reload")
    def closePort80_app(self):
        os.system("ufw deny 80")
        os.system("ufw reload")
    def openPort80_app(self):
        os.system("ufw allow 80")
        os.system("ufw reload")
    def close_app(self):
         sys.exit()

    def retranslateUi(self, MainWindow):
        _translate = QtCore.QCoreApplication.translate
        MainWindow.setWindowTitle(_translate("MainWindow", "UFW Control Panel"))
        self.openSSH.setText(_translate("MainWindow", "Open SSH"))
        self.closeSSH.setText(_translate("MainWindow", "Close SSH"))
        self.exit.setText(_translate("MainWindow", "Exit"))
        self.label.setText(_translate("MainWindow", "                UFW Commands"))
        self.closePort80.setText(_translate("MainWindow", "Close port 80"))
        self.openPort80.setText(_translate("MainWindow", "Open port 80"))
if __name__ == "__main__":
    import sys
    app = QtWidgets.QApplication(sys.argv)
    MainWindow = QtWidgets.QMainWindow()
    ui = Ui_MainWindow()
    ui.setupUi(MainWindow)
    MainWindow.show()
    sys.exit(app.exec_())
```