ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ

ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ
ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

ΤΟΜΕΑΣ ΕΠΙΚΟΙΝΩΝΙΩΝ ΗΛΕΚΤΡΟΝΙΚΗΣ ΚΑΙ
ΣΥΣΤΗΜΑΤΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ

Ανίχνευση επιθέσεων κίνησης με μεθόδους της θεωρίας πληροφορίας. Τεχνικές ανάλυσης και ανίχνευσης για επιθέσεις DoS/DDoS στο επίπεδο εφαρμογής.

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

του

Τσακάλη Ευάγγελου

Επιβλέπων : Μιλτιάδης Αναγνώστου
Καθηγητής Ε.Μ.Π.

Αθήνα, Νοέμβριος 2023

ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ

ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ
ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

ΤΟΜΕΑΣ ΕΠΙΚΟΙΝΩΝΙΩΝ ΗΛΕΚΤΡΟΝΙΚΗΣ ΚΑΙ
ΣΥΣΤΗΜΑΤΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ

Ανίχνευση επιθέσεων κίνησης με μεθόδους της θεωρίας πληροφορίας. Τεχνικές ανάλυσης και ανίχνευσης για επιθέσεις DoS/DDoS στο επίπεδο εφαρμογής.

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

του

Τσακάλη Ευάγγελου

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή την 15 Νοεμβρίου 2023.

.....	.....	.....
Μιλτιάδης Αναγνώστου	Ευστάθιος Συκάς	Ιωάννα Ρουσσάκη
Καθηγητής Ε.Μ.Π.	Καθηγητής Ε.Μ.Π.	Αναπληρώτρια Καθηγήτρια Ε.Μ.Π.

Αθήνα, Νοέμβριος 2023

.....

Τσακάλης Ευάγγελος

Διπλωματούχος Ηλεκτρολόγος Μηχανικός και Μηχανικός Υπολογιστών Ε.Μ.Π.

Περίληψη

Στις μέρες μας, η εμφάνιση επιθέσεων κατανεμημένης άρνησης παροχής υπηρεσιών (DDoS) αποτελεί σημαντικό κίνδυνο για τη συνέχεια και την αποτελεσματικότητα των υπηρεσιών του Διαδικτύου. Αποτελούν μία από τις πιο συχνές και αποδιοργανωτικές απειλές στον κυβερνοχώρο προκαλώντας σοβαρές ζημιές τόσο στη οικονομία των οργανισμών όσο και στην αξιοπιστία τους. Σκοπός της παρούσας διπλωματικής εργασίας είναι να διερευνήσει με την χρήση της θεωρίας της πληροφορίας την ανίχνευση επιθέσεων κατανεμημένης άρνησης παροχής υπηρεσιών (DDoS) αλλά και να πραγματοποιήσει μία πολύπλευρη προσέγγιση γύρω από το πεδίο της ανίχνευσης παρεισφρήσεων, ταξινομώντας τις επιθέσεις άρνησης υπηρεσίας και τα συστήματα που χρησιμοποιούνται για την ανίχνευση και πρόληψη τους.

Η θεωρία της πληροφορίας παρέχει ένα μαθηματικό πλαίσιο για την ανάλυση της ροής της πληροφορίας στα συστήματα επικοινωνίας. Η παρούσα διατριβή διερευνά την εφαρμογή εννοιών της θεωρίας της πληροφορίας, όπως η εντροπία, για την ανίχνευση επιθέσεων άρνησης υπηρεσιών βασιζόμενη σε πραγματική καταγραφή δικτύου συναρτήσει διαφορετικών χαρακτηριστικών των πακέτων που εμπεριέχονται στην καταγραφή αυτή. Η προτεινόμενη προσέγγιση περιλαμβάνει την ανάλυση της εντροπίας της κυκλοφορίας του δικτύου και τον εντοπισμό της παρουσίας ανωμαλιών που υποδηλώνουν επίθεση με τον ορισμό κατωφλίων που κατασκευάζονται κατά την λειτουργία του δικτύου όταν αυτό δεν βρίσκεται υπό απειλή.

Γίνεται χρήση του συνόλου δεδομένων CIC-IDS2017 του καναδικού ινστιτούτου για την κυβερνοασφάλεια του πανεπιστημίου του Νιού Μπράνζουικ και η μελέτη περιλαμβάνει τόσο θεωρητικές όσο και πρακτικές πτυχές, με έμφαση στην αξιολόγηση των επιδόσεων της προτεινόμενης προσέγγισης. Τα αποτελέσματα αυτής της έρευνας θα παράσχουν πολύτιμες πληροφορίες σχετικά με την αποτελεσματικότητα της θεωρίας πληροφορίας για την ανίχνευση επιθέσεων άρνησης υπηρεσιών.

Λέξεις Κλειδιά : εντροπία, κατανεμημένες επιθέσεις άρνησης υπηρεσιών, ανίχνευση παρεισφρήσεων, ασφάλεια, ανάλυση κίνησης δικτύου

Abstract

Nowadays, the emergence of distributed denial of service (DDoS) attacks is a significant risk to the continuity and effectiveness of Internet services. They are one of the most frequent and disruptive threats in cyberspace causing serious damage to both the economy of organizations and their reliability. The aim of this thesis is to investigate the detection of distributed denial of service (DDoS) attacks using information theory and also to carry out a comprehensive approach around the field of intrusion detection, classifying denial of service attacks and the systems used to detect and prevent them.

Information theory provides a mathematical framework for analyzing the flow of information in communication systems. This thesis explores the application of information theory concepts, such as entropy, for the detection of DDoS attacks based on real network log considering different characteristics of the packets contained in the log. The proposed approach involves analyzing the entropy of network traffic and detecting the presence of anomalies indicating an attack by defining thresholds that are constructed when the network is not under threat.

Using the CIC-IDS2017 dataset from the Canadian Institute for Cyber Security at the University of New Brunswick, the study includes both theoretical and practical aspects, with a focus on evaluating the performance of the proposed approach. The results of this research will provide valuable insights into the effectiveness of information theory for detecting denial of service attacks.

Key words : entropy, distributed denial of service attacks, intrusion detection, security, network traffic analysis

Ευχαριστίες

Η παρούσα διπλωματική εργασία αποτελεί την κορύφωση των σπουδών μου στο Εθνικό Μετσόβιο Πολυτεχνείο.

Θα ήθελα να εκφράσω την ειλικρινή μου ευγνωμοσύνη στον καθηγητή Μιλτιάδη Αναγνώστου για την αμέριστη υποστήριξη, την ενθάρρυνση και τον χρόνου του καθ' όλη την διάρκεια της ασχολίας μου με ένα τόσο ενδιαφέρον αντικείμενο.

Οφείλω να ευχαριστήσω τους φίλους μου και όλους όσους με στήριξαν κατά την διάρκεια των φοιτητικών μου σπουδών. Για τις αξέχαστες στιγμές που απέκτησα και για αυτές που θα έρθουν.

Τέλος το μεγαλύτερο ευχαριστώ χρωστώ στην οικογένεια μου, στον πατέρα μου Θοδωρή, στην μητέρα μου Ελένη και στον αδερφό μου Νίκο, για την υπομονή τους, την στήριξη τους και πάνω από όλα για την αγάπη τους.

Τσακάλης Ευάγγελος
Αθήνα 2023

Περιεχόμενα

Κατάλογος Εξισώσεων

Κατάλογος Πινάκων

Κατάλογος Σχημάτων

Κατάλογος Διαγραμμάτων

Έννοιες / Ακρώνυμα

DOS (denial-of-service attack): Επίθεση άρνησης υπηρεσίας

DDOS (distributed denial-of-service): Κατανεμημένη επίθεση άρνησης υπηρεσίας

OSI (Open System Interconnection): Διασύνδεση ανοικτών συστημάτων

PLATO (Programmed Logic for Automatic Teaching Operations): Πρώτο γενικευμένο σύστημα διδασκαλίας με τη βοήθεια υπολογιστή

IRC (Internet Relay Chat): Υπηρεσία συνδιάλεξης σε πραγματικό χρόνο

UDP (User Datagram Protocol): Βασικό πρωτόκολλο Διαδικτύου

IP (Internet Protocol): Διεύθυνση διαδικτυακού πρωτοκόλλου

TTL (Time to Live): χρονικό διάστημα ύπαρξης ενός πακέτου πριν απορριφθεί από το δίκτυο

SVM (Support Vector Machine): Τεχνική κατηγοριοποίησης ονόματι μηχανή διανυσμάτων υποστήριξης

KNN (K-nearest neighbors): Τεχνική κατηγοριοποίησης ονόματι Κ-κοντινότεροι γείτονες

TCP (Transmission Control Protocol): Βασικό πρωτόκολλο διαδικτύου

SYN (Synchronisation flag): Είναι μια σημαία στο τμήμα TCP

HTTP (Hypertext Transfer Protocol): Πρωτόκολλο επικοινωνίας

HTTPS (Hypertext Transfer Protocol Secure): Ασφαλή δικτυακή σύνδεση http

ACK (Acknowledgment flag): Σημαία γνωστοποίησης επιτυχημένης παραλαβής πακέτου

NTP (Network Time Protocol): Πρωτόκολλο δικτύου για συγχρονισμό ρολογιού

SIP (Session Initiation Protocol): Πρωτόκολλο σηματοδότησης που ενεργοποιεί το πρωτόκολλο Voice Over Internet

BGP (Border Gateway Protocol): Πρωτόκολλο εξωτερικής δρομολόγησης

DNS (Domain Name System): Σύστημα Ονοματοδοσίας Διαδικτύου

SMTP (Simple Mail Transfer Protocol): Πρωτόκολλο μετάδοσης μηνυμάτων ηλεκτρονικού ταχυδρομείου

SQL (Structure Query Language): Γλώσσα υπολογιστών στις βάσεις δεδομένων

IDS (Intrusion Detection System): Σύστημα Ανίχνευσης Εισβολών

NIDS (Network-based Intrusion Detection System): Σύστημα Ανίχνευσης Εισβολών Δικτύου

HIDS (Host-based Intrusion Detection System): Σύστημα ανίχνευσης εισβολής κεντρικού υπολογιστή

PIDS (Protocol-based Intrusion Detection System): Σύστημα ανίχνευσης εισβολής βάσει πρωτοκόλλου

APIDS (Application Protocol-based Intrusion Detection System): Σύστημα ανίχνευσης εισβολής βάσει πρωτοκόλλου εφαρμογών

IPS (Intrusion Prevention System): Σύστημα Πρόβλεψης Εισβολής

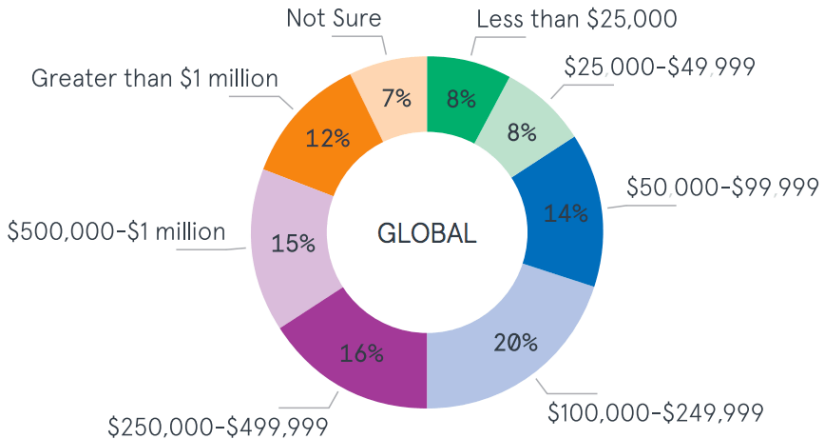
FIN (Finished – TCP flag): Υποδεικνύει το τέλος της μετάδοσης δεδομένων

RST (Reset – TCP flag): Αποστέλλεται από τον παραλήπτη στον αποστολέα όταν ένα πακέτο αποστέλλεται σε έναν συγκεκριμένο κεντρικό υπολογιστή που δεν το περίμενε.

Κεφάλαιο 1 : Εισαγωγή

1.1 Εισαγωγή

Σήμερα, σχεδόν όλοι οι εμπορικοί οργανισμοί και οι ιδιώτες εξαρτώνται από το διαδίκτυο. Από τη μία πλευρά, οι οργανισμοί το χρησιμοποιούν είτε για να προωθήσουν είτε για να παρέχουν τις υπηρεσίες τους, ενώ οι ιδιώτες το χρησιμοποιούν για την αναζήτηση και τη σύγκριση προϊόντων, τη συλλογή πληροφοριών, τις ηλεκτρονικές αγορές και την επικοινωνία με άλλους μέσω κοινωνικών δικτύων και ηλεκτρονικού ταχυδρομείου. Έτσι, το Διαδίκτυο παρέχει μια πλατφόρμα για την εκτέλεση των υπηρεσιών και την αποθήκευση ευαίσθητων πληροφοριών. Για ένα ευρύ φάσμα διαφόρων εφαρμογών και υπηρεσιών, η τεχνολογία δικτύων είναι απαραίτητη. Στα σύγχρονα δίκτυα υπάρχει χάσμα επικοινωνίας μεταξύ των προγραμματιστών δικτύων και των προγραμματιστών τεχνολογιών ασφαλείας. Σε αντίθεση με τον σχεδιασμό ασφαλών δικτύων, ο οποίος δεν είναι μια καθιερωμένη διαδικασία, ο σχεδιασμός δικτύων είναι μια αναπτυγμένη διαδικασία που έχει διάφορα προτερήματα, όπως η ευελιξία και η τυποποίηση των πρωτοκόλλων. Η πολυπλοκότητα των απαιτήσεων ασφάλειας δεν εξαρτάται από μια ειδική μεθοδολογία ή λύση. Κατά τη μεταφορά πακέτων από έναν κόμβο σε έναν άλλο κόμβο το κανάλι επικοινωνίας δεν πρέπει να είναι ευάλωτο σε επιθέσεις, οπότε η εξασφάλιση του δικτύου είναι εξίσου σημαντική με την εξασφάλιση των προσωπικών υπολογιστών.



Εικόνα 1: Μέση ωριαία απώλεια εσόδων από επιθέσεις DDoS

πηγή https://threatpost.com/ddos-attacks-can-cost-businesses-up-to-2-5m-per-attack-report-says/

Ο πιο αδύναμος κρίκος στα δικτυακά συστήματα είναι η ασφάλεια του δικτύου. Η κακόβουλη χρήση και οι επιθέσεις έχουν προκαλέσει τεράστιες απώλειες υποβαθμίζοντας τις λειτουργίες των δικτύων. Από όλες τις επιθέσεις που έχουν δημιουργηθεί και εκτελεστεί κατά καιρούς αυτές που αδιαμφισβήτητα έχουν προκαλέσει τεράστιες απώλειες είναι αυτές τις άρνησης υπηρεσιών ή κατανεμημένης άρνησης υπηρεσιών.

Οι επιθέσεις DoS και DDoS αποτελούν σήμερα την πιο συχνή πρόκληση που πρέπει να ξεπεράσουν οι υπηρεσίες διαδικτύου. Υπάρχουν πολυάριθμα εργαλεία που εκτελούν επιθέσεις άρνησης παροχής υπηρεσιών σε διακομιστές για να τους θέσουν εκτός λειτουργίας. Καθώς η τεχνολογία και οι μέθοδοι επίθεσης εξελίσσονται, η εκτέλεση αυτών των επιθέσεων γίνεται πιο απλή για τους επιτιθέμενους. Όταν πρόκειται για μεγάλα περιβάλλοντα δικτύων, γίνεται ακόμη πιο δύσκολη η ανίχνευση αυτών των επιθέσεων. Ως εκ τούτου, οι επιθέσεις αυτές έχουν εξελιχθεί σε σημαντική απειλή που κοστίζει σήμερα πολλά χρήματα στο Διαδίκτυο. Το επίπεδο μεταφοράς (Transport Layer), το επίπεδο δικτύου (Network Layer) και το επίπεδο εφαρμογής (Application Layer) είναι οι κύριοι στόχοι αυτών των επιθέσεων. Για την επίλυση αυτού του ζητήματος χρειαζόμαστε πιο προηγμένες τεχνικές για τον εντοπισμό και την άμυνα κατά αυτών των επιθέσεων. Αυτή η μελέτη παρέχει πληροφορίες σχετικά με τις στρατηγικές που έχουν τεθεί από διάφορους ερευνητές για να σταματήσουν και να προστατευτούν από επιθέσεις αυτής της φύσης. Αυτή η έρευνα επικεντρώνεται κυρίως στις επιθέσεις DDoS επιπέδου εφαρμογής και στους μηχανισμούς άμυνας τους.

1.2 Ιστορική Αναδρομή και Εξέλιξη

Πολλοί είναι αυτοί που πιστεύουν ότι η κυβερνοασφάλεια είναι μια πρόσφατη απειλή, η οποία εμφανίστηκε μόλις τα τελευταία δέκα περίπου χρόνια. Ωστόσο, η ιστορία της ασφάλειας στον κυβερνοχώρο ξεκίνησε τη δεκαετία του 1970, πολύ πριν η πλειοψηφία των ανθρώπων αποκτήσει υπολογιστές.

Η πρώτη καταγεγραμμένη κυβερνοεπίθεση μορφής άρνησης παροχής υπηρεσιών χρονολογείται στα μέσα της δεκαετίας του 70' και συγκεκριμένα το 1974 στην πολιτεία του Ιλινόις. Ο 13χρονός μαθητής David Dennis φοιτούσε στο University High School του Ιλινόις το οποίο βρισκόταν ακριβώς απέναντι από το Computer-Based Education Research Laboratory (CERL) του Πανεπιστημίου του Ιλινόις. Ο David είχε πρόσφατα μάθει για μια εντολή που μπορούσε να εκτελεστεί σε τερματικό PLATO του CERL. Στο συγκεκριμένο σύστημα η εντολή 'ext', συντομογραφία του external, χρησιμοποιούνταν για την επικοινωνία με εξωτερικές συσκευές, αλλά αν ένα σύστημα δεν ήταν συνδεδεμένο με μια εξωτερική συσκευή, τότε η εντολή 'ext' θα ανάγκαζε το σύστημα να κλείσει. Τελικά το πρόβλημα επιλύθηκε με την απενεργοποίηση της αποδοχής της εντολής "ext" από ένα απομακρυσμένο μηχάνημα.

Στα μέσα της δεκαετίας του 1990 όταν το Internet Relay Chat (IRC) απέκτησε για πρώτη φορά δημοτικότητα ορισμένοι αγωνίστηκαν για τον έλεγχο των μη εγγεγραμμένων καναλιών συνομιλίας, όπου ένας διαχειριστής χρήστης έχανε την εξουσία του αν αποσυνδεόταν. Ως αποτέλεσμα αυτής της συμπεριφοράς, οι χάκερ προσπάθησαν να αναγκάσουν τους χρήστες ενός καναλιού να αποσυνδεθούν, προκειμένου να εισέλθουν μόνοι τους στο κανάλι και να αποκτήσουν προνόμια διαχειριστή ως ο μόνος παρών χρήστης. Αυτές οι μάχες "βασιλιά του λόφου" - στις οποίες οι χρήστες προσπαθούσαν να αναλάβουν τον έλεγχο ενός καναλιού IRC και να το κρατήσουν απέναντι σε επιθέσεις από άλλους χάκερς διεξάγονταν χρησιμοποιώντας αρκετά απλές επιθέσεις άρνηση παροχής υπηρεσιών με βάση το εύρος ζώνης και πλημμύρας της συνομιλίας IRC.

Έκτοτε, το DoS αναβαθμίστηκε σε κατανεμημένο DoS ή DDoS και έγινε διαβόητο ως ένα από τα πιο καταστροφικά είδη κυβερνοεπίθεσης. Μια από τις πρώτες επιθέσεις DDoS μεγάλης κλίμακας σημειώθηκε τον Αύγουστο του 1999, όταν ένας χάκερ χρησιμοποίησε ένα εργαλείο που ονομαζόταν "Trinoo" για να θέσει εκτός λειτουργίας το δίκτυο υπολογιστών του Πανεπιστημίου της Μινεσότα για περισσότερες από δύο ημέρες. Το εργαλείο αυτό διέθετε ένα δίκτυο παραβιασμένων μηχανημάτων γνωστών ως "Masters" και "Daemons", δίνοντας στον επιτιθέμενο την δυνατότητα να στείλει μια εντολή DoS σε μερικούς Masters, τα οποία στη συνέχεια θα αναμετέδιδαν την εντολή σε εκατοντάδες Daemons για να ξεκινήσουν μια πλημμύρα UDP (UDP flood) κατά της διεύθυνσης IP του στόχου. Οι ιδιοκτήτες των δεν γνώριζαν ότι τα συστήματά τους είχαν παραβιαστεί και χρησιμοποιούνταν σε μια κατανεμημένη

επίθεση άρνηση παροχής υπηρεσιών, επειδή το εργαλείο δεν έκανε καμία προσπάθεια απόκρυψης των διευθύνσεων IP των Daemons.

Ερχόμενοι στο σήμερα, οι υπηρεσίες επιθέσεων DDoS πουλιούνται και αγοράζονται μέσω αγορών στο Darknet και το Clearnet - ένα φαινόμενο που συρρικνώνει το χάσμα μεταξύ εξειδικευμένων και ερασιτεχνών χάκερ και τροφοδοτεί μια εκθετική αύξηση των απειλών. Η αντίθεση με το παρελθόν είναι πλέον είναι χαοτική αναλογιζόμενοι ότι ένας χρήστης έχοντας ελάχιστες γνώσης περί δικτύων και προγραμματισμού υπολογιστών μπορεί να προκαλέσει καταστροφή. Ο αριθμός των δυνητικών επιτιθέμενων - και των στόχων - είναι μεγαλύτερος από ποτέ, καθώς αυξάνεται η πρόσβαση σε εργαλεία και υπηρεσίες επίθεσης.

1.3 Σχετική Βιβλιογραφία

1.3.1 Γενική σκοπιά

Έχουν γραφτεί πολυάριθμα άρθρα που συζητούν τις επιθέσεις DoS/DDoS γενικά και τις διάφορες μεθοδολογίες επιθέσεων DoS/DDoS ειδικότερα σε επίπεδο εφαρμογών (Application Layer). Κάθε μελέτη χρησιμοποιεί διαφορετική μεθοδολογία για την ανάλυση της επίθεσης και σχεδιασμού τεχνικών μετριασμού. Παρά το γεγονός ότι ορισμένες από αυτές τις μεθόδους και προτάσεις έχουν χρησιμοποιηθεί από τις εταιρείες ασφαλείας για τη μείωση των επιθέσεων, αυτού του είδους οι επιθέσεις συνεχίζουν να υπάρχουν και έχουν αρνητική επίδραση στους διαδικτυακούς πόρους και στον κυβερνοχώρο.

Υπό ένα γενικό πλαίσιο υπάρχουν δύο μέθοδοι που μπορούν να χρησιμοποιήσουν οι ομάδες ασφαλείας για να σταματήσουν ή να μειώσουν τις επιθέσεις DoS/DDoS ανάλογα με την περιοχή. Η πρώτη συζητά την εφαρμογή της τεχνικής μετριασμού τους κοντά στην πηγή της επίθεσης και η δεύτερη μιλάει για τη χρήση μιας λύσης κοντά στο στόχο της επίθεσης.

Η εφαρμογή των λύσεων κοντά στην πηγή του επιτιθέμενου θεωρείται συχνά από τους ειδικούς σε θέματα ασφάλειας ως μεγάλη πρόκληση για διάφορους λόγους. Για παράδειγμα, πώς να προβλέψει κανείς την ταυτότητα του επόμενου επιτιθέμενου. Οι επιτιθέμενοι μπορούν να στείλουν νόμιμα-έγκυρα αιτήματα που δεν μπορούν να απορριφθούν και οι περισσότερες επιθέσεις έχουν κατανεμημένη φύση, γεγονός που καθιστά την εφαρμογή οποιουδήποτε μέσου κοντά σε μία πηγή μη λειτουργική. Για αυτόν ακριβώς τον λόγο η πλειονότητα των λύσεων τοποθετούνται κοντά στον στόχο ή στα τερματικά που χρήζουν προστασία. Ωστόσο, υπάρχουν πολλές προκλήσεις και σε αυτό το σενάριο. Η δυσκολία εντοπισμού πακέτων επίθεσης αυξάνεται όσο αυξάνεται η πολυπλοκότητα της επίθεσης, ιδίως όταν οι επιτιθέμενοι χρησιμοποιούν ένα φυσιολογικό αίτημα από τους υπολογιστές των θυμάτων, δηλαδή παραβιάζουν έναν υπολογιστή για να στείλουν πακέτα επίθεσης. Αυτό κάνει την ανίχνευση πιο δύσκολη, παρόμοια με μια μάχη με έναν κρυφό εχθρό.

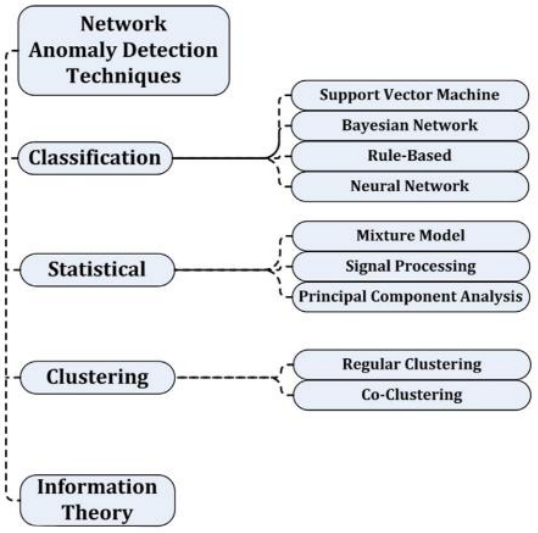
Στην έρευνα των Wang, Dunlap, Cho, & Qu (1) γίνεται αντιληπτό πως ορισμένες επιθέσεις, όπως οι επιθέσεις πλημμύρας, δεν μπορούν να αντιμετωπιστούν από την πλευρά του στόχου μόλις ξεκινήσουν, καθώς οι συσκευές θα κατακλύζονται από πακέτα επίθεσης και θα ήταν πολύ αργά για να αναλάβουν δράση σε αυτό το σημείο .

Γενικότερα, μια αμυντική απόκριση θα πρέπει να συνδυάζει όλα τα χαρακτηριστικά και τους μηχανισμούς ανίχνευσης που μπορούν να χρησιμοποιηθούν για τον εντοπισμό κακόβουλης κυκλοφορίας, όπως ο χρόνος ζωής (TTL), η διεύθυνση πλαστογραφημένων πακέτων, το μέγεθος πακέτων IP, τα πακέτα

αντανάκλασης και στην συνέχεια να προσεγγίζει την αντιμετώπιση της εκάστοτε απειλής με την κατάλληλη μεθοδολογία.

1.3.2 Τεχνικές ανίχνευσης

Πολυάριθμα βιβλία και έρευνες περιέχουν μια μεγάλη ποικιλία ερευνών σχετικά με τις μεθόδους ανίχνευσης ανωμαλιών δικτύων. Υπό το πρίσμα της ανίχνευσης ανωμαλιών οι λειτουργικές τεχνικές παρέχονται μέσω της στατιστικής ανάλυσης, της ομαδοποίησης, της θεωρίας πληροφορίας καθώς και του classification.



Εικόνα 2: Τεχνικές ανίχνευσης ανωμαλιών δικτύου

πηγή: *A survey of network anomaly detection techniques* (Ahmed, Mahmood, Hu) *(2)*

- Στατιστική Ανάλυση

Από στατιστικής πλευράς παρατηρείτε προσπάθεια δημιουργίας μοτίβων. Η μελέτη των Nooribakhsh και Mollamotalebi (3) επικεντρώθηκε σε τεχνικές για τον εντοπισμό στατιστικών ανωμαλιών στα πακέτα που λαμβάνονται για τον εντοπισμό επιθέσεων DDoS. Τα συστήματα ανίχνευσης ανωμαλιών, δημιουργούν ένα προφίλ για την κανονική συμπεριφορά της δικτυακής κίνησης. Οποιαδήποτε παραβίαση ή απόκλιση από το τυπικό προφίλ ερμηνεύεται έτσι ως ανώμαλη-ύποπτη συμπεριφορά.

- Clustering

Η ομαδοποίηση (clustering) μπορεί να χρησιμοποιηθεί ως τεχνική για την εκπαίδευση του μοντέλου κανονικότητας, όπου παρόμοια σημεία δεδομένων ομαδοποιούνται σε ομάδες χρησιμοποιώντας μια συνάρτηση απόστασης (4). Η ομαδοποίηση είναι κατάλληλη για την ανίχνευση ανωμαλιών, δεδομένου ότι δεν υπάρχει γνώση των κλάσεων επίθεσης. Στην έρευνα τους, οι Munz, Li και Carle (5) παρουσίασαν μια νέα προσέγγιση εξόρυξης δικτυακών δεδομένων που εφαρμόζει τον αλγόριθμο ομαδοποίησης K-means σε σύνολα δεδομένων χαρακτηριστικών που εξήχθησαν από αρχεία ροής. Παρατηρήθηκε πως εφαρμόζοντας τον K-means χωριστά για διαφορετικές υπηρεσίες (που προσδιορίζονται από το πρωτόκολλο μεταφοράς και τον αριθμό θύρας τους) μπορεί να επιτευχθεί σημαντική βελτίωση στην ποιότητα ανίχνευσης.

- Θεωρία Πληροφορίας

Η θεωρία της πληροφορίας είναι η επιστημονική μελέτη της ποσοτικοποίησης, της αποθήκευσης και της επικοινωνίας της πληροφορίας. Μετρικές όπως η εντροπία, η αμοιβαία, η κατευθυνόμενη πληροφορία και το κέρδος πληροφορίας (Kullback–Leibler divergence) παράγουν εν μέρει αποτελεσματικά συμπεράσματα για την συμπεριφορά του δικτύου. Και αναφέρουμε εν μέρει, καθώς η φυσιολογική κίνηση-συμπεριφορά μπορεί επίσης να αναγνωριστεί λανθασμένα ως επίθεση, με αποτέλεσμα ψευδή συναγερμό. Στην μελέτη τους οι Vitali, Villani, Spognardi, Battistoni, Mancini (6) κατάφεραν να αξιολογήσουν και να συγκρίνουν τις κύριες μετρικές παρατηρώντας πως η μέθοδος Kullback- Leibler ήταν η πιο αποτελεσματική από όλες αφού κατόρθωσε να ανιχνεύσει Dos και DDoS επίθεσης κρατώντας χαμηλά το επίπεδο ψευδών θετικών αποτελεσμάτων. Αυτό φυσικά δεν αποτελεί κανόνα καθώς τα δεδομένα μπορούν να παρουσιάζουν σοβαρές μεταβολές ως προς την συμπεριφορά και τα μοτίβα που παρέχουν. Παρατηρείται πως ανάλογα με το είδος επίθεσης ορισμένες μετρικές από αυτές που προαναφέρθηκαν μπορούν να μην δημιουργήσουν διαφοροποιήσεις που να μας οδηγήσουν σε συμπεράσματα, κάτι το οποίο θα γίνει και αντιληπτό στο πειραματικό μέρος αυτής της μελέτης.

- Classification

Η τεχνική της ταξινόμησης είναι μια μέθοδος που σχετίζεται με την κατηγοριοποίηση, την διαδικασία κατά την οποία οι έννοιες και τα αντικείμενα αναγνωρίζονται διαφοροποιούνται και κατανοούνται. Η ταξινόμηση επί της ουσίας είναι η ομαδοποίηση συναφών γεγονότων σε κατηγορίες. Υπό αυτή την λογική, στα συστήματα ανίχνευσης ανωμαλιών χρησιμοποιούνται τεχνικές ταξινόμησης όπως η μηχανή διανυσμάτων υποστήριξης SVM, τα νευρωνικά δίκτυα, ο ταξινομητής Naïve Bayes, ο αλγόριθμος Random Forest καθώς και ο K-nearest neighbors KNN.

Οι Maslan, Kamaruddin και Foozy (7) από το πανεπιστήμιο της Ινδονησίας δημιούργησαν ένα σύνολο δεδομένων περιλαμβάνοντας σύγχρονους τύπους επιθέσεων, οι οποίοι δεν είχαν συμπεριεληφθεί σε προηγούμενες μελέτες. Το σύνολο δεδομένων εκπαιδεύτηκε και δοκιμάστηκε με την χρήση τεχνικών ταξινόμησης και συμπερασματικά, πάντα για το συγκεκριμένο σύνολο δεδομένων, παρατηρήθηκε πως η Forest Random πέτυχε το υψηλότερο επίπεδο ακρίβειας.

1.4 Κίνητρο και Στόχος

Οι σημαντικότεροι παράγοντες που παρακινούν έναν ερευνητή να ολοκληρώσει τη μελέτη του σε έναν συγκεκριμένο τομέα είναι οι επίσημες στατιστικές που επιβεβαιώνουν ότι υπάρχει ανάγκη ή έλλειψη λύσεων σχετικά με τον συγκεκριμένο τομέα. Μερικές φορές είναι αναγκαίο να προσφέρονται νέες λύσεις που μπορούν να συμπληρώσουν τις παλαιότερες λύσεις λόγω της ανάπτυξης και της αυξανόμενης πολυπλοκότητας. Θεωρείται επιπλέον επιτακτική η προσέγγιση υπό ένα γενικότερο πλαίσιο που αναλύει ολοκληρωτικά το αντικείμενο καλύπτοντας όσο το δυνατό περισσότερες πτυχές του θέματος.

1.5 Περιγραφή Επόμενων Κεφαλαίων

Ο βασικός στόχος της παρούσας διπλωματικής εργασίας είναι να ακολουθήσει μια οικουμενική προσέγγιση γύρω από την ανάπτυξη τεχνικών για την ασφάλεια των δικτύων υπολογιστών στα βασικότερα επίπεδα από το οποία εκείνο απαρτίζεται. Σημαντική μνεία γίνεται στην αντιμετώπιση επιθέσεων σε επίπεδο εφαρμογής καθώς και στα συστήματα ανίχνευσης και πρόληψης παρεισφρήσεων.

Στο δεύτερο κεφάλαιο ταξινομούνται οι επιθέσεις άρνησης υπηρεσιών βάσει του μοντέλου αναφοράς Ανοικτής Διασύνδεσης Συστημάτων (OSI). Προσδιορίζονται οι όροι και οι έννοιες που απαρτίζουν τις επιθέσεις άρνησης υπηρεσιών και στην συνέχεια γίνεται αναφορά στα σημαντικότερα πρωτόκολλά που χρησιμοποιούνται κατά την διάρκεια επιθέσεων σε επίπεδο δικτύου μεταφοράς και εφαρμογών.

Στο τρίτο κεφάλαιο πραγματοποιείται εκτενής προσέγγιση γύρω από τα συστήματα και τις τεχνικές ανίχνευσης και πρόληψης παρεισφρήσεων. Αναλύονται διάφορες μεθοδολογίες σχετικά με την ανίχνευση εισβολών και οι βασικές λειτουργίες των συστημάτων πρόληψης παρεισφρήσεων. Αναφέρονται επιγραμματικά οι βασικές διαφορές μεταξύ των συστημάτων ανίχνευσης εισβολών και των συστημάτων πρόληψης εισβολών. Ολοκληρώνοντας παρουσιάζονται μηχανισμοί, μέθοδοι και τεχνικές οι οποίες χρησιμοποιούνται για την ανίχνευση παρεισφρήσεων.

Στο τέταρτο κεφάλαιο περιγράφεται ο στόχος της πειραματικής έρευνας συγκεκριμένης διπλωματικής εργασίας και η διαδικασία αναζήτησης συνόλου δεδομένων προς επεξεργασία. Παρουσιάζεται το θεωρητικό υπόβαθρο του οποίου η γνώση καθίσταται απαραίτητη για την κατανόηση της ανάλυσης καθώς και τα εργαλεία πού χρησιμοποιούνται στο πειραματικό μέρος. Επιπρόσθετα εξετάζεται η καταγραφή που θα χρησιμοποιήσουμε, το χρονοδιάγραμμα της και τα χαρακτηριστικά της. Τέλος πραγματοποιείται η πειραματική μελέτη το δεδομένων και ακολουθούν τα συμπεράσματα από την ανάλυση αυτή.

Στο πέμπτο και τελευταίο κεφάλαιο παρατίθενται τα συμπεράσματα που αντλήθηκαν από την παρούσα διπλωματική εργασία καθώς και μελλοντικές προτάσεις βελτιστοποίησης στον τομέα της ανίχνευσης παρεισφρήσεων.

Κεφάλαιο 2 : Ταξινόμηση Επιθέσεων Άρνησης Υπηρεσιών

2.1 Ορολογία Επιθέσεων Άρνησης Υπηρεσιών

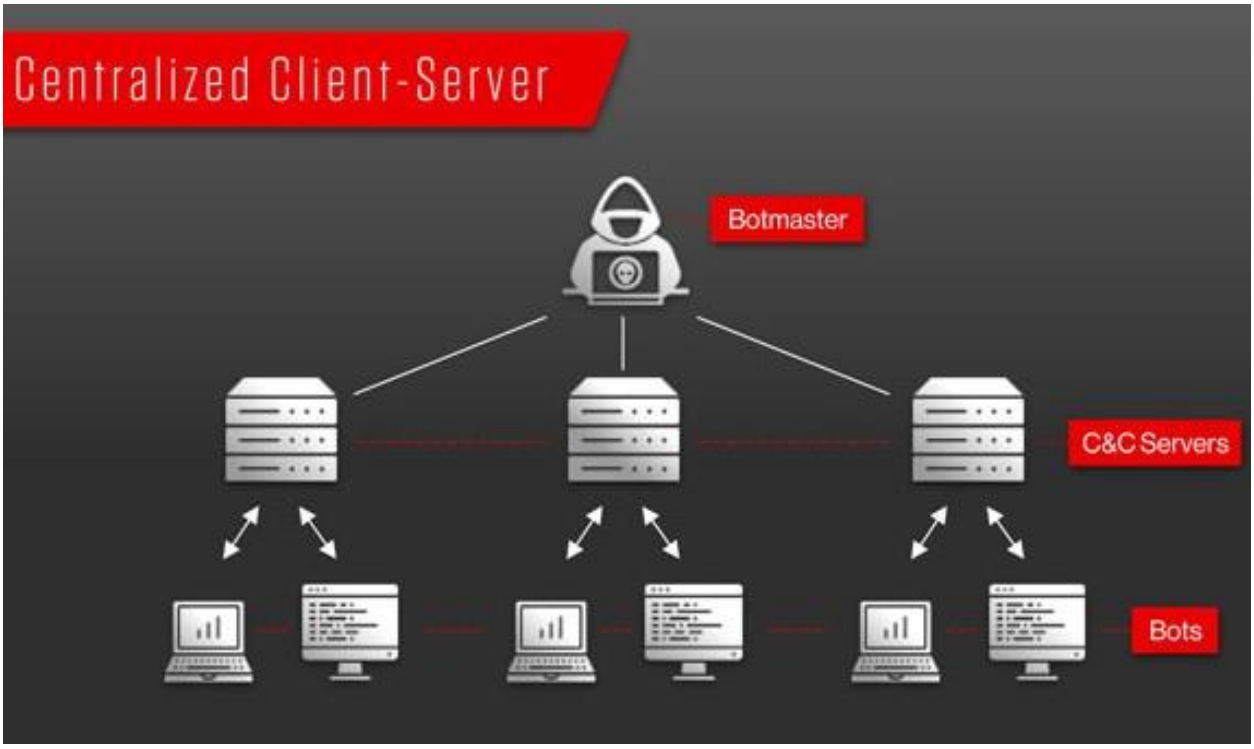
Οι επιθέσεις DoS/DDoS τροποποιούνται και ακολουθούν διαφορετικές προσεγγίσεις και μεθοδολογίες ανάλογα με την φύση του στοχευμένου θύματος. Κατά τη διάρκεια μιας επίθεσης άρνησης παροχής υπηρεσιών, στόχος μπορεί να είναι ένας διακομιστής, οι πόροι ενός δικτύου ή οποιαδήποτε άλλα τερματικά που ενδιαφέρουν τον επιτιθέμενο. Σκοπός του είναι να εμποδίσει ή να αρνηθεί στους νόμιμους πελάτες να λαμβάνουν υπηρεσίες από τους παρόχους υπηρεσιών.

Οι ειδικοί σε θέματα προστασίας έχουν πλέον προσθέσει μέτρα ασφαλείας για την αναγνώριση και την αναχαίτιση αυτών των επιθέσεων, αναγκάζοντας τους επιτιθέμενους να δημιουργήσουν εξελιγμένες μεθόδους εισάγοντας μεθοδολογίες κατανεμημένων επιθέσεων. Εκκινώντας τις επιθέσεις από διαφορετικές IP και από διαφορετικές τοποθεσίες καθιστάτε δύσκολη η ανίχνευση πακέτων επίθεσης λόγω της δυσκολίας διάκρισης μεταξύ επικίνδυνων και νόμιμων πακέτων, ειδικά όταν οι επιτιθέμενοι στέλνουν πακέτα κανονικού μεγέθους από χιλιάδες κατανεμημένες IP και τοποθεσίες. Οι επιτιθέμενοι δεν χρειάζεται να χρησιμοποιούν εκατοντάδες μηχανήματα για να διεξάγουν επιθέσεις εξάπλωσης. Το μόνο που χρειάζεται να κάνουν είναι να αναζητήσουν υπολογιστές, δίκτυα ή άλλους πόρους του διαδικτύου που διαθέτουν αδύναμα συστήματα και στη συνέχεια να επιστρατεύσουν αυτά τα συστήματα για να εργαστούν για τους διακομιστές εντολών τους. Μόλις ολοκληρωθεί αυτό, τα ελεγχόμενα, στρατολογημένα ή μολυσμένα μηχανήματα θα είναι έτοιμα να λάβουν μέρος και να χρησιμεύσουν ως πρωταγωνιστές στην επερχόμενη επίθεση. Οι μολυσμένοι υπολογιστές φέρουν διάφορα ονόματα, όπως bot, zombie και botnet.

Το "Bot" είναι μια συντομογραφία για το ρομπότ. Ένα bot ή ζόμπι είναι ένας υπολογιστής στον οποίο έχει εγκατασταθεί κακόβουλο λογισμικό, το οποίο συνήθως αναφέρεται ως δούρειος ίππος και το οποίο λειτουργεί με σκοπό την εξάντληση των πόρων ενός μηχανήματος. Η χρήση εκατοντάδων υπολογιστών εξελίσσει και κάνει αποτελεσματικότερη την επίθεση δίνοντας επίσης μεγαλύτερη διάρκεια συγκριτικά με την επίθεση από ένα και μόνο υπολογιστή. Ένα botnet είναι η συλλογική ονομασία για όλους αυτούς τους πόρους και όλοι όσοι συμμετέχουν στην επίθεση είναι δύσκολο να εντοπιστούν γρήγορα συγκριτικά με την ύπαρξη ενός και μόνο μηχανήματος.

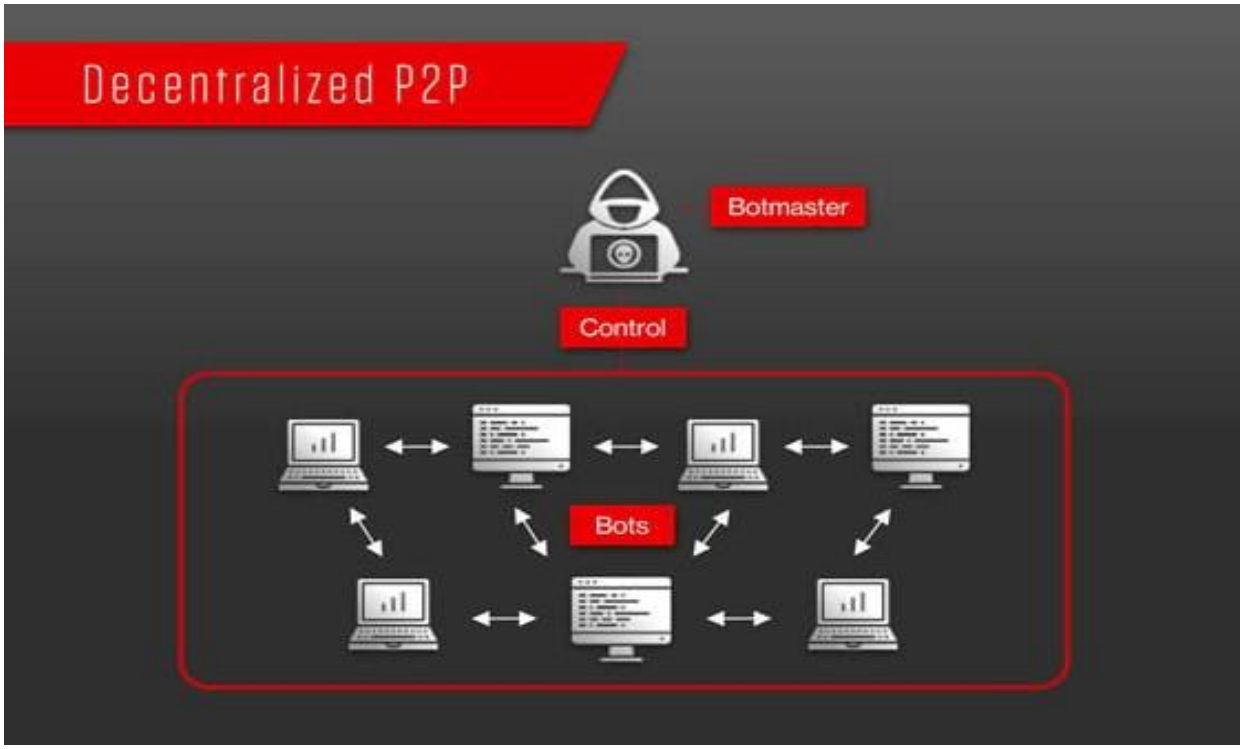
Ένα κέντρο ελέγχου και διοίκησης (C & C center), είναι μια μηχανή ή ένας διακομιστής που ενεργεί ως master ή διοικητής για τους slaves (υπολογιστές) ή τους στρατολογητές, που αντιπροσωπεύονται από bots ή botnets οι οποίοι είναι υπολογιστές που έχουν ήδη μολυνθεί με κακόβουλο λογισμικό,

χρησιμοποιώντας συγκεκριμένα σενάρια για έναν ή περισσότερους τύπους επιθέσεων άρνησης υπηρεσιών. Για να συνδεθούν με τα botnets τους, τα κέντρα C&C χρησιμοποιούν διάφορες μεθόδους, όπως το IRC (Internet Relay Chat), το πρόγραμμα περιήγησης Tor, το Facebook και άλλα. Σε αυτά τα κέντρα χρησιμοποιούνται διαφορετικές προσεγγίσεις σχεδιασμού, διαχείρισης και επικοινωνίας. Με μια διαμόρφωση αστέρα, όλοι οι σταθμοί εργασίας είναι φυσικά συνδεδεμένοι μεταξύ τους, ενώ ένας μοναδικός κεντρικός διακομιστής διαχειρίζεται εύκολα και αξιόπιστα ολόκληρο το botnet. Σε έναν σχεδιασμό τοπολογίας C&C, πολλαπλοί διακομιστές συνδέονται μεταξύ τους και λειτουργούν ως εφεδρείες ή εφεδρικά αντίγραφα ο ένας για τον άλλο. Ο σχεδιασμός αυτής της τοπολογίας εξαλείφει την εξάρτηση από έναν μόνο διακομιστή, ενώ ταυτόχρονα αυξάνει την πολυπλοκότητα με περισσότερα χαρακτηριστικά. Εάν, για οποιονδήποτε λόγο, ένας από τους διακομιστές εντοπιστεί, ο επιτιθέμενος δεν θα χάσει τον πλήρη έλεγχο.



Εικόνα 3: Κεντρικοποιημένο μοντέλο botnet

πηγή: https://www.crowdstrike.com/cybersecurity-101/botnets/



Εικόνα 4: Αποκεντρωμένο μοντέλο botnet

πηγή: https://www.crowdstrike.com/cybersecurity-101/botnets/

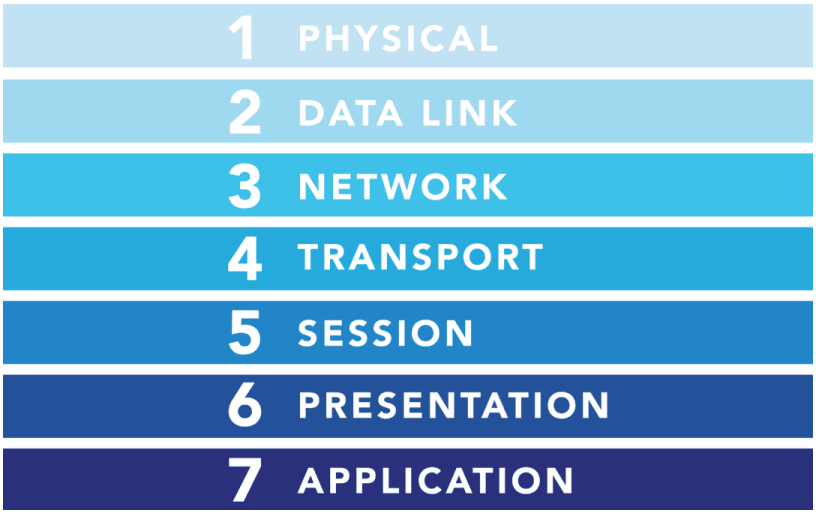
Η σύνδεση μεταξύ των επιπέδων ή των ιεραρχικών διακομιστών είναι βασισμένη σε επίπεδα, οπότε όταν ο κύριος διακομιστής θέλει να μεταδώσει ένα αίτημα, δεν θα την στέλνει απευθείας στα bot- αντίθετα, θα την στέλνει, για παράδειγμα, σε έναν άλλο διακομιστή, ο οποίος στη συνέχεια θα την στέλνει στα bots. Με αυτόν τον τρόπο, ο επιτιθέμενος προστατεύει τον εαυτό του. Αν όμως ποτέ βρεθεί ο διακομιστής που εκδίδει εντολές ή εντολές προς τα bots, ο επιτιθέμενος δεν θα χάσει, όπως αναφέρθηκε προηγουμένως, κάθε έλεγχο, αλλά αντίθετα μπορεί να επιλέξει έναν νέο διακομιστή και να ξεκινήσει από την αρχή.

Το τελευταίο συστατικό αυτής της διαδικασίας ονομάζεται κερκόπορτα (backdoor), η οποία είναι ένα λογισμικό ή ένα χαρακτηριστικό που επιτρέπει στο διαχειριστή του συστήματος να συνδεθεί και να εκτελέσει διαγνωστικές λειτουργίες στο σύστημα του υπολογιστή. Από τη σκοπιά του επιτιθέμενου, προσφέρει μια απλή τεχνική για να εισέλθει και να εκμεταλλευτεί τον υπολογιστή του θύματος προκειμένου να αναλάβει τον έλεγχό του. Τα backdoors μπορεί περιστασιακά να είναι σφάλματα λογισμικού που γνωρίζει ο προγραμματιστής του συστήματος αλλά δεν γνωρίζει ο αγοραστής του συστήματος.

Συμπληρωματικά, το κακοήθες λογισμικό που έχει εγκατασταθεί από επιτιθέμενους με κακόβουλη πρόθεση είναι μια άλλη μορφή κερκόπορτας. Όταν ο επιτιθέμενος παραβιάζει οποιονδήποτε υπολογιστή,

περνάει από πολλαπλά στάδια παραβίασης μέχρι να αποκτήσει πλήρη πρόσβαση και έλεγχο, οπότε αν ο επιτιθέμενος χάσει τη σύνδεσή του για οποιονδήποτε λόγο ή αν ένας γνήσιος χρήστης αλλάξει μια ρύθμιση, ο επιτιθέμενος θα χάσει την πρόσβασή του, αν δεν δημιούργησε ή δεν εγκατέστησε μια κερκόπορτα. Μια κερκόπορτα παίζει τον σημαντικό ρόλο της υποστήριξης των σταδίων επίθεσης, δίνοντας στον επιτιθέμενο γρήγορη και εύκολη πρόσβαση στον υπολογιστή του θύματος, εξοικονομώντας του πολύ χρόνο. Στις μέρες μας, υπάρχουν πολλοί τύποι backdoors, όπως ένα Trojan backdoor, το οποίο αποτελεί και την πιο συνηθισμένη μορφή και επιτρέπει σε έναν επιτιθέμενο να αποκτήσει πρόσβαση σε ένα σύστημα υπολογιστή και να κλέψει τα δεδομένα του χρήστη, καθώς να κατεβάσει και να εγκαταστήσει κακόβουλο λογισμικό για να δημιουργήσει τη δική του κερκόπορτα, η οποία του επιτρέπει να αποκτήσει πλήρη απομακρυσμένο έλεγχο του υπολογιστή ή των υπολογιστών του θύματος.

Οι επιθέσεις κατανεμημένης άρνησης υπηρεσίας μπορούν να ταξινομηθούν με βάση το μοντέλο OSI που δέχεται την επίθεση. Με την κατηγοριοποίηση των επιθέσεων με βάση το επίπεδο OSI, μπορούμε να κατανοήσουμε καλύτερα τη φύση της επίθεσης και να προσδιορίσουμε τι χρειάζεται για την αποτροπή ή τον μετριασμό της.



Εικόνα 5: Μοντέλο αναφοράς OSI

πηγή: https://www.polymerhq.io/blog/cloud-security/post-what-is-the-osi-model/

2.2 Επιθέσεις Άρνησης Υπηρεσιών Επιπέδου 3 (Network Layer)

2.2.1 Σχετικά Πρωτόκολλα

Σε αυτόν τον τύπο επίθεσης DoS/DDoS, το επίπεδο δικτύου είναι ο επιδιωκόμενος στόχος και χρησιμοποιούνται συχνότερα τα παρακάτω πρωτόκολλα:

- **IP:** Τα πακέτα δεδομένων δρομολογούνται μέσω του πρωτοκόλλου Διαδικτύου (IP), ώστε να φτάνουν στην επιθυμητή τοποθεσία. Κάθε συσκευή που συνδέεται στο Διαδίκτυο έχει μια διεύθυνση IP και κάθε πακέτο δεδομένων λαμβάνει τη σωστή διεύθυνση IP μέσω του πρωτοκόλλου IP.
- **IPsec:** Το IPsec είναι μια ομάδα πρωτοκόλλων και όχι ένα ενιαίο πρωτόκολλο. Ισχύει παρόμοια διάκριση μεταξύ HTTPS και HTTP, το IPsec είναι η κρυπτογραφημένη εκδοχή του IP.
- **ICMP:** Το ICMP χρησιμοποιείται κυρίως από δικτυακά λειτουργικά συστήματα υπολογιστών για την κοινοποίηση μηνυμάτων σφάλματος, όπως αυτά που υποδεικνύουν τη μη διαθεσιμότητα ενός διακομιστή ή την εξαφάνιση ενός μηχανήματος από το δίκτυο.

Ο επιτιθέμενος χρησιμοποιεί αυτά τα πρωτόκολλα για να παραδώσει άφθονες ποσότητες ανεπιθύμητης δικτυακής κίνησης, όπως συμβαίνει και σε άλλα είδη επιθέσεων άρνησης υπηρεσιών. Υπάρχουν πολλοί τύποι επιθέσεων σε αυτό το επίπεδο, αλλά σε αυτή την ενότητα θα καλυφθούν δύο από τις πιο συνηθισμένες επιθέσεις για να αποσαφηνιστεί η γενική ιδέα: η επίθεση "Ping of Death" και "Smurf".

2.2.2 Επίθεση Ping of Death

Στην επίθεση ping of death οι επιτιθέμενοι μεταδίδουν τροποποιημένα πακέτα που είναι μεγαλύτερα από το συνηθισμένο μέγεθος για πακέτα IP, το οποίο είναι 65.535 bytes. Το σύνολο πρωτοκόλλων TCP/IP παρέχει μια λειτουργία που τους επιτρέπει να διαχωρίζει πακέτα στο άκρο αποστολής και στη συνέχεια να τα συνδυάζει στο άκρο λήψης. Πολλά συστήματα δεν μπορούν να χειριστούν πακέτα αυτού του μεγέθους και θα κατέρρεαν ή θα πάγωναν αν λάμβαναν κάτι μεγαλύτερο από το τυπικό μέγεθος του πακέτου, επομένως ο επιτιθέμενος χρησιμοποιεί αυτή τη δυνατότητα για να τροποποιήσει το μέγεθος και να πραγματοποιήσει τις επιθέσεις του. Αυτού του είδους τα πακέτα αντιμετωπίζονται από διάφορους διακομιστές, τείχη προστασίας και συσκευές δικτύου χρησιμοποιώντας διάφορες προσεγγίσεις (8).

Οι περισσότεροι επιτιθέμενοι DoS/DDoS πρέπει να γνωρίζουν πολλές πληροφορίες σχετικά με τον στόχο για να ανακαλύψουν πώς οι ιδιοκτήτες του συστήματος κατασκεύασαν το σύστημά τους και τα χαρακτηριστικά που διαθέτει το σύστημα. Με την προαναφερθήσα επίθεση, ο κακόβουλος χρήστης αρκεί

να γνωρίζει τη διεύθυνση πρωτοκόλλου του στόχου του - δεν απαιτούνται περαιτέρω πληροφορίες. Επιπλέον, ο επιτιθέμενος μπορεί εύκολα να έχει παραποιήσει οποιαδήποτε IP πηγής για να εκτελέσει την επίθεσή του, γεγονός που την καθιστά πολύ δύσκολο να εντοπιστεί ή να ανακαλυφθεί.

2.2.3 Επίθεση Smurf

Για να πραγματοποιηθούν επιθέσεις κατανεμημένης (ή μη) άρνησης παροχής υπηρεσιών τύπου Smurf οι επιτιθέμενοι χρησιμοποιούν το Πρωτόκολλο Μηνυμάτων Ελέγχου Διαδικτύου (ICMP). Σε μια τυπική κατάσταση, ο πελάτης στέλνει ένα αίτημα echo σε άλλους πελάτες για να ελέγξει τη συνδεσιμότητα ή την καθυστέρηση της υπηρεσίας. Στην επίθεση Smurf, οι επιτιθέμενοι δημιουργούν το δικό τους αίτημα χρησιμοποιώντας κακόβουλο λογισμικό και το στέλνουν στη διεύθυνση IP εκπομπής του στοχευμένου δικτύου με μια πλαστή IP, τη διεύθυνση IP του θύματος. Με άλλα λόγια, ο επιτιθέμενος θα κάνει ping σε κάθε διακομιστή και τερματικό σε ένα δίκτυο. Αυτοί οι πόροι πληροφορικής θα μπορούσαν να είναι διακομιστές ή συσκευές συνδεδεμένες στο ενεργό δίκτυο. Η χρήση αυτής της μεθοδολογίας θα ενισχύσει το μέγεθος της επίθεσης με τον αριθμό των πελατών που θα λάβουν το αίτημα. Μόλις οι κεντρικοί υπολογιστές αρχίσουν να ανταποκρίνονται στα ερωτήματα, αναζητούν τη διεύθυνση IP προέλευσης του πακέτου, η οποία συχνά είναι η διεύθυνση IP του διακομιστή του θύματος. Ως αποτέλεσμα, κάθε κεντρικός υπολογιστής που λαμβάνει ένα αίτημα echo θα απαντήσει στο θύμα με μια απάντηση echo, πλημμυρίζοντας το θύμα.

2.3 Επιθέσεις Άρνησης Υπηρεσίας Επιπέδου 4 (Transport Layer)

2.3.1 Σχετικά πρωτόκολλα

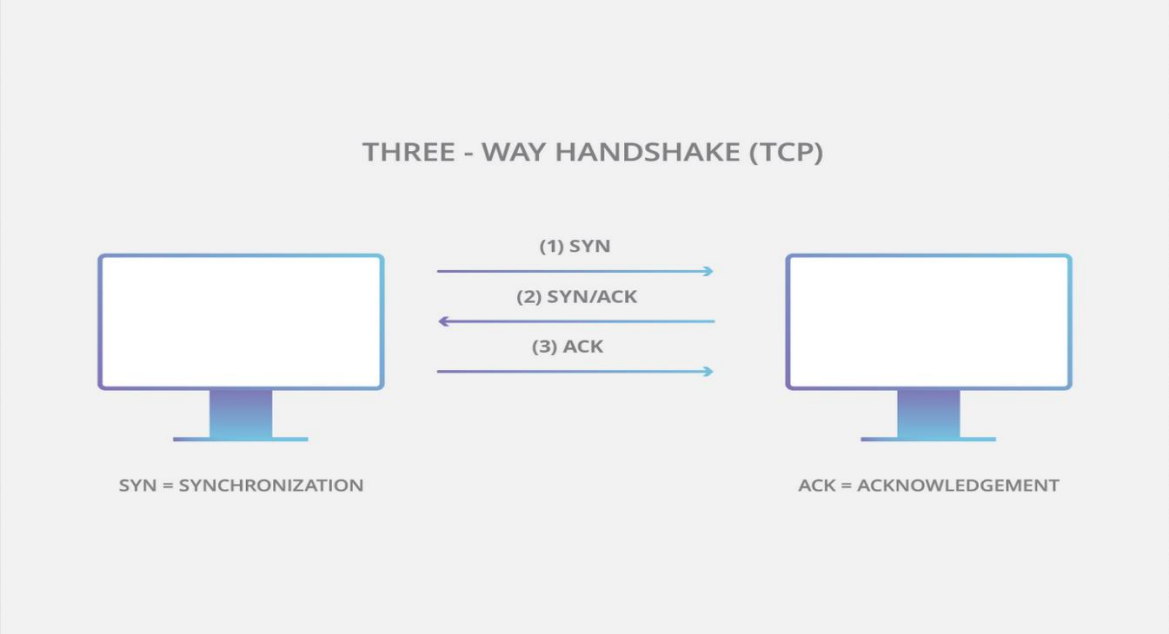
Σε αυτή τη βαθμίδα, οι επιθέσεις DoS/DDoS είναι πιο πιθανό να στοχεύουν μια συγκεκριμένη υπηρεσία παρά έναν μεμονωμένο κεντρικό υπολογιστή. Σε αντίθεση με το επίπεδο 3, το επίπεδο 4 διαθέτει μόνο δύο αξιοσημείωτα πρωτόκολλα:

- **TCP:** Η δικτυακή επικοινωνία μεταξύ των εφαρμογών εγκαθίσταται και διατηρείται σύμφωνα με το πρότυπο TCP. Το TCP συνεργάζεται με το Πρωτόκολλο Διαδικτύου (IP), το οποίο ορίζει τον τρόπο με τον οποίο οι υπολογιστές στέλνουν πακέτα δεδομένων μεταξύ τους. Μαζί, το TCP και το IP αποτελούν τους βασικούς κανόνες που καθορίζουν το διαδίκτυο.
- **UDP:** Το UDP είναι υπεύθυνο για χρονικά κρίσιμη μεταφορά δεδομένων όπως αναζητήσεις DNS, διαδικτυακά παιχνίδια και ροή βίντεο. Εξαλείφοντας την απαίτηση για επίσημη αμφίδρομη σύνδεση πριν από την έναρξη της μετάδοσης δεδομένων, αυτό το πρωτόκολλο επικοινωνίας αυξάνει τις ταχύτητες μεταφοράς. Ωστόσο, μπορεί επίσης να οδηγήσει σε απώλεια πακέτων κατά τη μεταφορά, ανοίγοντας την πόρτα για επιθέσεις άρνησης υπηρεσίας και άλλες μορφές εκμετάλλευσης.

Αυτή η ενότητα καλύπτει τις πιο συνηθισμένες επιθέσεις σε αυτό το επίπεδο.

2.3.2 Επίθεση Άρνησης Υπηρεσιών SYN

Στις επιθέσεις SYN αξιοποιείται η "χειραψία τριών κατευθύνσεων" (3-way handshake), μια τυπική διαδικασία του πρωτοκόλλου TCP για την εγκαθίδρυση μιας σύνδεσης μεταξύ δύο μηχανημάτων ή δύο πελατών. Με μια τυπικά ψεύτικη διεύθυνση IP, ο δράστης στέλνει ερωτήματα TCP SYN σε όλες τις θύρες των διακομιστών. Ο διακομιστής απαντά με το SYN-ACK και περιμένει την τελευταία απάντηση για να δημιουργήσει μια σύνδεση που δεν θα έρθει ποτέ. Με την αποστολή εκατοντάδων τέτοιων αιτήσεων, οι επιτιθέμενοι εξαντλούν τους πόρους του διακομιστή. Προκειμένου να διατηρήσει τον διακομιστή ενεργό και το buffer αιτήσεων γεμάτο, ο επιτιθέμενος θα προσπαθήσει ουσιαστικά να εξαντλήσει τους πόρους του θύματος περιμένοντας την περίοδο timeout του TCP προτού στείλει άλλο ένα αίτημα. Σε αυτή την περίπτωση, ο διακομιστής δεν μπορεί να δεχτεί άλλες κανονικές-νόμιμες αιτήσεις. Το buffer του διακομιστή του θύματος διατηρείται συνήθως σχεδόν γεμάτο από τους επιτιθέμενους, οι οποίοι χρησιμοποιούν περιορισμένα σενάρια που έχουν ρυθμιστεί ώστε να στέλνουν αιτήσεις σε χρόνους που καθορίζονται από τα χρονικά όρια των αιτήσεων (9).



Εικόνα 6: Εγκαθίδρυση σύνδεσης TCP με διαδικασία χειραψίας

πηγή: *https://www.cloudflare.com/learning/ddos/syn-flood-ddos-attack/*

2.3.3 Επίθεση Πλημμύρας SYN-ACK

Οι επιθέσεις πλημμύρας στοχεύουν στην άρνηση υπηρεσιών. Ο επιτιθέμενος υπερφορτώνει το σύστημα στέλνοντας μεγάλο όγκο πακέτων με υψηλό ρυθμό . Έτσι καθίσταται αδύνατο να εξεταστούν όλα τα αιτήματα και το σύστημα αδυνατεί να εξυπηρετήσει. Στην συγκεκριμένη περίπτωση ο επιτιθέμενος στέλνει ένα αίτημα SYN με ψεύτικη IP σε ανοιχτούς διακομιστές proxy διακομιστές και άλλους πόρους που υπάρχουν σε διαθεσιμότητα στο διαδίκτυο. Ακόμη, τροποποιεί κακόβουλα τους παραμέτρους ορισμένων εξ αυτών των πόρων ώστε να ανταποκρίνονται σε οποιοδήποτε αίτημα. Ο λόγος που γίνεται αυτό είναι πως είναι προφανές ,καθώς ακολουθείται η φυσιολογική διαδικασία εγκαθίδρυσης σύνδεσης μέσω TCP . Λόγω του μέτριου μεγέθους τους, του χαμηλού όγκου τους και άλλων φαινομενικά τυπικών απαιτήσεων, αυτά τα απλά αιτήματα μπορούν εύκολα να παρακάμψουν κάθε μέτρο ασφαλείας.

Οι ανοιχτοί πόροι που λαμβάνουν το αίτημα θα αναζητήσουν την διεύθυνση IP της πηγής και θα απαντήσουν σε αυτήν την πηγή που στην προκειμένη περίπτωση είναι του θύματος με συνέπεια να το πλημμυρήσουν. Αυτοί οι δημόσια προσβάσιμοι διακομιστές ενδέχεται να δημιουργήσουν δεκάδες χιλιάδες απαντήσεις για το στοχευμένο θύμα, κρατώντας τους πολύ απασχολημένους για να δεχτούν νόμιμα αιτήματα.

2.3.4 Επίθεση NTP

Το Network Time Protocol είναι ένα πρωτόκολλο Διαδικτύου που χρησιμοποιείται για τον συγχρονισμό των ρολογιών των υπολογιστών με κάποια χρονική αναφορά. Στην επίθεση ενίσχυσης NTP γίνεται εκμετάλλευση της διαφοράς στο κόστος εύρος ζώνης μεταξύ του επιτιθέμενου και του στοχευμένου πόρου. Ορισμένες εκδόσεις NTP ενδέχεται να εκτελούν επιπλέον λειτουργίες παρακολούθησης, γεγονός που επιτρέπει στους διαχειριστές να λάβουν μια λίστα με τους τελευταίους 600 κεντρικούς υπολογιστές που συνδέθηκαν σε έναν συγκεκριμένο ζωντανό διακομιστή.

Αυτό το πρωτόκολλο είναι μέλος της οικογένειας UDP, επομένως είναι ένα πρωτόκολλο χωρίς σύνδεση. Διαθέτει την εσωτερική εντολή "monlist" που μπορεί να χρησιμοποιηθεί για μια ποικιλία λειτουργιών, συμπεριλαμβανομένης της παρακολούθησης. Οι επιτιθέμενοι μπορούν να την αξιοποιήσουν στέλνοντας την στον διακομιστή NTP, με στόχο να αποκτήσουν τις λίστες του διακομιστή που είναι συγχρονισμένες με αυτόν. Ο διακομιστής NTP θα ανταποκριθεί σε αυτήν την εντολή με μια λίστα IP διακομιστών και συσκευών, η οποία μπορεί να περιλαμβάνει έναν αρκετά μεγάλο αριθμό διευθύνσεων πρωτοκόλλου που έχει συγχρονίσει αυτός ο διακομιστής NTP με το επιδιωκόμενο θύμα.

Ο επιτιθέμενος έχει την δυνατότητα να στέλνει, μέσω μια ψεύτικης διεύθυνσης πρωτοκόλλου, επανειλημμένα αυτό το είδους αίτησης σε έναν διακομιστή NTP ο οποίος θα αποκριθεί στην διεύθυνση προέλευσης που στην προκειμένη περίπτωση ανήκει στο θύμα. Αυτά τα αιτήματα κατακλύζουν το θύμα με πακέτα UDP που είναι σημαντικά περισσότερα από τα αρχικά αιτήματα που αποστέλλονται.

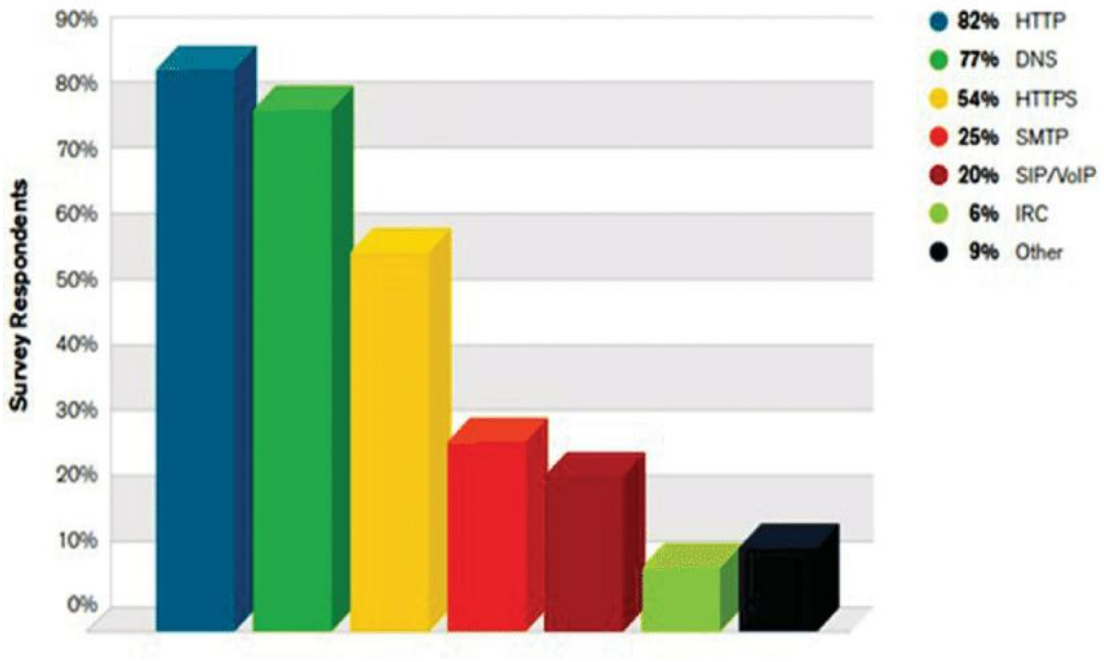
2.4 Επιθέσεις Άρνησης Υπηρεσιών Επιπέδου 7 (Application Layer)

2.4.1 Σχετικά Πρωτόκολλα

Οι επιθέσεις στο "ανώτερο" επίπεδο του μοντέλου OSI, όπου πραγματοποιούνται τυπικά αιτήματα στο διαδίκτυο, όπως HTTP GET και HTTP POST, αναφέρονται ως επιθέσεις επιπέδου εφαρμογής ή επιθέσεις κατανεμημένης άρνησης υπηρεσιών εβδόμου επιπέδο. Οι επιθέσεις σε αυτό το επίπεδο στοχεύουν εφαρμογές και συγκεκριμένα τρωτά σημεία ή παθογένειες με σκοπό την αδρανοποίηση και την στέρηση παροχής επικοινωνίας και παράδοσης περιεχομένου στους χρήστες. Οι εφαρμογές που συνήθως αποτελούν στόχο είναι διακομιστές ιστού, αλλά μπορεί επίσης να είναι υπηρεσίες φωνής SIP και υπηρεσίες εξωτερικής δρομολόγησης BGP.

Λόγω της φύσης του επιπέδου εφαρμογών τα βασικά πρωτόκολλα που χρησιμοποιούνται είναι τα παρακάτω:

- **HTTP:** Το πρωτόκολλο μεταφοράς υπερκειμένου αποτελεί την ραχοκοκαλιά του παγκοσμίου ιστού και είναι υπεύθυνο για την φόρτωση ιστοσελίδων μέσω συνδέσμων υπερκειμένου. Είναι σχεδιασμένο να μεταφέρει πληροφορίες μεταξύ δικτυακών συσκευών και εκτελείται πάνω από άλλα επίπεδα της στοίβας πρωτοκόλλων δικτύου.
- **DNS:** Το σύστημα ονοματοδοσίας DNS είναι ένα ιεραρχικό σύστημα που μετατρέπει τα ονόματα των ιστοτόπων σε μορφή διεύθυνσης πρωτοκόλλου IPv4 ώστε να μπορούν να βρεθούν και να φορτωθούν στο πρόγραμμα περιήγησης.
- **HTTPS:** Ίδιο πρωτόκολλο με το HTTP με την διαφορά πως παρέχει δικλείδες ασφαλείας μέσω κρυπτογράφησης και επαλήθευσής.
- **SMTP:** Το SMTP είναι ένα πρωτόκολλο μεταφοράς που επιτρέπει στους διακομιστές αλληλογραφίας να στέλνουν και να λαμβάνουν μηνύματα.



Εικόνα 7: Στόχοι επίθεσης στο επίπεδο εφαρμογων

πηγή: *https://www.researchgate.net/figure/Most-common-protocols-targeted-for-application-layer-attacks_fig3_309100353*

Οι επιθέσεις στο επίπεδο εφαρμογής δεν στοχεύουν στο εύρος ζώνης του δικτύου. Αντίθετα, επιτίθενται στο πρόγραμμα που παρέχει την υπηρεσία την οποία προσπαθούν να χρησιμοποιήσουν οι πελάτες. Για να γίνει αυτό, οι κύριοι στόχοι είναι ο διακομιστής, η εφαρμογή διακομιστή και οι πόροι back-end. Αυτές οι επιθέσεις αποσκοπούν στην αποστράγγιση των πόρων μιας υπηρεσίας, είτε επιβραδύνοντας την είτε σταματώντας την εντελώς.

2.4.2 Επίθεση Slowloris

Η εφαρμογή Slowloris είναι ένα είδος επίθεσης άρνησης παροχής υπηρεσιών που επινοήθηκε από τον Robert Hansen. Ο επιτιθέμενος στέλνει μερικά-ημιτελή αιτήματα HTTP στον εκάστοτε στοχευμένο διακομιστή και εν συνεχεία διατηρεί αυτές τις συνδέσεις ανοιχτές για όσο το δυνατό μεγαλύτερο χρονικό διάστημα.

Το συγκεκριμένο εργαλείο επιτρέπει σε ένα μόνο μηχάνημα να καταρρίψει τον διακομιστή ιστού ενός άλλου μηχανήματος με ελάχιστο εύρος ζώνης και παρενέργειες σε άσχετες υπηρεσίες και θύρες. Σε αντίθεση με τις επιθέσεις άρνησης υπηρεσίας που καταναλώνουν εύρος ζώνης, όπως για παράδειγμα στην επίθεση Network Time Protocol που αναφέρθηκε στην υποενότητα 2.3.4, αυτή η μέθοδος χρησιμοποιεί χαμηλό εύρος ζώνης και αντ' αυτού προσπαθεί να εξαντλήσει τους πόρους του διακομιστή στέλνοντας αιτήματα που φαίνονται να διακινούνται αργά αλλά συμπεριφέρονται κανονικά. Συνήθως

υπάρχει περιορισμένος αριθμός νημάτων στον στοχευμένο διακομιστή για τη διαχείριση πολλών συνδέσεων ταυτόχρονα. Η αργή αίτηση δεν θα ολοκληρωθεί ποτέ, επομένως κάθε νήμα του διακομιστή θα καταβάλλει προσπάθεια να συνεχίσει να εκτελείται ενώ περιμένει. Κάθε επόμενη σύνδεση δεν θα απαντηθεί αφού επιτευχθεί ο μέγιστος αριθμός συνδέσεων του διακομιστή, με αποτέλεσμα την άρνηση παροχής υπηρεσιών.

Η διαδικασία της εκτέλεσης ακολουθεί τα εξής βήματα :

1. Ο επιτιθέμενος δημιουργεί αρχικά πολλαπλές συνδέσεις με τον διακομιστή που δέχεται την επίθεση στέλνοντας πολλές μερικές-ελλιπείς επικεφαλίδες αίτησης HTTP.
2. Για κάθε εισερχόμενη αίτηση, ο στόχος δημιουργεί ένα νήμα, με σκοπό να τερματίσει το νήμα μετά την εγκαθίδρυση της σύνδεσης. Εάν η δημιουργία μιας σύνδεσης διαρκεί πολύ για λόγους αποδοτικότητας, ο διακομιστής θα τερματίσει τη σύνδεση, ανοίγοντας το νήμα για την επόμενη αίτηση.
3. Για να διασφαλίσει ότι ο στόχος δεν θα τερματίσει την σύνδεση, ο επιτιθέμενος στέλνει περιοδικά νέες μερικές-ελλιπείς επικεφαλίδες αίτησης HTTP.
4. Ενώ περιμένει το τέλος της αίτησης, ο στοχευόμενος διακομιστής δεν είναι ποτέ σε θέση να κλείσει καμία από τις ανοικτές μερικές συνδέσεις. Όταν χρησιμοποιηθούν όλα τα διαθέσιμα νήματα, θα προκύψει άρνηση παροχής υπηρεσιών, καθώς ο διακομιστής δεν θα είναι σε θέση να χειριστεί άλλα αιτήματα από τη συνήθη κυκλοφορία.

2.4.3 Επίθεση πλημμύρας HTTP

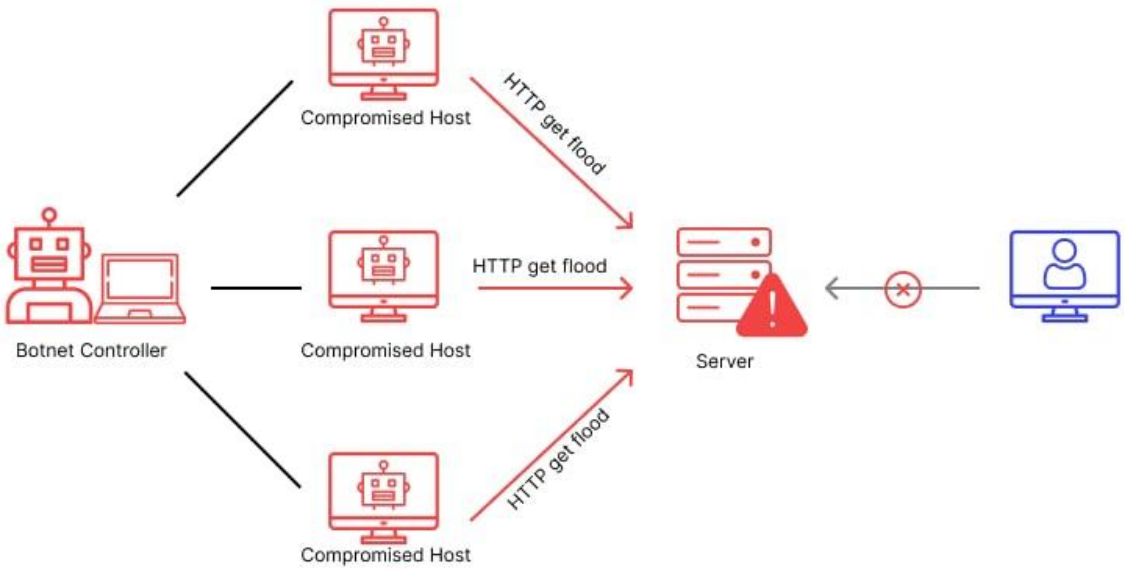
Η πλημμύρα στο πρωτόκολλο μεταφοράς υπερκειμένου είναι μια κατανεμημένη επίθεση άρνησης παροχής υπηρεσιών που αποσκοπεί στον κατακλυσμό ενός θύματος με αιτήσεις HTTP. Καθώς ο στόχος κορεστεί από αιτήματα δεν θα είναι σε θέση να ανταποκριθει σε φυσιολογικα αιτήματα από πραγματικους χρήστες.

Μια πλημμύρα HTTP συμβαίνει όταν οι πελάτες HTTP, όπως οι περιηγητές ιστού, συνδέονται με έναν διακομιστή ή μια εφαρμογή για να υποβάλουν αιτήσεις HTTP. Τα αιτήματα που στέλνονται μπορεί να είναι μορφής HTTP-GET ή HTTP-POST. Σκοπός της όλης διαδικασίας είναι ο εξαναγκασμός του διακομιστή να αφιερώσει όσο το δυνατό περισσότερους πόρους για την υποστήριξη της επίθεσης, αρνούμενος έτσι την πρόσβαση νόμιμων χρηστών στους πόρους του.

Για να επιτευχθεί μέγιστη αποτελεσματικότητα, οι κακόβουλοι χρήστες συχνά χρησιμοποιούν ή δημιουργούν botnets. Επιστρατεύοντας πολλές συσκευές που έχουν μολυνθεί, ο επιτιθέμενος είναι σε θέση να υπερδιπλασιάσει την λειτουργικότητα της επίθεσης, εκτοξεύοντας μεγαλύτερο όγκο κίνησης.

Η μεθοδολογία πλημμύρας HTTP απαρτίζεται από δύο συνηθέστερες προσεγγίσεις:

- **Επίθεση HTTP GET:** Αυτός ο τύπος επίθεσης περιλαμβάνει τη συντονισμένη χρήση πολλών υπολογιστών ή άλλων συσκευών για την υποβολή πολυάριθμων αιτημάτων για αρχεία, εικόνες ή άλλα στοιχεία από έναν στοχευμένο ιστότοπο. Η άρνηση παροχής υπηρεσιών θα συμβεί με την υποβολή περαιτέρω αιτημάτων από έγκυρες πηγές κίνησης όταν ο στόχος υπερφορτωθεί με εισερχόμενα αιτήματα και απαντήσεις.
- **Επίθεση HTTP POST:** Όταν πραγματοποιείται αίτημα POST ο διακομιστής πρέπει να ανταποκρίνεται στο εισερχόμενο αίτημα και να μεταφέρει τα δεδομένα σε ένα επίπεδο παραμονής, συνήθως σε μια βάση δεδομένων, όταν υποβάλλεται μια φόρμα σε έναν ιστότοπο. Η διαδικασία χειρισμού των δεδομένων της φόρμας και η εκτέλεση των απαραίτητων εντολών στην βάση δεδομένων είναι σχετικά επίπονη σε σύγκριση με το ποσό της επεξεργαστικής ισχύος και του εύρους ζώνης που απαιτείται για την αποστολή του αιτήματος POST. Η επίθεση αυτή εκμεταλλεύεται τη διαφορά στη σχετική χρήση πόρων με την αποστολή μεγάλου αριθμού αιτημάτων post απευθείας σε έναν στοχευμένο διακομιστή μέχρι να εξαντληθεί η χωρητικότητά του και να προκύψει άρνηση παροχής υπηρεσιών.



Εικόνα 8: Παρουσίαση επίθεσης πλημμύρας HTTP

πηγή: https://www.wallarm.com/what/website-security-and-prevention-of-a-http-flood-attack

2.4.4 Επίθεση Άρνησης Υπηρεσιών WordPress

Υπάρχουν πολλές μεθοδολογίες με τις οποίες μπορεί ένας να δημιουργήσει μια ιστοσελίδα, από δομημένα εργαλεία μέχρι την κατασκευή εξ ’ολοκλήρου από γλώσσες προγραμματισμού όπως η Java,

JavaScript, HTML, CSS. Ένα από αυτά τα εργαλεία αυτά είναι το WordPress το οποίο δημιουργήθηκε το 2003.

Το WordPress είναι ένα διαδικτυακό πρόγραμμα γενικού σκοπού που υποστηρίζει δύο διαφορετικά είδη διαδικτυακών υπηρεσιών. Το πρώτο είδος το αντλούμε πηγαίνοντας στην σελίδα WordPress.org και κατεβάζοντας τον πηγαίο κώδικα που χρησιμοποιεί το WordPress για να δημιουργήσει και κατασκευάσει ότι απαιτείται. Το δεύτερο είδος το αντλούμε πηγαίνοντας στην σελίδα WordPress.com το οποίο υποστηρίζει τους χρήστες να ξεκινήσουν μια νέα ιστοσελίδα σε μόλις μερικά δευτερόλεπτα.

Το συστατικό στοιχείο που εκμεταλλεύονται οι επιτιθέμενοι ονομάζεται XML-RPC (Remote Procedure Call) που παρουσιάζει πολλά οφέλη προς χρήση του επιτιθέμενου. Η ταχύτητα του Διαδικτύου δεν ήταν όπως είναι σήμερα όταν οι υπηρεσίες Διαδικτύου έγιναν για πρώτη φορά διαθέσιμες. Λόγω της αργής ταχύτητας των dial-up συνδέσεων που χρησιμοποιούσαν οι συγγραφείς και οι bloggers, η δημιουργία ιστοσελίδων στο διαδίκτυο ήταν απίστευτη πρόκληση. Ως εκ τούτου, τα άρθρα γράφονταν στον υπολογιστή και στη συνέχεια αντιγράφονταν στο διαδίκτυο. Αυτό δεν έλυνε πλήρως το πρόβλημα, διότι όταν οι αναρτήσεις τους είχαν κώδικες ή γραφικά οι δημιουργοί αντιμετώπιζαν ένα άλλο πρόβλημα, καθώς δεν μπορούσαν να φορτώσουν εικόνες και κώδικες με μια dial-up σύνδεση χαμηλής ταχύτητας, όπως πριν το WordPress. Από αυτό αναπτύχθηκε η έννοια του XML-RPC, το οποίο επέτρεψε στους κατασκευαστές ιστοσελίδων να γράφουν και να κατασκευάζουν τα ιστολόγιά τους ανεξάρτητα πριν τα συνδέσουν.

Αργότερα, όταν κυκλοφόρησαν έξυπνες συσκευές και νέες εφαρμογές WordPress, οι χρήστες μπορούσαν να συνδεθούν σε οποιοδήποτε WordPress με το όνομα χρήστη και τον κωδικό πρόσβασής τους και να απολαμβάνουν τα ίδια δικαιώματα ανεξάρτητα από το πού συνδέονταν. Αν κάποιος ανακάλυπτε αυτά τα στοιχεία σύνδεσης, έχει πλήρη πρόσβαση σε όλα τα ιστολόγια.

Το χαρακτηριστικό XML-RPC χρησιμοποιεί μία λειτουργία ονόματι “pingback”. Το pingback είναι ένας από τους τύπους ή τις λειτουργίες σχολίων που χρησιμοποιούνται για τη σύνδεση δύο ή περισσότερων ιστολογίων. Ο επιτιθέμενος μπορεί να εκμεταλλευτεί αυτό το χαρακτηριστικό για να εξαπολύσει την επίθεσή του. Ένα παράδειγμα αυτής της επίθεσης έλαβε χώρα, σύμφωνα με την Incapsula (πλατφόρμα παράδοσης εφαρμογών) το 2013. Χωρίς ποτέ να παραβιάσει αυτούς τους ιστότοπους, ο επιτιθέμενος χρησιμοποίησε έναν υπολογιστή για να δημιουργήσει χιλιάδες συνδέσμους σε δημοφιλείς και λιγότερο δημοφιλείς ιστότοπους και στη συνέχεια τους εκμεταλλεύτηκε. Είναι σαφές πώς αυτά τα αιτήματα θα μπορούσαν να ρίξουν γρήγορα οποιονδήποτε ιστότοπο με μεγάλο αριθμό συνδέσμων χρησιμοποιώντας όλους τους πόρους του διακομιστή.

2.4.5 Επίθεση SQL Injection

Η SQL (Structure Query Language) Injection είναι ένα είδος επίθεση που περιλαμβάνει την εκτέλεση κακόβουλων ερωτημάτων για την ανάκτηση μιας βάσης δεδομένων στο διαδίκτυο. Χρησιμοποιώντας κακόβουλο κώδικα, που συνήθως ονομάζεται payload, οι εισβολείς θα αναζητήσουν ευπάθεια, η οποία συχνά αντιπροσωπεύεται από την είσοδο χρήστη και απαιτεί ένα ερώτημα SQL. Οι επιτιθέμενοι εισάγουν το payload τους ή τον κακόβουλο κώδικα ως μέρος του ερωτήματος SQL, με σκοπό να αποκτήσουν πρόσβαση σε δεδομένα ιστού, η οποία θα οδηγήσει σε κλοπή ή τροποποίηση ευαίσθητων δεδομένων (10).

Ο παραπάνω τρόπος δεν είναι ο μοναδικός που μπορεί να επιτευχθεί μία επίθεση SQL Injection καθώς είναι δυνατό να εκτελεστεί ως επίθεση άρνησης υπηρεσίας ή ακόμα και μέσω της επίθεσης άρνησης υπηρεσίας. Συγκεκριμένα κάθε διαδικτυακό ερώτημα ή αίτηση δεδομένων που γίνεται για να ληφθούν δεδομένα από μια διαδικτυακή βάση δεδομένων και προκαλεί μεγάλη επιβάρυνση στους πόρους του διακομιστή ιστού, όπως ο επεξεργαστής και η μνήμη τυχαίας προσπέλασης, καθιστώντας τον πολύ απασχολημένο για να εκτελέσει έγκυρα αιτήματα, μπορεί να κατηγοριοποιηθεί ως επίθεση SQL Injection στον ορισμό της επίθεσης DoS. Για να υποστήριξη αυτήν την διαδικασία ο χρήστης θα στρατολογήσει bots ή botnets για να υποβάλουν πολλές εργασίες σε έναν ιστότοπο ταυτόχρονα, σε μια προσπάθεια να εξαντλήσουν τους πόρους του διακομιστή ιστού όπως επίσης θα προσπαθήσει να χρησιμοποιήσει πολύπλοκα αιτήματα POST αντί για τα απλούστερα αιτήματα GET. Όπως αναφέρεται στην δημοσίευση των Dubey και Gupta (11), υπάρχουν διαδικασίες ανίχνευσης που βασίζονται σε τεχνικές παρακολούθησης και επαλήθευσης για την ανεύρεση αυτών των αιτημάτων επίθεσης προτείνοντας μια νέα τεχνική με την ενοποίηση δύο υπαρχουσών τεχνικών στοχεύοντας στον διπλασιασμό ελέγχου και εγκυρότητας.

2.5 Περίληψη κεφαλαίου

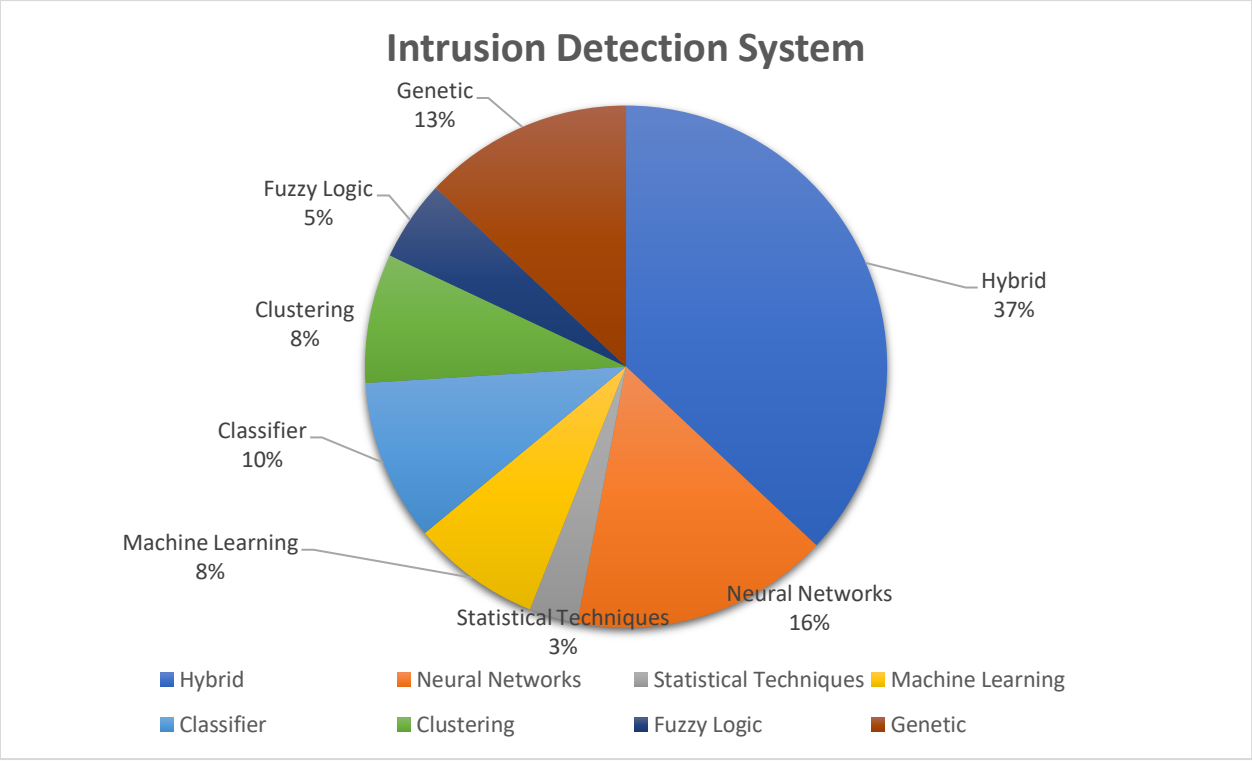
Σε αυτό το κεφάλαιο συζητήθηκαν και κατηγοριοποιήθηκαν οι επιθέσεις άρνησης υπηρεσιών σύμφωνα με το μοντέλο διασύνδεσης ανοικτών συστημάτων (OSI model). Σε κάθε επίπεδο αναλύθηκαν τα συχνότερα χρησιμοποιούμενα πρωτόκολλα μαζί με τις συνηθέστερες επιθέσεις που τα χρησιμοποιούν έτσι ώστε να απεικονιστεί όσο το δυνατό πιο ολοκληρωμένα η ιδέα γύρω από την μεθοδολογία και τον τρόπο δράσης των κακόβουλων χρηστών.

Κεφάλαιο 3 : Συστήματα και Τεχνικές Ανίχνευσης και Πρόληψης Εισβολής

3.1 Γενικό Πλαίσιο

Η ανίχνευση εισβολών έχει έναν φαινομενικά ευθύ σκοπό, την ανακάλυψη εισβολών. Το εγχείρημα καθίσταται δύσκολο καθώς τα συστήματα ανίχνευσης εισβολών στην πραγματικότητα δεν βρίσκουν τις εισβολές αυτές καθαυτές, αλλά ενδείξεις παραβίασης είτε ενώ αυτές συμβαίνουν είτε αφού έχουν ήδη συμβεί.

Σε αυτό το κεφάλαιο θα αναλύσουμε τις μεθόδους ανίχνευσής και αποτροπής παραβιάσεων μέσω του συστήματος ανίχνευσης εισβολών IDS (Intrusion Detection System).



Εικόνα 9: Ποσοστό κατανομής ερευνών για διαφορετικά IDS

πηγή: *https://www.researchgate.net/figure/the-percentage-distribution-of-the-number-of-papers-under-various-IDS-approaches_fig1_2360096773*

Ένα Σύστημα Ανίχνευσης Εισβολών είναι ένα εργαλείο για τον εντοπισμό ασυνήθιστης συμπεριφοράς στην κυκλοφορία του δικτύου και την αποστολή ειδοποιήσεων όταν εντοπίζεται. Πρόκειται για ένα κομμάτι λογισμικού που σαρώνει δίκτυα και συστήματα υπολογιστών για κακόβουλη συμπεριφορά και παραβιάσεις πρωτοκόλλων-πολιτικών.

3.2 Ανίχνευση Εισβολής

Στόχος της ανίχνευσης εισβολής είναι να αποκαλύψει τις προσπάθειες παραβίασης της διαθεσιμότητας, της εμπιστευτικότητας και της ακεραιότητας ενός πόρου. Αποσκοπεί στην αποκάλυψη τυχόν προσπαθειών για την παράκαμψη των ήδη θεσπισμένων περιορισμών ασφαλείας. Η παρακολούθηση των συμβάντων του συστήματος υπολογιστών και του δικτύου περιλαμβάνει την αναζήτηση τυχόν ενδείξεων ενεργειών που παραβιάζουν ή θέτουν σε κίνδυνο τα καθιερωμένα πρότυπα ασφαλείας, τις πολιτικές χρήσης και τις πολιτικές υπολογιστών (12) (13).

3.2.1 Σύστημα Ανίχνευσης Εισβολής Δικτύου (Network-based IDS)

Τα σύστημα ανίχνευσης εισβολής βασισμένα σε δίκτυο προσπαθούν να ανιχνεύσουν οποιαδήποτε παράξενη ή παράνομη συμπεριφορά στο δίκτυο. Χρησιμοποιούν συσκευές δικτύωσης για τη συλλογή και επεξεργασία πακέτων. Αξιοποιούνται συγκεκριμένα κριτήρια για να επισημάνουν την ύποπτη κυκλοφορία και λειτουργούν μόνο για να ειδοποιούν τους διαχειριστές για επικείμενο κίνδυνο. Για να διασφαλίσουν το σύστημα από τυχόν κινδύνους που βασίζονται στο δίκτυο, παρακολουθούν και εξετάζουν όλη την εισερχόμενη κυκλοφορία. Συχνά τα συστήματα ανίχνευσης εισβολής παρατηρούν και ελέγχουν την κίνηση του δικτύου σε συγκεκριμένα επιλεγμένα σημεία σε πραγματικό χρόνο σε μια προσπάθεια να ανιχνεύσουν παραβίαση. Μπορούν να ανιχνεύσουν δραστηριότητες πρωτοκόλλων επιπέδου εφαρμογής, δικτύου και μεταφοράς. Τα εργαλεία αυτά θα μπορούσαν να χαρακτηριστούν ως συστήματα παρακολούθησης, επειδή βασίζονται σε εκτενή επιθεώρηση των πακέτων που διαπερνούν το δίκτυο. Επιπρόσθετα έχουν την δυνατότητα να αναζητούν αποδοτικά την κίνηση του για αντικανονική συμπεριφορά επειδή είναι εμπλουτισμένα με υπογραφές επιθέσεων. Τα NIDS χαρακτηρίζονται για την φορητότητα και το επίπεδο αυτονομίας τους από ένα λειτουργικό σύστημα σε ένα άλλο. Ωστόσο τα συστήματα αυτά έχουν μειονεκτήματα καθώς η χρήση επιθέσεων με υπογραφές που κάνει το σύστημα να υστερεί σε σχέση με τις τελευταίες-πρόσφατες επιθέσεις. Επίσης παρουσιάζουν παθογένεια σε επίπεδο κλιμάκωσης ιδίως σε δίκτυα υψηλών ταχυτήτων καθώς τα συστήματα αυτά δεν μπορούν να σαρώσουν τα πρωτόκολλα (14).

3.2.2 Σύστημα Ανίχνευσης Εισβολής Κεντρικού Υπολογιστή (Host-based IDS)

Σε αντίθεση με τα IDS που βασίζονται στο δίκτυο, τα Host-based συστήματα ανίχνευσης εισβολής χρησιμεύουν για τον εντοπισμό οποιασδήποτε ανεπιθύμητης ή παράνομης δραστηριότητας σε μια συγκεκριμένη συσκευή και όχι σε ολόκληρο το δίκτυο. Συχνά εγκαθίστανται σε κάθε κεντρικό υπολογιστή, όπου παρακολουθούν το λειτουργικό σύστημα και τα προγράμματα που εκτελούνται. Κατά την διαδικασία πρόβλεψης χρησιμοποιούν ένα συνδυασμό ευρετικών μεθόδων, κανόνων και υπογραφών και νέων τεχνικών τεχνητής νοημοσύνης όπως η μηχανική μάθηση, η βαθιά μάθηση καθώς και τεχνικές υπολογισμού όπως η fuzzy logic (ασαφής λογική) (15). Σε κάθε κεντρικό υπολογιστή τοποθετούνται αισθητήρες που συλλέγουν διαδρομές ελέγχου στο σύστημα που παρακολουθείται. Στην ουσία συγκρίνεται το τρέχον στιγμιότυπο των αρχείων του συστήματος με το προηγούμενο στιγμιότυπο και εάν ορισμένα στοιχεία έχουν διαγραφεί ή τροποποιηθεί τότε δίνεται μία ειδοποίηση στον διαχειριστή.

3.2.3 Σύστημα Ανίχνευσης Εισβολής Βάσει Πρωτοκόλλου (Protocol-based IDS)

Το σύστημα ανίχνευσης εισβολών βάσει πρωτοκόλλου (PIDS) ελέγχει το πρωτόκολλο μεταξύ ενός χρήστη-συσκευής και του διακομιστή διαθέτοντας ένα σύστημα που βρίσκεται μόνιμα στο front-end του διακομιστή. Με τη συνεχή παρακολούθηση της ροής του πρωτοκόλλου HTTPS αλλά και την αποδοχή του σχετικού πρωτοκόλλου HTTP, προσπαθεί να προστατεύσει τον διακομιστή ιστού.

3.2.4 Σύστημα Ανίχνευσης Εισβολής Βάσει Πρωτόκολλο Εφαρμογής (Application protocol-based IDS)

Το σύστημα ανίχνευσης εισβολών βάσει πρωτοκόλλου εφαρμογής (APIDS) είναι ένα σύστημα που λαμβάνει θέση μέσα σε μία ομάδα διακομιστών. Παρακολουθεί την επικοινωνία σε συγκεκριμένα πρωτόκολλα επικοινωνιών εντοπίζοντας έτσι τυχόν παραβιάσεις. Παραδείγματος χάρη το εργαλείο APIDS μπορεί να παρακολουθεί το πρωτόκολλο SQL (Structure Query Language) που συναλλάσσεται με τη βάση δεδομένων του διακομιστή ιστού.

3.2.5 Υβριδικό Σύστημα Ανίχνευσης Εισβολής

Το υβριδικό σύστημα ανίχνευσης εισβολών κατασκευάζεται με τον συνδυασμό δύο ή περισσότερων μεθοδολογιών συστημάτων ανίχνευσης παραβιάσεων. Σε αυτή την υλοποίηση τα δεδομένα του συστήματος συγχωνεύονται με τα δεδομένα του δικτύου για τη δημιουργία μιας ολοκληρωμένης εικόνας του συστήματος δικτύου. Σε σύγκριση με άλλα συστήματα ανίχνευσης εισβολής, τα υβριδικά συστήματα ανίχνευσης εισβολής είναι πιο αποτελεσματικά.

3.3 Πρόληψη Εισβολής

Η διαδικασία εντοπισμού δραστηριοτήτων ή απειλών εισβολής και διαχείρισης των κατάλληλων αντιδράσεων σε όλο το δίκτυο σε αυτές που εντοπίζονται είναι γνωστή ως σύστημα πρόληψης εισβολής (IPS). Είναι η εφαρμογή της επέκτασης των ρόλων ενός συστήματος ανίχνευσης εισβολών ώστε να περιλαμβάνει τη δυνατότητα αποκλεισμού των κακόβουλων μη εξουσιοδοτημένων δραστηριοτήτων που ανιχνεύονται. Όταν εντοπίζονται πακέτα με κακόβουλη συμπεριφορά ή πακέτα που ταιριάζουν σε καθορισμένα προφίλ στην κυκλοφορία σε πραγματικό χρόνο, τα IPS παρέχουν συναγερμούς και μπορούν να απορρίπτουν ή να μπλοκάρουν την κυκλοφορία αυτή καθώς ταξιδεύει στο δίκτυο. (16)

Οι λειτουργίες που μπορεί να εκτελέσει ένα σύστημα πρόληψης εισβολών είναι οι εξής :

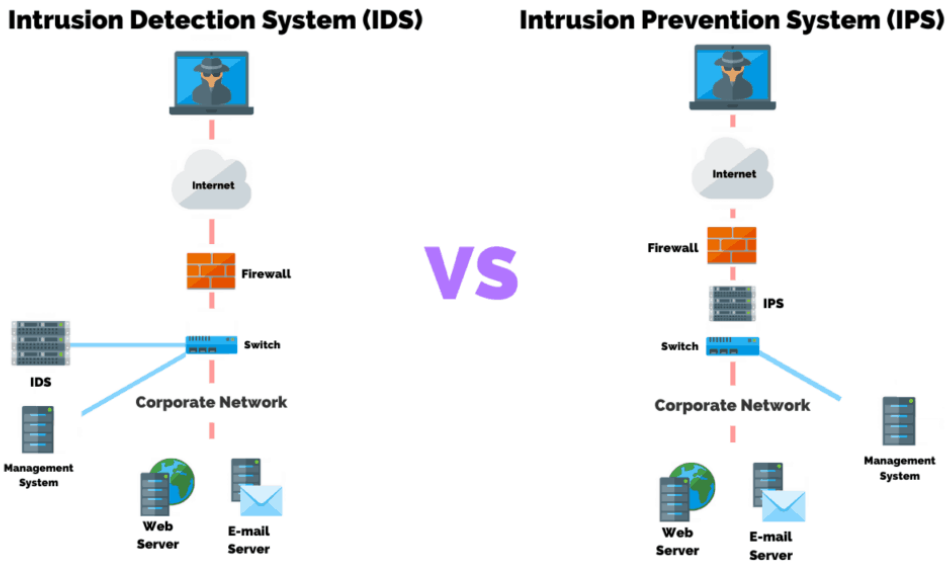
- Αποστολή συναγερμών-προειδοποιήσεων στον διαχειριστή του συστήματος.
- Απόρριψη κακόβουλων πακέτων.
- Αποκλεισμός της κυκλοφορίας από τη διεύθυνση προέλευσης.
- Επαναφορά σύνδεσης.

3.4 Διαφορές Μεταξύ Συστημάτων Ανίχνευσης (IDS) και Πρόληψης (IPS) Εισβολών

	IPS	IDS
Τύπος Συστήματος	Δραστικό (Παρακολούθηση και Προστασία)	Παθητικό (Παρακολούθηση και Παροχή Ειδοποιήσεων)
Μηχανισμοί Ανίχνευσης	Ανίχνευση υπογραφής Ευπάθεια Υπογράφων Στατιστική ανωμαλία	Ανίχνευση υπογραφής
Θέση στο δίκτυο	Εντός Γραμμής Επικοινωνίας	Εκτός Γραμμής Επικοινωνίας

Πίνακας 1: Διαφορές μεταξύ IPS και IDS

Πηγή: https://www.paloaltonetworks.com/cyberpedia/what-is-an-intrusion-detection-system-ids



Εικόνα 10: Διαφορές μεταξύ IDS και IPS

πηγή: https://purplesec.us/intrusion-detection-vs-intrusion-prevention-systems/

Οι πρωταρχικοί στόχοι των συστημάτων ανίχνευσης και πρόληψης εισβολών είναι να σταματήσουν τις πιθανές ζημιές από εντοπισμένες παραβιάσεις, να ελαχιστοποιήσουν τις ζημιές αυτές και να αναζητήσουν τους επιτιθέμενους ή νέα μοτίβα επιθέσεων. Πρέπει να διαθέτουν την απαραίτητη ακρίβεια για να διακρίνουν διαφορές μεταξύ νόμιμων και μη εξουσιοδοτημένων χρηστών καθώς και να είναι σε θέση να διεξάγουν σε πραγματικό χρόνο την ανίχνευση εισβολών, να αντέχουν στις επιθέσεις και να πραγματοποιούν ταχύτατα την ανάλυση της κίνησης (17).

3.5 Μηχανισμοί Ανίχνευσης Εισβολών

3.5.1 Μέθοδος Βάσει Υπογραφής (Signature-based)

Αυτός ο μηχανισμός ανίχνευσης εισβολών είναι περισσότερο λειτουργικός στην ταυτοποίηση ήδη γνωστών απειλών καθώς βασίζεται σε γνωστά πρότυπα, όπως συγκεκριμένες ακολουθίες κακοπροαίρετων εντολών που χρησιμοποιεί το κακόβουλο λογισμικό, επικεφαλίδες πακέτων, ακολουθίες byte και περιεχόμενο payload που μπορεί να υποδεικνύουν διείσδυση. Καταβάλλεται συνεπώς προσπάθεια για τον εντοπισμό κάποιας γνωστή υπογραφής καθιστώντας έτσι αυτήν την μέθοδο να παρουσιάζει ομοιότητες με τον πρόγραμμα προστασίας ιστού.

Η μέθοδος αυτή παρέχει υψηλή ακρίβεια δεδομένου ότι εάν μια επίθεση βρίσκεται στη βάση δεδομένων υπογραφών, θα σημάνει συναγερμός εάν η ίδια επίθεση βρίσκεται στα πακέτα ζωντανής κυκλοφορίας. Το συμβάν θα καταγραφεί για περαιτέρω διερεύνηση. Το σύστημα ανίχνευσης εισβολών που βασίζεται σε υπογραφές είναι τόσο καλό όσο και η βάση δεδομένων του. Δεδομένου ότι οι χάκερς αναπτύσσουν πάντα νέες τεχνικές για να παρακάμψουν το IDS, αν η βάση δεδομένων του δεν είναι πλήρως ενημερωμένη τότε καθίσταται ευάλωτη και υποαποδίδει (18). Για να διατηρείται το σύστημα επίκαιρο τα νέα δεδομένα υπογραφών καταγράφονται και αποθηκεύονται συνεχώς, ώστε να επιτυγχάνεται συνεχής ενημέρωση. Προκειμένου να χρησιμοποιηθούν για μελλοντική ανίχνευση, τα συστήματα που βασίζονται σε υπογραφές συχνά λαμβάνουν ένα αποτύπωμα μιας γνωστής επίθεσης ή ενός κακόβουλου λογισμικού, το οποίο μπορεί να είναι μια ακολουθία byte σε ένα αρχείο ή ένα κρυπτογραφικό κατακερματισμένο αρχείο.

Για την συγκεκριμένη μεθοδολογία έχει πραγματοποιηθεί σημαντική έρευνα καθώς παρατηρούνται πολλά άρθρα τα οποία προτείνουν εξελικτικούς χειρισμούς κρατώντας ατόφια την βασική ιδέα γύρω από τον τρόπο λειτουργίας της μεθόδου. Στην δημοσίευση τους, οι Yassin και Udzir (19) πρότειναν ένα ολοκληρωμένο σύστημα που θα απαρτίζεται από τους αλγορίθμους ταξινόμησης Naïve Bayes (NB) και

Random Forest (RF) με σκοπό την βελτιστοποίηση του ποσοστού αναγνώρισης ομαλής και κακόβουλης κίνησης καθώς και την δημιουργία υπογραφών επίθεσης για επιταχυμένη ανίχνευση στο μέλλον. Από τους Kwon Kim και Lee (20) προτάθηκε ένα σύστημα ελέγχου πραγματικού χρόνου, μια υβριδική μέθοδος ανίχνευσης διαταραχών που συγχωνεύει μεθόδους βασισμένες στην υπογραφή και στην συμπεριφορά. Επιπρόσθετα μια εφαρμογή που διατυπώθηκε από τον Hannes Holm (21) αφορά την χρήση συστημάτων βάσει υπογραφής για την ανίχνευση επιθέσεων τύπου Zero Day οδηγώντας μάλιστα σε εξαιρετικά ποσοστά ανίχνευσης των επιθέσεων αυτών.

Υπάρχουν δύο κατηγορίες ανίχνευσης υπογραφών που χρησιμοποιούνται από τα συστήματα πρόληψης εισβολών:

- Υπογραφές που στοχεύουν στην εκμετάλλευση. Βοηθούν στον εντοπισμό μεμονωμένων περιστατικών που ενεργοποιούν ένα συγκεκριμένο μοτίβο.
- Υπογραφές που στοχεύουν στις ευπάθειες. Στοχεύουν στις ευπάθειες του συστήματος-στόχου. Βοηθούν στην προστασία των συστημάτων έναντι ποικίλων απειλών, ωστόσο υπάρχει σημαντική πιθανότητα ψευδώς θετικών αποτελεσμάτων.

3.5.2 Μέθοδος Βάσει Ανωμαλίας

Τα συστήματα ανίχνευσης εισβολών βάσει ανωμαλίας συνήθως παράγουν ένα στατιστικό μοντέλο φυσιολογικής συμπεριφοράς. Είναι αναγκαίο να γίνει σωστή εκμάθηση του συστήματος διότι όσο μεγαλύτερος είναι ο αριθμός των πακέτων τόσο καλύτερα θα είναι αναγνωρίσιμο πότε μία συμπεριφορά στο δίκτυο αποκλίνει από την ομαλή. Η ανίχνευση μπορεί να γίνει βάση των αριθμών των πακέτων και των ρυθμό αποστολής ή παραλαβής τους. Διαταραχές στην φυσιολογικότητα της ροής μπορεί να προκληθούν για οποιοδήποτε από τους παρακάτω λόγους :

- Υψηλός ρυθμός πακέτων
- Πολύ μικρά ή πολύ μεγάλα μεγέθη πακέτων
- Ανωμαλίες βασισμένες στο πρωτόκολλα TCP όπως SYN, ACK, FIN και RST
- Επιθέσεις ενίσχυσης κίνησης
- Επιθέσεις μέσω πρωτοκόλλου UDP και ICMP
- Σάρωση διευθύνσεων και θυρών

Επειδή χρησιμοποιούν έναν ευρύτερο ορισμό του τι συνιστά φυσιολογική δραστηριότητα-κίνηση, τα συστήματα ανίχνευσης εισβολών που βασίζονται σε ανωμαλίες έχουν τη δυνατότητα να ανακαλύπτουν ένα ευρύ φάσμα δραστηριοτήτων στο δίκτυο. Η εκπαίδευση αυτού του εργαλείου με όσο το δυνατό περισσότερα δεδομένα το ειδικεύει στο να μπορεί να ξεχωρίζει την ομαλή από την ανώμαλη συμπεριφορά καθιστώντας το ικανό να ανιχνεύει νέες ή ακόμη και άγνωστες επιθέσεις (22).

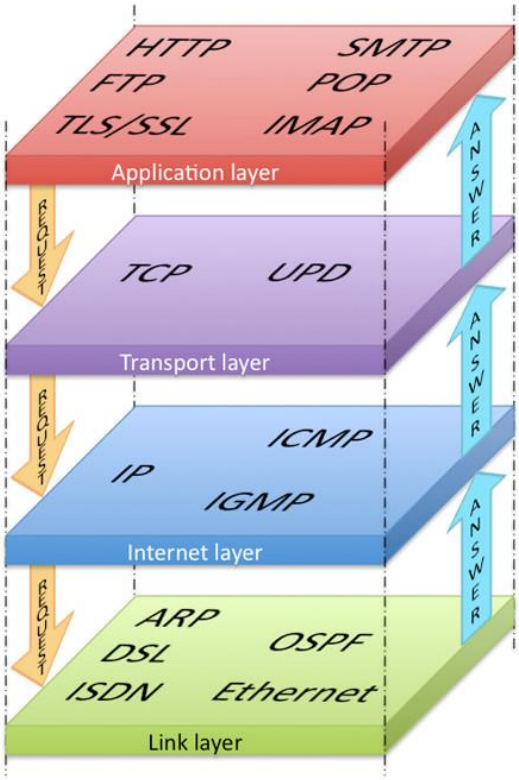
Σε αντίθεση με την ανίχνευση βάσει υπογραφής, η οποία επικεντρώνεται κυρίως στον τρόπο εκτέλεσης των συμβάντων, η ανίχνευση ανωμαλιών ασχολείται περισσότερο με γεγονότα που έχουν μετρήσιμο αντίκτυπο (23). Όσο μεγαλύτερη εξάρτηση υπάρχει στις μετρικές των γεγονότων τόσο μεγαλύτερη θα είναι η αποδοτικότητα της ανίχνευσης. Αυτά τα συστήματα επιλέγουν τυχαία δείγματα της κίνησης δικτύου και τα συγκρίνουν με το καθιερωμένο "κανονικό". Το σύστημα ανταποκρίνεται στην περίσταση εάν το επιλεγμένο δείγμα αποκλίνει από το προβλεπόμενο σύνολο παραμέτρων. Ωστόσο, λόγω της δυναμικής φύσης των δικτύων, τα συστήματα που βασίζονται σε ανωμαλίες μπορεί να φανούν αδύναμα καθώς είναι επιρρεπή σε υπερβολικό αριθμό ψευδώς θετικών αποτελεσμάτων. Επίσης καταναλώνουν πολύ χρόνο για να αναλύσουν, να ανιχνεύσουν και εν τέλει να ειδοποιήσουν σε περίπτωση ύπαρξη μη φυσιολογικής κίνησης.

Υπάρχουν πολλά άρθρα στην επιστημονική κοινότητα που αναλύουν και βελτιστοποιούν τα συστήματα ανίχνευσης εισβολών βάσει ανωμαλίας προτείνοντας ποικίλους τρόπους για τον εντοπισμό διαταραχών στην κίνηση του δικτύου. Οι Eskandar, Janjua, Vecchio και Antonelli (24) δημιούργησαν ένα ευφυές σύστημα ανίχνευσης εισβολών βάσει ανωμαλίας ονόματι **Passban** το οποίο είχε σχεδιαστεί ειδικά για να φιλοξενείτε και να εκτελείτε από συμβατικές edge συσκευές. Προσομοίωσαν ένα δίκτυο έξυπνο σπιτιού και διαπίστωσαν πως η υλοποίηση τους ήταν ικανή να προστατεύσει όλες τις IoT συσκευές που υπήρχαν στο δίκτυο. Ένα από τα πιο ελκυστικά χαρακτηριστικά του ήταν η ικανότητα του να εκπαιδεύεται αυτόματα χρησιμοποιώντας τις νόμιμες ροές κυκλοφορίας του δικτύου.
Μέθοδοι μηχανικής μάθησης όπως ο ταξινομητής Naïve Bayes προτάθηκε από τους Alaei και Noorbehbahani (25) οι οποίοι το χρησιμοποιούν για να προτείνουν ένα σύστημα ενεργητικής μάθησης για την ανίχνευση ανωμαλιών τόσο σε offline όσο και σε online προφίλ.
Οι Angelo και Drummond (26) μελέτησαν ένα σύστημα ανίχνευσης εισβολών με βάση τις ανωμαλίες όπου για την επιλογή χαρακτηριστικών για τη δημιουργία προφίλ εφάρμοσαν τεχνικές βασισμένες σε γενετικό αλγόριθμο που παρείχε επαναληπτική προσέγγιση για την βελτίωση της απόδοσης του συστήματος.

3.6 Τεχνικές Ανίχνευσης ανωμαλιών

3.6.1 Ανίχνευση Ανωμαλιών Πρωτοκόλλου

Στα σημερινά συστήματα ανίχνευσης εισβολών η ανίχνευση ανωμαλιών πρωτοκόλλου αποτελεί θεμελιώδες στοιχείο. Ξεπερνά τον απλό καθορισμό κανόνων των προηγούμενων υλοποιήσεων συστημάτων ανίχνευσης ανωμαλιών. Παρακολουθεί τυχόν αποκλίσεις από την προβλεπόμενη συμπεριφορά και μορφή ενός πρωτοκόλλου. Υπό το πρίσμα της ανίχνευσης ανωμαλιών, μπορούμε να διακρίνουμε ορισμένες πτυχές της στοίβας πρωτοκόλλων TCP/IP, είτε κάνοντας επανασυναρμολόγηση (reassembly) TCP είτε ανασυγκρότηση (defragmentation) IP ώστε να ελεγχθεί οποιαδήποτε ασυνήθιστη συμπεριφορά, ειδικότερα στα επίπεδα δικτύου (Επίπεδο Δικτύου 3), μεταφοράς (Επίπεδο Μεταφοράς 4) και εφαρμογής (Επίπεδο Εφαρμογής 7).



Εικόνα 11: Αναλυτική περιγραφή της στοίβας TCP/IP

πηγή: https://www.linkedin.com/pulse/what-tcpip-stack-phillip-zito/

Η ανίχνευση ανωμαλιών μπορεί να ανακαλύψει γεγονότα όπως αλλοιωμένα αθροίσματα ελέγχου, την συνέπεια η μη των σημαιών TCP καθώς επίσης και αντικανονικές ρυθμίσεις και χρήση του TCP σε επίπεδο μεταφοράς και δικτύου (23). Λόγω αδυναμίας κατανόησης της λειτουργίας του δικτύου, η στατιστική ανίχνευση ανωμαλιών δεν μπορεί να δημιουργήσει κανονικά στατιστικά στοιχεία για την κυκλοφορία του. Είναι δυνατή η ανίχνευση ανωμαλιών πρωτοκόλλου λόγω του γεγονότος ότι τα πρωτόκολλα είναι πλήρως τεκμηριωμένα.

3.6.2 Στατιστική ανωμαλία – Στατιστική κατανεμημένης άρνησης υπηρεσιών

Η τεχνική αυτή χρησιμοποιεί στατιστικές μεθόδους για την καταγραφή συγκεκριμένων συμπεριφορών της κυκλοφορίας. Δραστηριότητες εντός δικτύου όπως η κίνηση TCP παρακολουθούνται για να ενημερωθούμε πως γίνεται μια κανονική μετάδοση, δηλαδή η τριπλή χειραψία TCP, η μεταφορά δεδομένων και ο τερματισμός της σύνδεσης. Είναι επίσης δυνατή η καταγραφή των διαστημάτων μεταξύ των πακέτων, έτσι ώστε να μπορούν να συγκριθούν σε οποιαδήποτε χρονική στιγμή πραγματοποιηθεί μια επίθεση. Προς αποφυγή ψευδών συναγερμών το σύστημα θα πρέπει να είναι ικανό να διαφοροποιεί στο περιβάλλον εκπαίδευσης την υποτιθέμενη φυσιολογική μάθηση από τις βραχυπρόθεσμες αιχμές, ώστε να μπορεί να λειτουργήσει ομαλά σε ένα χαρακτηριστικά κανονικό περιβάλλον. (27) Λόγω των αιχμών στην κυκλοφορία που συμβαίνει κάθε φορά που πραγματοποιείται μια επίθεση, οι στατιστικές ανωμαλίες έχουν μεγαλύτερη πιθανότητα να αναγνωρίσουν τις επιθέσεις άρνησης υπηρεσιών ως μη φυσιολογική συμπεριφορά. Ένα καλό σύστημα στατιστικών ανωμαλιών θα πρέπει να είναι σε θέση να εντοπίζει και άλλα γεγονότα που επηρεάζουν την κυκλοφορία αλλά δεν είναι απαραίτητα επιθέσεις όπως, για παράδειγμα, μια απροσδόκητη αύξηση των επισκεπτών σε έναν ιστότοπο, η οποία οφείλεται συνήθως σε κάποιο αξιοσημείωτο γεγονός που μόλις έλαβε χώρα (flash crowd). Τα συστήματα στατιστικής ανίχνευσης ανωμαλιών προσδιορίζουν την "κανονική" συμπεριφορά του δικτύου και στη συνέχεια οποιαδήποτε κίνηση που αποκλίνει από αυτήν χαρακτηρίζεται ως ανώμαλη. Προφανώς αναζητείται και χτίζεται η δομή ενός παραγωγικού μοτίβου (28). Τα χαρακτηριστικά έχουν σημασία κάθε φορά που εφαρμόζεται μια στατιστική προσέγγιση. Οι ακριβείς ανιχνεύσεις απαιτούν την τροφοδοσία του συστήματος ανίχνευσης ανωμαλιών με τα κατάλληλα χαρακτηριστικά για την αποδοτική διαμόρφωση του (29).

Οι στατιστικές μέθοδοι μπορούν να χρησιμοποιηθούν για τον εντοπισμό διαφόρων επιθέσεων άρνησης παροχής υπηρεσιών, όπως :

- Επίθεση πλημμύρας ICMP
- Επίθεση πλημμύρας UDP
- Επίθεση πλημμύρας TCP SYN

3.6.3 Ανίχνευση Ωφέλιμου Φορτίου (Payload) Εφαρμογής

Με την εμπεριστατωμένη ανάλυση του πρωτοκόλλου εφαρμογής είναι δυνατόν να διαφοροποιηθούν τα λογικά πεδία και να καθοριστούν περιορισμοί συμπεριφοράς μεταξύ τους. Απαιτείται εις βάθος γνώση της σημασιολογίας της εφαρμογής. Η βαθιά επίβλεψη του συστήματος μπορεί να φανεί χρήσιμη στον εντοπισμό τεμαχίων κώδικα μικρού μήκους ονόματι shellcode (χρησιμοποιούνται ως payload) σε ορισμένα από τα πεδία με συνέπεια να μπορεί να χρησιμοποιηθεί για την ανίχνευση υπερχείλισης buffer και άλλων επιθέσεων εκμετάλλευσης που τα χρησιμοποιούν. Στην δημοσίευση των Wang και Stolfo (30) παρουσιάζεται ένας ανιχνευτής ωφέλιμου φορτίου (payload) ως ανιχνευτής, κατάλληλος για επιθέσεις που στοχεύουν στην εκμετάλλευση τρωτών σημείων του πρωτοκόλλου, παράγοντας αξιοσημείωτα ποσοστά αποτελεσματικότητας ανίχνευσης ειδικότερα στην θύρα 80 που αντιστοιχεί στο πρωτόκολλο επικοινωνίας στο διαδίκτυο HTTP.

3.7 Περίληψη κεφαλαίου

Σε αυτό το κεφάλαιο αναλύθηκαν τα συστήματα ανίχνευσης και πρόβλεψης εισβολών του δικτύου. Έγινε μια εκτενής αναφορά στις διαφορετικές μεθοδολογίες για τα συστήματα ανίχνευσης και αναφέρθηκαν οι ουσιώδεις διαφορές μεταξύ των δύο συστημάτων βάσει τύπου μηχανισμού και θέσης στο δίκτυο (IDS και IPS). Τέλος παρουσιάστηκαν τόσο μηχανισμοί όσο και τεχνικές για την δημιουργία και τον τρόπο λειτουργίας των συστημάτων ανίχνευσης παραβιάσεων.

Κεφάλαιο 4 : Πειραματικό Μέρος

4.1 Εισαγωγή

Η μελέτη και η εξέλιξη των τεχνικών ανίχνευσης παρεισφρήσεων αποτελεί στις μέρες μας τον ακρογωνιαίο λίθο της ασφάλειας των δικτύων. Είναι επιτακτική η ανάγκη δημιουργίας αξιόπιστων συστημάτων με χαμηλή ανοχή στα λανθασμένα συμπεράσματα. Από την ανάλυση που προηγήθηκε στην παρούσα διπλωματική εργασία αλλά και κατά γενική ομολογία της επιστημονικής κοινότητας γίνεται αντιληπτό πως η ύπαρξη πληρέστερων συνόλων δεδομένων προς επεξεργασία είναι ικανή να οδηγήσει σε αποδοτικότερα συμπεράσματα και λειτουργικότερα εργαλεία για των εντοπισμό απειλών στο χώρο του διαδικτύου. Όσα περισσότερα είναι τα δεδομένα τόσο αποτελεσματικότερα μπορούν να κατασκευαστούν συμπεριφορικά μοτίβα για τον εντοπισμό μη φυσιολογικών κινήσεων στον χώρο του δικτύου.

Σημαντικότερη δε, είναι η ύπαρξη έγκυρων και ρεαλιστικών δεδομένων. Αυτό είναι και στην ουσία το μεγαλύτερο τροχοπέδη στην προσπάθεια ενός ερευνητή κατά την ασχολία του με αυτό το επιχείρημα (31). Είναι προφανές πως κανείς οργανισμός δεν πρόκειται να δημοσιεύσει την καταγραφή του δικτύου του κατά την διάρκεια μίας επίθεσης. Η περιεκτικότητα του αρχείου σε ευαίσθητα δεδομένα, τόσο από την πλευρά της εκάστοτε επιχείρησης ή φορέα όσο και από την πλευρά των καλόβουλων χρηστών καθιστά απαγορευτική την έκδοση του.

Έχοντας ως στόχο την περιγραφή και εξέταση των επιθέσεων άρνησης υπηρεσιών αλλά και τους τρόπους τους οποίους μπορούμε τις ανιχνεύσουμε, σκοπός αυτής της διπλωματικής εργασίας είναι η παρατήρηση ενός υπάρχοντος συνόλου δεδομένων καθώς και η ανάλυση των επιμέρους τεχνικών προς εξαγωγή συμπερασμάτων.

Μετά από εκτενή αναζήτηση στο διαδίκτυο παρατηρήσαμε πως τα σύνολα δεδομένων που μπορούμε να έχουμε στην διάθεση μας είναι δύο ειδών :

- Δεδομένα πραγματικών επιθέσεων με την ύπαρξη αποκλειστικά των πακέτων που λαμβάνουν μέρος στην επίθεση και όχι αυτά της ομαλής κίνησης του δικτύου.
- Δεδομένα προσομοίωσης επιθέσεων όπου κάθε τερματικό στο δίκτυο φέρει συγκεκριμένη ετικέτα για τον ρόλο του (θύτης, θύμα, μηχανήματα εκτός επίθεσης).

Γίνεται αντιληπτό πως με την πρώτη μορφή δεδομένων είναι δύσκολο να εξάγουμε αξιόπιστα δεδομένα χρησιμοποιώντας βασικές έννοιες της θεωρίας πληροφορίας ή διαφορετικές μεθοδολογίες. Δεν είναι δυνατό να αποφανθούμε πότε είναι αναγκαίο να αναγνωρίσουμε μία επίθεση εάν δεν γνωρίζουμε πως

συμπεριφέρεται ένα δίκτυο υπό φυσιολογικές συνθήκες. Χρειαζόμαστε την ομαλή κίνηση για να μπορούμε να δημιουργήσουμε τα κατάλληλα μοτίβα έτσι ώστε να είναι εμφανείς διαφορές με την κακόβουλη κίνηση.

4.2 Θεωρητικό υπόβαθρο

4.2.1 Θεωρία πληροφορίας

Η θεωρία πληροφορίας είναι η μαθηματική επεξεργασία των ιδεών, των παραμέτρων και των κανονισμών που ρυθμίζουν τη μετάδοση των μηνυμάτων μέσω των δικτύων επικοινωνίας .Απαρτίζεται από την θεωρία πιθανοτήτων και την στατιστική. Θεμελιώθηκε γύρω στα μέσα του 20ού αιώνα από τον Claude Shannon και έκτοτε έχει εξελιχθεί σε ένα ιδιαίτερα ισχυρό πεδίο των μαθηματικών που υποστηρίζει την ανάπτυξη άλλων επιστημονικών κλάδων, όπως η στατιστική, η βιολογία, η επιστήμη της συμπεριφοράς, η νευρολογία και η στατιστική μηχανική (32). Θεωρείται πως η θεωρία πληροφοριών αποτελεί υποσύνολο της θεωρίας πιθανοτήτων, δεδομένου ότι οι τεχνικές που χρησιμοποιούνται σε αυτήν έχουν πιθανοτική φύση. Σε ένα σύνολο πιθανών γεγονότων, η πληροφορία ενός μηνύματος που περιγράφει ένα από αυτά τα γεγονότα ποσοτικοποιεί τα σύμβολα που απαιτούνται για την κωδικοποίηση του γεγονότος με πλήρως αποδοτικό τρόπο.
Η εντροπία είναι ένα μέτρο αβεβαιότητας που σχετίζεται με μία τυχαία μεταβλητή. Με απλά λόγια η μετρική της εντροπίας καθορίζεται ως εξής. Όσο πιο τυχαία είναι μια μεταβλητή πληροφορίας τόσο μεγαλύτερη είναι η εντροπία. Στον αντίποδα όσο μεγαλύτερη είναι η βεβαιότητα – συνέπεια μιας μεταβλητής πληροφορίας, τόσο μικρότερη είναι η εντροπία.

4.2.1.1 Εντροπία Shannon

Το 1948 ο Claude Shannon όρισε την μετρική της εντροπίας πληροφορίας για τον υπολογισμό της αβεβαιότητας, της τυχαιότητας ή της αταξίας στο φυσικό σύστημα (33). Ο τύπος του υπολογισμού της βάσει ενός συνόλου δεδομένων X:

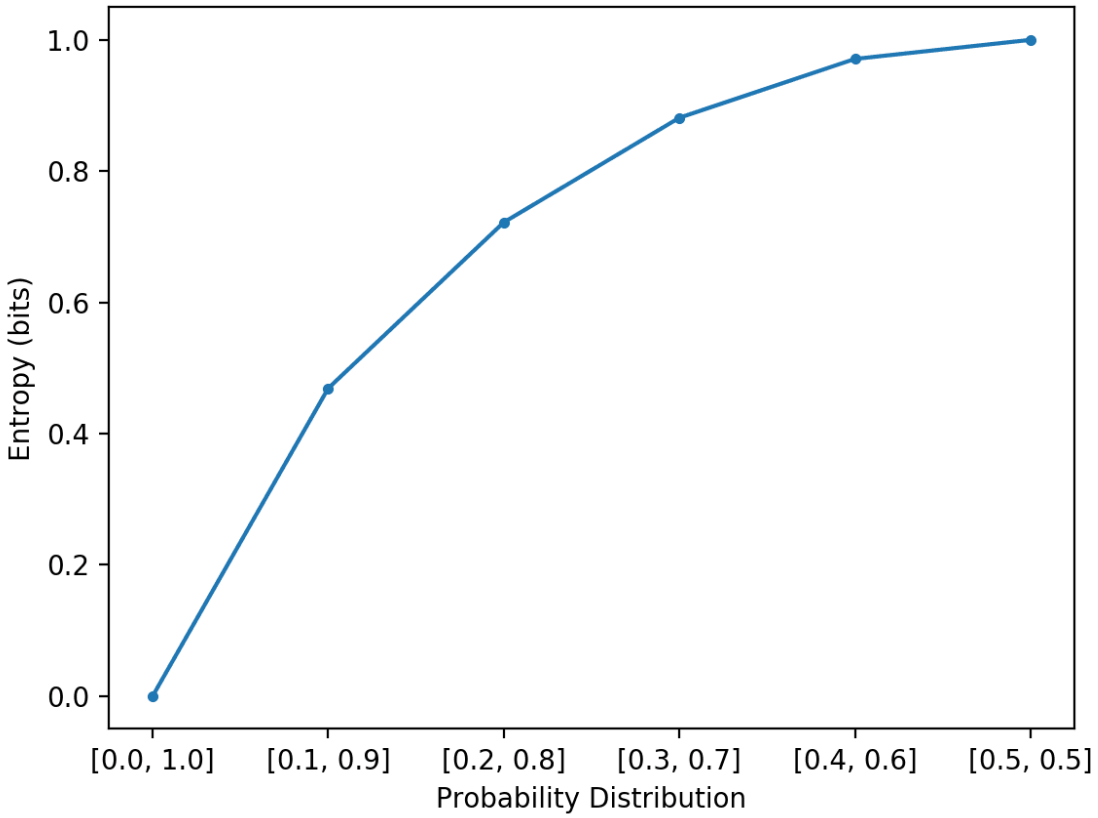
$$\square(\square) = \sum_{\square \in X} \square(\square)\square\square\square(\frac{1}{\square(\square)})$$

Εξίσωση 1: Εντροπία Shannon

όπου P(x) είναι η πιθανότητα εμφάνισης του x στο σύνολο X.

Η τυπική ερμηνεία της εντροπίας είναι ότι προσδιορίζει τον αριθμό των bits που απαιτούνται για την κωδικοποίηση (και μετάδοση) της ταξινόμησης ενός στοιχείου δεδομένων. Όπως προαναφέρθηκε η τιμή της εντροπίας είναι μικρότερη όταν η κατανομή των στοιχείων είναι δεν παρουσιάζει μεγάλη τυχαιότητα.

Για παράδειγμα εάν όλα τα δεδομένα ενός συνόλου δεν παρουσιάζουν τυχαιότητα τότε η εντροπία των στοιχείων είναι μηδενική και θα μεταχθούν 0 bit καθώς ο δέκτης γνωρίζει ότι υπάρχει μόνο ένα αποτέλεσμα. Αντίθετα, η τιμή της εντροπίας είναι μεγαλύτερη όταν η κατανομή των στοιχείων δεν παρουσιάζει μικρή τυχαιότητα. Παραδείγματος χάριν, εάν τα δεδομένα ενός συνόλου είναι ομοιόμορφα κατανεμημένα σε ξεχωριστές $|C_X|$ κλάσεις, τότε χρειάζονται $log|C_X|$ bits για να πραγματοποιηθεί η κωδικοποίηση του γεγονότος (34).



Εικόνα 12: Συσχέτιση της κατανομής πιθανότητας με την εντροπία ανάμεσα σε δύο τυχαίες μεταβλητές

πηγή: https://machinelearningmastery.com/what-is-information-entropy/

Για την ανίχνευση παρεισφρήσεων η εντροπία μπορεί να χρησιμοποιηθεί ως μέτρο της κανονικότητας των δεδομένων ελέγχου. Κάθε κλάση αντιπροσωπεύεται από μία ξεχωριστή εγγραφή σε ένα σύνολο δεδομένων ελέγχου (35).

4.2.1.2 Υπό Συνθήκη Εντροπία

Έστω ότι έχουμε στη διάθεση μας δύο σύνολα δεδομένων X και Y. Η υπό συνθήκη εντροπία καθορίζει την ποσότητα της που πληροφορίας που είναι απαιτούμενη για την περιγραφή μίας τυχαίας μεταβλητής

Y, δεδομένου ότι είναι γνωστή η τιμή μιας άλλης τυχαίας μεταβλητής X (36) (37). Η εντροπία του Y σε συνάρτηση με το X γράφεται ως ***H(Y | X)*** και ο τύπος της είναι ο εξής :

$$□(Y \mid □) = -\sum_{□∈□,□∈□} □(□,□)\,□□□\frac{p(x,y)}{p(x)}$$

Εξίσωση 2: Υπό Συνθήκη Εντροπία

4.2.1.3 Από κοινού Εντροπία

Η από κοινού εντροπία υπολογίζει πόση εντροπία περιέχεται σε ένα κοινό σύστημα δύο τυχαίων μεταβλητών (38). Έστω ότι οι τυχαίες μεταβλητές είναι οι X και Y. Τότε η από κοινού εντροπία γράφεται ως ***H(Y, X)*** και ο τύπος της είναι ο εξής :

$$□(X\,,□) = -\sum_{□∈□}\sum_{□∈□} P(□,□)\,□□□[P(x,y)]$$

Εξίσωση 3: Από κοινού Εντροπία

4.2.1.4 Αμοιβαία Πληροφορία

Στην θεωρία πληροφορίας η αμοιβαία πληροφορία είναι η ποσότητα που ορίζει την αμοιβαία εξάρτηση μεταξύ δύο τυχαίων μεταβλητών (39) (40). Εάν τα διανύσματα μεταφέρουν πολλές πληροφορίες το ένα για το άλλο τότε η τιμή της αμοιβαίας πληροφορίας είναι υψηλή. Αντίστοιχα εάν οι δύο τυχαίες μεταβλητές δεν παρουσιάζουν συσχέτιση τότε η μετρική της αμοιβαίας πληροφορίας παρουσιάζει χαμηλές τιμές. Η αμοιβαία πληροφορία γράφεται ως ***I(X ; Y)*** και ο τύπος είναι ο εξής :

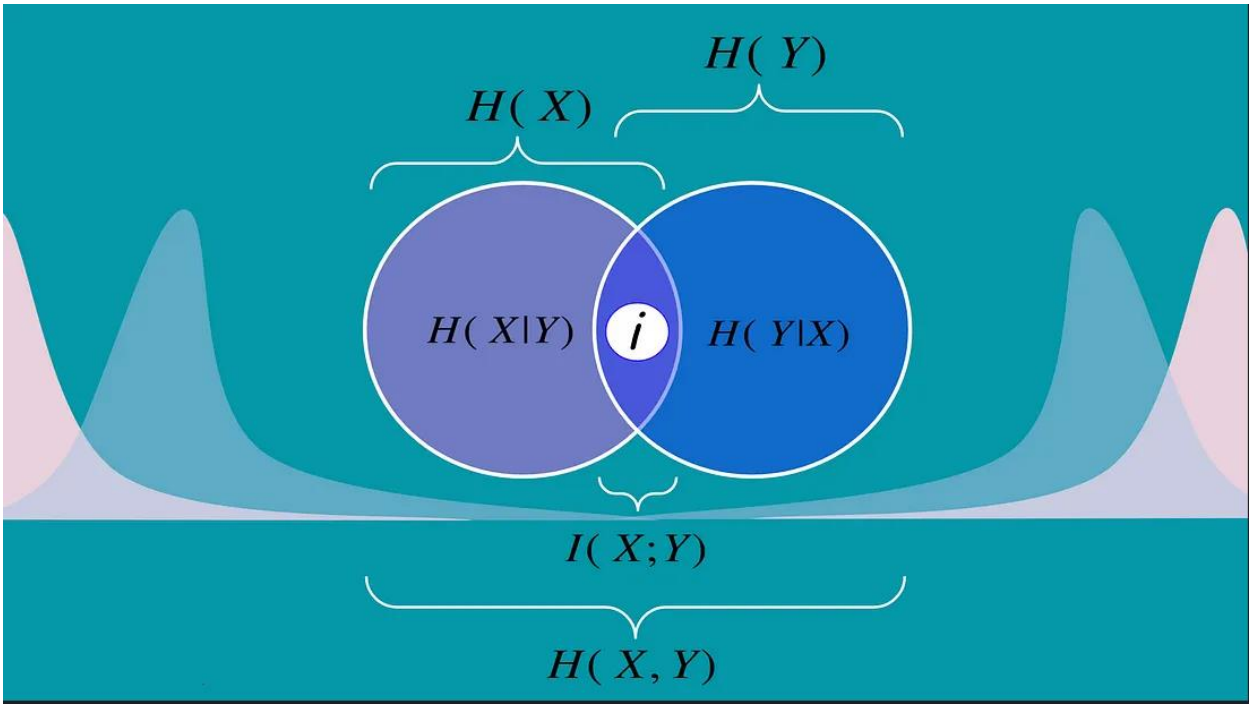
$$□(□\,;\,□) = \sum_{□∈□,□∈□} □(□,□)□□□\frac{□(□,□)}{□(□)□(□)}$$

Εξίσωση 4: Αμοιβαία Πληροφορία

Επιπρόσθετα, ο υπολογισμός της αμοιβαίας πληροφορίας μπορεί να προκύψει και από την σχέση :

$$I(X;Y) = H(X) - H(X|Y)$$

Στην παρακάτω εικόνα παρατίθεται το διάγραμμα Venn που δείχνει την αμοιβαία πληροφορία συναρτήσει των μέτρων πληροφορίας με προσθετικές και αφαιρετικές σχέσεις που συνδέονται με τις συσχετιζόμενες μεταβλητές X και Y από το οποίο προκύπτουν οι σχέσεις μεταξύ των μετρικών.



Εικόνα 13: Διάγραμμα Venn που δείχνει την αμοιβαία πληροφορία συναρτήσει των μέτρων πληροφορίας που συνδέονται με τις συσχετιζόμενες μεταβλητές X και Y

πηγή: https://medium.com/swlh/a-deep-conceptual-guide-to-mutual-information-a5021031fad0

4.2.1.5 Κανόνας Αλυσίδας

Για τον υπολογισμό των παραπάνω μετρικών κατά την πειραματική ανάλυση είναι αναγκαία η γνώση του κανόνα αλυσίδας, όπου συνδέει την εντροπία Shannon με την υπό συνθήκη και από κοινού εντροπία μεταξύ δύο τυχαίων μεταβλητών. Ο τύπος του κανόνα αλυσίδας είναι :

$$H(X,Y) = H(X) + H(Y|X)$$

Εξίσωση 5: Κανόνας Αλυσίδας

Η χρήση του κανόνα αλυσίδας εξοικονομεί υπολογιστικό χώρο και χρόνο κατά την συγγραφή του κώδικα καθώς με μία πράξη προσθαφαίρεσης εξοικονομούμε τον παραπανίσιο χρόνο που θα χρειαζόταν για το κάλεσμα μίας επιπλέον συνάρτησης.

4.3 Εργαλεία

4.3.1 Wireshark

Το εργαλείο Wireshark (41) είναι ένα λογισμικό ανοιχτού κώδικα με στόχο την ανίχνευση και ανάλυση πρωτοκόλλων δικτύου με βάση την διεύθυνση διαδικτυακού πρωτοκόλλου IP. Χρησιμοποιεί μορφοποιήσεις αρχείων όπως το pcap, το tcpdump για να διαβάζει πακέτα από το δίκτυο και να τα περιγράφει με απλό και κατανοητό τρόπο. Η λειτουργία αποτελείται από δύο μεθόδους. Στην πρώτη περίπτωση μπορεί να ανιχνεύσει ή να διαβάσει όλα τα πακέτα κίνησης στο κανάλι του δικτύου ενώ στην δεύτερη διαβάζει μόνο τα πακέτα που ανήκουν στον κόμβο όπου φιλοξενείται το λογισμικό.

Το Wireshark υποστηρίζει ένα ευρύ φάσμα χαρακτηριστικών για την αναπαράσταση πληροφοριών πακέτων IP όπως τα παρακάτω :

- Ζωντανή καταγραφή και ανάλυση εκτός σύνδεσης
- Ολοκληρωμένη ανάλυση εκατοντάδων πρωτοκόλλων, ενώ νέα προστίθενται σε τακτική βάση.
- Παροχή τυπικού φυλλομετρητή πακέτων τριών παραθύρων

Τέλος το Wireshark παρέχει προεπιλεγμένα πεδία εύχρηστα προς ανάλυση όπως :

- Αριθμός πακέτου
- Ώρα πραγματοποίησης αποστολής-λήψης πακέτου
- Διεύθυνση πηγής
- Διεύθυνση προορισμού
- Όνομα πρωτοκόλλου
- Πληροφορίες σχετικά με το πρωτόκολλο
- Αναλυτικά πεδία και τα περιεχόμενα και το μήκος των πακέτων

4.3.2 EditCap SplitCap

Το EditCap είναι ένα ενσωματωμένο βοηθητικό εργαλείο γενικής χρήσης του Wireshark για την τροποποίηση αρχείων καταγραφής. Η κύρια χρήση του είναι να αφαιρεί πακέτα από τα αρχεία σύλληψης, αλλά μπορεί επίσης να χρησιμοποιηθεί για να αλλάξει τις μορφές των αρχείων σύλληψης και να εξάγει πληροφορίες σχετικά με αυτά.

4.3.3 SplitCap

Το SplitCap είναι ένα εργαλείο το οποίο μας επιτρέπει να χωρίσουμε αρχεία καταγραφής (PCAP) σε μικρότερα αρχεία βασιζόμενοι σε κριτήρια όπως των αριθμό των πακέτων, τον χρόνο, την φυσική διεύθυνση κ.α.

4.3.4 Γλώσσα προγραμματισμού Python

Η Python είναι μια αντικειμενοστρεφής γλώσσα προγραμματισμού υψηλού επιπέδου με δυναμική σημασιολογία που αναπτύχθηκε από τον Guido van Rossum. Χρησιμοποιείται για την ανάπτυξη ιστοσελίδων από την πλευρά του διακομιστή, την ανάπτυξη λογισμικού, τα μαθηματικά και τη συγγραφή σεναρίων συστήματος και είναι δημοφιλής για την ταχεία ανάπτυξη εφαρμογών. Λόγω του γεγονότος ότι η Python είναι μια γλώσσα ανοικτού κώδικα της κοινότητας, ένας μεγάλος αριθμός ανεξάρτητων προγραμματιστών δημιουργεί συνεχώς βιβλιοθήκες και λειτουργίες για αυτήν.

Ορισμένες χρήσεις της Python είναι :

- Δημιουργία εφαρμογών ιστού σε διακομιστή
- Δημιουργία ροών εργασίας που μπορούν να χρησιμοποιηθούν σε συνδυασμό με λογισμικό
- Σύνδεση σε συστήματα βάσεων δεδομένων
- Ανάγνωση και επεξεργασία αρχείων
- Εκτέλεση σύνθετων μαθηματικών
- Επεξεργασία μεγάλων δεδομένων (Big data)
- Γρήγορη δημιουργία πρωτοτύπων
- Ανάπτυξη λογισμικού έτοιμου για παραγωγή

4.4 Δεδομένα

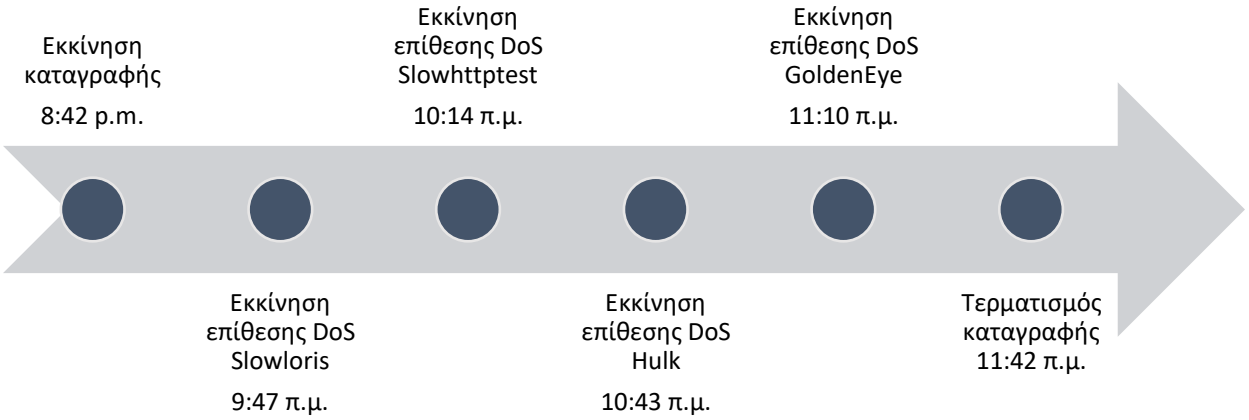
Το Ινστιτούτο Κυβερνοασφάλειας (CIC) του πανεπιστήμιο του Νιού Μπράνζουικ στον Καναδά διαθέτει στην ιστοσελίδα του ένα σύνολο δεδομένων αξιολόγησης ανίχνευσης εισβολής ονόματι Intrusion Detection Evaluation Dataset (CIC-IDS2017). Το CIC-IDS2017 περιέχει καλοήθη κίνηση σε συνδυασμό με τις πιο πρόσφατες κοινές επιθέσεις οι οποίες έχουν αρκετές ομοιότητες με τα αληθινά δεδομένα του πραγματικού κόσμου. Η βασική προτεραιότητα των συντελεστών ήταν να χτιστεί το συγκεκριμένο σύνολο δεδομένων με όσο το δυνατόν περισσότερο ρεαλιστική κίνηση. Αυτό επιτεύχθηκε σκιαγραφώντας την αφηρημένη συμπεριφορά των ανθρώπινων αλληλεπιδράσεων και δημιουργώντας μία φυσιολογική καλοήθη κυκλοφορία παρασκήνιο.
Η καταγραφή του αρχείου διήρκησε πέντε μέρες ξεκινώντας από τη Δευτέρα 3 Ιουλίου του 2017 στις 9:00 π.μ. και τελειώνοντας την Παρασκευή Ιουλίου του 2017 στις 5:00 μ.μ. Ωστόσο λόγω του αντικειμένου που πραγματευόμαστε στην παρούσα διπλωματική, θα χρησιμοποιήσουμε το σύνολο δεδομένων έλαβαν μέρος την Τετάρτη 5 Ιουλίου όπου πραγματοποιήθηκαν επιθέσεις κατανεμημένης και μη άρνησης υπηρεσιών.

4.4.1 Ταυτοποίηση Ρόλων

Κατά την καταγραφή των επιθέσεων, ρόλο θύματος και θύτη έχουν τα παρακάτω μηχανήματα:
Επιτιθέμενος (Attacker) : 205.174.165.73 Kali Linux.
Θύμα (Victim-Target): 205.174.165.68 (Local IP192.168.10.50) WebServer Ubuntu
Ωστόσο στο αρχείο καταγραφής, λόγω της μετάφρασης διεύθυνσης δικτύου (NAT) στο τείχος προστασίας θα δούμε τις IP να μορφοποιούνται ως εξής :
Επίθεση (Attack): 205.174.165.73 -> 205.174.165.80 (Valid IP of the Firewall) -> 172.16.0.1 -> 192.168.10.50
Απάντηση(Reply): 192.168.10.50 -> 172.16.0.1 -> 205.174.165.80 -> 205.174.165.73
4.4.2 Ροή Δεδομένων

Η εκκίνηση της καταγραφής γίνεται στις 8:42 π.μ. . Στο διάστημα μεταξύ 8:42 π.μ. και 9:46 π.μ. η κίνηση του δικτύου είναι φυσιολογική. Στις 9:47 π.μ. ξεκινά η πρώτη επίθεση είδους άρνησης υπηρεσιών **Slowloris** από το μηχάνημα 205.174.165.73 (Kali Linux) προς το θύμα 205.174.165.68 (WebServer Ubuntu). Η επίθεση άρνησης Slowloris τελειώνει 10:10 π.μ. και για τα επόμενα τέσσερα λεπτά (έως τις 10:13 π.μ.) η κίνηση του δικτύου είναι ομαλή. Στις 10:14 π.μ. εκκινείται από τον επιτιθέμενο (205.174.165.73) η δεύτερη επίθεση ονόματι Slowhttptest προς το θύμα 205.174.165.68 (WebServer Ubuntu). Η επίθεση άρνησης υπηρεσίας Slowhttptest τελειώνει 10:35 π.μ. και για τα επόμενα 7 λεπτά (έως τις 10:42 π.μ.) η κίνηση του δικτύου είναι ομαλή. Στις 10:43 π.μ. εκκινείται από τον επιτιθέμενο

(205.174.165.73) η τρίτη επίθεση είδους DoS Hulk προς το θύμα 205.174.165.68 (WebServer Ubuntu). Η συγκεκριμένη επίθεση τελειώνει 11:00 π.μ. και για τα επόμενα 9 λεπτά (έως τις 11:09 π.μ.) η κίνηση του δικτύου είναι ομαλή. Στις 11:10 π.μ. εκκινείται από τον επιτιθέμενο (205.174.165.73) η τέταρτη επίθεση άρνησης υπηρεσιών GoldenEye προς το θύμα 205.174.165.68 (WebServer Ubuntu).Η επίθεση DoS GoldenEye τελειώνει 11:23 π.μ. Στο σύνολο δεδομένων εκτελείτε και άλλη μία επίθεση είδους Heartbleed Port 444, στις 15:12 μ.μ. με διάρκεια είκοσι (20) λεπτών, ωστόσο για οικονομία υπολογιστικών πόρων και χρόνου θα παραλείψουμε αυτήν την επίθεση. Η καταγραφή την ημέρα Τετάρτη 5 Ιουλίου διαρκεί περίπου 8 ώρες και 40 λεπτά αλλά παραλείποντας την τελευταία επίθεση και λαμβάνοντας υπόψη ένα ορισμένο παράθυρο χρόνου ομαλής κίνησης μετά την τέταρτη επίθεση (GoldenEye) καταλήγουμε σε μια συνολική διάρκεια 3 ωρών (8:42 π.μ. έως 11:42 π.μ.).



Εικόνα 14: Χρονοδιάγραμμα καταγραφής

4.4.3 Διαχείριση Δεδομένων

Γνωρίζουμε πως η έκταση του τελικού αρχείου καταγραφής αποτελείται από περίπου 10.3 εκατομμύρια πακέτα. Είναι προφανές πως πρέπει να πραγματοποιηθεί κατακερματισμός των αρχείων για δύο λόγους. Ο πρώτος λόγος είναι πως ο κατακερματισμός της καταγραφής σε μικρότερα πακέτα μας εξοικονομεί πολύτιμο υπολογιστικό χρόνο. Σημειώνεται εδώ πως η μέγιστη πολυπλοκότητα του κώδικα για εξαγωγή μετρικών όπως η από κοινού Εντροπία μεταξύ δύο κατανομών, για παράδειγμα της διεύθυνσης πηγής και προορισμού, για ολόκληρη την καταγραφή μπορεί να φτάσει έως και $O(n^3)$. Οπότε κρίνεται αναγκαίο να μοιράσουμε τα πακέτα σε μικρότερα έτσι να επιτύχουμε μικρότερους υπολογιστικά χρόνους. Ο δεύτερος λόγος είναι η εξαγωγή συμπερασμάτων σε ότι αναφορά τις μετρικές που εμπλέκονται με την έρευνα μας.

Για παράδειγμα για να μπορούμε να εντοπίσουμε πότε ένα χρονικό παράθυρο κίνησης παρουσιάζει ανωμαλίες θα πρέπει να γνωρίζουμε ένα κατώφλι τιμών στο οποίο έχουμε, ή δεν έχουμε, φυσιολογική κίνηση. Αυτό καθίσταται δυνατό με την εύρεση μετρικών σε μικρότερα χρονικά παράθυρα, και στην συνέχεια, υπολογίζοντας την τυπική απόκλιση και διασπορά των τιμών αυτών να έχουμε μια πιο ολοκληρωμένη και αξιόπιστη εικόνα για το που θα κινηθούμε στον ορισμό των κατωφλιών και γενικότερα στο πως θα γίνεται αντιληπτή η κανονικότητα ή μη της κίνησης.

4.5 Πειραματικό μέρος

Στο πρώτο πειραματικό μέρος της παρούσας πτυχιακής εργασίας αναπτύσσοντας κώδικα σε γλώσσα γραφής Python (42) θα προσεγγίσουμε το σύνολο δεδομένων CIC-IDS2017 (43) του πανεπιστημίου του Νιού Μπράνζουικ παρατηρώντας μετρικές της θεωρίας πληροφορίας που προκύπτουν κατά την μελέτη του.

Σε αυτό το σημείο πρέπει να αναλογιστούμε ως προς ποιες μεταβλητές θα πρέπει να υπολογίσουμε έννοιες όπως την εντροπία του Shannon, την υπό συνθήκη εντροπία κ.α. Στην περίπτωση που το σύνολο δεδομένων περιείχε κατανεμημένη επίθεση τότε θα ήταν συνετό να εξετάσουμε την εντροπία του Shannon συναρτήσει της μεταβλητής διεύθυνσης προορισμού, διότι ευελπιστώντας να εξάγουμε συμπεράσματα, θα ήταν η μετρική που θα παρουσίαζε μικρότερη τυχαιότητα και κατά συνέπεια μικρότερη τιμή εντροπίας. Γνωρίζουμε πως κατά την διάρκεια μία κατανεμημένης επίθεσης άρνησης υπηρεσιών το δίκτυο botnet επιτίθεται από πολλά διαφορετικά τερματικά σε ένα κοινό στόχο-θύμα.

Ωστόσο η καταγραφή κίνησης που έχουμε στην διάθεση μας δεν έχει κατανεμημένη φύση. Η επίθεση απαρτίζεται από έναν και μόνο επιτιθέμενο. Για αυτό θα υπολογίσουμε την εντροπία τόσο βάση της διεύθυνσης πηγής όσο και της διεύθυνσης προορισμού. Επιπρόσθετα, για τις μετρικές από κοινού εντροπία και υπό συνθήκη εντροπία, τα δύο διανύσματα που θα εξεταστούν θα είναι και πάλι οι διευθύνσεις πηγής και προορισμού.

4.5.1 Ορισμός κατωφλιού μέσο της μελέτης της ομαλής κίνησης

Οι υπολογισμοί που αφορούν τις παραπάνω μετρικές εφαρμόστηκαν για την ομαλή αλλά και την ανώμαλη κίνηση. Έχοντας χωρίσει τα πακέτα σε παράθυρο χρόνου πέντε λεπτών όπως περιεγράφηκε στην ενότητα 4.4.3 Διαχείριση Δεδομένων, θα εξετάσουμε για αρχή μόνο την ομαλή κίνηση. Βασικός σκοπός μας είναι να προσδιορίσουμε ένα κατώφλι τιμών, γύρω από το οποίο θα μπορούμε να διαπιστώσουμε εάν η κίνηση του είναι φυσιολογική (44). Απομονώσαμε τα παράθυρα χρόνου κατά τα οποία η κίνηση είναι αυστηρά ομαλή.

Σημειώνεται πως στην αρχή της καταγραφής (8:42 έως 9:17) παρατηρούνται ασυνήθιστα χαμηλές τιμές στην μετρική της εντροπίας σχετικα με τις παραγόμενες από τα υπόλοιπα παράθυρα χρόνου που περιέχουν ομαλή κίνηση. Με την μελέτη του συνόλου δεδομένων στα πρώτα αυτά λεπτά διαπιστώνουμε πως ο λόγος ύπαρξης αυτών των τιμών είναι η φύση της καταγραφής και τίποτα παραπάνω. Παρατηρείται συνεχομένη λήψη και αποστολή μηνυμάτων μεταξύ ίδιων αλλά άσχετων με την επίθεση διευθύνσεων IP, πράγμα το οποίο τονίζει τα μειονεκτήματα ενός προσομοιωμένου συνόλου δεδομένων έναντι σε ένα πραγματικό (45). Τονίζεται πως η καθιέρωση των κατωφλιών είναι αυθαίρετη καθώς πολλές παράμετροι και ιδιαιτερότητες μπορούν να μεταβάλουν τα κριτήρια κατά τα οποία μπορούμε να αξιολογήσουμε και να συμπεράνουμε την φυσιολογικότητα ή μη της κίνησης.

Διάγραμμα 1: Τιμή Εντροπίας Shannon διεύθυνσης προορισμού αποκλειστικα για την ομαλή κίνηση

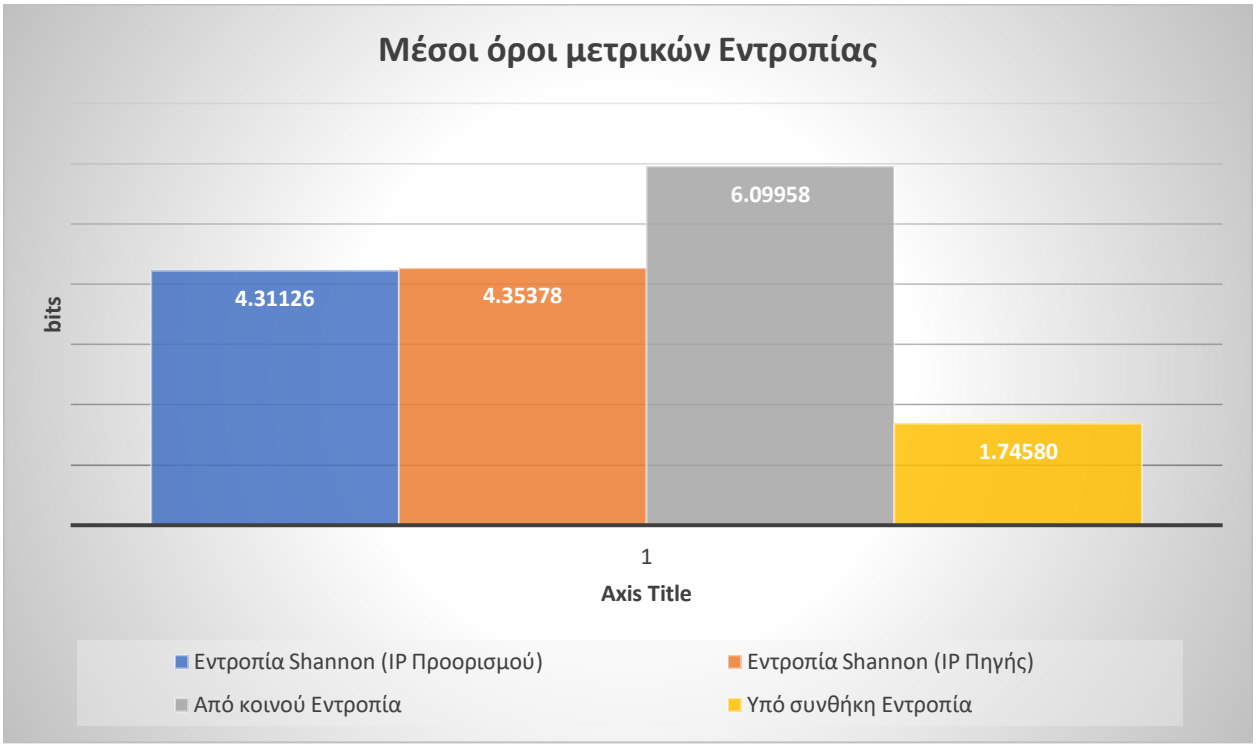
Διάγραμμα 2: Τιμή Εντροπίας Shannon διεύθυνσης πηγής αποκλειστικα για την ομαλή κίνηση

Διάγραμμα 3: Τιμή της Από κοινού Εντροπίας μεταξύ διεύθυνσης πηγής και προορισμού αποκλειστικα για την ομαλή κίνηση

Διάγραμμα 4: Τιμή της Υπό Συνθήκης Εντροπίας H(Διεύθυνση προορισμού | Διεύθυνση πηγής) αποκλειστικά για την ομαλή κίνηση

Στο Διάγραμμα 5 παρουσιάζονται οι μέσοι όροι που προέκυψαν από τις εξής μετρικές :

- Εντροπία Shannon, με τυχαία μεταβλητή της διεύθυνση προορισμού
- Εντροπία Shannon, με τυχαία μεταβλητή της διεύθυνση πηγής
- Από κοινού Εντροπία μεταξύ διευθύνσεων πηγής και προορισμού
- Υπό συνθήκη Εντροπία *H*(Διεύθυνση προορισμού | Διεύθυνση πηγής)



Διάγραμμα 5: Μέσοι όροι μετρικών Εντροπίας

Ο προσδιορισμός της τιμή του κατωφλίου εξαρτάται άμεσα από το εκάστοτε σύνολο δεδομένων. Βασιζόμενοι στο Διάγραμμα 5 θεωρούμε πως στην εν λόγω καταγραφή τα κατώφλια τιμών θα καθοριστούν με την βοήθεια των παραπάνω τιμών.

Έχουν ερευνηθεί διαφορετικές μεθοδολογίες για τον υπολογισμό και τον αποδοτικό προσδιορισμό του ορίου πέρα του οποίου η κίνηση θεωρείται μη φυσιολογική (46) (47). Ωστόσο στην μελέτη μας θα χρησιμοποιήσουμε μία στατιστική προσέγγιση προσπαθώντας να ορίσουμε ένα κατώτατο όριο της τιμής της εντροπίας (48). Είναι αντιληπτό πως η εντροπία της ανώμαλης κίνησης θα διαφέρει από αυτήν της ομαλής. Σαφέστατα, για ένα διαφορετικό σύστημά θα μπορούσε οι μέσοι όροι των μετρικών εντροπίας να κινούνται σε διαφορετικές περιοχές τιμών. Μια λογική πρακτική θα ήταν να πάρουμε την ελάχιστη τιμή και να ορίσουμε αυτή ως κατώτατο όριο. Κάτι τέτοιο όμως δεν θα ήταν λειτουργικό καθώς η εντροπία δεν παραμένει σταθερή σε κάθε παράθυρο χρόνου. Είναι αναγκαία η αποδοτική παραμετροποίηση του υπολογισμού του κατωφλιού καθώς δεν γνωρίζουμε εκ των προτέρων πως μπορούν να κινηθούν οι τιμές εντροπίας κατά την διάρκεια επίθεσης.

Προσεγγίζοντας το ζήτημα αναζήτησης του κατωφλιού στατιστικά θα προσδιορίσουμε την τιμή του χρησιμοποιώντας την εξίσωσηΕξίσωση 6)**:**

Τιμή κατωφλιού = μέση τιμή εντροπίας – τυπική απόκλιση

Εξίσωση 6: Τύπος υπολογισμού κατωφλιού

Η τυπική απόκλιση ενός δείγματος δίνεται από την εξίσωσηΕξίσωση 7) :

$$\sigma = \sqrt{\frac{1}{N}\sum_{i=1}^{N}(\tilde{x} - x_i)^2}$$

Εξίσωση 7: Τύπος τυπικής απόκλισης

Όπου N είναι το πλήθος των τιμών και $\tilde{x}$ είναι η μέση τιμή των τιμών του δείγματος x_i. Από τους υπολογισμούς έχουμε:

	Εντροπία Shannon (Διεύθυνση Προορισμού)	**Εντροπία Shannon (Διεύθυνση Πηγής)**	**Από κοινού Εντροπία**	**Υπό συνθήκη Εντροπία**
Μέσος όρος	4,31258	4,35378	6,09958	1,74580
Τυπική Απόκλιση	1,77705	1,81596	2,79864	0,99493
Τιμή Κατωφλίου	2.53553	2.53782	3,30094	0,75087

Πίνακας 2: Τιμές κατωφλίου Εντροπίας

4.5.2 Μελέτη της συνολικής κίνησης

Έχοντας ορίσει το φάσμα των τιμών στο οποίο παραδεχόμαστε πως η κίνηση του δικτύου είναι φυσιολογική-ομαλή θα παρατηρήσουμε την περιοχή που κυμαίνονται οι μετρικές της θεωρίας πληροφορίας για όλη την καταγραφή της κίνησης (ομαλή και μη).

Διάγραμμα 6: Τιμή Εντροπίας Shannon διεύθυνσης προορισμού

Διάγραμμα 7: Τιμή Εντροπίας Shannon διεύθυνσης πηγής

Διάγραμμα 8: Τιμή Από κοινού Εντροπίας μεταξύ διεύθυνσης πηγής και προορισμού

Διάγραμμα 9: Τιμή Υπό Συνθήκης Εντροπίας H(Διεύθυνση προορισμού | Διεύθυνση πηγής)

Στην συνέχεια υπολογίζουμε τον αριθμό αλλά και των ρυθμό των πακέτων που αποστέλλονται σε κάθε επίθεση ξεχωριστά στα χρονικά παράθυρα που έχουμε ορίσει (**Error! Reference source not found.** και Πίνακας 4).

Είδος επίθεσης	Χρονικό παράθυρο	Αριθμός πακέτων
Επίθεση Slowloris	9:47 - 9:52	85854
	9:52 – 9:57	94428
	9:57 – 10:02	92260
	10:02 – 10:07	100922
	10:07 – 10:10	25007
Επίθεση Slowhttptest	10:14 – 10:17	71326
	10:17 – 10:22	71019
	10:22 – 10:27	66554
	10:27 – 10:32	61437
	10:32 – 10:35	41332
Επίθεση DoS Hulk	10:43 – 10:47	**662056**
	10:47 – 10:52	**691411**
	10:52 – 10:57	**764569**
	10:57 – 11:00	**600856**
Επίθεση GoldenEye	11:10 – 11:12	102556
	11:12 – 11:17	70770
	11:17 – 11:22	103601
	11:22 – 11:23	12656

Πίνακας 3: Αριθμός πακέτων σε κάθε χρονικό παράθυρο εκάστοτε επίθεσης

Είδος επίθεσης	Χρονικό παράθυρο	Ρυθμός αποστολής πακέτων (packets/sec)
Επίθεση Slowloris	9:47 - 9:52	286.29
	9:52 – 9:57	314.84
	9:57 – 10:02	307.63
	10:02 – 10:07	336.43
	10:07 – 10:10	233.76
Επίθεση Slowhttptest	10:14 – 10:17	420.2
	10:17 – 10:22	236.83
	10:22 – 10:27	221.89
	10:27 – 10:32	204.59
	10:32 – 10:35	232.05
Επίθεση DoS Hulk	10:43 – 10:47	**2076.81**
	10:47 – 10:52	**2305.31**
	10:52 – 10:57	**2549.04**
	10:57 – 11:00	**2362.32**
Επίθεση GoldenEye	11:10 – 11:12	626.53
	11:12 – 11:17	235.9
	11:17 – 11:22	345.37
	11:22 – 11:23	124.87

Πίνακας 4: Ρυθμός αποστολής πακέτων σε κάθε χρονικό παράθυρο εκάστοτε επίθεσης

4.5.3 Συμπεράσματα μετρήσεων

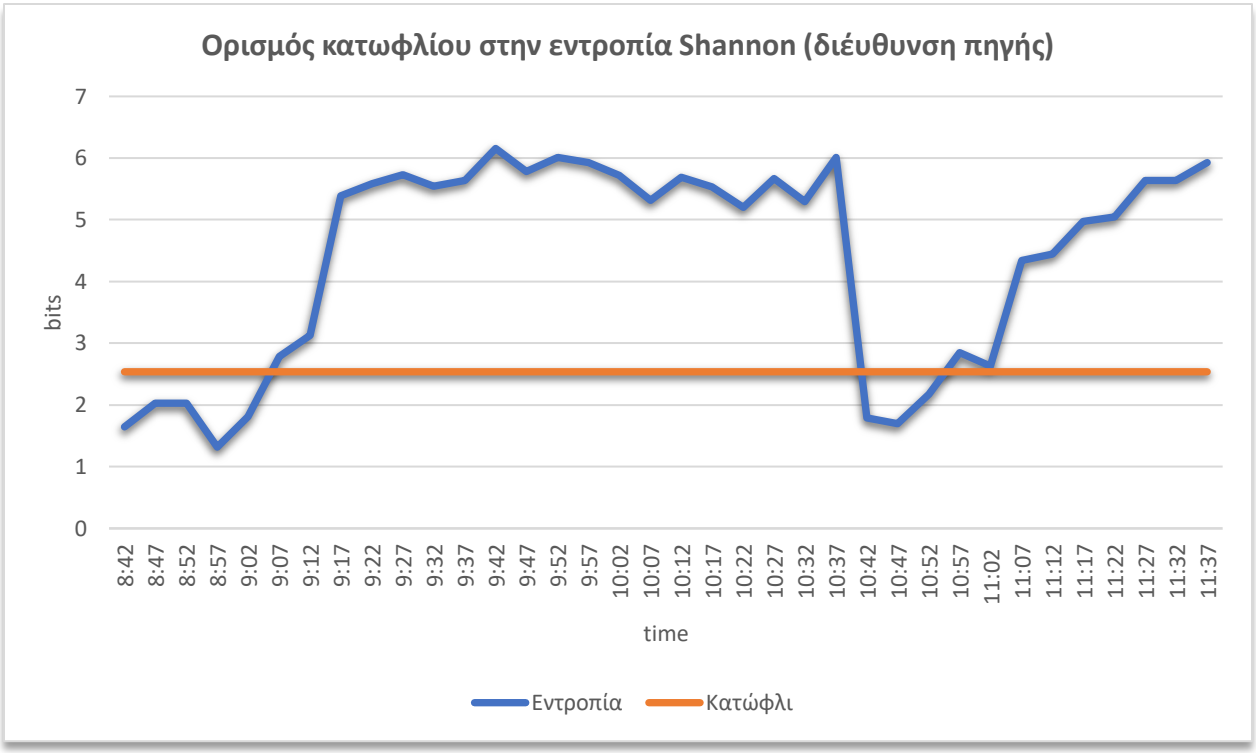
Εξετάζοντας τα αποτελέσματα των μετρήσεων μας φτάσαμε σε χρήσιμα συμπεράσματα σε ότι αφορά την συμπεριφορά τόσο των επιθέσεων όσο και των μαθηματικών εννοιών που χρησιμοποιήθηκαν για την μελέτη. Αρχικά πρέπει να αντιληφθούμε την φύση των επιθέσεων.

Όλες οι επιθέσεις που εφαρμόστηκαν κατά την διάρκεια της εξεταζόμενης καταγραφής, με εξαίρεση την επίθεση άρνησης υπηρεσιών Hulk, δεν βασίζονται στον όγκο πακέτων που αποστέλλουν για να βλάψουν τον στόχο-θύμα, άλλα στον ιδιαίτερο χειρισμό των αιτημάτων (46). Είναι οι λεγόμενες αργές επιθέσεις (slow attacks), μία από τις οποίες περιγράφεται εκτενέστερα στην ενότητα *2.4.2 Επίθεση Slowloris*. Τα

αποτελέσματα μαρτυρούν πως οι τιμές των μετρικών δικαιολογούν πλήρως την ύπαρξη της τρίτης επίθεσης (Hulk) ωστόσο δεν βοηθούν στην ανίχνευση των υπόλοιπων επιθέσεων. Συμπεραίνουμε συνεπώς πως η χρήση των εννοιών που πηγάζουν από την θεωρία πληροφορίας δεν μπορούν να φανούν λειτουργικές στην ανίχνευση αργών (slow) επιθέσεων και γενικά επιθέσεων που δεν σκοπεύουν να βλάψουν το θύμα με την αποστολή πακέτων με υψηλό ρυθμό (πλημμύρα).

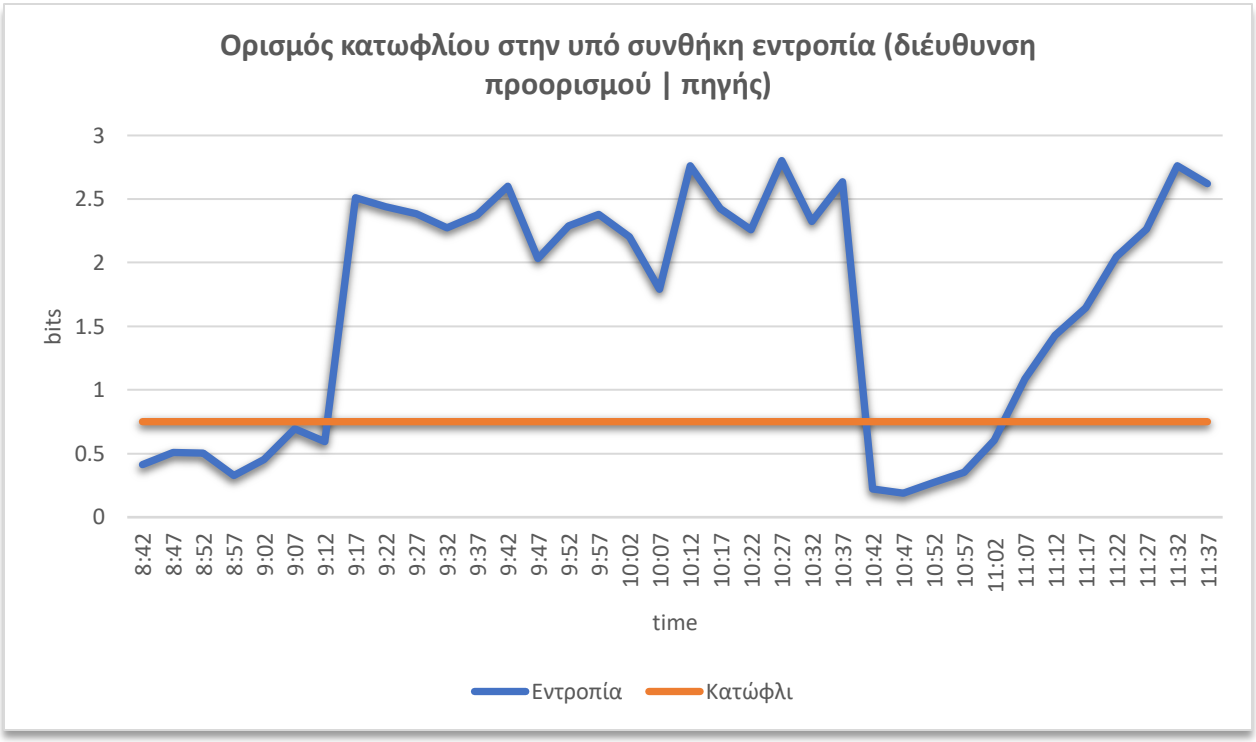
Στην ανίχνευση της επίθεσης Hulk συνδράμει επίσης η χρήση του κατωφλίου που ορίσαμε στην ενότητα 4.5.1 Ορισμός κατωφλιού μέσο της μελέτης της ομαλής κίνησης. Επαναλαμβάνουμε πως εξαιρούμε από τα συμπεράσματα μας τις τιμές στην αρχή της καταγραφής. Οι χαμηλές τιμές εντροπίας που ανιχνεύονται σε αυτά τα σημεία είναι απόρροια της φύσης του συνόλου δεδομένων και δεν περιέχουν επίθεση.

Διάγραμμα 10: Ορισμός κατωφλίου για εντροπία Shannon (διεύθυνση προορισμού)



Διάγραμμα 11: Ορισμός κατωφλίου για εντροπία Shannon (διεύθυνση πηγής)

Διάγραμμα 12: Ορισμός κατωφλίου στην απο κοινού εντροπία (διέυθυνση πηγής, διεύθυνση προορισμού)



Διάγραμμα 13: Ορισμός κατωφλίου στην υπό συνθήκη εντροπία (διεύθυνση προορισμού | πηγής)

Καταλήγουμε πως σε ένα σύστημα ανίχνευσης θα ήταν λειτουργικό το κατώφλι που χρησιμοποιήθηκε καθώς ξεπερνιέται μόνο κατά την διάρκεια της επίθεσης. Τονίζουμε ωστόσο πως σε μία διαφορετική καταγραφή οι τιμές τόσο του κατωφλίου όσο και των μετρικών της εντροπίας θα μπορούσαν να κυμαίνονται σε διαφορετικά επίπεδα.

4.5.4 Μεθοδολογία ανίχνευσης υπολοίπων επιθέσεων καταγραφής

Σε αυτήν την υποενότητα θα προσεγγίσουμε μια θεωρητική ανάλυση για την ανίχνευση των επιθέσεων που δεν μπορούσαν να γίνουν αντιληπτές με μετρικές από την θεωρία πληροφορίας. Ανατρέχοντας στην βιβλιογραφία της επιστημονικής κοινότητας διαπιστώνουμε πως η ανίχνευση αργών επιθέσεων (slow attacks) άρνησης υπηρεσιών είναι δυνατό να ανιχνευθούν με διάφορους τρόπους, με σημαντικότερους από αυτούς την συμπεριφορική ανάλυση του δικτύου (50) (51) και την ανάπτυξη τεχνικών μετρήσεων με σκοπό την ανακάλυψη στατιστικών ανωμαλιών εντός των αρχείων καταγραφής (52). Έχοντας ωστόσο στην διάθεση μας ένα σύνολο δεδομένων το οποίο δεν είναι πραγματικό αλλά αποτέλεσμα προσομοίωσης αποφανθήκαμε πως η συμπεριφορική ανάλυση του δικτύου είναι πιθανό να οδηγεί σε αναξιόπιστα αποτελέσματα. Για αυτό τον λόγο θα χρησιμοποιήσουμε την μελέτη των Tripathi, Hubballi και Singh (52) που ακολουθούν μια στατιστική προσέγγιση γύρω από την μελέτη του αρχείου

καταγραφής. Συγκεκριμένα, θεώρησαν ότι η τυπική διαδικτυακή κυκλοφορία είναι μια κατανομή πιθανοτήτων που αποτελείται από τους τέσσερις τύπους αιτήσεων HTTP που αναφέρονται παρακάτω:

- Ολοκληρωμένα GET αιτήματα
- Ολοκληρωμένα POST αιτήματα
- Μη ολοκληρωμένα GET αιτήματα
- Μη ολοκληρωμένα POST αιτήματα

Η ταυτοποίηση του τύπου αυτών των αιτημάτων προέρχεται από την παρουσία ή μη συγκεκριμένης ακολουθίας χαρακτήρων στον περιεχόμενο των αιτημάτων.

Χρησιμοποιώντας τις προαναφερθείσες τέσσερις κατηγορίες αιτημάτων HTTP, πραγματοποιείται παρακολούθηση και δημιουργία ενός προφίλ κατανομής για περιόδους παρατήρησής συγκεκριμένης διάρκειας που αποτελείται από τέσσερα γνωρίσματα . Τα $P_{GET\ Complete}$, $P_{POST\ Complete}$, $P_{GET\ Incomplete}$, $P_{POST\ Incomplete}$ τα οποία αντιπροσωπεύουν την πιθανότητα εμφάνισης του κάθε ενός αιτήματος αντίστοιχα.

Στην συνέχεια υπολογίζονται τα γνωρίσματα για κάθε εκάστοτε παράθυρο χρόνου και συγκρίνονται μεταξύ τους με την βοήθεια της απόστασης Hellinger (53).

Κατά την εξαγωγή συμπερασμάτων σημειώθηκε πως όταν υπάρχει επίθεση, υποβάλλονται συνολικά περισσότερες ελλιπείς HTTP αιτήσεις, με αποτέλεσμα η κατανομή των πιθανοτήτων αυτών των αιτήσεων να αποκλίνει από την κανονική κατανομή και εν τέλει να παρατηρείται παρείσφρηση.

Κεφάλαιο 5: Συμπεράσματα – Μελλοντικές Προτάσεις

Σκοπός της παρούσας διπλωματικής εργασίας υπήρξε η οικουμενική προσέγγιση των συστημάτων ανίχνευσης παρεισφρήσεων και η ανάλυση, κατανόηση και παρατήρηση ενός συνόλου δεδομένων όσο το δυνατότερο σχετικό με μία ρεαλιστική καταγραφή που περιέχει επίθεση.

Κατηγοριοποιήσαμε τις επιθέσεις σύμφωνα με μοντέλο ανοιχτής διασύνδεσης συστημάτων (OSI model) και δόθηκε έμφαση σε εκείνες που ανήκουν στο επίπεδο εφαρμογών, των οποίων το είδος απαρτίζει κατά βάση το σύνολο δεδομένων που μελετήθηκε. Στην συνέχεια αναλύθηκαν διεξοδικά τεχνικές και μεθοδολογίες λειτουργίας των συστημάτων ανίχνευσης και πρόληψης παρεισφρήσεων συμπεραίνοντας πως η ανάπτυξη του εκάστοτε συστήματος δεν ακολουθεί κάποιον συγκεκριμένο κανόνα. Η φύση του εκάστοτε συστήματος καθώς και οι αποφάσεις του υπεύθυνου ασφαλείας αυτού είναι οι μεταβλητές που προσδιορίζουν τα συστατικά και την τεχνική που θα χρησιμοποιηθεί. Δεν μπορεί να θεωρηθεί πως κάποια τεχνική η μεθοδολογία είναι λανθασμένη ή ορθή διότι συνήθως κάθε τρόπος αντιμετώπισης παρουσιάζει υψηλότερη αποδοτικότητα σε διαφορετικούς τύπους επιθέσεων.

Σε ένα ιδανικό σενάριο θα θέλαμε να αναλύσουμε μια πραγματική καταγραφή που να περιέχει συμπεριφορικά φυσιολογική κίνηση ώστε να καταλήξουμε σε ρεαλιστικά συμπεράσματα. Ωστόσο η εύρεση τέτοιων καταγραφών δεν είναι δυνατή για τους λόγους που προαναφέρθηκαν στην ενότητα 4.1 Εισαγωγή.

Καταλήξαμε στην επιλογή της καταγραφής του πανεπιστημίου του Νιού Μπράνζουικ στον Καναδά ονόματι Intrusion Detection Evaluation Dataset (CIC-IDS2017) που περιέχει προσομοίωση επίθεσης άρνησης παροχής υπηρεσιών. Ακολουθήθηκε μια στατιστικομαθηματική προσέγγιση με την χρήση εννοιών της θεωρίας πληροφορίας και κατά βάση της εντροπίας. Στις περιπτώσεις όπου η συγκεκριμένη μεθοδολογία δεν παρείχε επιθυμητά αποτελέσματα προτείνεται η προσέγγιση με την στατιστική τεχνική που αναλύθηκε στην ενότητα 4.5.4 Μεθοδολογία ανίχνευσης υπολοίπων επιθέσεων καταγραφής.

Μελετώντας το παραπάνω σύνολο δεδομένων καταλήξαμε στα εξής συμπεράσματα :

- Οι επιθέσεις που περιέχονται στο σύνολο δεδομένων,πέρα από την επίθεση άρνησης υπηρεσιών Hulk, δεν μπορούν να ανιχνευθούν με τις μετρικές της θεωρίας πληροφορίας και ειδικά με την εντροπία και τις επιμέρους εκδοχές της (βλέπε διαγράμματα Διάγραμμα 10Διάγραμμα 11Διάγραμμα 12 καιΔιάγραμμα 13). Η φύση των επιθέσεων αυτών δεν είναι ογκομετρική αλλά γίνεται εκμετάλλευση των τρωτών σημείων του συστήματος με την παραμετροποίηση των υπηρεσιών του πρωτοκόλλου HTTP/HTTPS.
- Η επίθεση άρνησης υπηρεσιών Hulk είναι παρεμφερείς με την Http Flood, που έχει αναλυθεί στην ενότητα 2.4.3, είναι μια ογκομετρική επίθεση και με την βοήθεια των μετρικών της θεωρίας πληροφορίας μπορεί αν ανιχνευθεί (βλέπε διαγράμματαΔιάγραμμα 10Διάγραμμα 11Διάγραμμα 12 καιΔιάγραμμα 13). Προϊδεασμός ύπαρξης παρείσφρησης μπορεί να προκύψει και από τον πίνακα Πίνακας 4: Ρυθμός αποστολής πακέτων σε κάθε χρονικό παράθυρο εκάστοτε επίθεσης όπου παρατηρείται υψηλή αύξηση στην ρυθμό αποστολής των πακέτων κατά την διάρκεια της συγκεκριμένης επίθεσης.
- Παρατηρώντας τα διαγράμματα που προέκυψαν από την μελέτη του δείγματος βλέπουμε ένα διάστημα στην αρχή της καταγραφής όπου οι τιμές των μετρικών της εντροπίας είναι ασυνήθιστα χαμηλές. Τόσο χαμηλές που κινούνται σε επίπεδα κοντά στις τιμές της εντροπίας που παρατηρούμε κατά την διάρκεια της επίθεσης Hulk. Σε περίπτωση που δεν γνωρίζαμε πότε

λαμβάνει μέρος επίθεση, από τις μετρικές της εντροπίας θα συμπεραίναμε πως στο συγκεκριμένο διάστημα εκτελείται επίθεση. Ωστόσο στο συγκεκριμένο σημείο δεν λαμβάνει χώρα καμία επίθεση. Υπάρχει μόνο ομαλή κίνηση. Μετά από εκτενή από εκτενή έλεγχο της καταγραφής διαπιστώνεται η επαναλαμβανόμενη αποστολή και λήψη μηνυμάτων μεταξύ συγκεκριμένων διευθύνσεων πρωτοκόλλου, γεγονός το οποίο έχει ως αποτέλεσμα της ύπαρξη χαμηλών τιμών εντροπίας.

- Το κατώφλι τιμών, άνω ή κάτω όριο ανάλογα με την μεθοδολογία που χρησιμοποιείται, αποτελεί μία αυθαίρετη διαδικασία που σχετίζεται άμεσα με την φύση του εκάστοτε συνόλου δεδομένων. Σε μία καταγραφή όπου τα μηχανήματα που αλληλοεπιδρούν είναι λίγα, χαμηλότερες τιμές εντροπίας θα οδηγήσουν σε χαμηλότερο κατώφλι, δυσκολεύοντας έτσι την εξαγωγή συμπερασμάτων. Ωστόσο σε ένα σύστημα που αποτελείται από πολλά τερματικά, η μεγαλύτερη τυχαιότητα του συστήματος θα οδηγήσει σε υψηλούς μέσους όρους εντροπίας, με συνέπεια μια ογκομετρική επίθεση να είναι ευκολότερο να ξεχωρίσει και να ανιχνευθεί.

Στο πλαίσιο των μελλοντικών προτάσεων της παρούσας διατριβής, θα αναλογιστούμε μεθοδολογίες που θα μπορούσαν να βελτιστοποιήσουν την πρόληψη και ανίχνευση επιθέσεων της μελέτης καταγραφών. Αναλύοντας πολλές επιθέσεις παρατηρήσαμε πως οι τεχνικές ανίχνευσης τους διαφέρουν ανάλογα με την φύση και την συμπεριφορά της επίθεσης. Κάθε επίθεση εκμεταλλεύεται ένα τρωτό σημείο του συστήματος και έτσι αναπτύσσοντας εργαλεία που χρησιμοποιούν μία μεθοδολογία αυξάνονται οι πιθανότητες να μην είναι δυνατή η ανίχνευση. Προτείνεται λοιπόν ένα υβριδικό σύστημα που θα συνδυάζει την ανάλυση της συμπεριφοράς του δικτύου τόσο από στατιστικομαθηματική πλευρά όσο και από την πλευρά εξέτασης παραμετροποιήσεων των ιδιοτήτων των πρωτοκόλλων που χρησιμοποιούνται για την αποστολή πακέτων. Επίσης προτείνεται ο ορισμός κατωφλίου από εκ νέου υπολογισμούς με κυλιόμενα παράθυρα σε εγγυημένα ασφαλής συνθήκες για το δίκτυο. Η ανάπτυξη του μεγέθους του παρόχου και η αύξηση της επισκεψιμότητας μπορεί να αλλάξει σημαντικά τα συστατικά της καταγραφής οπότε είναι συνετό να πραγματοποιείτε μια δυναμική εκτίμηση του κατωφλίου.

Βιβλιογραφικές Αναφορές

1. **Qian Wang, Timothy Dunlap, Youngho Cho, Gang Qu.** *DoS attacks and countermeasures on network devices.* s.l. : IEEE, 2017.

2. *A survey of network anomaly detection techniques.* **Mohiuddin Ahmed, Abdun Naser Mahmood , Jiankun Hu.** 2016.

3. **Mahsa Nooribakhsh, Mahdi Mollamotalebi.** *A review on statistical approaches for anomaly detection in DDoS attacks.* 2020.

4. **Sarita Tripathy, Prof(Dr.)Laxman Sahoo.** A Survey of different methods of clustering for anomaly detection. International Journal of Scientific & Engineering Research, Volume 6, 2015.

5. **Gerhard Münz, Sa Li, G. Carle.** *Traffic Anomaly Detection Using K-Means Clustering.* 2007.

6. **Domenico Vitali, Antonio Villani, Angelo Spognardi, Roberto Battistoni.** *DDoS detection with information theory metrics and netflows: A real case.* 2012.

7. **Andi Maslan, Kamaruddin Malik Bin Mohamad, Feresa Binti Mohd Foozy.** *Feature selection for DDoS detection using classification machine learning techniques.* 2020.

8. *Defensive performance comparison of firewall systems.* **Arunwan, Mingphum, Laong, Tanachad και Atthayuwat, Kiattichai.** s.l. : IEEE, 2016.

9. *A Model for Analysis of SYN Flood DoS Attacks.* **Nissanke, Nimal και Sun, Jun.** 2008.

10. *Enhanced Approach to Detection of SQL Injection Attack.* **Karuparthi, Raja Prasad και Zhou, Bing.** 2016.

11. *SQL filtering: An effective technique to prevent SQL injection attack.* **Rhythm Dubey, Himanshu Gupta.** s.l. : IEEE Conference on Computer Communications, 2016.

12. *Guide to Intrusion Detection and Prevention Systems (IDPS).* **Karen Scarfone (NIST), Peter Mell (NIST).** 2007.

13. *Counteract the Outflanking of DDoS Countermeasures : A Framework for Generating DDoS Defense Guidelines.* **Marcus Johansson, Peter Sjöholm.** 2015.

14. *Host vs Network-based intrusion detection systems.* **Institute, SANS.** s.l. : SANS Institute, 2000.

15. *Distributed Denial of Service Attack Detection Using a Machine Learning Approach.* **Gupta, Animesh.** 2018.

16. *INTRUSION DETECTION SYSTEM AND INTRUSION.* **Chakraborty, Nilotpal.** India : Devi Ahilya University, 2013.

17. *Difference between Intrusion Detection System (IDS) and Intrusion Prevention System (IPS).* **Asmaa Shaker Ashoor, Sharad Gore.** s.l. : Communications in Computer and Information Science, 2011.

18. *False alarm minimization techniques in signature-based intrusion.* **Neminath Hubballi, Vinoth Suryanarayanan.** India : Institute of Technology Indore, 2014.

19. *Signature-Based Anomaly intrusion detection using Integrated data mining classifiers.* **Warusia Yassin, Nur Izura Udzir.** s.l. : IEEE, 2014.
20. *Advanced Intrusion Detection Combining Signature-Based and Behavior-Based Detection Methods.* **Hee-Yong Kwon, Taesic Kim, Mun-Kyu Lee.** Korea : s.n., 2022.
21. *Signature Based Intrusion Detection for Zero-Day Attacks: (Not) A Closed Chapter?* **Holm, Hannes.** s.l. : IEEE, 2014.
22. **Karen Scarfone, Peter Mell.** *Guide to Intrusion Detection and Prevention Systems (IDPS).* National Institute of Standards and Technology : s.n., 2007.
23. *Deciphering Detection Techniques: Part II Anomaly-Based.* **Gong, Fengmin.** s.l. : McAfee Security, 2003.
24. **ojtaba Eskandari, Zaffar Haider Janjua, Massimo Vecchio, Fabio Antonelli.** *Passban IDS: An Intelligent Anomaly Based Intrusion Detection System for IoT Edge Devices.* 2020.
25. **Parisa Alaei, Fakhroddin Noorbehbahani.** *Incremental anomaly-based intrusion detection system using limited labeled data.* s.l. : IEEE, 2017.
26. **Paulo Angelo Alves Resende, André Costa Drummond.** *Adaptive anomaly-based intrusion detection system using genetic.* Brazil : s.n., 2018.
27. **Constantine Manikopoulos, Symeon Papavassiliou.** *Network Intrusion and Fault Detection: A Statistical Anomaly Approach.* s.l. : IEEE Communications Magazine, 2002.
28. **Symantec.** *Endpoint Protection: Statistical-Based Intrusion Detection.* 2003.
29. **David Goldberg, Yinan Shan.** *The Importance of Features for Statistical Anomaly Detection.* s.l. : USENIX, 2015.
30. *Anomalous Payload-based Network Intrusion.* **Ke Wang, Salvatore J. Stolfo.** Computer Science Department, Columbia University : s.n., 2017.
31. *An Evaluation Framework for Intrusion Detection Dataset.* **Amirhossein Gharib, Iman Sharafaldin , Arash Habibi Lashkari, Ali A. Ghorbani.** Pattaya, Thailand : IEEE, 2016.
32. *On the use of information theory metrics for detecting DDoS attacks and flash events: anempirical analysis, comparison, and future directions.* **Jagdeep Singh, Navjot Jyoti, Sunny Behal.** Ferozepur, Punjab, India : s.n., 2021.
33. *A Mathematical Theory of Communication.* **Shannon, Claude. E.** 1948.
34. *Information-Theoretic Measures for Anomaly Detection.* **Wenke Lee, Dong Xiang.** Oakland, CA, USA : IEEE, 2002 .
35. *An Entropy-Based Network Anomaly Detection Method.* **Przemysław Bereziński, Bartosz Jasiul, Marcin Szpyrka.** 2015.
36. *Conditional entropy approach for the evaluation of the coupling strength.* **A. Porta, G. Baselli, F. Lombardi, N. Montano, A. Malliani & S. Cerutti.** 1999.
37. *A conditional entropy bound for a pair of discrete random variables.* **H. Witsenhausen, A. Wyner.** s.l. : IEEE Transactions on Information Theory, 1975.

38. *Joint Entropy Analysis Model for DDoS Attack Detection.* **Hamza Rahmani, Nabil Sahli, Farouk Kammoun.** CRISTAL Lab., National School for Computer Sciences of Tunis : Fifth International Conference on Information Assurance and Security, 2009.

39. *Estimating mutual information.* **Alexander Kraskov, Harald Stögbauer, and Peter Grassberger.** 2004.

40. **Duncan, Tyrone E.** *SIAM Journal on Applied Mathematics - On the Calculation of Mutual Information.* 1970.

41. **Ulf Lamping, Richard Sharpe, and Ed Warnicke.** *Wireshark User's Guide.* 2004-2012.

42. **Organization, Python.** *What is Python? Executive Summary.* s.l. : Python Organization, 2023.

43. **Cybersecurity, Canadian Institute for.** *Intrusion Detection Evaluation Dataset (CIC-IDS2017).* s.l. : Canadian Institute for Cybersecurity, 2017.

44. *Deciding Optimal Entropic Thresholds to Calibrate the Detection Mechanism for Variable Rate DDoS Attacks in ISP Domain.* **Sardana, Anjali, Joshi, Ramesh και Kim, Tai-hoon.** Busan, Korea (South) : IEEE, 2008.

45. *Survey of intrusion detection systems: techniques, datasets and challenges.* **Ansam Khraisat, Iqbal Gondal, Peter Vamplew and Joarder Kamruzzaman.** 2019.

46. *An Online Entropy-Based DDoS Flooding Attack Detection System With Dynamic Threshold.* **Loïc D. Tsobdjou, Samuel Pierre, Alejandro Quintero.** s.l. : IEEE Transactions on Network and Service Management, 2022.

47. *An Entropy-Based Approach for Anomaly Detection in Activities of Daily Living in the Presence of a Visitor.* **Aadel Howedi, Ahmad Lotfi and Amir Pourabdollah.** s.l. : School of Science and Technology, Nottingham Trent University, Clifton Lane, Nottingham, 2020.

48. *A Statistical Approach to Detect Denial of Service Attacker.* **Mathew, Maria.** St.Joseph's College of Engineering & Technology, MACE, Kothamangalam : s.n., 2016.

49. **Enrico Cambiaso, Gianluca Papaleo, Giovanni Chiola, Maurizio Aiello.** *Trust Management in Computing and Communications, Chapter :Slow DoS attacks: definition and categorisation.* 2013.

50. *Detection of Slow DDoS Attacks based on User's Behavior Forecasting.* **Vitalii Savchenko, Oleh Ilin, Nikolay Hnidenko, Olga Tkachenko, Oleksander Laptiev, Svitlana Lehominova.** Kyiv, Ukraine : s.n., 2020.

51. *Detection of the botnets' low-rate DDoS attacks based on self-similarity.* **Sergii Lysenko, Kira Bobrovnikova, Serhii Matiukh, Ivan Hurman, Oleh Savenko.** Kyiv, Ukraine : s.n., 2020.

52. *How Secure are Web Servers? An Empirical Study of Slow HTTP DoS Attacks and Detection.* **Nikhil Tripathi, Neminath Hubballi, Yogendra Singh.** 2016.

53. **Shemyakin, Arkady.** Hellinger Distance and Non-informative Priors. 2014.

Παράρτημα κώδικα

```
#Υπολογισμος ρυθμού αποστολής πακέτων

from scapy.all import *

# Read the pcap file
packets = scapy.all.rdpcap('5minsample10…42_08_YES.pcapng')

# Calculate the packet rate
time_diff = packets[-1].time - packets[0].time
packet_count = len(packets)
packet_rate = packet_count / time_diff

# Print the packet rate
print("Packet rate: {:.2f}
packets/sec".format(packet_rate))



# Υπολογισμός Εντροπίας Shannon , Απο κοινου εντροπίας και
 # υπο συνθήκη εντροπίας διευθυνσης προορισμου και
διευθυνσης πηγη,

#### Functions ####
### Συνάρτηση υπολογισμού της εντροπίας μίας μεταβλητής με
βάση το θεώρημα Shannon
def shannon_entropy_cal(set):

    C= collections.Counter(set)
    counts= np.array(list(C.values()),dtype=float)
    prob= counts/counts.sum()
    shannon_entropy = (-prob*np.log2(prob)).sum()
    print("The value of Shannon_entropy is" ,
shannon_entropy)

#Συνάρτηση υπολογισμού της κοινής εντροπίας με βάση τον
πίνακα πιθανοτήτων (2 μεταβλητές)
def calculate_joint_entropy(given_matrix,rows,columns):
    calc = 0.0
    for i in range(rows):
        for j in range(columns):
```

```
            if given_matrix[i][j] == 0 :
                continue
            else:
                temp = (-given_matrix[i][j] *
np.log2(given_matrix[i][j])).sum()
                calc = calc + temp
    print(calc)
    return calc

# Συναρτηση υπολογισμου πίνακα συχνοτήτων
def
calculating_prob_matrix(divider,rows,columns,A,B,unique_A,u
nique_B):
    counter = 0
    #rowslen = len(unique_source_ips)
    #columnslen = len(unique_destination_ips)
    prob_matrix = [[0 for c in range(columns)] for r in
range(rows)]
    i = 0
    print("N is", N)
    while i < len(unique_A):
        j = 0
        while j < len(unique_B):
            k = 0
            while k < len(B):
                if (unique_B[j] == B[k] and
unique_A[i]==A[k]):
                    counter += 1
                k += 1
            prob_matrix[i][j] = counter / N
            counter = 0
            j += 1
        i += 1

    return(prob_matrix)

########Entropy calculation is made possible using pyitlib
library  #######

''' USEFUL THEORY
    H(X,Y)=H(Y|X)+H(X).
    Joint Entropy = Conditional Entropy + Shannon Entropy

'''
```

```
import pandas as pd
import numpy as np
import string
import random
import collections

#read CSV File
data = pd.read_csv('8-42-05.csv')
print('11')
#Create Lists with the columns of the CSV
time = data['Time'].tolist()
source_ips = data['Source'].tolist()
destination_ips = data['Destination'].tolist()
protocols = data['Protocol'].tolist()

print("Source Ip packet length" , len(source_ips))

#CREATE LISTS WITH THE UNIQUE VALUES
unique_source_ips = []
unique_destination_ips = []
unique_protocols = []

for x in source_ips:
    # check if exists in unique_list or not
    if x not in unique_source_ips:
        unique_source_ips.append(x)
print(len(unique_source_ips))
for x in destination_ips:
    if x not in unique_destination_ips:
        unique_destination_ips.append(x)
print(len(unique_destination_ips))
for x in protocols:
    if x not in unique_protocols:
        unique_protocols.append(x)
print(len(unique_protocols))

#initializing data

N = len(source_ips)
rowslen = len(unique_source_ips)
columnslen = len(unique_destination_ips)

## Call function to calculate probability matrix
```

```
matrix_from_def =
calculating_prob_matrix(N,rowslen,columnslen,source_ips,des
tination_ips,unique_source_ips,unique_destination_ips)
## Call function to calculate the joint entropy of sets A
and B given the probability matrix
joint_entropy_value =
calculate_joint_entropy(matrix_from_def,rowslen,columnslen)
## Call function to calculate Shannon Entropy
shannon_value = shannon_entropy_cal(source_ips)
print("The value of Shannon Entropy is : " ,shannon_value)
print("The value of Joint Entropy is : "
,joint_entropy_value)
#s_e = (joint_entropy_value)-(shannon_value)
print("The value of Conditional Entropy is : " ,
(joint_entropy_value)-(shannon_value))
```