ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ
ΤΜΗΜΑ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

ΤΟΜΕΑΣ ΕΠΙΚΟΙΝΩΝΙΩΝ,ΗΛΕΚΤΡΟΝΙΚΗΣ ΚΑΙ ΣΥΣΤΗΜΑΤΩΝ
ΠΛΗΡΟΦΟΡΙΚΗΣ

Συνδυαστικές κατανεμημένες επιθέσεις άρνησης υπηρεσιών μέσω πολλαπλών διεπαφών

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

του

ΕΥΑΓΓΕΛΟΥ Ν.
ΠΑΠΑΒΑΣΙΛΕΙΟΥ

Επιβλέπων: Συμεών Παπαβασιλείου
Καθηγητής Ε.Μ.Π.

Αθήνα, Οκτώβριος 2020

Εθνικο Μετσοβιο Πολυτεχνειο
ΤΜΗΜΑ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ
ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ
ΤΟΜΕΑΣ ΕΠΙΚΟΙΝΩΝΙΩΝ,ΗΛΕΚΤΡΟΝΙΚΗΣ ΚΑΙ
ΣΥΣΤΗΜΑΤΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ

Συνδυαστικές κατανεμημένες επιθέσεις άρνησης υπηρεσιών μέσω πολλαπλών διεπαφών

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

του

ΕΥΑΓΓΕΛΟΥ Ν.
ΠΑΠΑΒΑΣΙΛΕΙΟΥ

Επιβλέπων: Συμεών Παπαβασιλείου
Καθηγητής Ε.Μ.Π.

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή την 10η Οκτωβρίου 2020.

.....	.....	.....
Συμεών Παπαβασιλείου	Θεοδώρα Βαρβαρίγου	Ιωάννα Ρουσσάκη
Καθηγητής Ε.Μ.Π.	Καθηγήτρια Ε.Μ.Π.	Επ. Καθηγήτρια Ε.Μ.Π.

Αθήνα, Οκτώβριος 2020

.....
Ευάγγελος Ν. Παπαβασιλείου
Διπλωματούχος Ηλεκτρολόγος Μηχανικός και Μηχανικός Υπολογιστών Ε.Μ.Π.

Περίληψη

Είναι γεγονός ότι στη σύγχρονη εποχή χρησιμοποιείται το Διαδίκτυο όσο ποτέ άλλοτε αποτελώντας βασικό κομμάτι της καθημερινότητας για το μεγαλύτερο μέρος του πληθυσμού παγκοσμίως. Παράλληλα όμως, συνεχώς αυξάνονται και οι διαδικτυακές επιθέσεις και κυρίως οι κατανεμημένες επιθέσεις άρνησης υπηρεσιών (Distributed Denial of Service - DDoS) από κακόβουλους χρήστες του Διαδικτύου. Οι επιθέσεις αυτές έχουν ως στόχο εφαρμογές, ιστότοπους ή υπηρεσίες που παρέχονται στο Διαδικτύο αποσκοπώντας στην παρεμπόδιση της σωστής λειτουργίας τους και εξυπηρέτησης πιθανών πελατών και νόμιμων χρηστών. Οι επιθέσεις αυτές μάλιστα, γίνονται ολοένα και πιο αποτελεσματικές και έξυπνες. Έτσι παρόλο που έχουν προταθεί αρκετές λύσεις για την αντιμετώπιση τέτοιων επιθέσεων, οι μηχανισμοί άμυνας δεν καταφέρνουν να τις μετριάζουν σε όλες τις περιπτώσεις.

Σκοπός της παρούσας διπλωματικής αποτελεί η υλοποίηση μιας προηγμένης κατανεμημένης επίθεσης άρνησης υπηρεσιών σε συστήματα που κάνουν χρήση ασύρματων δικτύων μέσω πολλαπλών διεπαφών. Η επίθεση αυτή σχεδιάστηκε με βάση γνωστές τεχνικές όπως η Crossfire attack αλλά σε πιο εξελιγμένη μορφή, χρησιμοποιώντας συσκευές που διαθέτουν περισσότερες από μία διεπαφές σύνδεσης στο Διαδίκτυο. Με αυτόν τον τρόπο παρέχει στον επιτιθέμενο ακόμα μεγαλύτερη μυστικότητα και αποδοτικότητα. Επίσης στο πλαίσιο της εργασίας αυτής πραγματοποιήθηκαν πειράματα σε πραγματικά συστήματα ώστε να αξιολογηθεί η αποτελεσματικότητά της.

Η εργασία αυτή προτείνει ένα νέο τρόπο υλοποίησης επιθέσεων συμβάλλοντας στη βαθύτερη κατανόησή τους. Έτσι, παράλληλα, μπορέι να οδηγήσει σε σημαντικά συμπεράσματα που θα βοηθήσουν τη βελτίωση των μηχανισμών άμυνας για την αποδοτικότερη αντιμετώπιση τέτοιου είδους επιθέσεων.

Λέξεις Κλειδιά

Κατανεμημένες Επιθέσεις Άρνησης Υπηρεσιών, Bots, Χωρητικότητα, Διαθέσιμο Εύρος Ζώνης, Ασύρματα Δίκτυα, Σύνδεσμος - Στόχος, Crossfire Επίθεση

Abstract

It is a fact that in modern times the Internet is used more than ever before, being a key part of everyday life for most of the world's population. At the same time, however, cyber attacks and especially Distributed Denial of Service (DDoS) attacks by malicious Internet users are constantly increasing. These attacks target applications, websites or services provided on the Internet with the aim of preventing them from functioning properly and serving potential customers and legitimate users. In fact, these attacks are becoming more and more effective and clever. Therefore, although several solutions have been proposed to deal with such attacks, the defense mechanisms do not manage to mitigate them in all cases.

The purpose of this dissertation is to design and implement an advanced distributed denial of service attack on systems that use wireless networks through multiple interfaces. This attack is designed based on known techniques such as Crossfire attack but in a more advanced form, using devices that have more than one Internet connection interface. Thus, it provides the attacker with even greater secrecy and efficiency. Also in the context of this work, experiments were performed on real systems to evaluate its effectiveness.

This study proposes a new way of carrying out attacks whilst contributing to their deeper understanding. Therefore, it can lead to significant outcomes that will help improve the defense mechanisms to effectively deal with this type of attacks.

Key Words

Distributed Denial of Service, Bots, Capacity, Available Bandwidth, Wireless Networks, Target Link, Crossfire Attack

Ευχαριστίες

Αρχικά, θα ήθελα να ευχαριστήσω θερμά τον επιβλέποντα καθηγητή μου κ. Συμεών Παπαβασιλείου για την ανάθεση και την επίβλεψη της διπλωματικής μου εργασίας. Επιπρόσθετα, θα ήθελα να εκφράσω την ιδιαίτερη ευγνωμοσύνη μου στον καθηγητή κ. Βασίλειο Καρυώτη για τη συνεχή καθοδήγησή του κατά την εκπόνηση της διπλωματικής και την πολύτιμη του συμβολή για την επιτυχή ολοκλήρωση της εργασίας μου. Επίσης, θέλω να ευχαριστήσω θερμά την οικογένεια μου, τους γονείς μου και την αδερφή μου, για τη συνεχή υποστήριξη που μου προσέφεραν κατά τη διάρκεια των προπτυχιακών μου σπουδών. Τέλος, ευχαριστώ όλους τους φίλους μου για τις στιγμές που περάσαμε μαζί αλλά και για την στήριξη τους.

Ευάγγελος Ν. Παπαβασιλείου

Αθήνα, Οκτώβριος 2020

Περιεχόμενα

Περίληψη **5**

Abstract **7**

Ευχαριστίες **9**

Περιεχόμενα **11**

Κατάλογος Σχημάτων **13**

Κατάλογος Πινάκων **14**

1 Εισαγωγή **16**
1.1 Αντικείμενο της Διπλωματικής 16
1.2 Δομή της Εργασίας 17

2 Κατανεμημένες Επιθέσεις Άρνησης Υπηρεσιών- DDoS **18**
2.1 Κατηγορίες Επιθέσεων 18
2.2 Συνήθεις Επιθέσεις 19
2.3 Διάσημες Επιθέσεις DDoS 25

3 Τεχνολογικό Υπόβαθρο **27**
3.1 Ορισμοί 27
3.2 Εκτίμηση Bandwidth 30
3.2.1 VPS Probing 30
3.2.2 SLoPS 31
3.2.3 Packet Pair/Train Dispersion (PPTD) 31
3.2.4 Trains of Packet Pairs (TOPP) 32

4 Σχετικές Εργασίες **34**
4.1 Επίθεση Διασταυρούμενων Πυρών (Crossfire Attack) 34
4.1.1 Εισαγωγή 34
4.1.2 Στάδια Επίθεσης 36
4.2 Παλμοδικές Επιθέσεις 41
4.3 Προκαλώντας Συμφόρηση στο Διαδίκτυο μέσω Συντονισμένων και Αποκεντρωμένων Παλμοδικών Επιθέσεων 42
4.3.1 Εισαγωγή 42
4.3.2 Στάδια Επίθεσης 45

5 Υλοποίηση Επίθεσης **47**
5.1 Netmode Testbed 47
5.2 RT-WABest 48
5.2.1 Εκτίμηση της Χωρητικότητας 48
5.2.2 Εκτίμηση του Διαθέσιμου Εύρους Ζώνης 49
5.3 Περιγραφή Συστήματος 50
5.4 Στάδια της Επίθεσης 51
5.5 Αποτελέσματα 53

6 Συμπεράσματα **56**
6.1 Αξιολόγηση 56
6.2 Πιθανοί Τρόποι Αντιμετώπισης 56

Βιβλιογραφία **58**

Κατάλογος Σχημάτων

2.1 Μοντέλο OSI 18
2.2 Παράδειγμα επίθεσης UDP Flood 20
2.3 Τριμερής Χειραψία TCP 22
2.4 Παράδειγμα επίθεσης Syn Flood 23
2.5 HTTP Flood 23
2.6 NTP Amplification 24

3.1 Χωρητικότητα και Διαθέσιμο Εύρος Ζώνης 29
3.2 Διασπορά ζεύγους πακέτων 31

4.1 Τα στοιχεία της επίθεσης Crossfire 37
4.2 Σχεδίαση του Χάρτη Συνδέσμων 39
4.3 Προετοιμασία της Επίθεσης 40
4.4 Συντονισμός των Bots 41
4.5 Κατανεμημένες Παλμοδικές Επιθέσεις 43
4.6 Υλοποίηση της επίθεσης CICADAS 44
4.7 CICADAS's state machine 46

5.1 Netmode Testbed 47
5.2 Στάδια της επίθεσης 51
5.3 Τοπολογία 1ου σεναρίου 53
5.4 Διακύμανση διαθέσιμου εύρους ζώνης 1ου σεναρίου 54
5.5 Τοπολογία 2ου σεναρίου 54
5.6 Διακύμανση διαθέσιμου εύρους ζώνης 2ου σεναρίου 55

Κατάλογος Πινάκων

4.1 Crossfire and other DDoS 36

5.1 Ρόλος του κάθε κόμβου 50

Κεφάλαιο 1

Εισαγωγή

1.1 Αντικείμενο της Διπλωματικής

Οι κατανεμημένες επιθέσεις άρνησης υπηρεσιών (DDoS - Distributed Denial of Service), οι οποίες έχουν ως στόχο την παρεμπόδιση νόμιμων χρηστών από την πρόσβαση σε ιστοσελίδες ή υπηρεσίες του Διαδικτύου είναι γνωστές στην ερευνητική κοινότητα από τις αρχές της δεκαετίας του 1980. Οι επιθέσεις αυτές χρησιμοποιούν δύο βασικές μεθόδους κατά κύριο λόγο. Η πρώτη μέθοδος περιλαμβάνει την στοχευμένη αποστολή κάποιων τροποποιημένων πακέτων στο θύμα έτσι ώστε να εκμεταλλευτεί συγκεκριμένες ευπάθειες (vulnerabilities) του πρωτοκόλλου ή αδυνάμειες της εφαρμογής που τρέχει το θύμα [1]. Η δεύτερη μέθοδος που είναι και η πιο συνηθισμένη στοχεύει στη διακοπή της συνδεσιμότητας ενός νόμιμου χρήστη εξαντλώντας τους πόρους του δικτύου ή τους πόρους του διακομιστή (server) όπως για παράδειγμα τον επεξεργαστή του, τη μνήμη του και το δίσκο ή τις βάσεις δεδομένων του. Σήμερα, οι επιθέσεις αυτές πραγματοποιούνται από ένα τεράστιο αριθμό υπολογιστών, που είναι συνδεδεμένοι σε ένα δίκτυο και ελέγχονται από τον επιτιθέμενο, στέλνοντας συνεχώς τεράστιο όγκο κίνησης ή και αιτήματα υπηρεσιών στο σύστημα στόχου. Το σύστημα-στόχος είτε ανταποκρίνεται υπερβολικά αργά ώστε να μην μπορεί να ανταποκριθεί είτε καταρρέει εντελώς. Οι υπολογιστές αυτοί που αποτελούν μέρος ενός botnet είναι συνήθως μολυσμένοι από τη χρήση κακόβουλου λογισμικού [2]. Χρησιμοποιώντας τους πόρους των συσκευών αυτών είναι εφικτή η υλοποίηση καταστροφικών επιθέσεων.

Καθώς ολοένα και αυξάνεται η χρήση του Διαδικτύου σε μια ψηφιακή εποχή παράλληλα οι επιθέσεις DDoS εξελίσσονται και γίνεται συνεχώς πιο δύσκολο να αντιμετωπιστούν από τους υπάρχοντες μηχανισμούς άμυνας. Πλέον οι επιτιθέμενοι φροντίζουν να παράγουν κίνηση πολύ μικρού μεγέθους ανά συσκευή ώστε να μοιάζει με νόμιμη και να μην αναγνωρίζεται ως κακόβουλη ,όπως η επίθεση Crossfire. Έχοντας, όμως, στη διάθεση τους έναν τεράστιο αριθμό τέτοιων συσκευών μπορούν αθροιστικά να παράγουν τεράστιες ροές κίνησης με καταστροφικά αποτελέσματα. Σκοπός αυτής της διπλωματικής είναι η υλοποίηση μιας τέτοιας έξυπνης επίθεσης, όπως η Crossfire, η οποία δε γίνεται αντιληπτή καθώς η κίνηση που παράγει είναι πανομοιότυπη με αυτή νόμιμων χρηστών. Επίσης με τη χρήση ασύρματων δικτύων που έχουν πολλαπλές διεπαφές είναι εφικτό η κάθε συσκευή να διαχωρίσει την επίθεση της αυξάνοντας έτσι την μη αναγνωρισιμότητα της αλλά και την αποτελεσματικότητα της. Έτσι η υλοποιήση αυτής της επίθεσης προσφέροντας νέες ιδέες μπορεί να δημιουργήσει τη βάση μελέτης και καλύτερης αντιμετώπισης παρόμοιων κακόβουλων ενεργειών ενώ στο τέλος προτείνονται τρόποι αντιμετώπισης τέτοιου είδους επιθέσεων.

1.2 Δομή της Εργασίας

Η παρούσα διπλωματική εργασία είναι χωρισμένη σε έξι κεφάλαια. Στο Κεφάλαιο 2 παρουσιάζονται τα βασικά είδη των DDoS.

Στο Κεφάλαιο 3 παρατίθεται το επιστημονικό υπόβαθρο πάνω στο οποίο στηρίζεται η εργασία.

Το Κεφάλαιο 4 ορίζει τις εργασίες που έχουν γίνει πάνω στο αντικείμενο της διπλωματικής και στις οποίες βασίστηκε η υλοποίηση.

Στο Κεφάλαιο 5 περιγράφονται η υλοποίηση καθώς και τα αποτελέσματα της επίθεσης.

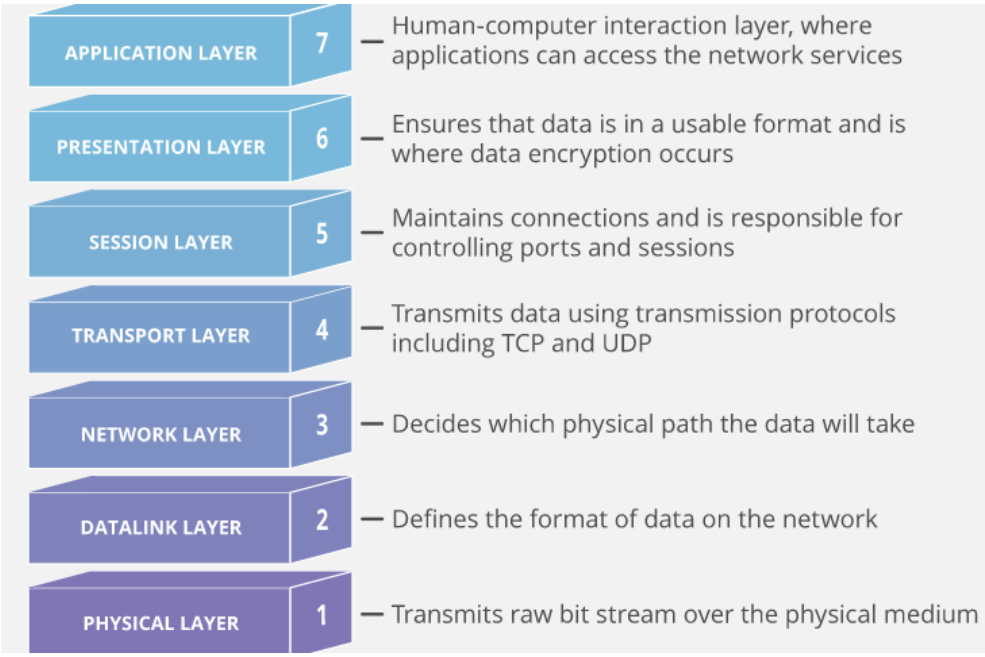
Τέλος, το Κεφάλαιο 6 περιλαμβάνει τα συμπεράσματα της εργασίας. Επίσης, συζητούνται πιθανές κατευθύνσεις επέκτασης και βελτιστοποίησης, καθώς και μελλοντικές εργασίες.

Κεφάλαιο 2

Κατανεμημένες Επιθέσεις Άρνησης Υπηρεσιών- DDoS

2.1 Κατηγορίες Επιθέσεων

Οι διάφορες επιθέσεις άρνησης υπηρεσιών [3] στοχεύουν διαφορετικά συστατικά ενός δικτύου τα οποία περιγράφονται από το μοντέλο OSI (OSI model). Το μοντέλο OSI [4] υποδιαιρεί τις λειτουργίες ενός δικτύου σε μια «κατακόρυφη» στοίβα από επίπεδα, για το καθένα από τα οποία μπορεί να οριστεί κάποιο πρωτόκολλο σε μία συγκεκριμένη υλοποίηση , στην ουσία δηλαδή περιγράφει τη συνδεσιμότητα του δικτύου χωρίζοντας το σε 7 διαφορετικά επίπεδα (βλ. Σχήμα 2.1).



Σχήμα 2.1: Μοντέλο OSI

Γενικά οι κατανεμημένες επιθέσεις άρνησης υπηρεσιών (DDoS) μπορούν να χωριστούν σε τρεις κατηγορίες [3, 5]:

- **Επιθέσεις Στρώματος Εφαρμογής (Application Layer Attacks)** :

  Επίσης αναφέρεται και ως επίθεση άρνησης υπηρεσιών του στρώματος 7 στο OSI Model (layer 7 DDoS Attack). Ο στόχος της είναι να εξαντληθούν οι πόροι του στόχου , στέλνοντας πραγματικά και φαινομενικά "άκακα" αιτήματα ώστε να "πνίξουν" κάποιο web server [5]. Χρησιμοποιούν απλά αιτήματα HTTP (HTTP requests) τα οποία στέλνονται εύκολα και γρήγορα ενώ για τον server μπορεί να είναι ιδιαίτερα χρονοβόρο να απαντήσει καθώς μπορεί να πρέπει να φορτώσει πολλαπλά αρχεία ή να διατρέξει τη βάση δεδομένων του. Αυτό το είδος των επιθέσεων είναι δύσκολο να αντιμετωπιστούν πολλές φορές καθώς η κίνηση του επιτιθέμενου δεν φαίνεται ως κακόβουλη. Σε αυτές περιλαμβάνονται GET/POST πλημμύρες (GET / POST floods) και επιθέσεις που εκμεταλλεύονται τις αδυναμίες των Windows , Apache και άλλα ενώ το μεγεθός τους προσμετράται σε αιτήματα ανά δευτερόλεπτο (requests per second).

- **Επιθέσεις Πρωτοκόλλου (Protocol Attacks)**

  Αυτό το είδος των επιθέσεων καταναλώνουν πραγματικούς πόρους των servers ή ενδιάμεσων μέσων επικοινωνίας όπως τείχων προστασίας (firewalls) και εξισορροπιστών φορτίων (load balancers) κ.τ.λ. Εκμεταλεύονται τις αδυναμίες των επιπέδων 3 και 4 στο μοντέλο OSI και καθιστούν ανέφικτο να προωθηθεί νόμιμη κίνηση προς τον server-στόχο. Το μέγεθος τους μετράται σε πακέτα ανά δευτερόλεπτο (packets per second - Pps) ενώ επιθέσεις τέτοιου είδους οι SYN floods, Ping Of Death, Smurf DDoS και άλλες.

- **Επιθέσεις Όγκου Δεδομένων (Volumetric Attacks)**

  Στόχος των επιθέσεων αυτών είναι να καταναλωθεί όλο το εύρος ζώνης (bandwidth) του site-θύματος ενώ το μέγεθος τους μετράται σε bits ανά δευτερόλεπτο (bits per second - bps). Ο επιτιθέμενος χρησιμοποιώντας συνήθως ένα botnet [6], δηλαδή ένα σύνολο συσκευών που έχουν μολυνθεί και βρίσκονται υπό την κατοχή του, δημιουργεί τεράστια κίνηση ποσότητας δεδομένων στέλνοντας τα προς το στόχο. Σε αυτή την κατηγορία ανήκουν UDP floods, ICMP floods και άλλες επιθέσεις "ψεύτικων" πακέτων (spoofed-packet floods).

2.2 Συνήθεις Επιθέσεις

Στη συνέχεια παρουσιάζονται κάποιες από τις πιο συνηθισμένες επιθέσεις.

UDP Flood

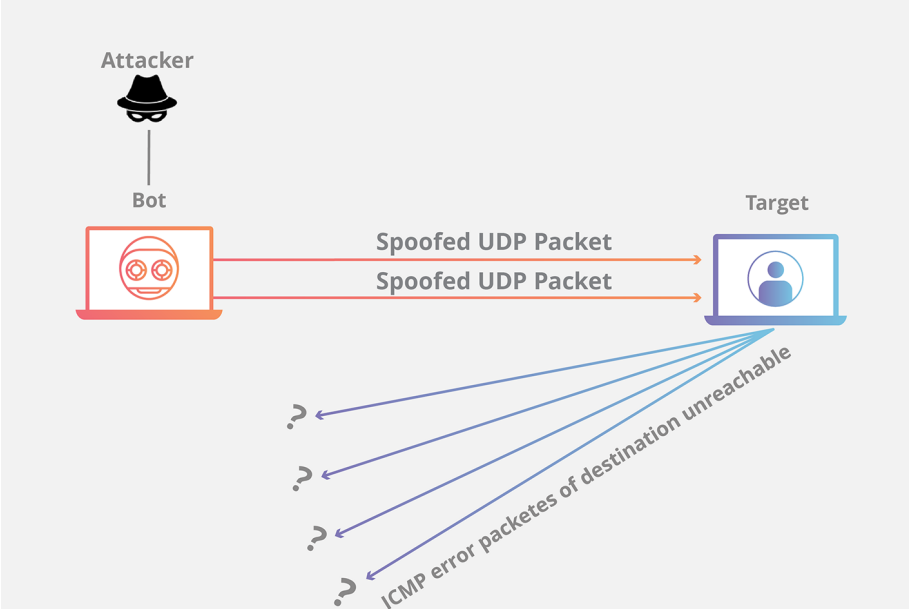
Η επίθεση πλημμύρας UDP [7] [8] είναι μια επίθεση άρνησης υπηρεσίας χρησιμοποιώντας το πρωτόκολλο User Datagram Protocol (UDP), ένα πρωτόκολλο δικτύωσης υπολογιστή χωρίς συσκέψεις (sessions). Η χρήση του UDP για επιθέσεις άρνησης υπηρεσίας δεν είναι τόσο απλή όσο με το πρωτόκολλο ελέγχου μετάδοσης (TCP). Ωστόσο, μια επίθεση πλημμύρας UDP μπορεί να ξεκινήσει στέλνοντας ένα μεγάλο αριθμό πακέτων UDP μέσω τυχαίων θυρών σε ένα απομακρυσμένο κεντρικό υπολογιστή - στόχο. Ως αποτέλεσμα, ο μακρινός κεντρικός υπολογιστής:

- Ελέγχει για την ακρόαση της εφαρμογής στη συγκεκριμένη θύρα.

- Βλέπει ότι καμία εφαρμογή δεν ακούει σε εκείνη τη θύρα.
- Απάνταει με πακέτο προορισμού ICMP Unreachable.

Έτσι, για ένα μεγάλο αριθμό πακέτων UDP, το θύμα θα αναγκαστεί να στείλει πολλά πακέτα ICMP, με αποτέλεσμα να μην μπορεί να εξυπηρετήσει άλλους πελάτες. Οι εισβολείς ενδέχεται επίσης να παραβιάζουν τη διεύθυνση IP των πακέτων UDP, εξασφαλίζοντας ότι τα πακέτα επιστροφής ICMP δεν φτάνουν τελικά ποτέ σε αυτά καθιστώντας κατ' αυτόν τον τρόπο ανώνυμη την τοποθεσία του δικτύου τους. Τα περισσότερα λειτουργικά συστήματα προσπαθούν να περιορίσουν τη ζημιά της επίθεσης μειώνοντας το ρυθμό αποστολής των απαντήσεων ICMP.

Αυτή η επίθεση μπορεί να αντιμετωπιστεί με την ανάπτυξη τείχους προστασίας (firewalls) σε βασικά σημεία ενός δικτύου για να φιλτράρει την ανεπιθύμητη κίνηση. Το πιθανό θύμα δεν λαμβάνει ποτέ τα κακόβουλα πακέτα UDP και δεν αποκρίνεται σε αυτά επειδή το τείχος προστασίας τους σταματά. Ωστόσο, καθώς τα τείχη προστασίας μπορούν να διατηρούν μόνο ένα συγκεκριμένο αριθμό "συνεδριών" (sessions) , τα τείχη προστασίας μπορούν επίσης να είναι επιρρεπή σε επιθέσεις πλημμύρας.



Σχήμα 2.2: Παράδειγμα επίθεσης UDP Flood

ICMP (Ping) Flood

Συνήθως, οι αιτήσεις ping χρησιμοποιούνται για τη δοκιμή της σύνδεσης δύο υπολογιστών, μετρώντας τον χρόνο που χρειάζεται ένα αίτημα echo ICMP ώστε να φτάσει στον αποδέκτη συν το χρόνο που χρειάζεται η echo απάντηση ICMP να γυρίσει πίσω στον αποστολέα. Κατά τη διάρκεια μιας επίθεσης, ωστόσο, χρησιμοποιούνται για την υπερφόρτωση ενός δικτύου στόχου με πακέτα δεδομένων [9].

Ο επιτιθέμενος [10] κάνει χρήση ενός botnet για να στείλει μεγάλες ποσότητες πακέτων ICMP στο διακομιστή προορισμού σε μια προσπάθεια εξάντλησης οποιασδήποτε διαθέσιμης εύρος ζώνης και να αποτρέψει την πρόσβαση στους νόμιμους χρήστες. Αυτή η επίθεση θεωρείται επιτυχής όταν τεράστιος αριθμός πηγών είναι σε θέση να στέλνουν επαρκή κυκλοφορία ICMP έτσι ώστε να καταναλώνουν και εξαντλήσει όλο το διαθέσιμο εύρος ζώνης του δικτύου θυμάτων. Παρόλο που η εντολή ping χρησιμοποιείται κυρίως για τη δοκιμή σύνδεσης μέσω δικτύου ελέγχοντας εάν η συσκευή μπορεί να στείλει και να λάβει δεδομένα από άλλη συσκευή στο δίκτυο μπορεί να δοθεί με διαφορετικές μεταβλητές κάνοντας το ping μεγαλύτερο σε μέγεθος και να στέλνεται πιο συχνά. Αποτελεσματική εφαρμογή τέτοιων παραμέτρων και με επαρκή κίνηση θα οδηγήσουν τελικά στην χρήση όλου του διαθέσιμου εύρους ζώνης του συστήματος.

Είναι εφικτός ο επαναπροσδιορισμός του περιμετρικού τείχους προστασίας (firewall) για τον αποκλεισμό pings - επιθέσεων που προέρχονται εκτός του δικτύου που θέλουμε να προστατευτεί. Παρόλα αυτά, το μπλοκάρισμα των αιτήσεων ping μπορεί να έχει απρόβλεπτες συνέπειες, συμπεριλαμβανομένης της αδυναμίας διάγνωσης προβλημάτων διακομιστή.

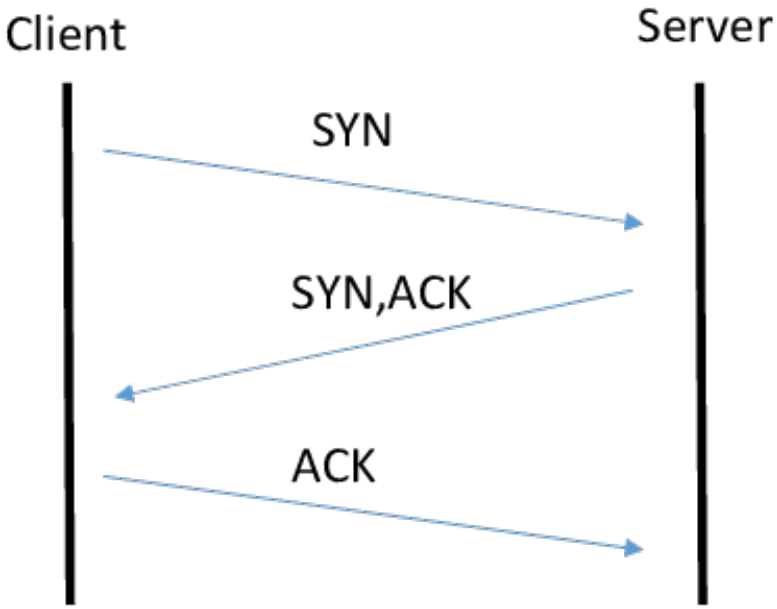
SYN Flood

Η επίθεση SYN flood αποτελεί ένα είδος επίθεσης άρνησης πρόσβασης στην οποία ο επιτιθέμενος αποστέλλει πολλαπλές αιτήσεις SYN προς το θύμα [11]. Σε αυτή την επίθεση χρησιμοποιείται η τεχνική χειραψίας TCP. Για να δημιουργηθεί μία σύνδεση TCP από έναν υπολογιστή-πελάτη σε έναν άλλο διακομιστή - server θα πρέπει να ακολουθηθούν τα βήματα του πρωτοκόλλου TCP. Συγκεκριμένα θα πρέπει οι δύο υπολογιστές να εμπλακούν σε μία διαδικασία που ονομάζεται τριμερής χειραψία (three-way handshake) (βλ. Σχήμα 2.3) , η οποία περιγράφεται ως εξής:

- Ο πελάτης στέλνει αίτημα δημιουργίας μίας σύνδεσης με ένα πακέτο TCP SYN στον server. Το όνομα του πακέτου προέρχεται από την λέξη syncronize που σημαίνει συγχρονισμός.
- Ο διακομιστής-server απαντά στην αίτηση του πελάτη στέλνοντάς του ένα πακέτο TCP SYN-ACK, από την αγγλική λέξη acknowledge που σημαίνει αναγνώριση, αποδοχή.
- Ο πελάτης απαντά με ένα πακέτο TCP ACK δηλώνοντας ότι αποδέχεται και αυτός την σύνδεση.

Μετά το πέρας αυτών των τριών βημάτων, η σύνδεση TCP έχει εγκαθιδρυθεί και μπορούν να αποσταλούν δεδομένα προς και από τους δύο υπολογιστές.

Η επίθεση SYN flood εκμεταλλεύεται μια γνωστή αδυναμία της παραπάνω χειραψίας [5]. Ο επιτιθέμενος αποστέλλει πολλαπλά αιτήματα SYN, αλλά είτε δεν ανταποκρίνεται στην απόκριση SYN-ACK του κεντρικού υπολογιστή, είτε στέλνει τα αιτήματα SYN από μια διεύθυνση IP με ψευδή στοιχεία. Ο διακομιστής - server, που αποτελεί τον στόχο της επίθεσης, συνεχίζει να περιμένει την απάντηση ACK για κάθε μία από τις

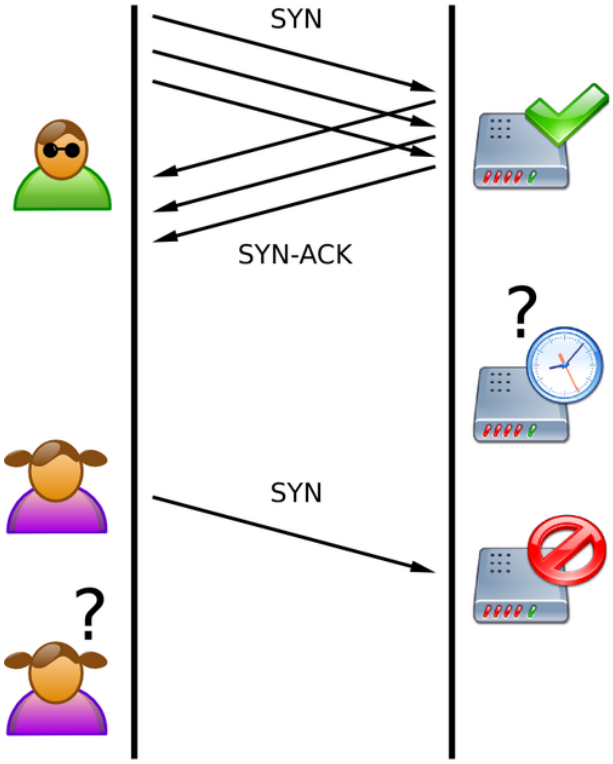


Σχήμα 2.3: Τριμερής Χειραψία TCP

αιτήσεις του πελάτη, δεσμεύοντας τους πόρους του και αφήνοντας "ανοικτές" συνδέσεις (βλ. Σχήμα 2.4). Σαν αποτέλεσμα οι νόμιμοι χρήστες που στέλνουν αιτήσεις δεν θα μπορούν να εξυπηρετηθούν καθώς ο διακομιστής κάποια στιγμή δεν θα μπορεί να ανοίξει να ανοίξει νέες συνδέσεις (Denial Of Service). Η πιο αποτελεσματική μέθοδος αντιμετώπισης αυτού του κινδύνου είναι η καταγραφή του αριθμού των συνδέσεων που έχει ξεκινήσει κάθε πελάτης και η απαγόρευση δημιουργίας νέων συνδέσεων όταν ο αριθμός αυτός ξεπεράσει κάποιο προκαθορισμένο όριο [11].

Ping Of Death

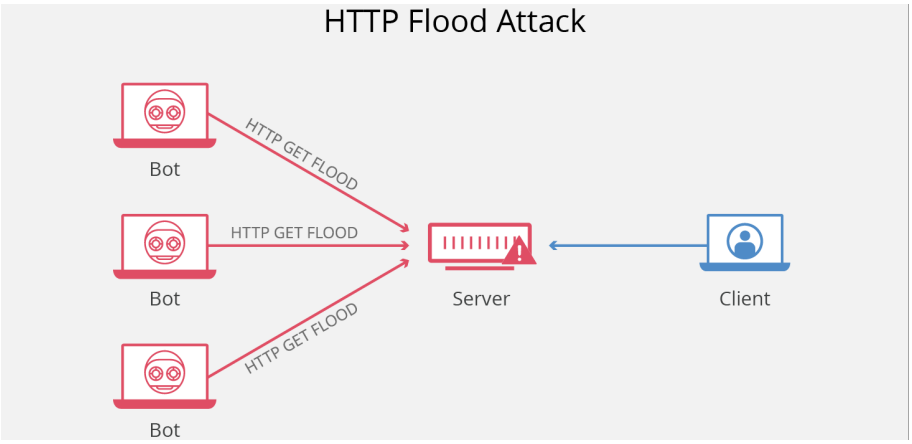
Κατά την επίθεση ping of death (POD) ο εισβολέας στέλνει πολλαπλά παραμορφωμένα ή κακόβουλα pings σε έναν υπολογιστή - στόχο [5]. Το μέγιστο μήκος πακέτου ενός πακέτου IP (συμπεριλαμβανομένης της επικεφαλίδας) είναι 65.535 byte. Ωστόσο, το επίπεδο Ζεύξης Δεδομένων (Data Link Layer) συνήθως θέτει όρια στο μέγιστο μέγεθος πλαισίου - για παράδειγμα 1500 bytes σε ένα δίκτυο Ethernet. Σε αυτήν την περίπτωση, ένα μεγάλο πακέτο IP χωρίζεται σε πολλαπλά πακέτα IP (γνωστά ως θραύσματα) και ο παραλήπτης επανασυνδέει τα θραύσματα IP στο πλήρες πακέτο. Σε ένα σενάριο Ping of Death, ακολουθώντας κακόβουλο χειρισμό του περιεχομένου των θραυσμάτων, ο παραλήπτης καταλήγει σε ένα πακέτο IP το οποίο είναι μεγαλύτερο από 65.535 byte όταν επανασυναρμολογείται. Αυτό μπορεί να υπερχειλίσει τον buffer μνήμης που έχουν διατεθεί για το πακέτο, προκαλώντας άρνηση υπηρεσίας για νόμιμα πακέτα.



Σχήμα 2.4: Παράδειγμα επίθεσης Syn Flood

HTTP Flood

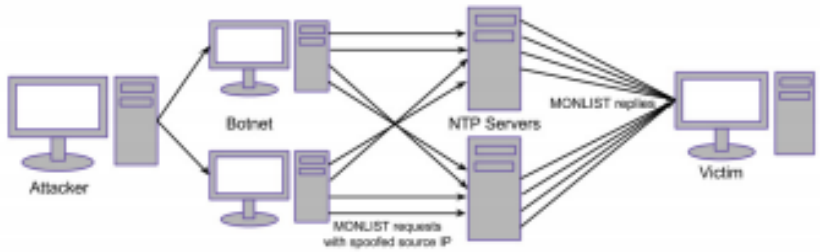
Σε αυτόν τον τύπο της επίθεσης, οι επιτιθέμενοι κάνουν κατάχρηση ενός πρωτοκόλλου αίτησης HTTP-GET και στέλνουν μεγάλο αριθμό κακόβουλων πακέτων σε ένα διακομιστή - στόχο [12]. Δεδομένου ότι αυτά τα πακέτα έχουν νόμιμο HTTP payload (ωφέλιμο φορτίο), οι διακομιστές - θύματα δεν μπορούν να διακρίνουν τα κανονικά αιτήματα HTTP-GET από τις κακόβουλες αιτήσεις. Έτσι, καθώς εξυπηρετούν όλα τα αιτήματα ως νόμιμα, εξαντλούν τελικά τους πόρους τους. Ο τρόπος επίθεσης των πλημμυρών HTTP-GET γίνεται όπως φαίνεται [13] και στο Σχήμα 2.5:



Σχήμα 2.5: HTTP Flood

NTP Amplification

Πρόκειται για κατανεμημένες επιθέσεις άρνησης εξυπηρέτησης που χρησιμοποιούν το Πρωτόκολλο Χρόνου Δικτύου (Network Time Protocol - NTP) [14]. Το Πρωτόκολλο Χρόνου Δικτύου (NTP) χρησιμοποιείται για τη διανομή πληροφοριών χρόνου σε δικτυωμένους Υπολογιστές με απόλυτη ακρίβεια. Υπάρχουν πολλοί δημόσιοι διακομιστές NTP σε ολόκληρη το Διαδίκτυο που χρησιμοποιούνται από νόμιμα συστήματα πελατών για το συγχρονισμό των ρολογιών συστήματος. Ένας διακομιστής NTP ο οποίος επιτρέπει τη χρήση της εντολής 'MONLIST' είναι ευάλωτος σε αυτό τον τύπο επίθεσης. Αυτό διότι η εντολή επιστρέφει μέχρι και τις τελευταίες 600 διευθύνσεις IP των πελατών που είναι συνδεδεμένοι σε ένα διακομιστή NTP. Το μέγεθος του πακέτου UDP του αιτήματος MONLIST είναι γύρω στα 64 bytes και μπορεί να προκαλέσει 100 απαντήσεις που φτάνουν τα 482 bytes. Είναι εμφανής δηλαδή η κλιμάκωση της επίθεσης. Επίσης η ευκολία χρήσης ψεύτικων διευθύνσεων των επιτιθέμενων κάνει τους διακομιστές NTP μια ιδανική πηγή για επιθέσεις DDoS. Όπως φαίνεται στο Σχήμα 2.6, η επίθεση πραγματοποιείται στέλνοντας αίτημα UDP σε έναν ευάλωτο διακομιστή NTP με μια ψεύτικη διεύθυνση προέλευσης που αποτελεί την πραγματική διεύθυνση του επιδιωκόμενου στόχου - θύματος. Ο διακομιστής στη συνέχεια στέλνει τις απαντήσεις στη διεύθυνση IP του θύματος με αποτέλεσμα να το πλημμυρίζει με μεγάλα πακέτα.



Σχήμα 2.6: NTP Amplification

Slowloris

Το "Slowloris" είναι το όνομα μιας επίθεσης που βασίζεται στην ευπάθεια του πρωτοκόλλου HTTP [15]. Κατά τη διάρκεια ενός φαινομενικά τυπικού αιτήματος HTTP GET, το οποίο σκόπιμα δεν ολοκληρώνεται ποτέ (με την αποστολή του χαρακτήρα νέας γραμμής), η υπηρεσία HTTP θα συνεχίσει να περιμένει τη σύνδεση μέχρι να κλείσει, με αποτέλεσμα τον κορεσμό του μέγιστου επιτρεπόμενου αριθμού συνδέσων στον εξυπηρετητή HTTP. Ως εκ τούτου, ο διακομιστής-στόχος θα παύει να ανταποκρίνεται σε νόμιμα αιτήματα, ενώ η επίθεση είναι εν ενεργεία. Ο επιτιθέμενος μπορεί να ανοίξει πολλές συνδέσεις μέχρις ότου να εκλείψει ο διαθέσιμος χώρος του διακομιστή για νέα σύνδεση. Συνεπώς, όταν ένας νόμιμος χρήστης επιχειρεί να στείλει αίτημα στον διακομιστή, δεν έχει χώρο για τη νέα σύνδεση. Καθώς η επίθεση Slowloris διατηρεί απεριόριστα τις συνδέσεις της, οι χρήστες δεν μπορούν ποτέ να συνδεθούν με το διακομιστή (άρνηση υπηρεσίας).

2.3 Διάσημες Επιθέσεις DDoS

Παρακάτω [16] παρουσιάζονται 5 από τις πιο διάσημες και μεγαλύτερες κατανεμημένες επιθέσεις άρνησης υπηρεσιών (DDoS attacks):

GitHub

Στις 28 Φεβρουαρίου του 2018, το GitHub, μια δημοφιλής πλατφόρμα προγραμματιστών, χτυπήθηκε από μια ξαφνική επίθεση με κίνηση που έφτανε στα 1,35 terabits ανά δευτερόλεπτο (terabits per second), ποσότητα κίνησης (traffic) που αποτελεί ρεκόρ. Σύμφωνα με το GitHub, η κίνηση προερχόταν από περισσότερα από χίλια διαφορετικά αυτόνομα συστήματα (ASNs) μεταξύ δεκάδων χιλιάδων τερματικών (unique endpoints). Αξιοσημείωτο αποτελεί ότι το site δεν είχε ιδέα ότι μπορούσε να συμβεί επίθεσης τόσης μεγάλης κλίμακας αν και γενικά ήταν προετοιμασμένο για επιθέσεις DDoS.

Occupy Central, Hong Kong

Η επίθεση PopVote DDoS διεξήχθη το 2014 με στόχο το κίνημα πολιτών στο Hong Kong που ήταν γνωστό ως Occupy Central. Το κίνημα προωθούσε ένα πιο δημοκρατικό σύστημα ψηφοφορίας. Οι επιτιθέμενοι έστειλαν μεγάλα ποσά κίνησης σε τρεις από τις υπηρεσίες φιλοξενίας ιστοσελίδων της Occupy Central, καθώς και σε δύο ανεξάρτητες τοποθεσίες, την PopVote, μια διαδικτυακή πλατφόρμα εκλογών και την Apple Daily. Η επίθεση πυροδότησε διακομιστές - servers με πακέτα που φαινόντουσαν ως νόμιμη κίνηση και εκτελέστηκε από πέντε botnets (!) φτάνοντας κίνηση έως και 500 gigabits ανά δευτερόλεπτο.

CloudFlare

Το 2014, ο φορέας παροχής ασφάλειας CloudFlare χτυπήθηκε από κίνηση περίπου 400 gigabit ανά δευτερόλεπτο. Η επίθεση απευθύνθηκε σε έναν μόνο πελάτη CloudFlare και στόχευσε εξυπηρετητές στην Ευρώπη εκμεταλλευόμενη ευπάθεια στο πρωτόκολλο Time Network Protocol (NTP). Παρόλο που η επίθεση απευθύνθηκε σε έναν μόνο από τους πελάτες του CloudFlare, ήταν τόσο ισχυρή που επηρέασε όλο το δίκτυο του CloudFlare. Λίγο μετά την επίθεση, η ομάδα ετοιμότητας έκτακτης ανάγκης των υπολογιστών των Ηνωμένων Πολιτειών (U.S. Computer Emergency Readiness Team) εξήγησε ότι οι επιθέσεις ενίσχυσης NTP είναι "ιδιαίτερα δύσκολο να αποκλειστούν", επειδή "οι απαντήσεις είναι νόμιμα δεδομένα που προέρχονται από έγκυρους διακομιστές".

Spamhaus

Το 2013, ξεκίνησε μια επίθεση DDoS εναντίον του Spamhaus, ενός μη κερδοσκοπικού φορέα παροχής πληροφοριών σχετικά με δίκτυα στο ίντερνετ. Παρόλο που ο Spamhaus, ως οργανισμός κατά του spam, απειλείται τακτικά, αυτή η επίθεση DDoS ήταν αρκετά μεγάλη ώστε να θέσει τον ιστότοπό τους εκτός σύνδεσης, καθώς και μέρος των υπηρεσιών ηλεκτρονικού ταχυδρομείου τους. Όπως και η επίθεση του 2014 στο CloudFlare που αναφέρθηκε παραπάνω, αυτή η επίθεση εκμεταλλεύτηκε το NTP για να υπερφορτώσει τους διακομιστές του Spamhaus με κίνηση 300 gigabit ανά

δευτερόλεπτο. Για την επίθεση υπεύθυνο ήταν ένα μέλος της ολλανδικής εταιρείας Cyberbunker, η οποία βρισκόταν στην μαύρη λίστα του Spamhaus.

Τράπεζες των Ηνωμένων Πολιτειών

Το 2012 έξι τεράστιες αμερικανικές τράπεζες, ανάμεσα στις οποίες ήταν η JP Morgan Chase και η Citigroup, έγιναν στόχοι από μια σειρά επιθέσεων DDoS. Η επίθεση διεξήχθη από εκατοντάδες μολυσμένους servers, οι οποίοι δημιούργησαν κίνηση άνω των 60 gigabit ανά δευτερόλεπτο ο καθένας. Αξίζει να τονιστεί ότι οι δράστες δεν εκτελούσαν μια απλή επίθεση DDoS αλλά χρησιμοποιούσαν πλήθος μεθόδων ώστε να βρουν μια που είχε αποτελέσμα. Έτσι, ακόμα και αν μια τράπεζα ήταν εξοπλισμένη για να αντιμετωπίσει μερικούς τύπους επιθέσεων DDoS, ήταν αδύνατο να είναι προετοιμασμένη όλες τις διαφορετικές εκδοχές επιθέσεων.

Κεφάλαιο 3

Τεχνολογικό Υπόβαθρο

Σε αυτό το κεφάλαιο παρουσιάζονται βασικές θεωρητικές έννοιες [17] σχετικά με τα δίκτυα, απαραίτητες για την κατανόηση της επίθεσης που υλοποιήθηκε στο πλαίσιο της παρούσας εργασίας. Αρχικά αναφέρονται γενικοί ορισμοί για το Bandwidth και τις μετρικές που σχετίζονται με αυτό, καθώς και πιο ειδικές τεχνικές που αφορούν άμεσα την επίθεση.

3.1 Ορισμοί

Εύρος Ζώνης (Bandwidth)

Το εύρος ζώνης ορίζεται ως ο μέγιστος ρυθμός δεδομένων με τον οποίο μπορεί να μεταφερθούν δεδομένα σε ένα σύνδεσμο δικτύου ή ένα μονοπάτι (Ορίζουμε μονοπάτι από άκρο-σε-άκρο (end-to-end path) από ένα σύστημα/πηγή σε ένα άλλο σύστημα/προορισμό ως την ακολουθία των hops που τα συνδέει μεταξύ τους). Πιο συγκεκριμένα αναφέρεται στο μέγεθος δεδομένων που μπόρει να μεταφερθεί ανά μονάδα χρόνου.

Segments

Πρόκειται για μετρική σχετιζόμενη με το Bandwidth. Το Segment συνήθως αναφέρεται σε ένα φυσικό σύνδεσμο σημείου προς σημείο (point-to-point link) , ένα εικονικό κύκλωμα (virtual circuit) ή ένα τοπικό δίκτυο κοινής πρόσβασης (shared access local area network). Τέλος πρόκειται για σύνδεσμο στο στρώμα σύνδεσης δεδομένων (data link layer - layer2).

Hops

Ένα hop αποτελείται από μια ακολουθία ενός ή περισσοτέρων segments συνδεδεμένων μέσω switches , γεφυρών (bridges) ή άλλως συσκευών. Πρόκειται για σύνδεσμο στο στρώμα IP (IP layer - layer3).

Χωρητικότητα (Capacity)

Κάθε segment ή σύνδεσμος μπορεί να μεταφέρει δεδομένα με ένα σταθερό ρυθμό, που ορίζεται ως ο ρυθμός μετάδοσης (Transmission rate). Ο ρυθμός αυτός περιορίζεται τόσο από τα φυσικό εύρος ζώνης του μέσου όσο και από το ηλεκτρονικό ή

οπτικό υλικό πομπού - δέκτη. Έτσι ορίζουμε ως Χωρητικότητα (Capacity) ενός hop ως το bit rate, που μετράται στο IP layer, με το οποίο μπορεί να μεταφέρει πακέτα IP μεγέθους MTU (MTU θεωρείται ο μέγιστος αριθμός απο bytes που μπορεί να μεταφέρει το φυσικό μέσο ανά πακέτο και συνήθως είναι 1500 bytes). Κατ' επέκταση του προηγούμενου ορισμού, χωρητικότητα C ενός μονοπατιού από άκρο σε άκρο είναι ο μέγιστος ρυθμός που μπορεί το μονοπάτι να μεταφέρει από την πηγή στον προορισμό. Με άλλα λόγια, η χωρητικότητα ενός μονοπατιού καθιερώνει ένα μέγιστο όριο ταχύτητας μεταφοράς που μπορεί να αναμένει ένας χρήστης να πάρει από αυτό. Ο σύνδεσμος με την ελάχιστη χωρητικότητα στο μονοπάτι καθορίζει και την χωρητικότητα C όλου του μονοπατιού από άκρο σε άκρο, δηλαδή:

$$C = \min_{i=1,\ldots,H} C_i \tag{3.1}$$

, όπου το C_i είναι η χωρητικότητα του i-οστού hop, ενώ το H ο αριθμός των hops στο μονοπάτι.

Πρέπει να προσέξουμε [18] ότι η χωρητικότητα είναι ανεξάρτητη της κίνησης που διατρέχει το σύνδεσμο ή το μονοπάτι.

Διαθέσιμο Εύρος Ζώνης(Available Bandwidth)

Μια ακόμα σημαντική μετρική είναι το διαθέσιμο εύρος ζώνης (Available Bandwidth) ενός συνδέσμου ή ενός μονοπατιού μια χρονική στιγμή. Ορίζεται ως την αχρησιμοποίητη ή περίσσεια χωρητικότητα του συνδέσμου τη συγκεκριμένη χρονική στιγμή. Εν αντιθέσει με την χωρητικότητα (Capacity) που εξαρτάται από την εν λόγω τεχνολογία και το φυσικό μέσο που χρησιμοποιείται, το διαθέσιμο εύρος ζώνης εξαρτάται επίσης από τον φόρτο κίνησης στο σύνδεσμο που εξετάζουμε (βλ. Σχήμα 3.1). Δηλαδή όπως γίνεται αντιληπτό η συγκεκριμένη μετρική είναι χρονικά μεταβαλλόμενη.

Για να ορίσουμε το διαθέσιμο εύρος ζώνης ενός συνδέσμου οφείλουμε να χρησιμοποιήσουμε το μέσο όρο της στιγμιαίας χρήσης του κατά το χρονικό διάστημα που εξετάζουμε. Η μέση χρησιμοποίηση $\overline{u}(t-\tau, t)$ για μια χρονική περίοδο $(t-\tau, t)$ δίνεται από τον τύπο:

$$\overline{u} = \frac{1}{\tau} \int_{t-x}^{t} u(x)dx \tag{3.2}$$

, όπου $u(x)$ είναι το στιγμιαίο διαθέσιμο εύρος ζώνης του συνδέσμου τη χρονική στιγμή x, ενώ το τ ο μέσος χρονικός ορίζοντας του διαθέσιμου εύρους ζώνης.

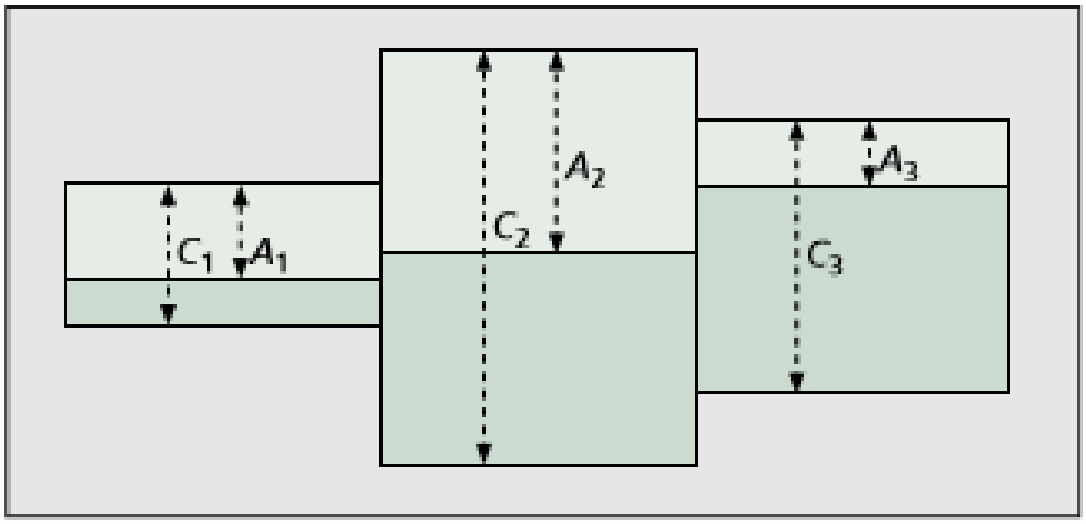
Θεωρώντας ως C_i την χωρητικότητα του i-οστού hop και u_i τη μέση χρησιμοποίηση του hop το συγκεκριμένο χρονικό διάστημα το μέσο διαθέσιμο εύρος ζώνης A_i του hop ορίζεται από τον τύπο:

$$A_i = (1 - u_i)C_i \tag{3.3}$$

Διευρύνοντας τον προήγουμενο ορισμό για ένα μονοπάτι P που αποτελείται από i hops το διαθέσιμο εύρος ζώνης του μονοπατιού H δίνεται από τον τύπο:

$$A = \min_{i=1,\ldots,P} A_i \tag{3.4}$$

Συγκεκριμένα το hop με το ελάχιστο διαθέσιμο εύρος ζώνης ορίζεται ως **σφικτός σύνδεσμος (Tight Link)** του μονοπατιού.



Σχήμα 3.1: Χωρητικότητα και Διαθέσιμο Εύρος Ζώνης

Το παραπάνω σχήμα (Σχήμα 3.1) δείχνει ένα παράδειγμα μονοπατιού όπου κάθε σύνδεσμος παρουσιάζεται ως ¨σωλήνας' (pipe) με πλάτος ίσο με τη συνολική χωρητικότητα του αντίστοιχου συνδέσμου. Η σκιαγραμμένη περιοχή κάθε συνδέσμου υποδεικνύει τη χρησιμοποιούμενη χωρητικότητα και έτσι μπορούμε να πάρουμε αντίστοιχα το διαθέσιμο εύρος ζώνης που προκύπτει από το πλάτος που μένει αχρησιμοποίητο. Ο σύνδεσμος 1 ως ο σύνδεσμος με την ελάχιστη χωρητικότητα του μονοπατιού(C_1) καθορίζει και τη συνολική χωρητικότητα ολόκληρου του μονοπατιού ενώ ο σύνδεσμος 3 καθορίζει το διαθέσιμο εύρος ζώνης του μονοπατιού (A_3) από άκρο σε άκρο τη συγκεκριμένη χρονικη στιγμή.

Γενικά επειδή το διαθέσιμο εύρος ζώνης μεταβάλλεται είναι σημαντικό να μπορούμε να το μετρήσουμε γρήγορα με τεχνικές που θα αναλύσουμε παρακάτω, ειδικά για

εφαρμογές που προσαρμόζουν το ρυθμό μετάδοσης ανάλογα με την εν λόγω μεταβολή. Αντίθετα η χωρητικότητα παραμένει σταθερή για μεγάλα χρονικά διαστήματα.

3.2 Εκτίμηση Bandwidth

Στη συνέχεια περιγράφονται βασικές τεχνικές για την εκτίμηση του Bandwidth σε ένα δίκτυο. Αυτές [17, 18] είναι η τεχνική variable packet size (VPS) probing, η τεχνική self-loading periodic streams (SLoPS), η τεχνική packet pair/train dispersion (PPTD) και η τεχνική trains of packet pairs (TOPP). Η VPS υπολογίζει την χωρητικότητα (capacity) μεμονωμένων hops, η PPTD την χωρητικότητα μονοπατιού από άκρο σε άκρο ενώ οι τεχνικές TOPP και SLoPS το διαθέσιμο εύρος ζώνης (available bandwidth) από άκρο σε άκρο.

3.2.1 VPS Probing

Αυτή η τεχνική χρησιμοποιεί το Round Trip Time-RTT ([19] ο χρόνος που απαιτείται για ένα πακέτο να σταλεί από την πηγή στον προορισμό συν την επιβεβαίωση παραλαβής που στέλνεται από τον προορισμό στην πηγή) προκειμένου να μετρήσει την χωρητικότητα του κάθε hop. Το TTL (Time-to-live) [20] πρόκειται για μια τιμή σε ένα IP πακέτο που καθορίζει εάν το πακέτο είναι μεγάλο χρονικό διάστημα στο δίκτυο και θα πρέπει να απορριφθεί. Ουσιαστικά μετράει πόσα hops έχει διατρέξει το πακέτο και χρησιμοποείται από τη VPS ώστε να αναγκάσει τα πακέτα να λήξουν σε συγκεκριμένο hop. Έτσι με τα μυνήματα ICMP που λαμβάνει η πηγή, λόγω της παραπάνω απόρριψης των πακέτων, μετράει το RRT του συγκεκριμένου hop.

Η τεχνική VPS στέλνει πολλαπλά πακέτα συγκεκριμένου μεγέθους σε κάθε hop του μονοπατιού. Το ελάχιστο RTT για πακέτο μεγέθους L για το i-οστό hop εκτιμάται:

$$T_i(L) = a + \sum_{k=1}^{i} \frac{L}{C_k} = a + \beta_i L \tag{3.5}$$

,όπου C_k είναι η χωρητικότητα του k-οστού hop, α η καθυστέρηση μέχρι το hop που είναι ανεξάρτητη του μεγέθους του πακέτου και β_i η κλίση του ελάχιστου RTT μέχρι τον i-οστό hop ανάλογο του μεγέθους L του πακέτου.

Επαναλαμβάνοντας τις μετρήσεις για τα ελάχιστα RTT όλων των hop η χωρητικότητα του i-οστού hop στο μονοπάτι εκτιμάται ως :

$$C_i = \frac{1}{\beta_i - \beta_{i-1}} \tag{3.6}$$

3.2.2 SLoPS

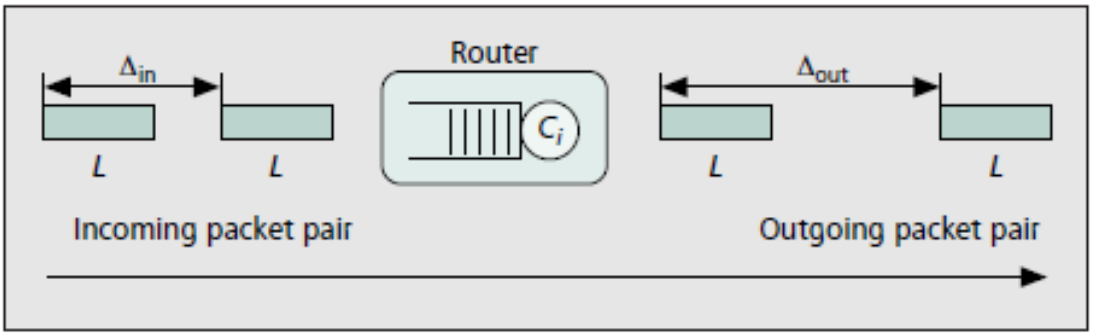
Στην τεχνική αυτή η πηγή στέλνει έναν αριθμό (περίπου 100) πακέτων ίσου μεγέθους περιοδικά με σταθερό ρυθμό R. Όταν ο ρυθμός αυτός R είναι μεγαλύτερος από το διαθέσιμο εύρος ζώνης του μονοπατιού τότε παρατηρείται καθυστέρηση και υπερφόρτωση στην ουρά (queue) του σφικτού συνδέσμου (tight link). Αντιθέτως εάν ο ρυθμός R είναι μικρότερος του διαθέσιμου εύρους ζώνης τότε δεν συμβαίνει καμία καθυστέρηση. Εφαρμόζοντας παρόμοιο αλγόριθμο με τη δυαδική αναζήτηση (binary search) η πηγή ή αλλιώς ο αποστολέας επιχειρεί να εξισώσει το ρυθμό R με το διαθέσιμο εύρος ζώνης ή να το προσεγγίσει αρκετά κοντά. Έτσι στέλνοντας η πηγή διαδοχικά "packet trains" σε διαφορετικούς ρυθμούς κάθε φορά ο αποστολέας ενημερώνει για τις καθυστερήσεις κάθε ρεύματος πακέτων. Πρέπει να τονιστεί ότι η πηγή κάθε στιγμή στέλνει μόνο ένα ρεύμα ενώ επίσης αφήνει μια περίοδο παύσης μεταξύ διαδοχικών ρευμάτων .

3.2.3 Packet Pair/Train Dispersion (PPTD)

Η τεχνική αυτή χρησιμοποιείται για την εκτίμηση της χωρητικότητας σε ένα από άκρο-σε-άκρο μονοπάτι. Η πηγή στέλνει πολλαπλά ζευγάρια πακέτων (packet pairs) προς τον παραλήπτη, όπου κάθε ζεύγος αποτελείται από 2 πακέτα ίδιου μεγέθους απεσταλμένα το ένα πίσω από το άλλο. Η διασπορά Δ_R (dispersion) ενός ζεύγους πακέτων σε έναν συγκεκριμένο σύνδεσμο είναι η χρονική διαφορά μεταξύ του πρώτου και του τελευταίου bit κάθε πακέτου (βλ. Σχήμα 3.2). Έτσι η διασπορά Δ_i για τον i-οστό σύνδεσμο με χωρητικότητα C_i δίνεται από τον παρακάτω τύπο:

$$\Delta_i = \frac{L}{C_i} \tag{3.7}$$

,όπου L το μέγεθος των πακέτων.



Σχήμα 3.2: Διασπορά ζεύγους πακέτων

Καθώς η δυάδα πακέτων περνάει από όλους τους σύνδεσμους (πλήθος H) του μονοπατιού η διασπορά Δ_R που θα μετρήσει ο παραλήπτης θα είναι:

$$\Delta_R = \max_{i=0,\ldots,H} \left(\frac{L}{C_i} \right) = \frac{L}{\min_{i=0,\ldots,H}(C_i)} = \frac{L}{C} \tag{3.8}$$

,όπου C είναι η χωρητικότητα του μονοπατιού από άκρο σε άκρο. Έτσι ο παραλήπτης υπολογίζει την χωρητικότητα του μονοπατιού από τον τύπο $C = L/\Delta_R$.

Παρομοίως η τεχνική packet train probing χρησιμοποιεί πολλαπλά ζευγάρια πακέτων το ένα πίσω από το άλλο. Η διασπορά σε αυτή την περίπτωση είναι η χρονική διαφορά μεταξύ του τελευταίου bit του πρώτου και του τελευταίου πακέτου.

3.2.4 Trains of Packet Pairs (TOPP)

Η τεχνική TOPP στέλνει πολλαπλά ζεύγη πακέτων από την πηγή στον παραλήπτη με σταδιακά αυξανόμενο ρυθμό. Αν το αρχικό ζεύγος πακέτων, με μέγεθος L bytes, έχει αρχική διασπορά (dispersion) Δ_S τότε ο ρυθμός αποστολής τους είναι $R_0 = L/\Delta_S$. Εφόσον ο ρυθμός R_0 είναι μεγαλύτερος από το διαθέσιμο εύρος ζώνης τότε το δεύτερο πακέτο θα καθυστερήσει και ο παραλήπτης θα μετρήσει ρυθμό $R_m < R_0$. Αντιθέτως εάν ο ρυθμός αποστολής R_0 είναι μικρότερος από το διαθέσιμο εύρος ζώνης τότε το ζεύγος πακέτων θα φτάσει στον αποδέκτη με τον ίδιο ρυθμό που στάλθηκε (δηλαδή $R_m = R_0$). Η βασική ιδέα μοιάζει αρκετά με την τεχνική SLoPS, ωστόσο η τεχνική TOPP δε χρησιμοποιεί δυαδική αναζήτηση αλλά αυξάνει γραμμικά το ρυθμό αποστολής. Επιπρόσθετα η τεχνική TOPP μπορεί να εκτιμήσει και την χωρητικότητα του σφικτού συνδέσμου.

Έστω ένα μονοπάτι με έναν σύνδεσμο χωρητικότητας C, διαθέσιμο εύρος ζώνης A και μέσο ρυθμό κίνησης (cross traffic) $R_c = C - A$. Τα ζεύγη πακέτων στέλνονται με σταθερά αυξανόμενο ρυθμό R_0 το οποίο όταν ξεπεράσει το A θα ισχύει για τον ρυθμό R_m που μετράει ο αποδέκτης:

$$R_m = \frac{R_0}{R_0 + R_C} C \tag{3.9}$$

ή

$$\frac{R_0}{R_m} = \frac{R_0 + R_C}{C} \tag{3.10}$$

Το διαθέσιμο εύρος ζώνης A υπολογίζεται ως ο μέγιστος δυνατός ρυθμός αποστολής ώστε να ισχύει $R_0 \approx R_m$. Η παραπάνω εξίσωση χρησιμοποιείται και για την εκτίμηση της χωρητικότητας C.

Σύμφωνα με τη τεχνική TOPP υπολογίζεται και στο πλαίσιο αυτής της διπλωματικής το διαθέσιμο εύρος ζώνης με το εργαλείο RT-WABest [21] που αναλύεται παρακάτω.

Κεφάλαιο 4

Σχετικές Εργασίες

Στο παρόν κεφάλαιο παρουσιάζονται επιθέσεις που είναι σχετικές με αυτή που υλοποιήθηκε στο πλαίσιο της παρούσας διπλωματικής.

4.1 Επίθεση Διασταυρούμενων Πυρών (Crossfire Attack)

4.1.1 Εισαγωγή

Πρόκειται για επίθεση DDoS που ανήκει στην κατηγορία των link flooding attacks. Οι επιθέσεις αυτές δεν έχουν ως στόχο συγκεκριμένους διακομιστές - servers [22] αλλά στοχεύουν στη διακοπή συνδεσιμότητας των συστημάτων στο Διαδίκτυο και την παρεμπόδιση της δρομολόγησης πακέτων. Οι συγκεκριμένες επιθέσεις παρ' όλα αυτά είναι δύσκολο να υλοποιηθούν σε πραγματικά σενάρια, κυρίως εξαιτίας της δυσκολίας επιλογής των συνδέσμων-στόχων. Απεναντίας, οι περισσότερες από αυτές τις επιθέσεις προκαλούν αστάθειες στη διαδρομή (route instabilities) [23] και διακοπή σύνδεσης στο Διαδίκτυο [24]. Ωστόσο, όταν ο στόχος μιας επίθεσης είναι να διακόψει κάποια κρίσιμη υποδομή (π.χ. διανομή ενέργειας, υπηρεσίες χρηματοδότησης, υπηρεσίες διοίκησης και ελέγχου) από το Διαδίκτυο, οι πλημμύρες συνδέσεων μπορεί να είναι εξαιρετικά αποτελεσματικές. Για παράδειγμα, ο μέγιστος ρυθμός μιας επίθεσης με ένα μόνο botnet μπορεί εύκολα να υπερβαίνει τα 100 Gbps [25], καθιστώντας δυνατόν να πλημμυρήσει την τεράστια πλειοψηφία των συνδέσμων που βρίσκονται στο Διαδίκτυο.

Παρομοίως με τις περισσότερες επιθέσεις τύπου DDoS, έτσι και η Crossfire attack υλοποιείται με την χρήση ενός ή περισσότερων botnets. Με τον όρο botnet εννοούμε ένα πλήθος από συσκευές συνδεδεμένες στο Διαδίκτυο (συνήθως υπό την ιδιοκτησία απλών χρηστών) οι οποίες έχουν μολυνθεί και τις έχει καταλάβει ο επιτιθέμενος αθέμιτα με σκοπό να τις χρησιμοποιήσει για την διεξαγωγή της επίθεσης. Οι συσκευές αυτές, επονομαζόμενες και bots, τρέχουν κάποιου είδους κακόβουλο λογισμικό (malicious software - malware), υπεύθυνο για την διεξαγωγή της επίθεσης, και την πιθανή επικοινωνία κάθε bot με έναν διαχειριστή (coordinator), ο οποίος ελέγχει τις δραστηριότητες του κάθε bot.

Η συγκεκριμένη επίθεση με τη χρήση botnets δεν μπορεί να αντιμετωπιστεί εύκολα από τους τρέχοντες μηχανισμούς άμυνας του Διαδικτύου για τρεις λόγους. Πρώτον, τα bots μπορούν να χρησιμοποιούν πραγματικές διευθύνσεις IP, και επομένως οποιαδήποτε μέθοδος άμυνας που βασίζεται στην ανίχνευση ή την αποτροπή της χρήσης

πλαστών διευθύνσεων IP (spoofed IP addresses) δε μπορεί να ανιχνεύσει την επίθεση. Δεύτερον τα bots μπορούν να "πλημμυρίσουν" τις συνδέσεις (links) χωρίς τη χρήση ανεπιθύμητης κίνησης, όπως για παραδείγμα στέλνοντας πακέτα μεταξύ τους με τρόπο που να στοχεύει συγκεκριμένες ομάδες δρομολογητές [26]. Τρίτον, ένα botnet μπορεί να ξεκινήσει μια επίθεση με κίνηση χαμηλής έντασης. Έτσι, παρ' όλο που το κάθε bot δεν παράγει μεγάλη κίνηση πακέτων αλλά φαινομενικά μικρή και νόμιμη, οι ροές όλων των bots διασχίζουν συγκεντρωτικά έναν στοχευμένο σύνδεσμο (link) σχεδόν την ίδια χρονική στιγμή και προκαλείται η πλημμύρα (flood) του συνδέσμου αυτού. Ο διαχειριστής του botnet μπορεί να βρει ένα σύνολο από servers με διευθύνσεις IP εμφανείς στο Διαδίκτυο και με όλη την κίνηση που προορίζεται προς εκείνους να διέρχεται από κοινούς συνδέσμους. Ύστερα μπορεί να προγραμματίσει τα bot να στείλουν μηδαμινή κίνηση προς αυτές τις διευθύνσεις IP. Αυτός ο τύπος της επίθεσης, η οποία ονομάζεται Crossfire attack δεν ανιχνεύεται από οποιονδήποτε διακομιστή βρίσκεται σε μια διεύθυνση IP - δόλωμα (decoy IP address). Επιπλέον, οι τρέχουσες τεχνικές διαχείρισης της κυκλοφορίας (traffic engineering) δεν μπορούν να αντιμετωπίσουν αυτές τις επιθέσεις. Ακόμη και αν τέτοιου είδους διαδικτυακές τεχνικές θα μπορούσαν να αναπτυχθούν για την αντιμετώπιση της επίθεσης , μια επιπρόσθετη επίθεση μπορεί να αλλάξει το σύνολο συνδέσμων στόχων σε πραγματικό χρόνο, παρακάμπτοντας έτσι τους μηχανισμούς άμυνας (traffic engineering defenses).

Συγκεκριμένα, η Crossfire Attack [27], [28] επιδιώκει να αποκόψει μια συγκεκριμένη ομάδα συστημάτων (στόχος) από το Διαδίκτυο, ενώ αποφεύγει να στείλει κακόβουλη κίνηση κατευθείαν στον στόχο ως εξής:

1. ο εισβολέας κατασκευάζει ένα χάρτη από συνδέσμους γύρω από το στόχο εκτελώντας traceroutes προς πολλά σημεία (κόμβους) στο δίκτυο.

2. εντοπίζει κρίσιμους συνδέσμους που συνδέουν τον επιδιωκόμενο στόχο με το Διαδίκτυο.

3. εντοπίζει ομάδες από servers (servers δολώματα) που δεν ανήκουν στην περιοχή του στόχου αλλά η κίνηση σε αυτά δρομολογείται μέσω των κρίσιμων συνδέσμων του προηγούμενου βήματος.

4. καταναλώνει το εύρος ζώνης (bandwidth) των κρίσιμων συνδέσμων στέλνοντας πολλαπλές ροές, με πολύ χαμηλό bandwidth η καθεμία (για παράδειγμα Μηνύματα HTTP), που προέρχονται από bots που ελέγχονται από τον επιτιθέμενο και προορίζονται για τους servers δολώματα (decoys) του προηγούμενου βήματος.

Έτσι, η περιοχή-στόχος χάνει τη συνδεσιμότητα της στο Διαδίκτυο, χωρίς ωστόσο να παρατηρηθεί η κίνηση του επιτιθέμενου. Αυτή η επίθεση μπορεί να διακόψει αποτελεσματικά τις συνδέσεις Διαδικτύου μιας στοχευμένης επιχείρησης (π.χ. μια πανεπιστημιούπολη, μια στρατιωτική βάση). Μπορεί επίσης να απενεργοποιήσει έως 53% του συνολικού αριθμού συνδέσεων Διαδικτύου ορισμένων πολιτειών των ΗΠΑ και έως και περίπου το 33% όλων των συνδέσεων της της Δυτική Ακτής των ΗΠΑ. Η επίθεση έχει την ταυτότητα της διαδικτυακής "τρομοκρατίας" καθώς είναι χαμηλού κόστους χρησιμοποιώντας μέσα που φαίνονται ως νόμιμα (π.χ. χαμηλής έντασης, πρωτόκολλο συμμόρφωσης κυκλοφορίας). Επίσης δεν μπορεί να προβλεφθεί το επίκεντρο της επίθεσης και δεν μπορεί να ανιχνευθεί μέχρι να έχει ήδη γίνει ουσιαστική,

επίμονη ζημιά. Τέλος το πιο σημαντικό, η επίθεση είναι έμμεση: ο άμεσος στόχος της επίθεσης (συγκεκριμένοι σύνδεσμοι στο Διαδίκτυο) δεν αποτελεί απαραίτητα και το τελικό θύμα (δηλαδή μια πολιτεία, περιοχή ή μικρή χώρα).

Στον πίνακα 4.1 βλέπουμε κάποια χαρακτηριστικά της επίθεσης σε σχέση με άλλες γνωστές επιθέσεις.

Στόχος	Παλιές DDoS	Coremelt(2009)	"Spamhaus" (2013)	Crossfire(2013)
Επεκτάσιμη επιλογή **Ν εξυπηρετητών - στόχων**	X	-	X	✓
Ανεξαρτησία στην κατανομή των **bots**	✓	X	-	✓
Μη διακρισιμότητα από **νόμιμες** ροές	X	✓	X	✓
Εξάρτηση μόνο στις **επιθυμητές ροές**	X	✓	X	X
Σταθερότητα	ΥΨΗΛΗ	ΧΑΜΗΛΗ	ΧΑΜΗΛΗ	ΥΨΗΛΗ

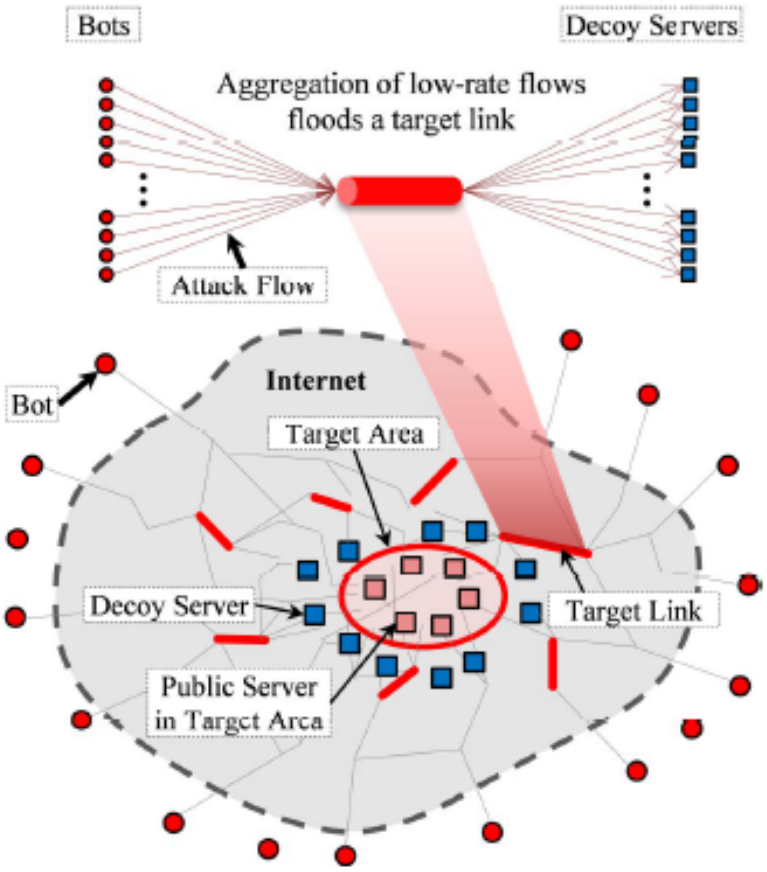
Table 4.1: Crossfire and other DDoS

4.1.2 Στάδια Επίθεσης

Σε αυτήν την ενότητα, παρουσιάζουμε τα βήματα της επίθεσης Crossfire [22]. Ο στόχος του επιτιθέμενου είναι να αποτρέψει τη νόμιμη κίνηση που ρέει σε μια συγκεκριμένη γεωγραφική περιοχή του Διαδικτύου, και για να επιτύχει αυτόν τον στόχο χρειάζεται να "πλημμυρίσει" μερικές συνδέσεις δικτύου μέσα και γύρω από αυτήν την περιοχή. Αρχικά, καθορίζονται οι δύο πιο κοινοί όροι που χρησιμοποιούνται σε αυτή την επίθεση: η περιοχή-στόχος (Target Area) και ο σύνδεσμος-στόχος (Target Link). Στη συνέχεια, περιγράφεται πώς ο επιτιθέμενος σχεδιάζει μια επίθεση χρησιμοποιώντας τα bots που ελέγχει. Το Σχήμα 4.1 απεικονίζει την έννοια της επίθεσης Crossfire.

Target Area

Αποτελεί μια γεωγραφική περιοχή του Διαδικτύου κατά της οποίας ξεκινά η επίθεση, η περιοχή δηλαδή που περικλείεται από τον κύκλο στο Σχήμα 4.1. Ένας τυπικός στόχος περιλαμβάνει τους διακομιστές (servers) ενός οργανισμού, μιας πόλης, μιας πολιτείας, ακόμη και μια χώρας .



Σχήμα 4.1: Τα στοιχεία της επίθεσης Crossfire

Target Link

Αποτελεί ένα στοιχείο ενός συνόλου συνδέσμων του δικτύου το οποίο πρέπει να "πλημμυρίσει" ο επιτιθέμενος έτσι ώστε η περιοχή στόχος να αποκοπεί από το υπόλοιπο Διαδίκτυο. Αυτοί οι σύνδεσμοι επιλέγονται προσεκτικά και δέχονται την επίθεση των ροών κίνησης ώστε να πληγεί ο πραγματικός στόχος.

Για να ξεκινήσει μια επίθεση Crossfire εναντίον μιας περιοχής στόχου, επιλέγεται ένα σύνολο δημόσιων διακομιστών εντός του στόχου - περιοχής και ένα σύνολο διακομιστών- δολωμάτων (decoy servers) που περιβάλλουν την περιοχή στόχου. Αυτοί οι διακομιστές μπορούν εύκολα να βρεθούν αφού έχουν επιλεγεί από διακομιστές που είναι δημοσίως προσβάσιμοι. Το σύνολο των δημόσιων διακομιστών χρησιμοποιείται για την κατασκευή μιας τοπολογίας επίθεσης με επίκεντρο την περιοχή - στόχο και το σύνολο των διακομιστών δολωμάτων χρησιμοποιείται για τη δημιουργία ροών επίθεσης. Τότε, ο επιτιθέμενος κατασκευάζει έναν «χάρτη συνδέσμων» (link map) , δηλαδή τον χάρτη των συνδέσμων 3ου επιπέδου (layer 3) από τις διευθύνσεις των bots προς εκείνες των δημόσιων διακομιστών. (Οι διαφορές μεταξύ ενός χάρτη συνδέσμου και ενός τυπικού χάρτη τοπολογίας δρομολογητή συζητείται παρακάτω.) Μόλις δημιουργηθεί ο χάρτης συνδέσμων, ο επιτιθέμενος το χρησιμοποιεί για να επιλέξει τους καλύτερους συνδέσμους-στόχους τους οποίους θα πλημμυρίσει έτσι ώστε να αποκόψει αποτελεσματικά την περιοχή-στόχο από το Διαδίκτυο. Στη συνέχεια , ο επιτιθέμενος συν-

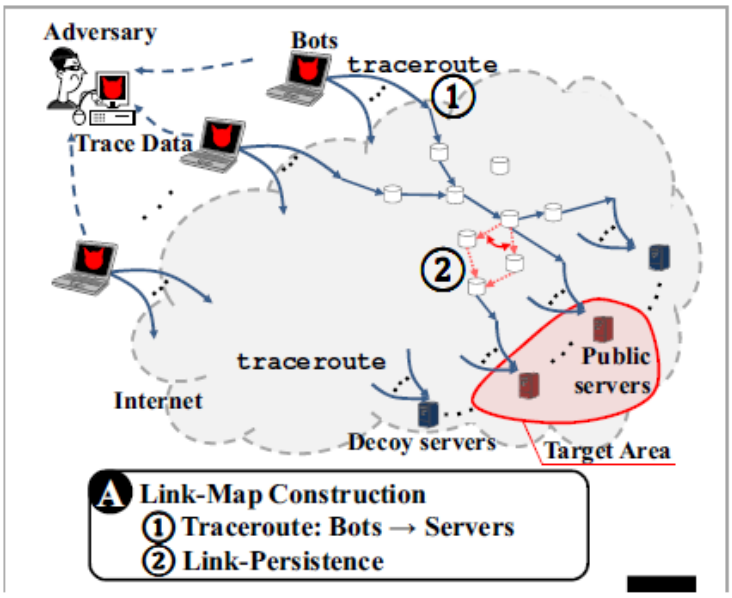
τονίζει τις ροές bot-decoy (διακομιστής) πλημμυρίζοντας τους συνδέσμους στόχους, οι οποίες τελικά θα μπλοκάρουν το μεγαλυτέρο ποσοστό των ροών που προορίζονται για την περιοχή στόχου. Τέλος, ο επιτιθέμενος επιλέγει πολλαπλά ανεξάρτητα σύνολα συνδέσμων στόχων για την ίδια περιοχή στόχου και διαλέγει να πλημμυρίζει με ροές κίνησης ένα σύνολο κάθε φορά, διαδοχικά. Με αυτό τον τρόπο θέλει να αποφευχθεί η ενεργοποίηση της αλλαγής δρομολόγησης των servers (route changes). Τα τρία βασικά βήματα που απαιτούνται για την εκκίνηση της επίθεσης Crossfire αποτελείται από τη σχεδίαση χάρτη συνδέσμων, την προετοιμασία της επίθεσης και το συντονισμό των bots, όπως φαίνεται στα Σχήματα 4.2, 4.3 και 4.4 παρακάτω. Πρέπει να τονιστεί ότι για να παραταθεί η διάρκεια της επίθεσης, το τελευταίο βήμα, δηλαδή το βήμα συντονισμού bot, εκτελείται συνεχώς από αλλάζοντας δυναμικά τα σύνολα συνδέσμων - στόχων. Παρακάτω ακολουθούν κάθε ένα από τα τα βήματα της επίθεσης.

(A) Σχεδίαση του χάρτη συνδέσμων

Ο επιτιθέμενος για να "πλυμμηρίσει" τον στόχο πρέπει πρωτίστως να κατασκευάσει έναν χάρτη με συνδέσμους του Διαδικτύου που περικλύει την περιοχή στόχο. Για να κατασκευάσει τον χάρτη συνδέσμων ο επιτιθέμενος, αρχικά ορίζει στα bots να τρέξουν traceroutes προς τους δημόσιους servers στην περιοχή - στόχο και στους servers - δολώματα. Το αποτέλεσμα του traceroute είναι η επιστροφή μίας λίστας από διευθύνσεις IP διαφόρων routers (με συνδέσμους/links να θε- ωρούμε τις διευθύνσεις IP των γειτόνων ενός router). Η λίστα αυτή δηλαδή δηλώνει το μονοπάτι από IPs που θα ακολουθήσει η κίνηση της επίθεσης. Ο χάρτης αυτός που κατασκευάζει ο επιτιθέμενος είναι διαφορετικός από μια τυπική τοπολογία δρομολόγησης [29] καθώς χρειάζεται μόνο τη λίστα συνδέσμων του layer-3. Επίσης αξίζει να σημειωθεί ότι συνήθως πραγματοποιούνται πολλάπλά traceroutes προς τους servers, έτσι ώστε να διαπιστωθεί η μονιμότητα και η πολυπλοκότητα της διαδρομής, χαρακτηριστικά απαραίτητα για την κατασκευή του χάρτη συνδέσμων. Συνήθως όμως ο επιτιθέμενος δεν είναι δυνατό να επιλέξει απευθείας τους συνδέσμους στόχους από τον χάρτη συνδέσμων καθώς πολλές από τις διαδρομές αυτές μεταβάλλονται με το χρόνο. Αυτό συμβαίνει λόγω των λειτουργιών διαχείρισης της κίνησης (traffic engineering) που χρησιμοποιούν οι ISP's (π.χ., εξισσορόπιση φορτίου - load balancing). Το αποτέλεσμα είναι τα διάφορα traceroutes προς τον ίδιο server να περιλαμβάνουν αρκετούς διαφορετικούς συνδέσμους κάθε φορά. Συνεπώς η επιλογή ενός τέτοιου συνδέσμου θα οδηγούσε τον επιτιθέμενο να προσπαθεί να "πνίξει" έναν ασταθή στόχο, γεγονός που θα καθιστούσε την επίθεση ανεπιτυχή. Τους συνδέσμους αυτούς τους ονομάζουμε μεταβλητούς (transient) σε αντίθεση με τους συνδέσμους, οι οποίοι εμφανίζονται πάντοτε σε μία διαδρομή τους οποίους ονομάζουμε μόνιμους (persistent). Ο επιτιθέμενος ενδιαφέρεται μόνο για τους μόνιμους συνδέσμους, οπότε τους διαχωρίζει από τους μεταβλητούς.

(B) Προετοιμασία της επίθεσης

Σε αυτό το στάδιο ο επιτιθέμενος εξακριβώνει τους κρίσιμους συνδέσμους (critical links), από το χάρτη συνδέσμων. Με τον όρο κρίσιμοι σύνδεσμοι εννοούμε τους μόνιμους συνδέσμους, οι οποίοι αν αποκοπούν αποκλείουν ταυτόχρονα το

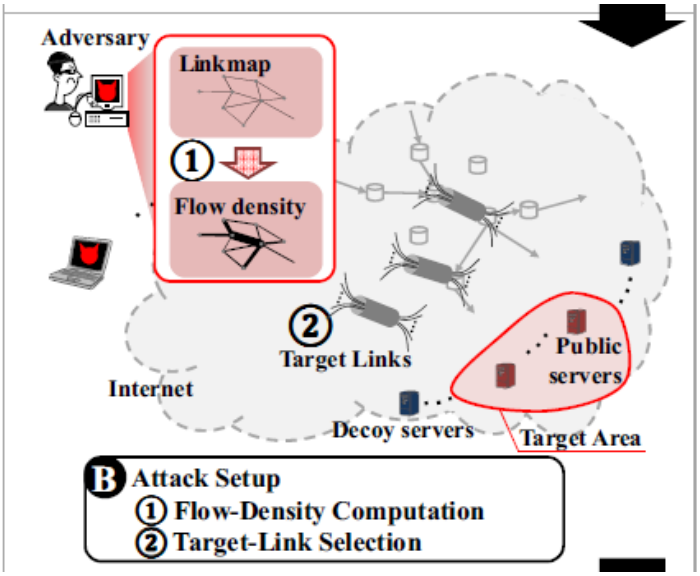


Σχήμα 4.2: Σχεδίαση του Χάρτη Συνδέσμων

μεγαλύτερο όγκο της κίνησης προς την περιοχή-στόχο. Συγκεκριμένα, ο επιτιθέμενος χρησιμοποιεί το χάρτη συνδέσμων και υπολογίζει την πυκνότητα ροής για κάθε σύνδεσμο του δικτύου στον χάρτη. Ως πυκνότητα ροής ενός μόνιμου συνδέσμου ορίζουμε τον αριθμό των ροών μεταξύ των bots και των servers της περιοχής- στόχου που μπορούν να δημιουργηθούν, εν μέσω του συνδέσμου αυτού. Μία μεγάλη πυκνότητα ροής σε έναν σύνδεσμο συνεπάγεται ότι ο σύνδεσμος μπορεί να μεταφέρει ένα υψηλό ποσό κίνησης προς μία περιοχή-στόχο (κακόβουλη και νόμιμη). Οπότε είναι προς το συμφέρον του επιτιθέμενου να επιλέξει αυτό το σύνδεσμο ως πιθανό στόχο. Έχει αποδειχθεί ότι η πυκνότητα ροής ακολουθεί μία κατανομή power-law σε ένα χάρτη συνδέσμων, καθιστώντας εύκολη την εύρεση των ροών με τη μεγαλύτερη πυκνότητα ροής προς την περιοχή στόχο από τον επιτιθέμενο. Έχοντας όλα τα παραπάνω δεδομένα, ο επιτιθέμενος επιλέγει στη συνέχεια διάφορα μη επικαλυπτόμενα σύνολα από συνδέσμους στόχους για να αποκόψει. Στόχος του επιτιθέμενου είναι να επιλέξει βέλτιστα δύο ή περισσότερα τέτοια σύνολα έτσι ώστε να καταφέρει να εμποδίσει την εισροή όσο περισσότερης κίνησης είναι εφικτό προς την περιοχή-στόχο. Για την επιλογή των συνόλων αυτών γίνεται χρήση του χαρτη συνδέσμων και της πυκνότητας ροής.

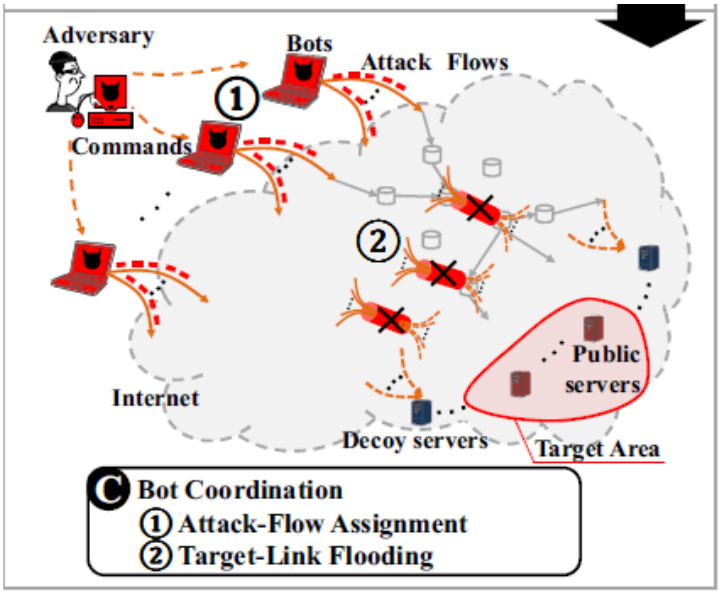
(Γ) Συντονισμός των bots

Με το πέρας των παραπάνω βημάτων ο επιτιθέμενος συντονίζει τα bots, ώστε να ξεκινήσουν την επίθεση. Για κάθε σύνολο συνδέσμων που θα βρίσκεται υπό επίθεση, ανατίθενται σε κάθε bot μία λίστα από servers δολώματα (decoy servers), αλλά και ο ρυθμός αποστολής της κίνησης προς καθέναν από αυτούς, αντίστοιχα. Ο ρυθμός αποστολής επιλέγεται προσεκτικά έτσι ώστε και η κίνηση που δημιουργεί το κάθε bot να μην ενεργοποιεί "συναγερμούς" των ISPs (είναι δηλαδή μηδαμινή) και



Σχήμα 4.3: Προετοιμασία της Επίθεσης

η συσσωρευμένη κίνηση από όλα τα bots, ταυτόχρονα, να επαρκεί, ώστε να "πνίξει" όλους τους συνδέσμους-στόχους (target links). Όπως αναφέρθηκε προηγουμένως η συσσωρευμένη κακόβουλη κίνηση προς κάθε σύνδεσμο-στόχο πρέπει να είναι αρκετά μεγάλη, έτσι ώστε να ξεπερνά την υπολοιπόμενη χωρητικότητα (capacity) ή bandwidth του εν λόγω συνδέσμου και άρα οι νόμιμες ροές που περνούν από τους συνδέσμους αυτούς να περιοριστούν σε σημαντικό βαθμό. Ο επιτιθέμενος πρέπει όμως να ικανοποιήσει δύο περιορισμούς. Ο πρώτος είναι η κάθε μεμονωμένη κίνηση από κάθε bot να είναι αρκετά μικρή έτσι ώστε να μην ενεργοποιηθούν οι μηχανισμοί ασφάλειας δικτύου. Συνήθως, τέτοιοι μηχανισμοί αφορούν τα Δίκτυα Καθοριζόμενα από το Λογισμικό (Software DefinedNetworks - SDN), όπου ο "χειριστής" (SDN Controller) παρακολουθώντας το δίκτυο μπορεί να καταλάβει αν η κίνηση είναι κακόβουλη. Επίσης την ίδια λειτουργία επιτελούν πιο στοχευμένα τα Συστήματα Εύρεσης Διεισδύσεων (Intrusion Detection Systems - IDS). Ο δεύτερος περιορισμός είναι η συσσωρευμένη κακόβουλη κίνηση που επαρκεί για να "πνίξει" τους συνδέσμους-στόχους να ανατίθεται ομοιόμορφα στα διάφορα bots και στους servers δολώματα. Το αποτέλεσμα είναι να επιτυγχάνεται πανομοιοτυπία των κακόβουλων ροών με τις νόμιμες καθώς και την μη αναγνωρισιμότητα από τους servers στην περιοχή στόχο και τους servers δολώματα. Ο επιτιθέμενος αναθέτει στα bots να ξεκινήσουν να στέλνουν τις κακόβουλες ροές. Σε κάθε bot έχουν ανατεθεί πολλές διαφορετικές ροές, κάθε μία από τις οποίες έχει ως στόχο και έναν διαφορετικό server δόλωμα ή bot. Τα bots έχουν επίσης την δυνατότητα να ρυθμίζουν δυναμικά κι τον ρυθμό με τον οποίο στέλνουν πακέτα στους στόχους τους. Συγκεκριμένα, ξεκινούν με χαμηλούς ρυθμούς και τους αυξάνουν σταδιακά μέχρι ο αντίστοιχος στόχος σύνδεσμος να "πνιγεί".



Σχήμα 4.4: Συντονισμός των Bots

(Δ) Κινούμενες Επιθέσεις

Ο επιτιθέμενος είναι δυνατό να αλλάξει το σύνολο των συνδέσμων στόχων κατά τη διάρκεια της επίθεσης, μέσα από τα διαφορετικά τέτοια σύνολα που έχουν αναφερθεί σε προηγούμενο βήμα. Η δυνατότητα αυτή συμβάλλει στην επέκταση του χρόνου εκτέλεσης της Crossfire επίθεσης, αφού όπως είναι λογικό αν το σύνολο ήταν πάντοτε σταθερό, τότε σε κάποια χρονική στιγμή θα ενεργοποιούνταν οι μηχανισμοί προστασίας του Διαδικτύου.

4.2 Παλμοδικές Επιθέσεις

Χρησιμοποιούμε τον όρο παλμοδική επίθεση για να περιγράψουμε μια κατηγορία Επιθέσεων (D)DoS που στέλνουν μόνο περιοδικές εκρήξεις παλμών αντί για πλημμύρες ροών. Εκμεταλλεύονται συνήθως τις προδιαγραφές πρωτοκόλλου δικτύου και έτσι καταφέρνουν να μειώσουν αποτελεσματικά τη διαθεσιμότητα της υπηρεσίας του θύματος. Σε αντίθεση με τις κλασικές link flooding επιθέσεις, η παλμοδική επίθεση μπορεί να προκαλέσει πολύ σημαντικότερη ζημιά στους νόμιμους χρήστες του Διαδικτύου [30]. Ακολουθούν δύο παραδείγματα τέτοιων επιθέσεων:

The Shrew Attack

Αποτελεί μια επίθεση [31] που στοχεύει το πρωτόκολο TCP και εκμεταλλεύεται την ομοιογένεια του ελάχιστου χρόνου αναμετάδοσης - minimum Retransmission Time Out (minRTO) του TCP πρωτοκόλλου. Σε υψηλό επίπεδο, η επίθεση Shrew επιδιώκει να προκαλέσει βραχυπρόθεσμη συμφόρηση συνδέσμων κάθε φορά που νόμιμες TCP ροές οδηγούνται σε εκ νέου μετάδοση. Κατά αυτόν τον τρόπο το πρωτόκολλο TCP "παραπλανάται" και οδηγείται στο συμπέρασμα ότι υπάρχει μια παρατεταμένη περίοδο συμφόρησης, μειώνοντας το ρυθμό αναμετάδοσης του σχεδόν στο μηδέν. Εξαιτίας της ομοιογένειας του minRTO, που σημαίνει ότι οι ροές που υφίστανται ταυτόχρονη απόρριψη πακέτων είναι πιθανό να μεταδώσουν εκ νέου τα πακέτα τους την ίδια

χρονική στιγμή, οι επιθέσεις Shrew μπορούν να προκαλέσουν σοβαρή ζημιά στέλνοντας προσεκτικά κατασκευασμένους κινούμενους τετραγωνικούς παλμούς σε μορφή ροής δεδομένων των οποίων η περίοδος προσεγγίζει το minRTO (π.χ. ένα δευτερόλεπτο) και η διάρκεια προσεγγίζει το maximum Round-Trip Time των νόμιμων ροών (π.χ. 200 χιλιοστά του δευτερολέπτου). Ακόμα χειρότερα, τα αναλυτικά αποτελέσματα της επίθεσης Shrew δείχνει ότι η επιλογή τυχαίων τιμών της παραμέτρου minRTO δεν μπορεί να περιορίσει πλήρως αυτήν την επίθεση.

The RoQ Attack

Η επίθεση RoQ (Reduce of Quality) στοχεύει στη μείωση της απόδοσης του συστήματος και όχι στην πλήρη απενεργοποίηση της υπηρεσίας, σε αντίθεση με την μεγαλύτερη πλειοψηφία των επιθέσεων DoS, ενώ η αποτελεσματικότητά της επίθεσης αξιολογείται από την αναλογία μεταξύ ζημιάς και κόστους [32]. Η συγκεκριμένη επίθεση μπορεί να εφαρμοστεί με παρόμοιο τρόπο όπως και η Shrew. Ο επιτιθέμενος κατευθύνει μια περιοδική κυματομορφή σε ένα σύνδεσμο - στόχο για να αποσταθεροποιήσει τη διαδικασία προσαρμογής του το σύστημα, εμποδίζοντας το έτσι να συγκλίνει σε σταθερή κατάσταση όπου η απόδοση είναι συνήθως βέλτιστη. Η κύρια διαφορά των επιθέσεων αυτών είναι ότι ενώ η επίθεση Shrew εκμεταλλεύεται τις ιδιαιτερότητες του πρωτοκόλλου TCP, η επίθεση RoQ δεν χρησιμοποιεί κάποιο συγκεκριμένο μηχανισμό ή πρωτόκολλο, απλώς υποβαθμίζει την απόδοση του στόχου - συστήματος προσπαθώντας να μεγιστοποιήσει την αναλογία μεταξύ ζημιάς και κόστους.

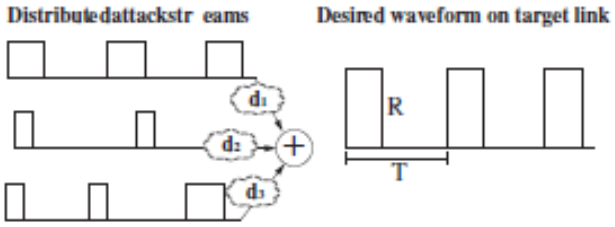
4.3 Προκαλώντας Συμφόρηση στο Διαδίκτυο μέσω Συντονισμένων και Αποκεντρωμένων Παλμοδικών Επιθέσεων

4.3.1 Εισαγωγή

Όπως περιγράψαμε και παραπάνω οι παλμοδικές επιθέσεις στοχεύουν συγκεκριμένους συνδέσμους στο Διαδίκτυο και μπορεί να είναι πιο επιβλαβείς από απλές link flooding επιθέσεις, γιατί μπορούν να εμποδίσουν τις νόμιμες ροές στέλνοντας περιοδικούς παλμούς. Για παράδειγμα, ειδικά σχεδιασμένοι περιοδικοί παλμοί σε ένα σύνδεσμο δικτύου μπορούν να εξαπατήσουν τις νόμιμες ροές TCP ώστε να βρίσκονται σε παρατεταμένη συμφόρηση. Σήμερα, ωστόσο, οι παλμοδικές επιθέσεις DDoS μεγάλης κλίμακας παρουσιάζουν δύο κύριους περιορισμούς που καθιστούν την επίθεση αναποτελεσματική ή εύκολα ανιχνεύσιμη από απλούς μηχανισμούς άμυνας. Οι δύο αυτοί περιορισμοί αναλύονται παρακάτω:

Κεντρικός Συντονισμός (Centralized Coordination)

Ο επιτιθέμενος πρέπει να συντονίσει τα κατανεμημένα bots έτσι ώστε να προστεθούν οι ροές του και αθροιστικά να δημιουργήσουν την επιθυμητή κυματομορφή που μοιάζει με περιοδικούς παλμούς μεγάλης έντασης στη σύνδεση στόχου, όπως απεικονίζεται και στο Σχήμα 4.5. Οι συνηθισμένες παλμοδικές επιθέσεις απαιτούν κεντρικό συντονισμό [33], [34] και έτσι θυσιάζεται η μυστικότητα, καθώς αυτός ο κεντρικός συντονιστής γίνεται από μόνος του σημείο αποτυχίας για την επίθεση.



Σχήμα 4.5: Κατανεμημένες Παλμοδικές Επιθέσεις

Μη Ακριβής εκτίμηση καθυστέρησης (Inaccurate delay estimation.)

Για την παραγωγή της επιθυμητής παλμοδικής κυματομορφής, τα βοτς πρέπει να συντονίζονται μεταξύ τους έτσι ώστε τα πακέτα επίθεσης να φτάσουν στο στόχο συγχρονισμένα. Δυστυχώς, συγχρονισμός ρολογιών εκατοντάδων χιλιάδων bots είναι δύσκολο σε ένα περιβάλλον ευρείας περιοχής. Επίσης αυτό που δυσχεραίνει ακόμη περισσότερο τη διαδικασία αποτελεί το γεγονός ότι ο ίδιος ο συγχρονισμός είναι ανεπαρκής λόγω της δυσκολίας της εκτίμησης της καθυστέρησης από κάθε bot μέχρι να φτάσει στο σύνδεσμο προορισμού. Έτσι οι παλμοδικές επιθέσεις κάνουν την υπόθεση ότι οι καθυστερήσεις παραμένουν αμετάβλητες καθ 'όλη τη διάρκεια της πορείας μιας επίθεσης και εκτιμούν τις τιμές καθυστέρησης μέσω μιας μοναδικής μέτρησης κατά την αρχή της επίθεσης. Λόγω της δυναμικής φύσης της κυκλοφορίας στο Διαδίκτυο, ειδικά κατά τη διάρκεια επιθέσεων, τα bots αποτυγχάνουν να συγχρονιστούν όταν βασίζονται σε μετρήσεις μιας φοράς ή ακόμη και σε περιοδικές μετρήσεις που όμως πραγματοποιούνται με ανώφελο τρόπο.

Τα εμπόδια αυτά ξεπεράστηκαν μέσω ενός πιο εξελιγμένου είδους παλμοδικής επίθεσης, το οποίο υλοποιεί τον αποκεντρωμένο συντονισμό και συγχρονισμό των bots, επιτυγχάνοτας συγχρόνως και την μέγιστη δυνατή καταστροφικότητα και μη εντοπισημότητα. Η επίθεση αυτή [30] η οποία προκαλεί συμφόρηση στο Διαδίκτυο μέσω συντονισμένων και αποκεντρωμένων παλμοδικών επιθέσεων (Congesting the Internet with Coordinated And Decentralized Pulsating Attacks - CICADAS) βασίζεται σε δύο βασικές ιδέες:

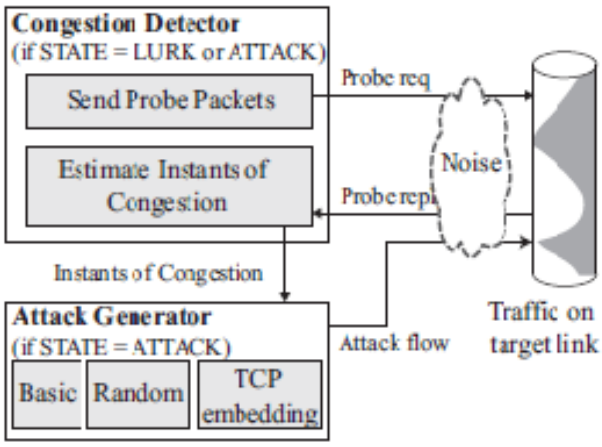
- **Χρησιμοποιώντας τη συμφόρηση ως έμμεσο σήμα συντονισμού:** Προκειμένου να συγχρονιστούν τα bots χωρίς κεντρικό ελεγκτή - συντονιστή, προτείνεται τα bots να χρησιμοποιούν τα στιγμιότυπα συμφόρησης στο σύνδεσμο προορισμού ως σήμα επικοινωνίας για συγχρονισμό μεταξύ τους. Η χρήσιμοποίση της συμφόρησης για κρυφή επικοινωνία έχει δύο πλεονεκτήματα. Πρώτον, το σήμα μπορεί να παρατηρηθεί από κάθε bot. Δεύτερον, επειδή το ίδιο το σήμα είναι κρίσιμο για σημαντικά πρωτόκολλα δικτύωσης όπως η αποφυγή συμφόρησης TCP, εξουδετερώνονται μηχανισμοί άμυνας που προσπαθούν να παρέμβουν στο σήμα.

- **Θεωρητική προσέγγιση ελέγχου για ακριβή εκτίμηση καθυστέρησης:** Προκειμένου να αντισταθμιστούν οι παραλλαγές καθυστέρησης

στον σύνδεσμο προορισμού, σχεδιάζουμε έναν αλγόριθμο ρύθμισης της ροής της επίθεσης που προσαρμόζει δυναμικά τη φάση και το μέγεθος κάθε ροής επίθεσης με βάση προηγούμενες μετρήσεις RTT. Εφαρμόζοντας μια μέθοδο θεωρίας ελέγχου (control theory concept), ο αλγόριθμος μπορεί να εκτιμήσει με ακρίβεια την επίθεση στέλνοντας χρόνο έτσι ώστε τα bots να δημιουργούν συλλογικά την επιθυμητή κυματομορφή στο σύνδεσμο στόχο.

Ο πρωταρχικός στόχος της επίθεσης CICADAS είναι ο συντονισμός της συμπεριφοράς των bots με αποκεντρωμένο τρόπο και με ελάχιστες παραδοχές σχετικά με την κατάσταση του Διαδικτύου, όπως διακυμάνσεις καθυστέρησης. Ως καταλύτης για την ενεργοποίηση των bots και κατά συνέπεια της επίθεσης, μπορεί να χρησιμοποιηθεί η συμφόρηση σε έναν σύνδεσμο στόχο. Κάθε bot μπορεί να παρατηρεί τον σύνδεσμο-στόχο για τυχόν συμφορήσεις (λειτουργούν ως σήμα συγχρονισμού) εξετάζοντας διάφορες μετρικές, όπως η απώλεια πακέτων ή η καθυστέρησή τους και να συγχρονίζονται με εκείνες. Συγκεκριμένα κάθε bot μπορεί να συμπεράνει το εύρος της συμφόρησης μέσω των διαφοροποιήσεων στην καθυστέρηση μεταφοράς στο σύνδεσμο - στόχο και αναλόγως να δράσει όπως φαίνεται και στο Σχήμα 4.6. Με βάση τα προαναφερθέντα, τα δύο σημαντικότερα συστατικά της επίθεσης αποτελούν:

- **Ο ανιχνευτής συμφόρησης (Congestion Detector)** ο οποίος εκτιμά τις στιγμές συμφόρησης στο σύνδεσμο - στόχο με βάση τα παρατηρούμενα RTTs.
- **Η γεννήτρια της επίθεσης (Attack Generator)** η οποία χρησιμοποιεί αυτές τις εκτιμήσεις για ρύθμιση της ροή επίθεσης, έτσι ώστε οι κατανεμημένες κακόβουλες ροές να μπορούν αθροιστικά να δημιουργούν περιοδικούς παλμούς στο σύνδεσμο - στόχο χωρίς τη βοήθεια ενός κεντρικού συντονιστή - ελεγκτή.



Σχήμα 4.6: Υλοποίηση της επίθεσης CICADAS

4.3.2 Στάδια Επίθεσης

Η επίθεση CICADAS διακρίνεται από 3 στάδια: α) τη φάση εκκίνησης (BOOTSTRAP), β) τη φάση παραμονής (LURK) και γ) τη φάση της επίθεσης (ATTACK). Τα στάδια αυτά ή αλλιώς οι καταστάσεις της επίθεσης εναλάσσονται μεταξύ τους όπως βλέπουμε και στο Σχήμα 4.7 ανάλογα με τις συνθήκες που επικρατούν στο δίκτυο. Παρακάτω περιγράφουμε τις ενέργειες των bots σε κάθε κατάσταση.

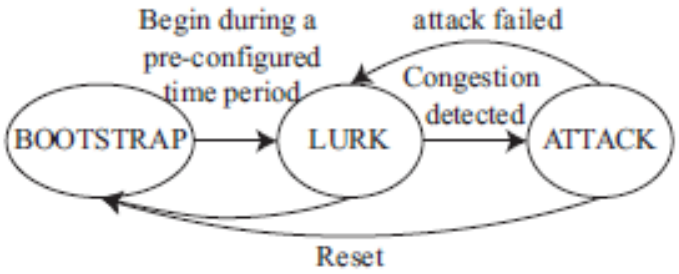
- **BOOTSTRAP:** Στη φάση εκκίνησης - BOOTSTRAP, κάθε bot λαμβάνει παραμέτρους επίθεσης, συμπεριλαμβανομένου του συνδέσμου στόχου και της κυματομορφής (δηλαδή, την περίοδο επίθεσης, το μήκος ξεσπάσματος και το πλάτος ξεσπάσματος). Για παράδειγμα, αυτή η φάση λαμβάνει χώρα όταν ο επιτιθέμενος δημιουργεί το "στρατό" του αποτελούμενο από τα bots. Στο τέλος αυτής της φάσης, τα bots δεν απαιτείται να στείλουν κάποια ροή κίνησης. Τα bots μπορούν να μετακινηθούν στην επόμενη κατάσταση (LURK) σε ένα προκαθορισμένη στιγμή ή όταν το εκτιμώμενο μέγεθος του botnet έχει περάσει ένα κατώτατο όριο [35], [36]. Πρέπει να σημειωθεί ότι τα bots μπορούν να εισέλθουν στην κατάσταση LURK σε διαφορετικούς χρόνους, δηλαδή δεν απαιτείται συγχρονισμός.

- **LURK:** Κάθε bot στην κατάσταση LURK παρακολουθεί κρυφά το σύνδεσμο - στόχο στέλνοντας RTTs. Μόλις ανιχνευθεί η συμφόρηση (π.χ., παρατηρούνται υψηλά RTTs), το bot μεταβαίνει στην κατάσταση ATTACK.

- **ATTACK:** Κατά τη διάρκεια της κατάστασης ATTACK, τα bots αρχίζουν να στέλνουν τετραγωνικούς παλμούς στο σύνδεσμο - στόχο με σκοπό να δημιουργήσουν περιοδική συμφόρηση σε αυτόν. Επιπλέον, τα bots προσαρμόζουν τη φάση και το μέγεθος του επόμενου παλμού με βάση τις παρατηρήσεις προηγούμενης συμφόρησης, ώστε να βελτιωθεί το επίπεδο συντονισμού μεταξύ τους και να αυξηθεί η συμφόρηση στο σύνδεσμο - στόχο. Ο αριθμός των bots που θα ενεργοποιηθούν είναι ζωτικής σημασίας για την επίθεση, καθώς αν είναι ικανός αυτός ο αριθμός θα παρατηρηθεί συμφόρηση στο στόχο ενώ η νόμιμη κίνηση θα περιορίζεται από τις κακόβουλες ροές. Εάν ο συντονισμός της επίθεσης αποτύχει (δηλαδή, υπάρχει έλλειψη σοβαρής συμφόρησης για μεγάλο χρονικό διάστημα του χρόνου), τότε τα bots επιστρέφουν στην κατάσταση LURK.

Εκτιμητής Συμφορήσεων

Όπως προαναφέρθηκε, η επίθεση CICADAS χρησιμοποιεί τον εκτιμητή συμφορήσεων για να συντονίσει τα bots και να πραγματοποιήσει την επίθεση. Ο εκτιμητής επιτελεί δύο λειτουργίες: α) αποστολή πακέτων εξερεύνησης (probes) στο σύνδεσμο στόχο και β) εκτίμηση της στιγμής συμφόρησης στον σύνδεσμο αυτόν. Ειδικότερα, στην πρώτη φάση πραγματοποιείται αποστολή πακέτων probes μεταξύ των bots, με την προϋπόθεση ότι εκείνα διέρχονται από τον σύνδεσμο στόχο. Στη συνέχεια, τα bots παρατηρούν τα RTTs των πακέτων αυτών τα οποία χρειάζονται κατά



Σχήμα 4.7: CICADAS's state machine

τη δεύτερη φάση. Η δεύτερη φάση του εκτιμητή περιλαμβάνει μετρήσεις των RTTs προκειμένου να αποφανθεί εάν στο σύνδεσμο στόχο γίνεται έναρξη, εξέλιξη ή υποχώρηση φαινομένου συμφόρησης, ενώ παράλληλα λαμβάνονται υπόψιν προηγούμενες εκτιμήσεις συμφορήσεων για λόγους ακριβείας. Το τελευταίο πραγματοποιείται με τη χρήση του φίλτρου Kalman (Kalman filter) όπου απορρίπτονται τυχόν παρεμβολές (θόρυβοι) που προκύπτουν από τη φύση και την πολυπλοκότητα του Διαδικτύου. Με τον τρόπο αυτό, η τελική εκτίμηση είναι πιο κοντά στην αναμενόμενη.

Γεννήτρια Επιθέσεων

Ο επιτιθέμενος έχει ως σκοπό να συντονίσει όλες τις μεμονωμένες ροές των bots σε έναν τετραγωνικό παλμό στο σύνδεσμο στόχο με αποτέλεσμα την πρόκληση ισχυρής συμφόρησης. Για τη δημιουργία των μεμονωμένων αυτών ροών η επίθεση CICADAS κάνει χρήση της τεχνικής TCP embedding, η οποία εκμεταλλεύεται τις ιδιαιτερότητες του πρωτοκόλλου TCP και συγκεκριμένα τον αλγόριθμο ελέγχου συμφορήσεων που υλοποιεί. Με τον τρόπο αυτό, η επίθεση CICADAS είναι δύσκολο να ανιχνευτεί από τους μηχανισμούς προστασίας του διαδικτύου, καθώς επίσης διατηρεί τη συμφόρηση για μεγαλύτερα χρονικά διαστήματα προκαλώντας μεγαλύτερη ζημιά στην περιοχή-στόχο.

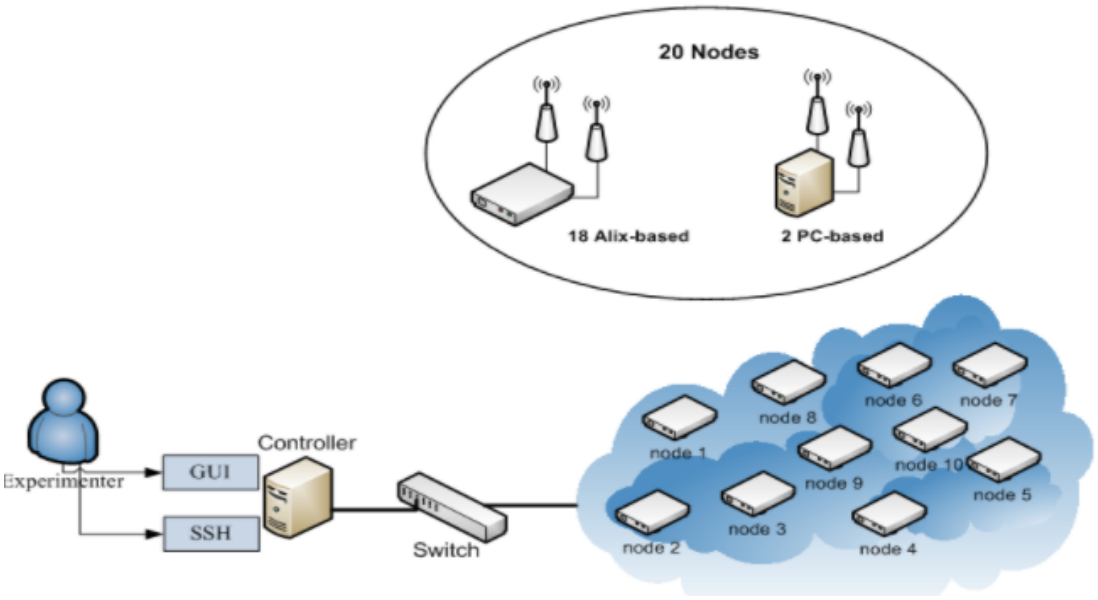
Κεφάλαιο 5

Υλοποίηση Επίθεσης

Σε αυτό το κεφάλαιο περιγράφεται ο σχεδιασμός της επίθεσης που υλοποιήθηκε στο πλαίσιο της διπλωματικής αυτής, τα εργαλεία που χρησιμοποίηθηκαν καθώς και τα αποτελέσματα.

5.1 Netmode Testbed

Η επίθεση πραγματοποιήθηκε σε πραγματικό σύστημα του εργαστηρίου, στο Netmode Testbed. Το σύστημα αυτό [37] αποτελείται από ένα διακομιστή (server) που έχει τον ρόλο του controller και από 20 ασύρματους κόμβους (2 κόμβοι pc-based και 18 alix-based). Όλοι οι κόμβοι συνδέονται μεταξύ τους μέσω ενός μεταγωγέα (switch). Όπως φαίνεται και παρακάτω στο Σχήμα 5.1 ο χρήστης μέσω του διακομιστή - controller, ο οποίος τρέχει ένα webserver με γραφικό περιβάλλον (GUI) αλλά και ένα SSH server, έχει πρόσβαση στους ασύρματους κόμβους. Όλες οι λειτουργίες του Testbed σχετικά με τον έλεγχο και τη διαχείριση του στηρίζονται στο OMF framework [38].



Σχήμα 5.1: Netmode Testbed

Ο controller χρησιμοποιεί λειτουργικό σύστημα Debian GNU/Linux 8 ενώ για το πείραμα χρησιμοποιήθηκαν scripts γραμμένα σε γλώσσα python.

5.2 RT-WABest

Το Round-Trip Wireless Available Bandwidth estimation tool (RT-WABest) αποτελεί ένα εργαλείο εκτίμησης του διαθέσιμου εύρους ζώνης και της χωρητικότητας σε ένα μονοπάτι από άκρο σε άκρο ή απλά σε ένα σύνδεσμο όπως το χρησιμοποιούμε στην παρούσα διπλωματική. Σημαντικό είναι το γεγονός ότι δεν χρειάζεται ο χρήστης να έχει τον έλεγχο και των δύο άκρων του μονοπατιού (ή αντιστοίχως του συνδέσμου) [21]. Επίσης, ενώ τα περισσότερα εργαλεία εκτίμησης διαθέσιμου εύρους ζώνης μπορούν να λειτουργήσουν αποκλειστικά σε ενσύρματα δίκτυα το RT-WABest έχει τη δυνατότητα να εκτιμά το εύρος ζώνης και σε ασύρματα δίκτυα. Τα χαρακτηριστικά αυτά το καθιστούν ως μία από τις ιδανικές επιλογές για τον υπολογισμό συμφορήσεων στην υλοποίηση της επίθεσης.

5.2.1 Εκτίμηση της Χωρητικότητας

Προκειμένου να εκτιμηθεί η χωρητικότητα (capacity) ενός μονοπατιού από άκρο σε άκρο, στο οποίο εκτελείται το RT-WABest, αποστέλλονται από την πηγή προς τον αποδέκτη N δυάδες πακέτων με μέγεθος L. Η χωρητικότητα C του μονοπατιού υπολογίζεται από τον τύπο:

$$C = median \frac{L}{RTT_2^i - RTT_1^i} \quad (i = 1, 2, ..., N) \tag{5.1}$$

όπου το RTT_1^i είναι το Round-Trip Time του πρώτου πακέτου της i-οστής δυάδας πακέτων και το RTT_2^i είναι το Round-Trip Time του δεύτερου πακέτου της δυάδας πακέτων. Για να υπολογίσουμε τη διασπορά με την οποία καταφθάνουν τα πακέτα απάντησης της συγκεκριμένης δυάδας πίσω στην πηγή (βλ. τεχνική TOPP) παίρνουμε τη διαφορά τους, δηλαδή το $RTT_2^i - RTT_1^i$. Στην ουσία όμως χρειαζόμαστε τη διαφορά μεταξύ των χρόνων που απαιτούνται έτσι ώστε να φτασουν τα πακέτα μόνο από την πηγή στον αποδέκτη και αντίστροφα. Παρακάτω βλέπουμε ότι τα RTTs εκφυλίζονται στους χρόνους αυτούς, λόγω της ιδιαιτερότητας των TCP RST πακέτων.

Συγκεκριμένα ο υπολογισμός των RTTs των πακέτων γίνεται μέσω της αποστολής TCP SYN πακέτων μεγέθους ίσο με την MTU σε μία πόρτα του αποδέκτη, η οποία ειναι "κλειστή". Αυτό εχει ως συνέπεια να αποστέλλονται πακέτα TCP RST ως απάντηση στα TCP SYN πακέτα, με την ιδιαιτερότητα όμως ότι το μικρό μέγεθός τους συμβάλλει στο να μην συναντούν σχεδόν καμία καθυστέρηση στην επιστροφή. Όπως έχει προαναφερθεί οι περισσότερες τεχνικές και εργαλεία εκτίμησης του διαθέσιμου εύρους ζώνης λειτουργούν μόνο σε ενσύρματα δίκτυα, καθώς σε αυτά δεν υπάρχει περίπτωση η απάντηση ενός πακέτου παλαιότερου σε σειρά να συναγωνιστεί την απάντηση ενός νεότερου. Το RT-WABest καταφέρνει να ξεπεράσει αυτό το εμπόδιο αποστέλλοντας μία συνεχόμενη (back-to-back) δυάδα πακέτων. Ειδικότερα,

το πρώτο πακέτο είναι TCP RST πακέτο μεγέθους ίσο με την MTU και το δεύτερο ένα TCP SYN πακέτο, και μεγέθους ίσο με την MTU. Το TCP RST πακέτο όμως δεν προκαλεί την δημιουργία απάντησης στο δίκτυο, οπότε δεν υπάρχει κάποια απάντηση, η οποία να συναγωνιστεί την απάντηση του δεύτερου TCP SYN πακέτου.

5.2.2 Εκτίμηση του Διαθέσιμου Εύρους Ζώνης

Εφόσον έχει υπολογιστεί η χωρητικότητα C του μονοπατιού από άκρο-σε-άκρο (ή ενός συνδέσμου), είναι δυνατό να υπολογιστεί τώρα το διαθέσιμο εύρος ζώνης A ολόκληρου του μονοπατιού (αντίστοιχα ενός συνδέσμου) μέσω του τύπου:

$$A = \begin{cases} 2C - \frac{C^2}{R}, if & (R \geq \frac{C}{2}) \\ 0, if & (R < \frac{C}{2}) \end{cases} \tag{5.2}$$

όπου το R είναι ο μέσος ρυθμός διασποράς στον αποδέκτη.

Για τον υπολογισμό του μέσου ρυθμού διασποράς R το RT-WABest στέλνει από την πηγή στον αποδέκτη ένα τραίνο πακέτων αποτελούμενο από K TCP SYN διαδοχικά πακέτα, σε μία ανενεργή πόρτα. Τα πακέτα αυτά δημιουργούν ως απαντήσεις πακέτα TCP RST. Όπως προαναφέρθηκε τα πακέτα αυτά δεν συναντούν μεγάλη καθυστέρηση στο μονοπάτι της επιστροφής λόγω του μικρού μεγέθους τους. Ο μέσος ρυθμός διασποράς υπολογίζεται τότε από τον τύπο:

$$R = \frac{L}{mean(T_i)} \quad (i = 1, 2, ..., K-1) \tag{5.3}$$

όπου το Ti αποτελεί τη διασπορά των πακέτων TCP RST πακέτων (όπως στην εξίσωση 5.1), που αποτελούν απάντηση στη δυάδα των TCP SYN πακέτων με αριθμούς $i+1$ και i, αντίστοιχα.

Ύστερα, μέσω της εξίσωσης 5.2 υπολογίζεται εύκολα το διαθέσιμο εύρος ζώνης του από άκρο-σε-άκρο μονοπατιού. Επίσης αξίζει να επισημανθεί ότι το RT-WABest φροντίζει, ώστε να μην έχουμε ανταγωνισμό μεταξύ ενός TCP SYN πακέτου και ενός προηγούμενου TCP RST πακέτου. Συγκεκριμένα, περιμένει κάποιο χρονικό διάστημα (timeout) μέχρι να φτάσει η απάντηση TCP RST ενός προηγούμενου TCP SYN πακέτου στην πηγή πριν στείλει το επόμενο TCP SYN πακέτο. Αν περάσει ο χρόνος αυτός τότε το TCP RST πακέτο θεωρείται ως "χαμένο" και προβαίνει στην αποστολή του επόμενου TCP SYN πακέτου.

5.3 Περιγραφή Συστήματος

Στα πλαίσια της διπλωματικής αυτής είχαμε τη δυνατότητα να χρησιμοποιήσουμε 7 κόμβους από το Testbed με διαφορετικούς ρόλους όπως φαίνεται και στον Πίνακα 5.1.

NodeId	Role
1	monitor
2	target
3	user
5	coordinator
6	attacker
14	attacker
16	user

Πίνακας 5.1: Ρόλος του κάθε κόμβου

Νόμιμοι χρήστες

Διαθέτουν μόνο μία διεπαφή για σύνδεση στο δίκτυο ενώ ο μοναδικός σκοπός τους είναι απλά να δημιουργήσουν νόμιμη κίνηση στο δίκτυο (Cross traffic), η οποία παρεμβάλλεται από την κακόβουλη κίνηση. Έτσι, οι κόμβοι 3 και 16 , που αποτελούν τους νόμιμους χρήστες του πειράματος, μέσω python scripts απλά αποστέλλουν στο δίκτυο κίνηση TCP η οποία όμως μεταβάλλεται με το χρόνο.

Περιοχή - στόχος

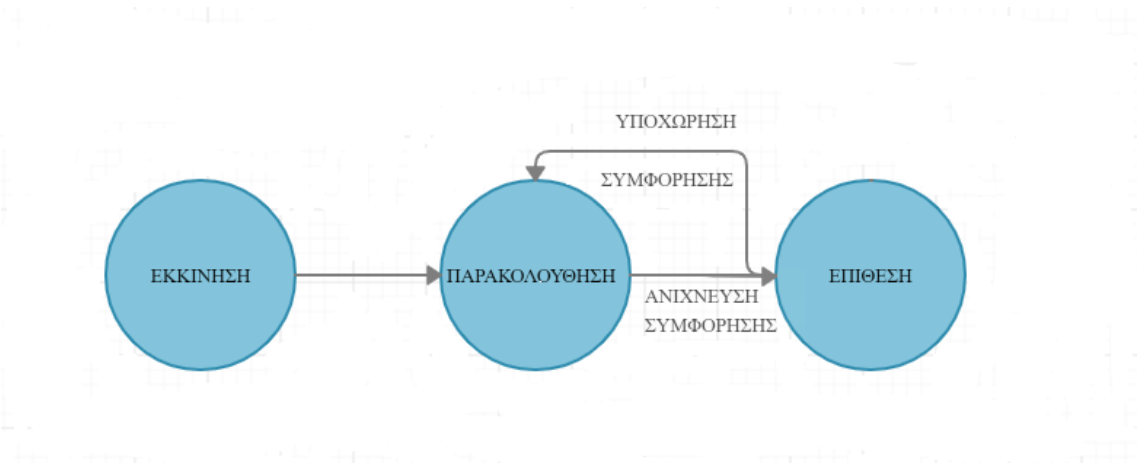
Ο κόμβος 6 που αποτελεί την περιοχή - στόχο της επιθέσης απλά δέχεται ροές κίνησης είτε νόμιμες είτε κακόβουλες.

Bots

Αποτελούν πολύπλοκα συστήματα καθώς διαθέτουν περισσότερες από 1 διεπαφές για τη σύνδεση στο δίκτυο. Κατά αυτόν τον τρόπο έχουν τη δυνατότητα να διαχωρίζουν την κίνηση τους στο δίκτυο ώστε να μην γίνονται αντιληπτά. Στα πλαίσια αυτής της εργασίας η κάθε διεπαφή αντιστοιχεί σε έναν κόμβο ο οποίος έχει μια διεπαφή συνδεδεμένη στο δίκτυο. Έτσι, χρησιμοποιώντας 2 διαφορετικούς κόμβους (6 και 14) με μία διεπαφή ο καθένας, προσωμοιώνουμε ένα bot με 2 διαφορετικές διεπαφές που έχει τη δυνατότητα να αποστέλλει κίνηση ταυτόχρονα μέσω πολλαπλών διεπαφών. Ο κόμβος 5 αναλαμβάνει το ρόλο του συντονιστή της επίθεσης. Οι κακόβουλοι αυτοί κόμβοι επίσης μέσω python scripts οργανώνουν την επίθεση τους. Πρέπει να σημειωθεί ότι λόγω περιορισμών του συστήματος μας εξετάζουμε μια βασική περίπτωση με 3 bots, 1 συντονιστή, 1 bot με 2 διεπαφές και 1 bot προκειμένου να μετράει το διαθέσιμο εύρος ζώνης, ενώ σε πραγματικά σενάρια επιθέσεων τα bots είναι χιλιάδες.

5.4 Στάδια της Επίθεσης

Η επίθεση μας χωρίζεται σε τρία στάδια: το στάδιο της Εκκίνησης, το στάδιο της Παρακολούθησης και τέλος το στάδιο της Επίθεσης, όπως φαίνεται και στο Σχήμα 5.2, με τις αντίστοιχες μεταβάσεις μεταξύ τους. Τα στάδια αυτά βρίσκονται σε αντιστοιχία με τα τρία στάδια της επίθεσης CICADAS [30] (BOOTSTRAP phase , LURK phase, ATTACK phase). Παρακάτω περιγράφεται αναλυτικά η κάθε φάση της επίθεσης.



Σχήμα 5.2: Στάδια της επίθεσης

Εκκίνηση

Κατά τη φάση της εκκίνησης συνδέονται τα bots στο σύστημα. Οι κόμβοι που αναλαμβάνουν τη διαδικασία της επίθεσης χωρίζονται σε ένα master (συντονιστής) και 3 slaves (οι 3 διεπαφές). Ο κάθε κόμβος με την ιδιότητα slave ανοίγει ένα socket ώστε να συνδεθεί με το συντονιστή και να επικοινωνεί μαζί του μέσω του socket. Όταν συνδεθούν όλοι οι κόμβοι και ο συντονιστής τους στείλει μέσω του socket τη διεύθυνση IP του στόχου μεταβαίνουμε στο στάδιο της παρακολούθησης. Παράλληλα, οι κόμβοι που αντιστοιχούν στους νόμιμους χρήστες έχουν ξεκινήσει την αποστολή ροών κίνησης.

Παρακολούθηση

Αποτελεί την πιο σημαντική διαδικασία και καθορίζει την επιτυχία της επίθεσης. Οι κόμβοι έχουν διαφορετικό ρόλο ο καθένας σε αυτή τη φάση. Συγκεκριμένα ο κόμβος 1, που είναι πιο κοντά στην περιοχή στόχου, κάνει χρήση του εργαλείου RT-WABest ώστε να υπολογίζει το διαθέσιμο εύρος ζώνης (available bandwidth) του συνδέσμου - στόχου. Πρέπει να σημειωθεί ότι γνωρίζουμε τη συνολική χωρητικότητα του συνδέσμου από μετρήσεις που έχουμε πραγματοποιήσει πριν το πείραμα. Έτσι λοιπόν, κάθε φορά που τρέχει η συνάρτηση του RT-WABest επιστρέφει μία τιμή

σε Mb/s που αποτελεί και το διαθέσιμο εύρος ζώνης του συνδέσμου που αποτελεί στόχο της επίθεσης. Διαιρώντας τον αριθμό αυτόν με τη συνολική χωρητικότητα του συνδέσμου υπολογίζουμε ένα ποσοστό που φανερώνει πόσο μεγάλο ή μικρό είναι το διαθέσιμο εύρος ζώνης σε σχέση με τη χωρητικότητα. Όταν αυτό το ποσοστό πέσει κάτω από ένα κατώφλι (threshold) το οποίο ορίζουμε εμείς στο μισό της συνολικής χωρητικότητας, τότε εξάγουμε το συμπέρασμα ότι υπάρχει συμφόρηση (congestion) και συνεπώς πρέπει να ξεκινήσει η επίθεση. Η συμφόρηση αυτή οφείλεται στην κίνηση που δημιουργείται από τους νόμιμους χρήστες (δηλαδή τους κόμβους 10 και 11). Η κίνηση αυτή όπως και σε πραγματικές συνθήκες μεταβάλλεται με το χρόνο και σαν αποτέλεσμα κάποιες στιγμές παρατηρείται συμφόρηση ενώ κάποιες άλλες όχι.

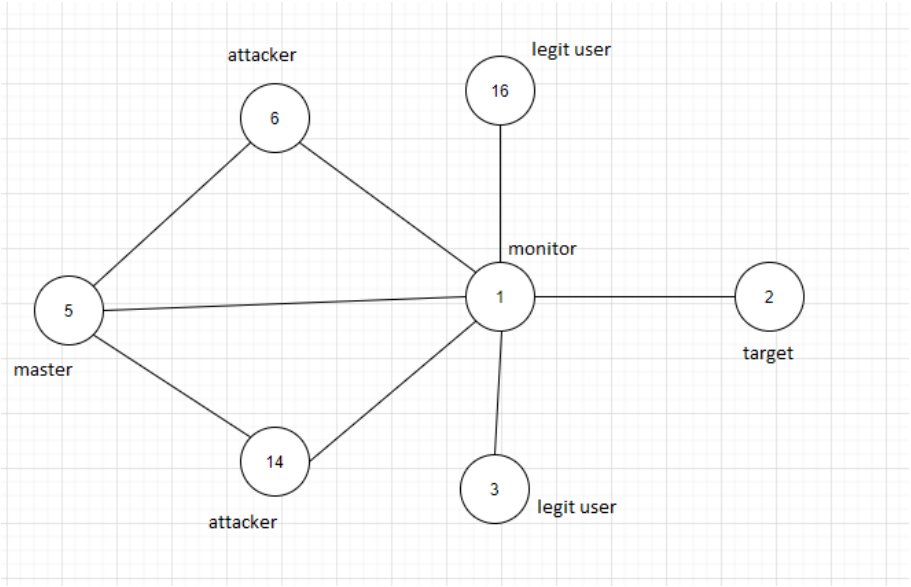
Η συγκεκριμένη συνάρτηση που τρέχει το εργαλείο RT-WABest καλείται ανά 2 δευτερόλεπτα από τον κόμβο 1. Παραλλήλα ο κόμβος ενημερώνει συνεχώς το συντονιστή για το διαθέσιμο εύρος ζώνης του στόχου στέλνοντας του την τιμή που γύρισε η παραπάνω συνάρτηση. Επομένως, για να είναι εφικτό να υλοποιεί παράλληλα δύο λειτουργίες έχει χρησιμοποιηθεί threading. Έτσι με ένα νήμα υλοποιείται η επικοινωνία με τον συντονιστή μέσω socket η οποία είναι διαρκής στέλνοντας πληροφορίες και με ένα άλλο νήμα καλείται η συνάρτηση του RT-WABest. Όταν η συνάρτηση επιστρέφει τιμή του bandwidth που ξεπερνάει το κατώφλι τότε ο συντονιστής συμπεραίνει ότι δεν υπάρχει συμφόρηση οπότε στέλνει μέσω των sockets στους κόμβους 6 και 14 ότι πρέπει να περιμένουν και παραμένουν αδρανείς. Γενικά στην κατάσταση παρακολούθησης οι κόμβοι αυτοί ενημέρωνονται διαρκώς από το συντονιστή για τις ενέργειες τους και όσο δεν υπάρχει συμφόρηση παραμένουν αδρανείς. Αν όμως η τιμή του διαθέσιμου εύρους ζώνης πέσει κάτω από το κατώφλι τότε ενημερώνεται ο συντονιστής, στέλνει εντολή στους κόμβους 6 και 14 να ξεκινήσουν την επίθεση και μεταβαίνουν στο στάδιο της επίθεσης. Επίσης, στέλνεται στους κόμβους αυτούς μέσω του socket τους με τον συντονιστή το μέγεθος της κίνησης που πρέπει να δημιουργήσουν ώστε να "πνίξουν" εντελώς το σύνδεσμο - στόχο.

Επίθεση

Το στάδιο αυτό αποτελεί το τελευταίο στάδιο της επίθεσης μας. Σε αυτό το στάδιο οι κόμβοι 6 και 14 αποστέλλουν πακέτα TCP SYN με ρυθμό ώστε να μηδενίσουν το διαθέσιμο εύρος ζώνης του συνδέσμου στόχου και να το αποκόψουν ουσιαστικά από το δίκτυο. Έτσι, διαχωρίζεται η επίθεση απο δύο διαφορετικές διαδρομές ώστε να προστεθούν αθροιστικά στο σύνδεσμο και να εξαντλήσουν το εύρος ζώνης του. Τα συγκεκριμένα πακέτα λειτουργούν και ως μάσκα για τα επίσης πακέτα TCP SYN που στέλνει το εργαλείο RT-WABest για τις μετρήσεις του. Παράλληλα με τη χρήση thread "ακούνε" διαρκώς, μέσω του socket με το συντονιστή, για τις εντολές του. Ο κόμβος 1 συνεχίζει όπως και στο προηγούμενο στάδιο να υπολογίζει με το εργαλείο RT-WABest το διαθέσιμο εύρος ζώνης του συνδέσμου - στόχου ενημερώνοντας το συντονιστή. Όσο διαρκεί η συμφόρηση ο συντονιστής δίνει εντολή στους επιτιθέμενους κόμβους και η επίθεση συνεχίζεται. Αν όμως, μειωθεί η νόμιμη κίνηση και έτσι η τιμή του bandwidth ξεπεράσει το κατώφλι που είχαμε θέσει ο συντονιστής αμέσως ενημερώνει τους επιτιθέμενους κόμβους και επιστρέφουν στο στάδιο παρακολούθησης.

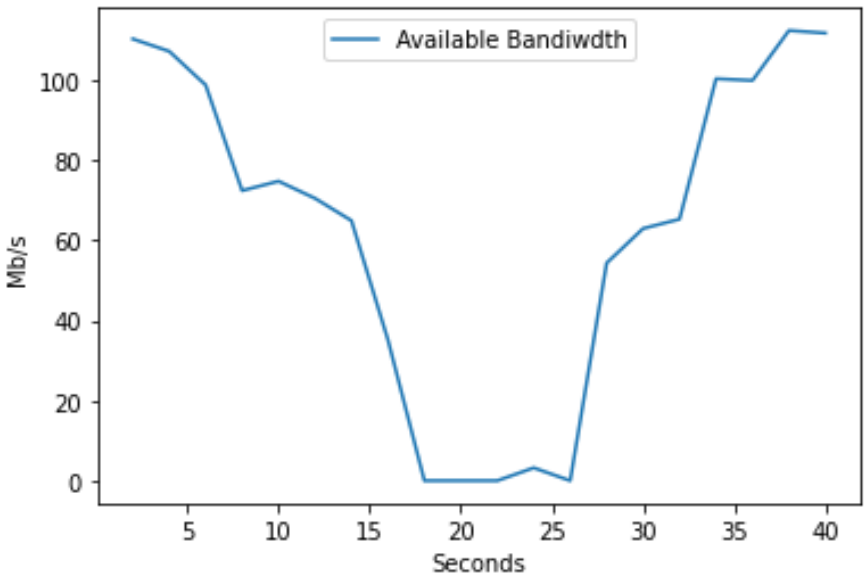
5.5 Αποτελέσματα

Στην υποενότητα αυτή παρουσιάζουμε τα σενάρια που τρέξαμε. Όπως περιγράψαμε και παραπάνω ο κόμβος 1 είχε το ρόλο του εκτιμητή συμφορήσεων επιστρέφοντας την τιμή του διαθέσιμου εύρους ζώνης στον κόμβο 5, που είναι ο συντονιστής. Ανάλογα την εκτίμηση τότε ο συντονιστής δίνει στους κόμβους 6 και 14 εντολή να ξεκινήσουν την επίθεση ή να περιμένουν. Οι κόμβοι 3 και 16 προσομοιώνουν τη λειτουργία των νόμιμων χρηστών ενώ ο κόμβος 2 αποτελεί το θύμα της επίθεσης με στόχο το σύνδεσμο 1-2. Επειδή όλοι οι κόμβοι είναι συνδεδεμένοι μεταξύ τους μέσω ενός μεταγωγέα αλλάξαμε τα routes του καθένα ώστε να δημιουργήσουμε τοπολογίες για τα πειράματα μας. Παρακάτω παρουσιάζεται η τοπολογία του πρώτου σεναρίου.



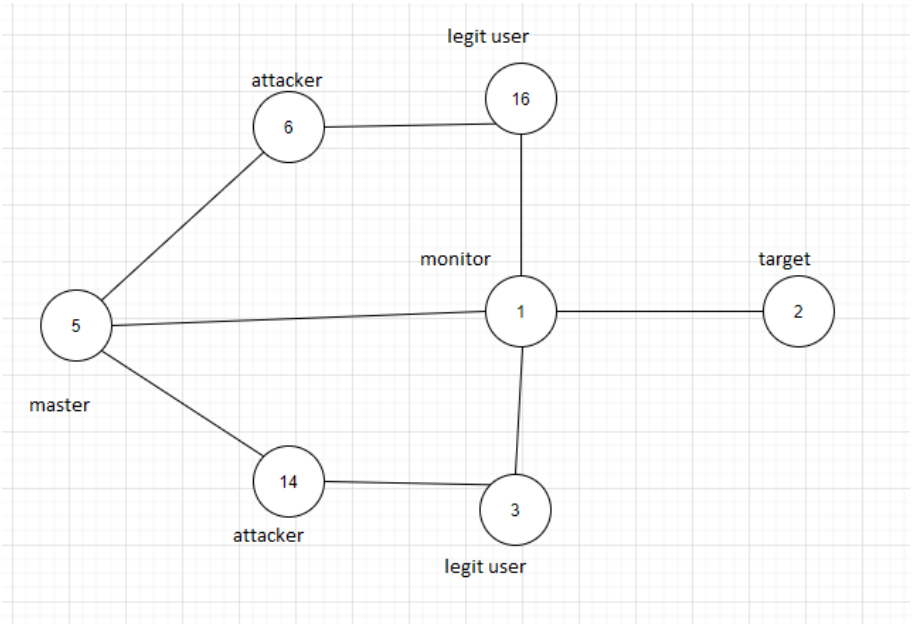
Σχήμα 5.3: Τοπολογία 1ου σεναρίου

Όπως φαίνεται και στο Σχήμα 5.3 στο 1ο σενάριο οι επιτιθέμενοι στέλνουν τις ροές της κίνησης τους κατευθείαν στο σύνδεσμο - στόχο. Το διαθέσιμο εύρος ζώνης του συνδέσμου στόχου έχει μετρηθεί περίπου 120 Mb/s ενώ το κατώφλι για να ξεκινήσει η επίθεση το έχουμε ορίσει στα 60 Mb/s. Έτσι όπως παρουσιάζεται και στο Σχήμα 5.4 όσο οι νόμιμες ροές κυμαίνονται από 120 έως 60 Mb/s οι επιτιθέμενοι απλά παρακολουθούν. Όταν όμως υπάρξει συμφόρηση και το διαθέσιμο εύρος ζώνης πέσει κάτω από τα 60 Mb/s ο συντονιστής δίνει εντολή για την εκκίνηση της επίθεσης. Αυτό συμβαίνει περίπου στο 15ο δευτερόλεπτο του πειράματος και διαρκεί για 10 δευτερόλεπτα. Με το που λήξει η συμφόρηση και οι νόμιμες ροές υποχωρούν, τότε αμέσως σταματάνε και την επίθεση τα bots.

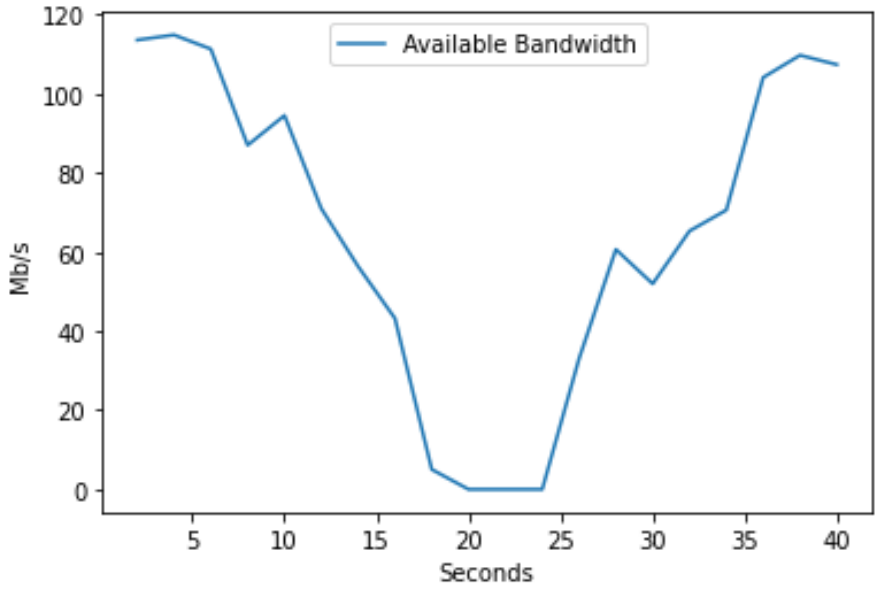


Σχήμα 5.4: Διακύμανση διαθέσιμου εύρους ζώνης 1ου σεναρίου

Στο 2ο σενάριο (βλ. Σχήμα 5.5 η διαφορά είναι οτι οι κακόβουλες ροές (που ξεκινάνε από τους κόμβους 6 και 14) περνάνε πρώτα από τους κόμβους 3 και 16 αντίστοιχα και δεν κινούνται απευθείας προς τον σύνδεσμο-στόχο. Όπως φαίνεται και στο Σχήμα 5.6 η επίθεση λειτουργεί το ίδιο αποτελεσματικά με πριν.



Σχήμα 5.5: Τοπολογία 2ου σεναρίου



Σχήμα 5.6: Διακύμανση διαθέσιμου εύρους ζώνης 2ου σεναρίου

Κεφάλαιο 6

Συμπεράσματα

6.1 Αξιολόγηση

Στη παρούσα διπλωματική εργασία, αρχικά, παρουσιάστηκαν οι βασικές κατανεμημένες επιθέσεις άρνησης υπηρεσιών (Distributed denial of Service - DDoS) αλλά επίσης και το βασικό θεωρητικό υπόβαθρο που διέπει μια τέτοια επίθεση και γενικότερα τα δίκτυα. Στη συνέχεια, αφού έγινε εκτενής αναφορά σε σχετικές εργασίες και εξελιγμένες τεχικές υλοποιήθηκε μια προηγμένη κατανεμημένη επίθεση άρνησης υπηρεσιών μέσω πολλαπλών διεπαφών. Τέλος, εκτελέσαμε σενάρια επίθεσης σε πραγματικά συστήματα στο Testbed του εργαστηρίου Netmode. Από τα αποτελέσματα αυτά μπορούμε να διακρίνουμε την αποτελεσματικότητα της επίθεσης καταναλώνοντας τους πόρους του συνδέσμου στόχου και διακόπτοντας ουσιαστικά τη συνδεσιμότητα του στόχου από το υπόλοιπο δίκτυο. Συμπεραίνουμε λοιπόν την καταστροφικότητα μιας επίθεσης η οποία είναι πολύ δύσκολα ανιχνεύσιμη καθώς οι ροές των bots φαίνονται σαν νόμιμες χωρίς κακόβουλο χαρακτήρα.

6.2 Πιθανοί Τρόποι Αντιμετώπισης

Καθώς οι απλές τεχνικές διαχείρισης κίνησης (Traffic engineering) δεν μπορούν να αντιμετωπίσουν τέτοιου είδους επιθέσεις εφόσον η αλλαγή δρομολόγησης στο δίκτυο δεν επιφέρει αποτέλεσμα. Οι έξυπνες επιθέσεις αλλάζουν με τη σειρά τους το σύνολο των συνδέσμων - στόχων και παρακάμπτουν το συγκεκριμένο μηχανισμό άμυνας. Προτείνεται έτσι ο συνδυασμός των παραπάνω τεχνικών με Λογισμικό Δικτύων (Software Defined Network) βελτιώνοντας έτσι την προσαρμοστικότητα και την ευελιξία του δικτύου όταν παρατηρείται συμφόρηση. Επίσης, τα νευρωνικά δίκτυα μπορούν να συμβάλλουν σημαντικά στην αντιμετώπιση τέτοιων επιθέσεων καθώς έχουν τη δυνατότητα να εκπαιδεύονται με βάση στοιχεία από άλλες επιθέσεις και να αναγνωρίζουν ανωμαλίες στο δίκτυο σε ελάχιστο χρόνο.

Βιβλιογραφία

[1] Saman Taghavi Zargar, James Joshi, and David Tipper. «A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks». In: *IEEE communications surveys & tutorials* 15.4 (2013), pp. 2046–2069.

[2] Vasileios Karyotis and MHR Khouzani. *Malware diffusion models for modern complex networks: theory and applications*. Morgan Kaufmann, 2016.

[3] *What Is a Distributed Denial-of-Service (DDoS) Attack?* `http://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack//`.

[4] *OSI model*. `https://en.wikipedia.org/wiki/OSI_model`.

[5] *DDoS Attack Types & Mitigation Methods | Imperva*. `https://www.imperva.com/learn/application-security/ddos-attacks/`.

[6] *What is a DDoS Botnet?* `https://www.cloudflare.com/learning/ddos/what-is-a-ddos-botnet/`.

[7] S. S. Kolahi, K. Treseangrat, and B. Sarrafpour. «Analysis of UDP DDoS flood cyber attack and defense mechanisms on Web Server with Linux Ubuntu 13». In: *2015 International Conference on Communications, Signal Processing, and their Applications (ICCSPA'15)*. Feb. 2015, pp. 1–5.

[8] *UDP Flood Attack*. `https://www.cloudflare.com/learning/ddos/udp-flood-ddos-attack/`.

[9] *Ping flood*. `https://www.imperva.com/learn/application-security/ping-icmp-flood/`.

[10] N. Gupta et al. «DDoS attack algorithm using ICMP flood». In: *2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom)*. Mar. 2016, pp. 4082–4084.

[11] *SYN flood*. `https://el.wikipedia.org/wiki/SYN_flood`.

[12] T. Yatagai, T. Isohara, and I. Sasase. «Detection of HTTP-GET flood Attack Based on Analysis of Page Access Behavior». In: *2007 IEEE Pacific Rim Conference on Communications, Computers and Signal Processing*. Aug. 2007, pp. 232–235. DOI: `10.1109/PACRIM.2007.4313218`.

[13] *HTTP Flood Attack*. `https://www.cloudflare.com/learning/ddos/http-flood-ddos-attack/`.

[14] L. Rudman and B. Irwin. «Characterization and analysis of NTP amplification based DDoS attacks». In: *2015 Information Security for South Africa (ISSA)*. Aug. 2015, pp. 1–5. DOI: `10.1109/ISSA.2015.7335069`.

[15] Evan Damon et al. «Hands-on Denial of Service Lab Exercises Using SlowLoris and RUDY». In: *Proceedings of the 2012 Information Security Curriculum Development Conference*. InfoSecCD '12. Kennesaw, Georgia: ACM, 2012, pp. 21–29. ISBN: 978-1-4503-1538-8. DOI: 10.1145/2390317.2390321. URL: http://doi.acm.org/10.1145/2390317.2390321.

[16] *5 Most Famous DDoS Attacks*. https://www.a10networks.com/blog/5-most-famous-ddos-attacks/.

[17] C. Dovrolis et al. «Bandwidth estimation: metrics, measurement techniques, and tools». In: vol. 17. 6. Apr. 2003, pp. 27–35.

[18] Sambuddho Chakravarty, Angelos Stavrou, and Angelos Keromytis. «LinkWidth: A Method to Measure Link Capacity and Available Bandwidth using Single-End Probes». In: (Jan. 2008).

[19] *Round-trip delay time*. https://en.wikipedia.org/wiki/Round-trip_delay_time.

[20] *Time to live*. https://searchnetworking.techtarget.com/definition/time-to-live.

[21] Tan Yang et al. «RT-WABest: A novel end-to-end bandwidth estimation tool in IEEE 802.11 wireless network». In: *International Journal of Distributed Sensor Networks* 13.2 (2017).

[22] M. S. Kang, S. B. Lee, and V. D. Gligor. «The Crossfire Attack». In: *2013 IEEE Symposium on Security and Privacy*. May 2013, pp. 127–141. DOI: 10.1109/SP.2013.19.

[23] Max Schuchard et al. «Losing control of the internet: using the data plane to attack the control plane». In: *Proceedings of the 17th ACM conference on Computer and communications security*. 2010, pp. 726–728.

[24] Steven Michael Bellovin and Emden R Gansner. «Using link cuts to attack Internet routing». In: (2003).

[25] Jose Nazario. «DDoS attack trends through 2009-2011». In: *NANOG 54* (2012).

[26] Ahren Studer and Adrian Perrig. «The coremelt attack». In: *European Symposium on Research in Computer Security*. Springer. 2009, pp. 37–52.

[27] Dimitrios Gkounis et al. «On the Interplay of Link-Flooding Attacks and Traffic Engineering». In: *SIGCOMM Comput. Commun. Rev.* 46.2 (May 2016), pp. 5–11. ISSN: 0146-4833. DOI: 10.1145/2935634.2935636. URL: http://doi.acm.org/10.1145/2935634.2935636.

[28] Dimitrios Gkounis, Vasileios Kotronis, and Xenofontas Dimitropoulos. «Towards defeating the crossfire attack using SDN». In: *arXiv preprint arXiv:1412.2013* (2014).

[29] Michalis Faloutsos, Petros Faloutsos, and Christos Faloutsos. «On power-law relationships of the internet topology». In: *ACM SIGCOMM computer communication review* 29.4 (1999), pp. 251–262.

[30] Yu-Ming Ke et al. «Cicadas: Congesting the internet with coordinated and decentralized pulsating attacks». In: *Proceedings of the 11th ACM on Asia Conference on Computer and Communications Security*. 2016, pp. 699–710.

[31] Aleksandar Kuzmanovic and Edward W Knightly. «Low-rate TCP-targeted denial of service attacks: the shrew vs. the mice and elephants». In: *Proceedings of the 2003 conference on Applications, technologies, architectures, and protocols for computer communications*. 2003, pp. 75–86.

[32] Mina Guirguis, Azer Bestavros, and Ibrahim Matta. «Exploiting the transients of adaptation for RoQ attacks on Internet resources». In: *Proceedings of the 12th IEEE International Conference on Network Protocols, 2004. ICNP 2004.* IEEE. 2004, pp. 184–195.

[33] Ying Zhang, Zhuoqing Morley Mao, and Jia Wang. «Low-Rate TCP-Targeted DoS Attack Disrupts Internet Routing.» In: *NDSS*. Citeseer. 2007.

[34] Mina Guirguis, Azer Bestavros, and Ibrahim Matta. «Bandwidth stealing via link targeted RoQ attacks». In: *Proceedings of the 2nd IASTED International Conference on Communication and Computer Networks*. Citeseer. 2004.

[35] Dionysios Kostoulas et al. «Decentralized schemes for size estimation in large and dynamic groups». In: *Fourth IEEE International Symposium on Network Computing and Applications*. IEEE. 2005, pp. 41–48.

[36] Laurent Massoulié et al. «Peer counting and sampling in overlay networks: random walk methods». In: *Proceedings of the twenty-fifth annual ACM symposium on Principles of distributed computing*. 2006, pp. 123–132.

[37] *Netmode Testbed*. `http://www.netmode.ntua.gr/main/index.php?option=com_content&view=article&id=103&Itemid=83`.

[38] *OMF framework*. `http://web.nitlab.inf.uth.gr/fibre/index.php/cmf/omf`.