ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

ΤΜΗΜΑ ΔΙΔΑΚΤΙΚΗΣ ΤΗΣ ΤΕΧΝΟΛΟΓΙΑΣ ΚΑΙ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

DDOS - Distributed Denial of Service Attack

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Του Φούτρη Παρασκευά

Υπεύθυνος Καθηγητής: ΣΩΚΡΑΤΗΣ ΚΑΤΣΙΚΑΣ

ΠΕΙΡΑΙΑΣ 2008

ΠΡΟΛΟΓΟΣ

Η παρούσα διπλωματική εργασία έχει ως θέμα την «Αντιμετώπιση κατανεμημένων επιθέσεων (DDoS)». Κατά τη διάρκεια της εκπόνησής της μου δόθηκε η ευκαιρία να εμβαθύνω ακόμη περισσότερο στο κρίσιμο θέμα της ασφάλειας και να γνωρίσω τις σύγχρονες τάσεις γύρω από το θέμα αυτό.

Παράλληλα, με την ολοκλήρωση της εργασίας αυτής αισθάνομαι την ανάγκη να ευχαριστήσω τον κ. Σωκράτη Κάτσικα, Καθηγητή Πανεπιστημίου Πειραιώς, ο οποίος μου εμπιστεύθηκε την εκπόνησή της, καθώς επίσης για την πολύτιμη βοήθειά του, την καθοδήγηση και τις χρήσιμες υποδείξεις του σε όλα τα στάδια εκτέλεσής της .

ΠΕΡΙΛΗΨΗ

Στην συγκεκριμένη εργασία γίνεται μία εισαγωγή στις DDoS επιθέσεις. Συγκεκριμένα δίνεται ο ορισμός τους ενώ περιγράφονται αναλυτικά όλες γνωστές μέχρι και σήμερα μέθοδοι που έχουν χρησιμοποιηθεί στα διάφορα στάδια αυτών των επιθέσεων. Στην συνέχεια ταξινομούμε τα είδη των επιθέσεων καθώς γίνεται μία συνοπτική αναφορά στα προβλήματα που δημιουργούν.

Σε συνέχεια των παραπάνω παραθέτουμε στοιχεία για τους μηχανισμού αντιμετώπισης που έχουν προταθεί ή εφαρμοστεί πρόσφατα. Στόχος μας είναι η βαθύτερη κατανόηση των DDoS επιθέσεων με απότερω σκοπό την καλύτερη και αποτελεσματικότερη προστασία. Αναλυτικότερα περιγράφουμε ένα είδος DDoS επίθεσης, την SYN Flood η οποία στηρίζει την αποτελεσματικότητα της σε μία συγκεκριμένη αδυναμία του πρωτοκόλλου TCP. Συνοψίζοντας παραθέτουμε και μερικές γενικές πληροφορίες για τους μηχανισμούς ανίχνευσης των επιθέσεων αυτών.

ABSTRACT

In this essay we make an introduction to DDoS attacks. More specific we define this kind of attacks and describe analytically the methods used till recently in all stages. Following we categorize those attacks and point out the consequences.

Following above mentioned we indicate all relevant data regarding the latest procedures suggested or applied in order to prevent those attacks. Based on this we have the opportunity to understand DDoS attacks and be able to explore more effectively the critical matter of protection. We also describe in detail a characteristic DDoS attack, SYN Flood, which takes advantage TCP protocol weakness. Finally we present some general information related to DDoS attacks tracking.

ΠΕΡΙΕΧΟΜΕΝΑ

ΛΙΣΤΑ ΣΧΗΜΑΤΩΝ

ΚΕΦΑΛΑΙΟ

<<ΕΙΣΑΓΩΓΗ>>

- Λίγα λόγια για τα δίκτυα
- Κατανόηση του tcp/ip πρωτοκόλλου
- Αναγκαιότητα ασφάλειας

1 ΕΙΣΑΓΩΓΗ

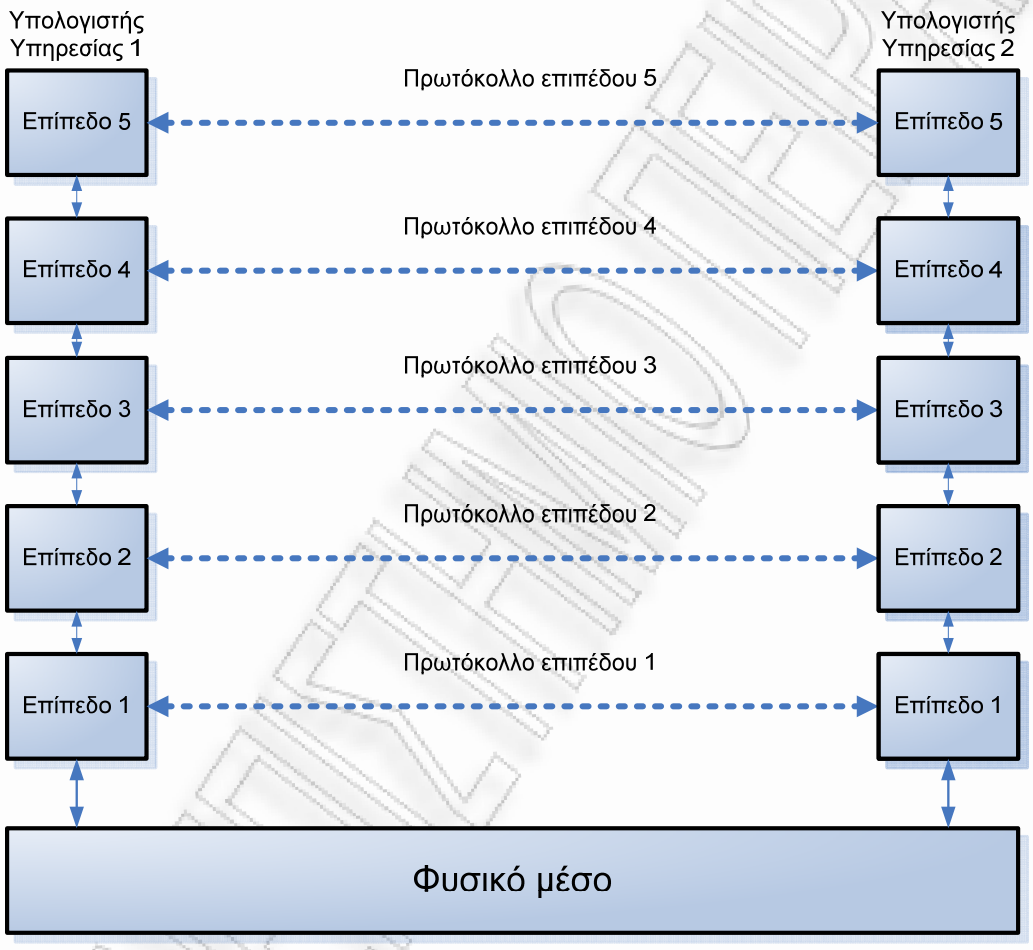
1.1 ΛΙΓΑ ΛΟΓΙΑ ΓΙΑ ΤΑ ΔΙΚΤΥΑ

Δίκτυο ηλεκτρονικών υπολογιστών ή απλά δίκτυο ονομάζεται ένα σύνολο αυτόνομων υπολογιστών που είναι διασυνδεδεμένοι με μια κοινή τεχνολογία. Δύο υπολογιστές λέμε ότι είναι διασυνδεδεμένοι αν είναι σε θέση να ανταλλάσσουν πληροφορίες. Η σύνδεση είναι δυνατόν να γίνεται με χάλκινο σύρμα, με οπτικές ίνες, μικροκύματα, υπέρυθρες ακτίνες και τηλεπικοινωνιακούς δορυφόρους. Κλασσικοί τύποι δικτύων είναι οι εξής:

- **WAN – Wide Area Network (Δίκτυο Ευρείας Περιοχής):** Εκτείνονται σε μια μεγάλη γεωγραφική περιοχή, όπως μια χώρα ή μια ήπειρο.
- **RAN – Regional Area Network**: Δίκτυα τα οποία εκτείνονται σε μια διοικητική περιφέρεια.
- **MAN – Metropolitan Area Network:** Πρόκειται για δίκτυα τα οποία εκτείνονται σε μία πόλη.
- **LAN – Local Area Network**: ιδιωτικά δίκτυα τα οποία βρίσκονται μέσα σε ένα μόνο κτίριο ή κτιριακό συγκρότημα, ή σε μια έκταση με μέγεθος μέχρι λίγα χιλιόμετρα.

Τα πρώτα δίκτυα υπολογιστών σχεδιάστηκαν κατά κύριο λόγω ως προς το υλικό, και μόνο δευτερευόντως εξέταζαν το λογισμικό. Η στρατηγική αυτή δεν αποδίδει πια. Πλέον το λογισμικό δικτύων είναι δομημένο σε υψηλό βαθμό. Για να μειωθεί η σχεδιαστική τους πολυπλοκότητα, τα περισσότερα δίκτυα οργανώνονται σαν μια στοίβα επιπέδων, με τα επίπεδα να χτίζονται το ένα πάνω στο άλλο. Στόχος κάθε επιπέδου είναι να προσφέρει κάποιες υπηρεσίες στα ανώτερα επίπεδα, κρύβοντας απ' τα επίπεδα αυτά τις λεπτομέρειες της υλοποίησης των παρερχομένων υπηρεσιών. Το επίπεδο n σε μια μηχανή πραγματοποιεί μια συνομιλία με το επίπεδο n σε κάποια άλλη μηχανή. Οι κανόνες και οι συμβάσεις που χρησιμοποιούνται σε αυτή τη συνομιλία ονομάζονται συνολικά "πρωτόκολλο του επιπέδου n". Το πρωτόκολλο είναι μια συμφωνία ανάμεσα στα επικοινωνούντα μέρη για το πως πρέπει να διεξάγεται η επικοινωνία. Στην πραγματικότητα, κανένα στοιχείο δεν μεταδίδεται άμεσα από το επίπεδο n της μιας μηχανής στο επίπεδο n της άλλης μηχανής. Αντίθετα, κάθε επίπεδο μεταβιβάζει τα δεδομένα και τις πληροφορίες ελέγχου στο επίπεδο που βρίσκεται ακριβώς κάτω από αυτό, μέχρι να φτάσουμε στο κατώτερο επίπεδο. Κάτω από το επίπεδο 1 βρίσκεται το φυσικό μέσο, μέσω του οποίου εκτελείται η πραγματική επικοινωνία. Ανάμεσα σε κάθε ζεύγος γειτονικών επιπέδων υπάρχει μια διασύνδεση (interface).

Η διασύνδεση ορίζει τις στοιχειώδεις λειτουργίες και υπηρεσίες τις οποίες διαθέτει το κατώτερο επίπεδο προς το ανώτερο επίπεδο. Το σύνολο επιπέδων και πρωτοκόλλων ονομάζεται αρχιτεκτονική δικτύου. Ούτε οι λεπτομέρειες υλοποίησης ούτε οι προδιαγραφές των διασυνδέσεων δεν είναι μέρος της αρχιτεκτονικής. Στον πίνακα 1 φαίνεται ένα τυπικό δίκτυο 5 επιπέδων.



Σχήμα 1 : Επίπεδα πρωτόκολλα και διασυνδέσεις

1.2 ΚΑΤΑΝΟΗΣΗ ΤΟΥ TCP/IP ΠΡΩΤΟΚΟΛΛΟΥ

Το TCP/IP στην πραγματικότητα δεν είναι ένα μόνο πρωτόκολλο, αλλά αποτελείται από έναν αριθμό πρωτοκόλλων, το καθένα από τα οποία παρέχει πολύ συγκεκριμένες υπηρεσίες. Η επιτυχία τους οφείλεται στο μικρό κόστος χρήσης και στην τεράστια εξάπλωση του Internet (που βασίζεται στη στοίβα πρωτοκόλλων TCP/IP) και ειδικά του World Wide Web. Δεν υπάρχει επίσημο μοντέλο αρχιτεκτονικής TCP/IP. Η στοίβα πρωτοκόλλων TCP/IP αποτελείται από τα εξής 4 ανεξάρτητα επίπεδα:

1.2.1 Το επίπεδο διαδικτύου

Η δουλειά του είναι να επιτρέπει στους υπολογιστές υπηρεσίας να εισάγουν τα πακέτα τους σε οποιοδήποτε δίκτυο και αυτά να ταξιδεύουν ανεξάρτητα προς το προορισμό τους. Τα πακέτα μπορεί να φτάσουν ακόμη και με διαφορετική σειρά από αυτήν με την οποία στάλθηκαν. Τότε τα ανώτερα επίπεδα θα πρέπει να αναδιατάξουν τα πακέτα, εάν είναι επιθυμητή η παράδοση με τη σειρά. Το επίπεδο διαδικτύου ορίζει μια επίσημη μορφή για τα πακέτα και ένα επίσημο πρωτόκολλο που ονομάζεται πρωτόκολλο διαδικτύου ή IP. Η δουλειά του επιπέδου διαδικτύου είναι να παραδίδει τα πακέτα εκεί που πρέπει να πάνε. Το βασικό ζήτημα είναι η δρομολόγηση των πακέτων, καθώς και αποφυγή συμφόρησης. Η αρχιτεκτονική των IP διευθύνσεων βασίζεται στο γεγονός ότι το μέγεθος μιας IP διεύθυνσης είναι 32 bits. Οι διευθύνσεις χωρίζονται σε κατηγορίες που ονομάζονται κλάσης και οι οποίες ορίζουν πως θα αντιμετωπίζουν τα συστήματα αυτές τις διευθύνσεις. Τα πρώτα 4 bits ορίζουν και την κλάση της διεύθυνσης. Τα 32 bits της διεύθυνσης χωρίζονται σε 2 μέρη. Το πρώτο αφορά τη διεύθυνση του δικτύου και το δεύτερο την τοπική διεύθυνση. Το πρώτο και πιθανά και τα επόμενα περισσότερο σημαντικά bytes ορίζουν το δίκτυο που ανήκει η διεύθυνση και τα λιγότερο σημαντικά bytes ορίζουν το συγκεκριμένο κόμβο που ανήκει η διεύθυνση.

1.2.2 Το επίπεδο μεταφοράς

Έχει σχεδιαστεί για να επιτρέπει στις ομότιμες οντότητες στους υπολογιστές υπηρεσίας προέλευσης και προορισμού να συνομιλούν. Έχουν οριστεί 2 πρωτόκολλα μεταφοράς από άκρο εις άκρο. Το πρωτόκολλο ελέγχου μετάδοσης ή TCP, είναι ένα αξιόπιστο συνδεσμοστρεφές πρωτόκολλο, το οποίο επιτρέπει σε μια ροή byte που προέρχεται από μια μηχανή να παραδίδεται χωρίς σφάλματα σε οποιαδήποτε άλλη μηχανή στο διαδίκτυο. Το πρωτόκολλο τεμαχίζει την εισερχόμενη ροή byte σε διακριτά μηνύματα και μεταβιβάζει το καθένα από αυτά στο επίπεδο διαδικτύου. Στον προορισμό, η διεργασία-παραλήπτης του TCP ανασυναρμολογεί τα μηνύματα που λαμβάνει σε μία ροή εξόδου. Το TCP χειρίζεται επίσης και τον έλεγχο ροής, εξασφαλίζοντας ότι ένας γρήγορος αποστολέας δεν θα μπορεί να κατακλύσει έναν αργό παραλήπτη με περισσότερα μηνύματα από όσα μπορεί αυτός να χειριστεί. Το δεύτερο πρωτόκολλο, αυτό των αυτοδύναμων πακέτων χρήστη ή UDP είναι ένα αναξιόπιστο πρωτόκολλο το οποίο προορίζεται για εφαρμογές που δεν χρειάζονται την παράδοση των πακέτων με τη σωστή σειρά ή τον έλεγχο ροής του TCP, αφού επιθυμούν να παρέχουν δικούς τους μηχανισμούς. Χρησιμοποιείται για μεμονωμένα μηνύματα τύπου αίτησης-απάντησης στο μοντέλο client-server, καθώς και για εφαρμογές όπου η γρήγορη παράδοση είναι πιο σημαντική από την ακριβή παράδοση, όπως η μετάδοση video.

1.2.3 Το επίπεδο εφαρμογών

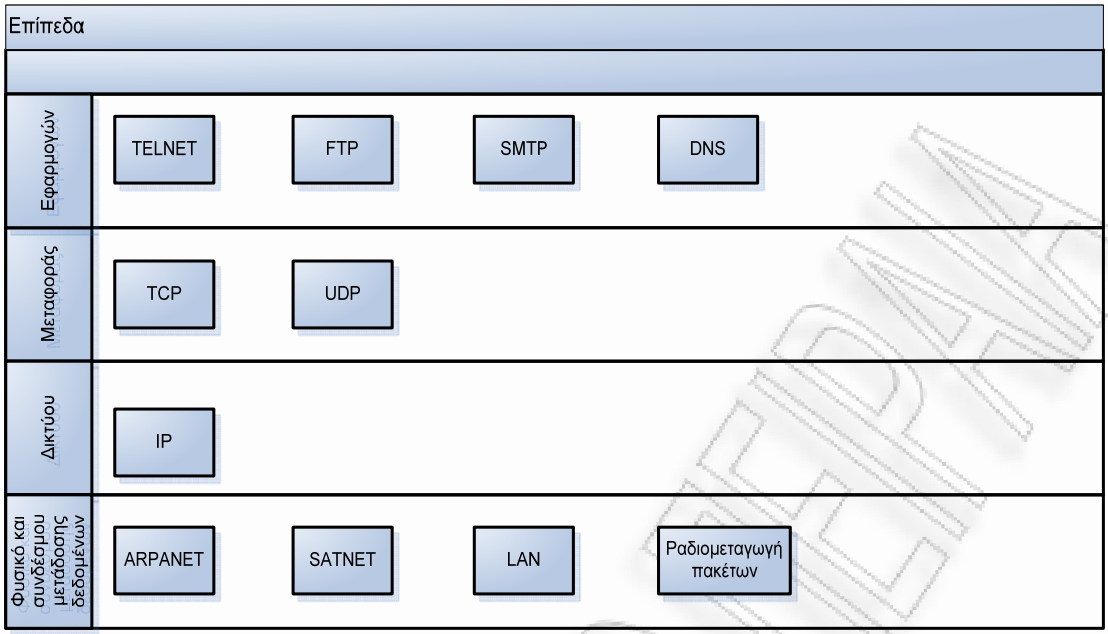
Περιέχει όλα τα πρωτόκολλα ανώτερου επιπέδου. Στην αρχή σε αυτά περιλαμβάνονταν το TELNET, το FTP και το ηλεκτρονικό ταχυδρομείο.

Το πρωτόκολλο TELNET επιτρέπει στους χρήστες μιας μηχανής να συνδέονται και να δουλεύουν σε μια μακρινή μηχανή. Το πρωτόκολλο FTP παρέχει έναν τρόπο αποτελεσματικής μεταφοράς δεδομένων από μηχανή σε μηχανή. Το ηλεκτρονικό ταχυδρομείο αρχικά ήταν απλώς ένα είδος μεταφοράς αρχείων. Αργότερα, αναπτύχθηκε ένα εξειδικευμένο πρωτόκολλο (SMTP) για αυτό. Άλλα πρωτόκολλα που αναπτύχθηκαν είναι τα DNS, NNTP, USENET, HTTP.

1.2.4 Το επίπεδο διασύνδεσης μεταξύ υπολογιστή, υπηρεσίας και δικτύου

Κάτω από το επίπεδο δικτύου έχουμε ένα μεγάλο κενό. Το μοντέλο αναφοράς TCP/IP δε λέει πολλά για το τι συμβαίνει εκεί, αλλά απλώς παρατηρεί ότι ο υπολογιστής υπηρεσίας πρέπει να συνδέεται με το δίκτυο χρησιμοποιώντας κάποιο πρωτόκολλο έτσι ώστε να μπορεί να στέλνει πακέτα IP. Το πρωτόκολλο αυτό δεν προσδιορίζεται, και διαφέρει από υπολογιστή σε υπολογιστή και από δίκτυο σε δίκτυο.

Το κάθε επίπεδο επικοινωνεί με το προηγούμενο και το επόμενό του και μπορεί να ανταλλάσσει δεδομένα. Στα δεδομένα, προκειμένου να μεταδοθούν από ένα επίπεδο προς ένα κατώτερο/ανώτερο, προστίθενται/αφαιρούνται κατάλληλες επικεφαλίδες (headers), μια λειτουργία που είναι γνωστή ως ενθυλάκωση (encapsulation). Η επικεφαλίδα IP περιέχει τη διεύθυνση δικτύου προορισμού και τις αιτήσεις υπηρεσιών ενώ η επικεφαλίδα TCP τη θύρα προορισμού, τον αριθμό ακολουθίας και το άθροισμα ελέγχου.



Σχήμα 2 : Πρωτόκολλα και δίκτυα στο αρχικό μοντέλο TCP/IP .

1.3 ΑΝΑΓΚΑΙΟΤΗΤΑ ΑΣΦΑΛΕΙΑΣ

Κατά τις πρώτες δεκαετίες της ύπαρξης τους, τα δίκτυα υπολογιστών χρησιμοποιούνταν κυρίως από τους πανεπιστημιακούς ερευνητές για αποστολή ηλεκτρονικού ταχυδρομείου και από υπάλληλους των εταιρειών για κοινή χρήση των εκτυπωτών. Υπό αυτές τις συνθήκες, δε δινόταν και πολλή σημασία στην ασφάλεια. Στη σημερινή εποχή, που εκατομμύρια άνθρωποι χρησιμοποιούν τα δίκτυα για τραπεζικές συναλλαγές, αγορές και υποβολή φορολογικών δηλώσεων, η ασφάλεια των δικτύων προβάλλει στον ορίζοντα ως ένα τεράστιο πρόβλημα. Τα περισσότερα προβλήματα ασφάλειας προκαλούνται σκόπιμα από κακόβουλα άτομα τα οποία προσπαθούν να αποκομίσουν κάποιο κέρδος, να προσελκύσουν την προσοχή, ή να βλάψουν κάποιον.

Είναι χαρακτηριστικά εύκολο να αποκτήσει κάποιος μια εξουσιοδοτημένη προσπέλαση σε ένα περιβάλλον με χαλαρή ασφάλεια και ταυτόχρονα να μην γίνει αντιληπτός. Ακόμα και αν χρήστες του δικτύου δεν έχουν κάτι χρήσιμο σε έναν υπολογιστή, αυτός μπορεί να γίνει η κεκρόπορτα για την εισβολή σε ένα δίκτυο. Οι επιπτώσεις μιας παραβίασης στην ασφάλεια μπορεί να είναι ο χαμένος χρόνος για την ανάκτηση της λειτουργικότητας των συστημάτων, η απώλεια χρημάτων και αξιοπιστίας, η αδυναμία συνέχισης της εργασίας, τα νομικά προβλήματα και σε εξαιρετικά σπάνιες περιπτώσεις ο κίνδυνος της ίδιας της ζωής. Γίνεται σαφές λοιπόν ότι η ανάπτυξη μηχανισμών παροχής ασφάλειας είναι μείζονος σημασίας για τη σωστή και δίκαιη λειτουργία των δικτύων οποιουδήποτε τύπου.

ΚΕΦΑΛΑΙΟ

<<ΑΠΑΙΤΗΣΕΙΣ ΑΣΦΑΛΕΙΑΣ ΚΑΙ ΕΠΙΘΕΣΕΙΣ>>

- **Πρότυπα Ασφάλειας**
- **Τρωτά Σημεία του Διαδικτύου**
- **Ειδή Επιθέσεων και Τεχνικές**

2 ΠΡΟΤΥΠΑ ΑΣΦΑΛΕΙΑΣ

Αυτό που παρατηρούμε στο πεδίο της ασφάλειας είναι κάποιοι καινούρια μέλη συν κάποια παλαιότερα που φαίνονται να τείνουν να επαναπροσδιορίσουν το ρόλο τους. Οι χρήστες δεν έχουν τον χρόνο και την ειδίκευση να μελετήσουν όλες τις γνωστές μεθόδους απόκρυψης για να επιλέξουν την πιο ασφαλή. Για αυτό έχουν δημιουργηθεί κάποια πρότυπα ασφάλειας (τα οποία είναι γνωστές ποσότητες). Η υιοθέτηση ενός προτύπου γίνεται αφού γίνουν κατανοητές οι αδυναμίες και τα πλεονεκτήματά του. Κάποιες ομάδες που δημιουργούν πρότυπα είναι οι παρακάτω:

The Clinton Administration

1) NIST
2) FTFSC
3) ANSI
4) NSA
5) IEEE
6) ISO
7) IAB
8) Ο χώρος των εταιριών
9) CSSPAB

Τα πρότυπα χωρίζονται στις εξής λειτουργικές κατηγορίες:

- **Η απόκρυψη (encryption)**:περικλείει το ανακάτεμα της πληροφορίας σε ψευδό-τυχαία μορφή έτσι ώστε μόνο κάποιος παραλήπτης με σωστό κλειδί να μπορεί να την αποκωδικοποιήσει.
- **Η πιστοποίηση (authentication)**:επιτυγχάνεται προσθέτοντας και μια “υπογραφή” στο τέλος του εγγράφου ή του αρχείου για τους εξής λόγους:

    1) Προκειμένου να αποδείξει ότι ο αποστολέας είναι πραγματικά ο δημιουργός.
    2) Απόδειξη ότι το αρχείο ή το έγγραφο δεν έχει αλλοιωθεί.
    3) Επιβεβαίωση ότι ο παραλήπτης είναι ο σκόπιμος παραλήπτης.
    4) Επιβεβαίωση ότι ο παραλήπτης πραγματικά πήρε το μήνυμα και συνεπώς δεν μπορεί να αρνηθεί την αποδοχή του.

- **Ο έλεγχος εκπομπών(emission control):**επιτυγχάνεται προασπίζοντας ή απομονώνοντας ηλεκτρομαγνητικές εκπομπές έτσι ώστε να μην παραληφθούν από μη σκόπιμους παραλήπτες. Αυτή η διεργασία καλείται TEMPEST.
- **Οι πολιτικές(policies) και οι διαδικασίες(procedures):**θα πρέπει να αναλυθούν λεπτομερώς σε πρότυπα που προάγουν την ασφάλεια (όπως μέγεθος και τρόποι αλλαγής των κωδικών πρόσβασης).
- **Ο σχεδιασμός έμπιστων συστημάτων (trusted systems):**εμπεριέχει τη δημιουργία υπολογιστικών συστημάτων και audit path και αποφέρει ένα τυπικά καθορισμένο επίπεδο ασφάλειας.

2.1 ΤΡΩΤΑ ΣΗΜΕΙΑ ΤΟΥ ΔΙΑΔΙΚΤΥΟΥ

Πολλά από τα πρωταρχικά δικτυακά πρωτόκολλα δε σχεδιάστηκαν έχοντας κατά νου την ασφάλεια. Χωρίς μια θεμελιώδη ασφαλή υποδομή, η άμυνα του δικτύου γίνεται πιο δύσκολη. Επιπλέον, το διαδίκτυο είναι ένα δυναμικό περιβάλλον, τόσο στην τοπολογία όσο και στην τεχνολογία.

Ο στόχος κατά το σχεδιασμό του IP ήταν η δημιουργία ενός πρωτοκόλλου που να διασυνδέει ετερογενή δίκτυα με τέτοιο τρόπο ώστε όλοι οι υπολογιστές να είναι μοναδικά προσδιορισμένοι, να μπορούν να ανταλλάσσουν δεδομένα με ένα κοινό format και τέλος να μεταδώσουν δεδομένα χωρίς να γνωρίζουν στοιχεία για τη δομή και τη μορφή των δικτύων που ανήκουν οι παραλήπτες και δεν τέθηκε θέμα ασφάλειας στο σχεδιασμό του IP. Λόγω της ραγδαίας εξάπλωσης του διαδικτύου το θέμα της ασφάλειας έπρεπε αναγκαστικά να αντιμετωπιστεί σε ένα υψηλότερο επίπεδο(επίπεδο μεταφοράς ,επίπεδο εφαρμογής).

Εξαιτίας του κληρονομούμενου ανοικτού περιβάλλοντος του διαδικτύου και του αρχικού σχεδιασμού των πρωτοκόλλων, οι επιθέσεις γενικά είναι γρήγορες, εύκολες ανέξοδες και σε πολλές περιπτώσεις δύσκολα ανιχνεύσιμες.

Μια άλλη μέθοδος ενίσχυσης της ασφάλειας που εμφανίστηκε τελευταία είναι αυτή της δημιουργίας ιδεατών ιδιωτικών δικτύων(VPNs).

Η βασική φιλοσοφία αυτών των μεθόδων είναι η κωδικοποίηση του πακέτου που πρόκειται να μεταδοθεί και κατόπιν η ενσωμάτωσή του σε ένα νέο πακέτο που αποστέλλεται στον προορισμό. Η μετατροπή δηλαδή του αρχικού IP πακέτου σε δεδομένα ενός άλλου IP πακέτου όπου τα πεδία που αφορούν τις διευθύνσεις αποστολέα και παραλήπτη είναι διαφορετικά από ότι στο αρχικό πακέτο (tunneling).

Παρά τις επιτυχημένες προσπάθειες σε όλες αυτές τις μεθόδους εξακολουθεί να υπάρχει ένα σοβαρό πρόβλημα. Αν χρησιμοποιείται ασφάλεια στο επίπεδο εφαρμογής τότε υπάρχει αρκετή πληροφορία που περιέχεται στην επικεφαλίδα του πακέτου στο οποίο ενσωματώνεται το κωδικοποιημένο πακέτο, που είναι ευάλωτο στις επιθέσεις.

Με χρήση προγραμμάτων ανάλυσης της δικτυακής κυκλοφορίας (sniffers) είναι δυνατόν να αποκαλυφθούν οι διεργασίες και τα συστήματα που ανταλλάσσουν πληροφορίες. Επίσης, το κόστος της υποστήριξης της ασφάλειας από κάθε εφαρμογή χωριστά στοιχίζει αρκετά σε σχέση με το να παρέρχονταν η ασφάλεια στο επίπεδο στο επίπεδο του δικτύου και κάθε εφαρμογή να έκανε χρήση αυτής.

Αν χρησιμοποιείται ασφάλεια στο επίπεδο μεταφοράς τότε αυτό σημαίνει ότι οι εφαρμογές που χρησιμοποιούν αυτή τη μέθοδο πρέπει να ξαναγραφτούν, ώστε τόσο ο εξυπηρετητής όσο και ο πελάτης να κάνουν χρήση αυτής της ασφάλειας.

Τέλος, η χρήση πρωτοκόλλων tunneling έχει μέτρια απόδοση και επιπλέον πάσχει από έλλειψη κάποιου προτύπου που θα μπορέσει να ακολουθηθεί.

Ένα άλλο τρωτό σημείο αποτελεί η ατεκμηρίωτη εμπιστοσύνη στο διαδίκτυο που δείχνουν αρκετοί οργανισμοί έχοντας άγνοια των κινδύνων που παραμονεύουν. Λαμβάνοντας υπόψη τις ταχύτατες αλλαγές στην τεχνολογία καθώς και τα εργαλεία που κατασκευάζουν οι εισβολείς, τα μέτρα που λαμβάνονται δεν ισχύουν μετά την πάροδο σύντομου χρονικού διαστήματος.

Εξαιτίας του ότι το μεγαλύτερο μέρος της κυκλοφορίας στο διαδίκτυο δεν είναι κρυπτογραφημένο, δεν είναι εφικτή η εμπιστευτικότητα και ακεραιότητα των πληροφοριών. Σαν αποτέλεσμα ένα site μπορεί να δεχθεί επιθέσεις από άλλο με χρήση εργαλείων, όπως ένας packet sniffer, που μπορεί να είναι εγκατεστημένος στο ένα και να μαζεύει πληροφορίες για το άλλο.

Η επιλογή του λειτουργικού συστήματος που εγκαθίσταται στον εξοπλισμό πρέπει να γίνεται με κριτήρια την ενίσχυση της ασφάλειας, και όχι με κριτήριο την ταχύτητα, τις επιδόσεις, την τιμή, την ευκολία χρήσης, τη διαχείριση και την υποστήριξη. Συνήθως η διαμόρφωση του λειτουργικού, όπως έρχεται από τον κατασκευαστή, δεν είναι κατάλληλη για τη διασφάλιση και ενίσχυση της ασφάλειας, δίνοντας τη δυνατότητα στους γνώστες να επιχειρήσουν επίθεση αμέσως μετά την πρώτη εγκατάσταση.

Οι τύποι τρωτών μπορούν να ταξινομηθούν στις εξής κατηγορίες:

1) Ελαττώματα στο λογισμικό ή στο σχεδιασμό των πρωτοκόλλων

Τα πρωτόκολλα είναι εκείνα που ορίζουν τους κανόνες και τις μεθόδους για να μπορούν οι υπολογιστές να επικοινωνούν μεταξύ τους στο δίκτυο. Αν το πρωτόκολλο έχει σχεδιαστικό λάθος είναι επισφαλές σε εκμετάλλευση του τρωτού σημείου ανεξάρτητα από το πόσο καλά υλοποιήθηκε. Ένα τέτοιο παράδειγμα είναι το NFS που επιτρέπει στα συστήματα να μοιράζουν αρχεία. Το πρωτόκολλο δεν περιλαμβάνει έναν τρόπο πιστοποίησης, έτσι ώστε ο χρήστης που συνδέεται δεν πιστοποιείται για το άν είναι αυτό που διατείνεται. Οι NFS Servers είναι στόχος για τους εισβολείς.

Όταν σχεδιάζεται το λογισμικό χωρίς η ασφάλεια να συμπεριλαμβάνεται στις αρχικές προδιαγραφές, υπάρχει το ενδεχόμενο το επιπλέον τμήμα που προστίθεται για την ενίσχυση της ασφάλειας, να μην αλληλεπιδρά όπως είχε αρχικά σχεδιαστεί και να προκύπτουν τρωτά σημεία.

Ακόμα το λογισμικό μπορεί να έχει τρωτά σημεία επειδή δε βρέθηκαν πριν την τελική έκδοση. Οι εισβολείς ψάχνουν και βρίσκουν αυτά τα ελαττώματα με δικά τους εργαλεία.

2) Αδυναμίες στη διαμόρφωση των συστημάτων και των δικτύων

Στην περίπτωση αυτή τα προβλήματα προέρχονται από τον τρόπο που τα πρωτόκολλα και το λογισμικό εγκαθίστανται και χρησιμοποιούνται. Τα προϊόντα παραδίδονται και συνήθως εγκαθίστανται με προκαθορισμένες παραμέτρους που οι εισβολείς μπορούν να εκμεταλλευτούν. Οι διαχειριστές συστημάτων και οι χρήστες μπορεί να μην αλλάξουν τις προκαθορισμένες παραμέτρους, με αποτέλεσμα το σύστημα να παρουσιάζει τρωτά.

Ένα παράδειγμα λανθασμένης διαμόρφωσης που συχνά εκμεταλλεύονται οι εισβολείς είναι η ανώνυμη χρήση της υπηρεσίας FTP. Οι οδηγίες για την ασφαλή διαμόρφωση αυτής της υπηρεσίας τονίζουν την ανάγκη το password file, τα βοηθητικά προγράμματα και τα αρχεία δεδομένων να βρίσκονται σε άλλη θέση στο σύστημα από το υπόλοιπο λειτουργικό σύστημα και αυτό να μην μπορεί να προσπελαστεί από το χώρο αποθήκευσης του FTP. Σε περίπτωση που τα sites δεν προσέξουν τη διαμόρφωση του FTP server τότε μη εξουσιοδοτημένοι χρήστες μπορούν να βρουν πληροφορίες πιστοποίησης και να τις εφαρμόσουν για να αποκτήσουν προσπέλαση.

2.2 ΕΙΔΗ ΕΠΙΘΕΣΕΩΝ ΚΑΙ ΤΕΧΝΙΚΕΣ

2.2.1 Επίθεση στις ιστοσελίδες

Τα sites με σελίδες του διαδικτύου είναι συχνά στόχος των hackers. Αυτό συμβαίνει επειδή δεν προσφέρουν κατά μέσο όρο ικανοποιητική ασφάλεια και τις σελίδες τους επισκέπτονται πολλοί άνθρωποι κάθε μέρα.

2.2.2 Επίθεση στην υπηρεσία ονοματολογίας (DNS)

Ένας άλλος τρόπος για να τροποποιηθούν οι ιστοσελίδες ενός site που βλέπουν οι χρήστες είναι να αλλάξει η IP διεύθυνση που υποτίθεται πως έχει από την υπηρεσία ονοματολογίας (DNS) ο κόμβος. Έτσι, θα μπορούσε κάποιος να αλλάξει τα στοιχεία της βάσης δεδομένων του DNS με αποτέλεσμα η νέα IP διεύθυνση του κόμβου να δείχνει σε ένα άλλου περιεχομένου site για την εξυπηρέτηση κάποιων συμφερόντων.

2.2.3 Επίθεση με Δούρειους Ίππους

Οι Δούρειοι Ίπποι (Trojan horses) είναι προγράμματα που προσποιούνται ότι έχουν άλλες λειτουργίες από αυτές που πραγματικά υλοποιούν. Συνήθως, κρύβονται σε άλλα προγράμματα, αλλά μπορούν να βρίσκονται και μεμονωμένα. Παράδειγμα Δούρειου Ίππου είναι ο Happy99.exe.

2.2.4 Επίθεση με “σκουλήκια”

Τα σκουλήκια (worms) είναι προγράμματα που δρουν αυτόνομα και “σέρνονται” από site σε site εκμεταλλευόμενοι τρύπες συστήματος. Σε κάθε site το σκουλήκι δρα αυτόματα και ανεξάρτητα από τα υπόλοιπα sites που προσπαθεί να “συρθεί”. Το πιο γνωστό σκουλήκι είναι το Internet Worm.

2.2.5 Επίθεση με ιούς

Οι ιοί (viruses) είναι τα γνωστά προγράμματα που προσπαθούν να εγκατασταθούν σε κάποιους υπολογιστές και να προσβάλουν την ακεραιότητα του συστήματος με διάφορους τρόπους (από τους πιο ανώδυνους αφήνοντας μια υπογραφή-ίχνος της παρουσίας τους ή πιο επώδυνους, με απώλεια δεδομένων, καταστροφή της διαμόρφωσης του συστήματος).

2.2.6 Επίθεση με “ανιχνευτές”

Οι ανιχνευτές (scanners) δικτυακής κίνησης είναι προγράμματα που χρησιμοποιούνται για τον έλεγχο της ασφάλειας συστημάτων. Ονομάζονται ανιχνευτές γιατί γνωρίζουν όλα τα πιθανά εξωτερικά σημεία που θα μπορούσε να εκμεταλλευτεί ένας επίδοξος hacker για να προσβάλει την ασφάλεια του συστήματος. Αν και αρχικά δημιουργήθηκαν για χρήση από τους διαχειριστές των συστημάτων, σύντομα έγιναν εργαλεία των hackers για να βρίσκουν πιθανούς στόχους. Τέτοια προγράμματα είναι το ISS, το Nmap και το SATAN.

2.2.7 Επίθεση στο πρωτόκολλο TFTP

Το πρωτόκολλο TFTP σχεδιάστηκε ως πρωτόκολλο για τη χωρίς δίσκο εκκίνησης πελατών (diskless client). Ωστόσο, δεν είχε δοθεί αρκετή προσοχή στην πρόσβαση σε συγκεκριμένους καταλόγους του συστήματος με αποτέλεσμα να μπορεί κανείς να αντιγράψει και άλλα αρχεία, το αρχείο κωδικών πρόσβασης.

2.2.8 Επίθεση στη δικτυακή υπηρεσία πληροφοριών (NIS)

Πρόκειται για την υλοποίηση της Sun Microsystems <<Κίτρινων Σελίδων>> για κατανεμημένη διαχείριση δικτυακών πληροφοριών (όπως αρχεία κωδικών πρόσβασης, χάρτες του δικτύου κτλ.). Ωστόσο, οι πληροφορίες αυτές περνούσαν πάνω από το δίκτυο και μπορούσε οποιοσδήποτε να τα παρακολουθήσει και να τα υποκλέψει. Το NIS αντικαταστάθηκε από το NIS+ το οποίο χρησιμοποιεί κρυπτογραφικές μεθόδους για τη μεταφορά ευαίσθητης πληροφορίας.

2.2.9 Επίθεση στο πρωτόκολλο μεταφοράς αρχείων (FTP)

Τα προβλήματα με το FTP μπορούν να συνδυαστούν με αυτά του TFTP, των αδύνατων κωδικών κτλ. Μέσω του FTP και μιας λανθασμένης διαμόρφωσης μπορεί κάποιος να υποκλέψει αρχεία του συστήματος.

2.2.10 Επίθεση στο σύστημα δικτυακής αρχειοθέτησης (NFS)

Το NFS αποτελεί πρωτοποριακή υλοποίηση από τη Sun Microsystems. Ωστόσο, με λάθος διαμόρφωση, μπορεί να μοιράσει ένα σύστημα αρχείων σε κακόβουλους χρήστες.

2.2.11 Επίθεση στο πρωτόκολλο ηλεκτρονικού ταχυδρομείου (SMTP)

Το πρωτόκολλο SMTP πρόκειται για το TCP/IP πρωτόκολλο επικοινωνίας των MTA της υπηρεσίας του ηλεκτρονικού ταχυδρομείου. Το κυριότερο πρόγραμμα που χρησιμοποιείται και αποτελεί πηγή του προβλήματος είναι το send mail.

2.2.12 Επίθεση στο ηλεκτρονικό ταχυδρομείο

Στην κατηγορία αυτή εμπίπτουν προβλήματα που προκύπτουν από την προβληματική χρήση του SMTP. Τέτοια είναι το mail spoofing, mail bombs, bin mail, mail race, mail abuse. Μια πρόσφατη τρωτότητα είναι και το spamming.

2.2.13 Επίθεση με <<έμπιστους υπολογιστές>>

Η υπηρεσία των έμπιστων υπολογιστών (trusted hosts) δημιουργήθηκε αρχικά για την ευκολία των χρηστών που είχαν πολλούς λογαριασμούς σε συστήματα και χρειάζονταν άμεση πρόσβαση χωρίς την καθυστέρηση για ταυτοποίηση μέσω κωδικών πρόσβασης. Το πρόβλημα αυτό παρουσιάζεται σε UNIX συστήματα στα αρχεία hosts.equiv και .rhosts.

2.2.14 Επίθεση μέσω διαμόρφωσης (weak configuration)

Επιθέσεις που έχουν καταγραφεί σε αυτήν την κατηγορία οφείλονται σε λάθη και παραλείψεις στη διαμόρφωση του συστήματος και κυρίως στη δικτυακή διαμόρφωση. Σε αυτές τις περιπτώσεις παραμένουν τα αρχικά passwords που δημιουργούνται κατά την εγκατάσταση ενός λογισμικού ή συστήματος και ο διαχειριστής δεν τα αλλάζει. Επίσης, μπορεί να παραμείνουν τα αρχικά δικαιώματα προσπέλασης που δεν είναι κατά ανάγκη ασφαλή.

2.2.15 Επίθεση από εύρεση των κωδικών πρόσβασης

Η τρωτότητα των κωδικών πρόσβασης είναι η πιο συχνή μορφή παραβίασης της πρόσβασης. Η εύρεση του κωδικού πρόσβασης ενός χρήστη μπορεί να γίνει με τους εξής τρόπους:

1. Αντιγραφή του αρχείου κωδικών και μετέπειτα επεξεργασία αυτού.
2. Σπάσιμο κωδικών πρόσβασης με χρήση προγραμμάτων που προσπαθούν να μαντέψουν passwords κωδικοποιώντας συνήθεις λέξεις.
3. Αδύνατοι κωδικοί που μπορεί εύκολα να βρει κανείς γνωρίζοντας το πρόσωπο στο οποίο ανήκει ο λογαριασμός.

2.2.16 Επίθεση με “ωτακουστές”

Οι ωτακουστές πακέτων είναι προγράμματα που μπορούν να παρακολουθούν (sniff) την κίνηση του δικτύου σε επίπεδο IP πακέτων. Με κατάλληλες τεχνικές, έχουν τη δυνατότητα να ανακατασκευάσουνε τα μηνύματα και να κάνουν αναγνώριση των πρωτοκόλλων που παίρνουν από το δίκτυο. Οι sniffers τρέχουν συνήθως σε τοπικά δίκτυα και κλέβουν

κωδικούς πρόσβασης ή παρακολουθούν τις πληκτρολογήσεις από συγκεκριμένους σταθμούς εργασίας. Με κατάλληλους μηχανισμούς ανασυνθέτουν τα πακέτα που μπορεί να έχουν χρήσιμη πληροφορία χωρίς όμως να επηρεάζουν το περιεχόμενό τους. Ο τρόπος επίθεσης με αυτούς δείχνει μια κλιμάκωση στον τρόπο δράσης: Ξεκινά από απλή ανίχνευση του στόχου και αφού εντοπίσει παραλείψεις στην ασφάλεια, εισβάλλει, σβήνει τα ίχνη, αποδυναμώνει την άμυνα του συστήματος και εγκαθιστά Trojans για την εξάπλωσή του.

2.2.17 Επίθεση με πλαστογράφηση

Η τεχνική αυτή βασίζεται στη δυνατότητα την οποία μπορεί να έχει ένας κόμβος να ισχυρίζεται πως έχει την IP διεύθυνση ενός άλλου. Προκειμένου να αποκτήσουν πρόσβαση, οι εισβολείς δημιουργούν πακέτα με ψεύτικες IP διευθύνσεις. Αυτό εκμεταλλεύεται τις εφαρμογές που χρησιμοποιούν ταυτοποίηση που βασίζεται στην IP διεύθυνση του αποστολέα και μπορεί να οδηγήσει ακόμα και στην απόκτηση πρόσβασης διαχειριστή στο σύστημα στόχο.Οι επιθέσεις αυτές μπορούν να αποτραπούν από firewalls που ελέγχουν τις διευθύνσεις πριν μπουν στο τοπικό, έμπιστο δίκτυο. Οι επιθέσεις τύπου IP spoofing είναι γενικά δύσκολο να εντοπιστούν αφού η πρώτη εντύπωση είναι ότι η επίθεση από την πλαστή διεύθυνση. Η επαλήθευση συνήθως αργεί, επιτρέποντας στο hacker να δρα ανενόχλητος για κάποιο διάστημα. Η πιο επαρκής λύση είναι η χρήση δρομολογητών που έχουν κατάλληλα διαμορφωθεί ώστε να αποτρέπουν είσοδο πακέτων από το εξωτερικό interface με εσωτερικές διευθύνσεις του δικτύου του.

2.2.18 Επίθεση με “πειρατεία” IP σύνδεσης

Με αυτήν την επίθεση ένας hacker μπορεί να καταλάβει τη σύνδεση ενός χρήστη με έναν εξυπηρετητή και να εκτελεί εντολές που έχει δικαίωμα ο χρήστης. Επιπλέον, μπορεί να βλέπει τι γράφει ο χρήστης. Αρχική αντιμετώπιση: Με τη δημιουργία κωδικοποιημένης σύνδεσης του χρήστη με τον εξυπηρετητή, μπορούμε να εμποδίσουμε το διάβασμα των στοιχείων, δεδομένων ή εντολών καθώς και τη χρήση της σύνδεσης από τον hacker που μη έχοντας το κλειδί κρυπτογράφησης βλέπει μόνο σκουπίδια.

2.2.19 Επίθεση με παραποίηση IP διεύθυνσης

Βασίζεται στο IP spoofing, ενώ εκμεταλλεύεται και αδυναμίες της υλοποίησης των IP και ICMP πρωτοκόλλων σε δικτυακές συσκευές. Το smurf είναι ένα πρόγραμμα, το οποίο προσποιείται ότι στέλνει πακέτα από άσχετο αποστολέα. Τα πακέτα αυτά είναι του πρωτοκόλλου ICMP το οποίο και χρησιμοποιείται από βασικές λειτουργίες του δικτύου. Στέλνοντας ένα ping πακέτο στη διεύθυνση εκπομπής ενός δικτύου, ο αποστολέας δέχεται απάντηση από κάθε έναν από τους κόμβους που δέχτηκαν το ICMP ping πακέτο. Αν και το ping πακέτο δεν είναι μεγάλο σε μέγεθος, εντούτοις ο παράγοντας ενίσχυσης είναι ίσος με τον αριθμό των μηχανημάτων. Είναι προφανές ότι μερικές εκατοντάδες πακέτα ping μπορούν να κάνουν άχρηστο το δίκτυο, δημιουργώντας μια κατάσταση άρνησης εξυπηρέτησης.

2.2.20 Επίθεση με υπερχείλιση προσωρινής μνήμης

Μερικές φορές οι hackers εισβάλουν σε συστήματα χωρίς να χρειάζεται να κάνουν login σε αυτά. Αντίθετα χρησιμοποιούν ένα πρόγραμμα που ήδη υπάρχει στον υπολογιστή και τρέχει στο σύστημα και του δίνουν να εκτελέσει ένα κομμάτι εντολών. Για να το πετύχουν αυτό φτιάχνουν ένα μεγάλο τμήμα από χαρακτήρες που περιέχει τις εντολές που θέλουν να εκτελεστούν, και το εισάγουν σαν παράμετρο εισόδου στο πρόγραμμα. Κανονικά το πρόγραμμα δεν εκτελεί το κώδικα που περνά σαν παράμετρος. Αν όμως το μήκος του κειμένου της παραμέτρου είναι μεγαλύτερο από το μήκος που έχει δοθεί σαν buffer για το πέρασμα τις παραμέτρου τότε μέρος του περνά στον χώρο του εκτελέσιμου προγράμματος και εκτελείται (buffer overflow). Μάλιστα ο κώδικας εκτελείτε με ότι προνόμια έχει το πρόγραμμα που εκτελείται. Αν λοιπόν μια διεργασία του συστήματος τρέχει με προνόμια διαχειριστή και καταφέρει ο hacker να περάσει με παράμετρο τον κώδικα του, τότε θα μπορέσει να εκτελέσει εντολές που θα του δώσουν διάφορα προνόμια (root access).

2.2.21 Επίθεση μέσω άρνησης παροχής υπηρεσιών (DoS)

Οι επιθέσεις αυτού του τύπου είναι οι πιο μοχθηρές και πιο δύσκολο να αντιμετωπιστούν, γιατί είναι εύκολο να γίνουν δύσκολο(μερικές φορές αδύνατο) να εντοπισθούν και το χειρότερο να μπορείς να αρνηθείς την υπηρεσία στον επιτιθέμενο χωρίς να κάνεις το ίδιο στις γνήσιες αιτήσεις για την υπηρεσία, από κανονικούς χρήστες. Η μεθοδολογία της DoS είναι απλή αν σταλούν σε έναν εξυπηρετητή περισσότερες αιτήσεις από όσες μπορεί να εξυπηρετήσει τότε οι λειτουργίες που επιβάλουν οι αιτήσεις αυτές, δεσμεύουν πόρους του συστήματος με αποτέλεσμα, μετά από κάποιο σύντομο χρονικό διάστημα το σύστημα να μην είναι σε θέση να εξυπηρετήσει τους χρήστες και να μην μπορεί να παρέχει αρκετούς πόρους για την εκτέλεση των διεργασιών. Παράδειγμα αποτελεί το mail spam. Αρχική αντιμετώπιση: χρήση packet filtering για την αποτροπή IP spoofed πακέτων να εισέλθουν στο σύστημα. Το σύστημα δεν πρέπει να τρέχει στα όρια των δυνατοτήτων και να έχει εγκατεστημένα τα τελευταία security patches.

2.2.22 Επίθεση με “μοχθηρό” κωδικό

Πρόκειται για εντολές οι οποίες δείχνουν να ξεκινούν διαδικασίες χρηστών, αλλά στην πραγματικότητα προσπαθούν να μαζέψουν ή να εκμεταλλευτούν ευαίσθητα δεδομένα. Για παράδειγμα, στην κατηγορία αυτή μπορούν να ενταχθούν οι προσπάθειες για σύνδεση μέσω του προγράμματος login μέσω συνδέσεων http και telnet.

3

ΚΕΦΑΛΑΙΟ

<< Δικτυακές Επιθέσεις, Μέθοδοι Υλοποίησης Τους και Επιπτώσεις >>

- Επιθέσεις
- Ποιος είναι ο τυπικός στόχος-θύμα μίας επίθεσης
- Επιτιθέμενοι
- Ποια είναι τα Κίνητρα των Επιτιθέμενων

3 ΕΠΙΘΕΣΕΙΣ

Επίθεση είναι οποιαδήποτε προσπάθεια για παραβίαση τη εμπιστευτικότητας*, ακεραιότητας* ή *διαθεσιμότητας* ενός συστήματος ή ενός δικτύου. Επίσης είναι οποιαδήποτε μη εξουσιοδοτημένη ενέργεια που έχει σκοπό να εμποδίσει, να παρακάμψει ή να αχρηστεύσει τους *μηχανισμούς ασφάλειας* και *ελέγχου πρόσβασης* ενός συστήματος ή ενός δικτύου.

3.1 ΠΟΙΟΣ ΕΙΝΑΙ Ο ΤΥΠΙΚΟΣ ΣΤΟΧΟΣ-ΘΥΜΑ ΜΙΑΣ ΕΠΙΘΕΣΗΣ

Ο στόχος μίας επίθεσης ποικίλει ανάλογα με τις ικανότητες και τους σκοπούς του κάθε επιτιθέμενου, καθώς και τον βαθμό δυσκολίας της υλοποίησης της επίθεσης όσο αναφορά τα μέτρα ασφάλειας που πρέπει να αντιμετωπιστούν.

Παρόλα αυτά οι πιο συνήθεις στόχοι μίας επίθεσης μπορεί να είναι:

3.1.1 Μικρά Τοπικά Δίκτυα LAN's

Κυρίως γιατί χαρακτηρίζονται από ανεπαρκή μέτρα ασφάλειας, καθώς ξοδεύονται μικρά χρηματικά ποσά για την ασφάλειά τους. Επίσης οι διαχειριστές τους ενώ έχουν ευρεία γνώση για την LAN τεχνολογία και τους τρόπους δικτύωσης και διαχείρισης τέτοιων δικτύων, συνήθως έχουν περιορισμένη γνώση όσο αναφορά την διασύνδεση των δικτύων τους με το υπόλοιπο Internet και την λειτουργία των πρωτοκόλλων

του TCP/IP.

3.1.2 Πανεπιστήμια

Κυρίως γιατί αποτελούνται από έναν μεγάλο αριθμό από δικτυωμένα συστήματα, προσφέροντας αυξημένη επεξεργαστική ισχύ που μπορεί ο επιτιθέμενος να εκμεταλλευτεί. Επίσης ένα πανεπιστήμιο φιλοξενεί πολυάριθμους χρήστες με εξουσιοδοτημένους λογαριασμούς, οι οποίοι συνήθως είτε δεν ελέγχονται ικανοποιητικά για την δραστηριότητά

τους, είτε δεν έχουν επαρκή γνώση για τους κινδύνους που προκύπτουν από την λανθασμένη χρήση των συστημάτων και των υπηρεσιών που αυτά παρέχουν, με αποτέλεσμα να δημιουργούνται τρύπες ασφάλειας που μπορεί ο επιτιθέμενος να εκμεταλλευτεί.

3.1.3 Κυβερνητικά Sites ή διάφοροι μεγάλοι οργανισμοί

Τέτοιου είδους στόχοι αποτελούν πρόκληση για τους επιτιθέμενους, καθώς μία επιτυχής επίθεση θα μπορούσε να έχει ως αποτέλεσμα την συλλογή κρίσιμων και απόρρητων πληροφοριών που θα μπορούσε ο επιτιθέμενος να εκμεταλλευτεί με σκοπό το κέρδος. Τέτοιου είδους πληροφορίες θα μπορούσε να ήταν αριθμοί πιστωτικών καρτών από μία τράπεζα ή απόρρητα έγγραφα ενός κυβερνητικού οργανισμού. Η αποστολή του επιτιθέμενου σε αυτήν την περίπτωση είναι σαφώς πιο δύσκολη και θα έχει μεγαλύτερο ρίσκο, καθώς τέτοιου είδους οργανισμοί συνήθως χαρακτηρίζονται από πολύ ισχυρά μέτρα ασφάλειας που είναι δύσκολο να παραβιαστούν. Για αυτόν τον λόγω η επιτυχία μίας επίθεσης με έναν τέτοιο στόχο, θα συνέβαλε θετικά στο γόητρο και την φήμη του επιτιθέμενου.

3.1.4 Πότε συμβαίνει μια επίθεση

Μία επίθεση σε κάποιο δίκτυο ή σύστημα θα μπορεί να συμβεί οποιαδήποτε στιγμή αυτό είναι συνδεδεμένο στο Internet. Τα σημερινά δίκτυα συνήθως συνδέονται στο Internet 24 ώρες την ημέρα. Η καταλληλότερη ώρα για να γίνει μια επίθεση, εφόσον γίνεται από κάποιον απομακρυσμένο χρήστη, είναι αργά το βράδυ σε σχέση με την τοποθεσία το στόχου. Αυτό συμβαίνει για τους παρακάτω λόγους :

1. Την ημέρα οι υποψήφιοι επιτιθέμενοι έχουν συνήθως άλλες ασχολίες της καθημερινής του ζωής, όπως την δουλειά τους ή το σχολείο τους.

2. Αργά το βράδυ υπάρχει μικρότερη δικτυακή κίνηση στο υποψήφιο δίκτυο-στόχο, άρα μεγαλύτερη ταχύτητα μεταφοράς δεδομένων που μπορεί ο επιτιθέμενος να εκμεταλλευτεί προς όφελός του.

Το βράδυ δεν υπάρχουν χρήστες που χρησιμοποιούν τα συστήματα του δικτύου τα οποία θα στοχεύσει ο επιτιθέμενος, κάτι που του επιτρέπει να ενεργεί χωρίς η δραστηριότητα του να μπορεί να γίνει άμεσα αντιληπτή από κάποιον χρήστη που δουλεύει στο ίδιο μηχάνημα. Επίσης του δίνεται η δυνατότητα να χρησιμοποιεί όλη την επεξεργαστική ισχύ του συστήματος για να εκτελέσει τις ενέργειές του. Συνήθως αυτή την ώρα δεν υπάρχει κάποιος αρμόδιος υπεύθυνος στο επιτιθέμενο δίκτυο, ώστε να μπορέσει να ανιχνεύσει έγκαιρα την επίθεση και να αντιδράσει.

3.2 Επιτιθέμενοι

3.2.1 Ποιοι εξαπολύουν επιθέσεις

Οι επιθέσεις πραγματοποιούνται από άτομα που έχουν πρόσβαση στους στόχους τους μέσω του Internet, από εξουσιοδοτημένους χρήστες που προσπαθούν να αποκτήσουν περισσότερα δικαιώματα από αυτά που τους έχουν δοθεί και από εξουσιοδοτημένους χρήστες οι οποίοι εκμεταλλεύονται τα δικαιώματα που τους έχουν δοθεί με κακό σκοπό. Συνήθως αυτοί που πραγματοποιούν τις επιθέσεις είναι γνωστοί ως Hackers ή Crackers. Παρόλο που αυτοί ο όροι λανθασμένα χρησιμοποιούνται κατά κόρον για να χαρακτηριστούν οι κακόβουλοι χρήστες, υπάρχουν διάφορες απόψεις που διαφοροποιούν την σημασία των δύο όρων.

Η πιο κοινά αποδεκτή προσέγγιση για τον διαχωρισμό των δύο παραπάνω εννοιών είναι η παρακάτω:

Hackers θεωρούνται αυτοί που συνεχώς προσπαθούν να διευρύνουν την γνώση τους γύρω από τον τρόπο λειτουργίας, οπουδήποτε υπολογιστικού συστήματος, λειτουργικού συστήματος ή λογισμικού γενικότερα. Μέσα από εξαντλητική χρήση των παραπάνω και εξέταση των λειτουργιών τους σε βάθος, εντοπίζουν διάφορα ελαττώματα και ατέλειες που μπορεί αυτά να

έχουν, τις οποίες γνωστοποιούν στο ευρύ κοινό ώστε να διορθωθούν από τους αρμόδιους. Συνήθως οι Hackers έχουν ανεπτυγμένες προγραμματιστικές ικανότητες και ευρεία γνώση και ενθουσιασμό για αυτό που κάνουν.

Σημαντικό χαρακτηριστικό των Hackers είναι ότι διαχέουν την γνώση που προκύπτει από την δραστηριότητά τους και σε καμία περίπτωση με τις ενέργειές τους δεν προκαλούν θελημένα κάποια ζημιά σε άλλους.

Crackers είναι οι Hackers που χρησιμοποιούν τις ικανότητές τους με κακόβουλους σκοπούς. Παραβιάζουν συστήματα στα οποία δεν έχουν εξουσιοδοτημένη πρόσβαση και προκαλούν προβλήματα σε αυτά και στους νόμιμους χρήστες τους. Συνήθως οι Hackers είναι γνωστοί και σαν Whitehats ενώ οι Crackers σαν Blachats. Ένας άλλος όρος που επίσης χρησιμοποιείται για να χαρακτηρίσει μία ομάδα χρηστών, οι οποίοι λειτουργούν με κακόβουλες προθέσεις, είναι ο όρος Script Kiddies.

Script Kiddy είναι ο χρήστης που πραγματοποιεί επιθέσεις χρησιμοποιώντας έτοιμες, γνωστές τεχνικές και μεθόδους που έχουν ανακαλυφθεί και χρησιμοποιηθεί πρωτύτερα από άλλους. Οι ικανότητες ενός Script Kiddy είναι συνήθως κατώτερου επιπέδου από αυτές ενός μέτριου χρήστη ηλεκτρονικού υπολογιστή και στις περισσότερες των περιπτώσεων δεν έχει ιδιαίτερες γνώσεις για αυτό που κάνει. Για να πραγματοποιήσει τον στόχο του χρησιμοποιεί έτοιμα εργαλεία που αυτοματοποιούν την διαδικασία της επίθεσης, ελπίζοντας να κερδίσει το επιθυμητό αποτέλεσμα χωρίς να καταλαβαίνει τον τρόπο με τον οποίο αυτό συνέβη. Το μεγαλύτερο μέρος της ύποπτης δραστηριότητας που παρατηρείται στο Internet οφείλεται στον μεγάλο αριθμό των Script Kiddies που υπάρχουν, ενώ ο βαθμός κινδύνου

που προκύπτει από τις ενέργειές τους, είναι συνυφασμένος με την αυξημένη περιέργεια και τον ενθουσιασμό που τους διακρίνει, καθώς και από την επικινδυνότητα των εργαλείων που έχουν στην διάθεσή τους.

3.2.2 Το προφίλ του τυπικού επιτιθέμενου

Στη συνέχεια περιγράφονται τα χαρακτηριστικά που σχηματίζουν το προφίλ ενός τυπικού επιτιθέμενου. Σε αυτήν την περιγραφή στον όρο επιτιθέμενος δεν συμπεριλαμβάνονται οι Script Kiddies. Γνωρίζει να προγραμματίζει και να κατανοεί προγράμματα σε C ,C++ και Perl, κυρίως γιατί τα περισσότερα εργαλεία ασφάλειας είναι γραμμένα σε αυτές τις γλώσσες. Έχει αρκετή γνώση για το πώς δουλεύει το TCP/IP και γενικότερα το Internet. Χρησιμοποιεί το Internet πολλές ώρες τον μήνα και έχει πλήρη γνώση του συστήματός του. Γνωρίζει καλά την χρήση και τον τρόπο λειτουργίας τουλάχιστον δύο λειτουργικών συστημάτων, το ένα από τα οποία είναι το Unix ή τοVMS. Το είδος των λειτουργικών συστημάτων που συνήθως οι επιτιθέμενοι χρησιμοποιούν έχει να κάνει με το κόστος απόκτησής τους και τις δυνατότητες που τους προσφέρουν για να πραγματοποιήσουν τις ενέργειές τους. Μερικά από αυτά τα συστήματα μπορεί να είναι:

- **Macintosh** Δεν προσφέρει αρκετά εργαλεία.
- **SUN** (Solaris X86 ή SCO)βρίσκονται εύκολα και με μικρό κόστος ιδιαίτερα για τους μαθητές.
- **UNIX** Χρειάζονται λίγη RAM για να έχουν καλή απόδοση, ενώ προσφέρουν μία μεγάλη γκάμα από εργαλεία.
- **Microsoft** (Windows 9x και κυρίως Windows NT/2000)

Επίσης είναι χρήσιμο για τους επιτιθέμενους να γνωρίζουν τα NT/2000 καθώς χρησιμοποιούνται σε πολλά δίκτυα που θέλουν να επιτεθούν.

Οι πιο έμπειροι έχουν ή είχαν κάποια δουλειά σχετική με την διαχείριση υπολογιστικών συστημάτων και δικτύων ή την ανάπτυξη κώδικα για εφαρμογές. Συλλέγει παλιό hardware και software υλικό καθώς αυτό μπορεί να προσφέρει λειτουργίες που δεν προσφέρονται στα νεότερα

3.3 Ποια είναι τα Κίνητρα των Επιτιθέμενων

Οι λόγοι που οδηγούν κάποια άτομα να εκτελούν επιθέσεις βασίζονται σε κίνητρα που διαφέρουν για τον καθένα και έχουν να κάνουν τόσο με την προσωπικότητα του κάθε επιτιθέμενου, όσο και με το κέρδος που προκύπτει από αυτές τις ενέργειες. Οι πιο συνήθης λόγοι είναι οι παρακάτω.

3.3.1 Από κακία ή εκδίκηση

Σε αυτήν την περίπτωση ο επιτιθέμενος νιώθει μίσος για τον στόχο του και θέλει να προκαλέσει ζημιά σε αυτόν, συνήθως παίρνοντας με αυτόν τον τρόπο εκδίκηση για κάποιο γεγονός που συνέβη στο παρελθόν και για το οποίο νιώθει ότι αδικήθηκε. Ένα τέτοιο παράδειγμα θα μπορούσε να είναι ένας υπάλληλος μίας εταιρίας που απολύθηκε και θέλει να πάρει εκδίκηση.

3.3.2 Για το γόητρο

Διεισδύοντας σε υποτιθέμενα γνωστά καλά ασφαλισμένα δίκτυα, προσπαθούν να εντυπωσιάσουν τους ομοειδής τους και να διευρύνουν την φήμη τους. Κάτι τέτοιο θα μπορούσε να τους βοηθήσει και στην μετέπειτα επαγγελματική τους καριέρα.

3.2.3.3 Για το κέρδος

Υπάρχουν εταιρίες που στα πλαίσια του ανταγωνισμού με τους αντίπαλούς τους, προσλαμβάνουν επαγγελματίες crackers με σκοπό να εισβάλουν στα συστήματα του ανταγωνιστή και να κατασκοπεύσουν τα σχέδιά του, ή ακόμα και να του προκαλέσουν προβλήματα και καταστροφές.

3.3.4 Από περιέργεια ή χόμπι

Είναι αρκετοί που πραγματοποιούν τέτοιου είδους ενέργειες είτε γιατί δεν έχουν κάτι καλύτερο να κάνουν και θέλουν να ξεφύγουν από την ανία τους, είτε γιατί διακατέχονται από αυξημένη περιέργεια και τους αρέσει να ψάχνουν τα ξένα πράγματα. Τέτοιου είδους άτομα, συνήθως δεν γνωρίζουν αρκετά για αυτό που κάνουν και αγνοούν τους κινδύνους που προκύπτουν από αυτήν την δραστηριότητά τους καθώς θεωρείται παράνομη και μπορεί να οδηγήσει στην νομική δίωξή τους.

3.3.5 Για πολιτικούς λόγους

Τέτοιου είδους δραστηριότητα έχει στόχο κυρίως κυβερνητικούς οργανισμούς, και έχει να κάνει με ιδεολογικά κίνητρα, που οδηγούν σε εκδηλώσεις διαμαρτυρίας ή σε ενέργειες κατασκοπίας και τρομοκρατίας.

3.4 Πως λειτουργούν οι επιτιθέμενοι

Οι περισσότεροι επιτιθέμενοι ανήκουν στην κατηγορία των Script Kiddies, οι οποίοι ανταλλάζουν πληροφορίες μεταξύ τους μέσω του διαδικτύου και παίρνουν την γνώση τους από άλλους που έχουν ενεργήσει πριν από αυτούς. Επίσης χρησιμοποιούν έτοιμα εργαλεία και τεχνικές που άλλοι έχουν επινοήσει και εφαρμόσει στο παρελθόν.

Τέτοιου είδους επιτιθέμενοι συνήθως αντιμετωπίζονται με μεγαλύτερη ευκολία, καθώς οι μέθοδοι και τα εργαλεία που χρησιμοποιούν είναι γενικότερα γνωστά και στους υπεύθυνους ασφάλειας των περισσοτέρων δικτύων. Παρόλα αυτά όμως υπάρχουν και crackers που φτιάχνουν δικά τους εργαλεία και χρησιμοποιούν δικές τους μεθόδους ή χρησιμοποιούν συνδυασμούς μεθόδων κάνοντας έτσι δυσκολότερη την ανίχνευση τους.

Συνήθως οι σοβαροί Crackes κάνουν διάφορες προσποιητές επιθέσεις πριν εξαπολύσουν την κύρια επίθεσή τους, με σκοπό να εντοπίσουν πως ανταποκρίνονται τα διάφορα μέτρα ασφάλειας του δικτύου που σχεδιάζουν να επιτεθούν. Επίσης εκτελούν πολλαπλό scanning (ενέργειες με τις οποίες ψάχνουν για ανοιχτές πόρτες και αδυναμίες σε ένα σύστημα) από διάφορες ψεύτικες IP διευθύνσεις, σε διαφορετικές χρονικές στιγμές, έτσι ώστε να μην γίνονται εύκολα αντιληπτοί.

4

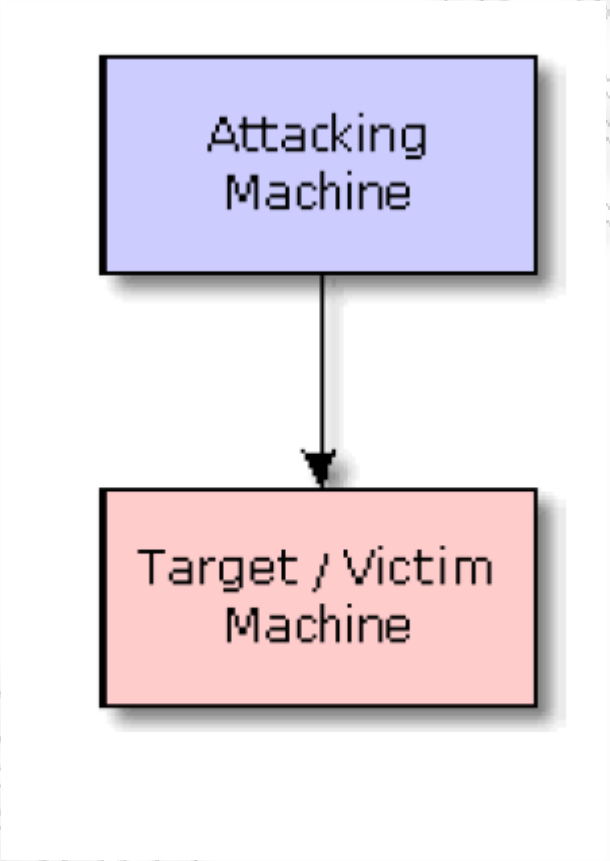
ΚΕΦΑΛΑΙΟ

<< Περιγραφή επίθεσης DDoS>>

- **Εισαγωγή**
- **Εξαπόλυση μιας επίθεσης DDoS ενάντια στον υπολογιστή ενός θύματος**
- **Στρατολόγηση τρωτών μηχανών**
- **Διάδοση Κακόβουλου κώδικα**

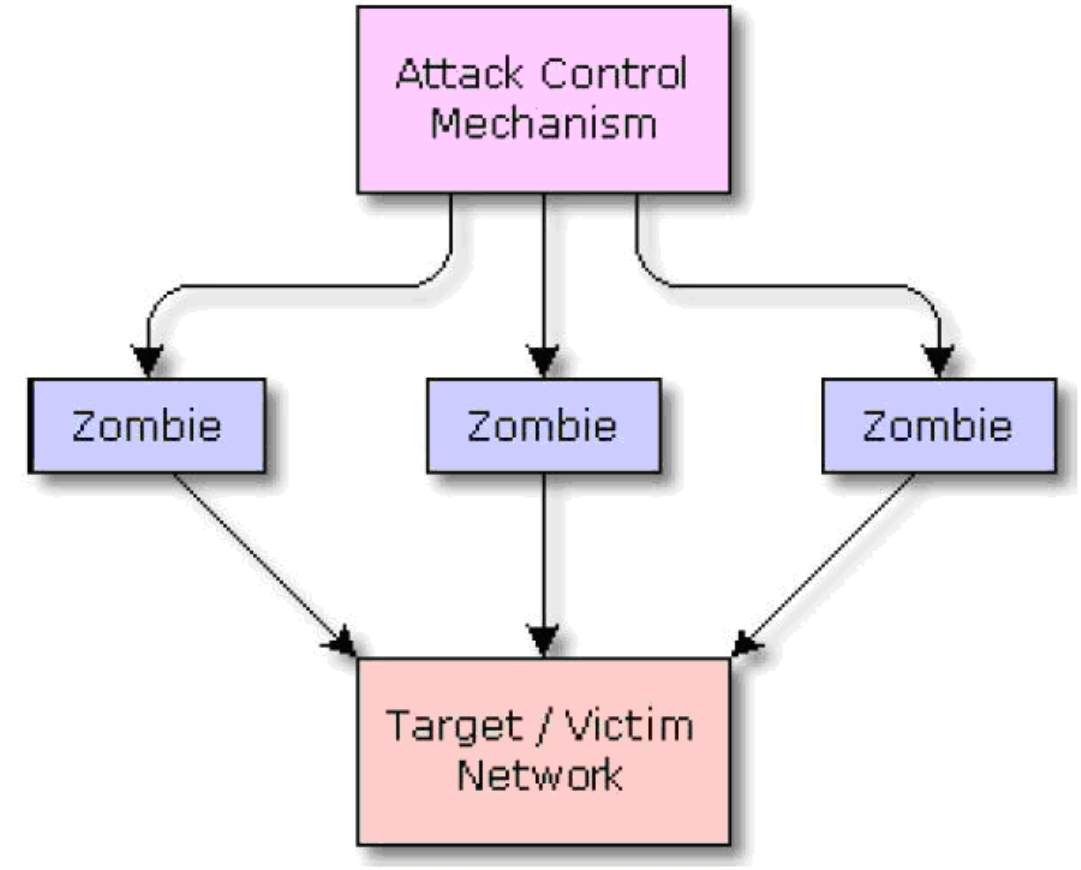
4 ΕΙΣΑΓΩΓΗ

Το Internet αποτελείται από εκατομμύρια υπολογιστών που βρίσκονται διάσπαρτη σε ολόκληρο τον κόσμο. Εκατομμύρια άνθρωποι χρησιμοποιούν το Διαδίκτυο καθημερινά και εκμεταλλεύονται πλήρως τις διαθέσιμες υπηρεσίες και σε προσωπικό και σε επαγγελματικό επίπεδο. Παρόλα αυτά, η υψηλή συνδεσιμότητα μεταξύ των υπολογιστών, στους οποίους το World Wide Web στηρίζεται, μετατρέπει τους κόμβους του Διαδικτύου σε έναν εύκολο στόχο για τους κακόβουλους χρήστες που προσπαθούν να εξαντλήσουν τους πόρους του εξαπολύοντας DoS επιθέσεις.



Σχήμα 3 : Επίθεση DOS

Μια denial-of-service (DoS) επίθεση είναι μια κακόβουλη προσπάθεια από ένα μεμονωμένο πρόσωπο ή μια ομάδα ανθρώπων να αναγκάσει το site ή τον κόμβο του θύματος να αρνηθεί υπηρεσία στους πελάτες του. Όταν αυτή η προσπάθεια προέρχεται από ένα συγκεκριμένο host του δικτύου, συνιστά μια DoS επίθεση (Σχήμα 3). Από την άλλη πλευρά, είναι επίσης δυνατό πολλοί κακόβουλοι hosts να συντονίζονται για να πλημμυρίσουν το θύμα με μια αφθονία πακέτων επίθεσης έτσι ώστε η επίθεση να πραγματοποιείται ταυτόχρονα από πολλά σημεία. Σε αυτήν την περίπτωση πρόκειται για μια κατανεμημένη επίθεση άρνησης υπηρεσίας (DDoS-Distributed Denial of Service Attack) (Σχήμα 4).



Σχήμα 4 : Επίθεση DDOS

4.1 Εξαπολυση μιας επιθεσης DDoS εναντια στον υπολογιστη ενος θυματος

Οι επιθέσεις Denial of service προσπαθούν να εξαντλήσουν τους πόρους του θύματος. Αυτοί οι πόροι μπορεί να είναι το εύρος ζώνης του δικτύου, υπολογιστική ισχύς ή δομές δεδομένων λειτουργικών συστημάτων. Για να εξαπολύσει μια επίθεση DDoS, ένας κακόβουλος χρήστης χτίζει αρχικά ένα δίκτυο υπολογιστών τους οποίους θα χρησιμοποιήσει για να παραγάγει τον όγκο της κίνησης που απαιτείται για να προκαλέσει την άρνηση των υπηρεσιών στους χρήστες υπολογιστών. Για να δημιουργήσουν αυτό το δίκτυο επίθεσης, οι επιτιθέμενοι ανακαλύπτουν τρωτά sites ή τρωτούς hosts που είναι διασυνδεμένοι με το δίκτυο. Τέτοιου είδους hosts είναι συνήθως εκείνοι που τρέχουν out-of-date anti-virus ή μη επιδιορθωμένο software. Οι τρωτοί αυτοί hosts *χρησιμοποιούνται* από τον επιτιθέμενο, που χρησιμοποιεί το ελάττωμά τους για να αποκτήσει πρόσβαση σε αυτούς. Το επόμενο βήμα

για τον εισβολέα είναι να εγκαταστήσει νέα προγράμματα (γνωστά ως εργαλεία επίθεσης) στους εκτεθειμένους hosts του δικτύου επίθεσης. Οι hosts που τρέχουν αυτά τα εργαλεία επίθεσης είναι γνωστοί ως "zombies" και μπορούν να πραγματοποιήσουν οποιαδήποτε επίθεση κάτω από τον έλεγχο του επιτιθέμενου.

Αλλά πώς μπορεί ένας επιτιθέμενος να ανακαλύψει τους hosts που θα αποτελέσουν το δίκτυο επίθεσης και πώς μπορεί αυτός να εγκαταστήσει τα εργαλεία επίθεσης σε αυτούς; Αν και αυτό το προπαρασκευαστικό στάδιο της επίθεσης είναι πολύ κρίσιμο, η ανακάλυψη τρωτών hosts και η εγκατάσταση των εργαλείων επίθεσης σε αυτούς έχουν γίνει μια πολύ εύκολη διαδικασία. Δεν υπάρχει καμία ανάγκη για τον εισβολέα να ξοδέψει χρόνο στη δημιουργία των εργαλείων επίθεσης δεδομένου ότι υπάρχουν ήδη έτοιμα προγράμματα τα οποία βρίσκουν αυτόματα τα τρωτά συστήματα, εισβάλουν σε αυτά και εγκαθιστούν τα απαραίτητα προγράμματα για την επίθεση. Μετά από αυτό, τα συστήματα που έχουν μολυνθεί από τον κακόβουλο κώδικα ψάχνουν άλλους τρωτούς υπολογιστές και εγκαθιστούν σε αυτούς τον ίδιο κακόβουλο κώδικα. Λόγω αυτής της ταχύτατης σάρωσης για τον προσδιορισμό θυμάτων, είναι δυνατό μεγάλα δίκτυα επίθεσης να μπορούν να κατασκευαστούν πολύ γρήγορα. Το αποτέλεσμα αυτής της αυτοματοποιημένης διαδικασίας είναι η δημιουργία ενός δικτύου επίθεσης DDoS που αποτελείται από τις μηχανές των handlers (κύριοι) και των agents (σκλάβοι, δαίμονες). Μπορεί να προκύψει από την προαναφερθείσα διαδικασία ότι κατά τη διάρκεια της οικοδόμησης του δικτύου επίθεσης, μια άλλη επίθεση DDoS πραγματοποιείται, δεδομένου ότι η ίδια η διαδικασία της οργάνωσης δικτύων επίθεσης δημιουργεί ένα σημαντικό ποσό κίνησης.

4.2 ΣΤΡΑΤΟΛΟΓΗΣΗ ΤΡΩΤΩΝ ΜΗΧΑΝΩΝ

Υπάρχουν διαφόρων ειδών τεχνικές (γνωστές ως τεχνικές σάρωσης) τις οποίες μπορεί ο επιτιθέμενος να χρησιμοποιήσει προκειμένου να βρει τις τρωτές μηχανές. Οι σημαντικότερες από αυτές παρουσιάζονται παρακάτω:

Τυχαία σάρωση: Σύμφωνα με αυτήν την τεχνική, το μηχάνημα που έχει μολυνθεί από τον κακόβουλο κώδικα (τέτοιο μηχάνημα μπορεί να είναι είτε ο επιτιθέμενος είτε ένα μέλος του στρατού του όπως ένα zombie) δοκιμάζει τυχαία διευθύνσεις IP από το χώρο διευθύνσεων IP και ελέγχει εάν τα μηχανήματα που αντιστοιχούν σε αυτές είναι τρωτά. Μόλις βρει μία τρωτή μηχανή, εισβάλει σε αυτήν και προσπαθεί να την μολύνει, εγκαθιστώντας σε αυτήν τον ίδιο κακόβουλο κώδικα με αυτόν που είναι εγκατεστημένος στο ίδιο. Η τεχνική αυτή δημιουργεί σημαντική κίνηση, αφού εξαιτίας της τυχαίας αυτής σάρωσης, ένας μεγάλος αριθμός εκτεθειμένων host δοκιμάζει και ελέγχει τις ίδιες IP διευθύνσεις. Ένα πλεονέκτημα αυτής της τεχνικής σάρωσης είναι ότι η εξάπλωση του κακόβουλου κώδικα μπορεί να είναι πολύ γρήγορη εξαιτίας του γεγονότος ότι οι σαρώσεις φαίνεται να προέρχονται από παντού. Παρόλα αυτά, ο γρήγορος ρυθμός με τον οποίο ο κακόβουλος κώδικας εξαπλώνεται δεν μπορεί να διαρκέσει για πάντα. Μετά από μια μικρή χρονική περίοδο, ο ρυθμός εξάπλωσης μειώνεται εξαιτίας του γεγονότος ότι και ο αριθμός των νέων IP διευθύνσεων που μπορούν να ανακαλυφθούν μειώνεται με το

πέρασμα του χρόνου. Αυτό γίνεται προφανές λαμβάνοντας υπόψη την ανάλυση του David Moore και του Colleen Shannon πάνω στην εξάπλωση του Code-Red (CRv2) Worm, το οποίο χρησιμοποιεί τυχαία σάρωση προκειμένου να διαδοθεί.

Hit list σάρωση: Πολύ πριν ο επιτιθέμενος αρχίσει την σάρωση, συγκεντρώνει σε μια λίστα έναν μεγάλο αριθμό πιθανών τρωτών μηχανημάτων. Στην προσπάθειά του να δημιουργήσει το στρατό του, αρχίζει να σαρώνει τη λίστα προκειμένου να βρει τρωτά μηχανήματα. Μόλις ανακαλύψει ένα, εγκαθιστά σε αυτό τον κακόβουλο κώδικα και διαιρεί τη λίστα στα δύο. Κατόπιν, δίνει το δεύτερο μισό στο μηχάνημα που μόλις έχει εκτεθεί στον κακόβουλο κώδικα, κρατά το άλλο μισό και συνεχίζει τη σάρωση της υπόλοιπης λίστας. Ο πρόσφατα μολυσμένος host αρχίζει τη σάρωση της λίστας που του αντιστοιχεί, προσπαθώντας και αυτός με τη σειρά του να βρει ένα τρωτό μηχάνημα. Όταν βρει κάποιο, εφαρμόζει την ίδια διαδικασία που περιγράφηκε παραπάνω, και με αυτόν τον τρόπο η hit list σάρωση πραγματοποιείται ταυτόχρονα από έναν συνεχώς αυξανόμενο αριθμό εκτεθειμένων μηχανών. Ο μηχανισμός αυτός εγγυάται την εγκατάσταση του κακόβουλου κώδικα σε όλες τις τρωτές μηχανές που περιλαμβάνονται στην hit list και μάλιστα μέσα σε μια μικρή χρονική περίοδο. Επιπρόσθετα, ο hit list κατάλογος τον οποίο κατέχει ένας πρόσφατα μολυσμένος host μειώνεται συνεχώς εξαιτίας της διαίρεσης του καταλόγου για την οποία έγινε λόγος παραπάνω. Ένα πρόσθετο πλεονέκτημα αυτού του τύπου της σάρωσης είναι ότι καμία σύγκρουση δεν εμφανίζεται κατά τη διάρκεια της σάρωσης από τη στιγμή που δεν είναι δυνατόν κάποιο από τα εκτεθειμένα μηχανήματα που ψάχνουν για τρωτούς υπολογιστές να εξετάζει ταυτόχρονα με κάποιο δεύτερο τον ίδιο υπολογιστή.

Όπως έχει ήδη αναφερθεί, η κατασκευή του hit list καταλόγου διεξάγεται αρκετό καιρό πριν από την έναρξη της σάρωσης από τον επιτιθέμενο. Για το λόγω αυτό, ο επιτιθέμενος έχει τη δυνατότητα να δημιουργήσει τον κατάλογο με πολύ αργούς ρυθμούς και για ένα αρκετά μεγάλο χρονικό διάστημα. Εάν ο επιτιθέμενος διεξάγει μια σάρωση με εξαιρετικά αργούς ρυθμούς, τότε είναι πιθανό αυτή η κακόβουλη δραστηριότητά του να μην παρατηρηθεί. Αυτό συμβαίνει γιατί μια διαδικασία σάρωσης που έχει ως σκοπό τη δημιουργία στρατού επίθεσης, πραγματοποιείται σε ένα δίκτυο συνήθως σε εξαιρετικά υψηλές ταχύτητες και ως εκ τούτου, μια σάρωση με πολύ αργούς ρυθμούς είναι δυνατόν να περάσει απαρατήρητη χωρίς κανένας να καταλάβει ότι πρόκειται για μια κακόβουλη σάρωση. Στο σημείο αυτό πρέπει επίσης να αναφερθεί ότι υπάρχουν δημόσιοι servers όπως η Net craft Survey , οι οποίοι είναι σε θέση να δημιουργήσουν τέτοιου είδους hit list καταλόγους χωρίς να υπάρχει ανάγκη σάρωσης.

Σάρωση τοπολογίας: Η τεχνική αυτή σάρωσης χρησιμοποιεί πληροφορίες που βρίσκονται αποθηκευμένες στον υπολογιστή του θύματος προκειμένου να βρει νέους στόχους. Σύμφωνα με αυτή την τεχνική, ένας ήδη εκτεθειμένος host εξετάζει το σκληρό δίσκο του μηχανήματος που πρόκειται να μολύνει για URLs. Κατόπιν, καθιστά αυτές τις URLs στόχους και ελέγχει εάν είναι τρωτές. Το γεγονός ότι αυτές οι URLs είναι έγκυροι web servers σημαίνει ότι ο εκτεθειμένος host σαρώνει πιθανούς στόχους αμέσως από την αρχή της

φάσης σάρωσης. Για το λόγο αυτό, η ακρίβεια της τεχνικής αυτής είναι εξαιρετικά καλή και η απόδοσή της φαίνεται να προσεγγίζει εκείνη της «hitlist σάρωσης». Ως εκ τούτου, η σάρωση τοπολογίας είναι ικανή να δημιουργήσει ένα μεγάλο στρατό από επιτιθέμενους εξαιρετικά γρήγορα και επιταχύνει με αυτό τον τρόπο την εξάπλωση του κακόβουλου κώδικα.

Σάρωση τοπικού δικτύου: Αυτό το είδος σάρωσης δρα πίσω από μια αντιπυρική ζώνη (firewall) σε μια περιοχή η οποία έχει μολυνθεί από το κακόβουλο πρόγραμμα σάρωσης. Ο εκτεθειμένος host ψάχνει τους στόχους του στο τοπικό του δίκτυο, χρησιμοποιώντας την πληροφορία που είναι κρυμμένη στις "τοπικές" (local) διευθύνσεις. Πιο συγκεκριμένα, ένα αντίγραφο του προγράμματος σάρωσης τρέχει πίσω από μια αντιπυρική ζώνη (firewall) και προσπαθεί να εισβάλει σε όλες τις τρωτές μηχανές οι οποίες σε αντίθετη περίπτωση θα προστατεύονταν από την συγκεκριμένη αντιπυρική ζώνη (firewall). Αυτός ο μηχανισμός μπορεί να χρησιμοποιηθεί σε συνδυασμό με άλλους μηχανισμούς σάρωσης: Για παράδειγμα, ένας εκτεθειμένος host μπορεί να αρχίσει τη διαδικασία ανίχνευσης τρωτών μηχανών με την σάρωση του τοπικού του δικτύου, ψάχνοντας για τρωτές μηχανές στο τοπικό του δίκτυο. Μόλις εξετάσει όλες τις τοπικές μηχανές, μπορεί να συνεχίσει την διαδικασία σάρωσης μεταπηδώντας σε έναν άλλο μηχανισμό σάρωσης προκειμένου να σαρωθούν μηχανές που βρίσκονται εκτός τοπικού δικτύου. Με αυτόν τον τρόπο, μπορεί να κατασκευαστεί ένας πολυάριθμος στρατός zombies με μια εξαιρετικά υψηλή ταχύτητα.

Σάρωση αντιμετάθεσης: Σύμφωνα με αυτόν τον μηχανισμό σάρωσης όλα τα μηχανήματα μοιράζονται έναν κοινό κατάλογο ψευδοτυχαίων IP διευθύνσεων που έχουν υποστεί αντιμετάθεση. Ένας τέτοιου είδους κατάλογος ονομάζεται κατάλογος αντιμετάθεσης. Ο κατάλογος αντιμετάθεσης μπορεί να κατασκευαστεί χρησιμοποιώντας ένα οποιοδήποτε block κρυπτογραφημάτων των 32 bits που έχει προκύψει εφαρμόζοντας ένα προεπιλεγμένο κλειδί σε ένα διάστημα IP διευθύνσεων. Εάν εκτεθειμένος host έχει μολυνθεί κατά τη διάρκεια είτε της hitlist σάρωσης είτε της σάρωσης τοπικού δικτύου, αρχίζει να σαρώνει τον κατάλογο από το σημείο εκείνο που του αντιστοιχεί, ψάχνοντας για τρωτά μηχανήματα προκειμένου να βρει νέους στόχους. Αντίθετα, εάν έχει μολυνθεί κατά τη διάρκεια της σάρωσης αντιμετάθεσης, αρχίζει τη σάρωση από ένα τυχαίο σημείο του καταλόγου αντιμετάθεσης. Οποτεδήποτε συναντά ένα ήδη μολυσμένο μηχάνημα, επιλέγει τυχαία ένα άλλο σημείο του καταλόγου αντιμετάθεσης και με τον τρόπο αυτό αρχίζει μια νέα διαδικασία σάρωσης, συνεχίζοντας την σάρωση από εκεί. Ένας εκτεθειμένος host έχει τη δυνατότητα να αναγνωρίσει μια ήδη μολυσμένη μηχανή μεταξύ εκείνων που δεν έχουν μολυνθεί, δεδομένου ότι οι μολυσμένες μηχανές αποκρίνονται διαφορετικά σε αυτόν από οποιαδήποτε άλλη μηχανή. Η διαδικασία της σάρωσης σταματά μόλις ο εκτεθειμένος host συναντήσει διαδοχικά έναν προκαθορισμένο αριθμό ήδη μολυσμένων μηχανών, χωρίς να έχει βρει κατά τη διάρκεια της χρονικής αυτής περιόδου νέους στόχους. Τότε ένα νέο κλειδί αντιμετάθεσης παράγεται και μια νέα φάση σάρωσης ξεκινά. Αυτός ο μηχανισμός σάρωσης εξυπηρετεί δύο σημαντικούς στόχους: Καταρχήν, αυτός ο μηχανισμός δεν επιτρέπει άσκοπες επαναμολύνσεις του ίδιου στόχου αφού

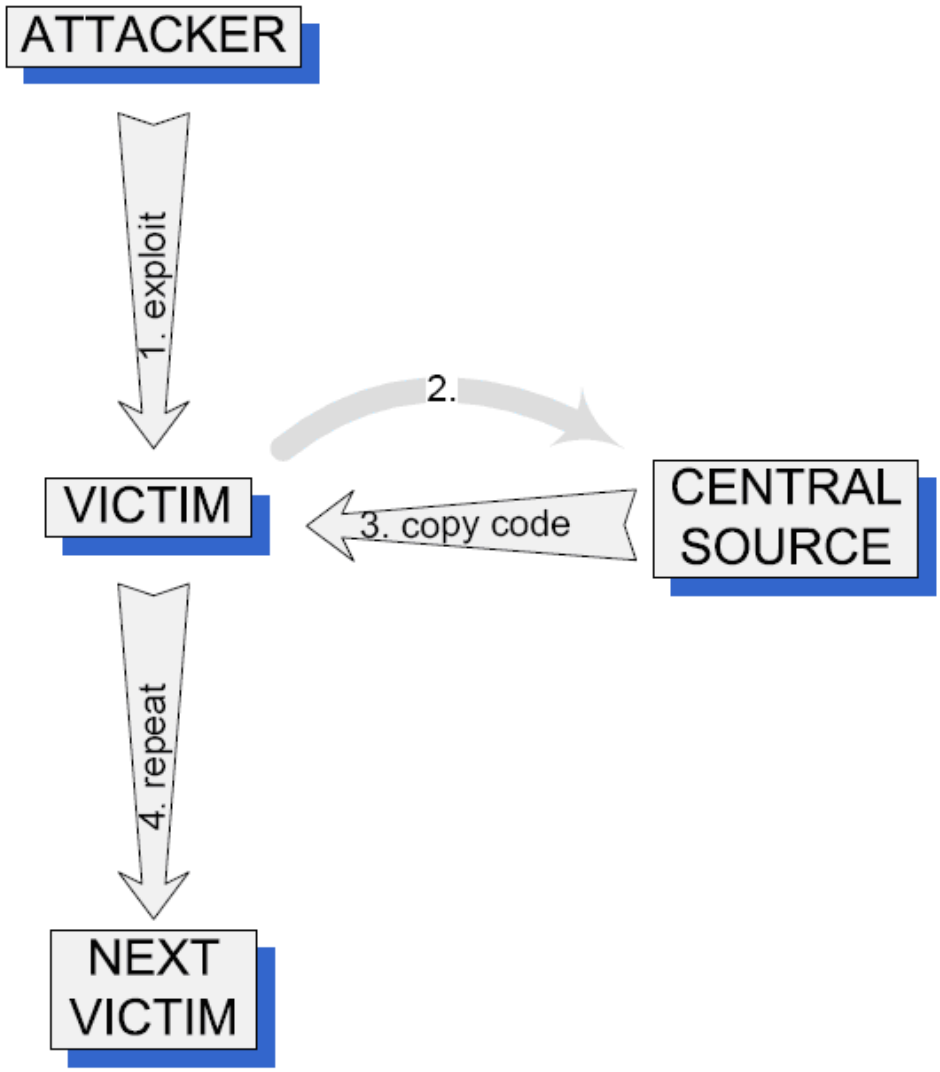
όταν ένας εκτεθειμένος host αντιληφθεί μια ήδη μολυσμένη μηχανή, αλλάζει τον τρόπο με τον οποίο εκμεταλλεύεται τον κατάλογο αντιμετάθεσης σύμφωνα με τη διαδικασία που περιγράφεται παραπάνω. Δεύτερον, αυτός ο μηχανισμός διατηρεί όλα τα πλεονεκτήματα της τυχαίας σάρωσης, δεδομένου ότι η σάρωση των νέων στόχων διεξάγεται με τυχαίο τρόπο. Ως εκ τούτου, η σάρωση αντιμετάθεσης μπορεί να χαρακτηριστεί ως μια συντονισμένη σάρωση με μια εξαιρετικά καλή απόδοση, μιας και η τυχαιότητα που αντιπροσωπεύει εγγυάται μεγάλες ταχύτητες σάρωσης.

Μια βελτιωμένη έκδοση της σάρωσης αντιμετάθεσης είναι η σάρωση διαιρεμένης αντιμετάθεσης. Αυτός ο τύπος σάρωσης είναι ένας συνδυασμός της σάρωσης αντιμετάθεσης και της hitlist σάρωσης. Σύμφωνα με το νέο μηχανισμό, ο εκτεθειμένος host έχει έναν κατάλογο αντιμετάθεσης, τον οποίο διαιρεί στα δύο όταν βρει το νέο στόχο του. Τότε, κρατά το ένα τμήμα του καταλόγου και δίνει το άλλο τμήμα στο πρόσφατα μολυσμένο μηχάνημα. Όταν ο κατάλογος αντιμετάθεσης, τον οποίο μια μολυσμένη μηχανή κατέχει, μειωθεί κάτω από ένα προκαθορισμένο επίπεδο, η μέθοδος σάρωσης μετατρέπεται από σάρωση διαιρεμένης αντιμετάθεσης σε σάρωση απλής αντιμετάθεσης.

4.3 ΔΙΑΔΟΣΗ ΚΑΚΟΒΟΥΛΟΥ ΚΩΔΙΚΑ

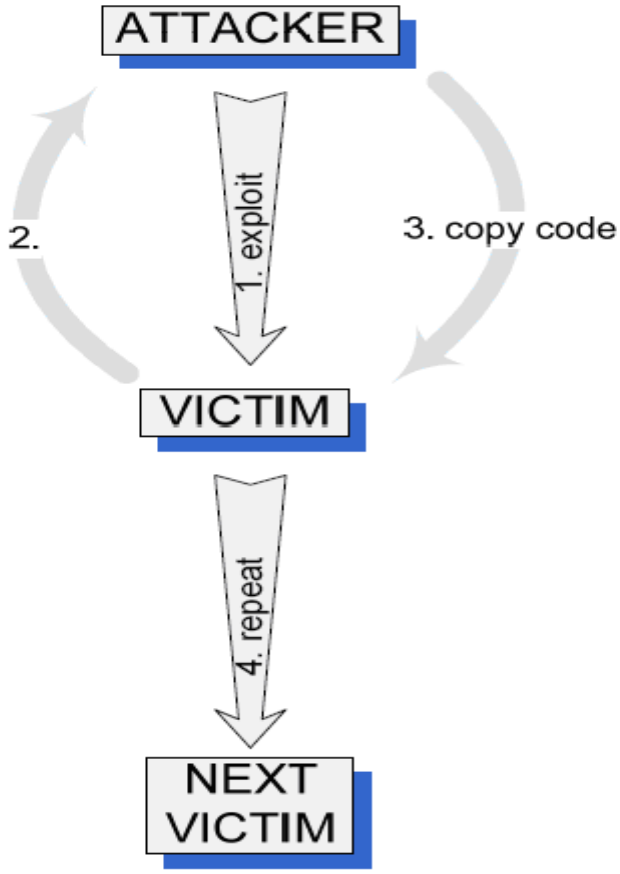
Προσπαθώντας να ομαδοποιήσουμε τους μηχανισμούς της κακόβουλης διάδοσης κώδικα και της οικοδόμησης του δικτύου επίθεσης, μπορούμε να προσδιορίσουμε τρεις ομάδες:

Κεντρική διάδοση κώδικα (Central source propagation): Σύμφωνα με αυτόν τον μηχανισμό, μετά την ανακάλυψη του τρωτού συστήματος που θα γίνει ένα από τα zombies, οδηγίες δίνονται σε μια κεντρική πηγή έτσι ώστε ένα αντίγραφο των εργαλείων επίθεσης να μεταφερθεί από την κεντρική πηγή στο πρόσφατα εκτεθειμένο σύστημα. Αφότου τα εργαλεία αυτά έχουν μεταφερθεί, μια αυτόματη εγκατάσταση τους σε αυτό το σύστημα πραγματοποιείται ελεγχόμενη από ένα scripting μηχανισμό. Αυτός αρχίζει έναν νέο κύκλο επίθεσης, όπου το πρόσφατα μολυσμένο σύστημα ψάχνει για άλλους τρωτούς υπολογιστές στους οποίους θα εγκαταστήσει το πακέτο εργαλείων επίθεσης χρησιμοποιώντας την ίδια διαδικασία με τον επιτιθέμενο. Όπως άλλοι μηχανισμοί μεταφοράς αρχείων, αυτός ο μηχανισμός χρησιμοποιεί συνήθως τα πρωτόκολλα HTTP, FTP, και RPC. Μια γραφική απεικόνιση αυτού του μηχανισμού παρουσιάζεται στο Σχήμα 5 :



Σχήμα 5 : Central Source Propagation

Back-chaining propagation (Back-chaining διάδοση): Σύμφωνα με αυτόν τον μηχανισμό, το πακέτο εργαλείων επίθεσης μεταφέρεται στο πρόσφατα εκτεθειμένο σύστημα από τον επιτιθέμενο. Πιο συγκεκριμένα, τα εργαλεία επίθεσης που είναι εγκατεστημένα στον επιτιθέμενο περιλαμβάνουν ειδικές μεθόδους για την αποδοχή μιας σύνδεσης από το εκτεθειμένο σύστημα και την αποστολή ενός αρχείου σε αυτό, το οποίο περιέχει τα εργαλεία επίθεσης. Αυτό το προς τα πίσω κανάλι αντιγραφής αρχείου μπορεί να υποστηριχθεί από απλούς port listeners που αντιγράφουν το περιεχόμενο αρχείων ή από πλήρως εγκατεστημένους από τον εισβολέα web servers, οι οποίοι δύο χρησιμοποιούν το πρωτόκολλο TFTP. Στο Σχήμα 6 παρουσιάζει τον μηχανισμό που περιγράφεται παραπάνω:



Σχήμα 6 : Back – Chaining Propagation

Αυτόνομη διάδοση (Autonomous propagation): σύμφωνα με αυτόν τον μηχανισμό, ο επιτιθέμενος host μεταφέρει το πακέτο εργαλείων επίθεσης στο πρόσφατα εκτεθειμένο σύστημα την ακριβή στιγμή κατά την οποία εισβάλει στο σύστημα. Αυτός ο μηχανισμός διαφέρει από τους προαναφερθέντες μηχανισμούς στο γεγονός ότι τα εργαλεία επίθεσης φυτεύονται στον εκτεθειμένο host από τον ίδιο τον επιτιθέμενο και όχι από μια εξωτερική πηγή αρχείων. Το σχήμα 7 εξηγεί την αυτόνομη διάδοση.

Σχήμα 7 : Autonomous Propagation

Μετά την κατασκευή του δικτύου επίθεσης, ο εισβολέας χρησιμοποιεί τις «handler» μηχανές για να διευκρινίσει τον τύπο επίθεσης και τη διεύθυνση του θύματος και περιμένει την κατάλληλη στιγμή προκειμένου να ξεκινήσει την επίθεση. Κατόπιν, είτε αυτός διατάζει από μακριά τους πράκτορες για την έναρξη της επιλεγμένης επίθεσης είτε οι δαίμονες "ξυπνούν" ταυτόχρονα, όπως ήταν προγραμματισμένοι για να κάνουν. Οι μηχανές των agent με τη σειρά τους αρχίζουν να στέλνουν μια ροή πακέτων στο θύμα, πλημμυρίζοντας με αυτόν τον τρόπο το σύστημα του θύματος με το άχρηστο φορτίο και εξαντλώντας τους πόρους του. Με αυτόν τον τρόπο, ο επιτιθέμενος καθιστά τη μηχανή του θύματος μη διαθέσιμη σε νόμιμους πελάτες και αποκτά δυνατότητα απεριόριστης πρόσβασης σε αυτή, έτσι ώστε να μπορεί να επιβάλει αυθαίρετα ζημία. Ο όγκος της κίνησης μπορεί να είναι τόσο υψηλός ώστε τα δίκτυα που συνδέουν τις επιτιθέμενες μηχανές με το θύμα μπορούν επίσης να πάσχουν από χαμηλή απόδοση. Ως εκ τούτου, η παροχή

υπηρεσιών πάνω από αυτά τα δίκτυα δεν είναι πλέον δυνατή, και με αυτόν τον τρόπο οι πελάτες τους στερούνται αυτών των υπηρεσιών. Για αυτόν τον λόγο, το δίκτυο που έχει φορτωθεί από το φορτίο επίθεσης μπορεί να θεωρηθεί ως ένα ακόμη θύμα της DDoS επίθεσης.

5

ΚΕΦΑΛΑΙΟ

<< Ταξινόμηση επιθέσεων DDoS >>

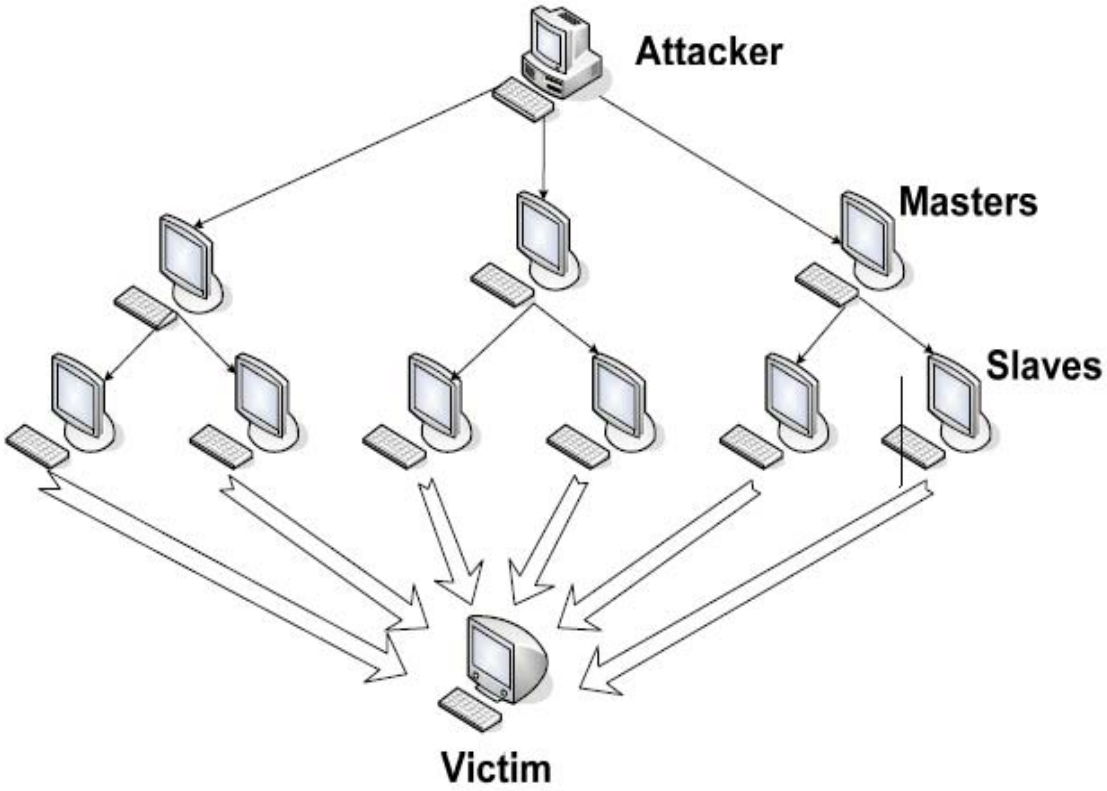
- **Ταξινόμηση Επιθέσεων DDOS**
- **Τυπικές Distributed Denial of Service (DDoS) Επιθέσεις**
- **Distributed Reflector denial of service (DRDoS) Επιθέσεις**
- **Προβλήματα Από Τις Επιθέσεις DDOS**

5 ΤΑΞΙΝΟΜΗΣΗ ΕΠΙΘΕΣΕΩΝ DDOS

Όπως έχει ήδη αναφερθεί, μια κατανεμημένη επίθεση άρνησης υπηρεσίας (DDoS) πραγματοποιείται όταν πολλές εκτεθειμένες μηχανές, που έχουν μολυνθεί από τον κακόβουλο κώδικα, ενεργούν ταυτόχρονα και συντονισμένα κάτω από τον έλεγχο ενός μόνο επιτιθέμενου προκειμένου να εισβάλουν στο σύστημα του θύματος, να εξαντλήσουν τους πόρους του και να το οδηγήσουν σε άρνηση υπηρεσίας στους πελάτες του. Υπάρχουν κυρίως δύο είδη DDoS επιθέσεων. Το πρώτο είδος είναι γνωστό ως *τυπική* DDoS *επίθεση*, ενώ το δεύτερο είδος είναι γνωστό ως *κατανεμημένων ανακλαστήρων επίθεση άρνησης υπηρεσιών (DRDoS)*. Στις ακόλουθες παραγράφους, αυτά τα δύο είδη περιγράφονται αναλυτικά.

5.1 ΤΥΠΙΚΕΣ DISTRIBUTED DENIAL OF SERVICE (DDOS) ΕΠΙΘΕΣΕΙΣ

Σε μια τυπική DDoS επίθεση, ο στρατός του επιτιθέμενου αποτελείται από "κυρίους-zombies" και "σκλάβους-zombies". Οι hosts και των δύο κατηγοριών είναι εκτεθειμένες μηχανές, οι οποίες έχουν προκύψει κατά τη διάρκεια της διαδικασίας σάρωσης και είναι μολυσμένες από τον ίδιο κακόβουλο κώδικα. Ο επιτιθέμενος συντονίζει και διατάζει τους "κυρίους-zombies" και αυτοί, με τη σειρά τους, συντονίζουν και πυροδοτούν τους "σκλάβους-zombies". Πιο συγκεκριμένα, ο επιτιθέμενος στέλνει μια εντολή επίθεσης στους "κυρίους-zombies" και ενεργοποιεί με αυτόν τον τρόπο όλες τις διαδικασίες επίθεσης σε εκείνες τις μηχανές, οι οποίες είναι σε χειμέρια νάρκη και περιμένουν την κατάλληλη εντολή προκειμένου να ξυπνήσουν και να αρχίσουν την επίθεση. Κατόπιν, οι "κύριοι-zombies", μέσω αυτών των διαδικασιών στέλνουν εντολές επίθεσης στους "σκλάβους-zombies", διατάζοντας τους να εξαπολύσουν DDoS μια επίθεση ενάντια στο θύμα. Με αυτόν τον τρόπο, οι μηχανές των agents ("σκλάβοι-zombies") αρχίζουν να στέλνουν έναν μεγάλο όγκο πακέτων στο θύμα, πλημμυρίζοντας με αυτόν τον τρόπο το σύστημά του με άχρηστο φορτίο και εξαντλώντας τους πόρους του. Η Εικόνα 3.1 είναι αντιπροσωπευτική αυτού του είδους DDoS επίθεσης.



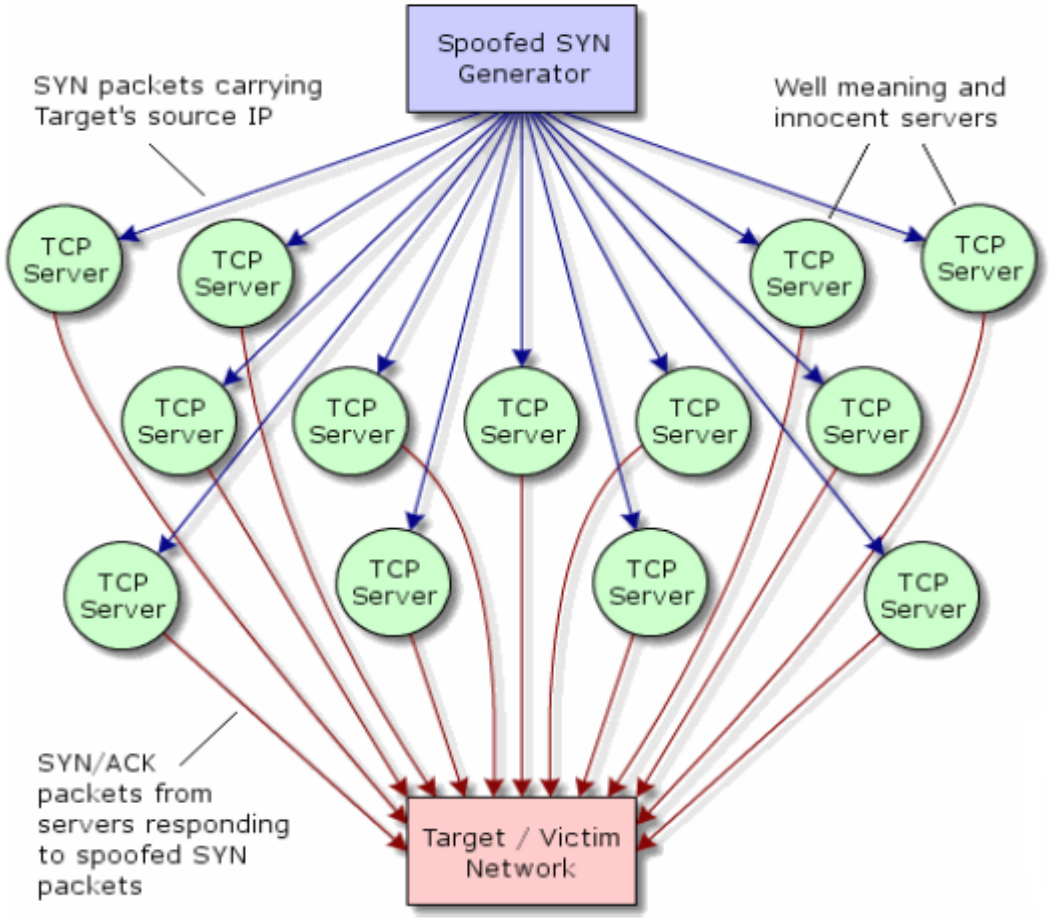
Σχήμα 8 : Μια επίθεση DDOS

Σε ορισμένες περιπτώσεις DDoS επιθέσεων, παραποιημένες IP διευθύνσεις πηγής χρησιμοποιούνται στα πακέτα της κίνησης της επίθεσης. Υπάρχουν δύο σημαντικοί λόγοι για τους οποίους ένας επιτιθέμενος προτιμά να χρησιμοποιήσει τέτοιες πλαστές IP διευθύνσεις πηγής: Καταρχήν, ο επιτιθέμενος θέλει να κρύψει την ταυτότητα των "zombies" προκειμένου να αποτρέψει τη δυνατότητα να ανιχνευθεί μέσω αυτών. Ο δεύτερος λόγος έχει να κάνει με την απόδοση της επίθεσης. Ο επιτιθέμενος θέλει να αποθαρρύνει οποιαδήποτε προσπάθεια του θύματος να φιλτράρει την κακόβουλη κίνηση και να αποβάλει οποιαδήποτε κακή αντήχηση της επίθεσης πάνω στη νόμιμη κίνηση.

5.2 DISTRIBUTED REFLECTOR DENIAL OF SERVICE (DRDOS) ΕΠΙΘΕΣΕΙΣ

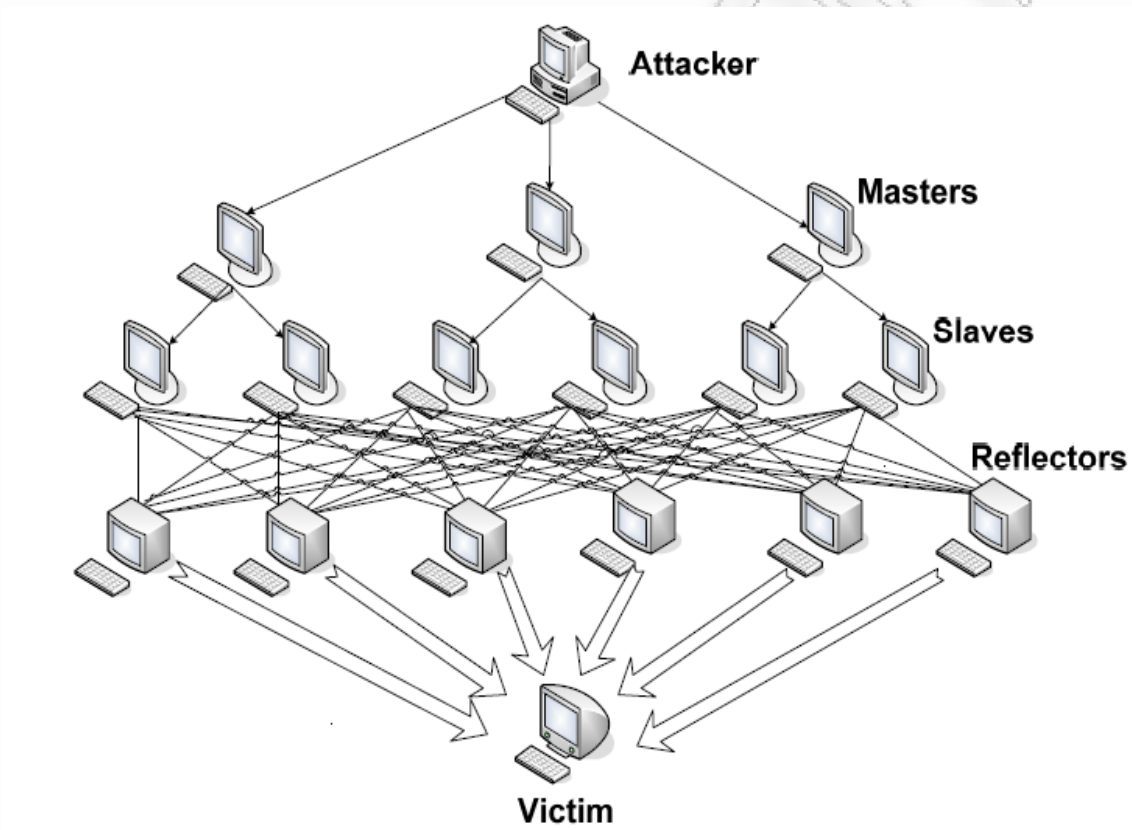
Αντίθετα από τις τυπικές denial of service επιθέσεις, στις DRDoS επιθέσεις ο στρατός των επιτιθέμενων περιλαμβάνει " κυρίους-zombies", "σκλάβους-zombies" και ανακλαστήρες. Το σενάριο αυτού του τύπου επίθεσης είναι το

ίδιο με αυτό των τυπικών DDoS επιθέσεων μέχρι ένα συγκεκριμένο στάδιο. Ο επιτιθέμενος έχει τον έλεγχο των "κυρίων- zombies", οι οποίοι, με τη σειρά τους, έχουν τον έλεγχο των "σκλάβων-zombies". Η διαφορά σε αυτόν τον τύπο επίθεσης συνίσταται στο γεγονός ότι οι "σκλάβοι-zombies" καθοδηγούνται από τους "κυρίους-zombies" για να στείλουν μια ροή πακέτων με τη διεύθυνση IP του θύματος ως διεύθυνση IP πηγής σε άλλες «αμόλυντες» μηχανές (γνωστές ως ανακλαστήρες), προτρέποντας αυτές τις μηχανές να συνδεθούν με το θύμα. Κατόπιν, οι ανακλαστήρες στέλνουν στο θύμα έναν μεγαλύτερο όγκο κίνησης, ως απάντηση στην παραίνεσή του για το άνοιγμα μιας νέας σύνδεσης με αυτούς, μιας και πιστεύουν ότι το θύμα ήταν ο host που το ζήτησε. Επομένως, στις DRDoS επιθέσεις, η επίθεση εξαπολύεται από μη-εκτεθειμένες μηχανές, οι οποίες ξεκινούν μια DRDoS επίθεση χωρίς να το γνωρίζουν (Σχήμα 9).



Σχήμα 9 : Μια επίθεση DRDOS

Συγκρίνοντας τα δύο σενάρια των distributed denial of service επιθέσεων, πρέπει να σημειώσουμε ότι μια DRDoS *επίθεση* είναι πιο καταστρεπτική από μια τυπική DDoS επίθεση. Αυτό συμβαίνει επειδή στην περίπτωση μιας DRDoS επίθεσης, υπάρχουν περισσότερες μηχανές για να μοιραστούν την επίθεση και ως εκ τούτου, η επίθεση γίνεται πιο κατανεμημένη. Ένας δεύτερος λόγος που δικαιολογεί το γεγονός ότι μια DRDoS *επίθεση* είναι πιο επικίνδυνη σε σχέση με μια τυπική DDoS επίθεση είναι ότι η πρώτη δημιουργεί έναν μεγαλύτερο όγκο κίνησης εξαιτίας του γεγονότος της πιο κατανεμημένης φύσης της. Το σχήμα 10 απεικονίζει γραφικά μια DRDoS επίθεση.



Σχήμα 10 : DRDoS επίθεση

5.3 ΓΝΩΣΤΕΣ DDOS ΕΠΙΘΕΣΕΙΣ

Αυτή η σύντομη έκθεση πάνω στις DDoS επιθέσεις θα ήταν ελλιπής εάν δεν γινόταν αναφορά σε μερικές από τις πιο γνωστές DDoS επιθέσεις. Για αυτόν τον λόγο, μερικές από τις πιο διάσημες καταγεγραμμένες DDoS επιθέσεις παρουσιάζεται συνοπτικά στη συνέχεια. Μάλιστα, η παρουσίαση αυτή γίνεται με ταυτόχρονη αναφορά στις αδυναμίες πρωτοκόλλων ή μηχανισμών του Διαδικτύου που είναι υπαίτιες για αυτές τις επιθέσεις:

Apache2 Αυτή η επίθεση εξαπολύεται ενάντια σε έναν apache web server από τον οποίο ο πελάτης ζητά μια υπηρεσία με την αποστολή ενός αιτήματος με πολλές HTTP επικεφαλίδες. Παρόλα αυτά, όταν ο apache web server λαμβάνει πολλά τέτοια αιτήματα, δεν μπορεί να αντιμετωπίσει το φορτίο και καταρρέει.

ARP Poison Οι ARP Poison επιθέσεις απαιτούν από τον επιτιθέμενο να έχει πρόσβαση στο τοπικό δίκτυο του θύματος. Ο επιτιθέμενος εξαπατά τους hosts του συγκεκριμένου LAN παρέχοντας τους λανθασμένες MAC διευθύνσεις για τους hosts με ήδη γνωστές IP διευθύνσεις. Αυτό μπορεί να επιτευχθεί από τον επιτιθέμενο μέσω της ακόλουθης διαδικασίας: Το δίκτυο ελέγχεται για "arp whohas" αιτήματα. Μόλις ένα τέτοιο αίτημα παραληφθεί, ο κακόβουλος επιτιθέμενος προσπαθεί να απαντήσει όσο το δυνατόν γρηγορότερα στον host που ρωτά προκειμένου να τον παραπλανήσει για τη ζητούμενη διεύθυνση.

Back Αυτή η επίθεση εξαπολύεται ενάντια σε έναν apache web server, ο οποίος πλημμυρίζει από αιτήματα που περιέχουν έναν μεγάλο αριθμό front slash χαρακτήρων στην περιγραφή του URL. Καθώς ο server προσπαθεί να επεξεργαστεί όλα αυτά τα αιτήματα, γίνεται ανίκανος να επεξεργαστεί άλλα νόμιμα αιτήματα και ως εκ τούτου αρνείται την υπηρεσία στους πελάτες του.

CrashIIS Το θύμα μιας CrashIIS επίθεσης είναι ένας κοινός Microsoft Windows NT IIS web server. Ο επιτιθέμενος στέλνει στο θύμα ένα δύσμορφο GET αίτημα, το οποίο προκαλεί την κατάρρευση του web server.

DoSNuke Σε αυτό το είδος επίθεσης, το Microsoft TM Windows NT θύμα πλημμυρίζεται με “out of band” δεδομένα (MSG_OOB). Τα πακέτα που στέλνονται από τις επιτιθέμενες μηχανές είναι σημαδευμένα ως "urg" εξαιτίας της MSG_OOB σημαίας. Σαν αποτέλεσμα, το θύμα καταρρέει και είναι δυνατό το μηχάνημά του να δείξει τη γνωστή σε όλους «μπλε οθόνη» των Windows (bluescreen of death”).

Land Στις Land επιθέσεις, ο επιτιθέμενος στέλνει στο θύμα ένα TCP SYN πακέτο το οποίο περιέχει την ίδια IP διεύθυνση τόσο ως διεύθυνση πηγής όσο και ως διεύθυνση προορισμού. Ένα τέτοιο πακέτο κλειδώνει ολοκληρωτικά το σύστημα του θύματος.

Mailbomb Στη Mail bomb επίθεση, η ουρά mail του θύματος πλημμυρίζεται από μια αφθονία μηνυμάτων, τα οποία προκαλούν την κατάρρευση του συστήματος.

SYN Flood Μια SYN flood επίθεση εμφανίζεται κατά τη διάρκεια της τριμερούς χειραψίας που χαρακτηρίζει την αρχή μιας σύνδεσης TCP/IP. Στην τριμερή χειραψία ένας πελάτης αιτείται για μια νέα σύνδεση, στέλνοντας ένα πακέτο TCP/SYN σε έναν server. Μετά από αυτό, ο server στέλνει ένα πακέτο SYN/ACK πίσω στον πελάτη και τοποθετεί το αίτημα σύνδεσης σε μια ουρά αναμονής. Τέλος, ο πελάτης επιβεβαιώνει το πακέτο SYN/ACK. Σε περίπτωση επίθεσης, εντούτοις, ο επιτιθέμενος στέλνει μια αφθονία πακέτων TCP/SYN στο θύμα, υποχρεώνοντας το τόσο να ανοίξει πολλές TCP συνδέσεις όσο και να αποκριθεί σε αυτές. Κατόπιν, ο επιτιθέμενος δεν εκτελεί το τρίτο βήμα της τριμερούς χειραψίας που ακολουθεί, καθιστώντας το θύμα ανίκανο να δεχτεί οποιεσδήποτε νέες εισερχόμενες συνδέσεις, δεδομένου ότι η ουρά αναμονής του είναι πλήρης από μισάνοιχτες TCP συνδέσεις.

Ping of Death Στην Ping of Death επίθεση, ο επιτιθέμενος δημιουργεί ένα πακέτο που περιέχει περισσότερα από 65536 bytes, το οποίο είναι το όριο που το πρωτόκολλο IP καθορίζει. Αυτό το πακέτο μπορεί να προκαλέσει διάφορες ζημιές στο μηχάνημα που θα το λάβει, όπως συντριβή και επανεκκίνηση.

Process Table Αυτή η επίθεση εκμεταλλεύεται το χαρακτηριστικό γνώρισμα μερικών υπηρεσιών δικτύου για να παραγάγει μια νέα διαδικασία κάθε φορά που οργανώνεται μια νέα TCP/IP σύνδεση. Ο επιτιθέμενος προσπαθεί να κάνει όσο το δυνατόν περισσότερες ανολοκλήρωτες συνδέσεις στο θύμα προκειμένου να αναγκάσει το σύστημα του θύματος να παραγάγει μια αφθονία διαδικασιών. Ως εκ τούτου, καθώς ο αριθμός των διαδικασιών που τρέχουν στο σύστημα δεν μπορεί να είναι απεριόριστα μεγάλος, η επίθεση καθιστά το θύμα ανίκανο να εξυπηρετήσει οποιοδήποτε άλλο αίτημα.

Smurf attack Σε μια "smurf" επίθεση, το θύμα πλημμυρίζεται από Internet Control Messages Protocol (ICMP) “echo-reply” πακέτα. Ο επιτιθέμενος στέλνει πολλά ICMP “echo-request” πακέτα στη broadcast διεύθυνση πολλών υποδικτύων. Αυτά τα πακέτα περιέχουν ως διεύθυνση IP πηγής αυτή του θύματος. Κάθε μηχάνημα που ανήκει σε οποιοδήποτε από αυτά τα υποδίκτυα αποκρίνεται στέλνοντας ICMP “echo-reply” πακέτα στο θύμα. Οι Smurf επιθέσεις είναι πολύ επικίνδυνες, δεδομένου ότι είναι έντονα κατανεμημένες επιθέσεις.

SSH Process table Όπως στην Process Table επίθεση, η επίθεση κάνει τις εκατοντάδες των συνδέσεων στο θύμα μέσω του ssh χωρίς ολοκλήρωση της διαδικασίας login. Με αυτόν τον τρόπο, το sshd daemon στο σύστημα του θύματος είναι υποχρεωμένο να γεννά τόσες πολλές διαδικασίες ώστε το θύμα να εξαντλείται.

Syslogd Η Syslogd επίθεση προκαλεί την κατάρρευση του syslogd προγράμματος ενός Solaris 2.5 server στέλνοντας του ένα μήνυμα με άκυρη IP διεύθυνση πηγής.

TCP Reset Στην TCP Reset επίθεση, το δίκτυο ελέγχεται για αιτήματα “tcpconnection” στο θύμα. Μόλις ένα τέτοιο αίτημα βρεθεί, ο κακόβουλος επιτιθέμενος στέλνει ένα αλλοιωμένο TCP RESET πακέτο στο θύμα και το υποχρεώνει να ολοκληρώσει την TCP σύνδεση.

Teardrop Ενώ ένα πακέτο ταξιδεύει από το μηχάνημα πηγής προς το μηχάνημα προορισμού, μπορεί να χωριστεί σε μικρότερα τεμάχια, μέσω της διαδικασίας του τεμαχισμού. Μια Teardrop επίθεση δημιουργεί μια ροή IP τεμαχίων με το πεδίο offset υπερφορτωμένο. Ο host προορισμού που θα προσπαθήσει να συναρμολογήσει εκ νέου αυτά τα δύσμορφα τεμάχια θα είναι μπροστά σε μια πολύ δύσκολη κατάσταση, η οποία θα προκαλέσει την κατάρρευσή του ή ακόμα και την επανεκκίνησή του.

UDPstorm Σε μια σύνδεση UDP, μια υπηρεσία παραγωγής χαρακτήρα ("chargen") παράγει μια σειρά χαρακτήρων κάθε φορά που λαμβάνει ένα πακέτο UDP, ενώ μια echo υπηρεσία επαναλαμβάνει οποιοδήποτε χαρακτήρα λαμβάνει. Εκμεταλλευόμενος αυτές τις δύο υπηρεσίες, ο επιτιθέμενος στέλνει ένα πακέτο με αλλοιωμένη την πηγή ώστε να είναι αυτή του θύματος σε ένα άλλο μηχάνημα. Κατόπιν, η echo υπηρεσία του αρχικού μηχανήματος επαναλαμβάνει τα δεδομένα του πακέτου πίσω στο μηχάνημα του θύματος, το οποίο με τη σειρά του, αποκρίνεται με τον ίδιο τρόπο. Ως εκ τούτου, δημιουργείται μια σταθερή ροή άχρηστου φορτίου που φορτώνει το δίκτυο.

5.4 ΠΡΟΒΛΗΜΑΤΑ ΠΟΥ ΠΡΟΚΥΠΤΟΥΝ ΑΠΟ ΤΙΣ ΕΠΙΘΕΣΕΙΣ DDoS ΚΑΙ ΑΝΤΙΜΕΤΡΑ

Τα αποτελέσματα των ανωτέρω επιθέσεων είναι καταστροφικά. Οι DDoS επιθέσεις έχουν δύο χαρακτηριστικά: είναι τόσο κατανεμημένες επιθέσεις όσο και επιθέσεις άρνησης υπηρεσιών. Το πρώτο σημαίνει ότι είναι επιθέσεις μεγάλης κλίμακας και ασκούν μεγάλη επίδραση στα θύματα. Το δεύτερο σημαίνει ότι ο στόχος τους είναι να αρνηθούν την πρόσβαση του θύματος σε ένα συγκεκριμένο πόρο (υπηρεσία). Αυτό δεν είναι πάρα πολύ δύσκολο

δεδομένου ότι το Διαδίκτυο δεν σχεδιάστηκε έχοντας την ασφάλεια ως πρώτο μέλημα.

Αρχικά, το διαθέσιμο εύρος ζώνης είναι ένα από τα "αγαθά" που οι επιτιθέμενοι προσπαθούν να καταναλώσουν. Πλημμυρίζοντας το δίκτυο με άχρηστα πακέτα, π.χ. ICMP echo πακέτα, εμποδίζουν τα νόμιμα πακέτα να ταξιδέψουν πάνω από το δίκτυο. Δεύτερον, οι επιτιθέμενοι προσπαθούν να καταναλώσουν την επεξεργαστική ισχύ. Παράγοντας χιλιάδες άχρηστες διαδικασίες στο τερματικό του θύματος οι επιτιθέμενοι κατορθώνουν να απασχολούν πλήρως τη μνήμη και τους πίνακες διαδικασιών. Με αυτόν τον τρόπο ο υπολογιστής του θύματος δεν μπορεί να εκτελέσει καμιά διαδικασία και το σύστημα καταρρέει. Χρησιμοποιώντας αυτήν την μέθοδο, ο επιτιθέμενος κατορθώνει να εμποδίσει τους πελάτες από την πρόσβαση στις υπηρεσίες του θύματος και διακόπτει τις τρέχουσες συνδέσεις. Τέλος, οι επιτιθέμενοι προσπαθούν να συντηρήσουν τις υπηρεσίες του θύματος κατειλημμένες έτσι ώστε κανένας άλλος να μην μπορεί να έχει πρόσβαση σε αυτές. Για παράδειγμα, αφήνοντας τις TCP συνδέσεις μισάνοιχτες, οι επιτιθέμενοι κατορθώνουν να καταναλώσουν τις δομές δεδομένων του θύματος, και με αυτόν τον τρόπο, κανένας άλλος δεν μπορεί να πραγματοποιήσει μια TCP-σύνδεση με το θύμα.

Ο αντίκτυπος των ανωτέρω επιθέσεων είναι καταστροφικός, ειδικά όταν τα θύματα δεν είναι άτομα αλλά επιχειρήσεις. Οι DDoS επιθέσεις εμποδίζουν τα θύματα είτε από τη χρησιμοποίηση του Διαδικτύου, είτε από το να βρίσκονται στη διάθεση άλλων ανθρώπων. Συνεπώς, όταν το θύμα είναι ένας ISP (Internet Service Provider – Πάροχος Internet), τότε τα αποτελέσματα μιας τέτοιας επίθεσης είναι ακόμη πιο σοβαρά.

Οι πελάτες των ISP δεν θα μπορούν να εξυπηρετηθούν. Το ηλεκτρονικό εμπόριο είναι επίσης στην κορυφή του καταλόγου στόχων. Το να είναι μερικές ώρες off-line, μπορεί να έχει ως αποτέλεσμα μια απώλεια μερικών εκατομμυρίων δολαρίων για έναν ISP. Τέλος, το γεγονός ότι οι επιχειρήσεις χρησιμοποιούν όλο και περισσότερο το Διαδίκτυο για διαφήμιση ή για να παράσχουν υπηρεσίες on-line, αυξάνει την καταστρεπτική δύναμη τέτοιων γεγονότων.

5.5 ΑΜΥΝΤΙΚΟΙ ΜΗΧΑΝΙΣΜΟΙ

Από την πρώτη στιγμή, όλοι οι νόμιμοι χρήστες έχουν προσπαθήσει να απαντήσουν στην παραπάνω απειλή. Πανεπιστημιακές κοινότητες και εταιρίες λογισμικού έχουν προτείνει διάφορες μεθόδους ενάντια στην DDoS απειλή. Παρά τις προσπάθειες, η λύση παραμένει ακόμα ένα όνειρο. Οι επιτιθέμενοι κατορθώνουν να ανακαλύπτουν διαρκώς άλλες αδυναμίες των πρωτοκόλλων και το χειρότερο είναι ότι εκμεταλλεύονται τους αμυντικούς μηχανισμούς προκειμένου να αναπτύξουν νέες επιθέσεις. Ανακαλύπτουν μεθόδους για να υπερνικήσουν αυτούς τους μηχανισμούς ή τους εκμεταλλεύονται για να παραγάγουν ψεύτικους συναγερμούς και να προκαλέσουν έτσι μια τεράστια αναστάτωση.

Πολλοί experts έχουν προσπαθήσει να ταξινομήσουν τους DDoS αμυντικούς μηχανισμούς προκειμένου να καταστήσουν τα πράγματα πιο σαφή. Αυτή η

ταξινόμηση βοηθά τους χρήστες να έχουν μια γενική άποψη της κατάστασης και τους developers αμυντικών μηχανισμών να συνεργάζονται ενάντια στην απειλή. Η βασική διάκριση είναι σε προληπτικούς και αντιδραστικούς αμυντικούς μηχανισμούς.

5.6 ΠΡΟΛΗΠΤΙΚΟΙ ΜΗΧΑΝΙΣΜΟΙ

Οι προληπτικοί μηχανισμοί προσπαθούν να εξαλείψουν τη δυνατότητα των DDoS επιθέσεων συνολικά ή να ενεργοποιήσουν τα πιθανά θύματα ώστε να υπομείνουν την επίθεση χωρίς άρνηση των υπηρεσιών στους νόμιμους πελάτες. Όσον αφορά στην πρόληψη επίθεσης, αντίμετρα μπορούν να ληφθούν πάνω στα θύματα ή πάνω στα zombies.

Αυτό σημαίνει τροποποίηση της διαμόρφωσης του συστήματος για να εξαλειφθεί η δυνατότητα αποδοχής μιας επίθεσης DDoS ή απρόθυμης συμμετοχής σε μια επίθεση DDoS. Οι hosts πρέπει να φρουρούνται από την παράνομη κίνηση από ή προς το μηχάνημα. Διατηρώντας τα πρωτόκολλα και το λογισμικό ενημερωμένο (up to date), μπορούμε να μειώσουμε τις αδυναμίες ενός υπολογιστή. Μια τακτική σάρωση του μηχανήματος είναι επίσης απαραίτητη προκειμένου να ανιχνευθεί οποιαδήποτε "ανώμαλη" συμπεριφορά. Παραδείγματα των μηχανισμών ασφαλείας του συστήματος αποτελούν η επιτήρηση της πρόσβασης στον υπολογιστή, εφαρμογές που κάνουν «download» και εγκαθιστούν τα «μπαλώματα» ασφαλείας αυτόματα, συστήματα firewall, ανιχνευτές ιών και συστήματα ανίχνευσης εισβολής. Η σύγχρονη τάση είναι προς επιχειρήσεις ασφαλείας που φρουρούν το δίκτυο ενός πελάτη και τον ενημερώνουν σε περίπτωση ανίχνευσης επίθεσης για να λάβει μέτρα υπεράσπισης. Διάφοροι αισθητήρες ελέγχουν την κίνηση του δικτύου και στέλνουν τις πληροφορίες σε έναν server προκειμένου να αποφασίσει για την "υγεία" της κατάστασης. Η διασφάλιση της ακεραιότητας του υπολογιστή μειώνει τη δυνατότητα όχι μόνο να είναι θύμα αλλά και zombie. Το τελευταίο είναι πολύ σημαντικό επειδή αφανίζει το στρατό των επιτιθέμενων. Όλα τα ανωτέρω μέτρα δεν μπορούν ποτέ να είναι 100% αποτελεσματικά, αλλά σίγουρα μειώνουν τη συχνότητα και τη δύναμη των DDoS επιθέσεων.

Υπάρχουν πολλά άλλα μέτρα που μπορούν να ληφθούν προκειμένου να μειώσουν το στρατό του επιτιθέμενου ή να περιορίσουν τη δύναμή του. Η μελέτη των μεθόδων επίθεσης μπορεί να οδηγήσει στην αναγνώριση «ελαττωμάτων» στα πρωτόκολλα. Για παράδειγμα οι διαχειριστές δικτύων θα μπορούσαν να ρυθμίσουν τους gateways του δικτύου τους προκειμένου να φιλτράρεται η κίνηση εισόδου και εξόδου. Η διεύθυνση IP της πηγής της κίνησης εξόδου πρέπει να ανήκει στο υποδίκτυο ενώ η διεύθυνση IP της πηγής της κίνησης εισόδου δεν πρέπει. Με αυτόν τον τρόπο, μπορούμε να μειώσουμε την κίνηση με αλλοιωμένες διευθύνσεις IP πάνω στο δίκτυο. Επιπλέον, κατά τη διάρκεια των τελευταίων ετών, διάφορες τεχνικές έχουν προταθεί προκειμένου να εξεταστούν τα συστήματα για πιθανά μειονεκτήματα, πριν λανσαριστούν στην αγορά. Πιο συγκεκριμένα, αντικαθιστώντας τα τμήματα ενός συστήματος με κακόβουλα μπορούμε να ανακαλύψουμε εάν το σύστημα μπορεί να επιζήσει της κακής κατάστασης στην οποία έχει περιπέσει. Σε περίπτωση που το σύστημα καταρρεύσει, τότε

ένα μειονέκτημα έχει ανιχνευθεί και οι υπεύθυνοι για την ανάπτυξή του πρέπει να το διορθώσουν.

Από την άλλη πλευρά οι μηχανισμοί πρόληψης DoS δίνουν τη δυνατότητα στο θύμα να υπομείνει τις προσπάθειες επίθεσης χωρίς άρνηση της υπηρεσίας στους νόμιμους πελάτες. Μέχρι τώρα δύο μέθοδοι έχουν προταθεί προς αυτήν την κατεύθυνση. Η πρώτη αναφέρεται σε πολιτικές που αυξάνουν τα προνόμια ενός χρήστη σύμφωνα με τη συμπεριφορά του. Όταν η ταυτότητα του χρήστη επιβεβαιώνεται, τότε καμιά απειλή δεν υπάρχει. Οποιαδήποτε παράνομη κίνηση από αυτόν μπορεί να οδηγήσει στην ποινική του δίωξη. Η δεύτερη μέθοδος είναι πάρα πολύ ακριβή. Αναφέρεται στην αύξηση των πόρων που βρίσκονται στο στόχαστρο των επιτιθέμενων σε τέτοιο βαθμό ώστε οι DDoS επιδράσεις να είναι αμελητέες. Ένα τέτοιο μέτρο είναι τις περισσότερες φορές αδύνατο να εφαρμοστεί.

5.7 ΑΝΤΙΔΡΑΣΤΙΚΟΙ ΜΗΧΑΝΙΣΜΟΙ

Οι Αντιδραστικοί μηχανισμοί (γνωστοί και ως early warning systems - συστήματα έγκαιρης προειδοποίησης) προσπαθούν να ανιχνεύσουν την επίθεση και να απαντήσουν σε αυτήν άμεσα. Ως εκ τούτου, περιορίζουν τον αντίκτυπο της επίθεσης

πάνω στο θύμα. Και πάλι όμως, υπάρχει ο κίνδυνος του χαρακτηρισμού μιας νόμιμης σύνδεσης ως επίθεση. Για αυτόν τον λόγω είναι απαραίτητο για τους ερευνητές να είναι πολύ προσεκτικοί.

Οι κύριες στρατηγικές ανίχνευσης είναι ανίχνευση-υπογραφής, ανίχνευση-ανωμαλίας και υβριδικά συστήματα. Οι μέθοδοι που είναι βασισμένες στην ανίχνευση- υπογραφής αναζητούν πρότυπα (υπογραφές) πάνω στην παρατήρησα κίνηση του δικτύου που ταιριάζουν με γνωστές υπογραφές επίθεσης μιας βάσης δεδομένων. Το πλεονέκτημα αυτών των μεθόδων είναι ότι μπορούν εύκολα και αξιόπιστα να ανιχνεύσουν γνωστές επιθέσεις, αλλά δεν μπορούν να αναγνωρίσουν νέες επιθέσεις.

Επιπλέον, η βάση υπογραφών πρέπει να ενημερώνεται τακτικά προκειμένου να διατηρηθεί η αξιοπιστία του συστήματος.

Τέλος, τα υβριδικά συστήματα συνδυάζουν και τις δύο ανωτέρω μεθόδους. Αυτά τα συστήματα ενημερώνουν τη βάση υπογραφών τους με επιθέσεις που ανιχνεύονται με βάση την ανίχνευση ανωμαλίας.

Και πάλι ο κίνδυνος είναι μεγάλος καθώς ένας επιτιθέμενος μπορεί να κοροϊδέψει το σύστημα οδηγώντας το στο χαρακτηρισμό μιας κανονικής κίνησης ως επίθεση. Σε αυτήν την περίπτωση το IDS (σύστημα ανίχνευσης εισβολής) σύστημα γίνεται ένα εργαλείο επίθεσης. Κατά συνέπεια οι σχεδιαστές IDS συστημάτων πρέπει να είναι πολύ προσεκτικοί επειδή η έρευνά τους μπορεί να γυρίσει μπούμερανγκ.

Μετά την ανίχνευση της επίθεσης, οι αντιδραστικοί μηχανισμοί απαντούν σε αυτή. Η ανακούφιση από τον αντίκτυπο της επίθεσης είναι ο πρωταρχικός στόχος. Μερικοί μηχανισμοί αντιδρούν περιορίζοντας το ποσοστό της αποδεχόμενης κίνησης. Αυτό σημαίνει ότι η νόμιμη κίνηση εμποδίζεται επίσης. Σε αυτήν την περίπτωση η λύση έρχεται με τις trace back τεχνικές που προσπαθούν να προσδιορίσουν τον επιτιθέμενο. Εάν ο επιτιθέμενος προσδιοριστεί, παρά τις προσπάθειές του να αλλοιώσει τη διεύθυνσή του,

τότε είναι εύκολο να φιλτραριστεί η κίνησή του. Το φιλτράρισμα είναι αποδοτικό μόνο εάν η ανίχνευση του επιτιθεμένου δεν είναι λανθασμένη. Σε οποιαδήποτε άλλη περίπτωση το φιλτράρισμα μπορεί να μετατραπεί σε εργαλείο επίθεσης.

5.8 ΔΥΣΚΟΛΙΕΣ ΣΤΗΝ ΑΝΤΙΜΕΤΩΠΙΣΗ ΤΩΝ ΕΠΙΘΕΣΕΩΝ

Η ανάπτυξη των εργαλείων ανίχνευσης και αντιμετώπισης είναι πολύ περίπλοκη. Οι σχεδιαστές πρέπει να σκεφτούν εκ των προτέρων κάθε πιθανή κατάσταση καθώς κάθε αδυναμία μπορεί να γίνει αντικείμενο εκμετάλλευσης των επιτιθέμενων. Οι δυσκολίες περιλαμβάνουν:

Οι DDoS επιθέσεις πλημμυρίζουν το θύμα με πακέτα. Αυτό σημαίνει ότι το θύμα δεν μπορεί να έρθει σε επαφή με κανέναν άλλο προκειμένου να ζητήσει βοήθεια. Έτσι είναι δυνατό ένας γείτονας στο δίκτυο να δέχεται επίθεση και κανείς να μην το ξέρει ή κανείς να μην μπορεί να βοηθήσει. Συνεπώς οποιαδήποτε μέτρα προκειμένου να υπάρξει αντίδραση μπορούν να ληφθούν μόνο εάν η επίθεση ανιχνευθεί νωρίς. Αλλά μπορεί μια επίθεση να ανιχνευθεί νωρίς; Συνήθως η ροή της κίνησης αυξάνεται ξαφνικά και χωρίς καμία προειδοποίηση. Για αυτόν το λόγο οι αμυντικοί μηχανισμοί πρέπει να αντιδρούν ταχύτατα.

Οποιαδήποτε προσπάθεια φιλτραρίσματος της εισερχόμενης ροής σημαίνει ότι και νόμιμη κίνηση θα απορριφθεί. Και εάν η νόμιμη κίνηση απορριφθεί, πώς θα αντιδράσουν εφαρμογές που περιμένουν τις πληροφορίες; Από την άλλη πλευρά, εάν τα zombies είναι χιλιάδες ή εκατομμύρια, η κυκλοφορία τους θα πλημμυρίσει το δίκτυο και θα καταναλώσει όλο το εύρος ζώνης. Σε αυτήν την περίπτωση το φιλτράρισμα είναι άχρηστο δεδομένου ότι τίποτα δεν μπορεί να ταξιδέψει πάνω από το δίκτυο.

Τα πακέτα επίθεσης έχουν συνήθως αλλοιωμένες IPs. Ως εκ τούτου είναι δυσκολότερο να ανιχνευθεί η πηγή τους. Επιπλέον δεν είναι σίγουρο ότι οι ενδιάμεσοι δρομολογητές και οι ενδιάμεσοι ISPs θα συνεργαστούν σε αυτήν την προσπάθεια. Μερικές φορές οι επιτιθέμενοι αλλοιώνοντας τη διεύθυνση IP της πηγής κατορθώνουν να δημιουργήσουν πλαστούς στρατούς. Τα πακέτα μπορεί να προέρχονται από χιλιάδες IPs, αλλά τα zombies είναι μόνο μερικές δεκάδες, για παράδειγμα.

Οι αμυντικοί μηχανισμοί εφαρμόζονται σε συστήματα με διαφορές στο λογισμικό και στην αρχιτεκτονική. Επίσης τα συστήματα διαχειρίζονται από χρήστες με διαφορετικό επίπεδο γνώσης. Οι developers πρέπει να σχεδιάσουν μια πλατφόρμα ανεξάρτητη από όλες αυτές τις παραμέτρους.

6

ΚΕΦΑΛΑΙΟ

<< Σύγχρονες τάσεις στην υπεράσπιση ενάντια στις επιθέσεις DDoS>>

- **HONEY POTS**
- **HONEY NET**

6 ΣΥΓΧΡΟΝΕΣ ΤΑΣΕΙΣ ΣΤΗΝ ΥΠΕΡΑΣΠΙΣΗ ΕΝΑΝΤΙΑ ΣΤΙΣ ΕΠΙΘΕΣΕΙΣ DDOS

Μέχρι τώρα, οι developers δεν έχουν κατορθώσει να αναπτύξουν έναν 100% αποτελεσματικό αμυντικό μηχανισμό. Όλοι οι μηχανισμοί που έχουν παρουσιαστεί είτε μπορούν να αντιμετωπίσουν μόνο συγκεκριμένες επιθέσεις DDoS ή τελικά γίνονται αντικείμενο εκμετάλλευσης των επιτιθέμενων. Λόγω αυτού του γεγονότος, οι developers εργάζονται αυτήν την περίοδο πάνω σε συστήματα αντιπερισπασμού των DDoS επιθέσεων. Τα Honeypots είναι ο βασικός αντιπρόσωπος αυτής της κατηγορίας.

6.1 HONEYPOTS

6.1.1 Εισαγωγή

Τα υπολογιστικά συστήματα που είναι σήμερα συνδεδεμένα με το διαδίκτυο, δέχονται διαρκώς επιθέσεις από worms, αυτοματοποιημένες επιθέσεις και εισβολείς. Θα έλεγε κανείς ότι βρίσκονται πάντα κάτω από ελέγχους (audits) και επιθέσεις που σκοπό έχουν να ανακαλύψουν και να εκμεταλλευτούν ακόμα και το παραμικρό κενό στην αλυσίδα της ασφάλειας. Ένα από τα πιο πρόσφατα εργαλεία στον “πόλεμο” για την αντιμετώπιση των δικτυακών επιθέσεων από κακόβουλους χρήστες και αυτοματοποιημένες επιθέσεις worms και autorooters είναι τα honeypots και τα honeynets. Ένα honeynet είναι μια συλλογή από συστήματα -τα honeypots-τα οποία προσποιούνται οτι είναι αληθινοί στόχοι, ώστε να δεχτούν επιθέσεις και τελικά να παραβιαστούν. Τα honeypots παρακολουθούνται ώστε να είναι εφικτή η καταγραφή των ενεργειών των επιτιθέμενων και να γνωστοποιούνται οι τεχνικές και τα εργαλεία τα οποία χρησιμοποίησαν για την εισβολή. Είναι χρήσιμα για να αποσπούν και να μπερδεύουν κάποιον από τα υπόλοιπα μηχανήματα ενός δικτύου, να ειδοποιούν για νέους τρόπους επιθέσεων/ευπαθειών, να παρέχουν ανάλυση σε μεγάλο βάθος του τι έγινε κατά τη διάρκεια μιας επίθεσης αλλά και μετά από αυτή. Τα honeynets σε αντίθεση με τα firewalls που εμποδίζουν τους επιτιθέμενους από το να εισβάλλουν σε ένα δίκτυο, λειτουργούν παθητικά στη συλλογή πληροφοριών για τη δράση των blackhats, χρησιμοποιούνται στον τομέα της πρόληψης, της ανίχνευσης, της συλλογής πληροφοριών, έρευνας και εκπαίδευσης.

6.2 ΤΙ ΕΙΝΑΙ ΤΑ HONEYPOTS

Ένας τρόπος για να εντοπίσουμε καινούργιες ευπάθειες συστημάτων -vulnerabilities-είναι να εγκαταστήσουμε συστήματα σε ένα δίκτυο και να τα παρακολουθούμε, ενώ περιμένουμε ότι κάποια στιγμή θα παραβιαστούν. Αφού τα συστήματα αυτά δεν είναι σχεδιασμένα να έχουν κάποια παραγωγική χρήση, κάθε προσπάθεια για επικοινωνία με αυτά τα συστήματα από το δίκτυο είναι εξορισμού ύποπτη και πρόκειται για προσπάθεια επίθεσης -για παράδειγμα απόπειρα για διείσδυση ή δραστηριότητα worm. Τέτοια συστήματα λέγονται honeypots. Είναι “ιδιαίτερα εποπτευόμενα” υπολογιστικά

συστήματα (φυσικά ή εικονικά) τα οποία σκοπεύουν στο να ανιχνευθούν, να δεχτούν επιθέσεις και να “σπάσουν” τελείως. Η αξία τους καθορίζεται από την πληροφορία που μπορεί να εξαχθεί. Τα ίδια τα συστήματα δεν έχουν κάποια αξία για τον διαχειριστή τους μιας και δεν τρέχουν υπηρεσίες κάποιας αξίας και δεν υπάρχουν πολύτιμα δεδομένα. Μια επίθεση που δεν είναι γνωστή μέχρι στιγμής μπορεί να ανιχνευτεί παρακολουθώντας την κίνηση που φεύγει από το honeypot.

Όταν ένα honeypot παραβιάζεται, μελετάμε τον τρόπο που χρησιμοποιήθηκε για την παραβίαση. Ένα honeypot μπορεί να τρέχει οποιοδήποτε λειτουργικό σύστημα και υπηρεσίες, τα οποία θα καθορίσουν πόσο εύκολα θα σπάσει. Τα honeypots δεν είναι ιδιαίτερα καινούργια ιδέα και χρησιμοποιούνται αρκετό καιρό, ωστόσο η λέξη honeypot είναι καινούργια και εισάγει σε μια νέα μορφή τεχνολογίας που γίνεται ολοένα και πιο σημαντική.

6.3 ΤΙ ΕΙΝΑΙ ΤΑ HONEYNETS

Τα honeynets είναι δίκτυα αποτελούμενα από συστήματα honeypots τα οποία παρακολουθούνται στενά ώστε να μπορούν να εντοπιστούν και να αναλυθούν οι επιθέσεις που δέχονται τα honeypots. Ένα honeynet συνήθως αποτελείται από διαφορετικού τύπου honeypots, δηλαδή συστήματα με διαφορετικές υπηρεσίες και λειτουργικά συστήματα, ώστε να συγκεντρώνονται ταυτόχρονα δεδομένα από διαφορετικά συστήματα αλλά και να αποτελούν ένα περισσότερο αληθοφανές δίκτυο. Μερικές φορές μάλιστα σχεδιάζονται ώστε να αποτελούν ολοκληρωμένα αντίγραφα δικτύων ή παραγωγικών συστημάτων.

Ο στόχος ενός honeynet είναι να συλλέγει δεδομένα από κάθε δυνατή πηγή, ενώ ταυτόχρονα προστατεύει το δίκτυο με το να περιορίζει τις κακόβουλες κινήσεις από τα κατειλημμένα honeypots. Αυτό γίνεται συνήθως με το να εφαρμόζεται κάποιο φίλτρο στον εξωτερικό router για την εξερχόμενη κίνηση, ώστε αν κατειληφθούν το συστήματα και οι επιτιθέμενοι προσπαθήσουν να κάνουν μια επίθεση denial of service πχ σε κάποιο άλλο δίκτυο, να μην είναι εφικτό.

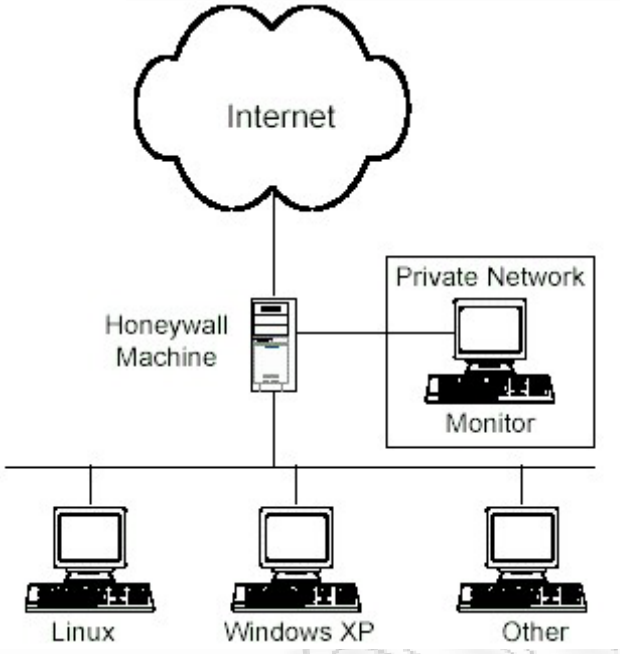
6.4 ΔΙΑΚΡΙΣΕΙΣ HONEYPOTS

Υπάρχουν δυο διακρίσεις για τα διάφορα είδη honeypots: τα φυσικά και τα εικονικά, καθώς επίσης τα υψηλής και τα χαμηλής αλληλεπίδρασης. Ένα φυσικό honeypot είναι ένα πραγματικό μηχάνημα με τη δικιά του ip διεύθυνση. Μπορεί να τρέχει οποιοδήποτε λειτουργικό σύστημα -linux, unix, windows, Mac Os, κτλ-και οποιαδήποτε υπηρεσία του ορίσουμε -πχ www, mysql, ftp .

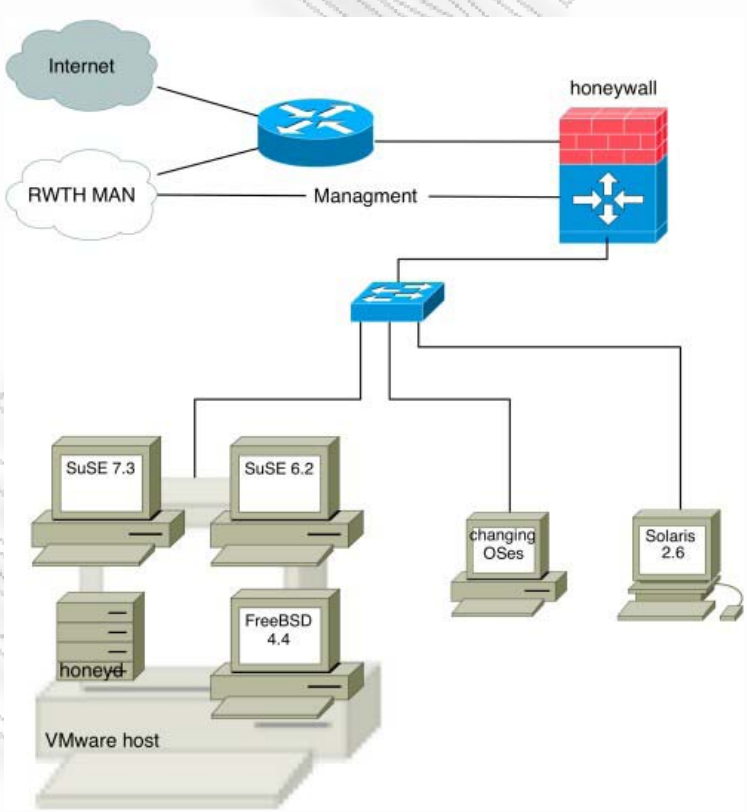
Επιπλέον μπορεί να ρυθμιστεί ένα υπολογιστικό σύστημα να φιλοξενεί μερικά εικονικά μηχανήματα, δεν πρόκειται δηλαδή για πραγματικά μηχανήματα αλλά για προσομοίωση συστημάτων σε κάποιον υπολογιστή. Αυτό προσφέρει πολύ ευκολότερη συντήρηση και λιγότερες φυσικές απαιτήσεις.

Για εικονικά honeypots χρησιμοποιούνται το Vmware [2] ή το user-mode linux [3] . Πρόκειται για λογισμικό που επιτρέπει να τρέχουν περισσότερα από ένα λειτουργικά συστήματα σε ένα μηχάνημα. Με ένα δυνατό σε ισχύ μηχάνημα μπορεί να τρέχουν αρκετά διαφορετικά λειτουργικά συστήματα, το καθένα από τα οποία θα έχει τη δική του ip και μπορούν να δημιουργηθούν ακόμα και αυθαίρετες δικτυακές τοπολογίες. Με διάκριση την αλληλεπίδραση, δηλαδή το βαθμό δραστηριότητας που επιτρέπεται να έχει ένας επιτιθέμενος σε ένα honeypot, μπορούμε να τα διαιρέσουμε σε χαμηλής και υψηλής αλληλεπίδρασης Τα υψηλής αλληλεπίδρασης honeypots παρέχουν ένα ολόκληρο λειτουργικό σύστημα και υπηρεσίες με τις οποίες ο επιτιθέμενος μπορεί να συνδεθεί. Είναι πραγματικοί υπολογιστές με πραγματικές εφαρμογές που οι επιτιθέμενοι μπορούν να παραβιάσουν και να πετύχουν απόλυτο έλεγχο του συστήματος. Αντίθετα τα χαμηλής αλληλεπίδρασης honeypots έχουν περιορισμένες δυνατότητες, καθώς προσομοιώνουν μερικά μόνο μέρη ,πχ τη στοίβα δικτύου. Αυτό που κάνουν είναι να εξομοιώνουν συστήματα και οι δραστηριότητες των επιτιθέμενων περιορίζονται σε αυτό που επιτρέπουν οι εξομοιωμένες υπηρεσίες. Δεν μπορεί να γίνει πλήρες compromise καθώς δεν πρόκειται για πραγματικά συστήματα με πλήρης εφαρμογές.

Ένα εργαλείο για τη δημιουργία χαμηλής αλληλεπίδρασης honeypots είναι το honeyd. Το honeyd είναι ένα μικρό πρόγραμμα το οποίο δημιουργεί virtual hosts σε ένα δίκτυο με το να προσομοιώνει την TCP/IP στοίβα διαφόρων λειτουργικών συστημάτων και μπορεί να ρυθμιστεί να τρέχει υπηρεσίες. Αυτές οι υπηρεσίες είναι συνήθων μικρά scripts που προσομοιώνουν πραγματικές υπηρεσίες όπως το POP3 ή το SMTP. Τα υψηλής αλληλεπίδρασης honeypots μπορούν να καταγράψουν μεγαλύτερη πληροφορία από τα χαμηλής αλληλεπίδρασης. Μπορούν να καταγράψουν ολόκληρη τη σύνδεση του επιτιθέμενου με το σύστημα από τη στιγμή της παραβίασης και μετά, το τι έκανε δηλαδή και πως έγινε αυτό, τι προγράμματα εγκατέστησε στο σύστημα κτλ. Πέρα από αυτό όμως τα υψηλής αλληλεπίδρασης honeypots θέλουν πολύ περισσότερη δουλειά για να στηθούν και να συντηρηθούν. Μιας και πρόκειται για πραγματικά συστήματα, αποτελούν κίνδυνο γιατί οι επιτιθέμενοι μπορεί να τα χρησιμοποιήσουν για να πραγματοποιούν από αυτά τις επιθέσεις τους ή αν βλάψουν άλλα συστήματα. Η δουλειά που πρέπει να γίνει σε αυτά είναι σημαντικά περισσότερη.

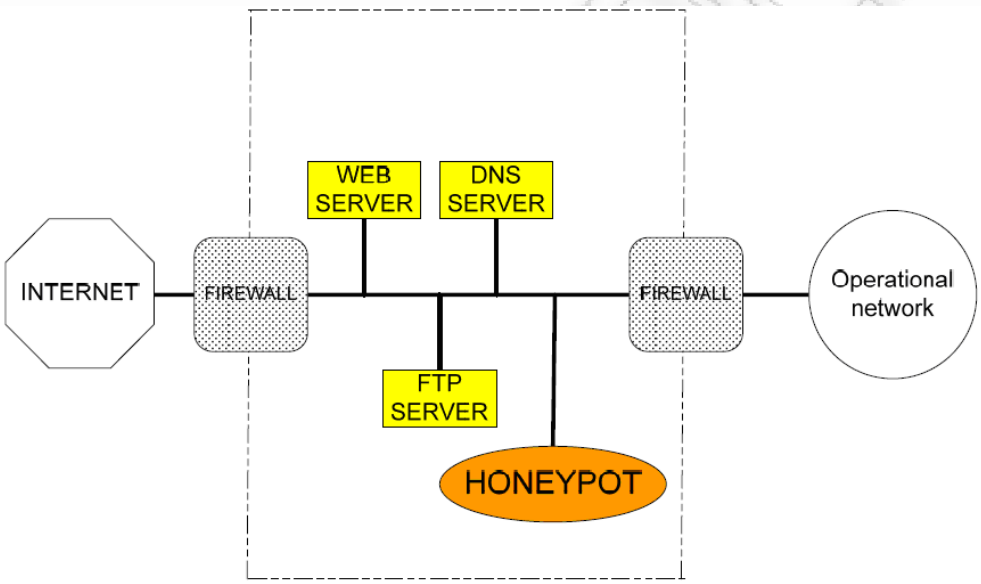


Σχήμα 11 :ένα *δίκτυο honeynet με τρία honeypots*



Σχήμα 12: Honeynet με φυσικούς και virtual hosts

Πιο συγκεκριμένα, υπάρχουν δύο βασικοί τύποι honey pots, τα χαμηλής-αλληλεπίδρασης honey pots και τα υψηλής αλληλεπίδρασης honey pots. Τα πρώτα αναφέρονται στη μίμηση των υπηρεσιών και των λειτουργικών συστημάτων. Είναι πάρα πολύ εύκολο και ασφαλές να εφαρμοστούν. Οι επιτιθέμενοι δεν επιτρέπεται να αλληλεπιδράσουν με το βασικό λειτουργικό σύστημα, αλλά μόνο με συγκεκριμένες υπηρεσίες. Για αυτόν τον λόγω, αυτός ο τύπος honey pots δεν μπορεί να παρέχει λεπτομερείς πληροφορίες για τις ενέργειες του επιτιθέμενου και μπορεί εύκολα να ανιχνευθεί. Παρόλα αυτά μπορούν να ανιχνευθούν προσπάθειες επικοινωνίας προς αχρησιμοποίητες IPs. Σε αυτήν την περίπτωση ένας συναγερμός πυροδοτείτε προειδοποιώντας ότι κάποιος προσπαθεί να επιτεθεί στο δίκτυο. Αλλά τι συμβαίνει εάν η επίθεση δεν κατευθύνεται ενάντια στο υποκατάστατο της υπηρεσίας (emulated service)



Σχήμα 13: Honeypot

Η απάντηση έρχεται από τα honey pots υψηλής αλληλεπίδρασης. Το Honey net δεν είναι μια λύση λογισμικού που μπορεί να εγκατασταθεί σε έναν υπολογιστή αλλά ολόκληρη αρχιτεκτονική, ένα δίκτυο που δημιουργείται για να δεχτεί επίθεση. Μέσα σε αυτό το δίκτυο, κάθε δραστηριότητα καταγράφεται και οι επιτιθέμενοι παγιδεύονται. Κρυπτογραφημένες SSH sessions, ηλεκτρονικό ταχυδρομείο, μεταφορές αρχείων και κάθε πιθανή δράση επιτιθέμενου καταγράφεται. Επιπλέον, μια πύλη Honey wall επιτρέπει την εισερχόμενη κίνηση, αλλά ελέγχει την εξερχόμενη χρησιμοποιώντας τεχνολογίες πρόληψης εισβολής. Αυτό επιτρέπει στον επιτιθέμενο να αλληλεπιδράσει με το Honey net σύστημα, αλλά τον εμποδίζει να βλάψει άλλα συστήματα εκτός Honey net. Μελετώντας τη συλληφθείσα κίνηση οι ερευνητές μπορούν να ανακαλύψουν τις νέες μεθόδους και εργαλεία και μπορούν να κατανοήσουν πλήρως τις τακτικές των επιτιθέμενων. Παρόλα αυτά, τα συστήματα Honey net είναι πιο πολύπλοκα στην εγκατάσταση ή την

εφαρμογή και ο κίνδυνος αυξάνεται καθώς οι επιτιθέμενοι αλληλεπιδρούν με πραγματικά λειτουργικά συστήματα και όχι με υποκατάστατα. Αλλά τι θα μπορούσε να συμβεί εάν κάποιος είχε «καταλάβει» ένα τέτοιο σύστημα; Οι συνέπειες θα ήταν καταστρεπτικές.

6.5 ΤΕΧΝΙΚΕΣ ΦΙΛΤΡΑΡΙΣΜΑΤΟΣ ΔΙΑΔΡΟΜΗΣ

Διαφορετικές προτάσεις σχετικά με την υπεράσπιση ενάντια στις επιθέσεις DDoS προέρχονται από την κοινότητα του Border Gateway Protocol. Όταν τα πρωτόκολλα δρομολόγησης σχεδιάστηκαν, οι υπεύθυνοι για την ανάπτυξή τους δεν εστίασαν την προσοχή τους στην ασφάλεια, αλλά στην οικοδόμηση μηχανισμών που καλύπτουν αποτελεσματικούς μηχανισμούς δρομολόγησης και αποφεύγουν τους βρόχους στη δρομολόγηση. Στην αρχή, οι επιτιθέμενοι άρχισαν να στρέφονται ενάντια στους δρομολογητές. Αποκτώντας πρόσβαση σε έναν δρομολογητή θα μπορούσαν να κατευθύνουν την κίνηση πάνω από επιβαρυμένες ζεύξεις, να δουν κρίσιμα στοιχεία, και να τα τροποποιήσουν. Η κρυπτογραφημένη πιστοποίηση της αυθεντικότητας ήρθε να μετριάσει αυτές τις απειλές. Λόγω της γειτονικής πιστοποίησης της αυθεντικότητας, η ενημέρωση των πινάκων δρομολόγησης προέρχεται από πηγή εμπιστοσύνης και δεν υπάρχει πιθανότητα κάποιος να μπορεί να δώσει στους δρομολογητές άκυρες πληροφορίες δρομολόγησης, προκειμένου να «καταλάβει» ένα δίκτυο. Από την άλλη πλευρά, τα φίλτρα δρομολόγησης είναι απαραίτητα για την παρεμπόδιση κρίσιμων διαδρομών και υποδικτύων από το να διαφημιστούν και υπόπτων διαδρομών από το να ενσωματωθούν στους πίνακες δρομολόγησης. Με αυτόν τον τρόπο, οι επιτιθέμενοι δεν ξέρουν τη διαδρομή προς κρίσιμους servers και ύποπτες διαδρομές δεν χρησιμοποιούνται.

Δύο άλλες τεχνικές φιλτραρίσματος διαδρομών, η black hole δρομολόγηση και η sinkhole δρομολόγηση, μπορούν να χρησιμοποιηθούν, όταν το δίκτυο δέχεται επίθεση. Αυτές οι τεχνικές προσπαθούν να μετριάσουν προσωρινά τον αντίκτυπο της επίθεσης. Η πρώτη αναφέρεται στη δρομολόγηση κίνησης σε μια μηδενική διεπαφή, όπου τελικά απορρίπτεται. Με μια πρώτη ματιά, θα ήταν τέλειο να οδηγείται η κακόβουλη κίνηση σε μια μαύρη τρύπα (blackhole). Αλλά είναι πάντα δυνατό να απομονωθεί η κακόβουλη από τη νόμιμη κίνηση; Εάν το θύμα ξέρει ακριβώς τα IPs που του επιτίθενται, τότε μπορεί να αγνοήσει την κίνηση που προέρχεται από αυτές τις πηγές. Με αυτόν τον τρόπο, ο αντίκτυπος της επίθεσης περιορίζεται δεδομένου ότι το θύμα δεν καταναλώνει χρόνο της CPU ή μνήμη σαν συνέπεια της επίθεσης. Μόνο εύρος ζώνης του δικτύου καταναλώνεται. Παρόλα αυτά, εάν τα IPs των επιτιθέμενων δεν μπορούν να διακριθούν και όλη η κίνηση οδηγείται στη μαύρη τρύπα, τότε και η νόμιμη κίνηση απορρίπτεται επίσης. Στην περίπτωση αυτή, αυτή η τεχνική φιλτραρίσματος αποτυγχάνει.

Η τεχνική δρομολόγησης sinkhole αναφέρεται στη δρομολόγηση ύποπτης ή όχι κίνησης σε μια έγκυρη διεύθυνση IP όπου η κίνηση μπορεί να αναλυθεί. Εκεί, εάν η κίνηση αποδειχθεί κακόβουλη, απορρίπτεται (δρομολογείται σε μια μηδενική διεπαφή), διαφορετικά δρομολογείται στον επόμενο κόμβο (hop). Ένα sniffer στο δρομολογητή sinkhole μπορεί να συλλάβει την κίνηση και να την αναλύσει. Αυτή η τεχνική δεν είναι τόσο αυστηρή όσο η προηγούμενη. Η

αποτελεσματικότητα κάθε μηχανισμού εξαρτάται από τη δύναμη της επίθεσης. Συγκεκριμένα, το sink holing δεν μπορεί να αντιδράσει σε μια άγρια επίθεση τόσο αποτελεσματικά όσο το black holing. Εντούτοις είναι μια πιο περίπλοκη τεχνική, δεδομένου ότι είναι πιο επιλεκτική στην απόρριψη της κίνησης.

Σύμφωνα με τα παραπάνω, το φιλτράρισμα της κακόβουλης κίνησης φαίνεται να είναι ένα αποτελεσματικό αντίμετρο ενάντια στις DDoS επιθέσεις. Μάλιστα, όσο πιο κοντά στον επιτιθέμενο εφαρμόζεται το φιλτράρισμα, τόσο πιο αποτελεσματικό είναι. Αυτό είναι φυσικό, γιατί όταν η κίνηση φιλτράρεται από το θύμα, τότε το θύμα "επιβιώνει", αλλά το δίκτυο του ISP έχει ήδη πλημμυρίσει. Συνεπώς, η καλύτερη λύση θα ήταν να φιλτράρεται η κίνηση στην πηγή της, το οποίο σημαίνει φιλτράρισμα της κίνησης των zombies.

Μέχρι τώρα, τρεις δυνατότητες φιλτραρίσματος έχουν αναφερθεί με κριτήριο το αντικείμενο φιλτραρίσματος. Η πρώτη αναφέρεται σε φιλτράρισμα με βάση τη διεύθυνση προέλευσης. Αυτή θα ήταν η καλύτερη μέθοδος φιλτραρίσματος, εάν κάθε φορά ξέραμε ποιος είναι ο επιτιθέμενος. Παρόλα αυτά, αυτό δεν είναι πάντα δυνατό καθώς οι επιτιθέμενοι συνήθως χρησιμοποιούν αλλοιωμένες διευθύνσεις IP. Επιπλέον οι επιθέσεις DDoS προέρχονται συνήθως από χιλιάδες zombies και έτσι κάνουν πάρα πολύ δύσκολη την ανακάλυψη όλων των διευθύνσεων IP που πραγματοποιούν την επίθεση. Κι αν ακόμη όλες αυτές οι IPs ανακαλυφθούν, η εφαρμογή ενός φίλτρου που θα απορρίπτει μερικές χιλιάδες IPs είναι πρακτικά αδύνατη να εφαρμοστεί.

Η δεύτερη δυνατότητα φιλτραρίσματος είναι φιλτράρισμα της υπηρεσίας. Αυτή η τακτική προϋποθέτει ότι εμείς ξέρουμε το μηχανισμό της επίθεσης. Σε αυτήν την περίπτωση, μπορούμε να φιλτράρουμε την κίνηση προς μια συγκεκριμένη πόρτα UDP ή μια σύνδεση TCP ή να φιλτράρουμε τα ICMP μηνύματα. Αλλά τι κάνουμε εάν η επίθεση κατευθύνεται προς μια πολύ κοινή πόρτα ή υπηρεσία; Τότε πρέπει ή να απορρίψουμε κάθε πακέτο (ακόμη και εάν είναι νόμιμο) ή να υπομείνουμε την επίθεση.

Τέλος, υπάρχει η δυνατότητα φιλτραρίσματος με βάση τη διεύθυνση προορισμού. Οι DDoS επιθέσεις κατευθύνονται συνήθως ενάντια σε έναν περιορισμένο αριθμό θυμάτων. Έτσι φαίνεται να είναι εύκολο να απορριφθεί όλη η κίνηση που κατευθύνεται προς αυτούς. Αλλά αυτό σημαίνει ότι η νόμιμη κίνηση απορρίπτεται επίσης. Σε περίπτωση μιας επίθεσης μεγάλης κλίμακας αυτό δεν πρέπει να είναι πρόβλημα δεδομένου ότι το θύμα σύντομα θα καταρρεύσει και δεν θα είναι σε θέση να εξυπηρετήσει κανένα. Έτσι το φιλτράρισμα προστατεύει το θύμα από την κατάρρευση κρατώντας το απλά απρόσιτο από τους υπόλοιπους.

6.6 ΥΒΡΙΔΙΚΕΣ ΜΕΘΟΔΟΙ ΚΑΙ ΚΑΤΕΥΘΥΝΤΗΡΙΕΣ ΓΡΑΜΜΕΣ

Σήμερα οι ερευνητές προσπαθούν να συνδυάσουν τα πλεονεκτήματα από όλες τις παραπάνω μεθόδους προκειμένου να καταπιέσουν τα μειονεκτήματά τους. Ως αποτέλεσμα, διάφοροι μηχανισμοί που εφαρμόζουν δύο ή περισσότερες από τις ανωτέρω τεχνικές έχουν προταθεί προκειμένου να μετριαστεί ο αντίκτυπος των επιθέσεων DDoS. Η καλύτερη λύση στο DDoS πρόβλημα φαίνεται να είναι η ακόλουθη: το θύμα πρέπει να ανιχνεύσει το

συντομότερο δυνατό ότι δέχεται επίθεση. Τότε πρέπει να εντοπίσει (trace back) τα IPs που προκαλούν αυτήν την επίθεση και να προειδοποιήσει τους administrators των zombies για το γεγονός ότι συμμετέχουν σε μια επίθεση. Σε αυτήν την περίπτωση, η επίθεση αντιμετωπίζεται αποτελεσματικά. Παρόλα αυτά, σύμφωνα με τα παραπάνω αυτό είναι προς το παρόν αδύνατο. Η έλλειψη ενός 100% αποτελεσματικού εργαλείου υπεράσπισης επιβάλλει την ανάγκη της ιδιωτικής επιφυλακής. Κάθε χρήστης πρέπει να φροντίσει για την ασφάλειά του. Μερικές βασικές προτάσεις είναι:

Αποτροπή της εγκατάστασης εργαλείων κατανεμημένων επιθέσεων στα συστήματά μας. Αυτός θα βοηθήσει στον περιορισμό του στρατού των zombies. Υπάρχουν διάφορες ενέργειες που το άτομο μπορεί να εκτελέσει. Αρχικά, πρέπει να διατηρεί τα πρωτόκολλα και τα λειτουργικά συστήματα ενημερωμένα (up-to-date). Με την εξάλειψη του αριθμού των αδυναμιών του συστήματός μας αποτρέπουμε την εκμετάλλευσή του από επιτήδειους και την έκθεσή του σε κίνδυνο.

Χρησιμοποίηση αντιπυρικών ζωνών (firewalls) στους gateways (πύλες) προκειμένου να φιλτραριστεί η εισερχόμενη και η εξερχόμενη κίνηση. Δεν είναι λογικό να υπάρχουν εισερχόμενα πακέτα με διεύθυνση IP πηγής που ανήκει στο υποδίκτυο και εξερχόμενα πακέτα με διεύθυνση IP πηγής που δεν ανήκει στο υποδίκτυο.

Εφαρμογή IDS συστημάτων (συστήματα ανίχνευσης εισβολής) προκειμένου να ανιχνευθούν οι τακτικές των επιθέσεων. Εφαρμογή anti-virus προγραμμάτων προκειμένου να ανιχνευθεί ο κακόβουλος κώδικας στο σύστημά μας.

6.7 ΕΡΓΑΛΕΙΑ

Αρχικά στήνεται ένα δίκτυο με υπολογιστές που τρέχουν διάφορα λειτουργικά συστήματα, πχ linux, windows, mac κτλ. Τα συστήματα αυτά μπορεί να είναι φυσικά είτε εικονικά. Ο αριθμός τους μπορεί να είναι από δυο-τρια μέχρι πολύ περισσότερα. Τα συστήματα αυτά συνήθως ρυθμίζονται να τρέχουν πολλές υπηρεσίες -web, ftp, sql κτλ-ώστε να υπάρχουν πολλά σημεία εισόδου για το σύστημα. Η καταγραφή των συμβάντων και των επιθέσεων γίνεται με τους εξής τρόπους:

1. Από τα log του firewall βλέπουμε ποιες συνδέσεις έγιναν και μπορούμε να μάθουμε πότε ξεκίνησε μια συγκεκριμένη σύνδεση.
2. Από τα log που αφήνουν οι υπηρεσίες, για παράδειγμα logs από τον apache web server, ή απο τον iis.

Με χρήση κάποιου συστήματος IDS, όπως το snort παίρνουμε αυτόματα ειδοποιήσεις όταν συμβαίνουν επιθέσεις. Υπάρχουν διάφορα εργαλεία και front-ends που χρησιμοποιούνται σε συνδυασμό με το snort για να γίνεται πιο αποδοτική η ανάλυση των logs

Από το αρχείο με τη δικτυακή κίνηση που κατέγραψε κάποιο sniffer το οποίο τρέχει στο δίκτυο. Το sniffer μπορεί να είναι το tcpdump ή οποιοδήποτε άλλο sniffer αλλά όπως θα δούμε στο κεφάλαιο 5 μπορεί να είναι και το ίδιο το snort.

Στο linux υπάρχει η δυνατότητα να παρακολουθήσουμε το τι έκανε ο επιτιθέμενος στο σύστημα αφότου απόκτησε πρόσβαση με το να εγκαταστήσουμε λογισμικό που πιάνει τις πληκτρολογήσεις του. Το πιο γνωστό εργαλείο που χρησιμοποιείται για τη δουλειά αυτή είναι το Sebek. Το sebek λειτουργεί ως client/server σύστημα, τρέχει στο honeypot που μας ενδιαφέρει και στέλνει τα δεδομένα σε κάποιο δικό μας server μέσω του syslog, ώστε ένας επιτιθέμενος να μην μπορεί να αντιληφθεί την ύπαρξη του. Το sebek μπορεί έτσι να πιάνει τη δραστηριότητα του επιτιθέμενου στο σύστημα, το τι προσπαθεί να κάνει σε άλλα συστήματα, καθώς επίσης και τα διάφορα αρχεία που κατεβάζει. Εφόσον το sebek εγκαθίσταται στο σύστημα, μπορεί να καταγράψει μια σύνδεση ssh, την οποία το ids δεν μπορεί να καταλάβει.

6.8 THE GLOBAL HONEYNET PROJECT

Ιδρυμένο το 1999, το Honeynet Project [1] είναι μια μη κερδοσκοπική ερευνητική οργάνωση στην οποία επαγγελματίες της ασφάλειας κάνουν έρευνα στον τομέα της ασφάλειας υπολογιστών. Το honeynet project είναι ένα group επαγγελματιών ερευνητών της ασφάλειας IT που στήνουν δίκτυα honeynets στο internet και παρακολουθούν πως παραβιάζονται με σκοπό να μάθουν τα εργαλεία, τις τακτικές και τα κίνητρα των δικτυακών εισβολέων και των blackhats και να τα διαθέσουν τη γνώση στο διαδίκτυο ελεύθερα για όλους. Ο όρος blackhat χρησιμοποιείται για να περιγράψει έναν επιτιθέμενο ο οποίος χρησιμοποιεί τις δυνατότητες του για μη ηθικούς ή καταστροφικούς σκοπούς.

Εισηγητής του καινούργιου αυτού όρου περιγραφής τέτοιων συστημάτων αλλά και ιδρυτής του honeynet project είναι ο Lance Spitzner. Στο honeynet project συμμετέχουν πολλοί διάσημοι ερευνητές αλλά και hackers, όπως οι George Kurtz (Foundstone), Elias Levy (securityfocus.com), Dug Song (dsniff writer), Fyodor (nmap writer), Jay Beale (Bastille linux), Rain Forest Puppy και άλλοι, ενώ τα ενεργά honeynet projects αυτή τη στιγμή είναι τα εξής:

Chinese Honey net Project, The Spanish Honey net Project, SIG^2 Internet Weather Forecast Centre, German Honey net Project, Portugal Honey net Project, Ga Tech Honey net Project, French Honey net Project, Italian Honey net Project, Pakistan Honey net Project, West Point Honeynet Project, UK Honey net Project, Honey net Project at the University of Texas at Austin, Brazilian Honey net Project, Azusa Pacific University Honeynet, Net Forensics Honey net, Internet Systematic Lab Honey net Project – Greece, Paladion Networks Honeynet Project – India, Norwegian Honeynet Project, Florida Honey Net Project.

Φυσικά, πέρα απο τα επίσημα honeynets του honeynet project υπάρχουν και τα πολύ περισσότερα honeypots και honeynets που έχουν στηθεί απο επιχειρήσεις και οργανισμούς για να ενημερώσουν τους υπαλλήλους τους, αλλά και κυρίως για να έχουν εικόνα του τι συμβαίνει στο δίκτυο τους. Οι στόχοι του project αναλυτικά είναι οι εξής:

6.8.1 Να ευαισθητοποιήσει σε θέματα ασφάλειας δικτύων

Το project στοχεύει στο να ενημερώσει τους χρήστες του internet για τους κινδύνους και τις απειλές που υπάρχουν σήμερα. Αυτό το καταφέρνει με το να στήνει πραγματικά δίκτυα και να μελετάει πως αυτά παραβιάζονται από πραγματικούς επιτιθέμενους. Όλα τα αποτελέσματα από την έρευνα δημοσιεύονται στο internet ώστε να μπορεί να τα δει οποιοσδήποτε, ενώ είναι γραμμένα σε κατανοητή γλώσσα ακόμα και για αρχαρίους και περιέχουν πολλές λεπτομέρειες. Οι περισσότεροι χρήστες του internet δεν γνωρίζουν για τους κινδύνους που αντιμετωπίζουν. Μάλιστα, πολλές φορές δεν ξέρουν ότι το σύστημα τους είναι ήδη παραβιασμένο! Ένας επιτιθέμενος τις περισσότερες φορές και ανάλογα με το επίπεδο του, θα προσπαθήσει να καλύψει τα ίχνη της παραβίασης ώστε να συνεχίσει να έχει πρόσβαση. Επιπλέον, τα περισσότερα σημερινά λειτουργικά συστήματα σε μια default εγκατάσταση έρχονται με ήδη υπάρχοντα προβλήματα ασφάλειας. Μέχρι να κάνει τις απαραίτητες ενέργειες ο χρήστης για να τα ασφαλίσει, πχ μέχρι να κατεβάσει και να εγκαταστήσει κάποιο patch, το σύστημα μπορεί να παραβιαστεί και να μην το καταλάβει ο χρήστης. Τα honeynets βοηθάνε στην ευαισθητοποίηση σε θέματα ασφάλειας με το να κάνουν ορατούς αυτούς τους κινδύνους. Πολλές φορές οι χρήστες υπολογιστών ξεγέλιουνται νομίζοντας ότι κανείς δεν θα προσέξει το σύστημα τους και δεν θα θελήσει να ασχοληθεί με αυτό. Το honeynet project έχει αποδείξει ότι ένα σύστημα που τρέχει την default εγκατάσταση του λογισμικού του συστήματος και συνδέεται με το internet, θα δεχτεί πολλαπλά scans και τελικά θα παραβιαστεί μετά από κάποιο χρόνο.

6.8.2 Έρευνα σε παλιές αλλά και καινούργιες τεχνικές

Τα honeynets παρέχουν την τεχνολογία και τις μεθόδους για να συγκεντρώνεται πληροφορία για τις επιθέσεις στο διαδίκτυο. Η ανάλυση των δεδομένων που συγκεντρώθηκαν μπορεί να βοηθήσει τους administrators να προστατεύσουν καλύτερα το δίκτυο τους. Με την ανάλυση της συμπεριφοράς ενός επιτιθέμενου, μπορούμε να καταλάβουμε πως έγινε η επίθεση, ποια ήταν τα κίνητρα, πως επιχείρησε να χρησιμοποιήσει το σύστημα μας και τι προσπάθησε να κάνει. Μιας και οι συνδέσεις που γίνονται καταγράφονται, τα συστήματα honeypots επίσης μπορούν να πιάσουν κάποιο νέο τύπο επίθεσης, που δεν είναι γνωστός μέχρι στιγμής.

6.8.3 Ενεργός δικτυακή προστασία

Τα honeynets μπορούν επίσης να αποτελέσουν μέρος της προστατευτικής υποδομής ενός δικτύου, γιατί μπορούν να μπερδέψουν τους επιτιθέμενους και να τους αποθαρρύνουν από το να συνεχίσουν τη διείσδυση στο δίκτυο. Επίσης, τα honeypots μπορούν να μας ειδοποιούν για τα μολυσμένα συστήματα στο δίκτυο μας, περίπτωση που αναλύεται σε επόμενο κεφάλαιο. Αυτό ισχύει επειδή μιας και τα honeypots δεν έχουν παραγωγική χρήση, όλες οι συνδέσεις είναι εξορισμού ύποπτες και δεν υπάρχουν τα false positives που θα βγάλει κάποιο ids. Σε ορισμένες περιπτώσεις τα honeypots μας ειδοποιούν για τα μολυσμένα συστήματα στο δίκτυο μας πολύ εγκυρότερα από τα ids. Έτσι μπορούμε να ειδοποιήσουμε τους διαχειριστές των συστημάτων αυτών για να διορθώσουν τα κενά στην ασφάλεια τους. Τέλος η τεχνολογία bait'n'switch αν και ελάχιστα χρησιμοποιείται σήμερα, αξίζει να τη δούμε αναλυτικότερα: Το bait'n'switch πραγματοποιείται σαν μια προέκταση του snort. Όποτε μια επιτυχημένη επίθεση εντοπίζεται ότι συμβαίνει, το ids φιλτράρει την επίθεση και η κίνηση του επιτιθέμενου προωθείται σε ένα σύστημα όμοιο με αυτό που δέχτηκε την επίθεση. Τη διαδικασία αυτή δεν την καταλαβαίνει ο επιτιθέμενος. Έτσι το πραγματικό σύστημα προστατεύεται από την επίθεση και η αλληλεπίδραση του επιτιθέμενου με το honeypot σύστημα μπορεί να μελετηθεί περισσότερο. Το σύστημα βέβαια αντιδρά μόνο σε επιθέσεις για τις οποίες έχει κανόνες ανανεωμένους.

6.8.4 Εκπαίδευση πάνω στην ασφάλεια

Ένα δίκτυο με honeypots μπορεί να χρησιμοποιηθεί από άτομα που θέλουν να μελετήσουν στην πράξη πώς συμβαίνουν οι δικτυακές επιθέσεις, μέσα από ένα ρεαλιστικό περιβάλλον και χωρίς τους κινδύνους της παραβίασης παραγωγικών συστημάτων. Έτσι τα άτομα αυτά μπορούν να αναλύσουν τα δεδομένα από τις επιθέσεις. Σε κάποια πανεπιστήμια ήδη χρησιμοποιούνται honeynets για τη διδασκαλία μαθημάτων ασφάλειας δικτύων.

6.8.5 Προβλήματα που πιθανόν να προκύψουν από ένα honeynet

Πέρα από τα πλεονεκτήματα που προσφέρει η εγκατάσταση honeypots και honeynets, πρέπει να ληφθούν υπόψη και τα προβλήματα που μπορεί να δημιουργήσουν, ώστε να γίνει σωστή αποτίμηση των πλεονεκτημάτων και μειονεκτημάτων στο περιβάλλον όπου σκοπεύει να γίνει η εγκατάσταση. Το να μπουν σε ένα δίκτυο honeypots σημαίνει ότι προστίθενται συστήματα με χαλαρή ασφάλεια ή και καθόλου ασφαλισμένα, έτσι ολόκληρη η ασφάλεια του δικτύου πιθανόν να κινδυνεύει. Επιπλέον, για όποιες παραβιάσεις γίνουν με τα honeypots σαν ενδιάμεσα σημεία (jumping points) για τους επιτιθέμενους, ο υπεύθυνος του δικτύου μπορεί να αντιμετωπίσει νομικά προβλήματα. Στη σελίδα του honeynet project πάντως υπάρχει άφθονο υλικό για το στήσιμο

ενός δικτύου με διακριτές περιοχές και υποδίκτυα, ώστε η παραβίαση των honeypots -που είναι άλλωστε και ο στόχος να μην δημιουργεί προβλήματα στο υπόλοιπο δίκτυο. Επίσης είναι σημαντικό ότι περιορίζονται αυστηρά οι πόροι των honeypots προς τα έξω, όπως η εξερχόμενη κίνηση . Έτσι αποτρέπεται ένα honeypot απο το να χρησιμοποιηθεί για denial of service σε εξωτερικά συστήματα ή να πραγματοποιήσει επιθέσεις. Ενδιαφέρει μόνο η αλληλεπίδραση με τον επιτιθέμενο και να μάθουμε τι προσπαθεί να κάνει και όχι απαραίτητα να το κάνει! Η παρακολούθηση των κινήσεων του επιτιθέμενου χωρίς τη γνώση του είναι ένα δύσκολο θέμα από την πλευρά ηθικής αλλά και για νομικούς λόγους. Η νομοθεσία που ισχύει στις ΗΠΑ, μια από τις πιο αυστηρές νομοθεσίες παγκοσμίως (ιδιαίτερα από 11/9 και μετά, με το “ανατριχιαστικό” Patriot act) ορίζει ως παγίδευση το εξής: “ένα άτομο παγιδεύεται όταν ωθείται ή παραπλανείται από τις δυνάμεις του νόμου να διαπράξει ένα έγκλημα το οποίο δε σκόπευε να κάνει”. Ο ορισμός τίποτα δεν έχει να κάνει με τις ενέργειες και τους στόχους του honeynet project. Η ομάδα δεν ενεργεί κάτω από τον έλεγχο του νόμου και κυρίως δεν έχει σαν στόχο την καταδίκη των επιτιθέμενων. Τα honeynets σχεδιάζονται να μοιάζουν με πραγματικά, παραγωγικά συστήματα και καμιά κίνηση δεν γίνεται για να πείσουν επιτιθέμενους να τους επιτεθούν. Αντίθετα, οι επιτιθέμενοι είναι αυτοί που εντοπίζουν και επιτίθενται στα συστήματα αυτά. Τα honeypots παρακολουθούνται όχι για να εντοπιστούν οι επιτιθέμενοι, αλλά για να μελετηθούν οι κινήσεις τους, οι τρόποι που πραγματοποιούν μια επίθεση και τα εργαλεία τους, ώστε να υπάρχει η γνώση για να μπορούν να αποτραπούν στα πραγματικά συστήματα.

7

ΚΕΦΑΛΑΙΟ

<< Επίθεση SYN FLOOD >>

- **Επιθέσεις SYN FLOOD**
- **Αδυναμία Του TCP**
- **Η Επίθεση**
- **Εισαγωγή στο Μηχανισμό Ανίχνευσης**

7 ΕΠΙΘΕΣΗ SYN FLOOD

7.1 ΕΙΣΑΓΩΓΗ

Το IP δεν παρέχει μέσα που να διαβεβαιώνουν ότι τα δεδομένα έφθασαν στον προορισμό τους και μάλιστα ότι έφθασαν εκεί άθικτα. Αυτό καθιστά το IP αναξιόπιστο ως μηχανισμό μεταφοράς. Δεδομένου ότι στην καθημερινότητα η αξιοπιστία αποδεικνύεται μερικές φορές απαραίτητη, εμφανίστηκε το TCP. Το TCP, ή Πρωτόκολλο Ελέγχου Μετάδοσης, είναι ένα αξιόπιστο πρωτόκολλο μεταφοράς το οποίο παρέχει αριθμούς ακολουθίας για τη διάταξη των πακέτων, μηνύματα ACK για την επιβεβαίωση της παραλαβής μηνυμάτων, παράθυρα συμφόρησης για τον έλεγχο ροής, και μηνύματα NACK για περιστασιακά προβλήματα, εάν βέβαια προκύψει κάποιο. Το TCP εξασφαλίζει ότι αμφότερα τα συμβαλλόμενα μέρη που συμμετέχουν στην επικοινωνία γνωρίζουν την κατάσταση της μεταφοράς δεδομένων. Το TCP μπορεί να θεωρηθεί ως μηχανή πεπερασμένων καταστάσεων, με καταστάσεις ανάλογα με τα χαρακτηριστικά της σύνδεσης.

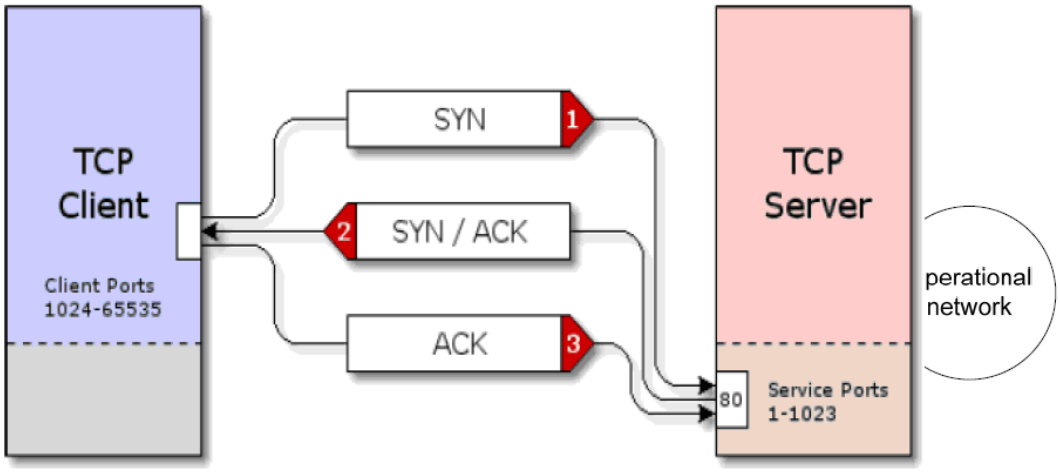
7.2 ΑΔΥΝΑΜΙΑ ΤΟΥ TCP

Για να μπορέσουμε να μελετήσουμε και να καταλάβουμε τους μηχανισμούς που διέπουν μια κατανεμημένη επίθεσης άρνησης υπηρεσιών (DDoS attack), η οποία εκμεταλλεύεται τις αδυναμίες του πρωτοκόλλου TCP, χρειάζεται να κατανοήσουμε πρώτα τη λειτουργία του TCP πρωτοκόλλου (Transmission Control Protocol), το οποίο χρησιμοποιείται για να συνδέσει απομακρυσμένους hosts μέσω του Διαδικτύου.

Όταν δύο hosts θελήσουν να κατευθύνουν και να στείλουν πακέτα δεδομένων ο ένας στον άλλο, διαπραγματεύονται πρώτα από όλα μια "συμφωνία σύνδεσης" (connection agreement). Το αποτέλεσμα της επιτυχούς διαπραγμάτευσής τους είναι μια "Εικονική σύνδεση TCP". Τα μεμονωμένα πακέτα TCP περιέχουν "flag bits" τα οποία διευκρινίζουν το περιεχόμενο και το σκοπό κάθε πακέτου. Παραδείγματος χάριν, ένα πακέτο με το "SYN" flag bit (bit συγχρονισμού) ενεργοποιημένο αρχίζει μια σύνδεση από τον αποστολέα του πακέτου προς τον παραλήπτη. Ένα πακέτο με το "ACK" flag bit (bit επιβεβαίωσης) ενεργοποιημένο επιβεβαιώνει την παραλαβή των πληροφοριών από τον παραλήπτη.

Ένα πακέτο με το "FIN" flag bit (bit τερματισμού) ενεργοποιημένο ολοκληρώνει τη σύνδεση από τον αποστολέα προς τον παραλήπτη.

Η δημιουργία μιας σύνδεσης TCP απαιτεί βασικά την ανταλλαγή τριών πακέτων μεταξύ των δύο μηχανών που πρόκειται να συνδεθούν η οποία είναι γνωστή ως TCP τριμερής χειραψία. Παρακάτω φαίνεται πως λειτουργεί η ανταλλαγή αυτή:



Σχήμα 14: Η τριμερής χειραψία

SYN: Ένας πελάτης TCP (όπως ένας web browser, ένας πελάτης FTP, κ.λ.π....) αρχίζει μια σύνδεση με έναν TCP εξυπηρετητή στέλνοντας ένα "SYN" πακέτο στον TCP εξυπηρετητή. Όπως φαίνεται στο παραπάνω σχήμα, το πακέτο SYN στέλνεται συνήθως από το port του πελάτη, που αριθμείται μεταξύ 1024 και 65535, στο port του εξυπηρετητή, που αριθμείται μεταξύ 1 και 1023. Προγράμματα πελατών που τρέχουν στη μηχανή του πελάτη ζητούν από το λειτουργικό σύστημα "να τους αναθέσει ένα port" για να συνδεθούν με έναν απομακρυσμένο εξυπηρετητή. Το σύνολο αυτών των ports, δηλαδή το σύνολο των ports μεταξύ 1024 και 65535 είναι γνωστό ως "σύνολο πελάτη" ή "εφήμερο σύνολο". Ομοίως, τα προγράμματα εξυπηρετητών που τρέχουν στη μηχανή των εξυπηρετητών ζητούν από το λειτουργικό τους σύστημα να έχουν το προνόμιο "του ακούσματος (listening)" της εισερχόμενη κυκλοφορία στους συγκεκριμένους αριθμούς ports. Έτσι, τα ports μεταξύ 1 και 1023 είναι γνωστά ως "ports υπηρεσιών". Παραδείγματος χάριν, το πρόγραμμα ενός web server αφουγκράζεται συνήθως τα εισερχόμενα πακέτα στο port 80 της μηχανής του, και οι web browsing πελάτες στέλνουν τα πακέτα τους στο port 80 των απομακρυσμένων web servers.Στο σημείο αυτό θα πρέπει να σημειωθεί ότι εκτός από τους αριθμούς ports πηγής και προορισμού, κάθε πακέτο περιέχει επίσης την IP διεύθυνση της μηχανής όπου δημιουργήθηκε το πακέτο (η πηγή IP) και την IP διεύθυνση της μηχανής στην οποία οι δρομολογητές του Διαδικτύου θα διαβιβάσουν το πακέτο (ο προορισμός IP). SYN/ACK: Όταν ένα πακέτο SYN (αίτηση σύνδεσης) παραλαμβάνεται σε ένα ανοιχτό "TCP port υπηρεσιών", το λειτουργικό σύστημα του εξυπηρετητή απαντά με ένα πακέτο "αποδοχής-σύνδεσης", δηλαδή με ένα πακέτο "SYN/ACK".

Αν και οι TCP συνδέσεις είναι διπλής κατευθύνσεως (full duplex), κάθε κατεύθυνση της σύνδεσης οργανώνεται και ρυθμίζεται ανεξάρτητα. Για το λόγο αυτό, ένας εξυπηρετητής TCP απαντά στο πακέτο SYN του πελάτη επιβεβαιώνοντας (Acknowledge) το πακέτο αυτό και στέλνοντας και αυτός με τη σειρά του το δικό του SYN πακέτο για να αρχίσει μια σύνδεση και στην κατεύθυνση επιστροφής. Τα δύο αυτά μηνύματα περικλείονται σε ένα ενιαίο πακέτο απόκρισης, το "SYN/ACK" πακέτο.

Ο παραλήπτης του πακέτου SYN στέλνει πίσω στον αποστολέα το πακέτο απόκρισης SYN/ACK , ανταλλάσοντας τις IP διευθύνσεις πηγής και προορισμού από το πακέτο SYN και τοποθετώντας τις στο πακέτο SYN/ACK. Η διαδικασία αυτή τοποθετεί στη διεύθυνση προορισμού του SYN/ACK πακέτου την IP διεύθυνση πηγής του SYN πακέτου, πράγμα το οποίο είναι ακριβώς αυτό που θέλουμε.

Στο σημείο αυτό θα πρέπει να σημειωθεί ότι στο παράδειγμα που παρουσιάστηκε παραπάνω, ενώ το πακέτο του πελάτη εστάλη στο "port υπηρεσιών" 80 του εξυπηρετητή, η απάντηση του εξυπηρετητή επιστρέφεται από το ίδιο "port υπηρεσιών", δηλαδή το port 80. Με άλλα λόγια, όπως ακριβώς ανταλλάσσονται οι IP διευθύνσεις πηγής και προορισμού στο πακέτο απόκρισης, το ίδιο συμβαίνει και με τα ports πηγής και προορισμού.

Η λήψη του πακέτου SYN/ACK από τον πελάτη επιβεβαιώνει την προθυμία του εξυπηρετητή να γίνει αποδεκτή η σύνδεση του πελάτη. Επιβεβαιώνει επίσης στον πελάτη, ότι υπάρχει ένα μετ' επιστροφής μονοπάτι (round-trip path) μεταξύ του πελάτη και του εξυπηρετητή. Στην περίπτωση που ο εξυπηρετητής ήταν ανίκανος ή απρόθυμος να δεχτεί τη σύνδεση TCP του πελάτη, θα είχε απαντήσει με ένα RST/ACK πακέτο (Reset Acknowledge), ή με ένα ICMP Port Unreachable πακέτο (απρόσιτο port), για να ενημερώσει τον πελάτη ότι το αίτημα σύνδεσής του έχει απορριφθεί.

ACK: Όταν ο πελάτης λάβει το πακέτο "αποδοχής-σύνδεσης" SYN/ACK από τον εξυπηρετητή, απαντά με ένα πακέτο ACK.Ο πελάτης επιβεβαιώνει την παραλαβή της απάντησης του εξυπηρετητή SYN/ACK με την αποστολή ενός πακέτου ACK πίσω στον εξυπηρετητή. Σε αυτό το σημείο, από την σκοπιά του πελάτη, μια νέα διπλής κατευθύνσεως σύνδεση TCP έχει εγκατασταθεί μεταξύ αυτού και του εξυπηρετητή, και τα δεδομένα μπορούν τώρα να ρέουν ελεύθερα προς οποιαδήποτε κατεύθυνση μεταξύ των δύο αυτών τερματικών σημείων.

Η λήψη του πακέτου ACK από τον εξυπηρετητή επιβεβαιώνει ότι το πακέτο του SYN/ACK ήταν σε θέση να επιστρέψει στον πελάτη μέσω του συστήματος δρομολόγησης πακέτων του Διαδικτύου. Σε αυτό το σημείο, ο εξυπηρετητής θεωρεί ότι μια νέα διπλής κατευθύνσεως σύνδεση TCP έχει εγκατασταθεί μεταξύ αυτού και του πελάτη και τα δεδομένα μπορούν τώρα να ρέουν ελεύθερα προς οποιαδήποτε κατεύθυνση μεταξύ των δύο αυτών τερματικών σημείων.

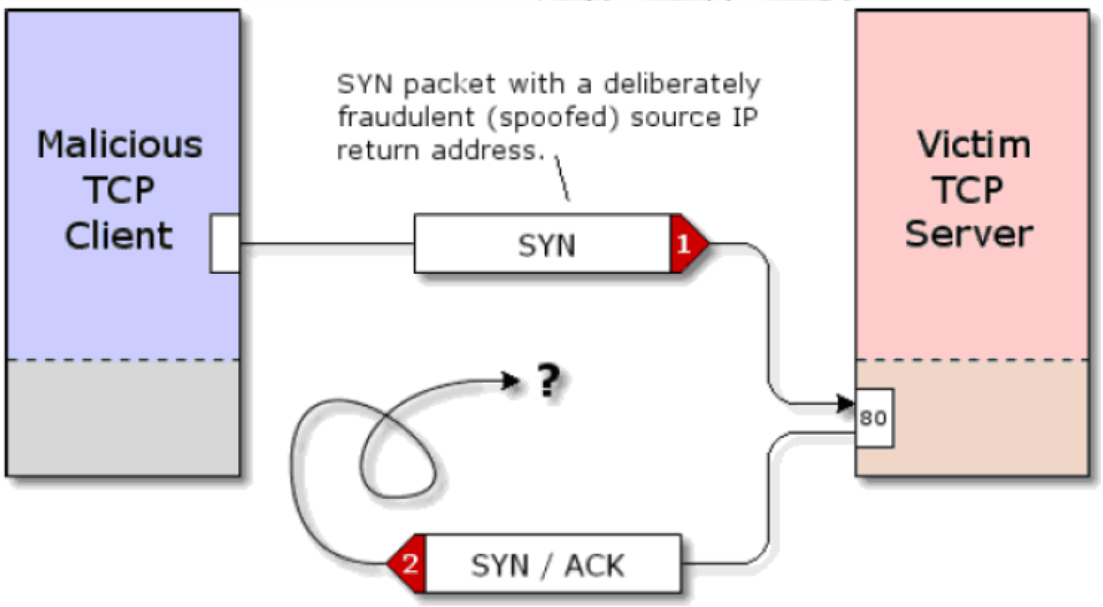
7.3 Η ΕΠΙΘΕΣΗ

Πριν από μερικά χρόνια, ανακαλύφθηκε μια αδυναμία πολλών λειτουργικών συστημάτων στο χειρισμό συνδέσεων TCP και χρησιμοποιήθηκε από τους κακόβουλους hackers του Διαδικτύου. Όπως φαίνεται στο παραπάνω διάγραμμα συναλλαγής TCP, η παραλαβή από τον εξυπηρετητή του πακέτου SYN ενός πελάτη αναγκάζει τον εξυπηρετητή να προετοιμαστεί για μια σύνδεση TCP. Ο εξυπηρετητής διαθέτει συνήθως memory buffers (απομόνωνες μνήμης) για την αποστολή και τη λήψη των δεδομένων της

σύνδεσης, και καταγράφει τις διάφορες παραμέτρους σύνδεσης του πελάτη, συμπεριλαμβανομένου της IP διεύθυνσης καθώς και του αριθμού του port σύνδεσής του.

Με τον τρόπο αυτό, ο εξυπηρετητής θα προετοιμαστεί για να δεχτεί το τελικό πακέτο ACK του πελάτη, έτσι ώστε να τελειώσει η διαδικασία εγκατάστασης της σύνδεσης. Σε περίπτωση που το πακέτο ACK του πελάτη αποτύχει να φθάσει, ο εξυπηρετητής θα στείλει εκ νέου το πακέτο SYN/ACK, θεωρώντας είτε ότι έχει χαθεί είτε ότι έχει απορριφθεί από κάποιον ενδιάμεσο δρομολογητή του Διαδικτύου.

Λαμβάνοντας υπόψη μας τα παραπάνω, καταλήγουμε στο συμπέρασμα ότι μια από τις συνέπειες της παραλαβής ενός πακέτου SYN είναι να διατίθενται μνήμη και άλλοι σημαντικοί πόροι σύνδεσης του εξυπηρετητή. Οι έξυπνοι αλλά συγχρόνως κακόβουλοι hackers του Διαδικτύου υποπτεύθηκαν ότι έπρεπε να υπάρξει ένα όριο στον αριθμό των "κατά το ήμισυ ανοικτών" συνδέσεων που ένας TCP εξυπηρετητής θα μπορούσε να χειριστεί, και βρήκαν απλά μέσα για να μπορέσουν να υπερβούν αυτό το όριο:



Σχήμα 15: Η επίθεση SYN Flood

Μέσω της χρήσης των "Raw Sockets", η "διεύθυνση επιστροφής" (source IP) του πακέτου μπορεί να αλλοιωθεί και να πλαστογραφήσει. Όταν ένα SYN πακέτο με μια spoofed source IP φθάνει στον server, εμφανίζεται ως οποιοδήποτε άλλο έγκυρο αίτημα σύνδεσης. Ο server θα διαθέσει τους απαραίτητους απομονωτές μνήμης (memory buffers), θα καταγράψει τις πληροφορίες για τη νέα σύνδεση, και θα στείλει ένα πακέτο απάντηση SYN/ACK πίσω στον πελάτη.

Αλλά δεδομένου ότι η source IP που περιέχεται στο SYN πακέτο πλαστογραφικέ σκόπιμα (είναι συχνά ένας τυχαίος αριθμός), το SYN/ACK θα σταλεί σε μια τυχαία IP διεύθυνση στο διαδίκτυο. Εάν το πακέτο απευθύνθηκε σε μια έγκυρη διεύθυνση IP, η μηχανή σε εκείνη την διεύθυνση μπορεί να

απαντήσει με ένα "RST" (reset) πακέτο για να ενημερώσει τον server ότι δεν ζήτησε σύνδεση. Αλλά με πάνω από 4 δισεκατομμύρια διευθύνσεις Διαδικτύου, οι πιθανότητες είναι ότι δεν θα υπάρξει καμία μηχανή στη διεύθυνση και το πακέτο θα απορριφθεί.

Το πρόβλημα είναι ότι ο server δεν έχει κανέναν τρόπο να γνωρίσει ότι το αίτημα σύνδεσης του κακόβουλου πελάτη ήταν ψευδές, έτσι πρέπει να το μεταχειριστεί όπως οποιοδήποτε άλλο έγκυρο εν αναμονή αίτημα σύνδεσης. Πρέπει να περιμένει κάποιο χρόνο για τον πελάτη να ολοκληρώσει την τριμερή χειραψία. Εάν το ACK δεν ληφθεί, τότε ο server πρέπει να στείλει εκ νέου το SYN/ACK έχοντας την πίστη ότι έχει χαθεί στο δρόμο του πίσω προς τον πελάτη.

Όπως μπορούμε να φανταστούμε, όλη αυτή η διαχείριση σύνδεσης καταναλώνει τους πολύτιμους και περιορισμένους πόρους του server. Εν τω μεταξύ, ο επιτιθέμενος πελάτης TCP συνεχίζει να βομβαρδίζει τον server με πρόσθετα ψευδή πακέτα SYN, αναγκάζοντας τον να συσσωρεύει μια συνεχώς αυξανόμενη ομάδα μη-ολοκληρωμένων συνδέσεων. Σε κάποιο σημείο, ο server θα είναι ανίκανος να αποδεχτεί άλλες "μισάνοιχτες" συνδέσεις και ακόμη και οι έγκυρες συνδέσεις θα αποτύχουν, δεδομένου ότι η ικανότητα του server να αποδεχτεί οποιαδήποτε νέα σύνδεση θα έχει κακόβουλα καταναλωθεί.

7.4 ΕΙΣΑΓΩΓΗ ΣΤΟ ΜΗΧΑΝΙΣΜΟ ΑΝΙΧΝΕΥΣΗΣ

Ένα χαρακτηριστικό και απλό αλλά δυναμικό μηχανισμό ανίχνευσης τόσο επιθέσεων DoS (*Denial of Service attacks*) όσο και επιθέσεων DDoS (*Distributed Denial of Service attacks)*, ο οποίος στηρίζεται στον έλεγχο της αύξησης των διευθύνσεων IP που είναι συνδεδεμένες πάνω στο θύμα. Αντίθετα από προηγούμενες προτάσεις για ανίχνευση επιθέσεων DDoS, οι οποίες στηρίζονταν στον έλεγχο της αύξησης του όγκου της κίνησης που δέχεται το θύμα, ο μηχανισμός που προτείνουμε είναι πολύ αποτελεσματικός για ευρέως κατανεμημένες επιθέσεις DDoS (*Highly Distributed Denial of Service attacks*). Ο μηχανισμός αυτός εκμεταλλεύεται ένα έμφυτο χαρακτηριστικό γνώρισμα των επιθέσεων DDoS, πράγμα το οποίο δυσκολεύει ιδιαίτερα τον επιτιθέμενο να τον αντιμετωπίσει, απλά αλλάζοντας της υπογραφή (*signature*) της επίθεσής του. Ο εν λόγω μηχανισμός χρησιμοποιεί μια ακολουθιακή μη-παραμετρική μέθοδο ανίχνευσης του σημείου μεταβολής μιας χαρακτηριστικής ποσότητας (*sequential nonparametric change point detection method*) για να βελτιώσει την ακρίβεια ανίχνευσης χωρίς να απαιτεί ένα λεπτομερές μοντέλο της κανονικής (νόμιμης) κίνησης και της κίνησης της επίθεσης. Αποδεικνύουμε, επίσης, ότι μπορούμε να επιτύχουμε υψηλή ακρίβεια ανίχνευσης σε ένα σύνολο διαφορετικών ροών πακέτων δεδομένων. Αυτή τη στιγμή, δεν υπάρχουν αποτελεσματικά μέσα εναντίον των επιθέσεων DDoS για τους εξής λόγους : Πρώτον, τόσο το πρωτόκολλο IP όσο και το TCP μπορούν να μετατραπούν πολύ εύκολα σε επικίνδυνα όπλα στα χέρια των hackers. Δεύτερον, δεδομένου ότι όλη η κυκλοφορία του Διαδικτύου είναι TCP/IP, οι επιτιθέμενοι μπορούν να εξαπολύουν τα κακόβουλα πακέτα τους στο Διαδίκτυο χωρίς να γίνονται

αντιληπτοί ή εύκολα ανιχνεύσιμοι. Τρίτον, εκείνο που αποτελεί απειλή είναι περισσότερο ο όγκος όλων των κακόβουλων πακέτων παρά τα χαρακτηριστικά των μεμονωμένων πακέτων. Επομένως, η λύση εναντίον μιας επίθεσης DDoS είναι πιο σύνθετη από ένα απλό φίλτρο σε έναν δρομολογητή.

Κατά την επίλυση επιθέσεων DDoS ένα βασικό πρόβλημα που καλούμαστε να αντιμετωπίσουμε είναι η *ανίχνευση της επίθεσης*. Η ανίχνευση μιας επίθεσης DDoS είναι σχετικά εύκολη κοντά στο θύμα, αλλά γίνεται πιο δύσκολη καθώς η απόσταση (δηλαδή ο αριθμός των hops) από το θύμα αυξάνεται. Ο λόγος είναι ότι οι περισσότερες DDoS επιθέσεις εξαπολύονται από κατανεμημένες πηγές. Αυτό σημαίνει ότι η κίνηση που προκαλεί μια επίθεση εξαπλώνεται στις πολλαπλές ζεύξεις (*links*) του δικτύου, πράγμα το οποίο καθιστά την επίθεση πιο διάχυτη και την ανίχνευσή της πιο δύσκολη. Οι περισσότερες από τις υπάρχουσες λύσεις στις επιθέσεις εύρους ζώνης γίνονται λιγότερο αποτελεσματικές όταν η κίνηση της επίθεσης γίνεται κατανεμημένη. Υπάρχουν δύο προκλήσεις στην ανίχνευση DDoS επιθέσεων. Η πρώτη πρόκληση είναι πώς να ανιχνεύσουμε την κακόβουλη κίνηση κοντά στην πηγή της. Αυτό είναι ιδιαίτερα δύσκολο όταν η επίθεση είναι ευρέως κατανεμημένη, δεδομένου ότι η κίνηση της επίθεσης από κάθε της πηγή μπορεί να είναι μικρή συγκρινόμενη με την κανονική κίνηση του υποβάθρου. Η δεύτερη πρόκληση είναι να ανιχνευθεί η DDoS επίθεση το συντομότερο δυνατόν χωρίς να ενεργοποιηθεί ένας ψευδής συναγερμός, έτσι ώστε το θύμα να έχει περισσότερο χρόνο για να λάβει μέτρα εναντίον του επιτιθέμενου.

Όπως είπαμε και παραπάνω, οι προτεινόμενες προσεγγίσεις για την ανίχνευση DDoS επιθέσεων που έχουν προηγηθεί στηρίζονται στον έλεγχο του όγκου της κίνησης που λαμβάνεται από το θύμα. Ένα σημαντικό μειονέκτημα αυτών των προσεγγίσεων είναι ότι δεν παρέχουν έναν τρόπο για να διαφοροποιούν τις αιφνίδιες εκρήξεις νόμιμων δεδομένων (flash crowds) από τις επιθέσεις DDoS. Λόγω της εγγενώς αιφνίδιας φύσης της κίνησης του Διαδικτύου, μια ξαφνική αύξηση στην κίνηση μπορεί να εκληφθεί ως επίθεση. Εάν καθυστερήσουμε την απόκριση του συστήματος μας προκειμένου να εξασφαλίσουμε ότι η αύξηση της κίνησης δεν είναι απλά μια παροδική έκρηξη, τότε κινδυνεύουμε να αφήσουμε το θύμα στο έλεος μιας πραγματική επίθεση. Επιπλέον, κάποιες επίμονες αυξήσεις στην κίνηση μπορούν να μην είναι επιθέσεις, αλλά πραγματικά γεγονότα "flash crowds", όπου ένας μεγάλος αριθμός νόμιμων χρηστών έχει πρόσβαση στο ίδιο website ταυτοχρόνως. Είναι σαφές, λοιπόν, ότι υπάρχει ανάγκη για μια καλύτερη προσέγγιση στην ανίχνευση των DDoS επιθέσεων. Μια καλύτερη προσέγγιση στην ανίχνευση τέτοιων επιθέσεων είναι η παρακολούθηση του αριθμού των IP διευθύνσεων που είναι συνδεδεμένες πάνω στο θύμα. Οι Jung et al. έχουν παρατηρήσει ότι κατά τη διάρκεια των DDoS επιθέσεων, οι περισσότερες IP διευθύνσεις πηγής είναι καινούργιες για το θύμα, ενώ οι περισσότερες από τις αντίστοιχες IP διευθύνσεις σε ένα flash crowd έχουν εμφανιστεί στο θύμα πρωτύτερα. Η παρατήρηση αυτή έχει χρησιμοποιηθεί στο παρελθόν σαν βάση σε έναν μηχανισμό, σύμφωνα με τον οποίο η κίνηση επίθεσης αποτρέπεται από το ίδιο το θύμα. Στην παρούσα μελέτη, προτείνουμε να παρακολουθούμε τον αριθμό των IP διευθύνσεων που είναι συνδεδεμένες πάνω στο θύμα προκειμένου να ανιχνευθούν οι DDoS επιθέσεις. Αποδεικνύουμε επίσης, ότι ο αριθμός των IP διευθύνσεων που είναι συνδεδεμένες πάνω στο θύμα είναι μια πολύ πιο ευαίσθητη μεταβλητή για την ανίχνευση των DDoS επιθέσεων από

ότι ο συνολικός όγκος της εισερχόμενης κίνησης. Επιπλέον, παρουσιάζουμε μια μέθοδο για να ανιχνεύουμε απότομες μεταβολές στη μεταβλητή ελέγχου μας, η οποία βασίζεται στον μη-παραμετρικό (*non-parametric*) αλγόριθμο του συσωρευτικού αθροίσματος (*Cumulative SUM algorithm*).

Ο αλγόριθμος CUSUM μειώνει την πιθανότητα ψευδούς συναγερμού, και έχει παρουσιάσει βέλτιστα χαρακτηριστικά όσον αφορά την ακρίβεια της ανίχνευσης και το υπολογιστικό φόρτο καθώς και πολύ καλή απόδοση.

Η κύρια συμβολή μας σε αυτή τη μελέτη είναι μια νέα προσέγγιση στην ανίχνευση των DDoS επιθέσεων ελέγχοντας το ρυθμό αύξησης των IP διευθύνσεων που είναι συνδεδεμένες πάνω στο θύμα. Αποδεικνύουμε, μάλιστα, ότι η προσέγγιση αυτή είναι πιο αποτελεσματική από τους προηγούμενους μηχανισμούς, ιδιαίτερα στην περίπτωση που υπάρχουν πολλαπλές πηγές επίθεσης και η κίνηση της επίθεσης είναι ιδιαίτερα κατανεμημένη. Πιο συγκεκριμένα προσαρμόζουμε τον μηχανισμό ανίχνευσης που προτείνεται από τους Tao Peng, Christopher Leckie και Kotagiri Ramamohanarao, ο οποίος είναι βασισμένος σε έναν προηγμένο μη-παραμετρικό αλγόριθμο ανίχνευσης μεταβολών, τον CUSUM αλγόριθμο, και αποδεικνύουμε ότι αυτή η προσέγγιση ανιχνεύει ένα ευρύ φάσμα προσομοιωμένων επιθέσεων γρήγορα και με μεγάλη ακρίβεια.

Τέλος, στο σημείο αυτό θα πρέπει να αναφερθεί ότι παρόμοιοι μηχανισμοί ανίχνευσης οι οποίοι χρησιμοποιούν τον αλγόριθμο CUSUM έχουν γίνει και στο παρελθόν. Ο μηχανισμός ανίχνευσης που προτείνεται από τους Tao Peng, Christopher Leckie και Kotagiri Ramamohanarao χρησιμοποιεί ως χαρακτηριστική μεταβλητή τον αριθμό των νέων IP διευθύνσεων που είναι συνδεδεμένες κάθε στιγμή στο θύμα, έχοντας ως βάση σύγκρισης μια βάση δεδομένων που περιέχει όλες εκείνες τις IP διευθύνσεις που το θύμα θεωρεί ως νόμιμες. Μια παρόμοια προσέγγιση έχουν κάνει και οι Haining Wang, Danlu Zhang και Kang G.Shin [72], οι οποίοι εκμεταλλεύονται το γεγονός ότι υπό συνθήκες νόμιμης κίνησης, η λήψη ενός πακέτου SYN συνεπάγεται και τη λήψη ενός πακέτου FIN. Με λίγα λόγια, εκμεταλλεύονται ένα έμφυτο χαρακτηριστικό του πρωτοκόλλου TCP, το ότι δηλαδή υπό κανονικές συνθήκες δικτύου τα πακέτα SYN και FIN εμφανίζονται κατά ζεύγη.

Για την ανίχνευση ιδιαίτερα κατανεμημένων επιθέσεων DDoS (*Highly Distributed Denial of Service-HDDoS*) προτείνετε ένας μηχανισμό που λέγεται Source IP address Monitoring-SIM (Παρακολούθηση των IP διευθύνσεων που είναι συνδεδεμένες πάνω στο θύμα). Αυτός ο μηχανισμός ανίχνευσης χρησιμοποιεί ένα έμφυτο χαρακτηριστικό γνώρισμα των επιθέσεων HDDoS, που δεν είναι άλλο από τον τεράστιο αριθμό των IP διευθύνσεων που είναι συνδεδεμένες πάνω στο θύμα κατά τη διάρκεια μιας επίθεσης. Αυτή η καινούργια προσέγγιση έχει το πλεονέκτημα ότι μπορεί να ανιχνεύσει την επίθεση στα αρχικά στάδιά της.

Σύμφωνα με τον μηχανισμό SIM, για την ανίχνευση μιας κατανεμημένης επίθεσης είναι απαραίτητη η συλλογή στατιστικών δεδομένων της εισερχόμενης κίνησης καθ' όλη τη διάρκεια της χρονικής περιόδου όπου το θύμα είναι συνδεδεμένο στο διαδίκτυο. Οι πληροφορίες αυτές λαμβάνονται για τακτά χρονικά διαστήματα Δn και μάλιστα συγκεντρώνονται στο τέλος του εκάστοτε τρέχοντος χρονικού διαστήματος Δn. Στο μηχανισμό αυτό, ένας μετρητής (counter) χρησιμοποιείται για να καταγράψει τον αριθμό των IP

διευθύνσεων που είναι συνδεδεμένες στο θύμα. Με τον τρόπο αυτό μπορούμε να υπολογίσουμε πόσες καινούργιες IP συνδέσεις έχουν εμφανιστεί μέσα στο χρονικό διάστημα Δn. Έτσι, παρακολουθώντας των αριθμών των IP συνδέσεων πάνω στο θύμα, είμαστε σε θέση να ανιχνεύσουμε μια HDDoS (*Highly Distributed Denial of Service-HDDoS*) επίθεση.

8

ΚΕΦΑΛΑΙΟ

<< Επίλογος - Περαιτέρω σκέψεις>>

- **Επίλογος - Περαιτέρω σκέψεις**

8 ΕΠΙΛΟΓΟΣ - ΠΕΡΑΙΤΕΡΩ ΣΚΕΨΕΙΣ

Το Διαδίκτυο δεν είναι σταθερό αλλά αλλάζει μορφές πολύ γρήγορα. Αυτό σημαίνει ότι τα DDoS αντίμετρα ξεπέρνιουνται πολύ γρήγορα. Νέες υπηρεσίες προσφέρονται μέσω του Διαδικτύου και νέες επιθέσεις εξαπολύονται προκειμένου να αποτραπούν οι πελάτες από την πρόσβαση σε αυτές τις νέες υπηρεσίες. Παρόλα αυτά, το βασικό θέμα είναι κατά πόσο οι DDoS επιθέσεις αντιπροσωπεύουν ένα δικτυακό πρόβλημα ή ένα πρόβλημα μεμονωμένου χρήστη ή και τα δύο. Στην πρώτη περίπτωση η λύση θα μπορούσε να προέλθει από αλλαγές στα πρωτόκολλα του Διαδικτύου. Συγκεκριμένα, οι δρομολογητές θα έπρεπε να φιλτράρουν την κακόβουλη κίνηση, οι επιτιθέμενοι δεν θα μπορούσαν να αλλοιώνουν τις διευθύνσεις IPs και δεν θα υπήρχε κανένα μειονέκτημα στα πρωτοκόλλα δρομολόγησης. Στη δεύτερη περίπτωση η λύση θα μπορούσε να προέλθει από ένα αποτελεσματικό IDS σύστημα, από έναν anti-virus ή από ένα άτρωτο firewall (αντιπυρική ζώνη). Οι επιτιθέμενοι τότε δεν θα μπορούσαν να «καταλάβουν» τα συστήματα προκειμένου να δημιουργήσουν έναν στρατό "zombies". Προφανώς, φαίνεται ότι και το δίκτυο και οι μεμονωμένοι hosts συνιστούν το πρόβλημα. Συνεπώς, αντίμετρα πρέπει να ληφθούν και από τις δύο πλευρές. Δεδομένου ότι οι επιτιθέμενοι συνεργάζονται προκειμένου να δημιουργήσουν τις τέλειες μεθόδους επίθεσης, οι νόμιμοι χρήστες και οι υπεύθυνοι για την ανάπτυξη συστημάτων ασφαλείας πρέπει επίσης να συνεργαστούν ενάντια στην απειλή. Οποιοσδήποτε δηλώνει ότι έχει κατορθώσει μόνος του να αντικρούσει πλήρως τις επιθέσεις DDoS λέει ψέματα. Η λύση θα προκύψει από το συνδυασμό και δικτυακών και μεμονωμένων αντιμέτρων.

9 ΒΙΒΛΙΟΓΡΑΦΙΑ

[1] Kevin Tsui. Tutorial-Virus(Malicious Agents).University of Calgary. October 22, 2001

[2] Nicholas Weaver. Warhol Worms: The Potential for Very Fast Internet Plagues http://www.iwar.org.uk/comsec/resources/worms/warhol-worm.htm 2001

[3] Nicholas Weaver, U.C. Berkeley BRASS group. Potential Strategies for High speed Active Worms: A Worst Case Analysis. February 4, 2002

[4] David Moore and Colleen Shannon. "The spread of the code red worm (crv2)".

http://www.caida.org/analysis/security/codered/coderedv2_analysis.xml#animations. July 24, 2001

[5] Kevin J. Houle, CERT/CC, George M. Weaver, CERT/CC, in collaboration with:

Neil Long, Rob Thomas. Trends in Denial of Service Attack Technology. V1.0 October 2001

[6] T. Peng, C. Leckie, K. Ramamohanarao. Detecting Distributed Denial of Service Attacks Using Source IP Address Monitoring. The University of Melbourne, Victoria 3010, Australia 2003

[7] Steve Gibson. Distributed Reflection Denial of Service Description and analysis of a potent, increasingly prevalent, and worrisome Internet attack. February 22, 2002

[8] http://www.ll.mit.edu/IST/ideval/docs/1999/attackDB.html

[9] Yanet Manzano. Tracing the Development of Denial of Service Attacks: A Corporate Analogy. http://www.acm.org/crossroads/xrds10-1/tracingDOS.html 2003

[10] Larry Rogers. What is a Distributed Denial of Service (DDoS) Attack and What Can I Do About It? http://www.cert.org/homeusers/ddos.html , February 10, 2004

[11] Jelena Mirkovic - Janice Martin - Peter Reiher, UCLA, A Taxonomy of DDoS Attacks and DDoS Defense Mechanisms

[12] Distributed Denial of Service Tools http://www.cert.org/incident_notes/IN-99-07.html

[13] P. Ferguson Cisco Systems Inc. - D. Senie Amaranth Networks Inc., Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing, May 2000

[14] A. Garg and A. L. Narasimha Reddy, "Mitigating denial of service attacks using QoS regulation," Texas A & M University Tech report, TAMU-ECE-2001-06

[15] TCP SYN Flooding attack http://www.cert.org/advisories/CA-1996-21.html