ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΑΤΡΩΝ
ΤΜΗΜΑ ΙΣΤΟΡΙΑΣ-ΑΡΧΑΙΟΛΟΓΙΑΣ

ΔΙΑΧΕΙΡΙΣΗ ΑΣΦΑΛΕΙΑΣ ΚΑΙ ΕΜΠΙΣΤΟΣΥΝΗΣ ΣΕ ΠΟΛΙΤΙΣΜΙΚΑ ΠΕΡΙΒΑΛΛΟΝΤΑ

ΔΙΔΑΚΤΙΚΗ ΕΝΟΤΗΤΑ 5

ΘΕΜΑ: ΕΠΙΘΕΣΕΙΣ ΑΡΝΗΣΗΣ ΕΞΥΠΗΡΕΤΗΣΗΣ

Δρ. Δημήτριος Κ. Κουκόπουλος
Αναπληρωτής Καθηγητής

ΠΕΡΙΕΧΟΜΕΝΑ

- Ορισμοί – Βασικές έννοιες
- Απλές Επιθέσεις Άρνησης Εξυπηρέτησης
  - TearDrop και Ping of Death
  - SYN
  - Πλημμύρα UDP
  - Smurf
- Κατανεμημένες Επιθέσεις Άρνησης Εξυπηρέτησης
  - Trin00
  - TFN/TFN2K
  - Stacheldraht
- Τρόποι Άμυνας για Αποφυγή Εισβολής
- Βιβλιογραφία

Ορισμός

Επίθεση άρνησης εξυπηρέτησης/υπηρεσίας (denial of service) είναι κάθε επίθεση που βασικό σκοπό έχει την άρνηση της πρόσβασης του θύματος σε έναν συγκεκριμένο πόρο.

Είδη

- Εσωτερικές επιθέσεις από το σύστημα του θύματος
- Εξωτερικές επιθέσεις από το σύστημα του θύματος

Σκοποί Επιθέσεων

- Μείωση της συνδεσιμότητας του δικτύου
- Μείωση του εύρους ζώνης (bandwidth)

Θύματα Επιθέσεων

Χρήστες στοχευόμενων συστημάτων.

Δρ. Δημήτριος Κ. Κουκόπουλος
Αναπληρωτής Καθηγητής

Συχνότητα Επιθέσεων

Το 27% των συνολικών επιθέσεων είναι επιθέσεις άρνησης υπηρεσίας. [Computer Security Institute, USA, 2000].

Λόγοι Έλλειψης Δημοσιότητας

- Προσβεβλημένες εταιρείες κρύβουν επιθέσεις λόγω φόβου αρνητικής δημοσιότητας.
- Μικρή ένταση επίθεσης με τοπικά χαρακτηριστικά

Ταξινόμηση Επιθέσεων Άρνησης Εξυπηρέτησης

- Απλές
  - Teardrop και Ping of Death
  - SYN
  - Πλημμύρα UDP
  - Smurf
- Κατανεμημένες
  - Trinoo
  - TFN/TFN2K
  - Stacheldraht

Επιθέσεις Teardrop και Ping of Death

- Παλιές επιθέσεις
- Απλές επιθέσεις
- Εύκολες στη διαχείριση
- Στηρίζονται σε λάθη στην υλοποίηση του πρωτοκόλλου IP

Αδυναμία IP σε Επίθεση Ping of Death

Τα πακέτα στο IP έχουν μέγιστο μήκος 65536 bytes. Το μήκος της επικεφαλίδας είναι 20 – 24 bytes.

Η βασική ιδέα πίσω από τις επιθέσεις είναι η αποστολή πακέτων μεγαλύτερων των 65536 bytes. Αυτό μπορεί να γίνει με τη χρήση του Internet Control Message Protocol (ICMP) που χρησιμοποιείται για την αποστολή μηνυμάτων λαθών και ελέγχου μεταξύ συστημάτων.

Χειραγώγηση Αδυναμίας

- Υπάρχουν δυο μηνύματα που καθορίζονται από το ICMP για έλεγχο δικτύωσης (ICMP_ECHO_REQUEST, ICMP_ECHO_REPLY).

- Μια μηχανή στέλνει στην άλλη το μήνυμα ICMP_ECHO_REQUEST και η άλλη μηχανή αν το λάβει απαντά με ICMP_ECHO_REPLY. Τα μηνύματα στέλνονται με την εντολή ping του λειτουργικού συστήματος.

- Η εντολή ping μπορεί να στείλει ICMP μηνύματα διαφορετικού μεγέθους καθοριζόμενου από τον χρήστη.

- Ο κακόβουλος χρήστης στέλνει με την ping υπερμεγέθη ICMP πακέτα σε έναν σταθμό και αυτός επειδή δε μπορεί να τα διαχειριστεί σταματά να λειτουργεί ομαλά (crash, hang, reboot).

Αδυναμία IP σε Επίθεση Teardrop

- Δυνατότητα αποσυναρμολόγησης πακέτων σε αποστολέα και συναρμολόγησης σε παραλήπτη. Κάθε πακέτο έχει τον δικό του αριθμό ταυτοποίησης και διεύθυνση μετατόπισης.

- Ο αριθμός ταυτοποίησης επιλύει το πρόβλημα της ταυτόχρονης λήψης συναρμολογημένων πακέτων.

- Η διεύθυνση μετατόπισης καθορίζει τη σειρά με την οποία το πακέτο συναρμολογείται σε σχέση με την αρχή του μηνύματος (8 bytes).

Χειραγώγηση Αδυναμίας

Η επίθεση Teardrop δημιουργεί συναρμολογημένα πακέτα με επικαλυπτόμενες διευθύνσεις μετατόπισης σε κάθε πακέτο.

Επίθεση SYN

- Η επίθεση SYN στηρίζεται στο άνοιγμα πολλών μισάνοιχτων συνδέσεων TCP. Για καθεμιά σύνδεση ο εξυπηρετητής πρέπει να δεσμεύει μνήμη για να την αποθηκεύει. Μόλις τελειώσουν οι πόροι του δε μπορεί να δεχτεί άλλες αιτήσεις σύνδεσης.

- Είναι ασύμμετρη επίθεση καθώς ο επιτιθέμενος δε στέλνει πολλά δεδομένα αλλά μικρές αιτήσεις TCP σύνδεσης.

- Είναι επίθεση που στηρίζεται στη μείωση της συνδεσιμότητας του δικτύου.

Αδυναμία TCP 1/2

- Μια σύνδεση TCP μπορεί να εγκατασταθεί μόνο ανάμεσα σε δυο υποδοχές (sockets) που βρίσκονται συνήθως σε διαφορετικές μηχανές και δε βρίσκονται ήδη σε σύνδεση. Μια υποδοχή καθορίζεται από την IP διεύθυνσή της και έναν αριθμό θύρας.

- Για την εγκατάσταση της TCP σύνδεσης και οι δυο υποδοχές πρέπει να συμφωνήσουν και να έχουν κατάλληλους πόρους. Η εγκατάσταση μιας σύνδεσης TCP γίνεται μέσω μιας χειραψίας τριών βημάτων:
  - Ένας σταθμός (πελάτης) αιτείται μια TCP σύνδεση στέλνοντας ένα σήμα SYN σε ένα δεύτερο σταθμό (εξυπηρετητής).
  - Ο εξυπηρετητής απαντά με ένα σήμα επιβεβαίωσης (SYNACK) και καταγράφει την αίτηση.
  - Ο πελάτης αφού λάβει SYNACK απαντά με μια επιβεβαίωση (ACK).

Αδυναμία TCP 2/2

- Μετά τη χειραψία η σύνδεση έχει εγκατασταθεί, ενώ κατά τη διάρκειά της είναι μισάνοιχτη. Αν ο εξυπηρετητής δε λάβει το σήμα ACK σε κάποιο χρονικό διάστημα θα απεγκαταστήσει την σύνδεση.

Λειτουργία Επίθεσης

- Ο επιτιθέμενος αποφεύγει την εγκατάσταση μιας σύνδεσης ανάμεσα στο σύστημά του και τον εξυπηρετητή γιατί αυτό μπορεί να αφορά μόνο μια σύνδεση. Ο επιτιθέμενος στέλνει τις αιτήσεις του για σύνδεση με πλαστή διεύθυνση πηγής.

- Ο εξυπηρετητής απαντά με ένα σήμα SYNACK σε κάποιο σταθμό που δε ζήτησε σύνδεση TCP μαζί του και δε θα του απαντήσει με σήμα ACK, ενώ δεσμεύει πόρους για τη μισάνοιχτη σύνδεση.

- Αν οι ψεύτικες αιτήσεις είναι πολλές θα καταναλωθούν οι πόροι του εξυπηρετητή και δε θα μπορεί να εξυπηρετήσει πραγματικές αιτήσεις.

Πρόληψη Επίθεσης SYN

- Μείωση του χρόνου αναμονής για λήψη σήματος ACK και αύξηση μνήμης για μισάνοιχτες συνδέσεις.

- Όχι πλήρης λύση. Δουλεύει για μικρές και μεσαίες επιθέσεις.

Επίθεση Πλημμύρας UDP

Η επίθεση πλημμύρας UDP (User Datagram Protocol) χρησιμοποιεί το ασυνδεσμικό πρωτόκολλο UDP για να δημιουργήσει υψηλή κυκλοφορία.

Αδυναμία UDP

- Είναι στο ίδιο επίπεδο με TCP. Χρησιμοποιείται ως πρωτόκολλο μεταφοράς για υπηρεσίες TFTP και RCP (Remote Call Procedure).
- Είναι ασυνδεσμικό πρωτόκολλο και επομένως αναξιόπιστο. Όταν ένα μήνυμα αποστέλλεται ο αποστολέας δε μπορεί να μάθει αν το μήνυμα παρελήφθη από προορισμό.
- Δεν έχει δυνατότητες ανάνηψης από λάθος.
- Χρήση όταν ταχύτητα και απλότητα είναι πιο σπουδαίες από αξιοπιστία.

Μορφές UDP Επίθεσης

Δύο μορφές:

- Αποστολή μεγάλης ποσότητας δεδομένων (brute force).
  - Δύσκολο να σταματήσει, αλλά ο επιτιθέμενος πρέπει να έχει πολλούς πόρους.
- Σύνδεση υπηρεσίας UDP echo (επανάληψη δεδομένων σε αποστολέα) με υπηρεσία UDP chargen (έλεγχος δικτύου, αποστολή χαρακτήρων σε socket μέχρι να λάβει αίτηση παύσης).
  - Διπλασιασμός έντασης κυκλοφορίας μεταξύ δυο συστημάτων με χρήση μόνο ενός πακέτου.
  - Μείωση ταχύτητας, όχι όμως πλήρες μπλοκάρισμα.
  - Είναι πιο εξελιγμένη μορφή επίθεσης, αλλά είναι πιο εύκολο να σταματήσει.

Λειτουργία Δεύτερης Μορφής UDP Επίθεσης

- Αποστολή κακόβουλης αίτησης σε υπηρεσία UDP chargen του πρώτου θύματος. Η αίτηση έχει πλαστή διεύθυνση πηγής και αριθμό θύρας που ανήκουν στο δεύτερο θύμα.

- Η κυκλοφορία της υπηρεσίας chargen που οφείλεται στην πρώτη αίτηση θα σταλεί στη θύρα UDP echo του δεύτερου θύματος.

- Η υπηρεσία echo του δεύτερου θύματος θα στείλει όλα τα δεδομένα πίσω στον αποστολέα.

Επίθεση Smurf

Η επίθεση smurf είναι σκληρή (brute force) και ασύμμετρη επίθεση που χρησιμοποιεί την διευθυνσιοδότηση απευθείας μετάδοσης του IP για να δημιουργήσει υψηλή κυκλοφορία.

Αδυναμία IP

- Το πρωτόκολλο IP παρέχει τη δυνατότητα μετάδοσης ενός μηνύματος σε όλα τα δίκτυα και τους σταθμούς με τη χρήση της IP διεύθυνσης που περιέχει 32 άσσους.

- Επίσης, το πρωτόκολλο IP παρέχει τη δυνατότητα απευθείας μετάδοσης ενός μηνύματος σε ένα μόνο δίκτυο. (Π.χ. αν το δίκτυο έχει αριθμό 180.50, τότε το μήνυμα με διεύθυνση 180.50.255.255 θα πάει σε όλους τους σταθμούς του δικτύου).

Λειτουργία Επίθεσης

- Χρήση αδυναμίας IP από επιτιθέμενο ως μέσο πολλαπλασιασμού μηνυμάτων.
  - Αποστολή μηνύματος ICMP_ECHO_REQUEST σε ένα δίκτυο χρησιμοποιώντας τη διευθυνσιοδότηση απευθείας μετάδοσης.
  - Ο δρομολογητής θα μεταδώσει το μήνυμα σε όλους τους σταθμούς του δικτύου και αυτοί θα απαντήσουν με πολλά μηνύματα ICMP_ECHO_REPLY.

- Αποστολή σειρών μηνυμάτων ICMP_ECHO_REQUEST σε ένα δίκτυο με τροποποιημένες διευθύνσεις πηγής. Οι απαντήσεις στέλνονται σε θύμα του οποίου η διεύθυνση τίθεται ως διεύθυνσης πηγής.

Θύματα Επίθεσης

- Δυο θύματα (όπως σε επίθεση πλημμύρας UDP):
  - Δίκτυο που δέχεται αιτήσεις μετάδοσης
  - Σταθμός που δέχεται απαντήσεις ICMP_ECHO_REPLY

- Τα θύματα υφίστανται μείωση εύρους ζώνης.

Πρόληψη Επίθεσης

- Στην πλευρά του δικτύου πολλαπλασιαστή πρέπει να μπλοκαριστούν όλες οι αιτήσεις μετάδοσης που προέρχονται εκτός του δικτύου.

- Στην πλευρά των θυμάτων ο δρομολογητής πρέπει να μπλοκάρει όλη την κυκλοφορία ICMP_ECHO_REPLY ή να τη μειώσει σε μικρό ποσοστό της όλης κυκλοφορίας.

Εξέλιξη Επιθέσεων Άρνησης Υπηρεσίας

- Η κατανάλωση εύρους ζώνης έγινε δύσκολη λόγω της αύξησης των ταχυτήτων.
- Ο περιοριστικός παράγοντας των σύγχρονων δρομολογητών δεν είναι το εύρος ζώνης, αλλά ο ρυθμός επεξεργασίας πακέτων.
- Οι επιτιθέμενοι φροντίζουν την ασφάλειά τους με τη δημιουργία πακέτων, όχι με πραγματικές IP διευθύνσεις πηγής, αλλά με διευθύνσεις θυμάτων τους.

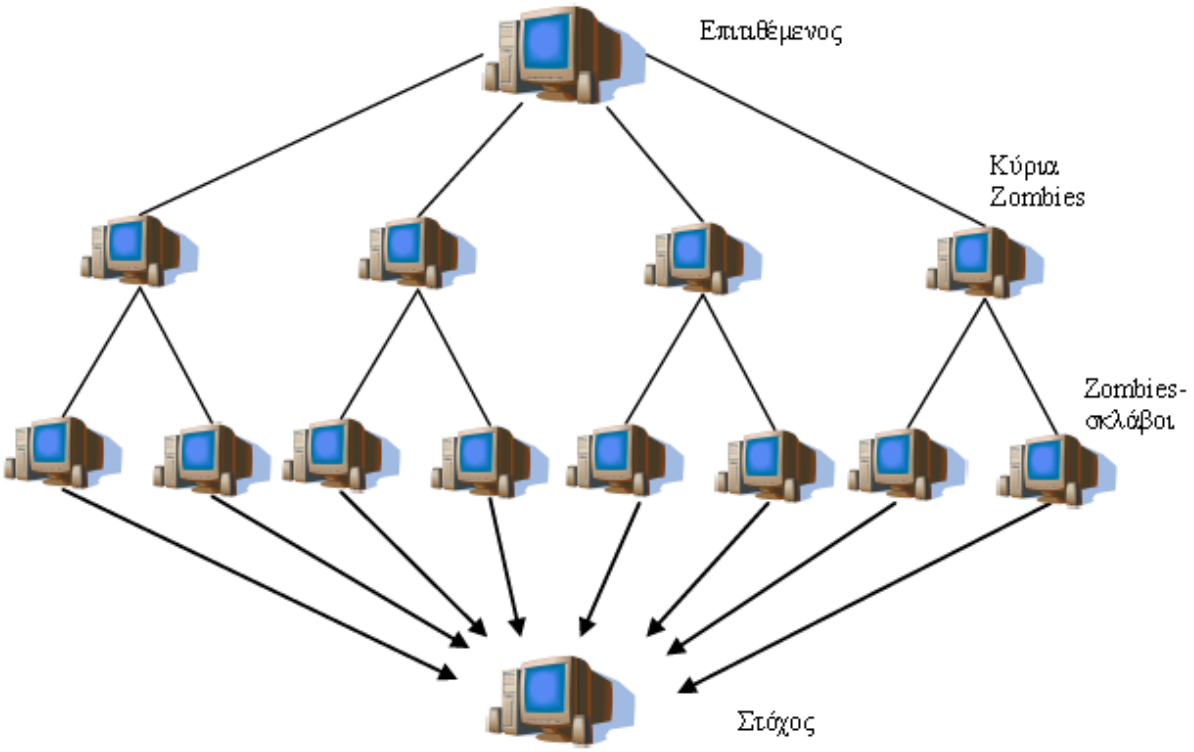
Βασική Ιδέα

- Τα πακέτα με πλαστογραφημένη διεύθυνση πηγής δημιουργούνται έτσι ώστε να απορριφθούν στον προορισμό τους (δείχνουν μια σπάνια σε χρήση θύρα) που είναι τυχαίες IP διευθύνσεις.
- Αφού τα πακέτα απορριφθούν ο «αποστολέας» ειδοποιείται με ICMP μήνυμα για την απόρριψη. Έτσι, το θύμα θα βιώσει μια πλημμύρα ICMP μηνυμάτων που έρχονται από διάφορες πηγές (επίθεση αντανάκλασης).
- Το θύμα είναι δύσκολο να σταματήσει την πλημμύρα επειδή δε μπορεί να φιλτράρει τα λανθασμένα ICMP πακέτα και να περάσει τα χρήσιμα λόγω του ότι οι διευθύνσεις πηγής των ICMP πακέτων είναι τυχαίες. Το πλήρες μπλοκάρισμα των ICMP πακέτων είναι αδύνατο γιατί είναι μέρος του IP και χωρίς αυτό δεν υπάρχει επικοινωνία.

Κατανεμημένα Εργαλεία Άρνησης Υπηρεσίας

- Κατανεμημένα εργαλεία ανοιχτού κώδικα
- Χρήση όλων των επιθέσεων άρνησης υπηρεσίας
- Δημιουργία δικτύων με ιεραρχική οργάνωση

Κατανεμημένες Επιθέσεις (Patrikakis et al. 2004)



Δρ. Δημήτριος Κ. Κουκόπουλος
Αναπληρωτής Καθηγητής

Ιεραρχική Οργάνωση

Οργάνωση σε τρία επίπεδα:

- Επίπεδο πελάτη (client)
- Επίπεδο χειριστή (handler)
- Επίπεδο πράκτορα (agent)

Επίπεδο Πελάτη

- Οι πελάτες χρησιμοποιούνται από τους επιτιθέμενους για τον έλεγχο των δικτύων κατανεμημένης άρνησης υπηρεσίας.

- Οι πελάτες είναι προγράμματα κονσόλας με απλές εντολές χρήσιμες για ενορχήστρωση επιθέσεων.

Επίπεδο Χειριστή

Οι χειριστές έχουν ως στόχο να δυσκολέψουν την ανίχνευση του επιτιθέμενου.

Επίπεδο Πράκτορα

- Οι πράκτορες είναι υπεύθυνοι για τις πλημμύρες από άχρηστα πακέτα.
- Οι πράκτορες προσπαθούν να κρυφθούν πλαστογραφώντας τη διεύθυνση πηγής ή με τη χρήση επιθέσεων αντανάκλασης.
- Ο επιτιθέμενος χρησιμοποιεί τον πελάτη για να ελέγξει τους χειριστές που ελέγχουν τους πράκτορες.
- Αν σε μια επίθεση ένα σύνολο πρακτόρων μπλοκαριστεί ή ανακαλυφθεί από το θύμα ο επιτιθέμενος αλλάζει απλά τον χειριστή που ελέγχει τους μη ενεργούς πράκτορες με άλλο χειριστή που ελέγχει άλλους πράκτορες.

Επίθεση Trin00 1/2

Η επίθεση Trin00 (Trin00 Distributed Denial of Service Attack) είναι ένα κατανεμημένο εργαλείο που χρησιμοποιείται για την έναρξη συντονισμένων επιθέσεων πλημμύρας UDP από πολλές πηγές.

- Ένα δίκτυο Trin00 περιέχει πελάτες, χειριστές και πράκτορες.
- Ο επιτιθέμενος χρησιμοποιώντας ήδη μοχλευμένα συστήματα ελέγχει το δίκτυο για πιθανούς πράκτορες. Μόλις εντοπίσει ένα κατάλληλο σύστημα εγκαθιστά το λογισμικό που χρειάζεται για να αρχίσει η επίθεση και κρύβει την παρουσία του.

Επίθεση Trin00 2/2

- Όταν έχουν βρεθεί αρκετοί πράκτορες η πραγματική επίθεση ξεκινά.
  - Ο πελάτης συνδέεται με τους χειριστές μέσω μιας σύνδεσης TCP
  - Οι χειριστές σχηματίζουν λίστα ενεργών πρακτόρων (χρήση UDP πακέτων για επικοινωνία χειριστών και πρακτόρων) και τη μεταφέρουν στον πελάτη
  - Ξεκινά μια πλημμύρα UDP πακέτων στο θύμα

Υπηρεσίες Trin00

- Κωδικοί εγκαθίστανται για αποφυγή μη εξουσιοδοτημένης προσπέλασης σε χειριστές και πράκτορες από άλλους επιτιθέμενους ή διαχειριστές συστήματος (αν οι κωδικοί βρεθούν από έναν διαχειριστή η επίθεση Trin00 σταματά)

- Χρήση κρυπτογράφησης για απόκρυψη επικοινωνίας ανάμεσα σε κόμβους δικτύου Trin00

- Εύκολη χρήση

Ανίχνευση Επίθεσης Trin00

- Οι κρυπτογραφημένοι κωδικοί (passwords) είναι ορατοί στη δυαδική εικόνα των πρακτόρων και των χειριστών. Αν κάποιος εντοπίσει έναν χειριστή ή πράκτορα Trin00 μπορεί μέσω αυτών των κωδικών να ταυτοποιήσει όλους τους κόμβους του δικτύου Trin00.

- Ο κωδικός των πρακτόρων μεταδίδεται ως απλό κείμενο και επομένως με επισταμένη παρακολούθηση της κυκλοφορίας κάποιος μπορεί να ανιχνεύσει τον κωδικό.

Απεγκατάσταση Δικτύου Trin00

- Αν εντοπιστεί ένας πράκτορας μπορεί να εξαχθεί η λίστα των χειριστών που πάντα υπάρχει σε αυτόν.
  - Οι υπολογιστές που λειτουργούν ως χειριστές ειδοποιούνται
  - Σε κάθε χειριστή εξάγεται η λίστα των υπολογιστών που λειτουργούν ως πράκτορες και αποστέλλεται μια εντολή κλεισίματος. Επίσης, η κυκλοφορία ελέγχεται μήπως ο επιτιθέμενος είναι ακόμη συνδεδεμένος.
  - Οι διαχειριστές συστημάτων με πράκτορες ενημερώνονται

- Αν εντοπιστεί ένας χειριστής τα δυο τελευταία βήματα επαναλαμβάνονται.

Επίθεση TFN 1/2

Η επίθεση TFN (Tribe Flood Network) είναι ένα κατανεμημένο εργαλείο που χρησιμοποιείται για έναρξη επιθέσεων (SYN, UDP, ICMP, Smurf).

- Μια επίθεση TFN (όπως η Trin00) αρχίζει με τη μόχλευση κατάλληλων συστημάτων σε χειριστές και πράκτορες και την εγκατάσταση κατάλληλου λογισμικού. Αυτή η μόχλευση είναι αυτοματοποιημένη, γίνεται με απλά κομμάτια κώδικα και περιλαμβάνει πολλά συστήματα σε σύντομο χρόνο.
- Μετά την εγκατάσταση ενός δικτύου TFN ο επιτιθέμενος στέλνει τη λίστα πρακτόρων και την IP διεύθυνση του στόχου σε έναν χειριστή.

Επίθεση TFN 2/2

- Ο χειριστής περνά τη διεύθυνση σε όλους τους πράκτορες που απαντούν με μήνυμα επιβεβαίωσης
- Οι πράκτορες ξεκινούν την πλημμύρα άχρηστων πακέτων στο στοχοποιημένο σύστημα.

Υπηρεσίες TFN

- Εξελίσσει την επίθεση Trin00.

- Υποστηρίζει:
  - Δημιουργία πακέτων με πλαστές IP διευθύνσεις πηγής
  - Κρυπτογραφημένες λίστες διευθύνσεων σε χειριστή από επιτιθέμενο (αλγόριθμος Blowfish)
  - Δυνατότητα έναρξης διαφορετικών τύπων επιθέσεων άρνησης υπηρεσίας

Προστασία από Επίθεση TFN

- Στον χειριστή υπάρχει πάντα μια λίστα διαθέσιμων πρακτόρων με τις IP διευθύνσεις τους. Αν η λίστα δεν είναι κρυπτογραφημένη οι πράκτορες μπορούν να αναγνωριστούν από τη λίστα.

- Διαμόρφωση δρομολογητή να μην επιτρέπει το πέρασμα πακέτων ICMP_ECHO_REPLY (χρήση ICMP_ECHO_REPLY σε επικοινωνία χειριστών-πρακτόρων)
  - Μπλοκάρισμα και χρήσιμων επικοινωνιών.

- Πλαστογράφηση ICMP πακέτων και αποστολή μηνύματος κλεισίματος σε πράκτορες. Οι πράκτορες δεν ελέγχουν την πηγή των μηνυμάτων ICMP_ECHO_REPLY.

Επίθεση TFN2K

- Εξελιγμένη έκδοση TFN.
- Διαφορές με TFN:
  - Οι πράκτορες είναι αθόρυβοι, δεν επιβεβαιώνουν τις εντολές που λαμβάνουν. Ο χειριστής στέλνει κάθε εντολή 20 φορές και ελπίζει ότι κάποια από αυτές θα φτάσει σε πράκτορα.
  - Επικοινωνία χειριστών-πρακτόρων με πακέτα ICMP, UDP και TCP
  - Κρυπτογράφηση εντολών με αλγόριθμο CAST-256 (RFC 2612)
  - Καθορισμός χειριστή με τυχαίες IP διευθύνσεις πηγής και αριθμούς θυρών TCP/UDP

Προστασία από Επίθεση TFN2K

Έλεγχος λίστας διεργασιών για παρουσία διεργασιών πρακτόρων σε περίπτωση που δεν έχει εγκατασταθεί κάποιο rootkit.

Επίθεση Stacheldraht 1/2

- Η λέξη Stacheldraht σημαίνει barbed σύρμα.
- Είναι ένα κατανεμημένο εργαλείο που χρησιμοποιείται για την έναρξη των επιθέσεων SYN, UDP, ICMP και Smurf.
- Υποστηρίζει (ομοίως με Trin00, TFN/TFN2K):
  - Αρχιτεκτονική client/server (επικοινωνία επιτιθέμενου και χειριστή μέσω TCP και επικοινωνία χειριστή και πράκτορα μέσω πακέτων ICMP_ECHO_REPLY)
  - Εύκολη στη χρήση διεπαφή
  - Ικανότητα αλλαγής τύπου, διάρκειας και έντασης επίθεσης

Επίθεση Stacheldraht 2/2

Υποστηρίζει μοναδικά:

- Αυτόματη ενημέρωση πρακτόρων
  - Ένας επιτιθέμενος με μια εντολή ειδοποιεί τους πράκτορες να κατεβάσουν νέο λογισμικό από συγκεκριμένο ιστότοπο.
  - Διασφαλίζει εύκολη ανάπτυξη και επιδιόρθωση σφαλμάτων σε λογισμικό πρακτόρων.
- Επικοινωνία χειριστών και πρακτόρων με χρήση κρυπτογράφησης (αλγόριθμος Blowfish)
- Αναγνώριση δικτύων που επιτρέπουν τη δημιουργία πακέτων με πλαστογραφημένη πηγή. Αυτά τα δίκτυα δε μπορούν να αναγνωρίσουν την πραγματική διεύθυνση ενός πράκτορα και να διαμορφώσουν το δρομολογητή ώστε να μπλοκάρει την πλημμύρα άχρηστων πακέτων.

Προστασία από Επίθεση Stacheldraht

Παρακολούθηση επικοινωνίας εισερχόμενης κυκλοφορίας.

Παρακολούθηση θυρών που χρησιμοποιούνται για ενημέρωση πρακτόρων.

Τρόποι Άμυνας για Αποφυγή Μόλυνσης

Οι επιθέσεις άρνησης υπηρεσίας μπορούν να ξεκινήσουν από τον καθένα, από οπουδήποτε κάθε στιγμή. Έτσι, είναι δύσκολο να εμποδιστούν. Μπορεί όμως να μειωθεί ο κίνδυνος με:

- Σωστή εγκατάσταση firewall σε δρομολογητές δικτύου
- Σωστή διαμόρφωση firewall

Εγκατάσταση Firewall

Το firewall πρέπει να εγκαθίσταται στη σύνδεση ανάμεσα στον πάροχο (ISP) και το χρήστη για να μην επιτρέπει σε ανεπιθύμητα πακέτα να περνούν.

Διαμόρφωση Firewall 1/2

- Άρνηση άκυρων διευθύνσεων IP πηγής
- Άρνηση ιδιωτικών και κρατημένων διευθύνσεων IP πηγής
- Απενεργοποίηση άμεσης μετάδοσης IP σε όλα τα συστήματα.
- Απενεργοποίηση υπηρεσιών chargen και echo
- Απενεργοποίηση και φιλτράρισμα όλων των άλλων αχρησιμοποίητων υπηρεσιών UDP.

Διαμόρφωση Firewall 2/2

- Συχνή ενημέρωση συστημάτων για διορθώσεις.
- Ενημέρωση από τα δελτία ασφαλείας της CERT/CC
- Πληροφορίες για όλα τα απορριφθέντα πακέτα πρέπει να κρατούνται σε log files.
- Οι διαχειριστές συστήματος πρέπει να έχουν χρόνο και υποστήριξη για εκπαίδευση και βελτίωση ικανοτήτων.
- Τα συστήματα πρέπει να ελέγχονται περιοδικά για τον καθορισμό της παρουσίας κακόβουλου λογισμικού.

Τρόποι Ανίχνευση Εισβολής

- Έλεγχος για αποδείξεις εισβολείς σε log files
- Έλεγχος για ίχνη κατανεμημένων εργαλείων (ενημέρωση από CERT/CC)
- Ενεργοποίηση ανίχνευσης unsolicited μηνυμάτων ICMP_ECHO_REPLIES
- Έλεγχος επιπέδων κυκλοφορίας

Άρση Εισβολής

- Προσδιορισμός εισβολής (το σύστημα δρα ως χειριστής ή πράκτορας):
  - Αν το σύστημα δρα ως πράκτορας υπάρχει πιθανότητα να έχει εγκατασταθεί στο σύστημα μια λίστα χειριστών που μπορεί να είναι κρυπτογραφημένη. Η λίστα πρέπει να εξαχθεί και όλα τα συστήματα χειριστές πρέπει να ειδοποιηθούν ότι λειτουργούν ως χειριστές της εισβολής. Σε κάθε χειριστή θα πρέπει να εντοπιστεί η λίστα των υπολοίπων πρακτόρων και να σταλεί μια εντολή κλεισίματος.
  - Αν το σύστημα δρα ως χειριστής θα πρέπει να εντοπιστεί η λίστα των υπολοίπων πρακτόρων και να τους σταλεί μια εντολή κλεισίματος.

- Ο διαχειριστής του συστήματος πρέπει να ειδοποιήσει τους ISPs, IRTs (Incident Response Teams) και τις ομάδες επιβολής του νόμου.

Συμπεράσματα

- Παρόλη την καλή υποδομή και το έμπειρο προσωπικό διαχείρισης δεν υπάρχει εγγύηση ότι η επίθεση θα εμποδιστεί ή θα σταματήσει εγκαίρως λόγω αδυναμιών άλλων συστημάτων που μπορούν να καταληφθούν και να χρησιμοποιηθούν για επιθέσεις.

- Η κατάσταση επιδεινώνεται από την οικιακή εξάπλωση των ευρυζωνικών συνδέσεων που παρέχουν μια μεγάλη βάση συστημάτων μικρής ασφάλειας προς χρήση από τους επιτιθέμενους.

- Υπάρχει καλή ενημέρωση στο Διαδίκτυο για τρόπους αποφυγής τέτοιων επιθέσεων.