Κεφάλαιο 1

Δικτυακές Επιθέσεις, Μέθοδοι Υλοποίησης Τους και Επιπτώσεις.

Περιεχόμενα

Επιθέσεις

Επίθεση είναι οποιαδήποτε προσπάθεια για παραβίαση της *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.

Σημείωση – Ορισμός

Εμπιστευτικότητα (Confidentiality)
Μία επίθεση προκαλεί την παραβίαση της εμπιστευτικότητας, όταν ο επιτιθέμενος αποκτά πρόσβαση σε πληροφορίες για τις οποίες δεν είναι εξουσιοδοτημένος από τον κάτοχό τους.

Ακεραιότητα (Integrity)
Μία επίθεση προκαλεί παραβίαση της ακεραιότητας, όταν επιτρέψει στον (μη εξουσιοδοτημένο) επιτιθέμενο να αλλάξει την κατάσταση του συστήματος ή οποιασδήποτε πληροφορίας βρίσκεται σε αυτό.

Διαθεσιμότητα (Availability)
Μια επίθεση προκαλεί την παραβίαση της διαθεσιμότητας, όταν μέσω αυτής δεν επιτρέπεται στους εξουσιοδοτημένους χρήστες να έχουν πρόσβαση σε συγκεκριμένους πόρους του συστήματος όταν, όποτε και με τον τρόπο που έχουν εξουσιοδοτηθεί.

Μηχανισμοί Ασφάλειας και Ελέγχου Πρόσβασης (Control)
Μία επίθεση προκαλεί την παραβίαση των μηχανισμών ασφάλειας, όταν μέσω αυτής, ο (μη εξουσιοδοτημένος) επιτιθέμενος αποκτά πρόσβαση στους μηχανισμούς ελέγχου της πρόσβασης του συστήματος.
Η παραβίαση των μηχανισμών ασφαλείας μπορεί να οδηγήσει σε παραβίαση της Εμπιστευτικότητας, Ακεραιότητας ή της Διαθεσιμότητας .

Ποιος είναι ο τυπικός στόχος-θύμα μίας επίθεσης

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:

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.

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.

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 λόγο η επιτυχία μίας επίθεσης με έναν τέτοιο στόχο, θα συνέβαλε θετικά στο γόητρο και την φήμη του επιτιθέμενου.

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 :

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

- 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.

Επιτιθέμενοι

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 εθελημένα 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.

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)
  Προσφέρουν πολλά εργαλεία ενώ τα NT είναι πιο αξιόπιστα.
  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.

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.

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.

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.

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.

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.

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.

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. Το scanning θα παρουσιαστεί με λεπτομέρεια παρακάτω.

Vulnerabilities – Exploits

Τι είναι όμως αυτό που επιτρέπει στους επιτιθέμενους να ενεργήσουν και καθιστά δυνατή την υλοποίηση μίας επίθεσης;
Σε αυτό το σημείο είναι που εμφανίζονται οι όροι *vulnerability* και *exploit.*

Vulnerability είναι η αδυναμία που προκύπτει από την ύπαρξη ενός ελαττώματος ή προβλήματος, η εκμετάλλευσή της οποίας μπορεί να οδηγήσει στην παραβίαση ενός συστήματος.

Exploit είναι η μέθοδος με την οποία επιτυγχάνεται η εκμετάλλευση μίας αδυναμίας και υλοποιείται μία επίθεση. Από την στιγμή που θα ανακαλυφθεί ένα vulnerability δημιουργείται και το ανάλογο exploit που μπορεί να την εκμεταλλευτεί, το οποίο θα χρησιμοποιηθεί σε μία επίθεση.

Τα vulnerabilities προκύπτουν, από ελαττώματα που υπάρχουν σε διάφορα λογισμικά που οφείλονται σε προγραμματιστικά λάθη, από λάθη που γίνονται στην ρύθμιση των συστημάτων, από ατέλειες σχεδιασμού λογισμικών ή από ανεπαρκή μέτρα ασφάλειας. Πιο αναλυτικά:

- **Ελαττώματα στην ανάπτυξη Λογισμικών**

Τα ελαττώματα που παρουσιάζουν διάφορα λογισμικά τις περισσότερες φορές οφείλονται σε προγραμματιστικά λάθη κατά την ανάπτυξή τους.
Τέτοιου είδους ελαττώματα μπορούν να κατηγοριοποιηθούν με τον εξής τρόπο:

Buffer Overflows
Τα Buffer Overflows ίσως αποτελούν τον στόχο των περισσότερων exploits. Τα Buffer Overflows προκύπτουν από την ανεξέλεγκτη είσοδο δεδομένων που χειρίζεται μία μεταβλητή σε ένα πρόγραμμα, που μπορεί να οδηγήσει σε απρόσμενη συμπεριφορά του προγράμματος.
Όταν τα δεδομένα που δίνονται από τον χρήστη σε μία μεταβλητή σαν είσοδο, ξεπεράσουν τα όρια της μεταβλητής αυτής, μπορεί η εκτέλεση του προγράμματος να υπερπηδήσει σε κάποιο σημείο της μνήμης του συστήματος εκτός του προγράμματος. Αν η ποσότητα των δεδομένων αυτών είναι κατάλληλα υπολογισμένη θα μπορούσε να δώσει την ευκαιρία στον επιτιθέμενο ακόμα και να πάρει τον έλεγχο του συστήματος. Τέτοιου είδους προβλήματα παρουσιάζουν γλώσσες προγραμματισμού όπως η C, στην οποία ο έλεγχος των ορίων μίας μεταβλητής δεν γίνεται από τους εσωτερικούς μηχανισμούς της γλώσσας, αλλά είναι στην ευθύνη του προγραμματιστή.

Απρόσμενη Είσοδο Δεδομένων
Τέτοιου είδους προβλήματα προκύπτουν όταν ένα πρόγραμμα δεν είναι έτσι σχεδιασμένο ώστε να μπορεί να χειρίζεται όλους τους πιθανούς συνδυασμούς με τους οποίους ο

χρήστης μπορεί να δώσει δεδομένα σαν είσοδο σε αυτό. Κάθε πρόγραμμα κατά τον σχεδιασμό του και μετά το τέλος της υλοποίησής του θα πρέπει να δοκιμάζεται και να ελέγχεται εξονυχίστηκα, ώστε να αποτρέπονται προβλήματα που μπορεί να δημιουργηθούν από την μη φυσιολογική χρήση του προγράμματος.

- **Ελαττώματα στην ρύθμιση των συστημάτων και των υπηρεσιών που προσφέρουν**

Τέτοιου είδους προβλήματα προκύπτουν από:

Εξ 'ορισμού Ρυθμίσεις
Οι εξ ορισμού ρυθμίσεις που έχουν τα περισσότερα συστήματα κατά την απόκτησή τους είναι συνήθως ανεπαρκείς και παρουσιάζουν αρκετά προβλήματα ασφάλειας. Ένα τέτοιο παράδειγμα μπορεί να αποτελεί η απόκτηση ενός Windows NT/2000 συστήματος. Η πρώτη προτεραιότητα σε αυτήν την περίπτωση θα ήταν το σύστημα αυτό να ενημερωθεί με τα τελευταία Service Packs που το αφορούν.

Λανθασμένη διαχείριση ενός συστήματος.
Πολλοί διαχειριστές συστημάτων, είτε γιατί έχουν άγνοια, είτε γιατί δεν ενδιαφέρονται αρκετά, δεν ενημερώνουν τακτικά τα συστήματά τους με νέες διορθώσεις ασφάλειας σε πιθανές αδυναμίες που αυτά μπορεί να έχουν. Επίσης δεν τηρούν κάποιους βασικούς κανόνες ασφάλειας στα συστήματα που διαχειρίζονται, όπως την εφαρμογή ασφαλών passwords στους λογαριασμούς των χρηστών και δεν παρακολουθούν συστηματικά τα αρχεία καταγραφής των συστημάτων αυτών.

Ύπαρξη υπηρεσιών που δεν χρειάζονται.
Πολλά προβλήματα μπορεί να προκύψουν όταν ένα σύστημα τρέχει υπηρεσίες οι οποίες δεν είναι χρήσιμες και δεν χρησιμοποιούνται από κάποιον. Αυτές οι υπηρεσίες πρέπει σε κάθε περίπτωση να απενεργοποιούνται. Με αυτόν τον τρόπο ελαχιστοποιείται ο κίνδυνος που προκύπτει από την εκμετάλλευση μίας αδυναμίας που μπορεί να έχει κάποια από αυτές τις υπηρεσίες. Επίσης οι υπηρεσίες που είναι ενεργές και δεν χρησιμοποιούνται συνήθως δεν ελέγχονται από τον διαχειριστή του συστήματος και δεν ενημερώνονται με νέες διορθώσεις που μπορεί να υπάρχουν για αυτές.

- **Ατέλειες στον αρχικό σχεδιασμό λογισμικού**

Ακόμα και αν ένα λογισμικό είναι σωστό σύμφωνα με τον σχεδιασμό του υπάρχει η πιθανότητα ο ίδιος ο σχεδιασμός να έχει ατέλειες. Ένα αντιπροσωπευτικό παράδειγμα αποτελεί ο σχεδιασμός των πρωτοκόλλων του TCP/IP.
Την εποχή που τα πρωτόκολλα αυτά σχεδιάστηκαν, οι ανάγκες που απαιτούνταν να καλύψουν, τόσο σε θέματα λειτουργικότητας όσο και ασφάλειας, ήταν πολύ λιγότερες από αυτές που προκύπτουν σήμερα με την ραγδαία ανάπτυξη του Internet και των υπηρεσιών που προσφέρει.

- **Ανεπαρκή μέτρα ασφάλειας**

Πολλά προβλήματα μπορούν να προκύψουν από την εφαρμογή ανεπαρκών μέτρων ασφάλειας σε ένα σύστημα ή ένα δίκτυο. Πολλοί θεωρούν ότι η εφαρμογή ενός Firewall σε ένα δίκτυο είναι αρκετή για να το προστατέψει επαρκώς από κάθε είδους επιθέσεις που μπορεί να έχουν στόχο το

δίκτυο αυτό. Αυτή είναι μία λανθασμένη προσέγγιση που μπορεί να οδηγήσει σε ανεπιθύμητα αποτελέσματα.

Από τα παραπάνω γίνεται εμφανές ότι τα vulnerabilities μπορούν να προέρχονται από διάφορες πηγές, ενώ καθημερινά εμφανίζονται και νέα, για κάθε ένα από τα οποία υπάρχει και το ανάλογο exploit που μπορεί να οδηγήσει σε μία πετυχημένη επίθεση.
Οι εταιρίες ανάπτυξης λογισμικού κάθε τόσο διανέμουν μέσω του διαδικτύου διάφορες διορθώσεις σε vulnerabilities που γνωστοποιούνται για τα προϊόντα τους, οι οποίες πρέπει να παρακολουθούνται συστηματικά και να λαμβάνονται σοβαρά υπόψη από τους διαχειριστές και τους υπεύθυνους ασφάλειας συστημάτων.

Η σημερινή εποχή χαρακτηρίζεται από έναν συνεχή αγώνα, της μίας πλευράς για την ανακάλυψη νέων vulnerabilities και εκμετάλλευσης αυτών και της άλλης πλευράς για την διόρθωσή τους και την προστασία από τα exploits που τα εκμεταλλεύονται.

Κατηγοριοποίηση των Επιθέσεων

Στις επόμενες σελίδες θα γίνει μία προσπάθεια κατηγοριοποίησης των διαφόρων ειδών επιθέσεων. Οι επιθέσεις μπορούν να ταξινομηθούν λαμβάνοντας υπόψη διαφορετικούς παράγοντες κάθε φορά, οι οποίοι έχουν να κάνουν με την θέση των συστημάτων που παίρνουν μέρος σε μία επίθεση, τον τρόπο που υλοποιείται μία επίθεση, την αλληλεπίδραση του επιτιθέμενου με τον στόχο, αλλά και τα αποτελέσματα μίας επίθεσης.

Τοπικές - Απομακρυσμένες Επιθέσεις

Ο διαχωρισμός αυτός έχει να κάνει με την θέση του επιτιθέμενου σε σχέση με τον στόχο του.

Τοπικές είναι οι επιθέσεις στις οποίες ο επιτιθέμενος έχει φυσική πρόσβαση στο σύστημα στο οποίο επιτίθεται. Στόχος του είναι είτε να αποκτήσει δικαίωμα πρόσβασης στο σύστημα ενώ δεν είναι εξουσιοδοτημένος για κάτι τέτοιο, είτε να αποκτήσει περισσότερα δικαιώματα από αυτά που του έχουν δοθεί ή να χρησιμοποιήσει τα δικαιώματα που του έχουν δοθεί με κακόβουλες προθέσεις.
Η πιο συνηθισμένη μέθοδος για να καταφέρει κάτι τέτοιο είναι με το να αποκτήσει το ***password*** (συνθηματικό) ενός εξουσιοδοτημένου λογαριασμού με περισσότερα δικαιώματα από τα δικά του. Η μέθοδος αυτή είναι γνωστή με τον όρο ***password stealing***.
Υπάρχουν διάφορες τεχνικές που κάποιος μπορεί να αποκτήσει ένα password που ανήκει σε κάποιον άλλον και οι περισσότερες από αυτές χρησιμοποιούν εργαλεία που αυτοματοποιούν την διαδικασία. Μερικές από αυτές τις τεχνικές αναφέρονται παρακάτω:

Τεχνικές Password Stealing

- **Social Engineering**
  Αυτή είναι μία από τις λιγότερο κοπιαστικές αλλά και πιο σπάνια επιτυχείς τεχνικές. Στην προκειμένη περίπτωση ο επιτιθέμενος καλεί στο τηλέφωνο το κέντρο διαχείρισης του δικτύου και προσποιείται ότι είναι ο κάτοχος του συστήματος. Υποστηρίζοντας ένα αρκετά πειστικό σενάριο, προφασίζεται ότι ξέχασε το password του λογαριασμού του και ότι είναι άμεσα επείγον να του το υπενθυμίσουν ή να το απενεργοποιήσουν ώστε να μπορέσει να ορίσει ένα άλλο. Η τεχνική αυτή έχει λειτουργήσει ικανοποιητικά στο παρελθόν ενώ σήμερα είναι μάλλον απίθανο κάποιος αρμόδιος σε ένα κέντρο διαχείρισης να πέσει σε αυτήν την παγίδα.

- **Ανεύρεση εύκολων passwords**
  Αυτή είναι επίσης μία αρκετά εύκολη τεχνική και πολλές φορές έχει θετικά αποτελέσματα. Ο επιτιθέμενος αυτό που έχει να κάνει είναι να προσπαθήσει να μαντέψει το password κάποιου χρήστη. Πολλοί χρήστες που έχουν άγνοια για την καθοριστική σημασία των passwords, επιλέγουν απλά και ανεπαρκή passwords που βάζουν σε κίνδυνο την ασφάλεια του

συστήματος. Τέτοια passwords μπορεί να είναι κάποιοι αριθμοί, η ημερομηνία γέννησης του χρήστη, το όνομά του κλπ. Ο επιτιθέμενος το μόνο που έχει να κάνει είναι να δοκιμάσει μερικά από τα κλασσικά passwords που συχνά χρησιμοποιούν αδαής χρήστες μέχρι που να καταφέρει να μπει στο σύστημα.

- **Dictionary Attacks**

  Η τεχνική αυτή είναι παρόμοια με την προηγούμενη μόνο που σε αυτήν την περίπτωση ο επιτιθέμενος χρησιμοποιεί ένα εργαλείο που την υλοποιεί. Τέτοιου είδους εργαλεία ονομάζονται ***password crackers*** και συνήθως χρησιμοποιούν μία βάση γνώσης η οποία αποτελείται από όλες τις λέξεις ενός λεξικού (συνήθως του Αγγλικού). Ο μηχανισμός του εργαλείου αυτού θα δοκιμάσει όλες τις λέξεις του λεξικού μέχρι να βρει αυτή που αντιστοιχεί στο password.
  Αυτό μπορεί να το κάνει με δύο τρόπους. Με τον 1ο θα δοκιμάζει κάθε λέξη που ελέγχει, αν θα του επιτρέψει να μπει στο σύστημα. Αυτό σημαίνει ότι θα κάνει πολλαπλές προσπάθειες για login. Με τον 2ο τρόπο ο επιτιθέμενος θα πρέπει να έχει πρόσβαση στο αρχείο του συστήματος που διατηρεί τα passwords όλων των χρηστών σε κρυπτογραφημένη μορφή. Στην συνέχεια το *password cracker*, κάθε λέξη του λεξικού που ελέγχει την κρυπτογραφεί και εξετάζει αν αυτή ταιριάζει με κάποια από τα κρυπτογραφημένα passwords του αρχείου.

- **Brute Force Attacks**

  Οι επιθέσεις αυτές είναι όμοιες με τις Dictionary Attacks, με την διαφορά ότι το password cracker εργαλείο δεν χρησιμοποιεί κάποιο λεξικό για να βρει το password, άλλα δοκιμάζει όλους τους δυνατούς συνδυασμούς χαρακτήρων, μέχρι να μπορέσει να πετύχει αυτόν που αντιστοιχεί στο password.
  Τόσο αυτή όσο και η προηγούμενη τεχνική μπορεί να εκτελούνται για μέρες μέχρι να φτάσουν σε κάποιο θετικό αποτέλεσμα.

- **Παρακολούθηση**

  Ο επιτιθέμενος παρακολουθώντας διακριτικά την ώρα που κάνει login ο χρήστης του οποίου θέλει να πάρει το password, προσπαθεί να δει το password την ώρα που το πληκτρολογεί. Αυτή είναι μία αρκετά απλή και καθόλου έξυπνη τεχνική.

- **Keystroke Logging –Sniffing**

  Αυτή η τεχνική μοιάζει κάπως με την προηγούμενη αλλά χρησιμοποιεί μία αρκετά πιο έξυπνη μέθοδο. Ο επιτιθέμενος εγκαθιστά στο σύστημα ένα εργαλείο το οποίο έχει την δυνατότητα να καταγράφει σε ένα αρχείο οτιδήποτε ο χρήστης πληκτρολογεί. Τα εργαλεία αυτά ονομάζονται ***Keyloggers***. Μέσω ενός ***Keylogger*** ο επιτιθέμενος μπορεί να υποκλέψει διάφορες πληροφορίες που πληκτρολογεί ο χρήστης, όπως διάφορα passwords που έχει για διαφορετικές εφαρμογές ή και αριθμούς πιστωτικών καρτών όταν ο χρήστης κάνει συναλλαγές μέσω του Internet.
  Η τεχνική του ***sniffing*** παρουσιάζεται παρακάτω.

Απομακρυσμένες είναι οι επιθέσεις που υλοποιούνται σε δικτυωμένα συστήματα. Ο επιτιθέμενος προσπαθεί μέσω δικτύου να επιτεθεί σε ένα απομακρυσμένο σύστημα με στόχο είτε να αποκτήσει πρόσβαση στο μηχάνημα αυτό εκτελώντας κάποιο exploit, είτε να του προκαλέσει προβλήματα εμποδίζοντας την κανονική λειτουργία του.

Εσωτερικές - Εξωτερικές Επιθέσεις

Αυτός ο διαχωρισμός έχει να κάνει με τις απομακρυσμένες επιθέσεις όσο αναφορά την θέση του επιτιθέμενου σε σχέση με το δίκτυο στο οποίο επιτίθεται.

Εσωτερικές θεωρούνται οι επιθέσεις που πραγματοποιούνται από κάποιον που βρίσκεται εντός του δικτύου στο οποίο και επιτίθεται. Σε αυτήν την περίπτωση ο επιτιθέμενος έχει κάποια εξουσιοδοτημένα δικαιώματα για τις ενέργειές του μέσα στο δίκτυο και προσπαθεί να αποκτήσει περισσότερα. Στατιστικά οι περισσότερες πετυχημένες επιθέσεις που συμβαίνουν σήμερα σε δικτυωμένα συστήματα, προέρχονται από άτομα που ανήκουν στο εσωτερικό του δικτύου, καθώς για αυτούς υπάρχει κάποιος βαθμός εμπιστοσύνης τον οποίο και εκμεταλλεύονται.
Τα άτομα αυτά συνήθως έχουν κάποιο λογαριασμό, έστω και με περιορισμένα δικαιώματα, στο σύστημα που επιτίθενται, γνωρίζουν κάποιες χρήσιμες πληροφορίες για το δίκτυο και το σύστημα που θα επιτεθούν, όπως τι είδους είναι και τι αδυναμίες μπορεί να παρουσιάζει, συνήθως έχουν συγκεκριμένο στόχο και λόγους που υλοποιούν την επίθεση και δεν χρειάζεται να αντιμετωπίσουν τους μηχανισμούς ασφάλειας που προστατεύουν το δίκτυο από εξωτερικούς κινδύνους.

Εξωτερικές είναι οι επιθέσεις που πραγματοποιούνται από άτομα που βρίσκονται εκτός του δικτύου. Σε αυτήν την περίπτωση η αποστολή του επιτιθέμενου είναι σαφώς πιο δύσκολη, καθώς υποτίθεται ότι γνωρίζει λίγα για το δίκτυο στο οποίο επιτίθεται, δεν έχει κάποιον εξουσιοδοτημένο λογαριασμό και για να μπορέσει να πετύχει το στόχο του πρέπει να καταφέρει να προσπεράσει τους μηχανισμούς προστασίας που προφυλάσσουν το δίκτυο από εξωτερικούς κινδύνους. Σε μία εξωτερική επίθεση ο επιτιθέμενος μπορεί και να μην έχει κάποιο συγκεκριμένο στόχο και απλά να ψάχνει να εντοπίσει κάτι που θα του φανεί χρήσιμο.

Παθητικές – Ενεργητικές Επιθέσεις

Ο διαχωρισμός αυτός έχει να κάνει με τον βαθμό της αλληλεπίδρασης που έχει ο επιτιθέμενος με τον στόχο του.

Παθητικές είναι οι επιθέσεις στις οποίες ο επιτιθέμενος εκτελεί ενέργειες που απαιτούν την ελάχιστη αλληλεπίδραση με τον στόχο του. Οι επιθέσεις αυτού του είδους δεν προκαλούν κάποια αλλαγή στην κατάστασή του θύματος και δεν έχουν σαν στόχο να το βλάψουν άμεσα. Οι ενέργειες του επιτιθέμενου έχουν να κάνουν με την παρακολούθηση του στόχου και συλλογή πληροφοριών για αυτόν.
Οι παθητικές επιθέσεις αποτελούν στην ουσία ενέργειες που προηγούνται μίας άλλης επίθεσης, καθώς τις πληροφορίες που θα συλλέξει ο επιτιθέμενος μέσω αυτών θα τις εκμεταλλευτεί ώστε να υλοποιήσει την κύρια επίθεση του.
Μία τέτοιου είδους ενέργεια είναι και το ***sniffing***. Με το *sniffing* ο επιτιθέμενος είναι ικανός να βλέπει όλα τα πακέτα που ανήκουν στην δικτυακή κίνηση (traffic), που δημιουργείται από την

επικοινωνία του θύματος με τα υπόλοιπα δικτυωμένα συστήματα και το Internet. Το *sniffing* συνήθως υλοποιείται από ειδικά προγράμματα τα οποία ονομάζονται ***sniffers*** και εκτελούνται σε κάποιο σημείο του δικτύου από το οποίο περνάει το traffic που αφορά το σύστημα-στόχο.
Για παράδειγμα σε ένα τοπικό LAN, που διάφορα συστήματα συνδέονται με ένα Hub, αν σε κάποιο από αυτά έχει εγκατασταθεί και λειτουργεί ένα *sniffer,* τότε αυτό μπορεί να βλέπει όλο το traffic του LAN και τις πληροφορίες που ανταλλάσσονται μεταξύ των συστημάτων του.
Μέσω του sniffing ο επιτιθέμενος μπορεί να συλλέξει σημαντική πληροφορία η οποία μεταφέρεται μέσα στα πακέτα που ανταλλάσσει το σύστημα-θύμα, όπως διάφορα passwords και usernames.

Ενεργητικές είναι οι επιθέσεις στις οποίες ο επιτιθέμενος έχει αυξημένη αλληλεπίδραση με τον στόχο του. Στην ουσία όλες οι επιθέσεις που δεν ανήκουν στις παθητικές είναι ενεργητικές. Ο επιτιθέμενος στέλνει διάφορα πακέτα στον στόχο του, μέσω των οποίων μπορεί να συλλέξει πληροφορίες για αυτόν ή και να υλοποιήσει ένα exploit.

Αναγνωριστικές - Penetration – Άρνησης Υπηρεσιών

Όλες ο επιθέσεις ανήκουν σε μία από αυτές τις κατηγορίες. Η διαφορά τους έχει να κάνει με το αποτέλεσμα που έχουν τόσο για το θύμα, όσο και για τον επιτιθέμενο.

Αναγνωριστικές είναι οι επιθέσεις τις οποίες εκτελεί ο επιτιθέμενος για να μαζέψει πληροφορίες για το θύμα του. Τέτοιες πληροφορίες μπορεί να είναι η τοπολογία του δικτύου στο οποίο θα επιτεθεί, το Λειτουργικό Σύστημα (Λ.Σ) του στόχου του, οι ανοιχτές πόρτες και οι υπηρεσίες που είναι διαθέσιμες προς εκμετάλλευση.
Οι αναγνωριστικές επιθέσεις είναι κυρίως μέθοδοι που χρησιμοποιεί ο επιτιθέμενος για μπορέσει να συγκεντρώσει πληροφορίες για το θύμα του, που θα του επιτρέψουν να εξαπολύσει στην συνέχεια την κύρια επίθεση με μεγαλύτερη πιθανότητα επιτυχίας. Η πιο διαδεδομένη μέθοδος αναγνώρισης του στόχου είναι το ***Scanning***.
Καθώς το scanning είναι το πιο συχνό φαινόμενο σήμερα στο Internet, όσο αναφορά τις δικτυακές επιθέσεις θα γίνει ειδική αναφορά για αυτό παρακάτω.

Penetration είναι οι επιθέσεις με τις οποίες ο επιτιθέμενος θα καταφέρει να παραβιάσει το σύστημα – στόχο και ως αποτέλεσμα θα αποκτήσει πρόσβαση σε αυτό.
Για να το καταφέρει, θα υλοποιήσει ένα exploit το οποίο θα εκμεταλλεύεται ένα συγκεκριμένο vulnerability που ο επιτιθέμενος εντόπισε στο θύμα του.
Η ζημιά που μπορεί να προκληθεί ως αποτέλεσμα μίας τέτοιας ενέργειας, εξαρτάται από τον βαθμό εξουσιοδότησης που θα έχει ο λογαριασμός με τον οποίο απέκτησε πρόσβαση ο επιτιθέμενος και την κρισιμότητα των πληροφοριών που περιέχονται στο σύστημα που παραβίασε.
Πολλές φορές ένα σύστημα που καταφέρνει να παραβιάσει ο επιτιθέμενος, το χρησιμοποιεί για να επιτεθεί στην συνέχεια μέσω αυτού σε άλλα συστήματα προσπαθώντας με αυτόν τον τρόπο να κρύψει κατά κάποιο τρόπο τα ίχνη του.

Άρνησης Υπηρεσιών είναι οι επιθέσεις που έχουν σαν στόχο να προκαλέσουν προβλήματα στην λειτουργία του συστήματος ή του δικτύου που πλήττουν ώστε να το εμποδίσουν να προσφέρει τις υπηρεσίες για τις οποίες είναι προορισμένο στους νόμιμους χρήστες του.
Τέτοιου είδους προβλήματα μπορεί να είναι η επανεκκίνηση, η παύση, η κατάρρευση ενός συστήματος ή η δημιουργία αυξημένου traffic και η συμφόρηση ενός δικτύου.

Οι επιθέσεις αυτές ονομάζονται ***(D)DoS*** – ***(Distributed)* Denial Of Service** επιθέσεις και εξηγούνται με περισσότερη λεπτομέρεια παρακάτω.

Αυτοματοποιημένες – Χειροκίνητες Επιθέσεις

Ο διαχωρισμός αυτός έχει να κάνει με τις επιθέσεις που υλοποιούνται αυτόματα από ένα πρόγραμμα και με αυτές που υλοποιεί ο ίδιος ο επιτιθέμενος έχοντας συνεχή αλληλεπίδραση με τον στόχο του.

Αυτοματοποιημένες είναι οι επιθέσεις που μέρος τους ή και ολόκληρες εκτελούνται από ένα πρόγραμμα που έχει γραφτεί για αυτόν τον σκοπό. Τέτοιου είδους προγράμματα μπορεί να είναι:

- **Viruses (ιοί)**
  Είναι βλαβερά προγράμματα που έχουν την ιδιότητα να συνυπάρχουν με κάποιο εκτελέσιμο αρχείο και να ενεργοποιούνται με την εκτέλεσή του. Η ενεργοποίηση του ιού έχει σαν αποτέλεσμα να εκτελεστεί ο κώδικάς του και να αναπαραχθεί, μολύνοντας και άλλα αρχεία του συστήματος με απρόβλεπτα αποτελέσματα για το σύστημα. Για να μολυνθεί κάποιο σύστημα με ιό θα πρέπει πρώτα το αρχείο που τον περιέχει να μπει με κάποιο τρόπο στο σύστημα και να εκτελεστεί. Ο πιο συνηθισμένος τρόπος που μπορεί να συμβεί αυτό, είναι με την μορφή επισυναπτόμενων μολυσμένων αρχείων που ανταλλάσσονται μέσω mail μηνυμάτων.

- **Worms**
  Είναι βλαβερά προγράμματα που έχουν την ικανότητα να μεταδίδονται από το ένα σύστημα στο άλλο μέσω δικτύου και να το μολύνουν. Τα worms αναπαράγονται αυτόματα και δεν απαιτείται η εκτέλεση του κώδικά τους από κάποιον.

- **Trojans**
  Τα Trojans είναι βλαβερά προγράμματα που έχουν την ικανότητα να συνυπάρχουν με άλλα προγράμματα του συστήματος, μεταβάλλοντας την λειτουργία τους όταν αυτά εκτελεστούν.

- **Rootkits**

  Τα rootkits είναι εργαλεία τα οποία ο επιτιθέμενος εγκαθιστά σε ένα σύστημα-θύμα και εκτελούν διάφορες λειτουργίες προς όφελός του. Ο επιτιθέμενος πρέπει προηγουμένως να έχει αποκτήσει πρόσβαση στο σύστημα-θύμα έτσι ώστε να μπορέσει να εγκαταστήσει ένα rootkit. Ένα rootkit είναι ένα σύνολο προγραμμάτων τα οποία επιτρέπουν στον επιτιθέμενο να συλλέγει κωδικούς από το θύμα, να βλέπει τα πακέτα που κινούνται από και προς το θύμα , να αφήσει ένα backdoor το οποίο θα του επιτρέπει μελλοντική πρόσβαση στο σύστημα-θύμα διατηρώντας έτσι τα δικαιώματα που είχε προηγουμένως αποκτήσει, να διατηρεί κρυφή την παρουσία του.

  Μερικά από τα κύρια συστατικά ενός rootkit είναι τα παρακάτω :

Backdoors
Η κύρια λειτουργία ενός rootkit είναι να δώσει την δυνατότητα στον επιτιθέμενο να μπορεί μελλοντικά να μπαίνει στο σύστημα-θύμα χωρίς να γίνεται αντιληπτός. Αυτό γίνεται εγκαθιστώντας ένα backdoor, συνήθως trojaned προγράμματα που χρησιμοποιούνται για απομακρυσμένη πρόσβαση στο σύστημα όπως telnet ή ssh.
Αυτά τα προγράμματα τρέχουν σε διαφορετική TCP ή UDP πόρτα από αυτή που προορίζονται στην κανονική τους λειτουργία.

Trojaned System Utilities
Τα rootkits για να κρύψουν τα ίχνη του επιτιθέμενου αντικαθιστούν κάποια διαγνωστικά εργαλεία του λειτουργικού συστήματος τα οποία χρησιμεύουν για να γίνεται παρακολούθηση των δραστηριοτήτων που συμβαίνουν στο σύστημα, όπως τα `ps, w, who, netstat, ls, find` , με κάποια παραλλαγή τους που έχει την ίδια λειτουργία, κρύβοντας όμως τις δραστηριότητες του επιτιθέμενου.

Παρακάτω παρουσιάζονται κάποια από τα πιο συνήθη προγράμματα ενός συστήματος που αντικαθιστούνται με trojaned εκδόσεις τους από ένα rootkit και οι λειτουργίες τους.

Το Πρόγραμμα Που Αντικαθιστά Το RootKit	**Η Κανονική Λειτουργία Του Προγράμματος**	**Η Λειτουργία Του Trojaned Προγράμματος**
du	Εμφανίζει την κατάσταση του δίσκου του συστήματος δείχνοντας το ποσό του δίσκου που είναι κατελημένο και αυτό που είναι διαθέσιμο.	Ψεύδεται για τον διαθέσιμο χώρο του δίσκου κρύβοντας τα sectors του δίσκου που χρησιμοποιούνται από τα εργαλεία του επιτιθέμενου.
find	Επιτρέπει στους χρήστες να βρίσκουν αρχεία και φακέλους καθώς και προγράμματα και αρχεία που τροποποιήθηκαν πρόσφατα.	Ψεύδεται για την παρουσία των αρχείων του επιτιθέμενου όπως προγράμματα και άλλα εργαλεία, κρύβοντας την παρουσία τους.
ifconfig	Εμφανίζει την κατάσταση των interfaces και δείχνει ποια interfaces είναι σε promiscuous mode	Κρύβει το promiscuous mode έτσι ώστε ο χρήστης να μην μπορέσει να εντοπίσει κάποιο sniffer που τρέχει στο σύστημα.
login	Επιτρέπει στους χρήστες να κάνουν login στο σύστημα.	Επιτρέπει στους χρήστες να κάνουν login στο σύστημα, αλλά επίσης δημιουργεί ένα backdoor κάνοντας διαθέσιμο στον επιτιθέμενο ένα root-level password.
ls	Δείχνει τα περιεχόμενα ενός καταλόγου.	Δείχνει τα περιεχόμενα ενός καταλόγου, κρύβοντας όμως την παρουσία των αρχείων του rootkit.

netstat	Χρησιμοποιείται για να εμφανίζει τα processes που ακούνε σε διάφορες TCP και UDP πόρτες και τις ενεργές συνδέσεις του συστήματος.	Ψεύδεται για συγκεκριμένες πόρτες που χρησιμοποιούνται από τον επιτιθέμενο, κρύβοντας το γεγονός ότι κάποιο process ακούει εκεί που μπορεί να χρησιμοποιηθεί σαν backdoor.
ps	Εμφανίζει μια λίστα των processes που τρέχουν στο σύστημα.	Ψεύδεται για τα processes που θέλει ο επιτιθέμενος να κρύψει.

Πίνακας 1-1: Trojaned Προγράμματα από ένα rootkit

Log – wiping utilities

Μια άλλη τεχνική που χρησιμοποιούν τα rootkits για να κρύψουν τα ίχνη του επιτιθέμενου είναι η χρήση κάποιων λειτουργιών με τις οποίες αλλάζουν τα log files του συστήματος, όπως τα messages, και syslog τα οποία κοιτάει ένας χρήστης για να ελέγξει τις δραστηριότητες που παίρνουν μέρος κάθε χρονική στιγμή στο σύστημα. Σε μερικές περιπτώσεις τα rootkits απενεργοποιούν τελείως την δυνατότητα του συστήματος να καταγράφει την δραστηριότητα που λαμβάνει μέρος. Κάτι τέτοιο όμως μπορεί να κινήσει υποψίες σε έναν χρήστη και δεν είναι χρήσιμο στον επιτιθέμενο σε περίπτωση που θέλει να μείνει αρκετή ώρα στο σύστημα.
Συνήθως τα rootkits τροποποιούν τα log files και διαγράφουν μόνο τις εγγραφές που αφορούν τις ενέργειες του επιτιθέμενου.

Sniffers and Keyloggers

Ορισμένα rootkits περιέχουν προγράμματα τα οποία χρησιμοποιούνται για να συλλέγουν κωδικούς για άλλα συστήματα και να ακούνε την κίνηση των πακέτων σε ένα δίκτυο. Για να το καταφέρουν αυτό τα rootkits θέτουν την λειτουργία της κάρτας δικτύου (NIC) του συστήματος-θύμα σε Promiscious mode.
Κατά την κανονική λειτουργία της η NIC ενός συστήματος που είναι συνδεδεμένο σε ένα τοπικό δίκτυο, ακούει στο κοινό μέσο σύνδεσης και κρατάει τα πακέτα που προορίζονται γι'αυτήν ενώ απορρίπτει όλα τα άλλα. Όταν όμως η NIC έχει τεθεί σε Promiscious mode έχει την δυνατότητα να ακούει την κίνηση που προορίζεται για άλλα συστήματα του δικτύου, και έτσι μπορεί κάποιος να συλλέξει ευαίσθητες πληροφορίες για άλλα συστήματα που ενδεχομένως να μην του επιτρεπόταν.
Τέτοιου είδους πληροφορίες μπορεί να είναι userids και passwords συμπεριλαμβανομένου και του root, για διάφορα σημαντικά συστήματα του δικτύου στο οποίο είναι συνδεδεμένο το σύστημα-θύμα.

Τα RootKits διατίθενται για μία μεγάλη ποικιλία από πλατφόρμες αλλά κυρίως για Unix συστήματα όπως Solaris, SunOS, Linux, AIX, HP-UX και άλλα.
Επίσης υπάρχουν και rootKits για Windows NT/2000 συστήματα τα οποία αντικαθιστούν κάποια DLL's (Dynamic Link Libraries) του συστήματος.

- **Scanners**

Είναι προγράμματα που αυτοματοποιούν την διαδικασία του Scanning που αναφέρθηκε παραπάνω και θα παρουσιαστεί με λεπτομέρεια στη συνέχεια.

- **Autorouters**

Είναι προγράμματα που κάνουν την ζωή των Script Kiddies πιο εύκολη. Οι autorouters είναι η πιο προχωρημένη μορφή της αυτοματοποιημένης επίθεσης καθώς εκτελούν όλα τα βήματα που απαιτούνται για την υλοποίησής της. Ένας autorouter θα εκτελέσει το απαραίτητο scanning για να εντοπίσει επιρρεπή συστήματα, θα δοκιμάσει να εκτελέσει το ανάλογο exploit σε αυτά ώστε να εκμεταλλευτεί τα πιθανά vulnerabilities που θα έχει το κάθε σύστημα και στην συνέχεια στα συστήματα που θα καταφέρει να πάρει πρόσβαση θα εγκαταστήσει κάποιο rootkit ώστε να κρύψει τα ίχνη της επίθεσης και να εγκαταστήσει κάποιο backdoor που θα επιτρέψει στον επιτιθέμενο να έχει πρόσβαση στο σύστημα όποτε επιθυμεί.
Το μόνο που έχει να κάνει ο επιτιθέμενος που έχει στην κατοχή του έναν autorooter, είναι απλά κάποιες απλές ρυθμίσεις και κυρίως να ορίσει το εύρος των IP διευθύνσεων στις οποίες επιθυμεί ο autorouter να ενεργήσει.

Χειροκίνητες είναι οι επιθέσεις στις οποίες το κάθε βήμα υλοποίησής τους γίνεται από ενέργειες του ίδιου του επιτιθέμενου και όχι από κάποιο έτοιμο πρόγραμμα. Οι επιθέσεις αυτού του είδους συνήθως υλοποιούνται από πιο έμπειρους επιτιθέμενους που έχουν πιο σοβαρούς σκοπούς και είναι πιο επικίνδυνοι.

Scanners και Scanning

Παραπάνω στην αναφορά στις αναγνωριστικές επιθέσεις έγινε νύξη στην τεχνική του Scanning και στα εργαλεία που αυτοματοποιούν την υλοποίησή της, τους Scanners.
Στη συνέχεια ακολουθεί μία αναλυτική παρουσίαση της τεχνικής αυτής και των μεθόδων με τις οποίες υλοποιείται.

Scanners είναι προγράμματα τα οποία με αυτόματες διαδικασίες εντοπίζουν αδυναμίες σε ένα τοπικό ή απομακρυσμένο σύστημα.

Χαρακτηριστικά των Scanners

- Έχουν την δυνατότητα να εντοπίζουν συγκεκριμένες μηχανές ή δίκτυα
- Έχουν την δυνατότητα αφού βρουν μία μηχανή, να βρουν ποιες υπηρεσίες τρέχουν σε αυτή την μηχανή και τέλος
- Έχουν την δυνατότητα να δοκιμάζουν αυτές τις υπηρεσίες για γνωστά vulnerabilities.

Όλα τα παραπάνω γίνονται αυτόματα αφού πρώτα έχουν γίνει οι κατάλληλες ρυθμίσεις στο configuration του scanner, ανάλογα με το βάθος του scanning που επιθυμείται.
Για παράδειγμα κάποιος θα μπορούσε να ορίσει σε ένα scanner να ελέγξει αυτόματα όλες τις μηχανές οι οποίες ανήκουν σε ένα συγκεκριμένο εύρος IP διευθύνσεων και να εντοπίσει αν παρέχουν την υπηρεσία telnet σε απομακρυσμένους χρήστες.

Πλατφόρμες και Απαιτήσεις του Συστήματος

Οι περισσότεροι Scanners είναι γραμμένοι για χρήση σε Unix μηχανές και μερικοί για Windows NT.
Οι απαιτήσεις του συστήματος για την χρήση ενός Scanner, εξαρτώνται από το Scanner, το Λ.Σ και την ποιότητα της σύνδεσης του συστήματος στο Internet.
Επίσης Scanners που λειτουργούν σε command line χρειάζονται λιγότερη RAM από αυτούς που λειτουργούν σε παραθυρικό περιβάλλον.

Τέλος δεν λειτουργούν όλοι οι Scanners το ίδιο σε διαφορετικές πλατφόρμες. Κάποιες επιλογές ή και κάποιες λειτουργίες ενός Scanner μπορεί να μην είναι διαθέσιμες από μία πλατφόρμα σε μία άλλη.

Νομιμότητα και Χρησιμότητα των Scanners

Πολλά Scanners είναι διαθέσιμα στο Internet ενώ δεν είναι παράνομο κάποιος να κατέχει ή να χρησιμοποιεί ένα scanner. Παρόλα αυτά, χρησιμοποιώντας κάποιος ένα scanner για την συλλογή πληροφοριών ενός ξένου συστήματος, χωρίς να έχει έγκριση για κάτι τέτοιο, μπορεί να επιφέρει την έντονη αντίδραση του διαχειριστή του συστήματος αυτού και ανάλογα με το βάθος του scanning να επιβληθούν νομικές κυρώσεις σε αυτόν που το προκάλεσε.

Η χρησιμότητα ενός Scanner είναι μεγάλη, καθώς όταν χρησιμοποιείται από έναν διαχειριστή μπορεί να εμφανίσει τις αδυναμίες ενός δικτύου και των συστημάτων του και να συμβάλει θετικά στην διόρθωσή τους και την ενδυνάμωση της ασφάλειας τους.

Είδη Scanners

- **Host Scanners**

Τρέχουν τοπικά σε ένα σύστημα και διερευνούνε για κρίσιμα αρχεία του συστήματος που έχουν τροποποιηθεί και για τυχόν αδυναμίες στην ασφάλεια του συστήματος.
(Εργαλεία : Cops , Tiger , Check.pl).

- **Network Scanners**

Τρέχουν σε ένα host εναντίον άλλων μηχανών και εντοπίζουν υπηρεσίες που έχουν αδυναμίες.
(Εργαλεία : NSS, SATAN, Strobe, Nmap, Network Supescanner, Postscanner,Queso)

- **Intrusion (ή Vulnerability) Scanners**

Είναι προγράμματα τα οποία εντοπίζουν αδυναμίες στην ασφάλεια ενός συστήματος και σε ορισμένες περιπτώσεις εκμεταλλεύονται τις αδυναμίες αυτές.
(Εργαλεία : Nessus, Saint, Cheops, Ftpcheck / Relaycheck, BASS)

- **Firewall Scanners**

Αυτά τα προγράμματα ενεργούν πάνω σε firewalls και εφαρμόζουν διάφορα τεστ επιθέσεων με στόχο να ανακαλύψουν αν έχει ρυθμιστεί σωστά το firewall.
(Εργαλεία : Firewalk)

Οι Scanners λειτουργούν εφαρμόζοντας διάφορους τύπους Scanning σε διάφορα συστήματα και δίκτυα.

Scanning Ονομάζεται η διαδικασία κατά την οποία στέλνονται TCP/IP πακέτα διαφόρων πρωτοκόλλων σε διάφορα συστήματα και από την εξέταση των απαντήσεων που επιστρέφονται (ή δεν επιστρέφονται), συλλέγονται χρήσιμες πληροφορίες, όπως για το ποια συστήματα υπάρχουν και ανταποκρίνονται, ποια λειτουργικά συστήματα χρησιμοποιούν, ποιες υπηρεσίες (πόρτες) τρέχουν ('ακούνε') και ποιες από αυτές τις υπηρεσίες είναι επιρρεπείς σε επιθέσεις.

Μια κατηγοριοποίηση των διαφόρων τύπων Scanning ανάλογα με τα αποτελέσματα που επιστρέφουν είναι η παρακάτω :

Τύποι Scanning

- Ping Sweeps
- OS Detection
- Port Scanning
- Scanning For Vulnerabilities
- Firewalking

➢ Ping Sweeps

Το Scanning αυτού του τύπου είναι χρήσιμο καθώς ελέγχει αν ένα μηχάνημα με δεδομένη IP διεύθυνση υπάρχει.
Η εφαρμογή αυτών των μεθόδων σε πολλά συστήματα ενός δικτύου μπορεί να αποκαλύψει την τοπολογία του δικτύου, κάτι που είναι γνωστό με τον όρο ***Network Mapping***.

Μέθοδοι

1. ICMP sweeps (ICMP ECHO requests)
Είναι από τις πιο απλές μεθόδους scanning κατά την οποία στέλνονται ICMP_ECHO πακέτα με σκοπό να ελεγχθεί αν ο στόχος υπάρχει και αν ανταποκρίνεται. Αν ισχύει αυτό τότε θα απαντήσει με ICMP_REPLY πακέτα.

2. Non- Echo ICMP
Σε περίπτωση που τα ICMP_ECHO πακέτα φιλτράρονται (πχ από ένα firewall) και δεν γίνονται δεκτά, μπορούν να σταλούν ICMP πακέτα τύπου 13 (timestamp) ή 17 (address mask request) που χρησιμοποιούνται για την αναζήτηση της τρέχουσας ώρας ενός μηχανήματος από ένα άλλο και κατά την εκκίνηση, από μηχανές χωρίς δίσκο για την αναζήτηση της μάσκας του υποδικτύου, αντίστοιχα.

3. TCP Sweeps
Επίσης αντί για ICMP_ECHO πακέτα μπορούν να σταλούν TCP SYN ή TCP ACK πακέτα σε σωστά επιλεγμένες πόρτες (συνήθως 21, 22 , 23 , 24 , 80) και να παρατηρηθούν οι απαντήσεις που επιστρέφονται.

4. UDP Sweeps
Η τεχνική αυτή στηρίζεται στο γεγονός ότι στα περισσότερα συστήματα στέλνοντας ένα UDP πακέτο σε μια κλειστή πόρτα, τότε θα επιστραφεί ένα ICMP "Port Unreachable " μήνυμα λάθους. Στέλνοντας όμως ένα τέτοιο UDP πακέτο σε μια ανοιχτή πόρτα, δεν θα επιστραφεί κάποια απάντηση και έτσι εντοπίζονται οι κλειστές πόρτες και με την " μέθοδο της αφαίρεσης ", εντοπίζονται στη συνέχεια οι ανοιχτές πόρτες.

➢ OS Detection

Αυτός ο τύπος Scanning αποκαλύπτει το είδος του Λειτουργικού Συστήματος (Λ.Σ) του υπό εξέταση μηχανήματος.

Η χρησιμότητα του καθορισμού του Λ.Σ που χρησιμοποιεί ο στόχος είναι σημαντική, καθώς υπάρχουν συγκεκριμένα vulnerabilities που ανήκουν στο κάθε Λ.Σ .

Μέθοδοι

- **Banner Grabbing**

Αυτή η μέθοδος εκμεταλλεύεται το γεγονός ότι κάποιες υπηρεσίες (πχ. telnet) εμφανίζουν κάποιους banners, οι οποίοι αποκαλύπτουν πληροφορίες για το Λ.Σ.

Αυτό είναι ένα παράδειγμα που απεικονίζει την πληροφορία που μπορεί να εξαχθεί με την προσπάθεια για μία telnet σύνδεση σε ένα σύστημα.

```
localhost > telnet hpux.u-aizu.ac.jp
Trying 163.143.103.12 ...
Connected to hpux.u-aizu.ac.jp.
Escape character is '^]'.
HP-UX hpux B.10.01 A 9000/715 (ttyp2)
login:
```

- **TCP / IP Stack Fingerprinting**

Είναι μια μέθοδος η οποία κάνει διάφορες ερωτήσεις στην TCP/IP στοίβα του στόχου και στηρίζεται στο γεγονός ότι το κάθε Λ.Σ δεν υλοποιεί με τον ίδιο τρόπο την TCP/IP στοίβα. Έχοντας προηγουμένως μελετήσει τις διαφορές στην απόκριση των διαφόρων Λ.Σ στις ερωτήσεις αυτές , η μέθοδος αυτή μπορεί να καθορίσει το Λ.Σ που χρησιμοποιεί ο στόχος. Υπάρχουν αρκετές τεχνικές που υλοποιούν αυτή την μέθοδο και μερικές από αυτές αναφέρονται παρακάτω :

1. FIN probe

Στέλνεται ένα FIN πακέτο σε μια ανοιχτή πόρτα και ενώ κανονικά δεν θα έπρεπε να επιστραφεί κάποια απάντηση, κάποια Λ.Σ όπως MS Windows, BSDI, CISCO, HP/UX, MVS και IRIX στέλνουν πίσω ένα RESET (RST) πακέτο.

2. The Bogus Flag Probe

Με αυτή την τεχνική στέλνονται SYN πακέτα στον στόχο με ακαθόριστα Flags.
Κάποια Λ.Σ θα επιστρέψουν RST πακέτα διακόπτοντας την σύνδεση, ενώ το Linux διατηρεί την σύνδεση στέλνοντας πίσω πακέτα με το ίδια flags.

3. TCP ISN (Initial Sequence Numbers) Sampling

Η ιδέα αυτή στηρίζεται στην εύρεση προτύπων για τα αρχικά sequence numbers που στέλνονται από το TCP / IP, ως απάντηση σε αιτήσεις για εγκατάσταση σύνδεσης.
Για παράδειγμα στις Windows μηχανές το ISN αυξάνεται κατά ένα σταθερό μικρό μέγεθος κάθε χρονική περίοδο, ενώ στο Linux τα ISN έχουν τυχαίες τιμές.

4. Don't Fragment bit

Πολλά Λ.Σ θέτουν το΄'Don't Fragment " bit σε ορισμένα IP πακέτα που στέλνουν, κυρίως για λόγους καλύτερης απόδοσης.
Παρατηρώντας αυτά τα πακέτα μπορούν να βγουν συμπεράσματα για το Λ.Σ του στόχου.

5. TCP Initial Window
Με αυτή την τεχνική ελέγχεται το μέγεθος του παραθύρου (Window Size) στα πακέτα που επιστρέφονται από τον στόχο. Η τιμή του window size που τίθεται από το κάθε Λ.Σ είναι σχεδόν σταθερή και καθορίζει μονοσήμαντα το λειτουργικό αυτό.
Για παράδειγμα το AIX χρησιμοποιεί την τιμή 0x3F25, ενώ τα NT, OpenBSD και FreeBSD χρησιμοποιούν την τιμή 0x402E.

6. ACK Value
Η τεχνική αυτή ελέγχει την τιμή του πεδίου ACK στα πακέτα που στέλνονται από τον στόχο, η οποία σε κάποιες περιπτώσεις είναι διαφορετική για κάθε Λ.Σ .
Για παράδειγμα όταν σταλεί ένα FIN | PSH | URG πακέτο σε μια κλειστή πόρτα στον στόχο, τα περισσότερα Λ.Σ θα στείλουν πακέτο με την τιμή του ACK ίδια με αυτή του Initial Sequence Number (ISN) που είχε το πακέτο που έλαβαν, ενώ τα Windows θα θέσουν στο ACK την τιμή ISN + 1.

7. ICMP Error Message Quenching
Πολλά Λ.Σ οριοθετούν τον ρυθμό με τον οποίο μπορούν να στέλνονται διάφορα μηνύματα λάθους.
Έτσι στέλνοντας για παράδειγμα πολλά πακέτα σε μια τυχαία υψηλή UDP πόρτα και μετρώντας τον αριθμό των πακέτων που επιστρέφονται τα οποία μεταφέρουν μήνυμα λάθους "Unreachable" , είναι δυνατό να αναγνωριστεί το Λ.Σ που χρησιμοποιεί ο στόχος.
Για παράδειγμα το Linux περιορίζει τον αριθμό των " Unreachable" μηνυμάτων που θα στείλει στα 80 ανά 4 δευτερόλεπτα.

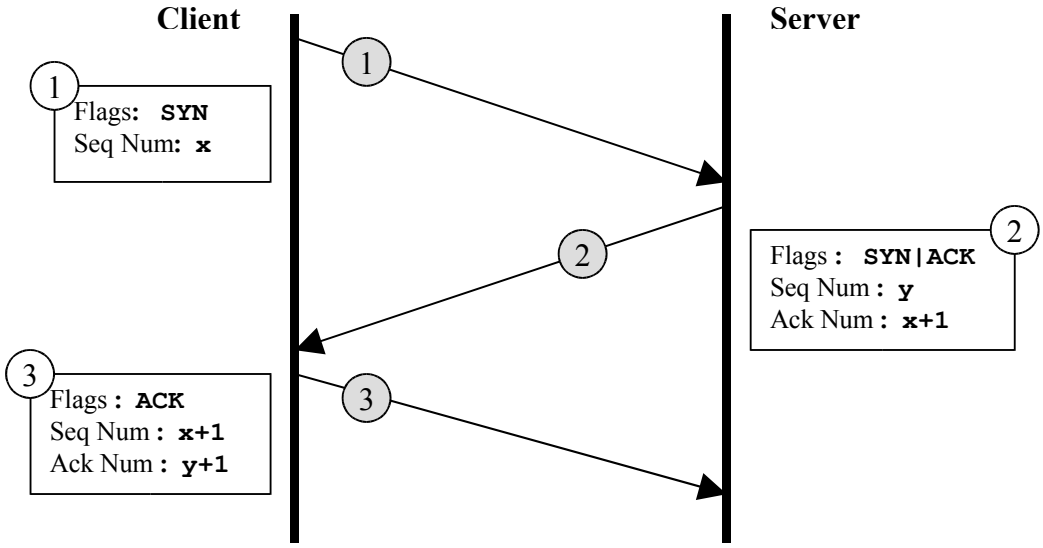
8. ICMP Message Quoting
Παρατηρώντας επίσης την μορφή των πακέτων που περιέχουν κάποιο μήνυμα λάθους είναι δυνατό να καθοριστεί το είδος του Λ.Σ που δημιούργησε αυτό το πακέτο.
Για παράδειγμα τα περισσότερα Λ.Σ στέλνουν πίσω σαν "Unreachable" μήνυμα λάθους μόνο τον απαραίτητο IP header + 8 bytes, ενώ οι Solaris μηχανές στέλνουν πίσω ένα bit παραπάνω και οι Linux μηχανές ακόμα περισσότερα.

9. Type of Service (TOS)
Μία ιδιαιτερότητα που έχει το Linux είναι ότι στα "Port Unreachable" μηνύματα λάθους που στέλνει θέτει την τιμή του πεδίου " Type Of Service (TOS)" σε 0xC0, ενώ τα περισσότερα Λ.Σ χρησιμοποιούν την τιμή 0.

10. TCP Options
Αυτή η τεχνική στηρίζεται στην παρατήρηση ότι όλα τα Λ.Σ δεν χρησιμοποιούν όλα τα options που είναι διαθέσιμα στα TCP πακέτα.
Έτσι στέλνοντας ένα πακέτο έχοντας κάποια options ενεργοποιημένα, ο στόχος θα στείλει πίσω πακέτα με ενεργοποιημένα τα options τα οποία υποστηρίζει.
Ακόμα και αν περισσότερα από ένα Λ.Σ υποστηρίζουν τα ίδια options, οι τιμές που θέτει σε αυτά το καθένα είναι διαφορετικές. Αλλά και στην περίπτωση που και τα options και οι τιμές τους είναι ίδια για διαφορετικά Λ.Σ, μπορεί να αλλάζει η σειρά με την οποία τα παρουσιάζει το καθένα.

➢ Port Scanning

Ο τύπος αυτός του Scanning εξετάζει ποιες υπηρεσίες (πόρτες) τρέχουν (ακούνε) στο υπό εξέταση σύστημα.
Για καλύτερη κατανόηση της λειτουργίας του Port Scanning και για λόγους συνοχής, σε αυτό το σημείο παρουσιάζεται με συνοπτικό τρόπο και με την μορφή σχήματος η διαδικασία του 3-Way Handshake που ακολουθείται από το connection oriented πρωτόκολλο TCP, για την εγκαθίδρυση μίας σύνδεσης, με τον συγχρονισμό δύο συστημάτων προκειμένου να επικοινωνήσουν μεταξύ τους.



Σχήμα 1-1: 3-Way Handshake – Εγκαθίδρυση σύνδεσης

Οι μέθοδοι που υλοποιούν το port scanning μπορούν να χωριστούν σε τέσσερις κατηγορίες:

A. Open Scan Methods

Αυτές οι μέθοδοι μπορούν εύκολα να ανιχνευτούν και να φιλτραριστούν.
Για να υλοποιηθούν απαιτείται να εγκατασταθεί μια πλήρης σύνδεση με κάποιον απομακρυσμένο χρήστη, χρησιμοποιώντας το TCP 3-way handshake.

B. Half Open Scan Methods

Αυτές οι μέθοδοι είναι πιο δύσκολο να γίνουν αντιληπτές από τον στόχο.
Για να υλοποιηθούν δεν απαιτείται εγκατάσταση πλήρους σύνδεσης με τον στόχο και ο επιτιθέμενος τερματίζει την σύνδεση προτού ολοκληρωθεί το 3-way handshake.

C. Stealth Scanning

Η μέθοδοι αυτές είναι πολύ δύσκολο να ανιχνευτούν και έχουν την δυνατότητα να περνάνε σχεδόν απαρατήρητες από firewalls, routers και μηχανές φιλτραρίσματος.
Για την υλοποίηση των μεθόδων αυτών χρησιμοποιούνται τα Flags του TCP header των πακέτων, καθώς και η τεχνική του Inverse Mapping κατά την οποία βρίσκοντας ποιες πόρτες είναι κλειστές, υπολογίζονται οι πόρτες που είναι ανοιχτές και το αντίθετο.

D. Διάφορες Άλλες.

A. Μέθοδοι Open Scanning

1. TCP connect() scanning

Είναι η βασικότερη μορφή του Open Scanning χρησιμοποιώντας TCP πακέτα.
Με την χρήση της κλήσης του συστήματος connect (), ξεκινάει η διαδικασία του 3-way handshake με κάθε ενδιαφέρουσα πόρτα σε ένα απομακρυσμένο σύστημα.
Αν η πόρτα "ακούει" τότε η connect () θα είναι επιτυχής αλλιώς η σύνδεση δεν θα ολοκληρωθεί τερματίζοντας την διαδικασία του 3-way handshake.
Περιληπτικά τα μηνύματα που ανταλλάσσουν οι δύο πλευρές είναι :

Σε ανοικτή port του server :

```
client -> SYN
server -> SYN|ACK
client -> ACK
```

Σε κλειστή port του server :

```
client -> SYN
server -> RST|ACK
client -> RST
```

Πλεονεκτήματα **:** Γρήγορη όταν χρησιμοποιούνται πολλά sockets παράλληλα, αξιόπιστη, και δεν απαιτούνται δικαιώματα root για να επιτευχθεί.
Μειονεκτήματα **:** Είναι πολύ εύκολα ανιχνεύσιμη.

2. TCP Reverse Ident Scanning

Το Ident πρωτόκολλο χρησιμοποιείται για καθοριστεί το username του ιδιοκτήτη μιας συγκεκριμένης TCP σύνδεσης επικοινωνώντας με την πόρτα 113.
Με την μέθοδο αυτή στέλνεται στον ident/auth daemon μια αίτηση για αναζήτηση του ιδιοκτήτη μιας συγκεκριμένης διαδικασίας που τρέχει.
Στόχος είναι να βρεθούν διαδικασίες που τρέχουν σαν root και στην συνέχεια να ερευνηθεί αν αυτές είναι επιρρεπείς σε επιθέσεις.

Το ident μπορεί να αποκαλύψει αρκετές πληροφορίες όπως :

- user info
- entities
- objects
- processes

Για παράδειγμα αν σταλεί κάτι σαν αυτό που ακολουθεί παρακάτω μαζί με τα δεδομένα σε μια απομακρυσμένη μηχανή στην πόρτα 113, τότε θα αποκαλυφθεί ο ιδιοκτήτης του process που τρέχει στην δεδομένη πόρτα.

```
<request> ::= <port-pair> <EOL>

<port-pair> ::= <integer> "," <integer>

<EOL> ::= "015 012"  ; CR-LF End of Line Indicator, octal \r\n equivalents

<integer> ::= 1*5<digit> ; 1-5 digits.
```

Πλεονεκτήματα **:** Γρήγορη, δεν απαιτεί δικαιώματα root για την εφαρμογή της .
Μειονεκτήματα **:** Είναι εύκολα ανιχνεύσιμη.

B. Μέθοδοι Half Open Scanning

1. TCP SYN scanning

Αυτή η τεχνική συχνά αναφέρεται ως "half-open" scanning καθώς είναι και η πιο αντιπροσωπευτική αυτού του είδους.
Αρχικά στέλνεται στον στόχο ένα SYN πακέτο (TCP πακέτο με το SYN flag ενεργοποιημένο) σαν αίτηση για εγκατάσταση σύνδεσης με τον στόχο. Στην περίπτωση που η αντίστοιχη πόρτα στον στόχο "ακούει", τότε θα στείλει σαν απάντηση ένα SYN | ACK πακέτο δηλώνοντας ότι επιθυμεί και αυτός την εγκατάσταση της σύνδεσης.
Τότε θα γίνει γνωστό ότι η συγκεκριμένη πόρτα "ακούει" και στέλνεται στον στόχο ένα RST πακέτο ώστε να διακοπεί η σύνδεση.
Σε περίπτωση που η πόρτα δεν "ακούει", ο στόχος αντί του SYN | ACK πακέτου θα στείλει ένα RST |ACK πακέτο.

Τα μηνύματα που ανταλλάσσονται είναι περιληπτικά :

Σε ανοικτή port του server :

```
client -> SYN
server -> SYN|ACK
client -> RST
```

Σε κλειστή port του server :

```
client -> SYN
server -> RST|ACK
```

Η μέθοδος αυτή σπάνια καταγράφεται από τον στόχο, αλλά υπάρχουν αρκετά εργαλεία όπως το Synlogger και το Courtney που μπορούν να την ανιχνεύσουν.

Πλεονεκτήματα **:** Γρήγορη , αξιόπιστη , δεν ανιχνεύεται από απλά IDS (Intrusion Detection Systems).
Μειονεκτήματα **:** Η εφαρμογή της απαιτεί root δικαιώματα .

2. IP ID header aka "dumb" scanning

Η μέθοδος αυτή είναι παρόμοια με την TCP SYN scan , με την διαφορά ότι εμπλέκει και μια τρίτη οντότητα που ονομάζεται "Dumb Host" ή "Silent Host ".
Ο "Dump Host" είναι κάποιος server ο οποίος γενικότερα στέλνει και λαμβάνει πολύ λίγα έως καθόλου πακέτα. Η εύρεση ενός τέτοιου server φυσικά δεν είναι εύκολη.
Ένα σενάριο για ένα scan όπως αυτό θα έμοιαζε με το παρακάτω :

Εμπλεκόμενοι hosts :

A: attacker host
B: dumb host
C: target host

Αρχικά ο A στέλνει συνεχόμενα Icmp Echo Request πακέτα στον B και ελέγχει την τιμή του πεδίου ID, που βρίσκεται μέσα στον IP header, στα Icmp Echo Reply πακέτα που παίρνει ως απάντηση από τον B.
Το πεδίο ID χρησιμοποιείται για να ταυτοποιεί μοναδικά το κάθε IP πακέτο και ειδικότερα στην περίπτωση κατακερματισμού ενός datagram σε μικρότερα fragments, έτσι ώστε να μπορεί ο δέκτης να προσδιορίσει σε ποιο datagram ανήκει το κάθε fragment που παραλαμβάνει (τα fragments που ανήκουν στο ίδιο datagram έχουν την ίδια τιμή στο πεδίο ID).
Ο B σε κάθε απάντηση που θα στέλνει σε κάθε Icmp Echo του A, θα αυξάνει την τιμή του πεδίου ID κατά 1. Έτσι η απάντηση του B θα μοιάζει με την παρακάτω :

```
60 bytes from BBB.BBB.BBB.BBB: seq=1 ttl=64 id+=1 win=0 time=96 ms
60 bytes from BBB.BBB.BBB.BBB: seq=2 ttl=64 id+=1 win=0 time=88 ms
60 bytes from BBB.BBB.BBB.BBB: seq=3 ttl=64 id+=1 win=0 time=92 ms
```

Στη συνέχεια ο A στέλνει ένα πλαστό (spoofed) πακέτο στον C χρησιμοποιώντας ως source IP address αυτή του B. Το πακέτο αυτό θα το στείλει, στην πόρτα του C που θέλει να ελέγξει αν είναι ανοιχτή ή κλειστή.

Αν η πόρτα του C είναι ανοιχτή (ακούει) τότε ο C στέλνει ένα SYN | ACK στον B και αυτός θα στείλει ένα πακέτο με το RST flag ενεργοποιημένο τερματίζοντας την σύνδεση.
Αν η πόρτα είναι κλειστή τότε ο C θα στείλει ένα RST | ACK πακέτο στον B και αυτός δεν θα κάνει τίποτα.

Ο A συνεχίζει να στέλνει Icmp Echo πακέτα στον B και να αναλύει τις απαντήσεις του B για να μπορέσει ελέγχοντας την τιμή του ID να προσδιορίσει αν αυτός έχει στείλει και κάπου αλλού πακέτα.

Αν η πόρτα του C είναι ανοιχτή, τότε ο C θα έχει στείλει κάποια πακέτα στον B, εξαιτίας του SYN πακέτου που του έστειλε ο A με source IP αυτή του B, και ο B με την σειρά του θα έχει στείλει κάποια πακέτα στον C, με αποτέλεσμα στις απαντήσεις που στέλνει πλέον ο B στα Icmp Echo Request πακέτα του A να μην αυξάνεται σταθερά η τιμή του ID πεδίου κατά 1, αλλά με τον τρόπο που φαίνεται παρακάτω :

```
60 bytes from BBB.BBB.BBB.BBB: seq=25 ttl=64 id+=1 win=0 time=92 ms
60 bytes from BBB.BBB.BBB.BBB: seq=26 ttl=64 id+=3 win=0 time=80 ms
60 bytes from BBB.BBB.BBB.BBB: seq=27 ttl=64 id+=2 win=0 time=83 ms
```

Σε περίπτωση που η πόρτα του C είναι κλειστή τότε οι απαντήσεις του B προς τον A θα ήταν οι ίδιες με τις αρχικές (δηλαδή με σταθερά αυξανόμενη τιμή του ID πεδίου κατά 1), καθώς ο B δεν έστειλε καθόλου πακέτα στον C.

Η αποτελεσματικότητα αλλά και η δυσκολία της μεθόδου αυτής εξαρτάται κατά πολύ από τον εντοπισμό του κατάλληλου "Dumb Host ", γιατί αν αυτός ανταλλάσσει πακέτα και με άλλα συστήματα εκτός από τα εμπλεκόμενα, τότε η ανάλυση των ID πεδίων από τον A στις απαντήσεις του B δεν θα γινόταν σε σωστή βάση και θα εξάγονταν λάθος συμπεράσματα.

C. Μέθοδοι Stealth Scanning

1. SYN /ACK Scanning

Αυτή η μέθοδος υλοποιεί λανθασμένα τη διαδικασία του 3-way handshake που γίνεται κατά την εγκατάσταση της σύνδεσης μεταξύ δύο hosts.
Τα μηνύματα που ανταλλάσσονται είναι :
Αν η πόρτα είναι κλειστή :

```
client -> SYN|ACK
server -> RST
```

Το TCP καταλαβαίνει, ότι έγινε κάποιο λάθος κατά την σύνδεση σε αυτή την πόρτα όταν παρέλαβε ένα SYN | ACK πακέτο, ενώ δεν είχε στείλει προηγουμένως κάποιο SYN και έτσι επιστρέφει ένα RST μήνυμα πίσω.

Αν η πόρτα είναι ανοιχτή :

```
client -> SYN|ACK
server -> -
```

Σε αυτή την περίπτωση ο server αγνοεί το πακέτο και δεν στέλνει κάποια απάντηση στον client.

Πλεονεκτήματα **:** Γρήγορη , δεν ανιχνεύεται από τα βασικά IDS / Firewalls
Μειονεκτήματα **:** Δεν είναι αξιόπιστη καθώς όταν δεν επιστρέφεται κάποια απάντηση δεν είναι ξεκάθαρο αν αυτό συμβαίνει επειδή η πόρτα είναι ανοιχτή ή αν το SYN|ACK πακέτο απλά δεν έφτασε στον προορισμό του.

2. TCP FIN scanning

Η τεχνική αυτή στηρίζεται στο γεγονός ότι κλειστές πόρτες σε ένα σύστημα απαντάνε σε ένα FIN πακέτο που λαμβάνουν με το κατάλληλο RST πακέτο καθώς δεν βρέθηκέ διαθέσιμη πόρτα :

```
client -> FIN
server -> RST
```

ενώ ανοικτές πόρτες συνήθως το αγνοούν :

```
client -> FIN
server -> -
```

Με την μέθοδο αυτή, αρχικά σχηματίζεται μια λίστα από τις πόρτες που θα εξεταστούν, στέλνονται FIN πακέτα σε αυτές τις πόρτες και στη συνέχεια εντοπίζονται οι ανοιχτές πόρτες αφαιρώντας από την λίστα τις πόρτες που έστειλαν απάντηση.

Πλεονεκτήματα **:** Δύσκολό να ανιχνευτεί.
Μειονεκτήματα **:** Δεν είναι αποτελεσματική όταν εφαρμόζεται σε κάποια συστήματα (πχ. Windows) τα οποία στέλνουν RST πακέτα σαν απάντηση στα FIN πακέτα, άσχετα από την κατάσταση της πόρτας.
Επίσης δεν είναι αξιόπιστη καθώς όταν δεν επιστρέφεται κάποια απάντηση, δεν είναι ξεκάθαρο αν αυτό συνέβη επειδή η πόρτα είναι ανοιχτή ή αν το FIN πακέτο απλά δεν έφτασε στον προορισμό του.

3. ACK Scanning

Αυτή η μέθοδος στηρίζεται σε κάποια ελαττώματα που υπάρχουν στο IP Layer σε κάποιες παλαιότερες εκδόσεις κάποιων Λ.Σ.
Η υλοποίησή της αποτελείται από την αποστολή ενός ACK πακέτου στον στόχο και στη συνέχεια μελέτη των TTL και Window πεδίων των πακέτων που στέλνει ο στόχος με το RST bit ενεργοποιημένο.

Το πεδίο TTL :
Σε μερικά Λ.Σ η τιμή του TTL πεδίου στα πακέτα που αφορούν απάντηση για μια ανοιχτή πόρτα είναι μικρότερη από αυτή που έχουν τα πακέτα που αφορούν κλειστές πόρτες και συνήθως μικρότερη του 64.
Διαδικασία :

```
client -> ACK
server -> RST -> (TTL <= 64)
```

Ένα δείγμα από τις απαντήσεις του server μετά από αποστολή ACK πακέτων στις πόρτες 20 έως 23.

```
packet 1: host XXX.XXX.XXX.XXX port 20: F:RST -> ttl: 70 win: 0   → κλειστή
packet 2: host XXX.XXX.XXX.XXX port 21: F:RST -> ttl: 70 win: 0   → κλειστή
packet 3: host XXX.XXX.XXX.XXX port 22: F:RST -> ttl: 40 win: 0   → ανοικτή
packet 4: host XXX.XXX.XXX.XXX port 23: F:RST -> ttl: 70 win: 0   → κλειστή
```

Το πεδίο Window :
Σε μερικές εκδόσεις του BSD (FreeBSD , OpenBSD) και του UNIX (AIX , DGUX) πακέτα που στέλνει ο server σαν απάντηση και αφορούν ανοιχτές πόρτες, η τιμή του πεδίου Window στα πακέτα είναι διάφορη του 0 , ενώ σε αυτά που αφορούν κλειστές πόρτες είναι 0.
Διαδικασία :

```
client -> ACK
server -> RST  (WINDOW ≠0)
```

Ένα δείγμα από τις απαντήσεις του server μετά από αποστολή ACK πακέτων στις πόρτες 20 έως 23.

```
packet 6: host XXX.XXX.XXX.XXX port 20: F:RST -> ttl: 64 win: 0     → κλειστή
packet 7: host XXX.XXX.XXX.XXX port 21: F:RST -> ttl: 64 win: 0     → κλειστή
packet 8: host XXX.XXX.XXX.XXX port 22: F:RST -> ttl: 64 win: 512   → ανοικτή
packet 9: host XXX.XXX.XXX.XXX port 23: F:RST -> ttl: 64 win: 0     → κλειστή
```

Σε αυτή την περίπτωση ενώ το TTL είναι το ίδιο σε όλα τα πακέτα, το πακέτο 8 όμως έχει στο πεδίο win την τιμή 512 που δηλώνει ότι αυτή η πόρτα είναι ανοιχτή.

Πλεονεκτήματα **:** Δύσκολο να ανιχνευτεί και να καταγραφεί.
Μειονεκτήματα **:** Δεν είναι συμβατή με όλα τα Λ.Σ.

4. Null Scanning

Με την τεχνική αυτή στέλνονται πακέτα σε διάφορες πόρτες τα οποία έχουν όλα τα flags (ACK , FIN, RST,SYN, URG , PSH) του IP header απενεργοποιημένα.
Αυτό έχει σαν συνέπεια σε ορισμένα Λ.Σ ανοιχτές πόρτες να απορρίψουν τα πακέτα :

```
client -> NULL (κανένα flag)
server -> -
```

ενώ οι κλειστές πόρτες, να απαντήσουν με πακέτα με ενεργοποιημένο το RST flag :

```
client -> NULL (κανένα flag ενεργοποιημένα)
server -> RST
```

Παρόλα αυτά σε πολλά Λ.Σ όπως τα Windows, Cisco, BSDI, HP/UX, MVS, IRIX, ανοιχτές πόρτες απαντούν επίσης με πακέτα με ενεργοποιημένο το RST flag .

Πλεονεκτήματα : Δύσκολα ανιχνεύσιμη αν και τα νεότερα IDSs την ανιχνεύουν εύκολα.
Μειονεκτήματα : Ισχύει για λίγα Λ.Σ (κυρίως το Unix) , δεν είναι αξιόπιστη καθώς όταν δεν επιστρέφεται κάποια απάντηση δεν είναι ξεκάθαρο αν αυτό συνέβη επειδή η πόρτα είναι ανοιχτή ή επειδή το πακέτο που στάλθηκε αρχικά απλά δεν έφτασε στον προορισμό του.

5. XMAS Scanning

Με αυτή την μέθοδο στέλνονται πακέτα με όλα τα flags του IP header ενεργοποιημένα.
Οι ανοιχτές πόρτες θα απορρίψουν αυτά τα πακέτα χωρίς να στείλουν πίσω κάποια απάντηση :

```
client -> XMAS (όλα τα flags ενεργοποιημένα)
server -> -
```

σε αντίθεση με τις κλειστές πόρτες, όπου το Λ.Σ νομίζει ότι ο client προσπαθεί να εγκαταστήσει μια σύνδεση με αυτή την πόρτα χωρίς να ακολουθεί τα βήματα του 3-way handshake και στέλνει στον client πακέτα με ενεργοποιημένο το RST flag :

```
client -> XMAS (όλα τα flags ενεργοποιημένα)
server -> RST
```

Πλεονεκτήματα **:** Δύσκολα ανιχνεύσιμη
Μειονεκτήματα **:** Ισχύει για λίγα Λ.Σ (κυρίως το Unix) , δεν είναι αξιόπιστη καθώς όταν δεν επιστρέφεται κάποια απάντηση δεν είναι ξεκάθαρο αν αυτό συνέβη επειδή η πόρτα είναι ανοιχτή ή επειδή το πακέτο που στάλθηκε αρχικά απλά δεν έφτασε στον προορισμό του.

D. Διάφορες Άλλες Μέθοδοι

1. Proxy Scanning / FTP Bounce Scanning

Η μέθοδος αυτή χρησιμοποιείται από τον επιτιθέμενο όταν θέλει να κάνει scanning σε συστήματα τα οποία ανήκουν σε ένα δίκτυο το οποίο μέσω ενός Firewall, απαγορεύει την διέλευση των πακέτων που υλοποιούν το scanning.
Ο επιτιθέμενος καθώς δεν μπορεί να στείλει απευθείας τα πακέτα του scanning στα συστήματα του δικτύου, τα στέλνει με έμμεσο τρόπο χρησιμοποιώντας ένα σύστημα εντός του δικτύου στο οποίο μπορεί να συνδεθεί με κάποιο τρόπο. Τέτοια συστήματα μπορεί να είναι αυτά που ανήκουν στην DMZ ενός δικτύου, τα οποία προστατεύονται από πιο χαλαρά μέτρα προστασίας έτσι ώστε να μπορούν να προσφέρουν κάποιες υπηρεσίες σε χρήστες εκτός του δικτύου.
Ο επιτιθέμενος για να υλοποιήσει την μέθοδο του FTP Bounce θα πρέπει πρώτα να έχει εντοπίσει στο δίκτυο-στόχο έναν FTP server, ο οποίος να του επιτρέπει να συνδεθεί με αυτόν.

Κάθε FTP session αποτελείται από δύο κανάλια επικοινωνίας. Ένα για την μεταφορά των εντολών, το *Control Channel* και ένα για την μεταφορά των data, το *Data Transfer Channel.*
Με το *Active Mode* λειτουργίας του FTP server, ο client αρχικά συνδέεται στην TCP πόρτα 21 του server εγκαθιστώντας έτσι το *Control Channel*.
Στην συνέχεια με την εντολή **`PORT`**, δηλώνει στον server την IP διεύθυνση και την πόρτα στην οποία ο server θα συνδεθεί με τον client για να εγκαταστήσει το *Data Transfer Channel,* μέσω του οποίου θα μεταφέρονται τα δεδομένα. Η IP διεύθυνση που δηλώνεται είναι αυτή του client και η πόρτα είναι συνήθως μία υψηλή πόρτα του client.

Ο επιτιθέμενος αφού συνδεθεί στον server, με την εντολή **`PORT`** ορίζει ως IP διεύθυνση μία που ανήκει στο σύστημα-στόχο στο οποίο θέλει να εκτελέσει το scanning και σαν πόρτα δίνει αυτή που θέλει να ελέγξει αν είναι ανοιχτή στο σύστημα αυτό.
Αν η πόρτα είναι ανοιχτή, τότε θα επιστραφούν από τον server μηνύματα του τύπου 150 και 226 στον επιτιθέμενο, αλλιώς αν η πόρτα είναι κλειστή θα επιστραφεί μήνυμα του τύπου 425.

Με αυτόν τον τρόπο ο επιτιθέμενος μπορεί να κάνει scanning σε συστήματα στα οποία δεν μπορεί να στείλει άμεσα τα πακέτα που θα το υλοποιήσουν, εξαιτίας της παρουσίας κάποιου firewall. Επίσης με αυτήν την μέθοδο ο επιτιθέμενος κρύβει την παρουσία του καθώς το scanning φαίνεται σαν να προέρχεται από τον FTP server.

Οι πρώτες εκδόσεις του WU-FTPD επέτρεπαν κάτι τέτοιο να συμβεί καθώς επίσης και οι εκδόσεις Sun FTP server in SunOS 4.1.x/5.x, SCO OpenServer 5.0.4, SCO UnixWare 2.1, AIX 3.2/4.2/4.2./4.3, Caldera 1.2, RedHat 4.X, Slackware 3.1 - 3.3.

Πλεονεκτήματα **:** Δεν ανιχνεύεται από τα firewalls , επιτρέπει πρόσβαση σε τοπικά δίκτυα.
Μειονεκτήματα **:** Αργή, στους περισσότερους FTP servers έχει διορθωθεί αυτή η αδυναμία.

Ο πίνακας που ακολουθεί παρουσιάζει συγκεντρωτικά, όλες τις μεθόδους του Port Scanning που αναφέρθηκαν παραπάνω, απεικονίζοντας και τα μηνύματα που ανταλλάσσονται μεταξύ του επιτιθέμενου (client ή C) και του στόχου (server ή S) σε κάθε περίπτωση.

ΕΙΔΟΣ ΜΕΘΟΔΟΥ		**ΚΑΤΑΣΤΑΣΗ ΠΟΡΤΑΣ**	
		ΑΝΟΙΧΤΗ	**ΚΛΕΙΣΤΗ**
OPEN SCANNING	TCP Connect ()	client -> SYN server -> SYN|ACK client -> ACK	client -> SYN server -> RST|ACK client -> RST
	Reverse Ident Scanning	**CLIENT** <request> ::= <port-pair> <EOL> <port-pair> ::= <integer> "," <integer> <EOL> ::= "015 012" ; CR-LF End of Line Indicator, octal \r\n equivalents <integer> ::= 1*5<digit> ; 1-5 digits. **SERVER** (Απαντάει με το username του ιδιοκτήτη του proccess)	
HALF OPEN SCANNING	SYN Scanning	client -> SYN server -> SYN|ACK client -> RST	client -> SYN server -> RST|ACK
	IP ID Header aka "dumb" Scanning	**C [ICMP_ECHO] -> Dumb** **Dumb [ICMP_REPLY(ID++)] -> C** **C [spoofed SYN] -> S** **S [SYN|ACK] -> Dumb** **Dumb [RST] -> S** **C [ICMP_ECHO] -> Dumb** **Dumb[ICMP_REPLY(ID+=x)] -> C**	**C [ICMP_ECHO] -> Dumb** **Dumb [ICMP_REPLY(ID++)]->C** **C [spoofed SYN] -> S** **S [RST|ACK] -> Dumb** **Dumb -> --** **C [ICMP_ECHO] -> Dumb** **Dumb [ICMP_REPLY(ID++)]->C**

STEALTH SCANNING	SYN|ACK Scanning	Client -> SYN|ACK server -> -	client -> SYN|ACK server -> RST
	FIN Scanning	client -> FIN server -> -	client -> FIN server -> RST
	ACK Scanning	client -> ACK server -> RST -> (TTL <= 64) **ή** client -> ACK server -> RST -> WINDOW (non-zero)	client -> ACK server -> RST -> (TTL >64) **ή** client -> ACK server -> RST -> WINDOW (zero)
	NULL Scanning	client -> NULL (no flags) server -> -	client -> NULL (no flags) server -> RST
	XMAS Scanning	client -> XMAS (all flags) server -> -	client -> XMAS (all flags) server -> RST
ΑΛΛΕΣ	UDP ICMP Port Unreachable Scanning	client -> udp packet server -> - client -> udp packet server -> -	client -> udp packet server->ICMP(PORT_UNREACH)
	Proxy / FTP Server Bounce Attack	**Client ->** FTP PORT command **FTP server -> 150** and 226 response	**Client ->** FTP PORT command **FTP server ->** "425 Can't build data connection: Connection refused" response

Πίνακας 1-2: Μέθοδοι Port Scanning

Τεχνικές για Εφαρμογή των Port Scanning Μεθόδων

Για να γίνει δυσκολότερη η ανίχνευση των παραπάνω επιθέσεων χρησιμοποιούνται διάφορες τεχνικές.

- **Random Port Scanning**

  Με την τεχνική αυτή γίνεται το scanning σε τυχαίες πόρτες (όχι διαδοχικές) καθώς πολλά από τα IDS και τα Firewalls ελέγχουν αν έχουν γίνει συνεχόμενες προσπάθειες για σύνδεση σε διαδοχικές πόρτες, οπότε και ανιχνεύουν το scanning που έγινε.

- **Slow Scan**

  Με την τεχνική αυτή το scanning γίνεται με μικρό ρυθμό, και συνήθως στέλνονται λίγα πακέτα με μεγάλη χρονική καθυστέρηση μεταξύ τους, καθώς πολλά IDS καταγράφουν και αναλύουν την κίνηση προς το δίκτυο που προστατεύουν ανά συγκεκριμένα χρονικά διαστήματα. Το χρονικό αυτό διάστημα ονομάζεται *Site*

Detection Threshold. Έτσι αν κάποια IP διεύθυνση έχει καταγραφεί πολλές φορές μέσα ένα τέτοιο χρονικό διάστημα, γίνεται αντιληπτή η προσπάθεια για scanning από αυτή την διεύθυνση.

- **TCP Fragmentation Scanning**

  Με την τεχνική αυτή αντί να σταλεί ολόκληρο το πακέτο που θα χρειαστεί για το Scanning, αυτό κατακερματίζεται σε μικρότερα IP Fragments. Έτσι χωρίζεται ο TCP header του πακέτου σε μικρότερα πακέτα και γίνεται δυσκολότερη η εξαγωγή και ο έλεγχος από τους μηχανισμούς φιλτραρίσματος των πακέτων, των πληροφοριών που περιέχει, όσο αναφορά τα πεδία του που θα χρησιμοποιηθούν για το scanning.

➢ Scanning For Vulnerabilities

Αφού εντοπιστούν ποιες υπηρεσίες τρέχουν σε ένα σύστημα, εξετάζεται αν αυτές οι υπηρεσίες έχουν κάποιο γνωστό vulnerability το οποίο μπορεί να χρησιμοποιηθεί για μία επίθεση στο σύστημα αυτό.
Το Scanning αυτού του είδους κάνει διάφορα τεστ στο σύστημα-στόχο, μερικά από τα οποία μπορούν να έχουν απρόβλεπτες συνέπειες καθώς εκτελούν και το ανάλογο exploit για κάποιο vulnerability που θα εντοπίσουν.

➢ Firewalking

Το Firewalking είναι ένα είδος Scanning το οποίο χρησιμοποιείται για την συλλογή πληροφοριών που αφορούν ένα απομακρυσμένο δίκτυο, το οποίο προστατεύεται από ένα Firewall.
Η τεχνική αυτή είναι όμοια με την λειτουργία του traceroute και στέλνοντας πακέτα διαφορετικών πρωτοκόλλων σε ένα δίκτυο, μπορεί να καθορίσει ποιες πόρτες είναι ανοιχτές ή κλειστές σε ένα firewall, ποια είδη πακέτων (όσο αναφορά το πρωτόκολλο) επιτρέπει ένα firewall να περνάνε καθώς επίσης και ποιοι hosts υπάρχουν πίσω από το firewall.

Για να εφαρμοστεί αυτή η τεχνική χρειάζεται να είναι γνωστά δύο πράγματα :
1. Η IP διεύθυνση του firewall που προστατεύει το δίκτυο.
2. Η IP διεύθυνση ενός host που βρίσκεται στο δίκτυο.

Η πρώτη διεύθυνση θα χρησιμοποιηθεί για να καθοριστούν για ποιες πόρτες επιτρέπονται πακέτα να περνάνε από το firewall (δηλαδή ποια πρωτόκολλα μπορούν να χρησιμοποιηθούν για να στείλουν πακέτα που θα περάσουν από το firewall).
Η δεύτερη διεύθυνση χρησιμοποιείται ως προορισμός για να μπορεί να κατευθυνθεί η ροή των πακέτων.

Αρχικά εκτελείται ένα traceroute προς τον host που βρίσκεται μέσα στο δίκτυο.

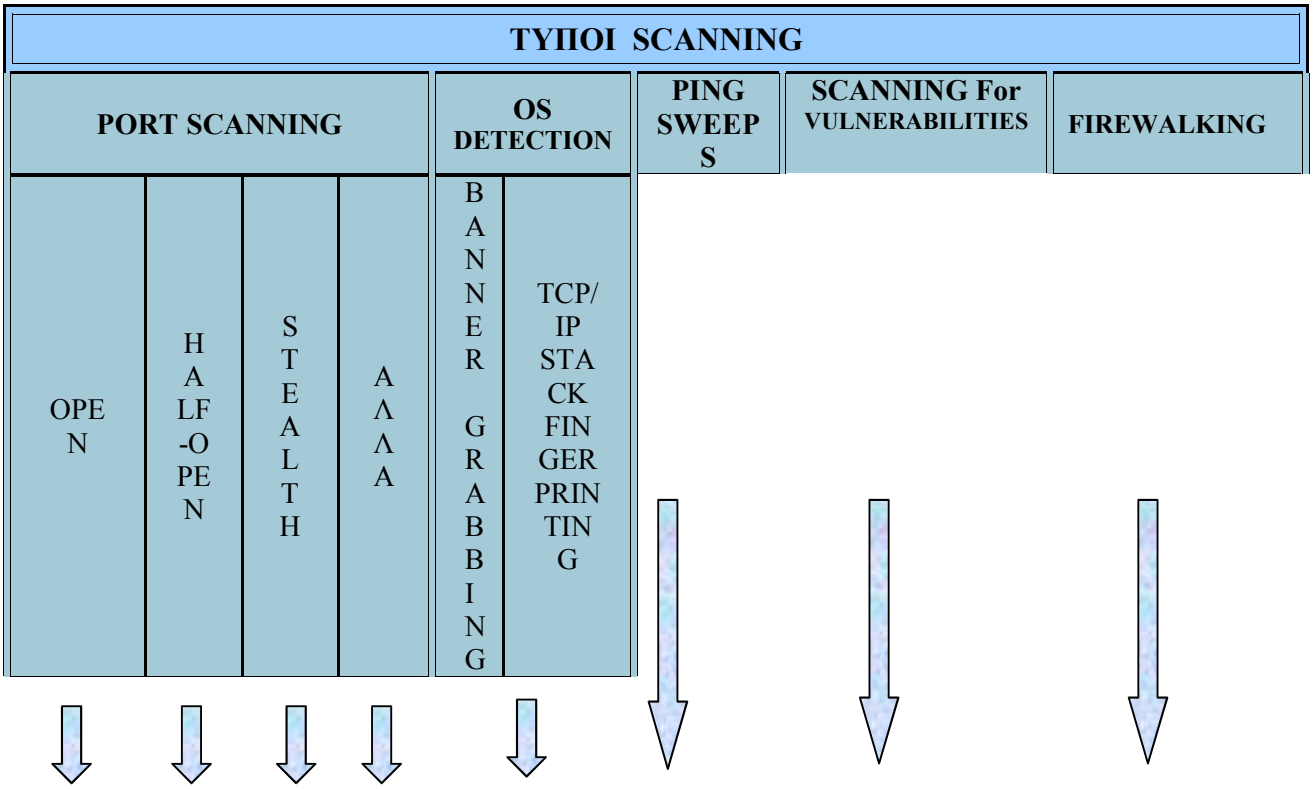
Αν το firewall δεν επιτρέψει το traceroute να φτάσει μέχρι τον host, τότε κοιτώντας τα αποτελέσματα του traceroute είναι δυνατό να εντοπιστεί η IP διεύθυνση του firewall.
Στη συνέχεια γίνονται και άλλες τέτοιου είδους αναζητήσεις χρησιμοποιώντας διαφορετικά πρωτόκολλα.

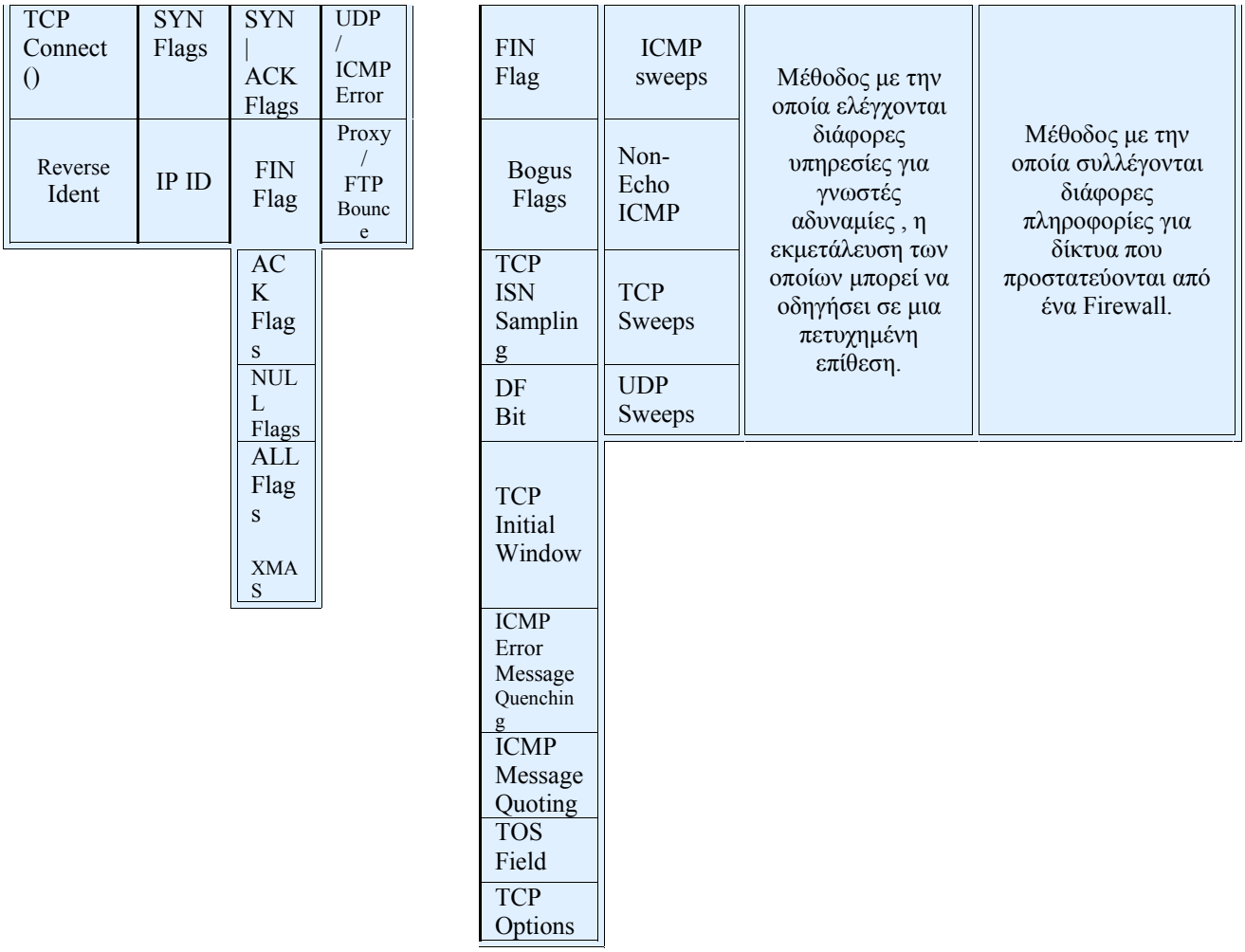
Όποια από αυτές πετύχει τότε εξάγονται δύο είδη συμπερασμάτων :

1. Ότι το firewall αφήνει αυτού του είδους τα πακέτα να περνάνε.
2. Ότι το σύστημα στο οποίο στέλνονται τα πακέτα υπάρχει και ανταποκρίνεται.

Έτσι στέλνοντας πολλά πακέτα διαφορετικών πρωτοκόλλων στο δίκτυο, σε διάφορες πόρτες ενός firewall και σε πολλούς hosts , μπορεί κάποιος να καθορίσει το σύνολο των κανόνων που χρησιμοποιεί το firewall καθώς επίσης και την τοπολογία του δικτύου.

Στο **Σχήμα 1-2** παρουσιάζονται συγκεντρωτικά όλοι οι τύποι του scanning που περιγράφηκαν παραπάνω.





Σχήμα 1-2: Τύποι Scanning

(Distributed) Denial Of Service [(D)DOS] Attacks

Οι (D)DoS επιθέσεις έχουν σαν στόχο να προκαλέσουν την δυσλειτουργία ενός συστήματος ή ενός δικτύου, έτσι ώστε αυτό να μην είναι δυνατόν να παρέχει στους νόμιμους χρήστες του, με τον τρόπο που θα έπρεπε, τις υπηρεσίες για τις οποίες είναι προορισμένο.

Οι παλιότερες επιθέσεις αυτού του είδους είναι οι DoS Attacks, οι οποίες υλοποιούνταν συνήθως point to point, από ένα σύστημα σε ένα άλλο και στόχος τους ήταν να οδηγήσουν το σύστημα-στόχο σε κατάρρευση ή γενικότερη δυσλειτουργία.
Αυτό γινόταν εφικτό με την εκμετάλλευση διαφόρων vulnerabilities του συστήματος, όπως το buffer overflow ή με την αποστολή πολλών πακέτων στο σύστημα αυτό, το οποίο δεν είχε αρκετούς πόρους να τα επεξεργαστεί.

Μεταγενέστερες (μετά το 1999) παραλλαγές των DoS Attacks χρησιμοποιούν πολλά συστήματα, τα οποία εξαπολύουν μια συγχρονισμένη επίθεση σε ένα σύστημα ή σε ένα δίκτυο.

Μία τέτοια επίθεση ονομάζεται ***Distributed Denial of Service Attack (DDoS)*** και όταν εξαπολυθεί εναντίον ενός δικτύου, προκαλεί μεγάλη συμφόρηση και εμποδίζει την κίνηση των νόμιμων πακέτων από και προς το δίκτυο αυτό.
Οι επιθέσεις αυτού του είδους συνήθως υλοποιούνται με την χρήση διαφόρων εργαλείων που αυτοματοποιούν την όλη διαδικασία.

Οι DDoS επιθέσεις υλοποιούνται σε 2 φάσεις :

- Η πρώτη φάση της επίθεσης χρειάζεται μεγάλο χρονικό διάστημα για να υλοποιηθεί .
  Ο επιτιθέμενος για μπορέσει να στείλει τις μεγάλες ποσότητες των πακέτων που απαιτούνται για να υλοποιηθεί η επίθεση, χρειάζεται να βρει αρκετούς, κατάλληλους υπολογιστές που θα τα δημιουργήσουν.
  Κατάλληλοι υπολογιστές είναι αυτοί που έχουν μειωμένη ασφάλεια, στους οποίους θα μπορέσει ο επιτιθέμενος σε πρώτο στάδιο να διεισδύσει και να εγκαταστήσει σε αυτούς τα DDoS εργαλεία καθώς και ένα rootkit το οποίο θα κρύβει την παρουσία τους.
  Αυτά τα DDoS προγράμματα, είναι συνήθως client-server εφαρμογές και στα συστήματα που παραβιάζει ο επιτιθέμενος εγκαθιστά το client κομμάτι τους με το οποίο μπορεί με κάποιο τρόπο να επικοινωνεί ανά τακτά χρονικά διαστήματα και να το ελέγχει.

- Η δεύτερη φάση της επίθεσης ξεκινάει αφού πρώτα ολοκληρωθεί με επιτυχία η πρώτη φάση.

Τα συστήματα στα οποία έχει εγκαταστήσει τα εργαλεία του ο επιτιθέμενος, θα δημιουργήσουν και θα στείλουν τεράστιες ποσότητες πακέτων στο στόχο.
Ο στόχος στον οποίο θα σταλούν τα πακέτα αυτά, δεν θα μπορέσει να τα χειριστεί με επιτυχία και αν ο στόχος είναι κάποιο δίκτυο τότε θα δημιουργηθεί μεγάλη κίνηση και συμφόρηση σε αυτό.

Τα συστήματα που λαμβάνουν μέρος σε μία DDoS επίθεση είναι υποχείρια του επιτιθέμενου και βέβαια θεωρούνται επίσης θύματα της επίθεσης. Ο επιτιθέμενος επικοινωνεί τακτικά με τα συστήματα αυτά μέσω των εργαλείων που έχει εγκαταστήσει, έως ότου αποφασίσει να δώσει το έναυσμα με το οποίο θα ξεκινήσει το τελικό στάδιο της επίθεσης που θα πλήξει τον στόχο με τις τεράστιες ποσότητες των πακέτων που θα παραχθούν.

Η κατανομή των συστημάτων που έχει στην διάθεσή του ο επιτιθέμενος μοιάζει με αυτή στο **Σχήμα 1-3**.

Σχήμα 1-3: Η κατανομή των συστημάτων σε μία DDoS

Τα συστήματα στα οποία θα εγκαταστήσει αρχικά τα εργαλεία του ο επιτιθέμενος (Client), είναι οι Handlers και οι Agents.
Οι Agents είναι αυτοί που θα δημιουργήσουν και θα στείλουν την τεράστια ποσότητα των πακέτων στον στόχο. Οι Handlers είναι αυτοί που ελέγχουν τους Agents.
Κάθε Handler διατηρεί μια λίστα με τους Agents που ελέγχει και δίνει το σήμα σε αυτούς όταν φτάσει η στιγμή να στείλουν τα πακέτα που θα υλοποιήσουν το τελικό στάδιο της επίθεσης.
Ο Client ελέγχει έναν ή περισσότερους Handlers και ίσως να είναι το σύστημα του ίδιου του επιτιθέμενου. Μέσω του Client ο επιτιθέμενος θα σώσει το τελικό σύνθημα να ξεκινήσει η επίθεση.

Μια DDoS επίθεση είναι πολύ δύσκολο να ανιχνευτεί πριν την εφαρμογή της τελικής φάσης της, λόγω της ικανότητας των εργαλείων που χρησιμοποιούνται να διατηρούν την παρουσία τους κρυφή στα συστήματα που βρίσκονται.
Τα εργαλεία αυτά χρησιμοποιούν μεθόδους κρυπτογραφημένης επικοινωνίας για την ανταλλαγή μηνυμάτων μεταξύ των Clients των Handlers και των Agents, έτσι ώστε να μην είναι εύκολο να αποκαλυφθούν τα μηνύματα αυτά.
Επίσης χρησιμοποιούν πλαστές IP διευθύνσεις στα πακέτα που στέλνουν έτσι ώστε να μην προδίδουν την τοποθεσία τους.
Αν το θύμα της επίθεσης καταφέρει να εντοπίσει την αληθινή τοποθεσία κάποιων Agents, θα πρέπει στη συνέχεια να εντοπίσει τις αληθινές IP διευθύνσεις των Handlers και τελικά του επιτιθέμενου, κάτι που είναι εξαιρετικά δύσκολο.

IP Spoofing

IP Spoofing είναι η τεχνική με την οποία στέλνονται IP πακέτα που έχουν ψεύτικη διεύθυνση αποστολέα.

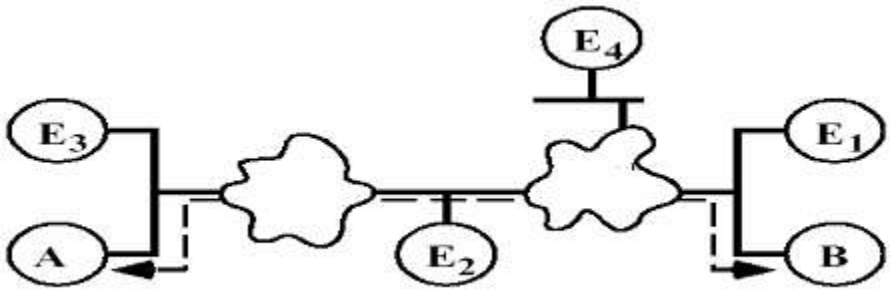
Το IP spoofing χρησιμοποιείται κατά κόρον από τους επιτιθέμενους καθώς τους δίνει την δυνατότητα να κρύβουν την πραγματική τους ταυτότητα σε διάφορες επιθέσεις που υλοποιούν.

Άμεση εφαρμογή έχει σε επιθέσεις οι οποίες εκμεταλλεύονται την αδυναμία που παρουσιάζουν ορισμένες υπηρεσίες, οι οποίες χρησιμοποιούν μεθόδους αυθεντικοποίησης βασισμένες μόνο στην IP διεύθυνση του αποστολέα.
Σε αυτό το μοντέλο μια υπηρεσία δημιουργεί ένα μήνυμα και το στέλνει στην αντίστοιχη υπηρεσία σε ένα απομακρυσμένο σύστημα. Η υπηρεσία στο απομακρυσμένο σύστημα κάνει δεκτή την αίτηση εξετάζοντας απλά την IP διεύθυνση που βρίσκεται μέσα στο μήνυμα. Συνήθως τέτοιου είδους αυθεντικοποίηση γίνεται όταν ο απομακρυσμένος host θεωρείται έμπιστος.
Δυστυχώς όμως οι IP διευθύνσεις δεν σχεδιάστηκαν για να προσφέρουν αυθεντικοποίηση και κάποιος κακόβουλος χρήστης μπορεί να δημιουργήσει μια ψεύτικη αίτηση.

Παρακάτω παρουσιάζεται μία επίθεση που στηρίζεται στην τεχνική του IP spoofing.

Η Επίθεση.

Στο σενάριο της επίθεσης υπάρχουν τρεις hosts, ο Α, ο Β και ο Ε. Ο Α και ο Β βρίσκονται σε διαφορετικά δίκτυα, ενώ ο Ε μπορεί να βρίσκεται σε μια από τις εναλλακτικές θέσεις όπως φαίνεται στο **Σχήμα 1-4**.



Σχήμα 1-4: Η τοπολογία των εμπλεκόμενων συστημάτων

Ο Β παρέχει στον Α κάποια δικαιώματα που του επιτρέπουν να μπορεί να στέλνει κάποια αιτήματα στον Β και αυτός να τα εκτελεί.
Ο Β για να μπορεί να επιβεβαιώσει ότι ο Α είναι αυτός που του ζητάει να εκτελέσει κάποιες ενέργειες, έχει καταχωρημένη την διεύθυνση του Α (πχ. στο αρχείο rhosts).
Ο Ε είναι αυτός που θα κάνει την επίθεση, με σκοπό να ξεγελάσει τον Β παριστάνοντας ότι είναι ο Α, έτσι ώστε να του δοθούν τα ανάλογα δικαιώματα.

Για να πετύχει ο Ε τον στόχο του θα πρέπει να υλοποιήσει την επίθεση σε δύο φάσεις:

1η. Να εγκαταστήσει μια ψεύτικη επικοινωνία με τον Β και

2η. Να εμποδίσει τον Α να ειδοποιήσει τον Β για το τι συμβαίνει, έως ότου να είναι πολύ αργά.

Φάση 1η

Ο Ε πρέπει να στέλνει πακέτα στον Β τα οποία έχουν ως διεύθυνση αποστολέα αυτή του Α. Έτσι ο Β θα έχει την εντύπωση ότι επικοινωνεί με τον Α .
Η επικοινωνία μπορεί να γίνει είτε με ένα connectionless πρωτόκολλο (πχ.UDP), είτε με ένα connection oriented πρωτόκολλο (πχ.TCP).
Στην πρώτη περίπτωση η αποστολή ενός μόνο πακέτου είναι αρκετή, ενώ στην δεύτερη περίπτωση πρέπει να στείλει πολλαπλά πακέτα ώστε να ολοκληρωθεί το 3-way handshake μεταξύ τους. Τα πακέτα που θα στέλνει ο Β θα έχουν ως διεύθυνση παραλήπτη αυτή του Α καθώς τα πακέτα που του στέλνει ο Ε έχουν την IP διεύθυνση του Α ως διεύθυνση αποστολέα. Έτσι ο Ε πρέπει να στέλνει πακέτα με σωστά περιεχόμενα στον Β, που να συμφωνούν με τις απαντήσεις (sequence numbers) που στέλνει ο Β στον Α.
Αν ο Ε βρίσκεται στις θέσεις Ε1, Ε2, Ε3 τότε μπορεί να μπορεί να παρατηρεί τις απαντήσεις του Β προς στον Α. Αν βρίσκεται στην Ε4 τότε πρέπει να μπορεί να δρομολογεί τις απαντήσεις του Β προς στον Α μέσα από το δικό του δίκτυο (αυτό μπορεί να γίνει με την τεχνική του *source routing).*
Μια άλλη μέθοδος είναι ο Ε να μαντέψει τα sequence numbers του Β με εφαρμογή ορισμένων τεχνικών.

Φάση 2η

Ο Ε μπορεί να εμποδίσει τον Α ώστε να μην αναμιχθεί στην επίθεση με διάφορους τρόπους.

Τρεις από αυτούς είναι οι εξής:

1. Να εμποδίσει τα πακέτα ώστε να μην φτάνουν στον Α.
2. Να εξαλείψει την δυνατότητα του Α να απαντάει στον Β.
3. Να ολοκληρώσει την επικοινωνία με τον Β πριν ο Α προλάβει να τον ειδοποιήσει.

Ο 1ος Τρόπος

Για να συμβεί κάτι τέτοιο θα πρέπει ο Ε

α) Αν βρίσκεται στη διαδρομή μεταξύ του Α και του Β (πχ. Αν είναι ένας router ή έχει χρησιμοποιήσει το source routing ώστε να αναγκάσει τα πακέτα να περνάνε μέσο αυτού) απλά δεν θα προωθεί τα πακέτα προς τον Α.

β) Αν δεν βρίσκεται στη διαδρομή θα πρέπει να αλλάξει τις πληροφορίες δρομολόγησης σε έναν από τους routers που βρίσκονται στην διαδρομή, ώστε να μην δρομολογούν σωστά τα πακέτα του Α.

Ο 2ος Τρόπος

Αυτό μπορεί να γίνει με 2 τρόπους :

α) Μπορεί να κάνει τον Α να καταρρεύσει (crash)
πχ. Εξαπολύοντας εναντίον του μια DOS επίθεση όπως η SYN Flood.

b) Μπορεί να μπλοκάρει την TCP/IP stack του Α.
πχ. Στέλνοντας του πολλαπλές αιτήσεις για σύνδεση στην rlogin πόρτα (port 513) από κάποιον host ο οποίος δεν υπάρχει.

Ο 3ος Τρόπος

Θα πρέπει η επικοινωνία μεταξύ του Ε και του Β να είναι πολύ πιο γρήγορη από αυτή του Α με τον Β.
Μετά την επιτυχία των δύο φάσεων ο Ε θα μπορεί να επικοινωνεί με τον Β σαν να ήταν ο Α και να εκμεταλλεύεται τα δικαιώματα που έχουν δοθεί από τον Β στον Α.

Το παράδειγμα αυτής της επίθεσης αποτελεί ένα μόνο μικρό δείγμα της χρήσης του IP spoofing σε διάφορες κακόβουλες ενέργειες. Τέτοιες ενέργειες μπορεί να είναι το scanning, (D)DoS Attacks, Covert Channels και πολλές άλλες. Μερικές από τις επιθέσεις που έχει εφαρμογή το IP Spoofing είναι οι παρακάτω:

- Land
- Teardrop
- NewTear
- SynDrop
- TearDrop2
- Bonk
- Boink
- Fragment overlap
- Ping of death
- IP source route
- Ping storm
- smurf
- ICMP unreachable storm
- Suspicious router advertisement
- UDP port loopback
- snork
- fraggle
- SYN flood

Το κύριο πλεονέκτημα του IP spoofing είναι ότι μέσω αυτού ο επιτιθέμενος μπορεί να κρύψει την πραγματική του ταυτότητα, δυσκολεύοντας έτσι τον εντοπισμό του και την ποινική δίωξή του αν προκύψει τέτοιο θέμα.
Καθώς με αυτήν την τεχνική ο επιτιθέμενος δεν χρησιμοποιεί την δικιά του IP στα πακέτα που στέλνει, οι απαντήσεις που προκύπτουν σε αυτά τα πακέτα στέλνονται στο σύστημα του οποίου ο επιτιθέμενος έκανε χρήση την IP διεύθυνση.
Για τον λόγο αυτόν το IP spoofing υλοποιείται ποιο εύκολα σε επιθέσεις που ο επιτιθέμενος δεν χρειάζεται να παίρνει κάποια απάντηση στα πακέτα που στέλνει και σε αυτές που υλοποιούνται με την χρήση connectionless πρωτοκόλλων. Αυτό γιατί τα connectionless πρωτόκολλα (πχ. ICMP) δεν απαιτούν την εγκαθίδρυση μίας σύνδεσης μεταξύ δύο συστημάτων προκειμένου αυτά να επικοινωνήσουν και έτσι ο επιτιθέμενος δεν χρειάζεται να υλοποιήσει την διαδικασία του 3-way handshake με τον στόχο του, κάτι που θα απαιτούσε την ανταλλαγή συγκεκριμένων πακέτων μεταξύ των δύο.

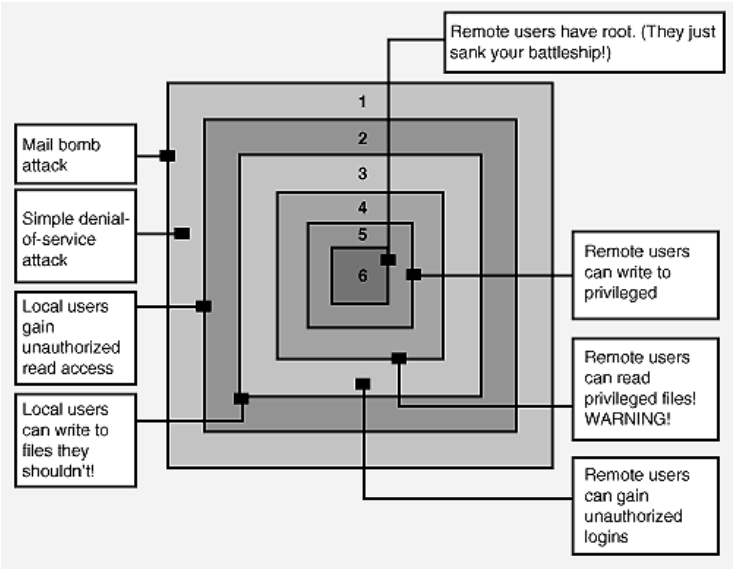
Ακόμα και στην περίπτωση που ο επιτιθέμενος χρειάζεται να βλέπει τις απαντήσεις που προκύπτουν από τα spoofed πακέτα που στέλνει, υπάρχουν διάφοροι τρόποι για να το καταφέρει αυτό, όπως με sniffing σε κάποιο σημείο του δικτύου που περνάνε αυτά τα πακέτα.

Στο Κεφάλαιο 3 παρουσιάζεται αναλυτικά μία μορφή του IP Spoofing, το Icmp Spoofing το οποίο υλοποιείται με την χρήση του ICMP πρωτοκόλλου.

Επίπεδα Ευαισθησίας Μίας Επίθεσης

Στις επόμενες σελίδες παρουσιάζεται ένα μοντέλο που κατηγοριοποιεί τα είδη των επιθέσεων σε ***επίπεδα ευαισθησίας***. Τα επίπεδα ευαισθησίας έχουν να κάνουν με τον βαθμό επικινδυνότητας που έχουν οι επιπτώσεις μίας πετυχημένης επίθεσης σε ένα σύστημα ή δίκτυο.

Στο **Σχήμα 1-5** απεικονίζεται αυτό το μοντέλο. Οι επιθέσεις που ανήκουν στο πρώτο επίπεδο θεωρούνται ή λιγότερο επιζήμιες, ενώ αυτές που ανήκουν στο έκτο επίπεδο θεωρούνται οι πιο βλαβερές.



Σχήμα 1-5: Το μοντέλο του SAM – Επίπεδα Ευαισθησίας

Επίπεδο 1

Επιθέσεις αυτού του τύπου παρενοχλούν το θύμα αποκόπτοντας κάποιες υπηρεσίες που έχει στην διάθεσή του. Οι επιθέσεις που μπορεί να οδηγήσουν σε τέτοια αποτελέσματα είναι κυρίως οι (D)DoS επιθέσεις.
Ο επιτιθέμενος δεν αποκτά κάποιο έλεγχο στο θύμα και δεν χρειάζεται να έχει μεγάλη εμπειρία για να υλοποιήσει τέτοιου είδους επιθέσεις.
Παρόλα αυτά υπάρχουν και τέτοιου είδους επιθέσεις που μπορεί να δημιουργήσουν σοβαρά προβλήματα σε ένα σύστημα ή ένα δίκτυο καθώς μπορεί να πλήξουν την αξιοπιστία και την φήμη ενός γνωστού οργανισμού όταν αυτός δεν θα μπορεί να προσφέρει την ανάλογη ποιότητα των υπηρεσιών που υπόσχεται στους χρήστες του.

Επίπεδα 2 Και 3

Το επίπεδο 2 αφορά τους τοπικούς χρήστες. Δηλαδή οποιονδήποτε έχει ένα password σε μια μηχανή που βρίσκεται στο τοπικό δίκτυο.
Τέτοιες επιθέσεις λαμβάνουν χώρα όταν τοπικοί χρήστες καταφέρνουν να διαβάσουν (read) ή να γράψουν (write) σε αρχεία που δεν τους επιτρέπεται.

Το επίπεδο 3 αφορά κυρίως απομακρυσμένους χρήστες οι οποίοι προσπαθούν να κάνουν login στο σύστημα ενώ δεν έχουν κάποιο εξουσιοδοτημένο λογαριασμό. Τέτοιου είδους επιθέσεις μπορούν να προκύψουν όταν κάποιος εφαρμόζει κάποια μέθοδο του password stealing.

Επίπεδο 4

Αυτό το επίπεδο αφορά απομακρυσμένους χρήστες που καταφέρνουν να διαβάσουν απόρρητα αρχεία.

Επίπεδα 5 Και 6

Επιθέσεις αυτού του τύπου μπορούν να προκαλέσουν σημαντικές ζημιές σε ένα σύστημα και να επιφέρουν ακόμα και την καταστροφή του.
Τέτοιου είδους επιθέσεις γίνονται με σκοπό απομακρυσμένοι χρήστες να αποκτήσουν read και write δικαιώματα σε αρχεία που δεν θα έπρεπε, καθώς και να εκτελέσουν οποιαδήποτε εντολή στο σύστημα.
Έτσι ο επιτιθέμενος προσπαθεί να αποκτήσει τα δικαιώματα του root και να δράσει εις βάρος του συστήματος. Επιθέσεις που οδηγούν στο επίπεδο 6 υλοποιούνται συνήθως με την εκτέλεση κάποιου exploit για buffer overflow.

Αν τα επίπεδα 2 έως 4 έχουν ασφαλιστεί σωστά, τότε είναι αρκετά δύσκολο να γίνει μια παραβίαση που να αφορά τα τελευταία επίπεδα.