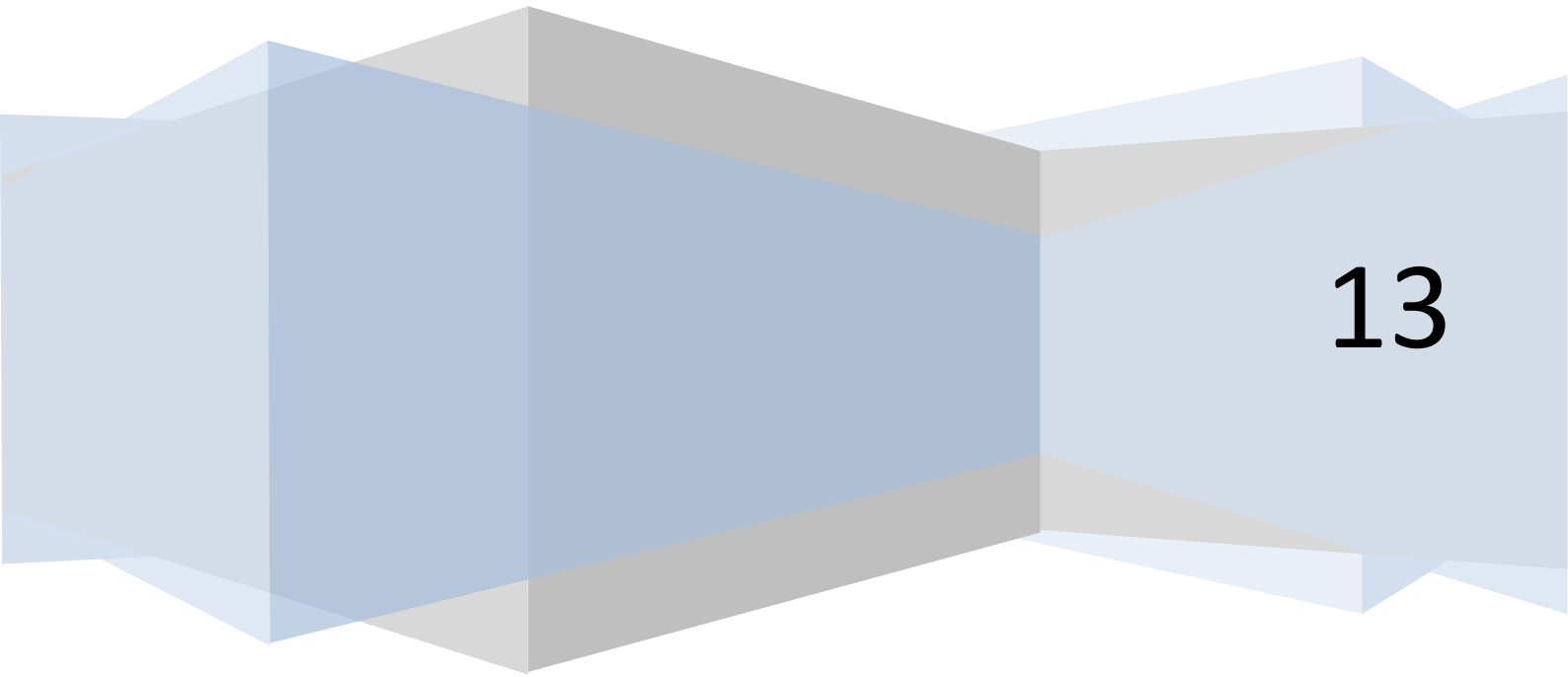
ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

ΑΣΦΑΛΕΙΑ ΚΑΙ ΕΥΠΑΘΕΙΕΣ ΔΙΚΤΥΩΝ

ΤΕΧΝΙΚΕΣ ΕΙΣΒΟΛΗΣ ΚΑΙ ΠΡΟΣΤΑΣΙΑΣ

ΚΡΑΝΑΣ ΧΑΡΑΛΑΜΠΟΣ



13

ΑΣΦΑΛΕΙΑ -ΚΑΙ ΕΥΠΑΘΕΙΕΣ ΔΙΚΤΥΩΝ

ΚΡΑΝΑΣ ΧΑΡΑΛΑΜΠΟΣ

ΕΞΑΜΗΝΟ 13^{Ο} Α.Μ. 9911 e-mail krbabis@gmail.com

Θα ήθελα να ευχαριστήσω τους φίλους μου Νικόλαο Καραγιάννη, Αρίστο Μπούση,Αθανάσιο Στεργίου καθώς επίσης και την οικογένεια μου που όλα αυτά τα χρόνια με στηρίζει και με βοηθάει. Θέλω να ευχαριστήσω και τους συμμάχους μου στο www.grepolis.com που απάντησαν στο ερωτηματολόγιο μου.

ΠΕΡΙΕΧΟΜΕΝΑ

Η παρούσα εργασία αποτελεί προϊόν αποκλειστικά δικής μου προσπάθειας. Όλες οι πηγές που χρησιμοποιήθηκαν περιλαμβάνονται στη βιβλιογραφία και γίνεται ρητή αναφορά σε αυτές μέσα στο κείμενο όπου έχουν χρησιμοποιηθεί.

ΠΕΡΙΛΗΨΗ

Στις μέρες που διανύουμε η ανάγκη για ασφάλεια στις επικοινωνίες μας είναι δεδομένη. Η επιστήμη της πληροφορικής και κατ επέκταση της ασφάλειας των δικτύων εξελίσσεται καθημερινά φέρνοντας στο φως τρωτά σημεία και ευπάθειες που μέχρι πριν λίγο καιρό ήταν άγνωστα στους διαχειριστές δικτύων.

Τα τελευταία χρόνια οι χρήστες του διαδικτύου έχουν αυξηθεί εκθετικά. Αυτό δίνει την δυνατότητα σε κακοπροαίρετους χρήστες να χρησιμοποιούν την ημιμάθεια των πολλών για προσωπικό τους όφελος όπως την εξαπάτηση για γρήγορο κέρδος την απόκτηση προσωπικών δεδομένων(έγγραφα, φωτογραφίες, κωδικούς πρόσβασης σε σελίδες κοινωνικής δικτύωσης) χωρίς την αδεία τους.

Στο πρώτο κεφάλαιο της πτυχιακής μου εργασίας δίνω στον αναγνώστη μια πρώτη επαφή με τις έννοιες που θα ακολουθήσουν. Το δεύτερο κεφάλαιο αποτελεί μια εισαγωγή-πρώτη γνωριμία με τα δίκτυα και τις ομάδες των κακόβουλων χρηστών. Στο τρίτο κεφάλαιο πλέον, και έχοντας υπόψη τα δύο προηγούμενα , μελετάω γνωστές τεχνικές εισβολής σε ένα δίκτυο και τις ευπάθειες του πρωτόκολλου TCP/IP που χρησιμοποιούν. Στο τέταρτο κεφάλαιο παρουσιάζω απλούς τρόπους προστασίας του χρήστη και ένα πιο σύνθετο. Το πέμπτο κεφάλαιο αποτελείται από τις δύο πιο γνωστές πλατφόρμες που χρησιμοποιούν οι Hackers για να αποκτήσουν πρόσβαση σε ένα δίκτυο. Τέλος το 6^{ο} και 7^{ο} κεφάλαιο είναι μια μικρή έρευνα που έκανα με τη χρήση ερωτηματολογίου και παραδίδω τα αποτελέσματα αλλά και το προσωπικό σχόλιο μέσα από τα συμπεράσματα.

1.ΒΑΣΙΚΕΣ ΕΝΝΟΙΕΣ

Πριν την ανάγνωση της εργασίας θα ήταν απαραίτητη η κατανόηση των παρακάτω όρων.

LAN = Local Area Network, τοπικό δίκτυο.[1]

Ethernet [1]=Το Ethernet είναι το συνηθέστερα χρησιμοποιούμενο πρωτόκολλο ενσύρματης τοπικής δικτύωσης υπολογιστών. Αναπτύχθηκε από την εταιρεία Xerox κατά τη δεκαετία του '70 και έγινε δημοφιλές αφότου η Digital Equipment Corporation και η Intel, από κοινού με τη Xerox, προχώρησαν στην προτυποποίησή του το 1980. Το 1985 το Ethernet έγινε

αποδεκτό επίσημα από τον οργανισμό IEEE ως το πρότυπο 802.3 για ενσύρματα τοπικά δίκτυα (LAN).

MAC [1] = Media Access Control έλεγχος πρόσβασης σε μέσα

TCP [1] =Transmission Control Protocol, Πρωτόκολλο Ελέγχου Μετάδοσης

IP [1] =Internet Protocol, Πρωτόκολλο επιπέδου Internet που χρησιμοποιείται για διευθηνσιοδότηση, παράδοση και δρομολόγηση datagram.

ARP [1] =Address Resolution Protocol, πρωτόκολλο επιπέδου Internet που χρησιμοποιείται για να βρίσκει την φυσική διεύθυνση που σχετίζεται με μια IP διεύθυνση. Υπάρχει και το rARP που κάνει ακριβώς το ανάποδο.

ICMP [1] =Internet Control Message Protocol

Άρνηση παροχής υπηρεσιών(Denial Of Service a.k.a D.O.S) = Παρεμποδίζεται η νόμιμη πρόσβαση σε πόρους και δεδομένα

Back Track 5[5]= Διανομή Linux, που περιέχει αρκετά εργαλεία για την παρακολούθηση του συστήματος. Στα πλαίσια της εργασίας μου και διδακτικούς και μόνο λόγους χρησιμοποίησα κάποια από αυτά

Πλατφόρμα = Λογισμικό που χρησιμοποιείται για συγκεκριμένο τρόπο για ειδικό σκοπό

Penetration Testing = Μία μέθοδος αξιολόγησης της ασφάλειας των δικτύων και των υπολογιστών.

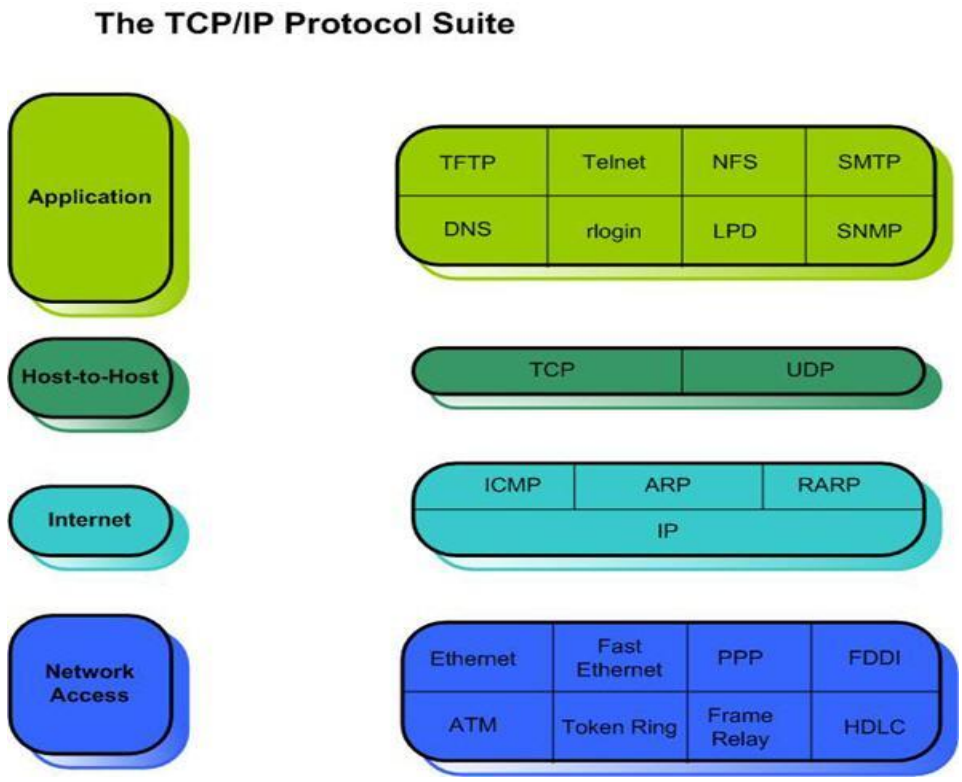
Reverse shell = αποστολή ενός Reverse shell είναι να τρέξει σε στο μηχάνημα στόχο και να συνδεθεί στο μηχάνημα του επιτιθέμενου, παρέχοντας ένα πλήρες κέλυφος εντολών.

Scripting = εκμετάλλευση διαφόρων ευπαθειών υπολογιστικών συστημάτων για την εισαγωγή κώδικα

Uptime = διάρκεια λειτουργίας, μέτρο χρόνου που είναι ανοιχτός ένας υπολογιστής

2.ΕΙΣΑΓΩΓΗ

Το TCP/IP είναι μια στοίβα από πρωτόκολλα επικοινωνίας στα οποία βασίζεται το διαδίκτυο. Πήρε το όνομα του από τα δύο βασικά πρωτόκολλα που χρησιμοποιεί, το TCP και το IP. Έχει τέσσερα επίπεδα. Το κάθε επίπεδο αποτελείται από πρωτόκολλα όπως φαίνετε και στην παρακάτω εικόνα.



TCP/IP με τα διάφορα πρωτόκολλα σε κάθε επίπεδο

Με την ανάπτυξη του διαδικτύου, βγήκαν στην επιφάνια ευπάθειες που έχουν τα πρωτόκολλα σε όλα τα επίπεδα του TCP/IP.Στις μέρες μας η ασφάλεια δικτύων είναι ένας τομέας που εξελίσσεται ακόμα. Σχεδόν κάθε μέρα υπάρχουν δημοσιεύματα για περιστατικά όπου διεθνής οργανισμοί και ερευνητικά κέντρα πέφτουν θύματα κακόβουλων επιθέσεων. Οι επιθέσεις αυτές δεν είναι καθόλου τυχαίες. Οι επιτιθέμενοι μπορούν να χωριστούν σε τρεις μεγάλες ομάδες:

- Ερασιτέχνες έφηβοι(script kiddies):Τα παιδιά που παίζουν. Έχουν στοιχειώδη γνώση των υπολογιστών και απλώς εφαρμόζουν script και τεχνικές εισβολής που είναι διαθέσιμες στο Internet.
- Ψυχαγωγικοί εισβολείς: Περιλαμβάνει ενήλικες εισβολείς και πολλά κίνητρα. Το πιο βασικό κίνητρο, τους είναι καθαρά η εγκεφαλική πρόκληση

- Επαγγελματίες: Είναι η πιο επικίνδυνη ομάδα και αποτελείτε από έμπειρους ειδικούς που ξέρουν πολλά γύρω από την επιστήμη της πληροφορικής και ειδικότερα για την ασφάλεια και τις ευπάθειες δικτύων. Είναι δύσκολο να βρεθούν γιατί ξέρουν αρκετούς τρόπους για να καλύψουν τα ίχνη τους.

Οι ομάδες που αναφέρθηκαν παραπάνω προσεγγίζουν τα δίκτυα για διαφορετικούς λόγους αλλά όλοι έχουν σαν κίνητρο την απόκτηση ελέγχου πάνω σε ένα δίκτυο.

3.ΤΕΧΝΙΚΕΣ ΕΙΣΒΟΛΗΣ ΣΕ ΔΙΚΤΥΑ

Όταν άρχισε ο σχεδιασμός των δικτύων, οι τότε ειδική δεν είχαν προβλέψει ότι κάποιοι θα προσπαθούσαν να αποσπάσουν πληροφορίες μέσα από τις ευπάθειες των πρωτοκόλλων. Τα τελευταία χρόνια με την ανάπτυξη του διαδικτύου αυξήθηκαν τα κρούσματα επιθέσεών κατά των δικτύων. Παρακάτω περιγράφονται τρεις από τις πιο γνωστές τεχνικές εισβολής σε ένα δίκτυο.

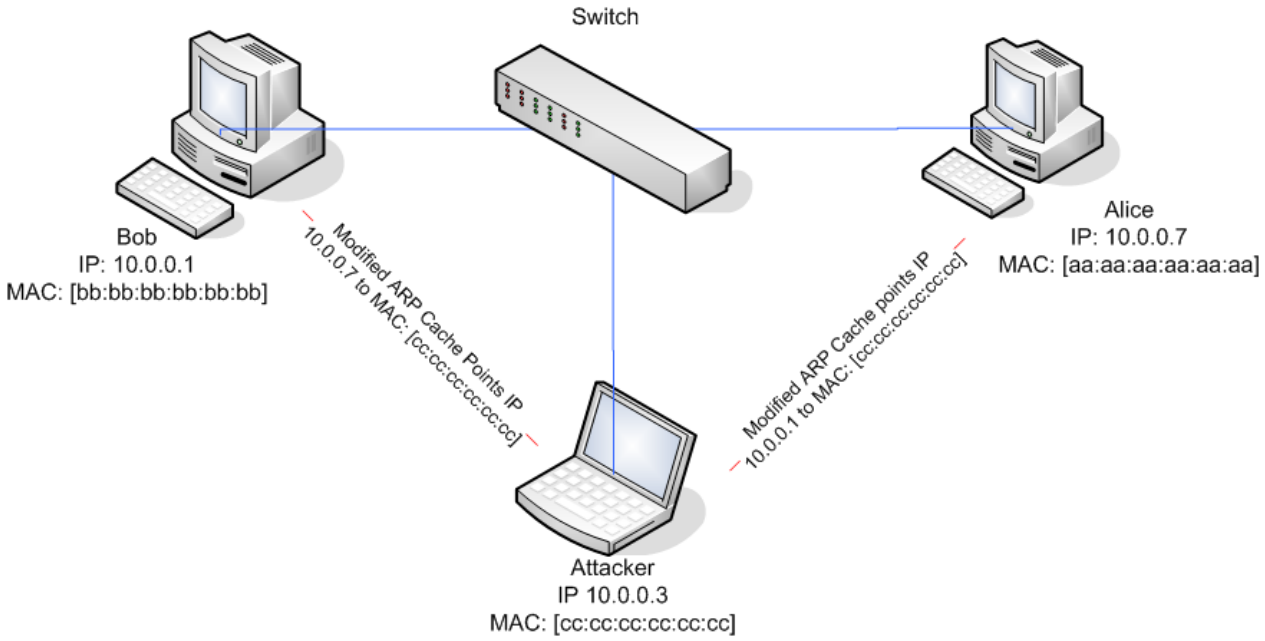
3.1. PACKET SNIFFER

Η διαδικασία με την οποία οι ενδιαφερόμενοι καταγράφουν τα δεδομένα ενός δικτύου λέγεται packet sniffing[4][10].Η τεχνική αυτή δεν ξεκίνησε ως κακόβουλη, αλλά βοηθούσε τους διαχειριστές στην παρακολούθηση του δικτύου τους. Όσοι πραγματοποιούν Packet Sniffing χρησιμοποιούν εργαλεία που χωρίς να τους έχει δοθεί άδεια από τον εκάστοτε διαχειριστή, παρακολουθούν την κίνηση του δικτύου και έχουν την δυνατότητα να καταγράψουν αλλά και να συλλάβουν τους κωδικούς πρόσβασης. Σκοπός του είναι όπως είπαμε και πιο πάνω η απόκτηση του πολυπόθητου κωδικού πρόσβασης και από εκεί και πέρα η παρακολούθηση όλου του δικτύου ή και ενός χρήστη μόνο. Με αυτή την τεχνική μπορούν να υποκλέψουν προσωπικά δεδομένα όπως φωτογραφίες έγγραφα και οτιδήποτε μπορεί να περάσει από το μυαλό κάποιου.

Οι πιο συνηθισμένοι χώροι όπου κάποιος μπορεί να κάνει Packet sniffing, αλλά και να πέσει θύμα είναι καφετέριες και γενικότερα δημόσιες τοποθεσίες οπού οι χρήστες δεν μπορούν να ξέρουν τι μορφή κρυπτογράφησης χρησιμοποιείτε για το δίκτυο που συνδέονται.

3.2 Man in The Middle (MiTM)

Σε κάθε δίκτυο LAN οι υπολογιστές που είναι μέλη, έχουν τουλάχιστον μία κάρτα δικτύου που μπορεί να είναι ενσύρματη ή ασύρματη και χρησιμοποιεί την τεχνολογία του Ethernet.Κάθε κάρτα έχει έναν μοναδικό αριθμό υλικού ο οποίος την ταυτοποιεί μονοσήμαντα. Οι διευθύνσεις υλικού αναφέρονται και ως MAC addresses.Χάρη στη μοναδικότητα των MAC, ένας οποιοσδήποτε υπολογιστής ενός LAN μπορεί να αποστέλλει απευθείας πακέτα σε οποιονδήποτε άλλο υπολογιστή του ίδιου δικτύου LAN. Επίσης μπορεί να εκπέμπει πακέτα, τα οποία λαμβάνουν όλοι οι άλλοι υπολογιστές του LAN.Σε ένα LAN έχουμε δύο μεθόδους δρομολόγησης των πακέτων. Η μία χαρακτηρίζεται ως τοπική και χρησιμοποιεί τις διευθύνσεις MAC.Η άλλη ως καθολική και κάνει χρήση του πρωτοκόλλου IP. Σύμφωνα με τα παραπάνω είναι προφανές ότι είναι απαραίτητη η παρουσία ενός μηχανισμού που θα γεφυρώνει τις MAC addresses με τις IP addresses.Ο μηχανισμός αυτός υπάρχει και περιγράφεται από το ARP(βλ. Βασικές έννοιες).Το πρωτόκολλο ARP είναι τόσο απλά σχεδιασμένο που τα ARP replies του να μην εμπεριέχουν κάποιον μηχανισμό ταυτοποίησης. Αυτό σημαίνει ότι οποιοδήποτε μηχάνημα του LAN είναι σε θέση να ισχυριστεί ότι έχει την τάδε IP,χωρίς κανείς να μπορεί να επαλήθευση την εγκυρότητα των λεγομένων του.



Man in the middle

Στη πράξη τώρα όταν σε ένα τοπικό δίκτυο θέλουμε να δρομολογήσουμε ένα πακέτο IP που προορίζεται για ένα από τα μηχανήματα του δικτύου μας πρέπει μεταξύ άλλων να ενσωματώσουμε μια διεύθυνση MAC.Αυτή η MAC address είναι εκείνη του NIC που φέρει ο παραλήπτης του πακέτου. Στο LAN που βρισκόμαστε υπάρχει περίπτωση ο δρομολογητής να γνωρίζει ήδη την MAC address ή να την γνώριζε κάποια στιγμή αλλά τώρα η περίοδος

εγκυρότητας της συγκεκριμένης πληροφορίας να έχει λήξει. Σε αυτή την περίπτωση ο δρομολογητής στέλνει ένα ARP request, προς όλα τα μηχανήματα του δικτύου. Τα μηχανήματα ακούνε αυτό το request και απαντάνε με ARP reply.Ο δρομολογητής όταν λάβει τα ARP replies τα καταγράφει σε ένα πίνακα που ονομάζεται ARP cache. Επίσης πίνακα arp cache έχουν όλα τα μηχανήματα του LAN, για να ανταλλάσουν πακέτα μεταξύ τους .Σε αυτό το σημείο φαίνετε η ευπάθεια του πρωτοκόλλου arp. Αν ένα μηχάνημα στείλει ένα κάλπικο reply σε ένα request του δρομολογητή, τότε ο δεύτερος θα ενημερώσει την ARP cache του με αχρηστεύοντας έγκυρη γνώση που είχε πριν το κάλπικο ARP reply. Το κακόβουλο μηχάνημα μπορεί ταυτόχρονα να στείλει σε ένα ή περισσότερα άλλα μέλη του δικτύου, ανάλογες κάλπικες πληροφορίες, πραγματοποιώντας αυτό που είναι γνωστό ως ARP cache poisoning. Το παραπάνω μηχάνημα με όλη αυτή τη δηλητηρίαση έχει πετύχει μια επίθεση τύπου Man In The Middle[4] [8].

3.3 Port Scanning

Η πρόσβαση σε εφαρμογές δικτύου γίνεται μέσω λογικών καναλιών που είναι γνωστά ως θύρες[4] και λειτουργούν στο επίπεδο μεταφοράς της στοίβας TCP/IP. Οι επιτιθέμενοι αποκτούν συνήθως πρόσβαση σε ένα σύστημα με την εύρεση μια ανοικτής θύρας που οδηγεί σε μια υπηρεσία του δικτύου που παρακολουθεί τις συνδέσεις του δικτύου. Σε μερικές περιπτώσεις η υπηρεσία μπορεί να εκτελείται εξ ορισμού χωρίς ο ιδιοκτήτης του συστήματος να το ξέρει. Άλλες φορές, η υπηρεσία μπορεί να διαμορφωθεί άσχημα ή μπορεί να επιτρέπει την πρόσβαση μέσω ενός προκαθορισμένου ή ανώνυμου λογαριασμού χρήστη.

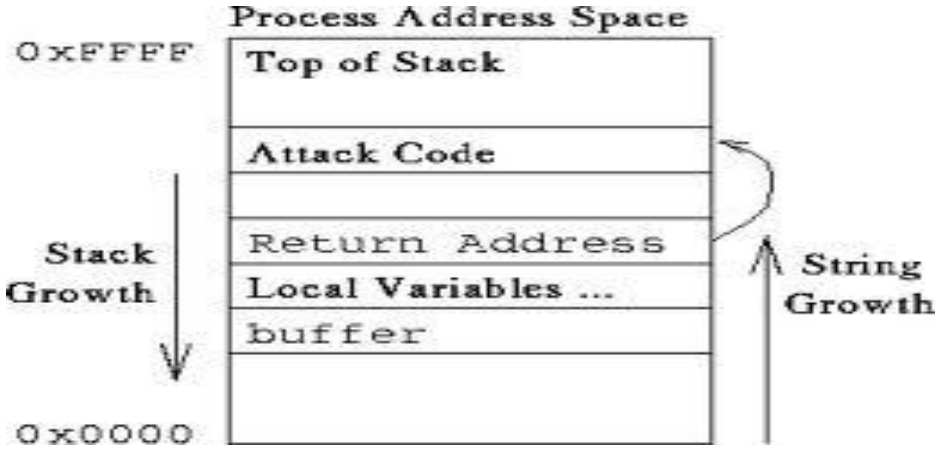
Υπάρχουν εργαλεία όπως το Nessus και Nmap(αναλύεται σε παρακάτω κεφάλαιο) που αυτοματοποιούν τη διαδικασία αναζήτησης ανοικτών θυρών. Αυτοί οι ανιχνευτές χρησιμοποιούνται και από τους εισβολείς που ψάχνουν για κενά ώστε να μπορούν να αποκτήσουν πρόσβαση αλλά και από επαγγελματίες των δικτύων που ψάχνουν για κενά ώστε να μπορούν να τα κλείσουν και να αποτρέψουν την πρόσβαση. Άλλα πιο εξειδικευμένα εργαλεία ψάχνουν για κενά σε συγκεκριμένα πρωτόκολλα και υπηρεσίες δικτύου. Σε πολλές περιπτώσεις η ύπαρξη μια ανοικτής θύρας δεν είναι αρκετή για να μπει ένας εισβολέας αλλά παρέχει στον επιτιθέμενο την ευκαιρία να ξεκινήσει μια επίθεση επιπέδου εφαρμογής ώστε να εκμεταλλευτεί ένα γνωστό τρωτό σημείο της υπηρεσίας που παρακολουθεί τη θύρα. Μερικές από τις πιο γνωστές θύρες φαίνονται στο παρακάτω πίνακα.

Port	**Description**	**Status**
1/TCP, UDP	TCPMUX (TCP port service multiplex)	official
5/TCP, UDP	RJE (remote job entry)	official
7/TCP, UDP	Echo protocol	official

21	FTP control (command port)	official
22/TCP, UDP	SSH (secure shell) χρησιμοποιείται για ασφαλείς συνδέσεις σε υπολογιστές Unix για τη μεταφορά αρχείων και για Port Forwarding	official
23/TCP, UDP	Telnet – μη κρυπτογραφημένη επικοινωνία	official
25/TCP, UDP	SMTP – χρησιμοποιείται για την διακίνηση των μηνυμάτων email μεταξύ των servers	official
53/TCP, UDP	DNS (Domain Name System)	official
80/ TCP	Http (Hyper Text Transfer Protocol)	official
88/TCP	Kerberos – χρησιμοποιείται για αυθεντικοποίηση χρηστών	official
443/TCP	Http / Https Protocol over TLS/SSL (κρυπτογραφημένη μεταφορά επικοινωνίας	official

3.4 Buffer Overflow

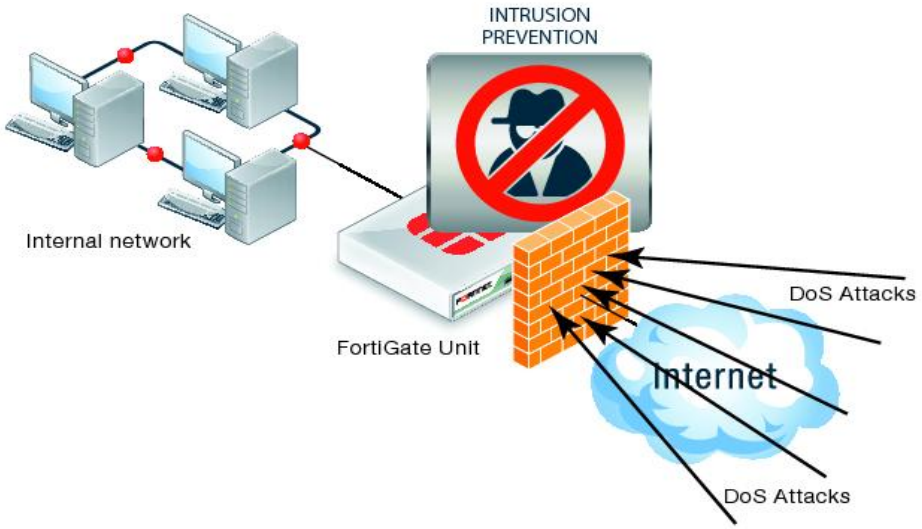
Μια τεχνική επίθεσης που βασίζεται σε ευπάθειες που υπάρχουν στο επίπεδο εφαρμογής. Όταν ένας διακομιστής λαμβάνει δεδομένα μέσω μιας σύνδεσης δικτύου ή ακόμα και όταν λαμβάνει δεδομένα από ένα πληκτρολόγιο πρέπει να διατηρεί αρκετό χώρο στη μνήμη για να λαμβάνει τι πλήρες σύνολο δεδομένων. Αυτός ο χώρος ονομάζεται buffer[2]. Αν η είσοδος του χρήστη υπερχείλιση το buffer συμβαίνουν περίεργα πράγματα. Αν ο τρόπος διαχείρισης της εισόδου δεν γίνεται σωστά, τα δεδομένα που υπερχειλίζουν το buffer μπορεί να παραμείνουν μόνιμα στην περιοχή εκτέλεσης της CPU, που σημαίνει ότι μπορούν να εκτελέσουν εντολές που στέλνονται στον υπολογιστή μέσω ενός υπερχειλισμένου buffer.



Οι εντολές εκτελούνται με τα δικαιώματα της εφαρμογής που έλαβε τα δεδομένα. Άλλες τέτοιες επιθέσεις υπερχείλισης buffer βασίζονται στο γεγονός ότι μερικές εφαρμογές τρέχουν σε ένα περιβάλλον μεγαλύτερης ασφάλειας που μπορεί να παραμένει ενεργό όταν η εφαρμογή τερματίσει απρόσμενα. Αρκετές φημισμένες εφαρμογές δικτύων είναι τρωτές στη υπερχείλιση buffer όπως ο διακομιστής ηλεκτρονικού ταχυδρομείου send mail του unix αλλά και ο Internet Information Server (IIS) της Microsoft.

3.3 Denial of Service (D.O.S.) Επιθέσεις

Οι επιθέσεις άρνησης παροχής υπηρεσιών (Denial Of Service) [2][4] έχουν γίνει κάτι απλό και καθημερινό. Είναι μια τεχνική που είναι σχεδόν αδύνατον να σταματήσει επειδή δεν απαιτεί από τον εισβολέα να έχει κάποια συγκεκριμένα δικαιώματα στο δίκτυο. Η εύκολη υλοποίηση των επιθέσεων D.O.S προσφέρει γρήγορη αναγνώριση στον επιτιθέμενο ανάμεσα στον "κόσμο" των Hackers. Σκοπός των επιθέσεων άρνησης παροχής υπηρεσιών είναι να υπερφορτώσουν το σύστημα αρκετά αποστέλλοντας πακέτα δεδομένων με υπερβολικά μεγάλο ρυθμό ώστε να καταρρεύσει ή να απενεργοποιηθεί.



Με ποιο απλό τρόπο η ουσία μια D.O.S επίθεσης έχει ως στόχο να εκμεταλλευτεί τις αδυναμίες του πρωτοκόλλου TCP/IP ή να εξαντλήσει, καταναλώσει όλους τους πόρους(μνήμη, CPU, Bandwidth) του συστήματος με αποτέλεσμα την διακοπή της λειτουργίας του. Οι πιο γνωστές επιθέσεις D.O.S είναι οι teardrop[3], smurf attack[2] και η ping of death[4] όπου αναλύονται παρακάτω για το πώς γίνονται και την προκαλούν στο δίκτυο που επιτίθενται

3.3.1 TEAR DROP

Είναι η πιο σύγχρονη επίθεση άρνησης παροχής υπηρεσιών. Για την ομαλή επικοινωνία μεταξύ δύο τερματικών, τα πακέτα δεδομένων που στέλνονται "σπάνε" σε μικρότερα κομμάτια που έχουν μια σειρά από στοιχεία ελέγχου(flag) και επανασυνδέονται όταν φτάσουν στον προορισμό τους.

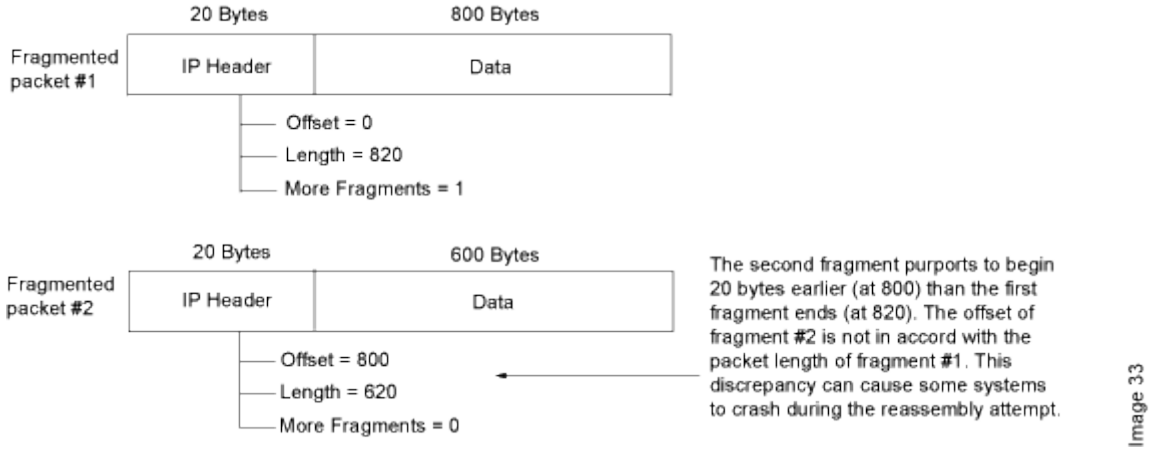


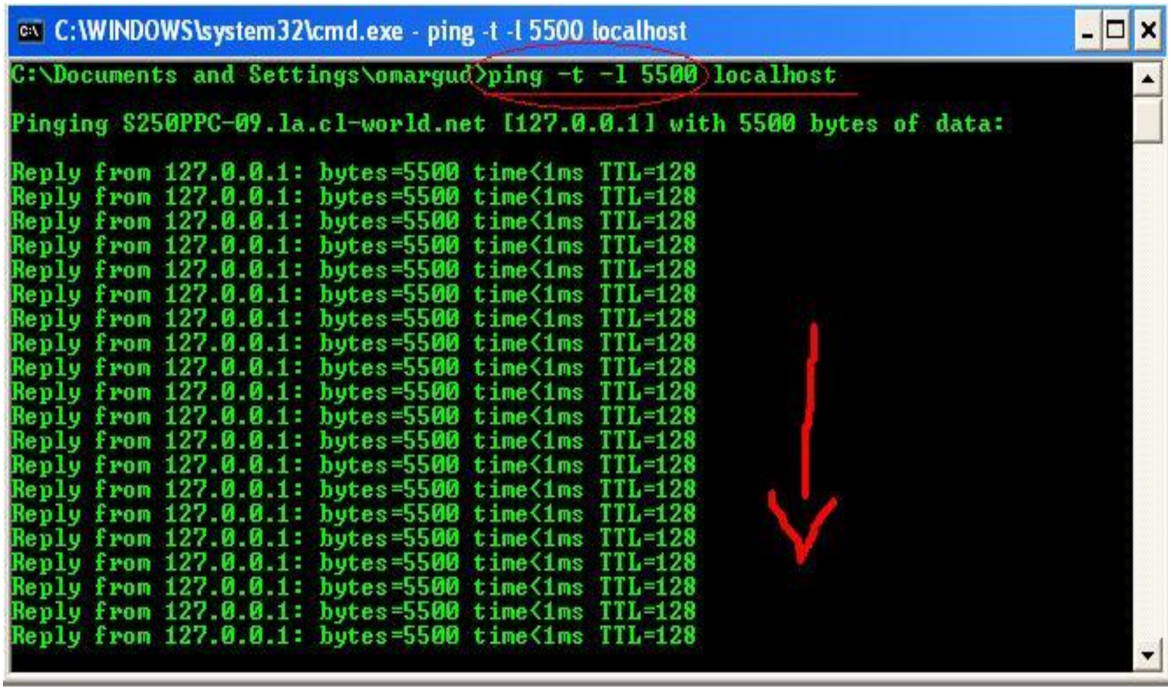
Image 33

Μία επίθεση κατακλυσμού σταγονιδίων(tear drop[4]) συμβαίνει όταν ένας επίδοξος εισβολέας στέλνοντας λανθασμένα στοιχεία ελέγχου εκμεταλλεύεται την αδυναμία του πρωτοκόλλου να συναρμολογήσει τα κομμάτια που αποσπασματικά έχουν σταλθεί. Με τον τρόπο αυτό καταφέρνει να προκαλέσει σύγχυση στο σύστημα που λαμβάνει αυτά τα πακέτα με αποτέλεσμα να καταρρεύσει από το μεγάλο όγκο προβληματικής πληροφορίας.

3.3.2 PING OF DEATH

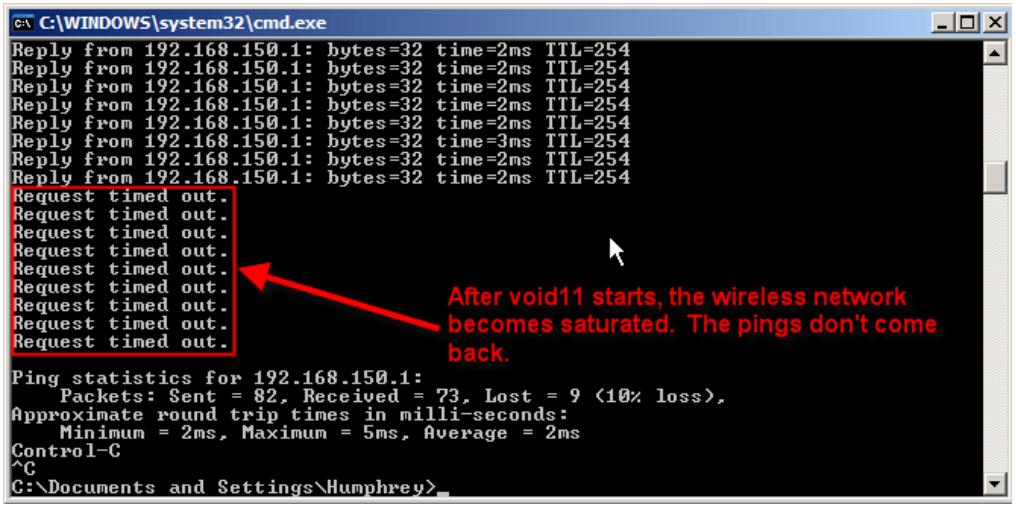
Είναι η πιο γνωστή επίθεση D.O.S To Ping of Death[4][11] είναι ένα είδος επίθεσης που εκμεταλλεύεται το πρωτόκολλο ICMP . Το ICMP συνήθως παραβλέπει το μέγεθος των δεδομένων γιατί η σημαντική πληροφορία βρίσκεται στην επικεφαλίδα. Το μέγιστο μέγεθος πακέτου ping στο IPv4 είναι 65536 bytes, στέλνοντας λοιπόν μεγαλύτερα πακέτα δεδομένων όταν ο υπολογιστής τα παραλάβει και τα συνδέσει θα έχει ένα πακέτο που θα ξεπερνά το όριο προκαλώντας σφάλματα τύπου υπερχείλισης στοίβας(buffer overflow) που οδηγούν σε δυσλειτουργία όλου του δικτύου. Σήμερα είναι σχετικά εύκολη η προστασία από μια τέτοια

επίθεση αναβαθμίζοντας τον Server με περισσότερη RAM ώστε να μπορεί να επεξεργαστεί πακέτα μεγαλύτερα του επιτρεπόμενου ορίου.



3.3.3 SMURF ATTACK

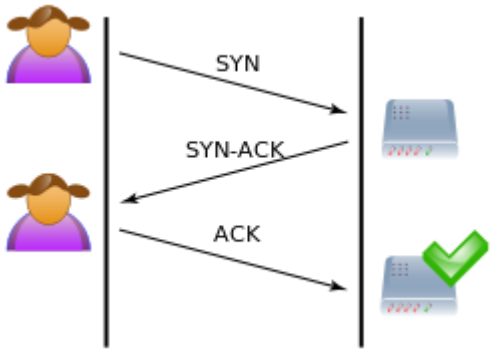
Η επίθεση smurf attack[2] χρησιμοποιεί το βοηθητικό πρόγραμμα Ping. Κάθε Server μπορεί να δεχθεί μηνύματα Ping στα οποία απαντά αποστέλλοντας μία σειρά από μηνύματα pong με τα οποία μετράται η ταχύτητα ανταπόκρισης του. Σκοπός της τεχνικής αυτής είναι ο Server να δεχθεί ένα τεράστιο αριθμό από Ping requests στα οποία πρέπει να αναπτήσει υποχρεωτικά(echo replies). Η κατανάλωση υπολογιστικής ισχύς αλλα και bandwidth του δικτύου έχει ως αποτέλεσμα την υπερφόρτωση(flood) του δικτύου και την διακοπή λειτουργίας του.



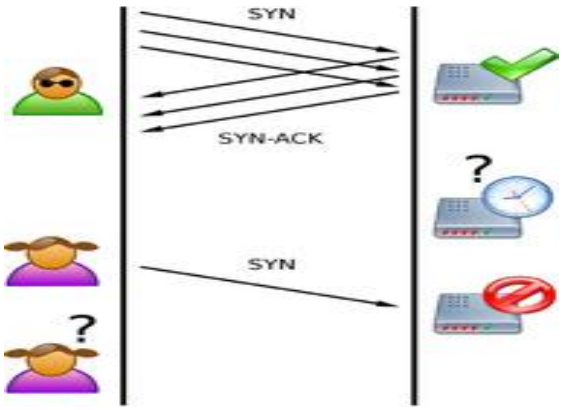
Στις μέρες μας αρκετοί Server έχουν αποκτήσει μεγάλους Ping buffers και έτσι μπορούν να απαντούν σε πολλά ping request χωρις να επηρεάζεται η λειτουργία τους, μπορούν επίσης να επεξεργάζονται όσα ping δέχονται αναγνωρίζοντας και αγνοώντας αυτόματα όποια αποτελούν προϊόν επιθέσεως.

3.3.4 SYN Flooding

Η αρχή κάθε σύνδεσης μεταξύ ενός τερματικού και ενός server γίνεται με μία σειρά βημάτων , όπως έχει ορισθέι από το πρωτόκολλο TCP. Συγκεκριμένα οι δύο πλευρές θα ακολουθήσουν μία διαδικασία που ονομάζεται τριμηερής χειραψία(three-way handshake). Ο ενδιαφερόμενος ζητά την δημιουργία μιας σύνδεσης στέλνοντας ένα πακέτο TCP SYN στο Server. Ο Server απαντά στην αίτηση του ενδιαφερόμενου στέλνοντας ένα πακέτο TCP SYN-ACK(aknownledge) που σημαίνει αναγνώριση και αποδοχή.Ο ενδιαφερόμενος απαντά με ένα πακέτο TCP ACK δηλώνοντας ότι αποδέχεται και αυτός τη σύνδεση.



Ο σκοπός της τεχνικής SYN Flooding[4] είναι ο επιτιθέμενος να στέλνει συνέχεια πακέτα SYN αλλά όχι ACK που είναι απαραίτητα για να ολοκληρωθεί η χειραψία. Ο server που δέχεται την επίθεση είναι υποχρεωμένος να περιμένει το ACK, δεσμεύοντας με την αναμονή του αυτή μεγάλο μέρος των πόρων του.

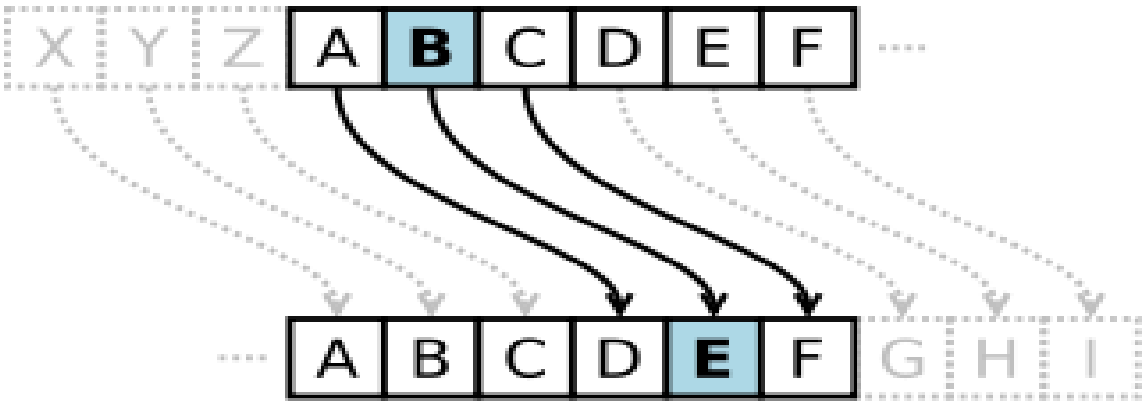


4 ΤΡΟΠΟΙ ΠΡΟΣΤΑΣΙΑΣ

Η ανάγκη για ασφάλεια στις μέρες είναι τεράστια. Τον τελευταίο χρόνο ακούμε συνεχεία για ομάδες όπως οι anonymous, που με σχετική ευκολία ξεπερνάνε την ασφάλεια ενός δικτύου και διαρρέουν δεδομένα στο διαδίκτυο. Η ασφάλεια είναι ένας τομέας που έχουν ξοδευτεί αρκετά εκατομμύρια και ακόμα δεν μπορούμε να χαρακτηρίσουμε τίποτα ασφαλή στο διαδίκτυο. Σε αυτό το κεφάλαιο υπάρχουν μερικοί απλοί τρόποι με τους οποίους μπορούμε σε μεγάλο βαθμό να διασφαλίσουμε την ακεραιότητα των δεδομένων μας από τα αδιάκριτα μάτια των άλλων.

4.1 ΚΡΥΠΤΟΓΡΑΦΗΣΗ

Από τότε που ο κόσμος άρχισε να γράφει μυστικά μηνύματα άρχισε να ψάχνει για κωδικούς ή τεχνάσματα για να διατηρεί αυτά τα μηνύματα μυστικά. Μία από τις απλούστερες και πιο γνωστές τεχνικές κωδικοποίησης στην κρυπτογραφία είναι ο κώδικας του καίσαρα. Η εφαρμογή του κώδικα καίσαρα συνίσταται στην αντικατάσταση κάθε γράμματος του κειμένου με ένα άλλο το οποίο έχει σταθερή απόσταση από αυτό το αλφάβητο. Στην εποχή των υπολογιστών ωστόσο, η κρυπτογράφηση έχει γίνει πιο εξειδικευμένη εξ αιτίας της ευκολίας με την οποία οι υπολογιστές μπορούν να χειρίζονται τεράστιους, πολύπλοκους αριθμούς. Οι περισσότεροι αλγόριθμοι κρυπτογράφησης προκύπτουν από τον χειρισμό μεγάλων πρώτων αριθμών.



Η κρυπτογράφηση[4][5][11] είναι η διαδικασία της αλλαγής των δεδομένων ώστε να μην διαβάζονται από τρίτους. Αυτό πετυχαίνετε με τη χρήση ενός αλγόριθμου που είναι ένας μαθηματικός τύπος ο οποίος εφαρμόζεται στην πληροφορία που θέλουμε να στείλουμε. Εκτός από τον αλγόριθμο κρυπτογράφησης χρειαζόμαστε και το κλειδί (encryption key) που είναι μία μοναδική και μυστική επιπλέον μεταβλητή. Υπάρχει η μορφή της συμμετρικής (συμβατική) κρυπτογράφησης και η ασύμμετρη κρυπτογράφηση που έχει αναπτυχθεί τα τελευταία 30 χρόνια.

Η πρώτη είναι η πιο συνηθισμένη μορφή, και πήρε το όνομα της επειδή η διαδικασία αποκρυπτογράφησης ήταν ακριβώς η αντίστροφη της διαδικασίας κρυπτογράφησης, ενώ η ασύμμετρη ονομάστηκε έτσι διότι το κλειδί για κρυπτογράφηση και αποκρυπτογράφηση είναι διαφορετικό.

Οι εφαρμογές κρυπτογράφησης ταξινομούνται, με βάση τρία ανεξάρτητα κριτήρια

- Τον τύπο των διαδικασιών που χρησιμοποιούνται για το μετασχηματισμό του αρχικού κειμένου σε κρυπτογράφημα.

Το σύνολο των αλγορίθμων κρυπτογράφησης στηρίζεται σε δύο γενικές αρχές: στην αντικατάσταση(substitution) του αρχικού κειμένου και στην μετάθεση(transposition) στην οποία τα στοιχεία του αρχικού κειμένου αναδιατάσσονται.

- Τον αριθμό των κλειδιών που χρησιμοποιούνται

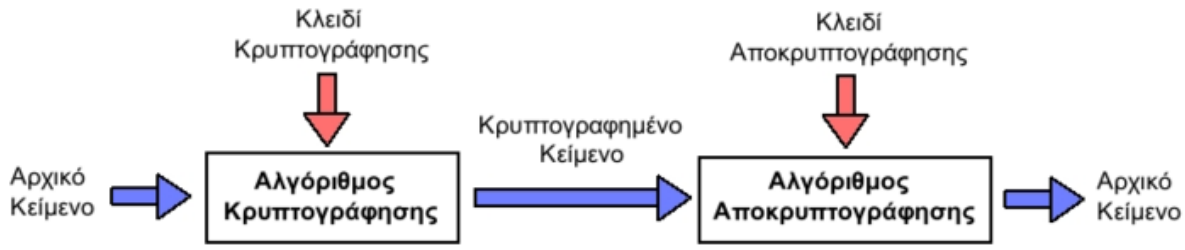
Εάν χρησιμοποιείται το ίδιο κλειδί τότε το σύστημα αναφέρεται ως συμμετρικό ή μοναδικού κλειδιού. Εάν όμως χρησιμοποιούν διαφορετικά κλειδιά, τότε το σύστημα αναφέρεται ως ασύμμετρο ή σύστημα ζεύγους κλειδιών.

- Τον τρόπο με τον οποίο επεξεργάζονται το αρχικό κείμενο.

Ένας κωδικοποιητής τμημάτων(block cipher) επεξεργάζεται την είσοδο παράγοντας κάθε φορά ένα τμήμα εξόδου για κάθε συγκεκριμένο τμήμα εισόδου. Αντίθετα, ένας κωδικοποιητής ροής (stream cipher) επεξεργάζεται κατά συνεχή τρόπο τα στοιχεία εισόδου και κάθε φορά παράγεται ως έξοδος ένα στοιχείο, με τη σειρά που καταφθάνουν τα δεδομένα.

4.1.1 ΣΥΜΜΕΤΡΙΚΗ ΚΡΥΠΤΟΓΡΑΦΙΑ

Η συμμετρική κρυπτογραφία (conventional cryptography) αναφέρεται και ως συμμετρική κρυπτογραφία(symmetric cryptography) ή κρυπτογραφία μυστικού κλειδιού(secret key cryptography)



Η συμμετρική κρυπτογραφία αποτελείται από πέντε επιμέρους οντότητές:

- Αρχικό κείμενο(plaintext): Αποτελεί το αρχικό μήνυμα ή τα αρχικά δεδομένα που εισάγονται στο αλγόριθμο κρυπτογράφησης
- Αλγόριθμος κρυπτογράφησης(encryption algorithm): Πραγματοποιεί τους απαραίτητους μετασχηματισμούς του αρχικού κειμένου για την επίτευξη κρυπτογράφησης ενός μηνύματος
- Μυστικό κλειδί(secret key): :Αποτελεί το βασικό μέρος της συμμετρικής κρυπτογράφησης διότι με βάση το μυστικό κλειδί γίνονται οι αντικαταστάσεις στο αρχικό μήνυμα καθώς επίσης και στην διαδικασία της αποκρυπτογράφησης.
- Κρυπτογράφημα ή κρυπτογραφημένο μήνυμα(cipher text): Είναι το μετασχηματισμένο μήνυμα που παράγεται ως έξοδος από τον αλγόριθμο κρυπτογράφησης
- Αλγόριθμος αποκρυπτογράφησης(decryption algorithm): Πρόκειται για έναν αλγόριθμο που πραγματοποιεί την ακριβώς αντίστροφη διαδικασία, δηλαδή λαμβάνει το κρυπτογράφημα και το ίδιο μυστικό κλειδί που χρησιμοποιήθηκε στη διαδικασία της κρυπτογράφησης και παράγει το αρχικό κείμενο.

Για την ασφαλή χρήση της συμβατικής κρυπτογραφίας απαιτείται η ύπαρξη ενός ισχυρού αλγορίθμου κρυπτογράφησης καθώς επίσης ο πομπός και ο δέκτης να έχουν παραλάβει τα αντίγραφα του μυστικού κλειδιού με ασφαλή τρόπο. Αδύναμο κρίκο στην ασφάλεια της συμβατικής κρυπτογραφίας αποτελεί μόνον η μυστικότητα του κλειδιού και όχι η μυστικότητα του αλγορίθμου που χρησιμοποιείται.

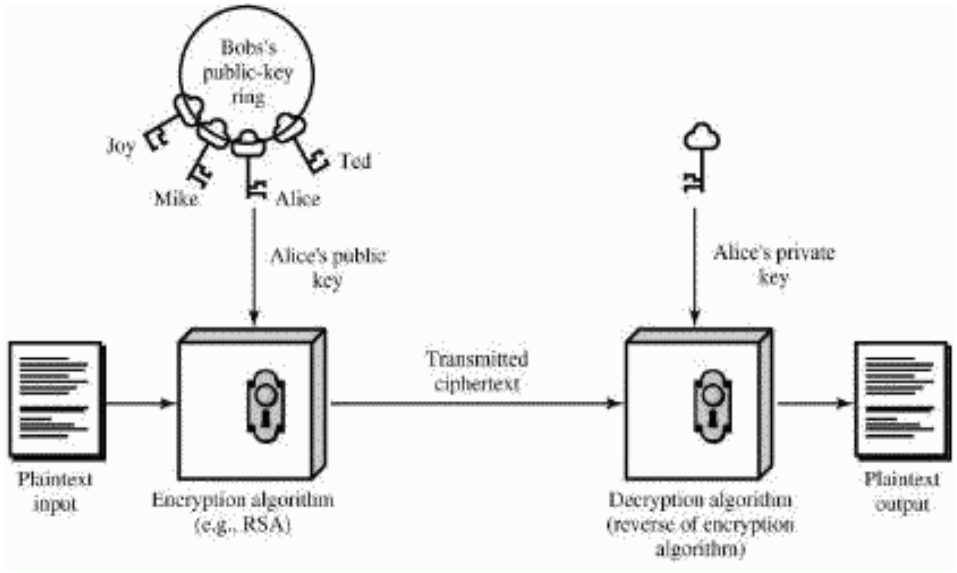
4.1.2 ΑΣΥΜΜΕΤΡΗ ΚΡΥΠΤΟΓΡΑΦΗΣΗ

Εξίσου σημαντική σπουδαιότητα με τα συμμετρικά κρυπτοσυστήματα έχει και η κρυπτογραφία δημοσίου κλειδιού (public key encryption) η οποία αξιοποιείται κατά την προτεραιότητα για αυθεντικοποίηση μηνυμάτων και διανομή δημοσίων κλειδιών.

Η κρυπτογράφηση δημοσίου κλειδιού (public key encryption) προτάθηκε το 19976 από τους W. Diffie και M. Hellman και υπήρξε ένα εξόχως σημαντικό βήμα στην περαιτέρω διάδοση της κρυπτογραφίας. Οι αλγόριθμοι κρυπτογραφίας δημοσίου κλειδιού βασίζονται σε μαθηματικές συναρτήσεις και όχι σε απλές πράξεις με bits. Επιπλέον, η κρυπτογραφία δημοσίου κλειδιού είναι ασύμμετρη (asymmetric) συμπεριλαμβάνοντας τη χρήση ξεχωριστών κλειδιών (key pair), σε αντίθεση με την συμμετρική που χρησιμοποιεί μόνον ένα κλειδί. Η χρήση δύο κλειδιών επιφέρει σημαντικές τροποποιήσεις σε θέματα που σχετίζονται με την εμπιστευτικότητα , την αυθεντικότητα και τη διανομή των κλειδιών.

Μια δομή δημοσίου κλειδιού αποτελείται από τις ίδιες συνιστώσες όπως και στην συμβατική κρυπτογραφία με τη διαφορά να είναι στο ζεύγος δημοσίου(public) και ιδιωτικού(private) κλειδιού. Ζεύγος κλειδιών που έχει επιλεγεί με τρόπον τέτοιο ώστε το δημόσιο

κλειδί του παραλήπτη να χρησιμοποιηθεί για την κρυπτογράφηση και το ιδιωτικό κλειδί του παραλήπτη για αποκρυπτογράφηση. Οι ακριβείς μετασχηματισμοί πραγματοποιούνται από τον αλγόριθμο κρυπτογράφησης/αποκρυπτογράφησης, εξαρτώμενοι από τις τιμές του δημοσίου και του ιδιωτικού κλειδιού που παρέχονται ως είσοδοι.



Όπως φαίνεται και στο παραπάνω σχήμα το δημόσιο κλειδί αποσκοπεί σε δημόσια χρήση ενώ το ιδιωτικό κλειδί το χρησιμοποιεί αποκλειστικά και μόνο ο κάτοχος του. Ένας γενικής χρήσης αλγόριθμος κρυπτογράφησης/αποκρυπτογράφησης βασίζεται σε ένα δημόσιο κλειδί για κρυπτογράφηση και σε ένα άλλο διαφορετικό αλλά μοναδικά συσχετιζόμενο κλειδί για αποκρυπτογράφηση. Τα βήματα που ακολουθεί αυτή η διαδικασία είναι

- Για κάθε χρήστη παράγεται ένα ζεύγος κλειδιών το οποίο θα χρησιμοποιηθεί για την κρυπτογράφηση και την αποκρυπτογράφηση των μηνυμάτων.
- Κάθε χρήστης αποθηκεύει ο δημόσιο κλειδί σε ένα χώρο ή σε αρχείο που είναι εύκολα προσβάσιμο. Το άλλο κλειδί το ιδιωτικό, αποθηκεύεται διατηρώντας τη μυστικότητα του. Για την λειτουργικότητα της επικοινωνίας απαιτείται κάθε χρήστης να είναι σε θέση να γνωρίζει τα δημόσια κλειδιά των άλλων.
- Έστω ότι ένας χρήστης Α θέλει να στείλει ένα μήνυμα στον χρήστη Β, τότε κρυπτογραφεί το μήνυμα με το δημόσιο κλειδί του Β, ο Β λαμβάνοντας το μήνυμα αποκρυπτογραφεί με το ιδιωτικό κλειδί του. Κανένας άλλος δε μπορεί να αποκρυπτογραφήσει το μήνυμα αφού μόνο ο Β γνωρίζει το ιδιωτικό κλειδί του. Με αυτό τον τρόπο διασφαλίζεται η ασφαλής επικοινωνία μεταξύ των δύο.

Βασική προϋπόθεση είναι ότι όλοι οι συμμετέχοντες να έχουν πρόσβαση στα δημόσια κλειδιά, ενώ τα ιδιωτικά να παράγονται τοπικά για τον κάθε συμμετέχοντα ώστε να διασφαλίζεται αυστηρά η μυστικότητα τους. Οποιαδήποτε στιγμή, ένας χρήστης μπορεί να τροποποιήσει το

ιδιωτικό του κλειδί και ταυτοχρόνως να δημοσιεύει το αντίστοιχο νέο δημόσιο κλειδί ώστε να αντικατασταθεί το προηγούμενο μη ισχύον πλέον κλειδί.

4.2 ΨΗΦΙΑΚΑ ΠΙΣΤΟΠΟΙΗΤΙΚΑ ΚΑΙ ΨΗΦΙΑΚΕΣ ΥΠΟΓΡΑΦΕΣ

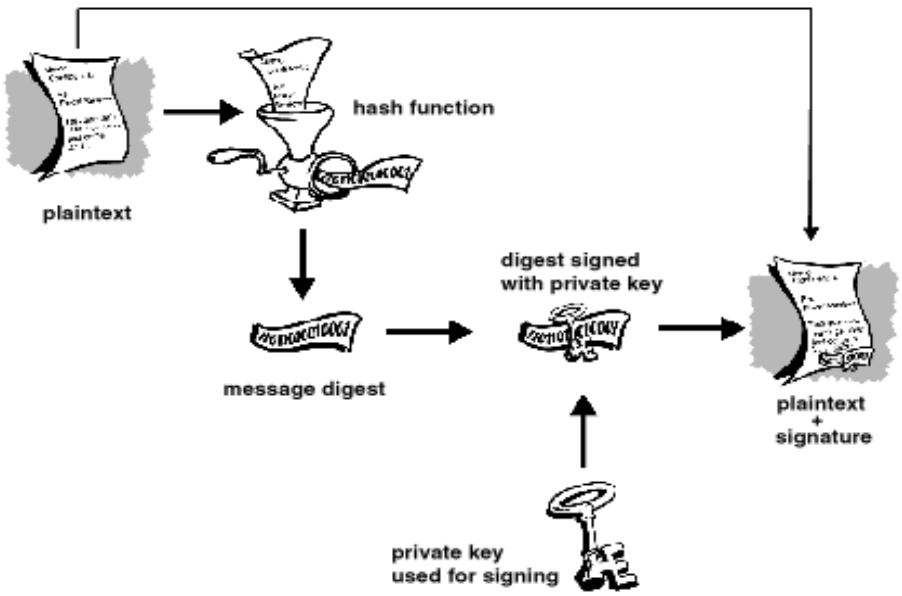
Εκτός από την κρυπτογράφηση[2] [5] υπάρχει η αναγκαιότητα της πιστοποίησης[13]. Πιστοποίηση είναι η διαδικασία η οποία μας εγγυάται πως τα δύο τερματικά που επικοινωνούν, είναι αυτά που ισχυρίζονται (βλ. κεφ. 3.2)

4.2.1 ΨΗΦΙΑΚΕΣ ΥΠΟΓΡΑΦΕΣ

Το 1976 ο Whitfield και ο Martin Hellman για πρώτη φορά παρουσίασαν την ιδέα των ψηφιακών υπογραφών. Αργότερα ο Ronald Rivest ,ο Adi Shamir και ο Len Adleman παρουσίασαν τον αλγόριθμο RSA ο οποίος χρησιμοποιήθηκε στις πρώτες ψηφιακές υπογραφές. Οι πρώτες ψηφιακές υπογραφές αποδείχθηκαν ότι δεν ήταν ασφαλείς. Το πρώτο ευρέος γνωστό στην αγορά λογισμικό που χρησιμοποίησε τέτοιες ψηφιακές υπογραφές ήταν το Lotus Notes 1.0 το οποίο κυκλοφόρησε το 1989

Η κρυπτογράφηση με ασύμμετρο τρόπο μπορεί να χρησιμοποιηθεί για την παραγωγή ψηφιακών υπογραφών. Έστω ότι δύο τερματικά θέλουν να επικοινωνήσουν αποστέλλοντας μηνύματα. Στις απαιτήσεις δεν περιλαμβάνεται πλέον η εμπιστευτικότητα του κειμένου , αλλά το τερματικό Α επιθυμεί να είναι σίγουρο για την προέλευση του κειμένου, δηλαδή απαιτεί αυθεντικοποίηση(authenticity) του αποστολέα του μηνύματος. Σε αυτή την περίπτωση το

τερματικό Β κρυπτογραφεί το μήνυμα με το ιδιωτικό του κλειδί. Όταν ο Α παραλάβει το κρυπτογραφημένο μήνυμα, το αποκρυπτογραφεί με το δημόσιο κλειδί του Β, εξασφαλίζοντας έτσι την ακεραιότητα του αρχικού μηνύματος. Κανένας άλλο δε γνωρίζει το ιδιωτικό κλειδί του Β συνεπώς κανένας άλλος δε μπορεί να δημιουργήσει κρυπτογραφημένο κείμενο το οποίο να αποκρυπτογραφείται με το δημόσιο κλειδί του Β. Έτσι, όλο το κρυπτογραφημένο κείμενο αποτελεί μια ψηφιακή υπογραφή(digital signature). Στην διαδικασία που αναλύθηκε υπάρχει ένα πρόβλημα που αφορά το χώρο αποθήκευσης. Κάθε μήνυμα πρέπει να είναι αποθηκευμένο σε μη κρυπτογραφημένη μορφή για πρακτικούς λόγους. Πρέπει επίσης να υπάρχει και αντίγραφο σε κρυπτογραφημένη μορφή, σε περίπτωση αμφισβήτησης ή διαφωνίας, να μπορούν εύκολα να προσδιοριστούν τα περιεχόμενα του μηνύματος. Η λύση στο παραπάνω πρόβλημα είναι να κρυπτογραφηθεί ένα μικρό τμήμα από bits, το οποίο θα αποτελεί συνάρτηση του κειμένου. Ένα τέτοιο μήνυμα ονομάζεται αυθεντικοποιητής (authenticator) και είναι αδύνατο να τροποποιηθεί το μήνυμα χωρίς να αλλάξει ο αυθεντικοποιητής.



Οι ψηφιακές υπογραφές είναι ένας άλλος τρόπος επαλήθευσης ότι τα δεδομένα δεν έχουν παραποιηθεί από κάποιον ενδιάμεσο και είναι το αρχικό μήνυμα που έχει σταλθεί από την πηγή. Σε αρκετές χώρες ανά τον κόσμο όπου τα διαδικτυακά εγκλήματα έχουν το ίδιο νομικό βάρος με τα υπόλοιπα, οι ψηφιακές υπογραφές έχουν νομική υπόσταση και θεωρούνται εξίσου αναγνωρίσιμες όσο και οι χειρόγραφες

4.2.2. ΨΗΦΙΑΚΑ ΠΙΣΤΟΠΟΙΗΤΙΚΑ

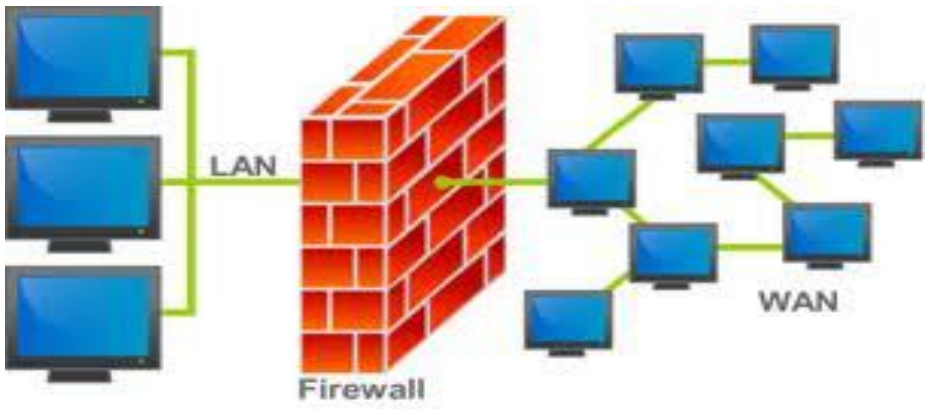
Για την αποτελεσματική λειτουργία της κρυπτογράφησης το δημόσιο κλειδί πρέπει να είναι γνωστό σε όσους ενδιαφέρονται. Εφόσον υπάρχει ένας ευρέος αποδεκτός αλγόριθμος κρυπτογράφησης και αποκρυπτογράφησης π.χ. RSA οποιοσδήποτε μπορεί να αποστείλει τι

δημόσιο κλειδί του σε κάποιον άλλο. Η μέθοδος αυτή παρουσιάζει αδυναμία διασφάλισης της ακεραιότητας και της αυθεντικοποίηση του αποστολέα κατά την αποστολή του μηνύματος που περιέχει το δημόσιο κλειδί. Λύση σε αυτό το πρόβλημα αποτελεί η χρήση ψηφιακού πιστοποιητικού (digital certificate) . Ένα πιστοποιητικό περιλαμβάνει το δημόσιο κλειδί του χρήστη και ένα κωδικό (user ID) του κατόχου του κλειδιού υπογεγραμμένα ψηφιακά από μια Έμπιστη Τρίτη Οντότητα (Thruster Third Party – TTP), η οποία συνήθως αποκαλείται Πάροχος Υπηρεσιών Πιστοποίησης(Certification Service Provider – CSP). Ο χρήστης παρουσιάζει το δημόσιο κλειδί του στον CSP με έναν αξιόπιστο τρόπο και λαμβάνει ένα πιστοποιητικό που το περιέχει ή στη γενική περίπτωση, ο CSP παράγει αποθηκεύει, διανέμει και ανακαλεί όταν απαιτείται τα πιστοποιητικά. Το πιο διαδομένο σύστημα πιστοποιητικού είναι το ISO/ITU-T X.509, το οποίο χρησιμοποιείται σε πολλές περιπτώσεις όπως στην ασφάλεια IP, στο TSL/SSL στο SET, στο S/MIME κλπ.

4.3 ΤΟΙΧΟΣ ΠΡΟΣΤΑΣΙΑΣ (FIREWALL)

Ένα τοίχος προστασίας είναι μία διάταξη εξειδικευμένων μηχανισμών ασφαλείας που ελέγχει την πρόσβαση και την μετακίνηση της πληροφορίας ενός δικτύου που εμπιστευόμαστε και ενός δικτύου που δεν εμπιστευόμαστε απαραίτητα.

Με τον όρο τοίχος προστασίας[2][3][5] (firewall) εννοούμε συστήματα ή ομάδες συστημάτων που υλοποιούν τους κανόνες μιας πολιτικής ασφάλειας μεταξύ δύο δικτύων. Τις περισσότερες φορές το ένα από τα δύο είναι το Internet αλλά πιο συχνά το τοίχος προστασίας μπορεί να τοποθετηθεί ανάμεσα και μεταξύ δύο τυχαίων δικτύων υπολογιστών. Ο ρόλος του firewall μπορεί να είναι τόσο η αποτροπή μη εξουσιοδοτημένων προσβάσεων σε μία ασφαλή περιοχή όσο και η αποτροπή μη εξουσιοδοτημένης εξόδου πληροφορίας από μία περιοχή. Μπορεί δηλαδή να λειτουργήσει ως θύρα ελέγχου της κίνησης και προς τις δύο κατευθύνσεις. Τέλος το τοίχος προστασίας αποτελεί την πρώτη γραμμή άμυνας του δικτύου απέναντι στους επίδοξους εισβολής αλλά σε καμία περίπτωση την μοναδική.



Οι βασικότερες λειτουργίες του firewall παρουσιάζονται παρακάτω

- Το τοίχος προστασίας αποτελεί το επίκεντρο των αποφάσεων που σχετίζονται με θέματα ασφάλειας.

  Το τοίχος προστασίας επιτρέπει στον διαχειριστή του δικτύου να ορίσει ένα κεντρικό σημείο ελέγχου (choke point) , το οποίο αποτρέπει την προσπέλαση μη εξουσιοδοτημένων χρηστών στις προστατευόμενες περιοχές.
- Το τοίχος προστασίας εφαρμόζει έλεγχο προσπέλασης (access control) από και προς το δίκτυο.

  Είναι ο λόγος που σχεδιάστηκε το τοίχος προστασίας στα τέλη της δεκαετίας του 1980 από τους μηχανικούς της D E C (Digital Equipment Corporation). Βασικός σκοπός ύπαρξης ενός firewall είναι η συγκέντρωση όσο το δυνατόν περισσότερης πληροφορίας για την ταυτότητα τόσο των πακέτων(packets) όσο και των συνόδων(sessions) που διέρχονται μέσα από το τοίχος προστασίας. Με βάση αυτή την πληροφόρηση και μία ήδη καθορισμένη πολιτική ασφάλειας η οποία περιγράφει ποια πακέτα και σε ποιες συνόδους επιτρέπεται η είσοδος ή η έξοδος το firewall αποφασίζει αν θα επιτρέψει ή θα αρνηθεί την είσοδο ή την έξοδο ενός πακέτου ή την έναρξη μιας συνεδρίας.
- Το προστασίας προσφέρει καταγραφή της δραστηριότητας στο δίκτυο

  Εφόσον όλη η κίνηση του δικτύου διέρχεται μέσα από το τοίχος προστασίας αυτό μπορεί να αποτελέσει ένα καλό σημείο για την συλλογή πληροφορίας σχετικά με τη χρήση τόσο των συστημάτων όσο και του δικτύου.
- Το τοίχος προστασίας έχει την δυνατότητα απόκρυψης των πραγματικών διευθύνσεων της επιχείρησης

  Το firewall έχει την δυνατότητα να ενσωματώνει το NAT (Network Address Translator) το οποίο μεταφράζει τις εσωτερικές διευθύνσεις σε πραγματικές και αντιμετωπίζει το

πρόβλημα της έλλειψης ή της αλλαγής διευθύνσεων στην περίπτωση που ένας οργανισμός αλλάξει παροχέα υπηρεσιών Internet

Το τοίχος προστασίας έχει και κάποιους περιορισμούς-αδυναμίες:

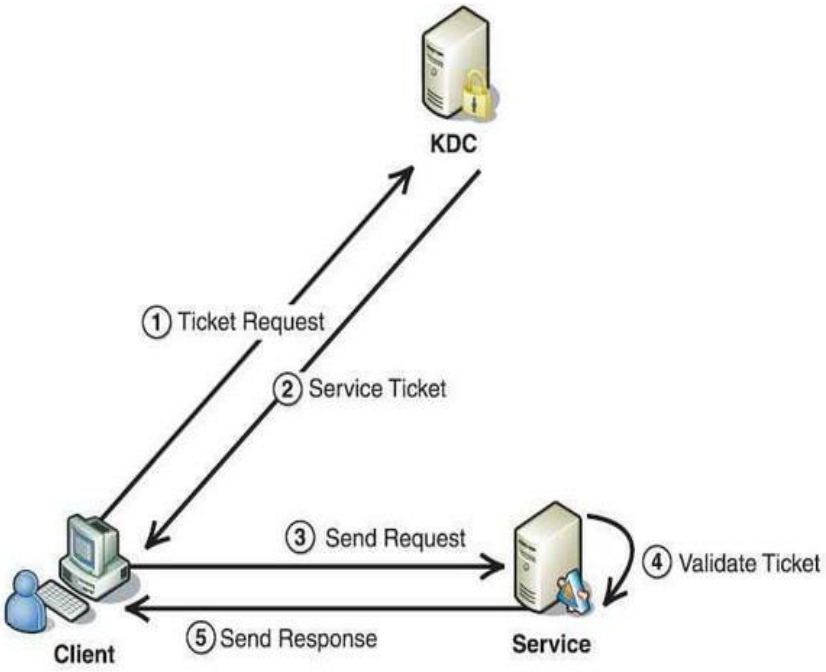
- Δε μπορεί να προστατέψει από συνδέσεις οι οποίες δε διέρχονται από αυτό.
- Δε μπορεί να προστατέψει από προγράμματα ιούς
- Δε μπορεί να προστατέψει απέναντι στις επιθέσεις κακόβουλων χρηστών από το εσωτερικό του δικτύου
- Δε μπορεί να προστατέψει το δίκτυο από απειλές αγνώστου τύπου

4.4 KERBEROS

Το κέρβερος[2] είναι μια διαδικασία ελέγχου ταυτότητας δικτύου και σύστημα πρόσβασης ελέγχου που έχει σχεδιαστεί να υποστηρίζει ασφαλή σύνδεση μέσα σε εχθρικά δίκτυα. Το κέρβερος αναπτύχθηκε στο MIT ως μέρος του έργου Athena και είχε αρχικά στόχο να χρησιμοποιηθεί από συστήματα Unix, αλλά από τότε έχει μεταφερθεί και σε άλλα περιβάλλοντα. Η Microsoft παρέχει μια έκδοση του κέρβερος σε δίκτυα των Windows. Ο κέρβερος προσφέρει μια μεθοδική διαδικασία διανομής των κλειδιών σε κύριους υπολογιστές οι οποίοι επικοινωνούν και επαληθεύουν τα πιστοποιητικά ενός πελάτη που ζητά να έχει πρόσβαση σε μια υπηρεσία.

Το σύστημα κέρβερος χρησιμοποιεί ένα διακομιστή που ονομάζεται Key Distribution Center (KDC) για να διαχειρίζεται την διαδικασία διανομής κλειδιών. Η διαδικασία πιστοποίησης του κέρβερος προκύπτει από μια σχέση τριών οντοτήτων:

- Ο πελάτης: Ένας υπολογιστής που ζητά πρόσβαση σε ένα διακομιστή
- Ο διακομιστής: Ένας υπολογιστής που προσφέρει υπηρεσίες στο δίκτυο
- ΤΟ KDC: Ένας υπολογιστής που έχει σχεδιαστεί να παρέχει κλειδιά για επικοινωνία τν δικτύων



Η διαδικασία πιστοποίησης του κέρβερος προϋποθέτει ότι το KDC έχει ήδη ένα κοινόχρηστο μυστικό κλειδί που μπορεί να χρησιμοποιήσει για να επικοινωνήσει με τον διακομιστή. Αυτά τα κλειδιά χρησιμοποιούνται για να κρυπτογραφηθεί ένα νέο κλειδί συνόδου το οποίο θα χρησιμοποιήσουν ο πελάτης και ο διακομιστής για να επικοινωνήσουν μεταξύ τους. Τα διάφορα κλειδιά που χρησιμοποιούνται από το KDC για κρυπτογράφηση των δεδομένων του πελάτη και του διακομιστή ονομάζονται μακροπρόθεσμα κλειδιά (long term keys).

Το κέρβερος χρησιμοποιεί συμβατική κρυπτογράφηση και όχι κρυπτογράφηση δημοσίου κλειδιού κατά την διαδικασία ελέγχου ταυτότητας και τα βήματα είναι τα εξής:

(1) Ο πελάτης θέλει να έχει πρόσβαση σε μια υπηρεσία του διακομιστή Α και στέλνει στο KDC μια αίτηση για πρόσβαση στην υπηρεσία του διακομιστή Α.

(2) Το KDC εκτελεί τα παρακάτω βήματα:

   a) Το KDC δημιουργεί ένα κλειδί συνόδου που θα χρησιμοποιηθεί για κρυπτογράφηση της επικοινωνίας μεταξύ του πελάτη και του διακομιστή Α

   b) Το KDC δημιουργεί ένα εισιτήριο συνόδου. Το εισιτήριο περιλαμβάνει ένα αντίγραφο του κλειδιού που δημιουργήθηκε στο βήμα 2α. Το εισιτήριο περιέχει επίσης πληροφορίες σφραγίδας χρόνου και πληροφορίες για τον πελάτη που ζητά πρόσβαση, όπως της ρυθμίσεις ασφάλειας του πελάτη.

c) Το KDC κρυπτογραφεί το εισιτήριο συνόδου χρησιμοποιώντας το μακροπρόθεσμο κλειδί του διακομιστή Α.

d) Το KDC περικλείει το κρυπτογραφημένο εισιτήριο συνόδου, ένα αντίγραφο του κλειδιού συνόδου και άλλες παραμέτρους απόκρισης για τον πελάτη και κρυπτογραφεί ολόκληρο το πακέτο χρησιμοποιώντας το κλειδί του πελάτη. Η απόκριση στέλνεται στον πελάτη.

(3) Ο πελάτης λαμβάνει την απόκριση από το KDC και την αποκρυπτογραφεί. Ο πελάτης παίρνει το απαραίτητο κλειδί συνόδου για την επικοινωνία με τον διακομιστή Α. Επίσης, συμπεριλαμβάνεται στο πακέτο το εισιτήριο συνόδου που κρυπτογραφείται με το μακροπρόθεσμο κλειδί του διακομιστή. Ο πελάτης δε μπορεί να διαβάσει το εισιτήριο συνόδου αλλά ξέρει ότι πρέπει να στείλει το εισιτήριο στο διακομιστή για να μπορεί να πιστοποιηθεί.

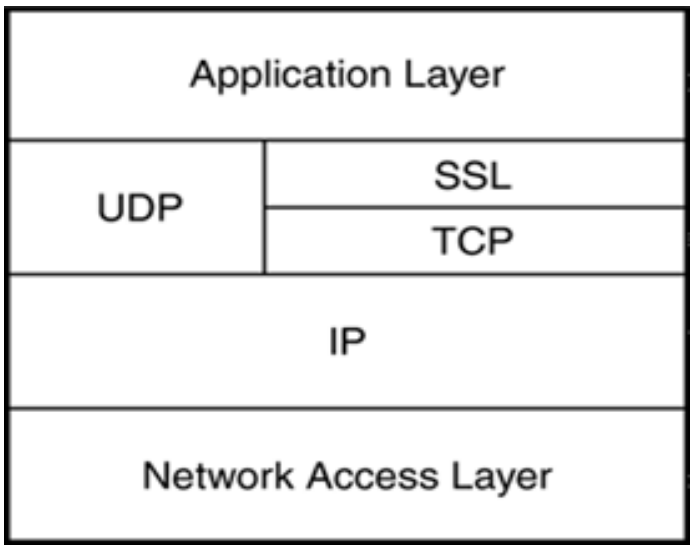
(4) Ο πελάτης στέλνει στο διακομιστή Α μια αίτηση πρόσβασης. Η αίτηση περιλαμβάνει το εισιτήριο συνόδου(κρυπτογραφημένο με το μακροπρόθεσμο κλειδί του διακομιστή) και τις πληροφορίες ελέγχου ταυτότητας(κρυπτογραφημένες με το κλειδί της συνόδου)

(5) Ο διακομιστής Α λαμβάνει την αίτηση και χρησιμοποιώντας το μακροπρόθεσμο κλειδί αποκρυπτογραφεί το εισιτήριο συνόδου. Ύστερα εξάγει το κλειδί από το εισιτήριο συνόδου και χρησιμοποιεί το κλειδί συνόδου για να αποκρυπτογραφήσει τις πληροφορίες ελέγχου ταυτότητας. Τέλος ο διακομιστής Α επαληθεύει ότι η πληροφορίες ελέγχου ταυτότητας ταιριάζουν με τις πληροφορίες που συμπεριλαμβάνονται στο εισιτήριο συνόδου.

(6) Ως προαιρετικό τελικό βήμα ο πελάτης μπορεί να επαληθεύσει τα πιστοποιητικά του διακομιστή Α αν θέλει.

4.5 SSL και TLS

Το SSL[2] (Secure Sockets Layer) δημιουργήθηκε από την εταιρεία Netscape για την ασφάλεια των διαδικτυακών επικοινωνιών, παρέχει κρυπτογράφηση ανάμεσα στο επίπεδο εφαρμογής και στο επίπεδο πρόσβασης δικτύου όπως φαίνεται και στην εικόνα παρακάτω.



TCP/IP με χρήση SSL

Το SSL χρησιμοποιεί μεθόδους κρυπτογράφησης των δεδομένων που ανταλλάσσονται μεταξύ δύο τερματικών εγκαθιδρύοντας μια ασφαλή σύνδεση μεταξύ του δικτύου. Χρησιμοποιεί ένα συνδυασμό ασύμμετρης και συμμετρικής κρυπτογράφησης. Η συμμετρική κρυπτογράφηση είναι σαφώς πιο γρήγορη και αποδοτική σε σχέση με την κρυπτογράφηση δημοσίου κλειδιού παρόλα αυτά η δεύτερη παρέχει καλύτερες τεχνικές πιστοποίησης. Η μετάδοση των πληροφοριών μέσω του διαδικτύου γίνεται χρησιμοποιώντας το πρωτόκολλο TCP/IP.Το SSL λειτουργεί πριν το TCP/IP και μετά τις εφαρμογές υψηλού επιπέδου, όπως είναι το HTTP (προβολή ιστοσελίδων), FTP (μεταφορά αρχείων), IMAP (email). Στην ουσία ο ρόλος του SSL είναι να τροφοδοτείτε με πληροφορίες από το υψηλό επίπεδο της στοίβας του TCP/IP , να τις κρυπτογραφεί και έπειτα να τις μεταδίδει προς το τερματικό στην απέναντι πλευρά που τις ζήτησε.

Ενώ λειτουργεί με το FTP, το http και το telnet συνήθως χρησιμοποιείται για την θωράκιση των Web servers, ιδιαίτερα στις ηλεκτρονικές οικονομικές συναλλαγές. Κάθε SSL σύνδεση ξεκινά πάντα με ανταλλαγή μηνυμάτων από τον εξυπηρετητή και τον πελάτη έως ότου επιτευχθεί η ασφαλή σύνδεση που ονομάζεται χειραψία handshake. Το SSL αποτελείται ακόμα από μία ομάδα πρωτοκόλλων που εκτελούν συγκεκριμένες υπηρεσίες. Τα πρωτόκολλα αυτά είναι SSL Handshake Protocol που χρησιμοποιείται για πρόσβαση στο TCP, SSL Change Cipher Spec Protocol το οποίο υπολογίζει αλλαγές σε ρυθμίσεις κρυπτογράφησης και SSL Alert Protocol που στέλνει ειδοποιήσεις.

Το TLS (Transport Layer Security) είναι πλέον ο διάδοχος του SSL 3.0 και αποτελείται από το TLS Record Protocol και το Handshake Protocol.

4.6 HONEYPOTS

4.6.1 ΤΙ ΕΙΝΑΙ

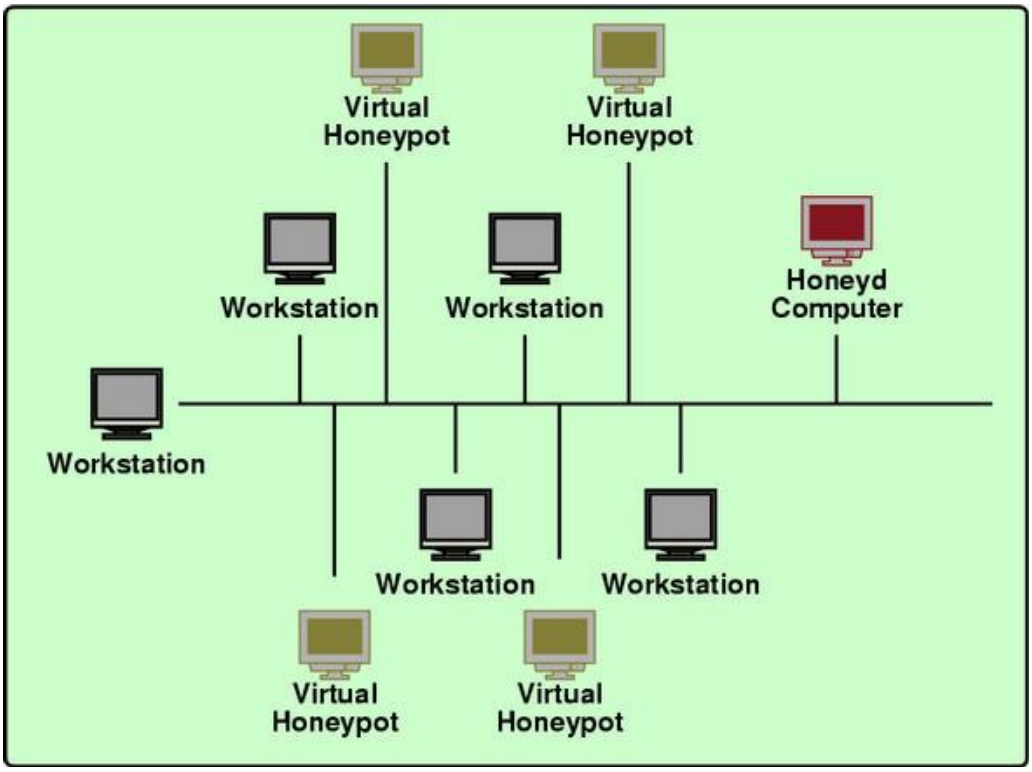
Τα honey pots[4] [6][3] που αποκλίνει από την παραδοσιακή φιλοσοφία περί ασφάλειας. Αυτό το σύστημα δεν προσπαθεί να τους επιτιθέμενους μακριά αλλά να τους έλκει. Η ιδιαίτερη αξία ενός honey pot δεν έγκειται στο ότι είναι απόρθητο, αλλά στο ότι θα δεχτεί επιθέσεις και κατά πάσα πιθανότητα δεν θα αντέξει. Τα honey pots αποτελούν από τη φύση τους τρωτά (vulnerable) συστήματα και η κύρια αποστολή τους είναι να παραβιαστούν. Κατά αυτόν τον τρόπο μπορούμε να συγκεντρώσουμε αρκετές πληροφορίες. Μπορούμε να πληροφορηθούμε για τα είδη των επιθέσεων που χρησιμοποιεί κάποιος , για τις προθέσεις του, αλλά και για τους

υπόλοιπους στόχους του, τους οποίους ενδέχεται να χτυπήσει μέσα από το δικό μας μηχάνημα. Με λίγα λόγια αποτελούν δικτυακές παγίδες στις οποίες εγκλωβίζονται οι επιτιθέμενοι και από θύτες γίνονται θύματα.

Τα honey pots υλοποιούνται συνήθως σε εικονικές μηχανές (virtual machines), ώστε να είναι όσο το δυνατό πιο εύκολη η διαχείριση τους. Αυτές οι εικονικές μηχανές χρησιμοποιούν ειδικό λογισμικό και κατάλληλες ρυθμίσεις ώστε να μοιάζουν με κάποιο φυσικό σύστημα που θα είχαμε στο δίκτυο μας. Τα Honey Pots καταγράφουν αναλυτικά όλες τις επιθέσεις εναντίον τους. Για παράδειγμα, αποθηκεύουν την διεύθυνση IP του attacker, τα ονόματα χρήστη και τους κωδικούς που χρησιμοποιεί, το είδος και την έκβαση της επίθεσης, τις εντολές που πληκτρολόγησε , τα αρχεία που τροποποίησε κ.ο.κ.

4.6.2ΤΡΟΠΟΣ ΛΕΙΤΟΥΡΓΙΑΣ

Η δυνατότητα των honey pots να προσομοιώνουν διάφορα είδη συστημάτων οφείλεται στη χρήση των λεγόμενων fingerprints. Αυτά τα αποτυπώματα αποτελούν κατά κάποιο τρόπο τα μοναδικά στοιχεία ταυτοποίησης που αφήνει κάθε λειτουργικό σύστημα. Η δικτύωση ενός υπολογιστή γίνεται δυνατή με τη χρήση της σουίτας πρωτοκόλλων TCP/IP. Ορισμένες παράμετροι του TCP/IP είναι μεταβλητές και ρυθμίζονται από το εκάστοτε λειτουργικό σύστημα. Με την παραπάνω διαδικασία μπορούμε να διακρίνουμε διαφορετικά λειτουργικά συστήματα όπως και διαφορετικές εκδόσεις του ίδιου λειτουργικού συστήματος από τις τιμές που χρησιμοποιούνται για τις συγκεκριμένες παραμέτρους του TCP/IP. Όλες αυτές οι παράμετροι μαζί φτιάχνουν μια υπογραφή των 67 bit ή αλλιώς το λεγόμενο από τύπωμα του συγκεκριμένου λειτουργικού συστήματος. Το nmap που αναλύεται πιο κάτω , αναγνωρίζει τα διάφορα fingerprints και με την παράμετρο -O μπορεί να μας ενημερώνει για το λειτουργικό σύστημα του στόχου. Καθώς οι τιμές των διαφόρων από αποτυπωμάτων είναι γνωστές τα honey pots τις χρησιμοποιούν για να υποδυθούν διάφορα λειτουργικά συστήματα αλλά και για να εξομοιώσουν διάφορες δικτυακές υπηρεσίες.



παράδειγμα δικτύου με honeypot

4.6.3 ΔΙΑΚΡΙΣΕΙΣ ΚΑΙ ΕΠΙΠΕΔΑ ΑΛΛΗΠΙΔΡΑΣΗΣ

Τα honey pots μπορούν να χωριστούν σε δύο κατηγορίες σύμφωνα με το σκοπό που εξυπηρετούν: τα honey pots παραγωγής και τα ερευνητικά honey pots.

Τα ερευνητικά honey pots είναι συστήματα με πρωταρχική αποστολή την καταγραφή όσο το δυνατόν περισσότερων πληροφοριών, ώστε να αυξάνεται η γνώση γύρω από τον τρόπο δράσης των επιτιθέμενων. Τα συγκεκριμένα honey pots προσομοιώνουν τις πιο διαδεδομένες υπηρεσίες, ώστε να είναι δελεαστικά και σχετικά προσιτά. Συνήθως υλοποιούνται σε ερευνητικά κέντρα, όπως πανεπιστήμια, κυβερνητικές ή στρατιωτικές υπηρεσίες και οργανισμούς οι οποιοι δραστηριοποιούνται στο χώρο της ασφάλειας. Η συγκεκριμένη κατηγορία δεν έχει άμεση σχέση με την ασφάλεια του ιδιοκτήτη τους αλλά βοηθάνε στην ενημέρωση και στην επαγρύπνηση των ειδικών στην ασφάλεια.

Τα honey pots παραγωγής δεν στοχεύουν στη γενικότερη απόκτηση γνώσης. Αυτά έχουν ως κύρια αποστολή την προστασία του ιδιοκτήτη τους. Τοποθετούνται συνήθως στο τοπικό δίκτυο μιας εταιρείας ή ενός οργανισμού και όπως όλα τα honey pots προσπαθούν να τραβήξουν την προσοχή των επιτιθέμενων. Από τις πληροφορίες που συγκεντρώνουν οι διαχειριστές μπορούν να πληροφορηθούν για τυχόν αδυναμίες που υπάρχουν στα κανονικά τους συστήματα όπως επίσης και για τις τεχνικές που αναπτύσσουν οι επιτιθέμενοι έναντι των συστημάτων της εταιρίας.

Πέρα από το διαχωρισμό με βάση την αποστολή, τα honey pots χωρίζονται και ως προς το επίπεδο αλληλεπίδρασης που επιτρέπουν στον εισβολέα να αναπτύξει μαζί τους. Τα επίπεδα αυτής αλληλεπίδρασης είναι τρία : Χαμηλό , μέτριο και υψηλό. Με βάση αυτό το κριτήριο τα honey pots χωρίζονται σε τρεις ομάδες. Αυτός ο διαχωρισμός παρουσιάζει το μεγαλύτερο ενδιαφέρον, εφόσον η αξία ενός honey pot τελικά σχετίζεται με το τι μπορεί να κάνει πάνω του ο επιτιθέμενος.

- *Χαμηλής αλληλεπίδρασης*: Αυτά τα honey pots προσομοιώνουν υπηρεσίες που δεν μπορούν να χρησιμοποιηθούν από τον εισβολέα ώστε να αποκτήσει πλήρη πρόσβαση στο ίδιο το honey pot. Αποτελούν δηλαδή πλήρως ελεγχόμενα περιβάλλοντα στα οποία ο επιτιθέμενος δεν θα αποκτήσει ποτέ πλήρη πρόσβαση. Σε ένα τέτοιο Honeypot δεν υπάρχει πραγματικό λειτουργικό σύστημα με το οποίο αλληλεπιδρά ο εισβολέας. Το γεγονός αυτό διευκολύνει τη γρήγορη και ασφαλή ανάπτυξη πολλών Honey pots σε ένα τοπικό δίκτυο. Συνήθως χρησιμοποιούνται για καταγραφή αυτοματοποιημένων επιθέσεων ή της δράσης διαφόρων Internet Worms.
- *Μεσαίας αλληλεπίδρασης*: Τα Honey pots αυτής της κατηγορίας είναι πιο αναπτυγμένα από τα προηγούμενα. Όπως κι εκείνα της χαμηλής αλληλεπίδρασης δεν τρέχουν κάποιο πραγματικό λειτουργικό. Ωστόσο παρέχουν περισσότερες υπηρεσίες, προσφέροντας περισσότερους στόχους στον επιτιθέμενο ενώ εκτελούν και πολλά scripts τα οποία εξομοιώνουν ένα ολόκληρο λειτουργικό σύστημα.
- *Υψηλής αλληλεπίδρασης*: Πρόκειται για τα πιο αναπτυγμένα honey pots. Αποτελούν αρκετά πολύπλοκα συστήματα τα οποία σχεδιάζονται με μεγάλη προσοχή και δεν έχουν καμία σχέση με εκείνα των προηγούμενων ομάδων. Αυτά τα Honey Pots δεν τρέχουν κάποια scripts που εξομοιώνουν τη συμπεριφορά ενός λειτουργικού ή κάποιον υπηρεσιών αλλά ένα κανονικό λειτουργικό. Συγκεκριμένα εκτελούν ένα επιτηδευμένα τρωτό σύστημα. Έτσι αν τα καταφέρει ο επιτιθέμενος μπορεί να το καταλάβει ολοκληρωτικά.

5. ΕΡΓΑΛΕΙΑ ΔΙΚΤΥΑΚΗΣ ΑΝΑΛΥΣΗΣ ΚΑΙ ΠΛΑΦΤΟΡΜΕΣ ΠΟΛΙΟΡΚΙΑΣ

5.1 NMAP

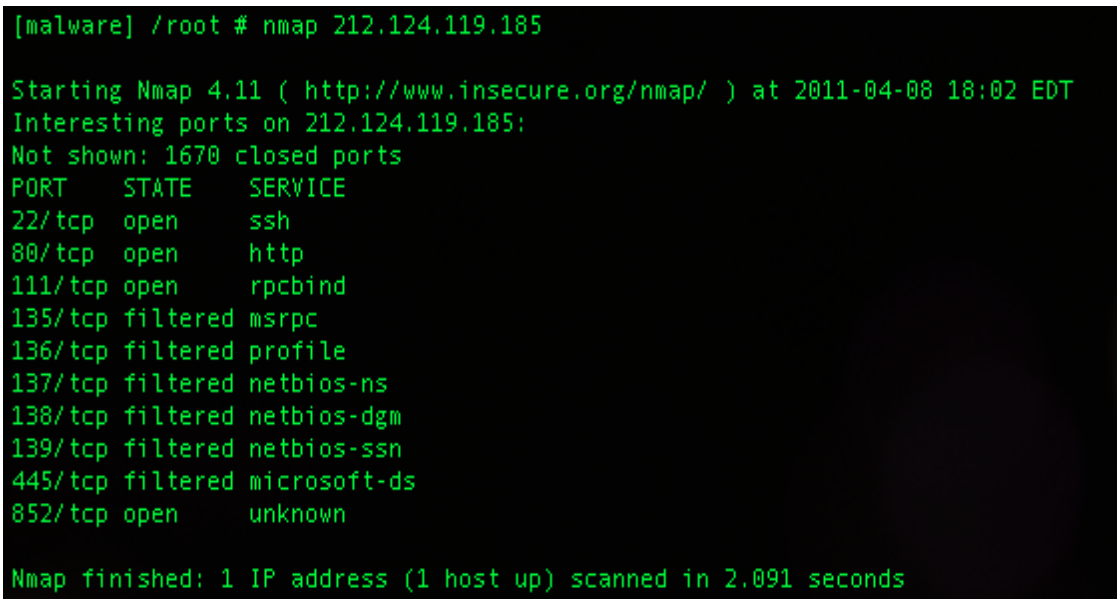
Το Σεπτέμβριο του 1997 το περιοδικό phrack[14] δημοσιεύει το NMAP[15] μαζί με τον πηγαίο κώδικα του. Είναι ένα λογισμικό το οποίο έγραψε ο Gordon Lyon Fyodor και εξελίσσεται μέχρι και σήμερα. Ένας αρχάριος χρήστης θα μπερδευτεί αρκετές φορές στην αρχή αλλά όταν αποκτήσει εξοικείωση με το Nmap τότε θα καταλάβει το πόσο ισχυρό είναι και τι δυνατότητες προσφέρει. Το Network Maper στην ουσία είναι ένα λογισμικό με το οποίο μπορείς να χαρτογραφήσεις ένα δίκτυο. Αποτελεί την πρώτη δουλειά που θα κάνει ένας hacker ώστε να συλλέξει πληροφορίες. Το NMAP προσφέρει στον επιτιθέμενο τη δυνατότητα να εξερευνήσει ένα δίκτυο και να βρει, ανακαλύψει απομακρυσμένους υπολογιστές αλλά και τις υπηρεσίες που μπορεί να τρέχουν σε ένα δίκτυο υπολογιστών. Καταφέρνει έτσι να έχει μια πλήρη εικόνα(χάρτη) του τι επικρατεί στο δίκτυο. Μπορεί ακόμα να δει λεπτομέρειες εκτός από τις θύρες που χρησιμοποιούνται και για άλλα στοιχεία των απομακρυσμένων υπολογιστών όπως τα λειτουργικά συστήματα τους, τον τύπο συσκευών, το uptime αλλά και τον αριθμό έκδοσης του προϊόντος. Ακόμα μπορεί να προσδιορίσει τις τεχνικές του Firewall και τον προμηθευτεί της κάρτας δικτύου. Το NMAP είναι συμβατό με όλα τα λειτουργικά συστήματα όπως Linux, Mac OS X και Windows και το πιο σημαντικό είναι ότι διανέμεται δωρεάν καθώς είναι μια εφαρμογή ανοιχτού κώδικα. Παρόλο που δεν παρέχει καμία πιστοποίηση το Nmap έχει από πίσω του μια κοινότητα από προγραμματιστές και χρήστες που βοηθάνε στην εξέλιξη του αλλά και στην λύση απρόσμενων προβλημάτων. Τέλος το Nmap έχει διακριθεί ως Προϊόν ασφάλειας πληροφοριών της χρονιάς από το Linux Journal ,το info world και το Code talker Digest.

Το Nmap κάνει χρήση εντολών προκειμένου να κάνει ανίχνευση στο απομακρυσμένο δίκτυο. Κάθε εντολή είναι της μορφής nmap [<scan type> …] [<options>]{target specifications>}. Στην έξοδο του δίνει μία λίστα από στόχους με συμπληρωματικές πληροφορίες σύμφωνα πάντα με τις παραμέτρους που του έχουμε δώσει. Στις πληροφορίες που δίνει το nmap περιλαμβάνονται ο αριθμός της θύρας και του πρωτοκόλλου , η ονομασία της υπηρεσίας αλλά και η κατάσταση στην οποία βρίσκεται. Η κατάσταση μπορεί να είναι ανοιχτή(open) που σημαίνει ότι μια αίτηση για

το μηχάνημα ακούει σε συνδέσεις ή πακέτα για αυτή τη θύρα. Μπορεί να είναι φιλτραρισμένοι(filtered) που σημαίνει ότι ένα τοίχος προστασίας εμποδίζει το nmap να πει αν είναι ανοιχτεί, μπορεί να είναι κλειστή(closed) , σε αυτή την περίπτωση σε απαντούν σε καμία αίτηση παρόλο που θα μπορούσαν να ανοίξουν οποιαδήποτε στιγμή. Τέλος μπορεί ναι είναι μη φιλτραρισμένοι (unfiltered) που σε αυτή την περίπτωση το nmap δε μπορεί να σαρώσει τη θύρα και δε μπορεί να προσδιορίσει αν είναι ανοιχτή ή κλειστή.

Οι πιο βασικές τεχνικές ανίχνευσης[16] του Nmap είναι :

- **TCP SYN scan (-sS)** : Χρησιμοποιεί απλές μεθόδους αναγνωρίσεις θυρών που δίνουν την δυνατότητα στο πρόγραμμα να συγκεντρώνει με ευκολία πληροφορίες για τις ανοιχτές θύρες, τις κλειστές ή τις φιλτραρισμένες θύρες χωρίς να ολοκληρώνει τη διαδικασία της TCP χειραψίας. Όταν βρεθεί μια ανοιχτή θύρα η διαδικασία της TCP χειραψίας μηδενίζεται με RST frame πριν αυτή ολοκληρωθεί. Αυτή η τεχνική αναφέρεται ως half open σάρωση.
- **Stealth scanning –FIN scan (-sF), Xmas Tree Scan (-sX), Null Scan (-sN):** Οι παραπάνω τεχνικές ταξινομούνται στις κρυφές σαρώσεις διότι στέλνουν ένα μοναδικό και απλοποιημένο TCP σε μια θύρα χωρίς οποιαδήποτε διαδικασία TCP χειραψίας πριν, ή άλλες επιπρόσθετες μεταφορές πακέτων περιμένοντας τελικά ανταπόκριση. Οι σαρώσεις αυτές λειτουργούν με την επεξεργασία των bit της TCP επικεφαλίδας έτσι ώστε να προκαλούν μια ανταπόκριση από την απομακρυσμένη συσκευή.
- **ACK Scan (-sA)**: Παρέχει πληροφορίες για την ύπαρξη κάποιου τοίχους προστασίας ή φίλτρων στην απέναντι πλευρά και ποτέ δεν εγκαθιδρύει μια σύνδεση με το στόχο.



Αποτελέσματα Scann 1

5.2 METASPLOIT

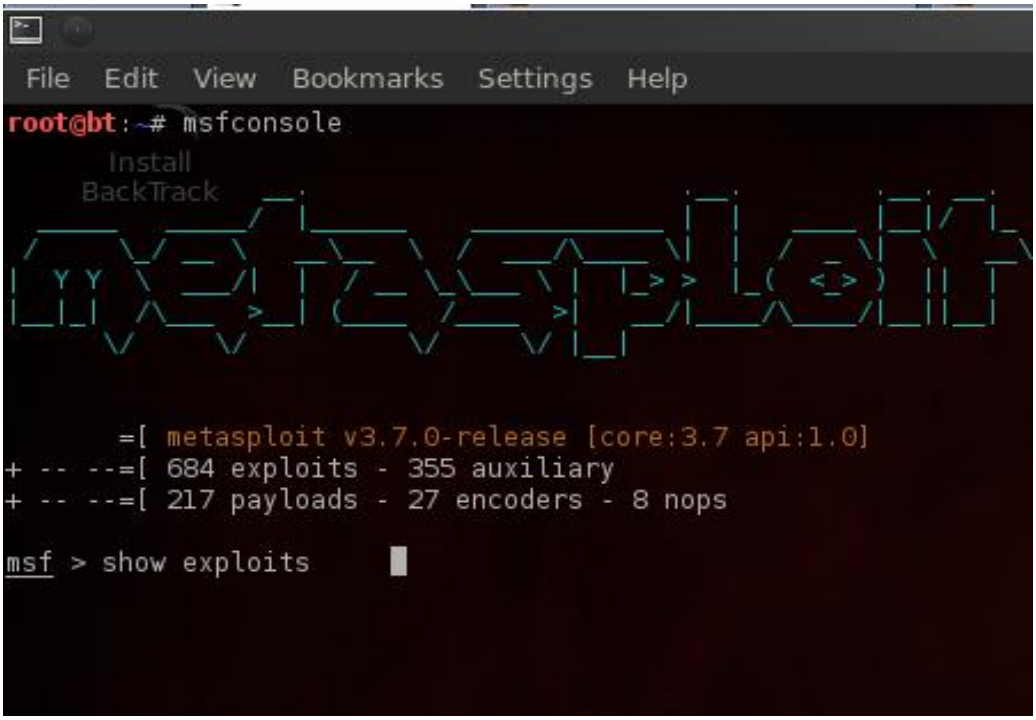
Ο πρωτεργάτης του Metasploit[7] είναι ο HD Moore. Όταν ο Moore εργαζόταν ως αναλυτής σε εταιρία ασφαλείας, στις ευθύνες του ήταν η αξιολόγηση κώδικα για exploits που κυκλοφορούσαν την περίοδο εκείνη. Κάποια στιγμή άρχισε να εργάζεται πάνω σε μια πλατφόρμα για τη δημιουργία κι ανάπτυξη exploits. Το 2003 έδωσε στο ευρύ κοινό την πρώτη έκδοση του Metasploit, το οποίο ήταν γραμμένο στη γλώσσα προγραμματισμού Perl και περιελάμβανε μόλις 11 exploits. Το 2004 κυκλοφόρησε η έκδοση 2.0 του Metasploit με 19 exploits και 27 τουλάχιστον Payloads. Σήμερα το Metasploit περιλαμβάνει πάνω από 1041 exploits και περισσότερα από 274 payloads.

Στα πλαίσια της πλατφόρμας του Metasploit Framework πρέπει να κατανοηθούν οι παρακάτω όροι.

- *Exploit:* Λάθη ή αλλιώς ευπάθειες σε λειτουργικά συστήματα, υπηρεσίες και εφαρμογές. Στόχος του είναι να βρει όσα περισσότερα μπορεί και μετά να τα εκμεταλλευτεί κατάλληλα προκειμένου να υποχρεώσει το λογισμικό σε συμπεριφορές που ο αρχικός δημιουργός δεν είχε φανταστεί. Με άλλα λόγια ο

εισβολέας αναζητά διαρκώς τα λεγόμενα exploits ώστε να τα εκμεταλλευτεί για δικούς του σκοπούς.

- *Payload:* Ο κώδικας που επιχειρεί ο επιτιθέμενος να εκτελέσει στο μηχάνημα στόχο, αφού έχει βρει ένα ή περισσότερα exploits, είναι αυτό που στα πλαίσια του metasploit framework ονομάζεται payload.
- *Module:* Η δύναμη του metasploit framework έγκειται στη χρήση μικρών, αυτόνομων οντοτήτων λογισμικού, τα λεγόμενα modules.
- *Listener:* Πρόκειται για μια λειτουργία του metasploit που χειρίζεται τις συνδέσεις από τα μηχανήματα-στόχους. Σε κάποιο εξ αυτών ο επιτιθέμενος ενδέχεται να έχει στείλει ένα Payload, το οποίο όταν εκτελεστεί, θα επιχειρήσει να συνδεθεί με τον υπολογιστή του επιτιθέμενου.



Από τη στιγμή που έχει εντοπιστεί μια ευπάθεια σε ένα σύστημα και ο επιτιθέμενος την έχει εκμεταλλευτεί επιτυχώς, περνάει τότε στη φάση του λεγόμενου post exploitation. Πλέον αυτό που τον απασχολεί δεν είναι το πώς θα αποκτήσει πρόσβαση, αλλά το τι θα κάνει τώρα που την έχει. Χάρη στον Meterpreter ο επιτιθέμενος αποκτά ένα ευέλικτο command shell στο μηχάνημα στόχο και μπορεί πλέον να το εκμεταλλευτεί περαιτέρω, να καλύψει τα ίχνη του ή να το εφαρμόσει σε άλλους υπολογιστές. Οι δυνατότητες που έχει ο εισβολέας από τον Meterpreter είναι:

- Αναβάθμιση δικαιωμάτων
- Λήψη των users hashes από την SAM database των windows
- Ηχογράφηση από το μικρόφωνο του συστήματος
- Φωτογράφηση του περιβάλλοντα χώρου από την web κάμερα
- Καταγραφή της πληκτρολόγησης του θύματος (keystroke logging)
- Καθαρισμός του event log(κάλυψη ιχνών)
- Απομακρυσμένη εκτέλεση εντολών
- Εντοπισμός όλων των ενεργών διεργασιών και προγραμμάτων
- Τερματισμός διεργασιών
- Λήψη και αντιγραφή αρχείων
- Επισκόπηση των ενεργών δικτυακών συνδέσεων του στόχου
- Επισκόπηση και μεταβολή του routing table

Όλα τα παραπάνω γίνονται μέσα από κάποιο περιβάλλον χρήσης που προσφέρει το Metasploit framework. Μερικά από αυτά είναι:

- *Msfconsole:* πρόκειται για ένα περιβάλλον γραμμής εντολών μέσα από το οποίο εργαζόμαστε με το Framework. Βρίσκουμε exploits, επιλέγουμε payloads, σηκώνουμε Listeners, σκανάρουμε το δίκτυο, εξαπολύουμε μαζικές επιθέσεις. Όταν κάποιος προσπαθεί να μάθει το Metasploit στην ουσία προσπαθεί να μάθει το Msfconsole
- *Msfcli:* Χρησιμοποιείται από τη γραμμή εντολών του εκάστοτε λειτουργικού συστήματος, κάτω από το οποίο τρέχει το Metasploit. Με το Msfcli μπορούμε να κάνουμε δουλείες που θα κάναμε και μέσα από το Msfconsole αλλά όχι διαδραστικά. Το εργαλείο είναι κατάλληλο για scripting, ενώ είναι ότι πρέπει για όταν ξέρουμε ακριβώς ποιο exploit module θέλουμε να χρησιμοποιήσουμε για ένα στόχο.
- *Armitage:* Είναι εντυπωσιακό για κάποιον που τώρα άρχισε να ασχολείται με το Penetration Testing αλλά είναι και παραπλανητικό για μπορεί να οδηγήσει σε λανθασμένα συμπεράσματα.

Άλλα χρήσιμα εργαλεία είναι το msfpayload και το msfencode

6.ΕΡΩΤΗΜΑΤΟΛΟΓΙΟ

Το ερωτηματολόγιο που έφτιαξα ήθελα να μου δώσει μια συνολική εικόνα για το πόσο οι χρήστες είναι ενημερωμένοι σχετικά με την ασφάλεια και τις ευπάθειες που κρύβουν τα δίκτυα πόσο η ενημερώσει παίζει ρόλο με την ηλικία , το μορφωτικό επίπεδο και γενικότερα με την ενασχόληση τους. Για τους παραπάνω λόγους έχει χωριστεί σε τρία μέρη όπου το πρώτο είναι γενικά δημογραφικά στοιχεία, το δεύτερο ερωτήσεις για ευπάθειες πρωτοκόλλων αλλά και για τεχνικές εισβολείς σε δίκτυα και τέλος στο τρίτο μέρος αν γνωρίζουν τρόπους προστασίας και αν χρησιμοποιούν. Το έχω δημοσιεύει στα εσωτερικά του forum της συμμαχίας μου στο www.grepolis.gr για να εξασφαλίσω την εγκυρότητα του.

ΜΕΡΟΣ 1^{ο} Δημογραφικά στοιχεία

1.Φύλλο

- Άνδρας-
- Γυναίκα

2. Ηλικία

- 1-10
- 11-18
- 19-25
- 26-35
- 35-50
- 50+

3- Εκπαίδευση

- Απόφοιτος γυμνασίου
- Απόφοιτος λυκείου
- Απόφοιτος- Σπουδαστής Α.Ε.Ι
- Απόφοιτος- Σπουδαστής Τ.Ε.Ι
- Μεταπτυχιακές σπουδές

4-Επάγγελμα

- Δημόσιος υπάλληλος
- Ιδιωτικός υπάλληλος
- Ελεύθερος επαγγελματίας
- Άνεργος
- Οικιακά
- Φοιτητής
- Άλλο

5-Πόσο χρόνια χρησιμοποιείτε το διαδίκτυο?

- 1
- 2-3
- 4-5
- 6+

6-Πόσο συχνά χρησιμοποιείτε το διαδίκτυο?

- Καθημερινά
- 1-3 φορές την βδομάδα
- 4-6 φορές την βδομάδα

7- Από ποιο μέρος χρησιμοποιείτε/συνδέεστε συχνότερα?

- Σπίτι
- Δουλεία
- Δημόσια δίκτυα
- Όλα τα παραπάνω

8-Για πιο λόγο χρησιμοποιείτε το διαδίκτυο?

- Ενημέρωση
- Διασκέδαση
- Παιχνίδια
- Όλα τα παραπάνω

9- Πόσο ασφαλής αισθάνεστε στο διαδίκτυο?

- Καθόλου
- Λίγο
- Αρκετά
- Πολύ

10-Εμπιστεύεστε τους ιστότοπους /δίκτυα που συνδέεστε?

- Ναι
- Όχι

11-Πόσο συχνά δίνετε προσωπικά σας δεδομένα?

- Ποτέ
- Σπάνια
- Πάντα

ΜΕΡΟΣ 2ο Τεχνικές εισβολείς και ευπάθειες

12-Για τις τεχνικές εισβολής σε δίκτυα που χρησιμοποιούν ευπάθειες πρωτοκόλλων γνωρίζετε?

- Ναι
- Όχι
- Έχω ακούσει

13-Έχετε πέσει ποτέ θύμα δικτυακών επιθέσεων?

- Ναι
- Όχι
- Δεν έχω καταλάβει κάτι

14-Τι γνώμη έχετε για τους εισβολής δικτύων

- Άσχημη
- Μέτρια
- Καλή
- Τους είδα στις ειδήσεις των 8 και ξετρελάθηκα

15- Πιστεύετε ότι πρέπει να τιμωρούνται πάντα οι επιτιθέμενοι σε ένα δίκτυο?

- Ναι
- Όχι
- Ανάλογα γιατί το κάνουν

Οι παρακάτω ερωτήσεις αναφέρονται σε όρους, σημειώστε πιο είναι το πρώτο πράγμα που σας έρχεται στο μυαλό

16- Man in the middle?

- Τίποτα
- Το γνωστό τραγούδι Black Country Communion- Man In The Middle
- Παραπλάνηση μηχανημάτων σε ένα δίκτυο

17-Smurf attack?

- Ταινία που τα στρουμφάκια παίρνουν εκδίκηση
- Τεχνική αποστολής πακέτων
- Τίποτα από τα παραπάνω

18-Teardrop

- Αποστολή κακοσχηματισμένων πακέτων
- Το τραγούδι από Massive Attack
- Κανένα από τα δύο

19-Ping of death

- Δε το γνωρίζω
- Τεχνική που μπορεί να χρησιμοποιήσει ο καθένας από το command window του υπολογιστή του.

20- Packet Sniffing

- Υποκλοπή πακέτων
- Δε το γνωρίζω

ΜΕΡΟΣ 3ο Τρόποι προστασίας

21-Χρησιμοποιείτε κάποιο antivirus ?

- Ναι
- Όχι

22- Χρησιμοποιείτε τις προκαθορισμένες ρυθμίσεις?(Αν απαντήσατε ναι στην προηγούμενη ερώτηση ,πρέπει να απαντήσετε και εδώ, αν όχι συνεχίστε με την επόμενη)

- Ναι
- Όχι

23-Κρυπρογράφηση

- Χρησιμοποιώ σε όλες τις συναλλαγές, συνομιλίες μέσα σε ένα δίκτυο
- Χρονοβόρα διαδικασία
- Κανένα από τα παραπάνω

23- Πιστοποίηση, ψηφιακές υπογραφές

- Πάντα κοιτάω, χρησιμοποιώ στα πακέτα που ανταλλάζω
- Δε γνωρίζω

24- SSL

- Τι είναι αυτό?
- Ασφάλεια στην διαδικτυακή επικοινωνία

25-Honeypot

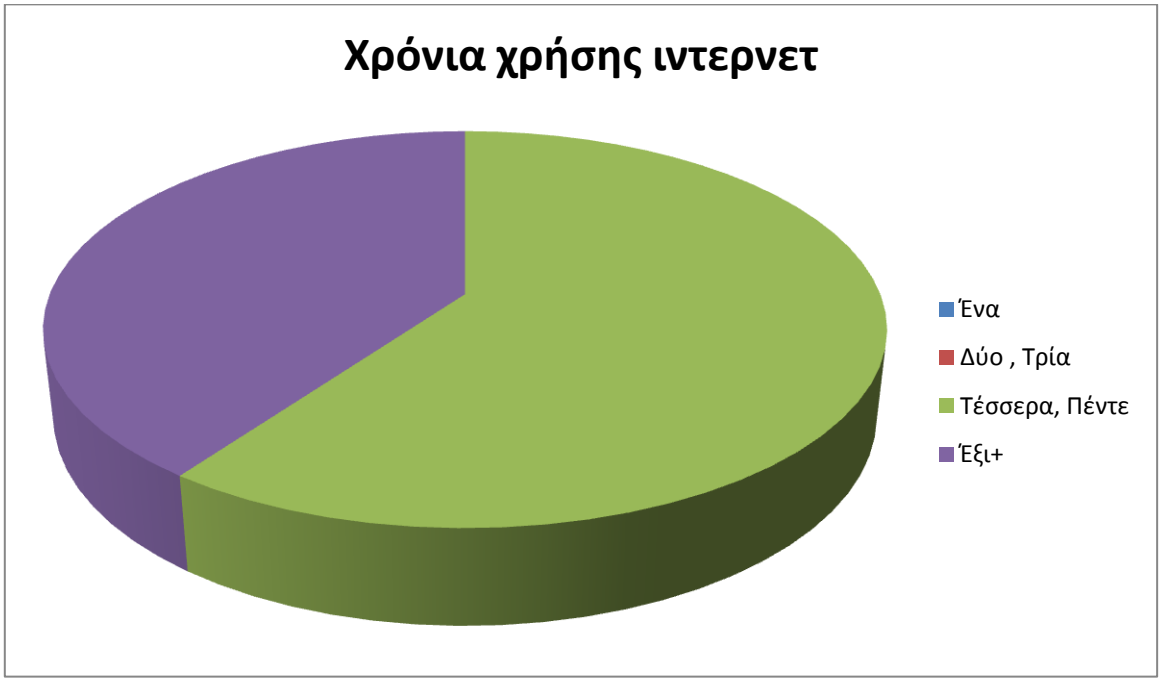
- Παγίδες που έχουν στόχο τους να δεχθούν επίθεση
- Δε γνωρίζω κάτι

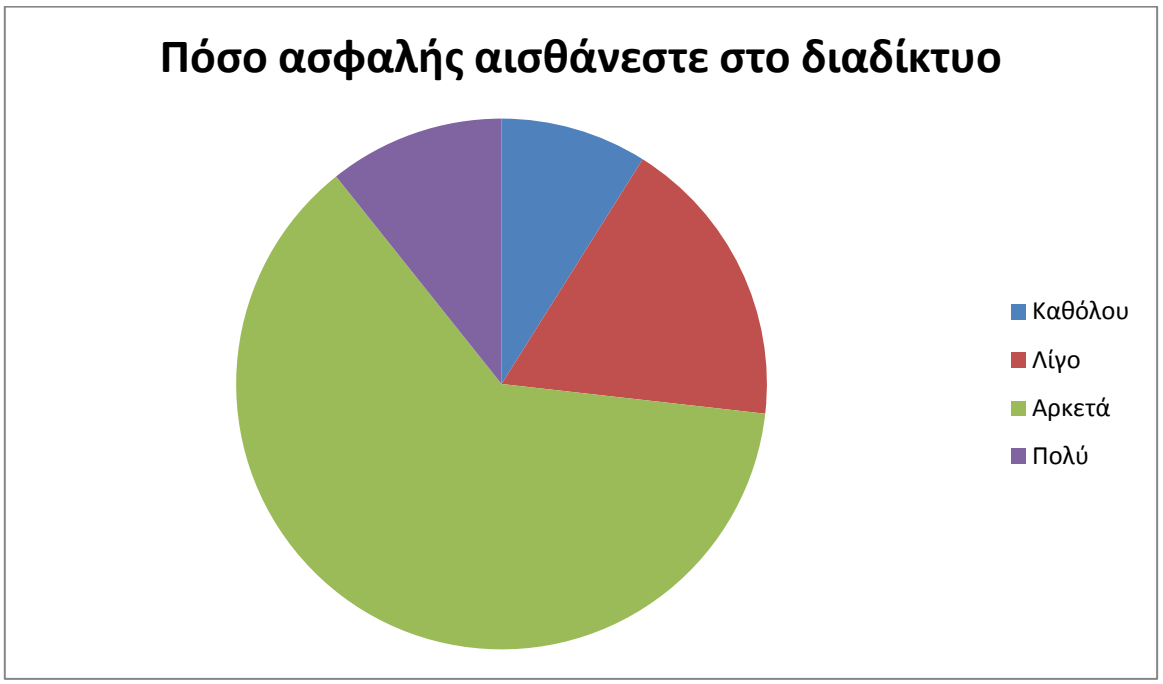
7.ΣΥΜΠΕΡΑΣΜΑΤΑ

7.1 ΣΧΟΛΙΑΣΜΟΣ ΕΡΕΥΝΑΣ

Αποτελέσματα 1ου μέρους

Το παραπάνω ερωτηματολόγιο απαντήθηκε από 20 άτομα εκ των οποίων οι 15 ήταν άντρες(75%) και 5 γυναίκες (25%). Στην πλειοψηφία τους ανήκουν στις ηλικιακές ομάδες 19-25 και 26-35 και δηλώνουν καθημερινοί χρήστες του ιντερνέτ. Οι περισσότεροι έχουν πανεπιστημιακή μόρφωση και τουλάχιστον πενταετή εμπειρία στο χώρο του ιντερνέτ . Το παράδοξο είναι ότι χρησιμοποιούν τα δημόσια δίκτυα χωρίς κανένα φόβο μην υποκλαπούν τα προσωπικά τους στοιχεία. Το διαδίκτυο αποτελεί για αυτούς χώρο που μπορούν να ενημερώνονται(ειδήσεις, άρθρα, πρωτοσέλιδα) αλλά και ως διέξοδο για ψυχαγωγία.





Αποτελέσματα 2ου μέρους

Τα αποτελέσματα του δευτέρου μέρους της έρευνας είναι ανησυχητικά διότι καθημερνοί και έμπειροι χρήστες του διαδικτύου δεν γνωρίζουν για τις πιο απλές μεθόδους παραβίασης των δικτύων. Χρησιμοποιούν το ίδιο εύκολα δημόσια δίκτυα όπως το οικιακό τους και είναι εύκολοι στόχοι για παθητικές τεχνικές παρακολούθησης τους (βλ. Packet Sniffer, Man In The Middle).

Η ενασχόληση τους με το δικτυακό παιχνίδι που παίζουμε τους έχει φέρει σε θέση να δεχτούν κάποιες Denial Of Service επιθέσεις και να μην έχουν γίνει αντιληπτές σχεδόν από κανέναν και μόνη τους παρατήρηση να είναι ότι οι servers του παιχνιδιού «κάποιες συγκεκριμένες φορές κρασάρουν». Τέλος η τεχνική ορολογία(tear drop, ping of death , buffer overflow ,κλπ)

στους περισσότερους ήταν εντελώς άγνωστη.

Αποτελέσματα 3ου μέρους

Στο τρίτο και τελευταίο μέρος του ερωτηματολογίου τα πράγματα δεν άλλαξαν και παραμένουν ανησυχητικά. Μόνο ένα μικρό ποσοστό χρησιμοποιεί τρόπους προστασίας και αυτός ο τρόπος είναι κάποιο συνηθισμένο τοίχος προστασίας(firewall) και μάλιστα με τις προκαθορισμένες ρυθμίσεις. Η κρυπτογράφηση, οι ψηφιακές υπογραφές τα πιστοποιητικά είναι έννοιες άγνωστες για το ευρύ κοινό του διαδικτύου και αυτό του καθιστά εύκολους στόχους. Ακόμα και στις αγορές μέσο διαδικτύου ούτε εκεί εφαρμόζουν τους απλούς μηχανισμούς

προστασίας (SSL).

7.2ΣΥΝΟΨΗ

Στην εργασία που πραγματοποίησα είχα την ευκαιρία να μάθω αρκετά πράγματα για την ασφάλεια των δικτύων αλλά και τεχνικές που χρησιμοποιούν ορισμένες ευπάθειες πρωτοκόλλων που περιέχονται στο TCP/IP. Για διδακτικούς και μόνο σκοπούς μπήκα στη θέση ενός εισβολέα χρησιμοποιώντας το Back Track 5 για να καταλάβω πιο είναι το κίνητρο του. Να δω από «μέσα» πως είναι να πραγματοποιείς Packet sniffing, MITM και DoS επιθέσεις. Έφτασα στο συμπέρασμα ότι το βασικότερο είναι η ικανοποίηση που νοιώθει μετά ο εισβολέας ότι νίκησε ένα σύστημα ασφαλείας(δείτε το σαν παιχνίδι) και ο έλεγχος που μπορεί να ασκήσει μετά μέσα στο δίκτυο. Έμαθα τρόπους θα μπορούσα να αποτρέψω τέτοιες επιθέσεις αν ήμουν ο διαχειριστής ενός δικτύου όπως είναι η κρυπτογράφηση, τα honeypots οι ψηφιακές υπογραφές και το SSL. Όπως επίσης ότι όσα μέτρα ασφάλειας και να πάρεις, αν οι χρήστες του δικτύου σου δεν είναι σωστά ενημερωμένοι τότε πάντα θα υπάρχει μία πίσω πόρτα για έναν εισβολέα.

Σύμφωνα με τις απαντήσεις που πήρα από το ερωτηματολόγιο που έφτιαξα κατάφερα να έχω μια συνολική εικόνα ότι το ευρύ κοινό δεν έχει τις σωστές βάσεις πάνω στην ασφάλεια των δικτύων. Ανεξάρτητα του φύλλου, της ηλικίας και του μορφωτικού επιπέδου το ποσοστό που

χρησιμοποιεί τις απαραίτητες διαδικασίες για την ασφάλεια του είναι πολύ μικρό, και ακόμα μικρότερο είναι το ποσοστό που ήξερε για τις ευπάθειες των πρωτοκόλλων. Τέλος κατέληξα στο ότι είναι λίγοι αυτοί που πραγματικά γνωρίζουν πώς να προστατέψουν τον εαυτό τους και αρκετοί που νομίζουν ότι ξέρουν. Όπως είναι και ο S. Hawking *«ο μεγαλύτερος εχθρός της γνώσης δεν είναι η αμάθεια, αλλά η ψευδαίσθηση ότι έχουμε γνώση»*

Κλείνοντας θέλω να τονίσω ότι δεν πρέπει πάντα να τιμωρούνται οι εισβολής σε ένα δίκτυο. Πρέπει πρώτα να εξετάσουμε προσεκτικά αν πρόκειται για διδακτικούς σκοπούς, αν είναι πάνω στην έρευνα για τρύπες στα συστήματα ασφάλειας ή με κίνητρο την απόκτηση προσωπικών δεδομένων.

ΒΙΒΛΙΟΓΡΑΦΙΑ

[1] Τερζόγλου Α., Αξούργος Γ., (2008) "*Πρωτόκολλα Επικοινωνίας Διαδικτύου*" , Τ.Ε.Ι Ηπείρου

[2]Joe Casad (2009) "*Μάθετε το Tcp/IP σε 24 ώρες*" Αθήνα, Έκδοση 4η , Εκδόσεις, Μ. Γκιούρδας.

[3]Brenton Chris, Hunt Cameron (2003) *"Ασφάλεια δικτύων"* Αθήνα, Έκδοση 2η Εκδόσεις, Μ. Γκιούρδας.

[4]Jon Erickson (2003) *"Hacking: The Art of Exploitation"*

[5]Γκριτζάλη *Στ., Κάτσικα Σ. Γκριτζάλη Δ.(2003) «Ασφάλεια Δικτύων Υπολογιστών»* Αθήνα Εκδόσεις Παπασωτηρίου

[6]*"* ∇hacker" (2012) τεύχος 006 – sneezy spring edition

[7]*"* ∇*hacker" (2013) τεύχος 017 – Misty mornings edition*

[8]*"* ∇hacker" (2011) τεύχος 001

[9]http://www.backtrack-Linux.org/about/ Ανακτήθηκε 29 Δεκεμβρίου 2012

[10]http://www.linuxjournal.com/content/packet-sniffing-basics Ανακτήθηκε 28 Δεκεμβρίου 2012

[11]http://el.wikipedia.org/wiki/%CE%9A%CF%8E%CE%B4%CE%B9%CE%BA%CE%B1%CF%82_%CF%84%CE%BF%CF%85_%CE%9A%CE%B1%CE%AF%CF%83%CE%B1%CF%81%CE%B1

[12] http://hacking-tips-tricks.blogspot.gr/2009/05/ping-of-death.html

http://en.wikipedia.org/wiki/Penetration_test

[13]http://www.eett.gr/opencms/opencms/EETT/Electronic_Communications/DigitalSignatures/IntroEsign.html

[14] http://en.wikipedia.org/wiki/Phrack

[15] http://nmap.org/bennieston-tutorial/

[16] http://nmap.org/book/man-port-scanning-techniques.html

ΠΑΡΑΡΤΗΜΑ Αποτελέσματα Έρευνας

Παραθέτω ξανά το ερωτηματολόγιο μαζί με το επί της εκατό(%) ποσοστό που συγκέντρωσε η κάθε απάντηση.

1.Φύλλο

Άνδρας- 75%
Γυναίκα 25%

2. Ηλικία

1-10 0%
11-18 10%
19-25 40%
26-35 40%
35-50 10%
50+ 0%

3- Εκπαίδευση

Απόφοιτος γυμνασίου 0%
Απόφοιτος λυκείου 25%
Απόφοιτος- Σπουδαστής Α.Ε.Ι 45%
Απόφοιτος- Σπουδαστής Τ.Ε.Ι 25%
Μεταπτυχιακές σπουδές 5%

4-Επάγγελμα

Δημόσιος υπάλληλος 10%
Ιδιωτικός υπάλληλος 60%
Ελεύθερος επαγγελματίας 5%
Άνεργος 15%
Οικιακά 0%
Φοιτητής 25%
Άλλο

5-Πόσο χρόνια χρησιμοποιείτε το διαδίκτυο?

1 0%

2-3 0%

4-5 60%

6+ 40%

6-Πόσο συχνά χρησιμοποιείτε το διαδίκτυο?

Καθημερινά 100%

1-3 φορές την βδομάδα 0%

4-6 φορές την βδομάδα 0%

7- Από ποιο μέρος χρησιμοποιείτε/συνδέεστε συχνότερα?

Σπίτι 20%

Δουλεία 0%

Δημόσια δίκτυα 0%

Όλα τα παραπάνω 80%

8-Για πιο λόγο χρησιμοποιείτε το διαδίκτυο?

Ενημέρωση 0%

Διασκέδαση 0%

Παιχνίδια 0%

Όλα τα παραπάνω 100%

9- Πόσο ασφαλής αισθάνεστε στο διαδίκτυο?

Καθόλου 10%

Λίγο 20%

Αρκετά 70%

Πολύ 0%

10-Εμπιστεύεστε τους ιστότοπους /δίκτυα που συνδέεστε?

Ναι 90%

Όχι 10%

11-Πόσο συχνά δίνετε προσωπικά σας δεδομένα?

Ποτέ 0%

Σπάνια 75%

Πάντα 25%

ΜΕΡΟΣ 2ο Τεχνικές εισβολείς και ευπάθειες

12-Για τις τεχνικές εισβολής σε δίκτυα που χρησιμοποιούν ευπάθειες πρωτοκόλλων γνωρίζετε?

Ναι 15%

Όχι 60%

Έχω ακούσει 25%

13-Έχετε πέσει ποτέ θύμα δικτυακών επιθέσεων?

Ναι 10%

Όχι 5%

Δεν έχω καταλάβει κάτι 85%

14-Τι γνώμη έχετε για τους εισβολής δικτύων

Άσχημη 35%

Μέτρια 10%

Καλή 45%

Τους είδα στις ειδήσεις των 8 και ξετρελάθηκα 10%

15- Πιστεύετε ότι πρέπει να τιμωρούνται πάντα οι επιτιθέμενοι σε ένα δίκτυο?

Ναι 80%

Όχι 15%

Ανάλογα γιατί το κάνουν 5%

16- Man in the middle?

Τίποτα 50%

Το γνωστό τραγούδι Black Country Communion- Man In The Middle 45%

Παραπλάνηση μηχανημάτων σε ένα δίκτυο 5%

17-Smurf attack?

Ταινία που τα στρουμφάκια παίρνουν εκδίκηση 35%

Τεχνική αποστολής πακέτων 10%

Τίποτα από τα παραπάνω 55%

18-Teardrop

Αποστολή κακοσχηματισμένων πακέτων 10%

Το τραγούδι από Massive Attack 80%

Κανένα από τα δύο 10%

19-Ping of death

Δε το γνωρίζω 75%

Τεχνική που μπορεί να χρησιμοποιήσει ο καθένας από το command window του υπολογιστή του. 25%

20- Packet Sniffing

Υποκλοπή πακέτων 20%

Δε το γνωρίζω 80%

ΜΕΡΟΣ 3ο Τρόποι προστασίας

21-Χρησιμοποιείτε κάποιο antivirus ?

- Ναι 95%

Όχι 5%

22- Χρησιμοποιείτε τις προκαθορισμένες ρυθμίσεις?(Αν απαντήσατε ναι στην προηγούμενη ερώτηση ,πρέπει να απαντήσετε και εδώ, αν όχι συνεχίστε με την επόμενη)

Ναι 100%

Όχι 0%

23-Κρυπρογράφηση

Χρησιμοποιώ σε όλες τις συναλλαγές, συνομιλίες μέσα σε ένα δίκτυο 5%

Χρονοβόρα διαδικασία 0%

Κανένα από τα παραπάνω 95%

23- Πιστοποίηση, ψηφιακές υπογραφές

Πάντα κοιτάω, χρησιμοποιώ στα πακέτα που ανταλλάζω 0%

Δε γνωρίζω 100%

24- SSL

Τι είναι αυτό? 60%

Ασφάλεια στην διαδικτυακή επικοινωνία 40%

25-Honeypot

Παγίδες που έχουν στόχο τους να δεχθούν επίθεση 0%

Δε γνωρίζω κάτι 100%