Π Α Ν Ε Π Ι Σ Τ Η Μ Ι Ο Π Α Τ Ρ Ω Ν

ΠΟΛΥΤΕΧΝΙΚΗ ΣΧΟΛΗ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΗΛΕΚΤΡΟΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ & ΠΛΗΡΟΦΟΡΙΚΗΣ

Ε Ρ Γ Α Σ Ι Α Ε Ξ Α Μ Η Ν Ο Υ

ΓΙΑ ΤΟ ΜΑΘΗΜΑ

ΔΙΚΤΥΑ ΔΗΜΟΣΙΑΣ ΧΡΗΣΗΣ & ΔΙΑΣΥΝΔΕΣΗ ΔΙΚΤΥΩΝ

ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΩΝ & ΥΠΟΛΟΓΙΣΤΩΝ

Μελέτη exploitation framework διαφόρων Linux Distribution

ΣΑΡΡΗΣ ΕΜΜΑΝΟΥΗΛ

Α.Μ 5191

ΔΙΔΑΣΚΩΝ: ΧΡΗΣΤΟΣ ΜΠΟΥΡΑΣ

ΠΑΤΡΑ 2016

ΠΕΡΙΕΧΟΜΕΝΑ

ΑΚΡΩΝΥΜΙΑ

• OSI Model: Open Systems Interconnection model

• Hackers (White & Black): Ως λευκοί hacker αναφέρονται εκείνοι που σκοπό έχουν την μελέτη των διαφόρων exploitation ενός δικτύου, με σκοπό την οχύρωσή του από αυτά. Ως Black Hacker αντίθετα, αναφέρονται εκείνοι που οι προθέσεις του είναι επιθετικές.

• Ciphertext: Ως Ciphertext αναφέρεται μια κρυπτογραφημένη πληροφορία.

• A.R.P.A.Net : Advance Research Projects Agency Network

• I.N.W.G : Internet Networking Working Group

• M.I.T: Massachusetts Institute of Technology

• Intranet: Τοπικό η ιδιωτικό δίκτυο επικοινωνίας, βασισμένο σε λογισμικό του World Wide Web.

• VPN: Virtual Private Network

• S/W: Software

• H/W: Hardware

• VoIP: Voice Over IP

ΣΗΜΕΙΩΣΗ ΣΥΓΓΡΑΦΕΑ

Η παρούσα αναφορά αποτελείται από δύο μέρη.

ΜΕΡΟΣ 1ο:

Θα αναλυθούν σε θεωρητικό επίπεδο όλοι οι μηχανισμοί και οι τεχνολογίες που αποτελούν παράγοντα του πεδίου της ηλεκτρονικής και διαδικτυακής ασφάλειας.

ΜΕΡΟΣ 2ο:

Θα γίνει παρουσίαση των πιο δημοφιλών Framework του Kali Linux.

Το *Kali Linux* (γνωστό στο παρελθόν ως BackTrack) αποτελεί μια διανομή Linux, με προ εγκατεστημένα πληθώρα εργαλείων και μηχανισμών, ικανών να συμβάλουν στο έλεγχο της ασφάλειας ενός υπολογιστικού συστήματος. Η διαδικασία ατή είναι γνωστή και ως Penetration Testing.

ΠΡΟΣΟΧΗ

Η παρούσα προσέγγιση των ζητημάτων διαδικτυακής και ηλεκτρονικής ασφάλειας, δεν αποτελεί τίποτα άλλο από μια βιβλιογραφική μελέτη των μηχανισμών αυτών και σε καμία περίπτωση δεν φέρεται ως εγχειρίδιο προς υλοποίηση επιθέσεων με τους τρόπους που περιγράφονται μέσα σε αυτή. Για οποιαδήποτε πρότινος χρήση ο συγγραφέας δεν φέρει καμία ευθύνη.

ΚΕΦΑΛΑΙΟ 1: ΓΕΝΙΚΑ

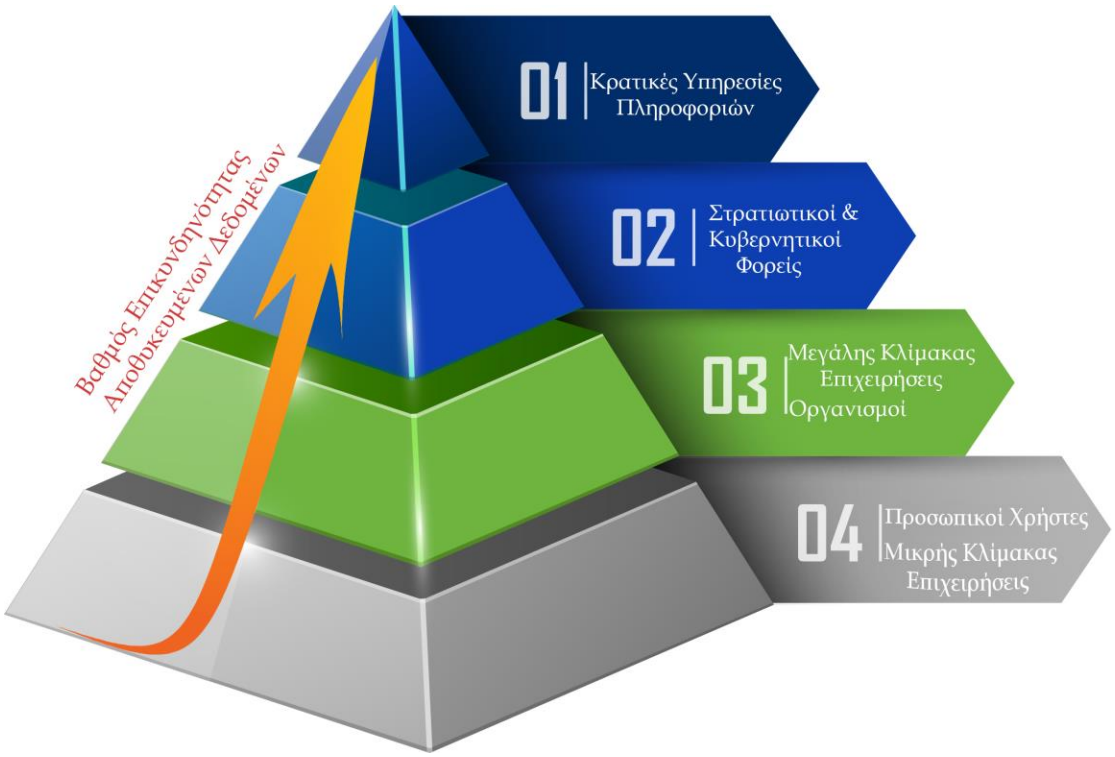
Η λειτουργία της σημερινής κοινωνίας βασίζει την αποτελεσματικότητα της, εάν όχι πλήρως τότε σε ένα μεγάλο βαθμό, στα υπολογιστικά συστήματα και στην διασύνδεση αυτών μέσω του διαδικτύου. Βασικές καθημερινές ανάγκες των ανθρώπων, όπως η ανάληψη μετρητών από ATM, δεν θα ήταν εφικτές δίχως την πρόοδο της τεχνολογίας στο συγκεκριμένο τομέα. Έτσι καθώς αυτή η καθημερινή τεκμηρίωση της ανθρώπινης ανάγκης για την χρήση της τεχνολογίας διογκώνεται, θα ήταν επιβλαβές να μη ληφθούν τα απαραίτητα μέτρα για την σωστή και ασφαλή χρήση αυτής. Για παράδειγμα κανείς μπορεί να σκεφτεί τι θα γινόταν εάν στο προσωπικό υπολογιστή του καθενός μπορούσε να εισχωρήσει ένας οποιασδήποτε και να αποκομίσει από ανούσια μέχρι σημαντικά για εκείνον η τη δουλειά του έγγραφα. Η δομή και ο πυρήνας λειτουργίας του Διαδικτύου ήταν εκείνη που επέτρεψε αρχικά πολλές περιπτώσεις επιθέσεων να λάβουν ύπαρξη. Μερικώς τροποποιημένες αρχιτεκτονικές του Διαδικτύου, μπορούν να παρέχουν μεγαλύτερα μέτρα ασφάλειας, μειώνοντας έτσι το κίνδυνο κάποιου cyber-attack. Ανακαλύπτοντας όμως και τα είδη όλων αυτών των επιθέσεων, επιχειρήσεις, οργανισμοί καθώς και ιδιώτες, μπορούν να προστατευτούν από αυτές με την χρήση firewall η μηχανισμών κρυπτογράφησης. Σε ειδικές περιπτώσεις επιχειρήσεων γίνεται χρήση του ‘Intranet’ με σκοπό να παραμείνει συνδεδεμένη η συγκεκριμένη επιχείρηση στο διαδίκτυο και ταυτόχρονα να είναι ασφαλής από πιθανούς κινδύνους.

Το πεδίο της ασφάλειας των υπολογιστών μπορεί να θεωρηθεί αχανές. Ταυτόχρονα επισημαίνεται ότι βρίσκεται σε στάδιο εξέλιξης, ειδικά σε σύγκριση με άλλα πεδία της τεχνολογίας της πληροφορικής και των υπολογιστών. Στη σημερινή εποχή επί παραδείγματι μπορεί κάποιος μέσω υπολογιστή και διαδικτύου να μιλήσει με εικόνα και ήχο σε πραγματικό χρόνο με κάποιον που θα βρίσκεται στην άλλη μεριά του πλανήτη, αλλά δεν υπάρχει τίποτα να του εγγυηθεί την ακεραιότητα μιας παρουσίασης που τυχόν να ετοιμάζει για την προαγωγή του στην εταιρεία που δουλεύει.

Με σκοπό να γίνει κατανοητός από κάποιον, ο σκοπός της ύπαρξης του ερευνητικού τομέα γύρω από το θέμα της ασφάλειας, η γνώση για τους τρόπους λειτουργίας του διαδικτύου, τα σημεία στα οποία είναι ευάλωτο αυτό καθώς και η τεχνογνωσία γύρω από την επιστήμη της ασφάλειας θεωρείται απαραίτητη και για αυτό το λόγο τα προαναφερθέντα θα αναλυθούν λεπτομερώς σε αυτή τη προσπάθεια της παρούσας προσέγγισης.

ΚΕΦΑΛΑΙΟ 2.0: ΕΙΣΑΓΩΓΗ ΣΤΗΝ ΑΣΦΑΛΕΙΑ

Την παρούσα στιγμή στον πλανήτη, υπάρχει με αχαλίνωτα ογκώδης ποσότητα πληροφορίας. Αυτή η πληροφορία υπάρχει με την μορφή δεδομένων, τα οποία μπορούν να αποτελούν νόμιμη ιδιοκτησία προσωπικών χρηστών, επιχειρήσεων, οργανισμών, κρατικών η στρατιωτικών φορέων καθώς και κυβερνητικών εκπροσώπων μια χώρας (*εικόνα 2.0.1).*



Εικόνα 2.0.1. Πυραμίδα κρίσιμης ύπαρξης δεδομένων, διαφόρων κατόχων.

Είναι κατανοητό λοιπόν ότι ειδικότερα όσο ανεβαίνουμε αυτή την ιεραρχία ο κίνδυνος για την τυχόν διαρροή αυτών των δεδομένων αυξάνεται σημαντικά.

2.1 Ασφάλεια Δικτύων

Επί του παρόντος αυτή τη στιγμή υπάρχουν δυο θεμελιώδης διαφορετικοί τύποι δικτύων. Τα δίκτυα δεδομένων και τα σύγχρονα δίκτυα. Το Ίντερνετ ανήκει

στην κατηγορία των δικτύων δεδομένων. Λαμβάνοντας την πληροφορία αυτή υπ' όψην, κανείς θα μπορούσε να προσκομίσει δεδομένα από το διαδίκτυο, εμφυτεύοντας κάποιο κακόβουλο λογισμικό (επί παραδείγματι αναφέρεται το Trojan Horse) σε κάποιο router το οποίο θα είναι computer based. Για αυτό το λόγο ο τομέας της ασφάλειας επικεντρώνει το ενδιαφέρον του στα δίκτυα δεδομένων, όπως είναι το Internet, η σε άλλα δίκτυα τα οποία συνδέουν την λειτουργία τους εν τέλη σε αυτό.

Ο μεγάλος αυτός τομέας της ασφάλειας δικτύων, μπορεί να αναλυθεί μελετώντας τα ακόλουθα:

i. Ιστορική αναδρομή στην ασφάλεια δικτύων.

ii. Αρχιτεκτονική λειτουργίας του Internet και τρωτά σημεία στο τρόπο λειτουργίας αυτού.

iii. Είδη επιθέσεων και μηχανισμοί άμυνας.

iv. Παρούσα κατάσταση της ασφάλειας των δικτύων, όσων αναφορά τα hardware και software.

Μελετώντας λοιπόν τις παραπάνω περιπτώσεις, θεσπίζεται η αφετηρία για την εισαγωγή στο πεδίο της ασφάλειας από κάποιον που προσελκύεται σε αυτό. Έχοντας ως γνώση λοιπόν βασικές αρχές αποκτώμενες από αυτά, σημαίνεται η αρχή της ένταξης ενός προγραμματιστή στο πεδίο της ασφάλειας.

Η τεχνολογία και η δομή αυτής που εκάστοτε υπάρχει, είναι το κλειδί και ο λόγος ύπαρξης των διαφόρων εφαρμογών λογισμικού που υπάρχουν. Στις μέρες μας, είναι σαφής η έννοια της ασφάλεια από πολλούς. Οι περισσότεροι έχοντας ακούσει περιπτώσεις επιθέσεων hacker σε τρίτους, έχουν σαν φόβο στο πίσω μέρος του μυαλού τους μήπως είναι εκείνοι ή η δουλειά τους τα επόμενα θύματα αυτών. Παρόλα αυτά όμως υπάρχει ένα σημαντικό κενό έλλειψης γνώσης του τρόπου λειτουργίας αυτής και των μεθόδων που χρησιμοποιούνται, με αποτέλεσμα να μπορεί εύκολα να παρακαμφθεί. Το γεγονός αυτό οφείλεται στην έλλειψη επικοινωνίας που υπάρχει μεταξύ των προγραμματιστών στο πεδίο της ασφάλειας και των προγραμματιστών στο πεδίο των δικτύων. Η ανάπτυξη του Internet γνώρισε τόσο ραγδαίους ρυθμούς, με αποτέλεσμα όλη η έρευνα και το ενδιαφέρον από τεχνολογικής πλευράς, να επικεντρωθεί περισσότερο στην διάχυση αυτού ανά την υφήλιο παρά στην ομαλή και υγιή εξάπλωσή του, συνοδευόμενο από όλα τα απαραίτητα εργαλεία οχύρωσης όλης αυτής της γνώσης που το διαρρέει καθημερινά.

Η δομή των δικτύων, αποτελεί πλέον μια εκτενώς υλοποιημένη διαδικασία που βασίζει την λειτουργία της στο μοντέλο OSI (*Open Systems Interconnection model).* Το μοντέλο αυτό παρέχει αρκετά πλεονεκτήματα στον σχεδιασμό δικτύων. Ευκολία στην χρήση, επεκτασιμότητα, ευελιξία επιλογών καθώς και ύπαρξη τυποποιημένων για αυτό πρωτοκόλλων επικοινωνίας, είναι μερικά από τα πλεονεκτήματα αυτά. Συνθέτοντας τα πρωτόκολλα που υπάρχουν για τα διάφορα επίπεδα αρχιτεκτονικής του μοντέλου OSI, μπορεί να υπάρξει εύκολα μια δυναμική υλοποίηση ενός δικτύου. Επίσης η τροποποίηση καθώς και η εισαγωγή, διαφόρων αυτοτελών επιπέδων του μοντέλου, μπορεί να λάβει χώρα και έπειτα από το πέρας της καθολικής υλοποίησης αυτού, προσφέροντας έτσι στο κάθε προγραμματιστή πληθώρα επιλογών δράσης.

Σε αντίθεση με την δομή των δικτύων, η δομή της ασφάλειας αυτών, δεν αποτελεί μια επαρκώς μελετημένη και ανεπτυγμένη έννοια. Ακόμα και σήμερα δεν υπάρχει κάποια μεθοδολογία στον τρόπο μελέτης της πολυπλοκότητας που θα χρειαστεί ένα δίκτυο για την πλήρη ασφάλεια του και τα στοιχεία που αυτήν θα πρέπει να απαρτίζουν. Επίσης πλεονεκτήματα που χαρακτηρίζουν την υλοποίηση ενός δικτύου, όπως αυτά που αναφέρθηκαν πρότινος, δεν υπάρχουν στην περίπτωση της δόμησης της ασφάλειας αυτού.

Όταν καλείται να υλοποιηθεί η ασφάλεια ενός δικτύου, πρέπει να υπολογιστούν όλα τα κομμάτια αυτού καθολικά, και όχι να υπάρξουν πτυχές που για διαφόρους λόγους να μείνουν ανοιχτές σε διάφορες απειλές. Η ασφάλεια αυτή επίσης δεν θα πρέπει να αφορά μόνο την ασφάλεια των υπολογιστικών συστημάτων που βρίσκονται στα άκρα ενός καναλιού επικοινωνίας. Έχοντας αυτή τη παραδοχή, κανείς θα μπορούσε απλά να αποκομίσει την πληροφορία με το να την αδράξει από το κανάλι κατά την διαδικασία μετάδοσής της, η απλά να εισάγει και εκείνος το δικό του λιθαράκι στα δεδομένα που είναι εκείνη την στιγμή προς μετάδοση. Ασφαλώς κάτι τέτοιο δεν είναι επιθυμητό. Έτσι η ασφάλιση του καναλιού επικοινωνίας είναι εξίσου σημαντική με την ασφάλεια των υπολογιστικών συστημάτων που βρίσκονται στα άκρα αυτού.

Εν κατακλείδι λοιπόν και έχοντας κατανοητά τα παραπάνω, για τον σχεδιασμό ενός ασφαλούς δικτύου, η γνώση των παρακάτω εννοιών είναι απαραίτητη:

i. Πρόσβαση: Ποιοι θα είναι εκείνοι οι χρήστες που θα έχουν τα αντίστοιχα δικαιώματα πρόσβασης στα εκάστοτε δίκτυα.

ii. Φύση Δεδομένων: Ποια είναι εκείνα τα δεδομένα που πρέπει να προστατευτούν με κάθε κόστος και ποια εκείνα τα οποία δεν πληρούν και τόσο αυτό το ενδιαφέρον.

iii. Πιστοποίηση: Λίστα η κατ' επέκταση βάση δεδομένων με τους χρήστες και τις εφαρμογές που έχουν δικαίωμα προσπέλασης των αρχείων του συστήματος.

iv. Ακεραιότητα: Πρέπει να υπάρχει ένας τρόπος να διασφαλίζεται ότι το περιεχόμενο των δεδομένων δεν έχει υποστεί κάποια ανεπιθύμητη αλλοίωση, από κάποιο τριτογενή παράγοντα.

v. Καταγραφή γεγονότων: Ποιες ενέργειες έγιναν στο σύστημα και από ποιους χρήστες, με σκοπό να είναι δυνατόν κάποιο είδος traceback, σε μια ανεπιθύμητη ενέργεια.

Η κατασκευή επομένως ενός ασφαλούς δικτύου, κατά γενικό κανόνα μπορεί να επιτευχθεί κατανοώντας τα προβλήματα που αντιμετωπίζει η ασφάλεια του δικτύου, την φύση πιθανών "black hacker" που έχουν σκοπό να επιτεθούν στο σύστημα, το απαιτούμενο επίπεδο ασφάλειας που πρέπει να υλοποιηθεί, αλλά και τους παράγοντες εκείνους που κάνουν ένα δίκτυο ευάλωτο με τη σύνδεσή του στο Internet. Τα βήματα αυτά τα οποία θα χρειαστούν για την επίτευξη των παραπάνω εννοιών θα αναλυθούν σε βάθος.

Για να 'οχυρωθεί' ένα υπολογιστικό σύστημα απέναντι στις απειλές που πλέον υπάρχουν, μια πληθώρα από λογισμικά είναι διαθέσιμη. Προϊόντα κρυπτογράφησης, μηχανισμοί πιστοποίησης, ανιχνευτές εισβολών, καθώς και τείχη προστασίας, είναι μερικά από τα ποιο δημοφιλή και απαραίτητα εργαλεία για αυτό το σκοπό. Διάφοροι συνδυασμοί των παραπάνω μπορούν να οδηγήσουν στην επιτυχημένη ασφάλιση ενός υπολογιστή και αυτό αποτελεί και έναν τρόπο, που πολλοί υπολογιστές προστατεύονται από τις διάφορες επιθέσεις. Η μελέτη της αρχιτεκτονικής του Internet είναι το μοναδικό μέσο να δημιουργηθούν τα κατάλληλα λογισμικά που θα προστατεύσουν τον καθένα από επιθέσεις, καθώς η κατανόηση της λειτουργίας του πυρήνα αυτού, είναι η οδός για την δημιουργία λογισμικών, που

στηρίζοντας την λειτουργία τους πάνω σε αυτή, έχουν σαν αποτέλεσμα την απαραίτητη ‘οχύρωση’ των εκάστοτε υπολογιστών.

Οι τύποι των επιθέσεων μέσα στο Internet, πρέπει επίσης να αναλυθούν και να μελετηθούν με σκοπό την προφύλαξη από αυτές. Συστήματα ανίχνευσης εισβολών έχουν αναπτυχθεί, με σκοπό την μελέτη και τον τρόπο διαφόρων επιθέσεων. Κάποια από τα ανιχνευμένα είδη αυτών, είναι πακέτα που έχουν σταλεί σε αυτό, με διαφόρους κάθε φορά σκοπούς. Αυτοί μπορεί να είναι:

- Για άσκοπη δέσμευση πόρων των συστημάτων με σκοπό την άρση λειτουργίας τους.
- Για παρεμβολή με διαφόρους τρόπους στις θεμελιώδεις λειτουργίες.
- Για προσκόμιση γνώσης με σκοπό την χρήση αυτής για περεταίρω επίθεση

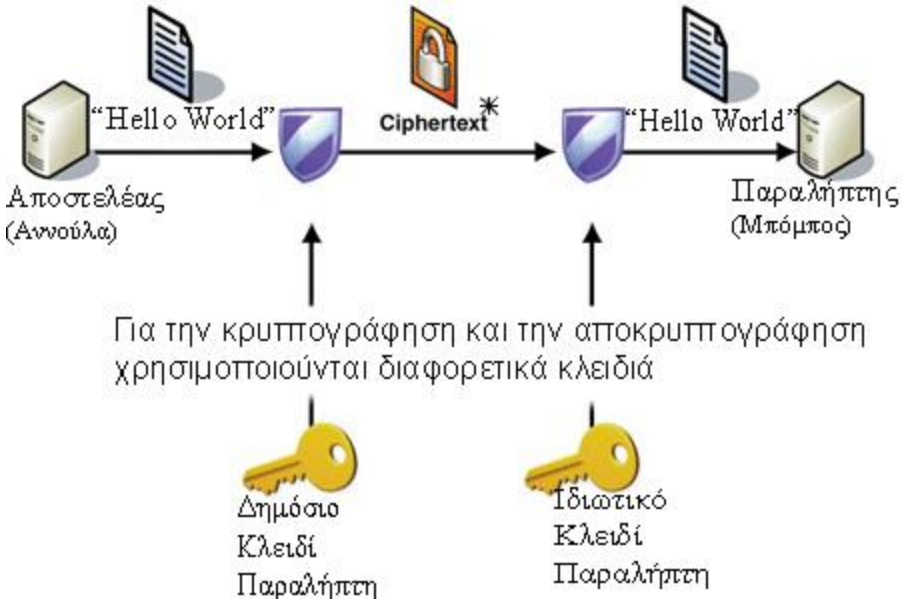
Ο μεγαλύτερος πλέον κίνδυνος έγκειται στην προσκόμιση γνώσεων, για αυτό και οι περισσότερες προσπάθειες οχύρωσης από τα παραπάνω επικεντρώνονται γύρω από αυτό.

Ένα τυπικό επίπεδο ασφάλειας παρέχεται σήμερα μέχρι και δωρεάν για τους υπολογιστές που είναι συνδεδεμένοι στο διαδίκτυο. Επίσης το μοντέλο OSI παρουσιάζει πλέον πρωτόκολλα ασφαλείας για κάθε ένα από τα επίπεδα λειτουργίας του. Σύγχρονες μελέτες μάλιστα, επικεντρώνουν το ενδιαφέρον τους γύρω από αυτό καθώς η συγκεκριμένη τεχνική φαίνεται να αποτελεί μια πλέον λειτουργική και αποτελεσματική περίπτωση ασφάλισης υπολογιστικών συστημάτων από το Internet.

2.2 Διαφορές Ασφάλειας Δικτύων & Ασφάλειας Δεδομένων

Η ασφάλεια των δεδομένων είναι η τεχνολογία εκείνη που πριν την αποστολή τους θα τα μετατρέψει σε πληροφορία μη αναγνώσιμη. Ακόμη λοιπόν και εάν υποκλαπούν τα δεδομένα αυτά, κάποιο ‘κλειδί’ θα χρειάζεται για την ανάγνωσή τους. Το πρόβλημα αυτό καλείται να λύσει η κρυπτογραφία. Αναφέρεται ότι η ερμηνεία του νόμου του Moore, αποτελεί ένα δαίμονα για το πεδίο της κρυπτογραφίας, καθώς με την σημερινή ισχύ που προσφέρουν οι υπολογιστές σε πράξεις ανά δευτερόλεπτο (FLOPS), η αποκρυπτογράφηση και συνεπώς η ερμηνεία διαφόρων παλαιών πρωτοκόλλων, γίνεται πλέον με πολύ πιο εύκολο τρόπο.

Για την μετάδοση κρυπτογραφημένης πληροφορίας, είναι ασφαλές να υπάρχει ένα προστατευμένο κανάλι επικοινωνίας μεταξύ πομπού και δέκτη. Αυτό είναι ευκόλως κατανοητό, μιας και αν αφεθούν δεδομένα τέτοιας φύσης στον οποιοδήποτε, αργά η γρήγορα μπορεί να ερμηνευτούν. Ένα ασφαλές κανάλι επίσης, προσφέρει και την εγγύτητα της ακεραιότητας των δεδομένων. Έτσι δεν θα υπάρχει η πιθανότητα να έχει εισαχθεί από κάποιον τρίτο περεταίρω πληροφορία στο απεσταλμένο πακέτο πληροφοριών (*εικόνα 2.2.1*).



Εικόνα 2.2.1. Πρόχειρη απεικόνιση τρόπου λειτουργίας ενός κρυπτογραφικού πρωτοκόλλου.
Πηγή: http://resources.infosecinstitute.com/role-of-cryptography/

Για την μετατροπή μιας πληροφορίας σε ciphertext υπάρχει πληθώρα επιλογών η οποία είναι διαθέσιμη στο κάθε χρήστη. Σημειώνεται όμως ότι η μετατροπή αυτή λαμβάνει χώρα στο επίπεδο της εφαρμογής. Συνεπώς δεν έχει επαφή με τα επίπεδα αρχιτεκτονικής του Διαδικτύου ή κατά σύμπτυξη τα επίπεδα του OSI. Έτσι λοιπόν δημιουργούνται δυο διαφορετικές σκοπιές εξετάζοντας το παρών ζήτημα. Η μία είναι εκείνη που αφορά την ασφάλεια την δεδομένων και η άλλη εκείνη που αφορά την ασφάλιση ενός δικτύου.

ΚΕΦΑΛΑΙΟ 3.0: ΣΥΝΤΟΜΗ ΙΣΤΟΡΙΚΗ ΑΝΑΔΡΟΜΗ ΤΗΣ ΑΣΦΑΛΕΙΑΣ ΔΙΑΔΙΚΤΥΩΝ

Ένα από τα μεγαλύτερα ονόματα στο χώρο του ηλεκτρονικού και ψηφιακού εγκλήματος, το οποίο μάλιστα υπήρξε και πηγή έμπνευσης για την άνθηση του τομέα της ασφάλειας των υπολογιστικών συστημάτων στο διαδίκτυο, είναι αυτό του Kevin Mitnick (*εικόνα 3.0.1*). Ο Kevin Mitnick διέπραξε το μεγαλύτερο ηλεκτρονικό έγκλημα στην ιστορία των Ηνωμένων Πολιτειών Αμερικής. Απόρροια αυτής της ενέργειας ήταν 80 εκατομμύρια δολάρια, πληροφορίες `σφραγισμένες` από δικαιώματα πνευματικής ιδιοκτησίας καθώς και πλήθος όγκου πηγαίου κώδικα που ανήκε στην κατοχή διαφόρων εταιριών. Έπειτα από την ενέργεια αυτή το 1995, το θέμα της ασφάλειας άρχισε να έρχεται στο παρασκήνιο με καταιγιστικούς σε σχέση με πριν ρυθμούς.


WANTED
BY U.S. MARSHALS

NOTICE TO ARRESTING AGENCY: Before arrest, validate warrant through National Crime Information Center (NCIC).
United States Marshals Service NCIC entry number: (NIC/ W721460021).

NAME: ..... MITNICK, KEVIN DAVID
AKS (S): ..... MITNIK, KEVIN DAVID
MERRILL, BRIAN ALLEN

DESCRIPTION:
Sex: ..... MALE
Race: ..... WHITE
Place of Birth: ..... VAN NUYS, CALIFORNIA
Date(s) of Birth: 08/06/63; 10/18/70
Height: ..... 5'11"
Weight: 190
Eyes: ..... BLUE
Hair: ..... BROWN
Skintone: ..... LIGHT
Scars, Marks, Tattoos: ..... NONE KNOWN

Εικόνα 3.0.1.Ένταλμα των αρχών των Η.Π.Α για τη σύλληψη του Kevin Mitnick (πηγή: https://www.wired.com/images_blogs/thisdayintech/2012/02/mitnick-2.jpg)

Τα δημόσια δίκτυα που υπάρχουν, χρησιμοποιούνται για μια πληθώρα ανταλλαγής πληροφοριών είτε αυτές είναι προσωπικές, είτε οικονομικές, είτε επιχειρησιακές. Η εξέλιξη και η καθολική παγίωση του Internet από την άλλη, έγινε το κανάλι μεταφοράς τεράστιου όγκου δεδομένων, τα οποία είναι ανοιχτά προς επιθέσεις από πολλούς. Έτσι μαζί με αυτή θα πρέπει να αναπτυχθεί και ο τομέας της ασφάλειας. Εξαιτίας του περιστατικού που σημειώθηκε με θύτη των Kevin Mitnick, οι εταιρίες και οι οργανισμοί πλέον δίνουν περισσότερη έμφαση στην ασφάλεια πνευματικής ιδιοκτησίας. Επομένως το Internet, μπορεί να θεωρηθεί και ο πατέρας του τομέα της ασφάλειας δικτύων, μιας και χωρίς την ύπαρξη αυτού δεν θα υπήρχε ο συγκεκριμένος.

Το Internet αρχικά κατασκευάστηκε ως ένα πειραματικό μέσω απομακρυσμένης επικοινωνίας με σκοπό την ανταλλαγή δεδομένων, μεταξύ των ερευνητικών μελών και επιστημόνων. Τα θεμέλια τα οποία επομένως τέθηκαν σε αυτό το σημείο, δεν είχαν ποτέ σαν σκοπό να υποστηρίξουν και την ιδέα της ασφάλειας, μιας και ακόμα η έκτασή του ήταν εν μέρη τοπική. Ακόμα και σήμερα το βασικό πρωτόκολλο επικοινωνίας TCP/IP, δεν περιέχει μεθόδους και αρχιτεκτονικές που να σχετίζονται με την ασφάλεια. Αυτό αφήνει φυσικά ένα μεγάλο εύρος για επιθέσεις. Σημειώνεται όμως, ότι σύγχρονοι μέθοδοι επικοινωνίας μέσω του διαδικτύου, καλύπτουν κάπως σε σχέση με το TCP/IP το κενό αυτό.

3.1 Ιστορική Αναδρομή στο Internet

Η γέννηση του Internet λαμβάνει χώρα το 1969 όταν το δίκτυο ARPANet, καλείται σε εντολή του Υπουργείου Αμύνης Αμερικής, να αναπτύξει έρευνα σχετικά με την δικτύωση υπολογιστών.

Το ARPANet στέφθηκε με επιτυχία ως οργανισμός από την αφετηρία του. Παρόλο που η τεχνολογία του e-mail αναπτύχθηκε για να επιτρέψει σε επιστήμονες και ερευνητές να μοιραστούν απομακρυσμένα πληροφορία, σύντομα γνώρισε και εμπορική επιτυχία. Όλοι οι ερευνητές και επιστήμονες που ήθελαν να μοιραστούν πληροφορίες καθώς και να κάνουν συζητήσεις πάνω σε διάφορα θέματα, χρησιμοποιούσαν το ηλεκτρονικό ταχυδρομείο αυτό. Μερικά από τα πρόσωπα εκείνα που χρησιμοποίησαν την ακμή αυτή της τεχνολογίας, στην συνέχεια αποτέλεσαν και πυρήνα της εκκολαπτόμενης οντότητας του Διαδικτύου. Μεταξύ αυτών υπήρξε και ο

Vinton Cerf, όπου στην συνέχεια εξελέγχεται πρόεδρος της επιτροπής INWG και στην πορεία μένει γνωστός στην ιστορία, ως ο πατέρας του Internet.

Την δεκαετία του 1980, ο Vinton Cerf μαζί με τον Bob Kahn αποτελούν ρόλους κλειδί σε μια ομάδα επιστημόνων, δημιουργώντας το βασικό πρωτόκολλο διαδικτυακής επικοινωνίας των υπολογιστών, γνωστό ως TCP/IP. Βασιζόμενα σε αυτό το πρωτόκολλο, τα επιμέρους δίκτυα του ARPANet πλέον γίνονται ένα «υπερ-δίκτυο» και το Internet όπως το γνωρίζουμε σήμερα ξεκινάει την καλπάζουσα πορεία του. Επίσης στα μέσα της δεκαετίας του 1980, σημειώνεται η πρώτη περίοδος απόκτησης και χρήσης προσωπικών υπολογιστών. Καθώς το κόστος το μέγεθος και άλλοι παράγοντες που πριν εμπόδιζαν στην δημιουργία τους μειώνεται, όλο και περισσότερες επιχειρήσεις αποκτούν το νέο αυτό 'φαινόμενο' του ηλεκτρονικού υπολογιστή και τον χρησιμοποιούν για να καλύψουν την βασική επικοινωνιακή τους ανάγκη, με τους άλλους κατόχους αυτού.

Τέλος, την δεκαετία του 1990 το Internet γίνεται διαθέσιμο προς το κοινό, ως ένα καταναλωτικό πλέον αγαθό. Η έννοια του παγκόσμιου ιστού εισάγεται στο παρασκήνιο και πολύ σύντομα αποτυπώνεται από το καθένα το επίπεδο ύπαρξης και σκοπιμότητάς της. Η εταιρείες NetScape και Microsoft, δίνουν μια φαινομενική μάχη για την κατασκευή μιας μηχανής πλοήγησης του διαδικτύου και κάπως έτσι μετά από λίγα ακόμα χρόνια φτάνουμε στο σήμερα, που η πλοήγηση στο Internet είναι εφικτή σχεδόν από όλους.

3.2 Ιστορική Αναδρομή στο Security

Όπως αναφέρθηκε στο *υποκεφάλαιο 2.2*, η ακεραιότητα των δεδομένων κατά την μεταφορά, επιτυγχάνεται με την σύμπτυξη του πεδίου της ασφάλειας και του πεδίου της κρυπτογραφίας. Έχοντας αυτό ως δεδομένο, είναι θεμιτό να οριοθετήσουμε ως προς το ξεκίνημα, την αρχή της ασφάλειας, στην δεκαετία του 1930.

Κατά την διάρκεια του Δευτέρου Παγκοσμίου Πολέμου, Πολωνοί κρυπτογράφοι επιστήμονες, ολοκλήρωσαν την κατασκευή μιας μηχανής κρυπτογράφησης μηνυμάτων, εν ονόματι Enigma. Τότε ο μαθηματικός Alan Turing, κατάφερε να 'σπάσει' τον τρόπο λειτουργίας του Enigma Machine, κάτι που τέλεσε καθοριστικό ρόλο στην πορεία του Δευτ. Παγκοσμίου Πολέμου.

Δεν θα μπορούσε σαφώς όμως να υπάρξει ιστορική αναδρομή στην έννοια της ασφάλειας, χωρίς να αναφερθούν οι ρίζες του πλέον πασίγνωστου όρου `Hacker`. Όλα ξεκίνησαν την δεκαετία του 1960 στο M.I.T. Μια ομάδα τρομερά ταλαντούχων και ιδιοφυών επιστημόνων, εφάρμοσε εκτενή άσκηση πάνω σε προηγμένα ζητήματα προγραμματισμού κυρίως με FORTRAN, αλλά και άλλες παλαιές γλώσσες προγραμματισμού. Η πλειοψηφία αναφερόταν σε αυτούς με λέξεις της καθημερινής αργού της Αγγλικής διαλέκτου όπως "nerds" η "geeks", η αλήθεια όμως ήταν ότι οι συγκεκριμένοι αποτέλεσαν τους πατέρες για τις επόμενες γενναίες των πραγματικών Hacker.
Οι πραγματικοί Hacker της σημερινής κοινωνίας, έχουν μια αστείρευτη δίψα για γνώση. Η ικανότητα τους προς αφομοίωση και συγκράτηση γνώσης είναι πέραν του κανονικού και το ταξίδι προς μια αέναη πηγή προσκόμισης συνεχούς ροής πρωτότυπης για αυτούς γνώση, δεν σταματά ποτέ.

Εν συνεχεία, το 1969, ο υπάλληλος της Bell Labs ονόματι Ken Thompson εφευρίσκει το UNIX. Το τοπίο στο πεδίο πλέον αλλάζει ολοκληρωτικά για το μέλλον τις βιομηχανίας των υπολογιστών. Έπειτα στις αρχές της δεκαετίας του 1970, ο Dennis Ritchie εφευρίσκει την γλώσσα προγραμματισμού C, η οποία δημιουργήθηκε για να τρέχει ειδικά και βέλτιστα πάνω στο UNIX. Η χρήση διαφόρων assembler από τους προγραμματιστές φτάνει στο πέρας της, και η C γίνεται ένα από τα κύρια μέσα προγραμματισμού.

Την δεκαετία του 1980, η έννοια του Hacker καθώς και πληθώρα ηλεκτρονικών εγκλημάτων ξεκινάει με γρήγορους ρυθμούς να βλέπει τα φώτα της δημοσιότητας. Νόμοι και προκηρύξεις όπως αυτή του 1986 για την Ηλεκτρονική Απάτη λαμβάνουν χώρα. Ένας απόφοιτος φοιτητής, ονόματι Robert Morris, καταδικάστηκε σε ποινή επειδή εξαπέλυσε στο διαδίκτυο το γνωστό Morris Worm, θέτοντας κατά την πράξη του hijack αυτού σχεδόν 6.000 υπολογιστές σε προσβολή. Ακολουθώντας την ψυχολογία του πλήθους που ήθελε ένα τέτοιο γεγονός να επαναληφθεί, η ομάδα CERT δημιουργείται με σκοπό να προειδοποιήσει του χρήστες ηλεκτρονικών υπολογιστών για τα θέματα ασφαλείας του διαδικτύου.

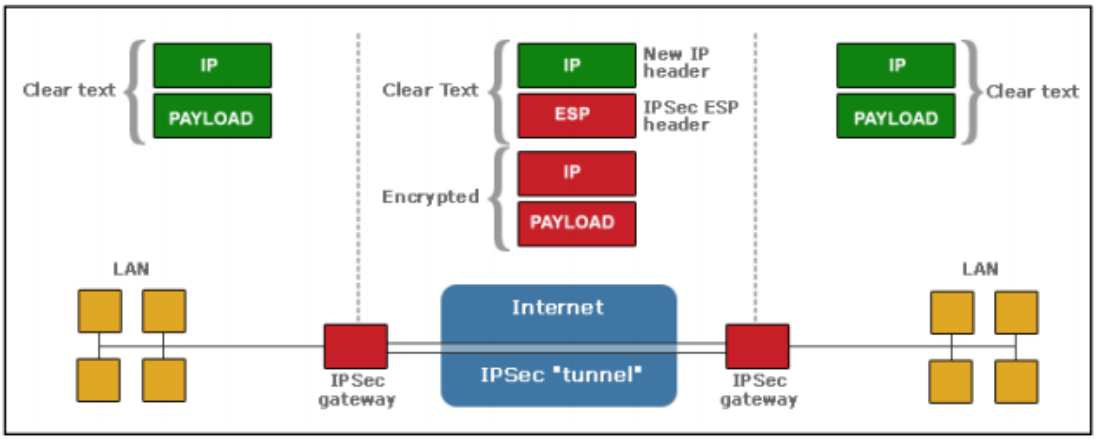
Στα μέσα της δεκαετίας του 1990, το Internet ξεκινά να γίνεται ευρέως διαθέσιμο προς το κοινό. Αυτό έχει ως αποτέλεσμα τα παράπονα για ασφάλεια στο διαδίκτυο να αυξάνονται συνεχώς. Σήμερα περίπου 1 δις ανθρώπων είναι καθημερινά συνδεδεμένοι στο διαδίκτυο. Καθημερινά λαμβάνουν χώρα περί τις 225 ηλεκτρονικές

επιθέσεις ευρείας κλίμακας και δεν υπάρχει τίποτα να διαφυλάσσει τον οποιοδήποτε ότι μια μέρα δεν θα γίνουν και ευρείας σοβαρότητας.

ΚΕΦΑΛΑΙΟ 4.0: ΛΕΙΤΟΥΡΓΙΑ ΑΡΧΙΤΕΚΤΟΝΙΚΗΣ INTERNET & ΕΥΑΛΩΤΑ ΣΗΜΕΙΑ ΕΠΙΘΕΣΕΩΝ

Ο φόβος για επιθέσεις και η ύπαρξη ενδεχόμενων κενών ασφαλείας στα δίκτυα, έχει οδηγήσει οργανισμούς και εταιρίες που χρησιμοποιούν το διαδίκτυο, στην χρήση ιδιωτικών δικτύων ή αλλιώς δικτύων τύπου Intranet*. Η κοινότητα Internet Engineering Task Force, είναι αυτή που έχει εισάγει στα διάφορα επίπεδα λειτουργίας του Internet μηχανισμούς ασφαλείας. Οι μηχανισμοί αυτοί προσφέρουν κάποια ασφάλεια στα δεδομένα που είναι προς μετάδοση πάνω στο διαδίκτυο.

Η αρχιτεκτονική αυτή ασφαλείας του διαδικτύου, ονομαζόμενη ως IP Security(IPSec), είναι γνωστή ως μια από τις καθιερωμένες μεθόδους που χρησιμοποιούνται για την παροχή ασφάλειας στην λειτουργία αυτού. Έχει σχεδιαστεί για να καλύπτει την παρούσα γενιά πρωτοκόλλων διαδικτύου (IPv4), καθώς και την διάδοχο αυτής (IPv6). Η λειτουργία της παρουσιάζεται και σχηματικά στην *εικόνα 4.0.1*.



Εικόνα 4.0.1. Σχηματικη αναπαράσταση τρόπου λειτουργίας του IP Sec
Πηγή: http://web.mit.edu/~bdaya/www/

Παρόλη τη δημιουργία διαφόρων τεχνικών ασφαλείας (συμπεριλαμβανομένου αυτής του IP Sec), εξακολουθούν και υπάρχουν τρόποι επιθέσεων με χρήση κενών που

παρουσιάζονται σε ένα σύστημα. Φυσικά εδώ εισάγεται και ο παράγοντας του ποιος θα κάνει την επίθεση και τις γνώσεις που αυτός μπορεί να κατέχει. Όσο και να έχει λοιπόν μελετηθεί η δομή αρχιτεκτονικής της λειτουργίας του δικτύου για να κατασκευαστεί πάνω σε αυτή ένα επίπεδο ασφάλειας, θα υπάρχει πάντα η πιθανότητα να υπάρχει κάποιος τρόπος για exploitation του δικτύου αυτού.

Τα παρώντα πρωτόκολλα επικοινωνίας καθώς και τα επερχόμενα μελετούνται και αναλύονται εκτενώς για την κατανόηση των κενών που μπορεί να παρουσιάζουν, με σκοπό φυσικά τη συγκάλυψη αυτών. Ακόμη και έπειτα από την πλήρη όμως κατανόηση και μελέτη, εξακολουθούν και υπάρχουν είδη και τρόποι επιθέσεων, από τους οποίους δεν μπορεί κανείς να προστατευτεί με ασφάλειες σε επίπεδο αρχιτεκτονικής λειτουργίας. Συνεπώς η χρήση περαιτέρω λογισμικών είναι απαραίτητη για την χορήγηση εκτενέστερης ασφάλειας σε ένα υπολογιστικό σύστημα.

4.1 Αρχιτεκτονική Λειτουργίας Πρωτοκώλων IPv4 & IPv6

Το πρωτόκολλο IPv4

Το πρωτόκολλο IPv4 σχεδιάστηκε το έτος 1980 και αντικατέστησε πρωτόκολλο NCP που χρησιμοποιούταν μέχρι τότε από το ARPANet. Για τα επόμενα 20 χρόνια η ύπαρξή του θεωρούταν αρκετή για την διευθυνσιοδότηση που μέχρι τότε ήταν απαραίτητη. Με την ραγδαία όμως εξέλιξη του διαδικτύου, το άνω φράγμα που παρείχε (περί του αριθμού των 4.3δις), έγινε κατανοητό ότι δεν θα είναι αρκετό. Έτσι η δημιουργία ενός νέου πρωτοκόλλου, του IPv6, πραγματοποιήθηκε, με κύριο απώτερο σκοπό την μελλοντική χρήση αυτού όταν οι διευθύνσεις που παρέχει το IPv4 εξαντληθούν. Το πρόβλημα αυτό έγινε γνωστό ως IPv4 Address Exhaustion. Σε αυτό το σημείο είναι πρέπον να σημειωθεί, ότι το IPv6 αποτελεί έναν νέο σχεδιασμό ηλεκτρονικού πρωτοκόλλου και δεν αποτελεί μια απλή επέκταση του IPv4.

Στην παρούσα προσέγγιση, δεν θα μελετηθούν όλα τα πρωτόκολλα λειτουργίας του διαδικτύου καθώς ανοίγουν ένα αχανές προς διερεύνηση πεδίο, αλλά κυρίως αυτά που σχετίζονται με την ασφάλεια.

Το πρωτόκολλο IPv4, πέραν του προβλήματος που αναφέρθηκε ήδη, παρουσίασε και μια άλλη πληθώρα προβλημάτων. Με σκοπό την γνώση αυτών για

την καλύτερη κατανόηση των μετέπειτα εννοιών που θα αναφερθούν σε επίπεδο ασφάλειας, αναφέρονται τα κυριότερα από αυτά:

I. Χώρος Διευθύνσεων (Address Space Exhaustion)

II. Δρομολόγηση

III. Διαχείριση και τροποποίηση

IV. Ασφάλεια

V. Ποιότητα λειτουργίας

Η δρομολόγηση έχει υπάρξει ως πρόβλημα αυτού του πρωτοκόλλου, καθώς το μέγεθος των πινάκων δρομολόγησης, ολοένα και αυξάνεται. Το θεωρητικό άνω φράγμα που παρέχεται με αυτή την αρχιτεκτονική, είναι περίπου οι 2.1δις εγγραφές.

Η TCP/IP λειτουργία του διαδικτύου με πρωτόκολλο επικοινωνίας το IPv4, προϋποθέτει ως δεδομένα παρεχόμενη κάποια ποσότητα πληροφορίας από το χρήστη, εάν αυτός θέλει να κάνει αλλαγές πάνω στο δίκτυο. Μερικές από τις πληροφορίες αυτές είναι η IP διεύθυνση, η διεύθυνση gateway, το Subnet Mask, καθώς και ο DNS Server. Συνεπώς το να υπάρξει τροποποίηση του δικτύου δεν αποτελεί εύκολη λειτουργία. Ο εκάστοτε χρήστης μπορεί να ζητήσει μια τροποποίηση στο δίκτυό του που να φαντάζει απλή, όμως για τους διαχειριστές αυτού να αποτελεί πραγματικό Γολγοθά.

Η έλλειψη κάποιου ενσωματωμένου τρόπου ασφάλειας στο πρωτόκολλο IPv4, έχει υπάρξει ο λόγος που πολλές από τις επιθέσεις που έχουν χαραχτεί στην ιστορία, έχουν κάνει την εμφάνισή τους μέχρι σήμερα. Μηχανισμοί για ασφαλή χρήση αυτού του πρωτοκόλλου υπάρχουν, αλλά δεν είναι απαραίτητοι για την λειτουργία του. Το IPSec όπως αναφέρθηκε, είναι ένας τρόπος παροχής ασφάλειας. Η λειτουργία του βασίζεται στην κρυπτογράφηση των προς αποστολή πακέτων με αποτέλεσμα την ακεραιότητα αυτών. Παρόλα αυτά όμως αυτή η κρυπτογράφηση μπορεί να σπάσει από κάποιον έμπειρο Hacker που θα είναι ικανός να αποκομίσει τα κατάλληλα κλειδιά.

Όταν κατασκευάστηκε το Internet, η ποιότητα λειτουργίας αυτού ερμηνεύτηκε από την πληροφορία και τα ποσοστά αυτής που αποστέλλονταν σε αυτό, καθώς η απεσταλμένη πληροφορία ήταν κατά βάση κειμενική. Σήμερα έννοιες όπως αυτή του video streaming είναι πολύ επικρατείς. Εκεί η ποιότητα λειτουργίας του

δικτύου δεν μπορεί να κριθεί με τον τρόπο αυτό και απαιτούνται άλλα μέσα. Τέλος το πρωτόκολλο IPv4, δεν παρέχει κάποιο τρόπο δυναμικής αλλαγής της μέτρησης της ποιότητας λειτουργίας του Internet, ανάλογα με το ποιόν του προς αποστολή περιεχομένου.

Το πρωτόκολλο IPv6

Κατά την δημιουργία του πρωτοκόλλου IPv6 δόθηκε ιδιαίτερη σημασία στις πτυχές του πρωτοκόλλου IPv4, οι οποίες παρουσίαζαν ελαττώματα στο τρόπο λειτουργίας του. Μερικές από τις βασικές λειτουργίες αυτές είναι:

I. Δρομολόγηση και Διευθυνσιοδότηση

II. Αρχιτεκτονική πολλαπλών πρωτοκόλλων

III. Αρχιτεκτονική Ασφάλειας

IV. Έλεγχος Κίνησης στο Δίκτυο

Θέλοντας να εξαγνιστεί το πρόβλημα του Address Exhaustion που παρουσίασε το IPv4, αυτή τη φορά στο πρωτόκολλο IPv6 χρησιμοποιήθηκε αναπαράσταση σε ακρίβεια των 128bit. Έτσι ο χώρος διευθύνσεων που είναι διαθέσιμος γνωρίζει το άνω φράγμα των <3.4 * (10)^38> διευθύνσεων προς ανάθεση.

Το σύστημα δρομολόγησης είναι πιο αποδοτικό και υποστηρίζει τεχνικές για χρήση μικρότερων σε μέγεθος πινάκων δρομολόγησης. Η ρυθμίσεις λειτουργίας των δρομολογητών έχουν γίνει πολύ απλούστερες και έχει προστεθεί η δυνατότητα για δυναμικές αλλαγές στις ρυθμίσεις αυτές. Αυτό το γεγονός φυσικά καθιστά πλέον εύκολη προσέγγιση στα διάφορα ζητήματα αλλαγών που μπορεί να παρουσιαστούν σε απλούς χρήστες καθώς και διαχειριστές συστημάτων.

Από άποψη ασφάλειας το IPv6 έχει συμπεριλάβει μεθόδους για την επίτευξή της. Το IPsec που αναφέρθηκε παραπάνω είναι ενσωματωμένο στην αρχιτεκτονική του IPv6. Στην παρούσα περίπτωση η χρήση του IPsec είναι δυνατή καθ' όλη την διαδρομή του πακέτου πάνω σε ένα δίκτυο σε αντίθεση με το IPv4 που το implantation αυτής γινόταν σε διαφορετικές φάσεις.

Το πρόβλημα του ελέγχου της παροχής υπηρεσιών γνώρισε επίσης λύση. Πακέτα με διαφορετικό περιεχόμενο ως προς την μεταβιβαζόμενη πληροφορία (όπως

παραδείγματος χάρη πακέτα βίντεο και πακέτα απλού κειμένου) είναι δυνατόν να κατηγοριοποιηθούν και να αντιμετωπιστούν με διαφορετικά κριτήρια βαθμολόγησης.

Βλέποντας εν κατακλείδι τη συνοπτική δόμηση του πρωτοκόλλου αυτού, το πλέον ασφαλές είναι να ειπωθεί ότι η ευκολία που προσφέρει σε αλλαγές και τροποποιήσεις, καθώς και το παρεχόμενο επίπεδο ασφαλείας, είναι άρδην βελτιωμένα σε σύγκριση με το προκάτοχο πρωτόκολλο αυτού IPv4. Παρόλα αυτά όμως τα κενά προς κατάχρηση εξακολουθούν να υπάρχουν. Όπως ήδη αναφέρθηκε το πεδίο της ασφάλειας είναι ένα πεδίο που εδρεύουν εκείνοι με τις περισσότερες γνώσεις και από τη στιγμή που η γνώση είναι κάτι αέναο και ατέρμονο, έτσι και οι πτυχές του πεδίου αυτού δεν θα γνωρίσουν κάποια στιγμή ολοκληρωτική αντιμετώπιση προς αποφυγή επιθέσεων.

4.2 Είδη επιθέσεων

4.2.1 Αναφορικά με το πρωτόκολλο IPv4

Τα βασικά χαρακτηριστικά τα οποία πρέπει να είναι διαθέσιμα σε ένα υπολογιστικό σύστημα για να πληρείται (όσο αυτό είναι δυνατόν) η διαδικτυακή ασφάλεια αυτού είναι η διαθεσιμότητα, η ιδιωτικότητα, η ακεραιότητα και η εμπιστευτικότητα. Για παράδειγμα, είναι διαθέσιμος ένας server (*διαθεσιμότητα*) στον οποιοδήποτε (*ιδιωτικότητα*) και εάν ναι τι δικαιώματα έχει αυτός ο χρήστης (*εμπιστευτικότητα)* πάνω στο server στον οποίο έχει αποκτήσει πρόσβαση *(ακεραιότητα)*. Η διαθεσιμότητα συνεπώς μεταφράζεται ως προς το ποιοι χρήστες είναι αυτοί που έχουν πρόσβαση σε έναν υπολογιστή. Η ιδιωτικότητα ως το δικαίωμα της προβολής η μη των εκάστοτε δεδομένων από τρίτους και τέλος η εμπιστευτικότητα με την ακεραιότητα, μπορούν να φέρουν συγκλίνοντα νοήματα στην ερμηνεία τους γεγονός που και πραγματοποιείται. Στον πίνακα της *εικόνας 4.2.1.1* παρουσιάζονται οι διάφορες κατηγορίες επιθέσεων ανά επιτιθέμενο χαρακτηριστικό αυτών και οι διάφοροι τρόποι μερικής η ολικής αντιμετώπισής τους.

Οι βασικές κατηγορίες του είδους των ηλεκτρονικών επιθέσεων θα καλυφθούν στην συνέχεια. Η φύση και οι τεχνικές που χρησιμοποιούνται για όλα τα είδη αυτών όμως δεν είναι εφικτό να προσεγγιστούν, μιας και αναφερόμαστε με το παρών σε μια άπειρη κλίμακα συμβάντων. Αυτό το γεγονός οφείλεται στους διαφόρους τρόπους με τους οποίους κάποιος μπορεί να επιτεθεί σε ένα σύστημα,

πολλοί από τους οποίους ίσως να μην είναι καν γνωστοί στο ευρύ ερευνητικό η μη κοινό.

Χαρακτηριστικά Ασφάλειας	Μέθοδοι Επιθέσεων	Τρόπος Αντιμετώπισης
Εμπιστευτικότητα	Eavesdropping, DoS,IP Spoofing, Phising	IDS, Firewall, Crypto Systems, IPsec, SSL
Ακεραιότητα	Virus, Worms, Trojans, DoS, Eavesdropping, IP Spoofing	IDS, Firewall, Anti-Malware S/W, IPsec, SSL
Ιδιωτικότητα	E-Mail Bombing, Spamming, Hacking, DoS, Cookies	IDS, Firewall, Anti-Malware S/W, IPsec, SSL
Διαθεσιμότητα	DoS, E-Mail Bombing, Spamming, Worms	IDS, Firewall, Anti-Malware S/W

Εικόνα 4.2.1.1 Διάφοροι τρόποι επιθέσεων ανά χαρακτηριστικό ασφάλειας και τρόποι αντιμετώπισής τους (Πηγή: http://washingtontorrent.jimdo.com/2015/12/23/internet-attack-methods-and-internet-security-technology/ *)*

Τα διάφορα είδη επιθέσεων όπως φαίνεται στην παραπάνω εικόνα, μπορούν εν μέρη να κατηγοριοποιηθούν. Άλλα αφορούν την προσκομιδή πληροφοριών, άλλα τη τροποποίηση ρυθμίσεων του συστήματος και άλλα έχουν απλά ως σκοπό τη άσκοπη δέσμευση πόρων με στόχο την άρση λειτουργίας του εκάστοτε συστήματος.

Στις παρακάτω κατηγορίες αναλύονται λεπτομερώς οι σημαντικότεροι τύποι επιθέσεων.

Eavesdropping

Η πλειοψηφία των διαδικτυακών επικοινωνιών γίνεται με μη ασφαλής συνδέσεις. Αυτό επιτρέπει σε κάποιο attacker που θα αποκτήσει πρόσβαση πάνω στο κανάλι επικοινωνίας να 'παρατηρήσει' τα δεδομένα που αποστέλλονται και κατά επέκταση να τα διαβάσει η να τα τροποποιήσει ως προς το περιεχόμενό τους. Η συγκεκριμένη μορφή 'επίθεσης' είναι και γνωστή ως sniffing ή snooping. Ο συγκεκριμένος τρόπος επίθεσης είναι ο σοβαρότερος σε βαρύτητα που αντιμετωπίζουν οι διαχειριστές συστημάτων σε εταιρίες. Χωρίς μεθόδους

κρυπτογράφησης για να κωδικοποιηθούν τα δεδομένα που αποστέλλονται, η υποκλοπή αυτών μπορεί να αποτελέσει και ταυτόχρονη προσπέλασή τους από τον οποιοδήποτε.

Data Modification

Αφού κάποιος επιτιθέμενος αποκτήσει πρόσβαση στα δεδομένα και τα διαβάσει, μπορεί να τα τροποποιήσει με κατάλληλο τρόπο προς δική του επιθυμία χωρίς κάποιος από τους αποστολέα η παραλήπτη να το γνωρίζει. Αυτό σαφώς μπορεί να αποβεί καταστροφικό εάν για παράδειγμα τα δεδομένα είναι τραπεζικοί αριθμοί και συναλλαγές και αλλαχθούν προς όφελος του επιτιθέμενου.

Identity Spoofing (IP Address Spoofing)

Όταν κάποιος υπολογιστής συνδέεται στο διαδίκτυο, χρησιμοποιεί την IP του διεύθυνση για να επικυρωθεί η ταυτότητά του από τους διάφορους Network Administrator. Το πρόβλημα που παρουσιάζεται είναι ότι είναι δυνατόν για κάποιον επιτιθέμενο να παρουσιάσει ψευδή IP διεύθυνση, με αποτέλεσμα να αποκτήσει πρόσβαση εκεί που αλλιώς δεν θα μπορούσε. Επίσης είναι πιθανό να κατασκευαστούν διάφορα πακέτα δρομολόγησης, τα οποία θα φέρουν ως IP διεύθυνση, αυτήν ενός συγκεκριμένου υπολογιστή ενός δικτύου Intranet. Από την στιγμή που αποκτήσει πρόσβαση με αυτό το τρόπο σε ένα δίκτυο, είναι ικανός να προβεί σε οποιαδήποτε ενέργεια αντιστοιχούν τα δικαιώματα της IP της οποίας πλαστογραφεί και κατά συνέπεια να τροποποιήσει ρυθμίσεις, να εκχωρήσει πληροφορία καθώς και να διαγράψει δεδομένα.

Password-Based Attacks

Σύνηθες ελάττωμα των διαφόρων λειτουργικών συστημάτων και των γραφικών η μη περιβαλλόντων διαχείρισης δικτύων, είναι ότι η πρόσβαση σε αυτά αποκτάται με την χρήση κάποιου κωδικού. Αυτό σημαίνει ότι για να καταλάβει ένας υπολογιστής την ταυτότητα του χρήστη στον οποίο είναι έτοιμος να απευθυνθεί, χρειάζεται μόνο δυο πράγματα, το username και το password αυτού. Συνήθως παλαιάς υλοποίησης εφαρμογές, δεν είχαν τρόπο να προστατεύσουν την ταυτότητα

του χρήστη όταν αυτή ήταν υπό αποστολή πάνω στο κανάλι. Με αυτό το τρόπο κάποιος *eavesdropper* θα μπορούσε να αποκτήσει πρόσβαση στο δίκτυο, γνωρίζοντας πλέον τα credentials κάποιου valid user. Εάν για παράδειγμα τα στοιχεία που υποκλαπούν ανήκουν στον administrator ενός συστήματος, ο επιτιθέμενος θα μπορούσε να δημιουργήσει κάποιο κρυφό account στο σύστημα αυτό, για περαιτέρω μελλοντική χρήση.

Denial-of-Service Attack

Το συγκεκριμένο είδος επίθεσης δεν έχει σαν σκοπό την προσκομιδή κάποιας πληροφορίας. Αντίθετα στοχεύει στην αστείρευτη δέσμευση των πόρων ενός υπολογιστικού συστήματος με αποτέλεσμα την άρση της λειτουργίας αυτού. Συνήθης τακτική σε αυτή τη περίπτωση είναι ο επιτιθέμενος αρχικά να τροποποιήσει τα αρχεία καταγραφής της λειτουργίας ενός δικτύου ,με αποτέλεσμα να έχει περισσότερο χρόνο στην διάθεση του σε περίπτωση που εντοπιστεί από κάποιον network administrator. Έπειτα αποστέλλει μη έγκυρα δεδομένα σε διάφορες εφαρμογές του δικτύου τερματίζοντας ανώμαλα έτσι την λειτουργία αυτών. Στην συνέχεια ο στόχος γίνονται οι υπολογιστικοί κόμβοι του δικτύου, καθώς γίνεται αποστολή μαζικής πληροφορίας προς έναν κόμβο, που το μέγεθός της δεν είναι διαχειρίσιμο, με αποτέλεσμα την πτώση του υπολογιστή αυτού από το δίκτυο. Τέλος θα μπορούσε να απαγορεύσει την κίνηση πακέτων, με αποτέλεσμα να μην υπάρχει πρόσβαση στο δίκτυο και τους πόρους του, από τους χρήστες αυτού.

Man-in-the-Middle Attack

Όπως το συμπέρασμα που προκύπτει από το τίτλο της κατηγορίας αυτής, έτσι και οι πράξεις της. Συγκεκριμένα το παρόν είδος επίθεσης προκύπτει όταν κάποιος μεταξύ δύο κόμβων που επικοινωνούν, παρεμβαίνει, παραμένοντας ταυτόχρονα στην αφάνεια και για τους δύο. Έτσι έχει πρόσβαση σε οτιδήποτε οι δυο κόμβοι αυτοί ανταλλάσσουν πάνω στο δίκτυο. Για παράδειγμα μπορεί να υπάρξει η περίπτωση της επαναδρομολόγησης ενός πακέτου. Σε περιπτώσεις που συγκεκριμένα ένας υπολογιστής επικοινωνεί σε χαμηλό ιεραρχικό επίπεδο, δεν είναι σε θέση να αναγνωρίσει την προέλευση των πακέτων που καταφθάνουν σε αυτόν. Το παρών είδος επίθεσης συμπεριλαμβάνει υψηλό κίνδυνο, καθώς το άτομο εκείνο που θα αναλάβει το ρόλο του *man-in-the-middle*, ουσιαστικά πλαστογραφεί την ταυτότητα του εκάστοτε αποστολέα, συντελώντας ο ίδιος πάνω στην πληροφορία με

το δικό του τρόπο, χωρίς να υπάρχει κάποιος τρόπος να γίνει αντιληπτός από κανέναν από τους κόμβους που συμμετέχουν στην επικοινωνία.

Compromised-Key Attack

Το κλειδί είναι ένας μυστικός κωδικός που είναι απαραίτητος για την υποκλοπή ασφαλισμένης από αυτό πληροφορίας. Η συγκεκριμένη διαδικασία μπορεί να είναι κοστοβόρα σε σχέση με τους πόρους που είναι απαιτούμενοι για την λειτουργία αυτής αλλά δεν παύει να είναι ανέφικτη. Όταν ένα ιδιωτικό κλειδί μαθευτεί από κάποιον επιτιθέμενο, τότε το κλειδί αυτό θεωρείται επικίνδυνο για χρήση αυτού και κατά επέκταση δεν χρησιμοποιείται. Το κλειδί αυτό χρησιμοποιείται με σκοπό να λάβει μέρος κάποιος στον διαμοιρασμό πληροφορίας, χωρίς κάποιον από τους παραλήπτη η αποστολέα να το γνωρίζουν. Με την κατοχή αυτού του κλειδιού μπορεί κάποιος να αποκρυπτογραφήσει ασφαλισμένη πληροφορία και να τροποποιήσει δεδομένα. Υπάρχουν περιπτώσεις επίσης που η υποκλοπή ενός κλειδιού μπορεί να οδηγήσει στην εύρεση υπολοίπων ασφαλισμένων κλειδιών, με την χρήση του πρώτου, και ως αποτέλεσμα αυτού να είναι η πρόσβαση σε περαιτέρω κανάλια επικοινωνίας.

Sniffer Attack

Ως *sniffer* αναφέρεται η εφαρμογή, ή, η συσκευή εκείνη η οποία θα υπάρχει με σκοπό να διαβάζει, να παρακολουθεί και να καταγράφει διαδικτυακές ανταλλαγές δεδομένων καθώς και να διαβάζει τα διαμοιραζόμενα πακέτα πάνω στα εκάστοτε δίκτυα. Εάν τα πακέτα αυτά δεν είναι κρυπτογραφημένα, παρέχεται μέσω αυτής πλήρης ανάγνωση των δεδομένων αυτών. Ακόμα και πακέτα *encapsulated,* μπορούν να 'ανοιχτούν' και να διαβαστούν, εάν δεν είναι κρυπτογραφημένα και ο επιτιθέμενος δεν έχει στην κατοχή του το κλειδί. Συνεπώς η χρήση ενός *sniffer* μπορεί να προσφέρει διαρκή παρακολούθηση ενός δικτύου, ανάγνωση δεδομένων και καταγραφή αυτών, με αποτέλεσμα να υπάρχει αρκετός όγκος πληροφορίας σε τρίτους που πλέον με αυτή θα μπορούν να κάνουν το δίκτυο να καταρρεύσει.

Application-Layer Attack

Μια επίθεση τέτοια τύπου στοχεύει στην εσκεμμένη βλάβη της λειτουργίας ενός λειτουργικού συστήματος η εφαρμογών αυτού, σε έναν server. Αυτό δίνει την δυνατότητα να παρακαμπτούν διάφοροι έλεγχοι ασφαλείας που μπορεί να έχουν

θεσπιστεί με την χρήση διαφόρων λογισμικών. Αφού απωλεσθεί ο έλεγχος από τον εκάστοτε server και περάσει στον επιτιθέμενος, τότε αυτός μπορεί να χειριστεί τις εφαρμογές, το σύστημα, το δίκτυο και να πράξει μια σειρά από ενέργειες πάνω σε αυτά. Οι ενέργειες αυτές είναι:

- Ανάγνωση, προσθήκη και τροποποίηση όλων δεδομένων, ακόμα και αυτών του λειτουργικού συστήματος.
- Εισροή ενός *virus* μέσα στο δίκτυο, με σκοπό εξάπλωση λειτουργιών επιθυμητών από τον επιτιθέμενο, σε όλο το δίκτυο.
- Εισροή ενός *sniffer* μέσα στο δίκτυο, με σκοπό την επίτευξη των στόχων που μπορεί να επιτύχει αυτό (αναλύθηκαν πρωτύτερα).
- Μη ομαλός τερματισμός δεδομένων εφαρμογών και λειτουργικού συστήματος.
- Απενεργοποίηση περαιτέρω μηχανισμών ασφαλείας με σκοπό μελλοντικές επιθέσεις.

4.2.2 Αναφορικά με το πρωτόκολλο IPv6

Από την οπτική γωνία της ασφάλειας, το πρωτόκολλο IPv6 υπερτερεί ξεκάθαρα σε σύγκριση με το IPv4. Παρόλο όμως τους διαφόρους μηχανισμούς άμυνας, συνεχίζει να παραμένει ανοιχτό σε επιθέσεις διαφόρων τύπων. Συγκεκριμένες περιοχές του πρωτοκόλλου IPv6 που υστερούν σε ασφάλεια, συνεχίζουν να παραμένουν σοβαρά προβλήματα προς αντιμετώπιση.

Το καινούργιο αυτό πρωτόκολλο επικοινωνίας δεν είναι ικανό να παρέχει άμυνα σε ελλιπώς τροποποιημένους server ή εφαρμογές. Ως αποτέλεσμα αυτού μπορούν να προκύψουν διάφορα προβλήματα, αλλά κυρίως θέματα σε:

- Διαχείριση Επικεφαλίδων Αρχείων
- Υπερχείλιση (Flooding)
- Διακίνηση στο δίκτυο (Mobility)

Το πρόβλημα της διαχείρισης των επικεφαλίδων των αρχείων προκύπτει από την ενσωματωμένη χρήση του IPsec. Η επέκταση των header αποτρέπει κάποιες από τις επιθέσεις που λαμβάνουν χώρα λόγο της χειραγώγησης αυτών. Το πρόβλημα προκύπτει επειδή οι επεκταμένες αυτές επικεφαλίδες πρέπει να επεξεργαστούν από τα

διάφορα επίπεδα αρχιτεκτονικής, με αποτέλεσμα πολύ μεγάλες τελικές επικεφαλίδες. Η επεξεργασία έτσι μεγάλων επικεφαλίδων που έχουν υποστεί αυτή τη διαδικασία, μπορεί να χρήσει μεγάλης ποσότητας επεξεργασίας από υπολογιστικούς κόμβους, και να θεωρηθεί ως τρόπος επίθεσης όταν γίνεται εσκεμμένα. Κατά επέκταση το spoofing συνεχίζει να αποτελεί ένα τρόπο επίθεσης στο πρωτόκολλο IPv6.

Υπάρχει ένα είδος επίθεσης το οποίο αποκαλείται *port scanning* (διερεύνηση θυρών). Στο παρόν αυτό είδος, γίνεται έλεγχος όλων των λειτουργιών ενός δικτύου, με σκοπό την χρήση μια εξ' αυτών η οποία να είναι ευάλωτη. Ο χώρος διευθύνσεων του πρωτοκόλλου μπορεί να είναι πολύ μεγάλος, αλλά αυτό δεν καθιστά λύση στο παρών πρόβλημα.

Το mobility είναι ένα νέο χαρακτηριστικό που συμπεριλαμβάνεται στο IPv6 με τη χρήση αυτού να χρειάζεται ισχυρούς μηχανισμούς άμυνας. Συνεπώς οι διαχειριστές πρέπει να γνωρίζουν την ανάγκη αυτή για ασφάλεια στην παρούσα περίπτωση, εάν θέλουν να χρησιμοποιήσουν το χαρακτηριστικό αυτό.

4.3 Ασφάλεια σε άλλης φύσης δίκτυα

Οι επιχειρήσεις σήμερα χρησιμοποιούν διάφορους συνδυασμούς από τείχη προστασίας, κρυπτογραφία, καθώς και μηχανισμούς πιστοποίησης, με σκοπό να δημιουργήσουν Intranets που είναι συνδεδεμένα με το Internet αλλά παράλληλα προστατευμένα από τους κινδύνους αυτού.

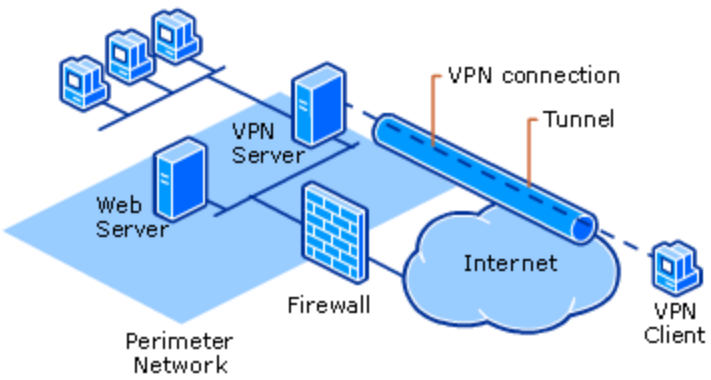
Όπως αναφέρθηκε ως Intranet αναφέρεται το ιδιωτικό εκείνο διαδίκτυο που χρησιμοποιεί πρωτόκολλα του διαδικτύου. Διαφέρουν από τα 'Extranet' για τον λόγο ότι αναφέρονται μόνο στους πρωταρχικούς παράγοντες του περιβάλλοντος μια επιχείρησης η ενός οργανισμού (π.χ. υπάλληλοι), ενώ τα Extranet αναφέρονται και στο καθολικό περιβάλλον που συντελεί τον εκάστοτε φορέα που τα χρησιμοποιεί. Συνεπώς δεν χρειάζεται πρόσβαση σε αυτό από το εσωτερικό περιβάλλον του οργανισμού καθώς η χρήση του Internet είναι αρκετή για την πρόσβαση σε αυτό το τύπο δικτύων. Όταν όμως είναι δυνατή τέτοιου είδους πρόσβαση, γίνεται μέσω ενός gateway με κάποιο firewall, καθώς και άλλους τρόπους ταυτοποίησης η πρόσβασης. Σε αυτή τη περίπτωση γίνεται συχνή χρήση των VPN (Virtual Private Network) δικτύων.

Παρόλο που τα Intranet υπάρχουν για την αποστολή δεδομένων σε ένα ευκόλως διαχειρίσιμο περιβάλλον, τα δεδομένα αυτά μπορεί να βρίσκονται ακόμα σε

κίνδυνο εάν δεν είναι ασφαλισμένα σωστά. Το μειονέκτημα ενός κλειστού δικτύου τύπου 'Intranet' είναι ότι κρίσιμα δεδομένα ίσως να μην μπορούν να φτάσουν σε αυτούς τους οποίους απευθύνονται. Τα Intranet είναι υλοποιημένα μέσα σε οργανισμούς αλλά για περεταίρω διακίνηση δεδομένων μπορούν να χρησιμοποιηθούν τα παρακάτω με σκοπό ένα επαρκές επίπεδο ασφάλειας:

- Firewall που εντοπίζουν και αναφέρουν, περιπτώσεις τυχόν επιθέσεων.
- Έλεγχος για ύπαρξη τυχόν Virus στο εσωτερικό της λειτουργίας του Firewall.
- Αυστηροί κανόνες για το άνοιγμα επισυναπτόμενων e-mail από το υπαλληλικό προσωπικό.
- Κρυπτογράφηση όλων των επικοινωνιών και των διαμοιρασμών δεδομένων.
- Πιστοποίηση από συγχρονισμένες πηγές, σε κωδικούς χρονικής λήξης, συνοδευόμενοι από πιστοποιητικά ασφαλείας.

Αναφέρθηκε ότι εάν το Intranet επιθυμεί πρόσβαση στο Internet, γίνεται χρήση δικτύων τύπου VPN. Intranet που υπάρχουν σε διάφορες γεωγραφικές τοποθεσίες συνήθως χρησιμοποιούν ιδιωτικές συνδέσεις στο διαδίκτυο πάνω στις οποίες μπορεί να λάβει χώρα μια νέα προσέγγιση της χρήσης VPN. Το VPN είναι ένα ιδιωτικό δίκτυο το οποίο χρησιμοποιεί ένα δημόσιο δίκτυο, με σκοπό να συνδέσει μαζί απομακρυσμένους χρήστες η ιστότοπους. Από το να χρησιμοποιηθεί έτσι μια ιδιωτική/μισθωμένη γραμμή δικτύου, αντ' αυτού χρησιμοποιείται μια 'εικονικά' ιδιωτική γραμμή για την σύνδεση σε πραγματικά ιδιωτικά δίκτυα. Στην *εικόνα 4.3.1* παρουσιάζεται σχεδιαστικά η λειτουργία ενός VPN δικτύου.



Εικόνα 4.3.1. Τρόπος λειτουργίας ενός VPN δικτύου. (Πηγή: https://i-technet.sec.s-msft.com/dynimg/IC195069.gif *)*

ΚΕΦΑΛΑΙΟ 5.0: ΔΡΟΜΕΝΑ ΔΙΚΤΥΑΚΗΣ ΑΣΦΑΛΕΙΑΣ & ΣΥΜΠΕΡΑΣΜΟΙ

Το πεδίο της ασφάλειας συνεχίζει την ίδια πορεία με την προγενέστερή του. Οι μεθοδολογίες που χρησιμοποιούνται παραμένουν οι ίδιες, με την μόνη αντίθεση να παρουσιάζεται στην εισαγωγή βιομετρικών τρόπων ταυτοποίησης που σαφώς ενισχύουν τα επίπεδα ασφάλειας λόγω της μοναδικότητάς τους. Νέες τεχνολογίες από την άλλη όπως οι έξυπνες κάρτες (Smart Card) αναδύονται σε ερευνητικό επίπεδο. Ο τομέας του υλικού παρά ταύτα παραμένει άκρως δυναμικός, αφήνοντας έτσι ενδεχόμενα επικείμενων επιθέσεων από μεριάς του.

Η έρευνα που γίνεται έχει ως σκοπό την κατανόηση της τρέχουσας κατάστασης των όλων προαναφερθέντων στα προηγούμενα κεφάλαια, πεδίων και τεχνολογιών.

5.0.1 Εξελίξεις στο Υλικό

Ο τομέας του υλικού δεν γνωρίζει ιδιαίτερη άνθιση. Οι βιομετρικοί μηχανισμοί και οι έξυπνες κάρτες είναι οι μόνες καινοτομίες που επηρεάζουν το παρασκήνιο.

Η πιο προφανής χρήση βιομετρικών ελέγχων ταυτοποίησης, είναι η χρήση αυτών για είσοδο σε σταθμούς εργασίας, πάνω στους οποίους συγκεντρώνεται μεγάλος όγκος διαδικτυακής κίνησης. Καθένας από αυτούς τους σταθμούς εργασίας, χρειάζεται την υποστήριξη από κάποιο ειδικό S/W καθώς και H/W, με σκοπό της ορθή λειτουργία της τεχνολογίας αυτής. Για παράδειγμα βιομετρικοί μηχανισμοί που βασίζονται στην αναγνώριση φωνής, είναι διαθέσιμοι έναντι μικρού αντίτιμου, γεγονός που μπορεί να κάνει την εξάπλωση τους εφικτή ακόμα και σε επιχειρήσεις ή οργανισμούς χαμηλού προϋπολογισμού.

Στόχος των βιομετρικών συστημάτων είναι να αντικαταστήσουν τα παρόντα συστήματα στα οποία η είσοδος είναι εφικτή απλά με την χρήση ενός password. Αυτό συμβαίνει γιατί για να διατηρηθεί η ακεραιότητα ενός κωδικού, πρέπει να τηρηθούν ενέργειες, που πολλές φορές δεν είναι εφικτές λόγω έλλειψης τεχνογνωσίας η χρηματικών απολαβών του εκάστοτε ενδιαφερόμενου.

Οι έξυπνες κάρτες είναι μέσα ψηφιακής αποθήκευσης κρυπτογραφικών κλειδιών και άλλων μέσων, απαραίτητων για μια διαδικασία online ταυτοποίησης. Η κύρια ιδέα που τις απαρτίζει είναι ότι παρέχουν αδιάψευστη συνθήκη ταυτοποίησης για την ηλεκτρονική περσόνα ενός χρήστη. Επίσης μηχανισμοί ασφάλειας τις προστατεύουν από την χρήση τους από τρίτους, γεγονός που τις καθιστά 'ξεχωριστές' έναντι των μέχρι τώρα φορητών μέσων ταυτοποίησης. Το γεγονός που τις καθιστά τόσο δημοφιλής, είναι ότι η διαδικασία ταυτοποίησης όταν κάποιος την χρησιμοποιήσει, δεν λαμβάνει χώρα μέσω του διαδικτύου, αλλά τοπικά στον εσωτερικό μηχανισμό της κάρτας. Έτσι καθίσταται αδύνατο για κάποιον να τις χρησιμοποιήσει ως στόχο επίθεσης. Αρνητικό χαρακτηριστικό των Smart Card είναι το κόστος. Βιομετρικά συστήματα ταυτοποίησης συνήθως είναι πολύ πιο χρηματικός επιζήμια και παράλληλα ισχυρότερα ως προς την παρεχόμενη ασφάλεια.

5.0.2 Εξελίξεις στο λογισμικό

Όπως έχει ήδη αναφερθεί, ο τομέας του λογισμικού στο περί ου ο λόγος πεδίο της ασφάλειας, είναι αχανής. Περιλαμβάνει μια τεράστια πληθώρα εφαρμογών (firewalls, antivirus, vpn κ.α.) γεγονός που θέτει μη εφικτή την πλήρη μελέτη του τομέα αυτού. Αποτέλεσμα είναι η εξέλιξη του 'λογικού' τομέα να οριοθετείτε. Ο τρόπος λειτουργίας της έχει περιοριστεί. Όταν κάποιο νέο είδος επίθεσης εμφανίζεται, τότε τα Firewall, προσομοιώνουν μέσω κάποιου update, τον τρόπο λειτουργίας τους για να αντιμετωπίσουν την νέα αυτή επίθεση. Το ίδιο συμβαίνει με το κακόβουλο λογισμικό. Μόνο τεχνολογικό επίτευγμα αποτελούν οι αλγόριθμοι που πλέον έχουν γίνει αρκετά περίπλοκοι προς κατανόηση από κάποιον τρίτο. Αυτοί οι αλγόριθμοι είναι και ο τρόπος που προστατεύονται από πλευράς υλικού τα υπολογιστικά συστήματα από το διαδίκτυο. Κάνοντας όμως αναφορά σε μικρουπολιστές και μικρουπολογιστικά συστήματα χαμηλής ισχύς που δεν έχουν την επεξεργαστική ισχύ να υποστηρίξουν τα προγράμματα που συνοδεύουν τους

αλγορίθμους αυτούς, τίθεται το ζήτημα ανάγκης light-weight αλγορίθμων ασφαλείας που δεν υπάρχει σε επαρκή βαθμό στον ερευνητικό τομέα

Αναφορικά με το μέλλον της ασφάλειας, θα μπορούσε να γίνει παρομοίωση αυτού με το ανθρώπινο ανοσοποιητικό σύστημα. Τα συστήματα ασφαλείας δηλαδή καθώς αντιμετωπίζουν μια απειλή, θα προσομοιώνουν την αρχιτεκτονική λειτουργίας τους, με σκοπό να γίνονται άτρωτα από παρόμοιες επιθέσεις. Το αρνητικό που θα μπορούσε να απονεμηθεί, είναι ότι η χρήση βιομετρικών τρόπων ασφαλείας θα έπρεπε να έχει ήδη παγιωθεί σε μεγαλύτερο βαθμό.

5.1 Σύνοψη

Η ηλεκτρονική ασφάλεια αποτελεί έναν τεχνολογικό τομέα που καθώς το Internet αναπτύσσεται, λαμβάνει όλο και περισσότερη προσοχή. Οι απειλές που συναθροίζονται εναντίων αυτής καθώς και τα ηλεκτρονικά πρωτόκολλα, αναλύθηκαν με σκοπό την κατανόηση της αναγκαιότητάς της. Το μεγαλύτερο μέρος της ασφάλειας υλοποιείται από μεριάς λογισμικού. Τεχνολογίες υλικού είναι επίσης διαθέσιμες αλλά όχι ευρέως καθιερωμένες. Τέλος το πεδίο της έρευνας δεν αποτελεί σημείο αναφοράς.

Η αρχική ιδέα ήταν ότι λόγο της σπουδαιότητας του τομέα αυτού το πεδίο της έρευνας θα γνώριζε ιδιαίτερη άνθιση. Αντίθετα όμως χρησιμοποιήθηκαν υπάρχουσες ιδέες με την προσπάθεια βελτίωσης μερικών από αυτές. Η ενσωματωμένη ασφάλεια που παρέχει το IPv6 πρωτόκολλο, ίσως να επωφελήσει πληθώρα χρηστών. Ο συνδυασμός του πρωτοκόλλου αυτού και διαφόρων 3rd party μηχανισμών ασφαλείας ενδέχεται να τεθεί αποτελεσματικός απέναντι σε επιθέσεις.

Το πεδίο της διαδικτυακής ασφάλειας χρειάζεται να αναπτυχθεί ραγδαία σε σχέση με τους τώρα ρυθμούς, με σκοπό την αποτελεσματική αντιμετώπιση και οχύρωση των διαφόρων υπολογιστικών συστημάτων από επιθέσεις και το κίνδυνο της χρήσης του διαδικτύου.

ΚΕΦΑΛΑΙΟ 6.0 ΕΙΣΑΓΩΓΗ ΣΤΟ KALI LINUX

Το Kali Linux είναι μια διανομή Linux, Debian Based, με στόχο το Penetration Testing και τους Ελέγχους Ασφαλείας. Περιέχει εκατοντάδες εργαλεία τα οποία είναι υλοποιημένα με σκοπό τις διάφορες εργασίες για την ασφάλεια ενός υπολογιστικού συστήματος. Το Kali Linux έχει αναπτυχθεί από την εταιρεία Offensive Security, που αποτελεί κορυφαία εταιρεία εκπαίδευσης σε θέματα ασφάλειας.

Στην πορεία θα αναλυθούν μερικά από τα πιο καθιερωμένα και σημαντικά εργαλεία του Kali Linux. Πριν γίνει αυτό όμως, θα παρουσιαστεί η ερμηνεία κάποιον όρων, που η γνώση αυτών κρίνεται απαραίτητη για περεταίρω μελέτη του συγκεκριμένου γνωστικού αντικειμένου.

System Exploitation: Ο όρος αυτός αναφέρεται στην προσπάθεια εκμετάλλευσης μιας αδυναμίας ενός συστήματος, ενός υπολογιστικού κέντρου, ή κατά επέκταση ενός διαδικτύου. Αυτό σημαίνει ότι τυπικά γίνεται ανίχνευση σε ένα διαδίκτυο με σκοπό την εύρεση ενός υπολογιστικού κόμβου, ο οποίος εμπεριέχει κενά ασφαλείας που μπορούν να εκτεθούν.

Payload: Ο όρος αυτός αναφέρεται σε ένα εισαγμένο κομμάτι κώδικα ή προγράμματος, σε ένα σύστημα το οποίο έχει εκτεθεί.

Shell/Shell session: Ως Shell η Shell session ορίζεται μια ημιμόνιμη σύνδεση μεταξύ δύο συστημάτων, η οποία επιτρέπει την μεταξύ τους επικοινωνία με κείμενο και συνήθως υποστηρίζει εντολές bash.

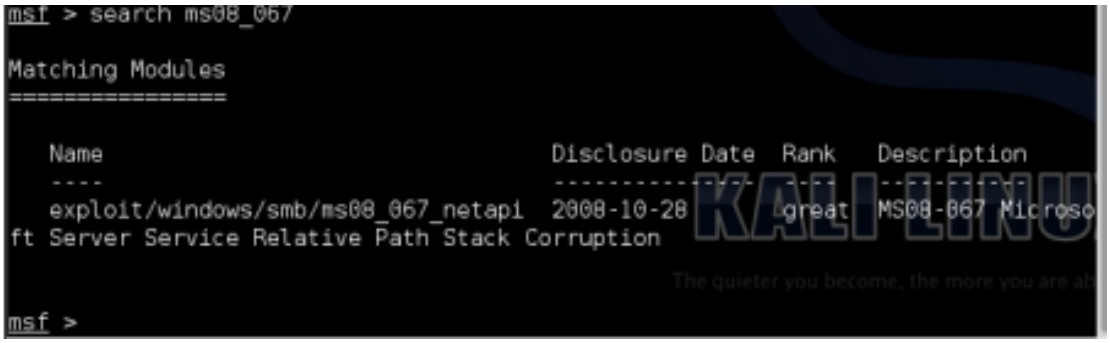
Meterpreter session: Ως Meterpreter Session ορίζεται μια ημιμόνιμη σύνδεση μεταξύ δύο συστημάτων η οποία επιτρέπει την μεταξύ τους επικοινωνία και προκύπτει από την χρήση ενός αντίστοιχου Payload. Αυτού του είδους το Session προσφέρει δυνατότητες πέρα από αυτές ενός απλού Bash Shell.

6.0.1 Metasploit

Το Metasploit είναι το πιο διαδεδομένο εργαλείο στον τομέα του penetration testing, διαθέτοντας μια τεράστια βιβλιοθήκη από προγράμματα τα οποία έχουν δημιουργηθεί για την εκμετάλλευση ήδη γνωστών τρυπών σε συστήματα και τα οποία μπορούν να παραμετροποιηθούν ανάλογα με την εκάστοτε περίπτωση.

Το Metasploit έχει συγγραφεί στην γλώσσα προγραμματισμού Ruby και αποτελεί περιβάλλον ανοιχτού κώδικα για Penetration Testing, IDS Signature Development και Exlpoit Research και αποτελείται από Web Server, Τερματικό και Signatures. Κύριο χαρακτηριστικό πλεονέκτημά του είναι η ευελιξία που αυτό παρέχει. Το ShellCode που περιλαμβάνεται, είναι ένα αρχείο από Payloads τα οποία έχουν δημιουργηθεί και είναι έτοιμα για χρήση μέσα στο Metasploit. Υπάρχει πληθώρα έτοιμων Payload για όλα τα πιο λειτουργικά συστήματα όπως Windows, Mac OS X, Solaris, Linux, BSDi και BSD.

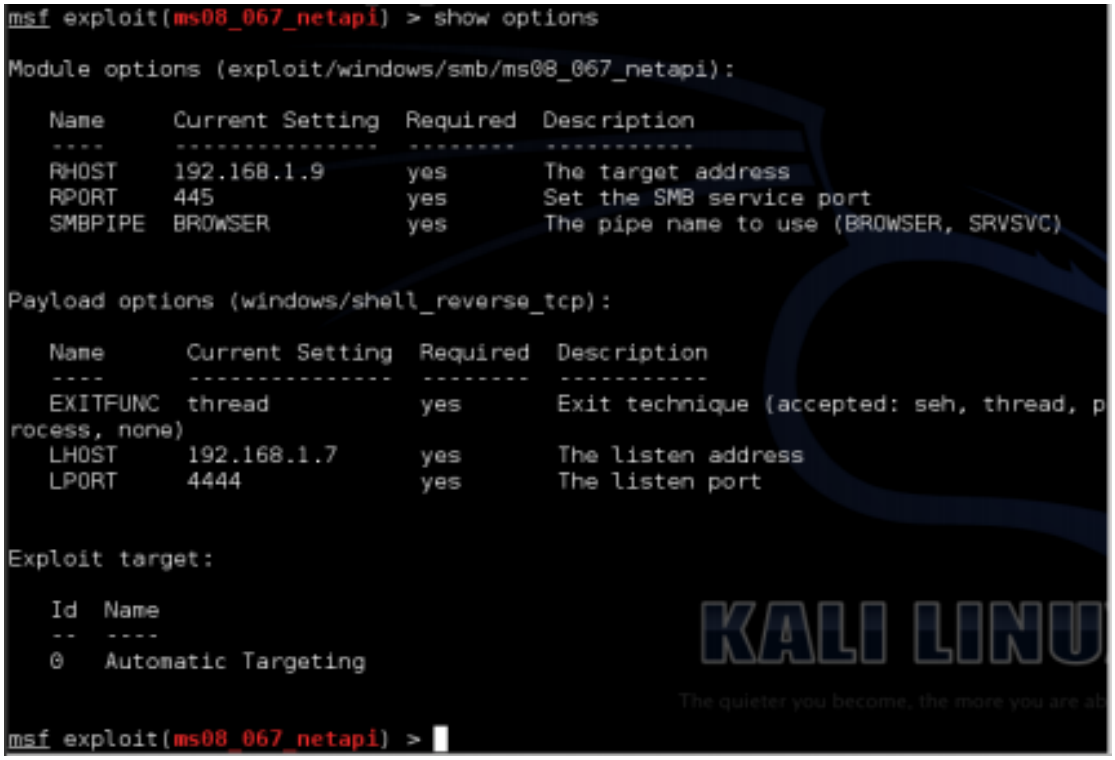
Ένα παράδειγμα χρήσης του Metasploit, είναι η εκμετάλλευση μια γνωστής ατέλειας στο λειτουργικό σύστημα Windows XP, που ενημερώθηκε στο Microsoft Security Bulletin MS08-067. Η τρύπα αυτή βρισκόταν στο netapi32.dll και επέτρεπε σε κάποιον χρησιμοποιώντας ένα remote procedure call request μέσω του SMB (Server Message Block) να καταλάβει στο σύστημα. [6] Όπως φάινεται στην *εικόνα 6.0.1.1,* με χρήση της εντολής Search μπορεί να βρεθεί ποιο module αντιστοιχεί στην συγκεκριμένη τρύπα.



Εικόνα 6.0.1.1. Metasploit search.

Στην συνέχεια γίνεται εκτέλεση της εντολής ‘use’ για να επιλεγεί το module. Με την εντολή ‘show options’ παρουσιάζονται στην *εικόνα 6.0.1.2* οι παραμέτροι που χρειάζονται για να εκτελεστεί το module και στη συνέχεια γίνεται συνήθως συμπλήρωση αυτών με την εντολή ‘set’. Το μόνο που απομένει είναι να γίνει εκτέλεση της εντολής exploit, έτσι ώστε να εκτελεστεί το module (*εικόνα 6.0.1.3*)

Στην *εικόνα 6.0.1.3* εμφανίζεται επίσης η εντολή 'set payload'. Η εντολή αυτή δίνει το έναυσμα στο module για το τι να κάνει μόλις αποκτήσει πρόσβαση στο σύστημα. Στο συγκεκριμένο παράδειγμα εκτελείται το άνοιγμα ενός command shell χρησιμοποιώντας μια σύνδεση reverse tcp. Έτσι φαίνεται ότι μόλις το module εκτελεστεί και καταφέρει να καταλάβει το σύστημα των Windows, ανοίγει αυτόματα ένα command shell που ο 'tester' μπορεί να εκμεταλλευτεί.



Εικόνα 6.0.1.2. Εκτέλεση εντολής 'show options'

Εικόνα 6.0.1.3 Εντολές set 'payload'/'exploit'

6.0.2 Wireshark

Το Wireshark είναι ένας αναλυτής πρωτοκόλλων. Επιτρέπει στο χρήστη αυτού να δει τι συμβαίνει στο δίκτυό του μέχρι και σε απόλυτα χαμηλό επίπεδο. Τα βασικά χαρακτηριστικά αυτού είναι:

• Εις βάθος ανάλυση πρωτοκόλλων διαδικτυακής επικοινωνίας.

• Ζωντανή καταγραφή και ανάλυση.

• Multi-Platform Support.

• Τα καταγραφέντα δεδομένα μπορούν να προβληθούν με τη χρήση ενός GUI.

• Ίσως τα πιο ισχυρά φίλτρα οπτικοποίησης από τους ανταγωνιστές του.

• Ανάλυση VoIP.

• Εγγραφή και ανάγνωση σχεδόν όλων των γνωστών file format.

• Ανάγνωση on-the-fly δεδομένων από Ethernet, IEEE 802.11, PPP/HDLC, ATM, Blueatooth, USB, Token Ring, Frame Relay, FDDI κ.α.

• Μηχανισμοί αποκρυπτογράφησης.

• Εξαγωγή δεδομένων σε μορφές όπως XML, PostScript, CSV.

6.0.3 NMap

Το NMap έχει ως στόχο την ανάλυση ενός δικτύου σε hosts και services με σκοπό την κατασκευή ενός ‘χάρτη’ για αυτό. Για την λειτουργία αυτή το NMap αποστέλει ειδικά πακέτα στους στόχους του και έπειτα αναλύει τις απαντήσεις.

Το λογισμικό του παρέχει μια πληθώρα από εργαλεία για διερεύνηση των χαρακτηριστικών ενός διαδικτύου, συμπεριλαμβανομένου του λειτουργικού συστήματος του Target. Η λειτουργία αυτών των εργαλείων μπορεί να επεκταθεί με την χρήση scripts και να παρέχει περαιτέρω λειτουργείες, όπως η ανίχνευση τρωτών σημείων, επιπλέον services που είναι κρυμμένα μέσα στον host κ.α.

6.0.4 AirCrack-NG

Το AirCrack-NG είναι μια πλήρης σουίτα εργαλείων για πρόσβαση σε WiFi δίκτυα. Όλα τα εργαλεία του είναι γραμμής εντολών, γεγονός που καθιστά δυνατή

την επέκταση των δυνατοτήτων του μέσω script. Στοχεύει σε μια πληθώρα των συντελεστών της ασύρματης ασφάλειας όπως:

• Monitoring: Καταγραφή πακέτων και εξαγωγή των δεδομένων αυτών για περετέρω ανάλυση από 3rd party tools.

• Attacking: Κατά εξακολούθηση επιθέσεις, αποταυτοποίηση, ψευδή σημεία πρόσβασης κ.α.

• Testing: Έλεγχος καρτών WiFi και Driver αυτών.

• Cracking: WEP και WPA PSK

6.1 Σύνοψη

Όπως ήδη αναφέρθηκε τα εργαλεία τα οποία εμπεριέχονται στο Kali Linux είναι μερικές εκατοντάδες και θα ήταν απίθανο να γίνει αναφορά σε όλα στην παρούσα προσέγγιση. Παρόλα αυτά τα σημαντικότερα από αυτά και συνοπτικά ο τρόπος λειτουργίας τους αναφέρεται παραπάνω.

Το Kali Linux, δεν αποτελεί μοναδικό ισχυρό εργαλείο για penetration testing. Για να κάνει σωστό έλεγχο κανείς για επιθέσεις, θα χρειαστεί πληθώρα λειτουργικών και προγραμμάτων, τα οποία να είναι γραμμένα και υλοποιημένα σε διαφορετικές γλώσσες, με σκοπό να εκμεταλλευτεί τα πλεονεκτήματα και τα μειονεκτήματα των εκάστοτε compiler.

Τέλος γίνεται ακόμα μια φορά ξεκάθαρο ότι η παρούσα προσέγγιση δεν αποτελεί εναρκτήριο λάκτισμα για penetration testing. Το penetration testing γίνεται σε authorized servers. Όταν δεν υπάρχει άδεια από τον κάτοχο του server, τότε αυτή η ενέργεια αποτελεί ηλεκτρονικό έγκλημα και στις περισσότερες χώρες διώκεται ποινικά.

Ο συγγραφές του παρόντος δεν φέρει καμία ευθύνη για ενέργειες εμπνευσμένες από την παρούσα αναφορά.

ΒΙΒΛΙΟΓΡΑΦΙΑ

Βιβλία:

[b.1] ‘The Hacker Playbook: Practical Guide To penetration Testing’, March 13, 2014, Author: Peter Kim

[b.2] ‘Metasploit: The Penetration Tester’s Guide’, Book by David M. Kennedy and Mati Aharoni

Δημοσιεύσεις:

[δ.1] Network Security: History, Importance, and Future. University of Florida Department of Elecrical and Computer Engineering. Bhavya Daya. Web.mit.edu/~bdaya/www/Network%20Security.pdf

URLs:

[1] https://en.wikipedia.org/wiki/Enigma_machine

[2] https://www.helpnetsecurity.com/2002/04/08/the-history-of-hacking/,

[3] https://en.wikipedia.org/wiki/IPv4

[4] https://en.wikipedia.org/wiki/IPv6

[5] https://technet.microsoft.com/en-us/library/cc959354.aspx

[6] https://support.microsoft.com/en-us/kb/958644

[7] https://www.wireshark.org/about.html

[8] https://en.wikipedia.org/wiki/Nmap

Αναφορές:

[α.1] Kartalopoulos, S. V., "Differentiating Data Security and Network Security," Communications, 2008. ICC '08.IEEE International Conference on, pp.1469-1473, 19-23 May 2008

[α.2] “Improving Security,” http://www.cert.org/tech_tips, 2006.

[α.3]“Internet History Timeline, ”www3.baylor.edu/~Sharon_P_Johnson/etg/inthistory.h tm

[α.4] Warfield M., “Security Implications of IPv6,” Internet Security Systems White Paper, documents.iss.net/whitepapers/IPv6.pdf “Internet History Timeline,” www3.baylor.edu/~Sharon_P_Johnson/etg/inthistory.h tm

[α.5] "Virtual private network." Wikipedia, The Free Encyclopedia. 30 Jun 2008, 19:32 UTC. Wikimedia Foundation, Inc. 2 Jul 2008 <http://en.wikipedia.org/w/index.php?title=Virtual_private_network&oldid=222715612>

Πρότυπα:

[π.1] Metasploit, y Rahul Bhutkar & Nikhil Birari, http://www.slideshare.net/devilback/finalppt-metasploit