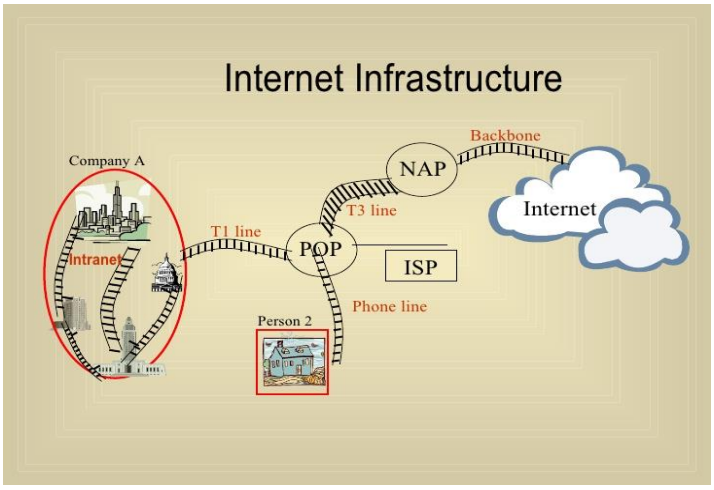
ΤΕΙ ΠΕΛΟΠΟΝΝΗΣΟΥ-ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

«Ανάλυση ασφάλειας και απειλών σε υποδομή Internet και καλές πρακτικές»



ΟΝΟΜΑΤΕΠΩΝΥΜΟ ΦΟΙΤΗΤΗ: ΦΙΛΙΠΠΟΣ ΤΣΟΛΑΚΟΣ

ΕΠΙΒΛΕΠΩΝ ΚΑΘΗΓΗΤΗΣ: ΙΩΑΝΝΗΣ ΠΙΚΡΑΜΜΕΝΟΣ

ΠΕΡΙΛΗΨΗ

Η υποδομή του Διαδικτύου στηρίζει την παγκόσμια ανταλλαγή πληροφοριών μέσω των φυσικών και λογικών αγαθών, όπως καλώδια, servers, πρωτόκολλα, υπηρεσίες. Αυτά τα αγαθά υποφέρουν από διάφορες απειλές που μπορούν να παρεμποδίσουν τη σύνδεση του δικτύου και να διαταράξουν το Διαδίκτυο.

Στο τοπίο των απειλών, η μελέτη αυτή δίνει μια λεπτομερή επισκόπηση των υφιστάμενων απειλών για την υποδομή του Διαδικτύου και τις τάσεις τους, έτσι ώστε οι ιδιοκτήτες των υποδομών του Διαδικτύου μπορούν να βελτιώσουν την ασφάλειά τους, χρησιμοποιώντας ορθές πρακτικές.

Για το σκοπό αυτό, η μελέτη αυτή αναλύει τα αγαθά της υποδομής του Διαδικτύου (διαρθρώνεται σε οκτώ κατηγορίες: υλικό, λογισμικό, πληροφορίες, το ανθρώπινο δυναμικό, τα πρωτόκολλα, τις υπηρεσίες, τις διασυνδέσεις, και υποδομές) και τον κατάλογο των απειλών που ισχύουν για αυτά τα αγαθά της υποδομής του Διαδικτύου. Τα αποτελέσματα αυτά διαρθρώνονται σε mindmaps. Η μελέτη στη συνέχεια ταξινομεί Σημαντικές συγκεκριμένες απειλές της υποδομής του Διαδικτύου - δηλαδή απειλές δρομολόγησης, οι DNS απειλές, άρνηση παροχής υπηρεσιών, καθώς και γενικές απειλές - και συνδέει κάθε απειλή με έναν κατάλογο των αγαθών που εκτίθενται.

Στον οδηγό ορθής πρακτικής, η μελέτη αναλύει έναν κατάλογο καλών πρακτικών που στοχεύουν στην εξασφάλιση ενός αγαθού υποδομής του Διαδικτύου από Σημαντικό συγκεκριμένες απειλές. Μια ανάλυση των ελλείψεων αναγνωρίζει ότι ορισμένα αγαθά δεν καλύπτονται από τις τρέχουσες καλές πρακτικές: το ανθρώπινο δυναμικό (διαχειριστές και φορείς) για την δρομολόγηση, DNS και Denial of Service, καθώς και διαμόρφωση του συστήματος και EssentialAddressingProtocols για Denial of Service.

Αυτή η μελέτη παρέχει στους ιδιοκτήτες των υποδομών του Διαδικτύου έναν οδηγό για την αξιολόγηση των απειλών που ισχύουν για τα αγαθά τους. Προτείνει, επίσης, συστάσεις για τη βελτίωση της ασφάλειας των υποδομών του Διαδικτύου.

Πίνακας περιεχομένων

ΕΙΣΑΓΩΓΗ

Το Διαδίκτυο, ως ένα δίκτυο ανεξάρτητων δικτύων υπολογιστών, έχει εξελιχθεί σε μια σημαντική παγκόσμια πλατφόρμα εμπορικού και ιδιωτικού συμφέροντος, καθώς και για την ηλεκτρονική διακυβέρνηση και τις δημόσιες υπηρεσίες για την κοινωνία μας, καθιστώντας έτσι μέχρι σήμερα ένα απαραίτητο εργαλείο για όλους τους τομείς της ζωής. Ως ένα πολύπλοκο σύστημα, αυτό εξαρτάται σε μεγάλο βαθμό από διάφορα εξαρτήματα, μηχανισμούς και λειτουργίες σε διάφορα επίπεδα αφαίρεσης. Η υποδομή του Διαδικτύου, όπως η υποκείμενη βάση, αποτελείται από υλικό, φυσικής υποδομής, διασύνδεση, το λογισμικό, τα πρωτόκολλα, τις πληροφορίες, τις υπηρεσίες και το ανθρώπινο δυναμικό. Για παράδειγμα, τα δίκτυα (αυτόνομα συστήματα) που συνδέονται με συστατικά των φυσικών στρωμάτων, αλλά αντιμετωπίζονται με λογική διευθυνσιοδότηση συστήματα, που μεταφέρουν δεδομένα μέσω ενός συνόλου πρωτοκόλλων στον επιθυμητό προορισμό, και φορέων μπορούν να κάνουν άλμα σε δράση όταν συμβαίνει κάποιο πρόβλημα. Μια αποτυχία αυτών των βασικών συστατικών δεν προκαλεί μόνο μια διάσπαση ενός δικτύου ή ορισμένων από τους συμμετέχοντες, αλλά μπορεί επίσης να επηρεάσει ένα μεγάλο μέρος του διαδικτύου, μέχρι το σύνολό του.

ΚΕΦΑΛΑΙΟ 1-

1.1. ΕΙΣΑΓΩΓΗ

Το Διαδίκτυο, προσφέρει αναμφισβήτητα στα Πληροφοριακά Συστήματα (ΠΣ) σημαντικές δυνατότητες επεκτασιμότητας, διασυνδεσιμότητας, και ολοκλήρωσης με χαμηλό κόστος και υψηλή αποτελεσματικότητα. Συγχρόνως όμως αυξάνονται τα προβλήματα τα σχετικά με την προστασία και ακεραιότητα των πληροφοριών (Πάγκαλου 2005). Για παράδειγμα παρατηρούμε μεγάλους οργανισμούς, που στην πλειοψηφία τους χρησιμοποιούν ευαίσθητα δεδομένα και υπηρεσίες, να πέφτουν όλο και συχνότερα θύματα παραβιάσεων ασφάλειας (GAO 1996). Οι επιθέσεις μέσω Internet έχουν γίνει ένα σύνηθες φαινόμενο που κάνει πλέον τους χρήστες επιφυλακτικούς όταν συναλλάσσονται μέσω του Διαδικτύου (Gordon, & Loep, 2012).

Η επιστημονική έρευνα στο χώρο της ασφάλειας πληροφοριών στο Διαδίκτυο έχει να παρουσιάσει ένα μεγάλο όγκο εργασιών με ιδιαίτερη έμφαση στην ανάπτυξη τεχνικών και μέσων προστασίας, όπως τεχνικές κρυπτογράφησης, αυθεντικοποίησης, ελέγχου πρόσβασης, ακεραιότητας κ.α. (Houle & Weaver, 2011). Παρά όμως την ανάπτυξη τεχνικών και εργαλείων ασφάλειας Διαδικτύου, η ανασφάλεια δεν φαίνεται να αμβλύνεται. Αντιθέτως, σχετικές μελέτες δείχνουν μια μάλλον ανεπαρκή αντιμετώπιση των κινδύνων της κοινωνίας της πληροφορίας.

Για το 2015 οι έρευνες ότι οι παραβιάσεις ασφαλείας αυξήθηκαν για τέταρτη συνεχή χρονιά κατά 31%. Το 91% των Διαδικτυακών ΠΣ της έρευνας δέχθηκαν παραβίαση ασφαλείας ενώ το 94% μολύνθηκε από ιό μέσω του Διαδικτύου(Tsohou και άλλοι, 2016). Ενδεικτικά καταγράφεται ότι η εμφάνιση του ιού “Melissa” κόστισε 80 εκατομμύρια δολάρια. Δυστυχώς, ένα μικρό ποσοστό των

επιχειρήσεων είχε επενδύσει σε τεχνολογίες και πολιτικές ασφάλειας. Συνεπώς το ζήτημα της ασφάλειας ΠΣ στο Διαδίκτυο παραμένει ένα ανοικτό ζήτημα, παρά την ανάπτυξη των τεχνικών και μέσων προστασίας. Σήμερα ο μεγαλύτερος όγκος πληροφοριών που διακινούνται στο Διαδίκτυο έχει τη μορφή ημιδομημένων (XML) δεδομένων, και αρκετοί ερευνητές βλέπουν πλέον το Web ως μια γιγαντιαία κατανεμημένη Βάση Δεδομένων (Ozsu 2009). Επιπλέον, η δυναμική εμφάνιση των XML δεδομένων, δίνει νέες προοπτικές στην μεταφορά και παρουσίαση πληροφοριών στο Διαδίκτυο και στην ενοποίηση ΠΣ.Η έλλειψη όμως Συστημάτων Διοίκησης XML δεδομένων καθιστούν' το πρόβλημα της ασφάλειάς τους κρίσιμο και αποφασιστικό για την διάδοση της XML τεχνολογίας(Jouinia et al, 2010)

Συνοψίζοντας, αφορμή για την παρούσα έρευνα αποτέλεσαν οι εξής διαπιστώσεις(Yang 2007):

• Η έλλειψη ασφάλειας στο Διαδίκτυο οδηγεί τους χρήστες σε επιφυλακτικότητα με συνέπεια την επιβράδυνση του ρυθμού ανάπτυξης χρήσης του Internet

. • Ενώ υπάρχει πληθώρα μηχανισμών και τεχνολογιών ασφάλειας τα Διαδικτυακά πληροφοριακά συστήματα καθώς και οι χρήστες τους, παραμένουν ευάλωτοι στους κινδύνους της κοινωνίας της πληροφορίας.

• Δεδομένου ότι αρκετοί μεγάλοι οργανισμοί διαθέτουν τεχνολογίες ασφάλειας όπως π.χ. Firewall, είναι απαραίτητο να μελετηθεί πως οι τεχνολογίες αυτές μπορούν να επηρεάσουν τον ορισμό πολιτικών ασφάλειας.

• Ενώ τα θέματα ασφάλειας των καθιερωμένων δεδομένων, όπως είναι τα σχεσιακά, τα ονποκεντρικά και τα υπερκείμενα δεδομένα, έχουν' μελετηθεί επαρκώς από την επιστημονική κοινότητα δεν συμβαίνει το ίδιο με τα Ημιδομημένα - XML δεδομένα.

Όπως έχει ορισθεί στο Trusted Computer System Evaluation Criteria, του υπουργείου Αμυνας των ΗΠΑ (DoD 1985): «Πολιτική Ασφάλειας είναι το σύνολο νόμων, κανόνων και πρακτικών που ρυθμίζουν πως ένας οργανισμός διαχειρίζεται, προστατεύει και κατανέμει ευαίσθητες πληροφορίες». Στον τομέα της ασφάλειας Π.Σ. μπορούμε να ξεχωρίσουμε τέσσερις κύριες προσεγγίσεις:

• την τεχνολογική η οποία δίνει έμφαση στα τεχνικά στοιχεία του ΠΣ. όπως είναι το υλικό, το λογισμικό και τα δεδομένα

• την ανθρωποκεντρική και κοινωνικο-τεχνική η οποία δίνει έμφαση στον άνθρωπο και στην κοινωνική διάσταση του ζητήματος της ασφάλειας.

• τη συστηματική η οποία προσδιορίζει καλά ορισμένα στάδια και βήματα τα οποία ακολουθούνται σειριακά.

• και τη συστημική η οποία αντιμετωπίζει το πρόβλημα της ασφάλειας ως ένα πρόβλημα συστήματος προς αντιμετώπιση. Η συστηματική σε συνδυασμό με την τεχνολογική προσέγγιση οδηγούν σε τεχνικές λύσεις και οδηγίες ασφάλειας και δίνουν τη δυνατότητα στους οργανισμούς να τις κατανοήσουν και να τις υλοποιήσουν' εύκολα.

Η μεθοδολογία που ακολουθούμε για την ανάπτυξη πολιτικής ασφάλειας Διαδικτυακών ΠΣ, έχει τα χαρακτηριστικά της συστηματικής και τεχνολογικής προσέγγισης, και συνίσταται:

• Στην οριοθέτηση αρχικά του προβλήματος και των χαρακτηριστικών της ασφάλειας στο περιβάλλον του Διαδικτύου,

• Στην αξιολόγηση του υφιστάμενου πλαισίου μηχανισμών και των διαθέσιμων τεχνολογιών ασφάλειας

• Στον προσδιορισμό ενός μεθοδολογικού πλαισίου για την ανάπτυξη πολιτικών ασφάλειας στο Διαδίκτυο.

Πιο συγκεκριμένα στις ενότητες που ακολουθούν ορίζουμε για το περιβάλλον του Διαδικτύου(Kevin et al, 2011):

- Το πρόβλημα της ασφάλειας (security problem)
- Τις απαιτήσεις (requirements) ασφαλείας
- Τις απειλές (threats) κατά της ασφάλειας
- Την ανάλυση επικινδυνότητας (risk analysis)

1.2. Το πρόβλημα της ασφάλειας σε περιβάλλον Internet

Το Internet, ξεκίνησε, σχεδιάστηκε, αναπτύχθηκε και υποστηρίχθηκε από την ακαδημαϊκή κοινότητα για την κάλυψη των αναγκών της, υλοποιώντας μία αξιοζήλευτη παγκόσμια υποδομή. Το 1967, ο οργανισμός ARPA (Advanced Research Projects Agency) ξεκίνησε μία ερευνητική δραστηριότητα με τα δίκτυα μεταγωγής δεδομένων, τα λεγάμενα Packed Switched Networks. Η τεχνική στα δίκτυα τέτοιας μορφής, βασίζεται στο τεμαχισμό σε πακέτα των δεδομένων που πρόκειται να μεταφερθούν, στη μετάδοση τους από κόμβο σε κόμβο και στην επανασυναρμολόγηση των πακέτων στο προορισμό τους (Dagon et al, 2007)

Η πρώτη αυτή ερευνητική προσπάθεια είχε ως αποτέλεσμα τη δημιουργία του περίφημου δικτύου ARPAnet, αρχικός στόχος του οποίου ήταν η κάλυψη των ερευνητικών αναγκών πανεπιστημιακών χρηστών του, για την αποτελεσματική λειτουργία και τη μεγίστη εκμετάλλευση των μεγάλων Η/Υ εκείνης της εποχής. Το ARPAnet, δηλαδή, εξυπηρέτησε την ιδέα του διαμοιρασμού πόρων (resource sharing). Με το πέρασμα του χρόνου, οι δημιουργοί του ARPAnet θέλησαν' να το διασυνδέσουν με τα άλλα υπάρχοντα δίκτυα, ενώ και το Πεντάγωνο επιθυμούσε τη

δημιουργία ενός δικτύου, το οποίο να μην αχρηστευόταν όταν ένας ή περισσότεροι κόμβοι έπεφταν και τίθονταν εκτός λειτουργίας, σκεπτόμενοι βέβαια το ενδεχόμενο πολέμου. Η ιδέα πίσω από αυτό ήταν η δημιουργία ενός διαδικτύου χωρίς κεντρική διαχείριση, στο οποίο ο χρήστης θα μπορούσε να έχει πρόσβαση από πολλούς διαφορετικούς κόμβους και μέσω, διαφορετικής εάν το επιθυμούσε, διαδρομής των πακέτων πληροφοριών του.

Έτσι, περίπου το 1980, συνδέθηκαν τα πρώτα δίκτυα υπολογιστών (πανεπιστημιακά στην πλειοψηφία τους), τα οποία χρησιμοποιούσαν το πρωτόκολλο TCP/IP, για να αποτελέσουν τα πρώτα στάδια ενός δικτύου που ονομάστηκε Internet ή ARPA Internet και το οποίο ακολουθώντας ραγδαίους ρυθμούς ανάπτυξης, αποτελεί σήμερα το γνωστό μας Διαδίκτυο. Το 1983, το TCP/IP έγινε το υποχρεωτικό πρωτόκολλο του Internet, δίνοντας τη δυνατότητα σε κάθε χρήστη να βλέπει με ομοιόμορφο τρόπο το Internet και τους διασυνδεδεμενους υπολογιστές του, ανεξάρτητα με το είδος σύνδεσης (ISDN, σειριακή γραμμή, δορυφορική σύνδεση κ.λπ.) (Pfleeger 1997). Το Internet λόγω αυτών των χαρακτηριστικών γνωρισμάτων και πλεονεκτημάτων του γρήγορα άνοιξε τις πύλες του στο ευρύ κοινό, παρέχοντας μεταξύ άλλων τη δυνατότητα εμπορικών συναλλαγών (ηλεκτρονικό εμπόριο) και ανταλλαγής πληροφοριών μέσω από ένα φιλικό προς το χρήστη περιβάλλον.

Η χρήση του Internet προσθέτει όμως επιπλέον απειλές κατά της ασφάλειας των πληροφοριών. Οι χρήστες ανησυχούν για τις απειλές κατά των πληροφοριών που διακινούν στο Internet, και τους κάνει αρκετές φορές επιφυλακτικούς στο να το χρησιμοποιούν' ευρέως για οικονομικές συναλλαγές και για την αποστολή προσωπικών δεδομένων. Επίσης για τις επιχειρήσεις που χρησιμοποιούν το Internet ως επιχειρηματική δραστηριότητα (ηλεκτρονικό εμπόριο) ή ως πλατφόρμα διασύνδεσης (Intranets), η ασφάλεια αποτελεί πρώτη προτεραιότητα

(Γκρίτζαλης, 2004)

Το Internet, προσφέρει αναμφισβήτητα στα Πληροφοριακά Συστήματα (ΠΣ) σημαντικές δυνατότητες διασυνδεσιμότητας. ολοκλήρωσης και επεκτασιμότητας. Αυξάνει όμως σημαντικά τα προβλήματα προστασίας και διαθεσιμότητας των πληροφοριών. Για το λόγο αυτό κάθε ΠΣ που συλλέγει, αποθηκεύει, μεταδίδει πληροφορίες και παρέχει υπηρεσίες μέσω του Διαδικτύου θα πρέπει να εφαρμόζει μια πολιτική ασφάλειας ικανή να εξασφαλίζει την εμπιστευτικότητα (confidentiality), την ακεραιότητα (integrity) και τη διαθεσιμότητα (availability) αυτών. Το θεμελιώδες πρόβλημα της ασφάλειας πληροφοριακών συστημάτων (ΠΣ) στο Internet είναι ότι το Internet σχεδιάστηκε να είναι ένα λειτουργικό περιβάλλον και όχι ασφαλές. (Γκρίτζαλης, 2004)

Τα περισσότερα από τα προβλήματα ασφάλειας στο Internet είναι εγγενή, εκ των' οποίων τα πιο χαρακτηριστικά είναι (Horacek, 2007):

• Εύκολη παρακολούθηση και ανίχνευση. Όλα οι πληροφορίες που κινούνται (με την μορφή πακέτων tcp/ip) μπορούν να παρακολουθηθούν εύκολα χρησιμοποιώντας ευρέως διαθέσιμο ελεύθερο software (π.χ. sniffer, satan). Αυτό είναι πάρα πολύ σημαντικό πρόβλημα μια και η πλειοψηφία των πληροφοριών που ανταλλάσσονται είναι μη κρυπτογραφημένη.

• Ευπαθείς Internet υπηρεσίες. Ένας αριθμός από τέτοιες υπηρεσίες δεν έχουν σχεδιασθεί να είναι ασφαλείς (π.χ. το ping, finger) και αποτελούν εύκολες πόρτες ‘εισόδου’ για εισβολείς.

• Απουσία πολιτικής ασφάλειας. Πολλά Πληροφοριακά Συστήματα στο Internet έχουν σχεδιασθεί να παρέχουν ελεύθερη πρόσβαση χωρίς να λαμβάνεται υπόψη μια πιθανή κατάχρηση των πόρων τους. Επίσης αρκετά επιτρέπουν την χρήση υπηρεσιών (π.χ. anonymous ftp) που δεν είναι απαραίτητες και δεν' περιορίζουν την πρόσβαση στους πόρους τους αφήνοντας έτσι πόρτες ανοιχτές στους εισβολείς.

1.3. Απαιτήσεις Ασφάλειας σε περιβάλλον Internet

Για τη δημιουργία ενός ασφαλούς Internet περιβάλλοντος θα πρέπει να εξασφαλίζονται τα παρακάτω (Γκριτζάλης, 2004):

- Έλεγχος αυθεντικότητας (Authentication).
- Εξουσιοδότηση (Authorization).
- Εμπιστευτικότητα (Confidentiality).
- Ακεραιότητα (Integrity).
- Μη αποποίηση ευθύνης (Non-repudation).
- Διαθεσιμότητα (Availability)

1.3.1. Αναγνώριση και αυθενπκοποίηση:

Η αναγνώριση και η αυθεντικοποίηση είναι η διαδικασία προσδιορισμού μιας οντότητας (χρήστη, εφαρμογής ή Η/Υ) και η απόδειξη της γνησιότητας της ταυτότητας που ισχυρίζεται ότι είναι. Η αυθεντικοποίηση είναι η βασικότερη υπηρεσία ασφάλειας καθώς παρεμποδίζει την εμφάνιση μιας οντότητας ως μια άλλη (impersonation) εξασφαλίζοντας τη γνησιότητα ενός μηνύματος, τη νομιμότητα ενός χρήστη ή αποστολέα και την εγκυρότητα ενός υπολογιστή. Η εφαρμογή της αποτελεί τη βάση για να επιτευχθεί έλεγχος πρόσβασης, εκχώρηση

προνομίων και αρμοδιοτήτων. εφαρμογή συνυπευθυνότητας και πολιτική μη αποποίησης μιας πράξης.

Η αυθεντικοποίηση σε περιβάλλον δικτύων υπολογιστών βασίζεται σε ένα ή περισσότερα από τα παρακάτω τέσσερα κριτήρια (Φωλίνας 2006):

• Από κάτι που κατέχει ο χρήστης (π.χ. έξυπνες κάρτες, κουπόνια)

• Από κάτι που γνωρίζει (π.χ. συνθηματικά, προσωπικοί αριθμοί αναγνώρισης)

• Από προσωπικά χαρακτηριστικά (π.χ. υπογραφή, δακτυλικά αποτυπώματα, αναγνώριση φωνής, χαρακτηριστικά της ίριδας, DNA)

• Από κάτι που προσδιορίζει τη θέση (Internet διεύθυνση, αριθμός τηλεφώνου που χρησιμοποιείται σε ένα σχήμα επανάκλησης) Η απλούστερη μορφή αυθεντικοποίησης βασίζεται στην τεχνική των συνθηματικών (passwords) ενώ οι ισχυρές τεχνικές αυθεντικοποίησης στηρίζονται σε κρυπτογραφικά συστήματα. Στο Internet περιβάλλον η αναγνώριση και ο προσδιορισμός της ταυτότητας ενός χρήστη (ή υπολογιστή) διαφοροποιείται γιατί αρκετές φορές οι συναλλασσόμενες οντότητες δεν γνωρίζονται μεταξύ τους και δεν μπορούν έτσι να αποδείξουν ότι είναι πράγματι αυτές που ισχυρίζονται ότι είναι

Διακρίνουμε τρεις κατηγορίες αυθεντικοποίησης(Μαυρίδη & Πάγκαλου, 2005) :

• Μονόδρομη αυθενπκοποίηση (one-way-authentication) κατά την οποία ο χρήστης δικτύου πρέπει να γνωστοποιήσει την ταυτότητά του στον υπολογιστή που πρέπει να χρησιμοποιήσει, ώστε να του επιτραπεί η προσπέλαση σε αυτόν.

• Αμφίδρομη αυθενπκοποίηση (two-way-authentication), κατά την οποία και ο χρήστης και ο υπολογιστής πρέπει να γνωστοποιήσουν ο ένας στον άλλον τις ταυτότητες τους.

• Αμφίδρομη αυθενπκοποίηση μέσω Τρίτης Έμπιστης Πηγής (Two-way authentication using Trusted Third Party) κατά την οποία μία τρίτη οντότητα, Τρίτη Έμπιστη Πηγή (ΤΕΠ) διευκολύνει τη διαδικασία αυθεντικοποίησης με την παροχή

των αναγκαίων πληροφοριών - πιστοποιητικών για κάθε εμπλεκόμενο χρήστη. Απαραίτητη προϋπόθεση είναι η αποδοχή του από όλα τα εμπλεκόμενα μέρη, καθώς η ΤΕΠ κατέχει και διαχειρίζεται πληροφορίες, η αποκάλυψη και τροποποίηση των οποίων συνεπάγεται την υπονόμευση του συστήματος ασφαλείας. (Μαυρίδη & Πάγκαλου, 2005)

1.3.2. Εξουσιοδότηση

Ο έλεγχος προσπέλασης δικτύων υπολογιστών περιλαμβάνει όλους τους τυπικούς μηχανισμούς ελέγχου που διατίθενται από τα λειτουργικά συστήματα και τα συστήματα βάσεων δεδομένων καθώς και τις επεκτάσεις των ελέγχων' αυτών για την' προστασία των συνδέσεων μεταξύ των κόμβων ενός δικτύου και των δεδομένων που διακινούνται μέσο) αυτών. Οι έλεγχοι προσπέλασης στα δεδομένα και τους υπολογιστικούς πόρους του δικτύου πρέπει να περιλαμβάνουν κάποια διαδικασία αυθεντικοποίησης του χρήστη (απλή ή ισχυρή) που καθορίζεται από το επιθυμητό επίπεδο ασφάλειας.

1.3.3. Εμπιστευτικότητα

Εξασφάλιση της εμπιστευτικότητας στο διαδίκτυο σημαίνει ότι οι πληροφορίες που είναι αποθηκευμένες αποκαλύπτονται μόνο σε εξουσιοδοτημένους χρήστες και επιπλέον δεν απειλούνται από μη εξουσιοδοτημένη αποκάλυψη κατά την μεταφορά τους. Η έννοια της εμπιστευτικότητας των δεδομένων που διακινούνται μέσω Internet μπορεί να εφαρμοστεί καθ' ολοκληρία ή σε ένα τμήμα τους Έτσι για παράδειγμα στα μηνύματα ηλεκτρονικού ταχυδρομείου μπορούμε να προστατέψουμε μόνο το περιεχόμενό τους και όχι τα χαρακτηριστικά τους. Η επιβολή της εμπιστευτικότητας

στο Internet γίνεται μέσα από πολιτικές ελέγχου πρόσβασης (Access Control Policies) σε συνδυασμό με την χρήση κρυπτογραφίας και τεχνολογιών Εικονικών Ιδιωτικών Δικτύων(Dagon et al, 2007).

1.3.4. Ακεραιότητα

Εξασφάλιση της ακεραιότητας δεδομένων στο Internet σημαίνει ότι δεν έχουμε μετατροπή, διαγραφή και δημιουργία δεδομένων από μη εξουσιοδοτημένους χρήστες (ή με παράνομο τρόπο) κατά την μεταφορά τους ή την αποθήκευσή τους . Στο Internet είναι σημαντικό για παράδειγμα ο παραλήπτης ενός μηνύματος να είναι σίγουρος ότι το μήνυμα που έλαβε δεν έχει παραποιηθεί κατά την μεταφορά του. Ο μηχανισμός που χρησιμοποιείται ευρέως για την εξασφάλιση της ακεραιότητας των δεδομένων κατά την μεταφορά τους είναι οι ψηφιακές υπογραφές και μπορεί να εφαρμοστεί είτε σε ολόκληρο το μήνυμα είτε σε επιλεγμένα τμήματά του.

Ενώ τα Λειτουργικά Συστήματα και τα Συστήματα Βάσεων Δεδομένων είναι υπεύθυνα για την ακεραιότητα των δεδομένων κατά την αποθήκευση τους

1.3.5. Μη αποποίηση ευθύνης

Επιπλέον της αυθεντικοποίησης ενός χρήστη και της ακεραιότητας των δεδομένων που διαιανούνται σε ένα δίκτυο υπολογιστών συχνά απαιτείται ο καταλογισμός της ευθύνης για την αποστολή ή παραλαβή δεδομένων [Bhimani 1996]. Δηλαδή για παράδειγμα στην περίπτωση του ηλεκτρονικού ταχυδρομείου, είναι απαραίτητο σε ορισμένες περιπτώσεις ο αποστολέας ή ο παραλήπτης ενός μηνύματος να μη μπορεί να απαρνηθεί τη ευθύνη αποστολής/ παραλαβής του συγκεκριμένου μηνύματος. Ένας μηχανισμός αντιμετώπισης του προβλήματος

αυτού είναι η χρήση ψηφιακής υπογραφής σε συνδυασμό με την ύπαρξη μιας Τρίτης Έμπιστης Πηγής (trusted third party)

1.3.6. Διαθεσιμότητα

Με την διασφάλιση της διαθεσιμότητας οι υπηρεσίες είναι διαθέσιμες και χωρίς καθυστέρηση στις εξουσιοδοτημένες οντότητες. Έτσι οι εξουσιοδοτημένοι χρήστες δεν πρέπει να αντιμετωπίζουν προβλήματα άρνησης εξυπηρέτησης (denial of service) όταν επιθυμούν να προσπελάσουν τις υπηρεσίες και τους πόρους που έχουν δικαίωμα. Η διαθεσιμότητα υπηρεσιών και πόρων σε περιβάλλον Internet απειλείται από την εξαπόλυση επιθέσεων τύπου 'πλημμύρας' (SYN). Στόχος της επίθεσης αποτελεί ο εξυπηρετητής - παροχέας των υπηρεσιών (π.χ. ο mail ή ο Web server) και η μέθοδος που ακολουθείται είναι ο βομβαρδισμός τους (απευθείας ή αναμετάδοση) με τεράστιο όγκο πληροφοριών που το καθιστούν εκτός λειτουργίας (Neumann 2000).

Η εξασφάλιση της διαθεσιμότητας είναι ζωτικής σημασίας για τις επιχειρήσεις που πραγματοποιούν ηλεκτρονικές συναλλαγές και αποτελεί τον κύριο λόγο εφαρμογής αντιμέτρων ασφάλειας από τους οργανισμούς που δραστηριοποιούνται στο Internet.Αν και πολλές από τις παραπάνω υπηρεσίες μπορούν να παρέχονται στα περισσότερα από τα επτά επίπεδα του μοντέλου αναφοράς OSI, υποστηρίζεται ότι οι υπηρεσίες αυτές είναι πιο λειτουργικό να παρέχονται στο επίπεδο εφαρμογής

1.4. Απειλές κατά της ασφάλειας σε Internet περιβάλλον

Με τον όρο απειλή κατά της ασφάλειας ενός Υπολογιστικού Συστήματος ορίζεται η πιθανή εκμετάλλευση μιας ευπάθειας του συστήματος με δυνητικό κίνδυνο την μη εξουσιοδοτημένη πρόσβαση, την αποκάλυψη πληροφοριών, την χρήση, την κλοπή ή την καταστροφή των πόρων του συστήματος. Το Internet, προσφέρει αναμφισβήτητα σημαντικά πλεονεκτήματα και δυνατότητες, αυξάνει όμως επίσης σημαντικά τα προβλήματα προστασίας και διαθεσιμότητας των πληροφοριών. Υπάρχουν τρεις κύριες περιοχές απειλών κατά της ασφάλειας πληροφοριών στο Internet (Γκριτζάλης, 2004)::

• Αποθήκευση, αναφέρεται στην προστασία των φυσικών θέσεων αποθήκευσης δεδομένων, οι οποίες μπορεί να είναι κατανεμημένες στο διαδίκτυο.
• Πρόσβαση, αφορά τον έλεγχο πρόσβασης (authorization) των χρηστών στους πόρους του Πληροφοριακού Συστήματος (δεδομένα και συστήματα Η/Υ) και τον προσδιορισμό της ταυτότητας του χρήστη.

• Μεταφορά, συσχετίζεται με την προστασία των δεδομένων κατά την μεταφορά τους μέσα από το διαδίκτυο. Πιο αναλυτικά οι σημαντικότερες απειλές, που πρέπει να εξετάσουμε προκειμένου να αναπτύξουμε ένα ασφαλές περιβάλλον στο διαδίκτυο, παρουσιάζονται εν συντομία παρακάτω (Γκριτζάλης, 2004):

• Ανεπάρκεια πόρων του ΠΣ (Component Failure). Έχει να κάνει με κακή σχεδίαση hardware/software του ΠΣ με αποτέλεσμα την άρνηση εξυπηρέτησης (denial of service). Χαρακτηριστικά παραδείγματα αυτής της απειλής είναι η άρνηση εξυπηρέτησης ενός Web ή ftp server εξαιτίας της συμπλήρωσης των επιτρεπόμενων χρηστών.

• Παρακολούθηση των καναλιών επικοινωνίας (Monitoring of communication lines). Με την παρακολούθηση των καναλιών επικοινωνίας οι υποκλοπείς μπορούν να αποκτήσουν' πρόσβαση σε μη εξουσιοδοτημένες πληροφορίες παραβιάζοντας έτσι την ιδιωτικότητα (privacy).

• Πρόβλεψη του κοινού κλειδιού (shared key guessing). Εάν κάποιος καταφέρει να ανακαλύψει το κοινό κλειδί μιας συμμετρικής κρυπτογραφημένης επικοινωνίας (είναι δυνατόν όταν' το μήκος του κλειδιού είναι μικρότερο από 56 bits) τότε όλη η συνεδρία μπορεί να αποκρυπτογραφηθεί και να υπάρξει κατά συνέπεια αποκάλυψη πληροφοριών.

• Υποκλοπή του κοινού κλειδιού (shared key stealing) Εάν κάποιος καταφέρει να υποκλέψει το κοινό κλειδί μιας συμμετρικής κρυπτογραφημένης επικοινωνίας, η συγκεκριμένη σύνοδος επικοινωνίας μπορεί να αποκρυπτογραφηθεί

• Μη εξουσιοδοτημένη τροποποίηση των πληροφοριών κατά τη μεταφορά (Unauthorised modification of information in transit). Πληροφορίες μπορούν να τροποποιηθούν κατά τη μεταφορά τους και μάλιστα με τέτοιο τρόπο ώστε ο παραλήπτης να μην αντιληφθεί τις διενεργηθείσες μεταβολές.

• Παραποίηση Internet διεύθυνσης (Forged Internet Addresses). Εάν δύο οντότητες στο Internet εμπιστεύονται η μία την άλλη στο να ανταλλάσσουν δεδομένα τότε είναι δυνατόν μία τρίτη οντότητα παραποιώντας την Internet διεύθυνσή της να προσποιηθεί ότι είναι μια από τις ‘έμπιστες’ οντότητες.

• Μεταμφίεση (Masquerade). Όταν ένας χρήστης υποκρίνεται ότι είναι κάποιος άλλος (τοπικός ή απομακρυσμένος) προκειμένου να αποκτήσει πρόσβαση σε πόρους για τους οποίους δεν' έχει εξουσιοδότηση.

• Κατάχρηση (Misuse). Η χρήση των πόρων για μη εξουσιοδοτημένους σκοπούς. Τέτοιο συνηθισμένο πλέον παράδειγμα είναι η χρήση ακαδημαϊκών Πληροφοριακών Συστημάτων για την εξαπόλυση Internet επιθέσεων.

ΚΕΦΑΛΑΙΟ 2- Η ασφάλεια των δικτύων

Η ασφάλεια δικτύων αποτελεί πλέον αναπόσπαστο κομμάτι της δικτύωσης υπολογιστών. Περιλαμβάνει πρωτόκολλα ,τεχνολογίες, συσκευές, εργαλεία και τεχνικές για την ασφάλεια των δεδομένων και την καταπολέμηση των απειλών. Λύσεις για την ασφάλεια των δικτύων εμφανίστηκαν την δεκαετία του 60 αλλά δεν είχαν "ωριμάσει" μέσα σ'ένα ολοκληρωμένο σύνολο λύσεων για τα σύγχρονα δίκτυα μέχρι και τη δεκαετία του 2000. Η ασφάλεια δικτύων προσπαθεί σε μεγάλο βαθμό να είναι προετοιμασμένη από κακόβουλους hackers. Ακριβώς όπως οι γιατροί επιχειρούν να αποτρέψουν νέες ασθένειες, ενώ θεραπεύουν τα υπάρχοντα προβλήματα, έτσι και οι επαγγελματίες της ασφάλειας δικτύων προσπαθούν να αποτρέψουν πιθανές επιθέσεις με την ελαχιστοποίηση των επιθέσεων σε πραγματικό χρόνο. Η επιχειρησιακή συνέχεια είναι μια άλλη σημαντική κινητήρια δύναμη της ασφάλειας δικτύων. (Wall, 2001)

Δημιουργήθηκαν οργανισμοί της ασφάλειας δικτύων για την θέσπιση επίσημων κοινοτήτων των επαγγελματιών. Αυτοί οι οργανισμοί ορίζουν πρότυπα ,ενθαρρύνουν τη συνεργασία, και παρέχουν ευκαιρίες ανάπτυξης του εργατικού δυναμικού για τους επαγγελματίες. Είναι σημαντικό για τους επαγγελματίες να γνωρίζουν τους πόρους που παρέχονται απ'αυτούς τους οργανισμούς. Η πολυπλοκότητα της ασφάλειας δικτύων καθιστά δύσκολο στο να κυριαρχήσει σε ο,τι το περικλείει. Διάφοροι οργανισμοί έχουν δημιουργήσει τομείς που υποδιαιρούν τον κόσμο της ασφάλειας δικτύων σε πιο εύχρηστα κομμάτια. Αυτός ο διαχωρισμός επιτρέπει στους επαγγελματίες να επικεντρωθούν σε πιο συγκεκριμένους τομείς εμπειρογνωμοσύνης στον τομέα της κατάρτισης τους,την έρευνα και την απασχόληση.

Πολιτικές ασφάλειας δικτύων δημιουργούνται από επιχειρήσεις και κυβερνητικούς οργανισμούς για την παροχή ενός πλαισίου για τους εργαζόμενους, ώστε να το ακολουθήσουν κατά την διάρκεια της εργασίας τους.Οι επαγγελματίες

σε επίπεδο διαχείρισης είναι υπεύθυνοι για τη δημιουργία και τη διατήρηση της πολιτικής για την ασφάλεια δικτύων. Όλες οι πρακτικές ασφάλειας δικτύων συνδέονται και καθοδηγούνται από την πολιτική ασφάλειας δικτύων. Όπως η ασφάλεια δικτύων αποτελείται απο τομείς της ασφάλειας,οι επιθέσεις στο δίκτυο ταξινομούνται έτσι ώστε να είναι πιο εύκολο να μάθουμε γι 'αυτές και να τις αντιμετωπίσουμε κατάλληλα. Ιοί, "σκουλήκια" και Δούρειοι Ιπποι είναι συγκεκριμένοι τύποι επιθέσεων δικτύου.

Γενικότερα, οι επιθέσεις στο δίκτυο ταξινομούνται ως επιθέσεις αναγνώρισης, πρόσβασης ή άρνησης της υπηρεσίας. Η δουλειά ενός επαγγελματία της ασφάλειας δικτύων είναι η αντιμετώπιση αυτών των επιθέσεων.

2.1. ΤΑΞΙΝΟΜΗΣΗ ΕΠΙΘΕΣΕΩΝ ΔΙΚΤΥΩΝ

2.1.1. Worms (Σκουλήκια)

Τον Ιούλιο του 2001 ,το "σκουλήκι" Code Red (Ερυθρός κώδικας) επιτέθηκε σε servers ιστοσελίδων σε παγκόσμιο επίπεδο μολύνοντας πάνω από 350.000 υπολογιστές. Το σκουλήκι δεν διατάρασσε μόνο την πρόσβαση στους μολυσμένους servers, αλλά επηρέαζε επίσης τα τοπικά δίκτυα που φιλοξενούν τους servers, κάνοντας τους αργούς και άχρηστους. (montz, 2002). Το Code Red προκάλεσε άρνηση των υπηρεσιών(DoS) σε εκατομμύρια χρήστες. Αν οι επαγγελματίες της ασφάλειας δικτύων που είναι υπεύθυνοι για τους μολυσμένους servers του Code Red είχαν αναπτύξει και εφαρμόσει μια πολιτική ασφαλείας τα "μπαλώματα" ασφαλείας θα είχαν εφαρμοστεί εγκαίρως. Θα μπορούσαν να το σταματήσουν, ώστε να μείνει απλώς σαν μια υποσημείωση στην ιστορία της ασφάλειας δικτύων. Η ασφάλεια δικτύων σχετίζεται άμεσα με την επιχειρησιακή συνέχεια ενός οργανισμού. Η παραβίασή της μπορεί να διαταράξει το ηλεκτρονικό εμπόριο,, να

προκαλέσει την απώλεια δεδομένων των επιχειρήσεων, να απειλείσει την ιδιωτικότητα των ανθρώπων (με τις πιθανές νομικές συνέπειες)και θέσει σε κίνδυνο την ακεραιότητα των πληροφοριών. Οι παραβιάσεις αυτές μπορούν να οδηγήσουν σε απώλεια εσόδων για τις επιχειρήσεις, σε κλοπή της πνευματικής ιδιοκτησίας ,καθώς και σε αγωγές,και μπορεί ακόμη να απειλήσουν τη δημόσια ασφάλεια.

Η διατήρηση ενός ασφαλούς δικτύου διασφαλίζει την ασφάλεια των χρηστών του δικτύου και προστατεύει τα εμπορικά συμφέροντα. Για την διατήρηση ενός ασφαλές δικτύου απαιτείται επαγρύπνηση από την πλευρά των επαγγελματιών της ασφάλειας δικτύων ενός οργανισμού.Οι επαγγελματίες πρέπει να είναι συνεχώς ενήμεροι για τις νέες και εξελισσόμενες απειλές και επιθέσεις σε δίκτυα και τα τρωτά σημεία των συσκευών και εφαρμογών. Οι πληροφορίες αυτές χρησιμοποιούνται για την προσαρμογή, την ανάπτυξη και την εφαρμογή τεχνικών μετριασμού .Ωστόσο,η ασφάλεια δικτύων είναι τελικά ευθύνη καθενός που την χρησιμοποιεί. Για το λόγο αυτό, είναι δουλειά του επαγγελματία να εξασφαλίσει ότι όλοι οι χρήστες έχουν λάβει εκπαίδευση ευαισθητοποίησης σε θέματα ασφάλειας .Η διατήρηση ενός ασφαλούς, προστατευμένου δικτύου παρέχει ένα πιο σταθερό, λειτουργικό περιβάλλον εργασίας για όλους.

Τα "σκουλήκια" είναι ένα ιδιαίτερα επικίνδυνο είδος εχθρικού κώδικα. Οι ίδιοι αναπαράγονται με ανεξάρτητες ευπάθειες εκμετάλλευσης στα δίκτυα. Τα "σκουλήκια" συνήθως επιβραδύνουν τα δίκτυα. Ενώ ο ιός απαιτεί ένα πρόγραμμα υποδοχής για να τρέξει, τα σκουλήκια μπορούν να τρέξουν από μόνα τους.Δεν απαιτούν τη συμμετοχή των χρηστών και μπορούν να εξαπλωθούν πολύ γρήγορα μέσω του δικτύου. Τα σκουλήκια είναι υπεύθυνα για μερικές από τις πιο καταστροφικές επιθέσεις στο Internet. Για παράδειγμα, το σκουλήκι SQL Slammer από τον Ιανουάριο του 2003 επιβράδυνε την παγκόσμια κίνηση στο Διαδίκτυο με αποτέλεσμα την άρνηση των υπηρεσιών. Πάνω από 250.000 χρήστες επλήγησαν εντός 30 λεπτών από την κυκλοφορία του. Το σκουλήκι εκμεταλλεύτηκε ένα σφάλμα υπερχείλισης στον SQL Server της Microsoft. Ένα patch για αυτήν την

ευπάθεια κυκλοφόρησε στα μέσα του 2002,έτσι ώστε οι διακομιστές που επηρεάστηκαν ήταν εκείνοι που δεν είχαν την ενημερωμένη έκδοση κώδικα που εφαρμόστηκε. Αυτό είναι ένα μεγάλο παράδειγμα γι'αυτό είναι τόσο σημαντικό για την πολιτική ασφάλειας από έναν οργανισμό να απαιτεί έγκαιρες ενημερώσεις και αναβαθμίσεις για τα λειτουργικά συστήματα και τις εφαρμογές.

Παρά τις τεχνικές μετριασμού που προέκυψαν με την πάροδο των ετών,τα σκουλήκια συνεχίζουν να εξελίσσονται με το Διαδίκτυο και εξακολουθούν να αποτελούν απειλή. Ενώ τα σκουλήκια έχουν γίνει πιο εκλεπτυσμένα με το πέρασμα του χρόνου, εξακολουθούν να βασίζονται στην εκμετάλλευση των αδυναμιών σε εφαρμογές λογισμικού. Οι περισσότερες επιθέσεις τύπου "σκουληκιού" έχουν τρία βασικά στοιχεία: Ενεργοποίηση ευπάθειας - 'Ενα worm εγκαθίσταται με τη χρήση ενός μηχανισμού εκμετάλευσης (συνημμένο email, εκτελέσιμο αρχείο, Δούρειος Ίππος) σε ένα ευάλωτο σύστημα.

Μηχανισμός Διάδοσης: Μετά την απόκτηση πρόσβασης σε μια συσκευή, το worm αναπαράγεται και εντοπίζει νέους στόχους.

Ωφέλιμο φορτίο: Κάθε κακόβουλος κώδικας που οδηγεί σε κάποια δράση. Τις περισσότερες φορές αυτός χρησιμοποιείται για να δημιουργήσει μια κερκόπορτα στον μολυσμένο ξενιστή. Τα "σκουλήκια" είναι αυτόνομα προγράμματα που επιτίθενται σ' ένα σύστημα για να εκμεταλλευτούν μια γνωστή ευπάθεια. Μετά την επιτυχής εκμετάλλευση, το "σκουλήκι" αντιγράφει τον εαυτό του από την επιτιθέμενο χρήστη στο νέο σύστημα εκμετάλλευσης και ο κύκλος αρχίζει ξανά.

2.1.2. Trojan Horses – Δούρειοι ίπποι

Οι Έλληνες πολεμιστές πρόσφεραν στο λαό της Τροίας ένα γιγάντιο κούφιο άλογο ως δώρο. Οι Τρώες έφεραν το γιγαντιαίο άλογο στην περιτοιχισμένη πόλη τους, ενώ δεν γνώριζαν ότι περιείχε πολλούς Έλληνες πολεμιστές. Το βράδυ,ενώ οι

περισσότεροι Τρώες κοιμόντουσαν, οι πολεμιστές προτάχτηκαν έξω από το άλογο και προσπέρασαν την πόλη.

Ένας Δούρειος Ίππος στον κόσμο των υπολογιστών είναι ένα κακόβουλο λογισμικό που εκτελεί κακόβουλες ενέργειες με το πρόσχημα μιας επιθυμητής λειτουργίας. Ένας Δούρειος Ίππος περιέχει κρυφό κακόβουλο κώδικα που εκμεταλλεύεται τα προνόμια του χρήστη που το τρέχει. Τα παιχνίδια μπορούν να έχουν συχνά Δούρειους Ίππους συνδεδεμένα με αυτά. Όταν εκτελείτε το παιχνίδι, αυτό λειτουργεί, αλλά στο παρασκήνιο, ο Δούρειος Ίππος έχει εγκατασταθεί στο σύστημα του χρήστη και συνεχίζει να τρέχει αφού το παιχνίδι έχει κλείσει. Η έννοια Δούρειος Ίππος είναι ευέλικτη. Μπορεί να προκαλέσει άμεση βλάβη, παρέχει απομακρυσμένη πρόσβαση στο σύστημα(πίσω πόρτα) ή εκτελεί ενέργειες σύμφωνα με οδηγίες εξ αποστάσεως, όπως "να μου στέλνετε το αρχείο κωδικού πρόσβασης μία φορά την εβδομάδα."

Κατηγορίες Trojan Horses

Οι Δούρειοι Ίπποι συνήθως κατατάσσονται ανάλογα με τη ζημιά που προκαλούν ή τον τρόπο με τον οποίο παραβιάζουν ένα σύστημα:

- Δούρειος Ίππος απομακρυσμένης πρόσβασης: επιτρέπει τη μη εξουσιοδοτημένη απομακρυσμένη πρόσβαση
- Δούρειος Ίππος αποστολής δεδομένων: παρέχει στον επιτιθέμενο ευαίσθητα δεδομένα όπως κωδικούς πρόσβασης
- Καταστροφικός Δούρειος Ίππος: διαφθείρει ή διαγράφει τα αρχεία
- Δούρειος Ίππος μεσολάβησης: λειτουργίες του υπολογιστή του χρήστη, όπως ένας διακομιστής μεσολάβησης
- FTP Δούρειος Ίππος: ανοίγει τη θύρα 21
- Δούρειος Ίππος απενεργοποίησης λογισμικού ασφαλείας: σταματά τα προγράμματα προστασίας από ιούς ή τα τείχη προστασίας

- Δούρειος Ίππος άρνησης των υπηρεσιών: επιβραδύνει ή σταματά τη δραστηριότητα του δικτύου.

2.2. Τρόποι επίθεσης υποδομών δικτύων

Υπάρχουν πολλοί διαφορετικοί τύποι επιθέσεων δικτύου, εκτός από ιούς, σκουλήκια και δούρειους ίππους .Για την καταπολέμηση των επιθέσεων είναι χρήσιμο πρώτα να κατηγοριοποιηθούν οι διάφοροι τύποι επιθέσεων. Με την κατηγοριοποίηση των επιθέσεων δικτύου είναι δυνατόν να αντιμετωπιστούν τα είδη των επιθέσεων, αντί οι μεμονωμένες επιθέσεις. Δεν υπάρχει κανένας τυποποιημένος τρόπος κατηγοριοποίησης των επιθέσεων δικτύου. (Osvik et al , 2010)

σε τρεις μεγάλες κατηγορίες.

Επιθέσεις αναγνώρισης: Οι επιθέσεις αναγνώρισης αφορούν τη μη εξουσιοδοτημένη ανακάλυψη και χαρτογράφηση των συστημάτων, υπηρεσιών,ή τρωτών σημείων. Οι επιθέσεις αναγνώρισης συχνά απασχολούν τη χρήση των sniffers πακέτων και των σαρωτών θυρών, τα οποία είναι ευρέως διαθέσιμα για δωρεάν λήψη στο διαδίκτυο. Η αναγνώριση είναι ανάλογη με έναν κλέφτη που ερευνά τη γειτονιά για ευάλωτα σπίτια ώστε να μπεί μέσα,όπως μία άδεια κατοικία ή ένα σπίτι με ανοιχτή πόρτα ή παράθυρο.

Επιθέσεις πρόσβασης:

Οι επιθέσεις πρόσβασης εκμεταλλεύονται γνωστά τρωτά σημεία στον τομέα των υπηρεσιών πιστοποίησης, υπηρεσίες FTP, καθώς και διαδικτυακές υπηρεσίες για να αποκτήσουν πρόσβαση σε λογαριασμούς στον ιστό, εμπιστευτικές βάσεις δεδομένων και άλλες ευαίσθητες πληροφορίες. Μια επίθεση πρόσβασης μπορεί να πραγματοποιηθεί με πολλούς διαφορετικούς τρόπους. Χρησιμοποιεί συχνά μία

επίθεση λεξικού για να μαντέψει κωδικούς πρόσβασης του συστήματος. Υπάρχουν επίσης εξειδικευμένα λεξικά για διαφορετικές γλώσσες που μπορούν να χρησιμοποιηθούν.

Επιθέσεις άρνησης υπηρεσιών(Denial of services) : Οι επιθέσεις άρνησης υπηρεσιών στέλνουν έναν εξαιρετικά μεγάλο αριθμό αιτημάτων πάνω σ'ένα δίκτυο ή το Internet. Αυτά τα αιτήματα προκαλούν τη συσκευή προορισμού να τρέξει υπο-βέλτιστα. Κατά συνέπεια, η επιτιθέμενη συσκευή δεν είναι διαθέσιμη για νόμιμη πρόσβαση και χρήση. Εκτελώντας εκμεταλλεύσεις ή συνδυασμούς εκμεταλλεύσεων, οι επιθέσεις DoS επιβραδύνουν ή συντρίβουν εφαρμογές και διεργασίες. (McAffe, 2017)

Η αναγνώριση είναι επίσης γνωστή ως συλλογή πληροφοριών και στις περισσότερες περιπτώσεις προηγείται της πρόσβασης ή της επίθεσης DoS. Σε μια επίθεση αναγνώρισης, ο κακόβουλος εισβολέας συνήθως ξεκινά με τη διεξαγωγή μίας σάρωσης ping του δικτύου στόχου για να καθορίσει ποιες IP διευθύνσεις είναι ενεργές. Ο εισβολέας στη συνέχεια καθορίζει ποιες υπηρεσίες ή θύρες είναι διαθέσιμες για τις ζωντανές IP διευθύνσεις.

Το Nmap είναι η πιο δημοφιλής εφαρμογή για την εκτέλεση σάρωσης θυρών. Από τις πληροφορίες των θυρών που λαμβάνονται, ο εισβολέας εξετάζει τις θύρες για να καθορίσει τον τύπο και την έκδοση της εφαρμογής και το λειτουργικό σύστημα που τρέχει στον κεντρικό υπολογιστή-στόχο. Σε πολλές περιπτώσεις, οι εισβολείς αναζητούν ευάλωτες υπηρεσίες που μπορούν να αξιοποιηθούν αργότερα, όταν υπάρχει μικρότερη πιθανότητα να έχουν "αλιευθεί". Οι επιθέσεις αναγνώρισης χρησιμοποιούν διάφορα εργαλεία για να αποκτήσουν πρόσβαση σε ένα δίκτυο. (McAffe, 2017)

2.3.1. Επιθέσεις Πρόσβασης

Οι χάκερ χρησιμοποιούν τις επιθέσεις πρόσβασης σε δίκτυα ή συστήματα για τρεις λόγους: ανάκτηση δεδομένων, απόκτηση πρόσβασης και κλιμάκωση προνομίων πρόσβασης. Οι επιθέσεις πρόσβασης χρησιμοποιούνται συχνά σε επιθέσεις κωδικών πρόσβασης για να μαντέψουν κωδικούς πρόσβασης του συστήματος. Οι επιθέσεις κωδικών πρόσβασης μπορούν να υλοποιηθούν με διάφορες μεθόδους, συμπεριλαμβανομένων των brute-force επιθέσεων, των προγραμμάτων Δούρειων Ίππων, του IP spoofing και των packet sniffers. (Michael, 2009)

Ωστόσο,οι περισσότερες επιθέσεις κωδικών αναφέρονται σε brute-force επιθέσεις, οι οποίες περιλαμβάνουν τις επανειλημμένες προσπάθειες που βασίζονται σε ένα ενσωματωμένο λεξικό για τον εντοπισμό ενός λογαριασμού χρήστη ή του κωδικού πρόσβασης.

Μια brute-force επίθεση συχνά εκτελείται χρησιμοποιώντας ένα πρόγραμμα που τρέχει σε όλο το δίκτυο και προσπαθεί να συνδεθεί σ'έναν κοινόχρηστο πόρο, όπως ένα διακομιστή. Μετά την απόκτηση πρόσβασης του εισβολέα σ'έναν πόρο, αυτός έχει τα ίδια δικαιώματα πρόσβασης με τον χρήστη του οποίου ο λογαριασμός τέθηκε σε κίνδυνο. Αν αυτός ο λογαριασμός έχει επαρκή δικαιώματα, ο εισβολέας μπορεί να δημιουργήσει μια πίσω πόρτα(back door) για μελλοντική πρόσβαση χωρίς ανησυχία για οποιαδήποτε κατάσταση και αλλαγή στον κωδικό πρόσβασης στον εκτεθειμένο λογαριασμό χρήστη. (Michael, 2009)

Για παράδειγμα, ένας χρήστης μπορεί να τρέξει το L0phtCrack,ή το LC5,εφαρμογή για την εκτέλεση brute-force επιθέσεων και την απόκτηση ενός κωδικού πρόσβασης Windows Server.Όταν ληφθεί ο κωδικός πρόσβασης, ο εισβολέας μπορεί να εγκαταστήσει ένα keylogger,το οποίο στέλνει ένα αντίγραφο όλων των πληκτρολογήσεων σ'έναν επιθυμητό προορισμό. Ή,ένας Δούρειος Ίππος μπορεί να εγκατασταθεί για να στείλει ένα αντίγραφο όλων των πακέτων που στέλνονται και λαμβάνονται από το στόχο σ'ένα συγκεκριμένο προορισμό,

καθιστώντας έτσι δυνατή την παρακολούθηση όλης της κίνησης προς και από αυτόν το διακομιστή.

2.3.2. Denial of Service

Μια επίθεση DoS είναι μια επίθεση ενός δικτύου που οδηγεί σε κάποιο είδος διακοπής της υπηρεσίας για τους χρήστες, τις συσκευές ή εφαρμογές. Αρκετοί μηχανισμοί μπορούν να δημιουργήσουν μια επίθεση DoS. Η απλούστερη μέθοδος είναι να παράγουν μεγάλες ποσότητες από ό,τι φαίνεται να είναι έγκυρη κίνηση δικτύου. Αυτού του είδους επίθεση δικτύου DoS οδηγεί στον κορεσμό του δικτύου, έτσι ώστε η έγκυρη κίνηση των χρηστών να μη μπορεί να περάσει. (Arbor, 2013)

Μια επίθεση DoS εκμεταλλεύεται το γεγονός ότι τα στοχευμένα συστήματα, όπως οι διακομιστές πρέπει να διατηρούν πληροφορίες κατάστασης. Οι εφαρμογές μπορούν να βασίζονται σε αναμενόμενα μεγέθη buffer και συγκεκριμένο περιεχόμενο των πακέτων δικτύου. Μια επίθεση DoS μπορεί να το εκμεταλλευτεί αυτό με την αποστολή μεγεθών πακέτων ή τιμών δεδομένων, που δεν αναμένονται από την εφαρμογή λήψης. (Arbor, 2013)

Υπάρχουν δύο βασικοί λόγοι για όταν μια επίθεση DoS συμβαίνει. Ένας χρήστης ή εφαρμογή αποτυγχάνει να χειριστεί μια απροσδόκητη κατάσταση, όπως κακόβουλα διαμορφωμένα δεδομένα εισόδου, μια απρόσμενη αλληλεπίδραση στοιχείων του συστήματος, ή απλά εξάντληση των πόρων. Ένα δίκτυο, χρήστης ή εφαρμογή είναι αδύνατο να χειριστεί μια τεράστια ποσότητα δεδομένων, με αποτέλεσμα το σύστημα να καταρρεύσει ή να γίνει εξαιρετικά αργό.

Οι DoS επιθέσεις επιχειρούν να θέσουν σε κίνδυνο τη διαθεσιμότητα του δικτύου, τον χρήστη, ή την εφαρμογή. Θεωρούνται ως ένας σημαντικός κίνδυνος,

επειδή μπορούν εύκολα να διακόψουν μια επιχειρηματική διαδικασία και να προκαλέσουν σημαντική απώλεια. Αυτές οι επιθέσεις είναι σχετικά απλό για να διεξαχθούν, ακόμη και από έναν ανειδίκευτο εισβολέα.

Ένα παράδειγμα μιας επίθεσης DoS είναι η αποστολή ενός δηλητηριώδες πακέτου. Το δηλητηριώδες πακέτο είναι ένα εσφαλμένα μορφοποιημένο πακέτο σχεδιασμένο έτσι ώστε να προκαλεί στη συσκευή λήψης την επεξεργασία του πακέτου με ακατάλληλο τρόπο. Το δηλητηριώδες πακέτο προκαλεί στη συσκευή λήψης να συντριφθεί ή να τρέχει πολύ αργά. Αυτή η επίθεση μπορεί να προκαλέσει σ'όλες τις επικοινωνίες προς και από τη συσκευή να διακοπούν.

Σε ένα άλλο παράδειγμα, ένας εισβολέας στέλνει μια συνεχή ροή πακέτων, η οποία κατακλύζει το διαθέσιμο εύρος ζώνης των συνδέσεων του δικτύου. Στις περισσότερες περιπτώσεις, είναι αδύνατο να γίνει διάκριση μεταξύ επιτιθέμενου και νόμιμης κίνησης και να εντοπιστεί μια επίθεση γρήγορα πίσω στην πηγή της. Εάν πολλά συστήματα στον πυρήνα του Διαδικτύου διακινδυνεύουν, ο εισβολέας μπορεί να είναι σε θέση να επωφεληθεί από το σχεδόν απεριόριστο εύρος ζώνης για να απελευθερώσει καταιγίδες πακέτων προς επιθυμητούς στόχους. Μία επίθεση κατανεμημμένης άρνησης υπηρεσιών(DDoS) είναι παρόμοια με μία επίθεση DoS, εκτός από το ότι μια επίθεση DDoS προέρχεται από πολλαπλές συντονισμένες πηγές. Μια επίθεση DDoS απαιτεί τον επαγγελματία της ασφάλειας δικτύων, ώστε να εντοπίσει και να σταματήσει τις επιθέσεις από κατανεμημένες πηγές, ενώ διηύθυνε μια αύξηση της επισκεψιμότητας.

Για παράδειγμα, μια επίθεση DDoS θα μπορούσε να προχωρήσει ως εξής: Ο χάκερ ψάχνει για συστήματα που είναι προσβάσιμα. Αφού ο hacker αποκτήσει πρόσβαση σε διάφορα συστήματα «χειριστή», ο χάκερ εγκαθιστά λογισμικό ζόμπι σ'αυτά. Τα ζόμπι στη συνέχεια σαρώνουν και μολύνουν τα συστήματα παράγοντα. Όταν ο χάκερ αποκτήσει πρόσβαση στα συστήματα παράγοντα,ο χάκερ φορτώνει λογισμικό επίθεσης τηλεχειρισμού για να πραγματοποιήσει την επίθεση DDoS.

2.4. Κακόβουλοι Χρήστες

Χάκερ

Η λέξη « χάκερ » έχει μια ποικιλία από σημασίες. Για πολλούς, αυτό σημαίνει ότι οι προγραμματιστές του Διαδικτύου προσπαθούν να αποκτήσουν μη εξουσιοδοτημένη πρόσβαση στο Διαδίκτυο. Αναφέρεται επίσης σε άτομα που τρέχουν προγράμματα για την πρόληψη ή την αργή πρόσβαση στο δίκτυο σε έναν μεγάλο αριθμό χρηστών ή την καταστροφή ή και σβήσιμο τον δεδομένων σε διακομιστές. Αλλά για μερικούς ,ο όρος χάκερ έχει μια θετική ερμηνεία όπως ένας επαγγελματίας δικτύου που χρησιμοποιεί εξελιγμένες ικανότητες προγραμματισμού του Διαδικτύου ώστε να εξασφαλίσει ότι τα δίκτυα δεν είναι ευάλωτα σε επιθέσεις. Καλό ή κακό, το hacking είναι η κινητήρια δύναμη για την ασφάλεια του δικτύου. (Storm, 2016)

Από την πλευρά των επιχειρήσεων, είναι σημαντικό να ελαχιστοποιηθούν οι επιπτώσεις των hackers με κακές προθέσεις. Οι επιχειρήσεις χάνουν την παραγωγικότητά τους όταν το δίκτυο είναι αργό ή αδιάφορο. Τα κέρδη των επιχειρήσεων επηρεάζονται από την απώλεια και την αλλοίωση δεδομένων. Η δουλειά του επαγγελματία της ασφάλειας δικτύων είναι να κάνει ένα βήμα μπροστά από τους hackers με την παρουσία τους σε εργαστήρια, τη συμμετοχή τους

σε οργανισμούς της ασφάλειας, την εγγραφή τους σε feeds πραγματικού χρόνου όσον αφορά τους κινδύνους και να περιεργάζονται ιστοσελίδες ασφαλείας σε καθημερινή βάση. Ο επαγγελματίας πρέπει επίσης να έχει πρόσβαση σε state-of-the art εργαλεία ασφαλείας ,πρωτόκολλα, τεχνικές και τεχνολογίες. (Storm, 2016)

Οι Επαγγελματίες της ασφάλειας δικτύων θα πρέπει να έχουν πολλά από τα ίδια χαρακτηριστικά όπως οι επαγγελματίες της επιβολής του νόμου. Θα πρέπει πάντα να παραμένουν ενήμεροι για κακόβουλες δραστηριότητες και να διαθέτουν τις δεξιότητες και τα εργαλεία για την ελαχιστοποίηση ή την εξάλειψη των απειλών που συνδέονται με τις δραστηριότητες αυτές. Το hacking έχει το ανεπιθύμητο αποτέλεσμα δημιουργίας υψηλής ζήτησης για τους επαγγελματίες της ασφάλειας δικτύων. Ωστόσο, σε σχέση με άλλα επαγγέλματα της τεχνολογίας, η ασφάλεια δικτύων έχει την πιο απότομη καμπύλη εκμάθησης και απαιτεί δέσμευση για συνεχής επαγγελματική ανάπτυξη. (Storm, 2016)

Το hacking ξεκίνησε τη δεκαετία του 1960 με το τηλεφωνικό freaking ή phreaking, το οποίο αναφέρεται στη χρήση διάφορων συχνοτήτων ήχου για την χειραγώγηση τηλεφωνικών συστημάτων. Το phreaking ξεκίνησε όταν η AT & T εισήγαγε αυτόματους διακόπτες στα τηλεφωνικά τους συστήματα. Οι τηλεφωνικοί διακόπτες της AT & T χρησιμοποιούσαν διάφορους ήχους,ή ήχους κλήσης για να δείξουν διαφορετικές λειτουργίες, όπως τερματισμό κλήσεων και της κλήσης. Κάποιοι πελάτες της AT & T συνειδητοποίησαν ότι με τη μίμηση έναν ήχου σφυρίζοντας, θα μπορούσαν να εκμεταλλευτούν τους διακόπτες τηλεφώνου για να κάνουν δωρεάν υπεραστικές κλήσεις.

Όπως τα συστήματα επικοινωνίας εξελίχθηκαν, το ίδιο έγινε ακριβώς και με τις μεθόδους hacking. Το wardialing έγινε δημοφιλής τη δεκαετία του 1980 με τη χρήση του μόντεμ του υπολογιστή. Τα Wardialing προγράμματα έλεγχαν αυτόματα αριθμούς τηλεφώνου μέσα σε μια τοπική περιοχή, καλώντας το καθένα για την έρευνα ηλεκτρονικών υπολογιστών, συστημάτων πίνακα ανακοινώσεων, και φαξ.

Όταν ένας αριθμός τηλεφώνου βρισκόταν, τα προγράμματα "σπασίματος" κωδικών χρησιμοποιούνταν για να αποκτήσουν πρόσβαση.

Το Wardriving ξεκίνησε τη δεκαετία του 1990 και εξακολουθεί να είναι δημοφιλής εώς σήμερα.Με το wardriving,οι χρήστες αποκτούν μη εξουσιοδοτημένη πρόσβαση σε δίκτυα μέσω ασύρματων σημείων πρόσβασης. Αυτό επιτυγχάνεται χρησιμοποιώντας έναν φορητό υπολογιστή ασύρματης δυνατότητας ή PDA. Τα προγράμματα "σπασίματος" κωδικών χρησιμοποιούνται για την επικύρωση, εάν είναι απαραίτητο, και είναι επίσης το λογισμικό για να σπάσουμε το σύστημα κρυπτογράφησης που απαιτείται για να γίνει η σύνδεση με το σημείο πρόσβασης. Άλλες απειλές έχουν εξελιχθεί από τη δεκαετία του 1960.Αυτές περιλαμβάνουν εργαλεία σάρωσης μέσω δικτύου, όπως το Nmap και SATAN,καθώς και hacking εργαλεία διαχείρισης απομακρυσμένου συστήματος όπως το Back Orifice. Οι επαγγελματίες της ασφάλειας δικτύων πρέπει να είναι εξοικειωμένοι με όλα αυτά τα εργαλεία.

Συναλλαγές αξίας τρισεκατομμυρίων δολαρίων πραγματοποιούνται μέσω του Internet σε καθημερινή βάση και τα μέσα διαβίωσης εκατομμυρίων ανθρώπων εξαρτώνται από το διαδικτυακό εμπόριο. Για το λόγο αυτό, η ποινική νομοθεσία είναι σε θέση να προστατεύσει τα ατομικά και εταιρικά περιουσιακά στοιχεία. Υπάρχουν πολυάριθμες περιπτώσεις ατόμων που είχαν να αντιμετωπίσουν το δικαστικό σύστημα,λόγω αυτών των νόμων. Ο πρώτος ιός e-mail, ο ιός Melissa, γράφτηκε από τον David Smith απ'το Aberdeen,Νιού Τζέρσεϊ. Αυτός ο ιός οδήγησε σε υπερχειλίσεις μνήμης σε διακομιστές ηλεκτρονικού ταχυδρομείου. Ο David Smith καταδικάστηκε σε 20 μήνες φυλάκισης στις ομοσπονδιακές φυλακές και πρόστιμο 5.000 δολλαρίων.(Kevin et al , 2011)

Ο Robert Morris δημιούργησε το πρώτο "σκουλήκι" στο Internet με 99 γραμμές κώδικα. Όταν το σκουλήκι Morris κυκλοφόρησε, το 10% των συστημάτων του Διαδικτύου είχαν ανακοπεί. Ο Robert Morris χρεώθηκε και έλαβε τρία χρόνια δοκιμασίας,400 ώρες κοινωφελούς εργασίας και πρόστιμο ύψους 10.000 δολαρίων.

Ένας από τους πλέον διαβόητους hackers στο Internet,ο Kevin Mitnick, φυλακίστηκε για hacking λογαριασμών πιστωτικών καρτών στις αρχές του 1990. Είτε η επίθεση είναι μέσω spam, ενός ιού, DoS ή απλά σπασίματος λογαριασμού, όταν η δημιουργικότητα των χάκερ χρησιμοποιείται για κακόβουλους σκοπούς, αυτοί συχνά καταλήγουν στη φυλακή, πληρώνοντας μεγάλα πρόστιμα, καθώς και στερούνται την πρόσβαση στο περιβάλλον στο οποίο ευδοκιμούν .(Kevin et al , 2011)

ΚΕΦΑΛΑΙΟ 3- Καλές πρακτικές

3.1. Ασφάλεια δρομολογητών (routers)

Η εξασφάλιση της υποδομής του δικτύου είναι ζωτικής σημασίας για τη συνολική ασφάλεια του δικτύου. Η υποδομή του δικτύου περιλαμβάνει routers, switches, servers, endpoints και άλλες συσκευές. Σκεφτείτε ένα δυσαρεστημένο υπάλληλο που αναζητά πάνω από τον ώμο του διαχειριστή του δικτύου, ενώ ο διαχειριστής συνδεθείτε σε έναν ακραίο δρομολογητή. Αυτό είναι γνωστό ως "σερφάρισμα ώμου" και είναι ένα εκπληκτικά εύκολος τρόπος για έναν εισβολέα να αποκτήσει μη εξουσιοδοτημένη πρόσβαση. Αν ένας εισβολέας αποκτήσει πρόσβαση σε ένα router,η ασφάλεια και η διαχείριση του συνόλου του δικτύου μπορεί να τεθεί σε κίνδυνο, αφήνοντας servers και τα endpoints σε κίνδυνο. Είναι ζωτικής σημασίας ότι οι κατάλληλες πολιτικές ασφάλειας και οι έλεγχοι πρέπει να εφαρμοστούν για την αποτροπή μη εξουσιοδοτημένης πρόσβασης σε όλες τις συσκευές υποδομής. Παρά το γεγονός ότι όλες οι συσκευές υποδομής βρίσκονται σε κίνδυνο,οι δρομολογητές είναι ο πρωταρχικός στόχος για τους επιτιθέμενους δικτύου. Αυτό είναι επειδή οι δρομολογητές ενεργούν ως τροχαία, που ρυθμίζει την κυκλοφορία εντός,εκτός και μεταξύ των δικτύων. (Cisco Systems, 2010)

Ο ακραίος δρομολογητής είναι το τελευταίο router μεταξύ του εσωτερικού δικτύου και ενός αναξιόπιστου δικτύου, όπως το Internet. Όλη η κίνηση στο Διαδίκτυο ενός οργανισμού περνά μέσα από αυτόν τον ακραίο δρομολογητή. Ως εκ τούτου, συχνά λειτουργεί ως η πρώτη και τελευταία γραμμή άμυνας για ένα δίκτυο. Μέσω του αρχικού και τελικού φιλτραρίσματος, ο ακραίος δρομολογητής βοηθά στη διασφάλιση της περιμέτρου ενός προστατευόμενου δικτύου. Είναι επίσης υπεύθυνο για την υλοποίηση δράσεων για την ασφάλεια που βασίζεται στις πολιτικές ασφάλειας του οργανισμού. Για τους λόγους αυτούς ,η εξασφάλιση των δρομολογητών δικτύου είναι επιτακτική. (Cisco Systems, 2010)

3.1.1. Εγκατάσταση logging

Η εφαρμογή μιας logging εγκατάστασης δρομολογητή είναι ένα σημαντικό μέρος οποιασδήποτε πολιτικής για την ασφάλεια του δικτύου.Οι δρομολογητές Cisco μπορούν να συνδέσουν πληροφορίες σχετικά με τις αλλαγές στις παραμέτρους, τις ACL παραβιάσεις,την κατάσταση της διεπαφής, και πολλά άλλα είδη συμβάντων. Οι δρομολογητές Cisco μπορούν να στείλουν τα μηνύματα καταγραφής σε πολλές διαφορετικές εγκαταστάσεις. Θα πρέπει να γίνει η ρύθμιση δρομολογητή για την αποστολή μηνυμάτων καταγραφής σ'ένα ή περισσότερα από τα ακόλουθα στοιχεία (Naveed, 2010):

Console - Η Console καταγραφή είναι ενεργοποιημένη από προεπιλογή. Τα μηνύματα καταγράφονται στην κονσόλα και μπορούν να προβληθούν κατά την τροποποίηση ή τη δοκιμή του δρομολογητή χρησιμοποιώντας το λογισμικό εξομοίωσης τερματικού, ενώ συνδέονται με την θύρα κονσόλας του δρομολογητή.

Terminal lines: Οι ενεργοποιημένες συνεδρίες EXEC μπορούν να να ρυθμιστούν ώστε να λαμβάνουν μηνύματα καταγραφής σε οποιαδήποτε τερματικές γραμμές. Παρόμοιο με το console logging,αυτό το είδος της καταγραφής δεν

αποθηκεύεται από το δρομολογητή και, ως εκ τούτου, είναι πολύτιμο μόνο για το χρήστη σε αυτή τη γραμμή.

Buffered logging: Το Buffered logging είναι λίγο πιο χρήσιμο ως εργαλείο ασφαλείας, επειδή τα μηνύματα καταγραφής αποθηκεύονται στη μνήμη του δρομολογητή για έναν χρόνο. Ωστόσο, τα συμβάντα εκκαθαρίζονται όταν ο δρομολογητής κάνει επανεκκίνηση.

SNMP traps: Ορισμένα κατώτατα όρια μπορούν να έχουν προρυθμιστεί σε δρομολογητές και άλλες συσκευές. Τα συμβάντα του δρομολογητή, όπως η υπέρβαση ενός ορίου, μπορούν να υποβληθούν σε επεξεργασία από τον δρομολογητή και να διαβιβάζονται ως SNMP παγίδες σ'έναν εξωτερικό διακομιστή SNMP.Οι παγίδες SNMP είναι μια βιώσιμη μονάδα καταγραφής ασφαλείας ,αλλά απαιτούν τη διαμόρφωση και τη συντήρηση ενός συστήματος SNMP.

Syslog: Οι δρομολογητές Cisco μπορούν να ρυθμιστούν για να διαβιβάσουν τα μηνύματα καταγραφής σε μια εξωτερική υπηρεσία syslog. Η υπηρεσία αυτή μπορεί να βρίσκεται σε οποιοδήποτε αριθμό δρομολογητών ή workstations,συμπεριλαμβανομένων των Microsoft Windows και τα συστήματα που βασίζονται σε UNIX. Το Syslog είναι το πιο δημοφιλές πρότυπο καταγραφής μηνυμάτων εφαρμογών, διότι παρέχει μακροπρόθεσμες δυνατότητες αποθήκευσης και μια κεντρική τοποθεσία για όλα τα μηνύματα δρομολογητή. Τα μηνύματα καταγραφής του δρομολογητή Cisco εμπίπτουν σε ένα από τα οκτώ επίπεδα. Όσο μικρότερος ο αριθμός του επιπέδου, τόσο υψηλότερο είναι το επίπεδο ασφαλείας. Τα μηνύματα καταγραφής του δρομολογητή περιέχουν τρία κύρια μέρη:

- Timestamp
- Όνομα Log message και
- επίπεδο ασφαλείας

Message text

3.1.2. Syslog

Το Syslog είναι το πρότυπο για τα γεγονότα του συστήματος καταγραφής. Οι εφαρμογές Syslog περιέχουν δύο τύπους συστημάτων.

Syslog servers: Επίσης γνωστοί ως log hosts,τα συστήματα αυτά δέχονται και κατεργάζονται μηνύματα καταγραφής από τους πελάτες syslog

Syslog clients - Δρομολογητές ή άλλα είδη εξοπλισμού που παράγουν και προωθούν μηνύματα καταγραφής σε syslog servers.

Το πρωτόκολλο syslog επιτρέπει τα login μηνύματα να σταλούν από έναν syslog πελάτη στο διακομιστή syslog. Ενώ η δυνατότητα της αποστολής logs σ'έναν κεντρικό server syslog είναι μέρος μιας καλής λύσης ασφάλειας, μπορεί επίσης ενδεχομένως να είναι μέρος ενός προβλήματος της ασφάλειας. Το μεγαλύτερο πρόβλημα είναι το μέγεθος του έργου της αξιολόγησης των πληροφοριών. Αυτό περιλαμβάνει λεπτομερής εξέταση μέσα από τα διάφορα logs και γεγονότα, συσχετίζοντας τα γεγονότα από διάφορες συσκευές του δικτύου και διακομιστές εφαρμογών και τον καθορισμό του τύπου της δράσης που θα παρθεί με βάση την εκτίμηση τρωτότητας του περιστατικού. (Roitman & Sudkovitch , 2010)

3.1.3. SNMP

Ένα άλλο κοινό εργαλείο παρακολούθησης είναι το SNMP.Το SNMP αναπτύχθηκε για τη διαχείριση των κόμβων, όπως servers,σταθμούς εργασίας,routers,switches,hubs και συσκευές ασφαλείας σ'ένα IP δίκτυο. Το SNMP είναι ένα Application Layer πρωτόκολλο που διευκολύνει την ανταλλαγή

πληροφοριών διαχείρισης μεταξύ των συσκευών του δικτύου. Το SNMP είναι μέρος της οικογένειας πρωτοκόλλων TCP/IP.Το SNMP επιτρέπει στους διαχειριστές του δικτύου να διαχειρίζονται την απόδοση του δικτύου, να βρίσκουν και να λύνουν τα προβλήματά του και να κάνουν σχέδια για την ανάπτυξή του. Υπάρχουν διαφορετικές εκδόσεις του SNMP: Έκδοση 1(SNMPv1),SNMP έκδοση 2(SNMPv2) και SNMP έκδοση 3(SNMPv3).

Και οι τρεις εκδόσεις χρησιμοποιούν managers(συστήματα διαχείρισης δικτύων [NMSs]),agents(διαχειριζόμενους κόμβους) και βάσεις πληροφοριών διαχείρισης(MIBs). Σε οποιαδήποτε ρύθμιση, τουλάχιστον ένας κόμβος manager τρέχει το SNMP λογισμικό διαχείρισης. Συσκευές δικτύου που πρέπει να διαχειρίζονται, όπως διακόπτες, δρομολογητές,servers,σταθμοί εργασίας, είναι εξοπλισμένες με μονάδες λογισμικού πράκτορα SMNP.Ο agent είναι υπεύθυνος για την παροχή πρόσβασης σε ένα τοπικό MIB των αντικειμένων που αντανακλά τους πόρους και τη δραστηριότητα στον κόμβο της. Οι MIBs αποθηκεύουν δεδομένα σχετικά με τη λειτουργία της συσκευής και προορίζονται να είναι διαθέσιμοι σε εξουσιοδοτημένους απομακρυσμένους χρήστες. (Chatzimisios et al, 2003)

Ο SNMP manager μπορεί να πάρει πληροφορίες από τον agent και αλλάξει ή ορίσει την πληροφορία στον agent.Τα σετ μπορούν να αλλάξουν τις μεταβλητές ρυθμίσεων στη συσκευή παράγοντα. Τα σετ μπορούν επίσης να ξεκινήσουν ενέργειες σε συσκευές. Η απάντηση σε ένα σετ δείχνει τη νέα ρύθμιση στη συσκευή. Για παράδειγμα, ένα σετ μπορεί να προκαλέσει την επανεκκίνηση του δρομολογητή, να στείλει ένα αρχείο ρυθμίσεων, ή να λάβει ένα αρχείο ρυθμίσεων. Τα SNMP traps ενεργοποιούν ένα agent να ειδοποιήσει τον σταθμό διαχείρισης σημαντικών γεγονότων, στέλνοντας ένα ανεπιθύμητο μήνυμα SNMP.Οι ενέργειες 'get' και 'set' είναι τα τρωτά σημεία που ανοίγουν το SNMP για να επιτεθεί. (Pattinson, 2011)

Οι SNMP agents δέχονται εντολές και αιτήματα από τα συστήματα διαχείρισης SNMP μόνο εφόσον τα συστήματα αυτά έχουν ένα σωστό community

string.Ένα SNMP community string είναι μια συμβολοσειρά κειμένου που μπορεί να επικυρώσει τα μηνύματα μεταξύ ενός σταθμού διαχείρισης και ενός SNMP agent και να επιτρέψει την πρόσβαση στις πληροφορίες των MIBs.Τα Community strings χρησιμοποιούνται κυρίως μόνο για την πιστοποίηση του κωδικού πρόσβασης των μηνυμάτων μεταξύ του NMS και του agent. Υπάρχουν δύο τύποι community strings:

Read-only community string: Παρέχει πρόσβαση μόνο για ανάγνωση σε όλα τα αντικείμενα της MIB,εκτός των community strings

Read-write community string: Παρέχει πρόσβαση ανάγνωσης και εγγραφής σε όλα τα αντικείμενα της MIB,εκτός των community strings. Αν ο manager στέλνει ένα εκ των σωστών μόνο για ανάγνωση community strings,μπορεί να πάρει πληροφορίες, αλλά να μην ορίσει πληροφορίες σ' έναν agent.Εάν ο manager χρησιμοποιεί ένα από τα σωστά community strings ανάγνωσης-εγγραφής, μπορεί να πάρει ή να ορίσει τις πληροφορίες στον agent. Στην πραγματικότητα, έχοντας set access σ'έναν δρομολογητή είναι ισοδύναμο έχοντας τον enable password του δρομολογητή. (Pattinson, 2011)

Από προεπιλογή, τα περισσότερα συστήματα SNMP χρησιμοποιούν το "public" σαν community string.Αν ρυθμίσετε τον SNMP agent του δρομολογητή σας να χρησιμοποιήσει αυτό το κοινώς γνωστό community string,ο καθένας μ'ένα σύστημα SNMP είναι σε θέση να διαβάσει το MIB router.Επειδή οι μεταβλητές του MIB router μπορεί να δείξουν πράγματα όπως πίνακες δρομολόγησης και άλλα κρίσιμα μέρη της ασφάλειας της διαμόρφωσης του δρομολογητή, είναι εξαιρετικά σημαντικό το γεγονός ότι μπορείτε να δημιουργήσετε τα δικά σας προσαρμοσμένα SNMP community strings. Ωστόσο, ακόμη και αν τα community strings αλλάζουν, τα strings αποστέλλονται σε plaintext.Αυτό είναι μία τεράστια ευπάθεια της SNMPv1 και SNMPv2 αρχιτεκτονικής.

Αν χρησιμοποιείτε in-band διαχείριση, για τη μείωση των κινδύνων ασφαλείας, η διαχείριση SNMP πρέπει να ρυθμιστεί έτσι ώστε να "τραβήξει" μόνο

τις πληροφορίες από τις συσκευές, αντί να τους επιτραπεί να ωθήσει το "σύνολο" αλλαγών στις συσκευές. Για να εξασφαλιστεί ότι η πληροφόρηση διαχείρισης "τραβιέται", κάθε συσκευή θα πρέπει να ρυθμιστεί μ'ένα SNMP community string μόνο για ανάγνωση. Κρατώντας την SNMP κυκλοφορία σ'ένα τμήμα διαχείρισης επιτρέπει την κίνηση να διασχίσει ένα απομονωμένο τμήμα, όταν η διαχείριση πληροφοριών έλκεται από τις συσκευές και όταν οι αλλαγές διαμόρφωσης ωθούνται σε μια συσκευή Ως εκ τούτου, αν χρησιμοποιείτε ένα δίκτυο OOB, είναι αποδεκτό να διαμορφώσετε ένα SNMP community string ανάγνωσης-εγγραφής. Ωστόσο, πρέπει να γνωρίζετε τον αυξημένο κίνδυνο ασφαλείας ενός plaintext string που επιτρέπει την αλλαγή των συνθέσεων της συσκευής.

3.2. Πρωτόκολλο SNMPv3

Το SNMPv3 είναι ένα πρωτόκολλο που βασίζεται σε πρότυπα για τη διαχείριση του δικτύου. Για την αντιμετώπιση των αδυναμιών των προηγούμενων εκδόσεων του SNMP, το SNMPv3 πιστοποιεί και κρυπτογραφεί τα πακέτα μέσω του δικτύου για να παρέχει ασφαλής πρόσβαση στις συσκευές. Το SNMPv3 παρέχει τις ακόλουθες δυνατότητες ασφαλείας(Hikvision, 2017):

Ακεραιότητα μηνύματος: Διασφαλίζει πως το πακέτο δεν έχει αλλοιωθεί κατά τη μεταφορά.

Πιστοποίηση: Καθορίζει ότι το μήνυμα προέρχεται από μία έγκυρη πηγή.

Κρυπτογράφηση: Ανακατεύει τα περιεχόμενα ενός πακέτου για να το αποτρέψει από το να προβληθεί από μία μη εξουσιοδοτημένη πηγή.

Έλεγχος πρόσβασης: Περιορίζει κάθε κεφάλαιο σε ορισμένες ενέργειες σε συγκεκριμένα τμήματα των δεδομένων. Ενώ συνιστάται ότι το SNMPv3

χρησιμοποιείται όπου είναι δυνατόν, λόγω των πρόσθετων χαρακτηριστικών ασφαλείας.

Κατά την ενεργοποίηση του SNMP, είναι σημαντικό να εξεταστεί το μοντέλο ασφαλείας και το επίπεδο ασφαλείας. Το μοντέλο ασφαλείας είναι μια στρατηγική ελέγχου ταυτότητας που έχει συσταθεί για ένα χρήστη και την ομάδα στην οποία βρίσκεται. (Hikvision, 2017)

Επί του παρόντος, το λογισμικό Cisco IOS υποστηρίζει τρία μοντέλα ασφάλειας:

το SNMPv1,

το SNMPv2c και το

SNMPv3.

Ένα επίπεδο ασφάλειας είναι το επιτρεπόμενο επίπεδο ασφάλειας μέσα σε ένα πρότυπο ασφαλείας. Το επίπεδο ασφαλείας είναι ένα είδος αλγορίθμου ασφαλείας που εκτελείται σε κάθε πακέτο SNMP. Υπάρχουν τρία επίπεδα ασφάλειας:

noAuth: - Πιστοποιεί ένα πακέτο από ένα string match του ονόματος χρήστη ή του community string.

Auth: Πιστοποιεί ένα πακέτο χρησιμοποιώντας είτε το Hashed Message Authentication Code(HMAC) με τη μέθοδο MD5 ή την μέθοδο Secure Hash Algorithms(SHA). Η μέθοδος HMAC περιγράφεται στο RFC 2104,HMAC:Keyed-Κατακερματισμός για έλεγχο ταυτότητας μηνύματος.

Priv: Πιστοποιεί ένα πακέτο είτε το HMAC MD5 ή τους αλγόριθμους SHA HMAC και κρυπτογραφεί το πακέτο χρησιμοποιώντας το Data Encryption Standard(DES),το Triple DES(3DES) ή τους αλγόριθμους Advanced Encryption Standard(AES).

Ο συνδυασμός του μοντέλου και του επιπέδου καθορίζει ποιός μηχανισμός ασφαλείας χρησιμοποιείται κατά το χειρισμό ενός πακέτου SNMP. Μόνο SNMPv3 υποστηρίζει τα επίπεδα ασφαλείας auth και priv. Ωστόσο,το CCP δεν υποστηρίζει τη διαμόρφωση του SNMPv3.

3.3. Access Control Lists

Οι λίστες ελέγχου πρόσβασης(ACLs) χρησιμοποιούνται ευρέως στη δικτύωση υπολογιστών και στην ασφάλεια των δικτύων για μείωση των επιθέσεων δικτύου και τον έλεγχο της κίνησης του δικτύου. Οι διαχειριστές χρησιμοποιούν ACLs για να καθορίσουν και ελέγξουν τις τάξεις της κυκλοφορίας σε συσκευές δικτύου που βασίζονται σε διάφορες παραμέτρους. Αυτοί οι παράμετροι είναι συγκεκριμένοι για το Layer 2, 3, 4, και 7 του μοντέλου OSI. Σχεδόν κάθε είδος κίνησης μπορεί να ορίζεται ρητά με τη χρήση ενός κατάλληλα αριθμημένου ACL. Για παράδειγμα, στο παρελθόν, το πεδίο τύπου Ethernet μιας κεφαλίδας πλαισίου Ethernet χρησιμοποιήθηκε για τον καθορισμό ορισμένων τύπων κυκλοφορίας. Ένας τύπος Ethernet 0x8035 έδειξε ένα αντίστροφο πλαίσιο πρωτοκόλλου ανάλυσης διευθύνσεων(RARP). Τα αριθμημένα ACLs με εύρος 200-299 χρησιμοποιήθηκαν για τον έλεγχο της κυκλοφορίας, σύμφωνα με τον τύπο Ethernet. (Davies et al, 2012)

Επίσης, ήταν κοινή η δημιουργία ACLs βάση των διευθύνσεων MAC.Ένα ACL αριθμημένο 700-799 υποδεικνύει τη κίνηση που ταξινομείται και ελέγχεται με βάση τις διευθύνσεις MAC. Μετά τον καθορισμό του τύπου της ταξινόμησης, οι παράμετροι ελέγχου που απαιτούνται γι αυτό το ACL μπορούν να οριστούν. Για παράδειγμα, ένα ACL αριθμημένο 700-799 θα μπορούσε να χρησιμοποιηθεί για να εμποδίσει έναν πελάτη με μια συγκεκριμένη διεύθυνση MAC από τη σύνδεση με ένα προκαθορισμένο σημείο πρόσβασης. Σήμερα, κατά την ταξινόμηση της κυκλοφορίας, τα πιο κοινά είδη παραμέτρων που χρησιμοποιούνται στα ACLs που

σχετίζονται με την ασφάλεια περιλαμβάνουν διευθύνσεις IPv4 και IPv6 καθώς και αριθμούς θυρών TCP και UDP. Για παράδειγμα, ένα ACL μπορεί να επιτρέπει σε όλους τους χρήστες με μια συγκεκριμένη διεύθυνση δικτύου IP να κατεβάσουν αρχεία από το Internet χρησιμοποιώντας ασφαλές FTP. Το ίδιο ACL μπορεί να χρησιμοποιηθεί για να αρνηθεί όλες τις διευθύνσεις IP από την παραδοσιακή πρόσβαση FTP. (Davies et al, 2012)

3.4. Standard ACLs

Τα ACLs αριθμημένα 1-99 ή 1300-1999 είναι IPv4 ACLs πρότυπα. Τα Standard ACLs ταιριάζουν τα πακέτα εξετάζοντας το πεδίο προέλευσης της διεύθυνσης IP στην κεφαλίδα IP αυτού του πακέτου. Αυτά τα ACLs χρησιμοποιούνται για το φιλτράρισμα πακέτων που βασίζονται αποκλειστικά στην πηγή πληροφορίας του Layer 3. (Csico Tools, 2012)

Η πρώτη τιμή καθορίζει τον αριθμό ACL.Η δεύτερη τιμή καθορίζει εάν θα επιτρέψει ή αρνηθεί την διαμορφωμένη κίνηση της IP διεύθυνσης πηγής. Η τρίτη τιμή είναι η IP διεύθυνση πηγής που πρέπει να ταιριαστεί. Η τέταρτη τιμή είναι η wildcard mask που πρέπει να εφαρμοστεί στην προηγουμένως διαμορφωμένη διεύθυνση IP για να δείξει το εύρος. (Davies et al, 2012)

Extended ACLs" Τα Extended ACLs ταιριάζουν τα πακέτα που βασίζονται στην πληροφορία πηγής και προορισμού του Layer 3 και Layer 4. Η πληροφορία του Layer 4 μπορεί να περιλαμβάνει την TCP και UDP πληροφορία θύρας. Τα Extended ACLs δίνουν μεγαλύτερη ευελιξία και έλεγχο πρόσβασης στο δίκτυο από τα standard ACLs.

Παρόμοιο με τα standard ACLs, η πρώτη τιμή καθορίζει τον αριθμό ACL.Τα ACLs αριθμημένα 100-199 ή 2000-2699 είναι extended ACLs.Η επόμενη τιμή καθορίζει αν θα επιτρέψει ή αρνηθεί σύμφωνα με τα κριτήρια που ακολουθεί. Η

τρίτη τιμή υποδεικνύει τον τύπο πρωτοκόλλου. Ο διαχειριστής πρέπει να ορίσει τα IP, TCP, UDP, ή άλλα συγκεκριμένα IP υπο-πρωτόκολλα. Η IP διεύθυνση πηγής και η wildcard mask καθορίζουν από που προέρχεται η κυκλοφορία. Η IP διεύθυνση προορισμού και η wildcard mask της χρησιμοποιούνται για να υποδείξουν τον τελικό προορισμό της κίνησης του δικτύου. Παρά το γεγονός ότι η παράμετρος θύρας ορίζεται ως προαιρετική, εάν ο διαχειριστής δεν προσδιορίζει την θύρα είτε από αριθμό ή με ένα πολύ γνωστό όνομα θύρας, το σύνολο της κίνησης στο συγκεκριμένο προορισμό θα πρέπει είτε να πέσει ή να επιτραπεί. Όλα τα ACLs λαμβάνουν μια σιωπηρή άρνηση, πράγμα που σημαίνει ότι αν ένα πακέτο δεν ταιριάζει με κανένα από τα κριτήρια που καθορίζονται στο ACL,το πακέτο απορρίπτεται. Μετά τη δημιουργία ενός ACL,συμπεριλάμβανε τουλάχιστον μία δήλωση άδειας, διαφορετικά όλη η κυκλοφορία θα πέσει όταν το ACL εφαρμοστεί σε μια διεπαφή. (Alfaro et al, 2008)

Τα standard και extended ACLs μπορούν να χρησιμοποιηθούν για να περιγράψουν τα πακέτα που εισέρχονται ή εξέρχονται από μια διεπαφή. Η λίστα ερευνάται σειριακά. Η πρώτη δήλωση που ταιριάζει σταματά την αναζήτηση μέσα από τη λίστα και καθορίζει τη δράση που πρέπει να ληφθεί. Μετά τη δημιουργία του standard ή extended ACL, ο διαχειριστής θα πρέπει να το εφαρμόσει στην κατάλληλη διεπαφή.

Σε σύγκριση με τα standard ACLs, τα extended ACLs επιτρέπουν για συγκεκριμένους τύπους κίνησης να αρνηθεί ή να επιτραπεί. Φανταστείτε ένα σενάριο στο οποίο η κίνηση FTP από ένα υποδίκτυο πρέπει να αμφισβητηθεί σε ένα άλλο υποδίκτυο. Σε αυτήν την περίπτωση, ένα extended ACL απαιτείται επειδή ένας συγκεκριμένος τύπος κυκλοφορίας φιλτράρεται.

Σ'αυτό το ACL,η FTP πρόσβαση αμφισβητείται από το υποδίκτυο 172.16.4.0/24 στο υποδίκτυο 172.16.3.0/24. Όλη η άλλη κυκλοφορία επιτρέπεται. Η TCP θύρα 21 χρησιμοποιείται για εντολές προγράμματος FTP.Η TCP θύρα 20 χρησιμοποιείται για τη μεταφορά δεδομένων FTP. Και οι δύο θύρες

αμφισβητούνται. Μία κατάσταση απαιτείται στο τέλος του ACL. Αλλιώς,όλη η κυκλοφορία αμφισβητείται λόγω της σιωπηρής αρνήσεως.

Η καλύτερη τοποθέτηση αυτού του ACL είναι εισερχόμενη στη διεπαφή Fa0/1. Αυτό εξασφαλίζει ότι η ανεπιθύμητη κίνηση FTP πέφτει πριν από τη σπατάλη πόρων επεξεργασίας του δρομολογητή. Λάβετε υπόψη ,με αυτό το ACL,μία καταχώρηση στο τέλος κάθε ACL.Αυτό σημαίνει ότι όλη η άλλη κυκλοφορία, συμπεριλαμβανομένης της κυκλοφορίας FTP που προέρχεται από το δίκτυο 172.16.4.0/24 που προορίζεται για κάθε δίκτυο, εκτός από το δίκτυο 172.16.3.0/24,θα πρέπει να επιτρέπεται.

Με την πάροδο του χρόνου, οι μηχανικοί έχουν δημιουργήσει πιο εξελιγμένες μορφές φίλτρων ελέγχου πρόσβασης που βασίζονται σε ολοένα και πιο ακριβείς παραμέτρους. Οι μηχανικοί έχουν επίσης επεκτείνει το φάσμα των πλατφορμών και το εύρος των ACLs τα οποία μπορούν να υποβληθούν σε επεξεργασία με την ταχύτητα του σύρματος. Αυτές οι βελτιώσεις στις πλατφόρμες και τα ACLs επιτρέπουν στους επαγγελματίες της ασφάλειας του δικτύου στην εφαρμογή λύσεων αιχμής τείχους προστασίας, χωρίς να θυσιάζεται η απόδοση του δικτύου. Σ'ένα σύγχρονο δίκτυο, ένα τείχος προστασίας του δικτύου πρέπει να τοποθετείται μεταξύ του εσωτερικού του δικτύου και του εξωτερικού του δικτύου. Η βασική ιδέα είναι ότι όλη η κυκλοφορία από το εξωτερικό θα πρέπει να αποκλειστεί από την είσοδό της στο εσωτερικό, εκτός εάν αυτό επιτρέπεται ρητά από ένα ACL, ή εάν η επιστρεφόμενη κίνηση ξεκινά από το εσωτερικό του δικτύου. Αυτός είναι ο θεμελιώδης ρόλος ενός τείχους προστασίας του δικτύου, είτε είναι μια ειδική συσκευή υλικού είτε ένας δρομολογητής Cisco με IOS τείχος προστασίας.

Πολλές εφαρμογές βασίζονται στο πρωτόκολλο TCP,το οποίο χτίζει ένα εικονικό κύκλωμα μεταξύ δύο τελικών σημείων. Η πρώτη γενιά λύσης φιλτραρίσματος της κυκλοφορίας IOS που υποστήριζε την αμφίδρομη φύση των TCP εικονικών κυκλωμάτων ήταν η TCP λέξη-κλειδί για επεκτάσιμα IP ACLs. Δημιουργήθηκαν το 1995, η TCP λέξη-κλειδί για επεκτάσιμα IP ACLs επέτρεψε ένα

πρωτόγονο τείχος προστασίας του δικτύου να δημιουργηθεί σ'έναν δρομολογητή Cisco. Απέκλεισε κάθε κίνηση που προέρχεται από το Διαδίκτυο, εκτός από την TCP reply κυκλοφορία που σχετίζεται με την καθιερωμένη TCP κυκλοφορία που ξεκίνησε από το εσωτερικό του δικτύου. (Meiners et al 2010)

Η δεύτερη γενιά IOS λύσης για το φιλτράρισμα της συνόδου ήταν τα reflexive ACLs. Τα Reflexive ACLs εισήχθησαν στο IOS το 1996. Αυτό το φίλτρο κυκλοφορίας των ACLs βασίζεται σε διευθύνσεις πηγής και προορισμού, καθώς και σε αριθμούς θυρών και παρακολουθεί τις συνεδρίες. Το φιλτράρισμα συνεδρίας του Reflexive ACL χρησιμοποιεί προσωρινά φίλτρα που αφαιρούνται όταν μια συνεδρία έχει τελειώσει. Η TCP επιλογή και τα reflexive ACLs είναι παραδείγματα πολύπλοκων ACLs.

3.4.1. Μετρητής ACL

Ένας ACL μετρητής μετράει πόσα πακέτα ταιριάζουν (επιτρέπονται ή απαγορεύονται) από κάθε γραμμή του ACL. Ο αριθμός αυτός εμφανίζεται ως ο αριθμός των matches. Με τον έλεγχο του αριθμού των matches με την εντολή, ένας διαχειριστής μπορεί να καθορίσει αν το ρυθμισμένο πρότυπο και τα extended IP ACLs φιλτράρονται σωστά. Για παράδειγμα, εάν μια καταχώρηση έχει σημαντικά περισσότερα matches απ'ότι αναμενόταν, η καταχώρηση μπορεί να είναι υπερβολικά ευρεία. Αυτό θα μπορούσε να σημαίνει ότι το ACL δεν έχει το επιδιωκόμενο αποτέλεσμα στην κίνηση του δικτύου. (Meiners et al 2010)

Το DNS, SMTP, και FTP είναι κοινές υπηρεσίες που συχνά πρέπει να επιτρέπονται μέσω του τείχους προστασίας. Επίσης, είναι αρκετά κοινό ότι ένα τείχος προστασίας χρειάζεται να ρυθμιστεί ώστε να επιτρέπει πρωτόκολλα που είναι απαραίτητα για τη διαχείριση ενός δρομολογητή. Για παράδειγμα, μπορεί να είναι αναγκαίο να επιτρέψει την κυκλοφορία μέσω ενός εσωτερικού δρομολογητή

που επιτρέπει την κυκλοφορία συντήρησης δρομολογητή από μια εξωτερική συσκευή. Το Telnet, SSH, syslog, και SNMP είναι παραδείγματα υπηρεσιών που ένας δρομολογητής ίσως πρέπει να συμπεριλάβει. Το SSH πάντα προτιμάται σε σχέση με το Telnet. Κρατήστε κατά νου, ενώ πολλές απ'αυτές τις υπηρεσίες είναι χρήσιμες, είναι σημαντικό να ελέγχονται και να παρακολουθούνται, καθώς η εκμετάλλευση των υπηρεσιών αυτών οδηγεί σε ευπάθειες ασφαλείας.

Οι χάκερ χρησιμοποιούν διάφορους τύπους μηνυμάτων ICMP για να επιτεθούν δίκτυα. Ωστόσο, διάφορες εφαρμογές διαχείρισης χρησιμοποιούν μηνύματα ICMP για τη συλλογή πληροφοριών. Η διαχείριση δικτύου χρησιμοποιεί μηνύματα ICMP που δημιουργούνται αυτόματα από το δρομολογητή. Οι χάκερ μπορούν να χρησιμοποιούν πακέτα ICMP echo για να ανακαλύψουν υποδίκτυα και hosts σ'ένα προστατευμένο δίκτυο και να δημιουργήσουν DoS flood επιθέσεις. Οι χάκερ μπορούν να χρησιμοποιούν μηνύματα ανακατεύθυνσης ICMP για να αλλάξουν τους πίνακες δρομολόγησης υποδοχής. Τόσο τα μηνύματα echo όσο και τα ανακατεύθυνσης ICMP θα πρέπει να μπλοκάρονται εισερχόμενα από το δρομολογητή. Πολλά μηνύματα ICMP συνιστώνται για τη σωστή λειτουργία του δικτύου και θα πρέπει να επιτρέπονται εισερχόμενα:

Echo reply: Επιτρέπει στους χρήστες να κάνου ping εξωτερικούς hosts.

Source quench: Ζητάει από τον αποστολέα να μειώσει το ποσοστό της κυκλοφορίας των μηνυμάτων.

Unreachable: Τα μηνύματα που δεν μπορούν να προσεγγιστούν δημιουργούνται για τα πακέτα που έχουν αρνηθεί διαχειριστικά από ένα ACL. Πολλά μηνύματα ICMP απαιτούνται για τη σωστή λειτουργία του δικτύου και θα πρέπει να να επιτρέπονται εξερχόμενα:

Echo Επιτρέπει στους χρήστες να κάνουν ping εξωτερικούς hosts.

Parameter problem: Ενημερώνει τον host για τα προβλήματα της κεφαλίδας του πακέτου.

Packet too big: Απαραίτητο για την ανακάλυψη πακέτου maximum transmission unit (MTU).

Source quench: Μειώνει την κυκλοφορία, όταν είναι αναγκαίο. Κατά κανόνα, μπλοκάρει όλα τα άλλα είδη μηνυμάτων ICMP εξερχόμενα. Τα ACLs χρησιμοποιούνται για να εμποδίσουν το spoofing της IP διεύθυνσης, επιλεκτικά επιτρέψουν συγκεκριμένες υπηρεσίες μέσω ενός τείχους προστασίας και να επιτρέψουν μόνο τα υποχρεωτικά μηνύματα ICMP.

Τα πρωτόκολλα διαχείρισης όπως το SNMP, ενώ είναι χρήσιμα για απομακρυσμένη παρακολούθηση και διαχείριση των δικτυακών συσκευών, μπορεί να αξιοποιηθούν. Αν το SNMP είναι αναγκαίο, η εκμετάλλευση των τρωτών σημείων του SNMP μπορούν να μετριαστούν με την εφαρμογή της διεπαφής των ACLs για το φιλτράρισμα πακέτων SNMP από μη εγκεκριμένα συστήματα. Το ACL μπορεί στη συνέχεια να επιτρέψει γνωστές διευθύνσεις προέλευσης που προορίζονται για την ίδια την iOS συσκευή, όπως αυτές τις συσκευές σ'ένα δίκτυο διαχείρισης. Θα πρέπει να σημειωθεί ότι ένα exploit μπορεί να εξακολουθεί να είναι δυνατό εάν το πακέτο SNMP προέρχεται από μια διεύθυνση που έχει εξαπατηθεί και επιτρέπεται από το ACL. Αν και τα μέτρα ασφαλείας είναι χρήσιμα, το πιο αποτελεσματικό μέσο για την πρόληψη της εκμετάλλευσης είναι η απενεργοποίηση του διακομιστή SNMP για τις συσκευές iOS που δεν το χρειάζονται. (Radack, 2009)

3.5. Ασφάλεια δικτύου με χρήση Firewall

3.5.1. Τεχνολογίες Firewall

Ο όρος τοίχος προστασίας αρχικά αναφερόταν σε ένα πυρίμαχο τοίχωμα(συνήθως κατασκευασμένο από πέτρα ή μέταλλο) που εμπόδισε τις φλόγες από την εξάπλωση σε συνδεδεμένες δομές. Αργότερα ο όρος τοίχος προστασίας εφαρμόστηκε στο μεταλλικό φύλλο που χώριζε το μέρος του κινητήρα του οχήματος ή αεροσκάφους από το θάλαμο επιβατών. Τελικά ο όρος προσαρμόστηκε για χρήση με τα δίκτυα υπολογιστών: ένα τείχος προστασίας εμποδίζει την ανεπιθύμητη κυκλοφορία από την είσοδο σε προβλεπόμενες περιοχές μέσα σε ένα δίκτυο.

Ένα τείχος προστασίας είναι ένα σύστημα ή μια ομάδα συστημάτων που επιβάλλει μια πολιτική ελέγχου πρόσβασης μεταξύ των δικτύων. Αυτό μπορεί να περιλαμβάνει επιλογές, όπως ένα φιλτράρισμα πακέτων δρομολογητή, ένα διακόπτη με δύο VLANs και πολλούς κεντρικούς υπολογιστές με λογισμικό τοίχου προστασίας. Τα τείχη προστασίας είναι διαφορετικά πράγματα σε διαφορετικούς ανθρώπους και οργανισμούς, αλλά όλα τα τείχη προστασίας έχουν κάποια κοινά χαρακτηριστικά:

Είναι ανθεκτικά σε επιθέσεις: Είναι το μόνο σημείο διέλευσης μεταξύ των δικτύων(όλη η κυκλοφορία ρέει μέσω του τείχους προστασίας).<

Επιβάλλουν την πολιτική ελέγχου πρόσβασης. Το 1988, η DEC δημιούργησε το πρώτο τείχος προστασίας δικτύου, με τη μορφή ενός packet filter firewall. Αυτά τα πρώτα τείχη προστασίας επιθεωρούσαν τα πακέτα για να δουν αν ταιριάζουν τα σύνολα κανόνων, με την επιλογή της προώθησης ή κατάργησης των πακέτων ανάλογα. Αυτό το είδος φιλτραρίσματος πακέτων, που είναι γνωστό ως stateless filtering, λαμβάνει χώρα ανεξάρτητα από το αν ένα πακέτο είναι μέρος μιας υπάρχουσας ροής δεδομένων. Κάθε πακέτο που φιλτράρεται βασίζεται αποκλειστικά στις τιμές ορισμένων παραμέτρων στην επικεφαλίδα του πακέτου, παρόμοιο με το πώς τα ACLs φιλτράρει πακέτα. Το 1989, η AT&T Bell Laboratories ανέπτυξε το πρώτο stateful firewall. (Radack, 2009)

Τα stateful firewalls φιλτράρουν τα πακέτα σε πληροφορίες που είναι αποθηκευμένες στο τείχος προστασίας με βάση τα στοιχεία που ρέουν μέσω του τείχους προστασίας. Τα stateful firewalls είναι σε θέση να καθορίσουν αν ένα πακέτο ανήκει σε μια υπάρχουσα ροή των δεδομένων. Οι στατικοί κανόνες, όπως στα packet filter firewalls, συμπληρώνονται με δυναμικούς κανόνες που δημιουργούνται σε πραγματικό χρόνο για να καθορίσουν αυτές τις δραστικές ροές. Τα stateful firewalls συμβάλουν στην καταπολέμηση των DoS επιθέσεων που εκμεταλλεύονται τις ενεργές συνδέσεις μέσω μιας συσκευής δικτύωσης.

Τα αρχικά τείχη προστασίας δεν ήταν αυτόνομες συσκευές, αλλά δρομολογητές ή servers με χαρακτηριστικά λογισμικού που προστίθενται για να παρέχουν λειτουργικότητα του τείχους προστασίας. Με την πάροδο του χρόνου, πολλές εταιρείες ανέπτυξαν αυτόνομα τείχη προστασίας. Οι ειδικές συσκευές τοίχους προστασίας ενεργοποίησαν δρομολογητές και διακόπτες για να ξεφορτώσουν την μνήμη και την υψηλής έντασης δραστηριότητα του επεξεργαστή του φιλτραρίσματος πακέτων. Οι σύγχρονοι δρομολογητές, όπως τα Cisco Integrated Services Routers (ISRs), μπορούν επίσης να χρησιμοποιηθούν ως εξελιγμένα stateful firewalls για οργανισμούς που ίσως δεν απαιτούν ένα ειδικό τείχος προστασίας.

Υπάρχουν πολλά οφέλη από τη χρήση ενός τείχους προστασίας σε ένα δίκτυο:

Η έκθεση των ευαίσθητων hosts και εφαρμογών σε μη έμπιστους χρήστες μπορεί να προληφθεί.

Η ροή πρωτοκόλλου μπορεί να εξυγιανθεί, με την πρόληψη της εκμετάλλευσης των ατελειών πρωτοκόλλου. Τα κακόβουλα δεδομένα μπορεί να μπλοκαριστούν από τους διακομιστές και τους πελάτες.

Η επιβολή της πολιτικής ασφαλείας μπορεί να γίνει απλή, επεκτάσιμη και ισχυρή με ένα σωστά ρυθμισμένο firewall.

Η επιβάρυνση του μεγαλύτερου μέρους του ελέγχου της πρόσβασης δικτύου σε μερικά σημεία στο δίκτυο μπορεί να μειώσει την πολυπλοκότητα της διαχείρισης της ασφάλειας.

Τα firewalls παρουσιάζουν επίσης ορισμένους περιορισμούς:

Αν δεν είναι σωστά ρυθμισμένο, ένα τείχος προστασίας μπορεί να έχει σοβαρές συνέπειες(μοναδικό σημείο αποτυχίας).

Τα δεδομένα από πολλές εφαρμογές δεν μπορούν να περάσουν πάνω από τα τείχη προστασίας με ασφάλεια.

Οι χρήστες ενδέχεται προληπτικά να αναζητήσουν τρόπους γύρω από το τείχος προστασίας για να λαμβάνουν αποκλεισμένο υλικό, εκθέτοντας το δίκτυο σε πιθανή επίθεση.

Η επίδοση του δικτύου μπορεί να επιβραδύνει.

Μη εξουσιοδοτημένη κίνηση μπορεί να διοχετευτεί ή κρυφτεί ως νόμιμη κίνηση μέσω του τείχους προστασίας.

Είναι σημαντικό να κατανοήσουμε τους διαφορετικούς τύπους των firewalls και των ειδικών ικανοτήτων τους, έτσι ώστε το σωστό firewall να χρησιμοποιείται σε κάθε κατάσταση.

3.5.2. Τύποι Firewall

Ένα σύστημα firewall μπορεί να αποτελείται από πολλές διαφορετικές συσκευές και εξαρτήματα. Ένα εξάρτημα είναι το φιλτράρισμα της κυκλοφορίας, το οποίο είναι αυτό που οι περισσότεροι άνθρωποι συνήθως ονομάζουν ένα τείχος προστασίας.

Τα ακόλουθα τέσσερα τείχη προστασίας καλύπτονται σε αυτό το κεφάλαιο (Fox et al, 2009):

Packet filtering firewall : Συνήθως είναι ένας δρομολογητής με την ικανότητα να φιλτράρει κάποιο περιεχόμενο του πακέτου, όπως Layer 3 και μερικές φορές Layer 4 πληροφορία.

Stateful firewall: Παρακολουθεί την κατάσταση των συνδέσεων, αν η σύνδεση είναι μια εισαγωγή, μεταφορά δεδομένων, ή κατάσταση τερματισμού.

Application gateway firewall (proxy firewall): Ένα firewall που φιλτράρει τις πληροφορίες στα Layers 3, 4, 5, και 7 του μοντέλου αναφοράς OSI. Το μεγαλύτερο μέρος του ελέγχου και το φιλτράρισμα του τείχους προστασίας γίνεται στο λογισμικό.

Μετάφραση διευθύνσεων δικτύου (NAT) firewall:Ένα τείχος που επεκτείνει τον αριθμό των διαθέσιμων IP διευθύνσεων και κρύβει το σχεδιασμό της διευθυνσιοδότησης δικτύου.

Άλλες μέθοδοι εφαρμογής firewalls περιλαμβάνουν: Host-based (server και personal) firewall. Ένα PC ή server με λογισμικό τείχους προστασίας που τρέχει σ'αυτό.

Transparent firewall: Ένα τοίχος προστασίας που φιλτράρει την IP κυκλοφορία μεταξύ ενός ζεύγους bridged διεπαφών.

Hybrid firewall: Ένα τείχος προστασίας που είναι ένας συνδυασμός διαφόρων τύπων τειχών προστασίας. Για παράδειγμα, ένα application inspection firewall συνδυάζει ένα stateful firewall μ'ένα application gateway firewall.

Δεδομένου ότι η ασφάλεια δικτύων έγινε αναπόσπαστο μέρος της καθημερινής λειτουργίας, συσκευές αποκλειστικά σε συγκεκριμένες λειτουργίες ασφάλειας δικτύων προέκυψαν. Ένα από τα πρώτα εργαλεία για την ασφάλεια

δικτύων ήταν το σύστημα ανίχνευσης εισβολής(IDS),που αναπτύχθηκε για πρώτη φορά από την SRI International το 1984. Ένα IDS παρέχει σε πραγματικό χρόνο ανίχνευση ορισμένων τύπων επιθέσεων, ενώ βρίσκονται σε εξέλιξη. Αυτή η ανίχνευση επιτρέπει στους επαγγελματίες της ασφάλειας δικτύων την πιο γρήγορη καταπολέμηση των αρνητικών επιπτώσεων από αυτές τις επιθέσεις σε συσκευές δικτύου και στους χρήστες. Στα τέλη της δεκαετίας του 1990,το σύστημα πρόληψης της διείσδυσης ή του αισθητήρα (IPS),άρχισε να αντικαθιστά τη λύση του IDS. Οι συσκευές IPS επιτρέπουν την ανίχνευση της κακόβουλης δραστηριότητας και έχουν την ικανότητα να μπλοκάρουν αυτόματα την επίθεση σε πραγματικό χρόνο. Εκτός από τις λύσεις του IDS και IPS, τα firewalls(τείχος προστασίας δικτύων) αναπτύχθηκαν για να αποτρέψουν την ανεπιθύμητη κυκλοφορία από την είσοδο που προβλέπονται περιοχές εντός ενός δικτύου, παρέχοντας έτσι περιμετρική ασφάλεια. Το 1988,η Digital Equipment Corporation (DEC) δημιούργησε το πρώτο τείχος προστασίας δικτύων, με τη μορφή ενός φίλτρου πακέτων. Τα πρώτα αυτά firewalls έλεγχαν τα πακέτα για να δούν αν ταιριάζουν τα σύνολα των προκαθορισμένων κανόνων, με την επιλογή της αποστολής ή κατάργησης των πακέτων αναλόγως. (Fernandez, 2008)

Τα Firewalls φιλτραρίσματος πακέτων ελέγχουν κάθε πακέτο σε απομόνωση χωρίς να εξετάσουν αν ένα πακέτο είναι μέρος μιας υπάρχουσας σύνδεσης. Το 1989,η AT & T Bell Laboratories ανέπτυξε το πρώτο stateful firewall. Όπως τα firewalls φιλτραρίσματος πακέτων, τα stateful firewalls χρησιμοποιούν προκαθορισμένους κανόνες για τη χορήγηση ή την απόρριψη της κυκλοφορίας.Σε αντίθεση με τα firewalls φιλτραρίσματος πακέτων,τα stateful firewalls παρακολουθούν εγκατεστημένες συνδέσεις και καθορίζουν αν ένα πακέτο ανήκει σε μια υπάρχουσα ροή δεδομένων, παρέχοντας μεγαλύτερη ασφάλεια και ταχεία επεξεργασία. Τα πρωτότυπα firewals ήταν χαρακτηριστικά λογισμικού που προστέθηκαν σε μια υπάρχουσα δικτύωση συσκευών, όπως οι δρομολογητές(routers). Με τον καιρό, πολλές εταιρείες ανάπτυξαν αυτόνομα, ή "προσηλωμένα"(dedicated) firewalls που ενεργοποιούσαν δρομολογητές(routers)

και διακόπτες(switches) για να απαλλαγούν από τη μνήμη και τον επεξεργαστή υψηλής έντασης των πακέτων φιλτραρίσματος. Το Adaptive Security Appliance της Cisco(ASA) είναι διαθέσιμο ως αυτόνομο firewall "επίγνωσης πλαισίου". Για τους οργανισμούς που δεν απαιτούν "προσηλωμένα"(dedicated) firewals,τα σύγχρονα routers, όπως το Integrated Services Router της Cisco(ISR),μπορούν να χρησιμοποιηθούν ως εξελιγμένα firewalls "επίγνωσης πλαισίου".

Η παραδοσιακή ασφάλεια βασίστηκε στη διαστρωμάτωση των προϊόντων και στη χρήση πολλαπλών φίλτρων. Ωστόσο, καθώς οι απειλές έγιναν πιο εξελιγμένες, αυτά τα φίλτρα απαιτήθηκαν για να εξεταστούν βαθύτερα τα επίπεδα ροής Δικτύων και Εφαρμογών. Οι απαιτήσεις ασφάλειας περιελάμβαναν πιο δυναμικές ενημερώσεις των πληροφοριών και μικρότερους χρόνους αντίδρασης σε απειλές. Για το λόγο αυτό, η Cisco σχεδίασε το Security Intelligence Operations(SIO).Το SIO είναι μια cloud- based υπηρεσία που συνδέει παγκόσμια πληροφορίες απειλών, υπηρεσίες με βάση τη φήμη και εμπεριστατωμένη ανάλυση για τις συσκευές ασφαλείας δικτύων της Cisco για την παροχή ισχυρότερης προστασίας με ταχύτερους χρόνους απόκρισης. (Fox et al, 2009)

Εκτός από την αντιμετώπιση των απειλών εκτός του δικτύου, οι επαγγελματίες της ασφάλειας δικτύων πρέπει επίσης να είναι προετοιμασμένοι για τις απειλές στο εσωτερικό του δικτύου .Οι εσωτερικές απειλές, είτε σκόπιμες είτε τυχαίες, μπορούν να προκαλέσουν ακόμη μεγαλύτερη ζημιά από ό, τι οι εξωτερικές απειλές λόγω της άμεσης πρόσβασης σε αυτά και τη γνώση του εταιρικού δικτύου και των δεδομένων. Παρά το γεγονός αυτό, έχει πάρει περισσότερα από 20 χρόνια μετά την εισαγωγή των εργαλείων και τεχνικών για την καταπολέμηση των εξωτερικών απειλών να αναπτυχθούν εργαλεία και τεχνικές για τον περιορισμό των εσωτερικών απειλών.

Ένα κοινό σενάριο για μια απειλή που προέρχεται από το εσωτερικό του δικτύου είναι ένας δυσαρεστημένος υπάλληλος με κάποιες τεχνικές δεξιότητες και την προθυμία να κάνει τη ζημιά. Οι περισσότερες απειλές από το εσωτερικό του

δικτύου αναμοχλεύουν πρωτόκολλα και τεχνολογίες που χρησιμοποιούνται για το τοπικό δίκτυο (LAN) ή την υποδομή μεταγωγής. Αυτές οι εσωτερικές απειλές εμπίπτουν σε δύο κατηγορίες (Storm, 2016) :

- Στην απάτη(spoofing) και
- στην άρνηση των υπηρεσιών(DoS).

Οι επιθέσεις απάτης(spoofing) είναι επιθέσεις κατά την οποία μία συσκευή επιχειρεί να εμφανιστεί σαν κάποια άλλη με το να παραποιεί τα στοιχεία. Για παράδειγμα ,το spoofing της διεύθυνσης MAC συμβαίνει όταν ένας υπολογιστής δέχεται πακέτα δεδομένων με βάση τη διεύθυνση MAC άλλου υπολογιστή. Οι επιθέσεις DoS κάνουν τους πόρους του υπολογιστή μη διαθέσιμους στους προβλεπόμενους χρήστες. Οι επιτιθέμενοι χρησιμοποιούν διάφορες μεθόδους για να εξαπολύσουν τις επιθέσεις DoS. (Storm, 2016)

3.6. Συστήματα ανίχνευσης και συστήματα πρόληψης εισβολής (Intrusion Detection Systems and Intrusion Prevention Systems)

Μία προσέγγιση για την πρόληψη των ιών και των "σκουληκιών" από την είσοδό τους σ' ένα δίκτυο είναι για έναν διαχειριστή να παρακολουθεί συνεχώς το δίκτυο και να αναλύει τα αρχεία καταγραφής που δημιουργούνται από τις συσκευές του δικτύου. Αυτή η λύση δεν είναι πολύ επεκτάσιμη. Μη αυτόματη ανάλυση των πληροφοριών του αρχείου καταγραφής είναι μια χρονοβόρα διαδικασία και παρέχει μια περιορισμένη εικόνα των επιθέσεων που ξεκίνησαν εναντίον ενός δικτύου. Ώσπου οι καταγραφές αναλύονται, η επίθεση έχει ήδη αρχίσει. Τα Συστήματα Ανίχνευσης Εισβολών (IDSs) υλοποιήθηκαν για να παρακολουθούν παθητικά την κίνηση στο δίκτυο. Μία IDS-enabled συσκευή αντιγράφει το ρεύμα της κυκλοφορίας και αναλύει την κυκλοφορία υπό παρακολούθηση παρά τα πραγματικά προωθούμενα πακέτα. Η εργασία χωρίς σύνδεση, συγκρίνει το

καταγεγραμμένο ρεύμα κυκλοφορίας με τις γνωστές κακόβουλες υπογραφές, παρόμοια με το λογισμικό που ελέγχει για ιούς.

Αυτό η offline IDS εφαρμογή αναφέρεται ως ετερόκλητη λειτουργία. Το πλεονέκτημα της λειτουργίας με ένα αντίγραφο της κίνησης είναι ότι το IDS δεν επηρεάζει αρνητικά την πραγματική ροή των πακέτων της διαβιβαζόμενης κίνησης. Το μειονέκτημα της λειτουργίας σ' ένα αντίγραφο της κίνησης είναι ότι το IDS δεν μπορεί να σταματήσει κακόβουλες single-packet επιθέσεις από την επίτευξη του στόχου πριν απαντήσει στην επίθεση. Ένα IDS απαιτεί συχνά βοήθεια από άλλες συσκευές δικτύωσης, όπως δρομολογητές και τείχη προστασίας, για να ανταποκριθεί σε μια επίθεση. Είναι καλύτερη η εφαρμογή μιας λύσης που ανιχνεύει και αντιμετωπίζει αμέσως ένα πρόβλημα δικτύου, όπως απαιτείται.

3.6.1. Intrusion Prevention Systems

Ένα σύστημα πρόληψης εισβολής (IPS) βασίζεται σε τεχνολογία IDS. Σε αντίθεση με το IDS, μια IPS συσκευή υλοποιείται σε inline λειτουργία. Αυτό σημαίνει ότι όλη η κίνηση εισόδου και εξόδου πρέπει να ρέει μέσα από αυτό για επεξεργασία. Ένα IPS δεν επιτρέπει τα πακέτα να εισέλθουν στην έμπιστη πλευρά του δικτύου, χωρίς πρώτα να αναλυθούν. Μπορεί να ανιχνεύσει και να αντιμετωπίσει άμεσα ένα πρόβλημα δικτύου, όπως απαιτείται. Ένα IPS παρακολουθεί την Layer 3 και Layer 4 κυκλοφορία και αναλύει τα περιεχόμενα και το ωφέλιμο φορτίο των πακέτων για πιο εξελιγμένες ενσωματωμένες επιθέσεις που θα μπορούσαν να περιλαμβάνουν κακόβουλο δεδομένα στα στρώματα 2 έως 7. Οι πλατφόρμες Cisco IPS χρησιμοποιούν ένα μίγμα των τεχνολογιών ανίχνευσης, συμπεριλαμβανομένου του signature-based, profile-based και ανάλυση πρωτοκόλλων ανίχνευσης εισβολής. Αυτή η βαθύτερη ανάλυση επιτρέπει το IPS να εντοπίζει, σταματάει και μπλοκάρει επιθέσεις που θα διαπερνούν μια παραδοσιακή συσκευή τείχους προστασίας. Όταν ένα πακέτο έρχεται μέσα από μια διεπαφή

σ'ένα IPS, αυτό το πακέτο δεν αποστέλλεται στην εξερχόμενη ή έμπιστη διεπαφή έως ότου να αναλυθεί το πακέτο.

Το πλεονέκτημα της λειτουργίας σε inline mode είναι ότι το IPS μπορεί να σταματήσει τις single-packet επιθέσεις από το να φθάσουν στον στόχο του συστήματος. Το μειονέκτημα είναι ότι ένα κακώς διαμορφωμένο IPS ή μια ακατάλληλη λύση IPS μπορεί να επηρεάσει αρνητικά τη ροή των πακέτων της διαβιβαζόμενης κυκλοφορίας. Η μεγαλύτερη διαφορά μεταξύ των IDS και IPS είναι ότι το IPS ανταποκρίνεται αμέσως και δεν επιτρέπει καμία κακόβουλη κυκλοφορία να περάσει, ενώ ένα IDS μπορεί να επιτρέψει κακόβουλη κυκλοφορίας να περάσει πριν απαντήσει.

Οι IDS και IPS τεχνολογίες μοιράζονται πολλά χαρακτηριστικά. Και οι δύο IDS και IPS τεχνολογίες αναπτύσσονται ως αισθητήρες. Ένας IDS ή IPS αισθητήρας μπορεί να είναι οποιοσδήποτε από τις ακόλουθες συσκευές: Δρομολογητής διαμορφωμένος με το Cisco IOS IPS λογισμικό. Συσκευή που έχει σχεδιαστεί ειδικά για να παρέχει ειδικές IDS ή IPS υπηρεσίες Μονάδα δικτύου που είναι εγκατεστημένη σε ένα προσαρμοστικό συσκευής ασφαλείας, διακόπτη ή δρομολογητή. Οι IDS και IPS τεχνολογίες χρησιμοποιούν υπογραφές για να εντοπίζουν μοτίβα της κακής χρήσης της κίνησης του δικτύου. Μια υπογραφή είναι ένα σύνολο κανόνων που χρησιμοποιεί ένα IDS ή IPS για την ανίχνευση τυπικής παρεμβατικής δραστηριότητας. Οι υπογραφές μπορεί να χρησιμοποιηθούν για την ανίχνευση σοβαρών παραβιάσεων της ασφάλειας, κοινές επιθέσεις στο δίκτυο, καθώς και τη συλλογή πληροφοριών. Οι IDS και IPS τεχνολογίες μπορούν να ανιχνεύσουν μοτίβα ατομικής υπογραφής (single-packet) ή μοτίβα σύνθετης υπογραφής (multi-packet). Ένας IPS αισθητήρας αντικαταστεί πλήρως έναν IDS αισθητήρα;

3.6.2. πλεονεκτήματα και μειονεκτήματα IDS

Ένα βασικό πλεονέκτημα μιας πλατφόρμας IDS είναι ότι έχει αναπτυχθεί σε promiscuous mode. Επειδή ο αισθητήρας IDS δεν είναι ενσωματωμένος, δεν έχει καμία επίπτωση στην απόδοση του δικτύου. Δεν εισάγει το latency, jitter, ή άλλα θέματα της κυκλοφοριακής ροής. Επιπλέον, εάν ένας αισθητήρας αποτύχει, αυτό δεν επηρεάζει τη λειτουργικότητα του δικτύου. Επηρεάζει μόνο την ικανότητα του IDS να αναλύσει τα δεδομένα. Αλλά υπάρχουν πολλά μειονεκτήματα από την ανάπτυξη μιας πλατφόρμας IDS σε promiscuous mode. Οι ενέργειες απόκρισης του IDS αισθητήρα δεν μπορούν να σταματήσουν το trigger πακέτο και δεν είναι εγγυημένα για να σταματήσουν μια σύνδεση. Επίσης, είναι λιγότερο χρήσιμες για τη διακοπή των ιών ηλεκτρονικού ταχυδρομείου και τις αυτοματοποιημένες επιθέσεις, όπως τα "σκουλήκια". Οι χρήστες που αναπτύσσουν ενέργειες απόκρισης του IDS αισθητήρα πρέπει να έχουν μια καλά μελετημένη πολιτική ασφάλειας, σε συνδυασμό με μια καλή επιχειρησιακή κατανόηση των IDS αναπτύξεών τους. Οι χρήστες πρέπει να περνούν το χρόνο του συντονίζοντας τους IDS αισθητήρες για να επιτύχουν τα αναμενόμενα επίπεδα ανίχνευσης εισβολής. Τέλος, επειδή οι αισθητήρες IDS δεν είναι inline, μια εφαρμογή IDS είναι πιο ευάλωτη σε τεχνικές υπεκφυγής της ασφάλειας δικτύου που χρησιμοποιείται από διάφορες μεθόδους σύνδεσης δικτύου. (Shankar et al, 2016)

3.6.3. IPS πλεονεκτήματα και μειονεκτήματα

Η ανάπτυξη μιας πλατφόρμας IPS σε λειτουργία inline έχει και πλεονεκτήματα και μειονεκτήματα. Ένα πλεονέκτημα σε σχέση με IDS είναι ότι ένας αισθητήρας IPS μπορεί να ρυθμιστεί ώστε να εκτελεί ένα packet drop που μπορεί να σταματήσει το trigger πακέτο, τα πακέτα σε μια σύνδεση, ή πακέτα από μια IP διεύθυνση προέλευσης. Επιπλέον, ένας αισθητήρας IPS μπορεί να χρησιμοποιήσει

τεχνικές κανονικοποίησης ρεύματος για τη μείωση ή την εξάλειψη πολλών δυνατοτήτων υπεκφυγής ασφαλείας δικτύου που υπάρχουν. Ένα μειονέκτημα του IPS είναι ότι τα σφάλματα, η αποτυχία, και η υπέρβαση του αισθητήρα IPS με πάρα πολύ κίνηση μπορεί να έχει αρνητική επίδραση στην απόδοση του δικτύου. Αυτό οφείλεται στο γεγονός ότι το IPS θα πρέπει να αναπτυχθεί inline και η κίνηση πρέπει να είναι σε θέση να περάσει μέσα από αυτό. Ένας αισθητήρας IPS μπορεί να επηρεάσει την απόδοση του δικτύου με την εισαγωγή του latency και jitter. Ένας αισθητήρας IPS πρέπει να είναι κατάλληλου μεγέθους και εφαρμοσμένος έτσι ώστε οι ευαίσθητες στον χρόνο εφαρμογές, όπως το VoIP, να μην επηρεάζονται αρνητικά(Shankar et al, 2016).

Deployment Considerations

Χρησιμοποιώντας μία αυτών των τεχνολογιών δεν αναιρεί τη χρήση του άλλου. Στην πραγματικότητα, οι IDS και IPS τεχνολογίες μπορούν να συμπληρώσουν η μία την άλλη. Για παράδειγμα, ένα IDS μπορεί να εφαρμοστεί για την επικύρωση της λειτουργίας του IPS, επειδή το IDS μπορεί να ρυθμιστεί για βαθύτερο έλεγχο πακέτου εκτός σύνδεσης. Αυτό επιτρέπει το IPS να επικεντρωθεί σε λιγότερα αλλά πιο κρίσιμα μοτίβα κίνησης inline. Αποφασίζοντας ποια εφαρμογή να χρησιμοποιήσετε βασίζεται στους στόχους ασφάλειας του οργανισμού, όπως αναφέρεται στην πολιτική ασφάλειας των δικτύων. (Shankar et al, 2016)

3.7. Ασφάλεια Ακραίου Δρομολογητή

Η εφαρμογή του ακραίου δρομολογητή ποικίλλει ανάλογα με το μέγεθος του οργανισμού και την πολυπλοκότητα της επιθυμητής ποιότητας σχεδιασμού του

δικτύου. Οι υλοποιήσεις του Router μπορούν να περιλαμβάνουν ένα ενιαίο router προστατεύοντας ένα ολόκληρο εσωτερικό του δικτύου ή δρομολογητή ως την πρώτη γραμμή άμυνας της προσέγγιση άμυνας σε βάθος. Ενιαία προσέγγιση Router. Στην ενιαία προσέγγιση router, ένα ενιαίο router συνδέει το προστατευόμενο δίκτυο, ή εσωτερικό LAN, στο Internet. Όλες οι πολιτικές ασφαλείας έχουν ρυθμιστεί σε αυτή τη συσκευή. Αυτό πιο συχνά αναπτύσσεται σε μικρότερες υλοποιήσεις site όπως κλάδοι και σελίδες SOHO. Σε μικρότερα δίκτυα, τα απαιτούμενα χαρακτηριστικά ασφαλείας μπορούν να υποστηριχθούν από τα ISRs χωρίς να εμποδίζουν τις επιδόσεις του δρομολογητή.

3.7.1. Προσέγγιση άμυνας σε βάθος

Μία προσέγγιση άμυνας σε βάθος είναι πιο ασφαλής από την ενιαία προσέγγιση router. Στην προσέγγιση αυτή, ο ακραίος δρομολογητής ενεργεί ως πρώτη γραμμή άμυνας και είναι γνωστός ως ένας δρομολογητής διαλογής. Περνάει όλες τις συνδέσεις που προορίζονται για την εσωτερική LAN στο τοίχο προστασίας. Η δεύτερη γραμμή άμυνας είναι το τείχος προστασίας. Το τείχος προστασίας συνήθως αντιλαμβάνεται όπου ο ακραίος δρομολογητής αφήνει κάτι ανοικτό και εκτελεί επιπλέον φιλτράρισμα. Παρέχει επιπλέον έλεγχο πρόσβασης με την παρακολούθηση της κατάστασης των συνδέσεων και ενεργεί ως σημείο ελέγχου της συσκευής. Ο ακραίος δρομολογητής έχει ένα σύνολο κανόνων που καθορίζει ποια κίνηση επιτρέπει και ποια αρνείται. Από προεπιλογή, το τείχος προστασίας αρνείται την έναρξη συνδέσεων από τα εξωτερικά(μη αξιόπιστα) δίκτυα στο εσωτερικό(αξιόπιστο) δίκτυο. Ωστόσο, επιτρέπει στους εσωτερικούς χρήστες να εγκαταστήσουν συνδέσεις με τα μη αξιόπιστα δίκτυα και επιτρέπει στις απαντήσεις να έρθουν πίσω από το τείχος προστασίας. Μπορεί επίσης να εκτελέσει έλεγχο ταυτότητας του χρήστη(έλεγχος ταυτότητας διακομιστή μεσολάβησης),όπου οι

χρήστες πρέπει να επικυρώνονται για να αποκτήσουν πρόσβαση σε πόρους του δικτύου.

3.7.2. Προσέγγιση DMZ

Μια παραλλαγή της προσέγγισης άμυνας σε βάθος είναι να προσφέρει μια ενδιάμεση περιοχή, που συχνά αποκαλείται η αποστρατικοποιημένη ζώνη(DMZ).Το DMZ μπορεί να χρησιμοποιηθεί για τους διακομιστές που πρέπει να είναι προσβάσιμοι από το διαδίκτυο ή κάποιο άλλο εξωτερικό δίκτυο. Το DMZ μπορεί να δημιουργηθεί ανάμεσα σε δύο δρομολογητές, με εσωτερικό δρομολογητή που συνδέεται με το προστατευόμενο δίκτυο και ενός εξωτερικού δρομολογητή που συνδέεται με το μη προστατευμένο δίκτυο. Εναλλακτικά,το DMZ μπορεί απλά να είναι μια πρόσθετη θύρα από ένα μόνο δρομολογητή. Το τείχος προστασίας, το οποίο βρίσκεται ανάμεσα στα προστατευόμενα και μη προστατευόμενα δίκτυα, έχει συσταθεί για να επιτρέπει τις απαραίτητες συνδέσεις(για παράδειγμα,HTTP) από τα εξωτερικά(μη αξιόπιστα) δίκτυα στους δημόσιους servers μέσα στο DMZ. Το τείχος προστασίας χρησιμεύει ως κύρια προστασία για όλες τις συσκευές στο DMZ. Στην προσέγγιση DMZ,ο δρομολογητής παρέχει κάποια προστασία με το φιλτράρισμα κάποιας κίνησης, αλλά αφήνει το μεγαλύτερο μέρος της προστασίας για το τείχος προστασίας. (Jalee, 2014)

ΚΕΦΑΛΑΙΟ 4- ΚΡΥΠΤΟΓΡΑΦΗΣΗ

4.1. Cryptographic Hashes

Μία συνάρτηση κατακερματισμού παίρνει δυαδικά δεδομένα, που ονομάζονται το μήνυμα, και παράγει μια συμπυκνωμένη αναπαράσταση, που

ονομάζεται message digest. Ο κατακερματισμός βασίζεται σε μια μονόδρομη μαθηματική συνάρτηση η οποία είναι σχετικά εύκολο να υπολογιστεί, αλλά σημαντικά πιο δύσκολο να αντιστραφεί. Η άλεση του καφέ είναι ένα καλό παράδειγμα μιας μονόδρομης συνάρτησης. Είναι εύκολη η άλεση κόκκων καφέ, αλλά είναι σχεδόν αδύνατη η τοποθέτηση όλων των μικροσκοπικών κομματιών μαζί για την ανοικοδόμηση των αρχικών κόκκων. (Jalee, 2014)

Η λειτουργία κρυπτογράφησης κατακερματισμού έχει σχεδιαστεί για να ελέγχει και να διασφαλίζει την ακεραιότητα των δεδομένων. Μπορεί επίσης να χρησιμοποιηθεί για την επαλήθευση ταυτότητας. Η διαδικασία παίρνει μια μεταβλητή μπλοκ δεδομένων και επιστρέφει ένα fixed-length bit string που ονομάζεται τιμή κατακερματισμού ή message digest.

Ο κατακερματισμός είναι παρόμοιος με τον υπολογισμό κυκλικού ελέγχου πλεονασμού (CRC) checksums, λλά είναι πολύ ισχυρότερος κρυπτογραφικά. Για παράδειγμα, δίνεται μια τιμή CRC, είναι εύκολο να παράγει δεδομένα με τον ίδιο CRC. Με συναρτήσεις κατακερματισμού, είναι υπολογιστικά ανέφικτο για δύο διαφορετικά σύνολα δεδομένων να καταλήξουν με την ίδια έξοδο κατακερματισμού. Κάθε φορά που τα δεδομένα αλλάζουν ή αλλοιώνονται, η τιμή κατακερματισμού αλλάζει επίσης. Εξαιτίας αυτού, οι κρυπτογραφικές τιμές κατακερματισμού καλούνται συχνά ψηφιακά αποτυπώματα. Μπορούν να χρησιμοποιηθούν για την ανίχνευση διπλών αρχείων δεδομένων, αλλαγές έκδοσης του αρχείου, και παρόμοιες εφαρμογές. Οι τιμές αυτές χρησιμοποιούνται για την προστασία από τυχαία ή σκόπιμη αλλαγή στα δεδομένα και από την τυχαία φθορά δεδομένων. Η λειτουργία κρυπτογράφησης κατακερματισμού εφαρμόζεται σε πολλές διαφορετικές καταστάσεις: Για την απόδειξη της γνησιότητας, όταν χρησιμοποιείται μ' ένα συμμετρικό μυστικό κλειδί ελέγχου ταυτότητας, όπως το IP Security(IPSec) ή πιστοποίηση δρομολόγησης πρωτοκόλλου. Για να παρέχει πιστοποίηση με τη δημιουργία one-time και μονόδρομων απαντήσεων στις προκλήσεις σε πρωτόκολλα ελέγχου ταυτότητας όπως το PPP Challenge Handshake

Authentication Protocol (CHAP). Για να παρέχει μια απόδειξη ελέγχου ακεραιότητας μηνύματος, όπως αυτά που χρησιμοποιούνται σε ψηφιακές υπογεγραμμένες συμβάσεις και πιστοποιητικά υποδομής δημόσιου κλειδιού (PKI), όπως αυτά που γίνονται δεκτά κατά την πρόσβαση σε ασφαλή τοποθεσία, χρησιμοποιώντας ένα πρόγραμμα περιήγησης.

Από μαθηματική άποψη, μια συνάρτηση κατακερματισμού (H) είναι μια διαδικασία που παίρνει μια είσοδο (χ) και επιστρέφει ένα σταθερού μεγέθους string, το οποίο ονομάζεται η τιμή κατακερματισμού. Μία κρυπτογραφική συνάρτηση κατακερματισμού θα πρέπει να έχει τις ακόλουθες ιδιότητες:

Η είσοδος μπορεί να είναι οποιουδήποτε μήκους.

Η έξοδος έχει ένα σταθερό μήκος.

Η H(x) είναι σχετικά εύκολο να υπολογιστεί για οποιαδήποτε δεδομένο χ.

Η H(x) είναι ένας τρόπος και όχι αναστρέψιμος.

Η H(x) είναι collision free, κάτι που σημαίνει ότι δύο διαφορετικές τιμές εισόδου θα οδηγήσουν σε διαφορετικές τιμές κατεκερματισμού.

Αν μια συνάρτηση κατακερματισμού είναι δύσκολο να αντιστραφεί, θεωρείται ένας μονόδρομος κατακερματισμός. Δύσκολο να αντιστραφεί σημαίνει ότι μια δεδομένη τιμή κατακερματισμού h, είναι υπολογιστικά ανέφικτο να βρεί κάποιο δεδομένο εισόδου, (x), έτσι ώστε η H(x) = h.

Οι συναρτήσεις κατακερματισμού είναι χρήσιμες όταν η διασφάλιση των δεδομένων δεν έχει αλλάξει κατά λάθος, αλλά δεν μπορούν να διασφαλίσουν ότι τα δεδομένα δεν έχουν αλλάξει σκόπιμα. Για παράδειγμα, ο αποστολέας επιθυμεί να διασφαλίσει ότι το μήνυμα δεν έχει αλλάξει στην πορεία του προς το δέκτη. Η συσκευή αποστολής εισάγει το μήνυμα σ 'έναν αλγόριθμο κατακερματισμού και υπολογίζει το σταθερού μήκους digest ή δακτυλικό αποτύπωμα. Τόσο το μήνυμα,

όσο και ο κατακερματισμός είναι σε απλό κείμενο. Αυτό το δακτυλικό αποτύπωμα συνδέεται στη συνέχεια στο μήνυμα και αποστέλλεται στο δέκτη. Η συσκευή λήψης αφαιρεί το δακτυλικό αποτύπωμα από το μήνυμα και εισάγει το μήνυμα στον ίδιο τον αλγόριθμο κατακερματισμού.

Αν ο κατακερματισμός που υπολογίζεται από τη συσκευή λήψης είναι ίσος μ'εκείνον που επισυνάπτεται στο μήνυμα, το μήνυμα δεν έχει αλλοιωθεί κατά τη μεταφορά. Όταν το μήνυμα διασχίζει το δίκτυο, ένας πιθανός εισβολέας θα μπορούσε να παρεμποδίσει το μήνυμα, να το αλλάξει, να υπολογίσει εκ νέου τον κατακερματισμό και να το προσαρτίσει στο μήνυμα. Ο κατακερματισμός αποτρέπει μόνο το μήνυμα από το να αλλάξει κατά λάθος, όπως από ένα σφάλμα επικοινωνίας. Δεν υπάρχει τίποτα το μοναδικό στον αποστολέα στη διαδικασία κατακερματισμού, έτσι ώστε ο καθένας να μπορεί να υπολογίσει ένα hash για κάθε δεδομένο, εφ 'όσον έχουν τη σωστή συνάρτηση κατεκερματισμού Αυτές είναι οι δύο γνωστές συναρτήσεις κατακερματισμού:< Message Digest 5 (MD5) με 128-bit digests Secure Hash Algorithm 1 (SHA-1) με 160-bit digests

4.2. Οργανισμοί ασφάλειας δικτύου

4.2.1. SANS

Η SANS ιδρύθηκε το 1989 ως μια συνεργατική έρευνα και ένας εκπαιδευτικός οργανισμός. Το επίκεντρο της SANS είναι η εκπαίδευση σε θέματα ασφάλειας πληροφοριών και πιστοποίησης. Η SANS αναπτύσσει την έρευνα εγγράφων σχετικά με διάφορες πτυχές της ασφάλειας των πληροφοριών. Μια σειρά από άτομα, από ελεγκτές και διαχειριστές του δικτύου μέχρι τον επικεφαλής υπάλληλο της ασφάλειας πληροφοριών, μοιράζουν μαθήματα και λύσεις σε διάφορα προβλήματα. Στην καρδιά του SANS βρίσκονται επαγγελματίες της

ασφάλειας σε ποικίλους παγκόσμιους οργανισμούς, από τις επιχειρήσεις ως τα πανεπιστήμια, που εργάζονται από κοινού για να βοηθήσουν ολόκληρη την κοινότητα της ασφάλειας πληροφοριών. (SANS, 2015)

Οι πόροι της SANS είναι σε μεγάλο βαθμό δωρεάν κατόπιν αιτήματος. Αυτοί περιλαμβάνουν το δημοφιλές Internet Storm Center,το σύστημα έγκαιρης προειδοποίησης Διαδικτύου, το NewsBites , η εβδομαδιαία σύνοψη των νέων @ Risk,η εβδομαδιαία σύνοψη ευπαθειών,flash προειδοποιήσεις ασφαλείας και πάνω από 1.200 βραβευμένες, πρωτότυπες ερευνητικές εργασίες. Η SANS αναπτύσσει μαθήματα ασφάλειας που μπορούν να ληφθούν για την προετοιμασία για την πιστοποίηση στη Παγκόσμια Διασφάλιση Πληροφοριών(GIAC) στον έλεγχο, τη διαχείριση, τη λειτουργία, τα νομικά θέματα, την διαχείριση της ασφάλειας και την ασφάλεια του λογισμικού. Το GIAC επικυρώνει τις δεξιότητες των επαγγελματιών της ασφάλειας δικτύων, που κυμαίνονται από το αρχικό επίπεδο της ασφάλειας πληροφοριών μέχρι τις προηγμένες περιοχές, όπως τον έλεγχο, την ανίχνευση εισβολέων, την αντιμετώπιση περιστατικών, τους τοίχους προστασίας και την περιμετρική προστασία, εγκληματολογία δεδομένων, τεχνικές χάκερ, την ασφάλεια λειτουργικών συστημάτων Windows και UNIX,την ασφάλεια λογισμικού και την κωδικοποίηση εφαρμογής. (SANS, 2015)

4.2.2. CERT

Το CERT αποτελεί μέρος του ομοσπονδιακά χρηματοδοτούμενου από τις ΗΠΑ Ινστιτούτου τεχνολογίας λογισμικού(SEI) στο Πανεπιστήμιο Carnegie Mellon.Το CERT είναι ναυλωμένο για να συνεργαστεί με την κοινότητα του Internet για τον εντοπισμό και την επίλυση περιστατικών ασφάλειας του υπολογιστή. Το "σκουλήκι" Morris ήταν κίνητρο για την δημιουργία της CERT με τις οδηγίες του Defense Advanced Research Projects Agency(DARPA).Το Κέντρο Συντονισμού CERT(CERT/CC) επικεντρώνεται στο συντονισμό της επικοινωνίας μεταξύ εμπειρογνωμόνων κατά τη

διάρκεια έκτακτης ανάγκης ασφάλειας για να βοηθήσουν στην πρόληψη μελλοντικών συμβάντων. Το CERT ανταποκρίνεται στα μείζονα συμβάντα ασφαλείας και αναλύει τα τρωτά σημεία του προϊόντος.

Το CERT εργάζεται για τη διαχείριση των αλλαγών που σχετίζονται με την τεχνική των εισβολέων και στη δυσκολία ανίχνευσης επιθέσεων και εντοπισμό των επιτιθέμενων. Το CERT αναπτύσσει και προωθεί τη χρήση κατάλληλων πρακτικών διαχείρισης της τεχνολογίας και των συστημάτων να αντισταθούν στις επιθέσεις δικτυωμένων συστημάτων, για τον περιορισμό των ζημιών, καθώς και την εξασφάλιση της συνέχειας των υπηρεσιών.

Το CERT επικεντρώνεται σε πέντε τομείς:

a) Την διασφάλιση του λογισμικού, την ασφάλεια των συστημάτων
b) την οργανωτική ασφάλεια
c) την συντονισμένη απόκριση
d) την εκπαίδευση και
e) την κατάρτιση.

Το CERT διαδίδει πληροφορίες με τη δημοσίευση άρθρων, εκθέσεων έρευνας και τεχνικών, καθώς και έγγραφα σχετικά με μια ποικιλία θεμάτων ασφάλειας. Το CERT συνεργάζεται με τα μέσα μαζικής ενημέρωσης για την ευαισθητοποίηση σχετικά με τους κινδύνους στο Διαδίκτυο και τα βήματα που μπορούν να κάνουν οι χρήστες για να προστατεύσουν τον εαυτό τους.Επίσης, συνεργάζεται με άλλες μεγάλες εταιρείες τεχνολογίας, όπως η FIRST και η Internet Engineering Task Force(IETF),ώστε να αυξηθεί η δέσμευση για την ασφάλεια και την ικανότητα επιβίωσης. Τέλος, το CERT συμβουλεύει κυβερνητικούς οργανισμούς των ΗΠΑ,όπως το Εθνικό Κέντρο Αξιολόγησης Απειλών, το Εθνικό Συμβούλιο Ασφαλείας, καθώς και το Συμβούλιο Εσωτερικής Ασφάλειας.

Η πιστοποίηση, η ακεραιότητα και η εμπιστευτικότητα είναι συστατικά της κρυπτογραφίας. Η κρυπτογραφία είναι τόσο η πρακτική, όσο και η μελέτη της απόκρυψης πληροφοριών. Οι υπηρεσίες κρυπτογράφησης είναι η βάση για πολλές εφαρμογές ασφάλειας και χρησιμοποιούνται για τη διασφάλιση της προστασίας των δεδομένων, όταν αυτά τα δεδομένα θα μπορούσαν να εκτεθούν σε μη αξιόπιστα μέρη. Η κατανόηση των βασικών λειτουργιών της κρυπτογραφίας και πώς η κρυπτογράφηση παρέχει εμπιστευτικότητα και ακεραιότητα είναι σημαντική για τη δημιουργία μιας επιτυχημένης πολιτικής ασφάλειας. Είναι επίσης σημαντικό να κατανοήσουμε τα ζητήματα που εμπλέκονται στη διαχείριση του κλειδιού κρυπτογράφησης. Η ιστορία της κρυπτογραφίας ξεκινά στους διπλωματικούς κύκλους πριν από χιλιάδες χρόνια. Οι αγγελιοφόροι από δικαστήριο του βασιλιά έπαιρναν κρυπτογραφημένα μηνύματα σε άλλα δικαστήρια. Περιστασιακά, άλλα δικαστήρια που δεν συμμετείχαν στην επικοινωνία προσπάθησαν να κλέψουν οποιοδήποτε μήνυμα που αποστέλλονταν σ' ένα βασίλειο που θεωρούσαν αντίπαλο. Λίγο καιρό μετά, οι στρατιωτικοί διοικητές άρχισαν να χρησιμοποιούν κρυπτογράφηση για να εξασφαλίσουν τα μηνύματα. Διάφοροι μέθοδοι κρυπτογράφησης, φυσικές συσκευές και βοηθήματα έχουν χρησιμοποιηθεί για την κρυπτογράφηση και αποκρυπτογράφηση κειμένου: Μία από τις πρώτες μεθόδους μπορεί να ήταν η σκυτάλη της αρχαίας Ελλάδας, μια ράβδος που φέρεται ότι χρησιμοποιήθηκε από τους Σπαρτιάτες ως βοήθημα για την κρυπτογράφηση μεταφοράς. Ο αποστολέας και ο παραλήπτης είχαν πανομοιότυπους ράβδους (σκυτάλη) στην οποία θα τύλιγαν ένα transposed messaged.

Το κρυπτογράφημα του Καίσαρα είναι ένα απλό κρυπτογράφημα υποκατάστασης που χρησιμοποιήθηκε από τον Ιούλιο Καίσαρα στο πεδίο της μάχης για να κρυπτογραφήσει γρήγορα ένα μήνυμα που θα μπορούσε εύκολα να αποκρυπτογραφηθεί από τους διοικητές του. Η μέθοδος για την κρυπτογράφηση θα μπορούσε να συγκρίνει δύο παπύρους γραμμάτων, μετακινώντας το ένα πάνω από ένα ενιαίο αριθμητικό πλήκτρο ή με την περιστροφή της εσωτερικής γραμμής των τροχών του κρυπρογραφήματος από ένα ενιαίο αριθμητικό πλήκτρο. Η

κρυπτογράφηση Vigenere εφευρέθηκε από τον Γάλλο Blaise de Vigenere τον 16ο αιώνα, χρησιμοποιώντας ένα πολυαλφαβητικοί σύστημα κρυπτογράφησης. Βάσει της κρυπτογράφησης του Καίσαρα, κρυπτογραφούσε το απλό κείμενο χρησιμοποιώντας ένα multi-letter κλειδί.

Ο Τόμας Τζέφερσον, ο τρίτος πρόεδρος των Ηνωμένων Πολιτειών, εφηύρε ένα σύστημα κρυπτογράφησης που πιστεύεται ότι χρησιμοποιήθηκε, όταν υπηρέτησε ως γραμματέας του κράτους 1790-1793. Ο Arthur Scherbius εφηύρε μια ηλεκτρο-μηχανική συσκευή κωδικοποίησης που ονομάζεται Enigma το 1918 και είχε πωληθεί στη Γερμανία. Χρησίμευε ως πρότυπο για τις μηχανές που όλοι οι μεγάλοι συμμετέχοντες στο Δεύτερο Παγκόσμιο Πόλεμο χρησιμοποίησαν. Εκτιμάται ότι, εάν 1000 κρυπτοαναλυτές δοκίμαζαν τέσσερα κλειδιά ανά λεπτό, όλη μέρα, κάθε μέρα, θα έπαιρνε 1.8 δισεκατομμύρια χρόνια για να τα δοκιμάσουν όλα. Η Γερμανία γνώριζε ότι τα κρυπτογραφημένα μηνύματά τους θα μπορούσαν να υποκλαπούν από τους συμμάχους, αλλά ποτέ δεν πίστευε ότι θα μπορούσαν να αποκρυπτογραφηθούν.

Επίσης κατά τη διάρκεια του Β 'Παγκοσμίου Πολέμου, η Ιαπωνία αποκρυπτογραφούσε κάθε κώδικα που είχαν οι Αμερικάνοι. Ένα πιο πολύπλοκο σύστημα κωδικοποίησης ήταν αναγκαίο και η απάντηση ήρθε με τη μορφή των Navajo code talkers. Όχι μόνο δεν υπήρχαν λέξεις στη γλώσσα Ναβάχο για στρατιωτικούς όρους, η γλώσσα ήταν άγραφη και λιγότερο από 30 άτομα έξω από τις Ναβάχο περιοχές θα μπορούσαν να την μιλήσουν και κανείς από αυτούς δεν ήταν Ιάπωνες. Μέχρι το τέλος του πολέμου, περισσότεροι από 400 Ινδιάνοι Ναβάχο εργάζονταν ως code talkers. Κάθε μία από αυτές τις μεθόδους κρυπτογράφησης χρησιμοποιεί ένα συγκεκριμένο αλγόριθμο, που ονομάζεται κρυπτογράφημα για την κρυπτογράφηση και αποκρυπτογράφηση μηνυμάτων. Το κρυπτογράφημα είναι μια σειρά από καλά καθορισμένα βήματα που μπορούν να ακολουθηθούν ως μια διαδικασία κατά την κρυπτογράφηση και αποκρυπτογράφηση μηνυμάτων. Υπάρχουν διάφορες μέθοδοι δημιουργίας κρυπτογραφημένου κειμένου.

ΒΙΒΛΙΟΓΡΑΦΙΑ

ΕΛΛΗΝΙΚΗ

Γ. Πάγκαλου, Ι. Μαυρίδη (2005) «Ασφάλεια Πληροφοριακών Συστημάτων και Δικτύων», Γ. Πάγκαλου, Ι. Μαυρίδη, Εκδόσεις Ανίκουλα

Δημήτρης Γκρίτζαλης (2004) «Ασφάλεια πληροφοριακών συστημάτων», Σωκρ. Κάτσικας, Δημήτρης Γκρίτζαλης, επιμέλεια: Στέφανος Γκρίτζαλης, Εκδόσεις Νέων Τεχνολογιών, 2004

Φωλίνας Δ.(2006), «Ολοκληρωμένα πληροφοριακά συστήματα διαχείρισης επιχειρηματικών πόρων», Αθήνα, Εκδόσεις Ανίκουλα

ΞΕΝΗ

Alfaro, J.G.; Cuppens, F.; Cuppens-Boulahia, N. Complete analysis of configuration rules to guarantee reliable network security policies. Int. J. Inf. Secur. 2008, 7, 103–122

Cisco Systems, (2010), Router Security Audit Logs , Americas Headquarters: Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Cisco Tools. Available online: http://tools.cisco.com/ITDIT/CFN/jsp/compareImages.jsp (accessed on 19 March 2012).

Chatzimisios P., Vafiadis A., Kamargiannis P., Stoimenos D., “A Survey of the Criteria on Selecting the Suitable Network Management System”, In Proc. of 7th World Multi-conference on Systemics, Cybernetics and Informatics (SCI 2003), Orlando, USA, July 2003.

Muhammad Naveed, Shams un Nihar, Mohammad Inayatullah Babar, NETWORK INTRUSION PREVENTION BY CONFIGURING ACLS ON THE ROUTERS, BASED ON SNORT IDS ALERTS, Emerging Technologies (ICET), 2010.

Sudkovitch M. and Roitman D. (2010), OSPF Security project book

Pattinson, C., “A Study of the Behaviour of the Simple Network Management Protocol” In Proc. of 12th International Workshop on Distributed Systems, Nancy, France, October, 2011

HikVision (2017) Network Security Hardening Guide v1.2 June 2017

John N. Davies , Paul Comerford and Vic Grout(2012), Principles of Eliminating Access Control Lists within a Domain, Future Internet 2012, 4, 413-429; doi:10.3390/fi4020413

Meiners, C.R.; Liu, A.X.; Torng, E. Hardware-Based Classification for High-Speed Internet Routers; 1st ed.; Springer: Berlin/Heidelberg, Germany, 2010; p. 2

Shirley Radack(2009), PROTECTING INFORMATION SYSTEMS WITH FIREWALLS: REVISED GUIDELINES ON FIREWALL TECHNOLOGIES AND POLICIES Editor Computer Security Division Information Technology Laboratory National Institute of Standards and Technology

Fox, R. Griffith, A. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, and I. Stoica, “Above the clouds: A berkeley view of cloud computing,” Dept. Electrical Eng. and Comput. Sciences, University of California, Berkeley, Rep. UCB/EECS, vol. 28, p. 13, 2009

Shankar Sharan Tripathi, Sonu Agrawal- “A Survey on Enhanced Intrusion Detection System in Mobile Ad hoc Network”-International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 1, Issue 7, September 2012.

Ms Asiya Jaleel -“Security Challenge in Cloud Computing”- Provided by International Journal of Engineering Sciences & Research Technology (IJESRT), Feb 2014

D. Dagon, G. Gu, C. Lee, and W. Lee. A Taxonomy of Botnet Structures. In Annual Computer Security Applications Conference (ACSAC), 2007

Gordon, L. A. & Loep, M. P. 2012. Budgeting Process for Information Security Expenditures. Communications of the ACM, Vol. 49, No. 1, pp. 121-125.

Kevin. J. Houle and George. M. Weaver(2011), “Trends in Denial of Service Attack Technology,” CERT Advisory, v1.0, Oct. 2011

Pfleeger, C. P. 1997. Security in Computing. Prentice Hall PTR.2nd Edition

Richard Clarke, “Looking at Vulnerability Issues in Cyber-Security,” Business Session of the President’s National Security Telecommunications Advisory Committee (NSTAC), Mar. 2002

S.H. Yang, X. Chen, J.L. Alty. Design issues and implementation of internet-based process control systems. In Control Engineering Practice, Volume 11, Number 6, pages 709–720, 2003.

L. Horacek. Protection on Demand, Information Security that Works for you, The IBM Approach to Security Protection from the Core to the Perimeter. IDC Security Roadshow Sofia, April-12-2007, 2007.

L. Yang and Yang S.H. A framework of security and safety checking for internet-based control systems. In Int. Journal of Information and Computer Security, Vol. 1, No. 1/2, pages 185–200, 2007.

Mouna Jouinia., Latifa Ben ArfaRabaia and Anis BenAissa(2010), Classification of Security Threats in Information Systems, Procedia Computer Science Volume 32, 2014, Pages 489-496

Tsohou, A., Kokolakis, S., Karyda, M., Kiountouzis(2013) E., "Investigating information security awareness: research and practice gaps", Information Security Journal: A Global Perspective, 17(5), pp. 207-227,

Arbor Networks, Google Ideas, & Big Picture Group. (2013). What is a DDoS Attack? Retrieved from http://www. digitalattackmap.com/understanding-ddos/

European Network and Information Security Agency. (2012, November). Good Practice Guide for Addressing Network and Information Security Aspects of Cybercrime. (Publication). Retrieved https://www.enisa.europa.eu/ publications/good-practice-guide-for-addressing-network-and-information-security-aspects-of-cybercrime/at_ download/fullReport

McAfee. (2017, April). McAfee Labs Threat Report: April 2017 (Rep.) Retrieved from https://www.mcafee.com/ca/ security-awareness/articles/mcafee-labs-threats-report-mar-2017.aspx

Michael, C. (2009, August). Computer Viruses Slow African Expansion. Guardian. Retrieved from https://www. theguardian.com/technology/2009/aug/12/ethiopia-computer-virus

SANS Institute. (2015, December). Infrastructure Security Architecture for Effective Security Monitoring. (Publication) Retrieved from https://www.sans.org/reading-room/whitepapers/bestprac/infrastructure-security-architectureeffective-security-monitoring-36512

Storm, D. (2016 February). Hackers Breach DOJ, dump details of 9,000 DHS employees, plan to leak 20,000 from FBI. Computerworld. Retrieved from http://www.computerworld.com/article/3030983/security/hackers-breach-dojdump-details-of-9-000-dhs-employees-plan-to-leak-20-000-from-fbi.html

D. A. Osvik, J. W. Bos, D. Stefan, and D. Canright. Fast software AES encryption, In Foundations of Software Engineering (FSE), 2010.

M. Al-Fares, A. Loukissas, A. Vahdat, “A scalable commodity data center network architecture”, Proc. of ACM SIGCOMM, Aug 2008.

Wall, D. S. (2001). Cybercrimes and the Internet. In D. S. Wall (Ed.), Crime and the Internet (pp. 1-17). London: Routledge

Sokolik, S. L. (1980). Computer crime—The need for deterrent legislation. Computer/Law Journal, 2, 353-383. Spafford, E. H. (1990). Crisis and aftermath. In P. J. Denning (Ed.), Computers under attack: Intruders, worms, and viruses (pp. 223-243). New York: Addison-Wesley.

Montz, L. B. (2002). The worm case: From indictment to verdict. In P. J. Denning (Ed.), Computers under attack: Intruders, worms, and viruses (pp. 260-263). New York: Addison-Wesley

E. B. Fernandez, H. Washizaki, and N. Yoshioka, "Abstract security patterns", Position paper in Procs. of the 2nd Workshop on Software Patterns and Quality (SPAQu'08), in conjuction with the 15th Conf. on Pattern Languages of Programs (PLoP 2008), October 18-20, Nashville, TN.