



ΙΟΝΙΟ ΠΑΝΕΠΙΣΤΗΜΙΟ

Τμήμα Πληροφορικής

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

Ακαδ. Έτος: 2021-2022

Ανίχνευση επιθέσεων του DARPA dataset 1998 με τη χρήση του Snort

Δημήτρης Αντωνούλης Π2017037

Τριμελής επιτροπή

Κ. Νταντογιάν Χριστόφορος

Κα. Χριστοπούλου Ελένη

Κα. Σωτηροπούλου Άννα

Επιβλέπων

Μέλος

Μέλος

ΠΕΡΙΛΗΨΗ

Στην εποχή της τεχνολογίας και του διαδικτύου η χρήση Intrusion Detection συστημάτων είναι απαραίτητη. Επιθέσεις και εισβολές γίνονται πλέον σε καθημερινή βάση τόσο σε μεμονωμένους χρήστες όσο και σε δίκτυα. Η πρόληψη και η ασφάλεια είναι μονόδρομος με τα IDS να κυριαρχούν στον χώρο. Ωστόσο για να επαληθευτούν οι ικανότητες ενός IDS και στην περίπτωση μας NIDS (Network-based Intrusion System) χρειάζονται τρόποι αξιολόγησης των δυνατοτήτων τους. Στη συγκεκριμένη διατριβή αξιολογείται το Snort το οποίο έρχεται αντιμέτωπο με το dataset της DARPA του 1998. Το Snort είναι ένα signature-based IDS στο οποίο ο χρήστης καλείται να εξοπλίσει με τους κατάλληλους κανόνες τους οποίους το πρόγραμμα χρησιμοποιεί για να ελέγξει πακέτα. Στην συγκεκριμένη αξιολόγηση το Snort καλείται να ελέγξει ένα dataset το οποίο αποτελεί μια προσομοίωση του δικτύου μιας αεροπορικής βάσης. Περιλαμβάνει δραστηριότητα από πολλαπλά μηχανήματα, χρήστες και επιτιθέμενους και οι κατηγορίες των επιθέσεων ποικίλλουν. Περιγράφονται αναλυτικά οι κατηγορίες Denial of Service, Remote to Local, User to Root αλλά και probe ή scan επιθέσεις και παρέχονται αναλυτικά σχεδιαγράμματα και εικόνες όπου είναι δυνατόν. Αναλύεται περιγραφικά ο τρόπος λειτουργίας των επιθέσεων back, land, syn flood (neptune), ping of death, smurf, syslogd καθώς και της teardrop για τις Denial of Service. Στη συνέχεια ακολουθούν οι επιθέσεις Remote to Local όπου παρέχεται ορισμός για τις dict, guest, ftp-write και phf επιθέσεις. Ακολουθούν οι User to Root επιθέσεις με τις eject, ffbconfig, fdformat, loadmodule και perl να αναλύονται και τέλος παρέχεται ορισμός για τις probe και scan επιθέσεις που αποτελούνται από τις ipsweep, nmap και satan. Πολύ σημαντική για την αξιολόγηση είναι η ρύθμιση του Snort και η επιλογή των παραμέτρων για τη σωστή λειτουργία του. Το πρόγραμμα έχει 3 συνολικά λειτουργίες και στη συγκεκριμένη περίπτωση χρησιμοποιήθηκε η Network Intrusion Detection system λειτουργία. Μετά την παρουσίαση και των υπόλοιπων παραμέτρων που χρησιμοποιήθηκαν, παρουσιάζεται ο τρόπος λειτουργίας και συγγραφής των κανόνων και επεξηγείται με ένα σχεδιάγραμμα. Στη συνέχεια έγινε μια έρευνα και επιλέχθηκε ένας συνδυασμός κανόνων σύμφωνα με τους οποίους έτρεξε το Snort σε αυτή την αξιολόγηση. Αφού το Snort έλεγξε τη

δραστηριότητα των 7 εβδομάδων εκπαίδευσης του προγράμματος, τα αποτελέσματα συλλέχθηκαν και για λόγους προσομοίωσης πραγματικού περιβάλλοντος, επαληθεύτηκαν με μια χειρωνακτική μέθοδο, τη χρήση ενός προγράμματος ανάλυσης πακέτων, το Wireshark. Τέλος παρουσιάζονται αναλυτικά τα αποτελέσματα που βρέθηκαν για κάθε μέρα των 7 εβδομάδων ξεχωριστά καθώς και μία σύντομη συμπερασματική ανακεφαλαίωση.

Λέξεις - Κλειδιά (Snort, DARPA 1998, Wireshark)

ΠΕΡΙΕΧΟΜΕΝΑ

1.	ΕΙΣΑΓΩΓΗ	7
1.1.	Intrusion Detection Systems	7
1.2.	Snort	8
1.3.	Dataset	9
1.4.	Δομή Εργασίας	10
2.	ΕΠΙΘΕΣΕΙΣ	12
2.1.	Επιθέσεις Denial of Service	12
2.2.	Επιθέσεις Remote to Local	17
2.3.	Επιθέσεις User to Root	20
2.4.	Επιθέσεις probe ή scan	22
3.	ΜΕΘΟΔΟΛΟΓΙΑ	25
3.1.	Λειτουργίες	25
3.2.	Κανόνες	26
3.3.	Παράμετροι	27
4.	ΑΠΟΤΕΛΕΣΜΑΤΑ	29
4.1.	1η Εβδομάδα	32
4.2.	2η Εβδομάδα	34
4.3.	3η Εβδομάδα	35
4.4.	4η Εβδομάδα	38
4.5.	5η Εβδομάδα	40
4.6.	6η Εβδομάδα	43
4.7.	7η Εβδομάδα	46
5.	ΣΥΜΠΕΡΑΣΜΑΤΑ	50
6.	ΒΙΒΛΙΟΓΡΑΦΙΑ	52

ΠΕΡΙΕΧΟΜΕΝΑ ΕΙΚΟΝΩΝ

1.	Πίνακας διαφόρων τύπων Denial Of Service επιθέσεων.....	13
2.	Επεξηγηματικό σχεδιάγραμμα λειτουργίας της Land επίθεσης.....	14
3.	Επεξηγηματικό σχεδιάγραμμα λειτουργίας της Syn Flood επίθεσης.....	15
4.	Επεξηγηματικό σχεδιάγραμμα λειτουργίας της Smurf επίθεσης.....	16
5.	Επεξηγηματικό σχεδιάγραμμα λειτουργίας της teardrop επίθεσης.....	17
6.	Πίνακας με R2L επιθέσεις και τρόπος λειτουργίας τους.....	18
7.	Επεξηγηματικό σχεδιάγραμμα λειτουργίας Dictionary επίθεσης.....	19
8.	Σχεδιάγραμμα επίθεσης ftp-write.....	20
9.	Στόχος R2L επιθέσεων.....	21
10.	Επεξηγηματικό διάγραμμα επίθεσης scan.....	23
11.	Βοηθητικό διάγραμμα σύνταξης κανόνων Snort.....	27
12.	Παράδειγμα επίθεσης land - ανάλυση αρχείου με Wireshark.....	31
13.	Αναλυτικός πίνακας συνολικών αποτελεσμάτων για κάθε επίθεση.....	49

1. ΕΙΣΑΓΩΓΗ

Ξεκινώντας την εκπόνηση της παρούσας πτυχιακής εργασίας σε αυτό το εισαγωγικό κεφάλαιο γίνεται μια αναφορά στα Intrusion Detection συστήματα. Αποδίδεται ένας σύντομος ορισμός και λίγα λόγια τόσο για το Short όσο και για το dataset που χρησιμοποιήθηκε. Τέλος δίνεται μια σύντομη περιγραφή της δομής που ακολούθησε η εργασία.

1.1. Intrusion Detection Systems

Τα τελευταία έτη το διαδίκτυο και τα συστήματα υπολογιστών έχουν εγείρει πολλά ζητήματα ασφαλείας λόγω της εκτεταμένης χρήσης των δικτύων. Ο αριθμός των εισβολών και επιθέσεων έχει αυξηθεί υπερβολικά. Η παραμικρή εισβολή ή επίθεση σε τρωτά σημεία ενός δικτύου, υπολογιστών και συστήματα πληροφοριών μπορούν να σημαίνουν σοβαρή ζημιά για το λόγο αυτό η ανάγκη για την χρήση συστημάτων ανίχνευσης εισβολής έχει αυξηθεί. Σύστημα Ανίχνευσης Εισβολής (Intrusion Detection System) ονομάζεται το σύστημα που καθιστά τη ανίχνευση για εισβολή μια αυτοματοποιημένη διαδικασία και έχει ως πρωτεύων σκοπό να ανιχνεύει ανεπιθύμητες επιθέσεις σε συστήματα. Η πρωταρχική ευθύνη του IDS είναι ο εντοπισμός ανεπιθύμητης και κακόβουλης κυκλοφορίας δικτύου. Οι δύο κύριοι τύποι συστημάτων ID(Intrusion Detection) είναι (i) συστήματα ID που λειτουργούν σε έναν κεντρικό υπολογιστή και ονομάζονται συστήματα αναγνώρισης που βασίζονται σε κεντρικό υπολογιστή (Host-based Intrusion Detection Systems) και (ii)

συστήματα αναγνώρισης που λειτουργούν στη ροή δεδομένων ενός δικτύου και ονομάζονται συστήματα αναγνώρισης που βασίζονται σε δίκτυο (Network-based Intrusion Detection Systems). Τα HIDS έχουν ως ρόλο να παρακολουθούν διαδικασίες και εφαρμογές που εκτελούνται σε συσκευές όπως “ servers “ και “ workstations”. Ταυτόχρονα, εκτελούν διάφορους ελέγχους και παρακολουθούν πολλούς τομείς ενός συστήματος όπως για παράδειγμα αλλαγές που έγιναν στις ρυθμίσεις μητρώου, κρίσιμες ρυθμίσεις παραμέτρων του συστήματος, τα αρχεία καταγραφής και περιεχομένου και φροντίζουν να στέλνουν ειδοποίηση για οποιαδήποτε μη εξουσιοδοτημένη ή ανώμαλη δραστηριότητα. Απο την άλλη τα NIDS τοποθετούνται σε στρατηγικό σημείο ή σημεία εντός του δικτύου και έχουν σχεδιαστεί για να παρακολουθούν κάθε κυκλοφορία απο και προς όλες τις συσκευές του δικτύου. Αυτό μπορεί να περιλαμβάνει για παράδειγμα παραβάσεις πολιτικής και σάρωση θυρών, καθώς και επισκεψιμότητα άγνωστης πηγής και προορισμού. Ένα από τα πιο δημοφιλή και αποτελεσματικά κατά τη χρήση τους NIDS θεωρείται το Snort.

1.2. Snort

Το Snort (www.snort.org) είναι ένα NIDS που βασίζεται σε κανόνες μέσω των οποίων παρακολουθεί την κατάσταση ενός δικτύου. Περιλαμβάνει μια μηχανή ανίχνευσης που αναλύει όλη την κίνηση του δικτύου, αναζητά κάθε είδους εισβολή και επιτρέπει την εγγραφή, προειδοποίηση και απόκριση σε οποιαδήποτε επίθεση έχει οριστεί μέσω των κανόνων προηγουμένως. Πιο συγκεκριμένα, το Snort χρησιμοποιεί μια σειρά κανόνων μέσω των οποίων εκτελεί ελέγχους στα πακέτα του δικτύου και τα εξετάζει για να δει αν κάποιο από αυτά αντιστοιχεί σε κάποιον από τους κανόνες. Στοχεύει σε οποιαδήποτε μορφή ίχνους που μπορεί να σημαίνει παραβίαση, βλάβη ή ακόμα και παρεμπόδιση της λειτουργικότητας του δικτύου είτε από εξωτερικούς είτε από εσωτερικούς χρήστες. Στην περίπτωση αυτή το Snort στέλνει ειδοποιήσεις που αντιστοιχούν στην κατάλληλη απειλή, προς τον χρήστη που το διαχειρίζεται, προετοιμάζοντάς τον έτσι για την πιθανή εισβολή ή γενικότερα κακόβουλη ενέργεια συμπεριλαμβάνοντας συχνά κάποιες πληροφορίες για αυτό που εντόπισε. Το Snort είναι διαθέσιμο υπό την GPL, είναι δωρεάν και εκτελείται σε Windows και GNU/Linux. Είναι ένα από τα πιο ευρέως χρησιμοποιούμενα και ενημερώνεται συνεχώς.



1.3. Dataset

Το 1998 η ομάδα Ασφάλειας Συστημάτων και Τεχνολογίας του MIT Lincoln Laboratory (ή προηγουμένως ονομαζόμενη DARPA), εντόπισε την ανάγκη για μαζική αξιολόγηση των Συστημάτων Εντοπισμού Εισβολής (IDS). Έτσι, υπέγραψε μια σύμβαση και συνεργάστηκε με το Ερευνητικό Πολεμικό εργαστήριο της αεροπορίας με στόχο να βρει μια λύση στο πρόβλημα. Με σκοπό τη δημιουργία μιας ολοκληρωμένης database (<https://archive.ll.mit.edu/ideval/data/1998data.html>) την οποία θα μπορούσε εύκολα ο καθένας να αξιολογήσει το IDS του, κατασκεύασαν μια προσομοίωση ενός δικτύου που αντιστοιχεί σε μια βάση Πολεμικής Αεροπορίας η οποία έχει σύνδεση στο διαδίκτυο. Η δραστηριότητα του δικτύου επιτεύχθηκε με την βοήθεια scripts και σε αυτά εντάχθηκαν επιθέσεις σε καθορισμένα σημεία. Οι επιθέσεις που συμπεριλαμβάνονται στο dataset κατατάσσονται σε κατηγορίες όπως Denial of Service, User to Root, Remote to Local αλλά

και probe ή αλλιώς scanning επιθέσεις. Η ποικιλία στις κατηγορίες των επιθέσεων που συμπεριλαμβάνονται στο dataset έχει ως σκοπό να παρέχει μια πιο ολοκληρωμένη πρόκληση για τα IDS τα οποία πρόκειται να το χρησιμοποιήσουν για την αξιολόγησή τους. Αφού κατάφεραν να κατασκευάσουν την προσομοίωση τους, φρόντισαν να συλλέξουν πληροφορίες για τη δραστηριότητα της προσομοίωσης συμπεριλαμβανομένου και των επιθέσεων και να παρέχουν αρχεία με 7 εβδομάδες δεδομένων στους ερευνητές για να τις χρησιμοποιήσουν για να εκπαιδεύσουν τα συστήματά τους. Μετά την εκπαίδευση σειρά είχε η δοκιμή των IDS σε αρχεία όπου οι επιθέσεις δεν μπορούσαν να επαληθευτούν, για αυτό τους παρείχαν 2 εβδομάδες δεδομένων όπου και μπορούσαν να αξιολογήσουν την αποτελεσματικότητα των συστημάτων τους. Μετά το τέλος της διαδικασίας, η DARPA φρόντισε τα αποτελέσματα των πειραμάτων που έγιναν να δημοσιευτούν σε σχετικές διατριβές.

1.4. Δομή Εργασίας

Η παρούσα πτυχιακή αναπτύχθηκε όσο πιο αναλυτικά γίνεται με σκοπό κάθε αναγνώστης να μπορεί να κατανοήσει πλήρως το νόημά της. Για κάθε επίθεση, τρόπος εκπόνησης των πειραμάτων και αποτέλεσμα, δίνεται μια αναλυτική περιγραφή.

Η εργασία ξεκινάει με μια ανάλυση όλων των επιθέσεων που διακρίνονται στο dataset. Πρώτη στη σειρά βρίσκεται η κατηγορία των Denial of Service επιθέσεων για τις οποίες δίνεται μια σύντομη περιγραφή και στη συνέχεια αναλύονται μια προς μια οι επιθέσεις που συναντήθηκαν στα πειράματα. Αμέσως μετά ακολουθούν οι Remote to Local επιθέσεις, μετά οι User to Root και τέλος οι probe επιθέσεις όπου για κάθε μια κατηγορία ακολουθείται η ίδια διαδικασία με την προσθήκη επεξηγηματικών διαγραμμάτων όπου ήταν δυνατό.

Στη συνέχεια ακολουθεί το κεφάλαιο της μεθοδολογίας όπου αναλύεται ο τρόπος με τον οποίο διεξήχθησαν τα πειράματα και η ροή της διαδικασίας όπως αυτή έγινε. Αναφέρεται ο τρόπος λειτουργίας του προγράμματος Snort και λίγα λόγια για τις εντολές και παραμέτρους που χρησιμοποιήθηκαν καθώς και για άλλες επιλογές που θα μπορούσαν να φανούν χρήσιμες σε διαφορετικές περιπτώσεις.

Τέλος γίνεται ανάλυση των αποτελεσμάτων που προέκυψαν από τα πειράματα. Γίνεται αναφορά σε κάθε επίθεση που συναντήθηκε κάθε ημέρα των 7 εβδομάδων και αναφέρεται ο αριθμός των πακέτων που εντοπίστηκαν από το Snort σε σύγκριση με τον αριθμό των πακέτων που στάλθηκαν για κάθε επίθεση. Εκεί περιγράφονται επίσης ορισμένα σενάρια επιθέσεων που δεν αναφέρθηκαν στο κεφάλαιο με τις επιθέσεις. Συνοψίζοντας ακολουθούν τα συμπεράσματα της παρούσας πτυχιακής και μια αναφορά στη συνεισφορά της.

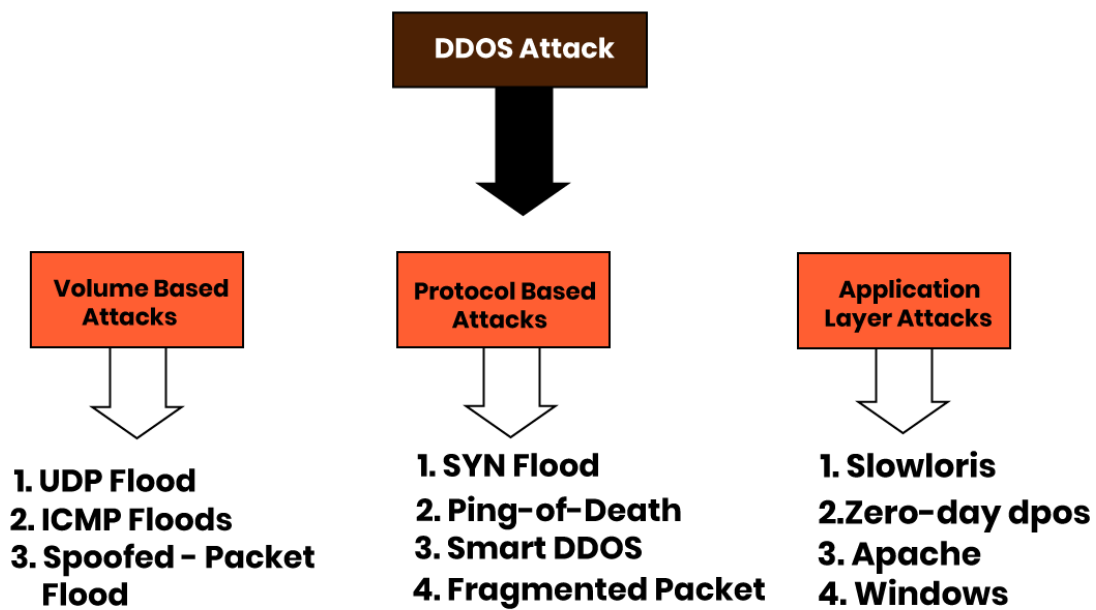
2. ΕΠΙΘΕΣΕΙΣ

Στο κεφάλαιο αυτό γίνεται μια ανασκόπηση των επιθέσεων που εντοπίζονται στο DARPA 1998. Γίνεται μια ανάλυση του κάθε είδους επιθέσεων που συναντήθηκε και μια σύντομη περιγραφή της κάθε επίθεσης.

Το dataset ή στα ελληνικά, σύνολο δεδομένων, περιλαμβάνει σε κάθε ημέρα εκπαίδευσης αμέτρητα πακέτα με την δραστηριότητα των μηχανημάτων. Ανάμεσα στα πακέτα αυτά εντοπίζονται και πολλές επιθέσεις διαφορετικού είδους οι οποίες χρησιμοποιήθηκαν σε έναν σεβαστό βαθμό που κρίθηκε απαραίτητος να πραγματοποιηθούν έτσι ώστε η αξιολόγηση συστημάτων ανίχνευσης να γίνει όσο το δυνατόν πιο σωστά τόσο κατά τη διάρκεια των επτά εβδομάδων εκπαίδευσης όσο και των δύο εβδομάδων δοκιμής. Οι επιθέσεις αυτές είχαν ποικίλους στόχους για αυτό και αποτελούνταν από διάφορες κατηγορίες όπως Denial of service (DoS), Remote to Local (R2L), User to Root, probes και scan επιθέσεις καθώς και επιθέσεις δεδομένων (data).

2.1. Επιθέσεις Denial of Service

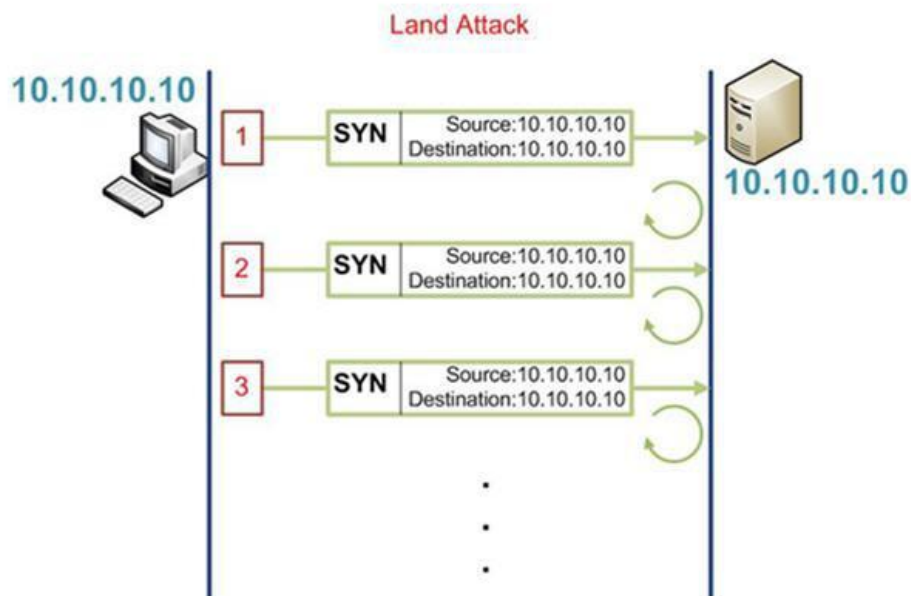
Οι Denial of Service(DoS) επιθέσεις είναι σχεδιασμένες για να διακόψουν έναν δέκτη ή μια υπηρεσία δικτύου. Ορισμένες επιθέσεις το καταφέρουν αυτό φορτώνοντας υπερβολικά κάποιες υπηρεσίες δικτύου, άλλες δημιουργούν πακέτα με κακή μορφή που αντιμετωπίζονται εσφαλμένα από το μηχάνημα του θύματος και άλλες εκμεταλλεύονται σφάλματα λογισμικού σε προγράμματα δικτύου. Πιο συγκεκριμένα, οι επιθέσεις που χρησιμοποιούνται στην κατηγορία DoS στο σύνολο δεδομένων του DARPA 1998 αναφέρονται παρακάτω αναλυτικά:



Πίνακας διαφόρων τύπων Denial Of Service επιθέσεων.

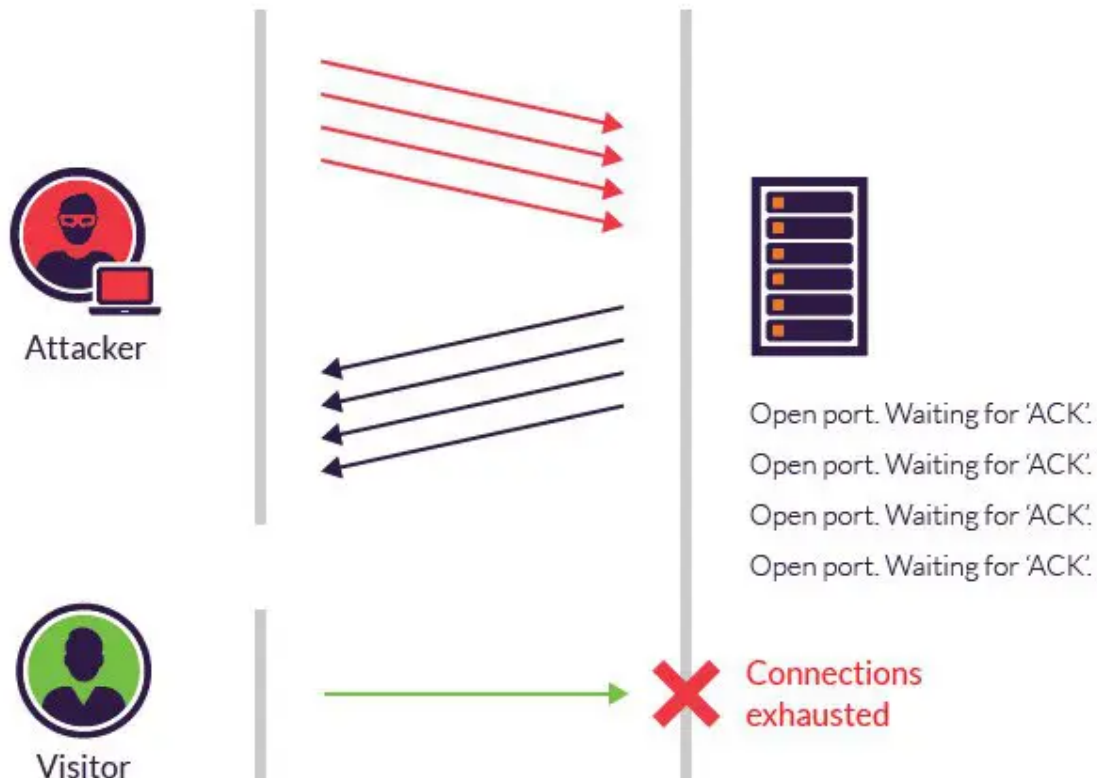
Back: Αυτή η επίθεση DoS γίνεται εναντίον ενός διακομιστή Ιστού Apache. Ο εισβολέας υποβάλλει αιτήματα με URLs που περιέχουν πολλές πρόσθετες καθετούς και καθώς ο διακομιστής προσπαθεί να επεξεργαστεί αυτά τα αιτήματα, επιβραδύνει λόγω του πλήθους των πληροφοριών και δεν μπορεί να επεξεργαστεί άλλα αιτήματα.

Land: Η επίθεση Land είναι μια επίθεση DoS που είναι αποτελεσματική σε ορισμένες παλαιότερες υλοποιήσεις TCP/IP. Η μόνη ευάλωτη πλατφόρμα που χρησιμοποιήθηκε στην αξιολόγηση DARPA του 1998 ήταν το SunOS 4.1. Η επίθεση Land συμβαίνει όταν ένας εισβολέας στέλνει ένα πλαστό πακέτο SYN στο οποίο η διεύθυνση προέλευσης είναι ίδια με τη διεύθυνση προορισμού.



Επεξηγηματικό σχεδιάγραμμα λειτουργίας της Land επίθεσης.

Syn Flood(Neptune): Το SYN Flood είναι μια επίθεση άρνησης υπηρεσίας στην οποία κάθε υλοποίηση TCP/IP είναι ευάλωτη (σε κάποιο βαθμό). Κάθε μισάνοιχτη σύνδεση TCP που γίνεται σε ένα μηχάνημα αναγκάζει τον διακομιστή 'tcpd' να προσθέσει μια εγγραφή στη δομή δεδομένων που αποθηκεύει πληροφορίες που περιγράφουν όλες τις εκκρεμείς συνδέσεις. Αυτή η δομή δεδομένων είναι πεπερασμένου μεγέθους και μπορεί να υπερχειλίσει δημιουργώντας σκόπιμα πάρα πολλές μερικώς ανοιχτές συνδέσεις. Η μισάνοιχτη δομή δεδομένων συνδέσεων στο διακομιστή σύστημα του θύματος τελικά θα γεμίσει και το σύστημα δεν θα μπορεί να δεχτεί νέες εισερχόμενες συνδέσεις μέχρι να αδειάσει ο πίνακας. Κανονικά υπάρχει ένα χρονικό όριο που σχετίζεται με μια εκκρεμή σύνδεση, επομένως οι μισάνοιχτες συνδέσεις θα λήξουν τελικά και το σύστημα διακομιστή του θύματος θα επαναλειτουργήσει. Ωστόσο, το σύστημα που επιτίθεται μπορεί απλώς να συνεχίσει να στέλνει πακέτα πλαστογραφημένα από IP που ζητούν νέες συνδέσεις πιο γρήγορα από ό,τι το σύστημα θύματος μπορεί να λήξει τις εκκρεμείς συνδέσεις. Σε ορισμένες περιπτώσεις, το σύστημα μπορεί να εξαντλήσει τη μνήμη, να καταρρεύσει ή να καταστεί μη λειτουργικό.

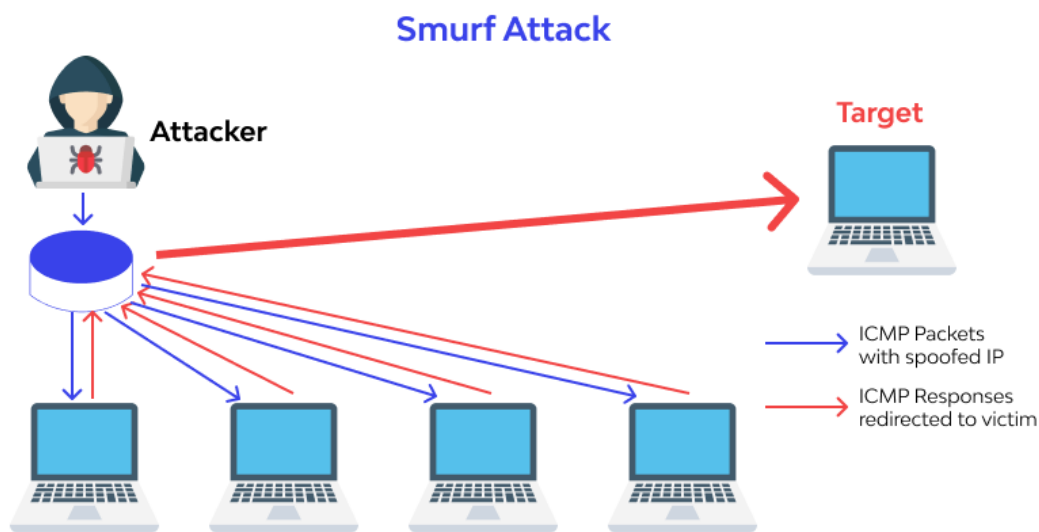


Επεξηγηματικό σχεδιάγραμμα λειτουργίας της Syn Flood επίθεσης.

Ping Of Death (POD): Το Ping of Death είναι μια επίθεση DoS που επηρεάζει πολλά παλαιότερα λειτουργικά συστήματα. Αν και οι αντίξοες επιπτώσεις μιας Ping of Death επίθεσης δεν μπορούσαν να αναπαραχθούν σε κανένα σύστημα θυμάτων που χρησιμοποιήθηκε στην αξιολόγηση DARPA του 1998, έχει αναφερθεί ευρέως ότι ορισμένα συστήματα θα αντιδράσουν με απρόβλεπτο τρόπο όταν λαμβάνουν πακέτα IP μεγάλου μεγέθους. Πιθανές αντιδράσεις περιλαμβάνουν κατάρρευση, πάγωμα και επανεκκίνηση.

Smurf: Στην επίθεση "smurf", οι εισβολείς χρησιμοποιούν πακέτα αιτήματος echo ICMP (Internet Control Message Protocol) γνωστά ως echo requests που κατευθύνονται προς τις διευθύνσεις IP των θυμάτων, από απομακρυσμένες τοποθεσίες για να δημιουργήσουν μια επίθεση DoS. Η επίθεση αυτή περιλαμβάνει τρία μέλη: τον εισβολέα, τον ενδιάμεσο και το θύμα (στην συγκεκριμένη επίθεση ο ενδιάμεσος θα μπορούσε επίσης να είναι θύμα). Ο εισβολέας στέλνει πακέτα echo request ICMP στη διεύθυνση εκπομπής με πολλά υποδίκτυα, με τη διεύθυνση πηγής να είναι πλαστογραφημένη ως αυτή του θύματος. Οποιοδήποτε

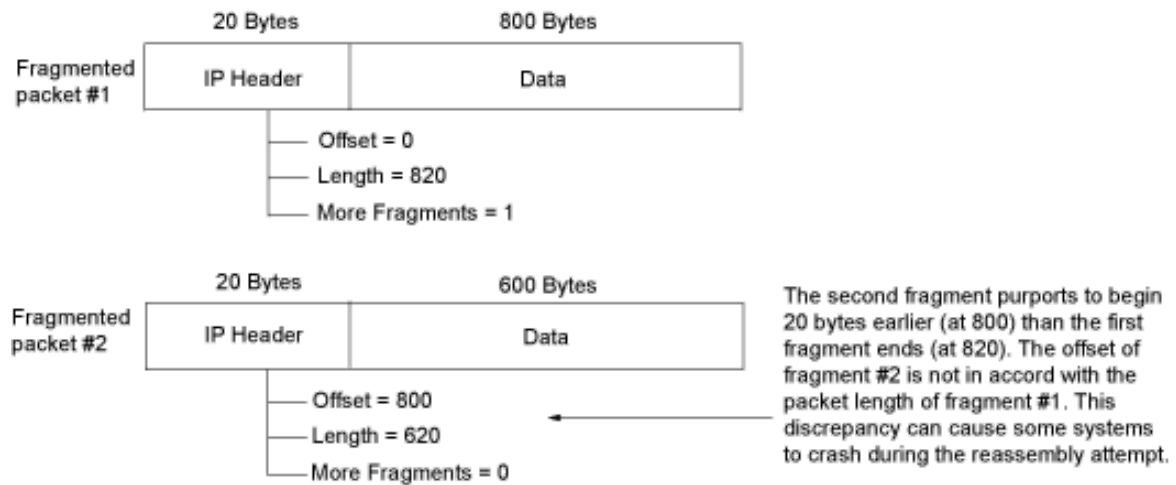
μηχάνημα ακούει σε αυτά τα υποδίκτυα θα ανταποκριθεί στέλνοντας πακέτα ICMP echo reply στο θύμα. Η smurf επίθεση είναι τόσο αποτελεσματική γιατί ο επιτιθέμενος μπορεί να χρησιμοποιήσει διευθύνσεις εκπομπής για να ενισχύσει αυτό που διαφορετικά θα ήταν ένα αβλαβές ping flood. Στην καλύτερη περίπτωση (για τον επιτιθέμενο), ο εισβολέας μπορεί να πλημμυρίσει το θύμα με όγκο πακέτων 255 φορές μεγαλύτερο από αυτό που θα μπορούσε να πετύχει χωρίς τέτοια ενίσχυση.



Επεξηγηματικό σχεδιάγραμμα λειτουργίας της Smurf επίθεσης.

Syslogd: Το Syslogd exploit είναι μια επίθεση DoS που επιτρέπει σε έναν εισβολέα να σκοτώσει εξ αποστάσεως την υπηρεσία syslogd σε έναν διακομιστή Solaris. Πιο αναλυτικά, όταν το Solaris syslogd λαμβάνει ένα εξωτερικό μήνυμα, επιχειρεί να πραγματοποιήσει αναζήτηση DNS στη διεύθυνση IP προέλευσης. Εάν αυτή η διεύθυνση IP δεν ταιριάζει με μια έγκυρη εγγραφή DNS, τότε το syslogd θα διακοπεί με σφάλμα τμηματοποίησης (Segmentation error).

Teardrop: Το teardrop exploit είναι μια επίθεση DoS που εκμεταλλεύεται ένα ελάττωμα στην υλοποίηση παλαιότερων TCP/IP στίβων. Ορισμένες υλοποιήσεις του κώδικα επανασυναρμολόγησης κατακερματισμού IP σε αυτές τις πλατφόρμες δεν χειρίζονται σωστά τα επικαλυπτόμενα τμήματα IP.



Επεξηγηματικό σχεδιάγραμμα της teardrop επίθεσης.

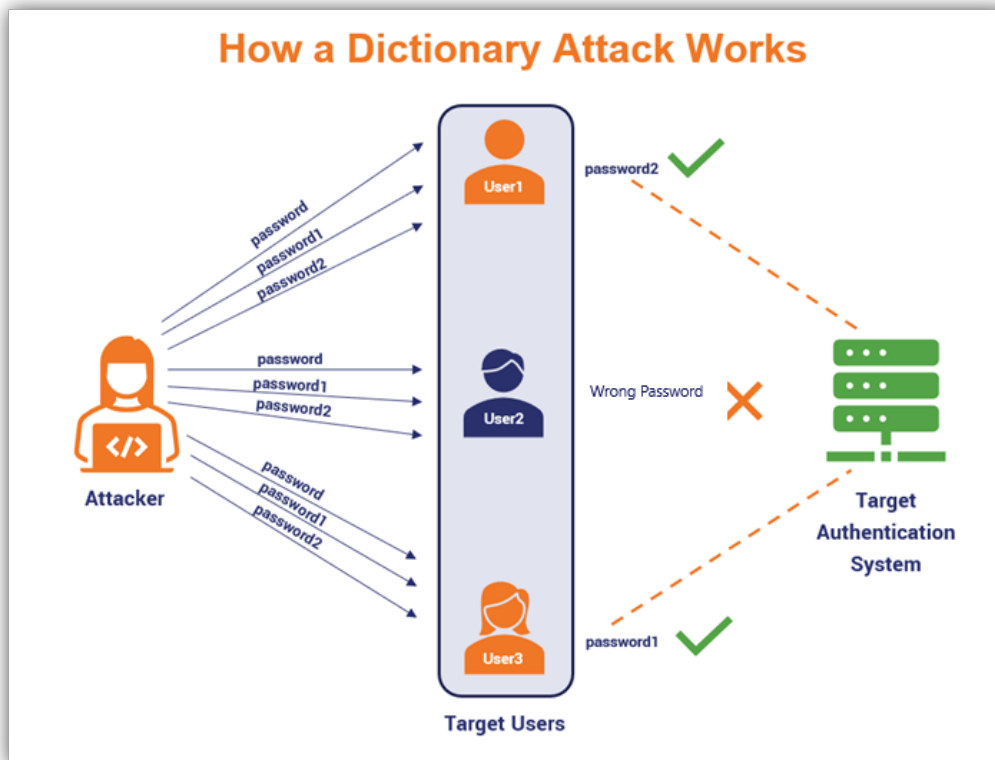
2.2. Επιθέσεις Remote to Local

Σε αυτές τις επιθέσεις, ένας εισβολέας που δεν έχει λογαριασμό στο μηχάνημα του θύματος, στέλνει πακέτα σε αυτό το μηχάνημα με σκοπό να αποκτήσει τοπική πρόσβαση. Ορισμένες επιθέσεις R2L εκμεταλλεύονται υπερχειλίσσεις buffer στο λογισμικό διακομιστή δικτύου άλλες εκμεταλλεύονται αδύναμες ή λάθος ρυθμισμένες πολιτικές ασφαλείας. Αναφορικά:

Attack type	Service	Mechanism	Effect of the attack
Dictionary	telnet, rlogin, pop, ftp, imap	Abuse features	Gains user access
Ftp-write	ftp	Misconfig	Gains user access
Guest	telnet, rlogin	Misconfig	Gains user access
Imap	Imap	Bug	Gains root access
Named	Dns	Bug	Gains root access
Phf	http	Bug	Executes command as http user
Sendmail	Smtplib	Bug	Executes commands as root
Xlock	Smtplib	Misconfig	Spoof user to obtain password
Xnsoop	Smtplib	Misconfig	Monitor key strokes remotely

Πίνακας με R2L επιθέσεις και τρόπος λειτουργίας τους.

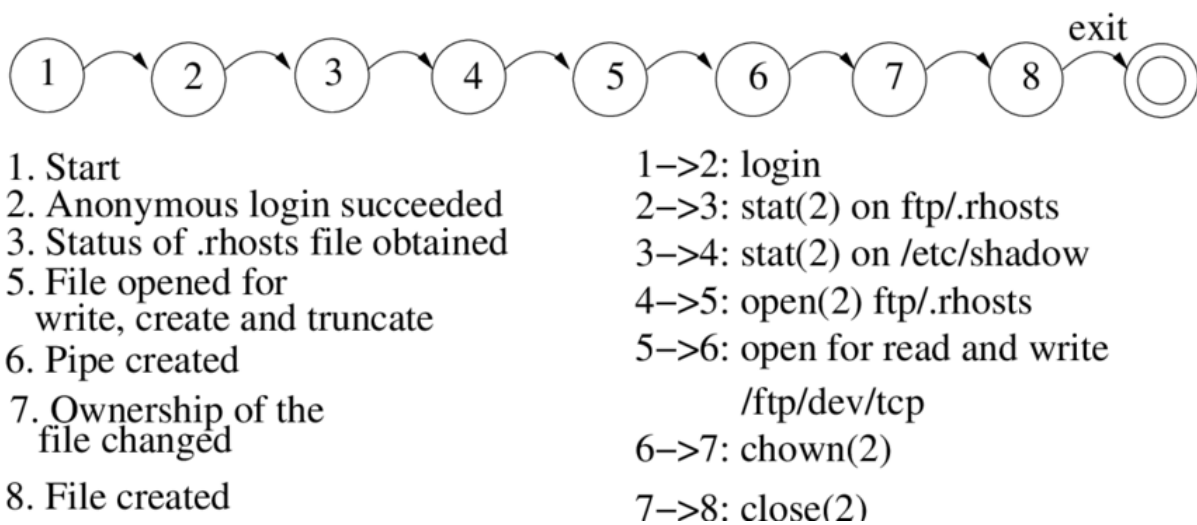
Dict: Η επίθεση λεξικού είναι μια επίθεση Remote to Local κατά την οποία ένας εισβολέας προσπαθεί να αποκτήσει πρόσβαση σε κάποιο μηχάνημα κάνοντας επανειλημμένες εικασίες για πιθανά ονόματα χρήστη και κωδικούς πρόσβασης. Οι χρήστες συνήθως δεν επιλέγουν καλούς κωδικούς πρόσβασης, επομένως ένας εισβολέας που γνωρίζει το όνομα χρήστη ενός συγκεκριμένου χρήστη (ή τα ονόματα όλων των χρηστών) με την επίθεση αυτή θα προσπαθήσει να αποκτήσει πρόσβαση στον λογαριασμό αυτού του χρήστη κάνοντας εικασίες για πιθανούς κωδικούς πρόσβασης. Η εικασία λεξικού μπορεί να γίνει με πολλές υπηρεσίες όπως Telnet, Ftp, Pop, Rlogin και imap.



Παράδειγμα λειτουργίας Dictionary επίθεσης.

Guest: Η επίθεση Guest είναι μια παραλλαγή της επίθεσης Dictionary. Σε συστήματα που δεν είναι σωστά ρυθμισμένα, οι λογαριασμοί επισκεπτών συχνά μένουν χωρίς κωδικό πρόσβασης ή με έναν εύκολο να μαντέψει κανείς κωδικό πρόσβασης. Επειδή τα περισσότερα λειτουργικά συστήματα αποστέλλονται με τον λογαριασμό επισκέπτη ενεργοποιημένο από προεπιλογή, αυτή είναι μια από τις πρώτες και απλούστερες ευπάθειες που θα προσπαθήσει να εκμεταλλευτεί ένας εισβολέας

Ftp write: Η επίθεση Ftp-write είναι μια επίθεση απομακρυσμένου σε τοπικό χρήστη που εκμεταλλεύεται μια γνωστή ανώνυμη εσφαλμένα διαμορφωμένη ftp. Ο ανώνυμος ριζικός κατάλογος ftp και οι υποκατάλογοι του δεν πρέπει να ανήκουν στον λογαριασμό ftp ή να ανήκουν στην ίδια ομάδα με τον λογαριασμό ftp. Εάν κάποιος από αυτούς τους καταλόγους ανήκει στο ftp ή ανήκει στην ίδια ομάδα με τον λογαριασμό ftp και δεν προστατεύεται από εγγραφή, ένας εισβολέας θα μπορεί να προσθέσει αρχεία (όπως ένα αρχείο rhosts) και να αποκτήσει τοπική πρόσβαση στο σύστημα.



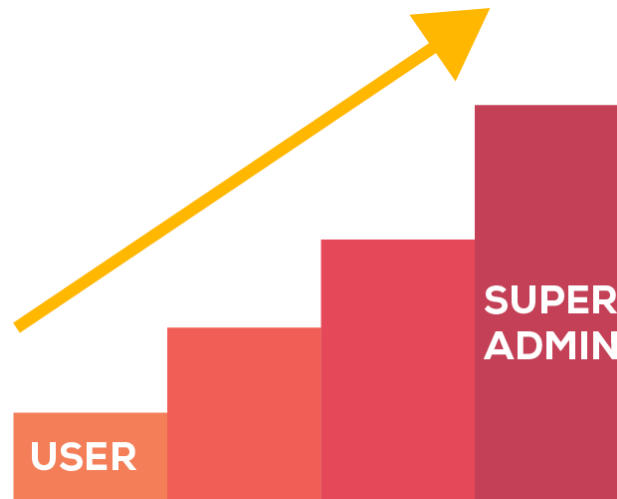
Σχεδιάγραμμα επίθεσης ftp-write.

Phf: Η επίθεση Phf κάνει κατάχρηση ενός κακογραμμένου script CGI για την εκτέλεση εντολών με το επίπεδο προνομίων του διακομιστή http. Οποιοδήποτε πρόγραμμα CGI που βασίζεται στη συνάρτηση CGI `escape_shell_cmd()` για να αποτρέψει την εκμετάλλευση κλήσεων βιβλιοθήκης που βασίζονται σε κέλυφος μπορεί να είναι ευάλωτο σε επίθεση. Συγκεκριμένα, αυτή η ευπάθεια εκδηλώνεται από το πρόγραμμα "phf" που διανέμεται με το παράδειγμα κώδικα για τον διακομιστή ιστού Apache.

2.3. Επιθέσεις User to Root

Επιθέσεις χρήστη σε root (δηλ. υπερχρήστη, το άτομο με το υψηλότερο επίπεδο προνομίων σε υπολογιστή Unix/Linux) κατά τη διάρκεια των οποίων ένας τοπικός χρήστης σε ένα μηχάνημα μπορεί να αποκτήσει προνόμια που κανονικά προορίζονται για τον υπερχρήστη του UNIX. Ορισμένες επιθέσεις U2R εκμεταλλεύονται κακώς γραμμένα προγράμματα συστήματος που εκτελούνται σε επίπεδο υπερχρήστη και είναι επιρρεπή σε υπερχειλίσσεις

buffer, άλλες εκμεταλλεύονται αδυναμίες στην επαλήθευση ονόματος διαδρομής, σφάλματα σε ορισμένες εκδόσεις του `suidperl` και άλλες αδυναμίες λογισμικού. Αναλυτικά:



Στόχος R2L επιθέσεων.

Eject: Η επίθεση Eject εκμεταλλεύεται μια υπερχείλιση buffer στο binary «eject» που διανέμεται με το Solaris 2.5. Στο Solaris 2.5, οι αφαιρούμενες συσκευές πολυμέσων που δεν διαθέτουν κουμπί εξαγωγής ή οι αφαιρούμενες συσκευές πολυμέσων που διαχειρίζονται από τη διαχείριση έντασης ήχου χρησιμοποιούν το πρόγραμμα εξαγωγής. Λόγω ανεπαρκών παραμέτρων που ελέγχουν τις εντολές στη βιβλιοθήκη διαχείρισης τόμου, `libvolmgt.so.1`, είναι δυνατό να αντικατασταθεί ο εσωτερικός χώρος στοίβας του προγράμματος εξαγωγής. Εάν εκμεταλλευτεί αυτή η ευπάθεια μπορεί να χρησιμοποιηθεί από τον κακόβουλο χρήστη για να αποκτήσει πρόσβαση υπερχρήστη σε συστήματα που έχουν δεχτεί την συγκεκριμένη επίθεση.

Ffbconfig: Η επίθεση Ffbconfig εκμεταλλεύεται μια υπερχείλιση buffer στο πρόγραμμα 'ffbconfig' που διανέμεται με το Solaris 2.5. Το πρόγραμμα ffbconfig ρυθμίζει τις παραμέτρους του Creator Fast Frame Buffer (FFB) Graphics Accelerator, το οποίο αποτελεί μέρος του πακέτου λογισμικού διαμόρφωσης FFB, `SUNWffbcf`. Αυτό το λογισμικό χρησιμοποιείται όταν είναι εγκατεστημένη η κάρτα επιτάχυνσης FFB Graphics. Λόγω

ανεπαρκών παραμέτρων ελέγχου των ορισμάτων, είναι δυνατή η αντικατάσταση του εσωτερικού χώρου στοίβας του προγράμματος `ffbconfig`.

Fdformat: Η επίθεση `Fdformat` εκμεταλλεύεται μια υπερχείλιση buffer στο πρόγραμμα `'fdformat'` που διανέμεται με το Solaris 2.5. Το πρόγραμμα `fdformat` κάνει format σε δισκέτες και κάρτες μνήμης PCMCIA. Το πρόγραμμα χρησιμοποιεί επίσης την ίδια βιβλιοθήκη διαχείρισης τόμου, `libvolmgt.so.1`, και εκτίθεται στην ίδια ευπάθεια με το πρόγραμμα εξαγωγής (επίθεση `eject`).

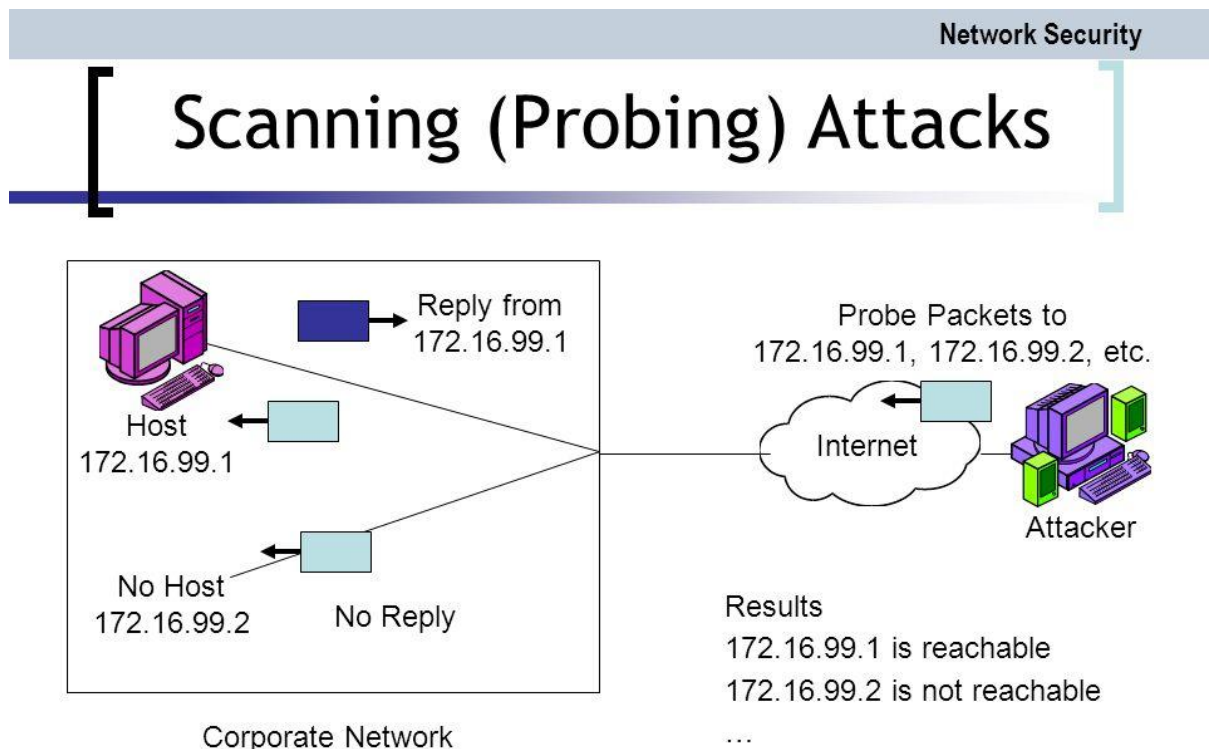
Loadmodule: Η επίθεση `Loadmodule` είναι μια επίθεση εναντίον συστημάτων SunOS 4.1 που χρησιμοποιούν το σύστημα παραθύρων `xnews`. Το πρόγραμμα `loadmodule` μέσα στο SunOS 4.1.x χρησιμοποιείται από τον διακομιστή συστήματος `xnews window` για τη φόρτωση δύο προγραμμάτων οδήγησης πυρήνα (`kernel drivers`) με δυνατότητα δυναμικής φόρτωσης στο τρέχον σύστημα και για τη δημιουργία ειδικών συσκευών στον κατάλογο `/dev` για τη χρήση αυτών των λειτουργικών μονάδων. Λόγω ενός σφάλματος στον τρόπο με τον οποίο το πρόγραμμα `loadmodule` απολυμαίνει το περιβάλλον του, οι μη εξουσιοδοτημένοι χρήστες μπορούν να αποκτήσουν πρόσβαση `root` στον τοπικό υπολογιστή.

Perl: Η επίθεση `Perl` είναι μια επίθεση που εκμεταλλεύεται ένα σφάλμα σε ορισμένες υλοποιήσεις της `Perl`. Το `Suidperl` είναι μια έκδοση της `Perl` που υποστηρίζει αποθηκευμένα σενάρια `set-user-ID` και `set-group-ID`. Στις πρώτες εκδόσεις του `suidperl`, ο διερμηνέας δεν χειρίζεται σωστά από τα δικαιώματα υπερχρήστη όταν αλλάζει τα αναγνωριστικά των χρηστών και ομάδων. Σε ένα σύστημα που έχει εγκατεστημένο το πρόγραμμα `suidperl` ή `sperl` και υποστηρίζει αποθηκευμένα `set-user-ID` και `save set-group-ID`, οποιοσδήποτε έχει πρόσβαση σε έναν λογαριασμό στο σύστημα μπορεί να αποκτήσει πρόσβαση υπερχρήστη.

2.4. Επιθέσεις `probe` ή `scan`

Αυτές περιλαμβάνουν προγράμματα που μπορούν να σαρώσουν αυτόματα ένα δίκτυο υπολογιστών και να συλλέξουν πληροφορίες ή να βρουν γνωστά ευάλωτα σημεία. Τέτοιοι ανιχνευτές είναι συχνά πρόδρομοι για πιο επικίνδυνες επιθέσεις επειδή παρέχουν έναν χάρτη

όλων των μηχανημάτων και υπηρεσιών και εντοπίζουν αδύναμα σημεία σε ένα δίκτυο. Μερικά από αυτά τα εργαλεία σάρωσης επιτρέπουν ακόμη και σε κάποιον ερασιτέχνη εισβολέα να ελέγξει εκατοντάδες μηχανήματα σε ένα δίκτυο και να λάβει αναφορά για οποιαδήποτε γνωστά τρωτά σημεία. Πιο συγκεκριμένα στο DARPA 1998 είδαμε:



Διάγραμμα επίθεσης scan.

Ipsweep: Μια επίθεση Ipsweep είναι μια σάρωση παρακολούθησης για να προσδιοριστεί ποιά μηχανήματα οικοδεσπότες(host machines) ακούν σε ένα δίκτυο. Αυτές οι πληροφορίες είναι χρήσιμες σε έναν εισβολέα για τη διοργάνωση επιθέσεων και την αναζήτηση ευάλωτων μηχανημάτων. Υπάρχουν πολλές μέθοδοι που μπορεί να χρησιμοποιήσει ένας εισβολέας για να εκτελέσει μια επίθεση Ipsweep. Η πιο συνηθισμένη μέθοδος και η μέθοδος που χρησιμοποιείται στην προσομοίωση είναι η αποστολή πακέτων Ping ICMP σε κάθε πιθανή διεύθυνση ενός υποδικτύου και η αναμονή για να δούμε ποια μηχανήματα ανταποκρίνονται. Οι ανιχνευτές Ipsweep στην προσομοίωση δεν ήταν μυστικοί και οι σαρώσεις πραγματοποιήθηκαν από μία μόνο πηγή.

Nmap: Το Nmap είναι ένα εργαλείο γενικής χρήσης που χρησιμεύει στην εκτέλεση σαρώσεων δικτύου. Το Nmap υποστηρίζει πολλούς διαφορετικούς τύπους επιλογών σάρωσης θυρών, όπως σάρωση SYN, FIN και ACK με TCP και UDP, καθώς και σάρωση ICMP (Ping). Το πρόγραμμα Nmap επιτρέπει επίσης στον χρήστη να καθορίσει ποιες θύρες θα σαρώσει, πόσο χρόνο θα περιμένει μεταξύ κάθε θύρας και εάν οι θύρες θα πρέπει να σαρωθούν διαδοχικά ή με τυχαία σειρά.

Satan: Το Satan στην απλούστερη λειτουργία του, συλλέγει όσο το δυνατόν περισσότερες πληροφορίες για απομακρυσμένους κεντρικούς υπολογιστές και δίκτυα εξετάζοντας υπηρεσίες δικτύου όπως το finger, NFS, NIS, ftp και tftp, rexd, statd και άλλες υπηρεσίες. Οι πληροφορίες που συλλέγονται περιλαμβάνουν την παρουσία διαφόρων υπηρεσιών πληροφοριών δικτύου καθώς και πιθανά ελαττώματα ασφαλείας. Αυτά τα ελαττώματα περιλαμβάνουν εσφαλμένες ρυθμίσεις ή διαμορφωμένες υπηρεσίες δικτύου, γνωστά σφάλματα σε βοηθητικά προγράμματα συστήματος ή δικτύου και κακές αποφάσεις πολιτικής ασφαλείας. Αν και το Satan δεν προορίζεται για χρήση ως εργαλείο επίθεσης, παρέχει πληροφορίες ασφαλείας που είναι αρκετά χρήσιμες σε έναν εισβολέα. Το Satan διανέμεται ως μια συλλογή προγραμμάτων perl και C και είναι γνωστό ότι τρέχει σε συστήματα Solaris, Linux και Irix. Το SATAN υποστηρίζει τρία επίπεδα σάρωσης: ελαφρύ, κανονικό και βαρύ. Τα τρωτά σημεία για τα οποία ελέγχει ο SATAN στη βαριά λειτουργία είναι: Εξαγωγή NFS σε μη προνομιούχα προγράμματα, εξαγωγή NFS μέσω portmapper, πρόσβαση σε αρχείο κωδικού πρόσβασης NIS, πρόσβαση REXD, πρόσβαση σε αρχείο tftp, απομακρυσμένη πρόσβαση κελύφους, απεριόριστη εξαγωγή NFS, απεριόριστη πρόσβαση διακομιστή X, οικιακός κατάλογος ftp με δυνατότητα εγγραφής, πολλά τρωτά σημεία του Sendmail καθώς και αρκετές ευπάθειες ftp. Οι σαρώσεις σε ελαφριά και κανονική λειτουργία απλώς ελέγχουν για μικρότερα υποσύνολα των ίδιων τρωτών σημείων.

3. ΜΕΘΟΔΟΛΟΓΙΑ

Σε αυτό το κεφάλαιο αναλύεται η διαδικασία και η ροή των πράξεων η οποία ακολουθήθηκε αναλυτικά για την διεξαγωγή των πειραμάτων. Περιγράφεται κάθε βήμα της διαδικασίας μετα απο μια συντομη περιγραφή του σκοπού.

Στόχος είναι η αξιολόγηση της αποτελεσματικότητας ενός NIDS και πιο συγκεκριμένα του Snort χρησιμοποιώντας το dataset της DARPA 1998. Για την αξιολόγηση χρησιμοποιούνται τα αρχεία από τις επτά εβδομάδες εκπαίδευσης που παρέχει το dataset τα οποία περιλαμβάνουν πακέτα με τη δραστηριότητα της αεροπορικής βάσης σε συνδυασμό με στοχευμένες επιθέσεις Denial of Service, User to Root, Remote to Local καθώς και probes και scan επιθέσεις. Με την χρήση του Snort, ελέγχονται ένα προς ένα τα αρχεία και συγκρίνονται τα πακέτα με τα “Rules” του Snort στις οποίες και δημιουργεί “alerts” σε οποιαδήποτε αντιστοίχιση υπάρξει. Στόχος είναι να εντοπιστούν αν όχι όλες τότε όσο το δυνατόν περισσότερες επιθέσεις σε κάθε μέρα των εβδομάδων και να παραχθούν τα κατάλληλα “ alerts “ που θα προειδοποιούν για την αντίστοιχη επίθεση ή ανωμαλία που υπάρχει στο δίκτυο.

3.1. Λειτουργίες

Για τον έλεγχο και ανάλυση του dataset DARPA 1998 χρησιμοποιήθηκε το πρόγραμμα Snort. Αναλυτικότερα, η διαδικασία ξεκίνησε με την εγκατάσταση και εξοικείωση με το πρόγραμμα και τις λειτουργίες του καθώς το Snort έχει 3 κύριες λειτουργίες, την λειτουργία “sniffer”, “packet logger” και “network intrusion detection system”.

- Sniffer: Στη λειτουργία sniffer, το πρόγραμμα διαβάζει και παρουσιάζει τα πακέτα δικτύου στην κονσόλα.

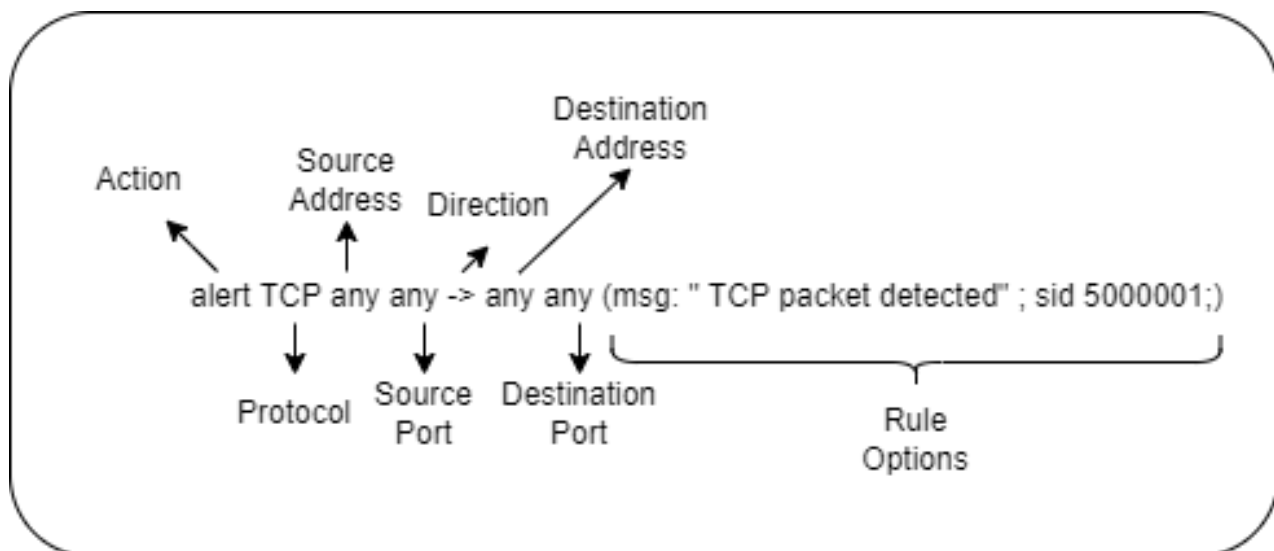
- Packet Logger: Στην λειτουργία αυτή απλώς καταγράφει πακέτα στον δίσκο.
- Network Intrusion Detection System: Στην λειτουργία αυτή το πρόγραμμα παρακολουθεί τη δραστηριότητα του δικτύου και την αναλύει με βάσει ένα σετ κανόνων που θέτει ο χρήστης.

Καθώς στη συγκεκριμένη περίπτωση χρησιμοποιήθηκε η τελευταία λειτουργία που αναφέρθηκε προηγουμένως αμέσως μετά την εξοικείωση με το πρόγραμμα έγινε η ρύθμιση των κανόνων “rules”.

3.2. Κανόνες

Για την διαδικασία αυτή χρειάστηκε κάποια έρευνα και αρχικά γράφτηκαν μερικοί κανόνες με το χέρι για να υπάρξει πλήρη κατανόηση του τρόπου γραφής, των παραμέτρων ενός κανόνα καθώς και το αποτέλεσμα που αυτός θα έχει. Η γραφή κανόνων με το χέρι είναι μια διαδικασία που κάθε χρήστης του Snort πρέπει να ξέρει καθώς μπορεί να αποβεί χρήσιμη σε οποιαδήποτε στιγμή. Για τα συγκεκριμένα πειράματα ωστόσο χρησιμοποιήθηκε ένας συνδυασμός των προκαθορισμένων κανόνων του Snort καθώς και των κανόνων της κοινότητας, που ανήλθε στον αριθμό περίπου 7600 κανόνων, ο οποίος και θεωρήθηκε επαρκής για την συγκεκριμένη αξιολόγηση.

Action	Protocol	Source Address	Source Port	Direction	Destination Address	Destination Port
--------	----------	----------------	-------------	-----------	---------------------	------------------



Βοηθητικό διάγραμμα σύνταξης κανόνων Snort.

3.3. Παράμετροι

Στη συνέχεια σειρά πήρε η συγκεντρώθηκαν και ταξινομήθηκαν σωστά τα απαραίτητα αρχεία από το DARPA 1998 dataset (<https://archive.ll.mit.edu/ideval/data/1998data.html>) σε φακέλους αναλυτικά για την κάθε ημέρα των επτά εβδομάδων, ξεκίνησαν τα πειράματα για κάθε μία από τις μέρες αυτές. Για την ανάλυση των αρχείων έγινε χρήση του Snort μέσω της εντολής `snort -A full -r /home/kali/Downloads/Week1/Friday/outside.tcpdump -c /etc/snort/snort.conf.comm` όπου στο `-A` ορίζεται η λειτουργία των “alerts” όπου υπάρχουν οι επιλογές

- **fast:** Λειτουργία γρήγορης ειδοποίησης όπου γράφει την ειδοποίηση σε απλή μορφή με χρονική σήμανση, μήνυμα ειδοποίησης και IP/θύρες προέλευσης και προορισμού
- **full:** Λειτουργία πλήρης ειδοποίησης κατά την οποία γίνεται αναλυτική αναφορά, επιπλέον από την “fast” εμφανίζει TTL, IP packet και IP header length, service, ICMP type και sequence number και ταυτόχρονα είναι η προκαθορισμένη επιλογή σε περίπτωση που δεν οριστεί η `-A` παράμετρος.
- **unsock:** Στέλνει ειδοποιήσεις σε μια υποδοχή UNIX την οποία μπορεί να ακούσει άλλο πρόγραμμα.
- **none:** Απενεργοποιεί τις ειδοποιήσεις.
- **console:** Στέλνει ειδοποιήσεις τύπου “fast” στην κονσόλα.

- `cmg`: Αυτή η λειτουργία αναπτύχθηκε από το Snort για δοκιμαστικούς σκοπούς, εκτυπώνει μια “full” ειδοποίηση στην κονσόλα χωρίς να αποθηκεύει αναφορές σε αρχεία καταγραφής.

Στην παράμετρο `-r` το πρόγραμμα διαβάζει και επεξεργάζεται το αρχείο (που πρέπει να έχει μορφή `tcpdump` ή `pcap`) και στην `-c` παράμετρο ορίζεται το `configuration file` ή στα ελληνικά το αρχείο με τις ρυθμίσεις του Snort. Στο τέλος κάθε ελέγχου δημιουργείται ένα αρχείο που ονομάζεται `alert/log file` και περιέχει όλες τις ειδοποιήσεις και αναλύσεις του Snort. Τα αρχεία αυτά συλλέχθηκαν, μετονομάστηκαν και ταξινομήθηκαν για να γίνει στη συνέχεια ο έλεγχος των αποτελεσμάτων.

4. ΑΠΟΤΕΛΕΣΜΑΤΑ

Στο Κεφάλαιο αυτό γίνεται μια ανάλυση των αποτελεσμάτων που προέκυψαν κατά τη διάρκεια των πειραμάτων. Πραγματοποιείται μια αναλυτική περιγραφή του τρόπου με τον οποίο συλλέχθηκαν αλλά και επαληθεύτηκαν τα αποτελέσματα για κάθε μια από τις επτά εβδομάδες εκπαίδευσης στο dataset και δίνεται ορισμός του Wireshark.

Ξεκινώντας από την Δευτέρα της πρώτης εβδομάδας και συνεχίζοντας με την σειρά, τα αρχεία του dataset έτρεξαν ένα προς ένα ενάντια στο Snort και τους κανόνες που ορίστηκαν. Για κάθε μια από τις ημέρες των εβδομάδων προέκυπτε ένα αρχείο το οποίο περιείχε κάθε alert που είχε προκύψει κατά τη διάρκεια του ελέγχου. Ο έλεγχος για να αξιολογηθεί ο αριθμός των alerts σε σύγκριση με τον αριθμό των πακέτων που είχαν σταλεί με κάθε επίθεση, στην αρχική ιδέα ήταν να γίνει αυτοματοποιημένα. Ωστόσο ως εναλλακτική και τελική λύση προτάθηκε ο έλεγχος με το χέρι, σε ένα πρόγραμμα που ελέγχει και αναλύει πακέτα. Η επιλογή αυτή ως κύριο θεμέλιο έχει την προσομοίωση στην πραγματικότητα όπου η ανάλυση των αποτελεσμάτων του Snort θα είναι απαραίτητη και τα αποτελέσματα με τον αριθμό των πακέτων για κάθε επίθεση δεν θα είναι διαθέσιμα. Έτσι λοιπόν αφού ήταν απαραίτητη η ανάλυση των πακέτων, έπρεπε να επιλεγεί ένα εργαλείο ανάλυσης πακέτων και αυτό ήταν το Wireshark.

Η ανάλυση πακέτων αποδεικνύεται χρήσιμη σε διάφορες περιπτώσεις όπως για παράδειγμα η διάγνωση ενός δικτύου σε περίπτωση επίθεσης,. Άλλες φορές αποτελεί απλώς βοήθεια στους διαχειριστές του δικτύου ώστε να εξετάσουν και να αναλύσουν την δραστηριότητα που υπάρχει σε ένα δίκτυο ή σε ένα αρχείο με πακέτα και να προσδιορίσουν προβλήματα που ενδέχεται να υπάρχουν. Μια τέτοια διαδικασία αποτελεί τα θεμέλια της αντιμετώπισης προβλημάτων σε δίκτυα και η χρήση εργαλείων ανάλυσης πακέτων όπως το Wireshark είναι απαραίτητη. Η ανάλυση πακέτων με στόχο την επιβολή της ασφάλειας του δικτύου μπορεί να βοηθήσει τους χρήστες να απαντήσουν σε διάφορες σημαντικές ερωτήσεις σχετικά με την

ασφάλεια των υπολογιστών ή του δικτύου όπως για παράδειγμα ποιος είναι ο εισβολέας και πώς διείσδυσε στις υπάρχουσες προφυλάξεις ασφαλείας, τι ζημιά έχει γίνει, αν εισβολέας άφησε κάτι όπως έναν νέο λογαριασμό χρήστη, δούρειο ίππο ή ίσως κάποιο νέο τύπο επίθεσης τύπου “worm”. Με πληροφορίες που μπορεί να συλλέξει απο μια τέτοια ανάλυση το κατάλληλο άτομο μπορεί ακόμα και να επιδιορθώσει το κενό στην ασφάλεια, να αναπαράγει την επίθεση και να επαληθεύσει ότι η επιδιόρθωση θα λειτουργήσει. Οι επιθέσεις δικτύου μπορούν να εντοπιστούν ως επί το πλείστον παρατηρώντας την εισερχόμενη και την εξερχόμενη κίνηση, επειδή η ασυνήθιστη συμπεριφορά προκύπτει από ύποπτα μοτίβα πακέτων. Οι λόγοι που επιλέχθηκε για την διαδικασία αυτή το Wireshark είναι αρκετοί αλλά κυρίως επικεντρώνονται στο γεγονός ότι το Wireshark είναι ίσως ο πιο δημοφιλής αναλυτής πακέτων δικτύου στον κόσμο και χρησιμοποιείται για την αντιμετώπιση προβλημάτων και την ανάλυση πρωτοκόλλων δικτύου και εφαρμογών σε μεγάλη ποικιλία τεχνολογιών. Είναι δωρεάν και διαθέσιμο σε πολλές πλατφόρμες, μεταξύ αυτών και των Windows, Linux, Mac OS καθώς και διάφορες Unix πλατφόρμες. Φροντίζει να διατηρείται διαρκώς ενημερωμένο και συνεχίζει να βελτιώνεται και να επεκτείνεται συνεχώς με την βοήθεια πολυάριθμων προγραμματιστών που συνεισφέρουν καθώς το πρόγραμμα είναι ανοιχτού κώδικα. Το Wireshark παρέχει έναν μεγάλο αριθμό χαρακτηριστικών ανάμεσα στα οποία είναι η λήψη, αποθήκευση και εισαγωγή αρχείων με πακέτα σε διάφορες μορφές. Παρέχει εκτεταμένο αριθμό φίλτρων που μπορούν να χρησιμοποιηθούν για διάφορους σκοπούς και σε διάφορους παραμέτρους, πολυάριθμες λεπτομέρειες σχετικά με πληροφορίες πρωτοκόλλου, στατιστικά στοιχεία και ενσωματωμένες λειτουργίες ανάλυσης και χρωματισμού πακέτων οι οποίες αποδείχθηκαν αρκετά χρήσιμες στην ανάλυση των αρχείων και τον εντοπισμό των επιθέσεων. Η διαδικασία εκμάθησης της χρήσης των φίλτρων καθώς και η εξοικείωση με τα ξεχωριστά χρώματα που αντιστοιχούν σε διάφορα είδη πρωτοκόλλων πήρε λίγο χρόνο στην αρχή αλλά μετά την πρώτη εβδομάδα ανάλυσης, η διαδικασία φάνηκε να κυλά ομαλά. Σύντομα, καθώς μερικές επιθέσεις επαναλαμβάνονται από την μια μέρα στην άλλη και μερικές φορές ακόμα περισσότερο από την μια εβδομάδα στην επόμενη, ορισμένα πακέτα ξεχώριζαν και ο εντοπισμός και η ανάλυση έγιναν γρήγορα.

No.	Time	Source	Destination	Protocol	Length	Info
10510	16607.663192	172.16.113.50	197.218.177.69	FTP	70	Request: USER anonymous
17650	28162.787050	172.16.113.50	197.218.177.69	FTP	70	Request: USER anonymous
19916	31897.737453	172.16.113.50	197.218.177.69	FTP	70	Request: USER anonymous
22059	35442.322756	172.16.113.50	172.16.113.50	TCP	60	23 → 23 [SYN] Seq=0 Win=2048 Len=0
10521	16625.922825	197.218.177.69	172.16.113.50	FTP-DATA	590	FTP Data: 536 bytes
10522	16626.123694	197.218.177.69	172.16.113.50	FTP-DATA	590	FTP Data: 536 bytes
17655	28172.998916	197.218.177.69	172.16.113.50	FTP-DATA	590	FTP Data: 536 bytes
19927	31920.526516	197.218.177.69	172.16.113.50	FTP-DATA	590	FTP Data: 536 bytes
19930	31922.112823	197.218.177.69	172.16.113.50	FTP-DATA	590	FTP Data: 536 bytes
19931	31922.311466	197.218.177.69	172.16.113.50	FTP-DATA	590	FTP Data: 536 bytes

Frame 22059: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)	
Ethernet II, Src: Dell_a3:58:23 (00:c0:4f:a3:58:23), Dst: Cisco_04:41:bc (00:00:0c:04:41:bc)	
Internet Protocol Version 4, Src: 172.16.113.50, Dst: 172.16.113.50	
Transmission Control Protocol, Src Port: 23, Dst Port: 23, Seq: 0, Len: 0	
Source Port: 23	
Destination Port: 23	
[Stream index: 406]	
[Conversation completeness: Incomplete, SYN_SENT (1)]	
[TCP Segment Len: 0]	
Sequence Number: 0 (relative sequence number)	
Sequence Number (raw): 3868	

0000	00 00 0c 04 41 bc 00 c0 4f a3 58 23 08 00 45 00	...A... 0·X#·E·
0010	00 28 0f 1c 00 00 ff 06 72 2e ac 10 71 32 ac 10	·(·..... r·...q2·
0020	71 32 00 17 00 17 00 00 0f 1c 00 00 00 00 50 02	q2·.....·P·
0030	08 00 5e 13 00 00 00 00 00 00 00 00	..Λ.....

Παράδειγμα επίθεσης land - ανάλυση αρχείου με Wireshark.

Σε αυτό το σημείο αξίζει να επισημανθεί ότι ορισμένες επιθέσεις ήταν προσδιορισμένο ότι έγιναν χωρίς κάποια πρόθεση να κρυφτούν και αυτές δηλωνόταν ως “clear” επιθέσεις και αυτό ήταν μέρος των πληροφοριών που υπήρχαν στα δεδομένα. Επομένως τέτοιου είδους επιθέσεις υπο φυσιολογικές συνθήκες θα έπρεπε να είναι φανερές στο αρχείο και επομένως πιο εύκολο στον εντοπισμό τους. Αντίστοιχα υπήρχαν επιθέσεις με τον προσδιορισμό “stealth” όπου σημαίνει ότι για τις συγκεκριμένες επιθέσεις έχουν γίνει προσπάθειες απόκρυψης στοιχείων sniffing και audit με κρυπτογράφηση, με τη διαδοση επίθεσης σε πολλαπλές περιόδους σύνδεσης ή με άλλες τεχνικές. Υπάρχουν διάφορες άλλες λέξεις-κλειδιά οι οποίες υποδεικνύουν, συνήθως προφανή, χαρακτηριστικά συγκεκριμένων επιθέσεων ή επιχειρήματα για διαφορετικά προγράμματα επίθεσης καθώς και διάφορες μικρές σημειώσεις για συγκεκριμένες επιθέσεις. . Επιπλέον υπάρχει η λέξη-κλειδί " fast " καθώς και η λέξη-κλειδί " many " που η “ fast “ σημαίνει ότι μια σάρωση έγινε σε σύντομο χρονικό διάστημα, ενώ η λέξη-κλειδί “ many “ αντίστοιχα σημαίνει ότι ένα portsweep προσπάθησε να συνδεθεί σε πολλές διαφορετικές θύρες. Επιπρόσθετα, υπάρχουν λέξεις κλειδιά που αναφέρονται σε επίπεδα σάρωσης στις επιθέσεις σάρωσης και ανίχνευσης όπως για παράδειγμα η λέξη-κλειδί " level 1 " αναφέρεται στο μεσαίο επίπεδο σάρωσης που

παρέχεται από το εργαλείο ανίχνευσης δικτύου `satan`. Άλλα σχόλια υποδεικνύουν επιθέσεις που χρησιμοποιούνται ως μέρη ενός σεναρίου που αποτελείται από πολλές περιόδους σύνδεσης. Για παράδειγμα, κατά την διάρκεια της τρίτης εβδομάδας εμφανίζεται το σχόλιο `"guest,runs crack"` σε μια απο τις ημέρες που σημαίνει ότι ένας εισβολέας συνδέεται σε έναν λογαριασμό επισκέπτη ως μέρος ενός σεναρίου `multihop` και εκτελεί το πρόγραμμα σπασίματος(`crack`) σε μια προσπάθεια να βρει κωδικούς πρόσβασης. Αυτό το σενάριο εμφανίζεται ξανά στην ίδια εβδομάδα αργότερα, όπου ένας εισβολέας χρησιμοποιεί την επίθεση `perlmagic` για να αποκτήσει πρόσβαση `root`.

4.1. 1η Εβδομάδα

Κατά τη διάρκεια της πρώτης εβδομάδας βλέπουμε ως επι το πλείστον δύο κατηγορίες επιθέσεων να επικρατούν, οι `Denial of Service` και οι `User to Root` επιθέσεις. Από την Δευτέρα ως την Παρασκευή φαίνεται να πραγματοποιούνται διάφορες επιθέσεις των δύο αυτών κατηγοριών όπως για παράδειγμα `Fdformat`, `Ffbformat`, `loadmodule`, `perl`, `neptune`, `smurf` και `teardrop` επιθέσεις. Σε σύγκριση με τις υπόλοιπες εβδομάδες μπορούμε να αντιληφθούμε ότι κατά τη διάρκεια της πρώτης εβδομάδας δεν εκτελούνται πολλές επιθέσεις κάθε μέρα και δεν ποικίλουν σε κατηγορία. Με τον αριθμό να ανέρχεται το περισσότερο σε μόνο δύο επιθέσεις ημερησίως και οι περισσότερες από αυτές να ανήκουν στην κατηγορία “`clear`”, δηλαδή να μην έχουν γίνει προσπάθειες να πραγματοποιηθούν κρυφά οι επιθέσεις, μπορούμε εύκολα να συμπεράνουμε ότι κατά τη διάρκεια της πρώτης εβδομάδας οι ημερήσιες επιθέσεις δεν ήταν αποπνικτικές. Πιο αναλυτικά:

- Δευτέρα: Η πρώτη μέρα της εβδομάδας γνωρίζαμε πως περιείχε στο σύνολο δύο επιθέσεις και από αυτές και οι δύο ήταν `User to Root` επιθέσεις. Κατά τη διάρκεια ελέγχου του αρχείου ενάντια στο `Snort`, ελέγχθηκε η δραστηριότητα της ημέρας η οποία όπως και σε όλες τις υπόλοιπες ημέρες των επτά εβδομάδων ανερχόταν σε έναν πολύ μεγάλο αριθμό πακέτων(ενδεικτικά, 249.679 πακέτα). Στο τέλος της διαδικασίας, το `Snort` δημιούργησε `alerts` για πακέτα τα οποία έφταναν τον αριθμό των 2349 εκ των οποίων 2 αντιστοιχούσαν στις επιθέσεις που έγιναν εκείνη την ημέρα. Η πρώτη επίθεση

που έγινε κατά τη διάρκεια της ημέρας ήταν η **Fdformat(clear)** επίθεση η οποία έγινε με την αποστολή ενός μόνο πακέτου όπως ακριβώς και η **ffbconfig(clear)**. Και στις δύο περιπτώσεις το Snort εντόπισε τα πακέτα επίθεσης και έστειλε το ανάλογο alert.

- Τρίτη: Η δεύτερη μέρα της εβδομάδας περιείχε στο σύνολο εξίσου δύο διαφορετικές επιθέσεις οι οποίες όμως κατατάσσονται στην ίδια κατηγορία όπως της προηγούμενης ημέρας, δηλαδή User to Root. Κατά τη διάρκεια του ελέγχου το Snort δημιούργησε 2018 alerts για πακέτα, εκ των οποίων ένα αντιστοιχούσε στην επίθεση **perl(clear)** το οποίο και εντόπισε το Snort και έστειλε το αντίστοιχο alert. Ωστόσο εκείνη την ημέρα υπήρχε και άλλη μια επίθεση, η επίθεση **loadmodule(clear)** η οποία έγινε μέσω ενός και μόνο πακέτου το οποίο το Snort απέτυχε να εντοπίσει.
- Τετάρτη: Την τρίτη μέρα της εβδομάδας πραγματοποιήθηκαν δύο επιθέσεις στο σύνολο οι οποίες και οι δύο ήταν Denial of Service επιθέσεις. Η πρώτη επίθεση που έγινε ήταν η **neptune** επίθεση και έγινε με την αποστολή 15 πακέτων στο σύνολο. Η δεύτερη επίθεση DoS ωστόσο η οποία ήταν η **smurf**, πραγματοποιήθηκε με τη χρήση 524 πακέτων αλλά παρόλα αυτά το Snort παρά τα 2511 alerts που δημιούργησε απέτυχε να εντοπίσει με επιτυχία οποιαδήποτε από τις δύο επιθέσεις.
- Πέμπτη: Κατά τη διάρκεια της Πέμπτης, πραγματοποιήθηκαν δύο ξεχωριστές επιθέσεις εκ των οποίων η μία ήταν Denial of Service επίθεση ενώ η άλλη Remote to Local. Πρώτα πραγματοποιήθηκε η R2L επίθεση με το όνομα **diet** η οποία έγινε με ένα μόνο πακέτο και εντοπίστηκε από το Snort. Η DoS επίθεση με το όνομα **Ping of Death**, παρά το γεγονός ότι χρησιμοποιήθηκαν 450 πακέτα το Snort δεν ήταν σε θέση να την εντοπίσει επιτυχώς.
- Παρασκευή: Την τελευταία μέρα της εβδομάδας πραγματοποιήθηκε μία και μόνο επίθεση η οποία κατατάσσεται στις Denial of Service επιθέσεις. Η

επίθεση ήταν η **teardrop** και έγινε με την χρήση ενός μοναδικού πακέτου του οποίου την πρόθεση το Snort δεν ήταν σε θέση να ξεχωρίσει και να στείλει alert.

4.2. 2η Εβδομάδα

Κατα τη διάρκεια της δεύτερης εβδομάδας παρατηρούμε ότι παρουσιάζονται αρκετές καινούργιες επιθέσεις που βλέπουμε για πρώτη φορά. Οι επιθέσεις αυτές ανήκουν στις κατηγορίες Remote to Local, Probes/scan και Denial of Service επιθέσεις. Από την πρώτη ως και την τελευταία ημέρα μπορούμε να διακρίνουμε να γίνονται διάφορες επιθέσεις καθημερινά οι οποίες είναι οι guest, portsweep, ipsweep, land, ftp-write, imap, back και syslog επιθέσεις. Από την αρχή της εβδομάδας διακρίνουμε να γίνονται κυρίως μια με δύο επιθέσεις την μέρα με εξαίρεση την Παρασκευή όπου και εκτελέστηκαν τέσσερις διαφορετικές επιθέσεις μέσα στην μέρα και την Πέμπτη κατα τη διάρκεια της οποίας δεν πραγματοποιήθηκε καμία επίθεση. Αναλυτικότερα:

- Δευτέρα: Η πρώτη μέρα της εβδομάδας περιείχε δύο διαφορετικού είδους επιθέσεις εκ των οποίων η μια ανήκει στην κατηγορία των scan επιθέσεων ενώ η δεύτερη είναι μια Remote to Local επίθεση. Η πρώτη επίθεση που έγινε κατα τη διάρκεια της ημέρας ήταν μια **portsweep** επίθεση η οποία πέρασε απαρατήρητη από το Snort το οποίο απέτυχε να εντοπίσει κάποιο από τα 113 πακέτα επίθεσης που στάλθηκαν παρόλο που η αναζήτηση για ανοιχτά ports έγινε σε λειτουργία fast, επομένως με καμία πρόθεση να κρυφτεί. Η δεύτερη επίθεση αντίστοιχα ήταν η **guest** επίθεση η οποία πραγματοποιήθηκε με τη χρήση 50 πακέτων επίθεσης μέσα από τα οποία έγινε η προσπάθεια να “μαντέψουν” οι επιτιθέμενοι με δοκιμές πιθανών ονομάτων και κωδικών και να συνδεθούν σε κάποιο λογαριασμό των μηχανημάτων. Για τα συγκεκριμένα 50 πακέτα επίθεσης το Snort έστειλε 148 alerts καθώς έστειλε παραπάνω από μια ειδοποιήσεις για κάθε πακέτο και για κάθε αποτυχημένη προσπάθεια.

- Τρίτη: Η δεύτερη μέρα της εβδομάδας περιείχε μόνο μία επίθεση στο σύνολο και αυτή ήταν η επίθεση **ipsweep** της κατηγορίας Scan. Για την επίθεση αυτή στάλθηκαν 930 πακέτα επίθεσης πράγμα που είναι απόλυτα φυσιολογικό καθώς μιλάμε για ping ICMP πακέτα με σκοπό την αναγνώριση των μηχανημάτων που ανταποκρίνονται. Η επίθεση αυτή εντοπίστηκε απο το Snort το οποίο έστειλε στο σύνολο 85 alerts που αντιστοιχούσαν στα πακέτα επίθεσης.
- Τετάρτη: Κατά τη διάρκεια της τρίτης μέρας της εβδομάδας πραγματοποιήθηκε μια μόνο επίθεση της κατηγορίας Denial of Service και αυτή ήταν η επίθεση **land**. Η επίθεση έγινε με την αποστολή ενός και μόνο πακέτου από και προς τον χρήστη “zeno” το οποίο και εντόπισε το Snort κατα τη διάρκεια του ελέγχου και έστειλε τα απαραίτητα alerts.
- Παρασκευή: Κατά τη διάρκεια της τελευταίας μέρας της εβδομάδας, πραγματοποιήθηκαν στο σύνολο 4 διαφορετικές επιθέσεις εκ των οποίων οι δύο πρώτες ανήκουν στη κατηγορία Remote to Local επιθέσεις και οι υπόλοιπες δύο ήταν Denial of Service επιθέσεις. Η πρώτη επίθεση που έγινε ήταν η **ftp-write** επίθεση η οποία πραγματοποιήθηκε μέσα από 4 πακέτα επίθεσης από τα οποία το Snort αναγνώρισε και έστειλε alert για τα 2. Η επόμενη επίθεση στη σειρά ήταν η επίθεση **imap** η οποία έγινε με τη χρήση ενός και μόνο πακέτου το οποίο και εντόπισε το Snort και έστειλε το ανάλογο alert. Στη συνέχεια σειρά είχε η πρώτη DoS επίθεση η οποία ήταν η **back** με τη βοήθεια της οποίας οι επιτιθέμενοι έστειλαν 11 χιλιάδες πακέτα ενάντια στον διακομιστή apache ενός μηχανήματος. Το Snort ξεχώρισε τα πακέτα και έστειλε πάνω από 11 χιλιάδες alerts καθώς συχνά φάνηκε να στέλνει παραπάνω από ένα alert για κάθε πακέτο επίθεσης που διέκρινε. Τελευταία στη σειρά ήταν η DoS επίθεση **syslogd** η οποία πραγματοποιήθηκε με τη χρήση ενός και μόνο πακέτου το οποίο το Snort δεν εντόπισε.

4.3. 3η Εβδομάδα

Κατά τη διάρκεια της τρίτης εβδομάδας παρατηρείται μεγαλύτερος αριθμός επιθέσεων στο σύνολο και εμφανίζονται επιθέσεις που αντιστοιχούν τόσο σε Denial of Service, User to Root, Remote to Local καθώς και scan/probe κατηγορίες επιθέσεων. Η κάθε μέρα εκτός της Τρίτης που δεν πραγματοποιήθηκαν επιθέσεις περιέχει ποικίλες επιθέσεις που αποτελούνται από **satan**, **phf**, **ffbconfig**, **portsweep**, **nmap**, **ftp-write**, **smurf**, **ipsweep**, **multihop**, **back**, **neptune**, **warez**, **imap**, **warezmaster** και **land**. Σε αντίθεση με τις έως τώρα εβδομάδες παρατηρείται ο αριθμός των 3 έως 5 επιθέσεων καθημερινά με διάφορες κατηγορίες επιθέσεων στην κάθε μέρα. Πιο συγκεκριμένα:

- Δευτέρα: Κατά τη διάρκεια της πρώτης μέρας της 3ης εβδομάδας εμφανίζονται 4 στο σύνολο επιθέσεις για τις οποίες έχουμε με τη σειρά μία Probe επίθεση, μια Remote to Local επίθεση, μια User to Root επίθεση και τέλος ακόμα μια Probe επίθεση. Πρώτη στη λίστα εμφανίζεται η επίθεση **satan** η οποία πραγματοποιείται με τη χρήση 31 πακέτων επίθεσης τα οποία το Snort εντοπίζει και στέλνει alert για κάθε ένα από αυτά. Στη συνέχεια ακολουθεί η **phf** επίθεση η οποία γίνεται με ένα και μόνο πακέτο επίθεσης το οποίο επίσης εντοπίζει και στέλνει alert το Snort. Αμέσως επόμενη είναι η **ffbconfig** επίθεση εξίσου με ένα πακέτο επίθεσης όπως η προηγούμενη επίθεση και όπως και πριν το Snort καταφέρνει να εντοπίσει την επίθεση και να στείλει το καταλληλο alert. Τελευταία στη σειρά είναι μια **portsweep** επίθεση η οποία έγινε μέσω 240 πακέτων επίθεσης τα οποία πέρασαν απαρατήρητα από το Snort το οποίο δεν κατάφερε να εντοπίσει καποιο από αυτά.
- Τετάρτη: Κατά τη διάρκεια της Τετάρτης εντοπίζονται 6 συνολικά επιθέσεις οι οποίες κατηγοριοποιούνται με τη σειρά ως μια Probe, μια Remote to Local, αλλη μια Probe, ενός σεναρίου επιθέσεων και μιας Denial of Service επίθεσης. Πρώτη από αυτές εμφανίζεται η **nmap** επίθεση η οποία παρά το γεγονός ότι εκτελέστηκε σε stealth λειτουργία το Snort κατάφερε να εντοπίσει και να στείλει alert για σχεδόν όλα τα 1337 πακέτα επίθεσης που στάλθηκαν προς το θύμα. Αμέσως επόμενη είναι η **ftp-write** επίθεση η οποία έγινε μέσω 4 πακέτων επίθεσης από τα οποία το Snort εντόπισε επιτυχώς τα 3. Συνέχεια

έχει η **ipsweep** επίθεση η οποία πραγματοποιήθηκε με την αποστολή 5632 πακέτων επίθεσης για τα οποία το Snort έστειλε περίπου τον τριπλάσιο αριθμό alerts καθώς για κάθε ένα από τα πακέτα επίθεσης έστειλε πολλαπλά alerts. Στη συνέχεια εμφανίζεται ένα σενάριο επιθέσεων που είναι δηλωμένο ως **multihop** στο οποίο πραγματοποιούνται διάφορες επιθέσεις αλλά πρώτα πρέπει ο επιτιθέμενος να αποκτήσει πρόσβαση σε ένα μηχάνημα. Απο τα 6 πακέτα που αντιστοιχούσαν στην προσπάθεια αυτή το Snort εντόπισε και έστειλε alert για το 1. Τέλος διακρίνεται μια **back** επίθεση DoS για την οποία και δημιουργήθηκαν 11 χιλιάδες πακέτα επίθεσης από τα οποία το Snort εντόπισε τα 1000 και έστειλε τα απαραίτητα alerts.

- Πέμπτη: Κατα τη διάρκεια της τέταρτης μέρας της εβδομάδας διακρίνονται 3 επιθέσεις οι οποίες ήταν με τη σειρά ένα σενάριο επίθεσης, μια Denial of Service επίθεση και μια warez επίθεση. Το σενάριο επίθεσης **multihop** έγινε πρώτο μέσα στη μέρα και αυτή τη φορά στόχευσε σε 2 διαφορετικούς χρήστες με 1 πακέτο επίθεσης για τον καθένα. Το Snort αναγνώρισε και τα 2 πακέτα και έστειλε το αντίστοιχο alert για το καθένα. Αμέσως μετά ακολούθησε η DoS επίθεση **neptune** η οποία προσπάθησε να πλημμυρίσει διάφορα διαθέσιμα ports με πακέτα επίθεσης για αυτό και έστειλε 204800 πακέτα επίθεσης. Το Snort κατάφερε να αναγνωρίσει μερικά από αυτά στέλνοντας 610 alerts που αντιστοιχούσαν στην επίθεση. Τέλος, εμφανίζεται η **warez** επίθεση σύμφωνα με την οποία ο επιτιθέμενος συνδέεται σε FTP site και δημιουργεί ένα κρυφό φάκελο. Αυτό έγινε με την αποστολή 1 μόνο πακέτου επίθεσης το οποίο και εντόπισε και δημιουργησε alert το Snort.
- Παρασκευή: Την τελευταία μέρα της εβδομάδας διακρίνονται 4 διαφορετικές μεταξύ τους επιθέσεις εκ των οποίων η πρώτη είναι μια Remote to Local επίθεση, η δεύτερη μια probe επίθεση, η τρίτη είναι μια warezmaster επίθεση και η τελευταία μια Denial of Service επίθεση. Πρώτη εμφανίζεται η επίθεση **imap** η οποία επαναλήφθηκε 2 φορές κατά τη διάρκεια της ημέρας με 6 πακέτα επίθεσης από τα οποία το Snort εντόπισε τα 2. Αμέσως μετά πραγματοποιήθηκε μια επίθεση υπερχειλίσης με πακέτα Echo ICMP με τη χρήση του εργαλείου **nmap**. Για την επίθεση αυτή στάλθηκαν 1020 πακέτα

επίθεσης για τα οποία το Snort έστειλε πολλαπλά alert για το καθένα. Επόμενη στη σειρά είναι η επίθεση **warezmaster** κατά τη διάρκεια της οποίας γίνεται ένα ανώνυμο upload αρχείων σε έναν διακομιστή FTP. Στην επίθεση αυτή αντιστοιχούσαν 19 πακέτα επίθεσης από τα οποία το Snort ξεχώρισε και έστειλα τα αντίστοιχα alerts για 4. Τελευταία πραγματοποιήθηκε η DoS επίθεση **land** με την αποστολή 8 πακέτων εκ των οποίων το Snort κατάφερε να εντοπίσει το 1.

4.4. 4η Εβδομάδα

Κατά τη διάρκεια της τέταρτης εβδομάδας παρατηρούμε ότι πραγματοποιούνται καθημερινά αρκετές επιθέσεις τόσο της κατηγορίας Denial of Service, User to Root καθώς και Probe και επιθέσεις σεναρίων. Από την πρώτη έως και την τελευταία μέρα βλέπουμε να πραγματοποιείται καθημερινά ένας συνδυασμός των επιθέσεων warezclient, ping of death, rootkit, smurf, satan, neptune, spy, teardrop, ipsweep, portsweep, syslogd, ffb, format, multihop αλλά και loadmodule. Πιο επιβαρυνμένες ημέρες με επιθέσεις φαίνεται να είναι η Τρίτη και η Παρασκευή με 7 επιθέσεις η κάθε μια και μερικές από αυτές να επαναλαμβάνονται παραπάνω από μια φορές κατά τη διάρκεια της ημέρας. Όσον αφορά τις υπόλοιπες μέρες παρατηρούνται 3 με 4 επιθέσεις στην κάθε μέρα. Πιο αναλυτικά:

- Δευτέρα: Η πρώτη μέρα της εβδομάδας δεν μπόρεσε να ελεγχθεί καθώς το αρχείο χαρακτηρίστηκε ως κατεστραμμένο από την ιστοσελίδα του MIT Lincoln Laboratory και για αυτό το λόγο έχει αφαιρεθεί και δεν είναι διαθέσιμο.
- Τρίτη: Τη δεύτερη μέρα της εβδομάδας διακρίνονται 7 διαφορετικές επιθέσεις οι οποίες αντιστοιχούν τόσο στην κατηγορία Denial of Service καθώς και στις probe επιθέσεις αλλά και σε σενάρια επίθεσης. Πρώτη κατά τη διάρκεια της ημέρας εμφανίζεται η **warezclient** επίθεση. Μια επίθεση κατά την οποία οι χρήστες κατεβάζουν παράνομο λογισμικό το οποίο έχει αναρτηθεί εκεί προηγουμένως μέσω File Transfer Protocol (FTP) μέσω της επίθεσης

warezmaster. Η λήψη αυτή έγινε αντιληπτή από το Snort το οποίο εντόπισε επιτυχώς και τα 538 πακέτα FTP-DATA και έστειλε τα αντίστοιχα alerts. Αμέσως επόμενη έγινε η επίθεση satan για την οποία και στάλθηκαν 9485 πακέτα επίθεσης. Από αυτά το Snort εντόπισε και έστειλε alerts για 6744. Στη συνέχεια έγινε η επίθεση DoS **neptune** για την οποία το Snort δεν έστειλε κανένα alert καθώς δεν την εντόπισε. Επόμενο στη σειρά πραγματοποιήθηκε το σενάριο **rootkit** το οποίο αποτελεί ένα πολυήμερο σενάριο σύμφωνα με το οποίο οι επιτιθέμενοι εγκαθιστούν ένα η περισσότερα μέρη ενός rootkit. Το **rootkit** είναι ένα λογισμικό που επιτρέπει την συνεχή πρόσβαση σε έναν υπολογιστή με προνόμια υπερχρήστη, ενώ κρύβει ενεργά την παρουσία του από τους διαχειριστές με το να ενσωματώνεται σε βασικά αρχεία του λειτουργικού συστήματος ή άλλων εφαρμογών. Για την επίθεση αυτή στάλθηκαν συνολικά 6 πακέτα επίθεσης τα οποία το Snort εντόπισε όλα και έστειλε alerts. Στη συνέχεια ακολούθησε ακόμα ένα πολυήμερο σενάριο, το **spy** σύμφωνα με το οποίο οι επιτιθέμενοι διεισδύουν σε ένα μηχάνημα με σκοπό να ανακαλύψουν σημαντικές πληροφορίες. Η επίθεση αυτή έγινε με 2 πακέτα τα οποία το Snort εντόπισε. Αμέσως μετά έγινε μια **ping of death** επίθεση με 670 πακέτα να έχουν σταλεί από τα οποία ωστόσο το Snort εντόπισε και έστειλε alerts μόνο για 4. Τελευταία έγινε η επίθεση **teardrop** για την οποία το Snort έστειλε 100 alerts απο τα 200 πακέτα επίθεσης που είναι καταγεγραμμένα.

- Τετάρτη: Η τρίτη μέρα της εβδομάδας κύλισε πιο ομαλά με μόνο 3 επιθέσεις να πραγματοποιούνται κατα τη διάρκεια της μέρας. Οι επιθέσεις αυτές ήταν οι **ping of death** που είναι Denial of Service επίθεση και οι **ipsweep** και **portsweep** που είναι probe επιθέσεις. Για την πρώτη επίθεση στάλθηκαν 900 πακέτα για τα οποία το Snort εντόπισε και έστειλε alerts για τα 4 μόνο. Για την ipsweep επίθεση στάλθηκαν 510 πακέτα για τα οποία το Snort παρήγαγε περίπου τα τριπλάσια alerts καθώς έστελνε μεγάλο αριθμό alert για κάθε πακέτο της ipsweep που έβρισκε. Τέλος, για την portweep επίθεση στάλθηκαν 300 πακέτα επίθεσης από τα οποία το Snort εντόπισε και έστειλε 98 alerts.

- Πέμπτη: Την Πέμπτη παρατηρούνται 3 στο σύνολο επιθέσεις να πραγματοποιούνται μέσα στη μέρα. Αυτές, με τη σειρά ήταν μια **warezclient** επίθεση, μια Denial of Service και μια probe επίθεση. Η **warezclient** επίθεση πραγματοποιήθηκε με την αποστολή 327 πακέτων από τα οποία το Snort κατάφερε να εντοπίσει και να στείλει alerts για τα 295. Αμέσως επόμενη έγινε η **syslogd** επίθεση με την αποστολή ενός και μόνο πακέτου το οποίο το Snort απέτυχε να εντοπίσει. Τελευταία πραγματοποιήθηκε μια **portsweep** επίθεση με την αποστολή 2010 πακέτων εκ των οποίων για τα 493 δημιουργήθηκαν alerts από το Snort.
- Παρασκευή: Την τελευταία μέρα της εβδομάδας διακρίνονται 7 συνολικά επιθέσεις οι οποίες ανήκουν τόσο σε σενάρια επιθέσεων, User to Root αλλά και probe επιθέσεις. Πρώτη επίθεση της ημέρας ήταν μια **warezclient** επίθεση η οποία πραγματοποιήθηκε με τη χρήση 72 πακέτων επίθεσης από τα οποία το Snort διέκρινε και έστειλε alerts για τα 48 από αυτά. Αμέσως μετά ακολούθησε ένα σενάριο επίθεσης **rootkit** για το οποίο στάλθηκε 1 και μόνο πακέτο το οποίο και εντόπισε και έστειλε alert το Snort. Στη συνέχεια ακολούθησαν 2 User to Root επιθέσεις, μια **ffbconfig** και μια **fdformat** επίθεση όπου και οι δύο πραγματοποιήθηκαν με την αποστολή ενός και μόνο πακέτου επίθεσης το οποίο και στις 2 περιπτώσεις το Snort εντόπισε και έστειλε τα αντίστοιχα alerts. Ακολούθησε ένα **multihop** σενάριο με την αποστολή 1 πακέτου το οποίο επίσης το Snort κατάφερε να εντοπίσει. Αργότερα στη μέρα πραγματοποιήθηκε μια **loadmodule** επίθεση με 6 πακέτα επίθεσης από τα οποία το Snort διέκρινε μόνο τα 2. Τελευταία, πραγματοποιήθηκε μια **ipsweep** επίθεση με 513 πακέτα να στάλθηκαν από τους επιτιθέμενους και 1664 alerts να παράχθηκαν από το Snort για την συγκεκριμένη επίθεση.

4.5. 5η Εβδομάδα

Κατά τη διάρκεια της πέμπτης εβδομάδας παρατηρούνται επιθέσεις από τις κατηγορίες Denial of Service, User to Root και probe. Όσον αφορά τις μέρες της εβδομάδας ξεχωριστά, μερικές δέχονται λιγότερες και μερικές αρκετά περισσότερες επιθέσεις κατά τη διάρκεια τις ημέρες με αριθμό να πηγαίνει από 3 έως και 7 διαφορετικές επιθέσεις τη μερα. Οι επιθέσεις που γίνονται αποτελούν έναν συνδυασμό των teardrop, smurf, pod, syslogd, neptune, land, ffbconfig, fdformat, eject, perlmagic, loadmodule, satan, ipsweep και portsweep επιθέσεων και συχνά, πολλές από αυτές επαναλαμβάνονται παραπάνω από μια φορά σε διαφορετικά χρονικά διαστήματα μέσα στη μέρα. Αναλυτικότερα:

- Δευτέρα: Την πρώτη μέρα της εβδομάδας διακρίνονται 3 στο σύνολο επιθέσεις οι οποίες με τη σειρά αποτελούν μια Denial of Service, μια probe και άλλη μια Denial of Service επίθεση. Πρώτη αντίστοιχα πραγματοποιήθηκε η **teardrop** επίθεση με 200 πακέτα επίθεσης για τα οποία το Snort έστειλε 100 alerts. Αμέσως επόμενη έγινε μια probe επίθεση που συγκεκριμένη περίπτωση ήταν η **satan** με 5203 πακέτα επίθεσης από τα οποία το Snort αναγνώρισε τα 2890 και έστειλε τα ανάλογα alerts. Τελευταία έγινε η **smurf** επίθεση η οποία πραγματοποιήθηκε με την αποστολή 7550 πακέτων από τα οποία το Snort δεν εντόπισε κάποιο.
- Τρίτη: Στην δεύτερη μέρα της εβδομάδας παρατηρούνται 5 συνολικά επιθέσεις που αντιστοιχούν σε probe, User to Root, probe, User to Root και μια Denial of Service κατηγορία αντίστοιχα. Πρώτη επίθεση της ημέρας ήταν η **ipsweep** η οποία έγινε με την αποστολή 778 πακέτων για τα οποία το Snort έστειλε πάνω από 778 alerts. Ακολούθησε η **eject** επίθεση για την οποία έγινε η αποστολή 2 πακέτων τα οποία και τα 2 εντοπίστηκαν από το Snort. Στη συνέχεια, η επίθεση που δέχτηκαν ήταν η **portsweep** με την αποστολή 1027 πακέτων από τα οποία το Snort εντόπισε μόνο τα 11 και έστειλε τα προβλεπόμενα alerts. Επόμενη επίθεση της ημέρας ήταν μια επίθεση **perlmagic**, η οποία ουσιαστικά ορίζει το αναγνωριστικό χρήστη σε root σε ένα perl script και δημιουργεί ένα κέλυφος root. Αυτή η επίθεση έγινε με 1 μοναδικό πακέτο το οποίο το Snort εντόπισε και έστειλε alert. Τέλος, πραγματοποιήθηκε μια **ping of death** επίθεση με 901 πακέτα από τα οποία

εντοπίστηκαν μόνο τα 4 απο το Snort και μόνο για 2 από όλες τις IP παρόλο που η επίθεση έγινε προς όλα τα μηχανήματα των θυμάτων.

- Τετάρτη: Την Τετάρτη έγιναν μόνο 4 επιθέσεις κατα τη διάρκεια της ημέρας που οι δύο πρώτες ήταν Denial of Service επιθέσεις, η τρίτη μια User to Root επίθεση ενώ η τέταρτη και τελευταία μια probe επίθεση. Πρώτη έγινε η **syslogd** επίθεση η οποία πραγματοποιήθηκε με την αποστολή 1 πακέτου το οποίο δεν εντοπίστηκε από το Snort. Στη συνέχεια ακολούθησε η **teardrop** επίθεση με 200 πακέτα επίθεσης για τα οποία δημιουργήθηκαν 100 alerts. Αρκετές ώρες μετά πραγματοποιήθηκε μια **eject** επίθεση με την αποστολή ενός πακέτου επίθεσης για το οποίο και δημιουργήθηκε το ανάλογο alert απο το Snort αφού εντοπίστηκε. Τελευταία έγινε μια **ipsweep** επίθεση με την αποστολή 1787 πακέτων από τους επιτιθέμενους για τα οποία το Snort δημιούργησε 5405 alerts καθώς έστελνε πολλαπλά alerts για κάθε ping που της ipsweep που έβρισκε.
- Πέμπτη: Την τέταρτη μέρα της εβδομάδας παρατηρήθηκαν 7 επιθέσεις στο σύνολο παρόλα αυτά βρέθηκαν να επαναλαμβάνονται πολλές φορές κατα τη διάρκεια της μέρας σε διαφορετικά χρονικά διαστήματα. Πρώτα θα αναλύσουμε την DoS επίθεση **ping of death** όπου επαναλήφθηκε αρκετές φορές μέσα στην ημέρα με συνολικά πακέτα επίθεσης 2219 τα οποία το Snort δεν εντόπισε σε καμια περίπτωση. Το ίδιο ισχύει για την επίσης DoS επίθεση που ακολούθησε η οποία ήταν η **smurf** για την οποία οι επιτιθέμενοι έστειλαν 7550 πακέτα στο σύνολο. Επόμενη στη σειρά είναι η DoS **teardrop** επίθεση για την οποία στάλθηκαν 772 πακέτα επίθεσης και το Snort δημιούργησε 386 alerts δηλαδή τα μισά όπως ακριβώς κάθε φορά με την συγκεκριμένη επίθεση. Στη συνέχεια ακολούθησε η DoS **neptune** επίθεση η οποία έγινε σε 2 διαφορετικά χρονικά σημεία με συνολικό αριθμό πακέτων 205457 για τα οποία το Snort δημιούργησε 610 alerts για την πρώτη επίθεση και 1 για την δεύτερη. Αμέσως επόμενη στη λίστα ήταν η DoS **land** επίθεση η οποία πραγματοποιήθηκε με την αποστολή 1 πακέτου για το οποίο και δημιουργήθηκε το αντίστοιχο alert απο το Snort. Τελος, έγινε και μια **portsweep** επίθεση με 1179 πακέτα για τα οποία δημιουργήθηκαν 13 alerts.

- Παρασκευή: Την τελευταία μέρα της εβδομάδας παρατηρούνται 7 στο σύνολο επιθέσεις εκ των οποίων οι 2 πρώτες που θα αναλύσουμε είναι User to Root επιθέσεις, μετά μια probe επίθεση, στη συνέχεια 2 Denial of Service επιθέσεις και τέλος μια rootkit επίθεση οι οποίες επαναλήφθηκαν μέσα στη μέρα. Η πρώτη επίθεση που αναφερόμαστε είναι η **format** επίθεση για την οποία υπήρξαν 6 πακέτα επίθεσης, από τα οποία το Snort εντόπισε και δημιούργησε alert για το 1. Επόμενη βλέπουμε την **loadmodule** επίθεση που έγινε με 1 πακέτο επίθεσης το οποίο και δεν αναγνωρίστηκε από το Snort. Στη συνέχεια έχουμε μια **portsweep** επίθεση για την οποία το Snort εντόπισε όλα τα 120 πακέτα επίθεσης και έστειλε τα κατάλληλα alerts. Μετά βλέπουμε μια **eject** επίθεση η οποία έγινε με 1 μόνο πακέτο το οποίο και εντοπίστηκε από το Snort. Επόμενη επίθεση είναι η **neptune** για την οποία στάλθηκαν 243635 πακέτα επίθεσης από τα οποία το Snort κατάφερε να εντοπίσει τα 750 και να στείλει alerts. Μετά έγινε μια **smurf** επίθεση η οποία πέρασε απαρατήρητη από το Snort παρά τα 1044 πακέτα επίθεσης της. Τέλος, έγινε ένα σενάριο **rootkit** που πραγματοποιήθηκε με την αποστολή 6 συνολικά πακέτων από τα οποία το Snort δεν εντόπισε κανένα.

4.6. 6η Εβδομάδα

Κατά τη διάρκεια της έκτης εβδομάδας παρατηρούνται επιθέσεις όλων των κατηγοριών που έχουμε συναντήσει δηλαδή Denial of Service, User to Root, Remote to Local αλλά και probe επιθέσεις. Πιο συγκεκριμένα, από τη μια μέρα στην άλλη διακρίνεται ένας συνδυασμός των neptune, ping of death, land, back, smurf, teardrop, eject, ffbconfig, perlmagic, phf, dict, satan, portsweep και ipsweep επιθέσεων. Όλες οι ημέρες με εξαίρεση την Πέμπτη επιβαρύνονται με 3 διαφορετικές επιθέσεις. Την Πέμπτη ωστόσο φαίνεται να πραγματοποιούνται επιθέσεις όλη την μέρα σχεδόν με τον αριθμό των διαφορετικών επιθέσεων να φτάνει τις 13 οι οποίες επαναλαμβάνονται συχνά έως και 6 φορές ανα χρονικά διαστήματα μέσα στη μέρα. Αναλυτικότερα:

- Δευτέρα: Την πρώτη μέρα της εβδομάδας παρατηρούνται 3 συνολικά επιθέσεις οι οποίες αντιστοιχούν με τη σειρά σε μια Remote to Local, μια probe και μια Denial of Service επίθεση. Πρώτη επίθεση της ημέρας φαίνεται να είναι η **phf** για την οποία χρησιμοποιήθηκε 1 μοναδικό πακέτο επίθεσης το οποίο το Snort εντόπισε και δημιούργησε το αντίστοιχο alert. Λίγες ώρες μετά ακολούθησε η επίθεση **satan** με 4 πακέτα επίθεσης τα οποία επίσης το Snort εντόπισε όλα. Τελευταία πραγματοποιήθηκε η DoS επίθεση **neptune** στην οποία αντιστοιχούσαν 800 πακέτα επίθεσης από τα οποία το Snort δεν κατάφερε να διακρίνει κανένα.
- Τρίτη: Την δεύτερη μέρα της εβδομάδας διακρίνονται επίσης 3 επιθέσεις στο σύνολο οι οποίες αποτελούνται από μια probe, και δύο Denial of Service επιθέσεις. Νωρίς το πρωί και πρώτη από όλες έγινε η επίθεση **portsweep** κατά τη διάρκεια της οποίας στάλθηκαν 1804 πακέτα που αντιστοιχούσαν στην επίθεση από τα οποία το Snort διέκρινε και έστειλε alerts για 3 από αυτά. Μερικές ώρες αργότερα ακολούθησε η επίθεση **ping of death** με 450 πακέτα επίθεσης για τα οποία το Snort έστειλε 4 συνολικά alerts. Τέλος, το απόγευμα, πραγματοποιήθηκε η τελευταία επίθεση της ημέρας που ήταν η **land** με 1 πακέτο επίθεσης το οποίο εντοπίστηκε από το Snort και το ανάλογο alert δημιουργήθηκε.
- Τετάρτη: Την Τετάρτη εξίσου διακρίνονται 3 επιθέσεις κατά τη διάρκεια της ημέρας όπου αντιστοιχούν σε μια probe και δύο Denial of Service επιθέσεις. Πρώτη φαίνεται να έγινε η **ipsweep** επίθεση με την αποστολή 510 πακέτων για να επιτευχθεί, για τα οποία το Snort έστειλε παραπάνω από δύο alerts για κάθε ένα από τα πακέτα. Στη συνέχεια πραγματοποιήθηκε η **neptune** επίθεση με 204571 πακέτα επίθεσης προς όλα τα ports για τα οποία παράχθηκαν 633 alerts από το Snort. Τελευταία έγινε η **back** επίθεση με την αποστολή 100 πακέτων όπου το Snort έστειλε 1200 alerts καθώς έστελνε πολλαπλό αριθμό alerts για κάθε πακέτο που διέκρινε.
- Πέμπτη: Την Πέμπτη διακρίνεται ένας ασυνήθιστος αριθμός επιθέσεων για μια μόνο μέρα που ανέρχεται στις 13 επιθέσεις. Οι επιθέσεις που

πραγματοποιήθηκαν κατά τη διάρκεια της Πέμπτης ανήκαν τόσο σε Denial of Service, User to Root, Remote to Local αλλά και probe επιθέσεις οι οποίες επαναλαμβάνονται μέσα στη μέρα πολλές φορές. Πρώτα θα αναλύσουμε μια probe επίθεση την **ipsweep**. Η ipsweep επαναλήφθηκε 5 φορές συνολικά μέσα στη μέρα με συνολικό αριθμό πακέτων επίθεσης τις 4653 και το Snort κατάφερε να στείλει alerts για κάθε φορά που έγινε η επίθεση ωστόσο ο αριθμός των alerts που δημιουργήθηκαν ξεπερνά κατά πολύ τα πακέτα επίθεσης. Επόμενη στη σειρά είναι η User to Root επίθεση **eject** η οποία πραγματοποιήθηκε 6 διαφορετικές φορές μέσα στη μέρα. Συνολικά 7 πακέτα επίθεσης στάλθηκαν δηλαδή από 1 κάθε φορά με εξαίρεση μια από τις 6 επιθέσεις που στάλθηκαν 2 πακέτα επίθεσης και το Snort εντόπισε με επιτυχία και τα 7 πακέτα και έστειλε alerts για κάθε περίπτωση ξεχωριστά. Μετά διακρίνεται μια User to Root επίθεση η **ffbconfig** η οποία έγινε 2 φορές μέσα στη μέρα με τη χρήση 1 πακέτου τη φορά τα οποία και στις 2 περιπτώσεις εντοπίστηκαν από το Snort. Ακολουθεί μια Denial of Service επίθεση **ping of death** η οποία επαναλήφθηκε 5 διαφορετικές χρονικές στιγμές της ημέρας. Με συνολικό αριθμό πακέτων τα 4010, το Snort έστειλε alerts μόνο για την δεύτερη, την τέταρτη και την πέμπτη φορά που έγινε η επίθεση και σε όλες τις περιπτώσεις από 2 μόνο alerts. Στη συνέχεια ακολουθεί μια Remote to Local επίθεση η **dict** κατά την διάρκεια της οποίας στάλθηκαν 881 πακέτα επίθεσης που αντιστοιχούσαν σε προσπάθειες να μαντέψουν τους κωδικούς ενός χρήστη. Το Snort εντόπισε την επίθεση και έστειλε πολλαπλά alerts για κάθε πακέτο που διέκρινε με τον αριθμό να φτάνει τα 2604. Στη συνέχεια βλέπουμε μια ακόμα Remote to Local επίθεση την **phf** η οποία πραγματοποιήθηκε μια μόνο φορά και με 1 πακέτο επίθεσης για το οποίο και παράχθηκε το ανάλογο alert από το Snort. Επόμενη στη λίστα έχουμε μια Denial of Service **neptune** επίθεση η οποία πραγματοποιήθηκε 2 φορές μέσα στη μέρα με συνολικό αριθμό πακέτων που στάλθηκαν να είναι τα 460765 πακέτα. Το Snort εντόπισε και τις 2 φορές την επίθεση ωστόσο έστειλε για 760 πακέτα, alerts την πρώτη φορά και για 613 τη δεύτερη. Ακολουθεί μια probe επίθεση η **portsweep** η οποία έγινε 3 φορές με συνολικό αριθμό πακέτων επίθεσης τα 1447 και το Snort να εντοπίζει 118 τη πρώτη φορά, 34 τη δεύτερη και 11 τη τρίτη. Στη συνέχεια έχουμε μια Denial of Service επίθεση την **smurf** η οποία έγινε μια φορά με 7547 πακέτα επίθεσης για τα οποία δημιουργήθηκαν 933

alerts. Επόμενη είναι ακόμα μια Denial of Service επίθεση η **land** η οποία έγινε μια φορά αλλά απο και προς όλους τους χρήστες με 16 πακέτα επίθεσης συνολικά από τα οποία τα 3 εντοπίστηκαν απο το Snort. Ακόμα μια Denial of Service επίθεση έγινε η οποία ήταν η **teardrop** με 400 πακέτα επίθεσης στο σύνολο, 200 για κάθε μια απο τις δυο φορές που έγινε η επίθεση. Για αυτά το Snort έστειλε 100 alerts σε κάθε μια από τις δύο περιπτώσεις που εντόπισε την επίθεση. Προτελευταία βλέπουμε μια probe επίθεση **satan** με 10922 πακέτα επίθεσης στο σύνολο, η οποία πραγματοποιήθηκε 2 φορές μέσα στη μέρα. Την πρώτη φορά το Snort έστειλε 890 alerts ενώ τη δεύτερη 12. Τέλος, διακρίνεται μια User to Root επίθεση **perlmagic** η οποία έγινε μια φορά με 2 πακέτα επίθεσης τα οποία και τα 2 εντοπίστηκαν απο το Snort.

- Παρασκευή: Την Παρασκευή παρατηρούνται 3 συνολικά επιθέσεις οι οποίες και οι τρεις ανήκουν στη κατηγορία Denial of Service. Πρώτη εμφανίζεται η teardrop επίθεση με 200 πακέτα επίθεσης απο τα οποία τα 100 εντοπίζονται απο το Snort το οποίο στέλνει τα αντίστοιχα alerts. Στη συνέχεια πραγματοποιείται μια neptune επίθεση με αποστολή 200 πακέτων συνολικά τα οποία δεν εντοπίζονται καθόλου από το Snort. Τελευταία επίθεση είναι η smurf η οποία παρά το γεγονός ότι πραγματοποιήθηκε με την αποστολή 36385 πακέτων το Snort επίσης δεν κατάφερε να εντοπίσει και να δημιουργήσει alerts για κανένα από αυτά τα πακέτα.

4.7. 7η Εβδομάδα

Κατά τη διάρκεια της έβδομης και τελευταίας εβδομάδας επικρατούν επιθέσεις τόσο της κατηγορίας Denial of Service αλλά και User to Root, Remote to Local και probe. Καθημερινά ο αριθμός ξεχωριστών επιθέσεων δεν είναι μεγάλος και ανέρχεται απο 2 εως 5 επιθέσεις ανάλογα την ημέρα. Οι επιθέσεις που βλέπουμε την τελευταία εβδομάδα είναι ένας συνδυασμός των syslogd, land, pod, teardrop, smurf, neptune, back, loadmodule, perlmagic, phf, satan, portsweep και ipsweep οι οποίες σε μερικές περιπτώσεις επαναλαμβάνονται πάνω από μια φορά μέσα στη μέρα. Αναλυτικότερα:

- Δευτέρα: Κατά τη διάρκεια της πρώτης μέρας διακρίνονται 4 ξεχωριστές μεταξύ τους επιθέσεις οι οποίες με τη σειρά ανήκουν στις κατηγορίες Probe, Denial of Service, Remote to Local και άλλη μια Denial of Service. Πρώτη στη μέρα πραγματοποιήθηκε η επίθεση **satan** η οποία έγινε με την αποστολή 8 πακέτων. Το Snort εντόπισε τα πακέτα αυτά και έστειλε 20 συνολικά alerts καθώς έστειλε για μερικά πακέτα πολλαπλά alerts. Στη συνέχεια ακολούθησε η **syslogd** επίθεση η οποία έγινε με την αποστολή 1 πακέτου το οποίο πέρασε απαρατήρητο από το Snort. Αμέσως επόμενη βλέπουμε την **phf** επίθεση για την οποία στάλθηκε 1 πακέτο το οποίο διέκρινε το Snort και έστειλε το αντίστοιχο alert. Τελευταία έγινε η **land** επίθεση από και προς διάφορους χρήστες με 8 ξεχωριστά πακέτα τα οποία όλα εντοπίστηκαν από το Snort και τα ανάλογα alerts δημιουργήθηκαν.
- Τρίτη: Κατά τη διάρκεια της Τρίτης πραγματοποιήθηκαν 4 συνολικά επιθέσεις εκ των οποίων οι κατηγορίες ήταν αντίστοιχα μια probe, μια Denial of Service, μια Remote to Local και μια User to Root επίθεση. Πρώτη εμφανίζεται η **portsweep** επίθεση η οποία έγινε με την αποστολή 1469 πακέτων από τα οποία το Snort διέκρινε και έστειλε alerts για 3 από αυτά. Στη συνέχεια πραγματοποιήθηκε μια **ping of death** επίθεση με την αποστολή 450 πακέτων επίθεσης τα οποία το Snort δεν ξεχώρισε. Οι τελευταίες 2 επιθέσεις που διακρίνονται είναι μια **phf** και μια **loadmodule** επίθεση η οποίες ωστόσο δεν μπόρεσαν να ελεγχθούν καθώς δεν υπάρχουν καταγεγραμμένα πόσα πακέτα επίθεσης υπήρχαν στο αρχείο για την κάθε μια επίθεση.
- Τετάρτη: Την Τετάρτη διακρίνονται 5 επιθέσεις στο σύνολο οι οποίες αντιστοιχούν στις Remote to Local, User to Root, Denial of Service και probe κατηγορίες αντίστοιχα. Πρώτη διακρίνεται η **phf** επίθεση με την αποστολή 1 μοναδικού πακέτου το οποίο και εντοπίστηκε επιτυχώς από το Snort. Στη συνέχεια σειρά έχει μια **loadmodule** επίθεση η οποία επίσης έγινε με την αποστολή ενός και μόνο πακέτου και σε αυτή τη περίπτωση όπως και πριν το Snort το εντόπισε και έστειλε το κατάλληλο alert. Ακολούθησε μια **teardrop** επίθεση η οποία πραγματοποιήθηκε με την αποστολή 200 πακέτων από τα

οποία το Snort αναγνώρισε τα 100 και έστειλε τα σωστά alerts. Τέλος διακρίνονται οι 2 probe επιθέσεις με πρώτη την **ipsweep** με 511 πακέτα επίθεσης τα οποία εντόπισε το Snort και έστειλε περίπου τα τριπλάσια σε αριθμό alerts καθώς στέλνει πολλαπλά alerts για κάθε πακέτο ping. Δεύτερη και τελευταία έγινε η **portsweep** επίθεση για την οποία στάλθηκαν 908 πακέτα από τα οποία το Snort ξεχώρισε τα 3.

- Πέμπτη: Την τέταρτη ημέρα της εβδομάδας πραγματοποιήθηκαν 4 επιθέσεις συνολικά οι οποίες ήταν μια Denial of Service, μια probe, μια User to Root και τέλος ακόμα μια probe, επιθέσεις. Πρώτη επίθεση εντοπίστηκε να είναι η **smurf** με 134 πακέτα να έχουν σταλεί για την συγκεκριμένη επίθεση τα οποία το Snort απέτυχε να εντοπίσει. Ακολουθεί μια **satan** επίθεση για την οποία στάλθηκαν 6968 πακέτα επίθεσης και από αυτά εντοπίστηκαν και δημιουργήθηκαν alerts για τα 3284 απο αυτά. Στη συνέχεια πραγματοποιήθηκε μια **perlmagic** επίθεση με 1 πακέτο το οποίο το Snort εντόπισε. Τέλος, έγινε μια probe επίθεση **ipsweep** η οποία έστειλε 512 πακέτα από τα οποία το Snort εντόπισε τα 405 και δημιούργησε τα αντίστοιχα alerts.
- Παρασκευή: Την τελευταία ημέρα της εβδομάδας παρατηρούνται 3 διαφορετικές μεταξύ τους επιθέσεις οι οποίες όλες τους ανήκουν στην κατηγορία Denial of Service. Πρώτη έγινε η **neptune** επίθεση η οποία επαναλήφθηκε μέσα στη μέρα άλλη μια φορά. Με συνολικά απεσταλμένα πακέτα τα 205600 το Snort κατάφερε να εντοπίσει και να στείλει alerts, την πρώτη φορά 610 και τη δεύτερη κανένα. Επόμενη επίθεση ήταν η **smurf** η οποία πραγματοποιήθηκε με την αποστολή 1044 πακέτων από τα οποία το Snort εντόπισε τα 14 από αυτά. Τελευταία επίθεση είναι η **back** επίθεση η οποία πραγματοποιήθηκε με την αποστολή 181 πακέτων τα οποία το Snort εντόπισε και έστειλε περίπου τα δεκαπλάσια σε αριθμό alerts καθώς τα alerts από την συγκεκριμένη επίθεση φτάνουν τα 1182.

	A	B	C	D
1	Denial of Service	Attack Packets	Snort Alerts	Packets/Alerts %
2	back	12281	12281	100,00%
3	land	35	15	42,00%
4	neptune	1526643	4587	0,30%
5	ping of death	10050	22	0,20%
6	smurf	61778	947	1,50%
7	syslogd	4	0	0,00%
8	teardrop	2173	1086	49,90%
9				
10	Remote to Local			
11	dict	882	882	100,00%
12	guest	50	50	100,00%
13	ftp-write	8	5	62,50%
14	phf	5	5	100,00%
15	imap	7	3	42,80%
16				
17	User to Root			
18	eject	11	11	100,00%
19	ffbconfig	5	5	100,00%
20	fdformat	8	3	37,50%
21	loadmodule	9	3	33,30%
22	perl	5	5	100,00%
23				
24	Probe scan			
25	ipsweep	15823	15823	100,00%
26	portsweep	9590	896	9,30%
27	nmap	2357	2186	92,70%
28	satan	32625	13867	42,50%
29				
30	Scenarios			
31	multihop	9	4	44,40%
32	warez	1	1	100,00%
33	warezmaster	19	4	21,00%
34	warezclient	937	881	94,00%

Αναλυτικός πίνακας συνολικών αποτελεσμάτων για κάθε επίθεση.

5. ΣΥΜΠΕΡΑΣΜΑΤΑ

Σε αυτό το κεφάλαιο παρουσιάζονται συμπεράσματα σχετικά με την αξιολόγηση του Snort στο DARPA 1998 dataset και αναφέρονται σχόλια για την διαδικασία καθώς και την αποδοτικότητα του Snort στις διάφορου τύπου επιθέσεις που συνάντησε.

Η πλειονότητα των κακόβουλων συνδέσεων στο σύνολο δεδομένων της DARPA 1998 προέρχεται από Denial of Service αλλά και probe επιθέσεις. Παρόλο που το Snort έχει την ικανότητα να ανιχνεύει τέτοιες επιθέσεις, οι συγκεκριμένου είδους ανιχνεύσεις δεν ήταν το κύριο επίκεντρο του σχεδιασμού του. Αυτό φαίνεται έντονα από το γεγονός ότι εμφανίζονται 7 συνολικά διαφορετικές επιθέσεις Denial of Service οι οποίες επαναλαμβάνονται πολύ συχνά κατά την διάρκεια των 7 εβδομάδων, συχνά και πολλές φορές στην ίδια μέρα και το Snort έχει στις 6 απο τις 7 ποσοστό επιτυχίας μικρότερο του 50%. Είναι ενδιαφέρον ότι πολλά από τα προηγμένα συστήματα ID που αξιολογήθηκαν είτε ως μέρος της αξιολόγησης DARPA είτε που αυτοαξιολογήθηκαν χρησιμοποιώντας αυτά τα δεδομένα, τα πήγαν πολύ καλά στις επιθέσεις DoS και probe, ενώ πολλά είχαν πρόβλημα με τις Remote to Local και User to Root επιθέσεις, όπου το Snort αποδίδει καλύτερα. Παρόλο που η προφανής λύση θα ήταν να γίνει αλλαγή του Snort και των κανόνων για μια καλύτερη, ποσοστιαία, απόδοση στις επιθέσεις Denial of Service και probe, μια καλύτερη και πιο αξιόπιστη λύση θα ήταν η συνδυαστική χρήση του Snort αλλά και ενός ακόμα NIDS για τις συγκεκριμένες κατηγορίες επιθέσεων και μόνο. Το Snort αντιμετώπισε σε αρκετά ικανοποιητικό βαθμό την δοκιμασία καθώς σχεδόν σε κάθε περίπτωση σε αρκετά μεγάλο ποσοστό φαίνεται να διέκρινε τις επιθέσεις και να έστειλε alerts που αντιστοιχούσαν σε αυτές. Ωστόσο, μεγάλος είναι και ο αριθμός των false positives που βλέπουμε ημερησίως καθώς το Snort παρήγαγε σε μεγάλο αριθμό πολύ περισσότερα alerts από αυτά που αντιστοιχούσαν στις επιθέσεις. Αυτό οφείλεται κυρίως στο γεγονός ότι η πλειονότητα των επιθέσεων αποτελούν Denial of Service ή probe επιθέσεις οι οποίες στέλνουν πολλά πακέτα για τα οποία το Snort δημιουργούσε πολλαπλά alerts. Παρόλα αυτά συχνά υπάρχουν περιπτώσεις που η προσομοίωση της δραστηριότητας στο DARPA dataset δούλεψε εναντίον του Snort. Για παράδειγμα φαίνεται πως για την προσομοίωση του προγράμματος αν όχι όλες, οι περισσότερες εικόνες που μεταφέρονταν ως μέρος της HTTP δραστηριότητας ήταν

0x0 μέγεθος πράγμα για το οποίο το Snort δημιουργούσε συνεχώς alerts καθώς τέτοιες εικόνες συχνά χρησιμοποιούνται ως μέσο για κακόβουλους σκοπούς. Παρόλα αυτά, κάτι τέτοιο είναι αμφιλεγόμενο αν μπορεί να θεωρηθεί αρνητικό καθώς σε ένα πραγματικό περιβάλλον χρήσης του Snort ένα τέτοιο alert θα ήταν σίγουρα απαραίτητο. Τέλος, παρόλο που το Darpa dataset αποτελεί ένα αξιόλογο dataset το οποίο χρησιμοποιούν πολλά IDS για την αξιολόγηση τους, ένα πιο ρεαλιστικό σύνολο δεδομένων είναι απαραίτητο. Το συγκεκριμένο dataset είναι πολλών ετών πίσω και υπάρχουν πολλές νέες απειλές που εμφανίστηκαν τα τελευταία χρόνια από την τελευταία αξιολόγηση (botnet, spyware, flash worms, κ.λπ.), τις οποίες ένα σύγχρονο IDS πρέπει να μπορεί να ανιχνεύσει και οι οποίες θα πρέπει να ελεγχθούν ενάντια στα IDS σε ένα τέτοιο σύνολο δεδομένων. Επιπλέον, ένα καλύτερο σύνολο δεδομένων θα πρέπει να περιλαμβάνει έναν ρεαλιστικό αριθμό επιθέσεων που θα μπορούσαν να ανιχνευθούν εύκολα από ένα NIDS που βασίζεται στην υπογραφή (signature-based) όπως το Snort.

Στην παρούσα πτυχιακή γίνεται εμφανής η αξία των Intrusion Detection Systems και πιο συγκεκριμένα η αξία και αποδοτικότητα του Snort. Αρχικά, περιγράφονται αναλυτικά οι κατηγορίες των επιθέσεων αλλά και μια προς μια οι επιθέσεις με τις οποίες ήρθε αντιμέτωπο το πρόγραμμα. Στη συνέχεια παρουσιάζεται ο τρόπος με τον οποίο ρυθμίστηκε αλλά και λειτούργησε το πρόγραμμα περιγράφοντας κάθε μια από τις παραμέτρους. Τέλος, παρουσιάστηκαν με άφθονες λεπτομέρειες τα αποτελέσματα που προέκυψαν από τα πειράματα με ανάλυση της κάθε ημέρας των 7 εβδομάδων.

BIBΛΙΟΓΡΑΦΙΑ

01. Richard P. Lippmann, David J. Fried, Isaac Graf, Joshua W. Haines, Kristopher R. Kendall, David McClung, Dan Weber, Seth E. Webster, Dan Wyschogrod, Robert K. Cunningham, and Marc A. Zissman. Evaluating Intrusion Detection Systems: The 1998 DARPA Off-line Intrusion Detection Evaluation. IEEE 2000
02. Wei-Chao Lin, Shih-Wen Ke, Chih-Fong Tsai. CANN: An intrusion detection system based on combining cluster centers and nearest neighbors. Article 2014
03. S Chakrabarti, M Chakraborty, I Mukhopadhyay. Study of Snort-Based IDS. *Computer-Communication Networks*. ICWET 2010
04. Martin Roesch. Snort – Lightweight Intrusion Detection for Networks. USENIX 1999
05. Muhammad Naveed , Shams un Nihar , Mohammad Inayatullah Babar. Network intrusion prevention by configuring ACLs on the routers, based on snort IDS alerts. IEEE 2010
06. J. Gómez, C. Gil, N. Padilla, R. Baños & C. Jiménez. Design of a Snort-Based Hybrid Intrusion Detection System. IWANN 2009
07. Nattawat Khamphakdee, Nunnapus Benjamas, Saiyan Saiyod. Improving Intrusion Detection System Based on Snort Rules for Network Probe Attacks Detection with Association Rules Technique of Data Mining. ITB 2015
08. G.C. Tjhai, M. Papadaki, S.M. Furnell, N.L. Clarke. Investigating the problem of IDS false alarms: An experimental study using Snort. IFIP 2008
09. Gina C. Tjhai, Maria Papadaki, Steven M. Furnell , Nathan L. Clarke. The Problem of False Alarms: Evaluation with Snort and DARPA 1999 Dataset. TrusBus 2008
10. S Terry Brugger, Jedadiah Chow. An Assessment of the DARPA IDS Evaluation Dataset Using Snort. 2005
11. Hung-Jen Liao, Chun-Hung Richard Lin, Ying-Chih Lin, Kuang-Yuan Tung. Intrusion detection system: A comprehensive review. *Journal of Network and Computer Applications* 2013
12. Usha Banerjee, Ashutosh Vashishtha, Mukul Saxena. Evaluation of the Capabilities of WireShark as a tool for Intrusion Detection. Paper 2010