Πανεπιστήμιο Πελοποννήσου

Πτυχιακή Εργασία

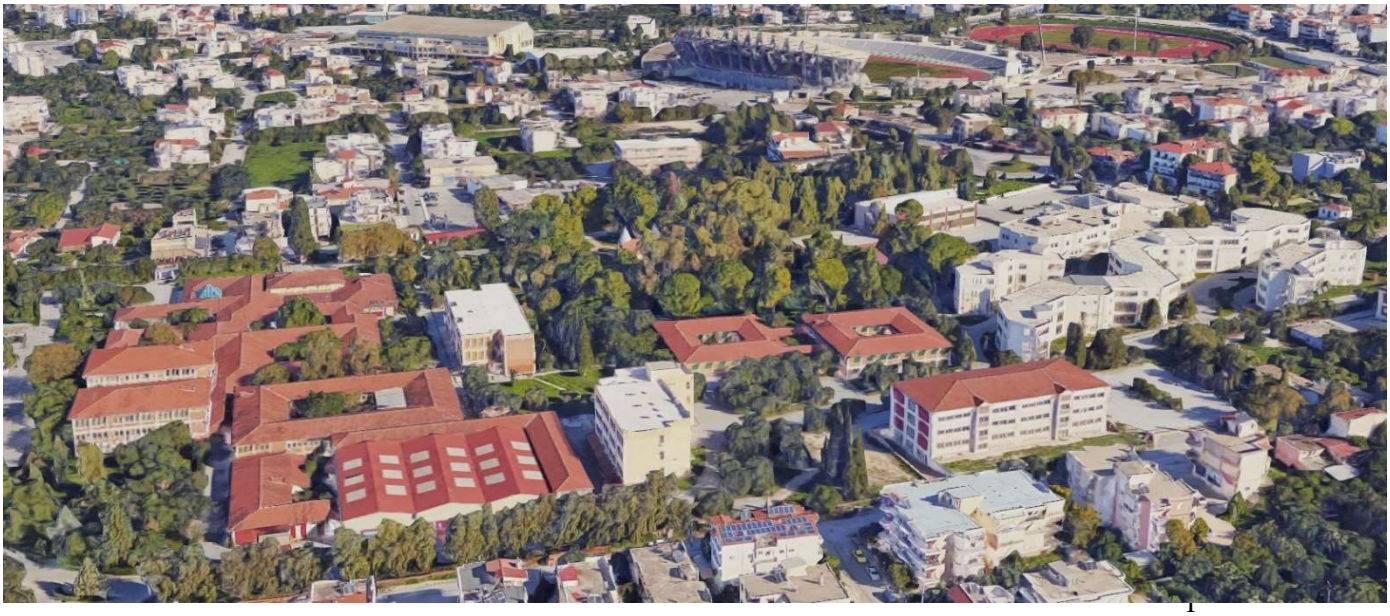
«Μελέτη κυβερνοεπιθέσεων και διαχείριση συμβάντων σε δικτυακά πληροφοριακά συστήματα»

Επιβλέπον: Στεφανίδης Κυριάκος

Φοιτητής: Παλιάτσας Νικόλαος

ΑΜ: 2014

• Τμήμα Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών, Πανεπιστήμιο Πελοποννήσου



Περιεχόμενα

1. Ασφάλεια δικτύων 5
1.2 Ανάγκη ασφάλειας δικτύων στην σημερινή εποχή 7
1.3 Προκλήσεις στην ασφάλεια δικτύων 8
2. Δικτυακές επιθέσεις 9
2.1 Sniffing 10
2.2 Man in the middle 11
2.3 TCP session Hijacking 12
2.4 Κλιμάκωση δικαιωμάτων σε επιθέσεις υπηρεσιών, δικτυακών συσκευών και λογισμικά πελατών 15
2.5 Επιθέσεις σε Web εφαρμογές 17
2.6 Άρνηση υπηρεσίας (Denial of Service) 17
2.7 Κατανεμημένη άρνηση υπηρεσίας (Distributed Denial of Service) 19
2.8 Επιθέσεις σε ασύρματα δίκτυα 20
3. Μελέτη επιθέσεων 23
3.1 Syslog server και syslog clients 23
3.2 SNMP traps tools 24
3.3 Συστήματα ανίχνευσης και συστήματα πρόληψης εισβολής (Intrusion Detection Systems and Intrusion Prevention Systems) 25
4. Προσομοιωτές δικτύων 28
4.1 Τύποι προσομοιωτών δικτύων 29
5. Sandbox 30
5.1 Ποιος ο σκοπός ενός Sandbox; 31
5.2 Πώς λειτουργεί ένα sandbox; 32
5.3 Οφέλη χρήσης sandbox 33
6. Προσομοιωτής δικτύων 33
6.1 GNS3-all-in-one 34
6.2 GNS Server 34
6.3 GNS3 Use Cases 35
6.4 Τοπολογία δικτύου 36
7. Σενάρια υλοποίησης 38
7.1 Περιγραφή σεναρίων 38
7.2 Υλοποίηση κοινών σημείων σεναρίων 41
7.3 Υλοποίηση Σεναρίου 1 43
7.3.1 Ανάλυση Αποτελεσμάτων Σεναρίου 1 47
7.4 Υλοποίηση Σεναρίου 2 57

7.4.1 Σύγκριση Αποτελεσμάτων Διαφορετικών Μεθόδων Επίθεσης..... 74
7.4.2 Ανάλυση Αποτελεσμάτων Σεναρίου 2 75
7.5 Πηγές..... 81

Περιεχόμενα Εικόνων

Εικόνα 1: Sniffing περιβάλλον 10
Εικόνα 2: Επίθεση man in the middle 11
Εικόνα 3: Αποσυγχρονισμός TCP session 13
Εικόνα 4: Δημιουργία καταιγίδας από TCP ACK 14
Εικόνα 5: Επίσκεψη πελάτη σε εχθρικό διακομιστή 16
Εικόνα 6: Περιεχόμενο επίθεσης στον πελάτη 16
Εικόνα 7: Περιεχόμενο επίθεσης στον πελάτη-2 17
Εικόνα 8: Χειραψία τριών κατευθύνσεων 18
Εικόνα 9: Δομή DDoS επιθέσεων 20
Εικόνα 10: Παθητική επίθεση 21
Εικόνα 11: Ενεργή επίθεση (1) 22
Εικόνα 12: Ενεργή επίθεση (2) 22
Εικόνα 13: Σπάσιμο κλειδιού 23
Εικόνα 14: Στιγμιότυπο GNS3 34
Εικόνα 15: Τοπολογία δικτύου 37
Εικόνα 16: Μοτίβο phishing e-mail 40
Εικόνα 17: HTTP κίνηση προς server επιτιθέμενου 45
Εικόνα 18: Αποτυχημένη προσπάθεια κατεβάσματος αρχείου 46
Εικόνα 19: Λειτουργία threat prevention τείχους προστασίας 47
Εικόνα 20: Wireshark-sandbox εγκαθίδρυση TCP επικοινωνίας 48
Εικόνα 21: Wireshark-sandbox κατέβασμα κακόβουλου λογισμικού 48
Εικόνα 22: Wireshark-sandbox μενού export objects 49
Εικόνα 23: IDS Security Onion alerts 50
Εικόνα 24: IDS PCAP εμφάνιση 50
Εικόνα 25: IDS PCAP εμφάνιση-2 51
Εικόνα 26: Cyber security chef αρχική σελίδα 51
Εικόνα 27: Cyber security chef αρχείο ASCII 52
Εικόνα 28: Virus total εντοπισμός 53
Εικόνα 29: Virus total εντοπισμός-2 53
Εικόνα 30: Virus total λεπτομέρειες 54
Εικόνα 31: Virus total λεπτομέρειες-2 54
Εικόνα 32: Virus total συμπεριφορά 55
Εικόνα 33: Virus total συμπεριφορά-2 56
Εικόνα 34: Virus total κοινότητα 56
Εικόνα 35: Τοπολογία σεναρίου 2 59
Εικόνα 36: Αποτελέσματα Nmap με προεπιλεγμένες ρυθμίσεις 60
Εικόνα 37: Αρχεία καταγραφής logs Checkpoint 63
Εικόνα 38: Αρχεία καταγραφής logs Checkpoint-2 65
Εικόνα 39: Αρχεία καταγραφής logs Wireshark Web-Server 66
Εικόνα 40: Αρχεία καταγραφής logs Wireshark web-server-2 67
Εικόνα 41: Αποτελέσματα Nmap σε stealth mode 68
Εικόνα 42: Αρχεία καταγραφής logs Checkpoint Stealth Mode 70
Εικόνα 43: Αρχεία καταγραφής logs Checkpoint Stealth Mode-2 72
Εικόνα 44: Αρχεία καταγραφής logs Wireshark web-server Stealth Mode 73
Εικόνα 45: Αρχεία καταγραφής logs Wireshark web-server Stealth Mode-2 74
Εικόνα 46: Ανάλυση log τείχους προστασίας 75
Εικόνα 47: Κανόνας 5 τείχους προστασίας 76
Εικόνα 48: Κανόνας 5 μετά την παραμετροποίηση 76

Εικόνα 49: Nmap με νέο κανόνα normal mode 77
Εικόνα 50: Nmap με νέο κανόνα stealth mode 78
Εικόνα 51: Checkpoint logs με νέο κανόνα normal mode 79
Εικόνα 52: Checkpoint logs με νέο κανόνα stealth mode 79
Εικόνα 53: Web-server Wireshark με νέο κανόνα normal mode 79
Εικόνα 54: Web-server Wireshark με νέο κανόνα stealth mode 80

1. Ασφάλεια δικτύων

Λαμβάνοντας υπόψιν την ραγδαία εξέλιξη της τεχνολογίας και πως η δομή του διαδικτύου είναι η διασύνδεση πολλαπλών δικτύων υπολογιστών μεταξύ τους, γίνεται εύκολα αντιληπτό πως ένα από τα σοβαρότερα ζητήματα πληροφορικής είναι η ασφάλεια των δεδομένων που διαχέονται μέσα στα δίκτυα. Ανατρέχοντας στα

προηγούμενα χρόνια, διαπιστώνεται πως οι προσπάθειες παράκαμψης της ασφάλειας των δικτύων εμφανίστηκε λίγο μετά την ευρεία χρήση τους κυρίως για στρατιωτικές και πολιτικές επικοινωνίες. Από τότε μέχρι σήμερα η ανάγκη για την ασφάλεια των δεδομένων αυξάνεται εκθετικά. Η αύξηση της χρήσης νέων τεχνολογιών και τεχνικών προσφέρει αδιαμφισβήτητα πλεονεκτήματα και ευκολίες στους χρήστες, από την άλλη όμως δημιουργεί μεγαλύτερες ανάγκες για την διασφάλιση των δεδομένων.

Η ασφάλεια δικτύων πλέον συγκαταλέγεται με τις πιο αναγκαίες προϋποθέσεις, όπως η ποιότητα και η απόδοση, για την ορθή λειτουργία μίας επιχείρησης ή ενός οργανισμού. Ο όρος λειτουργία συμπεριλαμβάνει το 80% των διαδικασιών μίας επιχείρησης, καθώς στις μέρες μας η επιστήμη της πληροφορικής έχει διεισδύσει σε σχεδόν όλα τα τμήματα και τις καθημερινές ενέργειες που απαιτούνται από αυτά. Η ασφάλεια δικτύων ορίζεται ως η έννοια που αναφέρεται στην διασφάλιση των πληροφοριών από καταστροφές, αλλοιώσεις και υποκλοπές. Επιπρόσθετα, αποτρέπει την χρήση των δικτυακών πόρων από μη εξουσιοδοτημένους χρήστες.

Για να επιτευχθούν όλα τα παραπάνω θα πρέπει να γίνεται σωστή πρόληψη και έγκαιρη ανίχνευση για τυχόν επιθέσεις και απώλειες. Ο κορμός διαδικασιών της ασφάλειας δικτύων αποτελείται από:

- **Πρόληψη**: Ενέργειες με σκοπό την αποφυγή φθοράς πόρων ενός δικτύου υπολογιστών.

- **Ανίχνευση**: Ενέργειες για τον εντοπισμό του δράστη, της χρονικής στιγμής και τον τρόπο που κάποιος προκάλεσε φθορά σε κάποιον πόρο του δικτύου.

- **Αντίδραση**: Ενέργειες για να αποκατασταθεί η φθορά του πόρου και γενικότερα η εύρυθμη λειτουργία του δικτύου.

Η ασφάλεια δικτύων σχετίζεται με την αντίσταση σε τυχαία συμβάντα η κακόβουλων λογισμικών που θέτουν σε κίνδυνο την αξιοπιστία, την διάθεση και την ακεραιότητα των δεδομένων που έχουν αποθηκευτεί σε δικτυακούς πόρους ή μεταδίδονται μέσω του δικτύου. Η συσχέτιση αυτή προέκυψε όταν αυξήθηκε η ανάγκη των επιχειρήσεων να συνδέονται με το διαδίκτυο. Σε αυτό το κομμάτι δικτυακής ασφάλειας οι προκλήσεις είναι πολύ μεγάλες, καθώς η επιχείρηση έρχεται σε δικτυακή επαφή με χιλιάδες άλλα δίκτυα ανά τον κόσμο, το οποίο αυξάνει τους κινδύνους επιθέσεων κατακόρυφα. Οι έννοιες που συσχετίζουν τα δίκτυα υπολογιστών με τις προκλήσεις είναι η διαθεσιμότητα, εμπιστευτικότητα και η ακεραιότητα.

Διαθεσιμότητα: Ορίζεται ως η ιδιότητα των υπηρεσιών να είναι προσπελάσιμες και χωρίς καθυστερήσεις όταν τις χρειαστούν εξουσιοδοτημένες οντότητες του δικτύου. Η

διαθεσιμότητα σε ένα δίκτυο απαιτείται να αγγίζει το 99%, χωρίς να επηρεάζεται από καταστάσεις όπως διακοπή ρεύματος, φυσικές καταστροφές, επιθέσεις από εξωγενείς παράγοντες και σφάλματα υλικού. Υπάρχει συγκεκριμένος τύπος επιθέσεων ο λεγόμενος άρνηση υπηρεσιών, που ο σκοπός του είναι η αποτροπή της πρόσβασης εξουσιοδοτημένων χρηστών σε δικτυακούς πόρους και υπηρεσίες. Ο τρόπος αντιμετώπισης του είναι η αποτροπή της σκόπιμης απώλειας διαθεσιμότητας των υπηρεσιών του οργανισμού. Μία από τις δημοφιλέστερες επιθέσεις άρνησης υπηρεσιών είναι η επίθεση flooding, όπου ο κακόβουλος χρήστης πλημμυρίζει έναν server με αιτήματα μέχρι να φτάνει σε σημείο να μην ανταποκρίνεται λόγω της πληθώρας αιτημάτων που έχει να εξυπηρετήσει.

Εμπιστευτικότητα: Ορίζεται ως η αποτροπή αποκάλυψης πληροφοριών που διαχέονται σε ένα δίκτυο σε μη εξουσιοδοτημένους χρήστες. Σε μερικές περιπτώσεις η εμπιστευτικότητα δεν αναφέρεται μόνο σε ανάγνωση ή υποκλοπή πληροφοριών, αλλά αναφέρεται και στην πληροφορία ύπαρξης των συγκεκριμένων πληροφοριών σε ένα δίκτυο.

Ακεραιότητα: Τα δεδομένα που αποστέλλονται μεταξύ χρηστών θα πρέπει να είναι ακέραια χωρίς να έχουν υποστεί καμία αλλοίωση. Στην ασφάλεια δικτύων η ακεραιότητα σχετίζεται με την πρόληψη αλλοίωσης δεδομένων από χρήστες που δεν έχουν εξουσιοδοτηθεί με το δικαίωμα μεταβολής δεδομένων.

1.2 Ανάγκη ασφάλειας δικτύων στην σημερινή εποχή

Πολλοί οργανισμοί και επιχειρήσεις θεωρούν την ασφάλεια δικτύων επιπρόσθετα έξοδα ή εντελώς περιττά έξοδα. Το επιχείρημα κάποιων μηχανικών για να υποστηρίξουν την παραπάνω άποψη είναι, πως εκτός από το κόστος σε χρόνο και χρήμα που αυξάνονται ταυτόχρονα μειώνεται η απόδοση του δικτύου. Η συγκεκριμένη θεωρία έχει μία βάση εφόσον τα πρωτόκολλα ασφαλείας προσθέτουν πληροφορία στα πακέτα που ανταλλάσσονται μέσα στο δίκτυο. Από την άλλη πλευρά όμως, το όφελος της ασφάλειας δεν μπορεί να θεωρηθεί σε καμία περίπτωση αντιστρόφως ανάλογο της απόδοσης. Πλέον στις μέρες μας η ασφάλεια θεωρείται αδιαμφισβήτητα αναγκαία για την εύρυθμη και σωστή λειτουργία των δικτύων όλων των οργανισμών, ανεξάρτητα της φύσεως και του μεγέθους τους. Κάποιοι αναρωτιούνται πως ίσως τα κόστη για την ασφάλεια των πληροφοριών να είναι δυσανάλογα με αυτά που προσφέρουν. Για αυτόν ακριβώς τον λόγο δημιουργήθηκαν οι πολιτικές ασφαλείας. Η πολιτική ασφαλείας εφαρμόζεται ξεχωριστά από κάθε οργανισμό και είναι αυτή που εξισορροπεί το κόστος υλοποίησης ασφάλειας με το κόστος ζημιών από πιθανολογούμενη απώλεια

πληροφοριών. Η κάθε πολιτική δεν θα πρέπει να είναι απόλυτη και κάθετη, αλλά να παρέχει την δυνατότητα επεκτασιμότητας και ευελιξίας σε περίπτωση μεταβολής των αναγκών ενός οργανισμού. Η αναγκαία πολιτική ασφάλειας καθορίζεται από μία δυναμική εκτίμηση του κόστους των μέτρων ασφαλείας σε σχέση με τις συνέπειες που θα προκύψουν για τον οργανισμό σε περίπτωση οποιαδήποτε πρόκλησης δυσλειτουργίας. Ο βασικός αυτός κανόνας ισχύει για όλους τους τομείς και όλα τα επίπεδα ασφάλειας. Έτσι, σε κάθε περίπτωση όπου απαιτείται η λήψη κάποιου μέτρου ασφαλείας, πρέπει πάντα να εξετάζεται η πιθανότητα να συμβεί κάποιο πρόβλημα και οι συνέπειες που αυτό θα προκαλέσει. Εάν η τιμή των δύο αυτών παραμέτρων είναι υψηλή, τότε πρέπει απαραίτητα να ληφθούν μέτρα, ανεξάρτητα από το κόστος πρόληψης. Ειδικά σε θέμα κόστους η ασφάλεια θα πρέπει να θεωρείται δυναμική και όχι στατική παράμετρος, καθώς οι τεχνολογίες, οι ανάγκες, ο ανταγωνισμός, οι κίνδυνοι απαιτούν την συνεχή αλλαγή των πολιτικών ασφαλείας με νέα δεδομένα και νέα μέτρα. Επομένως, γίνεται αντιληπτό πως κάθε οργανισμός θα πρέπει να επανεξετάζει συχνά τις πολιτικές που ακολουθεί ώστε να καλύπτει τις νέες ανάγκες που προκύπτουν.

1.3 Προκλήσεις στην ασφάλεια δικτύων

Η ανάγκη διασύνδεσης οργανισμών με μακρινές τοποθεσίες καθιστά την επικοινωνία την σημερινή εποχή πιο ευάλωτη από ποτέ. Αυτό συμβαίνει γιατί η πληροφορία αναγκαστικά μεταβαίνει εκτός του οργανισμού και ταξιδεύει κάνοντας χρήση μέσων που δεν μπορούν να ελεγχθούν από τις ομάδες του οργανισμού. Εκεί απαιτείται η σωστή επιλογή συνεργατών, οι οποίοι θα πρέπει να είναι έμπιστοι και άρτια καταρτισμένοι, ώστε να εξασφαλιστεί η ασφαλής μεταφορά δεδομένων. Ένα ακόμα θέμα που προκύπτει με τις συνδέσεις απομακρυσμένων σημείων είναι το υλικό στα οποία αυτές καταλήγουν. Τα πληροφοριακά συστήματα που συνδέονται στο δίκτυο του οργανισμού θα πρέπει να έχουν ελεγχθεί για κακόβουλα λογισμικά και εξουσιοδοτημένους χρήστες. Ιδανικό θα ήταν να μπορούσαν να ελεγχθούν από προσωπικό του ίδιου του οργανισμού, το οποίο στις περισσότερες περιπτώσεις είναι αδύνατο. Επομένως απαιτείται η ύπαρξη μιας υγειούς συνεργασίας μεταξύ των τεχνικών, με κοινό στόχο την δημιουργία σχέσεων εμπιστοσύνης και την αποτροπή απώλειας η διαστρέβλωσης δεοδμένων.

Έρευνες εντός των οργανισμών έχουν αποδείξει πως μεγάλο πλήθος συμβάντων απώλειας πληροφοριών και δεδομένων προκύπτουν από τους ίδιους τους εργαζομένους χωρίς να έχουν καμία σκοπιμότητα έκθεσης αυτών. Αυτές είναι ίσως από τις δυσκολότερες προκλήσεις των τεχνικών, εφόσον η γενική ιδέα της ασφάλειας είναι να οχυρωθεί ο οργανισμός από εξωγενείς παράγοντες και όχι τόσο από

ενδογενείς. Πλέον όμως τα τεχνικά τμήματα είναι αναγκασμένα να λαμβάνουν τα ίδια αυστηρά μέτρα για όλους τους παράγοντες, ώστε να εξασφαλίζουν την ακεραιότητα της υπηρεσίας τους. Σε επίπεδο χρηστών, τα αρμόδια τμήματα πραγματοποιούν εντατικές εκπαιδεύσεις στο προσωπικό με σκοπό να γνωρίζουν την σημαντικότητα της διασφάλισης δεδομένων, καθώς επίσης το πως μπορούν να αναγνωρίζουν τις τεχνικές phishing από τους εισβολείς και πως να τις αποφεύγουν. Σε επίπεδο συστημάτων απαιτείται ο διαχωρισμός των υποδικτύων, το οποίο βοηθά σε περιπτώσεις που κάποιος επιτιθέμενος έχει εισχωρήσει στο δίκτυο του οργανισμού. Αν το δίκτυο είναι χωρισμένο σε μικρά τμήματα και μεταξύ τους έχουν εφαρμοστεί πολιτικές ασφαλείας, τότε υπάρχουν μεγάλες πιθανότητες ο επιτιθέμενος να απομονωθεί μόνο σε μικρό τμήμα του δικτύου χωρίς να αποκτήσει πρόσβαση σε άλλες πληροφορίες και άλλους δικτυακούς πόρους.

2. Δικτυακές επιθέσεις

Στο δίκτυο ενός οργανισμού δεν ανήκουν μόνο οι δικτυακές συσκευές που συμμετέχουν στην εγκαθίδρυση της επικοινωνίας, αλλά ανήκουν και πληροφοριακά συστήματα για τα οποία η δικτυακή επικοινωνία κρίνεται απαραίτητη για την λειτουργία τους. Επομένως οι δικτυακές επιθέσεις δεν περιορίζονται μόνο σε συγκεκριμένου τύπου συσκευών, με αποτέλεσμα να δύναται να βλάψουν όλα τα συστήματα που επικοινωνούν κάνοντας χρήση δικτυακών πρωτοκόλλων. Οι δικτυακές επιθέσεις μπορούν να κατηγοριοποιηθούν ανάλογα με την επίπτωση που έχουν στους στόχους τους και ανάλογα με τη φύση των στόχων τους.

Η πρώτη κατηγορία επιθέσεων χωρίζεται στις υποκατηγορίες:

- Κλιμάκωση των προνομίων
- Άρνηση υπηρεσιών – DoS

Η δεύτερη κατηγορία επιθέσεων χωρίζεται στις υποκατηγορίες:

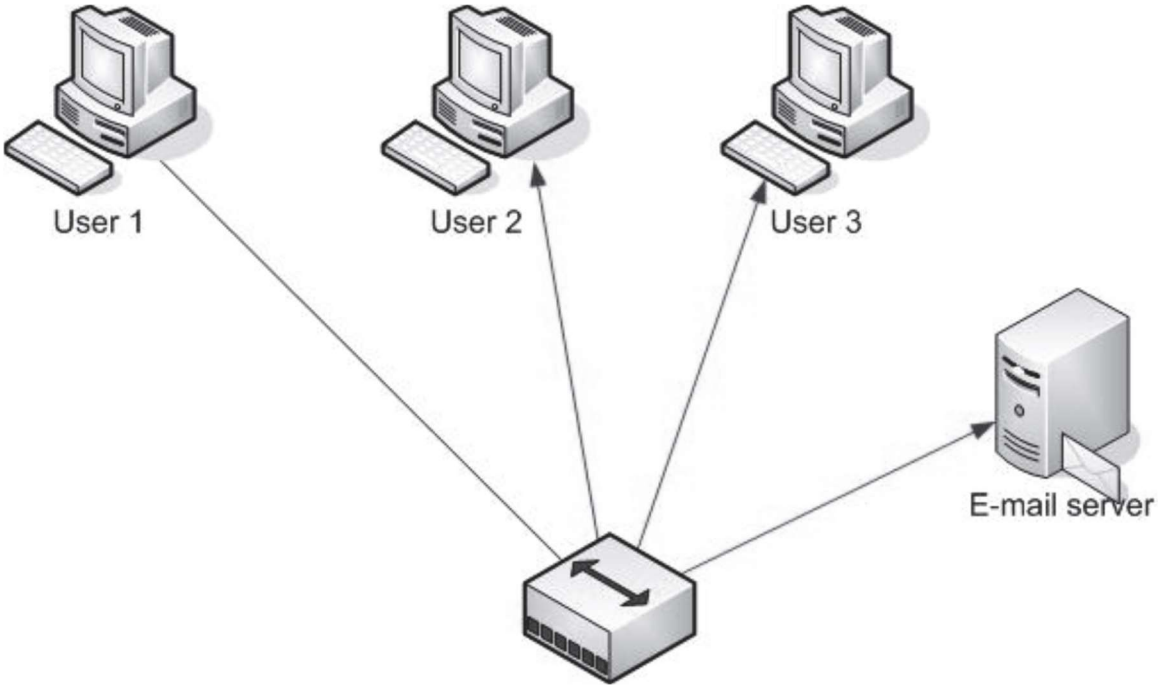
- Επιθέσεις με στόχο δικτυακές συσκευές
- Επιθέσεις με στόχο πληροφοριακά συστήματα

Οι επιθέσεις κλιμάκωσης προνομίων έχουν ως στόχο την απόκτηση κάποιου είδους προνομίων στον στόχο. Για παράδειγμα, έστω ένας οργανισμός Χ με μία δυναμική

ιστοσελίδα φόρτωσης περιεχομένου. Η ιστοσελίδα επικοινωνεί με μία βάση δεδομένων SQL από όπου διαχειρίζεται τα δεδομένα. Αν η ιστοσελίδα έχει ένα τρωτό σημείο που επιτρέπει την έγχυση SQL κώδικα στον server, τότε ο επιτιθέμενος μπορεί να στείλει ένα SQL query στον server, το οποίο θα ανοίγει λογαριασμό με δικαιώματα διαχειριστή στην ιστοσελίδα. Οι επιθέσεις άρνησης υπηρεσίας έχουν σαν στόχο την διακοπή της κανονικής λειτουργίας των δικτύων ή των πληροφοριακών συστημάτων. Οι περισσότερες επιθέσεις άρνησης υπηρεσίας είναι αποτέλεσμα ανεπιτυχών επιθέσεων κλιμάκωσης προνομίων. Οι επιθέσεις με στόχο δικτυακές συσκευές είναι επιθέσεις που εστιάζουν σε routers, switches, κ.ά. Οι επιθέσεις με στόχο πληροφοριακά συστήματα εστιάζουν σε servers ή τερματικές συσκευές χρηστών.

2.1 Sniffing

Το λεγόμενο sniffing δικτυακής κίνησης είναι η μέθοδος αντιγραφής πληροφοριών που περιέχονται σε ένα πακέτο χωρίς να αλλαχτούν. Το sniffing ανήκει στην κατηγορία των επιθέσεων κλιμάκωσης προνομίων. Ο κύριος σκοπός αυτών των επιθέσεων είναι να αποσπάσουν το όνομα χρήστη και τον κωδικό διαχειριστή του στόχου. Το sniffing επιτυγχάνεται λόγω του σχεδιασμού του TCP/IP πρωτοκόλλου και της έλλειψης κρυπτογράφησης σε αυτό. Άλλος ένας λόγος είναι ο αδύναμος σχεδιασμός ενός δικτύου από τους μηχανικούς. Ένα τέτοιο παράδειγμα σχεδιασμού είναι η διασύνδεση όλων των συσκευών μέσω ενός hub το οποίο θα αναλύσουμε παρακάτω. Ο χρήστης 1 αποστέλλει το όνομα χρήστη και τον κωδικό του στον e-mail server.



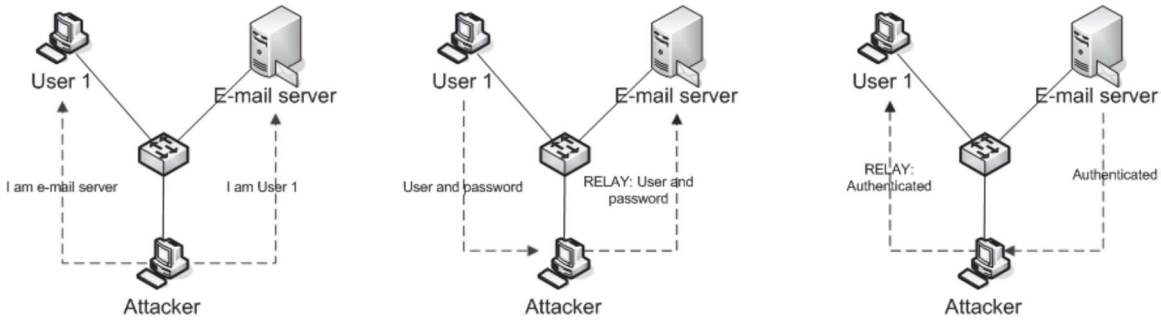
Εικόνα 1: Sniffing περιβάλλον

Το hub λαμβάνει τα πακέτα και τα στέλνει σε όλες τις πόρτες του εκτός αυτής από την οποία τα έλαβε. Αν κάποιος που συμμετέχει σε αυτήν την τοπολογία του δικτύου τρέχει ένα εργαλείο sniffing, έχει τη δυνατότητα να δει το όνομα χρήστη και τον κωδικό που αποστέλλει ο χρήστης 1.

2.2 Man in the middle

Το συγκεκριμένο είδος επίθεσης είναι παρόμοιο με το sniffing, θεωρείται όμως πιο προχωρημένο. Η βασική διαφορά τους είναι πως η επίθεση MITM χρησιμοποιείται για την αλλαγή των δεδομένων των TCP/IP πακέτων, το οποίο σημαίνει πως το sniffing μπορεί να πραγματοποιηθεί και σε κρυπτογραφημένα πακέτα. Για να είναι επιτυχημένη μία επίθεση MITM θα πρέπει να ξεγελαστούν τα τερματικά και να πιστέψουν πως ο επιτιθέμενος είναι αυτός στον οποίο επιθυμούν να στείλουν τα πακέτα. Δηλαδή σε μία επικοινωνία μεταξύ του υπολογιστή 1 και του υπολογιστή 2, ο επιτιθέμενος θα εμφανίζεται ως υπολογιστής 1 για τον υπολογιστή 2 και ως υπολογιστής 2 για τον υπολογιστή 1.

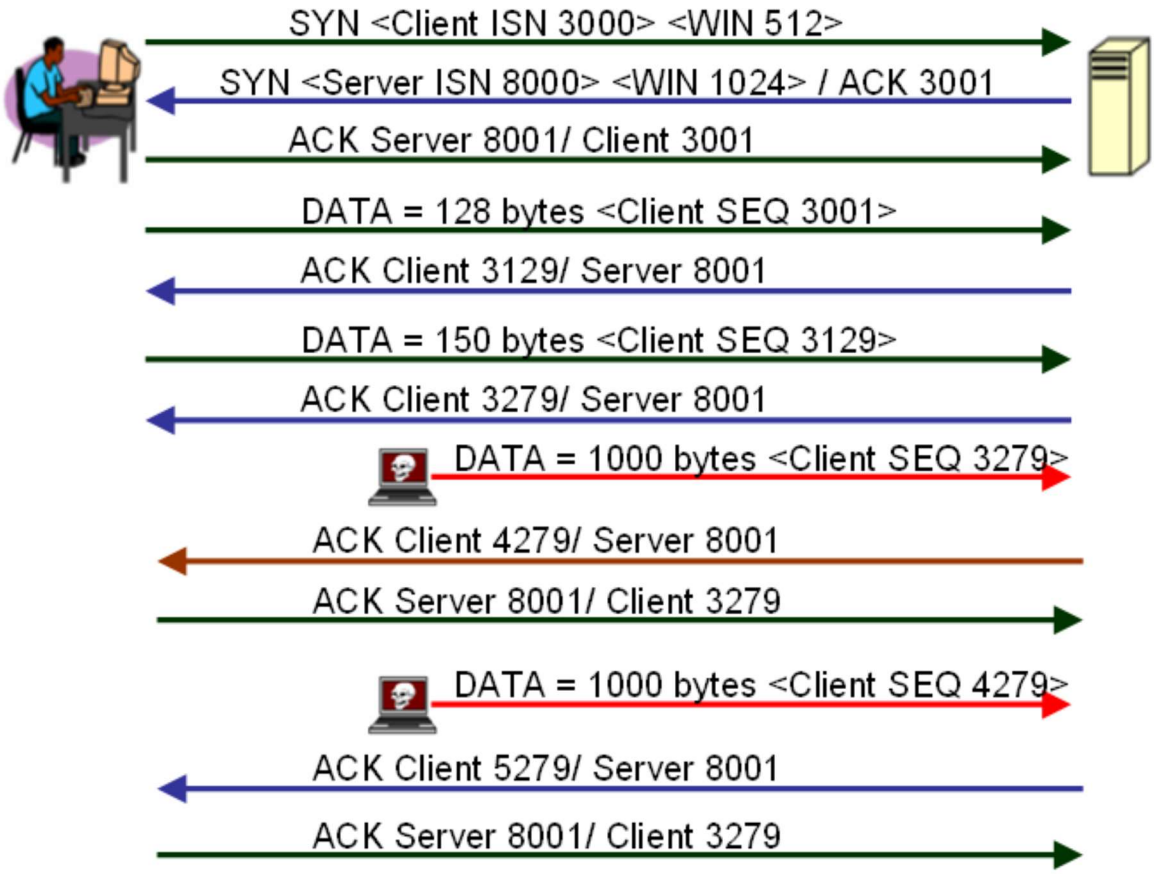
Τα κρυπτογραφημένα πακέτα μπορούν να υποκλαπούν την ώρα που ανταλλάζονται οι πληροφορίες σχετικά με τα κλειδιά κρυπτογράφησης. Αν μπορέσουν και αλλαχτούν τα κλειδιά επικοινωνίας μεταξύ του υπολογιστή 1 και υπολογιστή 2 με κλειδιά για τα οποία γνωρίζουμε τα ιδιωτικά κλειδιά, τότε είναι εφικτή η υποκλοπή κρυπτογραφημένων πακέτων μεταξύ των υπολογιστών. Αυτές οι επιθέσεις είναι υπερβολικά δύσκολο να εντοπιστούν. Η μόνη προστασία είναι η ανταλλαγή πιστοποιητικών μεταξύ των υπολογιστών και ο έλεγχος της εγκυρότητας τους σε επίπεδο εφαρμογής.



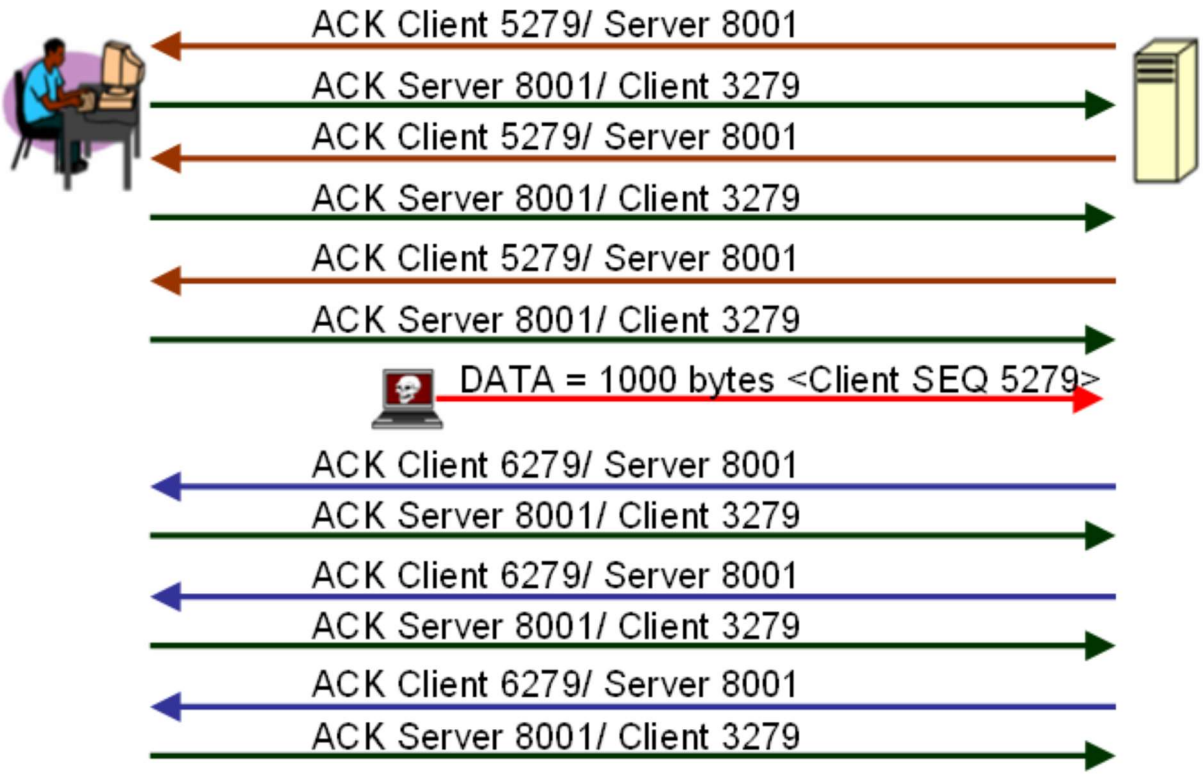
Εικόνα 2: Επίθεση man in the middle

2.3 TCP session Hijacking

Το TCP session hijacking αναφέρεται στην εισβολή ενός επιτιθέμενου σε μία ήδη εγκαθιδρυμένη TCP επικοινωνία, ο οποίος εγχέει πακέτα μέσα στην ροή, τα οποία επεξεργάζονται από τον παραλήπτη σαν να προέρχονται από τον αυθεντικό αποστολέα. Μία TCP επικοινωνία χαρακτηρίζεται από τέσσερα στοιχεία: διεύθυνση IP πελάτη, αριθμός πόρτας πελάτη, διεύθυνση IP διακομιστή, αριθμός πόρτας διακομιστή. Αν κάποιος καταφέρει να υποκλέψει τις παραπάνω πληροφορίες μίας TCP ροής και ξεκινήσει να γεμίζει την ροή με δικά του πακέτα κάνοντας χρήση των υποκλεμμένων πληροφοριών, κανένα μέλος της επικοινωνίας δεν θα αντιληφθεί ότι πρόκειται για κάποιον επιτιθέμενο.



Εικόνα 3: Αποσυγχρονισμός TCP session



Εικόνα 4: Δημιουργία καταιγίδας από TCP ACK

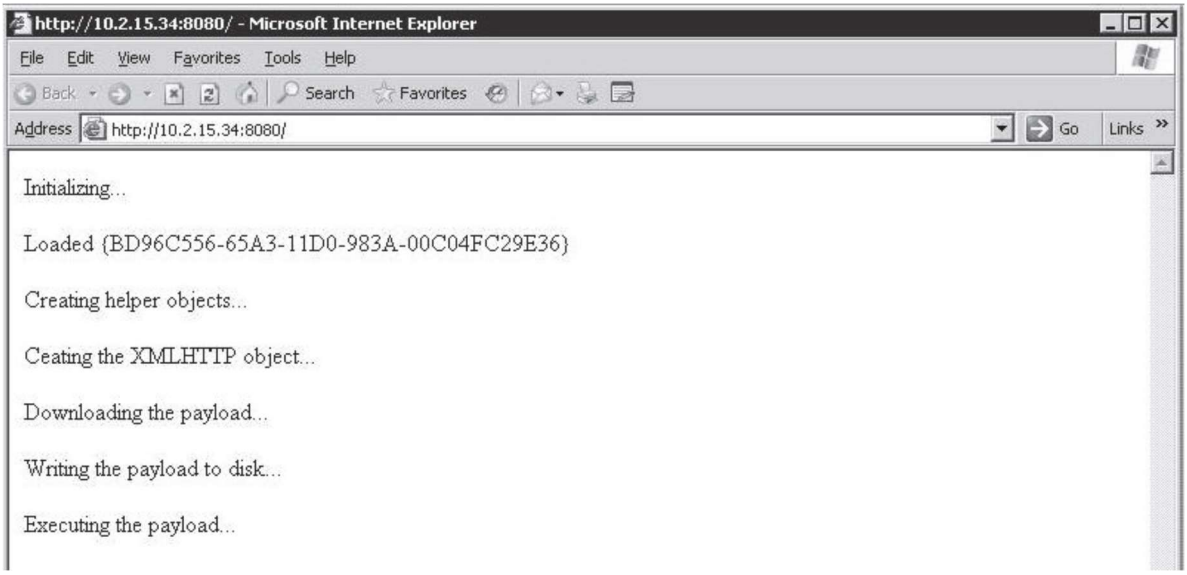
Για να θεωρηθεί επιτυχημένη μία τέτοια επίθεση, ο επιτιθέμενος θα πρέπει πρώτα να αποσυγχρονίσει την TCP συνεδρία και μετέπειτα να περάσει τα δικά του πακέτα στην ροή. Για τον αποσυγχρονισμό μίας υπάρχουσας TCP συνεδρίας μεταξύ ενός πελάτη και ενός διακομιστή, ο επιτιθέμενος θα πρέπει πρώτα να προβλέψει το sequence αριθμό που επρόκειτο να χρησιμοποιηθεί από τον πελάτη (ή τον διακομιστή) και ύστερα να τον χρησιμοποιήσει πριν από αυτόν. Εάν ο επιτιθέμενος χρησιμοποιεί κάποιο sniffing εργαλείο μπορεί να εντοπίσει τον sequence αριθμό με απόλυτη ακρίβεια. Σε αντίθετη περίπτωση, ο επιτιθέμενος θα πρέπει να χρησιμοποιήσει όλες τις άλλες μεθόδους για να μαντέψει τον sequence αριθμό. Όταν ο επιτιθέμενος πάρει πρόσβαση στην συνεδρία και ξεκινήσει να στέλνει πακέτα, ο διακομιστής θα ξεκινήσει να στέλνει ACK πακέτα στον αυθεντικό αποστολέα. Το πιο πιθανό είναι αυτά τα πακέτα να εμπεριέχουν ACK sequence αριθμούς που δεν θα συνάδουν με αυτά που περιμένει ο πελάτης, επομένως ο πελάτης θα προσπαθήσει να συγχρονίσει την επικοινωνία με τον διακομιστή ξανά, στέλνοντας ACK πακέτα με τον sequence αριθμό που ανέμενε. Από την πλευρά του ο διακομιστής θα λάβει το πακέτο συγχρονισμού αλλά με διαφορετικό ACK sequence αριθμό με αποτέλεσμα να στέλνει στον πελάτη ACK πακέτα με τον αριθμό που ανέμενε. Αυτός ο κύκλος ανταλλαγής ACK πακέτων είναι ατέρμονος και δημιουργεί την καταιγίδα TCP ACK που φαίνεται στην εικόνα 4. Ο επιτιθέμενος συνεχίζοντας να στέλνει πακέτα δημιουργεί όλο και περισσότερες καταιγίδες, με αποτέλεσμα την μείωση της απόδοσης του δικτύου. Μετά από έναν

αριθμό ανεπιτυχών προσπαθειών συγχρονισμού με τον διακομιστή, ο πελάτης κλείνει στην σύνδεση με τον διακομιστή.

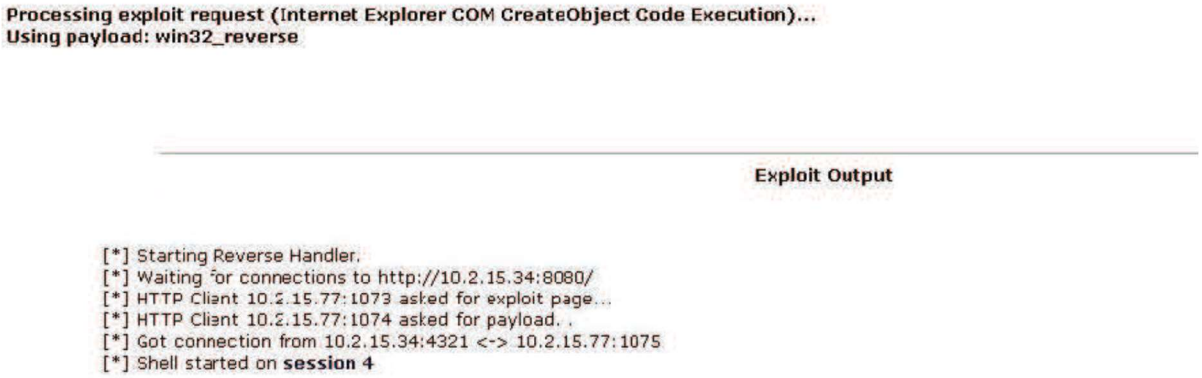
2.4 Κλιμάκωση δικαιωμάτων σε επιθέσεις υπηρεσιών, δικτυακών συσκευών και λογισμικά πελατών

Οι επιθέσεις αυτού του τύπου είναι από τις πιο δημοφιλείς επιθέσεις και οι επιπτώσεις τους τις καθιστούν από τις πιο επικίνδυνες. Η πρώτη επίθεση αυτού του τύπου εντοπίστηκε το 1985 και πήρε το όνομά του από τον συγγραφέα του «The Morris worm». Αυτοί οι τύποι επιθέσεων στοχεύουν στην εκμετάλλευση ορισμένων αδυναμιών ασφαλείας στον κώδικα της υπηρεσίας. Με την επιτυχή εκμετάλλευση της αδυναμίας, οι εισβολείς αποκτούν πρόσβαση σε ένα κέλυφος εντολών στο μηχάνημα-στόχο. Μέσω του κελύφους εντολών είναι σε θέση να εκτελέσουν εντολές συστήματος που συνήθως εκτελούνται με δικαιώματα διαχειριστή. Τα τρωτά σημεία ασφαλείας που γίνονται αντικείμενο εκμετάλλευσης είναι τα σημεία της γλώσσας προγραμματισμού στην οποία γράφτηκε η υπηρεσία. Οι πιο δημοφιλείς αδυναμίες είναι οι υπερχειλίσεις στοίβας, οι υπερχειλίσεις σωρού και οι υπερχειλίσεις συμβολοσειρών μορφοποίησης. Κυρίως είναι αδυναμίες της γλώσσας προγραμματισμού C/C++. Δεδομένου ότι η C/C++ είναι η γλώσσα προγραμματισμού που χρησιμοποιείται για τη σύνταξη λογισμικού συστήματος, γίνεται αντιληπτό ότι σχεδόν όλες οι υπηρεσίες, οι συσκευές δικτύου και το λογισμικό πελάτη μπορούν να περιέχουν τις προαναφερθείσες αδυναμίες ασφαλείας. Όταν πρόκειται για εκμετάλλευση συσκευών δικτύου, η μόνη διαφορά μεταξύ των φλοιών εντολών είναι ότι εκτελεί την εντολή συστήματος της συγκεκριμένη συσκευής δικτύου. Μετά από μια επιτυχημένη επίθεση, οι εισβολείς εγκαθιστούν σχεδόν πάντα μεθόδους εισόδου στα παραβιασμένα συστήματα υπολογιστών.

Το λογισμικό πελάτη είναι απρόσβλητο σε επιθέσεις υπηρεσιών, καθώς δεν ακούει ποτέ σε προσβάσιμες πόρτες εξωτερικών δικτύων. Εξαιτίας αυτού, μια επίθεση στο λογισμικό πελάτη εκδηλώνεται όταν ο πελάτης επισκέπτεται έναν εχθρικό διακομιστή. Στο παρακάτω παράδειγμα ο πελάτης επισκέπτεται έναν εχθρικό διακομιστή ιστού.



Εικόνα 5: Επίσκεψη πελάτη σε εχθρικό διακομιστή



Εικόνα 6: Περιεχόμενο επίθεσης στον πελάτη

```
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

C:\Documents and Settings\Administrator\Desktop>
>> dir

dir
 Volume in drive C has no label.
 Volume Serial Number is F86E-14BB

 Directory of C:\Documents and Settings\Administrator\Desktop

11/08/2006  01:27 PM    <DIR>          .
11/08/2006  01:27 PM    <DIR>          ..
08/04/2006  02:07 PM             1,898 Reporter.lnk
11/08/2006  01:27 PM    <DIR>          tftpd32.274
11/08/2006  01:26 PM           175,348 tftpd32.274.zip
11/08/2006  01:26 PM            98,468 TFTPServer1-1-980730.exe
               3 File(s)        275,714 bytes
               3 Dir(s)  12,706,107,392 bytes free

C:\Documents and Settings\Administrator\Desktop>
```

Εικόνα 7: Περιεχόμενο επίθεσης στον πελάτη-2

2.5 Επιθέσεις σε Web εφαρμογές

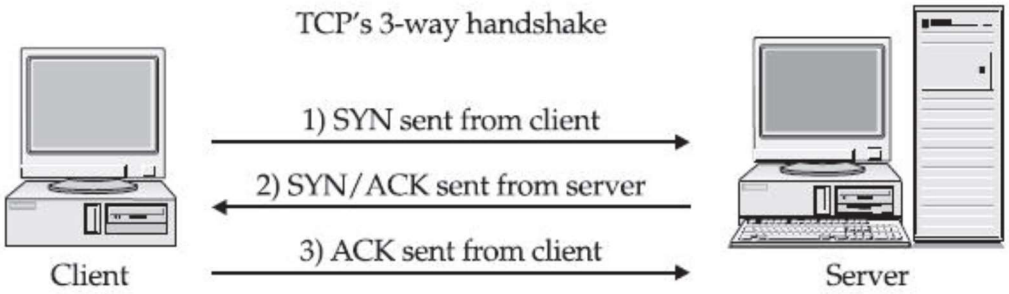
Τα τελευταία χρόνια οι επιθέσεις σε web εφαρμογές άρχισαν να αυξάνονται και να αποκτούν μεγάλη δημοτικότητα. Βασίζονται σε αδυναμίες των γλωσσών προγραμματισμού στις οποίες είναι γραμμένες. Οι επιθέσεις διαδικτυακών εφαρμογών περιορίζονται στη βάση δεδομένων στην οποία λειτουργεί η εφαρμογή web. Η αδυναμία μπορεί να βρεθεί στον κώδικα που εκτελεί ερωτήματα SQL και η εκμετάλλευση γίνεται με την εισαγωγή προσαρμοσμένων ερωτημάτων SQL του επιτιθέμενου στα υπάρχοντα ερωτήματα. Λόγω του SQL query injection, η επίθεση ονομάστηκε SQL injection και ο αντίκτυπος είναι υψηλότερος σε εφαρμογές web που χρησιμοποιούν MS SQL ή Oracle ως διακομιστή βάσης δεδομένων. Στην περίπτωση αυτών των δύο τύπων βάσεων δεδομένων, ο επιτιθέμενος μπορεί να εκτελέσει κώδικα συστήματος στον διακομιστή βάσης δεδομένων μέσω της χρήσης των προεπιλεγμένων αποθηκευμένων διαδικασιών που βρίσκονται σε αυτές. Δεδομένου ότι αυτή η επίθεση είναι ένα σφάλμα προγραμματισμού, η κατάλληλη πρόληψη είναι η εγγραφή ασφαλούς κώδικα. Αυτό μπορεί να γίνει φιλτράροντας όλες τις μεταβλητές από τα εισερχόμενα αιτήματα και αλλάζοντας/διαγράφοντας τις ύποπτες τιμές.

2.6 Άρνηση υπηρεσίας (Denial of Service)

Οι επιθέσεις άρνησης υπηρεσίας κέρδισαν τη δημοτικότητά τους το 1997 και έκτοτε αποτελούν μία από τις πιο δημοφιλείς επιθέσεις εναντίον δικτύων υπολογιστών. Είναι από τις πιο κρίσιμες και καταστροφικές για τις εταιρίες και τους οργανισμούς και τα τελευταία χρόνια οι αριθμοί απεικονίζουν πως οι απώλειες από επιθέσεις DoS είναι οι μεγαλύτερες. Το DoS μπορεί να χωριστεί σε επιθέσεις κατά εφαρμογών, επιθέσεις κατά συστημάτων υπολογιστών και επιθέσεις κατά συσκευών δικτύου. Χρησιμοποιώντας αυτή την κατηγοριοποίηση, μπορούμε να ορίσουμε δύο επιθέσεις DoS:

- SYN πλημμύρες
- Εκμετάλλευση αδυναμίας ασφαλείας
- Smurf
- Επιθέσεις κατά δρομολογητών

Οι επιθέσεις πλημμύρας SYN εκμεταλλεύονται μια αδυναμία στη σουίτα πρωτοκόλλου TCP/IP. Πιο συγκεκριμένα στην διαδικασία τριπλής χειραψίας. Η χειραψία τριών κατευθύνσεων ξεκινά από ένα πακέτο SYN το οποίο στη συνέχεια επικυρώνεται με ένα SYN/ACK από το άλλο μηχάνημα και στο τέλος ολοκληρώνεται από ένα πακέτο ACK. Το SYN flood εκμεταλλεύεται τη χειραψία τριών κατευθύνσεων εκκινώντας πολλές συνδέσεις στον διακομιστή ο οποίος δεν προλαβαίνει να απαντήσει ποτέ στο πακέτο SYN/ACK με ένα πακέτο ACK. Στην πλευρά του διακομιστή για κάθε πακέτο SYN, ο διακομιστής δεσμεύει ένα κομμάτι μνήμης και το διατηρεί για κάποιο χρονικό διάστημα. Ο επιτιθέμενος στέλνει μερικές χιλιάδες αιτήματα συνδέσεων, τα οποία καταλήγουν να καταναλώνουν την μνήμη του διακομιστή.



Εικόνα 8: Χειραψία τριών κατευθύνσεων

Η εκμετάλλευση μιας αδυναμίας ασφαλείας μπορεί να καταστρέψει τον διακομιστή ή να καταρρεύσει την εφαρμογή που τρέχει σε αυτόν. Ο αντίκτυπος εξαρτάται από την τοποθεσία της ευπάθειας. Για παράδειγμα, εάν η αδυναμία εντοπίζεται στον κώδικα πυρήνα του υπολογιστικού συστήματος ή της δικτυακής συσκευής και ο επιτιθέμενος καταφέρει να δράσει, τότε το αποτέλεσμα θα είναι να

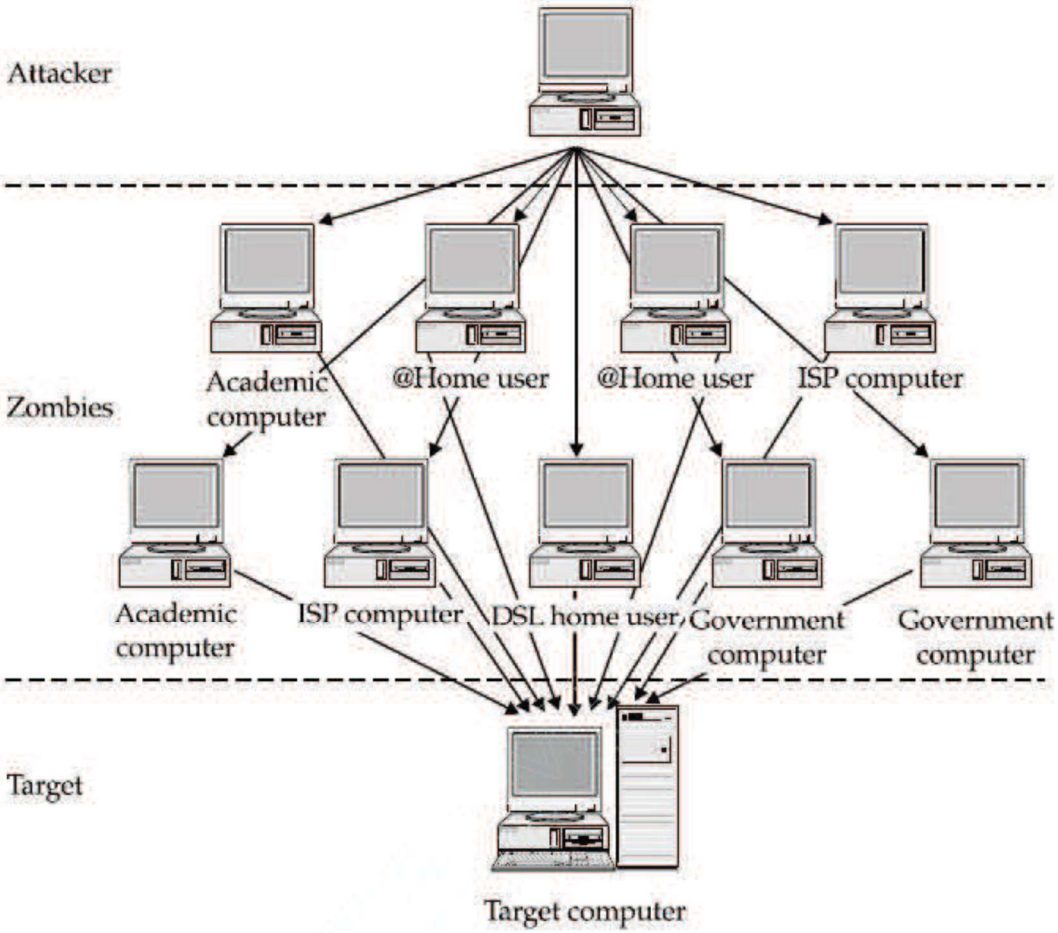
σταματήσει η λειτουργία της συσκευής ολοκληρωτικά.

Το smurf είναι η πρωτόγονη έκδοση των σημερινών κατανεμημένων επιθέσεων άρνησης υπηρεσίας (DDos). Η επίθεση γίνεται με την αποστολή ενός πακέτου ping σε μεγάλο αριθμό διευθύνσεων εκπομπής, όπου το πακέτο ping περιέχει μια πλαστή διεύθυνση IP από τον στόχο. Δεδομένου ότι το πακέτο ping στάλθηκε σε broadcast διευθύνσεις, όταν οι παραλήπτες ξεκινήσουν να απαντούν στα pings, πιθανότατα θα καταρρεύσουν το μηχάνημα αποστολέα εξαιτίας του τεράστιου αριθμού αιτημάτων.

Οι επιθέσεις σε δρομολογητές είναι αυτές που είναι πιο εκλεπτυσμένες όταν πρόκειται για την άρνηση υπηρεσίας. Λειτουργούν στέλνοντας ενημερώσεις πρωτοκόλλου δρομολόγησης και με αυτές τις ενημερώσεις δημιουργούν μαύρες τρύπες που καταρρέουν ολόκληρη την κυκλοφορία. Το πρόβλημα έγκειται στην χαμηλή ασφάλεια στις ενημερώσεις του πίνακα δρομολόγησης. Ένας άλλος τύπος επιθέσεων άρνησης υπηρεσίας είναι οι τοπικές επιθέσεις άρνησης υπηρεσίας. Η διαφορά μεταξύ αυτών και των απομακρυσμένων επιθέσεων άρνησης υπηρεσίας είναι ότι πρέπει να εκτελούνται τοπικά. Εντοπίζονται εύκολα γιατί πρέπει να εκτελεστούν από έναν τοπικό χρήστη του συστήματος.

2.7 Κατανεμημένη άρνηση υπηρεσίας (Distributed Denial of Service)

Οι πρώτες κατανεμημένες επιθέσεις άρνησης υπηρεσίας εντοπίστηκαν το 2000 όταν κατέρριψαν με επιτυχία τους διακομιστές του Yahoo, του CNN, του eBay και πολλών άλλων οργανισμών. Σχεδιαστικά, οι επιθέσεις DDoS υλοποιούν σχεδόν όλες τις προαναφερθείσες επιθέσεις DoS με τη διαφορά ότι οι επιθέσεις εκτελούνται από περισσότερα από ένα συστήματα. Το περιβάλλον DDoS έχει σχεδιαστεί έτσι ώστε να υπάρχει ένας κύριος διακομιστής που ελέγχει ολόκληρο το σύνολο των διακομιστών «ζόμπι» και όλοι μαζί είναι γνωστοί ως botnet. Όταν χρειάζεται να ξεκινήσει μια επίθεση, ο εισβολέας συνδέεται με τον κύριο διακομιστή από όπου ξεκινά την επίθεση και αυτός με τη σειρά του στέλνει εντολές και τη διεύθυνση IP στόχου στους διακομιστές «ζόμπι».



Εικόνα 9: Δομή DDoS επιθέσεων

Ένα botnet δημιουργείται με έκθεση συστημάτων υπολογιστών και με κλιμάκωση των προνομίων. Αφού παραβιαστεί το σύστημα του υπολογιστή, ο εισβολέας εγκαθιστά το λογισμικό DDoS στο σύστημα προορισμού και στη συνέχεια το διαμορφώνει ώστε να επικοινωνεί με τον κύριο διακομιστή. Μια νέα τάση για τους εισβολείς είναι να γράφουν worms που θέτουν σε κίνδυνο τα συστήματα υπολογιστών και έπειτα να ξεκινούν μια επίθεση DDoS σε έναν συγκεκριμένο στόχο. Αυτά τα worms θα κυκλοφορήσουν αργότερα στο διαδίκτυο. Αμυντικοί μηχανισμοί για τις DDoS επιθέσεις υπάρχουν στο εμπόριο αλλά θεωρούνται αρκετά ακριβοί.

2.8 Επιθέσεις σε ασύρματα δίκτυα

Όταν πρόκειται για επίθεση σε ασύρματα δίκτυα, πρέπει να προσθέσουμε μια ακόμη κατηγορία σε όλες τις προαναφερθείσες. Η επίθεση που τείνει να επιτίθεται στην κρυπτογράφηση που χρησιμοποιεί το ασύρματο δίκτυο. Το ασύρματο δίκτυο χρησιμοποιεί κρυπτογραφικούς αλγόριθμους μεταξύ των οποίων είναι οι WEP, WPA, LEAP, PEAP. Μερικοί από αυτούς τους, χρειάζονται ένα δεύτερο επίπεδο υποστήριξης

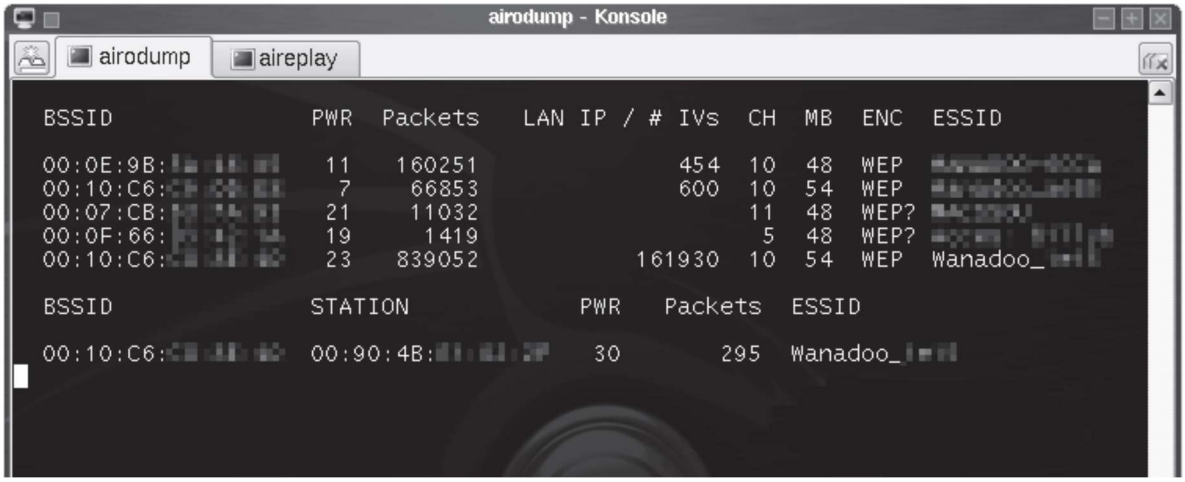
για να λειτουργήσουν. Οι αλγόριθμοι που δεν χρειάζονται υποστήριξη δεύτερου επιπέδου, WEP και WPA, δέχονται τις περισσότερες επιθέσεις και είναι οι πιο ανασφαλείς. Αυτή η επίθεση στοχεύει να ανακαλύψει το κλειδί που απαιτείται για τη σύνδεση στο επιλεγμένο SSID. Μπορεί να επιτευχθεί χρησιμοποιώντας δύο τύπους επιθέσεων:

- Παθητική επίθεση
- Ενεργή επίθεση

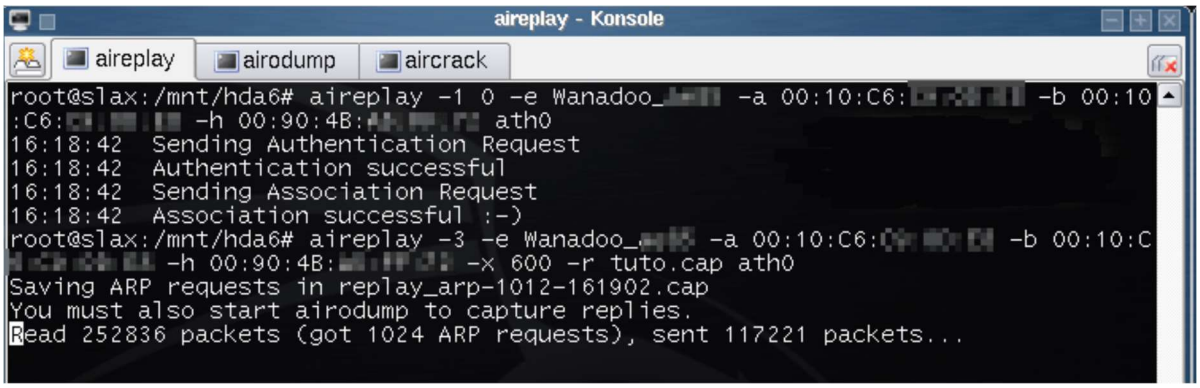
Η παθητική επίθεση είναι μια σιωπηλή επίθεση και συγκεντρώνει μόνο πακέτα που κυκλοφορούν στο ασύρματο δίκτυο. Αυτό σημαίνει ότι σε έναν υπολογιστή υπάρχει ένας ασύρματος ανιχνευτής που συλλέγει όλα αυτά τα δεδομένα μέχρι να βρει το κλειδί. Οι παθητικές επιθέσεις χρειάζονται χρόνο για να συγκεντρώσουν αρκετά πακέτα ώστε να ανακαλύψουν το κλειδί.

Εικόνα 10: Παθητική επίθεση

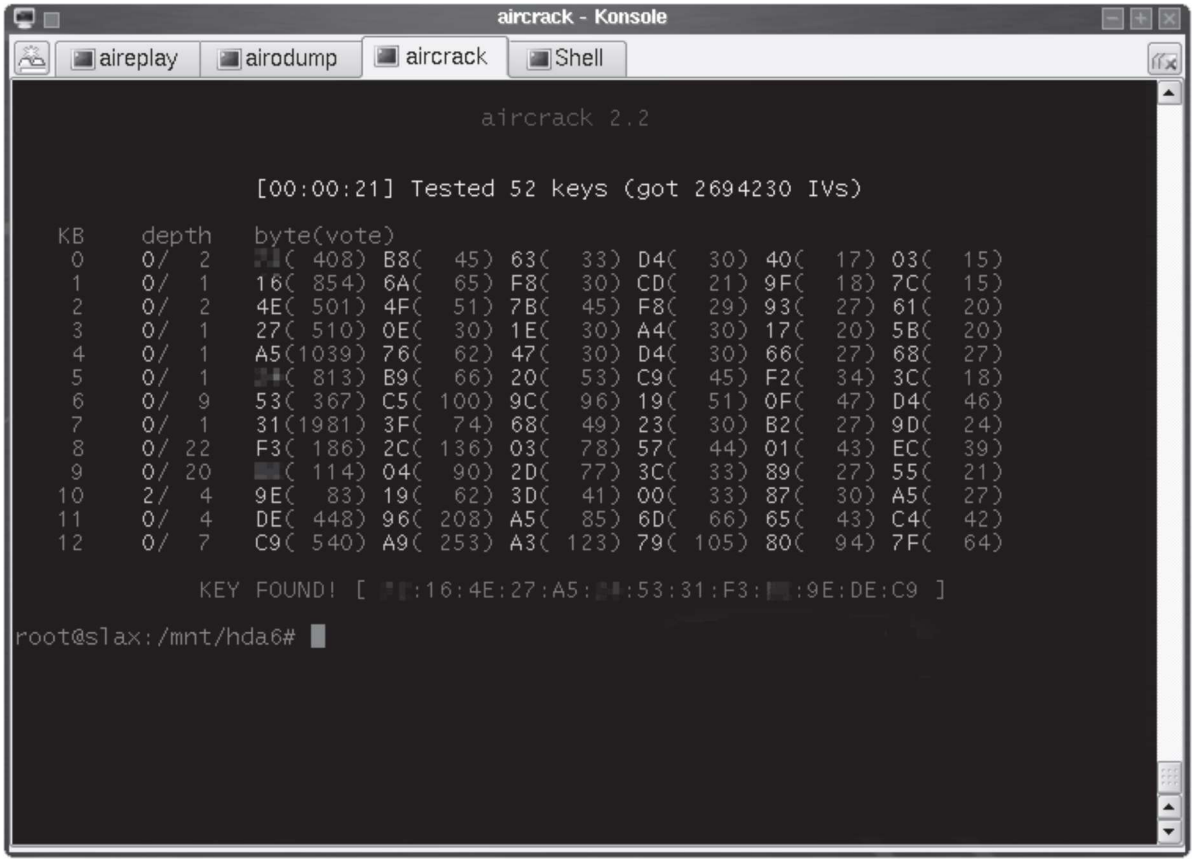
Η άλλη μορφή επιθέσεων δημιουργεί ενεργά κίνηση προς το σημείο πρόσβασης. Δημιουργώντας ενεργά ψευδή frames, ο επιτιθέμενος προσπαθεί να δημιουργήσει τα απαραίτητα πακέτα και την απαιτούμενη ποσότητα πακέτων. Αυτό γίνεται με τη δημιουργία ψευδών frames ελέγχου ταυτότητας και κατάργησης ταυτότητας προς το σημείο πρόσβασης. Με αυτόν τον τρόπο είναι δυνατή η εξαπάτηση του σημείου πρόσβασης για τη δημιουργία πακέτων ελέγχου ταυτότητας και κατάργησης ταυτότητας. Ο καλύτερος τρόπος πρόληψης από αυτού του τύπου επίθεσης είναι η αλλαγή του τύπου κρυπτογράφησης από WEP ή WPA σε LEAP ή PEAP.



Εικόνα 11: Ενεργή επίθεση (1)



Εικόνα 12: Ενεργή επίθεση (2)



Εικόνα 13: Σπάσιμο κλειδιού

3. Μελέτη επιθέσεων

3.1 Syslog server και syslog clients

Το βασικότερο εργαλείο και το πιο απαραίτητο σε δικτυακές υποδομές είναι η αποθήκευση και διατήρηση αρχείων καταγραφής από τις συσκευές. Στα αρχεία αυτά καταγράφονται όλες οι ενέργειες, αλλαγές και συνδέσεις που γίνονται στο συγκεκριμένο σύστημα, είτε αλλαγές που σχετίζονται με αυτό. Τα αρχεία καταγραφής μπορεί να αποθηκευτούν αυτόματα σε διαφορετικά μέσα ή ακόμα και στα ίδια τα μηχανήματα. Η αποθήκευση τοπικά στα μηχανήματα δεν θεωρείται ιδανική λύση για δύο λόγους. Ο πρώτος είναι πως αν κάποιος επιτεθεί στο μηχάνημα μπορεί να τα διαστρεβλώσει και ο δεύτερος είναι πως τις περισσότερες φορές οι συσκευές αυτού του τύπου δεν έχουν υψηλά μεγέθη χωρητικότητας, με αποτέλεσμα να μην μπορούν να διατηρήσουν αρχεία καταγραφής για μεγάλο χρονικό διάστημα χωρίς να χρειαστεί να σβήσουν παλαιότερα. Η λύση που προτείνεται από όλους τους κατασκευαστές είναι η χρήση των λεγόμενων syslog server. Οι syslog servers είναι δομημένοι για να μπορούν να διατηρούν πληθώρα αρχείων καταγραφών κατηγοριοποιημένα ανάλογα με την συσκευή. Στο κομμάτι που θα πρέπει να δοθεί έμφαση από τους διαχειριστές

συστημάτων είναι η συχνή εξαγωγή back ups ώστε σε περίπτωση τεχνικού προβλήματος ή επίθεσης στον server, να μπορούν να τον επαναφέρουν άμεσα με τις λιγότερες δυνατές απώλειες.

3.2 SNMP traps tools

Το SNMP (Simple Network Management Protocol) είναι ένα πρωτόκολλο που η λειτουργία του είναι η ανταλλαγή πληροφοριών μεταξύ συσκευών για την ευκολότερη διαχείριση των δικτυακών υποδομών. Παρέχει πληροφορίες στους διαχειριστές σχετικά με την απόδοση των δικτυακών πόρων, των υπολογιστικών συστημάτων, την ζωτικότητα των συσκευών, ακόμα και πληροφορίες για την επεκτασιμότητα του. Μέχρι σήμερα έχουν αναπτυχθεί τρεις εκδόσεις του συγκεκριμένου πρωτοκόλλου: το SNMPv1, το SNMPv2 και το SNMPv3.

Όλες οι εκδόσεις βασίζονται στον ίδιο κορμό αρχιτεκτονικής του πρωτοκόλλου. Ο κορμός αποτελείται από τους managers, τους agents και τις βάσεις πληροφοριών διαχείρισης. Σε κάθε δίκτυο που τρέχει το SNMP θα πρέπει να βρίσκεται εγκατεστημένος ένας manager όπου θα έχει δικαιώματα συλλογής πληροφοριών από τις βάσεις πληροφοριών. Οι συσκευές που θα παρακολουθούνται από το πρωτόκολλο έχουν εγκατεστημένο έναν SNMP agent ο οποίος είναι συνδεδεμένος με μία τοπική βάση πληροφοριών. Οι πληροφορίες καταγράφονται στην τοπική βάση και μετά ο agent είναι υπεύθυνος να επικοινωνήσει με τον manager και να του αποστείλει όλα τα δεδομένα που αναγράφονται στην τοπική βάση. Οι πληροφορίες που ζητάει ο manager δεν είναι προκαθορισμένες. Μπορεί κάθε φορά, με κατάλληλες ρυθμίσεις που ορίζονται από τον διαχειριστή, να ζητήσει διαφορετικού είδους πληροφορίες ανάλογα με τις ανάγκες του. Επιπρόσθετα, εκτός από πληροφορίες ο manager έχει την δυνατότητα να δημιουργεί κάποια σετ ρυθμίσεων και να τα αποστέλλει στις συσκευές. Για παράδειγμα ένα σετ ρυθμίσεων μπορεί να προκαλέσει επανεκκίνηση σε μία δικτυακή συσκευή ή έναν διακομιστή. Οι δύο βασικές εντολές των σετ ρυθμίσεων είναι η ‘get’ και η ‘set’.

Οι managers δεν μπορούν να στείλουν εντολές ή αιτήματα σε όλους τους agents. Για να υπάρχει μοναδική επικοινωνία μεταξύ τους, χρησιμοποιούν τα λεγόμενα community strings. Τα community strings είναι συμβολοσειρές κειμένου που επικυρώνουν τα μηνύματα μεταξύ ενός manager και των agents με στόχο την πρόσβαση στα δεδομένα των βάσεων πληροφορίων. Τα είδη των community strings είναι τα read-only community strings και τα read-write community strings.

- Read only community strings: Παρέχουν πρόσβαση μόνο για ανάγνωση σε όλα τα δεδομένα των βάσεων πληροφοριών, εκτός των community strings.

- Read-write community strings: Παρέχουν δικαιώματα εγγραφής-ανάγνωσης στα δεδομένα των βάσεων πληροφοριών, εκτός από τα community strings.

Επομένως, αν ένας manager αποστείλει ένα σωστό read-only community string μπορεί να διαβάσεις πληροφορίες από την βάση χωρίς να ορίσει ρυθμίσεις σε έναν agent. Από την άλλη πλευρά, στέλνοντας ένα σωστό read-write community string, ο manager μπορεί να αλλάξει και τις ρυθμίσεις ενός agent.

Το στοιχείο που θέλει προσοχή κατά την εγκατάσταση του SNMP στο δίκτυο είναι ο ορισμός των community strings. Συνήθως η προεπιλεγμένη τιμή του, που είναι ευρέως γνωστή, είναι η λέξη public. Αν ο υπεύθυνος εγκατάστασης δεν αλλάξει την συμβολοσειρά, ο οποιοσδήποτε γνώστης του default community string με μία εγκατάσταση ενός snmp manager θα μπορεί να επικοινωνήσει με όλους τους agents του δικτύου. Μερικές συσκευές στις βάσεις τους διατηρούν πολύ κρίσιμες πληροφορίες που αν βρεθούν στην κατοχή υποψήφιων επιτιθέμενων, μπορεί να προκληθεί μεγάλη ζημιά στην δικτυακή υποδομή. Για αυτό συνίσταται να αλλάζουν πάντα τα community strings κατά την αρχική εγκατάσταση.

Οι εκδόσεις SNMPv1 και SNMPv2 παρουσιάζουν την ευπάθεια πως αποστέλλουν τα community strings σε μορφή αναγνώσιμου κειμένου. Αυτό το θέμα ήρθε να το λύσει η έκδοση SNMPv3 το οποίο πιστοποιεί και κρυπτογραφεί τα SNMP πακέτα. Οι επιπρόσθετες δυνατότητες που προσφέρει είναι:

- Πιστοποίηση: Εξακριβώνει πως το πακέτο παραλαμβάνεται από έγκυρο αποστολέα.
- Κρυπτογράφηση: Κρυπτογραφεί τα πακέτα ώστε να μην μπορούν να διαβαστούν από μη εξουσιοδοτημένους παραλήπτες.
- Ακεραιότητα: Διασφάλισης μη διαστρέβλωσης μηνύματος κατά την μεταφορά του στο δίκτυο.
- Έλεγχος πρόσβασης: Περιορίζει τις ενέργειες σε συγκεκριμένους πόρους.

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

Η ανάπτυξη των δικτύων και η ανάγκη για επεκτασιμότητα, είχε ως αποτέλεσμα την δυσκολία ανάγνωσης πολλαπλών αρχείων καταγραφών από τους διαχειριστές. Επίσης, ο χρόνος που ξοδεύονταν ακολουθώντας μη αυτόματες διαδικασίες ήταν υπερβολικά πολύς. Τα εργαλεία που αναπτύχθηκαν για να προσπεραστούν αυτές οι δυσκολίες είναι τα λεγόμενα Συστήματα Ανίχνευσης Εισβολών (IDS).

Τα IDS είναι μία τεχνολογία προστασίας των δικτύων από ευπάθειες και παρέχουν την δυνατότητα γρήγορης ανταπόκρισης σε περιπτώσεις πλαστών, μη εξουσιοδοτημένων πακέτων που προσπαθούν να μολύνουν το δίκτυο. Το σύστημα καταγράφει όλη την εισερχόμενη και εξερχόμενη κίνηση και εκδίδει μία ειδοποίηση στον διαχειριστή σε περίπτωση που η συμπεριφορά της κίνησης αποκλίνει από κάποιο μοτίβο. Με αυτόν τον τρόπο γίνεται πρόληψη για πιθανές μελλοντικές απειλές εισβολής σε πρώιμο στάδιο, προσφέροντας περισσότερο χρόνο αντίδρασης στους διαχειριστές των δικτύων. Ωστόσο το IDS σύστημα θα πρέπει να είναι σωστά εγκατεστημένο, με σωστά δικαιώματα στο δίκτυο και με δυνατότητες επεκτασιμότητας, γιατί σε αντίθετες περιπτώσεις θα οδηγηθεί σε έκδοση εσφαλμένων συναγερμών.

Τα IDS συστήματα αναζητούν γνωστές υπογραφές επιθέσεων ή μη φυσιολογικές αποκλίσεις από τους καθορισμένους κανόνες. Τα αποκληθέντα μοτίβα κίνησης του δικτύου στέλνονται στην στοίβα για περαιτέρω διερεύνηση στα επίπεδα πρωτοκόλλου και εφαρμογής του μοντέλου OSI (Open Systems Interconnection). Τα συστήματα δεν τοποθετούνται ανάμεσα σε πραγματική επικοινωνία ενός αποστολέα και ενός παραλήπτη, αντίθετα χρησιμοποιούν κάποιες τεχνικές και αναλύουν ένα αντίγραφο της κίνησης του δικτύου. Με αυτές τις τεχνικές τα IDS προλαμβάνουν αποτελεσματικά την μόλυνση του δικτύου ή των δικτυακών συσκευών από κακόβουλες ενέργειες.

Οι τεχνικές στις οποίες βασίζονται τα IDS συστήματα, τα κατηγοριοποιούν αναλόγως:

- Σύστημα Ανίχνευσης Εισβολής Δικτύου (NIDS): Τα NIDS συστήματα είναι ανεπτυγμένα σε στρατηγικά σημεία του δικτύου, όπως για παράδειγμα στα υποδίκτυα που είναι πιθανότερο να τους επιτεθούν. Τα συστήματα αυτά παρακολουθούν όλη την εισερχόμενη και εξερχόμενη κίνηση από και προς τις δικτυακές συσκευές.

- Σύστημα ανίχνευσης εισβολής τερματικών (HIDS): Το HIDS είναι διαμορφωμένο σε όλους τους hosts οι οποίοι βρίσκονται μέσα στο δίκτυο. Παρακολουθούν την εισερχόμενη και εξερχόμενη κίνηση από το συγκεκριμένο τερματικό και προλαμβάνουν την μόλυνση άλλων υπολογιστών μέσω αυτού. Η ανίχνευση σε επίπεδο τερματικών, δεν μπορεί να επιτευχθεί από το NIDS.

- Σύστημα ανίχνευσης εισβολής που βασίζεται σε ανωμαλίες (AIDS): Τα συστήματα αυτά διαβάζουν την εισερχόμενη και εξερχόμενη κίνηση του

δικτύου, έπειτα την συγκρίνουν με κάποια υποδείγματα συμπεριφοράς κίνησης που γνωρίζει το λογισμικό και σε περίπτωση που διαπιστωθεί ανώμαλη συμπεριφορά ενημερώνουν τον διαχειριστή.

- Σύστημα ανίχνευσης εισβολής με βάση την υπογραφή (SIDS): Τα συστήματα αυτά διατηρούν μία ενσωματωμένη βάση υπογραφών, ή ιδιότητες που επιδεικνύονται από γνωστές εισβολές και ελέγχουν την δικτυακή κίνηση με βάση αυτό το κριτήριο. Αν ανακαλύψουν τις ίδιες υπογραφές στα δεδομένα που μεταφέρονται μέσα στο δίκτυο προβαίνουν στις ενέργειες που έχουν οριστεί από τον διαχειριστή.

Τα συστήματα πρόληψης εισβολών (IPS) βασίζονται στην τεχνολογία IDS. Τοποθετούνται σε σημεία πραγματικής ροής των δεδομένων δικτύου και ελέγχουν την κίνηση πριν την αφήσουν να περάσει σε έμπιστα υποδίκτυα. Έχουν την δυνατότητα εντοπισμού και άμεσης αντιμετώπισης εισβολών και κακόβουλων ενεργειών. Η ανάλυση ξεκινά από τα Layer3 και Layer4 των πακέτων και φτάνει μέχρι το Layer7. Τα περισσότερα IPS χρησιμοποιούν μία μίξη τεχνολογιών ανίχνευσης το οποίο τα καθιστά άκρως αποτελεσματικά και ταυτόχρονα πολύπλοκα. Όταν τα πακέτα προσπαθούν να περάσουν από μία διεπαφή IPS, το πακέτο δεν περνάει την διεπαφή εάν δεν έχει αναλυθεί πλήρως. Με αυτό τον τρόπο επιτυγχάνεται η πρόληψη από επιθέσεις μονού πακέτου αλλά ταυτόχρονα αυξάνεται η πολυπλοκότητα της υποδομής, εφόσον μία άστοχη εγκατάσταση IPS διεπαφών μπορεί να επηρεάσει σε μεγάλο βαθμό την συνολική απόδοση του δικτύου. Η μεγάλη διαφορά των IPS με τα IDS συστήματα είναι πως τα IPS μπορούν να σταματήσουν κακόβουλο πακέτο σε πραγματικό χρόνο, κάτι το οποίο τα IDS συστήματα δεν δύναται να το κάνουν.

Τα πλεονεκτήματα των IPS πλατφορμών είναι τα εξής:

- Έχουν την δυνατότητα να μπλοκάρουν κίνηση σε πραγματικό χρόνο προσθέτοντας ακόμα και φίλτρα που με βάση αυτά θα πραγματοποιείται το μπλοκάρισμα.

- Χρησιμοποιούν την κανονικοποίηση του ρεύματος για την μείωση ή εξάλειψη δυνατοτήτων υπεκφυγής ασφαλείας στο δίκτυο.

4. Προσομοιωτές δικτύων

Η εικονική αναπαράσταση ενός δικτύου ονομάζεται προσομοίωση δικτύου. Οι κύριοι τρόποι υλοποίησης προσομοιώσεων δικτύων είναι δύο. Ο πρώτος αφορά την υλοποίηση σε υπάρχοντα δίκτυα και ο δεύτερος στον σχεδιασμό δικτύων πριν την τελική κατασκευή τους. Ο σκοπός της προσομοίωσης κατά τον πρώτο τρόπο είναι η εύρεση προβλημάτων σε υπάρχοντα δίκτυα, ενώ ο σκοπός του δευτέρου τρόπου είναι ο εντοπισμός απροσδόκητων αλληλεπιδράσεων σε ένα δίκτυο που θα δημιουργηθεί μελλοντικά. Με τα εργαλεία αυτά οι οργανισμοί καταφέρνουν την αποφυγή προβλημάτων και βελτίωση της αξιοπιστίας των δικτύων τους, με ταυτόχρονη μείωση του κόστους συντήρησης τους.

Η ιδέα της προσομοίωσης δικτύων ξεκίνησε με την ανάπτυξη των δικτύων υπολογιστών μεγάλης κλίμακας. Οι ερευνητές δεν είχαν πλήρη εικόνα για την επίδοση των δικτύων αυτού του τύπου, οπότε με τις προσομοιώσεις που υλοποιούσαν προσπαθούσαν να εντοπίσουν το κατάλληλο υλικό για την ανάπτυξη των δικτύων τους. Με τον καιρό διαπιστώθηκε πως οι προσομοιώσεις μπορούν να φανούν χρήσιμες και μετά την ανάπτυξη των δικτύων, με στόχο τον εντοπισμό τυχόν προβλημάτων.

Οι προσομοιώσεις που υλοποιούνται πριν την δημιουργία του δικτύου ονομάζονται γεννήτριες κίνησης. Χρησιμοποιούν μαθηματικούς αλγορίθμους για να παραστήσουν τον τρόπο που θα συμπεριφερόταν ένα δίκτυο αν υλοποιούταν. Προφανώς θα πρέπει να δοθούν πλήρη στοιχεία στον αλγόριθμο σαν είσοδο, όπως ο εξοπλισμός του δικτύου, οι χρήστες του δικτύου και ο τρόπος λειτουργίας του.

Οι πιο ακριβείς προσομοιώσεις είναι αυτές που υλοποιούνται μετά την δημιουργία του δικτύου. Συγκεκριμένα λογισμικά που τρέχουν στο δίκτυο εντοπίζουν όλους τους φυσικούς πόρους και την χρήση που γίνεται από τους δικτυακούς χρήστες. Στην συνέχεια, διαφορετικά λογισμικά δέχονται ως είσοδο αυτήν την πληροφορία και δημιουργούν μία αποτύπωση του δικτύου η οποία μοιάζει με οδικό χάρτη. Στον χάρτη αυτό αποτυπώνονται όλα τα σημεία που έχουν αυξημένη χρήση πόρων, τα μοτίβα χρήσης των χρηστών και το πως μπορεί να βελτιωθεί η συμπεριφορά του δικτύου. Οι ανεπάρκειες που εντοπίζει το λογισμικό μπορεί να προκαλούν σφάλματα στο δίκτυο και επιβράδυνση της απόδοσης του. Μία επιπρόσθετη παρατήρηση είναι ότι πολλές φορές δεσμεύεται το εργατικό δυναμικό να ασχολείται με αυτά τα σφάλματα ενώ θα μπορούσε κάλλιστα να ασχολείται με άλλα ζητήματα.

Το κέρδος σε χρηματικό όφελος των οργανισμών που χρησιμοποιούν προσομοιωτές δικτύων είναι διπλό. Πρώτον, οι εργαζόμενοι λαμβάνουν τις πληροφορίες που χρειάζονται αυτοματοποιημένα και κυρίως την ώρα που τις χρειάζονται. Δεύτερον, μειώνουν το απαιτούμενο έργο από την πλευρά του προσωπικού από την στιγμή που τα αποτελέσματα φτάνουν στους εργαζομένους αυτοματοποιημένα. Αυτό έχει ως συνέπεια την απελευθέρωση του προσωπικού από

την παρακολούθηση του δικτύου, δίνοντας τους την ευχέρεια να ασχοληθούν με άλλα κομμάτια μέσα στο εργασιακό τους ωράριο.

4.1 Τύποι προσομοιωτών δικτύων

Παρακάτω φαίνεται μία λίστα με τους τύπους προσομοιωτών δικτύων που μπορεί κάποιος να βρει στο διαδίκτυο. Όλοι είναι ανοιχτού κώδικα, το οποίο σημαίνει ότι μπορεί να γίνει χρήση τους χωρίς καμία απολύτως χρέωση.

- Network Simulator version 2 (NS-2)
- Ns3
- Netkit
- Marionnet
- JSIM (Java-based Simulation)
- OPNET
- QualNet
- The open-source simulators are Marrionet, Netkit, NS2, JSIM
- The commercial simulators are OPNET and QualNet

Network Simulator Έκδοση 2 (NS-2)

Αντικειμενοστραφής προσομοιωτής που χρησιμοποιείται για την προσομοίωση πρωτοκόλλων δικτύωσης σε ενσύρματα και ασύρματα δίκτυα. Υλοποιείται με OTCI και C++.

Ns3

Προσομοιωτής με σκοπό την έρευνα και την εκπαίδευση. Ειδοποιός διαφορά με τον προσομοιωτή Ns2 είναι πως υλοποιείται με Python. Τα modules που μπορεί να εισάγει ο χρήστης είναι γραμμένα σε γλώσσες C++, Python, Netki.

Netki

Προσομοιωτής γραμμένος για λειτουργικό σύστημα Linux. Η χρήση του γίνεται μέσω γραμμής εντολών και είναι ιδανικός για την δημιουργία ενός δικτύου με σχεδόν μηδαμινή προσπάθεια από τον τελικό χρήστη.

Marionnet

Βασικός σκοπός χρήσης του είναι η εκπαίδευση, λόγω της έξυπνης γραφικής διεπαφής με τον χρήστη.

JSIM

Χρησιμοποιείται σε web-based προσομοιώσεις και στοχεύει στην επεξεργασία και ανάλυση πακέτων. Τα αποτελέσματα του πειράματος αναλύονται και συγκρίνονται με κάποια ποσοτικά αριθμητικά μοντέλα.

OPNET

Χρησιμοποιείται στην έρευνα και την ανάπτυξη παρέχοντας πλήρη ευελιξία σε μελέτες δικτύων επικοινωνίας, πρωτόκολλα και εφαρμογές. Όταν συνδυαστεί με προγραμματισμό, παρέχει στον χρήστη την δυνατότητα δημιουργίας δικτύου on demand.

QualNet

Χρησιμοποιείται από μελετητές και μηχανικούς για την κατασκευή εικονικών μοντέλων όλων των ειδών των δικτύων. Μπορεί και υποδηλώνει την κατάσταση του δικτύου με απόλυτη ακρίβεια ανά πάσα στιγμή.

5. Sandbox

Στον τομέα της κυβερνοασφάλειας ως sandbox ορίζεται ένα απομονωμένο περιβάλλον στο οποίο μπορεί να εκτελεστεί ένα πιθανά βλαβερό κομμάτι κώδικα χωρίς να μολύνει κανένα πόρο του δικτύου και καμία εφαρμογή. Οι ερευνητές στην κυβερνοασφάλεια κάνουν χρήση sandboxes για να τρέχουν ύποπτες εφαρμογές και τμήματα κώδικα από άγνωστες πηγές και URLs, με σκοπό την παρατήρηση της συμπεριφοράς του απομονωμένου δικτύου σε όλα τα επίπεδα. Εφόσον το περιβάλλον παρατήρησης είναι πλήρως απομονωμένο, οι ομάδες έρευνας μπορούν να επεξεργαστούν τις ύποπτες συμπεριφορές στο έπακρο χωρίς φόβο πρόκλησης κάποιου προβλήματος. Ακόμα και σε περιπτώσεις που ο κώδικας προσπαθεί να επικοινωνήσει προς τα έξω ή να κατεβάσει πρόσθετο λογισμικό, δεν το επιτρέπει το sandbox περιβάλλον από τη στιγμή που η βασική του αρχή είναι η πλήρη απομόνωση από άλλα περιβάλλοντα. Σε τομείς εκτός κυβερνοασφάλειας τα sandboxes χρησιμοποιούνται από προγραμματιστές για να ελέγχουν τους κώδικες που αναπτύσσουν πριν τους

εγκαταστήσουν σε διακομιστές της παραγωγής.

5.1 Ποιος ο σκοπός ενός Sandbox;

Σε ένα τυπικό περιβάλλον επιχειρηματικής παραγωγής, ένα sandbox μπορεί να παρεξηγηθεί ή να θεωρηθεί περιττό κόστος. Αλλά τα sandbox είναι κρίσιμα για πολλά σενάρια στην ανάπτυξη, την ασφάλεια στον κυβερνοχώρο και την έρευνα. Η βεβαίωση ότι το sandbox περιβάλλον είναι πραγματικά απομονωμένο είναι σημαντικότερη στον χώρο της κυβερνοασφάλειας από την έρευνα ανάπτυξης λογισμικού, επειδή ο κώδικας σαρώνει επιθετικά αναζητώντας εκμεταλλεύσιμα τρωτά σημεία.

Κατά την ανάπτυξη, ένα sandbox συνήθως περιλαμβάνει έναν διακομιστή ανάπτυξης και έναν διακομιστή σταδιοποίησης. Ο διακομιστής ανάπτυξης είναι διαχωρισμένος από το περιβάλλον παραγωγής, αλλά ενδέχεται να εξακολουθεί να απαιτεί βασική πρόσβαση στο δίκτυο. Οι προγραμματιστές χρησιμοποιούν αυτόν τον διακομιστή για να ανεβάσουν κώδικα και να τον δοκιμάσουν καθώς αλλάζει η δομή του. Ο διακομιστής σταδιοποίησης έχει σχεδιαστεί για να είναι ένα ακριβές αντίγραφο της παραγωγής. Αυτός ο διακομιστής είναι όπου η διασφάλιση ποιότητας (QA) ελέγχει τον κώδικα πριν από την ανάπτυξη στην παραγωγή. Επειδή το περιβάλλον σταδιοποίησης είναι το ίδιο με το περιβάλλον παραγωγής, ο κώδικας που εκτελείται χωρίς προβλήματα στη σταδιοποίηση θα πρέπει να εκτελείται χωρίς προβλήματα στην παραγωγή. Αφού δοκιμαστεί ο κώδικας, εγκαθίσταται στην παραγωγή.

Οι ερευνητές και οι αναλυτές στον τομέα της κυβερνοασφάλειας χρησιμοποιούν το περιβάλλον sandbox τους με παρόμοιο τρόπο. Σε αυτόν τον τρόπο χρήσης είναι πολύ πιο σημαντικό να διασφαλιστεί ότι δεν υπάρχουν πόροι δικτύου που πιθανώς να μολυνθούν από κακόβουλο λογισμικό. Το περιβάλλον sandbox έχει το δικό του δίκτυο και συχνά δεν έχει φυσική σύνδεση με πόρους παραγωγής. Ο σκοπός του sandbox είναι να εκτελέσει κακόβουλο κώδικα και να τον αναλύσει. Μερικές φορές, αυτός ο κώδικας θα μπορούσε να είναι μια εκμετάλλευση μηδενικής ημέρας όπου η επίδραση του κακόβουλου λογισμικού και το ωφέλιμο φορτίο είναι άγνωστα. Εξαιτίας αυτού, το sandbox δεν πρέπει να έχει πρόσβαση σε κρίσιμες υποδομές. Με ένα sandbox, οι ερευνητές και οι αναλυτές της κυβερνοασφάλειας μπορούν να κατανοήσουν τον τρόπο λειτουργίας του κακόβουλου λογισμικού και τι απαιτείται να συμβεί για να το σταματήσει. Αυτό είναι το πρώτο βήμα στο σχεδιασμό λογισμικού προστασίας από ιούς για να σταματήσει η εξάπλωση κακόβουλου λογισμικού σε άλλους πόρους και να αφαιρεθεί από τα ήδη μολυσμένα συστήματα. Για πολύπλοκες επιθέσεις, τα περιβάλλοντα sandbox είναι άμεσα διαθέσιμα για γρήγορη ανάλυση κακόβουλου λογισμικού και διακοπή του προτού γίνει μεγάλο ζήτημα. Το ransomware, για παράδειγμα, μπορεί να εξαπλωθεί παγκοσμίως και να καταστρέψει κρίσιμα

κυβερνητικά συστήματα. Αυτό καθιστά σημαντικό για τους ερευνητές να έχουν έτοιμα πλαίσια πρόσβασης για να το σταματήσουν.

5.2 Πώς λειτουργεί ένα sandbox;

Ανεξάρτητα με τον σκοπό χρήσης του sandbox, υπάρχουν κάποια κοινά βασικά χαρακτηριστικά για όλα τα περιβάλλοντα. Αυτά είναι τα εξής:

- Προσομοίωση μιας πραγματικής συσκευής. Αυτό θα μπορούσε να είναι προσομοίωση επιτραπέζιου ή κινητής συσκευής. Σε κάθε περίπτωση, η εφαρμογή που ελέγχεται πρέπει να έχει πρόσβαση στους ίδιους πόρους με τον κώδικα που αναλύεται, συμπεριλαμβανομένης της CPU, της μνήμης και της αποθήκευσης.

- Εξομοίωση του λειτουργικού συστήματος στόχου. Χρησιμοποιώντας μια εικονική μηχανή, η εφαρμογή πρέπει να έχει πρόσβαση στο λειτουργικό σύστημα. Με μια εικονική μηχανή, το sandbox είναι απομονωμένο από το υποκείμενο φυσικό υλικό, αλλά έχει πρόσβαση στο εγκατεστημένο λειτουργικό σύστημα.

- Εικονικό περιβάλλον. Συνήθως, ένα sandbox βρίσκεται σε μια εικονική μηχανή, έτσι ώστε να μην έχει πρόσβαση σε φυσικούς πόρους, αλλά να έχει πρόσβαση σε εικονικό υλικό.

Τα βασικά όπλα του sandbox, η εικονικοποίηση και εξομοίωση, δεν είναι ανυπέρβλητα. Ορισμένοι προγραμματιστές αναπτύσσουν κακόβουλα λογισμικά τα οποία είναι σχεδιασμένα να παραμένουν ανενεργά όταν αντιληφθούν πως τρέχουν σε sandbox περιβάλλοντα. Ο τρόπος αντίληψης ενός sandbox περιβάλλοντος από ένα κακόβουλο λογισμικό μπορεί να περιλαμβάνει την αναζήτηση τρόπους αλληλεπιδράσεων χρηστών που δεν συνάδει με αυτούς σε πραγματικά περιβάλλοντα. Ακόμα, κάποιοι ρυθμίζουν τα κακόβουλα λογισμικά έτσι ώστε να ελέγχουν συγκεκριμένες ρυθμίσεις που χαρακτηρίζουν τις εικονικές μηχανές και σε περίπτωση που τις αντιληφθούν να μένουν ενεργά. Ενεργοποιούνται μόνο όταν βρεθούν σε έναν πραγματικό φυσικό στόχο. Τέλος κάποιοι προσπαθούν να εξελίξουν τα κακόβουλα λογισμικά ακόμη περισσότερο προσπαθώντας να ελέγξουν αν το sandbox περιβάλλον είναι ασθενές με σκοπό να το βλάψουν όσο το δυνατόν περισσότερο.

5.3 Οφέλη χρήσης sandbox

Όπως ένα περιβάλλον δοκιμών ανάπτυξης, ένα sandbox μπορεί να χρησιμοποιηθεί για την εκτέλεση οποιασδήποτε εφαρμογής σε έναν ασφαλή πόρο προτού αυτή αναπτυχθεί στην παραγωγή ή της δοθεί πρόσβαση σε πόρους παραγωγής. Ένα sandbox επιτρέπει στους οργανισμούς να εκτελούν προγράμματα που θα μπορούσαν ενδεχομένως να προκαλέσουν προβλήματα, είτε από κακόβουλο λογισμικό είτε από ακούσια ελαττώματα λογισμικού, χωρίς να κολλήσουν ή να βλάψουν κρίσιμους πόρους για τις επιχειρήσεις. Ένα sandbox χρησιμοποιείται συχνά ως καραντίνα για άγνωστα email και συνημμένα. Τα φίλτρα email θα εντοπίσουν πιθανά κακόβουλα μηνύματα email και συνημμένα, αλλά ένας διαχειριστής χρειάζεται ένα ασφαλές μέρος για να τα δει και να εντοπίσει ψευδώς θετικά στοιχεία. Τα κακόβουλα έγγραφα ενδέχεται να περιέχουν μακροεντολές που εκμεταλλεύονται ελαττώματα σε δημοφιλείς εφαρμογές παραγωγικότητας, όπως για παράδειγμα το Microsoft Office. Ένας διαχειριστής μπορεί να χρησιμοποιήσει μια εικονική μηχανή sandbox για να ανοίξει συνημμένα και να προβάλει τις μακροεντολές για να δει εάν είναι ασφαλείς. Για οργανισμούς που δεν διαθέτουν εξειδικευμένο προσωπικό ασφάλειας στον κυβερνοχώρο, ένα sandbox μπορεί να χρησιμοποιηθεί από οποιονδήποτε υπάλληλο για την απομόνωση ύποπτων προγραμμάτων. Ένα sandbox μπορεί να επιτρέπει στους εργαζόμενους να εκτελούν άγνωστο κώδικα χωρίς να εκθέτουν τα συστήματά τους σε νέες απειλές.

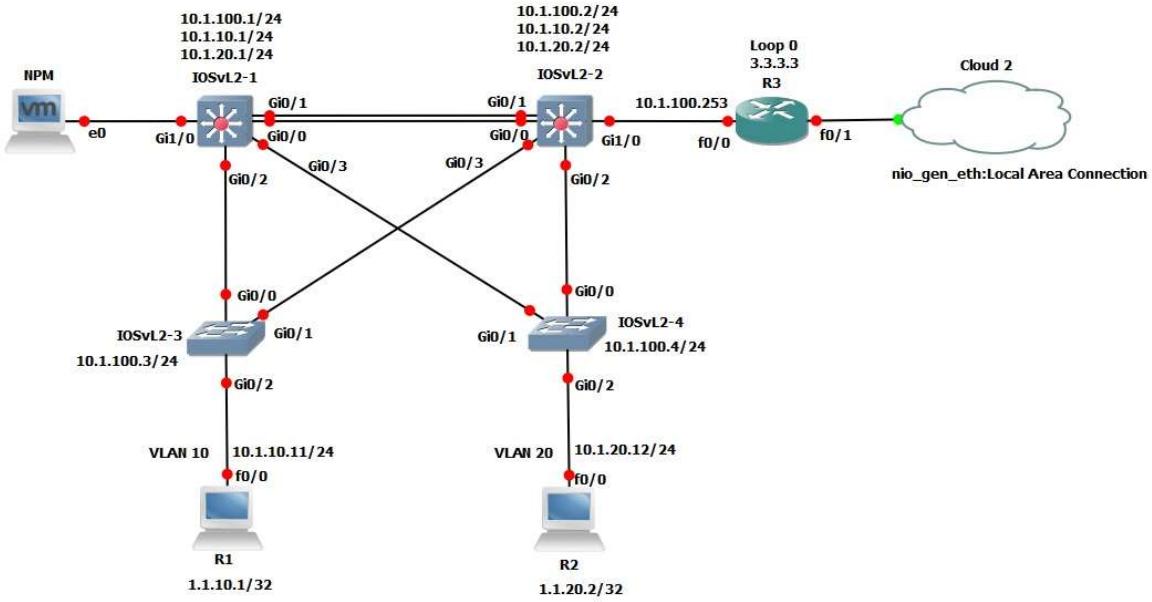
6. Προσομοιωτής δικτύων

Ο προσομοιωτής δικτύου που χρησιμοποιήθηκε για την υλοποίηση των σεναρίων είναι ο GNS3. Το GNS3 χρησιμοποιείται από εκατοντάδες χιλιάδες μηχανικούς δικτύου παγκοσμίως για την εξομοίωση, τη διαμόρφωση, τη δοκιμή και την αντιμετώπιση προβλημάτων εικονικών και πραγματικών δικτύων. Αναπτύσσεται ενεργά και υποστηρίζεται και έχει μια αυξανόμενη κοινότητα με περισσότερα από 800.000 μέλη. Το GNS3 έχει επιτρέψει στους μηχανικούς δικτύου να εικονικοποιούν πραγματικές συσκευές υλικού για περισσότερα από 10 χρόνια. Αρχικά, μιμούμενος μόνο συσκευές Cisco χρησιμοποιώντας λογισμικό που ονομάζεται Dynamips, το GNS3 έχει πλέον εξελιχθεί και υποστηρίζει πολλές συσκευές από πολλούς προμηθευτές δικτύου, όπως Cisco virtual switches, Cisco ASA, Brocade vRouters, Cumulus Linux switches, instances Docker, HPE VSR, πολλαπλές συσκευές Linux και πολλές άλλες.
Το GNS3 αποτελείται από δύο στοιχεία λογισμικού:

- Το λογισμικό GNS3-all-in-one (GUI)
- Η εικονική μηχανή GNS3 (VM)

6.1 GNS3-all-in-one

Αυτό είναι το τμήμα πελάτη του GNS3 και είναι γραφική διεπαφή χρήστη (GUI). Εγκαθιστάτε το λογισμικό all-in-one στον τοπικό σας υπολογιστή (Windows, MAC, Linux) και δημιουργείτε τις τοπολογίες σας χρησιμοποιώντας αυτό το λογισμικό. Αυτό είναι αυτό που συνήθως βλέπετε να εμφανίζεται σε στιγμιότυπα οθόνης όπως τα παρακάτω:



Εικόνα 14: Στιγμιότυπο GNS3

6.2 GNS Server

Όταν δημιουργείτε τοπολογίες στο GNS3 χρησιμοποιώντας τον πελάτη GUI λογισμικού all-in-one, οι συσκευές που δημιουργούνται πρέπει να φιλοξενούνται και να εκτελούνται από μια διαδικασία διακομιστή. Έχετε μερικές επιλογές για το τμήμα διακομιστή του λογισμικού:

1. Local GNS3 server
2. Local GNS3 VM
3. Remote GNS3 VM

Ο τοπικός διακομιστής GNS3 εκτελείται τοπικά στον ίδιο υπολογιστή όπου εγκαταστήσατε το λογισμικό GNS3 all-in-one. Εάν για παράδειγμα χρησιμοποιείτε υπολογιστή με Windows, τόσο το GNS3 GUI όσο και ο τοπικός διακομιστής GNS3 εκτελούνται ως διεργασίες στα Windows. Επιπλέον διεργασίες όπως το Dynamips θα εκτελούνται επίσης στον υπολογιστή σας. Εάν αποφασίσετε να χρησιμοποιήσετε το GNS3 VM (συνιστάται), μπορείτε είτε να εκτελέσετε το GNS3 VM τοπικά στον υπολογιστή σας χρησιμοποιώντας λογισμικό εικονικοποίησης όπως το VMware Workstation, το Virtualbox ή το Hyper-V. ή μπορείτε να εκτελέσετε το GNS3 VM απομακρυσμένα σε διακομιστή χρησιμοποιώντας VMware ESXi ή ακόμα και στο cloud.

6.3 GNS3 Use Cases

Το GNS3 είναι ίσως πιο διάσημο ως πλατφόρμα που χρησιμοποιείται για μάθηση και διδασκαλία. Το GNS3 χρησιμοποιείται εδώ και χρόνια από φοιτητές και μηχανικούς δικτύων για να βοηθήσει στην εξάσκηση και στην προετοιμασία για εξετάσεις πιστοποίησης προμηθευτών, όπως η εξέταση Cisco CCNA. Το GNS3 μπορεί ωστόσο να χρησιμοποιηθεί για άλλες περιπτώσεις χρήσης, όπως απόδειξη ιδεών και εμπορικές επιδείξεις. Το GNS3 παρέχει έναν εύκολο, οικονομικά αποδοτικό τρόπο για νέο λογισμικό, όπως λογισμικό διαχείρισης ή SDN. Σας επιτρέπει να δοκιμάσετε τη διαλειτουργικότητα πολλών προμηθευτών χρησιμοποιώντας ένα περιβάλλον εικονικού εργαστηρίου αντί να απαιτείτε αποκλειστικό φυσικό εξοπλισμό. Μια ολόκληρη τοπολογία GNS3 μπορεί να δημιουργηθεί και να εκτελεστεί σε έναν μόνο φορητό υπολογιστή. Αυτό επιτρέπει στους μηχανικούς να επιδείξουν τοπολογίες και λογισμικό σε πελάτες και άλλους. Τα περιβάλλοντα της τάξης μπορούν επίσης να επωφεληθούν από ένα προδιαμορφωμένο εργαστηριακό περιβάλλον που χρησιμοποιούν οι μαθητές για να μάθουν έννοιες και τεχνολογίες δικτύωσης. Μερικοί επιπλέον λόγοι για να χρησιμοποιήσετε το GNS3:

- Προσομοίωση δικτύου σε πραγματικό χρόνο για δοκιμές πριν από την ανάπτυξη χωρίς την ανάγκη υλικού δικτύου. Εκτελέστε το λειτουργικό σύστημα που προσομοιώνει την πραγματική συμπεριφορά του δικτύου.

- Δοκιμάστε περισσότερα από είκοσι διαφορετικούς προμηθευτές δικτύου σε εικονικό ακίνδυνο περιβάλλον. Εκτελέστε γρήγορα και δοκιμάστε πολλούς προμηθευτές υλικού χωρίς την ανάγκη αγοράς.

- Δημιουργήστε δυναμικούς χάρτες δικτύου για αντιμετώπιση προβλημάτων και δοκιμές απόδειξης σεναρίων (proof of concept). Δοκιμάστε τα δίκτυά

σας προτού τα δημιουργήσετε για να μειώσετε τον χρόνο που χρειάζεται για να τεθεί σε λειτουργία ένα δίκτυο παραγωγής.

- Συνδέστε το GNS3 σε οποιοδήποτε πραγματικό δίκτυο. Αξιοποιήστε το υπάρχον υλικό σας και επεκτείνετε το τρέχον εργαστήριό σας συνδέοντας τις τοπολογίες GNS3 απευθείας σε αυτό.

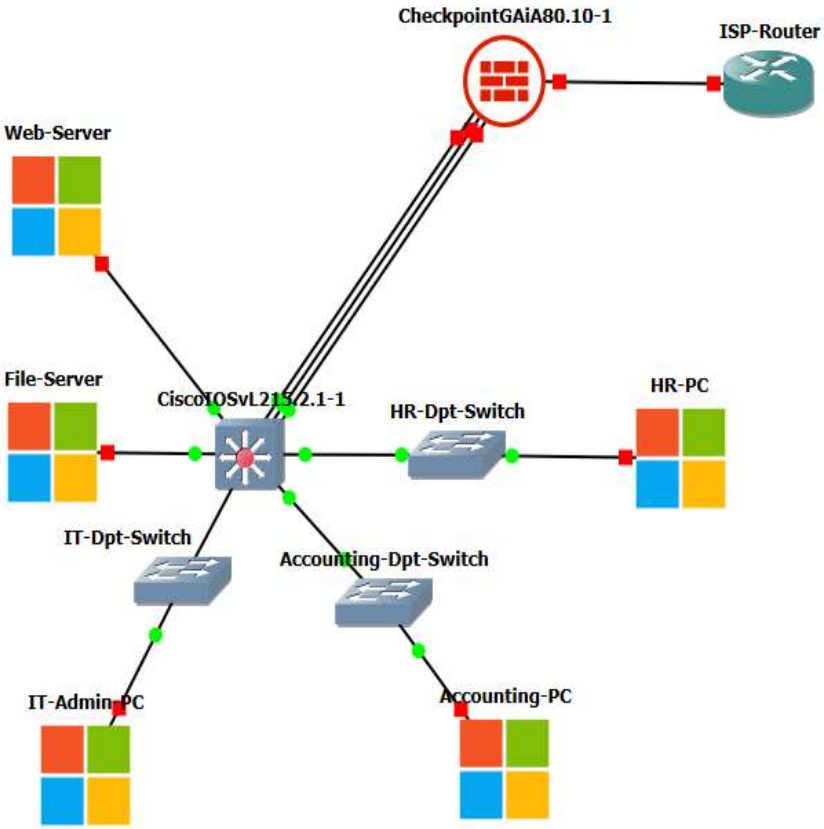
- Προσαρμοσμένες τοπολογίες και εργαστήρια εντός του GNS3 για εκπαίδευση πιστοποίησης δικτύου. Το GNS3 είναι το καλύτερο εργαλείο μελέτης για τους επίδοξους επαγγελματίες δικτυακών τεχνολογιών που αναζητούν τις πιστοποιήσεις τους, χωρίς την ανάγκη ανάπτυξης οικιακού εργαστηρίου.

6.4 Τοπολογία δικτύου

Ο σχεδιασμός της τοπολογίας του δικτύου εμπνεύστηκε από μία πραγματική υποδομή μίας εταιρίας. Είναι δεδομένο πως ο σκελετός μίας εταιρίας αποτελείται από περισσότερα τμήματα όμως από δικτυακής πλευράς, είτε υπάρχουν δύο τμήματα είτε περισσότερα, η λογική παραμένει η ίδια. Το σημαντικό είναι πως σε περιπτώσεις που απαιτείται πρόσθεση περισσότερων τμημάτων, να μπορεί να επιτευχθεί χωρίς να επηρεαστεί την υπάρχουσα υποδομή και την συνδεσιμότητα των χρηστών με τις ψηφιακές υπηρεσίες. Μία από τις αποδοτικότερες τοπολογίες για τις ανάγκες που αναφέρθηκαν παραπάνω είναι η τοπολογία αστέρα, η οποία χρησιμοποιήθηκε στην υλοποίηση της προσομοίωσης. Στην τοπολογία αστέρα κάθε δικτυακή συσκευή είναι συνδεδεμένη σε έναν κεντρικό κόμβο του δικτύου. Επομένως, κάθε πακέτο δεδομένων που έχει αφετηρία έναν από τους περιφερειακούς κόμβους κατευθύνεται πάντα προς τον κεντρικό. Αυτός με την σειρά του τον αναμεταδίδει ανάλογα με τους πίνακες δρομολόγησης και πίνακες φυσικών διευθύνσεων που διατηρεί. Είναι κατανοητό πως η εύρυθμη λειτουργία του δικτύου εξαρτάται άμεσα από την ύπαρξη του κεντρικού κόμβου. Για αυτόν τον λόγο, σε κάθε υλοποίηση τέτοιου τύπου οι περιφερειακοί κόμβοι συνδέονται με παραπάνω από μία συνδέσεις με τον κεντρικό, ώστε σε περίπτωση βλάβης στην μία διαδρομή να μην χαθεί πλήρως η επικοινωνία. Ο κόμβος συνήθως αποτελείται από συσκευές εγκατεστημένες σε μορφή cluster. Οπότε σε περίπτωση που χαλάσει μία συσκευή του του cluster, αναλαμβάνει η επόμενη συσκευή. Το cluster μπορεί να λειτουργεί σε μορφή active-standby ή active-active. Με τις προαναφερθέντες τεχνικές μειώνονται οι πιθανότητες για ολική απώλεια συνδεσιμότητας τμημάτων του δικτύου. Ένα τελευταίο χαρακτηριστικό της τοπολογίας αστέρα είναι η ευελιξία σε επεκτασιμότητα που προσφέρει. Το δίκτυο μπορεί να μεγαλώσει σε αριθμό εκατοντάδων χρηστών και η μόνη παρέμβαση που

απαιτείται είναι η σύνδεση των νέων περιφερειακών κόμβων με τον κεντρικό.

Η τοπολογία της προσομοίωσης στην οποία υλοποιήθηκαν τα σενάρια είναι βασισμένη σε τοπολογία αστέρα και φαίνεται στην παρακάτω εικόνα:



Εικόνα 15: Τοπολογία δικτύου

Ο κεντρικός κόμβος του αστέρα είναι ένα Cisco switch Cisco CBS250-16T με δυνατότητες δρομολόγησης (L3). Χρησιμοποιείται ως core switch και συγκεντρώνει όλη την κίνηση, την οποία δρομολογεί είτε εσωτερικά είτε προς το firewall με τελικό προορισμό το διαδίκτυο. Με δεδομένο πως υλοποιεί κεντρική διαχείριση κίνησης, οι πόροι του σε μνήμη, επεξεργαστική ισχύ και bandwidth θα πρέπει να είναι αυξημένες. Άρα, θα πρέπει να είναι ένας από τους πιο ακριβούς εξοπλισμούς της υποδομής μίας εταιρίας. Στο core switch συνίσταται να συνδέονται οι servers του οργανισμού, ειδικά

αυτοί που θεωρούνται κρίσιμοι για την λειτουργία του. Κάθε server συνδέεται σε μία θύρα του κεντρικού switch και είναι assign στο υποδίκτυο των servers. Σε κάθε τμήμα είναι εγκατεστημένα τα λεγόμενα switch πρόσβασης. Πρόκειται για διαχειρίσιμα switches layer 2, χαμηλότερων δυνατοτήτων σε σχέση με το κεντρικό, που εξυπηρετούν τους τελικούς χρήστες των τμημάτων. Στην τοπολογία έχει τοποθετηθεί μία τερματική συσκευή ανά τμήμα, για διευκόλυνση της υλοποίησης των σεναρίων. Η σύνδεση τους με τον κεντρικό κόμβο πραγματοποιείται με uplinks ρυθμισμένα σε μορφή trunk.

Η επικοινωνία με το διαδίκτυο πραγματοποιείται με την συσκευή τείχους προστασίας (firewall). Το firewall είναι εγκατεστημένο ανάμεσα στο κεντρικό switch του οργανισμού και τον δρομολογητή του παρόχου υπηρεσίας διαδικτύου. Ο σκοπός είναι η συνολική κίνηση του δικτύου να περνά μέσα από το firewall και σε αυτό να υλοποιούνται κανόνες φιλτραρίσματος κίνησης και περιεχομένου. Το firewall δίνει την δυνατότητα στου διαχειριστές δικτύων να εφαρμόσουν κανόνες NAT, κανόνες απόρριψης ή αποδοχής κίνησης, φίλτρα URL, φίλτρα περιεχομένου κ.ά. Με λίγα λόγια μπορεί να παρέχει υπηρεσίας ασφαλείας από layer 3 μέχρι και layer 7. Στην αγορά υπάρχουν πολλοί κατασκευαστές firewall συσκευών με μεγάλες διαφορές σε δυνατότητες και τιμές. Στα σενάρια υλοποίησης χρησιμοποιήθηκε η open server έκδοση της Checkpoint. Η Checkpoint θεωρείται από τους κολοσσούς κατασκευαστών συσκευών για ασφάλεια συστημάτων. Ξεχωρίζει στην αγορά για τις καινοτόμες ιδέες της και τα εξαιρετικά user interfaces που παρέχει. Η σύνδεση με τον κεντρικό κόμβο πραγματοποιείται με τρεις φυσικές συνδέσεις που οι συσκευές τα αντιλαμβάνονται σαν μία λογική σύνδεση επειδή είναι ρυθμισμένες με την τεχνολογία port-channel. Η τεχνολογία port-channel εξασφαλίζει μοίρασμα φόρτου της κίνησης και πλεονασμό σε περίπτωση απώλειας συνδεσιμότητας από μία διαδρομή.

7. Σενάρια υλοποίησης

7.1 Περιγραφή σεναρίων

Για την υλοποίηση των σεναρίων δημιουργήθηκε μία προσομοίωση υποδομής ενός οργανισμού. Όπως σε κάθε οργανισμό, έτσι και στην προσομοίωση, το δίκτυο είναι χωρισμένο σε τμήματα και ο διαχωρισμός γίνεται σύμφωνα με την θέση των εργαζομένων στα τμήματα αυτά. Ως ένα ξεχωριστό τμήμα θεωρείται και το τμήμα υποδομών, στο οποίο ανήκουν κυρίως οι servers και άλλα ψηφιακά συστήματα που είναι μέρος του κορμού υποδομής για την ορθή λειτουργία της εταιρίας. Το κάθε τμήμα έχει το δικό του switch πρόσβασης που παρέχει την συνδεσιμότητα των χρηστών σε όλα τα διαφορετικά υποδίκτυα. Τα switches πρόσβασης συνδέονται με το core switch

του οργανισμού, στο οποίο συγκεντρώνεται όλη η δικτυακή κίνηση είτε αυτή προορίζεται για το εσωτερικό δίκτυο, είτε για το διαδίκτυο. Η προεπιλεγμένη πύλη όλων των συσκευών για επικοινωνία με το διαδίκτυο και τα υπόλοιπα υποδίκτυα είναι το τοίχος προστασίας της εταιρίας. Το τοίχος προστασίας είναι ο συνδετικός κρίκος μεταξύ του κεντρικού switch και του δρομολογητή του παρόχου.

Για λόγους ευκολίας στην προσομοίωση δεν έχουν δημιουργηθεί όλα τα τμήματα από τα οποία μπορεί να αποτελείται ένας οργανισμός, παρά μόνο κάποια ενδεικτικά που θεωρούνται απαραίτητα για την στελέχωση του. Τα τμήματα που θα λάβουν μέρος στα σενάρια υλοποίησης είναι το τμήμα ανθρώπινου δυναμικού, το τμήμα λογιστηρίου, το τμήμα πληροφορικής και το τμήμα υποδομών. Το τμήμα ανθρώπινου δυναμικού είναι υπεύθυνο για την προσέγγιση μελλοντικών εργαζομένων της εταιρίας, για όλη την οργάνωση των γραφείων σε προμήθειες και ανάγκες, καθώς επίσης και για την επεξήγηση των δικαιωμάτων των εργαζομένων σε αυτούς, σε περίπτωση που οποιοσδήποτε έχει κάποια απορία επ' αυτών των θεμάτων. Το τμήμα λογιστηρίου είναι υπεύθυνο για την μισθοδοσία του προσωπικού, για τους ισολογισμούς της εταιρίας και για την διατήρηση ενημερωμένου αρχείου σε περιπτώσεις ελέγχων από τους αρμόδιους φορείς. Το τμήμα πληροφορικής είναι υπεύθυνο για την συντήρηση, αναβάθμιση και ανανέωση των ψηφιακών υποδομών της εταιρίας, καθώς επίσης για την υποστήριξη των εργαζομένων σε θέματα που αντιμετωπίζουν κατά την χρήση των ψηφιακών υποδομών του οργανισμού. Στην σημερινή εποχή, στις ευθύνες του τμήματος πληροφορικής έχει προστεθεί η εγγύηση ασφάλειας των δεδομένων από επιθέσεις και κακόβουλα λογισμικά, εφόσον πλέον είναι ένα από τα πιο φλέγοντα ζητήματα στον κόσμο της πληροφορικής.

Ένας από τους συχνότερους τρόπους για να εισχωρήσει κάποιο κακόβουλο λογισμικό σε μία εταιρία είναι τα λεγόμενα phishing ηλεκτρονικά μηνύματα. Η σύνταξη τους είναι μορφοποιημένη με τέτοιον τρόπο ώστε να είναι πανομοιότυπα με μηνύματα που ανταλλάζονται σε καθημερινή βάση εντός ενός οργανισμού. Ο σκοπός τους είναι η παραπλάνηση του χρήστη και η οδήγηση του να κάνει κλικ σε κάποιον προσαρμοσμένο υπερσύνδεσμο. Στο πρώτο σενάριο υλοποίησης ένα ηλεκτρονικό μήνυμα φτάνει σε έναν εργαζόμενο του τμήματος ανθρώπινου δυναμικού και έχει συνταχθεί με τρόπο να φαίνεται πως έχει αποσταλεί από το τμήμα πληροφορικής. Το μήνυμα αναφέρει πως ο κωδικός εισόδου στις ηλεκτρονικές υπηρεσίες της εταιρίας επρόκειτο να λήξει και για να πραγματοποιηθεί η ανανέωση του, θα πρέπει να ακολουθηθεί ένας συγκεκριμένος υπερσύνδεσμος. Το μοτίβο που χρησιμοποιήθηκε στο σενάριο φαίνεται στην παρακάτω εικόνα:

Εικόνα 16: Μοτίβο phishing e-mail

Ο υπάλληλος του τμήματος ανθρώπινου δυναμικού δεν αντιλήφθηκε πως το ηλεκτρονικό μήνυμα ήταν παραπλανητικό, οπότε έκανε κλικ στον υπερσύνδεσμο ανανέωσης κωδικού. Η συνέπεια ήταν να αποθηκεύσει τοπικά στον υπολογιστή του το κακόβουλο λογισμικό και αυτό με τη σειρά του να ενεργοποιηθεί. Στην αρχή θα μολύνει τα αρχεία του υπολογιστή και στην συνέχεια θα κάνει προσπάθειες να μολύνει όσες περισσότερες συσκευές του δικτύου καταφέρει. Οι τεχνικοί πληροφορικής θα τρέξουν εργαλεία συλλογής πακέτων κίνησης για να επεξεργαστούν την συμπεριφορά του κακόβουλου λογισμικού και μόλις αντιληφθούν την συμπεριφορά του, θα εξετάσουν τα log αρχεία σε όλες τις συσκευές, για να ανακαλύψουν πόσες τερματικές συσκευές έχουν μολυνθεί. Έπειτα, θα τοποθετήσουν τα logs σε ένα IDS σύστημα με σκοπό να εξάγουν πληροφορίες για την ταυτότητα του κακόβουλου λογισμικού. Το επόμενο βήμα είναι η εκκαθάριση των τερματικών συσκευών που μολύνθηκαν και η εξέταση τους για τυχόν απώλειες αρχείων, ή αλλαγές βασικών ρυθμίσεων τους. Τέλος, το τμήμα πληροφορικής θα πρέπει να οργανώσει ημερίδες ενημέρωσης των εργαζομένων για τους τρόπους αναγνώρισης και αποφυγής των phishing e-mails. Εκτός όμως από τις συναντήσεις ενημέρωσης, οι διαχειριστές θα πρέπει να οργανώσουν εσωτερικές συναντήσεις εντός του τμήματος, με σκοπό την ανάλυση των πεπραγμένων, τις ενέργειες που οδήγησαν σε αυτήν την κατάληξη και τι πρέπει να γίνει στο μέλλον για να αποτραπούν τέτοιου είδους επιθέσεις ή έστω να σμικρύνουν οι συνέπειες τους το περισσότερο δυνατό.

Ένα φαινόμενο που εμφανίστηκε με την αρχή της επανάστασης της πληροφορίας και διαδίδεται με γοργούς ρυθμούς πλέον, είναι οι επιθέσεις σε ψηφιακά συστήματα. Παλαιότερα οι περισσότεροι οργανισμοί δεν είχαν αντιληφθεί τους

τεράστιους κινδύνους αυτού του είδους των επιθέσεων και δεν έβαζαν καν το θέμα στην ατζέντα θεμάτων προς συζήτηση. Σήμερα, στις περισσότερες συναντήσεις που συμμετέχουν τα τμήματα πληροφορικής των εταιριών αναφέρονται ζητήματα και σκέψεις σχετιζόμενες με την ασφάλεια των ψηφιακών συστημάτων και των δεδομένων που διατηρούνται στις βάσεις δεδομένων τους. Με αφορμή τα παραπάνω, το δεύτερο σενάριο υλοποίησης αφορά μια απόπειρα επίθεσης στην εταιρία από εξωτερικό παράγοντα. Ο όρος εξωτερικός παράγοντας αναφέρεται σε χρήστη που δεν ανήκει στην εταιρία, αλλά προσπαθεί να της επιτεθεί μέσω του διαδικτύου. Γίνεται υπόθεση πως κάποιος χρήστης με γνώσεις πληροφορικής και νέων τεχνολογιών, ανακαλύπτει την δημόσια διεύθυνση IP της εταιρίας και προσπαθεί να διερευνήσει εκτεθειμένες διόδους για να εισχωρήσει στο εσωτερικό δίκτυο και τις υποδομές. Χρησιμοποιώντας τα κατάλληλα εργαλεία, εντοπίζει έναν server που τρέχει κάποιες υπηρεσίες και προσπαθεί να επιτεθεί σε αυτές. Οι τεχνικοί από την πλευρά τους που παρακολουθούν το firewall, διαπιστώνουν στα logs αρχεία πως υπάρχει ύποπτη κίνηση από το διαδίκτυο προς το εσωτερικό τους δίκτυο. Μετά από ανάλυση, ανακαλύπτουν πως κάποιες υπηρεσίες δεν θα έπρεπε να φαίνονται προς το διαδίκτυο και άμεσα παραμετροποιούν τους κανόνες που να επιτρέπουν μόνο τις επιθυμητές υπηρεσίες προς τα διαδίκτυο. Εφόσον αποφευχθεί η επίθεση, το τμήμα πληροφορικής θα πρέπει να οργανώσει συναντήσεις με στόχο την ανάλυση των αιτιών που υπηρεσίες που δεν θα έπρεπε ήταν εκτεθειμένες στο διαδίκτυο. Σαν τελικό βήμα θα ήταν συνετό να επανεξετάσουν όλους τους κανόνες και την σειρά τους στο τοίχος προστασίας ούτως ώστε να μην υπάρξουν ανάλογες περιπτώσεις διακινδύνευσης της εύρυθμης λειτουργίας των υποδομών με κατάληξη την απώλεια σημαντικών δεδομένων.

7.2 Υλοποίηση κοινών σημείων σεναρίων

Η φύση των σεναρίων που θα μελετηθούν παρακάτω είναι διαφορετική, παρ' όλα αυτά η κεντρική υποδομή παραμένει η ίδια. Οπότε αρχικά θα πρέπει να αναλυθεί το κοινό δικτυακό κομμάτι των σεναρίων και μετέπειτα να αναλυθούν οι διαφορές ανά περίπτωση. Τα λειτουργικά συστήματα που εγκαταστάθηκαν στις τερματικές και δικτυακές συσκευές είναι τα παρακάτω:

- Στις τερματικές συσκευές IT-Admin-PC, Accounting-PC, HR-PC εγκαταστάθηκε λειτουργικό Windows 10.
- Στους servers Wb-Server, File-Server εγκαταστάθηκε λειτουργικό Windows Server 2016.

- Στο Core Switch εγκαταστάθηκε Cisco IOS vios 12.

- Στον δρομολογητή ISR εγκαταστάθηκε Cisco IOS 3700 Software.

- Στο τείχος προστασίας Checkpoint εγκαταστάθηκε Gaia R80.10.

- Τα switches των τμημάτων είναι unmanaged χωρίς κάποιο λειτουργικό σύστημα.

Αναφορικά με τα δίκτυα της τοπολογίας και τον διαχωρισμό τους σε VLAN (Virtual Local Area Networks) ακολουθήθηκε ο παρακάτω σχεδιασμός:

- Οι servers που θα έχουν μόνο εσωτερικές προσβάσεις ανήκουν στο VLAN Servers 10 με υποδίκτυο 172.16.10.0/24 και προεπιλεγμένη πύλη την 172.16.10.1 που αντιστοιχεί στο Checkpoint. Ο file server έχει την IP 172.16.10.100 η οποία του έχει αποδοθεί στατικά.

- Οι servers που θα είναι προσβάσιμοι από το διαδίκτυο ανήκουν στο VLAN DMZ 20 με υποδίκτυο 172.16.20.0/24 και προεπιλεγμένη πύλη την 172.16.20.1 που αντιστοιχεί στο Checkpoint. Ο server που στο σενάριο θα είναι προσβάσιμος από το διαδίκτυο είναι ο web server με IP 172.16.20.100 η οποία του έχει αποδοθεί στατικά.

- Το τμήμα ανθρώπινου δυναμικού ανήκει στο VLAN HR 30 με υποδίκτυο 172.16.30.0/24 και προεπιλεγμένη πύλη την 172.16.30.1 που αντιστοιχεί στο Checkpoint. Στις τερματικές συσκευές που ανήκουν σε αυτό το υποδίκτυο αποδίδεται IP μέσω DHCP server.

- Το τμήμα πωλήσεων ανήκει στο VLAN Sales 40 με υποδίκτυο 172.16.40.0/24 και προεπιλεγμένη πύλη την 172.16.40.1 που αντιστοιχεί στο Checkpoint. Στις τερματικές συσκευές που ανήκουν σε αυτό το υποδίκτυο αποδίδεται IP μέσω DHCP server.

- Το τμήμα πληροφορικής ανήκει στο VLAN IT 50 με υποδίκτυο 172.16.50.0/24 και προεπιλεγμένη πύλη την 172.16.50.1 που αντιστοιχεί στο Checkpoint. Στην τερματική συσκευή που χρησιμοποιείται στην υλοποίηση, έχει αποδοθεί η IP 172.16.50.100. Είναι το μόνο τμήμα που οι IPs αποδίδονται στατικά επειδή όλο το υποδίκτυα έχει πρόσβαση σε όλα τα υπόλοιπα.

- Οι δικτυακές συσκευές ανήκουν στο VLAN Management 100 με υποδίκτυο 172.16.100.0/24 και προεπιλεγμένη πύλη την 172.16.100.1 που αντιστοιχεί στο Checkpoint. Όλες οι διευθύνσεις έχουν αποδοθεί στατικά. Η διεύθυνση διαχείρισης του Checkpoint είναι η 172.16.100.1 (interface eth0) και η διεύθυνση διαχείρισης του Core Switch είναι η 172.16.100.2. Τέλος έχει οριστεί η πόρτα GigabitEthernet 3/3 να ανήκει στο management vlan για περιπτώσεις που χρειαστεί troubleshooting.

- Το τείχος προστασίας είναι συνδεδεμένο με τον δρομολογητή παροχής υπηρεσίας διαδικτύου με το υποδίκτυα 10.10.10.0/29. Στο interface του δρομολογητή έχει αποδοθεί η IP 10.10.10.1 και στο interface του τείχους προστασίας η IP 10.10.10.2

- Τέλος θα πρέπει να αναφερθεί πως ο μηχανισμός DHCP για τα υποδίκτυα των πωλήσεων και του ανθρώπινου δυναμικού, έχει υλοποιηθεί στο Checkpoint.

7.3 Υλοποίηση Σεναρίου 1

Το πρώτο σενάριο σχετίζεται με τα γνωστά σε όλους πλέον phishing e-mails. Πρόκειται για emails που είναι προέρχονται από επιτιθέμενους και είναι δομημένα με τέτοιον τρόπο, ώστε να μοιάζουν πανομοιότυπα με emails που θα μπορούσαν να είχαν σταλεί από έμπιστους αποστολείς. Συνήθως περιέχουν επισυναπτόμενα αρχεία ή υπερσυνδέσμους που αν ανοιχτούν ο επιτιθέμενος μπορεί να εκτελεστεί μία διάφορες λειτουργίες στο τερματικό του χρήστη. Συνήθως σκοπεύουν στην ανάκτηση διαπιστευτηρίων σύνδεσης ή πληροφορίες λογαριασμών. Χρησιμοποιούνται ευρέως, καθώς είναι πολύ πιο εύκολο να εξαπατηθεί κάποιος να κάνει κλικ σε έναν κακόβουλο σύνδεσμο σε ένα φαινομενικά νόμιμο μήνυμα ηλεκτρονικού "ψαρέματος", παρά να ξεπεραστούν οι άμυνες ενός υπολογιστή. Παρόλο που τα περισσότερα από τα phishing μηνύματα είναι εύκολο να αναγνωριστούν από τους χρήστες, οι έρευνες δείχνουν πως έχουν υψηλά ποσοστά επιτυχίας.

Στο σενάριο που υλοποιήθηκε δημιουργήθηκε ένα template email (εικόνα 12) με σκοπό να παραπλανήσει τους χρήστες του οργανισμού. Το email έχει συνταχθεί με τρόπο ώστε να φαίνεται πως ο αυθεντικός αποστολέας είναι το εσωτερικό τμήμα πληροφορικής του οργανισμού. Πληροφορεί τον χρήστη πως ο κωδικός πρόσβασης για τις ηλεκτρονικές υπηρεσίες επρόκειτο να λήξει και για να ανανεωθεί θα πρέπει ο χρήστης να ακολουθήσει έναν υπερσύνδεσμο που βρίσκεται στο τέλος του μηνύματος. Ο εργαζόμενος στο τμήμα του ανθρώπινου δυναμικού με μία πρώτη ματιά δεν αντιλαμβάνεται ότι πρόκειται για phishing email και κάνει κλικ στον υπερσύνδεσμο.

Οι λειτουργίες που έχουν οριστεί από τον επιτιθέμενο κατά την πληκτρολόγηση του συνδέσμου είναι: να τρέξει ένας φυλλομετρητής στο παρασκήνιο, να συνδεθεί σε έναν web-server στο διαδίκτυο, να κατεβάσει ένα εκτελέσιμο αρχείο τύπου .exe τοπικά στον υπολογιστή το οποίο θα εκτελεστεί αυτόματα. Η επίθεση που εκκινεί η εκτέλεση του αρχείου ονομάζεται reverse_tcp.

Συνήθως οι επιθέσεις ξεκινούν από έξω προς τα μέσα και αυτό είναι το κομμάτι που τις κάνουν να αποτυγχάνουν τις περισσότερες φορές. Αυτό γιατί όλα τα τείχη προστασίας είναι δομημένα ώστε να μπλοκάρουν την κίνηση που έρχεται από έξω προς τα μέσα. Από την άλλη πλευρά όμως τα τείχη προστασίας επιτρέπουν τις απαντήσεις από έξω προς τα μέσα όταν το αρχικό αίτημα έχει σταλθεί από το εσωτερικό δίκτυο. Σε αυτήν ακριβώς την λειτουργία είναι βασισμένη και η επίθεση reverse_tcp. Αντί η επίθεση να εκκινήσει από τον server του επιτιθέμενου, εκκινεί από το τερματικό του ίδιου του χρήστη. Το τερματικό αφού μολυνθεί στέλνει αιτήματα σύνδεσης στον server του επιτιθέμενου ο οποίος λειτουργεί σαν ακροατής αιτημάτων. Μόλις το αίτημα φτάσει σε αυτόν, αυτός το αποδέχεται και έτσι εδραιώνεται η σύνδεση μεταξύ του μολυσμένου τερματικού και του server που χειρίζεται ο επιτιθέμενος. Με την επίτευξη της σύνδεσης, ο επιτιθέμενος αποκτά απομακρυσμένη πρόσβαση στο τερματικό του χρήστη και μπορεί να εκτελέσει οποιαδήποτε εντολή επιθυμεί. Η πιο συνηθισμένη πρόσβαση είναι σε επίπεδο γραμμής εντολών με διαχειριστικά δικαιώματα.

Η πρόκληση σε δικτυακό επίπεδο είναι να αναγνωριστεί η επίθεση από τις δικτυακές συσκευές και να προληφθεί. Στο σενάριο γίνεται προσπάθεια αναγνώρισης και παρεμπόδισης του κακόβουλου λογισμικού μέσω του blade Threat Emulation του τείχους προστασίας Checkpoint. Όταν το τείχος προστασίας αντιληφθεί πως κάποιος χρήστης επιθυμεί να κατεβάσει μορφές αρχείων που χρησιμοποιούνται σε επιθέσεις, παραλαμβάνει το αρχείο και το ανεβάζει στο threat cloud της Checkpoint. Εκεί το αρχείο ανοίγεται και τρέχει ταχύτατα σε sandboxes περιβάλλοντα με λειτουργικά συστήματα Windows XP, Windows 7, Windows Server, Windows 10, MacOS όπου ελέγχεται η συμπεριφορά του. Εάν η συμπεριφορά του είναι ύποπτη ή το αρχείο είναι αναγνωρισμένο σαν malware, απαγορεύει στον χρήστη να το κατεβάσει. Την ίδια στιγμή καταγράφει την κίνηση στα αρχεία καταγραφής του και υπάρχει επίσης η δυνατότητα να στείλει alerts στους διαχειριστές, εφόσον έχουν γίνει οι κατάλληλες ρυθμίσεις ενεργοποίησης από την πλευρά τους. Εκτός της πρόληψης οι διαχειριστές του δικτύου είναι υποχρεωμένοι να αναλύσουν την επίθεση και το είδος της, ώστε να γνωρίζουν τις επιπτώσεις. Στο συγκεκριμένο σενάριο υπάρχουν τα εξής δεδομένα:

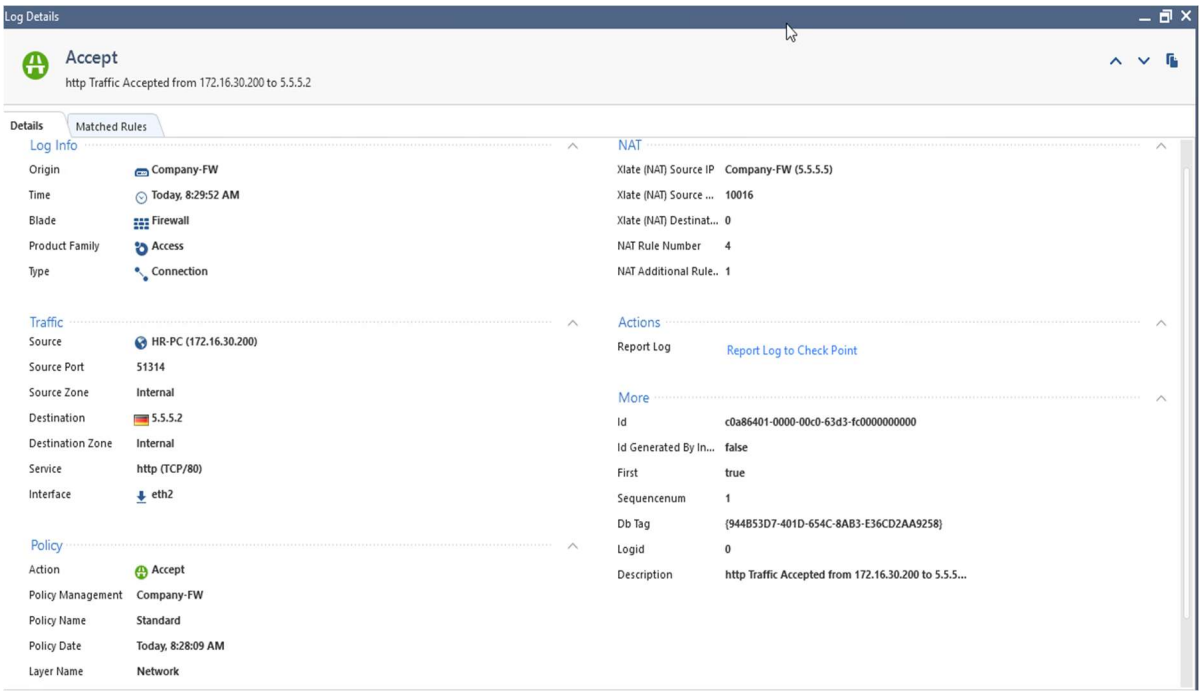
- Η τερματική συσκευή του χρήστη στο τμήμα ανθρώπινου δυναμικού έχει την IP διεύθυνση 172.16.30.200/24 που λαμβάνει με DHCP από το τείχος προστασίας. Προεπιλεγμένη πύλη είναι το τείχος προστασίας με IP 172.16.30.1/24

- Στο τείχος προστασίας υπάρχει κανόνας που επιτρέπει τις http και https κινήσεις από το υποδίκτυα του τμήματος ανθρώπινου δυναμικού και τμήματος πληροφορικής προς το διαδίκτυο.

- Στο διαδίκτυο υπάρχει ο server του επιτιθέμενου με IP διεύθυνση 5.5.5.2/24, ο οποίος τρέχει web υπηρεσίες και στην αρχειοθήκη του υπάρχει το κακόβουλο λογισμικό με ονομασία mal.exe.

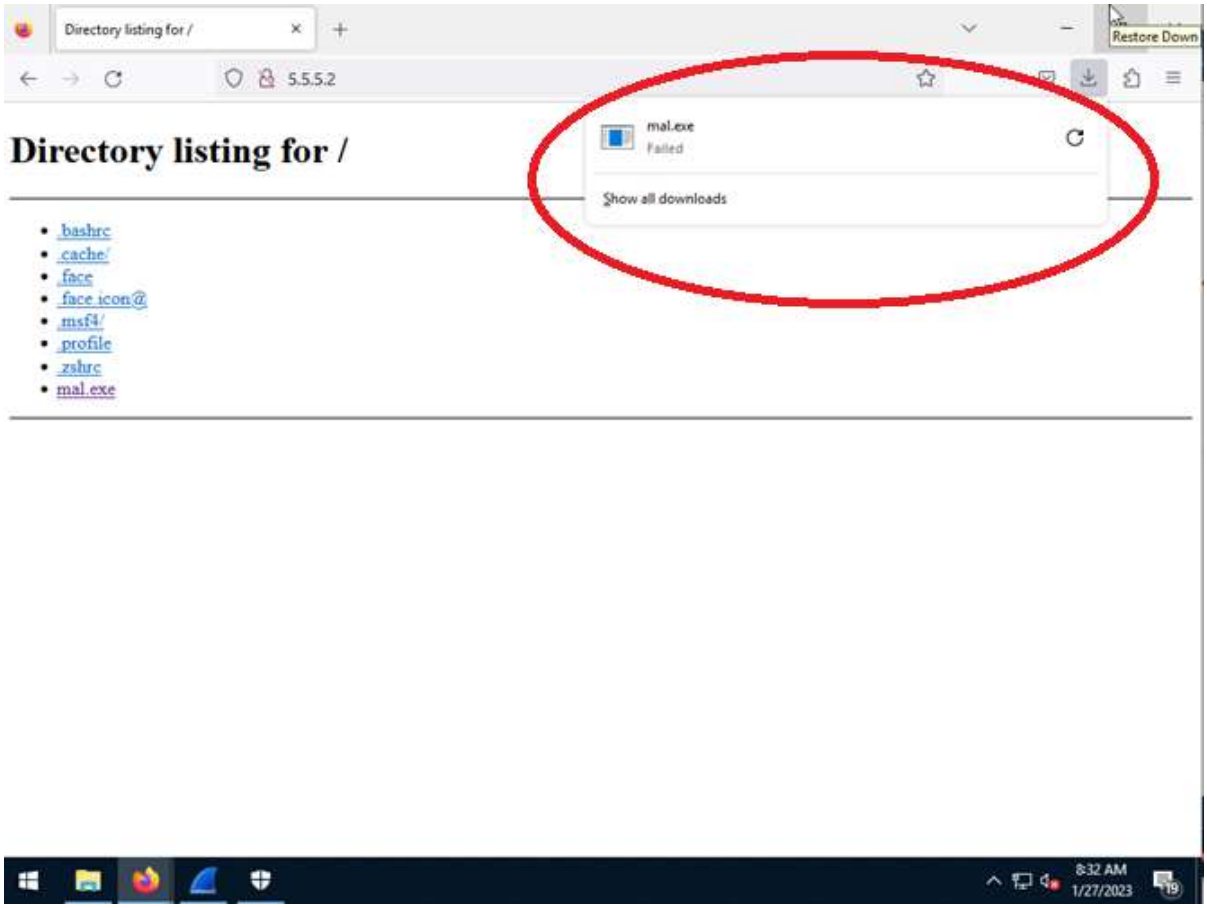
- Στο εσωτερικό δίκτυο αλλά σε άλλο υποδίκτυο βρίσκεται ο υπολογιστής του διαχειριστή δικτύου με IP 172.16.50.100/24 και προεπιλεγμένη πύλη το τείχος προστασίας με IP 172.16.50.1. το τερματικό έχει πρόσβαση σε όλα τα διαχειριστικά περιβάλλοντα των δικτυακών συσκευών του οργανισμού.

Ο χρήστης πατώντας στον υπερσύνδεσμο που περιέχει το phishing e-mail κάνει προσπάθεια σύνδεσης με τον server του επιτιθέμενου στην πόρτα 80, το οποίο επιτρέπεται από το τείχος προστασίας σύμφωνα με τους κανόνες που έχουν εφαρμοστεί. Την καταγραφή της κίνησης μπορεί να την παρακολουθήσουν μόνο οι διαχειριστές δικτύου μέσα από την διεπαφή του τείχους προστασίας.



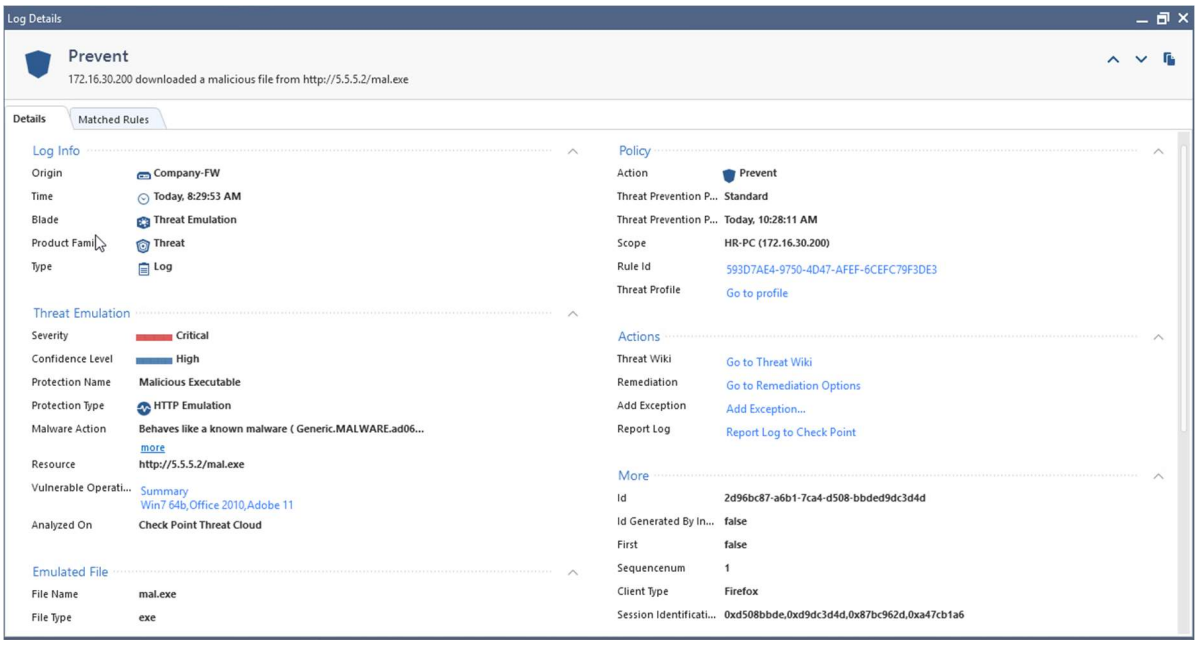
Εικόνα 17: HTTP κίνηση προς server επιτιθέμενου

Στην συνέχεια το τερματικό του χρήστη μέσω φυλλομετρητή προσπαθεί να κατεβάσει το κακόβουλο λογισμικό με όνομα mal.exe από την αρχειοθήκη του server. Το αρχείο ελέγχεται από το blade threat prevention, χαρακτηρίζεται ως κακόβουλο και το κατέβασμα μπλοκάρεται.



Εικόνα 18: Αποτυχημένη προσπάθεια κατεβάσματος αρχείου

Το τείχος προστασίας έχει καταγράψει την ενέργεια στα αρχεία καταγραφής του και έχει στείλει σχετικό alarm στους διαχειριστές του δικτύου. Ο διαχειριστής συνδέεται στο γραφικό περιβάλλον του Checkpoint και προσπελαύνει τα αρχεία καταγραφής. Η αναζήτηση στα αρχεία θα πρέπει να μην είναι γενική εφόσον όλη η κίνηση της εταιρίας περνά μέσα από το τείχος προστασίας. Έτσι, εφαρμόζεται φίλτρο με βάση την IP διεύθυνση του τερματικού που προσπάθησε να κατεβάσει το κακόβουλο λογισμικό. Στα αποτελέσματα φαίνεται η κίνηση στην οποία ενήργησε το blade του threat prevention.



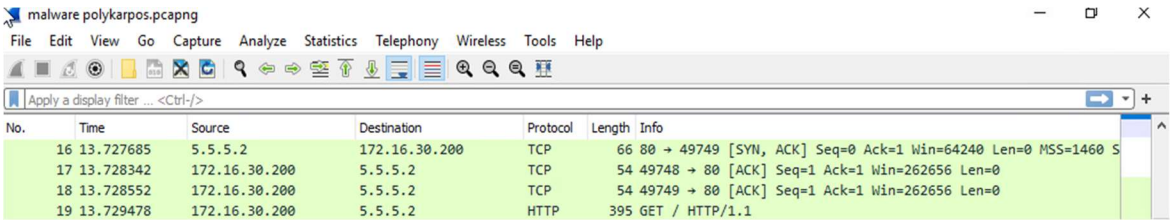
Εικόνα 19: Λειτουργία threat prevention τείχους προστασίας

Στην κορυφή του αρχείου καταγραφής φαίνεται το αποτέλεσμα της δράσης που έκανε το τείχος προστασίας, που είναι η prevent. Παρακάτω εμφανίζει πληροφορίες για το πότε πραγματοποιήθηκε η δράση και ποιο blade έδρασε. Στη συνέχεια παρέχει αναλυτικές πληροφορίες για το κακόβουλο λογισμικό που εντόπισε και πως κατέληξε στην δράση prevent. Ενημερώνει πως ενήργησε το threat emulation, αναγνώρισε το αρχείο σαν malicious εκτελέσιμο και το χαρακτήρισε ως υψηλής επικινδυνότητας. Αναλύει την συμπεριφορά του, αναφέρει από ποια IP διεύθυνση προήλθε και ότι αναλύθηκε στο threat cloud και όχι τοπικά. Στην συνέχεια δείχνει την ρυθμισμένη πολιτική που εμπόδισε το κατέβασμα του αρχείου και ποιες επιπρόσθετες δράσεις μπορούν να κάνουν οι διαχειριστές, εάν το επιθυμούν.

7.3.1 Ανάλυση Αποτελεσμάτων Σεναρίου 1

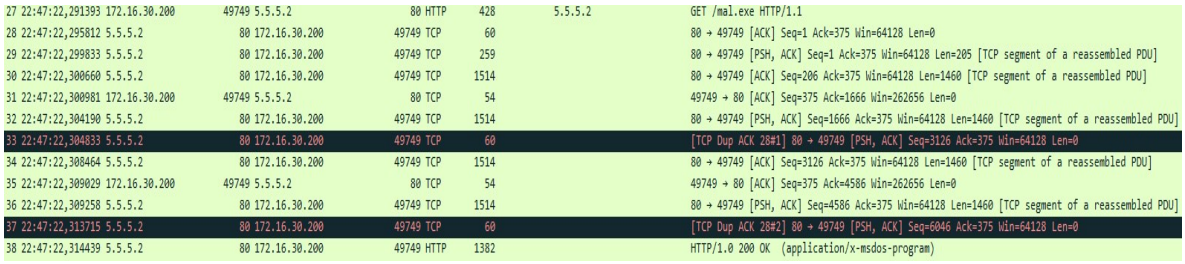
Σύμφωνα με τις συνιστώμενες πρακτικές, οι διαχειριστές αφού κατάφεραν να προλάβουν την μόλυνση του εσωτερικού δικτύου με τα εργαλεία που κατέχουν, θα πρέπει να αναλύσουν το είδος του κακόβουλου λογισμικού που προσπάθησε να εισχωρήσει στο δίκτυο. Με τον τρόπο αυτόν, θα αποκτήσουν πλήρη εικόνα των επιπτώσεων που θα υπήρχαν στα τερματικά του δικτύου σε περίπτωση που το τείχος προστασίας δεν αντιλαμβανόταν την παρουσία του. Η σωστή μέθοδος για να ανακτήσουν πλήρεις πληροφορίες για το κακόβουλο λογισμικό είναι η χρήση sandbox. Θα πρέπει να δημιουργήσουν ένα εικονικό μηχάνημα σε ένα απομονωμένο περιβάλλον και να του δώσουν πρόσβαση στο διαδίκτυο χωρίς να μεσολαβεί το τείχος προστασίας. Απαιτείται μεγάλη προσοχή ώστε το sandbox να είναι απομονωμένο από το εσωτερικό

δίκτυο και να έχει πρόσβαση μόνο στο διαδίκτυο. Όλες οι ρυθμίσεις και οι ενέργειες θα πρέπει να γίνουν ακριβώς με τον ίδιο τρόπο που έγιναν και στο παραγωγικό περιβάλλον του οργανισμού. Η διαφορά θα είναι πως αρχικά το κακόβουλο λογισμικό θα περάσει στο εικονικό μηχάνημα και δεύτερον πως στην εικονική μηχανή θα τρέχει το λογισμικό Wireshark για να καταγράφονται όλα τα πακέτα που περνάνε από την κάρτα δικτύου. Η εικονική μηχανή θα έχει στατικά την ίδια IP διεύθυνση που είχε το τερματικό του χρήστη του τμήματος ανθρώπινου δυναμικού 172.16.30.200/24 και έπειτα θα συνδεθεί κάποιος διαχειριστής σε έναν λογαριασμό ηλεκτρονικού ταχυδρομείου στον οποίο θα αποσταλεί το phishing e-mail που έλαβε ο εργαζόμενος της εταιρίας. Στο λογισμικό Wireshark έχει εφαρμοστεί φίλτρο με κριτήριο την IP διεύθυνση του server 5.5.5.2/24 που είναι γνωστή από τα αρχεία καταγραφής του τείχους προστασίας. Το λογισμικό Wireshark εμφανίζει τα παρακάτω:



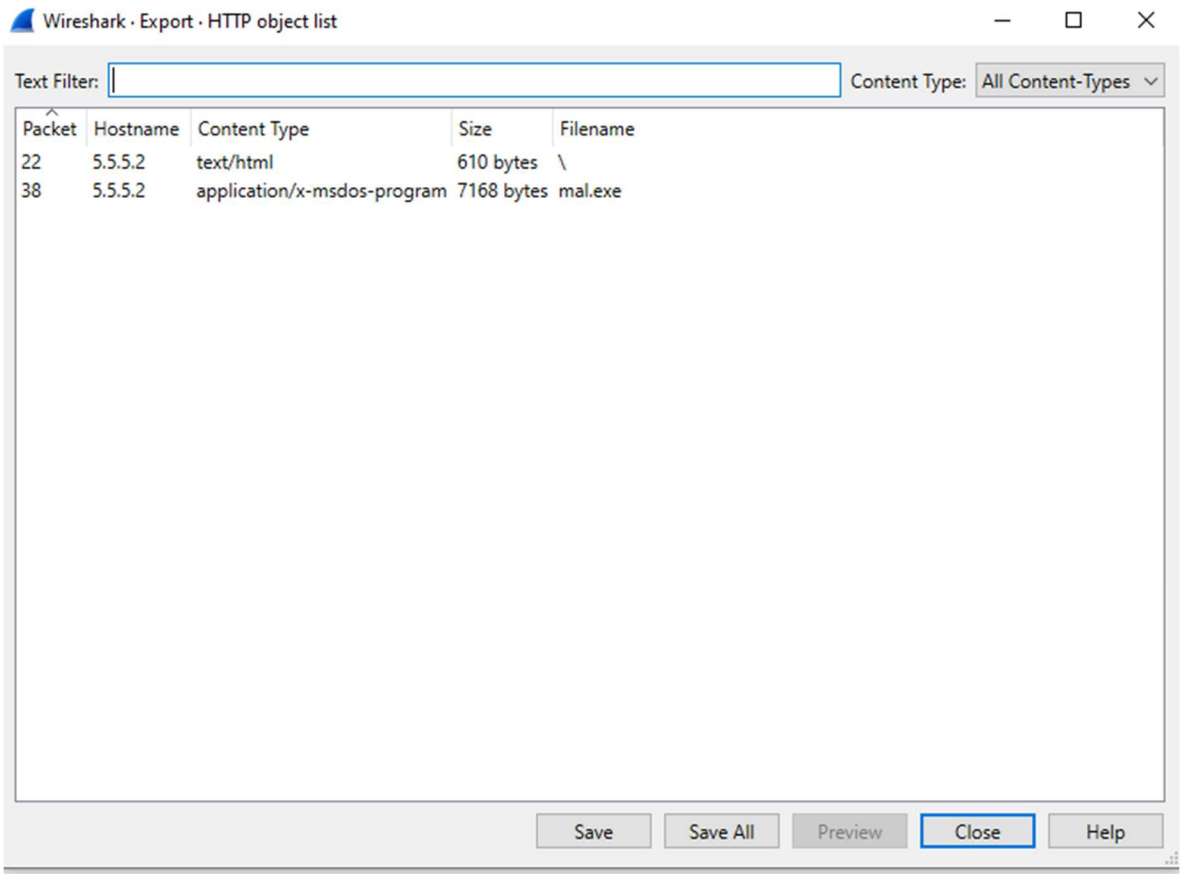
Εικόνα 20: Wireshark-sandbox εγκαθίδρυση TCP επικοινωνίας

Στις γραμμές 16-18 φαίνεται η ανταλλαγή πακέτων TCP SYN και TCP ACK για την εγκαθίδρυση της TCP επικοινωνίας.



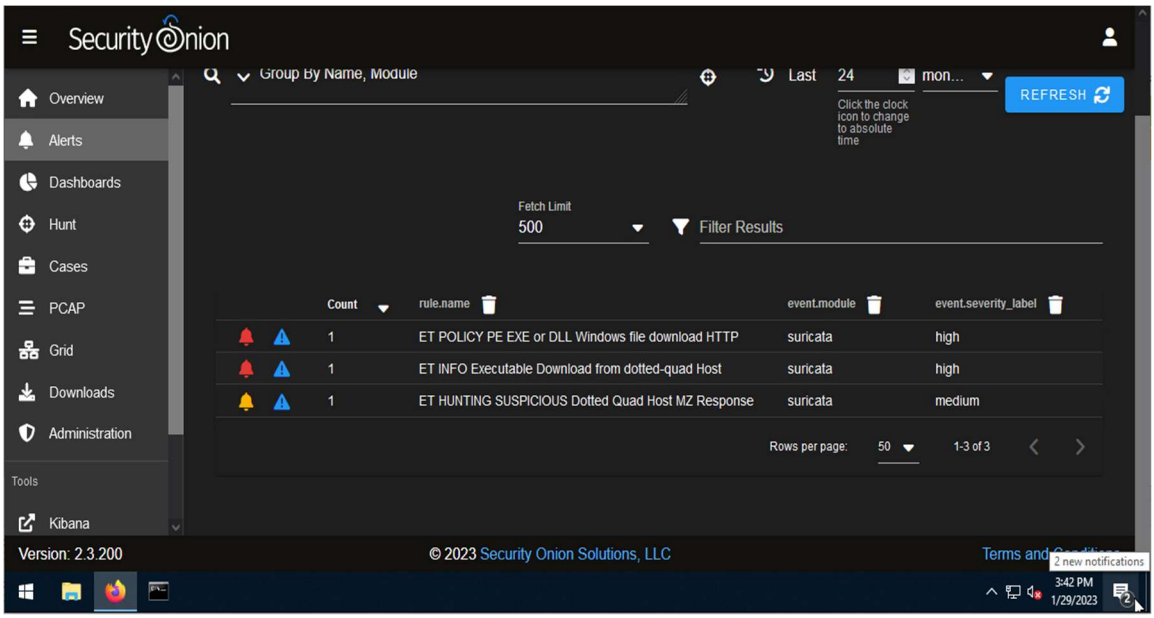
Εικόνα 21: Wireshark-sandbox κατέβασμα κακόβουλου λογισμικού

Στις γραμμές 27-38 φαίνεται η διαδικασία που η εικονική μηχανή ζητάει το κακόβουλο λογισμικό από τον server με ένα HTTP GET αίτημα, ο server το προσφέρει και η επικοινωνία σχετικά με το αρχείο κλείνει στην γραμμή νούμερο 38 που η εικονική μηχανή απαντά με ένα HTTP OK, που σημαίνει πως έχει παραλάβει το αρχείο. Οι διαχειριστές για να πιστοποιήσουν πως το αρχείο έχει κατέβει, πηγαίνουν στο μενού του Wireshark File → Export Object → HTTP και ελέγχουν τι αρχεία έχουν κατέβει μέσω HTTP πρωτοκόλλου.



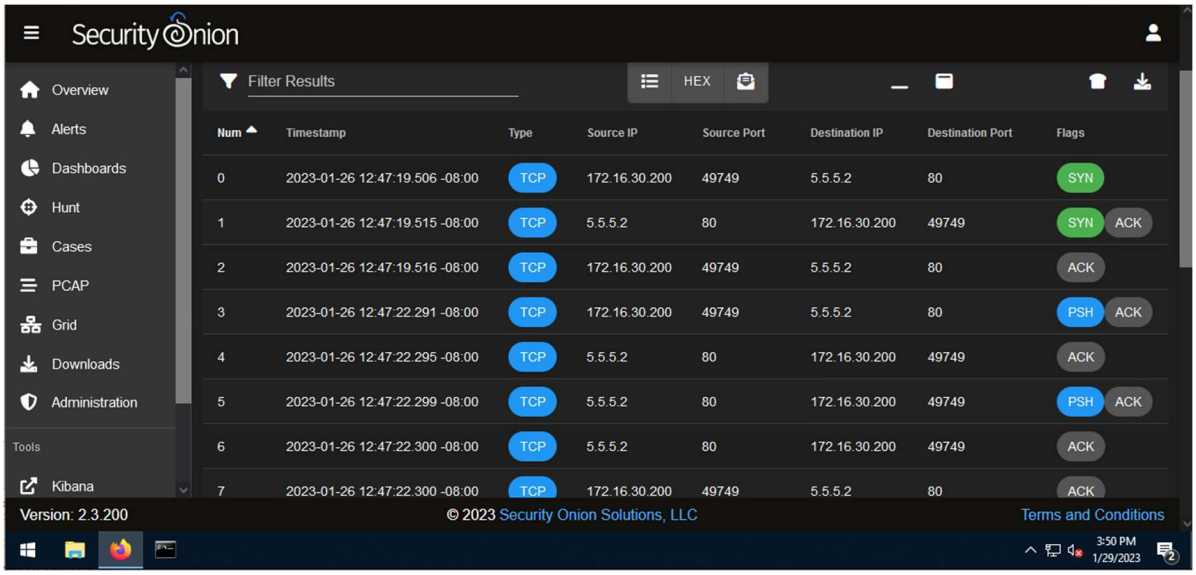
Εικόνα 22: Wireshark-sandbox μενού export objects

Σαν τελευταίο βήμα της διαδικασίας ανάλυσης, οι διαχειριστές θα πρέπει να σώσουν το αρχείο συλλογής κίνησης του Wireshark και να τα χρησιμοποιήσουν ως είσοδο σε ένα σύστημα IDS για να πραγματοποιηθεί ανάλυση της κίνησης. Στο σενάριο χρησιμοποιήθηκε το δωρεάν, βασισμένο σε linux εργαλείο, Security Onion. Μετά το ανέβασμα του αρχείου συλλογής κίνησης .pcap, ελέγχθηκαν τα alerts που δημιουργεί η πλατφόρμα στο μενού alerts, όπως φαίνεται στην παρακάτω εικόνα:

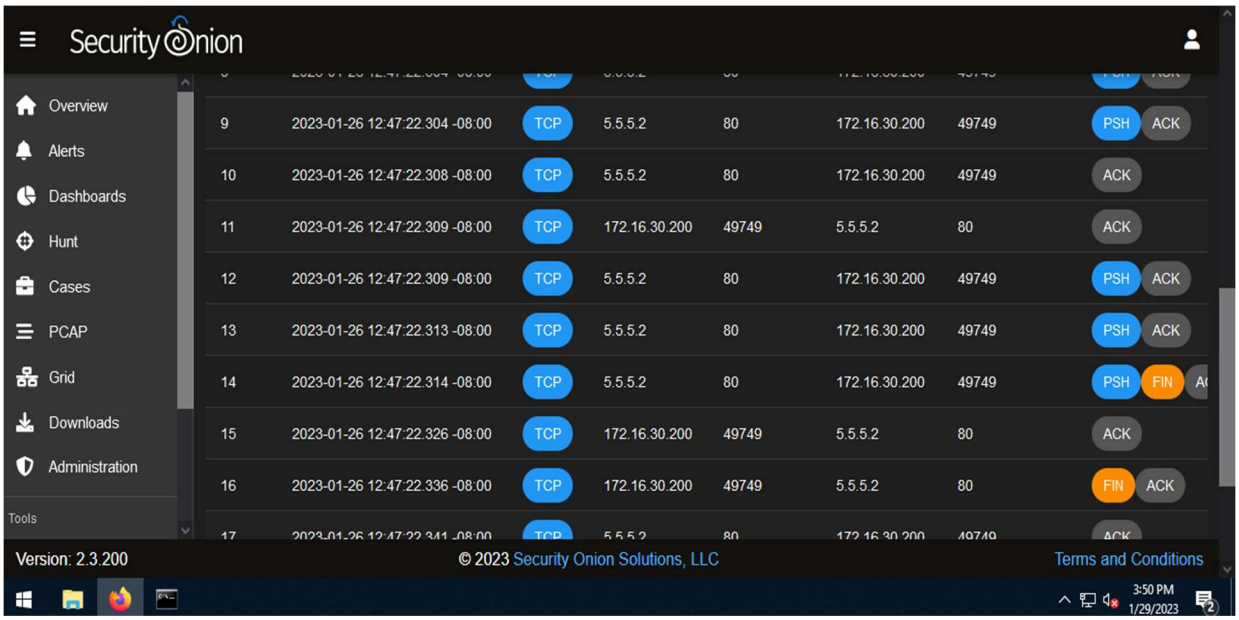


Εικόνα 23: IDS Security Onion alerts

Το σύστημα IDS αναγνωρίζει πως πραγματοποιήθηκε κατέβασμα αρχείου υψηλής επικινδυνότητας με χρήση HTTP πρωτοκόλλου. Στην συνέχεια ο διαχειριστής επιλέγει το alert που πραγματοποιήθηκε η ενέργεια και πατάει στο μενού Actions→PCAP. Η πλατφόρμα θα ανοίξει όλη την TCP συνεδρία και θα την εμφανίσει σε μορφή φιλική προς τον χρήστη, κάτι το οποίο δεν είναι εφικτό με το λογισμικό Wireshark.

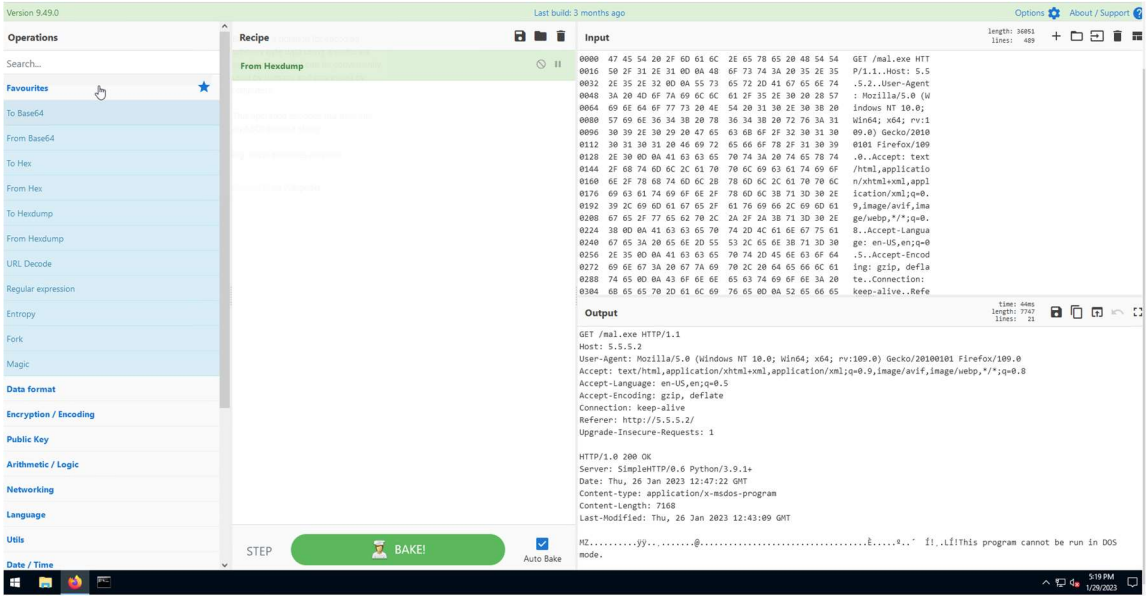


Εικόνα 24: IDS PCAP εμφάνιση



Εικόνα 25: IDS PCAP εμφάνιση-2

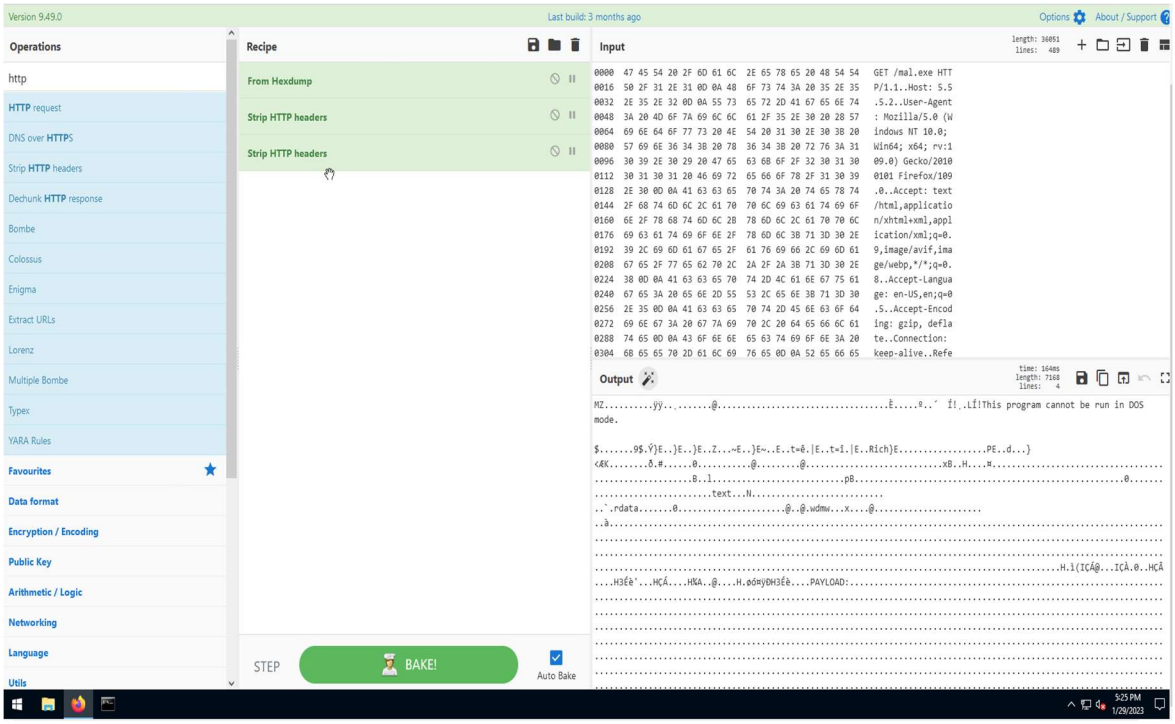
Εφόσον ελεγχθεί η επικοινωνία και συμβαδίζει με αυτήν που συνέλεξε το Wireshark, θα πρέπει να πατηθεί η επιλογή πάνω δεξιά send the transcript to Cyber security chef. Το Cyber security chef είναι μία λειτουργία ενσωματωμένη στο Security Onion, η οποία δίνει την δυνατότητα ανάλυσης και επεξεργασίας πακέτων από αρχεία .pcap. Πατώντας την επιλογή ανοίγει νέα καρτέλα και γίνεται σύνδεση στο εργαλείο cybersecurity chef.



Εικόνα 26: Cyber security chef αρχική σελίδα

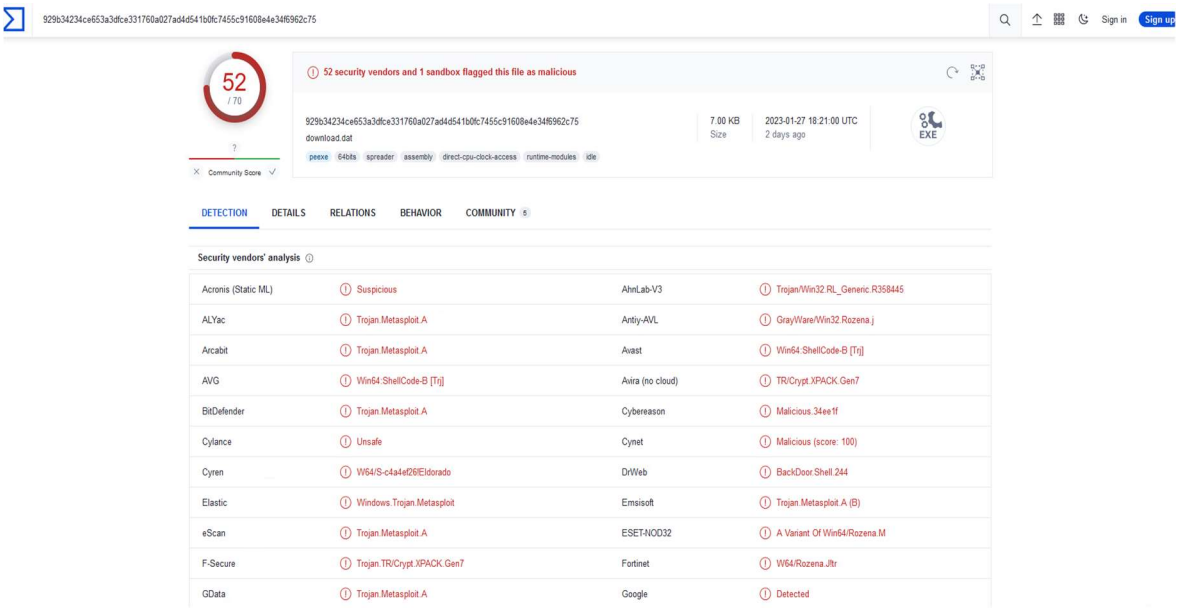
Στην διεπαφή εμφανίζονται τα πακέτα με την μορφή που τα απεικονίζει και το

λογισμικό Wireshark. Από τις επιλογές στα αριστερά γίνεται αναζήτηση για την ενέργεια strip HTTP headers. Αφού επιλεχθεί τοποθετείται στον κεντρικό χώρο του εργαλείου. Η ενέργεια αυτή αφαιρεί τα HTTP headers από το πακέτο, οπότε μένει μόνο το κακόβουλο λογισμικό σε μορφή ASCII.

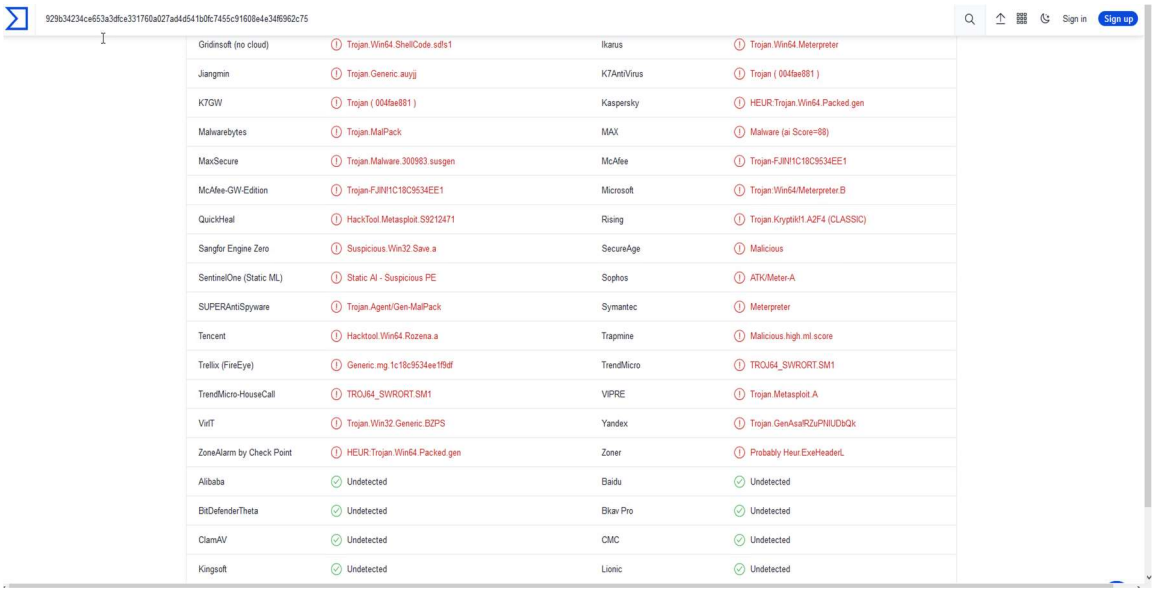


Εικόνα 27: Cyber security chef αρχείο ASCII

Στην συνέχεια θα πρέπει να πατηθεί το εικονίδιο με την δισκέτα για να αποθηκευτεί το αρχείο τοπικά στο τερματικό σε μορφή .dat. Το αρχείο δεν αποθηκεύεται σε εκτελέσιμη μορφή οπότε δεν υπάρχει περεταίρω κίνδυνος για το τερματικό. Το επόμενο βήμα είναι να ανέβει το αρχείο σε κάποια πλατφόρμα ανάλυσης αρχείων για να αναλυθεί η δομή του και η συμπεριφορά του. Το εργαλείο που επιλέχθηκε είναι το virus total. Η πλατφόρμα συγκρίνει τις πληροφορίες του αρχείου με πληροφορίες από τις δημοφιλέστερες βάσεις δεδομένων λογισμικών πρόληψης κακόβουλων αρχείων και εξάγει συμπέρασμα για το αν είναι κακόβουλο. Εάν το αναγνωρίσει παρέχει πληροφορίες όπως η συσχέτιση του με συγκεκριμένα URLs, λεπτομέρειες για το αρχείο, ανάλυση συμπεριφοράς, σχόλια της κοινότητας αναφορικά με την φύση του αρχείου.

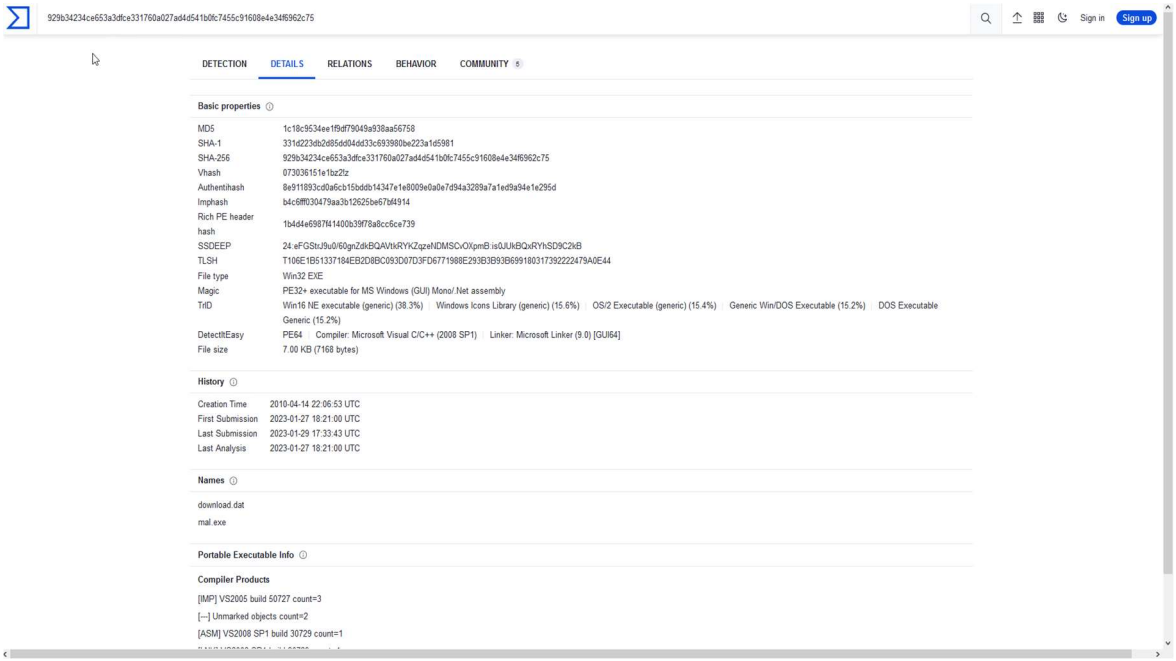


Εικόνα 28: Virus total εντοπισμός

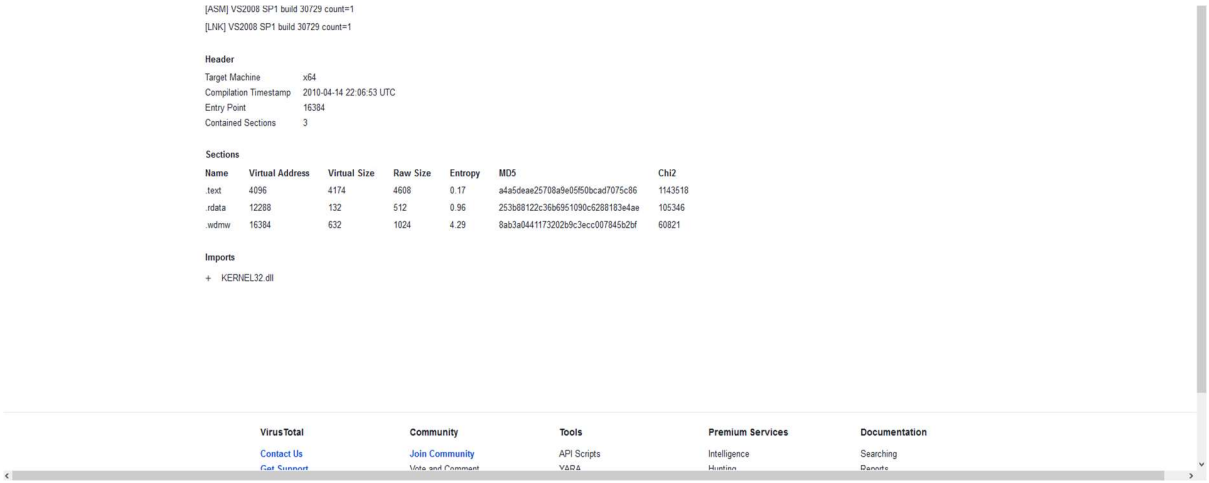


Εικόνα 29: Virus total εντοπισμός-2

Το μεγαλύτερο ποσοστό των λογισμικών απομάκρυνσης κακόβουλων λογισμικών χαρακτηρίζουν το αρχείο ως κακόβουλο που ανήκει την οικογένεια των trojans. Στην επόμενη καρτέλα εμφανίζονται λεπτομέρειες σχετικά με το SHA, το MDA, τον τύπο του αρχείου, την ονομασία και την εκτέλεση.



Εικόνα 30: Virus total λεπτομέρειες

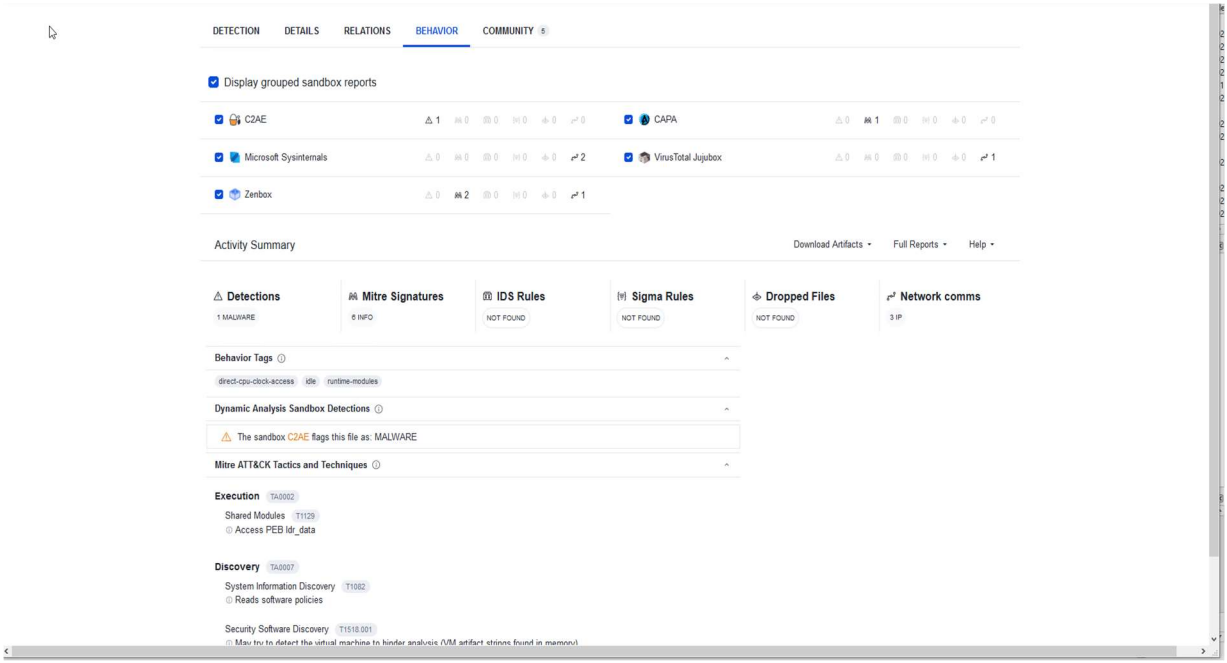


Εικόνα 31: Virus total λεπτομέρειες-2

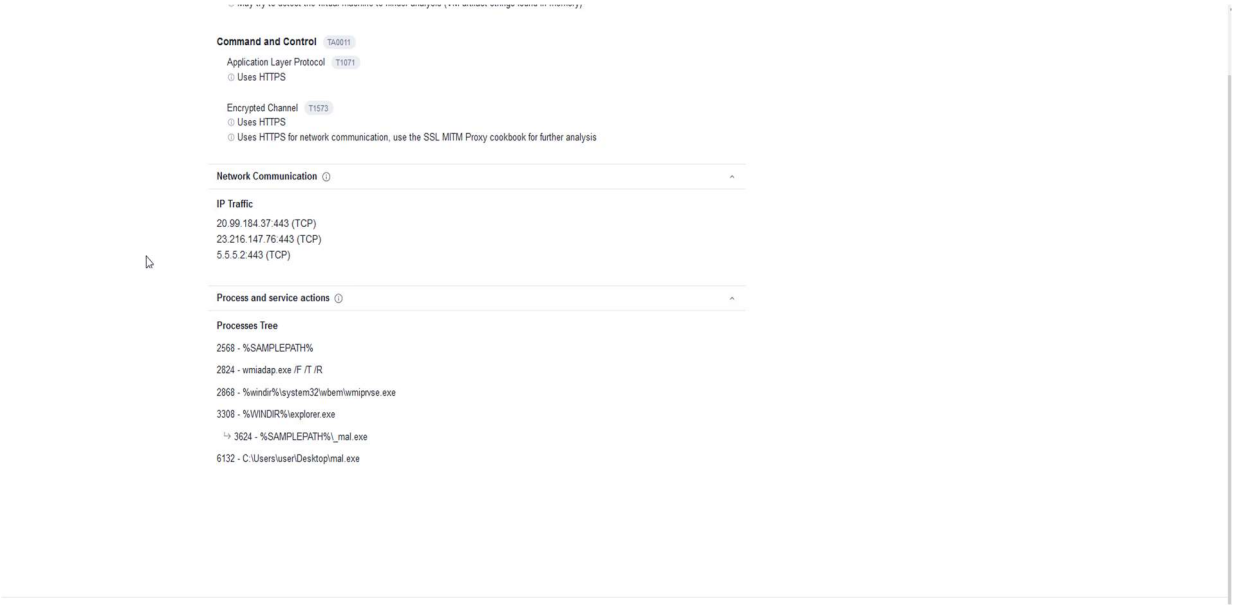
Η καρτέλα συμπεριφοράς υποδεικνύει πως το αρχείο χαρακτηριστικέ ως κακόβουλο από το sandbox που έτρεξε η πλατφόρμα, χρησιμοποίησε το πρωτόκολλο HTTP για να κατέβει, επικοινώνησε με την IP διεύθυνση 5.5.5.2/24 και οι η ροή διεργασιών που ακολούθησε ήταν:

- 2568 - %SAMPLEPATH%
- 2824 - wmiadap.exe /F /T /R

- 2868 - %windir%\system32\wbem\wmiprvse.exe
- 3308 - %WINDIR%\explorer.exe
- 3624 - %SAMPLEPATH%_mal.exe
- 6132 - C:\Users\user\Desktop\mal.exe

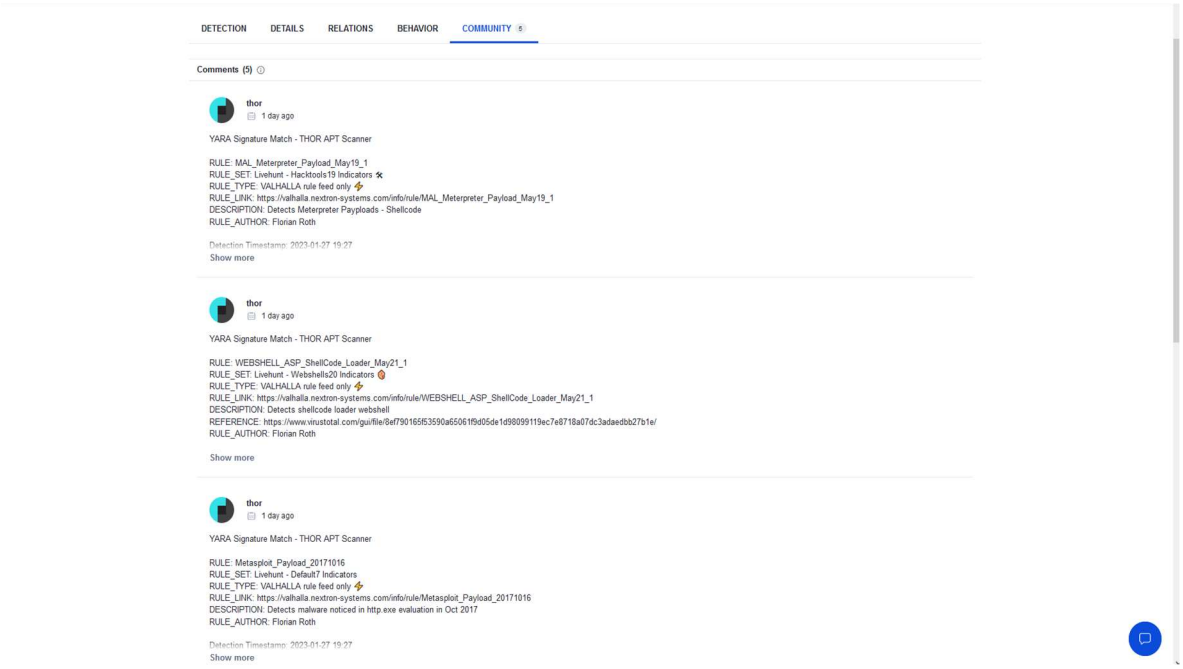


Εικόνα 32: Virus total συμπεριφορά



Εικόνα 33: Virus total συμπεριφορά-2

Στην κοινότητα της πλατφόρμας virus total χρήστες που έχουν έρθει αντιμέτωποι με ίδιων χαρακτηριστικών αρχεία παρέχουν πληροφορίες και συνδέσμους για επιπρόσθετη έρευνα αν κάποιος επιθυμεί.



Εικόνα 34: Virus total κοινότητα

Σε περίπτωση που οι διαχειριστές αποφασίσουν πως απαιτείται επιπρόσθετη ανάλυση του κακόβουλου αρχείο με περισσότερες λεπτομέρειες, θα πρέπει να

επικοινωνήσουν με το τμήμα ασφάλειας συστημάτων. Στο τμήμα αυτό θα λάβουν δράση οι διαχειριστές συστημάτων ή οι SOC αναλυτές, οι οποίοι διαθέτουν τα κατάλληλα μέσα και γνώσεις για να επεξεργαστούν το αρχείο σε επίπεδο εφαρμογής.

7.4 Υλοποίηση Σεναρίου 2

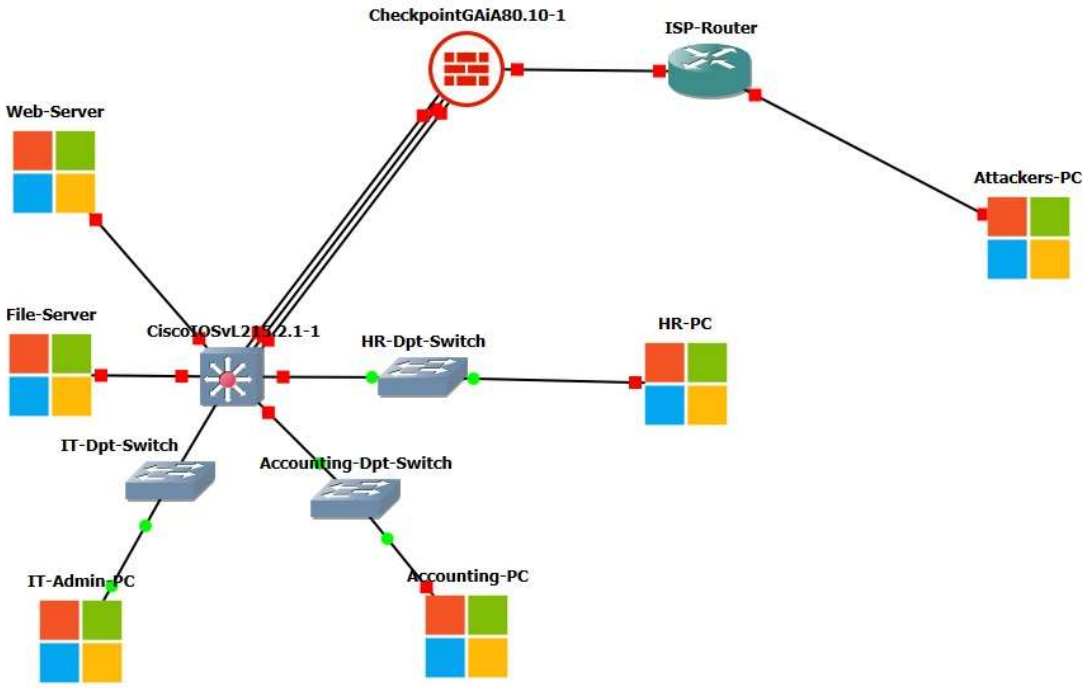
Όπως προαναφέρθηκε, το δεύτερο σενάριο αναφέρεται σε μία υποψήφια επίθεση στο εσωτερικό δίκτυο από κάποιον εξωτερικό χρήστη. Ο χρήστης έχοντας ανακαλύψει την δημόσια IP του οργανισμού, προσπαθεί με κατάλληλα εργαλεία να βρει ανοιχτές πόρτες που να οδηγούν στο εσωτερικό ιδιωτικό δίκτυο. Το λογισμικό που χρησιμοποιεί είναι το Nmap. Το Nmap ("Network Mapper") είναι λογισμικό ανοιχτού κώδικα που διανέμεται δωρεάν και χρησιμοποιείται για την σάρωση δικτύων και υπηρεσιών που τρέχουν σε αυτό. Πολλά συστήματα και διαχειριστές δικτύου το βρίσκουν επίσης χρήσιμο για εργασίες όπως το απόθεμα δικτύου, η διαχείριση χρονοδιαγραμμάτων αναβάθμισης υπηρεσιών και η παρακολούθηση του χρόνου λειτουργίας κεντρικού υπολογιστή ή υπηρεσίας. Το Nmap χρησιμοποιεί ακατέργαστα πακέτα IP με νέους τρόπους για να προσδιορίσει ποιοι κεντρικοί υπολογιστές είναι διαθέσιμοι στο δίκτυο, ποιες υπηρεσίες (όνομα εφαρμογής και έκδοση) προσφέρουν αυτοί οι κεντρικοί υπολογιστές, ποια λειτουργικά συστήματα (και εκδόσεις λειτουργικού συστήματος) εκτελούν, ποιος τύπος φίλτρων πακέτων/τείχη προστασίας είναι σε χρήση, και δεκάδες άλλα χαρακτηριστικά. Σχεδιάστηκε για γρήγορη σάρωση μεγάλων δικτύων, αλλά λειτουργεί καλά και σε μεμονωμένους κεντρικούς υπολογιστές. Το Nmap μπορεί να εγκατασταθεί σε όλα τα διάσημα λειτουργικά συστήματα υπολογιστών και τα επίσημα δυαδικά πακέτα είναι διαθέσιμα για Linux, Windows και Mac OS X. Εκτός από το κλασικό εκτελέσιμο αρχείο γραμμής εντολών Nmap, η σουίτα Nmap περιλαμβάνει προηγμένο GUI και πρόγραμμα προβολής αποτελεσμάτων (Zenmap). Ένα ευέλικτο εργαλείο μεταφοράς δεδομένων, ανακατεύθυνσης και εντοπισμού σφαλμάτων (Ncat), ένα βοηθητικό πρόγραμμα για τη σύγκριση των αποτελεσμάτων σάρωσης (Ndiff) και ένα εργαλείο δημιουργίας πακέτων και ανάλυσης απόκρισης (Nping).

Στην υποδομή της εταιρίας είναι εγκατεστημένος ένας web-server ο οποίος θα πρέπει να είναι προσβάσιμος από χρήστες του διαδικτύου. Για να υλοποιηθεί αυτό ακολουθείται η διαδικασία NAT (Network Address Translation). Επειδή οι διευθύνσεις IP δεν φτάνουν ώστε ο κάθε χρήστης παγκόσμια να έχει μία μοναδική διεύθυνση σερφάροντας στο διαδίκτυο, αναπτύχθηκε η τεχνική του NAT. Με την τεχνική αυτήν κάθε ιδιωτικό δίκτυο μπορεί να έχει ίδιες IP εσωτερικά με άλλα ιδιωτικά δίκτυα, αλλά οι δημόσιες IP τους στο διαδίκτυο είναι μοναδικές. Για παράδειγμα, δύο φίλοι μπορεί στα σπίτια τους να κάνουν χρήση του ιδιωτικού δικτύου 192.168.1.0/24 αλλά χωρίς

αμφιβολία ο service provider που έχουν επιλέξει θα τους δίνει διαφορετική IP για την δρομολόγηση της κίνησης τους στο διαδίκτυο. Στο σενάριο υλοποίησης η ιδιωτική IP του web-server (17216.20.100) έχει αντιστοιχηθεί με στατικό NAT σε μία δημόσια IP (10.10.10.2/29) που μπορεί να δρομολογηθεί στο διαδίκτυο. Αυτό σημαίνει πως αν κάποιος επικοινωνήσει με την δημόσια IP στο διαδίκτυο, επικοινωνεί απευθείας με τον web-server στην εσωτερική υποδομή της εταιρίας.

Ο επιτιθέμενος σαρώνει την δημόσια IP 10.10.10.2 ακολουθώντας δύο τεχνικές και αναμένει τα αποτελέσματα για να βρει ευκολότερο τρόπο δράσης. Αρχικά χρησιμοποιεί τα default scripts και τις default μεθόδους του λογισμικού Nmap πληκτρολογώντας την εντολή nmap -sC -sV -v. Τα αποτελέσματα που αναμένει σχετίζονται με τις ανοιχτές πόρτες στον server και όσο περισσότερες πληροφορίες μπορεί να αντλήσει σχετικά με το λειτουργικό του. Στην συνέχεια προσθέτοντας στην εντολή τις παραμέτρους -sS υλοποιεί το λεγόμενο stealth scanning. nmap -sC -sS -sV -v. Η σάρωση stealth είναι η πιο δημοφιλής επιλογή σάρωσης για πολλούς λόγους. Μπορεί να εκτελεστεί γρήγορα, σαρώνοντας χιλιάδες θύρες ανά δευτερόλεπτο σε ένα γρήγορο δίκτυο που δεν παρεμποδίζεται από περιοριστικά τείχη προστασίας. Η σάρωση SYN είναι σχετικά διακριτική και μυστική, καθώς δεν ολοκληρώνει ποτέ τις συνδέσεις TCP. Λειτουργεί επίσης ενάντια σε οποιαδήποτε συμβατή στοίβα TCP αντί να εξαρτάται από τις ιδιοσυγκρασίες συγκεκριμένων πλατφορμών όπως κάνουν οι σαρώσεις FIN/NULL/Xmas, Maimon και αδράνειας του Nmap. Επιτρέπει επίσης σαφή και αξιόπιστη διαφοροποίηση μεταξύ ανοικτών, κλειστών και φιλτραρισμένων καταστάσεων. Αυτή η τεχνική αναφέρεται συχνά ως μισάνοιχτη σάρωση, επειδή δεν ανοίγεται μια πλήρης σύνδεση TCP. Στέλνεται ένα πακέτο SYN, σαν να πρόκειται να ανοιχτεί μια πραγματική σύνδεση και μετά αναμένεται απάντηση. Ένα SYN/ACK υποδηλώνει ότι η θύρα ακούει (ανοιχτή), ενώ ένα RST (επαναφορά) είναι ενδεικτικό ενός μη ακροατή. Εάν δεν ληφθεί απάντηση μετά από πολλές αναμεταδόσεις, η θύρα επισημαίνεται ως φιλτραρισμένη.

Για την υλοποίηση όλων των παραπάνω η τοπολογία και οι ρυθμίσεις των συσκευών έχουν παραμετροποιηθεί. Στην τοπολογία προστέθηκε μία τερματική συσκευή που ανήκει στον επιτιθέμενο, η οποία είναι συνδεδεμένη στον ISP δρομολογητή. Σε πραγματικές συνθήκες οι υποψήφιοι επιτιθέμενοι δεν είναι συνδεδεμένοι απευθείας με τον ISP δρομολογητή των οργανισμών που σκοπεύουν να επιτεθούν, αλλά ανάμεσα τους και στον δρομολογητή ISP μεσολαβεί το διαδίκτυο. Η μορφή της νέας τοπολογίας φαίνεται στην παρακάτω εικόνα:



Εικόνα 35: Τοπολογία σεναρίου 2

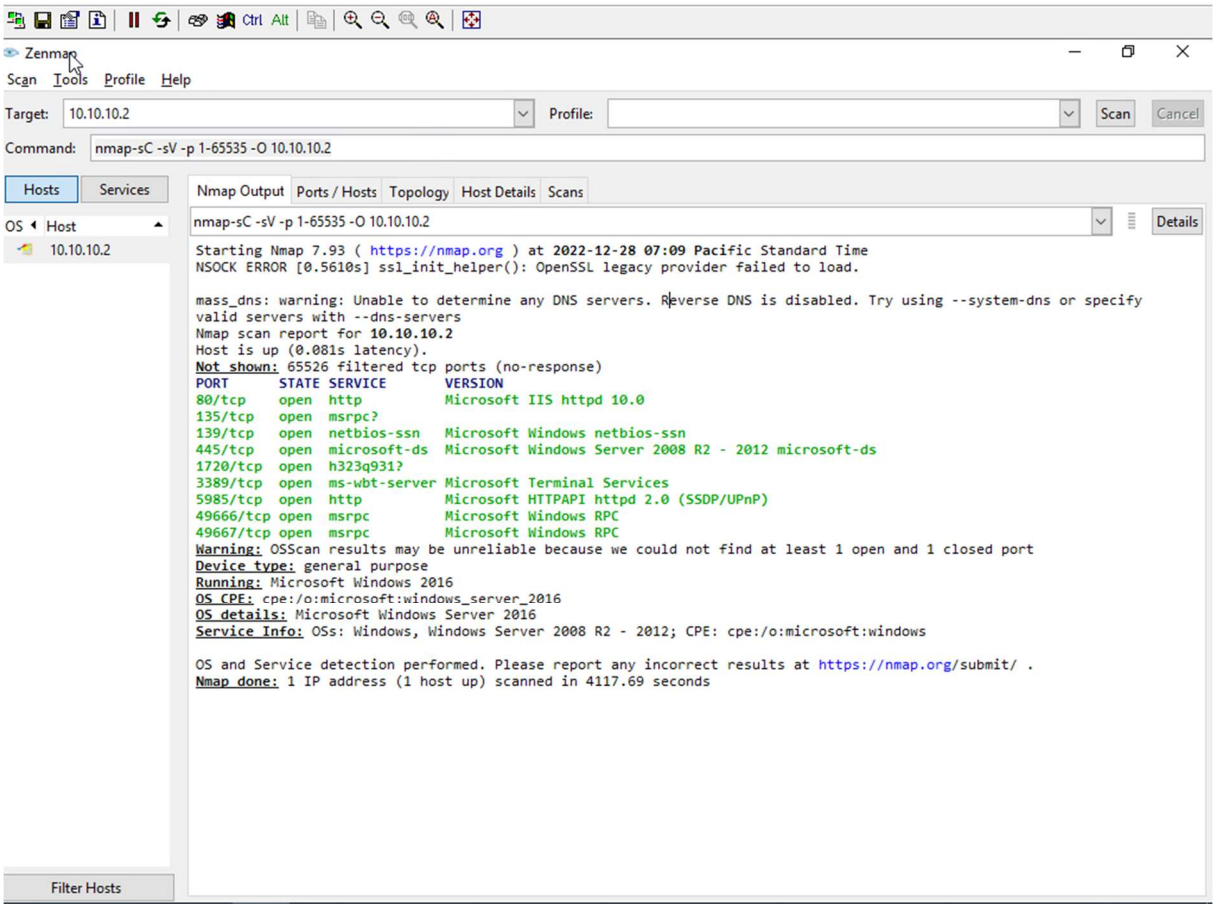
Αναφορικά με τις ρυθμίσεις των τερματικών συσκευών και των δικτυακών συσκευών της νέας τοπολογίας, υλοποιήθηκαν τα παρακάτω:

- Προστέθηκε υπολογιστής με λειτουργικό windows 10 και εγκαταστάθηκε σε αυτόν το λογισμικό Nmap.

- Ο υπολογιστής συνδέθηκε με τον ISP δρομολογητή με στατική IP 5.5.5.6/24. Η IP που δόθηκε στο interface του δρομολογητή είναι η 5.5.5.5/24.

- Στο τείχος προστασίας δημιουργήθηκε στατικός NAT κανόνας για τον web-server. Ο κανόνας ορίζει πως οτιδήποτε πακέτο έρχεται στο τείχος προστασίας με προορισμό την IP 10.10.10.2/24 να προωθείτε στην IP 172.16.20.100. Επίσης, όταν ο web-server προσπαθεί να επικοινωνήσει με κάποιον στο διαδίκτυο να μεταφράζεται η ιδιωτική του IP στην δημόσια 10.10.10.2.

Οι διαχειριστές δικτύου του οργανισμού γνωρίζοντας τους κινδύνους που παραμονεύουν με την έκθεση του τοπικού web-server στο διαδίκτυο, έχουν ρυθμίσει το τείχος προστασίας να διατηρεί logs για όλη την κίνηση με προορισμό τον web-server, καθώς επίσης έχουν ενεργοποιήσει στον web-server λογισμικό συλλογής κίνησης της κάρτας δικτύου. Και οι δύο ενέργειες έχουν σκοπό τον εντοπισμό ύποπτης κίνησης προς τον server η οποία θα οδηγήσει σε έγκαιρη πρόληψη ή σε έγκαιρη αντιμετώπιση επιθέσεων. Ο επιτιθέμενος τρέχει το λογισμικό Nmap και εκτελεί την εντολή nmap -sC -sV -p 1-65535 -O 10.10.10.2 για να εκκινήσει την σάρωση με τις προεπιλεγμένες ρυθμίσεις του προγράμματος. Μετά την ολοκλήρωση της διαδικασίας, τα αποτελέσματα που λαμβάνει είναι τα παρακάτω:



Εικόνα 36: Αποτελέσματα Nmap με προεπιλεγμένες ρυθμίσεις

Starting Nmap 7.93 (https://nmap.org) at 2022-12-30 11:14 Pacific Standard Time

NSOCK ERROR [0.5400s] ssl_init_helper(): OpenSSL legacy provider failed to load.

Nmap scan report for 10.10.10.2

Host is up (0.10s latency).

Not shown: 49992 filtered tcp ports (no-response)

PORT STATE SERVICE VERSION

80/tcp open http Microsoft IIS httpd 10.0

135/tcp open msrpc?

139/tcp open netbios-ssn Microsoft Windows netbios-ssn

445/tcp open microsoft-ds Microsoft Windows Server 2008 R2 - 2012 microsoft-ds

1720/tcp open h323q931?

3389/tcp open ms-wbt-server Microsoft Terminal Services

49666/tcp open msrpc Microsoft Windows RPC

49667/tcp open msrpc Microsoft Windows RPC

Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port

Device type: general purpose

Running: Microsoft Windows 2016

OS CPE: cpe:/o:microsoft:windows_server_2016

OS details: Microsoft Windows Server 2016

Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .

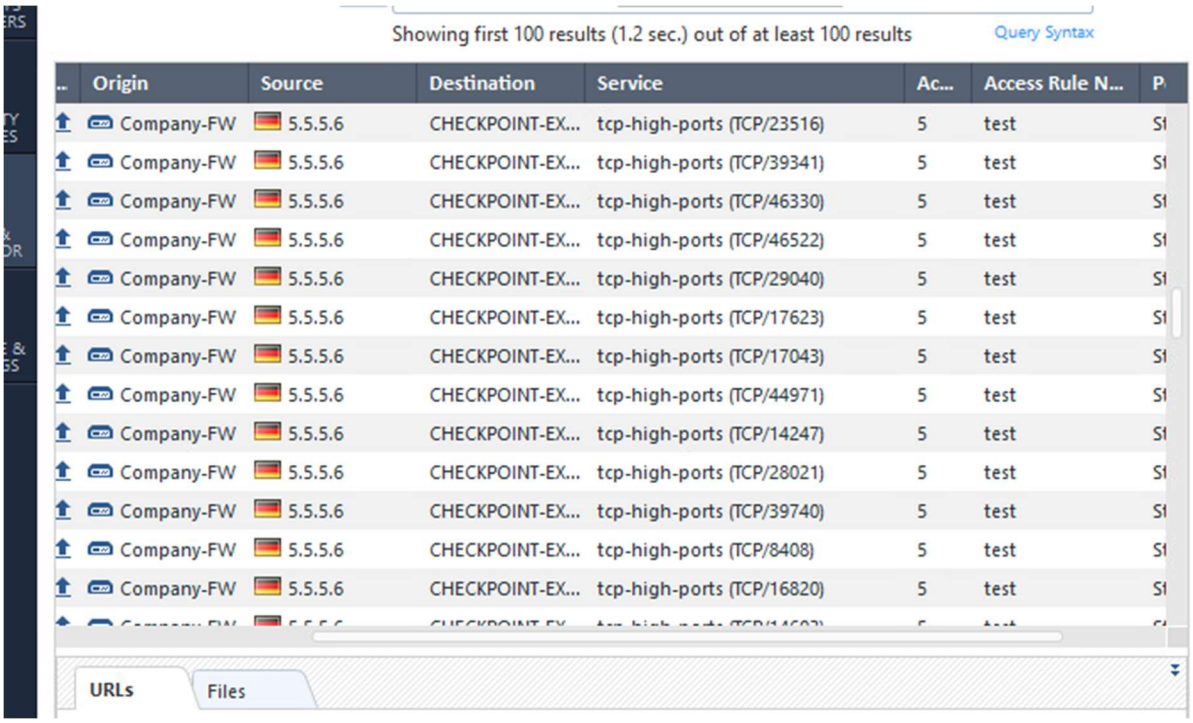
Nmap done: 1 IP address (1 host up) scanned in 1356.43 seconds

Τα παραπάνω στοιχεία ενημερώνουν τον επιτιθέμενο πως μετά την σάρωση της IP 10.10.10.2 το λογισμικό ανακάλυψε πως το λειτουργικό σύστημα της συσκευής που χρησιμοποιεί αυτήν την διεύθυνση είναι Windows και πιο συγκεκριμένα Windows Server 2016. Επιπλέον τον ενημερώνει πως ψάχτηκαν 65535 πόρτες και βρέθηκαν ανοιχτές οι 80, 135, 139, 445, 1720, 3389, 49666 και 49667. Στην ανάλυση των πορτών αναφέρεται το IPv4 πρωτόκολλο της πόρτας και ποιες εφαρμογές τις χρησιμοποιούν αυτές τις πόρτες. Οπότε:

- Πόρτα 80 → web services
- Πόρτα 135 → Windows remote access and remote management
- Πόρτα 139 → netbios session services
- Πόρτα 445 → Windows SMB Services
- Πόρτα 1720 → H.323 teleconferencing protocol
- Πόρτα 3389 → Windows Remote Desktop Connection
- Πόρτα 49666 → local ports, used by Task Scheduler, Spooler, Eventlog
- Πόρτα 49667 → local ports, used by Task Scheduler, Spooler, Eventlog

Όλες οι παραπάνω είναι πιθανοί δίοδοι για τον επιτιθέμενο με στόχο την εισχώρηση του στο εσωτερικό ιδιωτικό δίκτυο του οργανισμού. Ανάλογα με τις τεχνικές επιθέσεων που γνωρίζει να χειριστεί, θα στοχεύσει και στις ανάλογες πόρτες.

Την ίδια στιγμή που το Nmap παρείχε αυτές τις πληροφορίες στον επιτιθέμενο, οι διαχειριστές δικτύου λάμβαναν πληροφορίες από τα εργαλεία που είχαν εγκαταστήσει στις συσκευές τους. Το τείχος προστασίας παρουσίασε τα παρακάτω αρχεία logs:



Εικόνα 37: Αρχεία καταγραφής logs Checkpoint

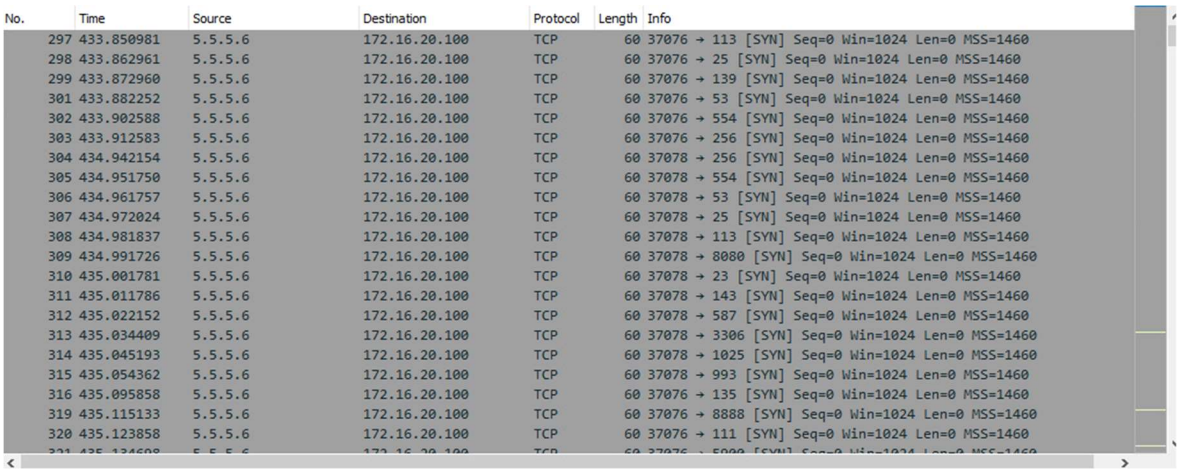
Time	Blade	Action	Source	Destination	Service/Port	Policy
12/30/2022 3:15:32 AM	Firewall	Accept	5.5.5.6	CHECPOINT-EXTERNAL(10.10.10.2)	TCP/8027	test
12/30/2022 3:15:32 AM	Firewall	Accept	5.5.5.6	CHECPOINT-EXTERNAL(10.10.10.2)	TCP/30307	test
12/30/2022 3:15:32 AM	Firewall	Accept	5.5.5.6	CHECPOINT-EXTERNAL(10.10.10.2)	TCP/30543	test
12/30/2022 3:15:32 AM	Firewall	Accept	5.5.5.6	CHECPOINT-EXTERNAL(10.10.10.2)	TCP/2193	test
12/30/2022 3:15:32 AM	Firewall	Accept	5.5.5.6	CHECPOINT-EXTERNAL(10.10.10.2)	TCP/8241	test
12/30/2022 3:15:32 AM	Firewall	Accept	5.5.5.6	CHECPOINT-EXTERNAL(10.10.10.2)	TCP/20117	test
12/30/2022 3:15:32 AM	Firewall	Accept	5.5.5.6	CHECPOINT-EXTERNAL(10.10.10.2)	TCP/32015	test
12/30/2022 3:15:32 AM	Firewall	Accept	5.5.5.6	CHECPOINT-EXTERNAL(10.10.10.2)	TCP/25510	test
12/30/2022 3:15:32 AM	Firewall	Accept	5.5.5.6	CHECPOINT-EXTERNAL(10.10.10.2)	TCP/11740	test
12/30/2022 3:15:32 AM	Firewall	Accept	5.5.5.6	CHECPOINT-EXTERNAL(10.10.10.2)	TCP/44605	test
12/30/2022 3:15:32 AM	Firewall	Accept	5.5.5.6	CHECPOINT-EXTERNAL(10.10.10.2)	TCP/23516	test
12/30/2022 3:15:32 AM	Firewall	Accept	5.5.5.6	CHECPOINT-EXTERNAL(10.10.10.2)	TCP/39341	test

12/30/2022 3:15:32 AM	Firewall	Accept	5.5.5.6	CHECPOINT-EXTERNAL(10.10.10.2)	TCP/16301	test
12/30/2022 3:15:32 AM	Firewall	Accept	5.5.5.6	CHECPOINT-EXTERNAL(10.10.10.2)	TCP/587	test
12/30/2022 3:15:32 AM	Firewall	Accept	5.5.5.6	CHECPOINT-EXTERNAL(10.10.10.2)	TCP/25	test
12/30/2022 3:15:32 AM	Firewall	Accept	5.5.5.6	CHECPOINT-EXTERNAL(10.10.10.2)	TCP/53	test
12/30/2022 3:15:32 AM	Firewall	Accept	5.5.5.6	CHECPOINT-EXTERNAL(10.10.10.2)	TCP/32352	test
12/30/2022 3:15:32 AM	Firewall	Accept	5.5.5.6	CHECPOINT-EXTERNAL(10.10.10.2)	TCP/11492	test
12/30/2022 3:15:32 AM	Firewall	Accept	5.5.5.6	CHECPOINT-EXTERNAL(10.10.10.2)	TCP/22130	test
12/30/2022 3:15:32 AM	Firewall	Accept	5.5.5.6	CHECPOINT-EXTERNAL(10.10.10.2)	TCP/13965	test
12/30/2022 3:15:32 AM	Firewall	Accept	5.5.5.6	CHECPOINT-EXTERNAL(10.10.10.2)	TCP/28406	test
12/30/2022 3:15:32 AM	Firewall	Accept	5.5.5.6	CHECPOINT-EXTERNAL(10.10.10.2)	TCP/14283	test
12/30/2022 3:15:32 AM	Firewall	Accept	5.5.5.6	CHECPOINT-EXTERNAL(10.10.10.2)	TCP/6563	test
12/30/2022 3:15:32 AM	Firewall	Accept	5.5.5.6	CHECPOINT-EXTERNAL(10.10.10.2)	TCP/41525	test
12/30/2022 3:15:32 AM	Firewall	Accept	5.5.5.6	CHECPOINT-EXTERNAL(10.10.10.2)	TCP/6175	test
12/30/2022 3:15:32 AM	Firewall	Accept	5.5.5.6	CHECPOINT-EXTERNAL(10.10.10.2)	TCP/2324	test
12/30/2022 3:15:32 AM	Firewall	Accept	5.5.5.6	CHECPOINT-EXTERNAL(10.10.10.2)	TCP/4415	test
12/30/2022 3:15:32 AM	Firewall	Accept	5.5.5.6	CHECPOINT-EXTERNAL(10.10.10.2)	TCP/9152	test
12/30/2022 3:15:32 AM	Firewall	Accept	5.5.5.6	CHECPOINT-EXTERNAL(10.10.10.2)	TCP/7689	test
12/30/2022 3:15:32 AM	Firewall	Accept	5.5.5.6	CHECPOINT-EXTERNAL(10.10.10.2)	TCP/7100	test
12/30/2022 3:15:32 AM	Firewall	Accept	5.5.5.6	CHECPOINT-EXTERNAL(10.10.10.2)	TCP/29957	test
12/30/2022 3:15:32 AM	Firewall	Accept	5.5.5.6	CHECPOINT-EXTERNAL(10.10.10.2)	TCP/61161	test
12/30/2022 3:15:32 AM	Firewall	Accept	5.5.5.6	CHECPOINT-EXTERNAL(10.10.10.2)	TCP/10212	test
12/30/2022 3:15:32 AM	Firewall	Accept	5.5.5.6	CHECPOINT-EXTERNAL(10.10.10.2)	TCP/5554	test
12/30/2022 3:15:32 AM	Firewall	Accept	5.5.5.6	CHECPOINT-EXTERNAL(10.10.10.2)	TCP/39940	test
12/30/2022 3:15:32 AM	Firewall	Accept	5.5.5.6	CHECPOINT-EXTERNAL(10.10.10.2)	TCP/22659	test

12/30/2022 3:15:32 AM	Firewall	Accept	5.5.5.6	CHECPOINT-EXTERNAL(10.10.10.2)	TCP/61147	test
12/30/2022 3:15:32 AM	Firewall	Accept	5.5.5.6	CHECPOINT-EXTERNAL(10.10.10.2)	TCP/54222	test
12/30/2022 3:15:32 AM	Firewall	Accept	5.5.5.6	CHECPOINT-EXTERNAL(10.10.10.2)	TCP/20622	test
12/30/2022 3:15:32 AM	Firewall	Accept	5.5.5.6	CHECPOINT-EXTERNAL(10.10.10.2)	TCP/47158	test
12/30/2022 3:15:32 AM	Firewall	Accept	5.5.5.6	CHECPOINT-EXTERNAL(10.10.10.2)	TCP/59507	test
12/30/2022 3:15:32 AM	Firewall	Accept	5.5.5.6	CHECPOINT-EXTERNAL(10.10.10.2)	TCP/2736	test
12/30/2022 3:15:32 AM	Firewall	Accept	5.5.5.6	CHECPOINT-EXTERNAL(10.10.10.2)	TCP/57454	test
12/30/2022 3:15:32 AM	Firewall	Accept	5.5.5.6	CHECPOINT-EXTERNAL(10.10.10.2)	TCP/5611	test
12/30/2022 3:15:32 AM	Firewall	Accept	5.5.5.6	CHECPOINT-EXTERNAL(10.10.10.2)	TCP/51911	test
12/30/2022 3:15:32 AM	Firewall	Accept	5.5.5.6	CHECPOINT-EXTERNAL(10.10.10.2)	TCP/53789	test
12/30/2022 3:15:32 AM	Firewall	Accept	5.5.5.6	CHECPOINT-EXTERNAL(10.10.10.2)	TCP/9434	test
12/30/2022 3:15:32 AM	Firewall	Accept	5.5.5.6	CHECPOINT-EXTERNAL(10.10.10.2)	TCP/17435	test
12/30/2022 3:15:32 AM	Firewall	Accept	5.5.5.6	CHECPOINT-EXTERNAL(10.10.10.2)	TCP/50637	test
12/30/2022 3:15:32 AM	Firewall	Accept	5.5.5.6	CHECPOINT-EXTERNAL(10.10.10.2)	TCP/65255	test

Εικόνα 38: Αρχεία καταγραφής logs Checkpoint-2

Τα παραπάνω στοιχεία είναι αρκετά ώστε έμπειροι μηχανικοί να αντιληφθούν πως η κίνηση αυτή είναι ασυνήθιστη και πρόκειται για το λεγόμενο port scanning. Οι κινήσεις τους θα πρέπει να είναι άμεσες και θα αναφερθούν παρακάτω. Για να υπάρχει ολοκληρωμένη εικόνα από την αρχή μέχρι το τέλος της κίνησης, οι διαχειριστές θα πρέπει να ελέγξουν και τα πακέτα που φτάνουν στον web-server αφού είναι προφανές πως πρόκειται για τον στόχο της επίθεσης. Ο έλεγχος αυτός πραγματοποιείται με λογισμικά συλλογής δικτυακής κίνησης. Στα συγκεκριμένα σενάρια γίνεται χρήση ενός από τα δημοφιλέστερα λογισμικά ανοικτού κώδικα στο διαδίκτυο, το Wireshark. Το Wireshark έχει πολλές δυνατότητες ανάλυσης κίνησης, αλλά στην συγκεκριμένη περίπτωση χρειάζεται μόνο να γίνει έλεγχος για τα ποια πακέτα φθάνουν στον web-server και σε ποιες πόρτες προσπαθούν να επικοινωνήσουν μαζί του.



No.	Time	Source	Destination	Protocol	Length	Info
297	433.850981	5.5.5.6	172.16.20.100	TCP	60	37076 → 113 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
298	433.862961	5.5.5.6	172.16.20.100	TCP	60	37076 → 25 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
299	433.872960	5.5.5.6	172.16.20.100	TCP	60	37076 → 139 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
301	433.882252	5.5.5.6	172.16.20.100	TCP	60	37076 → 53 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
302	433.902588	5.5.5.6	172.16.20.100	TCP	60	37076 → 554 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
303	433.912583	5.5.5.6	172.16.20.100	TCP	60	37076 → 256 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
304	434.942154	5.5.5.6	172.16.20.100	TCP	60	37078 → 256 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
305	434.951750	5.5.5.6	172.16.20.100	TCP	60	37078 → 554 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
306	434.961757	5.5.5.6	172.16.20.100	TCP	60	37078 → 53 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
307	434.972024	5.5.5.6	172.16.20.100	TCP	60	37078 → 25 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
308	434.981837	5.5.5.6	172.16.20.100	TCP	60	37078 → 113 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
309	434.991726	5.5.5.6	172.16.20.100	TCP	60	37078 → 8080 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
310	435.001781	5.5.5.6	172.16.20.100	TCP	60	37078 → 23 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
311	435.011786	5.5.5.6	172.16.20.100	TCP	60	37078 → 143 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
312	435.022152	5.5.5.6	172.16.20.100	TCP	60	37078 → 587 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
313	435.034409	5.5.5.6	172.16.20.100	TCP	60	37078 → 3306 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
314	435.045193	5.5.5.6	172.16.20.100	TCP	60	37078 → 1025 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
315	435.054362	5.5.5.6	172.16.20.100	TCP	60	37078 → 993 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
316	435.095858	5.5.5.6	172.16.20.100	TCP	60	37076 → 135 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
319	435.115133	5.5.5.6	172.16.20.100	TCP	60	37076 → 8888 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
320	435.123858	5.5.5.6	172.16.20.100	TCP	60	37076 → 111 [SYN] Seq=0 Win=1024 Len=0 MSS=1460

Εικόνα 39: Αρχεία καταγραφής logs Wireshark Web-Server

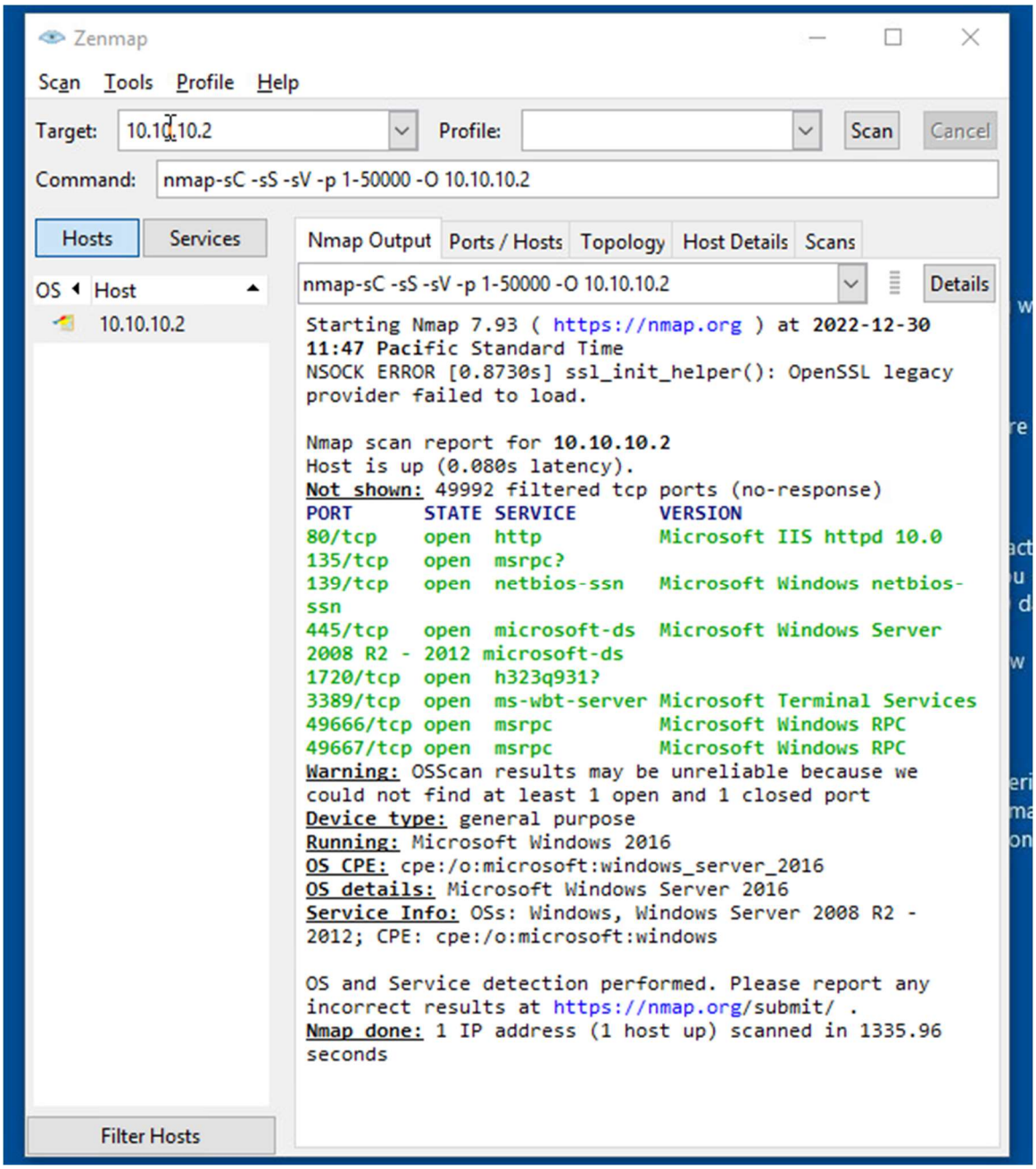
Packet No.	Time	Source	Destination	Protocol	Length	Info
240	401	5.5.5.6	172.16.20.100	TCP	60	49942 --> 80
242	401	5.5.5.6	172.16.20.100	TCP	60	49942 --> 80
243	401	5.5.5.6	172.16.20.100	TCP	60	49942 --> 80
244	401	5.5.5.6	172.16.20.100	TCP	60	49942 --> 80
246	402	5.5.5.6	172.16.20.100	TCP	60	49943 --> 80
248	402	5.5.5.6	172.16.20.100	TCP	60	49943 --> 80
249	402	5.5.5.6	172.16.20.100	TCP	60	49943 --> 80
251	402	5.5.5.6	172.16.20.100	TCP	60	49943 --> 80
257	402	5.5.5.6	172.16.20.100	TCP	60	49943 --> 80
258	402	5.5.5.6	172.16.20.100	TCP	60	49943 --> 80
276	420	5.5.5.6	172.16.20.100	TCP	60	37076 --> 993
278	420	5.5.5.6	172.16.20.100	TCP	60	37076 --> 1025
279	420	5.5.5.6	172.16.20.100	TCP	60	37076 --> 587
288	433	5.5.5.6	172.16.20.100	TCP	60	37076 --> 3306
289	433	5.5.5.6	172.16.20.100	TCP	60	37076 --> 143
290	433	5.5.5.6	172.16.20.100	TCP	60	37076 --> 23
291	433	5.5.5.6	172.16.20.100	TCP	60	37076 --> 80
292	433	5.5.5.6	172.16.20.100	TCP	60	37076 --> 8080
293	433	5.5.5.6	172.16.20.100	TCP	60	37076 --> 113
294	433	5.5.5.6	172.16.20.100	TCP	60	37076 --> 25
296	433	5.5.5.6	172.16.20.100	TCP	60	37076 --> 139
297	433	5.5.5.6	172.16.20.100	TCP	60	37076 --> 53
298	433	5.5.5.6	172.16.20.100	TCP	60	37076 --> 554
299	433	5.5.5.6	172.16.20.100	TCP	60	37076 --> 256
301	433	5.5.5.6	172.16.20.100	TCP	60	37078 --> 256
302	433	5.5.5.6	172.16.20.100	TCP	60	37078 --> 554
303	433	5.5.5.6	172.16.20.100	TCP	60	37078 --> 53
304	434	5.5.5.6	172.16.20.100	TCP	60	37078 --> 25

305	434	5.5.5.6	172.16.20.100	TCP	60	37078 --> 113
306	434	5.5.5.6	172.16.20.100	TCP	60	37078 --> 8080
307	434	5.5.5.6	172.16.20.100	TCP	60	37078 --> 23
308	434	5.5.5.6	172.16.20.100	TCP	60	37078 --> 143
309	434	5.5.5.6	172.16.20.100	TCP	60	37078 --> 587
310	435	5.5.5.6	172.16.20.100	TCP	60	37078 --> 3306
311	435	5.5.5.6	172.16.20.100	TCP	60	37078 --> 1025
312	435	5.5.5.6	172.16.20.100	TCP	60	37078 --> 993
313	435	5.5.5.6	172.16.20.100	TCP	60	37078 --> 135
314	435	5.5.5.6	172.16.20.100	TCP	60	37076 --> 8888
315	435	5.5.5.6	172.16.20.100	TCP	60	37076 --> 111
316	435	5.5.5.6	172.16.20.100	TCP	60	37076 --> 5900
319	435	5.5.5.6	172.16.20.100	TCP	60	37076 --> 995
320	435	5.5.5.6	172.16.20.100	TCP	60	37076 --> 1723
321	435	5.5.5.6	172.16.20.100	TCP	60	37076 --> 21
322	435	5.5.5.6	172.16.20.100	TCP	60	37076 --> 3389
323	435	5.5.5.6	172.16.20.100	TCP	60	37076 --> 110
324	435	5.5.5.6	172.16.20.100	TCP	60	37076 --> 22

Εικόνα 40: Αρχεία καταγραφής logs Wireshark web-server-2

Από τις παραπάνω εικόνες είναι φανερό πως τα πακέτα ερωτημάτων για ανοιχτές πόρτες φθάνουν στον web-server.

Στην δεύτερη φάση υλοποίησης του σεναρίου πραγματοποιήθηκε σάρωση με stealth mode (αναλύθηκε παραπάνω) ώστε να παρατηρηθεί η συμπεριφορά των συσκευών και λογισμικών συλλογής κίνησης, Τα αποτελέσματα φαίνονται στις παρακάτω εικόνες:



Εικόνα 41: Αποτελέσματα Nmap σε stealth mode

Starting Nmap 7.93 (https://nmap.org) at 2022-12-30 11:47 Pacific Standard Time

NSOCK ERROR [0.8730s] ssl_init_helper(): OpenSSL legacy provider failed to load.

Nmap scan report for 10.10.10.2

Host is up (0.080s latency).

Not shown: 49992 filtered tcp ports (no-response)

PORT STATE SERVICE VERSION

80/tcp open http Microsoft IIS httpd 10.0

135/tcp open msrpc?

139/tcp open netbios-ssn Microsoft Windows netbios-ssn

445/tcp open microsoft-ds Microsoft Windows Server 2008 R2 - 2012 microsoft-ds

1720/tcp open h323q931?

3389/tcp open ms-wbt-server Microsoft Terminal Services

49666/tcp open msrpc Microsoft Windows RPC

49667/tcp open msrpc Microsoft Windows RPC

Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port

Device type: general purpose

Running: Microsoft Windows 2016

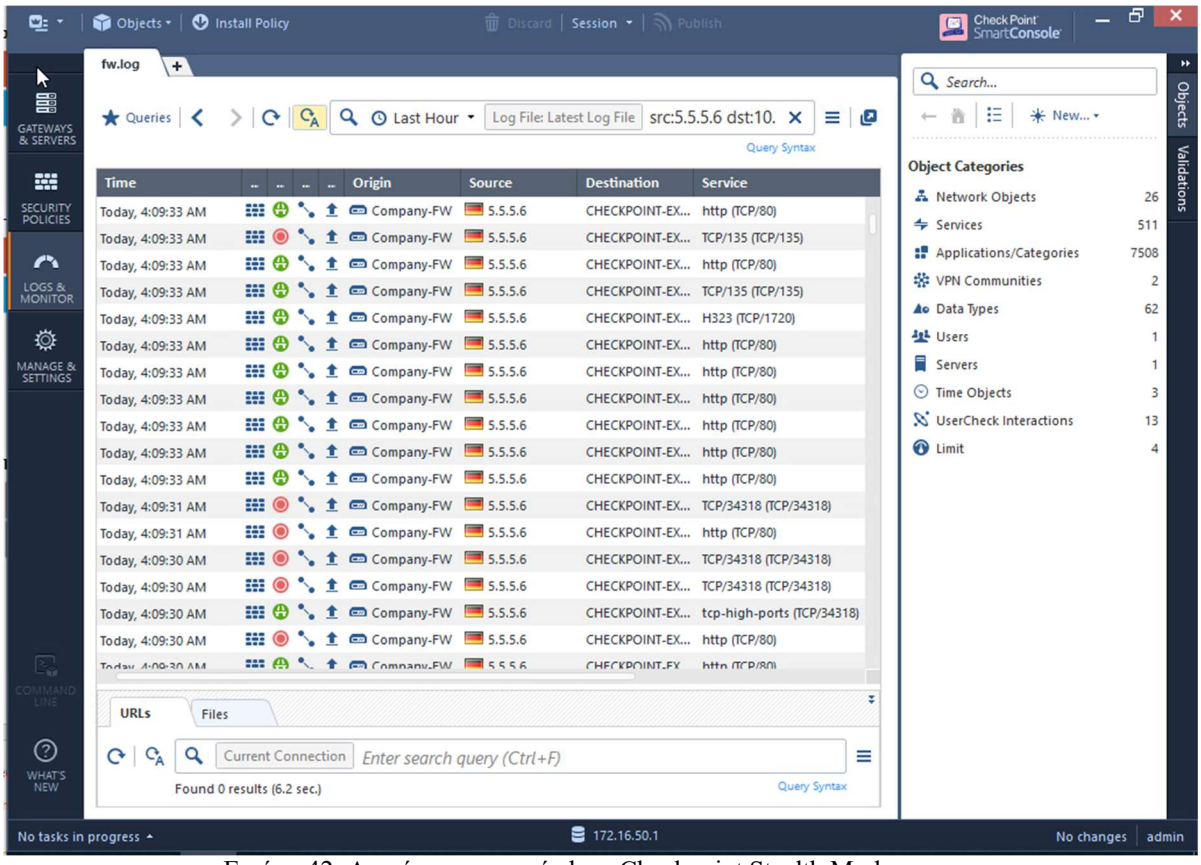
OS CPE: cpe:/o:microsoft:windows_server_2016

OS details: Microsoft Windows Server 2016

Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .

Nmap done: 1 IP address (1 host up) scanned in 1335.96 seconds



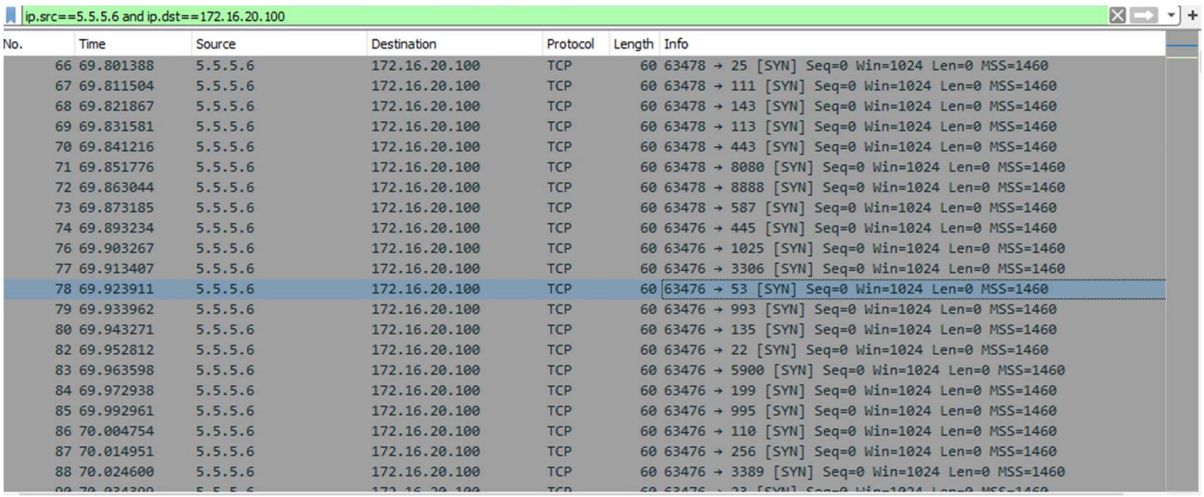
Εικόνα 42: Αρχεία καταγραφής logs Checkpoint Stealth Mode

Time	Blade	Action	Source	Destination	Service/Port	Policy
12/30/2022 4:06:52 AM	Firewall	Accept	5.5.5.6	CHECPOINT-EXTERNAL(10.10.10.2)	TCP/139	test
12/30/2022 4:06:52 AM	Firewall	Accept	5.5.5.6	CHECPOINT-EXTERNAL(10.10.10.2)	TCP/135	test
12/30/2022 4:06:52 AM	Firewall	Accept	5.5.5.6	CHECPOINT-EXTERNAL(10.10.10.2)	TCP/80	test
12/30/2022 4:06:51 AM	Firewall	Accept	5.5.5.6	CHECPOINT-EXTERNAL(10.10.10.2)	TCP/1121	test
12/30/2022 4:06:51 AM	Firewall	Accept	5.5.5.6	CHECPOINT-EXTERNAL(10.10.10.2)	TCP/49061	test
12/30/2022 4:06:51 AM	Firewall	Accept	5.5.5.6	CHECPOINT-EXTERNAL(10.10.10.2)	TCP/21945	test
12/30/2022 4:06:51 AM	Firewall	Accept	5.5.5.6	CHECPOINT-EXTERNAL(10.10.10.2)	TCP/9273	test
12/30/2022 4:06:51 AM	Firewall	Accept	5.5.5.6	CHECPOINT-EXTERNAL(10.10.10.2)	TCP/8061	test
12/30/2022 4:06:51 AM	Firewall	Accept	5.5.5.6	CHECPOINT-EXTERNAL(10.10.10.2)	TCP/13857	test

12/30/2022 4:06:51 AM	Firewall	Accept	5.5.5.6	CHECPOINT-EXTERNAL(10.10.10.2)	TCP/11596	test
12/30/2022 4:06:51 AM	Firewall	Accept	5.5.5.6	CHECPOINT-EXTERNAL(10.10.10.2)	TCP/16369	test
12/30/2022 4:06:51 AM	Firewall	Accept	5.5.5.6	CHECPOINT-EXTERNAL(10.10.10.2)	TCP/5048	test
12/30/2022 4:06:51 AM	Firewall	Accept	5.5.5.6	CHECPOINT-EXTERNAL(10.10.10.2)	TCP/59592	test
12/30/2022 4:06:51 AM	Firewall	Accept	5.5.5.6	CHECPOINT-EXTERNAL(10.10.10.2)	TCP/49971	test
12/30/2022 4:06:51 AM	Firewall	Accept	5.5.5.6	CHECPOINT-EXTERNAL(10.10.10.2)	TCP/24900	test
12/30/2022 4:06:51 AM	Firewall	Accept	5.5.5.6	CHECPOINT-EXTERNAL(10.10.10.2)	TCP/37887	test
12/30/2022 4:06:51 AM	Firewall	Accept	5.5.5.6	CHECPOINT-EXTERNAL(10.10.10.2)	TCP/4254	test
12/30/2022 4:06:51 AM	Firewall	Accept	5.5.5.6	CHECPOINT-EXTERNAL(10.10.10.2)	TCP/446	test
12/30/2022 4:06:51 AM	Firewall	Accept	5.5.5.6	CHECPOINT-EXTERNAL(10.10.10.2)	TCP/4179	test
12/30/2022 4:06:51 AM	Firewall	Accept	5.5.5.6	CHECPOINT-EXTERNAL(10.10.10.2)	TCP/30009	test
12/30/2022 4:06:51 AM	Firewall	Accept	5.5.5.6	CHECPOINT-EXTERNAL(10.10.10.2)	TCP/50968	test
12/30/2022 4:06:51 AM	Firewall	Accept	5.5.5.6	CHECPOINT-EXTERNAL(10.10.10.2)	TCP/11565	test
12/30/2022 4:06:51 AM	Firewall	Accept	5.5.5.6	CHECPOINT-EXTERNAL(10.10.10.2)	TCP/44507	test
12/30/2022 4:06:51 AM	Firewall	Accept	5.5.5.6	CHECPOINT-EXTERNAL(10.10.10.2)	TCP/14691	test
12/30/2022 4:06:51 AM	Firewall	Accept	5.5.5.6	CHECPOINT-EXTERNAL(10.10.10.2)	TCP/61174	test
12/30/2022 4:06:51 AM	Firewall	Accept	5.5.5.6	CHECPOINT-EXTERNAL(10.10.10.2)	TCP/23823	test
12/30/2022 4:06:51 AM	Firewall	Accept	5.5.5.6	CHECPOINT-EXTERNAL(10.10.10.2)	TCP/15204	test
12/30/2022 4:06:51 AM	Firewall	Accept	5.5.5.6	CHECPOINT-EXTERNAL(10.10.10.2)	TCP/56336	test
12/30/2022 4:06:51 AM	Firewall	Accept	5.5.5.6	CHECPOINT-EXTERNAL(10.10.10.2)	TCP/34326	test
12/30/2022 4:06:51 AM	Firewall	Accept	5.5.5.6	CHECPOINT-EXTERNAL(10.10.10.2)	TCP/16731	test
12/30/2022 4:06:51 AM	Firewall	Accept	5.5.5.6	CHECPOINT-EXTERNAL(10.10.10.2)	TCP/27937	test
12/30/2022 4:06:51 AM	Firewall	Accept	5.5.5.6	CHECPOINT-EXTERNAL(10.10.10.2)	TCP/52743	test
12/30/2022 4:06:51 AM	Firewall	Accept	5.5.5.6	CHECPOINT-EXTERNAL(10.10.10.2)	TCP/24054	test
12/30/2022 4:06:51 AM	Firewall	Accept	5.5.5.6	CHECPOINT-EXTERNAL(10.10.10.2)	TCP/12765	test

12/30/2022 4:06:51 AM	Firewall	Accept	5.5.5.6	CHECPOINT-EXTERNAL(10.10.10.2)	TCP/11555	test
12/30/2022 4:06:51 AM	Firewall	Accept	5.5.5.6	CHECPOINT-EXTERNAL(10.10.10.2)	TCP/17797	test
12/30/2022 4:06:51 AM	Firewall	Accept	5.5.5.6	CHECPOINT-EXTERNAL(10.10.10.2)	TCP/46566	test
12/30/2022 4:06:51 AM	Firewall	Accept	5.5.5.6	CHECPOINT-EXTERNAL(10.10.10.2)	TCP/45769	test
12/30/2022 4:06:51 AM	Firewall	Accept	5.5.5.6	CHECPOINT-EXTERNAL(10.10.10.2)	TCP/39810	test
12/30/2022 4:06:51 AM	Firewall	Accept	5.5.5.6	CHECPOINT-EXTERNAL(10.10.10.2)	TCP/37168	test
12/30/2022 4:06:51 AM	Firewall	Accept	5.5.5.6	CHECPOINT-EXTERNAL(10.10.10.2)	TCP/1768	test
12/30/2022 4:06:51 AM	Firewall	Accept	5.5.5.6	CHECPOINT-EXTERNAL(10.10.10.2)	TCP/17381	test
12/30/2022 4:06:51 AM	Firewall	Accept	5.5.5.6	CHECPOINT-EXTERNAL(10.10.10.2)	TCP/39530	test
12/30/2022 4:06:51 AM	Firewall	Accept	5.5.5.6	CHECPOINT-EXTERNAL(10.10.10.2)	TCP/52738	test
12/30/2022 4:06:51 AM	Firewall	Accept	5.5.5.6	CHECPOINT-EXTERNAL(10.10.10.2)	TCP/58952	test
12/30/2022 4:06:51 AM	Firewall	Accept	5.5.5.6	CHECPOINT-EXTERNAL(10.10.10.2)	TCP/24388	test
12/30/2022 4:06:51 AM	Firewall	Accept	5.5.5.6	CHECPOINT-EXTERNAL(10.10.10.2)	TCP/16746	test
12/30/2022 4:06:51 AM	Firewall	Accept	5.5.5.6	CHECPOINT-EXTERNAL(10.10.10.2)	TCP/53482	test
12/30/2022 4:06:51 AM	Firewall	Accept	5.5.5.6	CHECPOINT-EXTERNAL(10.10.10.2)	TCP/575	test
12/30/2022 4:06:51 AM	Firewall	Accept	5.5.5.6	CHECPOINT-EXTERNAL(10.10.10.2)	TCP/31428	test

Εικόνα 43: Αρχεία καταγραφής logs Checkpoint Stealth Mode-2



Εικόνα 44: Αρχεία καταγραφής logs Wireshark web-server Stealth Mode

Packet No.	Time	Source	Destination	Protocol	Length	Info
63	401	5.5.5.6	172.16.20.100	TCP	60	63478 --> 21
64	401	5.5.5.6	172.16.20.100	TCP	60	63478 --> 1723
65	401	5.5.5.6	172.16.20.100	TCP	60	63478 --> 554
66	401	5.5.5.6	172.16.20.100	TCP	60	63478 --> 25
67	402	5.5.5.6	172.16.20.100	TCP	60	63478 --> 111
68	402	5.5.5.6	172.16.20.100	TCP	60	63478 --> 143
69	402	5.5.5.6	172.16.20.100	TCP	60	63478 --> 111
70	402	5.5.5.6	172.16.20.100	TCP	60	63478 --> 443
71	402	5.5.5.6	172.16.20.100	TCP	60	63478 --> 8080
72	402	5.5.5.6	172.16.20.100	TCP	60	63478 --> 8888
73	420	5.5.5.6	172.16.20.100	TCP	60	63478 --> 587
74	420	5.5.5.6	172.16.20.100	TCP	60	63476 --> 445
76	420	5.5.5.6	172.16.20.100	TCP	60	63476 --> 1025
77	433	5.5.5.6	172.16.20.100	TCP	60	63476 --> 3306
78	433	5.5.5.6	172.16.20.100	TCP	60	63476 --> 53
79	433	5.5.5.6	172.16.20.100	TCP	60	63476 --> 993
80	433	5.5.5.6	172.16.20.100	TCP	60	63476 --> 135
82	433	5.5.5.6	172.16.20.100	TCP	60	63476 --> 22
83	433	5.5.5.6	172.16.20.100	TCP	60	63476 --> 5900
84	433	5.5.5.6	172.16.20.100	TCP	60	63476 --> 199
85	433	5.5.5.6	172.16.20.100	TCP	60	63476 --> 995
86	433	5.5.5.6	172.16.20.100	TCP	60	63476 --> 110
87	433	5.5.5.6	172.16.20.100	TCP	60	63476 --> 256
88	433	5.5.5.6	172.16.20.100	TCP	60	63476 --> 3389

90	433	5.5.5.6	172.16.20.100	TCP	60	63476 --> 23
91	433	5.5.5.6	172.16.20.100	TCP	60	63476 --> 80
93	433	5.5.5.6	172.16.20.100	TCP	60	63476 --> 19084
94	434	5.5.5.6	172.16.20.100	TCP	60	63476 --> 42564
95	434	5.5.5.6	172.16.20.100	TCP	60	63476 --> 22487
96	434	5.5.5.6	172.16.20.100	TCP	60	63476 --> 6487
98	434	5.5.5.6	172.16.20.100	TCP	60	63476 --> 42716
99	434	5.5.5.6	172.16.20.100	TCP	60	63476 --> 16378
100	434	5.5.5.6	172.16.20.100	TCP	60	63476 --> 49359
101	435	5.5.5.6	172.16.20.100	TCP	60	63476 --> 26102
102	435	5.5.5.6	172.16.20.100	TCP	60	63476 --> 17536
103	435	5.5.5.6	172.16.20.100	TCP	60	63476 --> 28679
104	435	5.5.5.6	172.16.20.100	TCP	60	63476 --> 35686
105	435	5.5.5.6	172.16.20.100	TCP	60	63476 --> 9067
106	435	5.5.5.6	172.16.20.100	TCP	60	63476 --> 43144
107	435	5.5.5.6	172.16.20.100	TCP	60	63476 --> 40470
108	435	5.5.5.6	172.16.20.100	TCP	60	63476 --> 38719
109	435	5.5.5.6	172.16.20.100	TCP	60	63476 --> 30120
110	435	5.5.5.6	172.16.20.100	TCP	60	63476 --> 7507
111	435	5.5.5.6	172.16.20.100	TCP	60	63476 --> 48855
112	435	5.5.5.6	172.16.20.100	TCP	60	63476 --> 43637
113	435	5.5.5.6	172.16.20.100	TCP	60	63476 --> 1881

Εικόνα 45: Αρχεία καταγραφής logs Wireshark web-server Stealth Mode-2

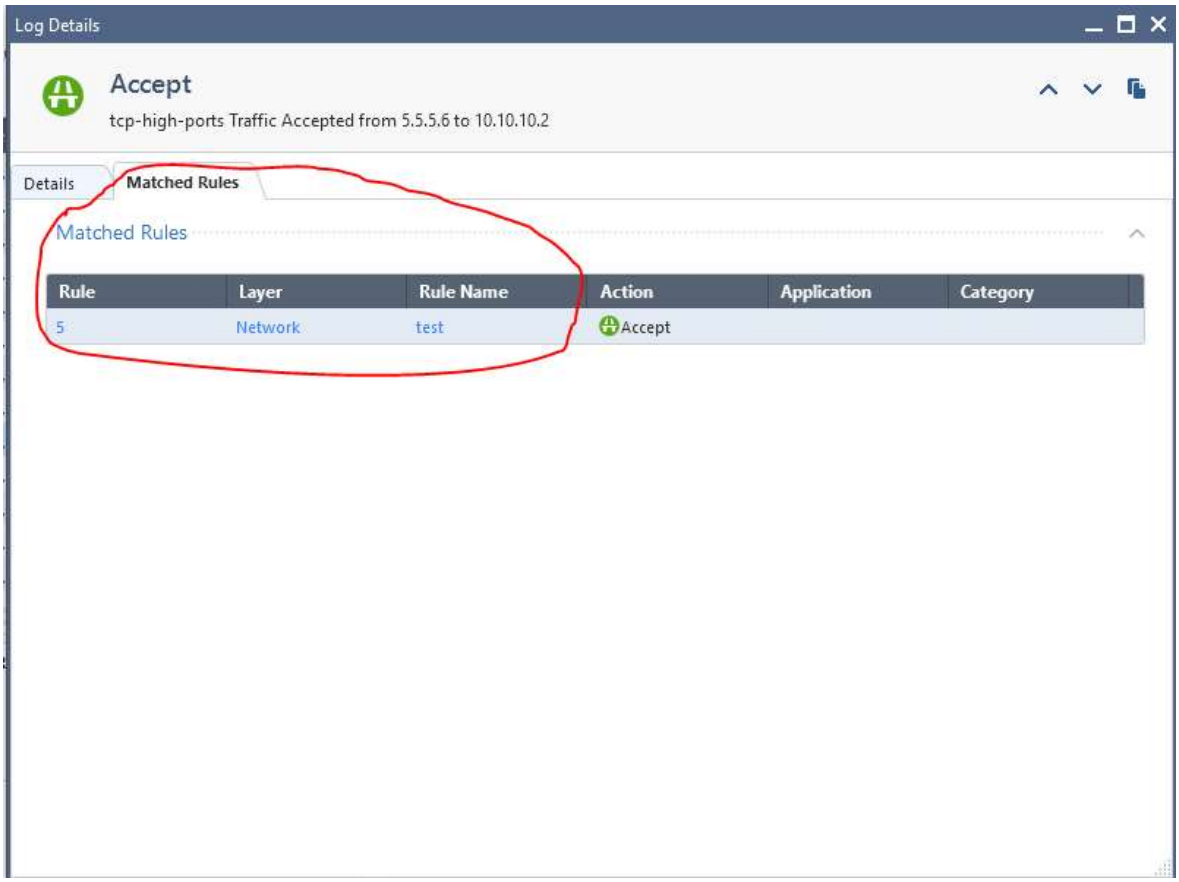
7.4.1 Σύγκριση Αποτελεσμάτων Διαφορετικών Μεθόδων Επίθεσης

Μελετώντας τα αποτελέσματα των δύο μεθόδων ανίχνευσης με το εργαλείο Nmap, διαπιστώνεται πως και οι δικτυακές συσκευές, αλλά και τα λογισμικά ανίχνευσης κίνησης ανταπεξήλθαν άριστα. Όλοι οι μηχανισμοί προστασίας και πρόληψης επιθέσεων λειτούργησαν εξαιρετικά χωρίς να τους ξεφύγει κάποια ύποπτη κίνηση. Ειδικά το τείχος προστασίας που είναι ο δίαυλος επικοινωνίας με το διαδίκτυο και το πρώτο φίλτρο κίνησης, δεν άφησε να περάσει κανένα πακέτο χωρίς να το καταγράψει στα log αρχεία του. Αξιοσημείωτο είναι πως το λογισμικό συλλογής πακέτων Wireshark εντόπισε όλα τα πακέτα, το οποίο σημαίνει πως αν και ο οποιοσδήποτε μπορεί να το αποκτήσει δωρεάν, οι προγραμματιστές του δεν το αφήνουν ανενημέρωτο και ακολουθεί τα βήματα ανάπτυξης των νέων τεχνολογιών. Πέρα από την ανίχνευση των κινήσεων και την συλλογή των απαραίτητων πληροφοριών, θα πρέπει να αναλυθούν οι δράσεις που έγιναν από τα εργαλεία που χρησιμοποιήθηκαν. Ξεκινώντας από το Nmap, θα μπορούσε κάποιος να αναφέρει πως

απέδωσε τα μέγιστα εφόσον πραγματοποίησε την ανίχνευση όπως θα έπρεπε, συν ότι πρόσφερε πολλές πληροφορίες σχετικά με τις υπηρεσίες και το λειτουργικό που τρέχει στον web-server. Στην ίδια κατηγορία μπορεί να ενταχθεί και το Wireshark. Μετά από τα κατάλληλα φιλτραρίσματα των αποτελεσμάτων δόθηκε πολύ καθαρή εικόνα για το αν και ποια πακέτα φτάσανε στην κάρτα δικτύου του web-server. Ποια όμως η απόδοση του τείχους προστασίας;

7.4.2 Ανάλυση Αποτελεσμάτων Σεναρίου 2

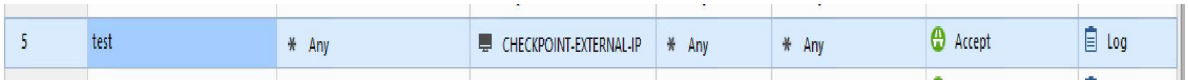
Αναλύοντας βαθύτερα τις αιτίες που το τείχος προστασίας επέτρεψε να περάσουν όλα αυτά τα πακέτα, οι διαχειριστές θα πρέπει να εντοπίσουν την πολιτική που σχετίζεται με αυτές τις δράσεις και να την επεξεργαστούν. Η ανάλυση αυτή οδηγεί στο αποτέλεσμα που φαίνεται στην παρακάτω εικόνα:



Εικόνα 46: Ανάλυση log τείχους προστασίας

Υποδεικνύει τον κανόνα από τον οποίο πέρασε η κίνηση από τον επιτιθέμενο προς τον web-server της υποδομής. Πατώντας πάνω στον υπερσύνδεσμο που αναγράφει τον αριθμό 5, το λειτουργικό σύστημα του τείχους προστασίας μας οδηγεί στο μενού των

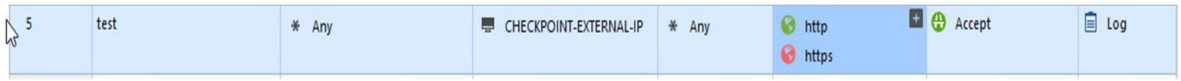
κανόνων εστιάζοντας στον συγκεκριμένο που επιλέχθηκε.



Εικόνα 47: Κανόνας 5 τείχους προστασίας

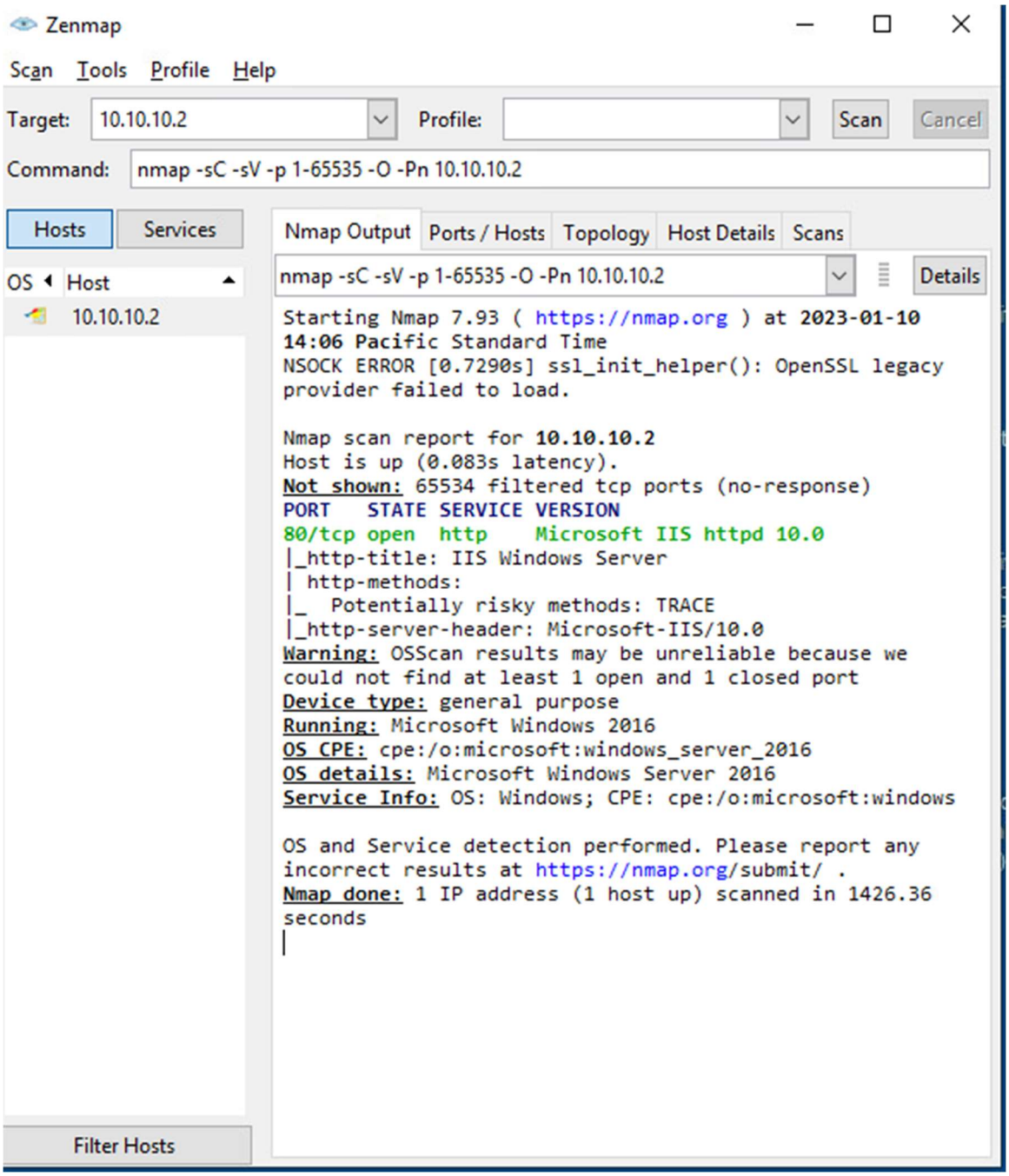
Οι πληροφορίες που εξάγονται από τον παραπάνω κανόνα είναι: Η ονομασία του κανόνα είναι test, η εκκίνηση αποστολής πακέτων γίνεται από οπουδήποτε, ο προορισμός των πακέτων είναι η δημόσια IP του τείχους προστασίας, επιτρέπονται όλα τα πρωτόκολλα, η ενέργεια για αυτά τα πακέτα που θα πραγματοποιεί το τείχος προστασίας είναι αποδοχή και τέλος να καταγράφονται τα πακέτα σε log αρχείο. Οι διαχειριστές θα πρέπει να αντιληφθούν άμεσα κατά την ανάγνωση του κανόνα πως πρόκειται για μία παραμετροποίηση εντελώς αυθαίρετη, από την στιγμή που ο σκοπός είναι να επιτραπεί μόνο οι web υπηρεσίες.

Οι τεχνικοί θα πρέπει να παραμετροποιήσουν τον κανόνα με πιο αυστηρά κριτήρια, να πραγματοποιήσουν δοκιμές από εξωτερικό δίκτυο και να ελέγξουν τα αρχεία log του τείχους προστασίας. Επομένως η ρύθμιση του κανόνα θα πρέπει να είναι η εξής:

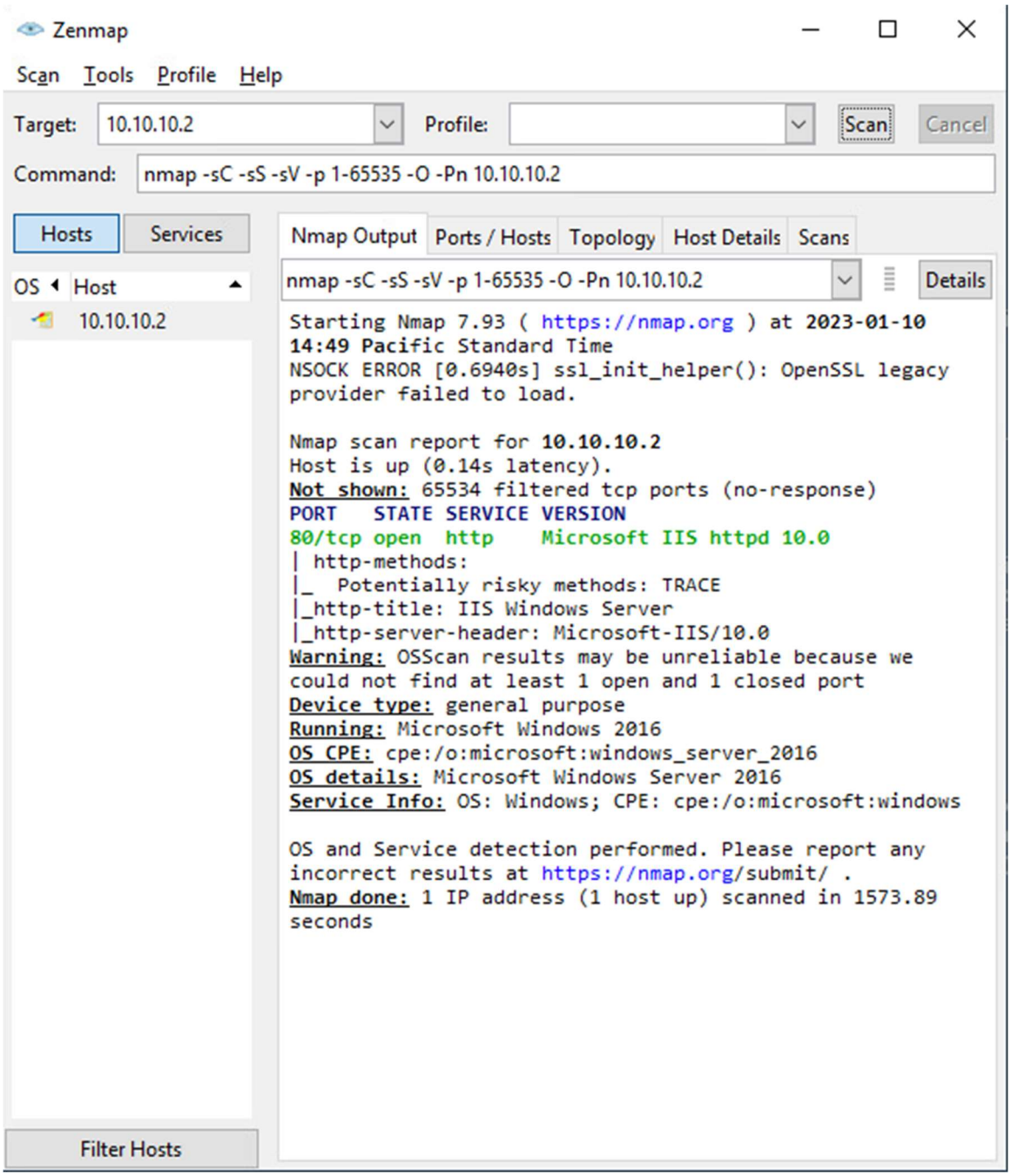


Εικόνα 48: Κανόνας 5 μετά την παραμετροποίηση

Εφόσον οι εξωτερικοί χρήστες θα πρέπει να έχουν πρόσβαση μόνο στις web υπηρεσίες του server, ο κανόνας δεν θα πρέπει να είναι τόσο γενικός και να επιτρέπει όλες τις υπηρεσίες προς τον server. Επομένως, η μοναδική αλλά άκρως σημαντική αλλαγή που πραγματοποιήθηκε στον κανόνα είναι η αλλαγή των υπηρεσιών που θα επιτρέπονται από εξωτερικούς χρήστες προς τον web-server. Μετά την αλλαγή στον κανόνα θα πρέπει να πραγματοποιηθούν δοκιμές εκ νέου, ώστε να διαπιστωθεί εάν η αλλαγή στον κανόνα είναι αρκετή ή μήπως χρειάζονται και περεταίρω ενέργειες. Οι δοκιμές με το λογισμικό Nmap σε normal και stealth λειτουργία από εξωτερικό χρήστη έδειξαν τα παρακάτω:



Εικόνα 49: Nmap με νέο κανόνα normal mode



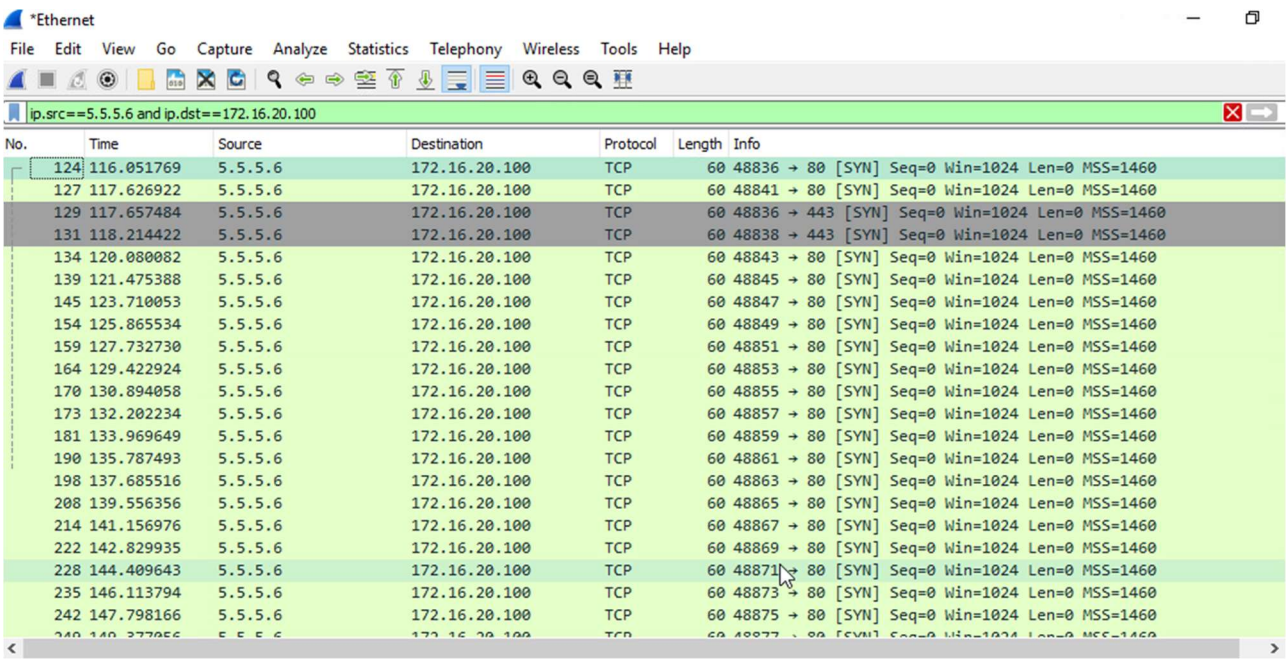
Εικόνα 50: Nmap με νέο κανόνα stealth mode

Time	..	..	..	..	Origin	Source	Destination	Service	Ac...	Access Rule N...	Policy...	Description
Today, 6:32:34 AM					Company-FW	5.5.5.6	CHECKPOINT-EX...	TCP/61682 (TCP/61682)	7	Cleanup rule	Standard	TCP/61682 Traffic Dropped from 5.5.5...
Today, 6:32:34 AM					Company-FW	5.5.5.6	CHECKPOINT-EX...	TCP/41105 (TCP/41105)	7	Cleanup rule	Standard	TCP/41105 Traffic Dropped from 5.5.5...
Today, 6:32:34 AM					Company-FW	5.5.5.6	CHECKPOINT-EX...	TCP/12721 (TCP/12721)	7	Cleanup rule	Standard	TCP/12721 Traffic Dropped from 5.5.5...
Today, 6:32:34 AM					Company-FW	5.5.5.6	CHECKPOINT-EX...	TCP/40785 (TCP/40785)	7	Cleanup rule	Standard	TCP/40785 Traffic Dropped from 5.5.5...
Today, 6:32:34 AM					Company-FW	5.5.5.6	CHECKPOINT-EX...	TCP/40318 (TCP/40318)	7	Cleanup rule	Standard	TCP/40318 Traffic Dropped from 5.5.5...
Today, 6:32:34 AM					Company-FW	5.5.5.6	CHECKPOINT-EX...	TCP/23969 (TCP/23969)	7	Cleanup rule	Standard	TCP/23969 Traffic Dropped from 5.5.5...
Today, 6:32:34 AM					Company-FW	5.5.5.6	CHECKPOINT-EX...	TCP/11846 (TCP/11846)	7	Cleanup rule	Standard	TCP/11846 Traffic Dropped from 5.5.5...
Today, 6:32:34 AM					Company-FW	5.5.5.6	CHECKPOINT-EX...	TCP/51737 (TCP/51737)	7	Cleanup rule	Standard	TCP/51737 Traffic Dropped from 5.5.5...
Today, 6:32:34 AM					Company-FW	5.5.5.6	CHECKPOINT-EX...	TCP/19293 (TCP/19293)	7	Cleanup rule	Standard	TCP/19293 Traffic Dropped from 5.5.5...
Today, 6:32:34 AM					Company-FW	5.5.5.6	CHECKPOINT-EX...	TCP/22262 (TCP/22262)	7	Cleanup rule	Standard	TCP/22262 Traffic Dropped from 5.5.5...
Today, 6:32:34 AM					Company-FW	5.5.5.6	CHECKPOINT-EX...	TCP/12615 (TCP/12615)	7	Cleanup rule	Standard	TCP/12615 Traffic Dropped from 5.5.5...
Today, 6:32:34 AM					Company-FW	5.5.5.6	CHECKPOINT-EX...	TCP/42176 (TCP/42176)	7	Cleanup rule	Standard	TCP/42176 Traffic Dropped from 5.5.5...

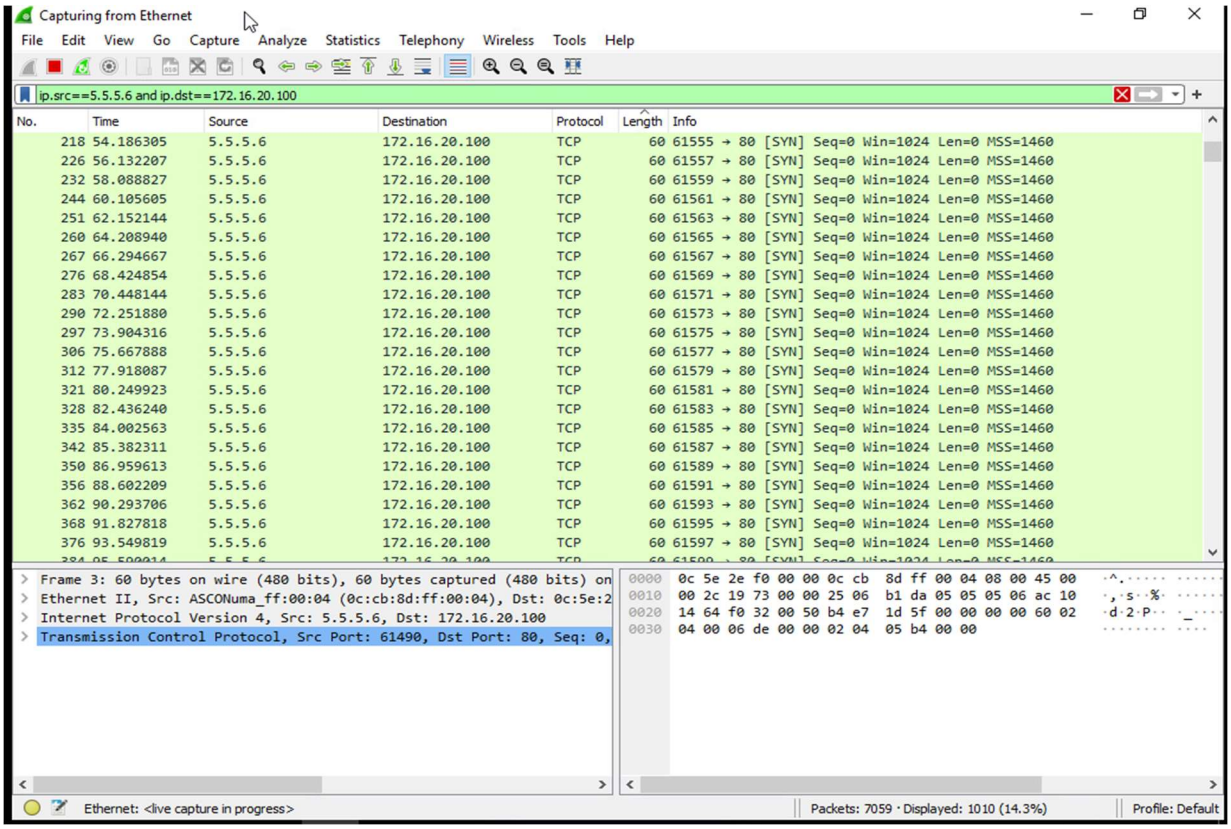
Εικόνα 51: Checkpoint logs με νέο κανόνα normal mode

Time	..	..	..	..	Origin	Source	Destination	Service	Ac...	Access Rule N...	Policy...	Description
Today, 6:32:34 AM					Company-FW	5.5.5.6	CHECKPOINT-EX...	TCP/61682 (TCP/61682)	7	Cleanup rule	Standard	TCP/61682 Traffic Dropped from 5.5.5...
Today, 6:32:34 AM					Company-FW	5.5.5.6	CHECKPOINT-EX...	TCP/41105 (TCP/41105)	7	Cleanup rule	Standard	TCP/41105 Traffic Dropped from 5.5.5...
Today, 6:32:34 AM					Company-FW	5.5.5.6	CHECKPOINT-EX...	TCP/12721 (TCP/12721)	7	Cleanup rule	Standard	TCP/12721 Traffic Dropped from 5.5.5...
Today, 6:32:34 AM					Company-FW	5.5.5.6	CHECKPOINT-EX...	TCP/40785 (TCP/40785)	7	Cleanup rule	Standard	TCP/40785 Traffic Dropped from 5.5.5...
Today, 6:32:34 AM					Company-FW	5.5.5.6	CHECKPOINT-EX...	TCP/40318 (TCP/40318)	7	Cleanup rule	Standard	TCP/40318 Traffic Dropped from 5.5.5...
Today, 6:32:34 AM					Company-FW	5.5.5.6	CHECKPOINT-EX...	TCP/23969 (TCP/23969)	7	Cleanup rule	Standard	TCP/23969 Traffic Dropped from 5.5.5...
Today, 6:32:34 AM					Company-FW	5.5.5.6	CHECKPOINT-EX...	TCP/11846 (TCP/11846)	7	Cleanup rule	Standard	TCP/11846 Traffic Dropped from 5.5.5...
Today, 6:32:34 AM					Company-FW	5.5.5.6	CHECKPOINT-EX...	TCP/51737 (TCP/51737)	7	Cleanup rule	Standard	TCP/51737 Traffic Dropped from 5.5.5...
Today, 6:32:34 AM					Company-FW	5.5.5.6	CHECKPOINT-EX...	TCP/19293 (TCP/19293)	7	Cleanup rule	Standard	TCP/19293 Traffic Dropped from 5.5.5...
Today, 6:32:34 AM					Company-FW	5.5.5.6	CHECKPOINT-EX...	TCP/22262 (TCP/22262)	7	Cleanup rule	Standard	TCP/22262 Traffic Dropped from 5.5.5...
Today, 6:32:34 AM					Company-FW	5.5.5.6	CHECKPOINT-EX...	TCP/12615 (TCP/12615)	7	Cleanup rule	Standard	TCP/12615 Traffic Dropped from 5.5.5...
Today, 6:32:34 AM					Company-FW	5.5.5.6	CHECKPOINT-EX...	TCP/42176 (TCP/42176)	7	Cleanup rule	Standard	TCP/42176 Traffic Dropped from 5.5.5...

Εικόνα 52: Checkpoint logs με νέο κανόνα stealth mode



Εικόνα 53: Web-server Wireshark με νέο κανόνα normal mode



Εικόνα 54: Web-server Wireshark με νέο κανόνα stealth mode

Παρατηρώντας τα παραπάνω αποτελέσματα των δοκιμών, διαπιστώνεται πως το τείχος προστασίας μετά την συγκεκριμενοποίηση του γενικού κανόνα 5 κατάφερε να μπλοκάρει οποιαδήποτε μορφή κίνησης προς το εσωτερικό δίκτυο εκτός από αυτήν προς τις πόρτες 80 και 443. Αρχικά τα αποτελέσματα του Nmap στον εξωτερικό χρήστη φαίνεται να βρίσκουν ανοιχτή πρόσβαση μόνο στην πόρτα 80 που αντιστοιχεί στην υπηρεσία http. Την ίδια στιγμή τα αρχεία logs του τείχους προστασίας φαίνεται να μπλοκάρουν όλες τις προσπάθειες σάρωσης για ανοιχτές πόρτες στον server, εκτός από αυτές που επιτρέπει ο κανόνας. Η επαλήθευση έρχεται από το λογισμικό Wireshark που εκτελείται στον web-server, το οποίο συλλέγει κίνηση και από εξωτερικούς χρήστες φαίνονται πακέτα μόνο προς την πόρτα 80. Εφόσον η λειτουργία του λογισμικού είναι να συλλέγει όλων των ειδών των πακέτων που καταφθάνουν στην κάρτα δικτύου, η παραπάνω συλλογή μπορεί να θεωρηθεί ως πως αποδεικνύει πως από εξωτερικούς παράγοντες φθάνουν πακέτα στην κάρτα δικτύου μόνο με προορισμό υπηρεσίες που τρέχουν στην πόρτα 80. Το σύνολο αποτελεσμάτων της ανάλυσης δείχνει πως για το συγκεκριμένο σενάριο υποψήφιας επίθεσης η παραμετροποίηση του κανόνα ήταν επαρκής κίνηση για την προστασία του web-server. Είναι ένα μικρό δείγμα της εξέλιξης των λειτουργιών και της τεχνολογίας των τειχών προστασίας χρόνο με τον χρόνο.

7.5 Πηγές

- https://www.researchgate.net/publication/292186843_A_systematic_analysis_of_the_science_of_sandboxing
- http://nestor.teipel.gr/xmlui/bitstream/handle/123456789/18015/%CE%91%CE%BD%CE%AC%CE%BB%CF%85%CF%83%CE%B7%20%CE%B1%CF%83%CF%86%CE%AC%CE%BB%CE%B5%CE%B9%CE%B1%CF%82%20%CE%BA%CE%B1%CE%B9%20%CE%B1%CF%80%CE%B5%CE%B9%CE%BB%CF%8E%CE%BD%20%CF%83%CE%B5%20%CF%85%CF%80%CE%BF%CE%B4%CE%BF%CE%BC%CE%AE%20Internet%20%CE%BA%CE%B1%CE%B9%20%CE%BA%CE%B1%CE%BB%CE%AD%CF%82%20%CF%80%CF%81%CE%B1%CE%BA%CF%84%CE%B9%CE%BA%CE%AD%CF%82.pdf?sequence=1
- https://www.researchgate.net/publication/258778792_Analysis_of_Computer_Network_Attacks
- https://kouloukith.blogspot.com/p/3.html?m=1
- https://www.tek-tools.com/security/what-is-an-intrusion-detection-system-ids
- https://www.easytechjunkie.com/what-is-network-simulation.htm
- https://www.offensive-security.com/metasploit-unleashed/about-meterpreter/
- https://www.elprocus.com/what-is-network-simulation-types-and-its-advantages/
- https://blog.eldernode.com/gns3-software-for-network-engineers/
- https://www.proofpoint.com/uk/threat-reference/sandbox
- https://docs.gns3.com/docs/
- https://www.techtarget.com/searchsecurity/definition/phishing
- https://medium.com/@mzainkh/how-it-works-reverse-tcp-attack-d7610dd8e55
- https://arxiv.org/ftp/arxiv/papers/1412/1412.6017.pdf
- http://ciit.finki.ukim.mk/data/papers/5CiiT/5CiiT-02.pdf
- https://www.researchgate.net/publication/292186843_A_systematic_analysis_of_the_science_of_sandboxing
- http://nestor.teipel.gr/xmlui/bitstream/handle/123456789/18015/%CE%91%CE%BD%CE%AC%CE%BB%CF%85%CF%83%CE%B7%20%CE%B1%CF

%83%CF%86%CE%AC%CE%BB%CE%B5%CE%B9%CE%B1%CF%82%20%CE%BA%CE%B1%CE%B9%20%CE%B1%CF%80%CE%B5%CE%B9%CE%BB%CF%8E%CE%BD%20%CF%83%CE%B5%20%CF%85%CF%80%CE%BF%CE%B4%CE%BF%CE%BC%CE%AE%20Internet%20%CE%BA%CE%B1%CE%B9%20%CE%BA%CE%B1%CE%BB%CE%AD%CF%82%20%CF%80%CF%81%CE%B1%CE%BA%CF%84%CE%B9%CE%BA%CE%AD%CF%82.pdf?sequence=1