Τμήμα Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών, ΕΛ.ΜΕ.ΠΑ. Κρήτης



Ελληνικό Μεσογειακό Πανεπιστήμιο

Τμήμα Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών

Πρόγραμμα Σπουδών Μηχανικών Πληροφορικής ΤΕ

Τίτλος:

Πλατφόρμα εκμάθησης σε διάφορα θέματα κυβερνοασφάλειας μέσα από ένα Capture the Flag (CTF).

Title:

A Capture the Flag (CTF) platform for training users on various cyber-security topics.

Σφενδουράκης Μάριος (ΤΡ 4970)

Επιβλέπων εκπαιδευτικός :

Επιτροπή Αξιολόγησης :

- **Μαρκάκης Ευάγγελος**
- **Μαστοράκης Γεώργιος**
- **Μπουρδένα Αθηνά**

Ημερομηνία παρουσίασης: 3 Απριλίου 2025

Ευχαριστίες

Ξεκινώντας, θα ήθελα να ευχαριστήσω τον επιβλέποντα καθηγητή μου, Δρ. Ευάγγελο Μαρκάκη, Διευθυντή του Εργαστηρίου Pasiphae και Επίκουρο Καθηγητή του Τμήματος Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών του Ελληνικού Μεσογειακού Πανεπιστημίου, για τις πολύτιμες συμβουλές του.
Επιπλέον, θα ήθελα να ευχαριστήσω τους επιστημονικούς συνεργάτες του Εργαστηρίου Pasiphae, Νικόλαο Αστυρακάκη για τις συμβουλές που μου παρείχε κατά τη διάρκεια υλοποίησης της πτυχιακής μου εργασίας, καθώς, και τον Μάνο Ρομπογιαννάκη για τις πολύτιμες διορθώσεις του και την καθοδήγηση που μου προσέφερε σε στιγμές που είχα βρεθεί σε αδιέξοδο. Τέλος, την Καλλιόπη και την οικογένεια μου για την ψυχολογική υποστήριξη που μου παρείχαν στις δύσκολες στιγμές που είχα να αντιμετωπίσω.

Περίληψη

Καθώς η τεχνολογία εξελίσσεται με γοργούς ρυθμούς τα τελευταία χρόνια όλο και περισσότερο αναγκαία είναι η ύπαρξη ασφάλειας των προσωπικών δεδομένων των ανθρώπων. Οι κακόβουλοι χρήστες είτε εκμεταλλεύονται ευπάθειες των ηλεκτρονικών συστημάτων, είτε χρησιμοποιούν τις ανθρώπινες αδυναμίες με σκοπό να βλάψουν τους χρήστες και να αποκομίσουν κέρδος από αυτούς. Το καίριο ζήτημα με το οποίο έρχεται αντιμέτωπη η σύγχρονη κοινωνία είναι η αδήριτη ανάγκη για μείωση των ποσοστών των θυμάτων ηλεκτρονικού εγκλήματος. Επομένως, η εκπαίδευση των χρηστών αποτελεί μια πρακτική λύση για να επιτευχθεί ο συγκεκριμένος στόχος. Αναλυτικότερα, υπάρχουν διαδικτυακοί διαγωνισμοί που έχουν ως σκοπό την εκπαίδευση των χρηστών σε θέματα κυβερνοασφάλειας υπό τη μορφή παιχνιδιού με όνομα Capture the Flag (CTF). Επίσης, οι συγκεκριμένοι διαγωνισμοί αποτελούνται από πληθώρα προκλήσεων (challenges), οι οποίες ανήκουν σε διαφορετικές κατηγορίες. Κάθε μια κατηγορία ενισχύει διαφορετικές δεξιότητες των χρηστών, και το κάθε challenge αποτελεί το εργαλείο για την ενίσχυση αυτή. Βασικός στόχος της εργασίας αυτής είναι η δημιουργία προκλήσεων μέσω της βοήθειας του docker. Το docker αποτελεί μια τεχνολογία η οποία έχει αλλάξει τον τρόπο με τον οποίο αναπτύσσονται εφαρμογές τα τελευταία χρόνια. Η τεχνολογία αυτή παρέχει την δυνατότητα δημιουργίας containers τα οποία περιέχουν την απαραίτητη πληροφορία για την ανάπτυξη της εφαρμογής, επιτρέποντας στον χρήστη να περιηγηθεί σε ένα απομονωμένο περιβάλλον. Ακόμα, το πλαίσιο (framework) το οποίο θα φιλοξενήσει τις συγκεκριμένες προκλήσεις ονομάζεται CTFd και θα αποτελέσει την βάση πάνω στην οποία θα αναπτυχθεί ο CTF διαγωνισμός. Η επιλογή του προέκυψε μετά από την σύγκριση πολλών παρόμοιων frameworks με στόχο την εύρεση του πιο αποτελεσματικού. Επιπρόσθετα, το CTFd παρέχει πολλαπλές λειτουργίες και περιβάλλον φιλικό προς τον χρήστη, γεγονός που το καθιστά κατάλληλο για την υλοποίηση του συγκεκριμένου CTF. Το κίνητρο για την εκπόνηση της πτυχιακής εργασίας ήταν η ανάπτυξη προκλήσεων κυνερνοασφάλειας, οι οποίες θα χρησιμοποιηθούν στο open-source CTF framework από το Ελληνικό Μεσογειακό Πανεπιστήμιο για την εκπαίδευση των φοιτητών σε θέματα κυβερνοασφάλειας. Συνοψίζοντας, σκοπός της πτυχιακης αυτής, είναι να ωθήσει τους φοιτητές του πανεπιστήμιου σαν πρώτο στάδιο να ασχοληθούν περισσότερο με τον τομέα της κυβερνοασφάλειας, είναι η δημιουργία προκλήσεων βασισμένες στο μάθημα Ασφάλεια Δικτύων.

Πίνακας Περιεχομένων

Περίληψη 3
Πίνακας Περιεχομένων 4
Κατάλογος Εικόνων 6
Κατάλογος Πινάκων 7
1. Εισαγωγή 8
2. Βιβλιογραφική Ανασκόπηση 10
3. Εργαλεία Τεχνολογίας 13
3.1 Python 13
3.2 Flask 13
3.3 Docker 13
3.4 HTML 13
3.5 CSS 14
3.6 Virtualbox 14
3.7 CTFd 14
3.8 SSH 14
3.9 FTP 14
3.10 Nmap 15
4. Υλοποιημένες CTF προκλήσεις 16
5. Υλοποίηση 17
5.1 Αρχιτεκτονική Συστήματος 17
5.2 Προκλήσεις 18
5.2.1 1η Πρόκληση: What is RSA? 19
5.2.2 2η Πρόκληση: Where is the map ? 23
5.2.3 3η Πρόκληση: Brute Force Attack 26
6. Αποτελέσματα 32
6.1 Αποτελέσματα 1ης Πρόκλησης 32
6.2 Αποτελέσματα 2ης Πρόκλησης 33
6.3 Αποτελέσματα 3ης Πρόκλησης 34
7. Αξιολόγηση 35

7.1 Πώς θα αξιολογούσατε τη συνολική εμπειρία στα challenges (σε κλίμακα από 1 έως 5); 35

7.2 Πόσο διασκεδαστικά σου φάνηκαν τα challenges (σε κλίμακα από 1 έως 5);.....36

7.3 Πως θα αξιολογούσατε την δυσκολία των challenges συνολικά (σε κλίμακα από 1 έως 5); 37

7.4 Σε ποιο βαθμό υπήρξε κάτι που δεν σας ικανοποίησε (σε κλίμακα από 1 έως 5); 38

7.5 Σε τι βαθμό πιστεύετε ότι τα challenges σας πρόσφεραν νέες γνώσεις ή δεξιότητες (σε κλίμακα από 1 έως 5);.....39

7.6 Θα προτείνατε αυτά τα challenges σε άλλους χρήστες (σε κλίμακα από 1 έως 5);.....40

8. Συμπεράσματα 41

9. Μελλοντικά πλάνα.....42

References.....43

Appendix A.....44

CTFd Framework.....44

Κατάλογος Εικόνων

Εικόνα 1 Αρχιτεκτονική Συστήματος 18
Εικόνα 2 Σχεδιάγραμμα πρώτης πρόκλησης 20
Εικόνα 3 Επεξήγηση RSA αλγορίθμου μέσα από το rsa1.py 21
Εικόνα 4 Επεξήγηση RSA αλγορίθμου μέσα απο το rsa2.py 22
Εικόνα 5 Το flag της πρώτης πρόκλησης και πληροφορίες για την επόμενη 23
Εικόνα 6 Σχεδιάγραμμα 2ης πρόκλησης 24
Εικόνα 7 Σύνδεση ssh με το kali docker container 25
Εικόνα 8 Ανάλυση δικτύου με το Nmap 25
Εικόνα 9 Σύνδεση ssh με το docker ftp server 26
Εικόνα 10 Αποτελέσματα του users.py script 26
Εικόνα 11 Περιεχόμενα του sccript με την εντολή cat στο users.py 26
Εικόνα 12 Σχεδιάγραμμα 3ης πρόκλησης 27
Εικόνα 13 Σύνδεση μέσω ssh στο container που θα εκτελέσει το attack 28
Εικόνα 14 Αρχικοποίηση των απαραίτητων μεταβλητών 29
Εικόνα 15 Αποτελέσματα επίθεσης 30
Εικόνα 16 Σύνδεση με το ευπαθές container μετά την ολοκλήρωση της επίθεσης 30
Εικόνα 17 Η λύση της 3ης πρόκλησης 31
Εικόνα 18 Οι Απαντήσεις των χρηστών στην 1η ερώτηση κατά Μ.Ο 36
Εικόνα 19 Οι Απαντήσεις των χρηστών στην 2η ερώτηση κατά Μ.Ο 37
Εικόνα 20 Απαντήσεις των χρηστών στην 3η ερώτηση κατά Μ.Ο 38
Εικόνα 21 Απαντήσεις των χρηστών στην 4η ερώτηση κατά Μ.Ο 39
Εικόνα 22 Απαντήσεις των χρηστών στην 5η ερώτηση κατά Μ.Ο 40
Εικόνα 23 Απαντήσεις των χρηστών στην 5η ερώτηση κατά Μ.Ο 41
Εικόνα 24 Αρχική Εικόνα CTFd 44
Εικόνα 25 Πίνακας αποτελεσμάτων 45
Εικόνα 26 Κεντρική σελίδα προκλήσεων 46
Εικόνα 27 Υποσελίδα στατιστικών 47
Εικόνα 28 Λίστα παικτών απο το πανελ του διαχειριστή 48
Εικόνα 29 Πληροφορία για έναν συγκεκριμένο χρήστη 48
Εικόνα 30 Λίστα προκλήσεων απο το πάνελ του διαχειριστή 49
Εικόνα 31 Δημιουργία πρόκλησης μέσα απο το πάνελ του διαχειριστή 50
Εικόνα 32 Τροποποίηση των προκλησεων 51
Εικόνα 33 Τροποποιηση των προκλησεων (2) 52
Εικόνα 34 Υποβολές 53
Εικόνα 35 Διαμόρφωση του CTF 54
Εικόνα 36 Διακριτικό πρόσβασης 55
Εικόνα 37 Περιγραφή πρώτης πρόκλησης 56
Εικόνα 38 Περιγραφή δεύτερης πρόκλησης 57
Εικόνα 39 Περιγραφή τρίτης πρόκλησης 58

Κατάλογος Πινάκων

Πίνακας 1 Χρόνος επίλυσης καθε πρόκλησης απο τους χρήστες 32
Πίνακας 2 Χρόνος επίλυσης για την δεύτερη πρόκληση για τον κάθε χρήστη 33
Πίνακας 3 Χρόνος επίλυσης για την 3η πρόκληση 34
Πίνακας 4 Μέσος χρόνος επίλυσης καθε πόκλησης 35
Πίνακας 5 Απαντήσεις των χρηστών στην πρώτη ερώτηση 36
Πίνακας 6 Απαντήσεις των χρηστών στην 2η ερώτηση 37
Πίνακας 7 Απαντήσεις των χρηστών στην 3η ερώτηση 38
Πίνακας 8 Απαντήσεις των χρηστών στην 4η ερώτηση 39
Πίνακας 9 Απαντήσεις των χρηστών στην 5η ερώτηση 40
Πίνακας 10 Απαντήσεις των χρηστών στην 6η ερώτηση 41

1. Εισαγωγή

Στις σύγχρονες κοινωνίες η προστασία των δεδομένων αποτελεί ένα σημαντικό ζήτημα. Όπως είναι ευρέως γνωστό κακόβουλοι χρήστες προσπαθούν να υποκλέψουν δεδομένα και προσωπικές πληροφορίες με στόχο να βλάψουν το θύμα ή να τις εκμεταλλευτούν για προσωπικό τους όφελος. Οι hackers εκμεταλλεύονται την έλλειψη γνώσης των χρηστών σε θέματα κυβερνοασφάλειας έτσι ώστε να αποκτήσουν πρόσβαση σε ευαίσθητα δεδομένα. Επομένως, καθίσταται αναγκαία η εκπαίδευση των χρηστών, με σκοπό τη μείωση των θυμάτων ηλεκτρονικού εγκλήματος και την καλύτερη προστασία των προσωπικών τους στοιχείων.

Η εκπαίδευση των χρηστών από μικρή ηλικία είναι μια τακτική η οποία μπορεί να συνεισφέρει στην ελάττωση του ηλεκτρονικού εγκλήματος. Μεγάλη μερίδα των μαθητών/φοιτητών ασχολείται ενεργά με τα ψηφιακά παιχνίδια. Επομένως, η δημιουργία αυτών όπου θα χρησιμοποιηθούν ως εργαλεία εκπαίδευσης των μαθητών αποτελεί μια αποτελεσματική προσέγγιση [1]. Μια άλλη τακτική η οποία είναι αποδοτική και φαίνεται να υπερτερεί έναντι του παραδοσιακού τρόπου εκπαίδευσης είναι η ψηφιακή εκμάθηση. Οι μαθητές/φοιτητές προτιμούν την ψηφιακή εκμάθηση σε σχέση με τον παραδοσιακό τρόπο εκπαίδευσης, καθώς θεωρούν πιο ελκυστική την παρακολούθηση ενός βίντεο σε σχέση με την μελέτη ενός βιβλίου. Η ψηφιακή μάθηση ενισχύει το μαθησιακό κίνητρο καθώς και τις δεξιότητές των μαθητών, γεγονός που οδηγεί σε αποδοτικότερα μαθησιακά αποτελέσματα [2], [3]. Επιπλέον, μια εναλλακτική προσέγγιση στην εκπαίδευση για θέματα κυβερνοασφάλειας είναι η χρήση ψηφιακών παιχνιδιών, που μέσω της παιχνιδοποιήσης μπορούν να προσφέρουν μια δια δραστική και αποτελεσματική μαθησιακή εμπειρία.[2], [3].

Εκτός από την εκπαίδευση των νεότερων χρηστών, είναι εξίσου σημαντικό να εκπαιδευτούν και οι μεγαλύτερης ηλικίας χρήστες, ώστε να μπορούν και αυτοί να προστατεύονται από τέτοιου είδους κινδύνους. Μια αποτελεσματική στρατηγική για την εκπαίδευση όλων των ηλικιακών ομάδων σε θέματα κυβερνοασφάλειας είναι η χρήση διαδικτυακών εφαρμογών (web-based applications), οι οποίες ενθαρρύνουν τους χρήστες να εξοικειωθούν με την κυβερνοασφάλεια και να αναπτύξουν τις απαραίτητες δεξιότητες [3]. Το Capture The Flag (CTF) είναι ένας διαγωνισμός κυβερνοασφάλειας βασισμένος σε web-based εφαρμογές, όπου οι συμμετέχοντες βελτιώνουν τις γνώσεις τους μέσω της επίλυσης προβλημάτων σχετικών με την κυβερνοασφάλεια. Στόχος τέτοιων διαγωνισμών είναι η ανάπτυξη και η ενίσχυση των δεξιοτήτων των συμμετεχόντων στον τομέα της κυβερνοασφάλειας [3][4]. Οι προκλήσεις που περιλαμβάνονται θα πρέπει να προσαρμόζονται στο επίπεδο γνώσεων των χρηστών και το περιεχόμενό τους να ανταποκρίνεται στις σύγχρονες ανάγκες και απειλές [4]. Ένα χρήσιμο εργαλείο για την δημιουργία των CTF προκλήσεων είναι το docker το οποίο επιτρέπει την εκτέλεση διεργασιών μέσα σε απομονωμένο περιβάλλον, δηλαδή ο κάθε χρήστης να εκτελεί τις προκλήσεων σε ιδιωτικό δίκτυο. Επίσης, με την χρήση του docker οι προκλήσεις δεσμεύουν τους απολύτως απαραίτητους πόρους από το σύστημα [5].

Ο στόχος της πτυχιακής είναι η αξιοποίηση ενός open-source CTF framework και η δημιουργία προκλήσεων στον τομέα της κυβερνοασφάλειας, μέσα από τα οποία οι μαθητές του μαθήματος Ασφάλειας Δικτυών θα έρθουν σε επαφή με προβλήματα τα οποία θα πρέπει να φέρνουν εσπέρας με επιτυχία. Επομένως, σκοπός των προκλήσεων αυτών είναι να εξοικειωθούν οι φοιτητές με

ευπάθειες καθώς και ορισμούς πάνω στον τομέα της κυβερνοασφάλειας, στοχεύοντας έτσι στην εξέλιξη τους. Επιπροσθέτως, το περιεχόμενο και το επίπεδο δυσκολίας των προκλήσεων προσαρμόστηκε στο επίπεδο γνώσης των φοιτητών με σκοπό την ενίσχυση των δυνατοτήτων τους, καθώς και στην θεωρία του μαθήματος (Ασφάλεια Δικτύων).

Η πτυχιακή δομείται στα εξής 8 Κεφάλαια:

1. **Εισαγωγή**: Σε αυτό το κεφάλαιο αναφέρονται εισαγωγικά δεδομένα σχετικά με τους CTF διαγωνισμούς και ο στόχος της πτυχιακής.
2. **Βιβλιογραφική Ανασκόπηση**: Σε αυτό το κεφάλαιο παρατίθενται επιστημονικά άρθρα σχετικά με τη δημιουργία CTF προκλήσεων.
3. **Τεχνολογίες/Εργαλεία**: Όπως αναγράφεται και στον τίτλο αυτού του κεφαλαίου, γίνεται αναφορά στα εργαλεία που χρησιμοποιήθηκαν στην πτυχιακή.
4. **Προτεινόμενες προκλήσεις**: Στο τέταρτο κεφάλαιο της πτυχιακής παρουσιάζονται οι προκλήσεις που υλοποιήθηκαν και σχετικές πληροφορίες γι’ αυτά.
5. **Υλοποίηση**: Σε αυτό το κεφάλαιο αναγράφεται η υλοποίηση του CTFd framework, καθώς και η δημιουργία των προκλήσεων μέσω της χρήσης docker containers.
6. **Αποτελέσματα**: Τα αποτελέσματα των μετρήσεων αναγράφονται σε αυτό το κεφάλαιο μέσα από την ολοκλήρωση των προκλήσεων από πραγματικούς χρήστες.
7. **Αξιολόγηση**: Σε αυτό το κεφάλαιο αναλύονται και αξιολογούνται οι συνολικές εμπειρίες των χρηστών στις προκλήσεις, αλλά και σε ολόκληρο τον διαγωνισμό.
8. **Συμπεράσματα**: Τα συμπεράσματα που προέκυψαν από την δημιουργία προκλήσεων μέσα από docker containers και όχι από virtual machines.
9. **Μελλοντικά πλάνα**: Στο συγκεκριμένο κεφάλαιο αναλύονται τα μελλοντικά πλάνα για την εξέλιξη της εφαρμογής αυτής.

2. Βιβλιογραφική Ανασκόπηση

Παρακάτω παρουσιάζονται επιστημονικά άρθρα τα οποία περιγράφουν και συγκρίνουν τις διαθέσιμες πλατφόρμες για δημιουργία CTF, καθώς και την παιδαγωγική ικανότητα κάθε πλατφόρμας. Επίσης, παρουσιάζονται επιστημονικά άρθρα τα οποία περιγράφουν τον τρόπο δημιουργίας και λειτουργίας CTF challenges τα οποία χρησιμοποιούνται σε CTF διαγωνισμούς.

Αρχικά, μια σύγκριση μεταξύ διαθέσιμων open source CTF frameworks παρουσιάζεται στο [6]. Οι συγγραφείς της δημοσίευσης, αναφέρουν τέσσερα Open CTF platforms (Facebook CTF, CTFd, Mellivora, Root the Box) για την δημιουργία μιας CTF εφαρμογής. Επίσης, ορίζουν τα κριτήρια αξιολόγησης για την σύγκριση των εφαρμογών τα οποία είναι: η λειτουργικότητα, η επεκτασιμότητα καθώς και η διδακτική υπόσταση. Συμπληρωματικά, αναφέρουν ότι το Facebook CTF δημιουργήθηκε ώστε να προσφέρει μια απλή μέθοδο για την οργάνωση και την δημιουργία ενός CTF διαγωνισμού. Το CTFd από την άλλη με την πλούσια σε χαρακτηριστικά σε συνδυασμό με την ευκολία στην εγκατάσταση, τη χρήση και τις επιλογές προσαρμογής το καθιστούν μια ελκυστική λύση για τους διοργανωτές. Το Mellivora, λόγω της απλότητας που παρέχει είναι μια αρκετά καλή επιλογή για τους διοργανωτές CTF διαγωνισμών. Τέλος, το Root the box προσφέρει προκλήσεις που περιλαμβάνουν μια σειρά από μικρότερες εργασίες που πρέπει να υλοποιηθούν έτσι ώστε να προχωρήσει στην επόμενη πρόκληση ο χρήστης. Σύμφωνα με τα διαγράμματα που παρουσιάζονται είναι εύκολο να κατανοηθεί πως το CTFd και το Root the box αποτελούν τις καλύτερες μεθόδους για να υλοποιηθεί ένας CTF διαγωνισμός. Συμπεραίνουν λοιπόν, πως οι προαναφερθέντες πλατφόρμες έχουν περισσότερα χαρακτηριστικά και στοχεύουν στην δημιουργία μοναδικών προκλήσεων που παρέχουν ένα βαθύ εκπαιδευτικό υπόβαθρο. Τέλος, ορισμένα χαρακτηριστικά μπορούν να τροποποιηθούν προκειμένου να βελτιωθούν τα στοιχεία της παιχνιδοποίησης.

Μια έρευνα που επικεντρώνεται στην λειτουργία της CTFd πλατφόρμας παρουσιάζεται στο [7]. Οι ερευνητές της δημοσίευσης, αναφέρουν ότι η γλώσσα προγραμματισμού του CTFd είναι κατάλληλη για αρχάριους χρήστες. Αποδεικτικό για τον παραπάνω ισχυρισμό αποτελούν οι απόψεις τον χρηστών καθώς και η αυξανόμενη δημόσια χρήση του. Επίσης, το CTFd παρέχει εύκολη διαχείριση για τους οργανωτές. Ακόμα, διαθέτει αρκετά χαρακτηριστικά που την καθιστούν μια ευέλικτη εφαρμογή ώστε να αναπτυχθεί το κομμάτι της εκπαίδευσης με σκοπό να ενισχύσει τον τομέα της κυβερνοασφάλειας. Επιπλέον, όλοι όσοι λαμβάνουν συμμετοχή σε έναν διαγωνισμό CTF αποκτούν γνώσεις και συζητούν τις εμπειρίες τους από τον διαγωνισμό με τους υπόλοιπους συμμετέχοντες δημιουργώντας έτσι ένα κλίμα ομαδικότητας. Τέλος, ο πηγαίος κώδικας του CTFd αλλάζει με γοργούς ρυθμούς, επομένως είναι μια πρόκληση για τους προγραμματιστές να διατηρήσουν την δομή του CTFd ακέραιη.

Επιπροσθέτως, οι συγγράφεις του άρθρου [8] αναφέρουν τον τρόπο με τον οποίο σχεδίασαν ένα CTF, με σκοπό την εκπαίδευση φοιτητών του Ιονίου Πανεπιστημίου. Αρχικά, επισημαίνουν ότι η διατήρηση υψηλού επιπέδου στον τομέα της κυβερνοασφάλειας είναι ένα δύσκολο εγχείρημα, καθώς πολλοί συμμετέχοντες δεν διαθέτουν γνώσεις πάνω στον τομέα. Επιπλέον, αναφέρουν ότι όλες οι απαραίτητες πληροφορίες για τη δημιουργία των προκλήσεων που θα κληθούν να λύσουν

οι φοιτητές έχουν αντληθεί από το VulnHub[1]. Η συγκεκριμένη ιστοσελίδα παρέχει πληθώρα από προκλήσεις τα οποία έχουν υλοποηθεί σε Virtual Machine (VM). Ακόμα, προσθέτουν ότι οι CTF προκλήσεις αποτελούν το κύριο εργαλείο για την ενίσχυση της εκπαιδευτικής διαδικασίας επιτρέποντας ενεργή συμμετοχή, επιτυγχάνοντας έτσι υψηλά επίπεδα αφοσίωσης. Εν κατακλείδι, η πλατφόρμα που χρησιμοποιήσαν είναι το CTFd προσαρμόζοντας τις επιλεγμένες προκλήσεις, παρέχοντας στους χρήστες περισσότερες λεπτομέρειες για κάθε βήμα.

Ένα ακόμα επιστημονικό άρθρο το οποίο εστιάζει στην σχεδίαση νέων CTF προκλήσεων, καθώς και την δημιουργία προκλήσεων στην πλατφόρμα του CTFd για εκπαιδευτικούς λογούς είναι το άρθρο [9]. Οι συγγραφείς παραθέτουν αρκετές από τις βασικές λειτουργίες και δυνατότητες που παρέχει η πλατφόρμα αυτή. Επιπρόσθετα, αναφέρουν ότι δημιούργησαν είκοσι προκλήσεις που καλύπτουν θέματα όπως: Encryption, Networking, Linux , Web and Exploitation. Τα έντεκα από τα είκοσι προκλήσεις είναι παραλλαγές εργασιών μαθημάτων, τέσσερις είναι ειδικά σχεδιασμένες για τον διαγωνισμό, δύο τροποποιήθηκαν από προηγούμενα CTF, και τρια από αυτά αποτελούν server-style. Διευκρινίζουν πως οι έντεκα προκλήσεις αποτελούν την πιο εύκολη κατηγορία, η οποία βαθμολογείται με 10 πόντους. Τόσο η εκτέλεση ενός brute force attack, με σκοπό την απόκτηση πρόσβασης σε κλειδωμένο αρχείο, όσο και η εφαρμογή ssh σε ένα container με απώτερο σκοπό την εύρεση κάποιου credential βαθμολογούνται με 20 πόντους. Ενώ όταν εκτελούν οι χρήστες κάποιο buffer overflow λαμβάνουν 50 πόντους. Πληροφορίες σχετικά με την περιγραφή και υλοποίηση των προκλήσεων είναι διαθέσιμες στα Gitlab έπειτα από έγκριση πρόσβασης από τους διοργανωτές. Επιπλέον, παρουσιάζουν τα αποτελέσματα μιας έρευνας που διεξήχθη μετά την ολοκλήρωση του CTF διαγωνισμού. Σύμφωνα με τα ευρήματα της έρευνας, οι διαγωνιζόμενοι απέκτησαν νέες γνώσεις και είχαν θετική άποψη για τον διαγωνισμό. Ωστόσο, δεν παρέχονται λεπτομέρειες σχετικά με τις ερωτήσεις που τέθηκαν στους συμμετέχοντες, οι οποίες οδήγησαν στα συγκεκριμένα συμπεράσματα.

Στην παρατιθέμενη δημοσίευση [10] οι συγγράφεις αναλύουν 3 κατηγορίες πάνω στις οποίες δημιουργήθηκαν οι προκλήσεις. Επιπλέον, αναφέρουν ότι για την ανάπτυξη του CTF χρησιμοποιούν το CTFd framework. Αναλυτικότερα, οι τρεις βασικές κατηγορίες των challenges είναι οι εξής: Meet-The-Others Flag, Combining-Code Flag, Talk-With-Host Flag. Η πρώτη κατηγορία απαιτεί από τους διαγωνιζόμενους να επικοινωνούν μεταξύ τους και να ανταλλάσσουν πληροφορίες, ώστε οι παίκτες να ανακαλύψουν στοιχεία για τους άλλους διαγωνιζόμενους, τα οποία ενδεχομένως θα τους βοηθήσουν να εντοπίσουν το flag. Αναλυτικότερα, το flag έχει συγκεκριμένη μορφή και αποτελεί την λύση της πρόκλησης. Στην δεύτερη κατηγορία κάθε διαγωνιζόμενος ξεκινά με έναν μοναδικό δυαδικό κωδικό. Στη συνέχεια, πρέπει να βρουν έναν άλλο διαγωνιζόμενο και να κάνουν πράξη XOR μεταξύ των κωδικών τους, προκειμένου να αποκαλύψουν το flag. Ενώ για την τελευταία κατηγορία οι διαγωνιζόμενοι πρέπει να αλληλεπιδράσουν με τους διοργανπαπερωτές, έτσι ώστε να αντλήσουν πληροφορίες ή βοήθεια από αυτούς για να προχωρήσουν στο challenge. Τα παραπάνω challenges επικεντρώνονται κυρίως στην επικοινωνία και τη συνεργασία μεταξύ των συμμετεχόντων, παρά στην εκμάθηση νέων τεχνικών δεξιοτήτων ή εργαλείων στον τομέα της κυβερνοασφάλειας. Ακόμα, περιγράφουν πως μετά την ολοκλήρωση του CTF από τους συμμετέχοντες, τους παρουσιάζεται ένα ερωτηματολόγιο σχετικά με την εμπειρία τους χωρίς όμως να παραθέτουν το ερωτηματολόγιο ή τις απαντήσεις των χρηστών.

[1] https://www.vulnhub.com/

Στην παραπάνω δημοσίευση έγιναν συγκρίσεις ανάμεσα στις διαθέσιμες πλατφόρμες για δημιουργία CTF διαγωνισμού, καθώς και την παιδαγωγική ικανότητα κάθε πλατφόρμας. Το CTFd αναφέρεται ως μια από τις ιδανικότερες λύσεις για τον συγκεκριμένο σκοπό, αφού προσφέρει αρκετές λειτουργίες, όπως για παράδειγμα αυτή της επιλογής ατομικής ή ομαδικής διεξαγωγής του διαγωνισμού. Επίσης, το docker αναφέρεται ως η καταλληλότερη μέθοδος για δημιουργίας των challenges τα οποία θα πρέπει να φέρει εις πέρας ο χρήστης. Όπως παρατηρήθηκε στις περισσότερες CTF προκλήσεις έχουν υλοποιηθεί μέσω VMs, πράγμα που τα καθιστά πεπερασμένα. Επιπλέον, μετά την ολοκλήρωση των περισσότερων διαγωνισμών, δεν πραγματοποιούνται ερωτηματολόγια για την αξιολόγηση των challenges. Στους διαγωνισμούς που διεξάγονται ερωτηματολόγια, δεν παρέχονται επαρκείς λεπτομέρειες σχετικά με τη διαδικασία, από την οποία προήλθαν τα συμπεράσματα. Σκοπός είναι, λοιπόν, η δημιουργία νέων CTF προκλήσεων χρησιμοποιώντας docker, τα οποία θα δοκιμαστούν και θα αξιοποιηθούν στην πλατφόρμα CTFd από τους χρήστες. Παράλληλα, οι χρήστες θα κληθούν να συμπληρώσουν ένα ερωτηματολόγιο, το οποίο θα αξιολογεί τη χρήση των προκλήσεων.

3. Εργαλεία Τεχνολογίας

3.1 Python

Η python είναι γλώσσα προγραμματισμού υψηλού επιπέδου (high level). Η python αποτελεί μια από τις πιο δημοφιλής γλώσσες προγραμματισμού αφού βρίσκει εφαρμογή σε πληθώρα από εφαρμογές για παράδειγμα: αυτοματοποίηση εργασιών μέσα από διάφορα scripts, στην τεχνητή νοημοσύνη όπου αναπτύσσονται εξελιγμένα μοντέλα. Επίσης, διαθέτει έτοιμες βιβλιοθήκες και εργαλεία με τα οποία οι χρήστες μπορούν εύκολα να υλοποιήσουν σύνθετα ζητήματα. Με την χρήση της συγκεκριμένης γλώσσας προγραμματισμού υλοποιήθηκε το κομμάτι δημιουργίας των docker containers για τους χρήστες.

3.2 Flask

Το Flask αποτελεί ένα micro web framework το οποίο βοηθάει τους προγραμματιστές να υλοποιήσουν ιστοσελίδες με χρήση της python. Επιπλέον, χρησιμοποιεί τις απαραίτητες επεκτάσεων ανάλογα με τις ανάγκες του προγραμματιστή οπότε είναι ένα lightweight application και αποτελεί μια εξαιρετική επιλογή για την υλοποίηση μικρών εφαρμογών διαδικτύου. Λόγω του ότι το CTFd το χρησιμοποιεί, έτσι για την δημιουργία του παραπάνω python script για τα docker containers χρησιμοποίησα αυτό το framework.

3.3 Docker

Το docker αποτελεί μια τεχνολογία που χρησιμοποιείται κατά κόρον τα τελευταία χρόνια για την υλοποίηση εφαρμογών. Αυτό συμβαίνει διότι το docker παρέχει όλες τις απαραίτητες λειτουργίες για την υλοποίηση μιας εφαρμογής σε docker images. Κάθε ένα από αυτά τα images μπορεί να υλοποιηθεί μέσα σε ένα docker container. Το κάθε ένα από αυτά τα containers περιέχει όλες τις απαραίτητες πληροφορίες για την εκάστοτε λειτουργία, παραδείγματος χάριν μια βάση δεδομένων η οποία συνδέεται άμεσα με την εφαρμογή. Ακόμα, τα dockers χρησιμοποιούν images για την υλοποίηση των λειτουργιών τους, τα οποία είναι προσβάσιμα από τον οποιονδήποτε μέσω του docker hub. Το docker hub αποτελεί ένα αποθετήριο (repository) για images τα οποία είτε παρέχονται από τις ίδιες τις εταιρίες είτε από προγραμματιστές που τις έχουν υλοποιήσει. Επίσης, τα images είναι εκείνα τα οποία έχουν την πληροφορία για την εκάστοτε λειτουργία και μέσα από αυτές υπάρχει αλληλεπίδραση με τον χρήστη της εφαρμογής. Βασικό πλεονέκτημα που προσφέρουν τα dockers έναντι των εικονικών μηχανημάτων είναι η απόδοση τους λόγω των χαμηλών σε μέγεθος αρχείων που παράγουν. Τέλος, μέσα από τα dockers, δημιουργήθηκαν όλες οι προκλήσεις, είτε από έτοιμα images που προσφέρουν στο repository του docker hub είτε από την δημιουργία μοναδικών docker containers.

3.4 HTML

Hypertext Markup language (HTML) είναι μια γλώσσα περιγραφής για ιστοσελίδες. Η HTML καθορίζει τη διαμόρφωση και το περιεχόμενο της ιστοσελίδας στον browser μέσα από ένα σύνολο κανόνων. Με την χρήση της HTML προστέθηκε το κουμπί όπου μεταφέρει τους χρήστες από την εφαρμογή μέσα στο webterminal docker container όπου εκτελούνται όλα τα challenges.

3.5 CSS

Η CSS είναι μια γλώσσα υπολογιστή η οποία καθορίζει την εμφάνιση των components που έχουν δημιουργηθεί από την HTML. Η CSS βασίζεται σε labels της HTML για να μπορέσει να επεξεργαστεί την εμφάνιση συγκεκριμένων components. Με την βοήθεια της CSS μορφοποιήθηκε το κουμπί που προστέθηκε μέσα από την HTML ώστε να ταιριάζει στο χρώμα της υπόλοιπης εφαρμογής.

3.6 Virtualbox

Το Virtualbox είναι ένα πρόγραμμα το οποίο δημιουργεί virtual machines. Ο χρήστης μπορεί να εγκαταστήσει οποιοδήποτε λειτουργικό σύστημα επιθυμεί και να καθορίσει τους πόρους που θα δεσμεύσει το virtual machine από το πραγματικό μηχάνημα. Επιπλέον, μπορεί να υλοποιήσει εφαρμογές και να εγκαταστήσει προγράμματα στο virtual machine, έτσι ώστε να κάνει δοκιμές πάνω σ' ένα εικονικό μηχάνημα και όχι στο πραγματικό μηχάνημα. Επομένως, οι χρήστες αποφεύγουν να εκθέσουν σε κίνδυνο το πραγματικό μηχάνημα σε περίπτωση που υπάρξουν επιπλοκές από τα προγράμματα. Το Virtual Box χρησιμοποιήθηκε ώστε να στηθεί το λειτουργικό linux πάνω στο οποίο δημιουργήθηκαν όλα τα παραπάνω.

3.7 CTFd

Το CTFd framework αποτελεί ένα εργαλείο το οποίο δημιουργεί κατά κύριο λόγο capture the flag διαγωνισμούς μέσα από τους οποίους οι χρήστες/μαθητές εκπαιδεύονται πάνω στον τομέα της ασφάλειας δικτύων (network security). Επομένως, οι χρήστες αποκτούν γνώσεις πάνω σε πεδία της ασφάλειας δικτύων όπως είναι η Κρυπτογραφία, το Networking. Επίσης, παρέχει μεγάλη γκάμα από features όπως στατιστικά των παικτών, δηλαδή πόσα challenge έχουν ολοκληρώσει με επιτυχία, και διάφορες άλλες λεπτομέρειες σχετικά με τις επιδόσεις των παικτών. Επιπλέον, η βάση δεδομένων του CTFd είναι υλοποιημένη με dockers, παρέχοντας ευκολία στην διαχείριση. Συνεπώς, είναι μια από τις καλύτερες επιλογές για την υλοποίηση ενός capture the flag διαγωνισμού. Το CTFd αποτέλεσε την βάση πάνω στην οποία δημιουργήθηκαν οι περίγραφες των challenges, καθώς και την βάση για όλη την εφαρμογή εκτός των challenges.

3.8 SSH

Το Secure Socket Shell (SSH) είναι ένα πρωτόκολλο δικτύου που χρησιμοποιείται από χρήστες και διαχειριστές έτσι ώστε να αποκτούν απομακρυσμένη πρόσβαση σε έναν υπολογιστή. Το ssh χρησιμοποιεί τον RSA αλγόριθμο για την δημιουργία κλειδιών. Μέσα από αυτό το πρωτόκολλο, συνδέονται οι χρήστες στο ανάλογο docker container το οποίο υλοποιεί και το ανάλογο challenge.

3.9 FTP

Το File Transfer Protocol (FTP) είναι ένα πρωτόκολλο το οποίο χρησιμοποιείται για την

μεταφορά δεδομένων από έναν client σε έναν server αλλά και το αντίστροφο, κάνοντας έτσι την μεταφορά απλή και γρήγορη. Το FTP εσνωματοθηκε πανω σε ενα docker container οπου εχει το flag για την ολοκληρωση του challenge.

3.10 Nmap

Το Nmap σαν εργαλείο προσφέρει γρήγορη σάρωση ενός δικτύου, παρέχει παράλληλα στον χρήστη μια αναλυτική εικόνα του προς ελέγχου δικτύου, φανερώνοντας πιθανά προβλήματα και ελλείψεις ασφάλειας. Τέλος, το Nmap χρησιμοποιήθηκε για την ανίχνευση ανοικτών ports στο δίκτυο από τους χρήστες με σκοπό την ολοκλήρωση του challenge.

4. Υλοποιημένες CTF προκλήσεις

Οι προκλήσεις οι οποίες δημιουργήθηκαν στα πλαίσια της πτυχιακής εργασίας για την εκπαίδευση φοιτητών πάνω στον τομέα της κυβερνοασφάλειας ανέρχονται στα τρία. Κάθε ένα από αυτά ανήκει σε διαφορετική κατηγορία: κρυπτογράφηση (crypto), δικτύωση (networking) και επίθεση (attack). Επιπρόσθετα, η έμπνευση για την δημιουργία των συγκεκριμένων προκλήσεων προέρχεται μέσα από την διδακτέα ύλη του μαθήματος Ασφάλεια Δικτύων. Στην συνέχεια θα αναφερθούν ορισμένα χαρακτηριστικά για κάθε μια πρόκληση.

Το πρώτο challenge με τίτλο “What is RSA ?” στοχεύει στην εκμάθηση των χρηστών στον τρόπο με τον οποίο ένας αλγόριθμος κρυπτογραφεί και αποκρυπτογραφεί δεδομένα. Αναλυτικότερα, για την πρόκληση αυτή γίνεται χρήση του αλγορίθμου RSA, ο οποίος αποτελεί έναν δημοφιλή αλγόριθμο κρυπτογράφησης. Επιπρόσθετα, οι χρήστες για την επίλυση του challenge αυτού πρέπει να αξιοποιήσουν τα δεδομένα που τους παρέχονται στην περιγραφή της πρόκλησης. Ο κύριος παράγοντας ώστε να ξεκινήσει η διαδικασία είτε της κρυπτογράφησης είτε της αποκρυπτογράφησης είναι οι πρώτοι αριθμοί (prime numbers). Ακόμα, μέσα από την βοήθεια αυτών των αριθμών και του δημόσιου κλειδιού (public key), ο χρήστης ανακαλύπτει το ιδιωτικό κλειδί (private key). Έχοντας στην κατοχή του και τα δυο είδη κλειδιών ο χρήστης είναι σε θέση να αποκρυπτογραφεί και να κρυπτογραφεί δεδομένα. Επίσης, για την ολοκλήρωση της πρόκλησης πρέπει να αποκρυπτογραφήσει τα κρυπτογραφημένα δεδομένα και να βρει την αρχική πληροφορία, η οποία αποτελεί τον κωδικό για το κλειδωμένο αρχείο. Συνοψίζοντας, σκοπός αυτού του challenge είναι οι χρήστες να κατανοήσουν την ιδέα της αποκρυπτογράφησης και πιο συγκεκριμένα την λειτουργία του RSA αλγορίθμου.

Ο τίτλος του δεύτερου challenge είναι “Where is the map ?” και ανήκει στην κατηγορία networking. Πρόκειται για μια πρόκληση κατά την οποία οι χρήστες πρέπει να διερευνήσουν το τοπικό τους δίκτυο χρησιμοποιώντας την εντολή Nmap, προκειμένου να εντοπίσουν πληροφορίες για τις ενεργές διευθύνσεις του δικτύου τους. Μια από αυτές τις διευθύνσεις αποτελεί έναν ftp server, του οποίου τα credentials έχουν δοθεί κατά την λύση του 1^{ου} challenge. Εν κατακλείδι, μόλις ο χρήστης αποκτήσει τα στοιχεία σύνδεσης και την αντίστοιχη διεύθυνση, το μόνο που χρειάζεται να κάνει είναι να συνδεθεί μέσω αυτής χρησιμοποιώντας το SSH. Μέσω αυτού του challenge, οι χρήστες θα εξοικειωθούν με τη χρήση της εντολής Nmap και θα κατανοήσουν τα αποτελέσματα που προκύπτουν από την εκτέλεσή της.

Το τρίτο challenge, το οποίο ανήκει στην κατηγορία attack, έχει τίτλο “Brute Force Attack”. Αυτό το challenge περιλαμβάνει δύο ρόλους: τον επιτιθέμενο και τον αμυνόμενο, ο οποίος είναι ένας docker container και όχι πραγματικός χρήστης. Ο στόχος του επιτιθέμενου είναι να χρησιμοποιήσει τα δεδομένα που του δίνονται για να βρει την σωστή αλληλουχία ονόματος και κωδικού, αποκτώντας πρόσβαση στα δεδομένα του αμυνόμενου. Για την ολοκλήρωση του challenge, ο επιτιθέμενος θα χρησιμοποιήσει το Metasploit framework για να εκτελέσει brute force attack και να εντοπίσει ευπάθειες στο σύστημα του αμυνόμενου. Σκοπός του challenge είναι να κατανοήσουν οι χρήστες τις βασικές λειτουργίες του Metasploit και την εφαρμογή του brute force attack για την εκμετάλλευση ευπαθειών.

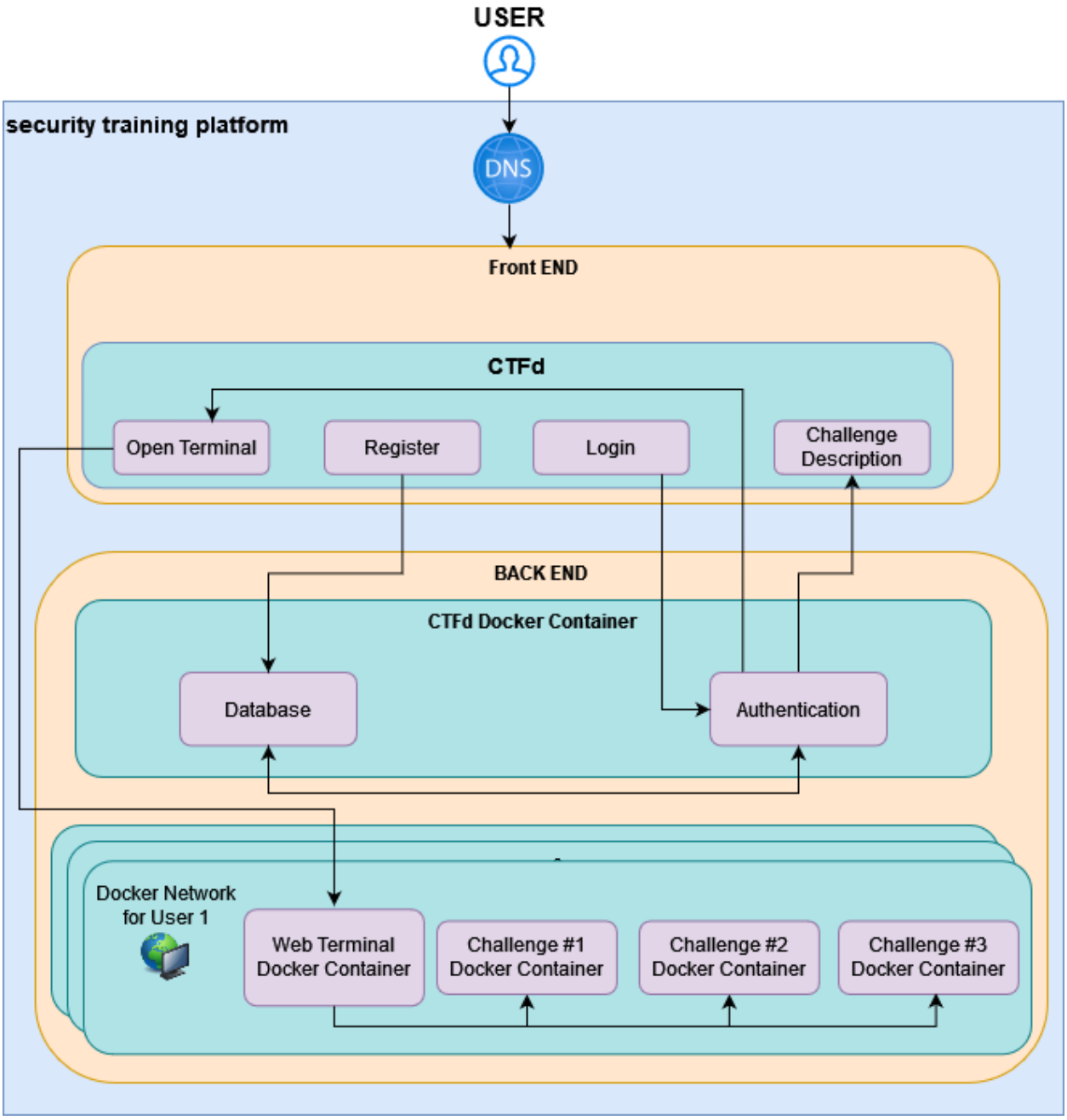
Περισσότερες πληροφορίες για την κάθε μια πρόκληση καθώς και για την υλοποίηση τους θα αναφερθούν στο επόμενο κεφάλαιο.

5. Υλοποίηση

Αρχικά, ξεκίνησε η διαδικασία εγκατάστασης του CTFd σ' ένα VM με Linux Ubuntu 20.04 λειτουργικό σύστημα. Στο documentation του CTFd framework αναφέρεται ότι για την εγκατάσταση του χρειάζονται τα εξής εργαλεία: docker, καθώς και το docker compose. Ύστερα από την εγκατάσταση των παραπάνω εργαλείων έγινε η κλωνοποίηση του CTFd από το github και η εγκατάσταση του στο VM. Αφού πραγματοποιηθούν όλα τα απαραίτητα βήματα ο διαχειριστής εισέρχεται στο CTFd και ξεκινάει την διαδικασία υλοποίησησης των προκλήσεων. Για να γίνει αυτό θα πρέπει να μεταβεί στον φάκελο όπου έγινε η κλωνοποίηση του CTFd, να εισέλθει στον sub folder που ονομάζεται CTFd. Στην συνέχεια, μέσα στο console εκτελώντας την εντολή "docker compose up" υλοποιεί την εφαρμογή. Με αυτή την εντολή λοιπόν υλοποιούνται όλα τα docker images τα οποία χρησιμοποιεί το CTFd ώστε να τρέξει σαν ένα συνολικό multi container. Το multi container όπως αναφέρει και η εντολή "docker compose up" είναι μια σύνθεση από πολλά διαφορετικά docker images τα οποία σαν σύνολο υλοποιούν την εφαρμογή. Έτσι, θα έχουν ολοκληρωθεί όλες οι διαδικασίες ώστε να υπάρχει πρόσβαση στην εφαρμογή μέσα από το διαδίκτυο και γράφοντας localhost:8000 στον browser. Το 8000 είναι το port στο οποίο είναι διαθέσιμο το front-end του CTFd framework. Συμπληρωματικά, όλες οι πληροφορίες σχετικά με το CTFd βρίσκονται στο ξεχωριστό κεφάλαιο Appendix, το οποίο βρίσκεται στο τέλος.

5.1 Αρχιτεκτονική Συστήματος

Η αρχιτεκτινική που απεικονίζεται στην Εικόνα 1 παρακάτω αποτελεί τον τρόπο με τον οποίο ο χρήστης θα πλοηγείται εντός της πλατφόρμας, καθώς και την επικοινωνία που υπάρχει αναμεσά στο front end και στο back end. Πιο συγκεκριμένα, κατά την είσοδο του χρήστη στο url το DNS θα τον ανακατευθύνει στο front end της CTFd πλατφόρμας. Για να έχει την πλήρη πρόσβαση σε αυτή θα πρέπει να ολοκληρώσει την εγγραφή του στην εφαρμογή. Έπειτα θα είναι σε θέση να πλοηγηθεί στις διάφορες επιλογές που υπάρχουν. Συνεπώς, μετά την σύνδεση του χρήστη στην εφαρμογή, μπορεί να διαβάσει τις περίγραφες των προκλήσεων, πράγμα που θα τον βοηθήσει να φτάσει στην ολοκλήρωση τους. Επιπρόσθετα, ο χρήστης μπορεί μέσα από το front end του CTFd framework με το πάτημα του κουμπιού web terminal, να δημιουργήσει και στην συνέχεια να ανακατευθυνθεί στο δικό του ξεχωριστό docker δίκτυο. Το συγκεκριμένο δίκτυο αποτελείται από όλα τα απαραίτητα docker containers πάνω στα οποία έχουν στηθεί όλες οι προκλήσεις. Μέσω της περιγραφής των προκλήσεων στο front end της πλατφόρμας μπορεί ο χρήστης να αξιοποιήσει τις IP διευθύνσεις που του έχουν δοθεί και με αυτόν τον τρόπο να εισέλθει στο docker container που αποτελεί την πρόκληση. Συνοψίζοντας, με το πάτημα του κουμπιού ο χρήστης δημιουργεί στο backend τα δικά του docker containers μέσα από τα οποία στήνονται οι προκλήσεις.



Εικόνα 1 Αρχιτεκτονική Συστήματος

5.2 Προκλήσεις

Η σχεδίαση και η υλοποίηση των προκλήσεων είναι ανεξάρτητη από την πλατφόρμα του CTFd. Η σύνδεση των προκλήσεων με το CTFd έχει πραγματοποιηθεί με την βοήθεια του κουμπιού open terminal, όπως φαίνεται και στο διάγραμμα παραπάνω. Το κουμπί αυτό έχει προστεθεί στο fronted του CTFd και σκοπό έχει να μεταφέρει τον χρήστη από το CTF μέσα στο docker δίκτυο που έχει δημιουργηθεί για εκείνον. Κατά την είσοδο του χρήστη στο δίκτυο αυτό, συνδέεται με το βασικό docker container το οποίο θα τον βοηθήσει καθ' όλη την διάρκεια του CTF. Το όνομα αυτού του είναι web terminal. Σκοπός λοιπόν του προαναφερθέντος container είναι η διαχείριση των

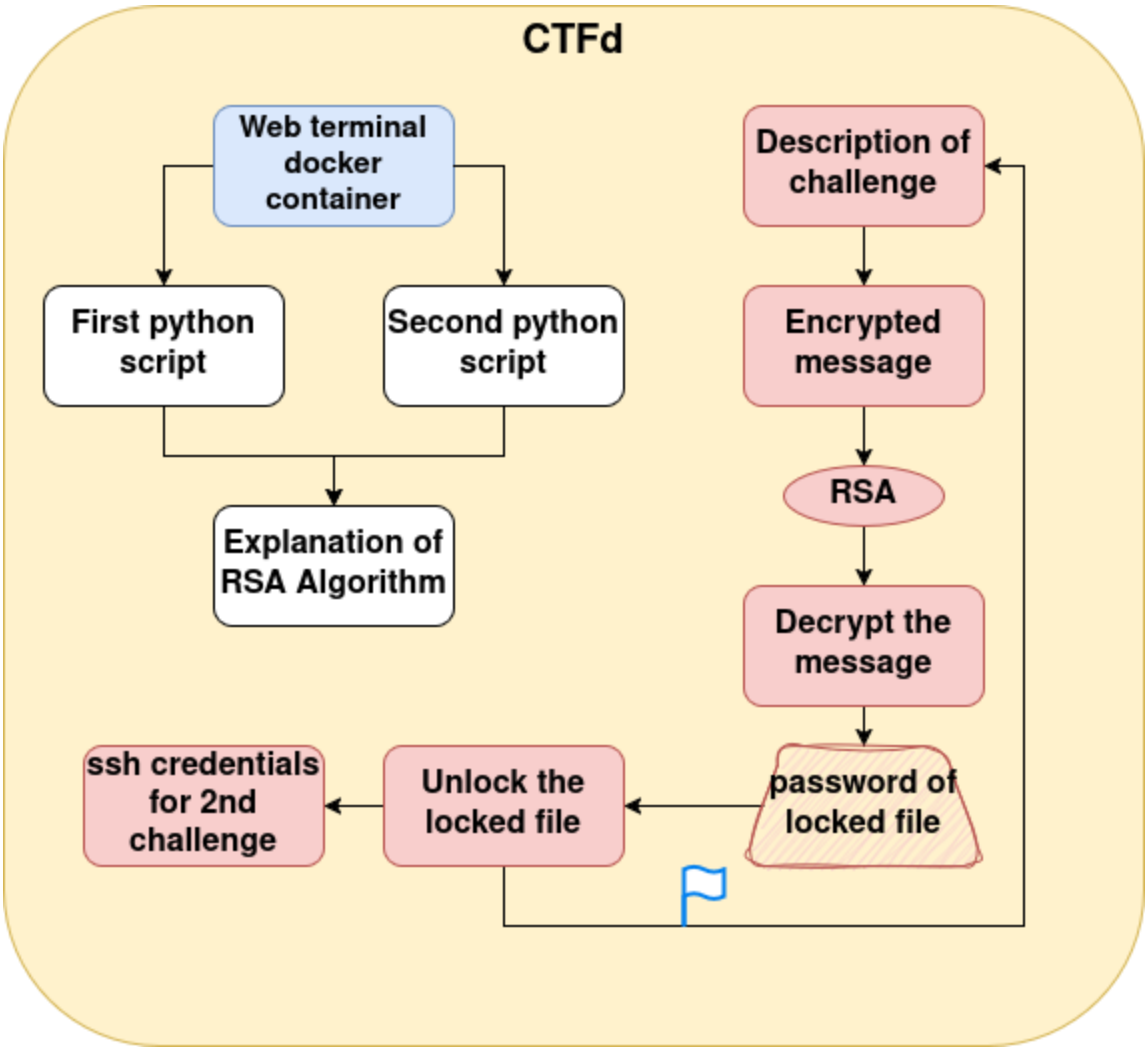
υπολοίπων τριών challenges. Λεπτομέρειες για τον τρόπο λειτουργίας των containers, καθώς και τα βήματα που θα πρέπει να ακολουθήσουν οι χρήστες μέχρι να φτάσουν στην επίλυση των challenges θα αναλυθούν στην συνέχεια.

5.2.1 1η Πρόκληση: What is RSA?

Το συγκεκριμένο challenge περιέχει δυο python scripts τα οποία περιγράφουν αναλυτικά την διαδικασία και τα βήματα που ακολουθεί ο RSA αλγόριθμος ώστε να δημιουργήσει τα κλειδιά κρυπτογράφησης και να κρυπτογραφήσει τα δεδομένα. Το πρώτο python script με όνομα rsa1.py, το οποίο βρίσκεται μέσα στον φάκελο python scripts του docker container, αποτελεί βοηθό για τους χρήστες να κατανοήσουν τον αλγόριθμο. Το αποτέλεσμα της εκτέλεσης του 1ου python script είναι η κωδικοποίηση και η αποκωδικοποίηση ενός αριθμού. Το δεύτερο script, το οποίο βρίσκεται στον ίδιο φάκελο και αυτό αλλά με όνομα rsa2.py, αποτελεί μια πιο ρεαλιστική απεικόνιση του αλγορίθμου. Σκοπός αυτού του script είναι να παρουσιάσει πως ένα πραγματικό μήνυμα μπορεί να κρυπτογραφηθεί μέσα από τον αλγόριθμο RSA. Για την επίτευξη αυτού του στόχου, το πρώτο βήμα είναι να μετατραπούν τα γράμματα σε ASCII αριθμούς. Έπειτα, μέσα από το ιδιωτικό κλειδί κωδικοποιούνται στην μεριά του αποστολέα, ενώ ο παραλήπτης με την βοήθεια του public key τα αποκωδικοποιεί και βρίσκει το αρχικό μήνυμα που του στάλθηκε.

Σκοπός των χρηστών είναι να βρουν τον κωδικό με τον οποίο προστατεύεται το ZIP file το οποίο τους έχει παραχωρηθεί στην περιγραφή του challenge (Εικόνα 37 η οποία βρίσκεται στο appendix A) με όνομα credentials.zip. Έχοντας αξιοποιήσει οι χρήστες τους αριθμούς από την περιγραφή του challenge με τον σωστό τρόπο, θα έχουν ξεκλειδώσει το αρχείο όπου βρίσκεται το flag, καθώς και πληροφορίες που σχετίζονται με την 2η πρόκληση.

Η Εικόνα 2 απεικονίζει τα στάδια που πρέπει να περάσει ο χρήστης με σκοπό την επίλυση της πρώτης πρόκλησης. Αναλυτικότερα, μέσα από το web terminal docker container ο χρήστης αξιοποιώντας τα δυο python scripts, τα οποία βρίσκονται στον φάκελο python_scripts, μπορεί να κατανοήσει την λειτουργία του RSA. Το επόμενο βήμα είναι η αξιοποίηση των λεπτομερειών που του παρέχονται στην περιγραφή της πρόκλησης. Συμπερασματικά, εάν έχει κατανοήσει πως λειτουργεί ο RSA, τότε θα είναι σε θέση να ξεκλειδώσει το αρχείο.



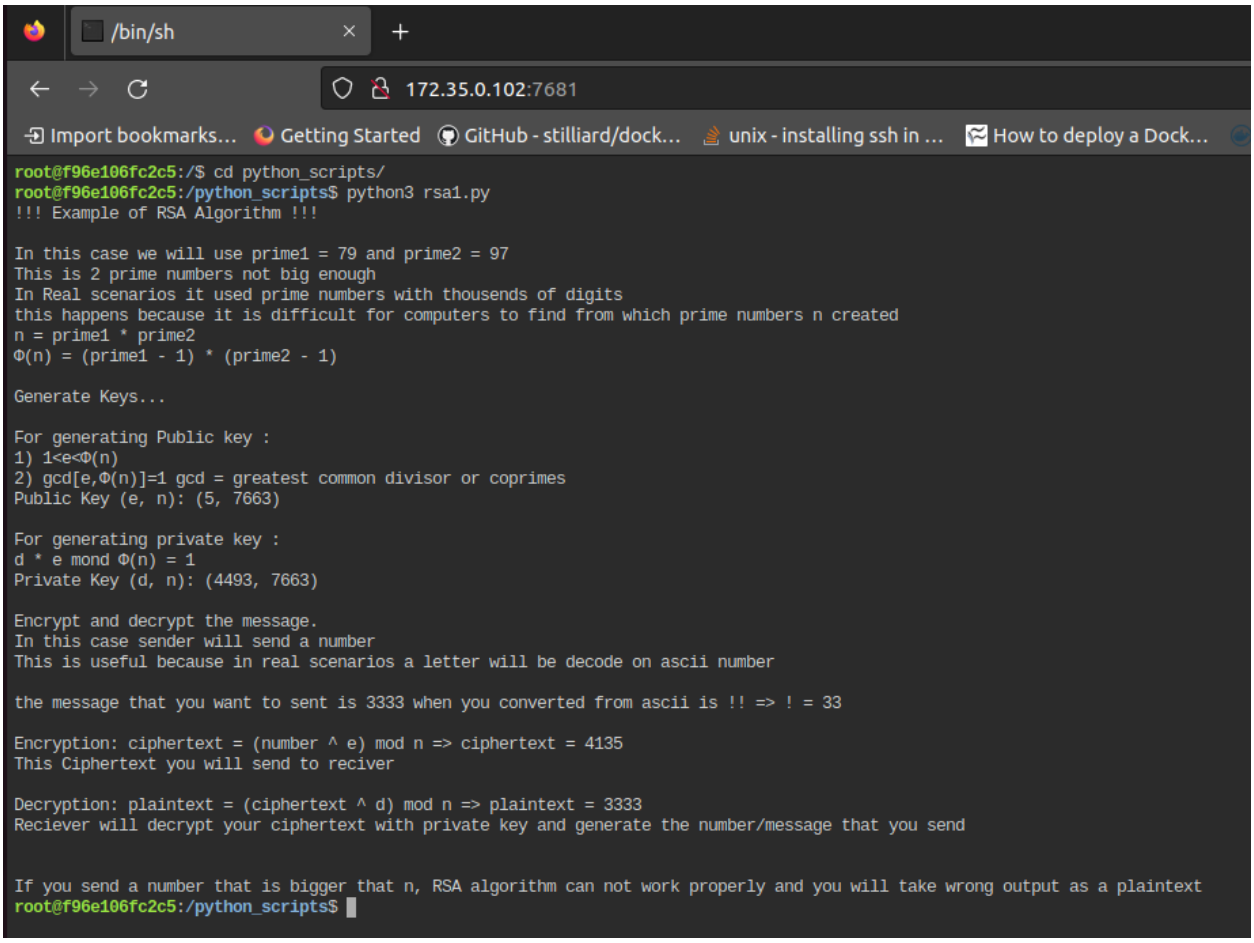
Εικόνα 2 Σχεδιάγραμμα πρώτης πρόκλησης

Για την ολοκλήρωση της 1ης πρόκλησης από τους χρήστες, απαραίτητη είναι η σύνδεση τους μέσα από το frontend της εφαρμογής στο docker container της 1ης πρόκλησης μέσα από το κουμπί open terminal.

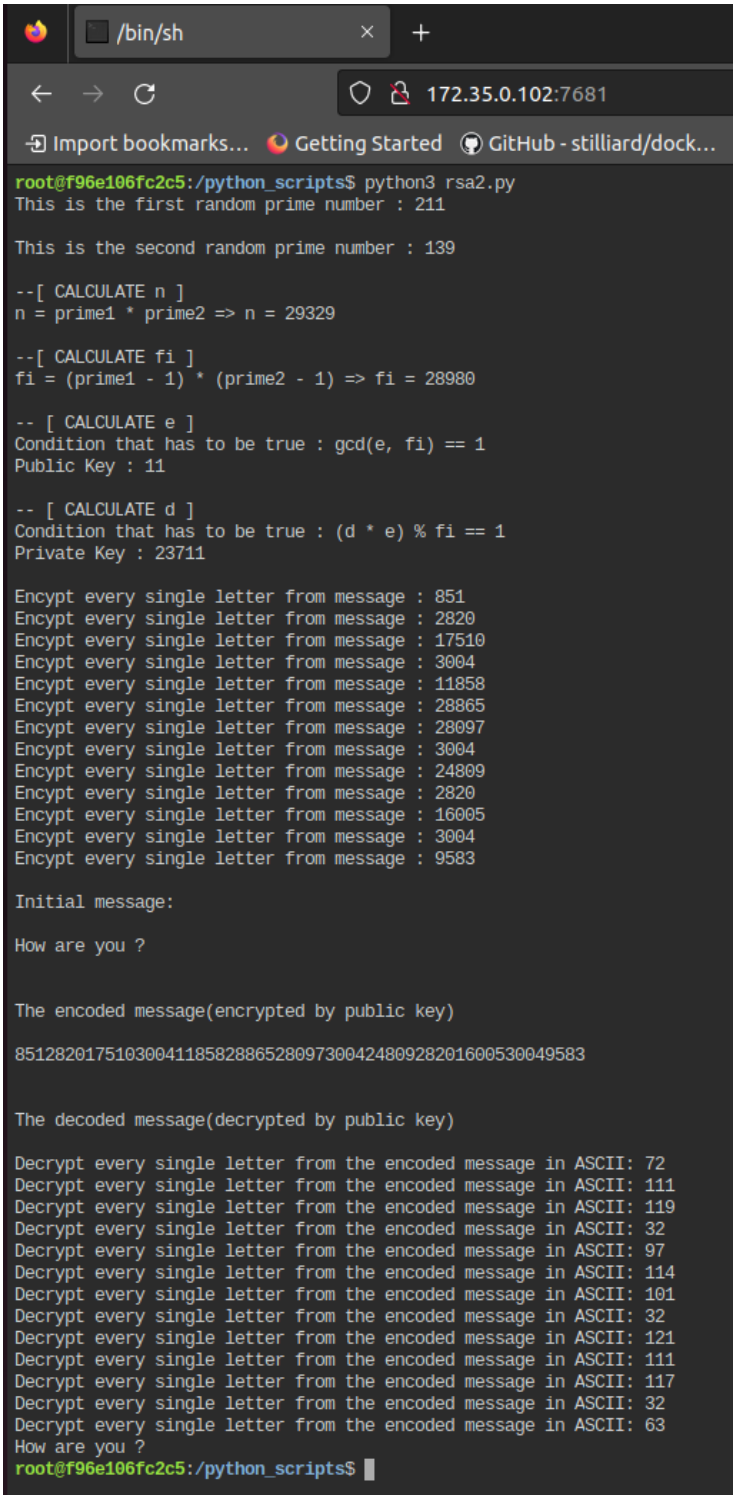
Μετά την ολοκλήρωση της παραπάνω σύνδεσης οι χρήστες θα πρέπει να ακολουθήσουν την περιγραφή που τους έχει δοθεί ώστε να φέρουν εις πέρας την πρόκληση. Τα βήματα που πρέπει να ακολουθήσουν είναι τα εξής:

1. Είσοδος του χρήστη στον φάκελο python scripts μέσα στο container. (βλ. Εικόνα 3)
2. Μέσα από την python να κάνει compile τα δυο scripts (rsa1.py, rsa2.py) που του παρέχονται. (βλ. Εικόνα 3 - Εικόνα 4)
3. Η κατανόηση του RSA αλγορίθμου μέσα από τα παραπάνω scripts και η επίλυση του.

Οι Εικόνα 3 και Εικόνα 4 που ακολουθούν αποτελούν τα δυο scripts που έχουν αναφερθεί παραπάνω. Η πρώτη αποτελεί το rsa1.py ενώ η δεύτερη αποτελεί το rsa2.py.



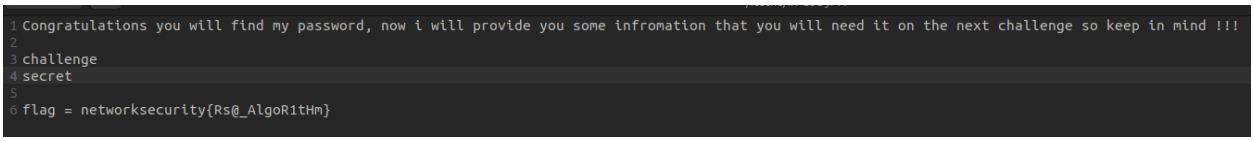
Εικόνα 3 Επεξήγηση RSA αλγορίθμου μέσα από το rsa1.py



Εικόνα 4 Επεξήγηση RSA αλγορίθμου μέσα απο το rsa2.py

Μέσα από την περιγραφή της 1ης πρόκλησης παρέχεται στον χρήστη ένας “κλειδωμένος” φάκελος. Σκοπός του χρήστη είναι να αποκρυπτογραφήσει τα δεδομένα που του έχουν παρατεθεί και να βρει τον κωδικό για να ξεκλειδώσει τον φάκελο. Όπως φαίνεται στην Εικόνα 5 χρήστης θα δει τα ακόλουθα:

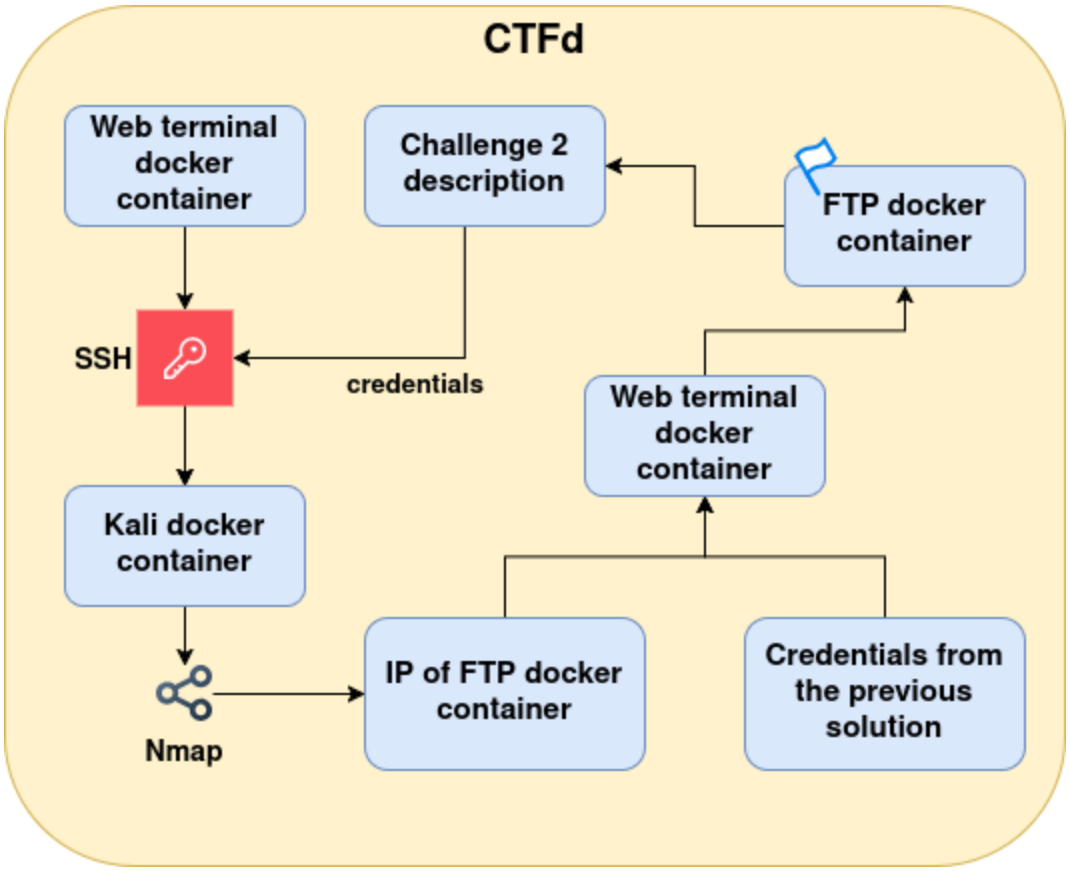
1. Το flag, το οποίο πρέπει να καταθέσει στο CTFd ως λύση της πρόκλησης.
2. Και τα στοιχεία σύνδεσης που θα χρησιμοποιήσει ο χρήστης κατά την διάρκεια της 2ης πρόκλησης για την σύνδεση του στον ftp server.



Εικόνα 5 Το flag της πρώτης πρόκλησης και πληροφορίες για την επόμενη

5.2.2 2η Πρόκληση: Where is the map ?

Η 2η πρόκληση με την σειρά του στόχο έχει την εξοικείωση των χρηστών με το εργαλείο nmap. Πιο συγκεκριμένα, αποτελείται από 3 docker containers (kali container, web terminal container, ftp server container). Τα βήματα που ακολουθούν για να ολοκληρωθεί με επιτυχία αυτό το challenge είναι τα παρακάτω: σύνδεση μέσα από το web terminal με ssh στο container kali το οποίο περιέχει το εργαλείο nmap. Το επόμενο βήμα που θα ακολουθήσει από τους συμμετέχοντες είναι να κάνουν scan το δίκτυο τους και να παρατηρήσουν πως υπάρχει ένας ανοικτός ftp server, καθώς και την IP του. Όταν λοιπόν ολοκληρωθεί το παραπάνω βήμα, σειρά έχει να επιστρέψουν πίσω στο web terminal του container και να συνδεθούν με ssh στον ftp server. Για την σύνδεση αυτή, η IP του ftp server container εντοπίστηκε από το nmap scan που πραγματοποιήθηκε στο δίκτυο. Τα στοιχεία σύνδεσης που απαιτούνται για την σύνδεση αυτή δόθηκαν από στην επίλυση της $1^{ης}$ πρόκλησης. Όμως, ο ftp server περιέχει αρκετά αρχεία οπότε οι χρήστες πρέπει να ανακαλύψουν εκείνο το οποίο περιέχει το flag και να το καταθέσουν στην εφαρμογή. Συνοψίζοντας σκοπός αυτής της πρόκλησης είναι να διδάξει την βασική λειτουργία του εργαλείου nmap πάνω στο network scanning. Η παραπάνω περιγραφή αντιστοιχεί στο Εικόνα 6 η οποία δείχνει τα βήματα του χρήστη μέχρι την επίλυση της πρόκλησης.



Εικόνα 6 Σχεδιάγραμμα 2ης πρόκλησης

Στην 2η πρόκληση τα βήματα που πρέπει να ακολουθήσουν οι χρήστες είναι τα εξής:

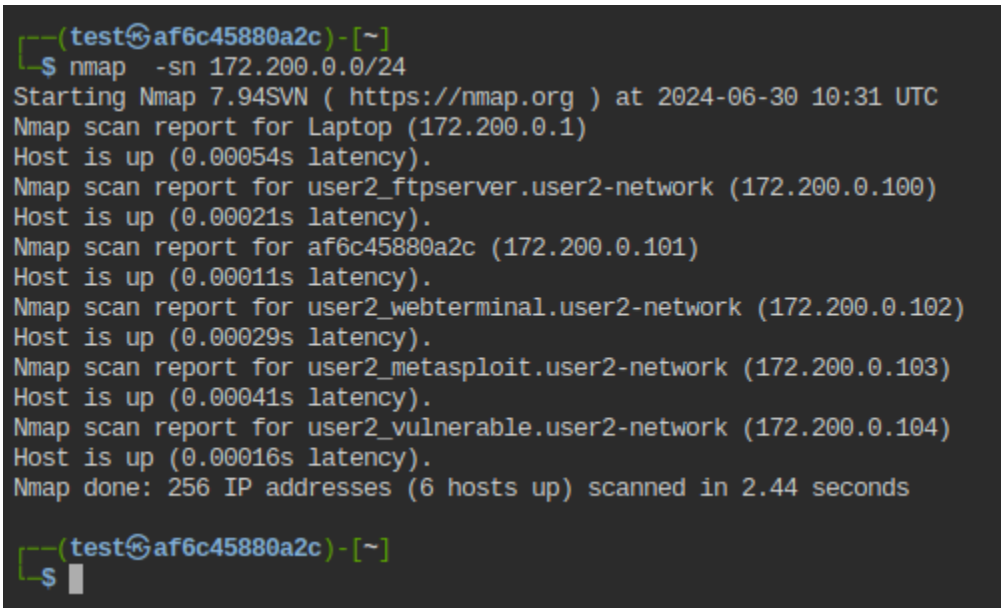
1. Σύνδεση με ssh στην IP που υπάρχει στην περιγραφή της πρόκλησης.
2. Χρήση του εργαλείου nmap για την ανάλυση του δικτύου που βρίσκεται ο χρήστης.
3. Παρατήρηση των αποτελεσμάτων του nmap και κατανόηση που πρέπει να συνδεθεί.
4. Σύνδεση στον ftp server με τα credentials από την 1η πρόκληση.
5. Απεικόνιση της λύσης του προβλήματος με την χρήση του command cat και την απόκτηση του flag μέσα από το αρχείο users.py.

Στην παρακάτω Εικόνα 7 παρουσιάζεται η μέθοδος σύνδεσης με το kali container μέσα από το web terminal container με την χρήση του ssh.



Εικόνα 7 Σύνδεση ssh με το kali docker container

Αφού ολοκληρωθεί το παραπάνω βήμα με επιτυχία, στην συνέχεια ο χρήστης θα πρέπει να αναλύσει το δίκτυο του με την χρήση του nmap. Στην Εικόνα 8 φαίνεται το nmap command το οποίο παρουσιάζει τις βασικές πληροφορίες για τις διεργασίες που τρέχουν σε αυτό το υποδίκτυο που έχει οριστεί. Επίσης, ο χρήστης μπορεί να ενημερωθεί για περισσότερες πληροφορίες εκτελώντας το command nmap 172.200.0.0/24 χωρίς δηλαδή την παράμετρο -sn.



Εικόνα 8 Ανάλυση δικτύου με το Nmap

Η Εικόνα 9 που προβάλλεται παρακάτω αποτελεί την σύνδεση του χρήστη με τον ftp server μετά από την χρήση του Nmap στο προηγούμενο βήμα. Ακόμα, τα στοιχεία σύνδεσης για τον ftp server έχουν αποκτηθεί κατά την επίλυση της 1ης πρόκλησης (βλ. Εικόνα 9).

```
root@f038fec12285:/$ ssh challenge@172.200.0.100
challenge@172.200.0.100's password:
Linux fe567843070b 6.5.0-35-generic #35~22.04.1-Ubuntu SMP PREEMPT_DYNAMIC Tue May  7 09:00:52 UTC 2 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: Sun Jun 30 10:51:14 2024 from 172.200.0.102
challenge@fe567843070b:~$ ls
flag
challenge@fe567843070b:~$
```

Εικόνα 9 Σύνδεση ssh με το docker ftp server

Αφού ολοκληρωθούν τα προαναφερθέντα βήματα με επιτυχία από την πλευρά του χρήστη σειρά έχει να εντοπίσει το flag το οποίο βρίσκεται μέσα στον ftp server. Καθώς εισέρχεται στον φάκελο Lab θα παρατηρήσει πως υπάρχουν 2 αρχεία .py (βλ Εικόνα 10), το ένα από αυτά περιέχει το συνθηματικό που θα πρέπει να καταθέσει στο CTFd framework ως λύση του προβλήματος. Ακόμα, μετά το πέρας της εκτέλεσης του αρχείου users.py θα παρατηρήσει πως αυτό το αρχείο περιέχει τον Employee με το flag.

```
challenge@fe567843070b:~/flag/Lab$ ls
app.py  users.py
challenge@fe567843070b:~/flag/Lab$ python3 users.py
Employee : Dimitra clearhas not something to tell you
Employee : Manos clearhas not something to tell you
Employee : Kwstantina clearhas not something to tell you
You find me read my story i have something UNIQUE for you
 find my story first
Employee : Stamatis clearhas not something to tell you
Employee : Marios clearhas not something to tell you
Employee : Nikos clearhas not something to tell you
Employee : Xenofon clearhas not something to tell you
Employee : Aggelos clearhas not something to tell you
Employee : Kalliopi clearhas not something to tell you
challenge@fe567843070b:~/flag/Lab$
```

Εικόνα 10 Αποτελέσματα του users.py script

Τέλος, στην Εικόνα 11 έχουμε την ανάλυση του users.py με το command cat. Επίσης, στην τελευταία γραμμή του Employee Andreas υπάρχει το flag, καθώς είναι ο μοναδικός employee που δεν παρουσιάζεται μετά το compile του users.py αρχείου.

```
#Andreas as an employee has to tell you this story :

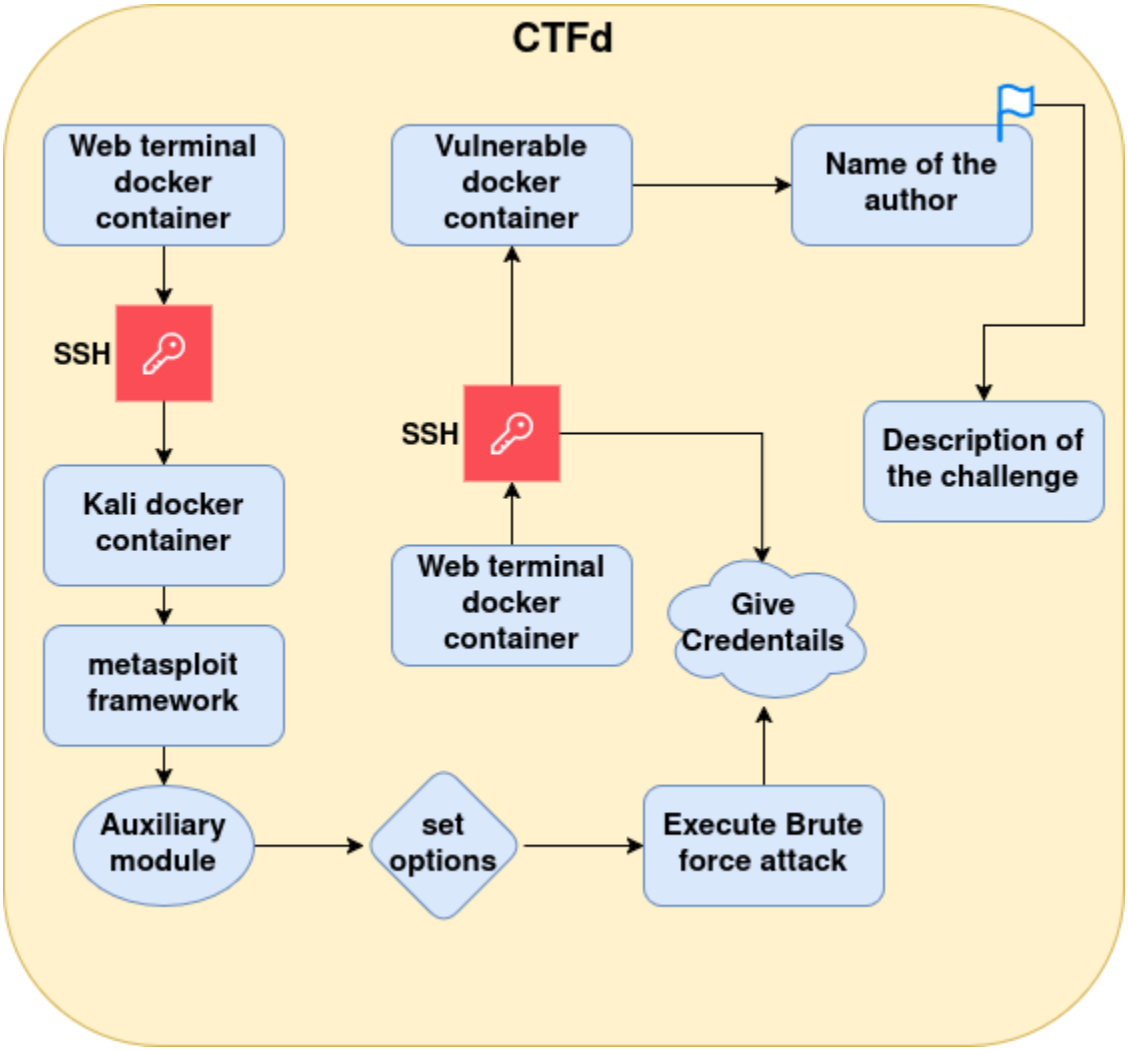
#Integer varius at augue quis sodales. Nunc vehicula, ex ac porttitor condimentum, tellus elit posuere mi, in posuere enim neque in ante. Phasellus laoreet molestie justo, nec luctus risus laoreet a. Cras sit amet vestibulum neque, ac porta ipsum. Aenean tortor tortor,
posuere sed augue a, tincidunt lacinia purus. Curabitur tortor libero, pretium quis posuere in, scelerisque a velit. Phasellus lobortis ligula mollis mattis dictum. Morbi ornare ullamcorper venenatis.
#Aenean non efficitur orci. Morbi bibendum molestie quam vitae placerat. Orci varius natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus. Phasellus laoreet molestie justo, nec luctus risus laoreet a. Cras sit amet vestibulum neque, ac porta ipsum.
Aenean tortor tortor, posuere sed augue a, tincidunt lacinia purus. Curabitur tortor libero, pretium quis posuere in, scelerisque a velit. Phasellus lobortis ligula mollis mattis dictum. Morbi ornare ullamcorper venenatis.
#Sed egestas dui et vehicula tempor. Sed cursus mi a feugiat aliquam. Curabitur tortor libero, pretium quis posuere in, scelerisque a velit. Phasellus lobortis ligula mollis mattis dictum. Morbi ornare ullamcorper venenatis. Curabitur tortor libero, pretium quis posuere
in, scelerisque a velit. Phasellus lobortis ligula mollis mattis dictum. Morbi ornare ullamcorper venenatis. networksecurity{This_is_Th3_F1AG} Donec gravida fringilla sapien, eget accumsan nisl ultrices nec.
```

Εικόνα 11 Περιεχόμενα του sccript με την εντολή cat στο users.py

5.2.3 3η Πρόκληση: Brute Force Attack

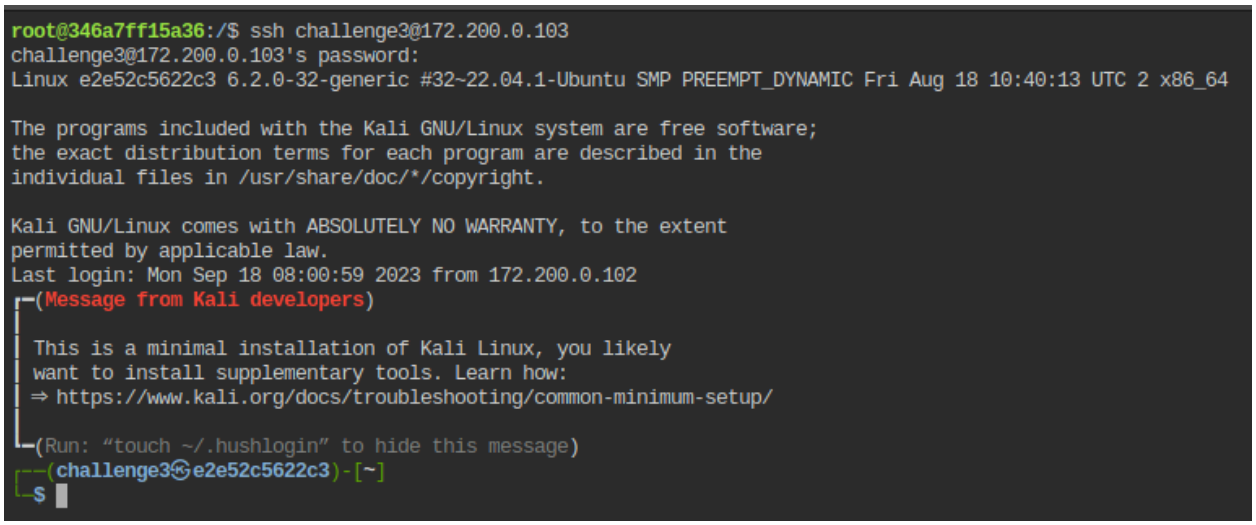
Η 3η προκληση, είναι τύπου brute force attack. Η πρόκληση αυτή στοχεύει να διδάξει τους συμμετέχοντες τον τρόπο με τον οποίο υλοποιείται ένα brute force attack. Αρχικά αυτό η

πρόκληση αποτελείται από 2 containers τα οποία είναι στο ίδιο δίκτυο όπως και τα υπόλοιπα. Το πρώτο container αποτελεί τον επιτιθέμενο (kali container), ενώ το δεύτερο αποτελεί το μηχάνημα στο οποίο θα γίνει το attack (vulnerable container). Απώτερος σκοπός της συγκεκριμένης πρόκλησης είναι η εκμάθηση του brute force attack στους χρήστες, καθώς και η εξοικείωση τους με το metasploit framework και τις ευπάθειες που μπορεί να έχει ένα σύστημα. Αξίζει να σημειωθεί ότι το victim container το οποίο αποτελεί και τον στόχο όπου θα γίνει η προσομοίωση αυτής της επίθεσης, είναι docker container με προεγκατεστημένες ευπάθειες. Τέλος, στο διάγραμμα που ακολουθεί παρουσιάζονται τα βήματα για την υλοποίηση της πρόκλησης αυτής.



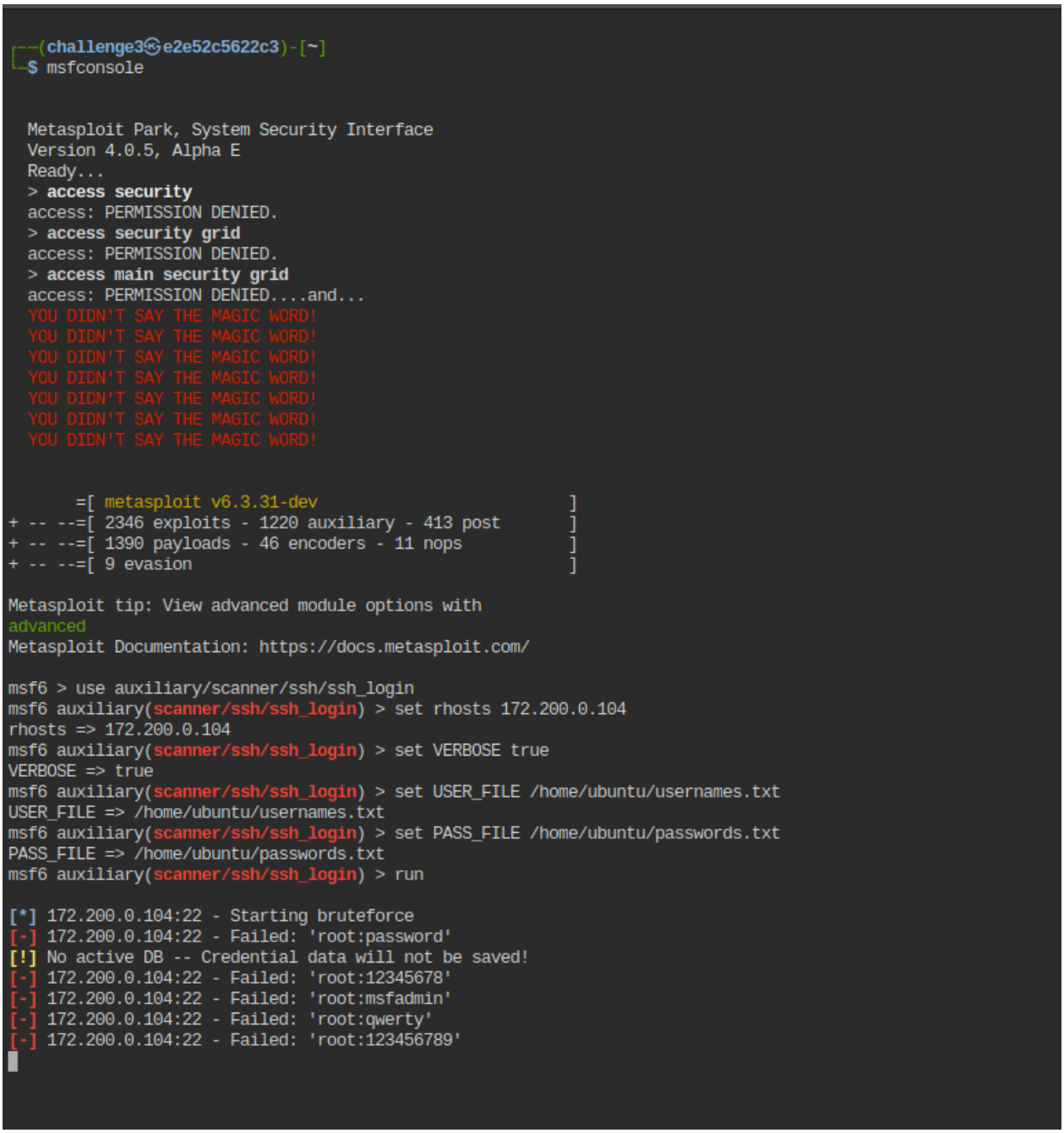
Εικόνα 12 Σχεδιάγραμμα 3ης πρόκλησης

Η 3η πρόκληση αποτελεί ένα brute force attack σ' ένα docker container το οποίο περιέχει ευπάθειες. Το πρώτο βήμα είναι η σύνδεση του χρήστη με ssh στο container που θα εκτελέσει το attack, τα στοιχεία σύνδεσης και η IP του container αναγράφονται στην περιγραφή της 3ης πρόκλησης.



Εικόνα 13 Σύνδεση μέσω ssh στο container που θα εκτελέσει το attack

Μετά την σύνδεση στο container μέσα απο το οποίο, ο χρήστης χρησιμοποιεί το metasploit framework για να πραγματοποιήσει το brute force attack. Το msfconsole command ενεργοποιεί το console του metasploit, μέσα από το οποίο θα διεξαχθεί η επίθεση. Επίσης, για να ολοκληρωθεί το attack με επιτυχία θα πρέπει ο χρήστης να χρησιμοποιήσει τα κατάλληλα options όπως φαίνεται και στην
εικόνα παρακάτω. Πιο συγκεκριμένα τα options, αποτελούν τον κύριο παράγοντα ώστε να ολοκληρωθεί το attack με επιτυχία, καθώς επίσης ορίζονται διάφορες παράμετροι όπως αυτή της διεύθυνσης του αμυνόμενου. Επιπρόσθετα, ορίζεται όχι μόνο η διεύθυνση του, άλλα και τα αρχεία τα οποία περιέχουν ονόματα και κωδικούς αναγκαία για να ολοκληρωθεί το attack.



Εικόνα 14 Αρχικοποίηση των απαραίτητων μεταβλητών

Στις Εικόνα 14 - Εικόνα 15 παρουσιάζεται η υλοποίηση του brute force attack καθώς και τα αποτελέσματα τα οποία προβάλλονται μετά την ολοκλήρωση του. Επίσης, τα αρχεία που χρησιμοποιείσαι στο παραπάνω βήμα ως USER_FILE και PASS_FILE, περιέχουν credentials τα οποία αξιοποιεί το metasploit για την εύρεση του σωστού κωδικού έτσι ώστε να πάρει πρόσβαση στο container με τις ευπάθειες και να πάρει το flag.

```
[*] 172.200.0.104:22 - Starting bruteforce
[-] 172.200.0.104:22 - Failed: 'root:password'
[!] No active DB -- Credential data will not be saved!
[-] 172.200.0.104:22 - Failed: 'root:12345678'
[-] 172.200.0.104:22 - Failed: 'root:msfadmin'
[-] 172.200.0.104:22 - Failed: 'root:qwerty'
[-] 172.200.0.104:22 - Failed: 'root:123456789'
[-] 172.200.0.104:22 - Failed: 'root:12345'
[-] 172.200.0.104:22 - Failed: 'root:1234'
[-] 172.200.0.104:22 - Failed: 'root:dragon'
[-] 172.200.0.104:22 - Failed: 'root:123123'
[-] 172.200.0.104:22 - Failed: 'root: '
[-] 172.200.0.104:22 - Failed: 'admin:password'
[-] 172.200.0.104:22 - Failed: 'admin:12345678'
[-] 172.200.0.104:22 - Failed: 'admin:msfadmin'
[-] 172.200.0.104:22 - Failed: 'admin:qwerty'
[-] 172.200.0.104:22 - Failed: 'admin:123456789'
[-] 172.200.0.104:22 - Failed: 'admin:12345'
[-] 172.200.0.104:22 - Failed: 'admin:1234'
[-] 172.200.0.104:22 - Failed: 'admin:dragon'
[-] 172.200.0.104:22 - Failed: 'admin:123123'
[-] 172.200.0.104:22 - Failed: 'admin: '
[-] 172.200.0.104:22 - Failed: 'msfadmin:password'
[-] 172.200.0.104:22 - Failed: 'msfadmin:12345678'
[+] 172.200.0.104:22 - Success: 'msfadmin:msfadmin' 'uid=1000(msfadmin) gid=1000(msfadmin) groups=4(adm),20(dialout),24(cdrom),25(flo
ppy),29(audio),30(dip),44(video),46(plugdev),107(fuse),111(lpadmin),112(admin),119(sambashare),1000(msfadmin) Linux 6bcdba552322 6.2.
0-32-generic #32~22.04.1-Ubuntu SMP PREEMPT_DYNAMIC Fri Aug 18 10:40:13 UTC 2 x86_64 GNU/Linux '
[*] SSH session 1 opened (172.200.0.103:37537 -> 172.200.0.104:22) at 2023-09-18 08:14:17 +0000
[-] 172.200.0.104:22 - Failed: 'test:password'
[-] 172.200.0.104:22 - Failed: 'test:12345678'
[-] 172.200.0.104:22 - Failed: 'test:msfadmin'
^C[*] Caught interrupt from the console...
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/ssh/ssh_login) >
```

Εικόνα 15 Αποτελέσματα επίθεσης

```
root@346a7ff15a36:/$ ssh msfadmin@172.200.0.104
msfadmin@172.200.0.104's password:
Linux 32554753bfe5 4.13.0-21-generic #24-Ubuntu SMP Mon Dec 18 17:29:16 UTC 2017 x86_64

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

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
Last login: Mon Sep 18 04:10:10 2023 from user2_webterminal.user2-network
msfadmin@6bcdba552322:~$ ls
vulnerable
msfadmin@6bcdba552322:~$ cd vulnerable/
msfadmin@6bcdba552322:~/vulnerable$ ls
mysql-ssl  samba  tikiwiki  twiki20030201
msfadmin@6bcdba552322:~/vulnerable$ cd twiki20030201/
msfadmin@6bcdba552322:~/vulnerable/twiki20030201$ ls
TWiki20030201.tar.gz  twiki-source
msfadmin@6bcdba552322:~/vulnerable/twiki20030201$ cd twiki-source/
msfadmin@6bcdba552322:~/vulnerable/twiki20030201/twiki-source$ ls
bin  data  index.html  lib  license.txt  pub  readme.txt  templates  TWikiDocumentation.html  TWikiHistory.html
msfadmin@6bcdba552322:~/vulnerable/twiki20030201/twiki-source$ cat readme.txt
```

Εικόνα 16 Σύνδεση με το ευπαθές container μετά την ολοκλήρωση της επίθεσης

Ολοκληρώνοντας το brute force attack με επιτυχία ο χρήστης έχει τα στοιχεία για να πραγματοποιήσει ssh connection στο victim container. Μέσα από το web terminal του attack container μπορεί να συνδεθεί στο victim container όπως φαίνεται και παρακάτω. Στο victim container περιέχονται οδηγίες για την εύρεση του flag στο readme.txt αρχείο. Ύστερα από την ανάγνωση του αρχείου ο χρήστης εντοπίζει το αρχείο που περιέχει το flag (TWikHistory.html)

```
TWiki Installation, Support
---------------------------

It is important to follow the installation instructions in
TWikiDocumentation.html located in the distribution, also at
http://TWiki.org/cgi-bin/view/TWiki/TWikiDocumentation

Important note: Once you installed TWiki on your own system,
make sure to add yourself to the list of TWikiInstallations
at http://TWiki.org/cgi-bin/view/Main/TWikiInstallations .
This helps to get more exposure --> attract more developers
--> result in a better product.

Please add a "Powered by TWiki" logo to your TWiki home page.
Review details in
http://TWiki.org/cgi-bin/view/Main/PoweredByTWikiLogo

TWiki is free software and does not include any support. There
is a TWiki web for support questions, run by TWiki users for
TWiki users. Visit http://TWiki.org/cgi-bin/view/Support/ if
you have any installation questions or questions about TWiki
deployment; please do not contact the developers directly.


TWiki News, Development and Deployment
--------------------------------------

You can always find out the latest news at the TWiki home
page at http://TWiki.org/ .

The place to collaborate on further TWiki development is at
http://TWiki.org/cgi-bin/view/Codev/ . ReadmeFirst tells you
how to collaborate. Subscribe in WebNotify to stay up to
date on latest development issues.

A side note in case you intend to use TWiki on your Intranet:
TWiki is successfully deployed as a collaboration tool and
dynamic Intranet tool at many major companies. You need to
consider some important points to reach that goal. Do not
underestimate the initial effort it takes to get a
collaboration tool accepted within the company. Support from
upper management is a must. A company with a culture that
encourages information sharing is much more likely to succeed
than one where information hoarding is the norm. There is
also an initial catch 22 problem if you intend to use it as a
knowledge base: "Why should I use the tool, there is so
little information in it". An incentive program to reward
contributions, and a dedicated knowledge engineer can help in
the initial phase of deployment.

Good luck with your collaboration effort and with TWiki.
Happy collaboration and twiki'ing.

Best regards,
PeterThoeny - Peter@Thoeny.com
msfadmin@6bcdba552322:~/vulnerable/twiki20030201/twiki-source$
```

Εικόνα 17 Η λύση της 3ης πρόκλησης

6. Αποτελέσματα

Σε αυτή την ενότητα θα αναλυθούν οι μετρήσεις και τα αποτελέσματα που προέκυψαν μέσα από τις προκλήσεις. Οι μετρήσεις πραγματοποιήθηκαν με την συμμετοχή πραγματικών χρηστών, ο συνολικός αριθμός των συμμετεχόντων ανέρχεται στους πέντε. Παρακάτω παρουσιάζονται τα αποτελέσματα που προέκυψαν σε κάθε challenge για τους χρήστες.

6.1 Αποτελέσματα 1ης Πρόκλησης

Για την 1η πρόκληση στον Πίνακας 1 παρουσιάζεται ο χρόνος επίλυσης που χρειάστηκε ό κάθε χρήστης για να επιλύσει της πρόκλησης αυτής.

Πίνακας 1 Χρόνος επίλυσης καθε πρόκλησης απο τους χρήστες

Χρήστης	Χρόνος Επίλυσης (minutes)
User 1	64
User 2	37
User 3	95
User 4	20
User 5	28

Ο User 1 χρειάστηκε 64 λεπτά για την επίλυση της πρόκλησης χωρίς να έχει ιδιαίτερες γνώσεις στον αλγόριθμο. Τα scripts που παρέχονται στους χρήστες τον βοήθησαν ώστε να φέρει εις πέρας την δοκιμασία αυτή, αποτελώντας έτσι οδηγό στον τρόπο επίλυσης του. Ακόμα, παρατηρήθηκε μετά την επιτυχής ολοκλήρωση του challenge ότι ο χρήστης απέκτησε γενικές γνώσεις πάνω στην κρυπτογράφηση και αποκρυπτογράφηση δεδομένων.

Ο User 2 με την σειρά του ολοκλήρωσε την πρόκληση σε 37 λεπτά. Σε αντίθεση με τον προηγούμενο χρήστη, δεν έκανε χρήση των scripts καθώς κατείχε γνώσεις σχετικά με τον αλγόριθμο. Για τις αρχικές πράξεις, όπως αυτή της εύρεσης του δεύτερου prime number, έκανε χρήση του calculator. Από την άλλη, για την εύρεση του private key χρησιμοποίησε και αυτός python script όπου καταχώρησε τις τιμές που βρήκε προηγουμένως και υλοποιώντας συνάρτηση όπου πραγματοποιεί την εύρεση του κλειδιού. Επιπρόσθετα, παρατηρήθηκε ότι η επίλυση της πρόκλησης βοήθησε τον χρήστη ώστε να κατανοήσει σε μεγαλύτερο βαθμό την λειτουργία του σε ένα πιο ρεαλιστικό επίπεδο, παρότι είχε γνώση του αλγορίθμου. Τέλος, ο συγκεκριμένος χρήστης απάντησε με μεγαλύτερη σιγουριά στην ερώτηση που αφορούσε αυτήν την πρόκληση.

Ο User 3 που πήρε μέρος στην δοκιμασία αυτή δεν είχε απολύτως καμία γνώση για τον RSA. Επομένως, χρειάστηκε να παρακολουθήσει και να διαβάσει ενδελεχώς τον αλγόριθμο και έπειτα πέρασε στην υλοποίηση του challenge. Συνεπώς, ο χρήστης χρειάστηκε 95 λεπτά ώστε να λύσει το challenge. Εν συνέχεια, τα scripts τον βοήθησαν ώστε να κατανοήσει προγραμματιστικά τον τρόπο λειτουργίας του αλγορίθμου σ’ έναν βαθμό. Έχοντας κατανοήσει τα scripts πέρασε στην ιστοσελίδα του wolfram alpha και μέσω αυτής έκανε τις πράξεις ώστε να βρει το αποτέλεσμα, ολοκληρώνοντας και αυτός το challenge με επιτυχία.

Ο επόμενος χρήστης User 4, εκτέλεσε τα challenges με την μεγαλύτερη επιτυχία, αλλά και σε πολύ λίγο χρονικό διάστημα. Πιο συγκεκριμένα για το πρώτο challenge φαίνεται να έχει δει τον αλγόριθμο RSA. Τα πρώτο του βήμα ήταν να διαβάσει τα scripts που έχουν παρατεθεί σαν βοήθεια. Στην συνέχεια έγραψε γρήγορα το δικό του script λύνοντας έτσι το challenge σε χρόνο μόλις 20 λεπτών. Εν κατακλείδι, το ερώτημα που του τέθηκε στο τέλος να απαντήσει δεν του φάνηκε δύσκολο, δίνοντας μια πλήρης απάντηση.

Ο τελευταίος χρήστης User 5 είχε και αυτός αρκετά γρήγορους χρόνους, με το επίπεδο του να είναι λίγο κατώτερο από του προηγουμένου χρήστη. Ξεκινώντας το challenge 1 κατάφερε να το ολοκληρώσει σε μόλις 28 λεπτά. Παρακολούθησε κάποια βίντεο σχετικά με τον αλγόριθμο πριν ξεκινήσει το challenge, τα οποία του φάνηκαν χρήσιμα για την επίλυση του. Η ερώτηση μετά την ολοκλήρωση του challenge, φάνηκε και σε αυτόν εξίσου εύκολη απαντώντας ορθά και εκείνος.

6.2 Αποτελέσματα 2ης Πρόκλησης

Στον Πίνακας 2 παρουσιάζεται ο χρόνος επίλυσης που χρειάστηκε ο κάθε χρήστης για την 2η πρόκληση.

Πίνακας 2 Χρόνος επίλυσης για την δεύτερη πρόκληση για τον κάθε χρήστη

Χρήστης	Χρόνος Επίλυσης (minutes)
User 1	32
User 2	72
User 3	58
User 4	25
User 5	30

Ο User 1 σε αυτό την πρόκληση χρειάστηκε 32 λεπτά καθώς το εργαλείο Nmap το είχε ξαναχρησιμοποιήσει στο παρελθόν. Το challenge αυτό παρακίνησε τον συγκεκριμένο χρήστη ώστε να ψάξει κάποιες από τις βασικές λειτουργίες του εργαλείου.

Ο User 2 δεν γνώριζε το εργαλείο αυτό, επομένως χρειάστηκε να διαβάσει στο διαδίκτυο τις λειτουργίες του εργαλείου. Επομένως, ο χρήστης χρειάστηκε 72 λεπτά για να ολοκληρώσει την πρόκληση αυτή. Ακόμα, παρατηρήθηκε πως μετά το πέρας της διαδικασίας ο χρήστης απέκτησε γνώσεις πάνω σε βασικά commands, καθώς και αντίληψη στον τρόπο λειτουργίας και τον σκοπό του συγκεκριμένου εργαλείου.

Ο διαγωνιζόμενος User 3, δεν είχε χρησιμοποιήσει ποτέ το εργαλείο. Έτσι, ο χρόνος της επίλυσης της πρόκλησης ανυέρχεται στα 58 λεπτά. Ο συγκεκριμένος χρήστης εξοικειώθηκε με το εργαλείο μέσα από την πρόκληση χωρίς να έχει κάποια εμπειρία.

Ο User 4 για την δεύτερη πρόκληση έκανε έναν από τους καλυτέρους χρόνους σε σχέση με τους υπολοίπους χρήστες. Επιπρόσθετα, το εργαλείο Nmap το έχει ξανά χρησιμοποιήσει στο παρελθόν, έτσι η διαδικασία επίλυσης του προβλήματος του φάνηκε αρκετά εύκολη. Τέλος, ο χρόνος μέχρι την ολοκλήρωση του ήταν μόλις 25 λεπτά.

Ο τελευταίος διαγωνιζόμενος User 5, ολοκλήρωσε την συγκεκριμένη πρόκληση στα 30 λεπτά. Δυσκολεύτηκε παραπάνω στην επίλυση σε σχέση με τον προηγούμενο καθώς προσπαθούσε να βρει τις σωστές παραμέτρους (οι οποίες έχουν αναφερθεί στην περιγραφή της πρόκλησης), με βάση τις οποίες μπορεί να υλοποιηθεί πιο γρήγορα το scan.

6.3 Αποτελέσματα 3ης Πρόκλησης

Στον Πίνακας 3 παρουσιάζεται ο χρόνος επίλυσης που χρειάστηκε ο κάθε χρήστης για την 3η πρόκληση.

Πίνακας 3 Χρόνος επίλυσης για την 3η πρόκληση

Χρήστης	Χρόνος Επίλυσης (λεπτά)
User 1	52
User 2	116
User 3	80
User 4	30
User 5	45

Στην τελευταία πρόκληση ο User 1 είχε κάνει ξανά χρήση του metasploit framework παλαιοτέρα. Έτσι, ο χρόνος επίλυσης του προβλήματος στην περίπτωση αυτή ανέρχεται στα 52 λεπτά. Συμπερασματικά, ο συγκεκριμένος χρήστης εάν και είχε ξανά χρησιμοποιήσει το metasploit δεν είχε εκτελέσει στο παρελθόν τέτοιου είδους attack οπότε κατανόησε σε μεγάλο βαθμό τον τρόπο λειτουργίας του, καθώς επίσης και πως πρέπει να στηθούν τα options έτσι ώστε να τρέξει με επιτυχία.

Για τον επόμενο χρήστη User 2, ο χρόνος που χρειάστηκε ώστε να φέρει εις πέρας την πρόκληση αυτή ήταν 116 λεπτά. Ακόμα, οι γνώσεις του πάνω στο θέμα δεν ήταν επαρκείς επομένως χρειάστηκε να αναζητήσει πληροφορίες στο διαδίκτυο όπως και στο προηγούμενο challenge. Συμπερασματικά, φαίνεται πως η πρόκληση του έδωσε γνώσεις στο συγκεκριμένο εργαλείο του οποίου έγινε χρήση.

Ο User 3 από την πλευρά του, εάν και είχε διδαχθεί το metasploit framework δεν το είχε χρησιμοποιήσει ποτέ. Εάν και οι γνώσεις που είχε ήταν επαρκείς δυσκολεύτηκε στο να βρει το σωστό module το οποίο έπρεπε να εκμεταλλευτεί. Για τον παραπάνω λόγο ο χρόνος που χρειάστηκε ο συγκεκριμένος χρήστης, ήταν 80 λεπτά. Ο χρήστης αυτός έχοντας το θεωρητικό υπόβαθρο, ήταν σε θέση να υλοποιήσει την πρόκληση με επιτυχία, όπου με βάση τα λεγόμενα του οι γνώσεις που είχε του φάνηκαν χρήσιμες.

Ο επόμενος διαγωνιζόμενος User 4, για ακόμα μια φορά έχει τον χαμηλότερο χρόνο ο οποίος ανέρχεται στα 30 λεπτά ακόμα και στην πιο απαιτητική πρόκληση. Αναφέρει επίσης, πως είχε ξανά εκτελέσει παλαιοτέρα ένα διαφορετικού είδους attack. Επομένως, οι γνώσεις του πάνω στα modules καθώς και τον τρόπο με τον οποίο πρέπει να ορίσει τα options ώστε να ολοκληρωθεί το attack του φάνηκαν αρκετά εύκολα.

Με την σειρά του ο User 5 ολοκλήρωσε με επιτυχία την πρόκληση σε χρόνο μόλις 45 λεπτών. Ακόμα, επισήμανε πως το εργαλείο metasploit το έχει ξανά χρησιμοποιήσει όπως και άλλοι χρήστες παραπάνω, κατά την διάρκεια μαθήματος. Συμπερασματικά, φαίνεται να έχει αρκετές γνώσεις πάνω στο κομμάτι της ασφάλειας, άσχετα που δεν κατάφερε να τα ολοκληρώσει με τον καλύτερο δυνατό χρόνο.

Οι χρήστες με περισσότερη εμπειρία και προηγούμενη χρήση των εργαλείων ολοκλήρωσαν τις προκλήσεις γρηγορότερα σε σύγκριση με τους υπόλοιπους. Αντίθετα, οι χρήστες που δεν είχαν προηγούμενη εμπειρία με τα εργαλεία χρειάστηκαν περισσότερο χρόνο, αλλά κατάφεραν να εξοικειωθούν με αυτά και να προχωρήσουν στην επίλυση των προβλημάτων.

Στον παρακάτω πίνακα παρουσιάζεται ο μέσος χρόνος επίλυσης που χρειάστηκαν οι χρήστες για κάθε challenge σε λεπτά βάση των χρόνων επίλυσης των προκλήσεων που αναφέρθηκαν στους παραπάνω πίνακες.

Πίνακας 4 Μέσος χρόνος επίλυσης καθε πόκλησης

Challenge	Μέσος Χρόνος Επίλυσης (λεπτά)
1	48.8
2	43.4
3	64.6

Στον παραπάνω πίνακα (Πίνακας 4) παρατηρούμε ότι η 3η πρόσκληση ήταν η πιο δύσκολη, καθώς οι χρήστες χρειάστηκαν περισσότερο χρόνο για να την επιλύσουν, σε σύγκριση με τις άλλες δύο προκλήσεις, τα οποία είχαν παρόμοιο μέσο όρο επίλυσης από τους χρήστες.

7. Αξιολόγηση

Σε αυτή την ενότητα θα αναλυθούν οι απαντήσεις των χρηστών στα ερωτήματα που τους τέθηκαν μετά την επιτυχής ολοκλήρωση των προκλήσεων. Το ερωτηματολόγιο δημιουργήθηκε χωρίς καθοδήγηση από άλλο υπάρχον ερωτηματολόγιο. Οι ερωτήσεις διατυπώθηκαν έτσι ώστε να συλλεχθούν πληροφορίες για τις γνώσεις που απέκτησαν οι χρήστες, τα προβλήματα που αντιμετώπισαν και τη γενική τους ικανοποίηση από τα challenges. Οι χρήστες κλήθηκαν να αξιολογήσουν την εμπειρία τους κατά τη διάρκεια των challenges, χρησιμοποιώντας κλίμακα από το 1 έως το 5, όπου το 1 αντιστοιχεί σε αρνητική εμπειρία και το 5 σε υψηλό επίπεδο ικανοποίησης. Οι ερωτήσεις που τέθηκαν, καθώς και οι απαντήσεις τους, παρουσιάζονται παρακάτω.

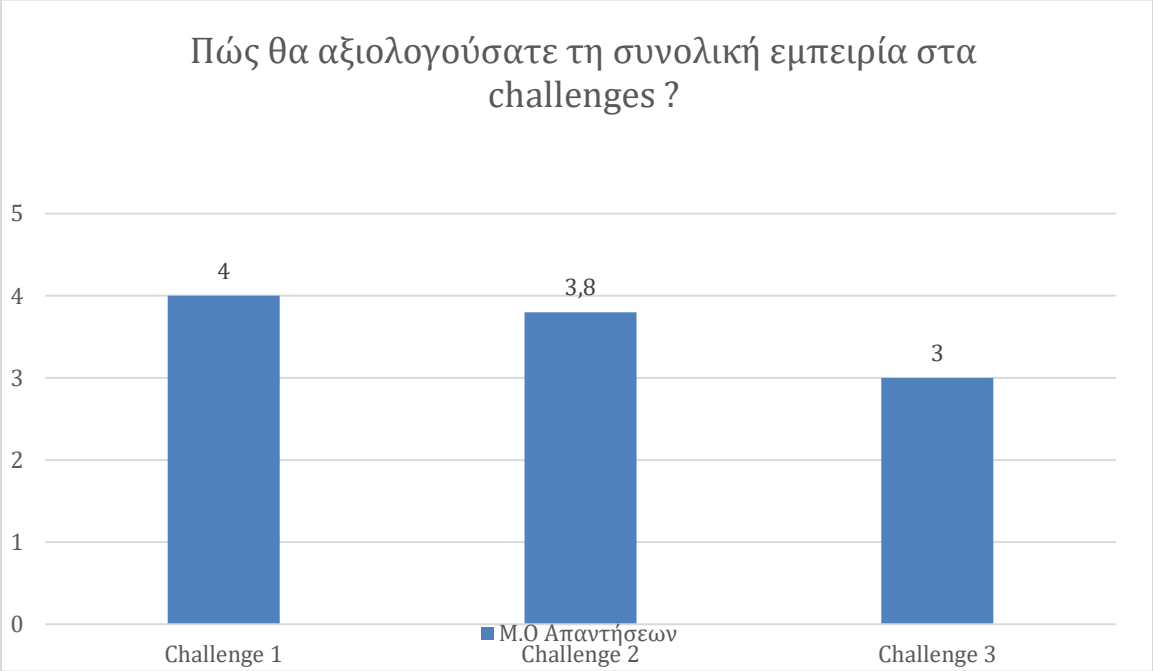
7.1 Πώς θα αξιολογούσατε τη συνολική εμπειρία στα challenges (σε κλίμακα από 1 έως 5);

Στον Πίνακας 5 παρουσιάζονται οι απαντήσεις των χρηστών σχετικά με τη συνολική εμπειρία τους σε κάθε πρόκληση. Στο πρώτο challenge, οι χρήστες δήλωσαν γενικά ικανοποιημένοι από την εμπειρία τους. Στην δεύτερη πρόκληση, παρατηρείται επίσης θετική αποδοχή, με εξαίρεση τον User 2, ο οποίος αξιολόγησε χαμηλά την εμπειρία λόγω δυσκολιών στη χρήση του εργαλείου Wolfram. Στην τελευταία πρόκληση, η πλειοψηφία των χρηστών απάντησε ότι είχε σχετική ικανοποιητική εμπειρία. Στην Εικόνα 18 παρουσιάζεται η συνολική βαθμολογία που έλαβαν τα

challenges αναφορικά με την εμπειρία των χρηστών, βάσει των απαντήσεών τους. Η 1η πρόκληση συγκέντρωσε την υψηλότερη βαθμολογία, ενώ η 3η πρόκληση την χαμηλότερη, υποδεικνύοντας ότι η πρόκληση αυτή ήταν πιο απαιτητική, ειδικά για τους χρήστες που δεν είχαν εμπειρία.

Πίνακας 5 Απαντήσεις των χρηστών στην πρώτη ερώτηση

	Challenge 1	Challenge 2	Challenge 3
User 1	4	4	4
User 2	4	2	1
User 3	3	3	3
User 4	5	5	4
User 5	4	5	3



Εικόνα 18 Οι Απαντήσεις των χρηστών στην 1η ερώτηση κατά Μ.Ο

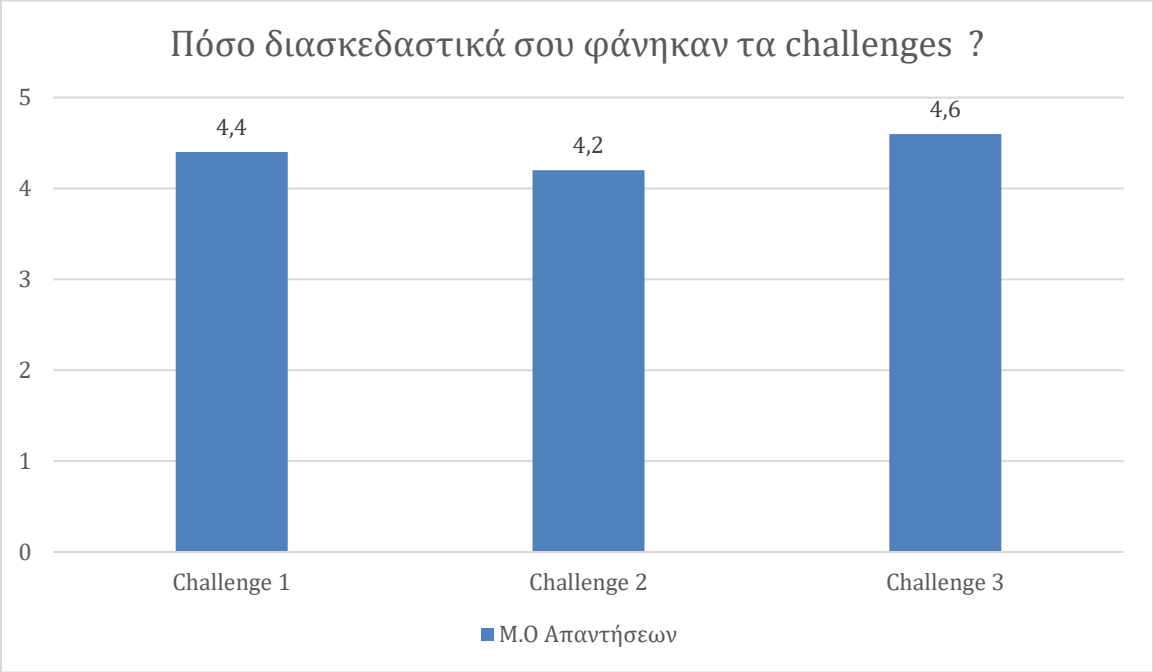
7.2 Πόσο διασκεδαστικά σου φάνηκαν τα challenges (σε κλίμακα από 1 έως 5);

Οι πέντε χρήστες που συμμετείχαν στην πρόκληση φαίνεται να το απόλαυσαν αρκετά, όπως προκύπτει από τις θετικές βαθμολογίες που έδωσαν στις διάφορες προκλήσεις οι οποίες παρουσιάζονται στον Πίνακας 6. Όλοι οι χρήστες ανέφεραν ότι οι προκλήσεις ήταν ενδιαφέροντες και διασκεδαστικές, με μερικούς να εκφράζουν προτιμήσεις για συγκεκριμένα σενάρια ή εργαλεία. Γενικότερα, η εμπειρία τους ήταν θετική και καταγράφηκαν θετικά σχόλια, υποδεικνύοντας ότι το σύνολο των προκλήσεων κατάφερε να κρατήσει το ενδιαφέρον τους και να προσφέρει μια ευχάριστη εμπειρία. Στην Εικόνα 19, αντικατοπτρίζει τον μέσο όρο στις απαντήσεις που έδωσαν οι χρήστες στην προαναφερθέντα ερώτηση. Συμπερασματικά, η 3η

πρόκληση φαίνεται να αποτελεί η πιο διασκεδαστική πρόκληση σε σχέση με τα άλλα δυο, καθώς αποτελεί ένα πραγματικό σενάριο επίθεσης.

Πίνακας 6 Απαντήσεις των χρηστών στην 2η ερώτηση

	Challenge 1	Challenge 2	Challenge 3
User 1	4	5	5
User 2	5	3	5
User 3	3	4	4
User 4	5	5	4
User 5	5	4	5



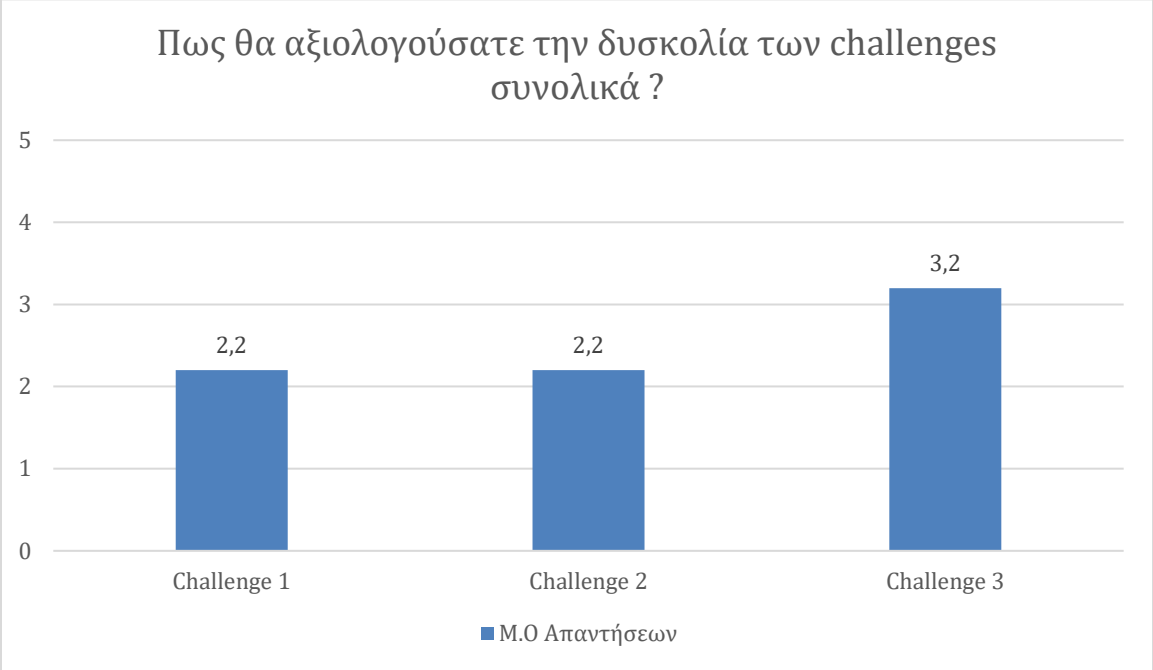
Εικόνα 19 Οι Απαντήσεις των χρηστών στην 2η ερώτηση κατά Μ.Ο

7.3 Πως θα αξιολογούσατε την δυσκολία των challenges συνολικά (σε κλίμακα από 1 έως 5);

Στον Πίνακας 7 διακρίνονται οι απαντήσεις των χρηστών στην ερώτηση σχετικά με την δυσκολία των προκλήσεων. Γενικά, οι χρήστες φαίνεται να είχαν διαφορετικές αντιδράσεις ανάλογα με τις γνώσεις τους και την εμπειρία τους με τα εργαλεία και τους αλγόριθμους. Ορισμένοι χρησιμοποίησαν τα εργαλεία πιο άνετα, αξιολογώντας την 1η και 2η πρόκληση ως πιο εύκολες, ενώ η 3η πρόκληση τους φάνηκε πιο απαιτητική. Αντίθετα, άλλοι χρήστες, οι οποίοι είχαν λιγότερες γνώσεις ή δεν ήταν εξοικειωμένοι με τα εργαλεία, βρήκαν όλες τις προκλήσεις δύσκολες. Εν κατακλείδι, στο Εικόνα 20 παρουσιάζεται η 1η πρόκληση να είναι παρόμοιας δυσκολίας με αυτή της 2ης πρόκλησης ενώ αυτή της 3ης πρόκλησης να είναι κατά μια μονάδα δυσκολότερη σε σχέση με τις άλλες δύο, για τους χρήστες.

Πίνακας 7 Απαντήσεις των χρηστών στην 3η ερώτηση

	Challenge 1	Challenge 2	Challenge 3
User 1	3	2	3
User 2	2	4	5
User 3	4	3	4
User 4	1	1	2
User 5	1	1	2



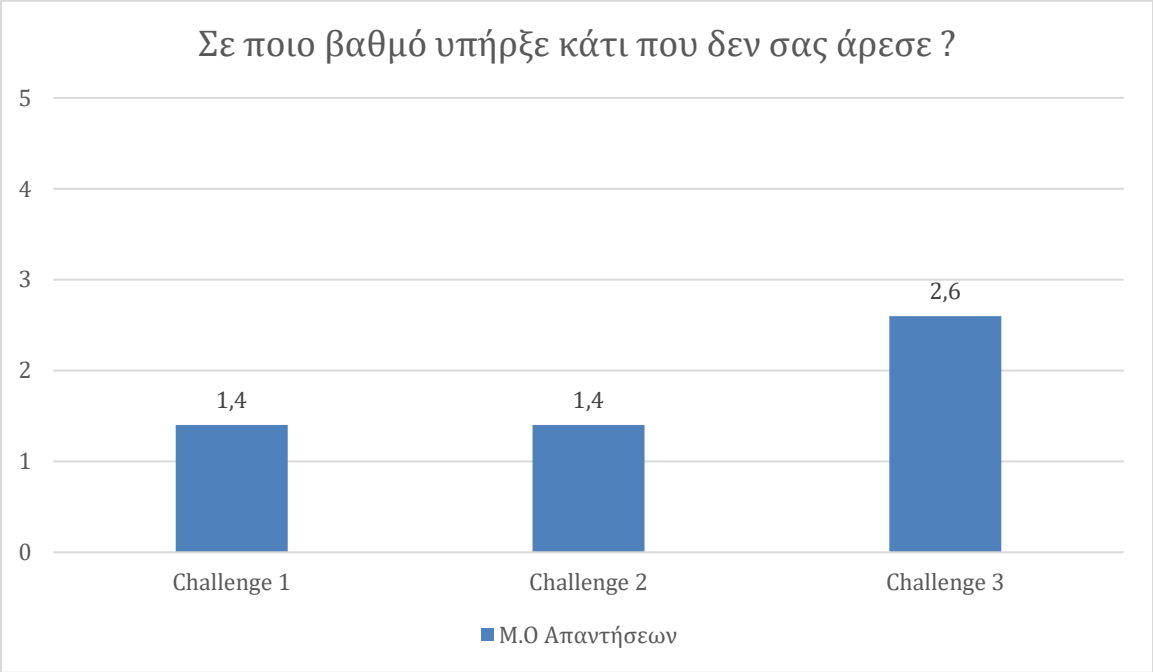
Εικόνα 20 Απαντήσεις των χρηστών στην 3η ερώτηση κατά Μ.Ο

7.4 Σε ποιο βαθμό υπήρξε κάτι που δεν σας ικανοποίησε (σε κλίμακα από 1 έως 5);

Ο βαθμός μη ικανοποίησης των παικτών αναδεικνύεται στον Πίνακας 8. Μέσα από τις απαντήσεις τους φαίνεται ότι δεν τους δυσαρέστησε κάτι. Απεναντίας, οι User 2 και User 3, οπου έχουν και τις λιγότερες γνώσεις σε σχέση με τους υπόλοιπους, φαίνεται στην 3η προκληση να τους φάνηκε αρκετά πιο δυσνόητο συγκριτικά με τις άλλες, για αυτό και έβαλαν χαμηλή βαθμολογία. Τέλος, στο Εικόνα 21 ομοίως οι προκλήσεις 1 και 2 έχουν τον μέσο όρο στις απαντήσεις που έδωσαν οι χρήστες, ενώ η 3η πρόκληση φαίνεται να δυσαρέστησε τους χρήστες περισσότερο.

Πίνακας 8 Απαντήσεις των χρηστών στην 4η ερώτηση

	Challenge 1	Challenge 2	Challenge 3
User 1	2	1	2
User 2	1	2	4
User 3	2	2	3
User 4	1	1	2
User 5	1	1	2



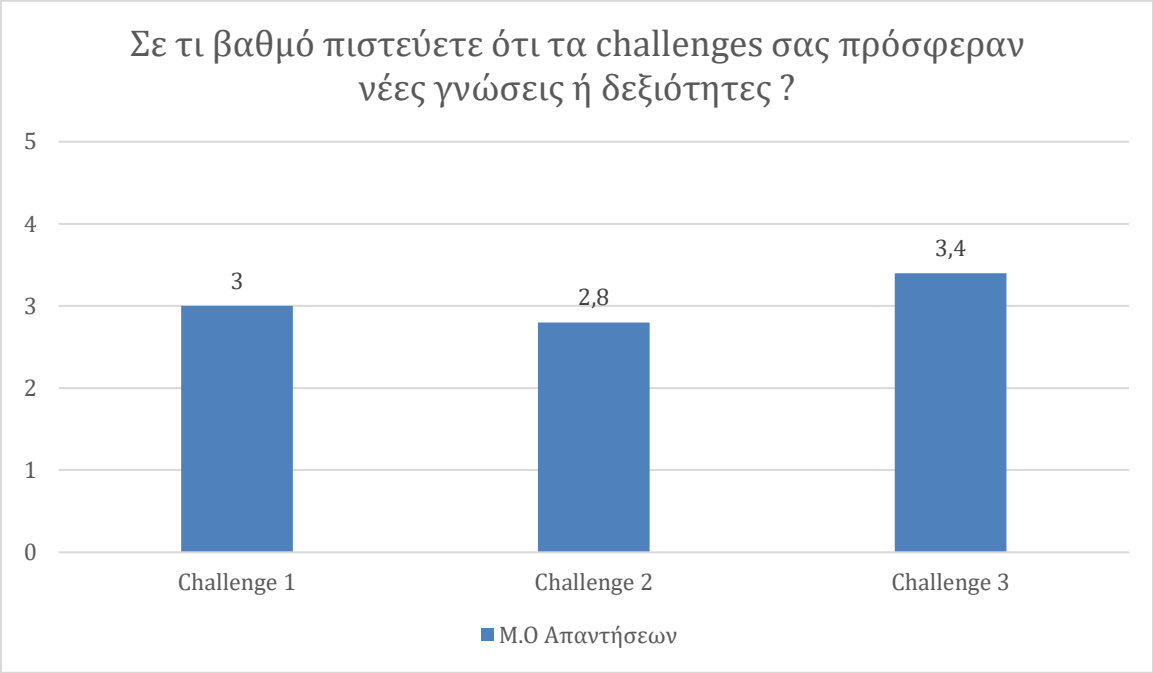
Εικόνα 21 Απαντήσεις των χρηστών στην 4η ερώτηση κατά Μ.Ο

7.5 Σε τι βαθμό πιστεύετε ότι τα challenges σας πρόσφεραν νέες γνώσεις ή δεξιότητες (σε κλίμακα από 1 έως 5);

Το συμπέρασμα σχετικά με το πόσο οι προκλήσεις προσέφεραν νέες γνώσεις και δεξιότητες στους χρήστες αναλύεται στον Πίνακας 9, με βάση τις απαντήσεις τους. Επιπρόσθετα, ο User 2 και User 3, οι οποίοι, όπως φάνηκε σε προηγούμενη ερώτηση, αντιμετώπισαν μεγαλύτερη δυσκολία, αποκόμισαν τις περισσότερες νέες γνώσεις σε σχέση με τους υπόλοιπους χρήστες. ο User 1 βρήκε ότι η 1η πρόκληση του παρείχε νέες γνώσεις, ενώ οι υπόλοιπες δύο απλά του υπενθύμισαν παλαιότερες. Οι Users 4 και 5 αξιολόγησαν τις προκλήσεις 1 και 3 ως ευκαιρίες για την ανανέωση γνώσεων σχετικά με διάφορες εντολές, ενώ η 2η πρόκληση δεν φαίνεται να τους παρείχε νέες γνώσεις. Κλείνοντας, το Εικόνα 22 απεικονίζει τον μέσο όρο στις απαντήσεις των χρηστών στο παραπάνω ερώτημα. Το συμπέρασμα που προκύπτει, είναι πως η 3η πρόκληση πρόσφερε σε μεγαλύτερο βαθμό γνώσεις/δεξιότητες συγκριτικά με τις υπόλοιπες δυο προκλήσεις.

Πίνακας 9 Απαντήσεις των χρηστών στην 5η ερώτηση

	Challenge 1	Challenge 2	Challenge 3
User 1	4	3	3
User 2	3	5	5
User 3	4	3	5
User 4	2	2	2
User 5	2	1	2



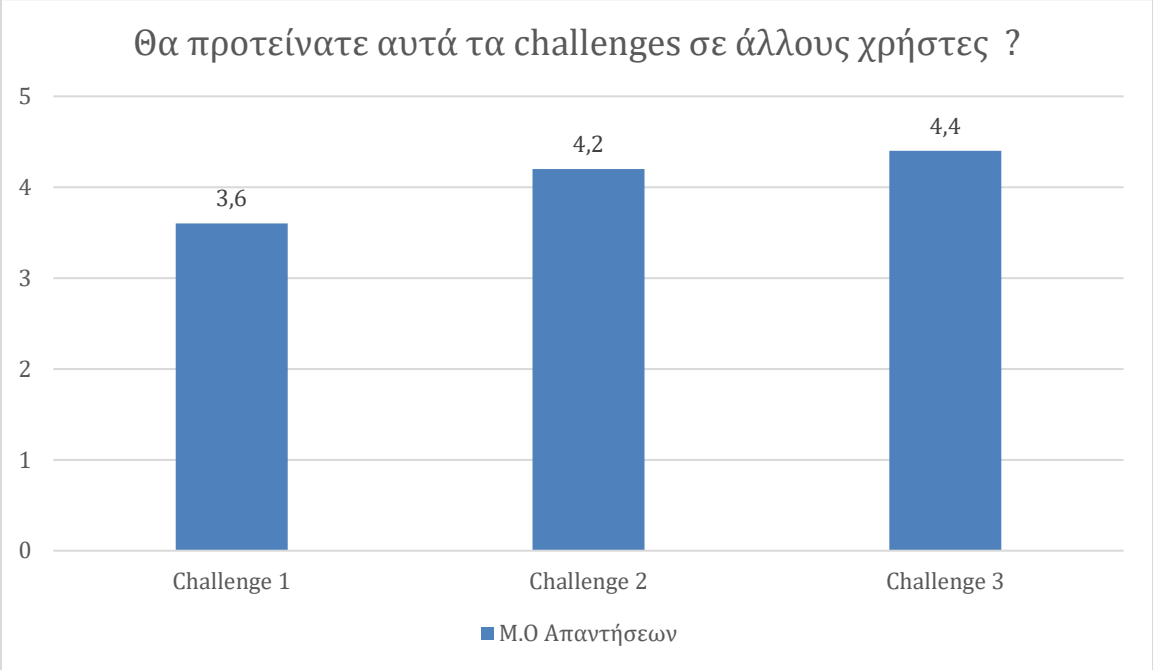
Εικόνα 22 Απαντήσεις των χρηστών στην 5η ερώτηση κατά Μ.Ο

7.6 Θα προτείνατε αυτά τα challenges σε άλλους χρήστες (σε κλίμακα από 1 έως 5);

Παρακάτω παρατίθεται ο Πίνακας 10 όπου παρουσιάζονται οι απαντήσεις των χρηστών στην τελευταία ερώτηση. Ο χρήστης που έδωσε τη χαμηλότερη βαθμολογία είναι ο User 4, ο οποίος αξιολόγησε τις προκλήσεις 1 και 2 ως μέτριας προτίμησης, ενώ την 3η πρόκληση την θεώρησε πιο προτιμητέα και θα την συνιστούσε περισσότερο σε σχέση με τις υπόλοιπες. Αυτή η τάση γίνεται εμφανής και από τις απαντήσεις των υπόλοιπων χρηστών, όπως φαίνεται στον Πίνακας 10. Συμπερασματικά, στο Εικόνα 23 όπου οι χρήστες απάντησαν με αρκετά υψηλό βαθμό, φαίνεται από τον μέσο όρο να αποτελούν ένα χρήσιμο εργαλείο για την εκπαίδευση των χρηστών πάνω στην κυβερνοασφάλεια.

Πίνακας 10 Απαντήσεις των χρηστών στην 6η ερώτηση

	Challenge 1	Challenge 2	Challenge 3
User 1	4	5	5
User 2	4	5	5
User 3	4	4	4
User 4	3	3	4
User 5	3	4	4



Εικόνα 23 Απαντήσεις των χρηστών στην 5η ερώτηση κατά Μ.Ο

Από τις απαντήσεις των χρηστών προέκυψε ότι η 3η πρόκληση θεωρήθηκε η πιο δύσκολη, αλλά και η πιο εποικοδομητική, καθώς προσέφερε τη μεγαλύτερη ανάπτυξη γνώσεων. Η ανάγκη για μετάβαση από το ένα container στο άλλο αύξησε την πολυπλοκότητα της, καθιστώντας τη πιο απαιτητική. Επιπλέον, οι χρήστες οι οποίοι δεν είχαν γνώσεις φαίνεται να τους βοήθησαν οι προκλήσεις να αναπτύξουν νέες δεξιότητες πάνω στα συγκεκριμένα εργαλεία. Αντίθετα, οι χρήστες που είχαν γνώση των εργαλείων φάνηκε να διασκεδάζουν με τις προκλήσεις και ενίσχυσαν τις ικανότητές τους, μαθαίνοντας νέα στοιχεία για αυτά. Η πλειοψηφία των χρηστών φαίνεται να συνιστά τις συγκεκριμένες προκλήσεις σε νέους χρήστες ως έναν αποτελεσματικό τρόπο εκπαίδευσης. Τέλος, ακόμα και για όσους βρήκαν τις προκλήσεις πιο δύσκολες, η συνολική ικανοποίηση παρέμεινε υψηλή.

8. Συμπεράσματα

Συμπερασματικά, η παρούσα έρευνα εξετάζει την εφικτότητα υλοποίησης ενός CTF βασισμένου αποκλειστικά σε docker containers. Από τα αποτελέσματα προκύπτει ότι το εγχείρημα αυτό είναι

εφικτό, καθώς τα docker containers χρησιμοποιήθηκαν με επιτυχία για τη δημιουργία των challenges. Επιπλέον, τα challenges, σύμφωνα με τα διαγράμματα και τα δεδομένα που αναλύθηκαν, φαίνεται να προσφέρουν νέες γνώσεις σε χρήστες που δεν είχαν προηγούμενη εμπειρία με τα εργαλεία και τις διαδικασίες του κυβερνοασφάλειας. Ο στόχος ανάπτυξης νέων δεξιοτήτων και εκμάθησης εργαλείων στον τομέα της κυβερνοασφάλειας επιτεύχθηκε με θετικό αντίκτυπο.

9. Μελλοντικά πλάνα

Για το υπάρχον project, υπάρχουν διάφορα πλάνα που στοχεύουν στην αναβάθμιση του CTF και στην επέκτασή του. Αρχικά, η ενσωμάτωση δυνατότητας διαχείρισης πολλαπλών χρηστών και η δημιουργία νέων προκλήσεων σε περισσότερους τομείς της κυβερνοασφάλειας θα διευρύνει τους γνωστικούς ορίζοντες των χρηστών. Με αυτόν τον τρόπο, οι χρήστες θα εκπαιδευτούν σε ένα ευρύτερο φάσμα θεμάτων, ενισχύοντας τις δεξιότητές τους και μειώνοντας την πιθανότητα να υποπέσουν σε λάθη. Επίσης, η δυνατότητα δημιουργίας ομάδων χρηστών είναι ένα χαρακτηριστικό που θα ενισχύσει τη συνεργατική εργασία, προσφέροντας έναν ακόμα πιο αποτελεσματικό τρόπο εκπαίδευσης. Τέλος, ένα χρήσιμο εργαλείο που προσφέρει το CTFd framework είναι τα APIs, τα οποία παρέχουν τη δυνατότητα ανάπτυξης λειτουργιών, όπως η επιστροφή πληροφοριών χρηστών μέσω ενός ενεργού access token. Αυτό καθιστά δυνατή, τη διαχείριση και παρακολούθηση της συμμετοχής των χρηστών στον διαγωνσμό, προσφέροντας ευελιξία και επεκτασιμότητα για μελλοντικές αναβαθμίσεις του συστήματος.

References

[1] Z. C. Schreuders and E. Butterfield, “Gamification for Teaching and Learning Computer Security in Higher Education,” in *2016 USENIX Workshop on Advances in Security Education (ASE 16)*, Austin, TX: USENIX Association, Aug. 2016. [Online]. Available: https://www.usenix.org/conference/ase16/workshop-program/presentation/schreuders

[2] R. Al-Azawi, F. Al-Faliti, and M. Al-Blushi, “Educational Gamification Vs. Game Based Learning: Comparative Study,” *International Journal of Innovation, Management and Technology*, pp. 131–136, 2016, doi: 10.18178/ijimt.2016.7.4.659.

[3] M. Beltran, M. Calvo, and S. Gonzalez, “Experiences Using Capture The Flag Competitions to Introduce Gamification in Undergraduate Computer Security Labs,” in *2018 International Conference on Computational Science and Computational Intelligence (CSCI)*, IEEE, Dec. 2018, pp. 574–579. doi: 10.1109/CSCI46756.2018.00116.

[4] A. Mansurov, “A CTF-Based Approach in Information Security Education: An Extracurricular Activity in Teaching Students at Altai State University, Russia,” *Mod Appl Sci*, vol. 10, no. 11, p. 159, Aug. 2016, doi: 10.5539/mas.v10n11p159.

[5] A. S. Raj, B. Alangot, S. Prabhu, and K. Achuthan, “Scalable and Lightweight CTF Infrastructures Using Application Containers (Pre-recorded Presentation),” in *2016 USENIX Workshop on Advances in Security Education (ASE 16)*, Austin, TX: USENIX Association, Aug. 2016. [Online]. Available: https://www.usenix.org/conference/ase16/workshop-program/presentation/raj

[6] S. Karagiannis, E. Maragkos-Belmpas, and E. Magkos, “An Analysis and Evaluation of Open Source Capture the Flag Platforms as Cybersecurity e-Learning Tools,” 2020, pp. 61–77. doi: 10.1007/978-3-030-59291-2_5.

[7] K. Chung, “Live Lesson: Lowering the Barriers to Capture The Flag Administration and Participation,” in *2017 USENIX Workshop on Advances in Security Education (ASE 17)*, Vancouver, BC: USENIX Association, Aug. 2017. [Online]. Available: https://www.usenix.org/conference/ase17/workshop-program/presentation/chung

[8] S. Karagiannis and E. Magkos, “Adapting CTF challenges into virtual cybersecurity learning environments,” *Information & Computer Security*, vol. 29, no. 1, pp. 105–132, May 2021, doi: 10.1108/ICS-04-2019-0050.

[9] Z. Kaplan, N. Zhang, and S. V. Cole, “A Capture The Flag (CTF) Platform and Exercises for an Intro to Computer Security Class,” in *Proceedings of the 27th ACM Conference on on Innovation and Technology in Computer Science Education Vol. 2*, New York, NY, USA: ACM, Jul. 2022, pp. 597–598. doi: 10.1145/3502717.3532153.

[10] K. Zhang, S. Wuthier, K. Yoon, and S.-Y. Chang, “Designing and Using Capture The Flag for Coordination and Interaction in Engineering Education,” in *2022 IEEE Global Engineering Education Conference (EDUCON)*, IEEE, Mar. 2022, pp. 1555–1560. doi: 10.1109/EDUCON52537.2022.9766724.

Appendix A

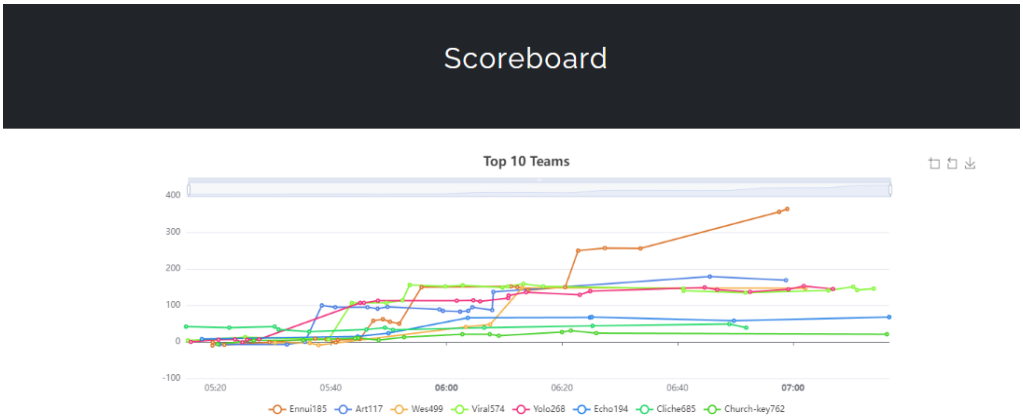
CTFd Framework

Στο Εικόνα 24 αποτυπώνεται το landing page το οποίο παρουσιάζεται στους χρήστες μετά την χρήση του url στο web browser. Το landing page παρέχει στους χρήστες την δυνατότητα επιλογής υποσελίδας μέσα από το navigation bar, οι οποίες είναι (users, scoreboard, challenges, register και login). Τέλος, στο landing page υπάρχουν οι επιλογές register και login στα δεξιά του selection bar όπου έχουν ως σκοπό την εγγραφή και είσοδο του χρήστη μέσα στην εφαρμογή. Για να είναι πιο αποτελεσματική και σωστή αυτή η διαδικασία έχει γίνει σύνδεση με μια βάση δεδομένων μέσα από το SQL alchemy που παρέχει η python.



Εικόνα 24 Αρχική Εικόνα CTFd

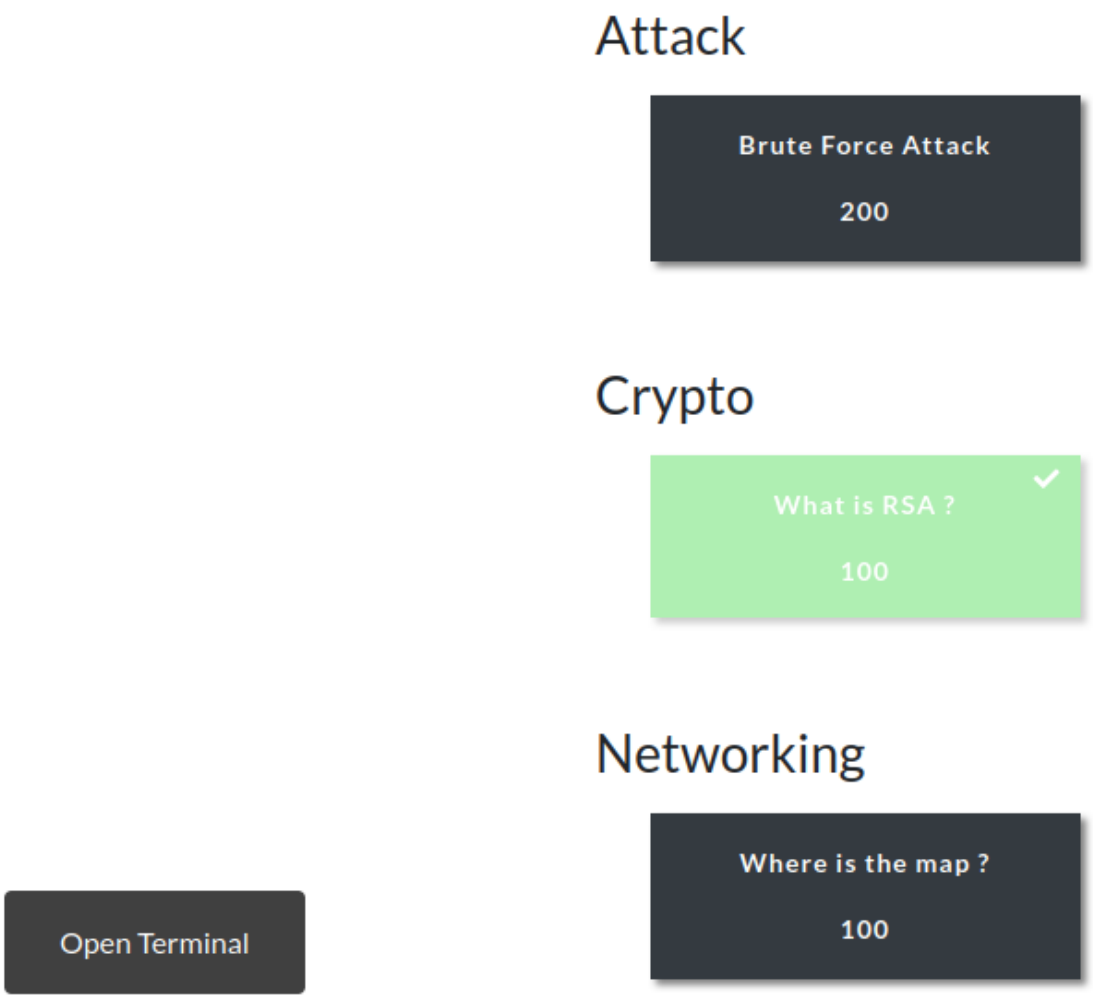
Επιπλέον, στην Εικόνα 25 εμφανίζεται το Scoreboard το οποίο είναι η συνολική βαθμολογία όλων των παικτών καθώς και ένα γράφημα το οποίο αναλύει τους πόντους κάθε ομάδας ή κάθε παίκτη ανάλογα με το πως έχουν διαμορφωθεί. Η συγκεκριμένη εικόνα αποτελεί μέρος του demo του CTFd.



Place	Team	Score
1	Ennui185	364
2	Art117	169
3	Wes499	147
4	Viral574	146
5	Yolo268	145
6	Echo194	68
7	Cliche685	39
8	Church-key762	21

Εικόνα 25 Πίνακας αποτελεσμάτων

Τέλος, στην Εικόνα 26 φαίνεται το περιεχόμενο της καρτέλας challenges οπού εκεί βρίσκονται όλες οι προκλήσεις τα οποία πρέπει να φέρουν εις πέρας οι χρήστες. Η παρακάτω φωτογραφία δεν αποτελεί μέρος του demo του CTFd. Όπως φαίνεται υπάρχουν 3 προκλήσεις τις οποίες μπορεί να το τροποποιήσει ο admin. Στην περίπτωση αυτή παρουσιάζονται 3 κατηγορίες (Attack, Crypto και Networking) και σε κάθε μια από αυτή υπάρχει και μία πρόκληση.



Εικόνα 26 Κεντρική σελίδα προκλήσεων

Στην Εικόνα 27 που παρουσιάζεται παρακάτω αποτελεί την υποσέλιδα statistics στο navigation bar. Οι πληροφορίες που μπορεί ο διαχειριστής να παρατηρήσει είναι αρκετές. Μερικές από αυτές αποτελούν σημαντικές πληροφορίες όσον αφορά την πρόοδο του χρήστη. Αναλυτικότερα, στο πρώτο διάγραμμα απεικονίζονται πληροφορίες σχετικά με τις προκλήσεις, καθώς και με τους χρήστες(π.χ. Πόσοι έχουν κάνει εγγραφή, πόσοι είναι οι διαθέσιμοι πόντοι). Στο δεύτερο διάγραμμα εμφανίζονται οι πόντοι των χρηστών. Ενώ στο τρίτο διάγραμμα αναγράφεται το ποσοστό επιτυχίας για κάθε μια πρόκληση. Τέλος, στις

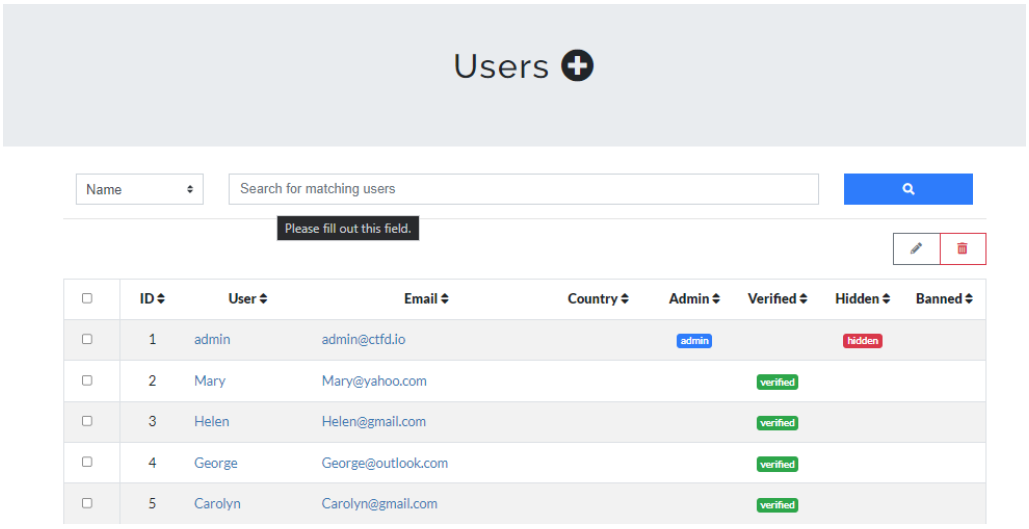
πίτες η αριστερή παρουσιάζει τις λανθασμένες και ορθές απαντήσεις από τους χρήστες, ενώ στην δεξιά πίτα φαίνεται πόσες προκλήσεις έχει η κάθε μια κατηγορία.



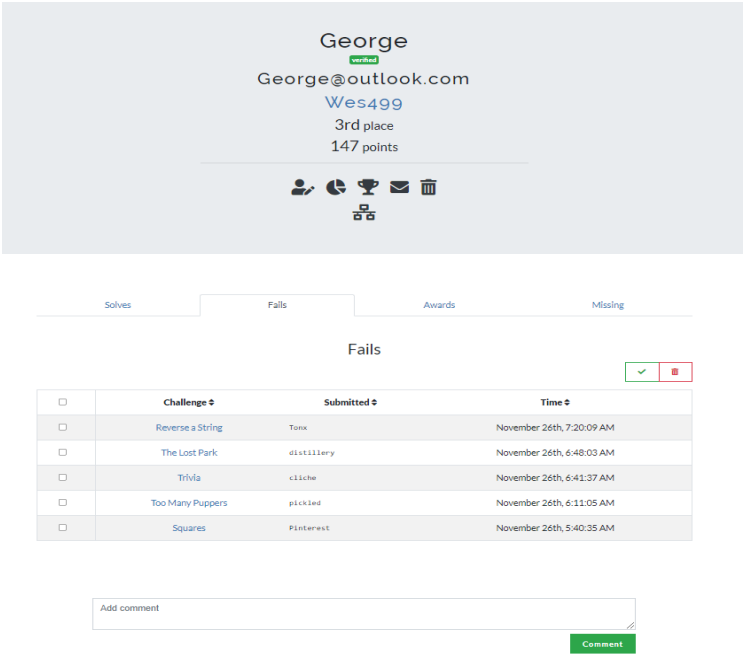
Εικόνα 27 Υποσελίδα στατιστικών

Η Εικόνα 28 είναι μια λίστα όλων των εγγεγραμμένων χρηστών στην εφαρμογή. Επιπλέον, παρέχεται η δυνατότητα στον διαχειριστή να ψάξει για κάποιον συγκεκριμένο χρήστη όπως φαίνεται στην Εικόνα 29 εάν το επιθυμεί, καθώς και οι επιλογές της διαγράφης και της επεξεργασίας (κάδος-μολύβι) κάποιου χρήστη. Συμπληρωματικά, υπάρχει και η

δυνατότητα από τον διαχειριστή να ενημερωθεί για την δραστηριότητα όποιου χρήστη επιθυμεί, πατώντας πάνω στο όνομα του μέσα από την λίστα.

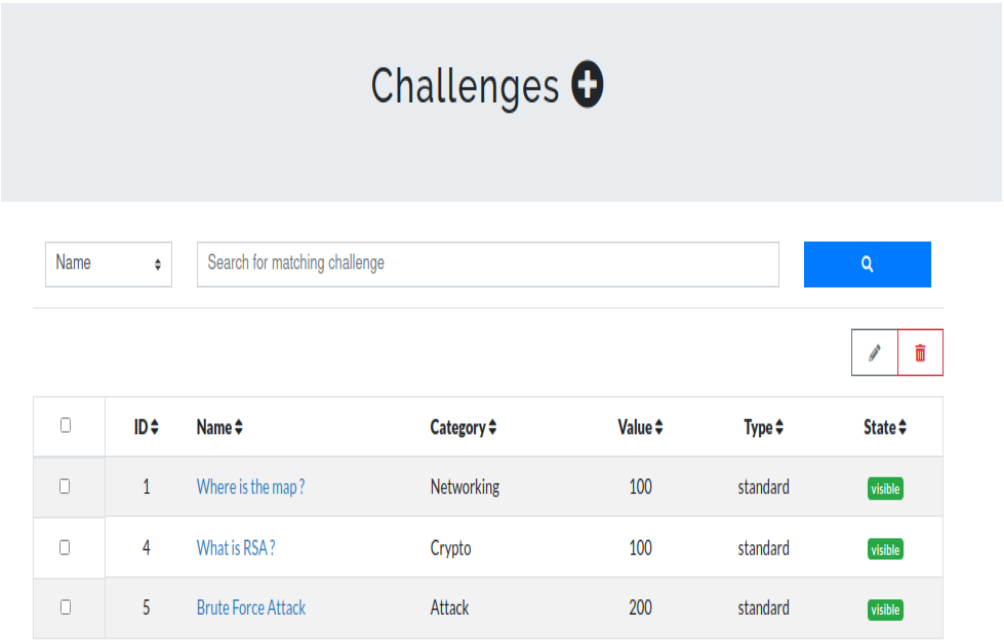


Εικόνα 28 Λίστα παικτών απο το πανελ του διαχειριστή



Εικόνα 29 Πληροφορία για έναν συγκεκριμένο χρήστη

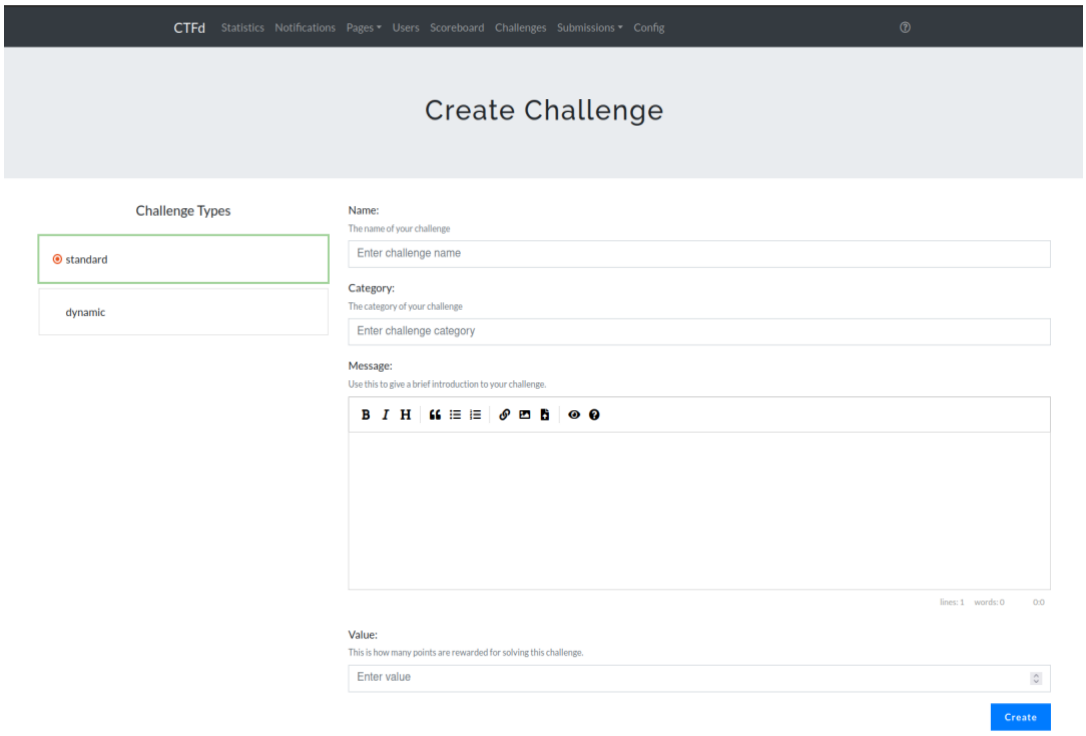
Στην Εικόνα 30 ο διαχειριστής μπορεί να ενημερωθεί για τις διάφορες πληροφορίες που διέπουν την προόκληση. Για παράδειγμα εάν είναι ορατή για τους χρήστες καθώς επίσης και τον τύπο του. Ακόμα, μπορεί να αντλήσει στοιχεία για το είδος της κατηγορίας αλλά και για τους πόντους που θα διεκδικήσουν εφόσον ολοκληρωθεί η πρόκληση με επιτυχία από τους χρήστες.



ID	Name	Category	Value	Type	State
1	Where is the map?	Networking	100	standard	visible
4	What is RSA?	Crypto	100	standard	visible
5	Brute Force Attack	Attack	200	standard	visible

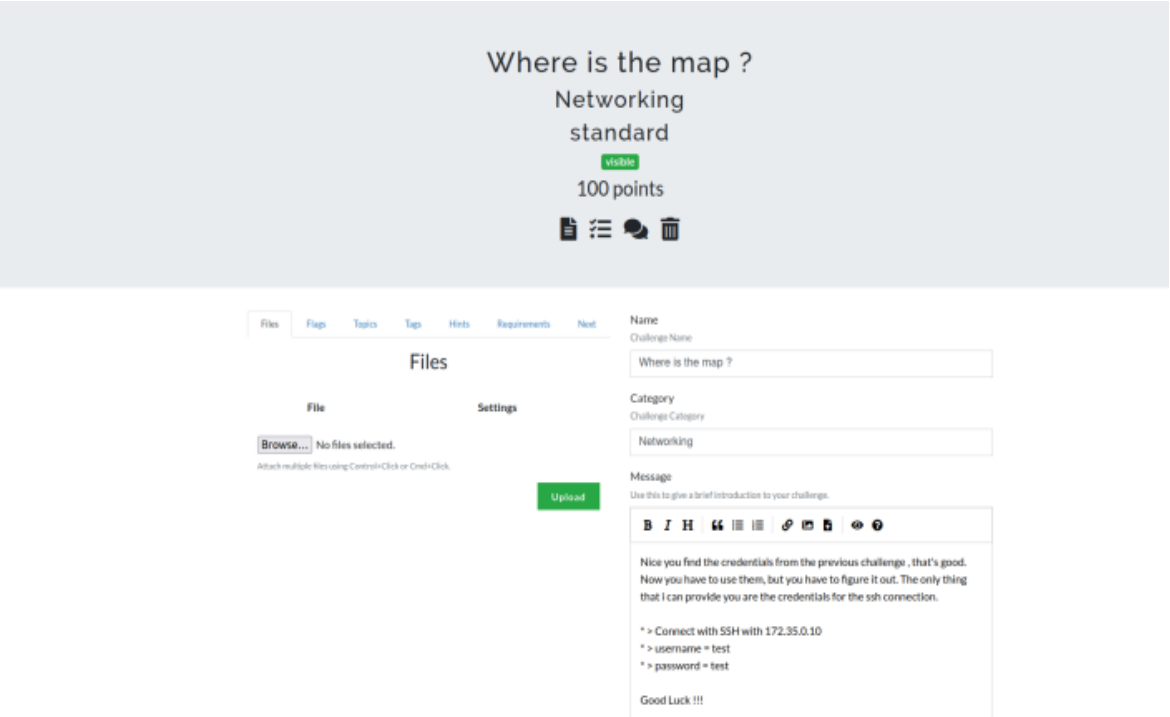
Εικόνα 30 Λίστα προκλήσεων απο το πάνελ του διαχειριστή

Στη συνέχεια, στην Εικόνα 31 που ακολουθεί περιγράφει το είδος της πρόκλησης το οποίο θα δημιουργήσει ο διαχειριστής. Υπάρχουν δυο κατηγορίες, η standard και η dynamic. Η διαφορά αυτών των δυο κατηγοριών είναι ότι στην πρώτη ο χρήστης δίνει μια και μοναδική λύση για την πρόκληση, ενώ στην δεύτερη επιλογή ο χρήστης μπορεί να δώσει παραπάνω από μια λύσεις στην πρόκληση αυτή. Επιπρόσθετα, ο διαχειριστής μπορεί να ορίσει το όνομα, την κατηγορία καθώς και την περιγραφή της εκάστοτε πρόξκλησης που θα δημιουργήσει μαζί με τους πόντους που θα διεκδικούν οι χρήστες μετά την επίλυση της.

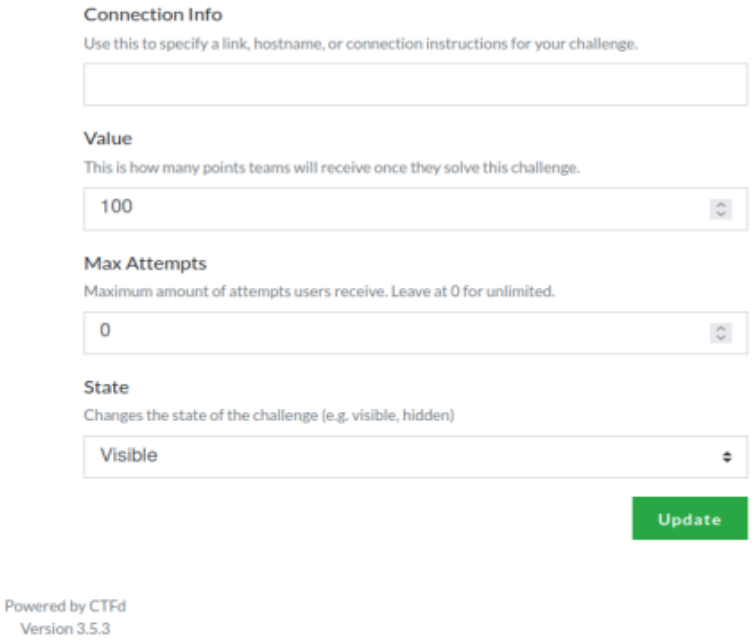


Εικόνα 31 Δημιουργία πρόκλησης μέσα απο το πάνελ του διαχειριστή

Εικόνα 32 - Εικόνα 33 απεικονίζουν την περιγραφή των προκλήσεων που έχει επιλέξει ο διαχειριστής μέσα από την λίστα των ενεργών προκλήσεων (όπως παρουσιάζεται στην Εικόνα 30). Επιπλέον, του δίνεται η δυνατότητα να τροποποιήσει τις επιλογές της προεπιλεγμένης πρόκλησης, όπως αυτή του ονόματος, της κατηγορίας, της περιγραφής και τέλος των πόντων που διεκδικούν οι χρήστες.

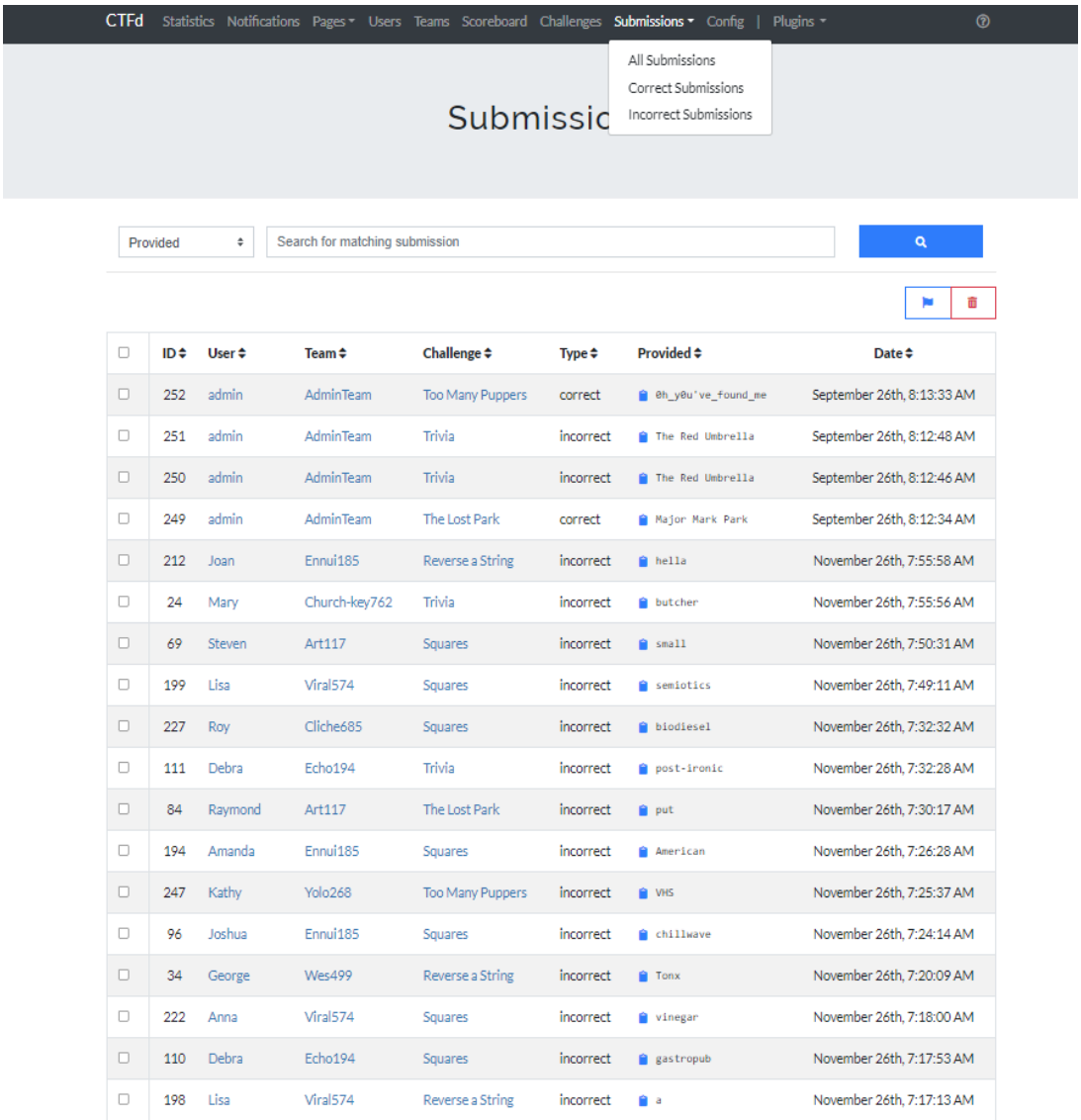


Εικόνα 32 Τροποποίηση των προκλησεων



Εικόνα 33 Τροποποιηση των προκλησεων (2)

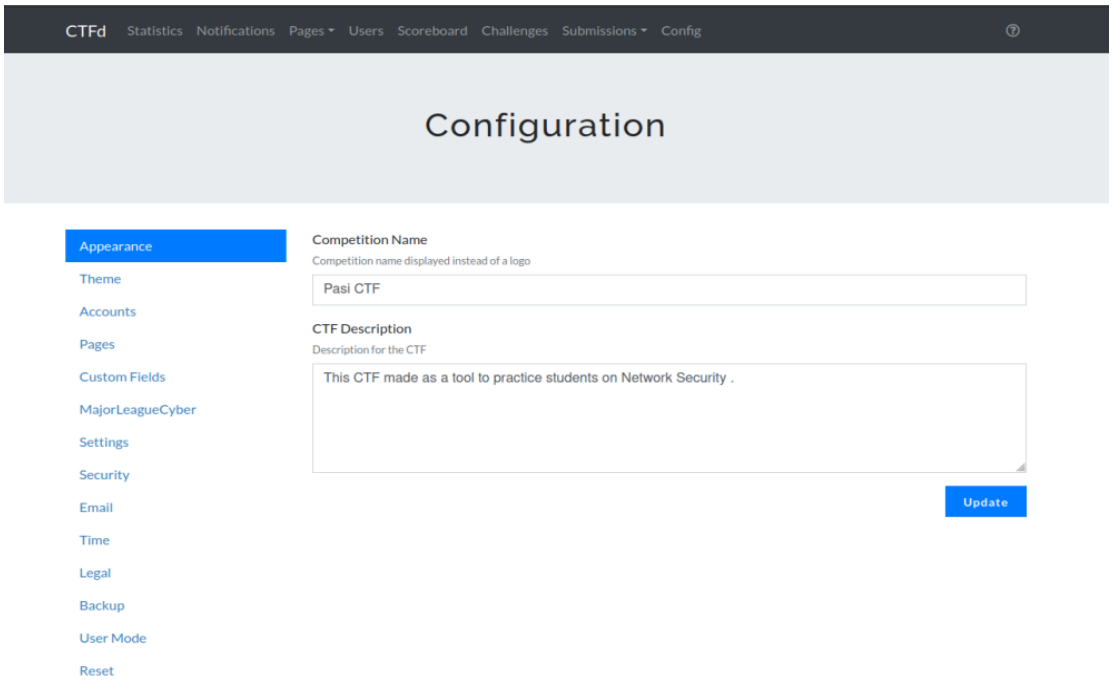
Στη καρτέλα submissions υπάρχουν τρεις επιλογές: all submissions, correct submissions και incorrect submissions. Αυτές οι τρεις επιλογές λειτουργούν σαν φίλτρα και παρέχουν στον administrator έναν τρόπο ώστε να παρακολουθεί την πορεία τον παιχτών. Μέσω της αρχικής επιλογής, η οποία είναι το all submissions, παρατηρεί όλες τις προσπάθειες που έχουν γίνει. Η ημερομηνία και η ώρα αποτελούν κάποιες εξτρά πληροφορίες που παρέχονται στον διαχειριστή. Τέλος, οι επιλογές incorrect και correct submissions φιλτράρουν μεμονωμένα όλα τα submissions που έχουν γίνει από τους χρήστες.



ID	User	Team	Challenge	Type	Provided	Date
252	admin	AdminTeam	Too Many Puppers	correct	0h_y0u've_found_me	September 26th, 8:13:33 AM
251	admin	AdminTeam	Trivia	incorrect	The Red Umbrella	September 26th, 8:12:48 AM
250	admin	AdminTeam	Trivia	incorrect	The Red Umbrella	September 26th, 8:12:46 AM
249	admin	AdminTeam	The Lost Park	correct	Major Mark Park	September 26th, 8:12:34 AM
212	Joan	Ennui185	Reverse a String	incorrect	hella	November 26th, 7:55:58 AM
24	Mary	Church-key762	Trivia	incorrect	butcher	November 26th, 7:55:56 AM
69	Steven	Art117	Squares	incorrect	small	November 26th, 7:50:31 AM
199	Lisa	Viral574	Squares	incorrect	semiotics	November 26th, 7:49:11 AM
227	Roy	Cliche685	Squares	incorrect	biodiesel	November 26th, 7:32:32 AM
111	Debra	Echo194	Trivia	incorrect	post-ironic	November 26th, 7:32:28 AM
84	Raymond	Art117	The Lost Park	incorrect	put	November 26th, 7:30:17 AM
194	Amanda	Ennui185	Squares	incorrect	American	November 26th, 7:26:28 AM
247	Kathy	Yolo268	Too Many Puppers	incorrect	VHS	November 26th, 7:25:37 AM
96	Joshua	Ennui185	Squares	incorrect	chillwave	November 26th, 7:24:14 AM
34	George	Wes499	Reverse a String	incorrect	Tonx	November 26th, 7:20:09 AM
222	Anna	Viral574	Squares	incorrect	vinegar	November 26th, 7:18:00 AM
110	Debra	Echo194	Squares	incorrect	gastropub	November 26th, 7:17:53 AM
198	Lisa	Viral574	Reverse a String	incorrect	a	November 26th, 7:17:13 AM

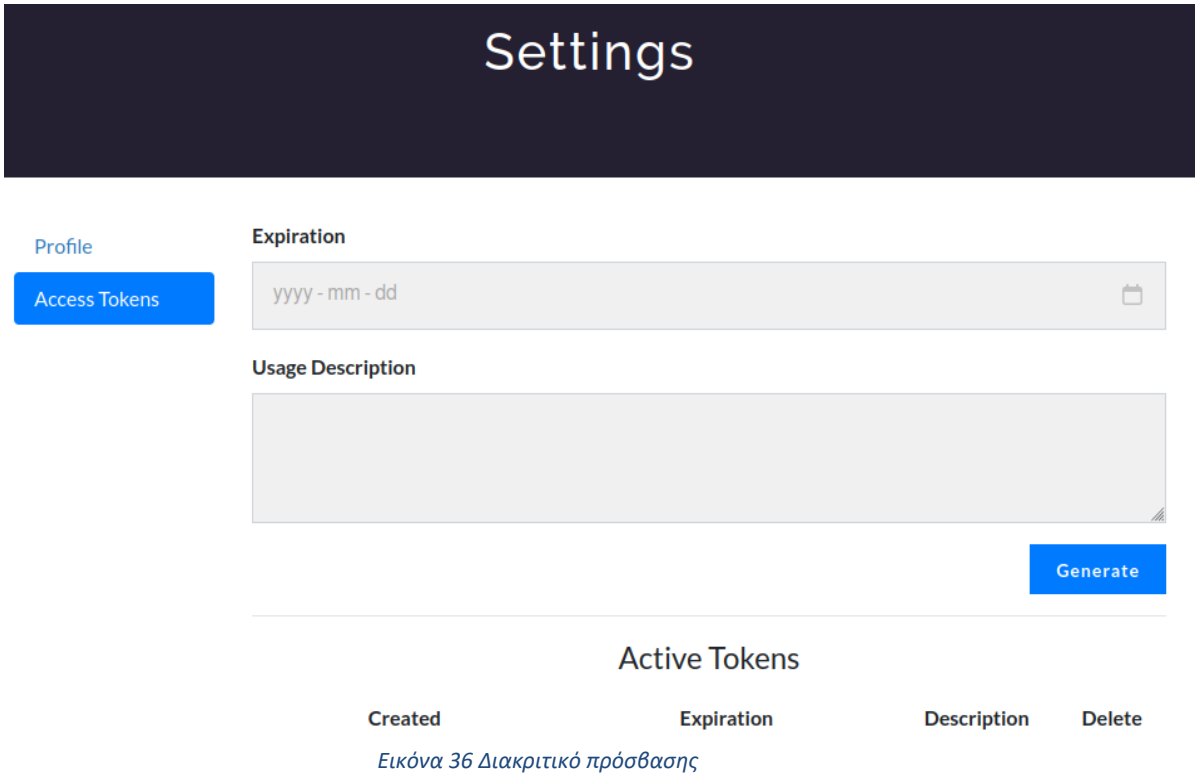
Εικόνα 34 Υποβολές

Ακολουθεί η επόμενη καρτέλα που ονομάζεται configuration και παρέχει την δυνατότητα στον διαχειριστή να μπορεί να κάνει αλλαγές στο όνομα και την περιγραφή της πρόκλησης, καθώς επίσης και μια πληθώρα από επιλογές οι οποίες φαίνονται στα αριστερά με χρώμα μπλε. Μια από αυτές είναι το User Mode το οποίο τροποποιει τον διαγωνισμό από ομαδικό σε ατομικό και το αντίστροφο. Επιπλέον, μέσα από την επιλογή back up δίνεται η δυνατότητα στον διαχειριστή να κρατήσει αρχείο σε περίπτωση που κάτι χαθεί να μπορεί ευκολά να το ανακτήσει.



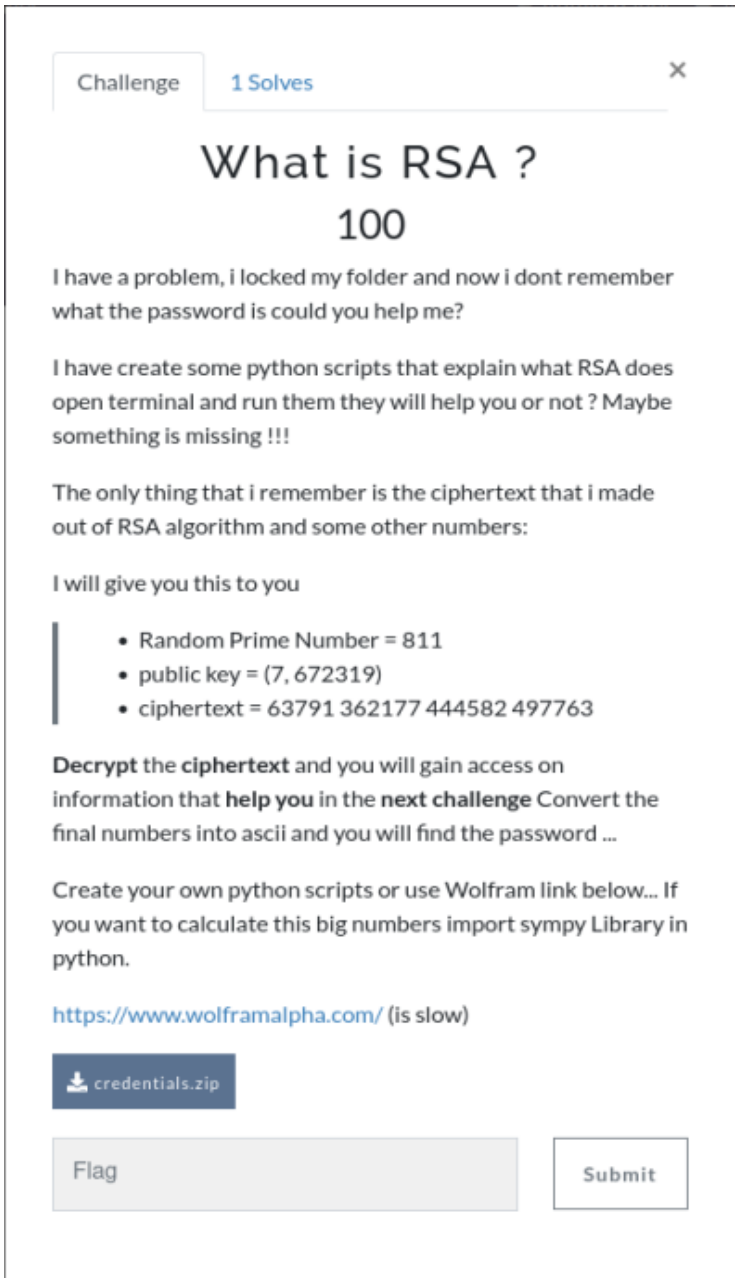
Εικόνα 35 Διαμόρφωση του CTF

Τα access tokens είναι ένας μηχανισμός ο οποίος παρέχει την δυνατότητα διαχείρισης. Αποτελούν τρόπο ταυτοποίησης του χρήστη, με σκοπό το σύστημα να αντιλαμβάνεται εάν είναι εξουσιοδοτημένος. Επίσης, όσο το token του χρήστη βρίσκεται σε ισχύ, του διατίθεται πρόσβαση σε διάφορες λειτουργίες του εκάστοτε framework. Στην περίπτωση αυτή το συγκεκριμένο token, έχει δημιουργηθεί ώστε να επιστρέφει τους χρήστες που έχουν ολοκληρώσει την εγγραφή τους στο CTFd. Ακόμα, τα access tokens δεν πρέπει να δημοσιεύονται καθώς μπορεί να χρησιμοποιηθούν για κακόβουλους σκοπούς.

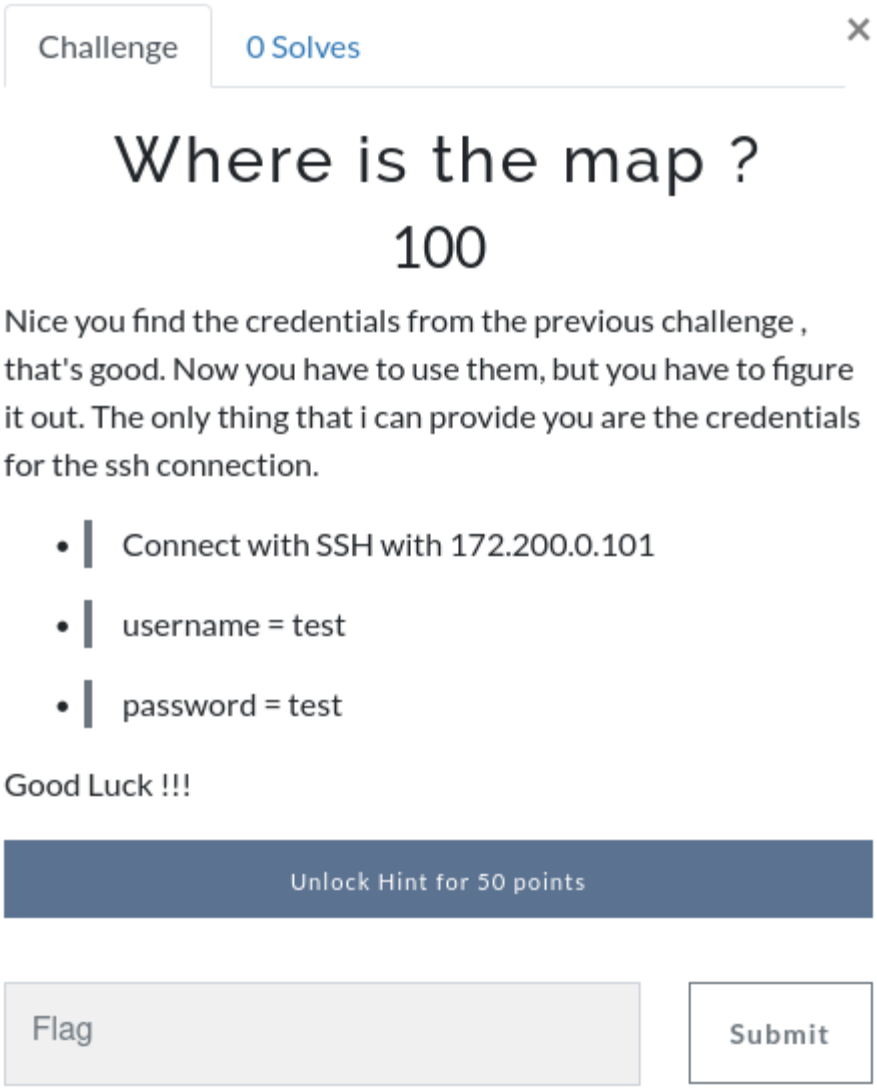


Εικόνα 36 Διακριτικό πρόσβασης

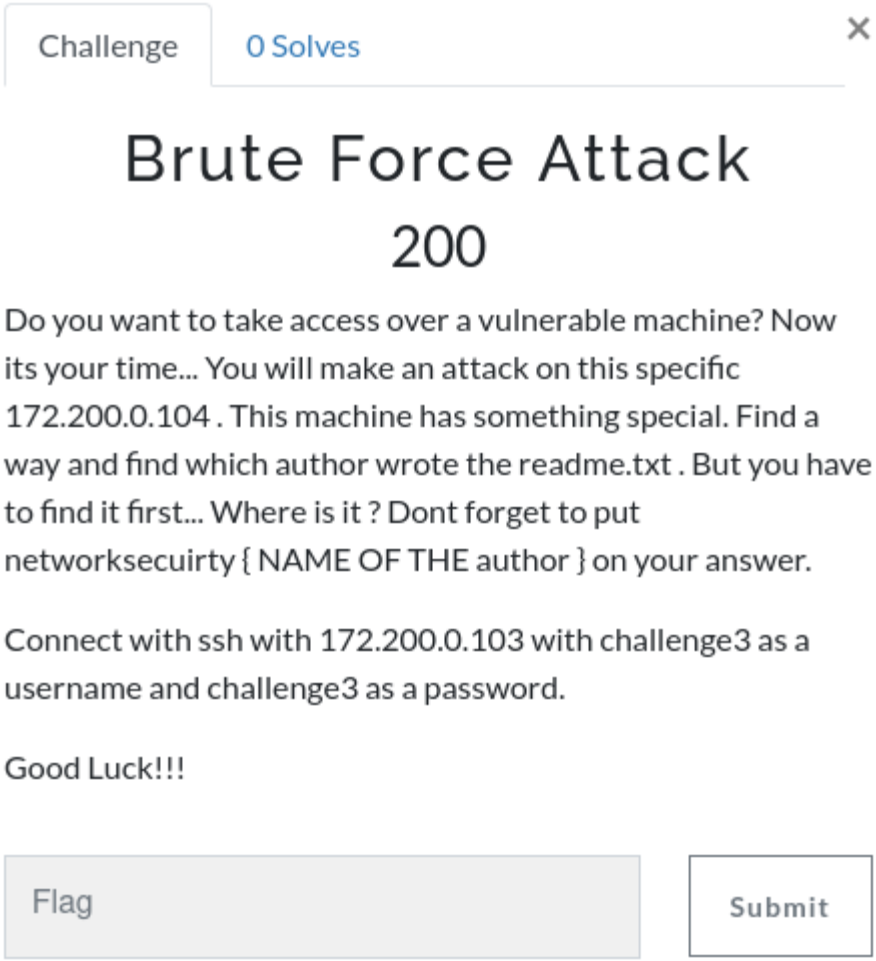
Στη συνέχεια ακολουθούν τα Εικόνα 37 - Εικόνα 38 - Εικόνα 39 όπου περιγράφουν στους χρήστες όλες τις απαραίτητες πληροφορίες που χρειάζονται για την επίλυση της εκάστοτε πρόκλησης. Συγκεκριμένα αποτελούν οι περίγραφες των προκλήσεων. Ακόμα μέσα από αυτές, οι χρήστες αντλούν όλες τις απαραίτητες πληροφορίες καθώς και τα βήματα που θα ακολουθήσουν ώστε να το επιλύσουν.



Εικόνα 37 Περιγραφή πρώτης πρόκλησης



Εικόνα 38 Περιγραφή δεύτερης πρόκλησης



Εικόνα 39 Περιγραφή τρίτης πρόκλησης