Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Ασφάλεια Υπολογιστών και Δικτύων

Μεταπτυχιακή Διατριβή

Πλατφόρμα Εκπαίδευσης Red Teaming Ανοιχτού Κώδικα

Δημήτρης Αργύρης

Επιβλέπων Καθηγητής

Σταύρος Σιαηλής

Δεκέμβρης 2022

Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Ασφάλεια Υπολογιστών και Δικτύων

Μεταπτυχιακή Διατριβή

Πλατφόρμα Εκπαίδευσης Red Teaming Ανοιχτού Κώδικα

Δημήτρης Αργύρης

Επιβλέπων Καθηγητής

Σταύρος Σιαηλής

Η παρούσα μεταπτυχιακή διατριβή υποβλήθηκε προς μερική εκπλήρωση των απαιτήσεων για απόκτηση μεταπτυχιακού τίτλου σπουδών στην Ασφάλεια Υπολογιστών και Δικτύων από τη Σχολή Θετικών και Εφαρμοσμένων Επιστημών του Ανοικτού Πανεπιστημίου Κύπρου.

Δεκέμβρης 2022

Περίληψη

Η παρούσα διατριβή στοχεύει στη διεξοδική μελέτη των υπαρχουσών πλατφορμών Penetration Testing, ανοιχτού και κλειστού κώδικα, την ανάλυση τους αλλά και τον εντοπισμό βελτιώσεων αυτών. Επιπλέον θα προταθεί ως λύση στις τυχόν ελλείψεις ή αδυναμίες που εντοπιστούν, μια πλατφόρμα ανοιχτού κώδικα ειδικά τροποποιημένη με τέτοιο τρόπο ώστε οι χρήστες να μπορέσουν να εκπαιδευτούν κατάλληλα πάνω σε διάφορες ευπάθειες, αλλά και να εξοικειωθούν με τους διάφορους ελέγχους παρείσδυσης. Οι έλεγχοι παρείσδυσης εκτελούνται από εξουσιοδοτημένα άτομα που ειδικεύονται στην ασφάλεια πληροφοριακών συστημάτων και αποσκοπούν στην αναγνώριση και εκμετάλλευση σοβαρών κενών ασφάλειας στα συστήματα στόχους και γνωστοποίηση αυτών στους εκάστοτε κατόχους των συστημάτων. Με τη γνωστοποίηση των ευρημάτων, οι κάτοχοι των ευάλωτων συστημάτων καλούνται να διορθώσουν τις ευπάθειες προτού αυτές εντοπιστούν και γίνουν αντικείμενο εκμετάλλευσης από κακόβουλες τρίτες οντότητες που έχουν στόχο να προξενήσουν κάθε είδους ζημιά σε αυτά τα ευπαθή συστήματα και κατ' επέκταση τον ίδιο τον οργανισμό.

Οι επαγγελματίες αυτού του τομέα, για να εντοπίσουν και να εκμεταλλευτούν επιτυχώς αυτές τις ευπάθειες, κάνουν χρήση διάφορων εργαλείων, ερμηνεύουν τα αποτελέσματα τους και προχωρούν στις απαραίτητες ενέργειες για να αποκτήσουν πρόσβαση στο σύστημα στόχο. Το πιο γνωστό λειτουργικό σύστημα που διαθέτει την πλειονότητα αυτών των εργαλείων είναι το Kali Linux. Για να διασφαλιστεί ότι όλοι οι εκπαιδευόμενοι θα διαθέτουν τα κατάλληλα εργαλεία για να εξοικειωθούν με τις διάφορες τεχνικές παρείσδυσης, δημιουργήθηκε ειδικός μηχανισμός που παρέχει στιγμιότυπα (snapshots) του λειτουργικού συστήματος Kali σε κάθε εκπαιδευόμενο τα οποία θα είναι προσβάσιμα από όλους μέσα από τον περιηγητή διαδικτύου (browser) του εκάστοτε εκπαιδευόμενου. Τέλος, στα πλαίσια της παρούσας διατριβής, θα δοθούν σε περιβάλλον docker, συστήματα στόχοι που περιέχουν διακομιστές που θα φιλοξενούν ευπαθείς εφαρμογές ιστού αλλά και υπηρεσίες δικτύου ώστε να επιτευχθεί κατάλληλη εκπαίδευση των φοιτητών πάνω στο αντικείμενο του Cyber Security.

Summary

This thesis aims at the thorough study of the existing open and closed source Penetration Testing platforms, their analysis and the identification of their improvements. In addition, an open source platform specially modified in such a way that users can be properly trained on various vulnerabilities, but also familiarize themselves with the various intrusion controls, will be proposed as a solution to any shortcomings or weaknesses identified. Intrusion checks are performed by authorized persons specializing in IT security and aim to identify and exploit serious security gaps in the target systems and communicate them to the respective system owners. Upon disclosure of the findings, the owners of vulnerable systems are required to correct the vulnerabilities before they are identified and exploited by malicious third-party entities that aim to cause any kind of damage to these vulnerable systems and, by extension, to the organization itself.

Professionals in this field, in order to successfully identify and exploit these vulnerabilities, make use of various tools, interpret their results and take the necessary actions to gain access to the target system. The best-known operating system that has the majority of these tools is Kali Linux. In order to ensure that all trainees will have the appropriate tools to familiarize themselves with the various intrusion techniques, a special mechanism has been created that provides snapshots of the Kali operating system to each trainee that will be accessible to everyone through the browser of each trainee.

Finally, in the context of this thesis, target systems containing servers that will host vulnerable web applications and network services will be provided in a docker environment in order to achieve appropriate training of students on the subject of Cyber Security.

Ευχαριστίες

Στην ενότητα αυτή θα ήθελα να ευχαριστήσω όλους όσους βοήθησαν στη διεκπεραίωση της παρούσας μεταπτυχιακής διατριβής.

Περιεχόμενα

Κεφάλαιο 1
Εισαγωγή

Αντικείμενο της παρούσας διατριβής είναι η δημιουργία μιας πλατφόρμας που αφορά την εκπαίδευση των φοιτητών του Ανοιχτού Πανεπιστημίου της Κύπρου στο εξειδικευμένο αντικείμενο της ασφάλειας πληροφοριακών συστημάτων, Penetration Testing. Η πλατφόρμα αυτή αποτελείται από το ανοιχτού κώδικα λογισμικό, Root The Box [1], το οποίο τροποποιήθηκε ειδικά για της ανάγκες της παρούσας διατριβής ώστε να παρέχει τη δυνατότητα να εκκινεί ευπαθή μηχανήματα στα οποία οι φοιτητές του πανεπιστημίου μπορούν να εκπαιδευτούν πάνω σε συγκεκριμένες ευπάθειες. Πιο συγκεκριμένα, στον ήδη υπάρχον κώδικα του Root The Box, προστέθηκαν νέα τμήματα κώδικα τα οποία δημιουργούν κουμπιά στο γραφικό περιβάλλον της πλατφόρμας, στην ενότητα του κάθε challenge, όπου το πάτημα τους πραγματοποιεί την εκκίνηση του εκάστοτε ευπαθούς μηχανήματος. Η λειτουργία αυτή επιτυγχάνεται με την αποστολή αιτημάτων HTTP, από το Root The Box, σε ένα νέο custom Flask script που είναι αρμόδιο να συλλέγει αυτά τα αιτήματα και να εκτελεί τις ανάλογες εντολές τοπικά, στον διακομιστή που φιλοξενεί την εφαρμογή.

Επιπλέον, για τη διευκόλυνση και την ομαλή εκπαίδευση των φοιτητών πάνω στην πλατφόρμα του Root The Box, προστέθηκε κώδικας που είναι υπεύθυνος για την εκκίνηση ατομικών στιγμιότυπων του λειτουργικού συστήματος Kali Linux. Τα στιγμιότυπα αυτά εκκινούνται και πάλι με το πάτημα ενός κουμπιού μέσα από το γραφικό περιβάλλον της εφαρμογής και αποτελούν το λειτουργικό σύστημα που θα χρησιμοποιεί κάθε φοιτητής για να εξαπολύσει κάθε είδους επίθεση ενάντιων του εκάστοτε ευπαθούς συστήματος.

Στη συνέχεια αυτής της διατριβής θα πραγματοποιηθεί αναφορά και ανάλυση άλλων ήδη διαθέσιμών πλατφορμών, εμπορικών αλλά και ανοιχτού κώδικα, τέτοιου είδους, η οποία θα έχει στόχο εντοπίσει αλλά και να καταγράψει τυχόν ανάγκες αυτών για βελτίωση.

1.1 Σκοπός

Σκοπός της παρούσας έρευνας είναι να παρουσιάσει τις υπάρχουσες διαθέσιμες πλατφόρμες Penetration Testing, ανοιχτού αλλά και κλειστού κώδικα, να εντοπίσει τις διαφορές τους και να καταγράψει τυχόν ανάγκες αυτών για βελτίωση. Επιπλέον θα παρουσιαστεί μία ήδη διαθέσιμη πλατφόρμα ανοιχτού κώδικα, ειδικά τροποποιημένη ως πρόταση για τις ανάγκες της παρούσας διατριβής, για τις ελλείψεις που εντοπίστηκαν. Η πλατφόρμα αυτή θα χρησιμοποιηθεί για την αποτελεσματικότερη εκπαίδευση των φοιτητών του πανεπιστημίου πάνω στο αντικείμενο του offensive cyber security και για αυτό το λόγο θα δίδεται η δυνατότητα σε κάθε φοιτητή να έχει πρόσβαση στο δικό του λειτουργικό σύστημα Kali Linux κάνοντας απλά χρήση του περιηγητή ιστού του (browser).

1.2 Βασικά Ερευνητικά Ερωτήματα

1. Τα τελευταία χρόνια έχει παρατηρηθεί μια μεγάλη αλλαγή στον τρόπο εκμάθησης του εξειδικευμένου αντικείμενου του cyber security. Η εκμάθηση του συγκεκριμένου αντικειμένου εστίαζε στην αφομοίωση θεωρίας κάτι που πλέον φαίνεται να έχει αλλάξει καθώς η εκπαίδευση σήμερα επιτυγχάνεται και επιταχύνεται με τη χρήση των διάφορων πλατφορμών ανοιχτού και κλειστού κώδικα εστιάζοντας πλέον σε ένα πιο πρακτικό μοντέλο εκμάθησης. Σε αυτές τις πλατφόρμες ο εκάστοτε ενδιαφερόμενος μπορεί να εκπαιδευτεί σε πραγματικό χρόνο έχοντας απέναντι του πραγματικά «ζωντανά» συστήματα στόχους ευπαθή από κατασκευής τους. Άρα μπορεί κανείς να συμπεράνει ότι αυτές οι πλατφόρμες έχουν βοηθήσει σημαντικά σε αυτή την αλλαγή εκμάθησης, με το ερευνητικό

ερώτημα που προκύπτει, να είναι, ποια είναι η καταλληλότερη πλατφόρμα για εκπαίδευση πάνω στο αντικείμενο του cyber security.

2. Πώς η ευκολία εύρεσης πληροφορίας, λόγω της "ανοιχτής" φύσης του διαδικτύου αλλά και της διάχυτης πληροφορίας που αυτό προσφέρει, επηρεάζουν τη μαθησιακή ικανότητα των ατόμων που αναζητούν πληροφορίες πάνω στο αντικείμενο του εντοπισμού και της εκμετάλλευσης ευπαθειών των πληροφοριακών συστημάτων όταν η πληροφορία που αναζητούν και τελικά βρίσκουν γίνεται αντικείμενο απομνημόνευσης και όχι άμεσης εφαρμογής με πρακτικό τρόπο;
3. Ποιος είναι ο καταλληλότερος τρόπος ώστε, οι θεωρητικές γνώσεις των εκπαιδευόμενων πάνω στο εξειδικευμένο αντικείμενο της κυβερνοασφάλειας, να εφαρμοστούν στην πράξη προτού αυτοί εκτεθούν σε πραγματικές συνθήκες και έρθουν αντιμέτωποι με «ζωντανά» συστήματα στον επαγγελματικό τομέα;

1.3 Αναγκαιότητα / Σπουδαιότητα Έρευνας

Η παρούσα διατριβή θα αναλύσει τις διάφορες διαθέσιμες πλατφόρμες ανοιχτού και κλειστού κώδικα, που είναι κατάλληλες για την καλύτερη εκπαίδευση των φοιτητών του πανεπιστημίου στο αντικείμενο του cyber security. Θα γίνει παράθεση των μεταξύ τους διαφορών και τέλος θα παρουσιάσει μια λύση που εμφανίζει αρκετά πλεονεκτήματα έναντι των άλλων ήδη γνωστών πλατφορμών εκπαίδευσης στην κυβερνοασφάλεια. Η λύση αυτή αφορά την ανοιχτού κώδικα εφαρμογή Root The Box που έχει τροποποιηθεί σε επίπεδο κώδικα ώστε να παράσχει την καλύτερη δυνατή εκπαίδευση στο αντικείμενο του cyber security στους φοιτητές του πανεπιστημίου.

1.4 Προσδοκώμενα Αποτελέσματα

Στα πλαίσια αυτής της διατριβής θα τροποποιηθεί σε επίπεδο κώδικα η open source εφαρμογή Root The Box και θα διερευνηθεί κατά πόσο υπερτερεί έναντι των υπόλοιπων διαθέσιμων ανοιχτού η κλειστού κώδικα πλατφορμών ως προς την εκπαίδευση των φοιτητών του πανεπιστημίου στο αντικείμενο της κυβερνοασφάλειας. Η τροποποιημένη

μορφή της εφαρμογής Root The Box θα παρέχει αρκετά πλεονεκτήματα, έναντι των υπόλοιπων πλατφορμών, στους εκπαιδευόμενους καθώς αναμένεται να δίνει μεγαλύτερο έλεγχο ως προς τον τρόπο που δημιουργούνται και γίνονται διαθέσιμα τα challenge, το οικονομικό κόστος επιβάρυνσης είναι μηδενικό καθώς επίσης δίνεται, επίσης χωρίς κόστος, πρόσβαση σε ατομικά στιγμιότυπα του λειτουργικού συστήματος Kali Linux που περιλαμβάνει όλα τα πολύτιμα εργαλεία που χρειάζεται ο εκπαιδευόμενος για να εκπαιδευτεί πάνω στις ευπάθειες που εκείνος επιθυμεί.

Κεφάλαιο 2

Βιβλιογραφική Ανασκόπηση

2.1 Η σημαντικότητα της κυβερνοασφάλειας

Η ραγδαία ανάπτυξη της τεχνολογίας αλλά και της επιστήμης της πληροφορικής σήμερα είναι κάτι που δε μπορεί να αμφισβητηθεί. Τα οφέλη που παρέχει είναι αμέτρητα, τόσο για την καθημερινότητα των ανθρώπων όσο για τις επιχειρήσεις αλλά και την παγκόσμια οικονομία. Η ικανότητα των υπολογιστών να εκμηδενίζουν τις αποστάσεις, να «ενώνουν» μεταξύ τους άτομα σε απομακρυσμένες τοποθεσίες, να επεξεργάζονται ταχύτατα δεδομένα και να παράγουν επιθυμητά αποτελέσματα στον σωστό χρόνο είναι αυτό που «ανάγκασε» το σύνολο των ανθρώπων σήμερα να τους αποκτήσουν και να τους κάνουν μέρος της ζωής τους είτε σε προσωπικό, είτε σε επαγγελματικό επίπεδο με στόχο να μεγιστοποιήσουν την παραγωγική ικανότητα των επιχειρήσεων τους και να ανταπεξέλθουν στις σημερινές δύσκολες ανταγωνιστικές εμπορικές συνθήκες. Επειδή ακριβώς οι υπολογιστές λαμβάνουν, επεξεργάζονται, στέλνουν και αποθηκεύουν δεδομένα, πρέπει να διασφαλίζεται ότι οι ίδιοι και κατ επέκταση αυτά τα δεδομένα είναι προστατευμένα από κακόβουλες τρίτες οντότητες που θέλουν να τα κλέψουν και να τα χρησιμοποιήσουν για δικό τους οικονομικό όφελος.

Η ανάγκη αυτή της προστασίας των πληροφοριακών συστημάτων απέναντι σε κακόβουλες επιθέσεις τρίτων τα περασμένα χρόνια οδήγησε πολλά άτομα να ασχοληθούν με αυτόν τον τομέα της πληροφορικής. Σήμερα όμως, λόγο και των διαρκώς αυξανόμενων αναγκών των επιχειρήσεων απέναντι σε τέτοιους κινδύνους, άλλα και της δυσκολίας εκμάθησης αυτού του αντικειμένου, παρατηρείται έλλειψη εξειδικευμένου προσωπικού σε αυτό τον τομέα πράγμα που αναφέρει και ο Gonzalez σε μια έρευνα [2] που πραγματοποίησε. Η έρευνα αυτή αναφέρει μάλιστα ότι η έλλειψη αυτή είναι πλέον εύκολα διακριτή και οδήγησε και τα πανεπιστήμια στο να προσθέσουν μαθήματα cyber security στα πρόγραμμα σπουδών τους. Αυτό όμως από μόνο του δε μπορεί να εξαλείψει το πρόβλημα καθώς η εκμάθηση σε μόλις ένα εξάμηνο δεν είναι αρκετή. Για αυτό το λόγο στην ίδια έρευνα παρουσιάζει την πρόταση της εκπαίδευσης των ενδιαφερόμενων μέσα από κάποιου είδους «παιχνιδοποιημένης» εκμάθησης. Ο Gonzalez δεν ήταν ο μόνος που έβλεπε την ανάγκη της αλλαγής του τρόπου εκπαίδευσης από την καθαρή θεωρία στην «παιχνιδοποιημένη», πρακτική εκμάθηση των ενδιαφερόμενων. Σε έρευνα που δημοσιεύτηκε το 2021 [3], ο M. Malone είναι ακόμη ένας που παρουσιάζει την «παιχνιδοποιημένη» εμπειρία εκμάθησης του cyber

security ως μέσο απόκτησης της γνώσης και των τεχνικών που είναι απαραίτητα σήμερα για την επίλυση σύνθετων προβλημάτων βασισμένα σε ένα πολύ ανταγωνιστικό περιβάλλον που δίνει κίνητρο στους εκπαιδευόμενους.

2.2 Αλλαγή τρόπου εκπαίδευσης

Έτσι, εμφανίστηκε η ανάγκη της αλλαγής του τρόπου εκπαίδευσης από την εφαρμοσμένη θεωρία, στην πρακτική εκμάθηση. Σε αυτό βοήθησαν πάρα πολύ οι διάφορες πλατφόρμες ανοιχτού αλλά και κλειστού κώδικα που είναι διαθέσιμες σήμερα προς χρήση, πχ. HackTheBox, RootTheBox και πολλές άλλες.

Οι πλατφόρμες αυτές ουσιαστικά εκθέτουν τους εκπαιδευόμενους σε διάφορες ευπάθειες, τεχνολογίες, σενάρια ασφάλειας και ευπαθή συστήματα. Οι συμμετέχοντες επιβραβεύονται για κάθε challenge που θα «λύσουν» επιτυχώς, καταλαμβάνοντας το αντίστοιχο “flag” που έχει τη δική του βαθμολογική βαρύτητα βάση της δυσκολίας του. Οι πόντοι έχουν μεγάλη σημασία καθώς κάνουν τους εκπαιδευόμενους να «σκαρφαλώνουν» μια βαθμολογική σκάλα, παρέχοντας τους αυξημένο κίνητρο καθώς οι ίδιοι αποκτούν και την αναγνώριση μεταξύ των συμμετεχόντων. Με αυτό τον τρόπο επιτυγχάνεται και η επιτάχυνση της μαθησιακής διαδικασίας αλλά και διατηρείται σε πολύ υψηλό βαθμό το κίνητρο του κάθε εκπαιδευόμενου.

2.3 Πλατφόρμες εκπαίδευσης και διαφορές

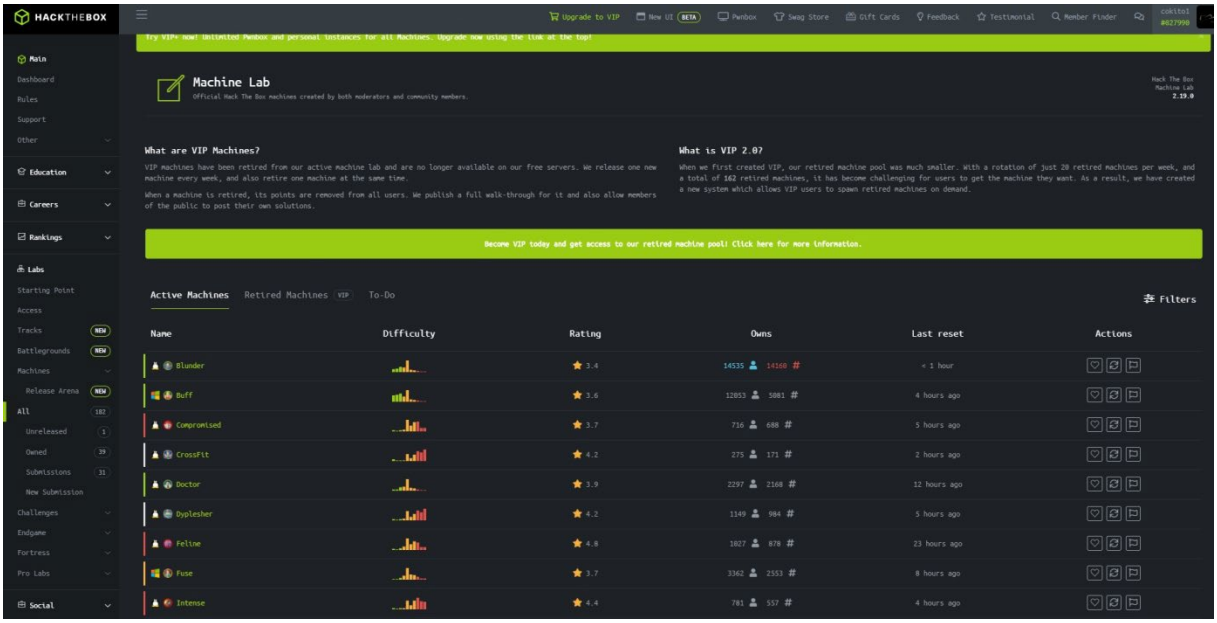
2.3.1 Εμπορικές πλατφόρμες

Στην ενότητα αυτή θα παρουσιάσουμε τις ποιο γνωστές εμπορικές πλατφόρμες κλειστού κώδικα και κάποια από τα βασικότερα χαρακτηριστικά τους.

2.3.1.1 *HackTheBox*

Το HackTheBox [4] αποτελεί μια από τις κορυφαίες πλατφόρμες εκπαίδευσης στο αντικείμενο της κυβερνοασφάλειας. Διαθέτει πολλά ευπαθή συστήματα τα οποία έχουν βαθμό δυσκολίας που δίνεται από τον δημιουργό του μηχανήματος αλλά και από την κοινότητα της πλατφόρμας, δηλαδή τους χρήστες του. Οι χρήστες μπορούν να βαθμολογήσουν το μηχάνημα με την επιτυχή απόκτηση και τοποθέτηση στην πλατφόρμα και των δύο flag, του user flag και του root flag. Σε κάθε flag που υποβάλλεται η πλατφόρμα επιβραβεύει τον χρήστη ή την ομάδα του χρήστη, αν ανήκει σε κάποια, με βαθμούς, με την σημαία του root να δίνει και τους περισσότερους πόντους καθώς αυτή σηματοδοτεί την πλήρη πρόσβαση στο μηχανή με τα μέγιστα

δικαιώματα, αυτά του Root User. Το HackTheBox κατηγοριοποιεί τα μηχανήματα σε active και retired. Η κατηγοριοποίηση αυτή στηρίζεται στη χρονική διάρκεια ύπαρξης του μηχανήματος από τη στιγμή της διάθεσης του στο κοινό. Συνήθως ένα μηχάνημα χαρακτηρίζεται ως ενεργό τις πρώτες 120 μέρες της διάθεσης του ενώ μετά αποσύρεται και χαρακτηρίζεται ως retired ενώ παράλληλα δίνεται και ο τρόπος απόκτησης των 2 flag διευκολύνοντας με αυτό τον τρόπο και τη μαθησιακή διαδικασία σε περίπτωση που κάποιος δεν έχει καταφέρει να βρει τον τρόπο να αποκτήσει και τα δύο flag. Τα retired μηχανήματα δεν δίνουν πόντους και είναι διαθέσιμα μόνο σε premium συνδρομητές. Νέα μηχανήματα προστίθενται κάθε βδομάδα αφού περάσουν από αξιολόγηση των moderator της πλατφόρμας ώστε να πληρούν κάποια συγκεκριμένα κριτήρια που έχουν οριστεί από την εταιρία. Επιπλέον, το HackTheBox διαθέτει και μια ακαδημαϊκή ενότητα για εκμάθηση θεωρητικών αλλά και πρακτικών θεμάτων για τους πιο αρχάριους χρήστες της πλατφόρμας. Τέλος, υπάρχουν “labs” τα οποία είναι διαθέσιμα επίσης σε premium συνδρομητές και αυτά αποτελούνται από ομάδες μηχανημάτων που κατά κάποιο τρόπο σχετίζονται μεταξύ τους καθώς προσομοιάζουν εταιρικά περιβάλλοντα και είναι αυξημένης δυσκολίας.

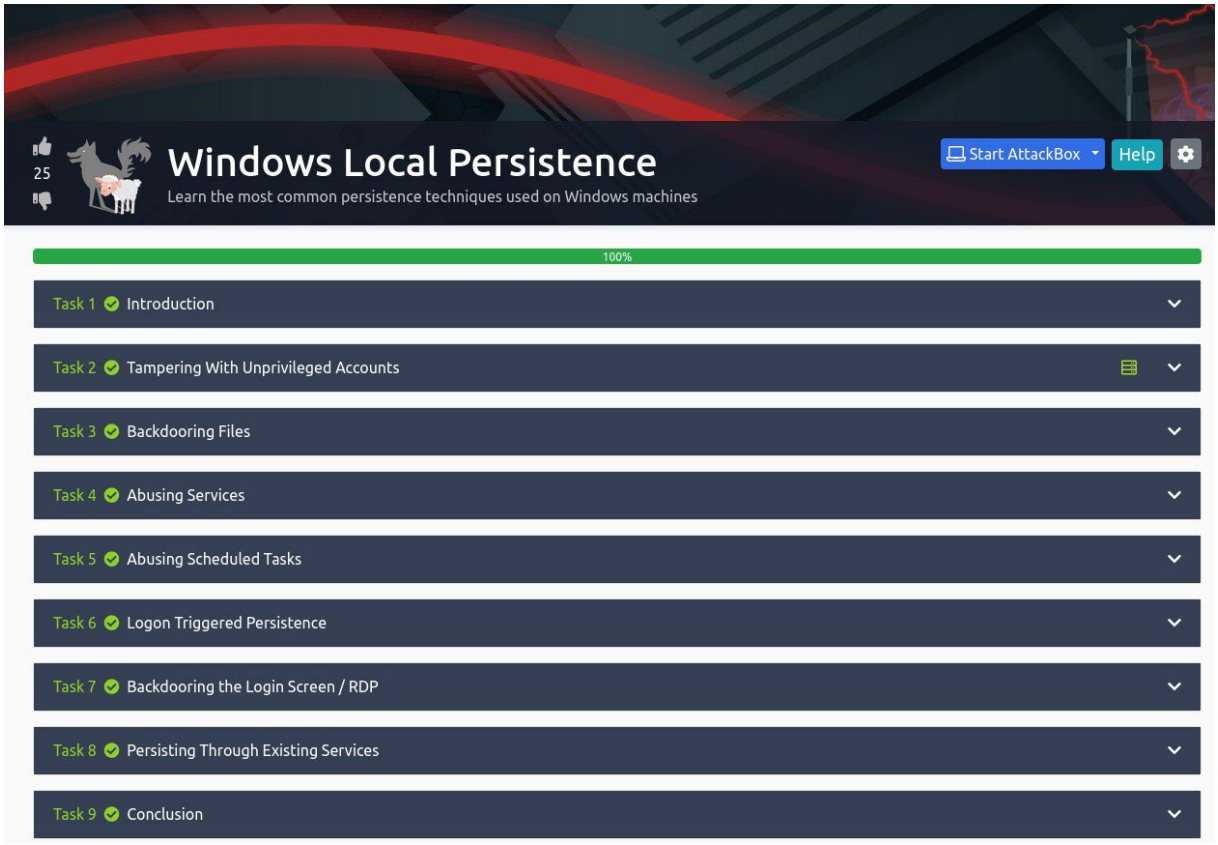


Εικόνα 1.

2.3.1.2 *TryHackMe*

Το TryHackMe [5] αποτελεί επίσης μια από τις πιο γνωστές πλατφόρμες εκπαίδευσης στο χώρο του cyber security. Η εκπαίδευση στην πλατφόρμα αυτή γίνεται από τους ενδιαφερόμενους με την μορφή challenges όπου κάθε βδομάδα προστίθεται νέα από την κοινότητα της πλατφόρμας. Με την ολοκλήρωση κάθε challenge ο χρήστης επιβραβεύεται με πόντους οι οποίοι προστίθενται στη συνολική βαθμολογία του και έτσι κάθε χρήστης μπορεί να αναρριχηθεί στην «σκάλα» των χρηστών σε ατομικό ή εθνικό επίπεδο. Τα challenge ολοκληρώνονται με την απάντηση όλων των ερωτήσεων που έχει θέσει ο δημιουργός του. Το TryHackMe δίνει τη δυνατότητα στους χρήστες να

δημιουργήσουν και να ανεβάσουν εικονικές μηχανές και να θέσουν τις δικές τους ερωτήσεις οι οποίες, αν απαντηθούν σωστά, αποτελούν και κριτήριο επίλυσης της εικονικής μηχανής η όχι. Οι εικονικές μηχανές μπορούν να προσπελαστούν από τους υπόλοιπους χρήστες με το διαμοιρασμό κώδικα από τον δημιουργό της κάτι που αποτελεί πλεονέκτημα για challenges καθοδηγούμενα από τους χρήστες η την κοινότητα της πλατφόρμας. Το TryHackMe διαθέτει επίσης διάφορες ενότητες εκμάθησης ακαδημαϊκού τύπου για τους πιο αρχάριους χρήστες του.

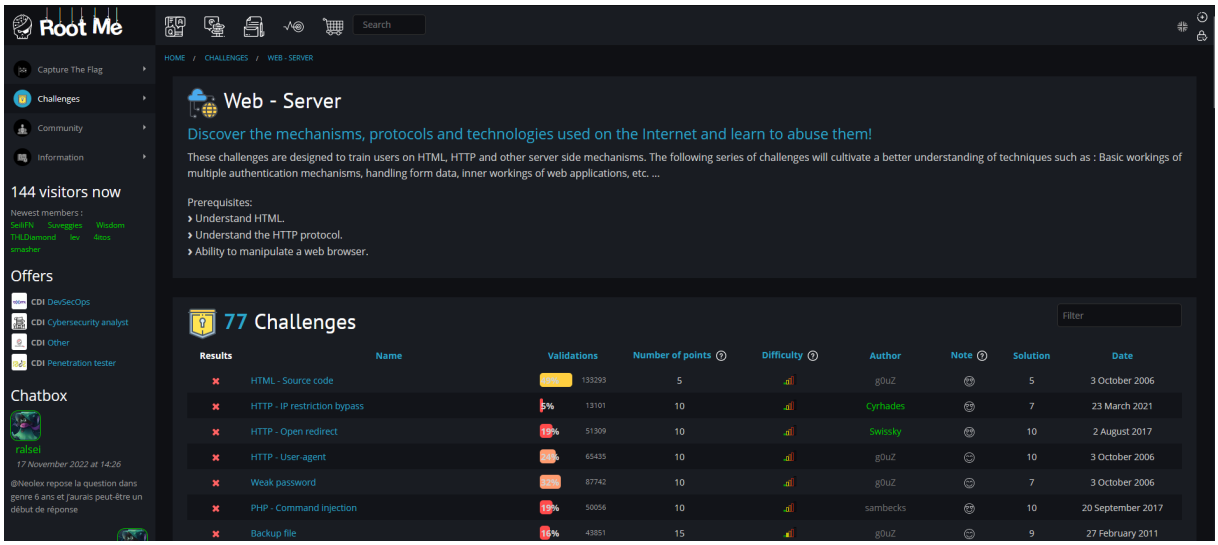


Εικόνα 2.

2.3.1.3 *RootMe*

Η πλατφόρμα RootMe [6] προσφέρει μεγάλη ποικιλία στα challenges που διαθέτει, όπου όμοια challenges ομαδοποιούνται σε ίδιες ενότητες μαζί με το αντίστοιχο εκπαιδευτικό υλικό για εκμάθηση. Οι ενότητες, όπως και το εκπαιδευτικό υλικό, εκτίνονται από απλές ιστοσελίδες για web application penetration testing, μέχρι reverse engineering ή challenges που αφορούν ολόκληρα εικονικά δίκτυα. Όπως και στις προηγούμενες εμπορικές πλατφόρμες που αναλύσαμε, έτσι και στο RootMe, η ολοκλήρωση των challenge από τους χρήστες επιβραβεύεται με πόντους , όπου βάση του αθροίσματος τους οι χρήστες κατατάσσονται στην γενική κατάταξη της πλατφόρμας. Εκπαιδευτικό υλικό παρέχεται και εδώ καθώς επίσης και η δυνατότητα κάποιου εγγεγραμμένου χρήστη ή εκπαιδευτή να διοργανώνει events για

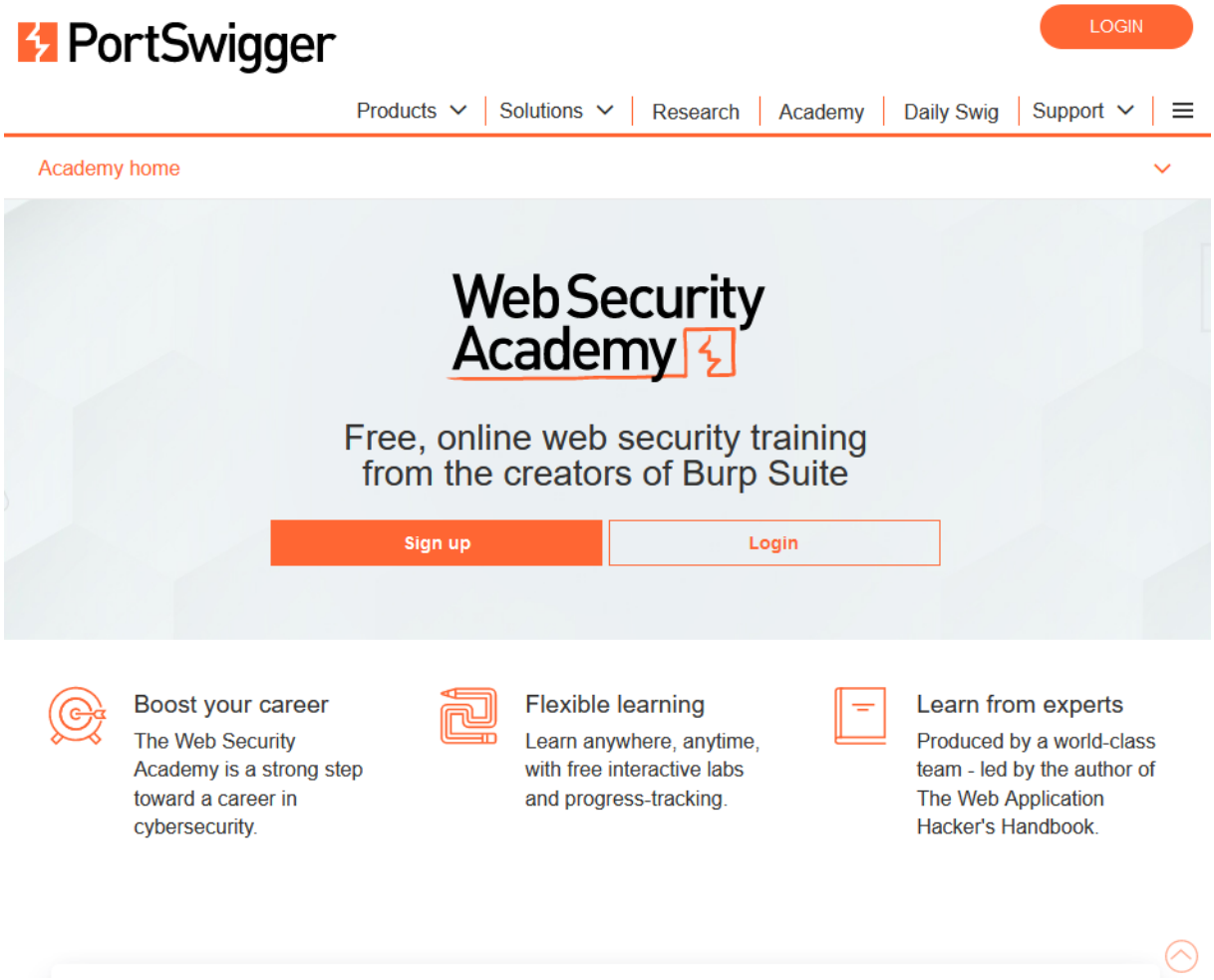
συγκεκριμένους χρήστες η να διαμοιράζει tasks μεταξύ αυτών. Παρέχει επίσης τη δυνατότητα επιβολής χρονικού περιορισμού στα challenges ή μειωμένη επιβράβευση βαθμών σε περίπτωση καθυστερημένης υποβολής απαντήσεων.



Εικόνα 3.

2.3.1.4 *Web Security Academy*

Η πλατφόρμα Web Security Academy [7] έχει δημιουργηθεί από την εταιρία Portswigger η οποία έχει φτιάξει το BurpSuite εργαλείο ασφάλειας εφαρμογών και ιστοσελίδων. Η πλατφόρμα αυτή προσφέρει αλληλεπιδραστική πρακτική εξάσκηση στο εξειδικευμένο αντικείμενο της ασφάλειας πληροφοριακών συστημάτων. Στην πλατφόρμα αυτή τα challenge βρίσκονται πάνω σε μηχανήματα και γίνονται διαθέσιμα στους εκπαιδευόμενους με τη μορφή στιγμιότυπων ώστε ο κάθε χρήστης να χρησιμοποιεί το δικό του στιγμιότυπο και να μην επηρεάζει την μαθησιακή πρακτική εμπειρία των υπόλοιπων χρηστών. Ένα σημαντικό πλεονέκτημα αυτής της πλατφόρμας είναι ότι τα μηχανήματα των challenge, μπορούν να προσπελαστούν από τους χρήστες χωρίς τη χρήση κάποιου VPN, σε αντίθεση με τις προηγούμενες εμπορικές πλατφόρμες που η χρήση του ήταν απαραίτητη. Στο Web Security Academy τα challenge χωρίζονται σε ατομικά “labs” όπου κάθε ένα από αυτά επικεντρώνεται σε διαφορετικές περιοχές της ασφάλειας εφαρμογών και ιστοσελίδων ώστε να διευκολυνθεί η εμπειρία εκμάθησης του χρήστη. Και σε αυτή την περίπτωση οι χρήστες επιβραβεύονται από την πλατφόρμα με πόντους όταν ολοκληρώνουν επιτυχως ένα lab και οι πόντοι προστίθενται στους συνολικούς πόντους του χρήστη κατατάσσοντας τον σε ανάλογη θέση στον πίνακα με τις βαθμολογίες των υπόλοιπων χρηστών. Έτσι κάθε εκπαιδευόμενος μπορεί να ελέγχει την πρόοδο του με μεγάλη ακρίβεια. Τέλος , το Web Security Academy platform περιλαμβάνει μόνο μεθόδους, πρακτικές και θεωρία που αφορούν το web application penetration test και δεν ασχολείται με άλλα θέματα που αφορούν την κυβερνοασφάλεια όπως δικανική υπολογιστών και άλλα.



Εικόνα 4.

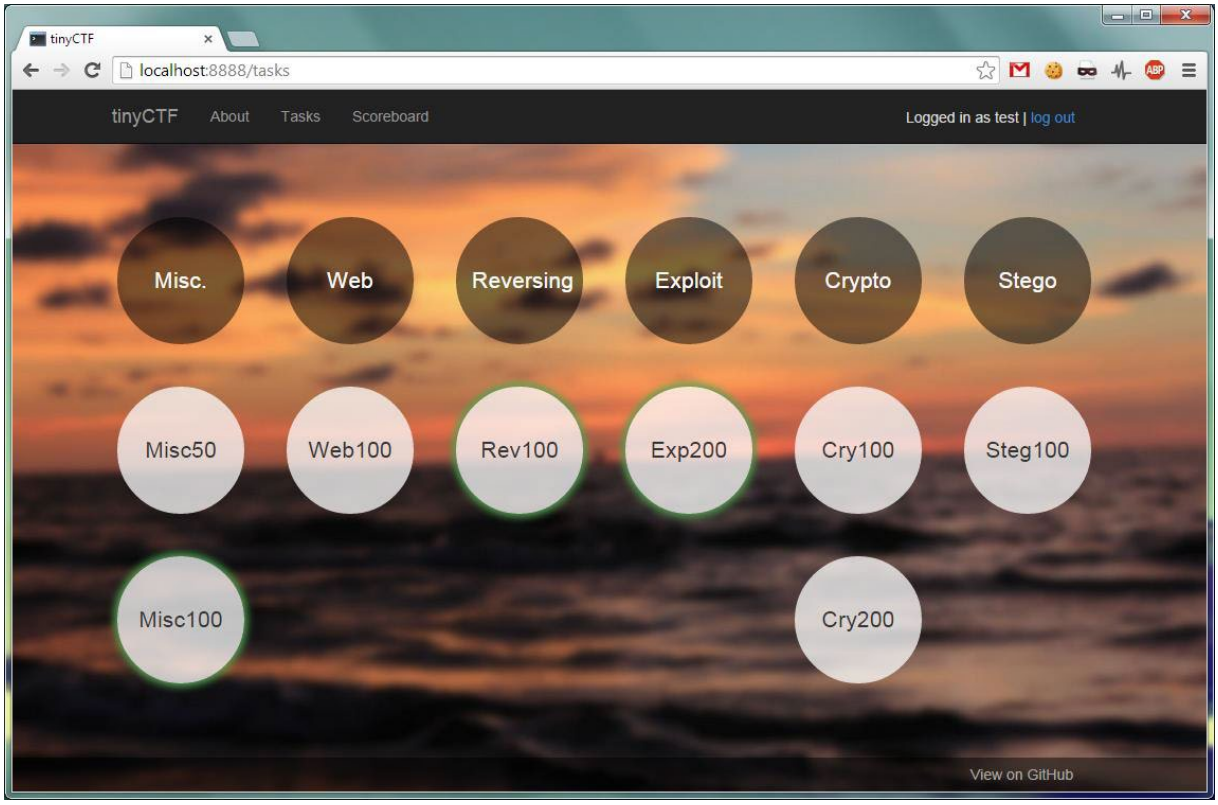
2.3.2 Πλατφόρμες Ανοιχτού Κώδικα

Στην ενότητα αυτή θα παρουσιάσουμε κάποιες από τις πιο γνωστές πλατφόρμες ανοιχτού κώδικα και κάποια από τα βασικότερα χαρακτηριστικά τους.

2.3.2.1 *TinyCTF*

Η πλατφόρμα TinyCTF [8] είναι μια από τις πιο πολυχρησιμοποιημένες πλατφόρμες για CTF (capture the flag) events με ευρεία χρήση σε μικρής ή μεγάλης κλίμακας διαγωνισμούς capture the flag. Αυτή η πλατφόρμα είναι προγραμματισμένη σε γλώσσα Python και JavaScript ενώ χρησιμοποιεί το Flask component της Python ως διακομιστή για να μπορούν οι χρήστες της να προσπελάσουν τα διάφορα challenge όταν ο αναμενόμενος αριθμός των συμμετεχόντων είναι μικρός. Σε διαφορετική περίπτωση, οι οδηγίες αυτής της πλατφόρμας αναφέρουν ότι θα ήταν καλύτερο να γίνει χρήση κάποιου κανονικού διακομιστή όπως για παράδειγμα ενός Apache ή Nginx. Στην πλατφόρμα TinyCTF τα challenges είναι περασμένα σε κάποιο JSON αρχείο το οποίο

στη συνέχεια γίνεται import από την πλατφόρμα κάνοντας χρήση ενός υπάρχον Python script που ανήκει στην πλατφόρμα. Αυτό παρέχει μεγάλη ευκολία στη διαχείριση και μορφοποίηση των challenges που έχουν πολλαπλά στάδια ή flags. Αξίζει να σημειωθεί ότι η συγκεκριμένη πλατφόρμα υποστηρίζει εύκολη ενσωμάτωση σε EC2 στιγμιότυπα κάτι που της δίνει χαρακτηρίστηκα ευκολίας τόσο στο «χτίσιμο» , τη ρύθμιση και την ανάπτυξη της με κλιμακούμενο τρόπο. Το TinyCTF μπορεί επίσης να εγκατασταθεί χειροκίνητα σε πολλά και διαφορετικά λειτουργικά συστήματα Linux.

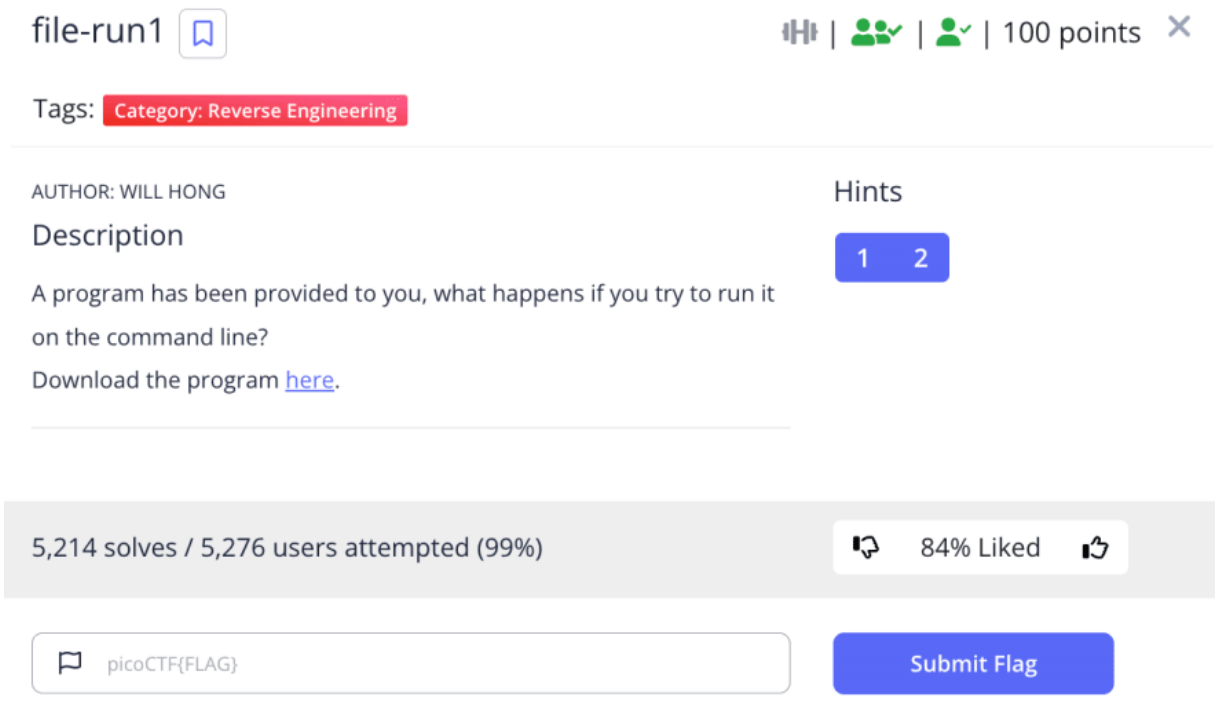


Εικόνα 5.

2.3.2.2 *PicoCTF*

Το PicoCTF είναι μία πλατφόρμα που σχεδιάστηκε από το Carnegie Mellon University και στην αρχή χρησιμοποιούταν στα πλαίσια ενός ετήσιου διαγωνισμού. Στην πορεία αυτό άλλαξε καθώς οι δημιουργοί της πλατφόρμας αποφάσισαν να δημοσιεύσουν την πλατφόρμα ώστε και άλλοι διοργανωτές τέτοιων διαγωνισμών να μπορούν να την χρησιμοποιήσουν ελεύθερα και να δημιουργήσουν τα δικά τους capture the flag events. Όπως αναφέρεται στην ιστοσελίδα της πλατφόρμας [9], οι συμμετέχοντες πρέπει να είναι σε θέση να σκεφτούν δημιουργικά για να λυσσούν τα challenges και να αποκτήσουν τα flags. Τα challenges καλύπτουν πολλές ενότητες του αντικείμενου του cyber security όπως reverse engineering, decryption και άλλα. Ως προς τα ποιο τεχνικά σημεία της πλατφόρμας, είναι προγραμματισμένη σε γλώσσες Python και JavaScript ενώ η παραμετροποίηση των challenges γίνεται κάνοντας αλλαγές σε HTML templates

που παρέχονται ως μέρος της πλατφόρμας. Η πλατφόρμα όπως έχει σχεδιαστεί είναι αρκετά ευέλικτη ως προς τη δυνατότητα που δίνει στους χρήστες για να πραγματοποιήσουν τις αλλαγές που θέλουν, διαθέτει ενσωματωμένα API και ένα κέλυφος διακομιστή (Shell) που πρέπει να αναπτυχθεί παράλληλα με την πλατφόρμα καθώς αυτός ο διακομιστής είναι αυτός με τον οποίο θα αλληλεπιδρούν οι εκπαιδευόμενοι για να συμμετάσχουν στο διαγωνισμό, είτε μέσω του περιηγητή τους είτε μέσω σύνδεσης τους με το VPN της πλατφόρμας. Σαν πλατφόρμα παρέχει πάρα πολλές δυνατότητες και είναι αρκετά πλήρεις ως προς τα χαρακτηριστικά της καθώς επιτρέπει εκτενή παραμετροποίηση. Για την χειροκίνητη ανάπτυξη της σε περιβάλλον επιλογής του εκάστοτε χρήστη, επιτρέπει χρήση τεχνολογίας Vagrant [10] δίνοντας τη δυνατότητα ταυτόχρονης εκκίνησης παράθυρου κέλυφους, στιγμιότυπο διακομιστή αλλα και την ίδια την πλατφόρμα όπως αναφέρεται και στις οδηγίες εγκατάστασης της.

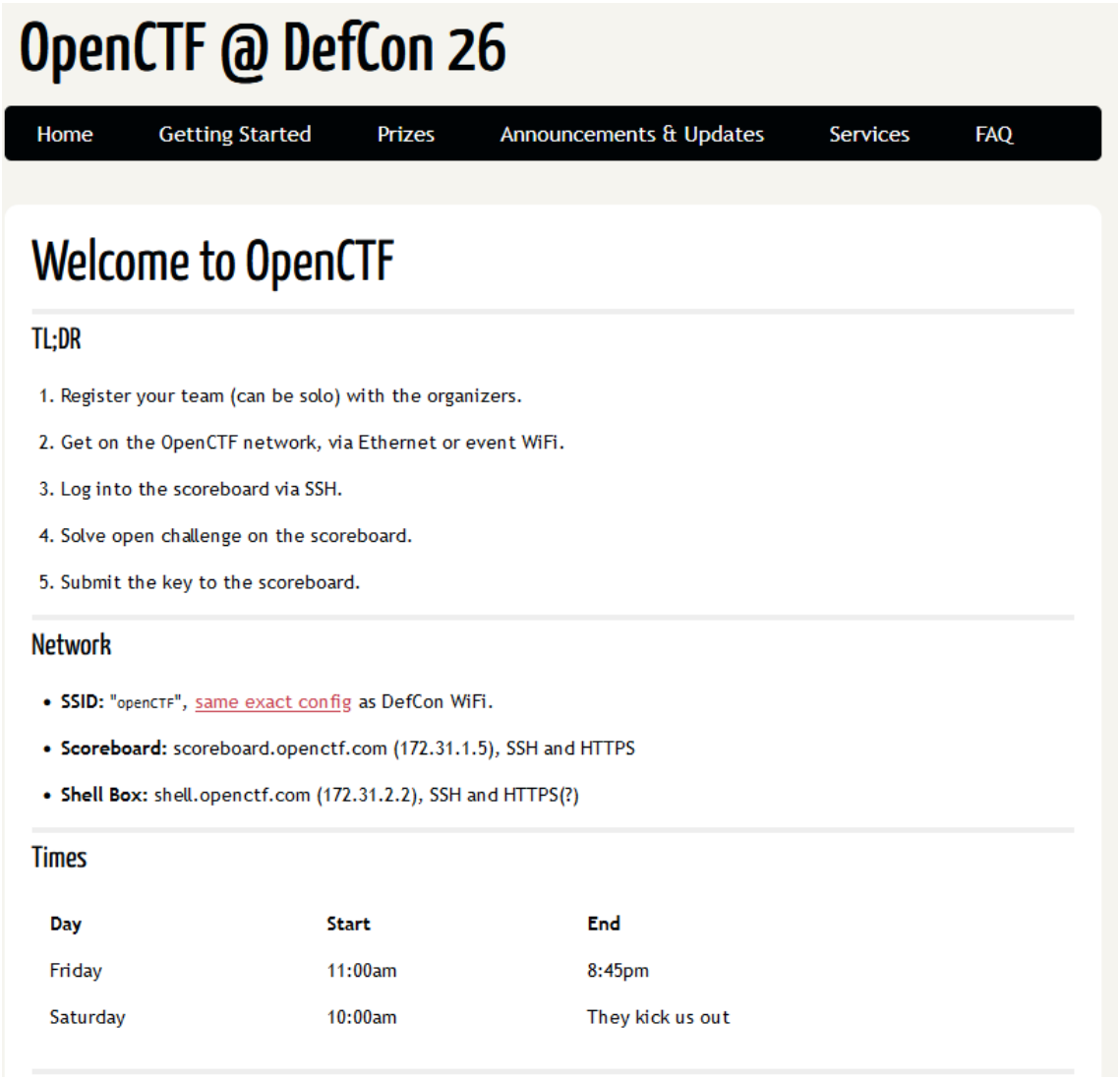


Εικόνα 6.

2.3.2.3 *OpenCTF*

Το OpenCTF [11] είναι άλλη μια capture the flag πλατφόρμα, γραμμένη σε γλώσσα PHP. Παρέχει διεπαφή χρήστη ιστού, πίνακα βαθμολογιών και υποστηρίζει δυνατότητα «κατεβάσματος» για τα διάφορα challenges που διαθέτει. Είναι εξαιρετικά ελαφριά και εύκολη στη χρήση της καθώς μπορεί να τρέξει σε ένα και μόνο NPM minimal HTTP module [12] της Node.js γλώσσας. Τα διάφορα challenges μπορούν να αναπτυχθούν πάρα πολύ εύκολα απλά τροποποιώντας τον αντίστοιχο πίνακα στη βάση δεδομένων της πλατφόρμας. Αυτή η δυνατότητα επιτρέπει την παράλληλη δημιουργία και

εκκίνηση πολλαπλών challenge που τρέχουν πάνω στον ίδιο διακομιστή κάνοντας χρήση τεχνολογίας container (dockers). Όλα τα παραπάνω καθιστούν το OpenCTF μια πολύ ευέλικτη, εύκολα παραμετροποιήσιμη και ισχυρή πλατφόρμα για challenges τύπου capture the flag.



Εικόνα 7.

2.3.2.4 *FBCTF*

Άλλη μια πλατφόρμα που μπορεί να φιλοξενήσει διαγωνισμούς capture the flag είναι η πλατφόρμα FBCTF [13] ή αλλιώς FacebookCTF. Η πλατφόρμα αυτή δημιουργήθηκε από μια ομάδα εργαζόμενων του Facebook η οποία μάλιστα δημοσίευσε και τον κώδικα της πλατφόρμας που δημιούργησαν για να τρέχουν τα δικά τους event. Το FBCTF είναι μια αρκετά όμορφη στιλιστικά πλατφόρμα που δίνει τη δυνατότητα στους χρήστες της να πραγματοποιούν πολλαπλές αλλαγές στις ρυθμίσεις των event κάνοντας απλά χρήση της web ενότητας της εφαρμογής που αφορά την παραμετροποίηση των challenge.

Είναι ιδανική για event μεγάλης κλίμακας καθώς περιέχει πολλά χαρακτηριστικά καλύτερου ελέγχου συμπεριλαμβανομένου δυναμικών χρονομέτρων, πίνακα αποτελεσμάτων (score board – leader board) καθώς επίσης και ευκολότερη διαχείριση του εκάστοτε εν εξελίξει διαγωνισμού αλλά και μεμονωμένων καθηκόντων.

Εικόνα 8.

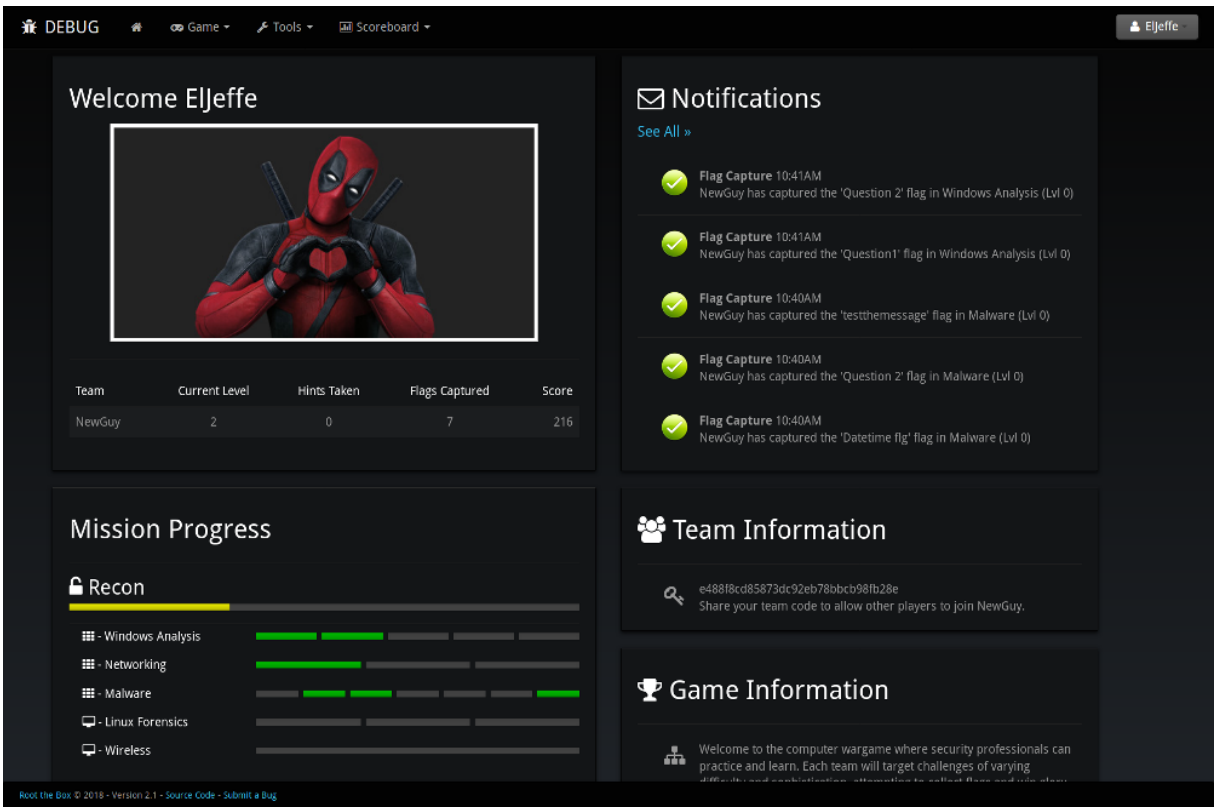
2.3.2.5 *RootTheBox*

Το RootTheBox [14] platform είναι άλλη μια πλατφόρμα ανοιχτού κώδικα capture the flag καθώς επίσης και μια μηχανή scoring που είναι γραμμένη σε γλώσσα προγραμματισμού Python. Διαθέτει πολλά καινοτόμα χαρακτηριστικά που δεν υπάρχουν σε άλλες capture the flag πλατφόρμες ανοιχτού ή κλειστού κώδικα. Μερικά από αυτά τα χαρακτηριστικά είναι τα ακόλουθα:

- Διαθέτει τραπεζικό σύστημα (banking system) όπου τα χρήματα της πλατφόρμας μπορούν να χρησιμοποιηθούν από τους χρήστες για τους ακόλουθους λόγους:
    - Ξεκλείδωμα επιπέδου (level)
    - Αφορά «βοήθειας» (hint) για την κατάκτηση ενός flag
    - Κατέβασμα πηγαίου κώδικα ενός συστήματος στόχου
    - Επίθεση σε άλλους παίχτες (SWAT mode)
- Τα hash των κωδικών των τραπεζικών λογαριασμών αντίπαλων παικτών μπορούν να είναι ορατά προς όλους τους χρήστες, επιτρέποντας με αυτό τον τρόπο στους αντιπάλους τους να προσπαθούν να τα «σπάσουν» ώστε να αποκτήσουν πρόσβαση στον τραπεζικό τους λογαριασμό με σκοπό να τους κλέψουν τα χρήματα.

- Υποστηρίζει πραγματικού χρόνου κινούμενα γραφήματα και ενημερώσεις αυτών σε πραγματικό χρόνο κάνοντας χρήση web socket.
- Υποστηρίζει πολλαπλούς τύπους flag, όπως:
    - Regex
    - Datetime
    - Multiple Choice
- Υπάρχει δυνατότητα επιβολής penalty, δυνατότητα hint, επιβράβευση ανεβάσματος επιπέδου, δυναμικό σύστημα scoring και άλλα.
- Ενσωματωμένο chat που μπορούν να κάνουν χρήση οι ομάδες ώστε να ανταλλάσουν πληροφορίες για ευάλωτα συστήματα η να μοιράζονται μεταξύ τους αρχεία.
- Διαθέτει ενσωματωμένο το πολυεργαλείο CyberChef [15] στο μενού «εργαλεία».
- Υποστήριξη ομαδικού chat με ενσωματωμένη τεχνολογία Rocket Chat για ασφαλέστερη επικοινωνία μεταξύ των μελών.
- Πάγωμα του πίνακα των score κατ' επιλογήν επιτρέποντας την έναρξη της αντιστροφής μέτρησης για τη λήξη του διαγωνισμού CTF.
- Δυνατότητα story mode που υποστηρίζει εισαγωγικούς (intro) διαλόγους με γραφικά.
- Wall of sheep – Αναρτώνται οι χρήστες των οποίων οι κωδικοί έσπασαν επιτυχώς από άλλους αντίπαλους παίχτες.
- Δυνατότητα «εξαγωγής» (Export) και διαμοιράσματος των ευπαθών μηχανημάτων ή των flag.
- Υποστήριξη πολλαπλών γλωσσών.
- Εύκολη ανάπτυξη στο «νέφος» (cloud) με χρήση docker ή direct.
- Ύπαρξη πολλαπλών οπτικών θεμάτων (Theme)

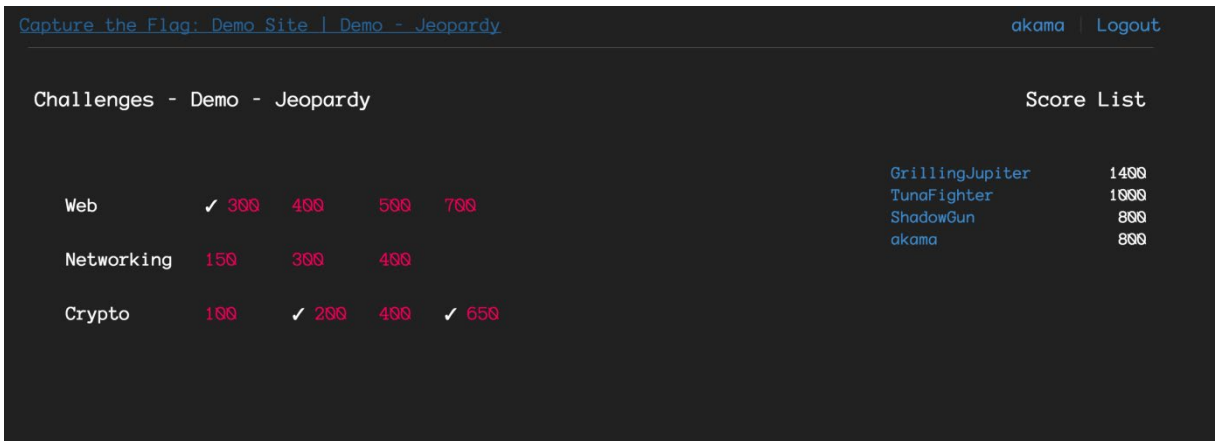
Όλα τα παραπάνω καθιστούν το RootTheBox μια capture the flag πλατφόρμα που παρέχει εκμάθηση του αντικειμένου του cyber security μέσω της «παιχνιδοποίησης» της μαθησιακής διαδικασίας παρά μια αυστηρά CTF πλατφόρμα, συνδυάζοντας μια videogame οπτική με ρεαλιστικά challenge που επαφίενται στον πραγματικό κόσμο και άπτονται στους τομείς του incident response, δικανική υπολογιστών (digital forensics), threat hunting και άλλα. Αξίζει να σημειωθεί ότι η συγκεκριμένη πλατφόρμα παρέχει τη δυνατότητα της προσθήκης ευπαθών μηχανών , challenges, εικονικών μηχανών μέσω ενός πλήρως καθοδηγούμενου τρόπου με τη χρήση της γραφικής διεπαφής χρήστη (GUI) καθιστώντας την πλατφόρμα ιδανική για υποστήριξη πολλαπλών challenge με εύκολο τρόπο.



Εικόνα 9.

2.3.2.6 *NightShade*

Η NightShade [16] capture the flag πλατφόρμα, είναι σχετικά νεότερη από τις υπόλοιπες που αναφέρθηκαν μέχρι στιγμής. Κάνει χρήση του Django web framework που ενθαρρύνει τη γρήγορη ανάπτυξη εφαρμογών σε αυτό ενώ χρησιμοποιεί ένα μείγμα της γλώσσας JavaScript για τη διεπαφή χρήστη με ταυτόχρονη χρήση της γλώσσας προγραμματισμού Python για να φιλοξενεί την εφαρμογή στο παρασκήνιο. Η πλατφόρμα αυτή είναι αρκετά απλή στη χρήση της και στον τρόπο που μπορεί κανείς να παραμετροποιήσει τα διάφορα challenge που θέλει να κάνει διαθέσιμα στους συμμετέχοντες. Τα ίδια τα challenge μπορούν να παραμετροποιηθούν απευθείας από την ιστοσελίδα της εφαρμογής μετά την πλήρη ανάπτυξη της πλατφόρμας. Όλα τα παραπάνω την καθιστούν ιδανική για όλους όσους αναζητούν ένα απλό και εμφανίσιμο σύστημα μου μπορεί να παραμετροποιηθεί και να τεθεί σε λειτουργία χωρίς να χρειάζεται ο διαχειριστής να προβεί σε αμέτρητες αλλαγές στη βάση των ρυθμίσεων της πλατφόρμας. Η ενδεδειγμένη ανάπτυξη της πλατφόρμας αναφέρει ιδανικά τη χρησιμοποίηση των διακομιστών Nginx και Gunicorn ως διακομιστές ιστού και υποδομής αντίστοιχα. Τα κύρια πλεονεκτήματα της NightShade CTF platform είναι η απλότητα της , η θεματική διεπαφή χρήστη, ο πίνακας βαθμολογιών για μεμονωμένους χρήστες αλλά και ομάδες, χωρίς να χρειάζονται επιπλέον παραμετροποιήσεις για την εύρυθμη λειτουργία της.



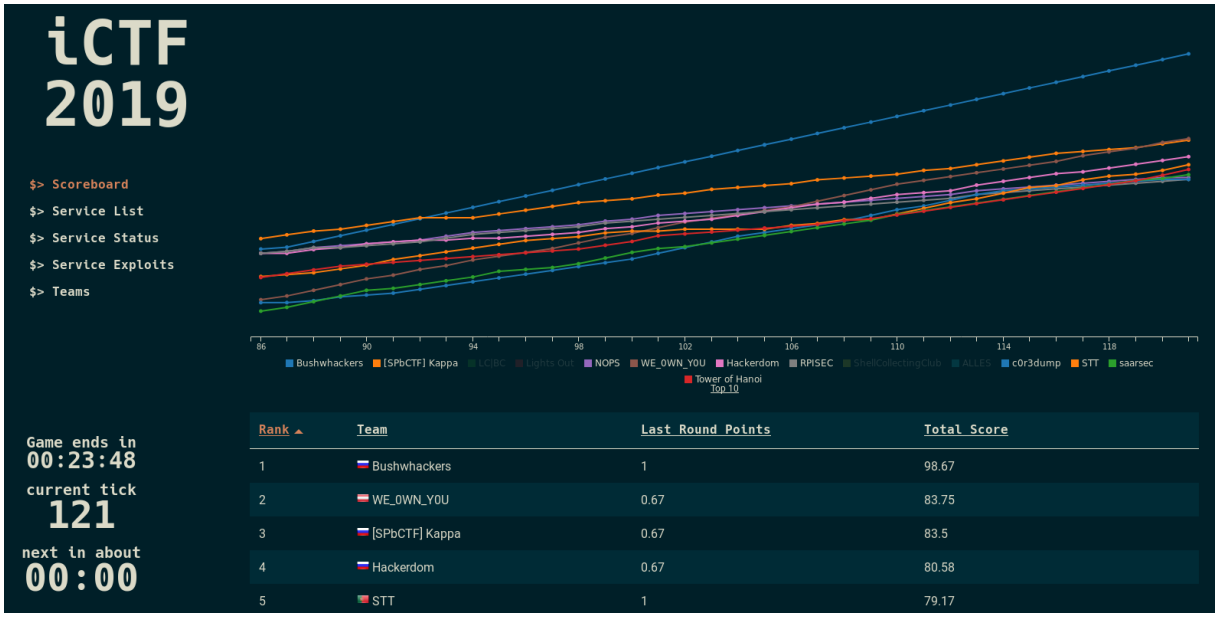
Εικόνα 10.

2.3.2.7 *iCTF Framework*

Το framework iCTF [17] , είναι άλλη μια πλατφόρμα επιθετικών – αμυντικών challenge που άπτονται στο αντικείμενο της κυβερνοασφάλειας. Η πλατφόρμα αυτή σχεδιάστηκε από το Πανεπιστημιακό κολέγιο Santa Barbara με στόχο να τρέχει τον διαγωνισμό iCTF που είναι ένας από τους μεγαλύτερους σε διάρκεια ενεργούς εκπαιδευτικούς διαγωνισμούς hacking. Οι προγραμματιστές αυτής της πλατφόρμας δημοσίευσαν τον κώδικα της στο κοινό έτσι ώστε να μπορεί κάθε ενδιαφερόμενος να την χρησιμοποιεί για να τρέχει τον δικό του capture the flag διαγωνισμό. Το συγκεκριμένο framework χωρίζεται σε τέσσαρα (4) επί μέρους δομικά στοιχεία:

- Βάση δεδομένων. Η βάση δεδομένων «ακολουθεί» την κατάσταση του παιχνιδιού. Κάνει χρήση του RESTful API και τρέχει στην εικονική μηχανή της βάσης δεδομένων.
- GameBot. Είναι ένα απαραίτητο συστατικό που είναι υπεύθυνο για την εξέλιξη του διαγωνισμού, ενώ ο ίδιος ο διαγωνισμός χωρίζεται σε χτύπους (ticks). Στην αρχή κάθε χτύπου, το GameBot αποφασίζει πια script πρέπει να εκτελεστούν από το ScriptBot και γράφει το πρόγραμμα εργασιών στην κεντρική βάση δεδομένων. Στη συνέχεια, εξάγει από τη βάση δεδομένων τα δεδομένα για τον προηγούμενο χτύπο (flag, έλεγχος υπηρεσιών) και υπολογίζει τη βαθμολογία που πρέπει να δοθεί σε κάθε ομάδα. Τα νέα βαθμολογικά αποτελέσματα αποθηκεύονται στη βάση έτσι ώστε να μπορούν να δημοσιευτούν στον πίνακα αποτελεσμάτων.
- ScriptBot. Το ScriptBot είναι υπεύθυνο για την εκτέλεση των script που δρομολογούνται από το GameBot. Το ScriptBot εξάγει τα script που επιλέγονται προς εκτέλεση από την κεντρική βάση δεδομένων και στη συνέχει τα εκτελεί.
- Router. Το συστατικό Router είναι υπεύθυνο για τη δρομολόγηση της δικτυακής κίνησης μεταξύ των ομάδων που συμμετέχουν στο διαγωνισμό κάνοντας χρήση της OpenVPN υπηρεσίας. Πιο συγκεκριμένα, σε κάθε ομάδα δίνεται μια εικονική μηχανή που λειτουργεί ως δρομολογητής για αυτή την ομάδα. Η δικτυακή κίνηση μεταξύ των ομάδων πρέπει να υποστεί ανωνυμοποίηση ώστε να αποτρέψει τις

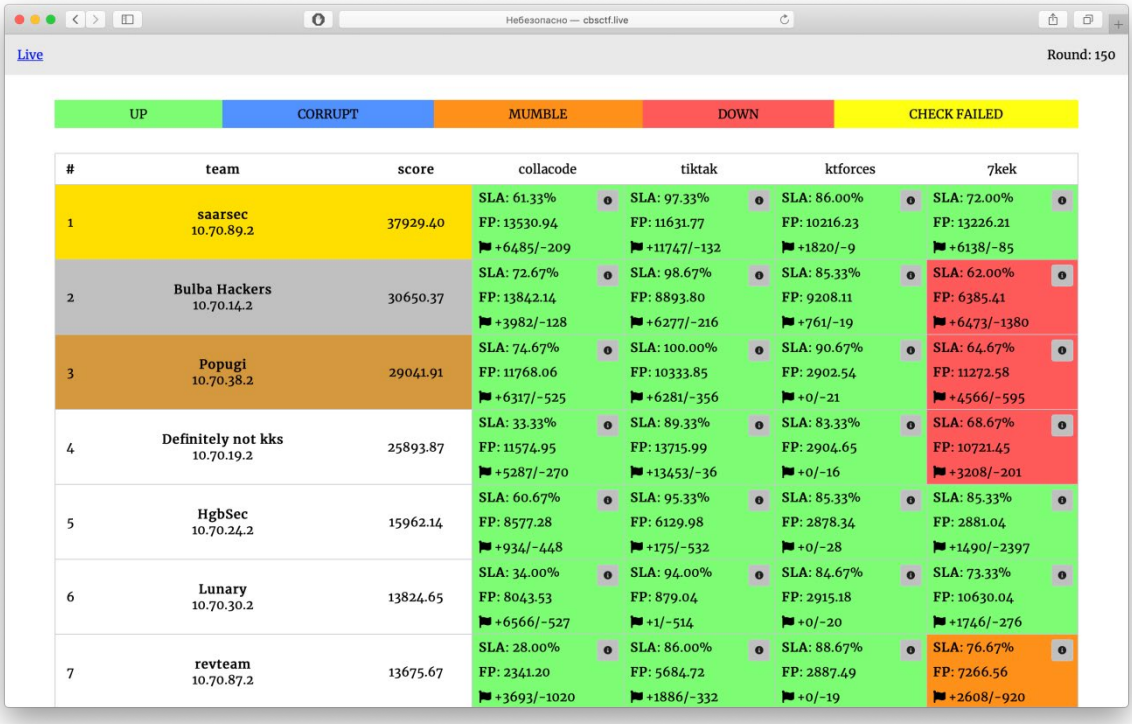
ομάδες από το να διακρίνουν την δικτυακή κίνηση που δημιουργείται από το ScriptBot από αυτή που δημιουργείται από κάθε ομάδα.



Εικόνα 11.

2.3.2.8 *ForcAD*

Η πλατφόρμα ForcAD [18] , είναι επίσης μια capture the flag πλατφόρμα, επιθετικού – αμυντικού προσανατολισμού, με εξαιρετικές δυνατότητες επεκτασιμότητας που υποστηρίζει πολυάριθμες ρυθμίσεις και συστήματα κάποια εκ των οποίων ενδεχομένως να μη συναντώνται συχνά σε άλλες capture the flag πλατφόρμες. Πέρα της βασικής λειτουργίας που αφορά την προσθήκη του flag στην εφαρμογή, των ατομικών αλλά και ομαδικών πινάκων βαθμολογιών και των έγχρωμων διεπαφών χρήστη, η συγκεκριμένη πλατφόρμα κάνει χρήση ενός μοναδικού χαρακτηριστικού ταξινόμησης των συμμετεχόντων βάση βαθμολογίας, το ELO σύστημα. Το ELO σύστημα ουσιαστικά υπολογίζει τη βαθμολογική διαφορά μεταξύ δύο ομάδων και η ομάδα με την υψηλότερη βαθμολογία ανταμείβεται με λιγότερους πόντους από την πλατφόρμα κατά την υποβολή κάποιου flag, ενώ η ομάδα με τη χαμηλότερη βαθμολογία ανταμείβεται με περισσότερους βαθμούς για την υποβολή της ίδιας σημαίας. Στα πιο τεχνικά χαρακτηριστικά της πλατφόρμας, το χτίσιμο της δεν εξαρτάται από ένα και μόνο δομικό στοιχείο αλλά από μικρότερα όπως τα ενσωματωμένα API που δίνουν μεγάλο έλεγχο στον διαχειριστή για παραμετροποίηση σε πολλούς τομείς όπως το σύστημα μέτρησης βαθμολογιών, τον έλεγχο των υποβληθέντων flag καθώς επίσης και έλεγχο συμφόρησης δικτυακής κίνησης.



Εικόνα 12.

2.3.2.9 *CTF01d*

Άλλη μια πλατφόρμα capture the flag , είναι η CTF01d [19] , επίσης προσανατολισμένη σε ένα αμυντικό-επιθετικό μοτίβο διαγωνισμών. Είναι στην πραγματικότητα ένα Python framework και παρουσιάζει εξαιρετική λεπτομέρεια τόσο στο σύνολο της όσο σε επιμέρους στοιχεία όπως στο σύστημα των score και τον πίνακα βαθμολογιών. Το σύστημα υποβολής των flag είναι αρκετά εύκολο στη χρήση του και επιτρέπει στον διαχειριστή της πλατφόρμας να εφαρμόσει κανονισμούς μειωμένης επιβράβευσης των ομάδων κατά την υποβολή του flag βάση χρόνου ενώ παράλληλα επιτρέπει την «κοστολόγηση» της εκάστοτε σημαίας έτσι ώστε να ταιριάζει στο βαθμό δυσκολίας του κάθε ευπαθούς συστήματος. Όπως προαναφέρθηκε η συγκεκριμένη πλατφόρμα είναι προσανατολισμένη σε ένα αμυντικό-επιθετικό μοτίβο διαγωνισμών capture the flag, πράγμα που σημαίνει ότι:

- Οι σημαίες επίθεσης της μιας ομάδας είναι οι σημαίες άμυνας της αντίπαλης ομάδας.
- Στο τέλος του διαγωνισμού αν κάποια ομάδα δεν έχει υποβάλει καμία σημαία επίθεσης τότε η αντίπαλη ομάδα επιβραβεύεται από την πλατφόρμα με την προσθήκη της βαθμολογίας μιας αμυντικής σημαίας στο συνολικό score της ομάδας και το αντίστροφο.

Η πλατφόρμα CTF01d είναι γραμμένη κατά κύριο λόγο σε γλώσσα προγραμματισμού C++ και υποστηρίζει την Αγγλική και την Ρώσικη γλώσσα. Η διεπαφή χρήστη είναι

αρκετά απλή και επεξηγηματική ενώ τα challenge του διαγωνισμού γίνονται εύκολα διαθέσιμα στους συμμετέχοντες, έχουν πολύ λεπτομέρεια στην περιγραφής τους και ο πίνακας των βαθμολογιών έχει πολύ λεπτομέρεια στους χρωματισμούς του. Στα θετικά στοιχεία αυτής της capture the flag πλατφόρμας συγκαταλέγεται το ότι επιτρέπει την εύκολη ανάπτυξη της καθώς κάνει χρήση docker τεχνολογίας.

Εικόνα 13.

2.4 Αδυναμίες Πλατφορμών Ανοιχτού και κλειστού κώδικα

2.4.1 Εμπορικές Πλατφόρμες

Στην ενότητα αυτή θα παρουσιάσουμε κάποιες από τις αδυναμίες των πιο γνωστών εμπορικών πλατφορμών κλειστού κώδικα.

2.4.1.1 *HackTheBox*

Ενώ το HackTheBox είναι μια από τις πιο γνώστες και πολυχρησιμοποιημένες πλατφόρμες εκπαίδευσης πάνω στο cyber security, φέρει και κάποια σημαντικά ελαττώματα. Είναι εμπορικού τύπου, οι χρήστες δεν μπορούν να εκπαιδευτούν πάνω σε όποιο μηχάνημα στόχο επιθυμούν, πάρα μόνο σε όσα είναι διαθέσιμα εκείνη τη στιγμή από την ίδια την πλατφόρμα. Για να εκπαιδευτεί κάποιος πάνω στα μηχανήματα-στόχους που έχουν αποσυρθεί, πρέπει να ανήκει στο premium πλάνο χρηστών. Επιπλέον, κάποιος χρήστης που ανήκει στο free πλάνο συνδρομής πέρα της μειωμένης δυνατότητας για επιλογή όποιου μηχανήματος επιθυμεί, είναι αναγκασμένος να εκπαιδεύεται πάνω στα διαθέσιμα από την πλατφόρμα μηχανήματα, ταυτόχρονα με τους υπόλοιπους χρήστες που επίσης ανήκουν στο ίδιο free πλάνο συνδρομής. Αυτό πρακτικά σημαίνει ότι πολλές φορές τα μηχανήματα μπορεί να μην είναι διαθέσιμα για διάφορους λόγους:

- Κάποιο exploit που χρησιμοποιήθηκε σε κάποιο service του μηχανήματος για να αποκτηθεί πρόσβαση στο μηχάνημα, έκανε το μηχάνημα μη προσπελάσιμο για όλους τους υπόλοιπους χρήστες.
- Δυνατότητα μόλις ενός reset στα μηχανήματα ανά μέρα. Σε περιπτώσεις όπως αυτή που περιγράφεται παραπάνω, όταν ένα μηχάνημα δεν είναι προσπελάσιμο συχνά πρέπει να γίνει reset από κάποιο χρήστη. Άρα η ύπαρξη ενός και μοναδικού reset δεν είναι αρκετή όταν το ίδιο μηχάνημα «χτυπούν» ταυτόχρονα πολλοί παίχτες.
- Τα μηχανήματα δεν επιδέχονται παραμετροποίησης, είναι ακριβώς όπως δημιουργήθηκαν εξαρχής και δεν αλλάζουν.
- Κάποιος παίχτης εσκεμμένα διέγραψε ή τροποποίησε κάποιο αρχείο ή σταμάτησε κάποιο service ώστε να επιβραδύνει την πρόοδο των υπόλοιπων παιχτών πάνω στο μηχάνημα.

2.4.1.2 *TryHackMe*

Στα μειονεκτήματα της πλατφόρμας TryHackMe επίσης συγκαταλέγεται το γεγονός ότι δεν είναι ανοιχτού κώδικα. Όπως και στο HackTheBox, έτσι και στο TryHackMe, κάποιος χρήστης για να αξιοποιήσει όλες τις δυνατότητες της πλατφόρμας θα πρέπει να καταβάλλει το ανάλογο αντίτιμο. Επιπλέον, και σε αυτή την περίπτωση οι αλλαγές που μπορούν να πραγματοποιήσουν οι χρήστες πάνω στα ήδη υπάρχον μηχανήματα-στόχους είναι από ελάχιστες ως μηδαμινές. Επιπλέον, τα μηχανήματα που μπορεί να δημιουργήσει και να ανεβάσει κάποιος χρήστης στην πλατφόρμα, δεν είναι διαθέσιμα προς όλους του χρήστες αλλά μόνο σε αυτούς που θα έχουν στην κατοχή τους τον κωδικό που θα τους δώσει ο δημιουργός του μηχανήματος, έτσι οι υπόλοιποι χρήστες ούτε θα μπορούν να εκπαιδευτούν πάνω στο συγκεκριμένο μηχάνημα αλλά ούτε θα έχουν γνώση της ύπαρξης του, περιορίζοντας αρκετά το εύρος μηχανημάτων προς χρήση πάνω στα οποία μπορούν να εκπαιδευτούν. Τέλος, από το TryHackMe απουσιάζει τελείως η δυνατότητα ενσωμάτωσης του API με άλλες υπηρεσίες για τη δημιουργία εξωτερικών πινάκων βαθμολογίας η ομαδικής επικύρωσης.

2.4.1.3 *Web Security Academy*

Ενώ πρόκειται για μια εξαιρετική πλατφόρμα εκπαίδευσης πάνω στον τομέα του cyber security, οι διαθέσιμοι τομείς είναι πολύ περιορισμένοι καθώς αφορούν αποκλειστικά την εκπαίδευση πάνω σε ιστοσελίδες και εφαρμογές ιστού. Έτσι, κάποιος χρήστης μπορεί να θέλει να εκπαιδευτεί πάνω σε ευπάθειες που αφορούν ευπάθειες συστήματος ή υπηρεσιών συστήματος δε θα έχει αυτή τη δυνατότητα.

2.4.1.4 *RootMe*

Επίσης πρόκειται για μια εξαιρετική πλατφόρμα εκπαίδευσης πάνω στο cyber security με πληθώρα επιλογών πάνω σε τομείς που κάποιος επιθυμεί να εκπαιδευτεί. Σημαντικό της μειονέκτημα είναι ότι δεν είναι ανοιχτού κώδικα, αρά κάθε χρήστης έχει τη δυνατότητα να εκπαιδευτεί πάνω σε ήδη διαθέσιμα challenge, δε μπορεί να τα τροποποιήσει ούτε και να δημιουργήσει τα δικά του.

2.4.2 Πλατφόρμες Ανοιχτού Κώδικα

Στην ενότητα αυτή θα παρουσιάσουμε κάποιες από τις αδυναμίες των πιο γνωστών πλατφορμών ανοιχτού κώδικα.

2.4.2.1 *OpenCTF*

Η πλατφόρμα OpenCTF εκτός από τα αρκετά πλεονεκτήματα της έχει και κάποια μειονεκτήματα. Από οπτικής άποψης, η διεπαφή χρήστη είναι αρκετά απλή κάτι που ενδεχομένως να την κάνει την ίδια την πλατφόρμα να φαίνεται απαρχαιωμένη. Επίσης, κάποια χαρακτηρίστηκα που υπάρχουν σε άλλες πλατφόρμες, απουσιάζουν από αυτήν όπως, δεν υπάρχει παρακολούθηση ομάδων (team monitoring) αλλά ούτε και ειδοποιήσεις βαθμολογίας που να εμφανίζονται σε πραγματικό χρόνο.

2.4.2.2 *TinyCTF*

Ένα από τα σημαντικότερα μειονεκτήματα αυτής της πλατφόρμας έγκειται στο γεγονός ότι η διεπαφή χρήστη δεν είναι τόσο απλοϊκή όπως συμβαίνει σε άλλες πλατφόρμες ενώ από άποψης απαιτούμενων πόρων για την εύρυθμη λειτουργιά της θα την χαρακτήριζε κανείς ελαφριάς ή μέσης ανάγκης ως προς την κατανάλωσης πόρων.

2.4.2.3 *PicoCTF*

Για αυτή την πλατφόρμα, το βασικό της πλεονέκτημα είναι και το μειονέκτημα της. Από πλευράς εξατομίκευσης η πλατφόρμα αυτή είναι πολύ ισχυρή και αυτό συμβαίνει λόγο της μεγάλης και πολύπλευρης φύσης της. Ενώ αυτό είναι ένα πολύ σημαντικό πλεονέκτημα έναντι των άλλων πλατφορμών, ταυτόχρονα καθιστά τη διαχείριση της ίδιας της πλατφόρμας αρκετά πολύπλοκη και ιδιαίτερα απαιτητική σε πόρους που καταλαμβάνει από το πληροφοριακό σύστημα.

2.4.2.4 *NightShade*

Η πλατφόρμα NightShade χαρακτηρίζεται ως μία πολύ απλοϊκή εφαρμογή όσο αφορά τη διαχείριση και παραμετροποίηση των challenge. Όμως αυτή της η απλοϊκότητα την κάνει να υστερεί σε κάποια χαρακτηριστικά όπως στην ύπαρξη επεκτάσιμων δυνατοτήτων που παρέχονται από το API της, στην ύπαρξη web shells και άλλα. Τέλος, όσα challenge περιλαμβάνουν exploitation απομακρυσμένων μηχανημάτων στόχων θα πρέπει να παραμετροποιηθούν ως προς τις ρυθμίσεις τους μεμονωμένα.

2.4.2.5 *FBCTF*

Η πλατφόρμα FBCTF έχει επίσης αρκετά μειονεκτήματα, αυτά είναι τα ακόλουθα:

- Πρόκειται για μια πολύ «βαριά» και απαιτητική πλατφόρμα από άποψη πόρων.
- Δεν υπάρχει λειτουργία ενσωματωμένου web shell που να επιτρέπει στα διάφορα challenges να γίνονται διαθέσιμα με απομακρυσμένο τρόπο ή να γίνονται προσπελάσιμα μέσα από την ίδια την πλατφόρμα.
- Τα challenges που περιλαμβάνουν ευπάθειες που είναι τρωτές με άμεσο και ευθύ τρόπο στο μηχάνημα-στόχο πρέπει να τα διαχειρίζεται κανείς μεμονωμένα.
- Η διεπαφή χρήση δεν περιλαμβάνει πολύ λεπτομέρεια και είναι αχρείαστα πολύπλοκη.
- Πολλές ρυθμίσεις εργασιών είναι συνδεδεμένες με διάφορες χώρες σε ένα παγκόσμιο incident-response στυλ κάτι που μπορεί να μη ταιριάζει με όλα τα διαφορετικά θέματα του εκάστοτε διαγωνισμού.

2.4.2.6 *iCTF*

Και το iCTF capture the flag platform παρουσιάζει κάποια μειονεκτήματα ενώ βρίσκεται πολλά χρόνια μεταξύ των πιο γνωστών πλατφορμών για τέτοιους διαγωνισμούς. Ενώ δεν είναι πολύ απαιτητικό από άποψη υπολογιστικών πόρων όταν δεν υπάρχουν πολύ συμμετέχοντες στο event ή πολύς φόρτος στο σύστημα, όταν οι χρήστες είναι αρκετοί τότε οι ανάγκες τις πλατφόρμας για πόρους αυξάνονται εκθετικά κάτι που κάνει την πλατφόρμα μη ιδανική για εξατομικευμένα τοπικά challenge όπου ο αριθμός των παικτών αναμένεται να είναι μεγάλος. Άλλο είναι μειονέκτημα της είναι το στυλ του διαγωνισμού, attack-defense, που υποστηρίζει. Αυτό το στυλ μπορεί να μην καλύπτει πλήρως τις ανάγκες όλων των συμμετεχόντων. Τέλος, η ίδια η δομή της πλατφόρμας και τα δομικά στοιχεία από τα οποία αποτελείται, database-gamebot-scriptbot-router, είναι αρκετά πολύπλοκα στη λειτουργία τους με αποτέλεσμα οποιαδήποτε αλλαγή στην πλατφόρμα να είναι αρκετά δύσκολη διότι μπορεί να κάνει την πλατφόρμα μη λειτουργική.

2.4.2.7 *ForcAD*

Η ForcAD πλατφόρμα παρουσιάζει επίσης κάποια μειονεκτήματα. Το είδος challenge attack-defense μπορεί να μην καλύπτει τις ανάγκες κάθε χρήστη που συμμετέχει στο διαγωνισμό. Επιπλέον, ενώ καινοτόμο, το βασισμένο στο ELO scoring system της πλατφόρμας κάποιες φορές ενδεχομένως να μην είναι τόσο δίκαιο για τις ομάδες που συμμετέχουν στο διαγωνισμό. Για παράδειγμα, μια ομάδα που αποτελείται από πολύ καλούς παίχτες και βρίσκεται ψηλά στον πίνακα των βαθμολογιών, αν καταφέρει να κατακτήσει τις σημαίες ενός πολύ δύσκολου μηχανήματος-στόχου, τότε οι βαθμοί που λάβει η ομάδα ως ανταμοιβή, θα είναι αρκετά μειωμένοι επειδή το ELO system ανταμείβει τις ομάδες στις υψηλότερες θέσεις με μειωμένους βαθμούς.

2.4.2.8 *RootTheBox*

Και η πλατφόρμα RootTheBox παρά τα πολλά της πλεονεκτήματα, πάσχει από κάποια μειονεκτήματα. Στα μειονεκτήματα της πλατφόρμας συγκαταλέγεται η αυξημένη ζήτηση από την εφαρμογή, των πόρων του συστήματος που την φιλοξενεί. Επιπλέον, δεν παρέχονται από τον δημιουργό της πλατφόρμας επαρκείς οδηγίες ή υποστήριξη για πολλαπλή ταυτόχρονη ανάπτυξη διακομιστών εγγενώς, επομένως ενδέχεται η ανάπτυξη μεγάλων διαγωνισμών με τη χρήση αυτής της πλατφόρμας να δημιουργήσει προβλήματα.

2.4.2.9 *CTF01d*

Η CTF01d πάσχει επίσης από κάποια μειονεκτήματα. Και σε αυτή την περίπτωση το στυλ του διαγωνισμού που υποστηρίζει αφορά το μοτίβο Attack-Defense που μπορεί να μη καλύπτει την πλειοψηφία όλων των συμμετεχόντων. Επιπλέον, η συγκεκριμένη πλατφόρμα διαθέτει τεράστιο αποθετήριο κώδικα λόγω των πολλών χαρακτηριστικών που προσφέρει, κάτι που όμως λειτουργεί αρνητικά σε περιπτώσεις που κάποιος διαχειριστής της πλατφόρμας αποφασίσει να κάνει αλλαγές σε επίπεδο κώδικα στην εφαρμογή καθώς οποιαδήποτε αλλαγή στον κώδικα, μπορεί να προκαλέσει αστάθεια στην πλατφόρμα στο σύνολο της. Άλλο μειονέκτημα της είναι η έλλειψη εκτεταμένης τεκμηρίωσης από τον δημιουργό της κάτι που καθιστά πολύ δύσκολο τον γενικό έλεγχο του συστήματος. Τέλος, σημαντικό μειονέκτημα χαρακτηρίζεται και η έλλειψη υποστήριξης σε παραπάνω από δύο γλώσσες καθώς μέχρι στιγμής υπάρχει υποστήριξη μόνο για τις γλώσσες της Αγγλικής και της Ρώσικης.

2.5 Συνοψίζοντας

Σε αυτή την ενότητα έγινε περιγραφή όλων των μειονεκτημάτων κάθε πλατφόρμας ανοιχτού αλλά και κλειστού κώδικα. Ως προς τις πλατφόρμες ανοιχτού κώδικα μπορεί

κανείς να συμπεράνει από την ανάλυση που έγινε νωρίτερα ότι όλες τους έχουν μειονεκτήματα τα οποία είναι σημαντικά και τις καθιστούν μη ιδανικές επιλογές για κάθε ενδιαφερόμενο που θα ήθελε να επιλέξει κάποια πλατφόρμα ανοιχτού κώδικα για να φιλοξενήσει το δικό του διαγωνισμό capture the flag.

Συνοψίζοντας, τα μειονεκτήματα αφορούν τις ακόλουθες κατηγορίες:

- Έλλειψη ελέγχου προόδου ομάδων μέσω πινάκων προβολής βαθμολογίας
- Έλλειψη δυνατότητας προβολής βαθμολογίας σε πραγματικό χρόνο
- Πολύπλοκη διεπαφή χρήστη
- Μεγάλο αποθετήριο κώδικα πλατφόρμας που δυσχεραίνει την εύκολη παραμετροποίηση της
- Έλλειψη επεκτάσιμων δυνατοτήτων που παρέχονται από τα API των πλατφορμών
- Ύπαρξη συγκεκριμένου μοτίβου διαγωνισμού (attack-defense)
- Έλλειψη δυνατότητας διαχείρισης των μηχανημάτων στόχων (power up/power off) μέσω της πλατφόρμας CTF
- Έλλειψη επαρκών οδηγιών όσο αφορά τη δυνατότητα παραμετροποίησης της πλατφόρμας
- Έλλειψη υποστήριξης πληθώρας γλωσσών

Λαμβάνοντας υπόψη όλες τις παραπάνω ελλείψεις που εντοπίστηκαν κατά την ανάλυση και περιγραφή των πιο γνωστών open source platform, κληθήκαμε να επιλέξουμε την πλατφόρμα που παρουσιάζει τις λιγότερες ελλείψεις σε σχέση με τις υπόλοιπες και να τη χρησιμοποιήσουμε στη συνέχεια της έρευνας μας ώστε να τη βελτιώσουμε και να την αναπτύξουμε περαιτέρω με στόχο η τροποποιημένη μορφή της να αποτελέσει ιδανική επιλογή για οποιονδήποτε επιθυμεί να παρέχει τους δικούς τους διαγωνισμούς CTF συμβάλλοντας κατά αυτό τον τρόπο στην εκπαίδευση των συμμετεχόντων στο εξειδικευμένο αντικείμενο της κυβερνοασφάλειας.

Βάση των παραπάνω, τις λιγότερες ελλείψεις παρουσιάζει η πλατφόρμα ανοιχτού κώδικα RootTheBox. Μοναδική της ομοιότητα με τις ελλείψεις που παρουσιάζονται σε άλλες πλατφόρμες είναι ότι είναι κάπως απαιτητική από άποψη πόρων συστήματος διότι τα μηχανήματα-στόχοι που προστίθενται σε αυτή είναι κατά κύριο λόγο εικονικές μηχανές. Οι εικονικές μηχανές, αν και μπορεί κανείς να τροποποιήσει τις απαιτήσεις τους σε κάποιο βαθμό, είναι ιδιαίτερα απαιτητικές αν σκεφτεί κανείς ότι κατ' ελάχιστο μια εικονική μηχανή δεσμεύει οπωσδήποτε ένα πυρήνα επεξεργαστή (1 CPU Core) και ένα ποσοστό προσωρινής μνήμης (RAM) από το μηχάνημα που την εκκινεί. Άρα αν κάποιος θελήσει να διαθέσει στους συμμετέχοντες ακόμα και ένα πολύ μικρό αριθμό challenge που τρέχουν πάνω σε εικονικές μηχανές τότε γίνεται εύκολα αντιληπτό ότι θα πρέπει να έχει στην κατοχή του ένα πολύ υψηλών δυνατοτήτων μηχάνημα, άρα και αρκετά ακριβό από οικονομικής άποψης.

Για αυτό το λόγο, επιλέχθηκε και τροποποιήθηκε σε επίπεδο κώδικα η πλατφόρμα RootTheBox ώστε να μπορεί να συνεργαστεί κατάλληλα με τεχνολογίες λιγότερο απαιτητικές από άποψης υπολογιστικών πόρων συστήματος, όπως η τεχνολογία docker [20].

Πίνακας Σύγκρισης Βασικότερων Χαρακτηριστικών Πλατφόρμας

Πλατφόρμες	Τύπος Πλατφόρμας	Πολυπλοκότητα διεπαφής χρήστη	Συγκεκριμένο Μοτίβο Challenge	Επαρκείς Οδηγίες Παραμετροποίησης	Τροποποίηση/Δημιουργία Challenge	Πίνακας παρακολούθησης ομάδων	Αυξημένοι πόροι συστήματος	Υποστήριξη Πολλαπλών Γλωσσών
HackTheBox	Εμπορική	ΟΧΙ	ΟΧΙ	ΟΧΙ	ΟΧΙ	ΝΑΙ	Ν/Α	ΝΑΙ
TryHackMe	Εμπορική	ΟΧΙ	ΟΧΙ	ΟΧΙ	ΟΧΙ	ΝΑΙ	Ν/Α	ΝΑΙ
RootMe	Εμπορική	ΟΧΙ	ΟΧΙ	ΟΧΙ	ΟΧΙ	ΝΑΙ	Ν/Α	ΟΧΙ
Web Security Academy	Εμπορική	ΟΧΙ	ΝΑΙ	ΟΧΙ	ΟΧΙ	ΝΑΙ	Ν/Α	ΟΧΙ
OpenCTF	Ανοιχτού κώδικα	ΟΧΙ	ΟΧΙ	ΝΑΙ	ΝΑΙ	ΟΧΙ	ΟΧΙ	ΝΑΙ
TinyCTF	Ανοιχτού κώδικα	ΝΑΙ	ΟΧΙ	ΝΑΙ	ΝΑΙ	ΝΑΙ	ΟΧΙ	ΝΑΙ
PicoCTF	Ανοιχτού κώδικα	ΝΑΙ	ΟΧΙ	ΝΑΙ	ΝΑΙ	ΝΑΙ	ΝΑΙ	ΝΑΙ
NightShade	Ανοιχτού κώδικα	ΟΧΙ	ΟΧΙ	ΝΑΙ	ΝΑΙ	ΝΑΙ	ΟΧΙ	ΝΑΙ
FBCTF	Ανοιχτού κώδικα	ΝΑΙ	ΟΧΙ	ΝΑΙ	ΝΑΙ	ΝΑΙ	ΝΑΙ	ΝΑΙ
RootTheBox	Ανοιχτού κώδικα	ΟΧΙ	ΟΧΙ	ΟΧΙ	ΝΑΙ	ΝΑΙ	ΝΑΙ	ΝΑΙ
CTF01d	Ανοιχτού κώδικα	ΟΧΙ	ΝΑΙ	ΟΧΙ	ΝΑΙ	ΝΑΙ	ΟΧΙ	ΟΧΙ
ForcAD	Ανοιχτού κώδικα	ΟΧΙ	ΟΧΙ	ΝΑΙ	ΝΑΙ	ΝΑΙ	ΟΧΙ	ΝΑΙ
iCTF	Ανοιχτού κώδικα	ΟΧΙ	ΝΑΙ	ΟΧΙ	ΝΑΙ	ΝΑΙ	ΟΧΙ	ΝΑΙ

Κεφάλαιο 3
Προτεινόμενη Λύση

Σε αυτό το κεφάλαιο θα γίνει αναλυτική περιγραφή του τρόπου λειτουργίας της τροποποιημένης πλατφόρμας, των διαδικασιών τροποποίησης, σε επίπεδο κώδικα, της πλατφόρμας RootTheBox, καθώς και όλων των νέων χαρακτηριστικών που προστέθηκαν ώστε να διευκολυνθεί η μαθησιακή διαδικασία των συμμετεχόντων μέσω της «παιχνιδοποιημένης» εκπαίδευσης που προσφέρει η συγκεκριμένη πλατφόρμα.

Πιο συγκεκριμένα, όπως προαναφέρθηκε, η opensource πλατφόρμα RootTheBox, για τις ανάγκες της παρούσας διατριβής, τροποποιήθηκε σε επίπεδο κώδικα σε μεγάλο βαθμό ώστε να παρέχει σε κάθε συμμετέχοντα της παιχνιδοποιημένης μαθησιακής διαδικασίας τις απαραίτητες συνθήκες εκμάθησης αλλά και τα απαραίτητα εργαλεία. Επιπλέον, μέσω της τροποποίησης κώδικα έγινε προσπάθεια μείωσης των υπολογιστικών πόρων που ζητά η πλατφόρμα από το σύστημα που την φιλοξενεί καθώς στην αρχική της μορφή τα μηχανήματα – στόχοι ήταν κυρίως εικονικές μηχανές που από μόνες τους είναι ιδιαίτερα απαιτητικές από άποψη πόρων, πόσο μάλλον όταν είναι και αριθμητικά πολλές στο σύνολο τους. Στην τελική της μορφή η πλατφόρμα κάνει πλέον χρήση τεχνολογίας docker μειώνοντας έτσι αισθητά τις ανάγκες για πόρους , των μηχανημάτων – στόχων , που ζητούν από το σύστημα που φιλοξενεί την εφαρμογή.

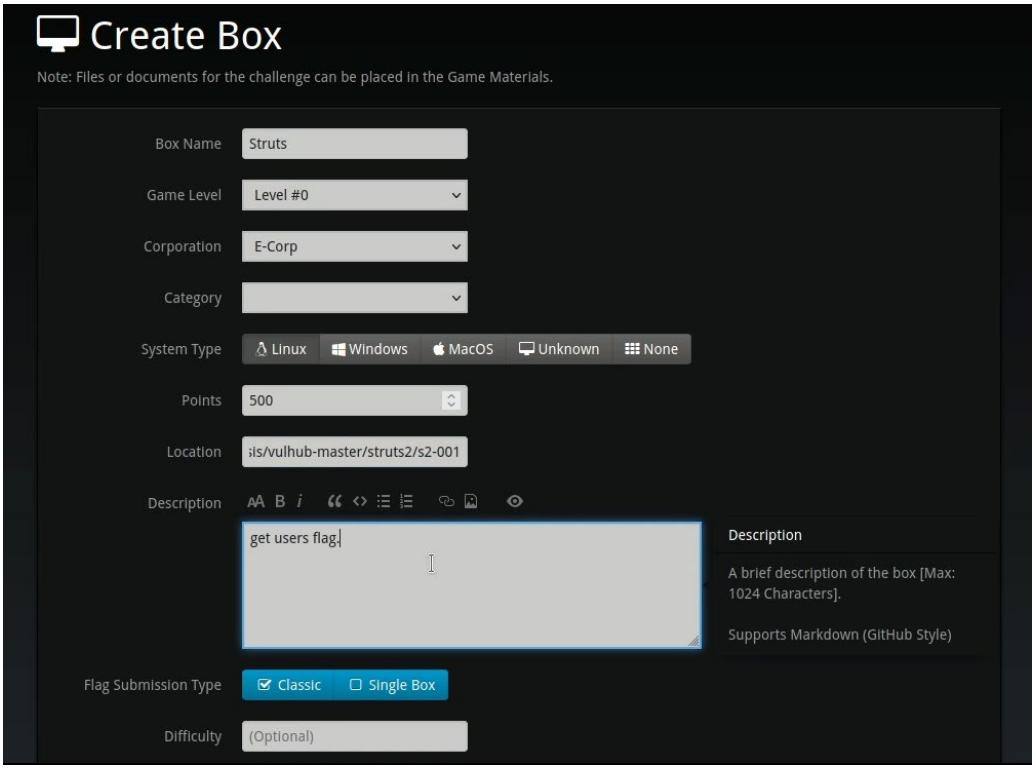
3.1 Περιγραφή Λειτουργίας Πλατφόρμας

Στην ενότητα αυτή θα γίνει αναλυτική περιγραφή του τρόπου λειτουργίας της τροποποιημένης πλατφόρμας RootTheBox. Η περιγραφή περιλαμβάνει όλη τη διαδικασία δημιουργίας, από τον διαχειριστή του διαγωνισμού, από την αρχή, του εκάστοτε challenge, μέχρι τον τρόπο που κάθε συμμετέχοντας στον διαγωνισμό εγγράφεται στην πλατφόρμα και τελικά ξεκινάει το μηχάνημα-στόχο πάνω στο οποίο επιθυμεί να εκπαιδευτεί αλλά και τον τρόπο με τον οποίο γίνεται η προσπέλαση του μηχανήματος από τον κάθε χρήστη.

3.1.1 Ενέργειες Διαχειριστή Πλατφόρμας

Ο διαχειριστής της πλατφόρμας αφού δημιουργήσει τα δικά του αναγνωριστικά εισόδου (administrative credentials) τα χρησιμοποιεί και κάνει log in στην πλατφόρμα. Η πλατφόρμα διαθέτει διάφορες επιλογές, επιλέγει “Create” για να δημιουργήσει το challenge που θέλει να κάνει διαθέσιμο στους συμμετέχοντες του διαγωνισμού. Στο μενού “Create” υπάρχουν επιπλέον επιλογές, επιλέγει “New Box”. Στο νέο μενού που εμφανίζεται υπάρχουν διάφορα πεδία προς συμπλήρωση όπως:

- Box Name
- Game Level
- Corporation
- Category
- System Type
- Points
- Location
- Description
- Flag Submission Type
- Difficulty

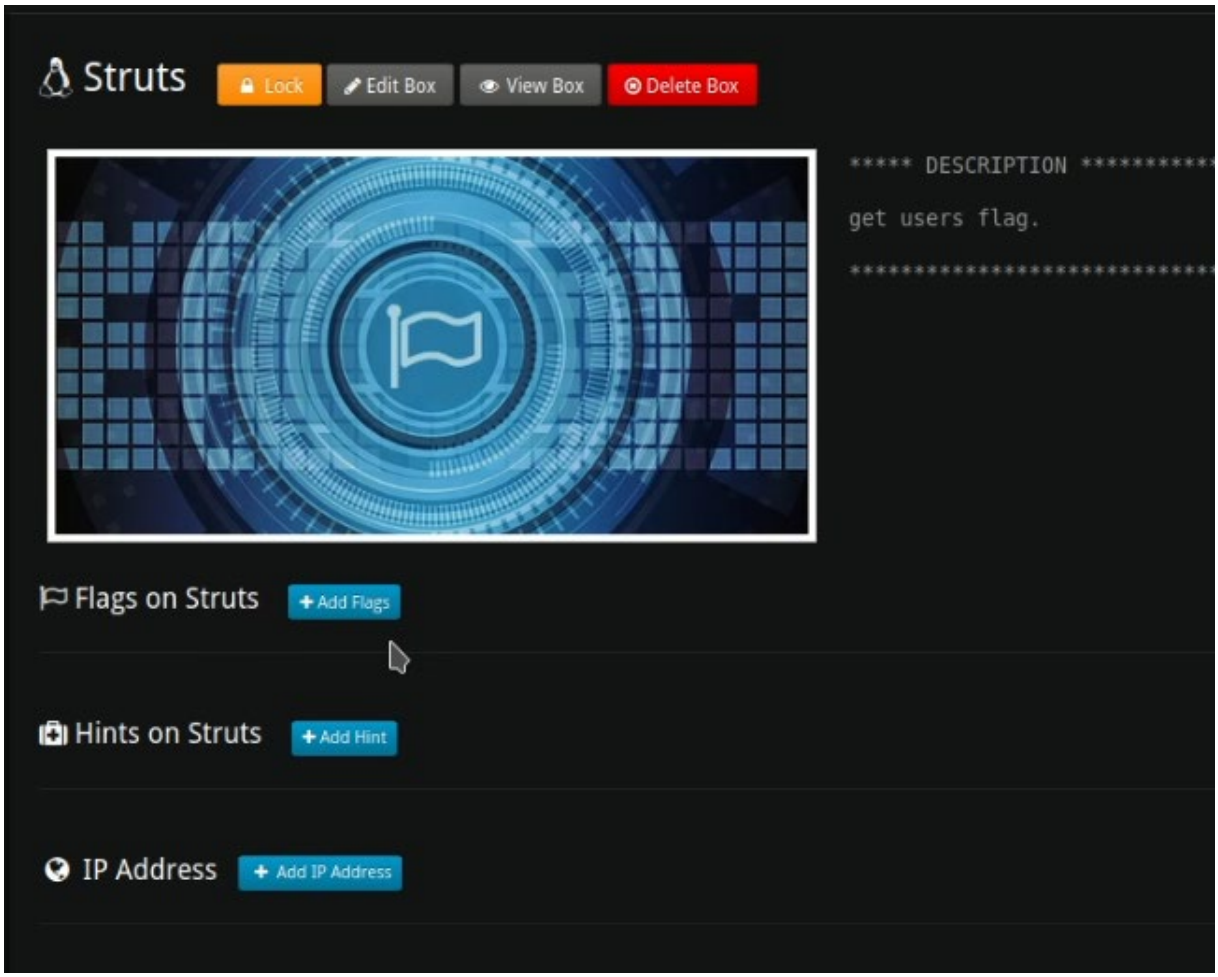


Εικόνα 14.

Αφού συμπληρώσει τα απαιτούμενα πεδία επιλέγει το κουμπί “Create Box” για να δημιουργήσει το νέο μηχάνημα στο μενού της πλατφόρμας. Με το πάτημα του

παραπάνω κουμπιού, η πλατφόρμα τον οδηγεί στο μενού του νέο μηχανήματος που δημιούργησε μόλις, όπου πρέπει να συμπληρώσει τα ακόλουθα πεδία:

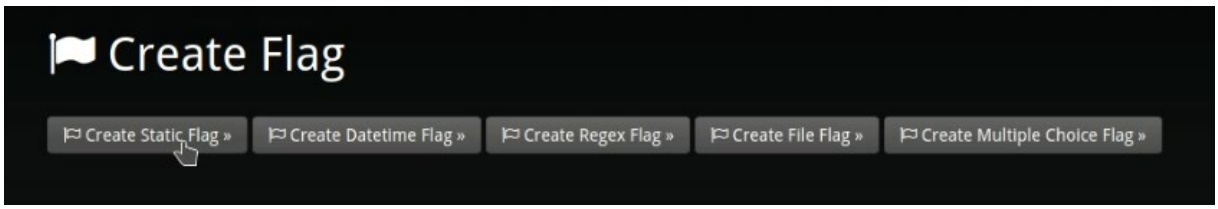
- Flags (Υποχρεωτικό πεδίο)
- Hints (Προαιρετικό πεδίο)
- IP Address (Υποχρεωτικό πεδίο πριν την τροποποίηση του κώδικα της πλατφόρμας, ώστε να γνωρίζουν οι συμμετέχοντες την IP διεύθυνση του μηχανήματος – στόχου. Με τις τροποποιήσεις που έχουν γίνει αυτό το πεδίο πλέον δεν είναι υποχρεωτικό προς συμπλήρωση)



Εικόνα 15.

Στη συνέχεια επιλέγει “Flags” και η πλατφόρμα τον μεταφέρει σε ένα νέο μενού που αφορά την δημιουργία του “Flag”. Και εδώ υπάρχουν πολλές επιλογές όπως:

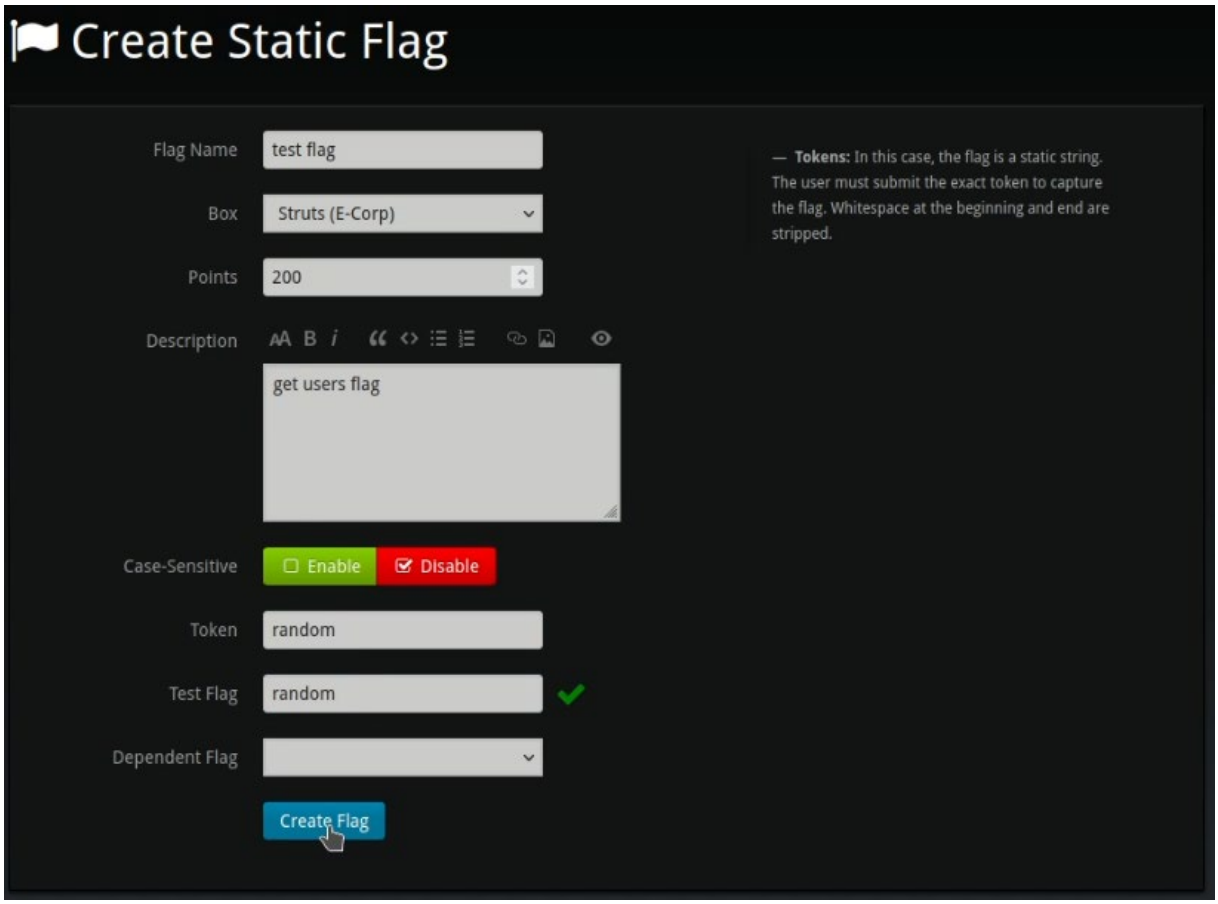
- Create Static Flag
- Create DateTime Flag
- Create Regex Flag
- Create File Flag
- Create Multiple Choice Flag



Εικόνα 16.

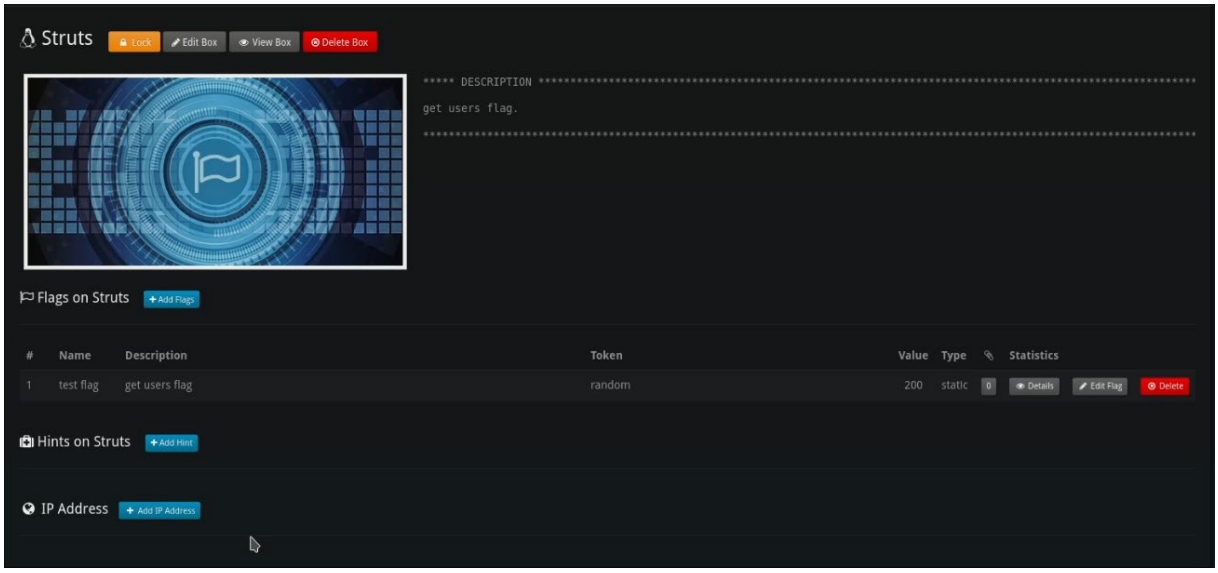
Για τις ανάγκες της παρούσας διατριβής θα δημιουργήσουμε στατικά Flag, οπότε ο διαχειριστής επιλέγει “Create Static Flag” και οδηγείται σε μία νέα σελίδα με επιπλέον πεδία προς συμπλήρωση, που είναι τα ακόλουθα:

- Flag Name
- Box
- Points
- Description
- Case Sensitive
- Token
- Test Flag
- Dependent Flag



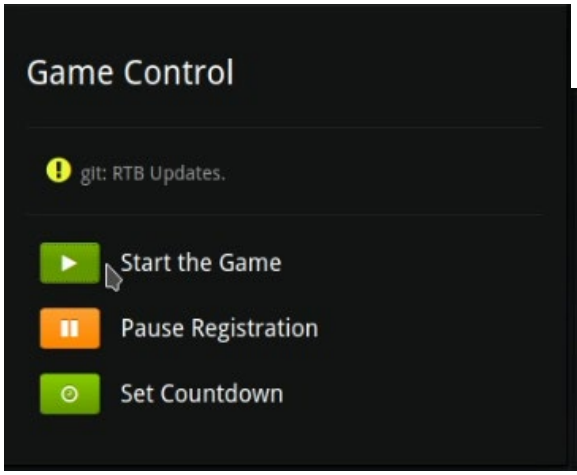
Εικόνα 17.

Αφού συμπληρώσει τα απαραίτητα πεδία επιλέγει το κουμπί “Create Flag”. Σε αυτό το σημείο το flag του μηχανήματος-στόχου είναι έτοιμο όπως φαίνεται στην παρακάτω εικόνα.

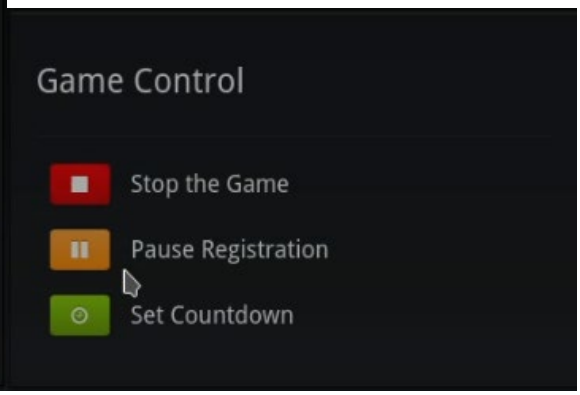


Εικόνα 18.

Τέλος, από το μενού στην κορυφή της πλατφόρμας, ο διαχειριστής επιλέγει το εικονίδιο home για να μεταβεί στην αρχική σελίδα του administration panel και στη συνέχεια από το μενού “Game Control”, στα αριστερά, επιλέγει “Start the Game”.



Εικόνα 19.



Εικόνα 20.

Στο σημείο αυτό το challenge είναι ενεργοποιημένο και γίνεται διαθέσιμο σαν επιλογή στο μενού επιλογών κάθε χρήστη της πλατφόρμας.

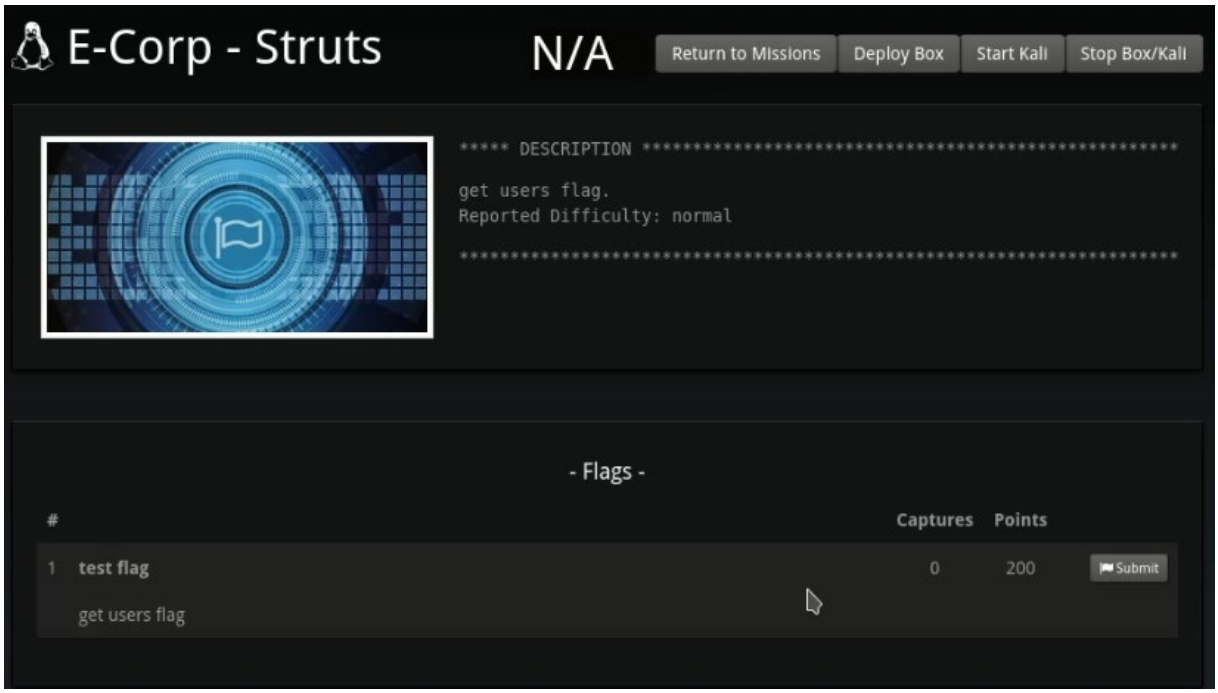
3.1.2 Ενέργειες Συμμετέχοντα Πλατφόρμας

Ο συμμετέχον του διαγωνισμού, αφού εγγραφεί στην πλατφόρμα στην συνέχεια εισέρχεται στην εφαρμογή κάνοντας login. Όπως εξηγήσαμε παραπάνω, στις ενέργειες του διαχειριστή, όταν επιλέξει “Start The Game” τότε το challenge γίνεται διαθέσιμο

στους υπόλοιπους user της πλατφόρμας (E-Corp – Struts στην περίπτωση μας). Κατά την είσοδο του στην εφαρμογή ο χρήστης στο αριστερό μέρος της πλατφόρμας στο πλάισιο “Player Mission Progress” μπορεί να διακρίνει τα διαθέσιμα challenge.

Εικόνα 21.

Επιλέγει το challenge που τον ενδιαφέρει και μεταφέρεται σε ένα νέο παράθυρο στον περιηγητή του, αυτό το παράθυρο αφορά το μηχάνημα-στόχο που επέλεξε.



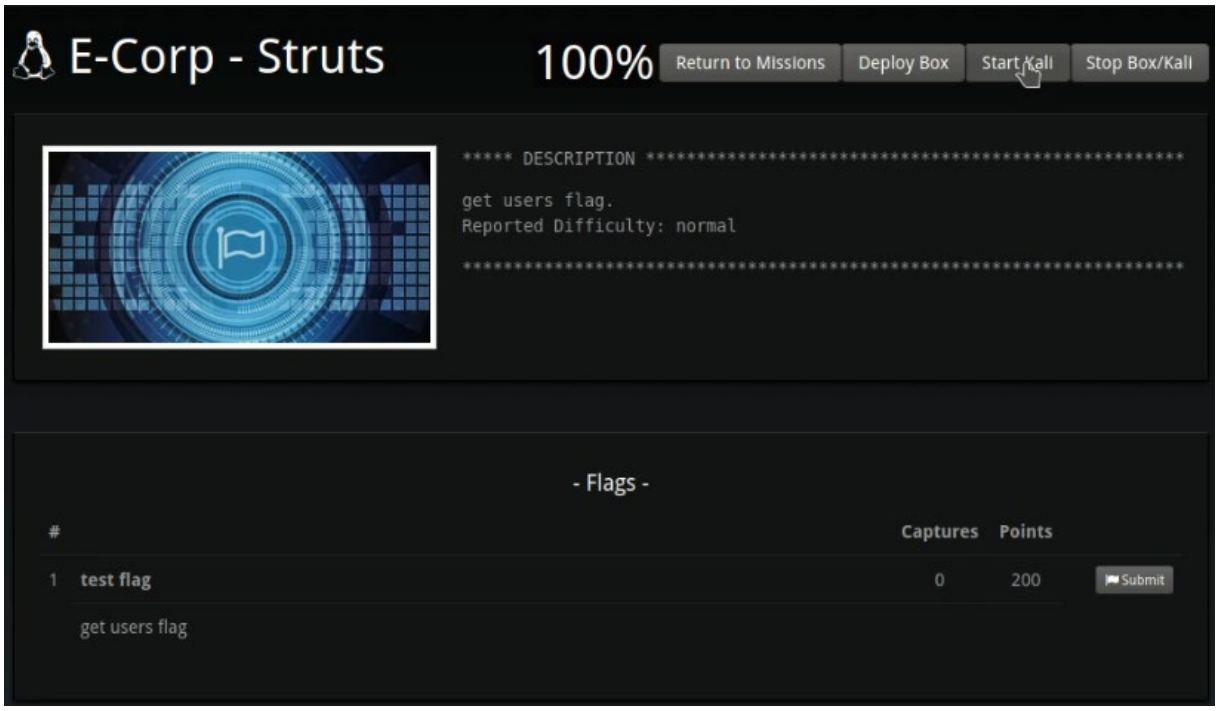
Εικόνα 22.

Στο νέο αυτό παράθυρο υπάρχουν οι ακόλουθες επιλογές:

- Return to Missions
- Deploy Box
- Start Kali
- Stop Box/Kali

Ο χρήστης επιλέγει “Deploy Box” ώστε η πλατφόρμα να ξεκινήσει το ανάλογο μηχάνημα-στόχο στο σύστημα. Με το που επιλέξει το συγκεκριμένο κουμπί τότε εμφανίζεται ένας ποσοστιαίος μετρητής που δείχνει την πρόοδο εκκίνησης του μηχανήματος-στόχου στο σύστημα. Όταν ο μετρητής γίνει 100% τότε το μηχάνημα-

στόχος είναι φορτωμένο στο σύστημα και είναι έτοιμο για προσπέλαση. Επόμενο βήμα του χρήστη είναι να εκκινήσει το λειτουργικό σύστημα Kali που διαθέτει όλα τα απαραίτητα penetration testing εργαλεία που χρειάζεται ώστε να αρχίσει να επιτίθεται στο μηχάνημα-στόχο.

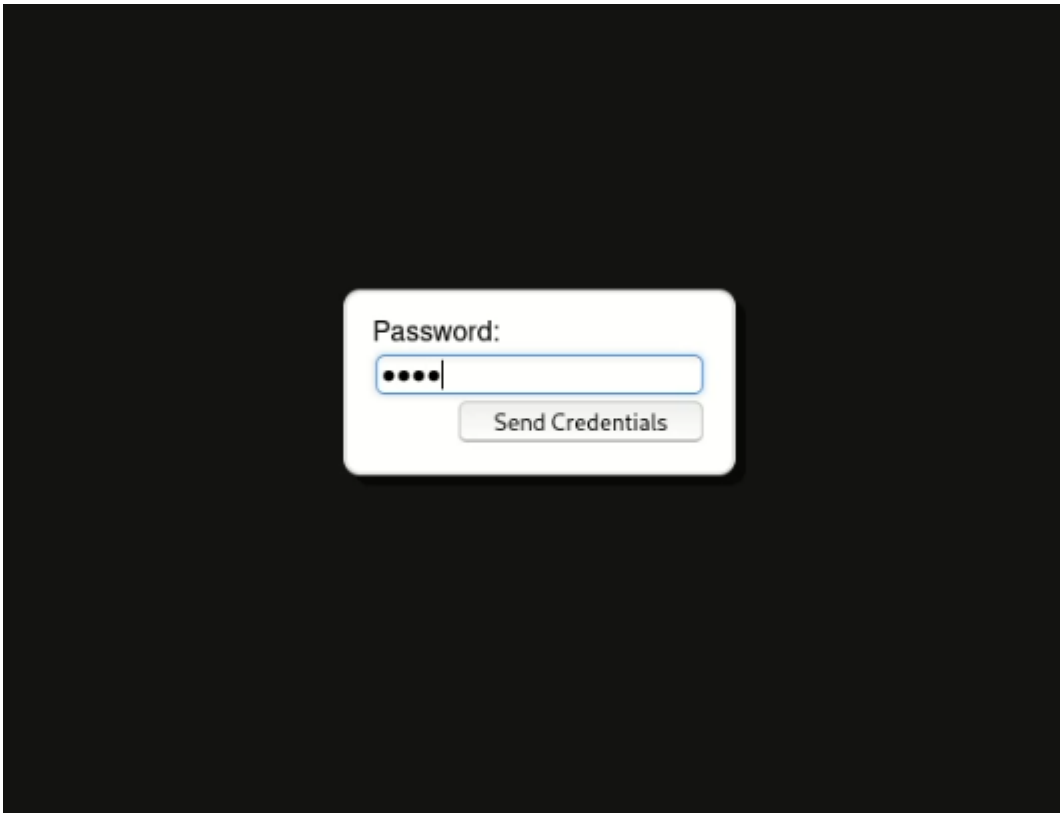


Εικόνα 23.

Με το που επιλέξει ο χρήστης το κουμπί “Start Kali”, τότε η πλατφόρμα ανοίγει στον περιηγητή του ένα νέο παράθυρο εισαγωγής συνθηματικών, αυτό του λειτουργικού συστήματος Kali Linux.

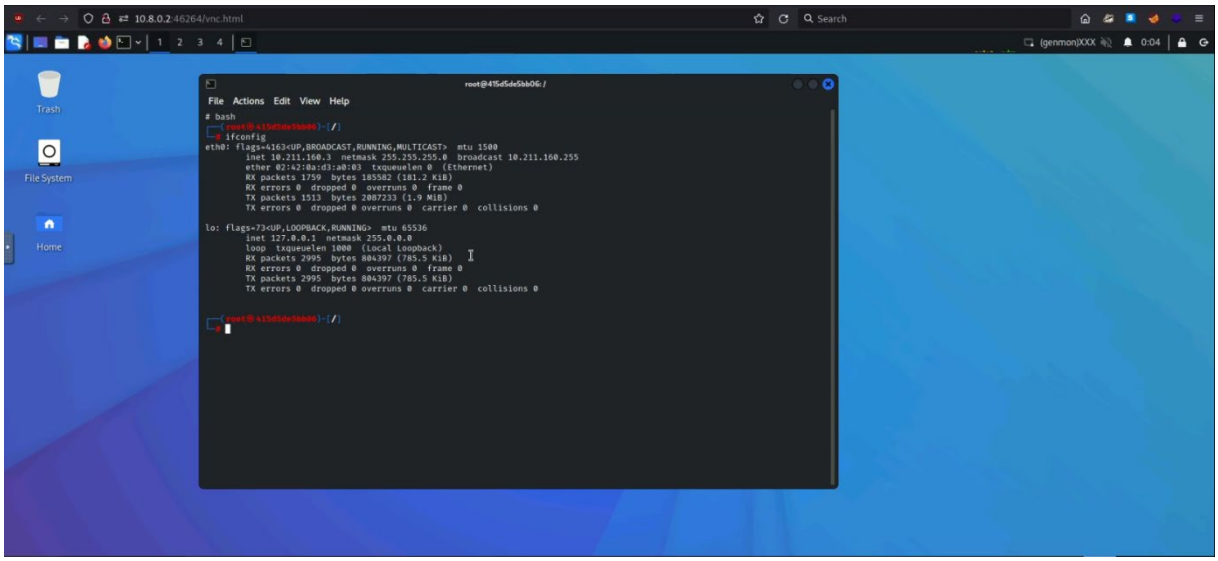
Εικόνα 24.

Στην συνέχεια επιλέγει “Connect” και εμφανίζεται το πεδίο εισαγωγής κωδικού του λειτουργικού συστήματος Kali Linux.



Εικόνα 25.

Εισάγει τον κωδικό πρόσβασης του συστήματος και επιλέγει “Send Credentials” για να κάνει login στο λειτουργικό σύστημα Kali Linux.



Εικόνα 26.

3.2 Γενική Περιγραφή Αλλαγών

Στην ενότητα αυτή θα παρουσιαστούν με συνοπτικό τρόπο όλες οι αλλαγές που έγιναν στην πλατφόρμα RootTheBox σε επίπεδο κώδικα.

1. Προσθήκη πεδίου στον λογαριασμό του διαχειριστή στη σελίδα δημιουργίας των μηχανημάτων-στόχων (πεδίο “Location”).
2. Δημιουργία Flask εφαρμογής η οποία τρέχει παράλληλα με την πλατφόρμα RootTheBox και διαχειρίζεται όλα τα αιτήματα για εκκίνηση, τερματισμό κ.α των μηχανημάτων-στόχων καθώς επίσης και του λειτουργικού συστήματος Kali Linux.
3. Δημιουργία κουμπιού “Deploy Box” στη σελίδα κάθε διαθέσιμου challenge που είναι υπεύθυνο για την εκκίνηση του κάθε μηχανήματος-στόχου από τους χρήστες.
4. Δημιουργία κουμπιού “Start Kali” στη σελίδα κάθε διαθέσιμου challenge που είναι υπεύθυνο για την εκκίνηση του λειτουργικού συστήματος Kali Linux.
5. Δημιουργία κουμπιού “Stop Box/Kali” στη σελίδα κάθε διαθέσιμου challenge που είναι υπεύθυνο για τον τερματισμό του μηχανήματος-στόχου καθώς επίσης και του λειτουργικού συστήματος Kali Linux.
6. Δημιουργία νέου πίνακα (identifiers) στη βάση δεδομένων του RootTheBox ώστε πλέον να μπορεί η βάση δεδομένων να αποθηκεύει σημαντικά δεδομένα που είναι απαραίτητα για την ταυτόχρονη λειτουργία της πλατφόρμας RootTheBox, των μηχανημάτων-στόχων αλλά και του λειτουργικού συστήματος Kali Linux.
7. Προσθήκη block κώδικα στην Flask εφαρμογή για δημιουργία isolated network ranges που δίδονται στα μηχανήματα-στόχους αλλά και στο λειτουργικό σύστημα Kali Linux.
8. Τοποθέτηση custom script στο docker image του λειτουργικού συστήματος Kali Linux ώστε να είναι δυνατή η προσπέλαση του από τους χρήστες μέσω του περιηγητή ιστού τους.
9. Εγκατάσταση λογισμικών NoVNC [21] και TightVNCServer [22] στο λειτουργικό σύστημα Kali Linux ώστε να είναι δυνατό οι χρήστες να αποκτήσουν πρόσβαση σε αυτό κάνοντας χρήση αποκλειστικά του περιηγητή ιστού τους.
10. Τροποποίηση σελίδων του RootTheBox και προσθήκη συναρτήσεων AJAX για κλήση των Flask Routes μέσα από την ίδια πλατφόρμα RootTheBox.
11. Δημιουργία σε επίπεδο κώδικα, Progress Bar, στην σελίδα εκκίνησης των μηχανημάτων-στόχων που δείχνει την πρόοδο του μηχανήματος ως προς την εκκίνηση του κατά το πάτημα του κουμπιού “Deploy Box”.
12. Δημιουργία μοναδικών αναγνωριστικών (identifiers) σε επίπεδο κώδικα ώστε να αποφευχθεί λανθασμένος τερματισμός κάποιου μηχανήματος-στόχου κατά το πάτημα του κουμπιού “Stop Box/Kali”.
13. Προσθήκη κώδικα για αφαίρεση από τον διακομιστή, των μηχανημάτων-στόχων κατά το πάτημα του κουμπιού “Stop Box/Kali” ώστε να αποφευχθεί άσκοπη χρήση δίσκου και επιβάρυνση του ίδιου του διακομιστή.

14. Προσθήκη πολλαπλών ελέγχων σε επίπεδο κώδικα ώστε να διασφαλίζεται ότι:
    a. Ο κάθε χρήστης μπορεί να πραγματοποιήσει εκκίνηση μόνο ενός μηχανήματος-στόχου αλλά και του Kali στιγμιότυπου, τη φορά.
    b. Δεν επιτρέπεται σε κανένα χρήστη να εκτελέσει των κώδικα του κουμπιού “Stop Box/Kali” όταν κανένα από τα δύο δεν τρέχουν.
    c. Αν κάποιο μηχάνημα-στόχος ή Kali στιγμιότυπο έχει τερματιστεί, τότε ο χρήστης μπορεί και πάλι να τα εκκινήσει χωρίς να χρειάζεται reload/refresh της ιστοσελίδας ή οποιαδήποτε άλλη ενέργεια.
15. Προσθήκη κώδικα JavaScript που παρέχει δυνατότητες persistence ως προς τις πληροφορίες που κρατάει η πλατφόρμα αλλά και ο περιηγητής ιστού του χρήστη, για καλύτερη διαχείριση των μηχανημάτων-στόχων που ήδη τρέχουν.
16. Δημιουργία JavaScript κώδικα και εισαγωγή του σε ήδη υπάρχουσα σελίδα της πλατφόρμας RootTheBox ώστε να συνεργάζεται με τις δυνατότητες της πλατφόρμας για session timeout αλλά και session logout με το πέρας ενός συγκεκριμένου χρονικού διαστήματος που ορίζεται στο configuration file της πλατφόρμας.

3.3 Αναλυτική Περιγραφή Αλλαγών

1. Προσθήκη πεδίου στον λογαριασμό του διαχειριστή στη σελίδα δημιουργίας των μηχανημάτων-στόχων (πεδίο “Location”). Η πλατφόρμα πλέον παρέχει τη δυνατότητα στους χρήστες να εκκινούν από το μενού του εκάστοτε μηχανήματος το κάθε μηχάνημα στόχο. Το πεδίο αυτό (Εικόνα 14) ήταν απαραίτητο να δημιουργηθεί καθώς κατά την εκκίνηση του μηχανήματος-στόχου από τον χρήστη, η εφαρμογή αλλάζει διαδρομή συστήματος σε αυτή που περιέχει το πεδίο και εκεί βρίσκει το αρχείο του μηχανήματος, το οποίο και εκτελεί. Ανάλογες αλλαγές ήταν απαραίτητο να γίνουν και στη βάση της πλατφόρμας. Δημιουργήθηκε επιπλέον πεδίο στον πίνακα “Box” της MySQL ώστε το μονοπάτι συστήματος που ορίζει ο διαχειριστής στο μενού δημιουργίας του challenge, να διατηρείται εκεί, όπως φαίνεται στην ακόλουθη εικόνα.

```
mysql> describe box;
+----------------------+-----------------------------------------+------+-----+---------+----------------+
| Field                | Type                                    | Null | Key | Default | Extra          |
+----------------------+-----------------------------------------+------+-----+---------+----------------+
| id                   | int                                     | NO   | PRI | NULL    | auto_increment |
| created              | datetime                                | YES  |     | NULL    |                |
| uuid                 | varchar(36)                             | NO   | UNI | NULL    |                |
| corporation_id       | int                                     | NO   | MUL | NULL    |                |
| category_id          | int                                     | YES  | MUL | NULL    |                |
| _name                | varchar(32)                             | NO   | UNI | NULL    |                |
| _operating_system    | varchar(16)                             | YES  |     | NULL    |                |
| _description         | varchar(1024)                           | YES  |     | NULL    |                |
| _capture_message     | varchar(1024)                           | YES  |     | NULL    |                |
| _difficulty          | varchar(16)                             | YES  |     | NULL    |                |
| game_level_id        | int                                     | NO   | MUL | NULL    |                |
| _avatar              | varchar(64)                             | YES  |     | NULL    |                |
| _value               | int                                     | YES  |     | NULL    |                |
| _locked              | tinyint(1)                              | NO   |     | NULL    |                |
| _location            | varchar(60)                             | YES  |     | NULL    |                |
| garbage              | varchar(32)                             | NO   | UNI | NULL    |                |
| flag_submission_type | enum('CLASSIC','SINGLE_SUBMISSION_BOX') | YES  |     | NULL    |                |
+----------------------+-----------------------------------------+------+-----+---------+----------------+
17 rows in set (0.00 sec)
```

Εικόνα 27.

Ακολουθεί εικόνα του στιγμιότυπου του κώδικα που έχει γραφεί και πραγματοποιεί την παραπάνω ενέργεια.

```python
@app.route("/spawn")
def spawn():

    uuid = request.args.get("uuid")
    user_handle = request.args.get("user_handle")

    euuid = create_euuid(uuid)
    uuid = euuid.split("@")[0]

    query_select = """SELECT _location FROM box WHERE uuid='{}'""".format(uuid)
    path = select_query(query_select, 1)

    os.chdir(path[0])
    with open("docker-compose.yml", "r") as file:
        contents = file.readlines()

    parts = extract_parts(contents)
    subnet = get_subnet()
    euuid_id = temp_docker_file_name(euuid)
    docker_network = create_network(subnet, euuid_id)
```

Εικόνα 28.

Ανάλογος κώδικας έπρεπε να εισαχθεί και στα ακόλουθα αρχεία HTML της πλατφόρμας RootTheBox, για να γίνει ορατό το πεδίο προς συμπλήρωση:

- RootTheBox/templates/admin/create/box.html
- RooTheBox/models/Box.py
- RootTheBox/handlers/AdminHandlers/AdminGameObjectHandlers.py

Οι κώδικες αυτοί φαίνονται παρακάτω.

```
<div class="control-group">
        <label class="control-label" for="Location">{{_("Location")}}</label>
        <div class="controls">
            <input id="location" name="location" maxlength="60" type="text" placeholder="({{_('Insert Location')}})"
                rel="popover"
                data-original-title="{{_('Location')}}"
                data-content="{{_('Docker System Location')}} [Max: 60 {{_('Characters')}}]">
        </div>
    </div>
```

Εικόνα 29 (box.html)

```
@property
def location(self):
    return self._location
```

Εικόνα 30 (Box.py)

```
# Location
location = self.get_argument("location", "")
```

Εικόνα 31 (AdminGameObjectHandlers.py)

Να σημειωθεί ότι στον κώδικα προβλέφθηκε η δημιουργία συνάρτησης που πραγματοποιεί “on the fly” αλλαγή των περιεχομένων του αρχείου του μηχανήματος-στόχου, όπως φαίνεται παρακάτω.

```
def construct(contents, parts, euuid_id):
    constructed = []

    for i, line in enumerate(contents):

        if "ports" in line:
            space = line.split("ports")[0]
            line = line.replace("ports", "expose")

        if i not in parts.keys():
            constructed.append(line)
        else:
            if i == list(parts.keys())[-1]:
                tmp = parts[i]["spaces"] + parts[i]["docker_port"] + "\n" + space + "networks:\n" + parts[i]["spaces"][:-1] + euuid_id + "\n"
                constructed.append(tmp)
            else:
                tmp = parts[i]["spaces"] + parts[i]["docker_port"]
                constructed.append(tmp)

    add = "\nnetworks:\n  {0}:\n          external: true\n".format(euuid_id)
    constructed.append(add)

    return(constructed)
```

Εικόνα 32.

Αυτή η συνάρτηση ήταν αναγκαίο να δημιουργηθεί καθώς by default κατά την εκκίνηση του μηχανήματος-στόχου, οι πόρτες του μηχανήματος γίνονται publish στον διακομιστή που τρέχει την πλατφόρμα RootTheBox. Αυτή η συμπεριφορά δεν ήταν επιθυμητή καθώς θα υπήρχε περιορισμός των διαθέσιμων ports του συστήματος (65535) αλλά επίσης το κάθε μηχάνημα θα ήταν προσπελάσιμο από κάθε χρήστη. Με τις αλλαγές που πραγματοποιεί στο αρχείο της μηχανής ο παραπάνω κώδικας, όταν γίνεται εκκίνηση του μηχανήματος οι πόρτες του δεν γίνονται πλέον publish στον διακομιστή, επιτυγχάνοντας καταυτό τον τρόπο isolation μεταξύ κάθε μηχανήματος-στόχου που εκκινείται από τους χρήστες.

2. Δημιουργία Flask εφαρμογής η οποία τρέχει παράλληλα με την πλατφόρμα RootTheBox και διαχειρίζεται όλα τα αιτήματα για εκκίνηση, τερματισμό κ.α των μηχανημάτων-στόχων καθώς επίσης και του λειτουργικού συστήματος Kali Linux. Όπως αναφέρθηκε στα πρώτα κεφάλαια της παρούσας διατριβής, η πλατφόρμα RootTheBox επιλέχθηκε διότι συγκέντρωνε στο σύνολο τους όλα τα πλεονεκτήματα, πλην ελαχίστων, που ήταν αναγκαίο να παρουσιάζει μία πλατφόρμα ανοιχτού κώδικα ώστε να υποστηρίζει με τον καλύτερο δυνατό τρόπο την εκμάθηση-εκπαίδευση των συμμετεχόντων στο αντικείμενο του cyber security μέσω της παιχνιδοποιημένης εκπαίδευσης. Μοναδικό μειονέκτημα της συγκεκριμένης πλατφόρμας ήταν ότι από μόνη της δεν ήταν δυνατό να παρέχει λειτουργίες εκκίνησης-τερματισμού των μηχανημάτων-στόχων μέσα από την ίδια την πλατφόρμα και δεν παρείχε τη δυνατότητα στους συμμετέχοντες να έχει ο καθένας το δικό του στιγμιότυπο του λειτουργικού συστήματος Kali Linux με όλα τα απαραίτητα εργαλεία για να μπορεί να τρέξει τα challenge με μεγαλύτερη ευκολία μέσα από τον περιηγητή ιστού του. Όλα τα παραπάνω υλοποιήθηκαν με τη συγγραφή του κώδικα του οποίου η δομή φαίνεται στην εικόνα που ακολουθεί.

```
1   from flask import Flask, render_template, request, url_for, Response, redirect
2   from flask_cors import CORS
3   from random import randint, choice
4   import subprocess, ipaddress, json, os, re, psutil, db_conn, time, docker, math, sys
5
6   app = Flask(__name__)
7   CORS(app)
8
9   @app.route("/kali_instance")
10  def kali_instance():
13
14  @app.route("/undeploy")
15  def undeploy():
76
77  def cleanup(status=False):
80
81  @app.route("/kali")
82  def kali():
115
116 @app.route("/spawn")
117 def spawn():
151
152 def progress_bar(dir_contents, uuid, euuid, temp_docker_file, subnet, euuid_id, user_handle):
233
234 def create_euuid(uuid):
238
239 def get_subnet():
246
247 def select_query(query, num):
262
263 def insert_query(query):
273
274 def delete_query(query):
284
285 def create_network(subnet, network_name):
291
292 def random_name():
295
296 def boot_docker(euuid_id, docker_file):
313
314 def construct(contents, parts, euuid_id):
337
338 def temp_docker_file_name(euuid):
341
342 def system_ports():
345
346 def extract_parts(contents):
363
364 def random_port(num):
382
383 if __name__ == "__main__":
386
```

Εικόνα 33.

3. Δημιουργία κουμπιού “Deploy Box” στη σελίδα κάθε διαθέσιμου challenge που είναι υπεύθυνο για την εκκίνηση του κάθε μηχανήματος-στόχου από τους χρήστες. Για να δημιουργηθεί αυτό το χαρακτηριστικό στην πλατφόρμα έπρεπε να γράφει συγκεκριμένη συνάρτηση στο Flask Application αλλά και να εισαχθεί επιπλέον κώδικας στα ήδη υπάρχοντα αρχεία της πλατφόρμας. Ακολουθούν εικόνες των στιγμιότυπων κώδικα του Flask Application που είναι αρμόδιο για την εκκίνηση του εκάστοτε μηχανήματος-στόχου αλλά και του κώδικα που εισήχθη στα HTML αρχεία της πλατφόρμας (RootTheBox/templates/missions/box.html).

```
<a style="float:right; margin-top: 10px;"  class="btn" target="_blank" onclick="showProgress();">{{ _("Deploy Box") }}</a>
```

Εικόνα 34.1 (box.html)

```
function showProgress() {

    if (window.localStorage.getItem("euuid") === null) {
        var username = $('#user-handle').data("name");
        var source = new EventSource("http://10.8.0.2:8889/spawn?uuid={{box.uuid}}&user_handle="+username);
        source.onmessage = function(event) {
            $('.progress-bar').css('width', event.data+'%').attr('aria-valuenow', event.data);
            $('.progress-bar-label').text(event.data.split("\n")[0]+'%');
            if(event.data.split("\n")[0] == 100) {
                source.close();
                euuid = event.data.split("\n")[1];
                window.localStorage.setItem("euuid", euuid);
                alert("Machine has been deployed successfully. Start Kali to attack it.");
            }
        }
    } else {
        alert("You can not start a new Box when one is already running.");
    }
}
```

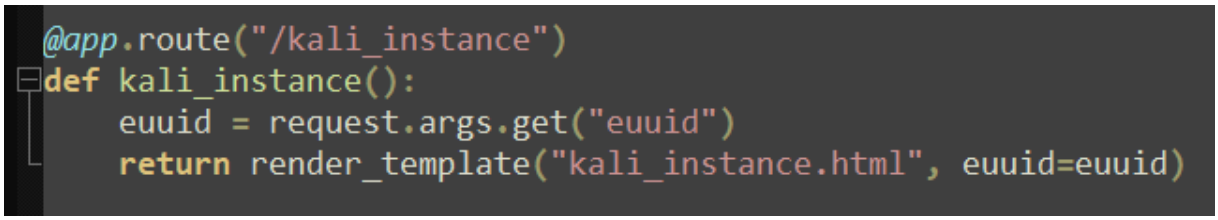
Εικόνα 34.2 (box.html)

```
@app.route("/spawn")
def spawn():

    uuid = request.args.get("uuid")
    user_handle = request.args.get("user_handle")

    euuid = create_euuid(uuid)
    uuid = euuid.split("@")[0]

    query_select = """SELECT _location FROM box WHERE uuid='{}'""".format(uuid)
    path = select_query(query_select, 1)

    os.chdir(path[0])
    with open("docker-compose.yml", "r") as file:
        contents = file.readlines()

    parts = extract_parts(contents)
    subnet = get_subnet()
    euuid_id = temp_docker_file_name(euuid)
    docker_network = create_network(subnet, euuid_id)

    if docker_network == 0:
        const_contents = construct(contents, parts, euuid_id)
    else:
        return('Docker Network Create Error.')

    temp_docker_file = "docker-compose-" + euuid_id + ".yml"

    with open(temp_docker_file, "w") as file:
        for line in const_contents:
            file.write(line)

    dir_contents = os.listdir('.')
    print("About to run return response function")
    return(Response(progress_bar(dir_contents, uuid, euuid, temp_docker_file, subnet, euuid_id, user_handle), mimetype='text/event-stream'))
```

Εικόνα 35.1 (Flask Route Spawn)

Εικόνα 35.2 (Flask Progress Bar)

4. Δημιουργία κουμπιού “Start Kali” στη σελίδα κάθε διαθέσιμου challenge που είναι υπεύθυνο για την εκκίνηση του λειτουργικού συστήματος Kali Linux. Ακολουθούν εικόνες των στιγμιότυπων κώδικα του Flask Application που είναι αρμόδιο για την εκκίνηση του λειτουργικού συστήματος Kali Linux αλλά και του κώδικα που εισήχθη στα HTML αρχεία της πλατφόρμας (RootTheBox/templates/missions/box.html).



Εικόνα 36 (Flask Application Route)

Εικόνα 37 (kali_instance.html)

```
function kali_instance(){

    if (window.localStorage.getItem("euuid") === null) {
        alert("You first have to spawn target machine. Then spawn Kali attack box.");
    } else {
        euuid = window.localStorage.getItem("euuid");
        window.open("http://10.8.0.2:8889/kali_instance?euuid="+euuid);
    }
}
```

Εικόνα 38 (box.html)

5. Δημιουργία κουμπιού “Stop Box/Kali” στη σελίδα κάθε διαθέσιμου challenge που είναι υπεύθυνο για τον τερματισμό του μηχανήματος-στόχου καθώς επίσης και του λειτουργικού συστήματος Kali Linux. Ακολουθούν εικόνες των στιγμιότυπων κώδικα του Flask Application που είναι αρμόδιο για τον τερματισμό του λειτουργικού συστήματος Kali Linux αλλά και του κώδικα που εισήχθη στα HTML αρχεία της πλατφόρμας (RootTheBox/templates/missions/box.html).

```
@app.route("/undeploy")
def undeploy():
    user_handle = request.args.get("user_handle")
    if user_handle == None:
        euuid = request.args.get("euuid")
        get_network_name = """SELECT network_name FROM identifiers WHERE euuid='{}'""".format(euuid)
    elif user_handle == "admin":
        return(str("Admin logged out"))
    else:
        get_network_name = """SELECT network_name FROM identifiers WHERE user_handle='{}'""".format(user_handle)

    network_name = select_query(get_network_name, 1)

    if network_name == None:
        return(str("User logged out before spawning anything."))

    docker_network_inspect = subprocess.run(["docker network inspect {0}".format(network_name[0])], shell=True, check=True, capture_output=True)
    docker_network_inspect_json = json.loads(docker_network_inspect.stdout)
    docker_container_values = list(docker_network_inspect_json[0]['Containers'].values())
    docker_container_name = str(docker_container_values[0]['Name'])

    try:
        kali_docker_name = str(docker_container_values[1]['Name'])
        docker_stop = subprocess.run(["docker stop {0} {1}".format(docker_container_name, kali_docker_name)], shell=True, check=True, capture_output=True)
    except:
        docker_stop = subprocess.run(["docker stop {0}".format(docker_container_name)], shell=True, check=True, capture_output=True)

    if docker_stop.returncode == 0:
        print("Docker(s) stopped successfully")
        docker_remove_unused = subprocess.run(["docker rm $(docker ps -a -q)"], shell=True, check=True, capture_output = True)
        if docker_remove_unused.returncode == 0:
            print("Docker(s) wiped successfully")
            docker_network_prune = subprocess.run(["docker network prune -f"], shell=True, check=True, capture_output=True)
            if docker_network_prune.returncode == 0:
                print("Docker networks wiped successfully")

                try:
```

Εικόνα 39 (Flask Application Route)

```
function undeploy() {

    if (window.localStorage.getItem("euuid") === null) {
        alert("You can not stop something that is not already running.");
    } else {
        alert("Stopping running Machines, Please wait...");
        euuid = window.localStorage.getItem("euuid");

        var source = new EventSource("http://10.8.0.2:8889/undeploy?euuid="+euuid);
        source.onmessage = function(event) {

            if (event.data.split("\n")[0] == "True") {
                window.localStorage.removeItem("euuid");
                alert("Machines stopped Successfully.");
            }
        }
    }
}
```

Εικόνα 40 (box.html)

6. Δημιουργία νέου πίνακα (identifiers) στη βάση δεδομένων του RootTheBox ώστε πλέον να μπορεί η βάση δεδομένων να αποθηκεύει σημαντικά δεδομένα που είναι απαραίτητα για την ταυτόχρονη λειτουργία της πλατφόρμας RootTheBox, των μηχανημάτων-στόχων αλλά και του λειτουργικού συστήματος Kali Linux. Ο νέος πίνακας identifiers αποτελείται από τα ακόλουθα πεδία:

    - **id**. Αυξανόμενος μετρητής της βάσης δεδομένων
    - **uuid**. User ID, δημιουργείται από την πλατφόρμα RootTheBox κατά την εγγραφή ενός χρήστη στην πλατφόρμα.
    - **euuid**. Extended User ID (custom). Αποτελείται από το default uuid της πλατφόρμας, το σύμβολο "@" και μια τυχαία ακολουθία έξη ψηφίων. Δημιουργήθηκε με στόχο η τιμή του πεδίου του να χρησιμοποιείται για τη μετονομασία των εκάστοτε docker file κατά την on the fly δημιουργία τους ώστε να υπάρχει μεγαλύτερος έλεγχος ως προς το ποιο μηχάνημα-στόχος ξεκίνησε από ποιο docker file, καθώς μπορούν να υπάρχουν ταυτόχρονα παραπάνω από ένα ίδια μηχανήματα που ξεκίνησαν από περισσότερους από ένα χρήστες κάνοντας χρήση του ίδιου base docker file. Το αναγνωριστικό αυτό βοηθά επίσης στον έλεγχο της ύπαρξης ή όχι μηχανημάτων-στόχων αλλά και στιγμιότυπων του λειτουργικού συστήματος Kali Linux, που βρίσκονται ήδη σε κατάσταση Running. Το αναγνωριστικό αυτό αποθηκεύεται στον περιηγητή ιστού του χρήστη και αν υπάρχει τότε οι έλεγχοι που πραγματοποιούνται αποτρέπουν τον εκάστοτε χρήστη να ξεκινήσει περισσότερες από μία μηχανες-στόχους ή στιγμιότυπα του Kali Linux.
    - **docker_file**. Στο πεδίο αυτό αποθηκεύεται το όνομα του τελικού docker file από το οποίο ξεκίνησε το εκάστοτε μηχάνημα. Το docker file αποτελείται από το όνομα του default docker file ακολουθούμενου από την τιμή του eeuid.
    - **subnet**. Στο πεδίο αυτό αποθηκεύεται το isolated subnet που δημιουργήθηκε προς χρήση από το μηχάνημα-στόχο και το στιγμιότυπο του λειτουργικό συστήματος Kali Linux. Με αυτό τον τρόπο και το μηχάνημα-στόχος αλλά και το Kali Linux θα ανήκουν στο ίδιο subnet και θα είναι πλήρως isolated από τα υπόλοιπα μηχανήματα.
    - **network_name**. Ονομασία δικτύου.
    - **user_handle**. Ονομασία χρήστη (user handle).

```
mysql> describe identifiers;
+--------------+--------------+------+-----+---------+----------------+
| Field        | Type         | Null | Key | Default | Extra          |
+--------------+--------------+------+-----+---------+----------------+
| id           | int unsigned | NO   | PRI | NULL    | auto_increment |
| uuid         | varchar(100) | NO   |     | NULL    |                |
| euuid        | varchar(100) | NO   |     | NULL    |                |
| docker_file  | varchar(50)  | NO   |     | NULL    |                |
| subnet       | varchar(15)  | NO   |     | NULL    |                |
| network_name | varchar(6)   | NO   |     | NULL    |                |
| user_handle  | varchar(25)  | NO   |     | NULL    |                |
+--------------+--------------+------+-----+---------+----------------+
7 rows in set (0.00 sec)
```

Εικόνα 41.

7. Προσθήκη block κώδικα στην Flask εφαρμογή για δημιουργία isolated network ranges που δίδονται στα μηχανήματα-στόχους αλλά και στο λειτουργικό σύστημα Kali Linux. Βασική προϋπόθεση για την χωρίς προβλήματα εκπαίδευση των συμμετεχόντων μέσω της παιχνιδοποιημένης εκπαίδευσης ήταν η δημιουργία απομονωμένων δικτύων τα όποια δίδονταν σε κάθε μηχάνημα-στόχο αλλά και στιγμιότυπο του λειτουργικού συστήματος Kali Linux έτσι ώστε κάνεις από τους εκπαιδευόμενους να μη μπορεί να αλληλεπιδράσει με τον κάποιον άλλο χρήστη με σκοπό να δημιουργήσει πρόβλημα στο μηχάνημα-στόχο του άλλου. Ακολουθούν στιγμιότυπα κώδικα των συναρτήσεων του flask application που δημιουργεί και χρησιμοποιεί αυτά τα απομονωμένα δίκτυα.

```python
def get_subnet():
    subnets = []
    for ip in ipaddress.ip_network('10.0.0.0/8').subnets(new_prefix=24):
        subnets.append(ip)

    random_selection = choice(subnets)
    return(random_selection)
```

Εικόνα 42.1

```python
def create_network(subnet, network_name):
    try:
        network = subprocess.run(["docker network create -d bridge --subnet {0} {1}".format(subnet, network_name)], shell=True, check=True, capture_output=True)
        return(network.returncode)
    except:
        return(1)
```

Εικόνα 42.2

8. Εγκατάσταση λογισμικών NoVNC [21] και TightVNCServer [22] στο λειτουργικό σύστημα Kali Linux ώστε να είναι δυνατό οι χρήστες να αποκτήσουν πρόσβαση σε αυτό κάνοντας χρήση αποκλειστικά του περιηγητή ιστού τους.

9. Τοποθέτηση custom script στο docker image του λειτουργικού συστήματος Kali Linux ώστε να είναι δυνατό οι χρήστες να αποκτήσουν πρόσβαση σε αυτό κάνοντας χρήση αποκλειστικά του περιηγητή ιστού τους. Στο script αυτό

τοποθετούνται δυο εντολές όπου η μια αφορά το TightVNCServer ενώ η άλλη το NoVNC.

```
┌──(root㉿347af114377a)-[~]
└─# cat conf.sh
#!/bin/bash
nohup sh -c "tightvncserver :0 -geometry $1 -depth 16 -pixelformat rgb565" > /dev/null &
nohup sh -c "/usr/share/novnc/utils/launch.sh --listen 5901 --vnc localhost:5900" > /dev/null &
```

Εικόνα 43.

Η πρώτη εντολή είναι υπεύθυνη για την εκκίνηση του TightVNCServer στην οθόνη :0 με ύψος και πλάτος που δίνεται στην μεταβλητή $1 κατά την ενεργοποίηση του λειτουργικού συστήματος Kali Linux από το Flask script που βρίσκεται στον διακομιστή, με βάθος χρωμάτων 16 και μορφοποίηση χρώματος για αναπαράσταση pixel RBG565. Η εντολή nohup (no hang up) προστάζει το λειτουργικό σύστημα να μη τερματίσει τις διεργασίες που εκτελούνται ακόμα κ μετά το κλείσιμο του shell που την εκτελεί (bash). Η δεύτερη εντολή αφορά το noVNC και ουσιαστικά ανοίγει την πόρτα 5901 (**--listen 5901**) στην οποία περιμένει για εισερχόμενες συνδέσεις τις οποίες τις μεταβιβάζει (**--vnc localhost:5900**) σε ένα ήδη υπάρχον VNC server, στην περίπτωση μας δηλαδή στο TightVNCServer που ακούει στην πόρτα 5900. Τέλος ακολουθεί η εντολή του Flask Script που εκτελεί το "conf.sh" αρχείο στο λειτουργικό σύστημα Kali Linux που αναφέραμε παραπάνω.

```
if boot_kali.returncode == 0:
    start_vnc = subprocess.run(["docker exec {0} /root/conf.sh {1}".format(kali_id, resolution)], shell=True, check=True, capture_output=True)
```

Εικόνα 44.

10. Τροποποίηση σελίδων του RootTheBox και προσθήκη συναρτήσεων AJAX για κλήση των Flask Routes μέσα από την ίδια πλατφόρμα RootTheBox. Η σελίδα που τροποποιήθηκε είναι η "box.html" και βρίσκεται στη διαδρομή συστήματος /path/to/RootTheBox/templates/missions/box.html. Η γραμμή κώδικα JavaScript που προστέθηκε φαίνεται στην εικόνα του ακολουθεί.

```
<script src="/static/js/pages/missions/box.js"></script>
<script src="/static/js/libs/commonmark.min.js"></script>
<script src="/static/js/libs/jstree.js"></script>
<script src="https://ajax.googleapis.com/ajax/libs/jquery/3.5.1/jquery.min.js"></script>

{% end %}
```

Εικόνα 45.

11. Δημιουργία σε επίπεδο κώδικα, Progress Bar, στην σελίδα εκκίνησης των μηχανημάτων-στόχων που δείχνει την πρόοδο του μηχανήματος ως προς την εκκίνηση του κατά το πάτημα του κουμπιού "Deploy Box". Η λειτουργία αυτή προστέθηκε για οπτικούς λόγους αλλά και λόγους αξιοπιστίας, ώστε να είναι εμφανής η πρόοδος εκκίνησης του μηχανήματος-στόχου κατά το πάτημα του κουμπιού "Deploy Box". Στιγμιότυπο του κώδικα του Progress Bar του Flask Script αλλά και του κώδικα JavaScript που προστέθηκε σε υπάρχουσα σελίδα του RooTheBox (/path/to/RootTheBox/templates/missions/box.html) φαίνεται παρακάτω.

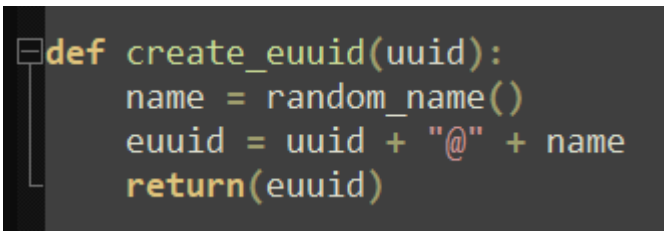
```
function showProgress() {

    if (window.localStorage.getItem("euuid") === null) {
        var username = $('#user-handle').data("name");
        var source = new EventSource("http://10.8.0.2:8889/spawn?uuid={{box.uuid}}&user_handle="+username);
        source.onmessage = function(event) {
            $('.progress-bar').css('width', event.data+'%').attr('aria-valuenow', event.data);
            $('.progress-bar-label').text(event.data.split("\n")[0]+'%');
            if(event.data.split("\n")[0] == 100) {
                source.close();
                euuid = event.data.split("\n")[1];
                window.localStorage.setItem("euuid", euuid);
                alert("Machine has been deployed successfully. Start Kali to attack it.");
            }
        }
    } else {
        alert("You can not start a new Box when one is already running.");
    }
}
```

Εικόνα 46 (box.html – JavaScript κώδικας)

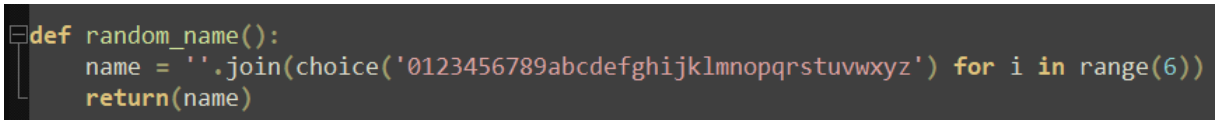
```
    return(Response(progress_bar(dir_contents, uuid, euuid, temp_docker_file, subnet, euuid_id, user_handle), mimetype='text/event-stream'))

def progress_bar(dir_contents, uuid, euuid, temp_docker_file, subnet, euuid_id, user_handle):
    if "Dockerfile" in dir_contents:
        with open("Dockerfile", "r") as file:
            repository = file.readline().split(" ")[1].rstrip("\n")
    else:
        with open("docker-compose.yml", "r") as file:
            for line in file.readlines():
                if "image:" in line:
                    repository = line.split("image: ")[1].rstrip("\n")
                    break

    try:
        exists = subprocess.run(["docker inspect --type=image {0}".format(repository)], shell=True, check=True, capture_output=True)

        if exists.returncode == 0:
            x = 0
            while x <= 100:
                if x != 100:
                    yield "data:" + str(x) + "\n\n"
                else:
                    yield "data:" + str(x) + "\n"
                    yield "data:" + euuid + "\n\n"
                x += 50
                time.sleep(0.2)

            docker_id = boot_docker(euuid_id, temp_docker_file)
            query_insert = """INSERT INTO identifiers (uuid, euuid, docker_file, subnet, network_name, user_handle) VALUES ('{0}', '{1}', '{2}', '{3}', '{4}', '{5}')""".format(uuid,
             euuid, temp_docker_file, subnet, euuid_id, user_handle)
            insertion = insert_query(query_insert)
            print("Hitting exit point as machine was already downloaded and is now loaded.")
            sys.exit(0)
```

Εικόνα 47 (Flask Application – Progress Bar Snapshot)

12. Δημιουργία μοναδικών αναγνωριστικών (euuid identifiers) σε επίπεδο κώδικα ώστε να αποφευχθεί λανθασμένος τερματισμός κάποιου μηχανήματος-στόχου κατά το πάτημα του κουμπιού “Stop Box/Kali”. Όπως αναφέρθηκε παραπάνω (bullet 6 – euuid) ήταν αναγκαίο να δημιουργηθούν μοναδικά identifiers για να υπάρχει πιο αξιόπιστη διαχείριση των μηχανημάτων-στόχων αλλά και των στιγμιότυπων του λειτουργικού συστήματος Kali Linux των χρηστών διότι λόγω εκτεταμένης χρήσης τεχνολογίας Docker από την εφαρμογή RootTheBox, τα base file των Docker που χρησιμοποιούνται είναι ίδια και χρησιμοποιούνται ταυτόχρονα από πολλούς χρήστες που είναι πιθανό στον ίδιο χρόνο να τρέχουν διαφορετικά στιγμιότυπα του ίδιου μηχανήματος-στόχου. Εισάγοντας αυτή τη λειτουργία στον κώδικα Flask διασφαλίζεται ότι για κάθε μηχάνημα-στόχο θα δημιουργείται, κατά την εκτέλεση του, και το αντίστοιχο docker-compose.yml αρχείο όπου στην ονομασία του θα περιλαμβάνεται και μία εξαψήφια τυχαία ακολουθία χαρακτήρων. Έτσι η διαχείριση κάθε μηχανήματος-στόχου γίνεται πλέον κάνοντας χρήση του δικού του αρχείου που δημιουργείται “on the fly” κατά την εκκίνηση του εκάστοτε μηχανήματος. Ο κώδικας που δημιουργεί αυτές τις τυχαίες ακολουθίες φαίνεται στις επόμενες εικόνες.



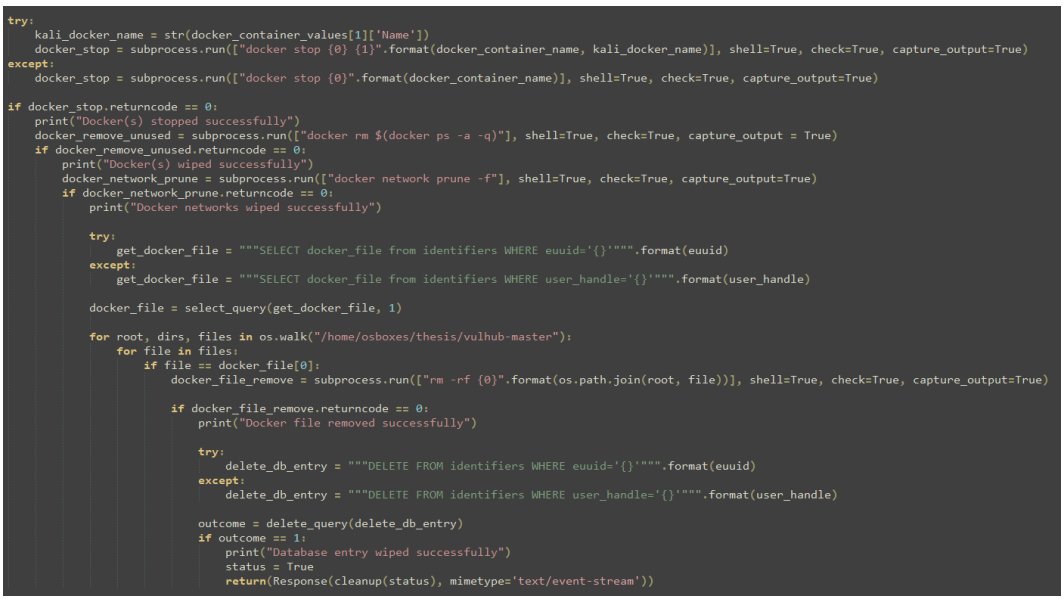
Εικόνα 48.1



Εικόνα 48.2

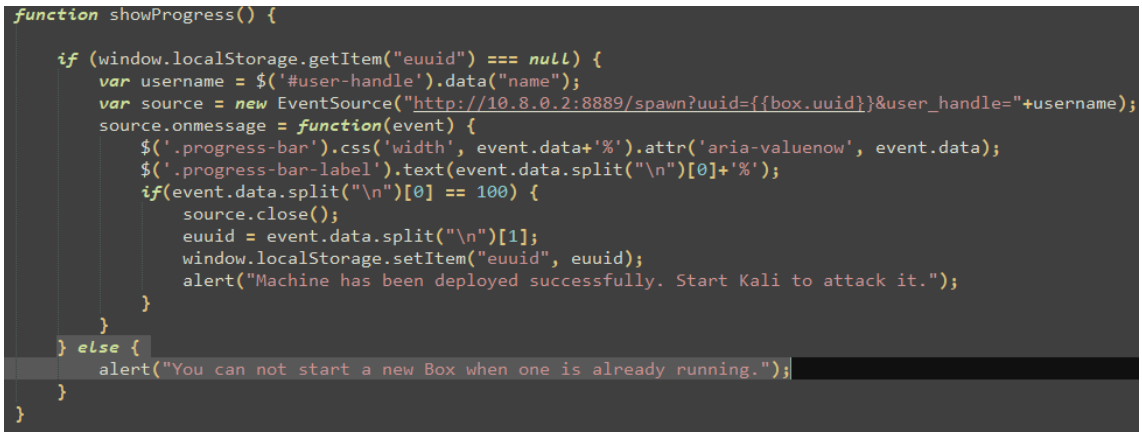
13. Προσθήκη κώδικα για αφαίρεση από τον διακομιστή, των μηχανημάτων-στόχων κατά το πάτημα του κουμπιού “Stop Box/Kali” ώστε να αποφευχθεί άσκοπη χρήση δίσκου και επιβάρυνση του ίδιου του διακομιστή. Είναι άλλο ένα απαραίτητο χαρακτηριστικό για την εύρυθμή λειτουργία του διακομιστή που φιλοξένει την πλατφόρμα RootTheBox. Κάθε χρήστης αυτής της πλατφόρμας μπορεί να εκκινεί τα δικά του στιγμιότυπα των μηχανημάτων-στόχων αλλά και του λειτουργικού συστήματος Kali Linux. Η τεχνολογία Docker παρέχει από μόνη της «ελαφριά» containers από άποψη μεγέθους που καταλαμβάνουν αυτά στο δίσκο αλλά και υπολογιστικών πόρων γενικότερα. Όμως αν κάθε στιγμιότυπο του μηχανήματος-στόχου που εκκινεί ο χρήστης παραμένει ενεργοποιημένο και σε κατάσταση running ακόμα και μετά την ολοκλήρωση του challenge ή την έξοδο του χρήστη από την πλατφόρμα τότε ο χώρος που θα καταλαμβάνεται από αυτά στον δίσκο, θα είναι ικανός για να επιβραδύνει την πλατφόρμα και να δημιουργήσει προβλήματα απόδοσης στο διακομιστή γενικότερα. Για αυτό το λόγο προβλέφθηκε η δημιουργία συνάρτησης στο Flask script που είναι αρμόδια για την εκκαθάριση κάθε docker που έχει τερματιστεί από τον χρήστη αλλά και της διαγραφής των ανάλογων εγγραφών από την ίδια τη βάση δεδομένων της πλατφόρμας. Πιο συγκεκριμένα, εκτελούνται οι ακόλουθες διαδικασίες εκκαθάρισης:
    - Διαγραφή docker network
    - Διαγραφή εγγραφών από τη βάση MySQL της πλατφόρμας
    - Διαγραφή docker-compose.yml αρχείου του εκάστοτε μηχανήματος-στόχου
    - Αφαίρεση του στιγμιότυπου του λειτουργικού συστήματος Kali Linux που προηγουμένως ήταν attached στο docker network που είχε δημιουργηθεί

    Ακολουθεί στιγμιότυπο του Flask κώδικα που εκτελεί τις παραπάνω ενέργειες εκκαθάρισης.



Εικόνα 49.

14. Προσθήκη ελέγχων σε επίπεδο κώδικα ώστε να διασφαλίζεται ότι:
    a. Ο κάθε χρήστης μπορεί να πραγματοποιήσει εκκίνηση μόνο ενός μηχανήματος-στόχου αλλά και του Kali Linux στιγμιότυπου, τη φορά. Ο μηχανισμός αυτός υλοποιείται με τον έλεγχο ύπαρξης του αναγνωριστικού “euuid”. Αν το “euuid” δεν υπάρχει τότε εκτελείται ο κώδικας της “if” και πραγματοποιείται η εκκίνηση, διαφορετικά η ροή ελέγχου περνάει στην “else” και έτσι ο κώδικας αποτρέπει την εκκίνηση παραπάνω μηχανημάτων-στόχων η στιγμιότυπων Kali Linux.



Εικόνα 50.1.

    b. Δεν επιτρέπεται σε κανένα χρήστη να εκτελέσει των κώδικα του κουμπιού “Stop Box/Kali” όταν κανένα από τα δύο δεν τρέχουν. Και αυτός ο μηχανισμός υλοποιείται με τον έλεγχο ύπαρξης της μεταβλητής “euuid”. Όταν η μεταβλητή “euuid” έχει τιμή “null” σημαίνει ότι δεν υπάρχει κανένα μηχάνημα-στόχος ή στιγμιότυπο Kali Linux που να έχει ξεκινήσει από τον χρήστη, έτσι ο κώδικας σταματά να εκτελείται εμφανίζοντας την ανάλογη ειδοποίηση στον περιηγητή ιστού του χρήστη.

```
function undeploy() {

    if (window.localStorage.getItem("euuid") === null) {
        alert("You can not stop something that is not already running.");
```

Εικόνα 50.2

c. Αν κάποιο μηχάνημα-στόχος ή Kali στιγμιότυπο έχει τερματιστεί, τότε ο χρήστης μπορεί και πάλι να τα εκκινήσει χωρίς να χρειάζεται reload/refresh της ιστοσελίδας ή οποιαδήποτε άλλη ενέργεια. Ο μηχανισμός αυτός υλοποιείται με τον έλεγχο ύπαρξης του αναγνωριστικού "euuid". Αν το "euuid" δεν υπάρχει τότε εκτελείται ο κώδικας της "if" και πραγματοποιείται η εκκίνηση.

```
function showProgress() {

    if (window.localStorage.getItem("euuid") === null) {
```

Εικόνα 50.3

15. Προσθήκη κώδικα JavaScript που παρέχει δυνατότητες persistence ως προς τις πληροφορίες που κρατάει η πλατφόρμα αλλά και ο περιηγητής ιστού του χρήστη, για καλύτερη διαχείριση των μηχανημάτων-στόχων που ήδη τρέχουν. Ο μηχανισμός αυτός υλοποιείται με τη χρήση της ιδιότητας "localStorage" [23] της διεπαφής window του περιηγητή ιστού του χρήστη. Όταν γίνεται εκκίνηση κάποιου μηχανήματος-στόχου η στιγμιότυπου του λειτουργικού συστήματος Kali Linux τότε η μεταβλητή "euuid" παίρνει κάποια τιμή η οποία με τη σειρά της αποθηκεύεται με τη χρήση της ιδιότητας localStorage στο browser του χρήστη. Αντίστοιχα όταν κάποιο μηχάνημα-στόχος η στιγμιότυπο Kali τερματίζεται τότε αυτόματα διαγράφεται η τιμή της μεταβλητής από τον περιηγητή ιστού του χρήστη.

```
euuid = event.data.split("\n")[1];
window.localStorage.setItem("euuid", euuid);
alert("Machine has been deployed successfully.
```

Εικόνα 51.1

```
if (event.data.split("\n")[0] == "True") {
    window.localStorage.removeItem("euuid");
    alert("Machines stopped Successfully.");
```

Εικόνα 51.2

16. Δημιουργία JavaScript κώδικα και εισαγωγή του σε ήδη υπάρχουσα σελίδα της πλατφόρμας RootTheBox ώστε να συνεργάζεται με τις δυνατότητες της

πλατφόρμας για session timeout αλλά και session logout με το πέρας ενός συγκεκριμένου χρονικού διαστήματος που ορίζεται στο configuration file της πλατφόρμας. Για να επιτευχθούν τα παραπάνω παραμετροποιήθηκε κατάλληλα το configuration file της πλατφόρμας (/path/to/RootTheBox/files/configuration.cfg) και ορίστηκε χρόνος αδράνειας δύο ωρών για αποσύνδεση του χρήστη από την πλατφόρμα όπως φαίνεται στην επόμενη εικόνα.

```
# [ Server ]
origin = "ws://localhost:8888"
listen_port = 8888
listen_interface = "0.0.0.0"
session_age = 120
x_headers = False
ssl = False
certfile = ""
keyfile = ""
admin_ips = ['127.0.0.1', '::1']
autoreload_source = True
webhook_url = None
```

Εικόνα 52.

Παράλληλα, εισήχθη JavaScript κώδικας στο ήδη υπάρχον αρχείο “main.html” της πλατφόρμας που βρίσκεται στο μονοπάτι συστήματος “/path/to/RootTheBox/templates/main.html” ώστε κατά την αποσύνδεση του χρήστη από το σύστημα να αποστέλεται αίτημα στη συνάρτηση “undeploy” του Flask Script και να τερματίζεται η λειτουργία κάθε μηχανήματος-στόχου αλλά και του στιγμιότυπου Kali Linux. Ο JavaScript κώδικας που υλοποιεί τα παραπάνω φαίνεται στην επόμενη εικόνα.

```
<script>
    if (window.localStorage.getItem("euuid") === null) {
        //do nothing
    } else {
        alert("Application detected that there are machines still running.\nCleaning Up, Please wait...");
        euuid = window.localStorage.getItem("euuid");
        var source = new EventSource("http://10.8.0.2:8889/undeploy?euuid="+euuid);
        source.onmessage = function(event) {
            if (event.data.split("\n")[0] == "True") {
                window.localStorage.removeItem("euuid");
                alert("Machines stopped Successfully.");
            }
        }
    }
</script>
```

Εικόνα 53.

Κεφάλαιο 4
Δοκιμή Πλατφόρμας

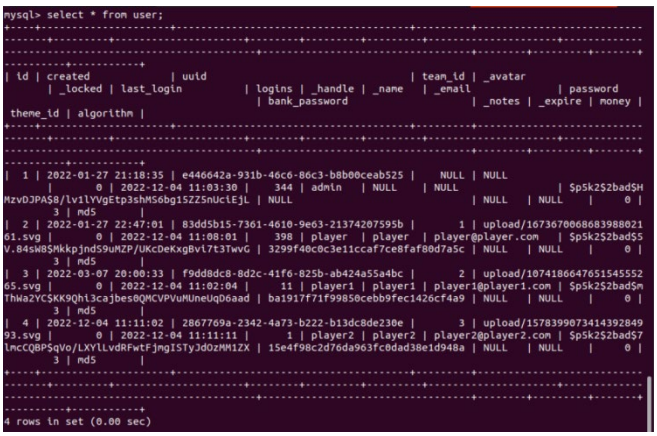
Στο κεφάλαιο αυτό θα γίνει η δοκιμή της πλατφόρμας από τρεις (3) διαφορετικούς χρήστες ταυτόχρονα με σκοπό να γίνει έλεγχος στους ακόλουθους τομείς:

1. Χρήση CPU (επεξεργαστή) / Χρήση RAM (προσωρινής μνήμης)
2. Επικοινωνία Kali Linux λειτουργικού συστήματος με μηχάνημα-στόχο
3. Έλεγχος σωστής δημιουργίας απομονωμένων εικονικών δικτύων
4. Σωστός τερματισμός μηχανήματος-στόχου και Kali Linux λειτουργικού συστήματος
5. Έλεγχος διαγραφής των docker compose αρχείων που δημιουργούνται “on the fly” για το ίδιο μηχάνημα-στόχο
6. Έλεγχος διαγραφής των MySQL δεδομένων που διατηρούνται στη βάση για τη σωστή λειτουργία των μηχανημάτων-στόχων και του λειτουργικού συστήματος Kali Linux

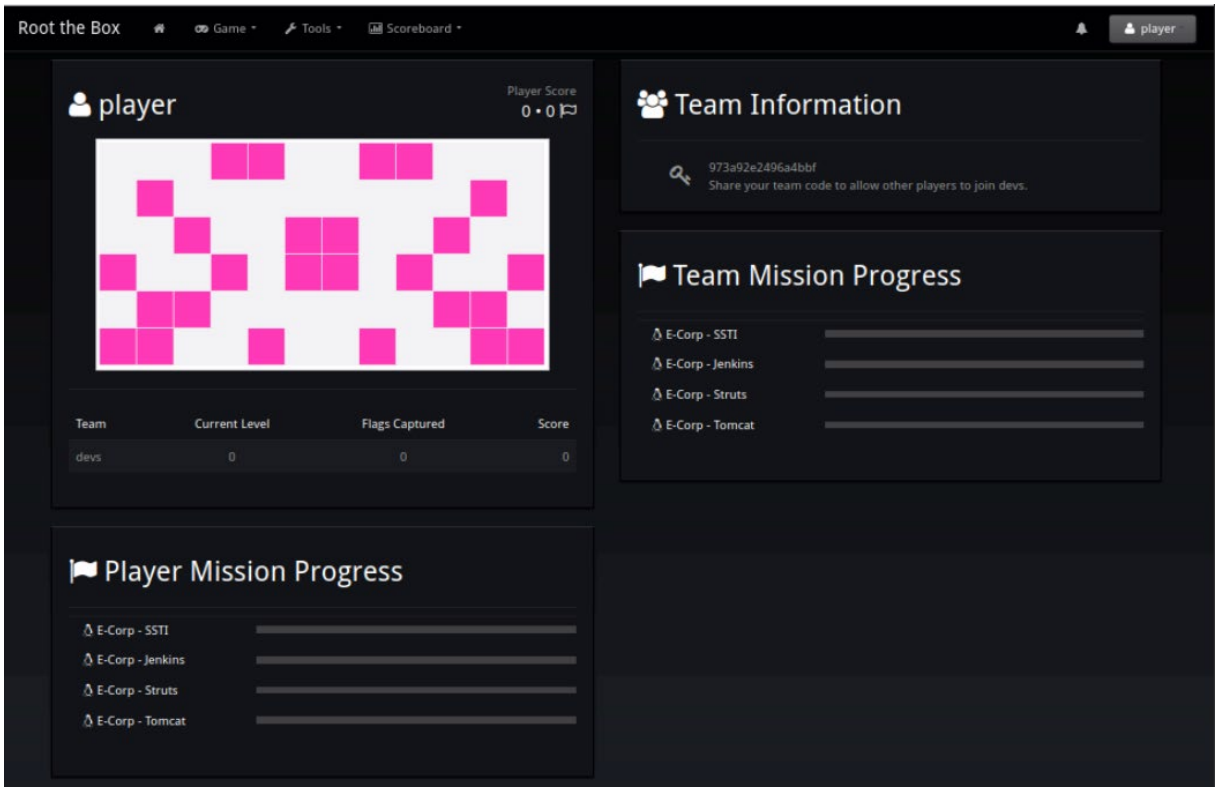
4.1 Αποτελέσματα Εκτέλεσης

Στην ενότητα αυτή θα γίνει δοκιμή της πλατφόρμας σε πραγματικές συνθήκες και θα παρουσιαστεί με τη μορφή screenshot η διαδικασία εκκίνησης των μηχανημάτων-στόχων καθώς επίσης και των snapshot του λειτουργικού συστήματος Kali Linux αλλά και ο τερματισμός τους.

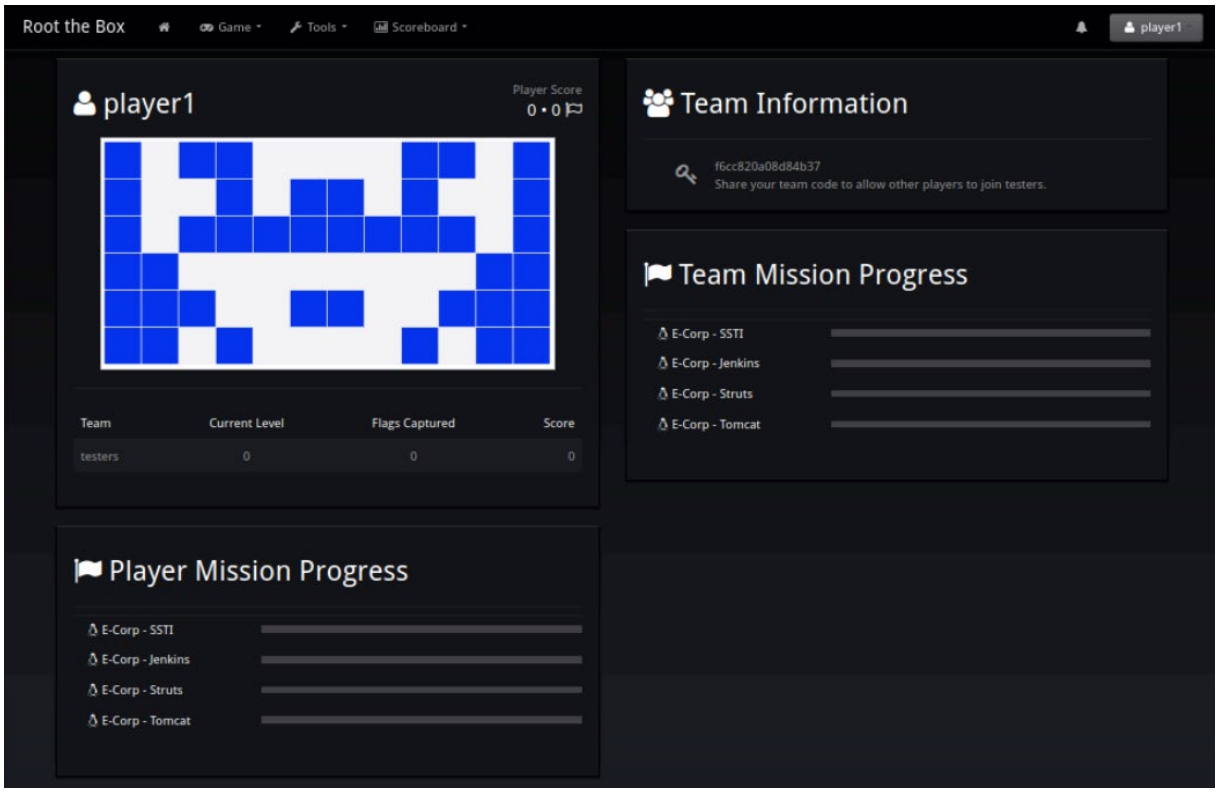
Στην πλατφόρμα βρίσκονται εγγεγραμμένοι και συνδεδεμένοι τρεις διαφορετικοί χρήστες με τα nicknames player, player1 και player2.



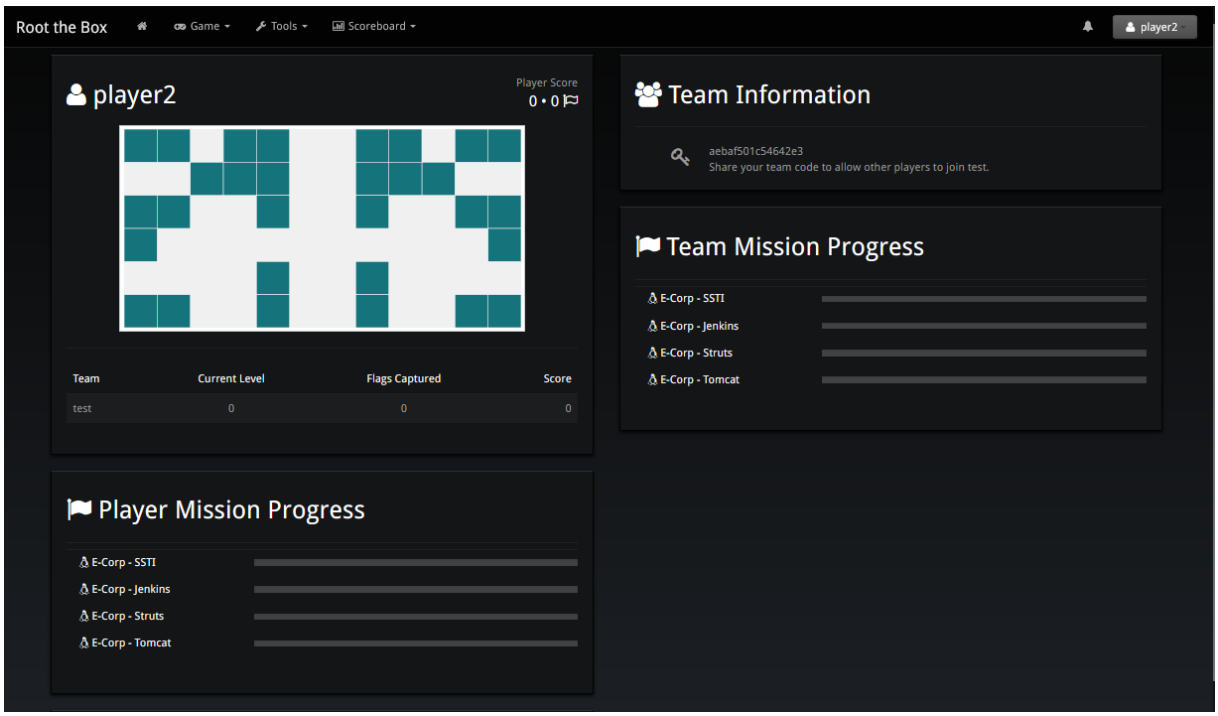
Εικόνα 54.



Εικόνα 55. (player – χρήστης 1)



Εικόνα 56. (player1 – χρήστης 2)



Εικόνα 57. (player2 – χρήστης 3)

1. Χρήση CPU (επεξεργαστή) / Χρήση RAM (προσωρινής μνήμης)

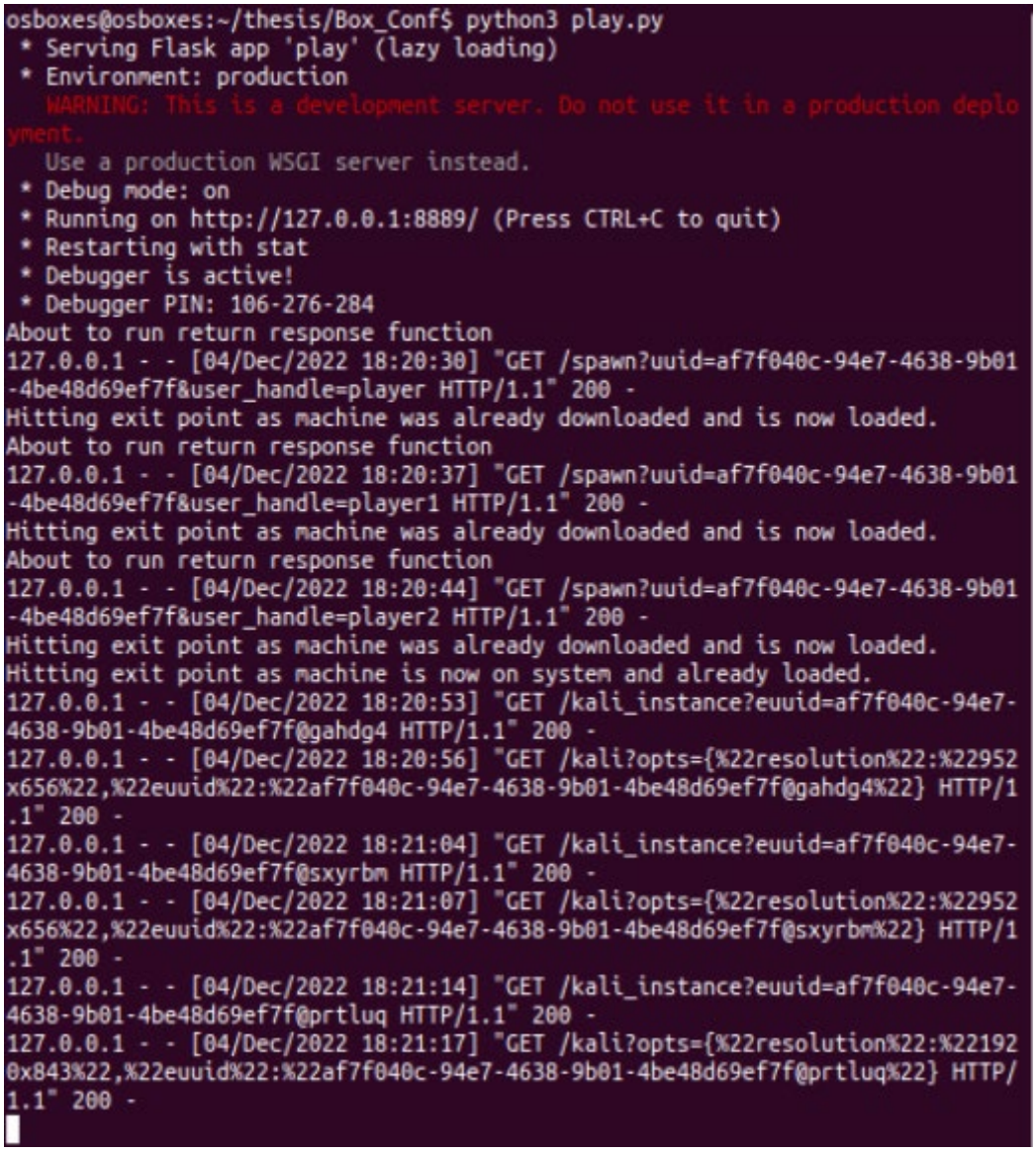
Για να δείξουμε τις διαφορές στη χρήση της CPU/RAM του συστήματος, θα παραθέσουμε screenshot της CPU/RAM του συστήματος προτού οι χρήστες ξεκινήσουν οποιοδήποτε μηχάνημα-στόχο ή στιγμιότυπο του λειτουργικού συστήματος Kali Linux και δεύτερο screenshot αφού και οι τρεις χρήστες έχουν ξεκινήσει το ίδιο μηχάνημα-στόχο αλλά και τα δικά τους στιγμιότυπα του λειτουργικού Kali Linux.

<u>Screenshot συστήματος σε κατάταση ηρεμίας</u>

Εικόνα 58.

Screenshot συστήματος σε πλήρη ανάπτυξη των μηχανημάτων-στόχων αλλά και των στιγμιότυπων του λειτουργικού Kali Linux

Στο επόμενα screenshot παρουσιάζονται, το output του Flask Application που αποδεικνύει την ταυτόχρονη έναρξη των μηχανημάτων-στόχων και των στιγμιότυπων του λειτουργικού συστήματος Kali Linux αλλά και των πόρων CPU/RAM του συστήματος ενώ όλα βρίσκονται σε πλήρη εξέλιξη.



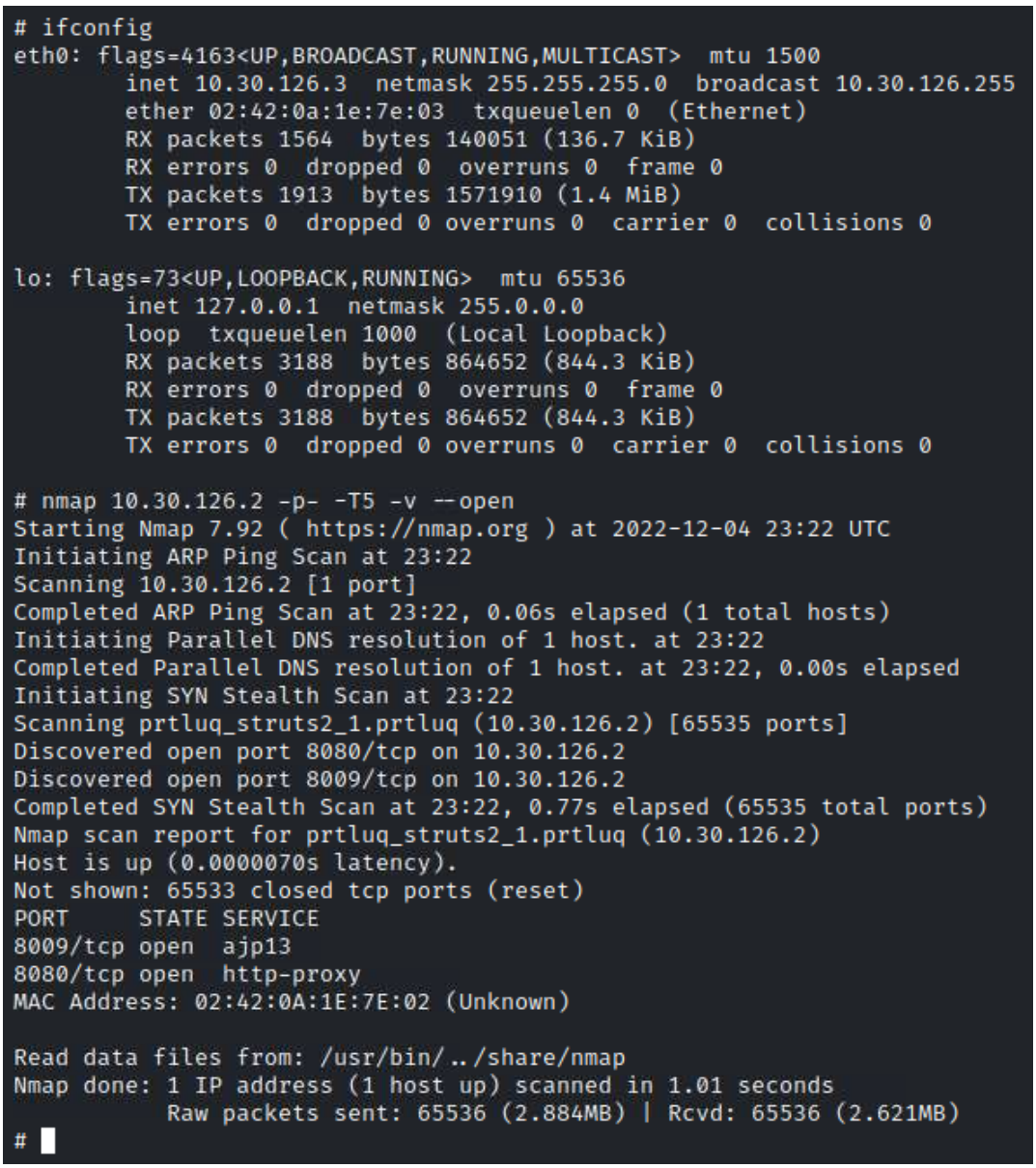
Εικόνα 59.

Εικόνα 60.

Βάση των παραπάνω συγκρίσεων παρατηρούμε ότι δεν υπάρχει καμία ουσιαστική αύξηση στη χρήση της CPU του διακομιστή που φιλοξενεί την πλατφόρμα, παρά μόνο στη προσωρινή μνήμη RAM, πράγμα φυσιολογικό καθώς τρέχουν ταυτόχρονα τρία στιγμιότυπα του λειτουργικού συστήματος Kali Linux και τρία μηχανήματα-στόχοι που έχουν ξεκινήσει από το ίδιο base docker compose αρχείο. Η Αύξηση που παρατηρείται στην προσωρινή μνήμη RAM είναι μόλις 1.1 GB για τρείς χρήστες που εκπαιδεύονται ταυτόχρονα με τη βοήθεια της πλατφόρμας.

2. Επικοινωνία Kali Linux λειτουργικού συστήματος με μηχάνημα-στόχο

Σε αυτό το σημείο θα δείξουμε με screenshots ότι κάθε στιγμιότυπο του λειτουργικό συστήματος Kali Linux μπορεί να επικοινωνήσει σωστά με το μηχάνημα-στόχο.


ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 10.30.126.3 netmask 255.255.255.0 broadcast 10.30.126.255
ether 02:42:0a:1e:7e:03 txqueuelen 0 (Ethernet)
RX packets 1564 bytes 140051 (136.7 KiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 1913 bytes 1571910 (1.4 MiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
inet 127.0.0.1 netmask 255.0.0.0
loop txqueuelen 1000 (Local Loopback)
RX packets 3188 bytes 864652 (844.3 KiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 3188 bytes 864652 (844.3 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
nmap 10.30.126.2 -p- -T5 -v --open
Starting Nmap 7.92 (https://nmap.org) at 2022-12-04 23:22 UTC
Initiating ARP Ping Scan at 23:22
Scanning 10.30.126.2 [1 port]
Completed ARP Ping Scan at 23:22, 0.06s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 23:22
Completed Parallel DNS resolution of 1 host. at 23:22, 0.00s elapsed
Initiating SYN Stealth Scan at 23:22
Scanning prtluq_struts2_1.prtluq (10.30.126.2) [65535 ports]
Discovered open port 8080/tcp on 10.30.126.2
Discovered open port 8009/tcp on 10.30.126.2
Completed SYN Stealth Scan at 23:22, 0.77s elapsed (65535 total ports)
Nmap scan report for prtluq_struts2_1.prtluq (10.30.126.2)
Host is up (0.0000070s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE
8009/tcp open ajp13
8080/tcp open http-proxy
MAC Address: 02:42:0A:1E:7E:02 (Unknown)
Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 1.01 seconds
Raw packets sent: 65536 (2.884MB) | Rcvd: 65536 (2.621MB)
#

Εικόνα 61.

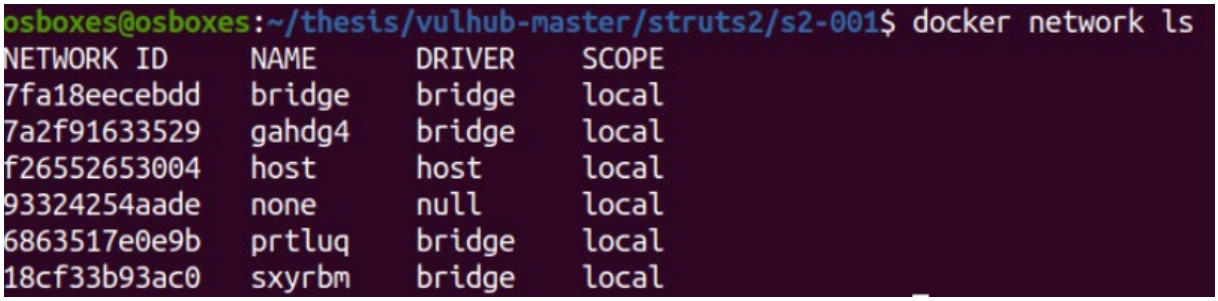
Εικόνα 62.

Εικόνα 63.

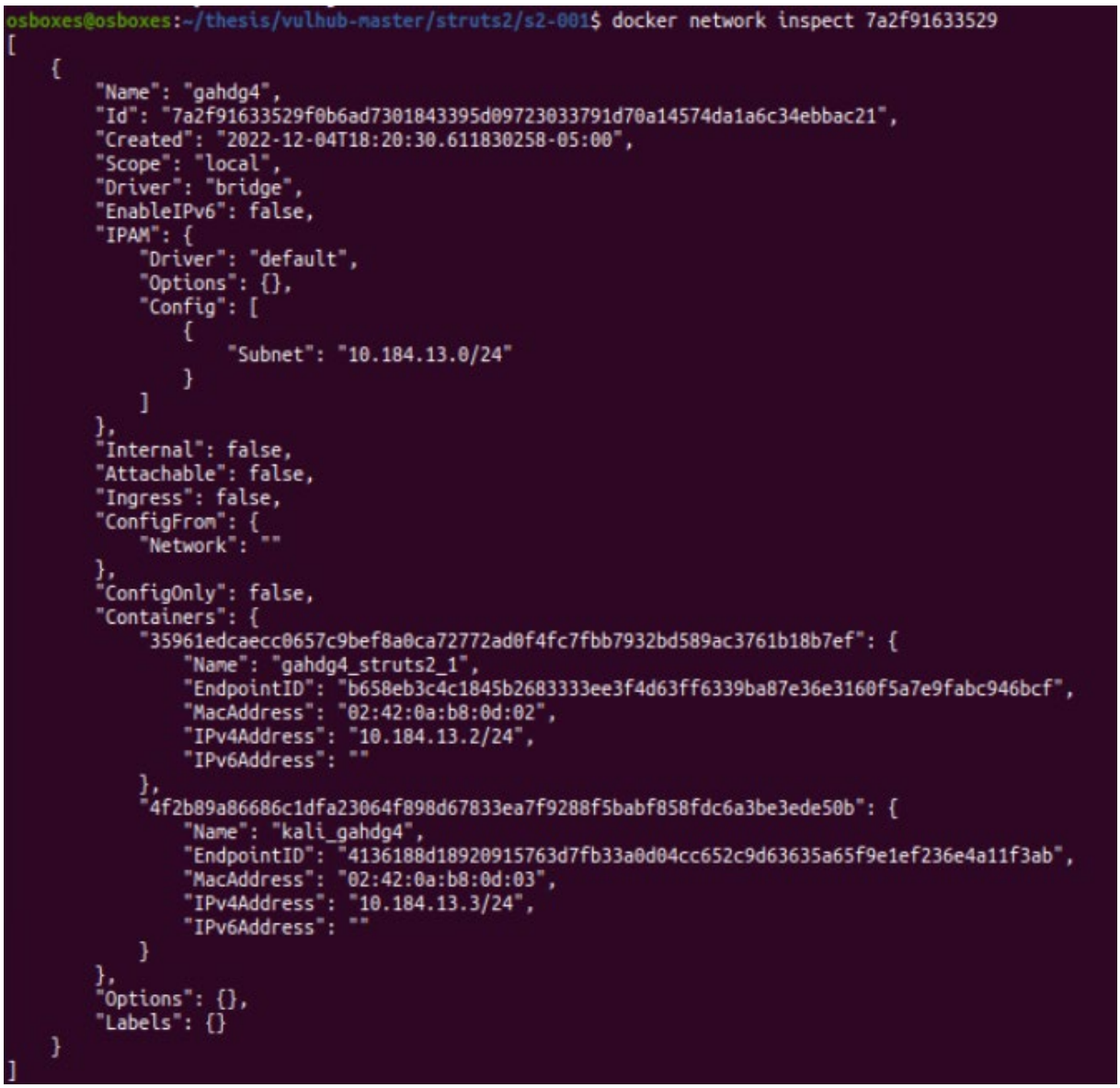
Στις παραπάνω εικόνες βλέπουμε ότι υπάρχει σωστή επικοινωνία μεταξύ κάθε στιγμιότυπο του λειτουργικού συστήματος Kali Linux τοθ χρήστη και των μηχανημάτων-στόχων αντίστοιχα, που έχουν ξεκινήσει από κάθε χρήστη. Τα μηχανήματα-στόχοι που ξεκίνησαν οι χρήστες είναι όμοια γι αυτό το λόγο και το αποτέλεσμα της εντολής nmap παρουσιάζει και στις τρείς περιπτώσεις δύο πόρτες.

3. Έλεγχος σωστής δημιουργίας απομονωμένων εικονικών δικτύων

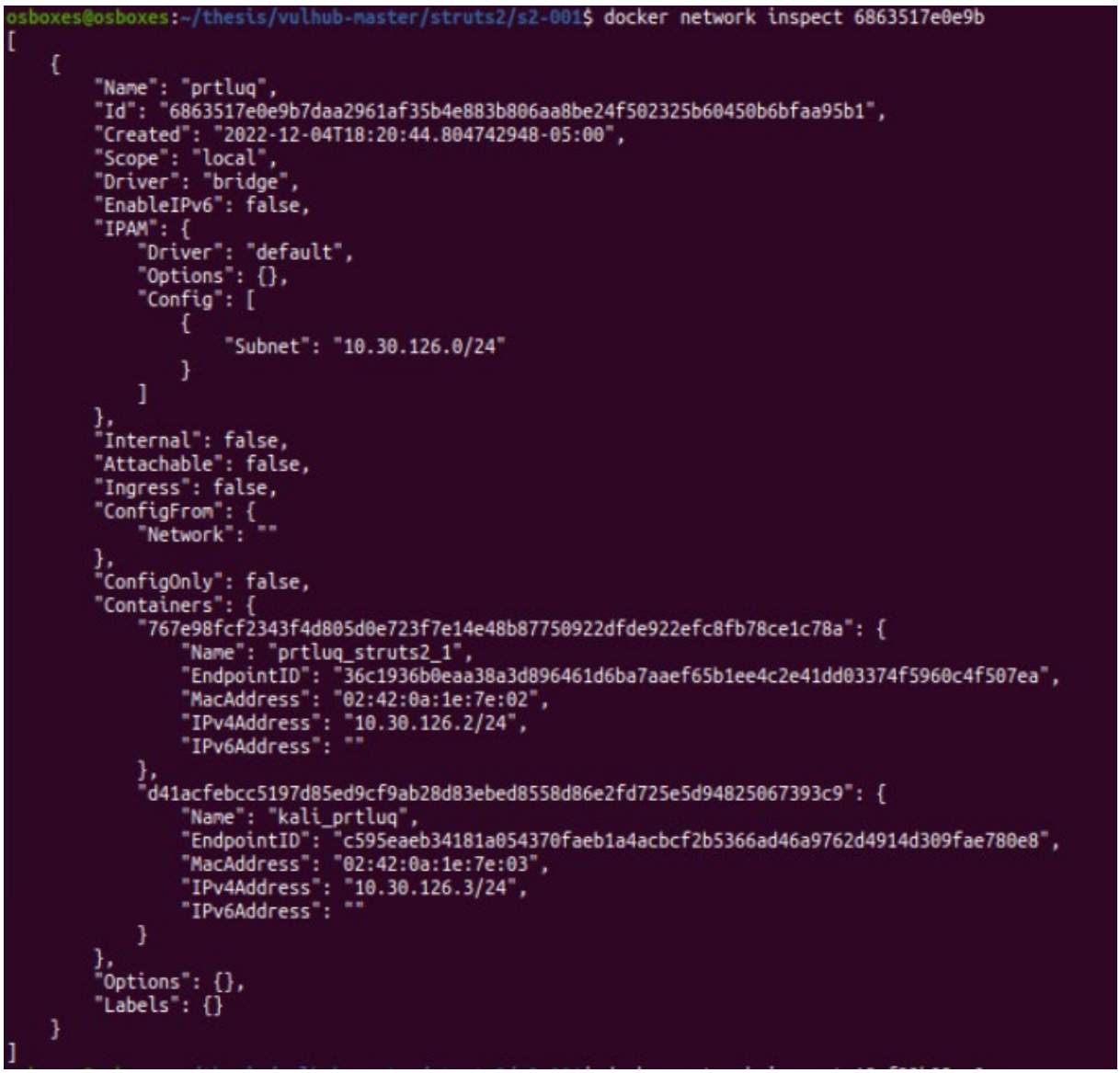
Όπως αναφέρθηκε στην περιγραφή των βασικών χαρακτηριστικών της πλατφόρμας, προβλέφθηκε η δημιουργία ξεχωριστών απομονωμένων δικτύων για κάθε χρήστη που συμμετέχει στην πλατφόρμα και εκπαιδεύεται με τη χρήση της. Σκοπός αυτών αυτής της λογικής είναι να αποφευχθεί η πιθανότητα κάποιος χρήστης να επιχειρήσει να «ενοχλήσει» κάποιον άλλο χρήστη χτυπώντας το μηχάνημα-στόχο του με τέτοιο τρόπο ώστε ο χρήστης να μη μπορεί να εκτελέσει κανονικά όποια ενέργεια επιθυμεί. Στις επόμενες εικόνες παρουσιάζεται η σωστή δημιουργία αυτών των απομονωμένων δικτύων.



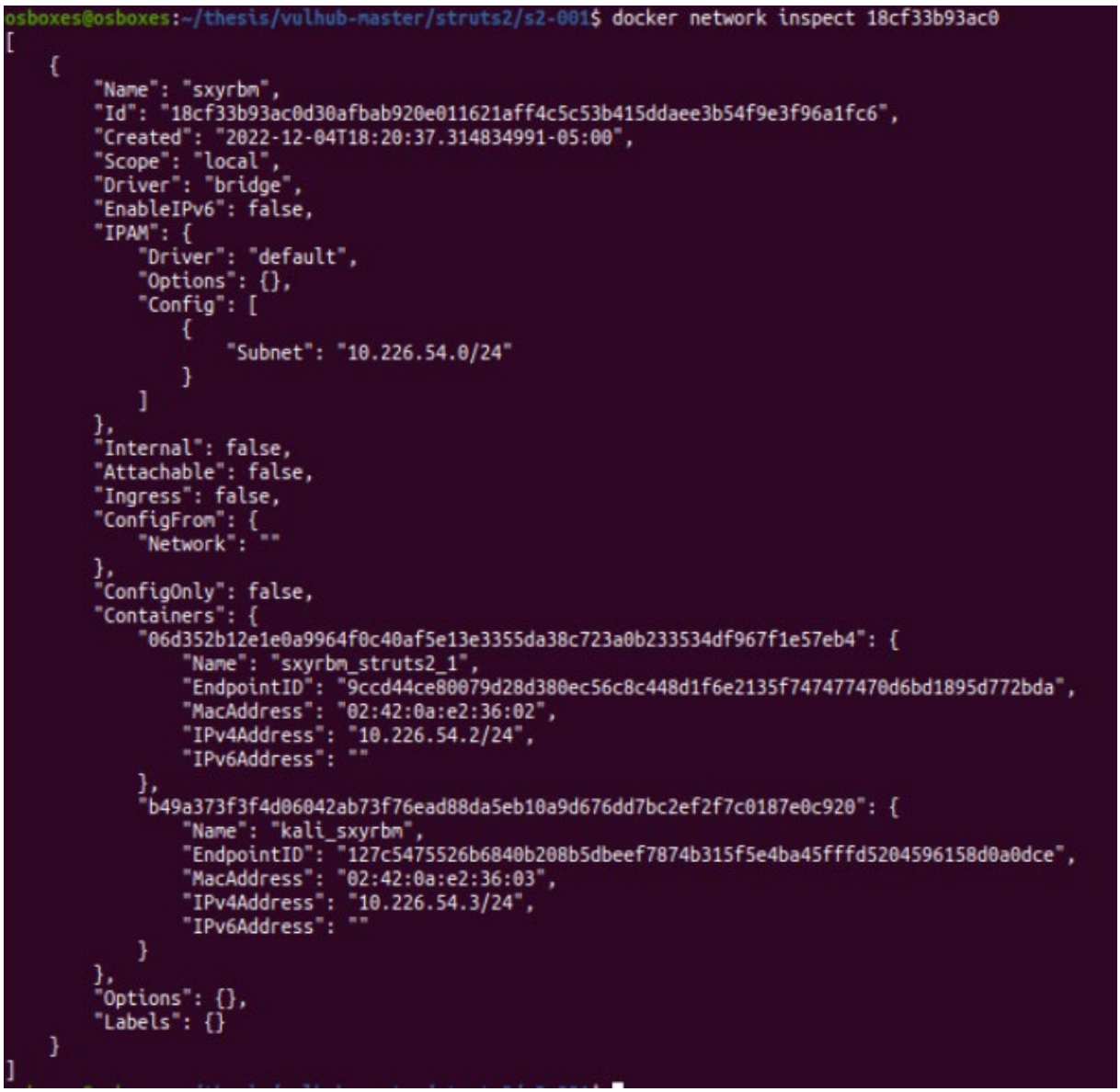
Εικόνα 64.


osboxes@osboxes:~/thesis/vulhub-master/struts2/s2-001$ docker network inspect 7a2f91633529
[
{
"Name": "gahdg4",
"Id": "7a2f91633529f0b6ad7301843395d09723033791d70a14574da1a6c34ebbac21",
"Created": "2022-12-04T18:20:30.611830258-05:00",
"Scope": "local",
"Driver": "bridge",
"EnableIPv6": false,
"IPAM": {
"Driver": "default",
"Options": {},
"Config": [
{
"Subnet": "10.184.13.0/24"
}
]
},
"Internal": false,
"Attachable": false,
"Ingress": false,
"ConfigFrom": {
"Network": ""
},
"ConfigOnly": false,
"Containers": {
"35961edcaecc0657c9bef8a0ca72772ad0f4fc7fbb7932bd589ac3761b18b7ef": {
"Name": "gahdg4_struts2_1",
"EndpointID": "b658eb3c4c1845b2683333ee3f4d63ff6339ba87e36e3160f5a7e9fabc946bcf",
"MacAddress": "02:42:0a:b8:0d:02",
"IPv4Address": "10.184.13.2/24",
"IPv6Address": ""
},
"4f2b89a86686c1dfa23064f898d67833ea7f9288f5babf858fdc6a3be3ede50b": {
"Name": "kali_gahdg4",
"EndpointID": "4136188d18920915763d7fb33a0d04cc652c9d63635a65f9e1ef236e4a11f3ab",
"MacAddress": "02:42:0a:b8:0d:03",
"IPv4Address": "10.184.13.3/24",
"IPv6Address": ""
}
},
"Options": {},
"Labels": {}
}
]

Εικόνα 65.


osboxes@osboxes:~/thesis/vulhub-master/struts2/s2-001$ docker network inspect 6863517e0e9b
[
{
"Name": "prtluq",
"Id": "6863517e0e9b7daa2961af35b4e883b806aa8be24f502325b60450b6bfaa95b1",
"Created": "2022-12-04T18:20:44.804742948-05:00",
"Scope": "local",
"Driver": "bridge",
"EnableIPv6": false,
"IPAM": {
"Driver": "default",
"Options": {},
"Config": [
{
"Subnet": "10.30.126.0/24"
}
]
},
"Internal": false,
"Attachable": false,
"Ingress": false,
"ConfigFrom": {
"Network": ""
},
"ConfigOnly": false,
"Containers": {
"767e98fcf2343f4d805d0e723f7e14e48b87750922dfde922efc8fb78ce1c78a": {
"Name": "prtluq_struts2_1",
"EndpointID": "36c1936b0eaa38a3d896461d6ba7aaef65b1ee4c2e41dd03374f5960c4f507ea",
"MacAddress": "02:42:0a:1e:7e:02",
"IPv4Address": "10.30.126.2/24",
"IPv6Address": ""
},
"d41acfebcc5197d85ed9cf9ab28d83ebed8558d86e2fd725e5d94825067393c9": {
"Name": "kali_prtluq",
"EndpointID": "c595eaeb34181a054370faeb1a4acbcf2b5366ad46a9762d4914d309fae780e8",
"MacAddress": "02:42:0a:1e:7e:03",
"IPv4Address": "10.30.126.3/24",
"IPv6Address": ""
}
},
"Options": {},
"Labels": {}
}
]

Εικόνα 66.



Εικόνα 67.

Σε όλες τις παραπάνω εικόνες παρατηρούμε την σωστή δημιουργία των απομονωμένων δικτύων, κάθε μηχάνημα-στόχος βρίσκεται στο ίδιο subnet με το αντίστοιχο στιγμιότυπο του λειτουργικού συστήματος Kali Linux και κάθε subnet είναι τελείως διαφορετικό με τα υπόλοιπα. Άρα κανείς χρήστης δεν μπορεί να επηρεάσει με κάποιο τρόπο την διαδικασία εκπαίδευσης του άλλου.

4. Σωστός τερματισμός μηχανήματος-στόχου και Kali Linux λειτουργικού συστήματος.

Ο σωστός τερματισμός υλοποιείται με το πάτημα του κουμπιού “Stop Box/Kali”. Κατά το πάτημα του κουμπιού ένα αίτημα τερματισμού στέλνεται στο Flask Script το οποίο με τη σειρά του σταματάει και αφαιρεί τα μηχανήματα καθώς και τα στιγμιότυπα του

λειτουργικού συστήματος Kali Linux. Ακολουθούν εικόνες που δείχνουν τα μηχανήματα-στόχους αλλά και τα λειτουργικά Kali Linux πριν και μετά την αποστολή του αιτήματος τερματισμού τους καθώς επίσης και εικόνα του output του Flask Script που εκτελεί τις λειτουργίες που μόλις αναφέρθηκαν.

Πριν τον τερματισμό

```
osboxes@osboxes:~/thesis/vulhub-master/struts2/s2-001$ docker ps
CONTAINER ID   IMAGE            COMMAND             CREATED          STATUS          PORTS
                                                                                    NAMES
d41acfebcc51   kali-updated     "/bin/bash"         32 minutes ago   Up 32 minutes   59000/tcp, 0.0.0.0:
22366->5900/tcp, :::22366->5900/tcp, 0.0.0.0:52882->5901/tcp, :::52882->5901/tcp   kali_prtluq
b49a373f3f4d   kali-updated     "/bin/bash"         33 minutes ago   Up 33 minutes   59000/tcp, 0.0.0.0:
28830->5900/tcp, :::28830->5900/tcp, 0.0.0.0:34267->5901/tcp, :::34267->5901/tcp   kali_sxyrbm
4f2b89a86686   kali-updated     "/bin/bash"         33 minutes ago   Up 33 minutes   59000/tcp, 0.0.0.0:
51013->5900/tcp, :::51013->5900/tcp, 0.0.0.0:14596->5901/tcp, :::14596->5901/tcp   kali_gahdg4
767e98fcf234   prtluq_struts2   "catalina.sh run"   33 minutes ago   Up 33 minutes   8080/tcp
                                                                                    prtluq_struts2_1
06d352b12e1e   sxyrbm_struts2   "catalina.sh run"   33 minutes ago   Up 33 minutes   8080/tcp
                                                                                    sxyrbm_struts2_1
35961edcaecc   gahdg4_struts2   "catalina.sh run"   33 minutes ago   Up 33 minutes   8080/tcp
                                                                                    gahdg4_struts2_1
```

Εικόνα 68.

Output Flask Script κατά τη λήψη αιτήματος τερματισμού από τους χρήστες

```
osboxes@osboxes:~/thesis/Box_Conf$ python3 play.py
 * Serving Flask app 'play' (lazy loading)
 * Environment: production
   WARNING: This is a development server. Do not use it in a production deployment.
   Use a production WSGI server instead.
 * Debug mode: on
 * Running on http://127.0.0.1:8889/ (Press CTRL+C to quit)
 * Restarting with stat
 * Debugger is active!
 * Debugger PIN: 100-278-284
About to run return response function
127.0.0.1 - - [04/Dec/2022 18:20:30] "GET /spawn?uuid=af7f040c-94e7-4638-9b01-4be48d09ef7f&user_handle=player HTTP/
1.1" 200 -
Hitting exit point as machine was already downloaded and is now loaded.
About to run return response function
127.0.0.1 - - [04/Dec/2022 18:20:37] "GET /spawn?uuid=af7f040c-94e7-4638-9b01-4be48d09ef7f&user_handle=player1 HTTP
/1.1" 200 -
Hitting exit point as machine was already downloaded and is now loaded.
About to run return response function
127.0.0.1 - - [04/Dec/2022 18:20:44] "GET /spawn?uuid=af7f040c-94e7-4638-9b01-4be48d09ef7f&user_handle=player2 HTTP
/1.1" 200 -
Hitting exit point as machine was already downloaded and is now loaded.
Hitting exit point as machine is now on systen and already loaded.
127.0.0.1 - - [04/Dec/2022 18:20:53] "GET /kali_instance?euuid=af7f040c-94e7-4638-9b01-4be48d09ef7f@gahdg4 HTTP/1.1
" 200 -
127.0.0.1 - - [04/Dec/2022 18:20:56] "GET /kali?opts={%22resolution%22:%22952x656%22,%22euuidN22:%22af7f040c-94e7-4
638-9b01-4be48d09ef7f@gahdg4%22} HTTP/1.1" 200 -
127.0.0.1 - - [04/Dec/2022 18:21:04] "GET /kali_instance?euuid=af7f040c-94e7-4638-9b01-4be48d09ef7f@sxyrbm HTTP/1.1
" 200 -
127.0.0.1 - - [04/Dec/2022 18:21:07] "GET /kali?opts={%22resolution%22:%22952x656%22,%22euuidN22:%22af7f040c-94e7-4
638-9b01-4be48d09ef7f@sxyrbm%22} HTTP/1.1" 200 -
127.0.0.1 - - [04/Dec/2022 18:21:14] "GET /kali_instance?euuid=af7f040c-94e7-4638-9b01-4be48d09ef7f@prtluq HTTP/1.1
" 200 -
127.0.0.1 - - [04/Dec/2022 18:21:17] "GET /kali?opts={%22resolution%22:%221920x843%22,%22euuidN22:%22af7f040c-94e7-
4638-9b01-4be48d09ef7f@prtluq%22} HTTP/1.1" 200 -
Docker(s) stopped successfully
Docker(s) wiped successfully
Docker networks wiped successfully
Docker file removed successfully
Database entry wiped successfully
127.0.0.1 - - [04/Dec/2022 21:37:17] "GET /undeploy?euuid=af7f040c-94e7-4638-9b01-4be48d09ef7f@gahdg4 HTTP/1.1" 200
-
Docker(s) stopped successfully
Docker(s) wiped successfully
Docker networks wiped successfully
Docker file removed successfully
Database entry wiped successfully
127.0.0.1 - - [04/Dec/2022 21:37:20] "GET /undeploy?euuid=af7f040c-94e7-4638-9b01-4be48d09ef7f@sxyrbm HTTP/1.1" 200
-
127.0.0.1 - - [04/Dec/2022 21:37:22] "GET /undeploy?euuid=af7f040c-94e7-4638-9b01-4be48d09ef7f@gahdg4 HTTP/1.1" 200
-
Docker(s) stopped successfully
Docker(s) wiped successfully
Docker networks wiped successfully
Docker file removed successfully
Database entry wiped successfully
127.0.0.1 - - [04/Dec/2022 21:37:25] "GET /undeploy?euuid=af7f040c-94e7-4638-9b01-4be48d09ef7f@prtluq HTTP/1.1" 200
-
127.0.0.1 - - [04/Dec/2022 21:37:25] "GET /undeploy?euuid=af7f040c-94e7-4638-9b01-4be48d09ef7f@sxyrbm HTTP/1.1" 200
-
127.0.0.1 - - [04/Dec/2022 21:37:30] "GET /undeploy?euuid=af7f040c-94e7-4638-9b01-4be48d09ef7f@prtluq HTTP/1.1" 200
-
```

Εικόνα 69.

Μετά τον τερματισμό

```
osboxes@osboxes:~/thesis/vulhub-master/struts2/s2-001$ docker ps
CONTAINER ID   IMAGE     COMMAND   CREATED   STATUS    PORTS     NAMES
osboxes@osboxes:~/thesis/vulhub-master/struts2/s2-001$
```

Εικόνα 70.

Όπως φαίνεται από τις παραπάνω εικόνες, μετά τις ενέργειες του Flask Script για τον τερματισμό των μηχανημάτων-στόχων και των στιγμιότυπων του λειτουργικού συστήματος Kali Linux, η εντολή εμφάνισης των running docker στο σύστημα (docker ps) δεν επιστρέφει τίποτα άρα όλα τα docker που φαίνονται στην εικόνα 68 τερματίστηκαν επιτυχώς.

5. **Έλεγχος διαγραφής των docker compose αρχείων που δημιουργούνται "on the fly" για το ίδιο μηχάνημα-στόχο.**

Πριν τον τερματισμό

```
osboxes@osboxes:~/thesis/vulhub-master/struts2/s2-001$ ls -la
total 3640
drwxrwxr-x  2 osboxes osboxes    4096 Dec  4 18:20 .
drwxrwxr-x 20 osboxes osboxes    4096 Jan  5  2022 ..
-rw-rw-r--  1 osboxes osboxes  390217 Jan  5  2022 1.jpeg
-rw-rw-r--  1 osboxes osboxes     141 Dec  4 18:20 docker-compose-gahdg4.yml
-rw-rw-r--  1 osboxes osboxes     141 Dec  4 18:20 docker-compose-prtluq.yml
-rw-rw-r--  1 osboxes osboxes     141 Dec  4 18:20 docker-compose-sxyrbm.yml
-rw-rw-r--  1 osboxes osboxes      72 Jan  5  2022 docker-compose.yml
-rw-rw-r--  1 osboxes osboxes     239 Jan  5  2022 Dockerfile
-rw-rw-r--  1 osboxes osboxes    1821 Jan  5  2022 README.md
-rw-rw-r--  1 osboxes osboxes    1665 Jan  5  2022 README.zh-cn.md
-rw-rw-r--  1 osboxes osboxes 3296352 Jan  5  2022 S2-001.war
```

Εικόνα 71.

Μετά τον τερματισμό

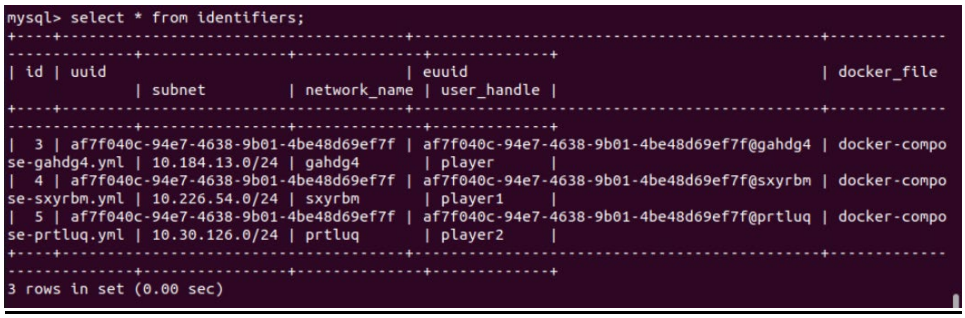
```
osboxes@osboxes:~/thesis/vulhub-master/struts2/s2-001$ ls -la
total 3628
drwxrwxr-x  2 osboxes osboxes    4096 Dec  4 15:11 .
drwxrwxr-x 20 osboxes osboxes    4096 Jan  5  2022 ..
-rw-rw-r--  1 osboxes osboxes  390217 Jan  5  2022 1.jpeg
-rw-rw-r--  1 osboxes osboxes      72 Jan  5  2022 docker-compose.yml
-rw-rw-r--  1 osboxes osboxes     239 Jan  5  2022 Dockerfile
-rw-rw-r--  1 osboxes osboxes    1821 Jan  5  2022 README.md
-rw-rw-r--  1 osboxes osboxes    1665 Jan  5  2022 README.zh-cn.md
-rw-rw-r--  1 osboxes osboxes 3296352 Jan  5  2022 S2-001.war
```

Εικόνα 72.

Όπως φαίνεται στην παραπάνω εικόνα τα αρχεία των μηχανημάτων-στόχων έχουν διαγραφεί επιτυχώς καθώς στη διαδρομή συστήματος του συγκεκριμένου μηχανήματος υπάρχει μόνο το base docker compose file (docker-compose.yml).

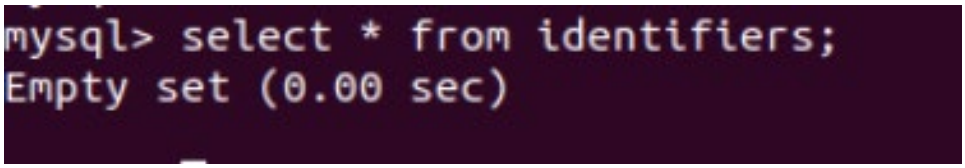
6. **Έλεγχος διαγραφής των MySQL δεδομένων που διατηρούνται στη βάση για τη σωστή λειτουργία των μηχανημάτων-στόχων και του λειτουργικού συστήματος Kali Linux.**

Πριν τον τερματισμό



Εικόνα 73.

Μετά τον τερματισμό



Εικόνα 74.

Στην εικόνα 74 βλέπουμε ότι και οι εγγραφές της βάσης MySQL που αφορούσαν τα running docker των μηχανημάτων-στόχων αλλά και του λειτουργικού συστήματος Kali Linux, διεγράφησαν επιτυχώς.

4.2 Συμπέρασμα

Από όλα τα παραπάνω συμπεραίνουμε ότι οι έλεγχοι που πραγματοποιήθηκαν στους τομείς που αναφέρθηκαν στην αρχή του κεφαλαίου τέσσερα (4) ήταν επιτυχείς. Η πλατφόρμα ελέχθη από τρία άτομα ταυτόχρονα και διαπιστώθηκε ότι:

- Υπάρχει σωστή επικοινωνία μεταξύ των στιγμιότυπων του λειτουργικού συστήματος Kali Linux και των μηχανημάτων-στόχων
- Το Flask Application δημιουργεί σωστά τα απομονωμένα εικονικά δίκτυα
- Το Flask Application τερματίζει σωστά τα μηχανήματα-στόχους και τα στιγμιότυπα του λειτουργικού συστήματος Kali Linux

- Το Flask Application διαγράφει σωστά τα αρχεία docker που χρησιμοποιούνται για την εκκίνηση των μηχανημάτων-στόχων
- Το Flask Application διαγράφει σωστά τις εγγραφές της βάσης MySQL που αφορούν τα μηχανήματα-στόχους αλλά και τα στιγμιότυπα του λειτουργικού συστήματος Kali Linux

Κεφάλαιο 5
Επίλογος

5.1 Σύνοψη

Στην ενότητα αυτή θα πραγματοποιήσουμε μια ανασκόπηση σε ότι έχει αναλυθεί στα προηγούμενα κεφάλαια της παρούσας διατριβής. Αναλύθηκε η σημασία του τρόπου αλλαγής εκπαίδευσης πάνω στο ειδικευμένο αντικείμενο της κυβερνοασφάλειας λόγω της δυσκολία εκμάθησης του αντικειμένου αλλά και του ελάχιστου χρόνου που διατίθεται από τα πανεπιστημιακά ιδρύματα για την διδασκαλία του. Έτσι καταλήξαμε ότι η εκμάθηση του συγκεκριμένου αντικειμένου μέσα από την παιχνιδοποιημένη εκπαίδευση μπορεί πραγματικά να αποδώσει. Στη συνέχεια παρουσιάσαμε και αναλύσαμε διεξοδικά όλες τις διαθέσιμες πλατφόρμες που επιτρέπουν την εκπαίδευση των συμμετεχόντων πάνω στην κυβερνοασφάλεια, τα δυνατά τους στοιχεία, τις αδυναμίες τους αλλά και κάποια από τα τεχνικά τους χαρακτηριστικά. Τέλος, επιλέχθηκε η ανοιχτού κώδικα πλατφόρμα RootTheBox καθώς ήταν αυτή που συγκέντρωνε τα περισσότερα πλεονεκτήματα ή τα λιγότερα μειονεκτήματα αντίστοιχα και τροποποιήθηκε σε μεγάλο βαθμό ο κώδικας της πλατφόρμας ώστε να μειωθούν οι υπολογιστικοί πόροι που ζητά από το λειτουργικό σύστημα που την φιλοξενεί αλλά και να παρέχει στους εκπαιδευόμενους χαρακτηριστικά που η ίδια δεν διέθετε πριν.

5.2 Περιοχές Βελτίωσης

Η παρούσα διατριβή παρουσίασε μια βελτιωμένη έκδοση της πλατφόρμας ανοιχτού κώδικα RootTheBox που απαιτεί λιγότερους υπολογιστικούς πόρους από το λειτουργικό σύστημα που τη φιλοξενεί αλλά παρουσιάζει επίσης και νέα χαρακτηριστικά που η ίδια δεν διέθετε πριν. Οι αλλαγές αυτές έγιναν πράξη μέσω της εκτεταμένης τροποποίησης κώδικα που υπέστη σε υπάρχον κώδικα αλλά και με τη βοήθεια ενός Flask Application που δημιουργήθηκε για τις ανάγκες της διατριβής και που προσδίδει την πλατφόρμα όλα αυτά τα νέα χαρακτηριστικά που αναλύθηκαν διεξοδικά στα προηγούμενα κεφάλαια. Ενώ οι αλλαγές αυτές είναι ένα σημαντικό βήμα στην ανάδειξη της τροποποιημένης έκδοσης της πλατφόρμας RootTheBox ως μία ικανοποιητική λύση για τη χρήση της από άτομα που θέλουν να εκπαιδευτούν πάνω στο αντικείμενο της κυβερνοασφάλειας, σίγουρα υπάρχουν και χαρακτηριστικά που θα πρέπει να εισαχθούν ως μελλοντικές βελτιώσεις ώστε να κάνουν την επιλογή αυτής της τροποποιημένης εκδοχής της πλατφόρμας, ιδανική για κάθε ενδιαφερόμενο που εκπαιδεύεται στο αντικείμενο της κυβερνοασφάλειας μέσω της παιχνιδοποιημένης εκμάθησης.

Οι βελτιώσεις αυτές είναι οι ακόλουθες:

- Υποστήριξη Windows μηχανημάτων-στόχων είτε με τη χρήση docker είτε μέσω συνεργασίας της πλατφόρμας με εικονικές μηχανές Windows.
- Υποστήριξη Active Directory Περιβάλλοντος για εκπαίδευση πάνω σε περιβάλλοντα που προσομοιάζουν εταιρικά δίκτυα.
- Εισαγωγή multi-threading μηχανισμού για καλύτερη και ταχύτερη υποστήριξη περισσότερων συμμετεχόντων.
- Δυνατότητα σύνδεσης των προσωπικών υπολογιστών των συμμετεχόντων στα απομονωμένα εικονικά δίκτυα που βρίσκονται τα μηχανήματα στόχοι ώστε οι χρήστες να έχουν μια επιπλέον επιλογή ως προς το λειτουργικό σύστημα που θα χρησιμοποιήσουν αν δεν καλύπτονται από το Kali Linux που δίδεται ως λύση.
- Εισαγωγή κέλυφους (shell) στον λογαριασμό του διαχειριστή της πλατφόρμας για διαχείριση όλων των μηχανημάτων αποκλειστικά μέσα από την πλατφόρμα RootTheBox.
- Δυνατότητα μηχανισμού reset των μηχανημάτων στόχων. Οι χρήστες μπορεί να είναι οι μοναδικοί που εκπαιδεύονται πάνω στα μηχανήματα στόχους, λόγο της χρήσης τεχνολογίας docker, αλλά σε περίπτωση που το μηχάνημα στόχος τεθεί εκτός λειτουργίας λόγο κάποιας ενέργειας του χρήστη, θα ήταν καλό να υπάρχει η δυνατότητα reset του μηχανήματος αντί για τον τερματισμό του και την ενεργοποίηση του.
- Δυνατότητα δημιουργίας ενός τυχαίου αλλά σταθερού εύρους απομονωμένου δικτύου για κάθε συμμετέχοντα ώστε όλα τα μηχανήματα στόχοι να ανήκουν σε αυτό το εύρος, αντί για δημιουργία τυχαίων μεμονωμένων δικτύων για τον ίδιο χρήστη κάθε φορά που θέλει να εκπαιδευτεί σε ένα διαφορετικό μηχάνημα-στόχο.
- Προβολή διευθύνσεων IP μηχανημάτων στόχων και στιγμιότυπων λειτουργικού Kali Linux σε κάθε ενότητα μηχανήματος.
- Ανάθεση σταθερών IP διευθύνσεων σε κάθε μηχάνημα-στόχο και στιγμιότυπο λειτουργικού συστήματος Kali Linux.

Βιβλιογραφία

1. moloch. (2022, June 12). *RootTheBox*. Retrieved from github.com: https://github.com/moloch--/RootTheBox
2. H. Gonzalez, R. L. (2017). Cybersecu-rity teaching through gamification: Aligning training resources to our syllabus. *Res. Comput. Sci.*, (pp. 35-43).
3. M. Malone, Y. W. (2021). M. Malone, Y. Wang, K. James, M. Anderegg,J. Werner, and F. Monrose, “To gamify or not? on leaderboard effects, student engagement and learning outcomes in a cybersecurity intervention. 1135–1141. New York, NY, USA.
4. HackTheBox. (2022). *HackTheBox*. Retrieved from hackthebox.eu: https://www.hackthebox.eu/
5. TryHackMe. (2022). *TryHackMe*. Retrieved from tryhackme.com: https://tryhackme.com/
6. RootMe. (2022). *RootMe*. Retrieved from root-me.org: https://www.root-me.org
7. PortSwigger. (n.d.). *web-security*. Retrieved from portswigger.net: https://portswigger.net/web-security
8. internetwache. (2021, March 28). *Internetwache-CTF-2016*. Retrieved from github.com: https://github.com/internetwache/Internetwache-CTF-2016/blob/master/README.tinyctf.md
9. University, C. M. (2022). *picoCTF - CMU CyberSecurity Competition*. Retrieved from picoctf.org: https://picoctf.org/
10. HashiCorp. (2022). *Vagrant by HashiCorp*. Retrieved from vagrantup.com: https://www.vagrantup.com/
11. DefCon26. (n.d.). *Welcome to OpenCTF*. Retrieved from openctf.com: http://openctf.com/
12. *stack - npm*. (2022). Retrieved from npmjs.com: https://www.npmjs.com/package/stack
13. Facebook. (2022). *Facebook*. Retrieved from facebook.com: https://m.facebook.com/nt/screen/?params={%22note_id%22%3A2819180938304567}&path=%2Fnotes%2Fnote%2F&refsrc=deprecated&_rdr
14. moloch. (2022, July 12). *RootTheBox*. Retrieved from https://github.com: https://github.com/moloch--/RootTheBox
15. *CyberChef*. (2022). Retrieved from github.io: https://gchq.github.io/CyberChef/
16. UnrealAkama. (2017, March 28). *A simple capture the flag framework*. Retrieved from github.com: https://github.com/UnrealAkama/NightShade

17. shellphish. (2022, June 29). *The iCTF Framework, presented by Shellphish!* Retrieved from github.com: https://github.com/shellphish/ictf-framework

18. pomo-mondreganto. (2022, August 16). *Pure-python distributable Attach-Defence CTF platform, created to be easily set up.* Retrieved from github.com: https://github.com/pomo-mondreganto/ForcAD

19. sea-kg. (2022, September 2). *Jury System for attack-defence ctf game (ctf-scoreboard). Or you can use it for training.* Retrieved from github.com: https://github.com/sea-kg/ctf01d

20. *Docker: Accelerated, Containerized Application Development*. (2022). Retrieved from docker.com: https://www.docker.com/

21. Joel Martin, S. M. (2022). *noVNC*. Retrieved from novnc.com: https://novnc.com/info.html

22. *VNC-Compatible Free Remote Control / Remote Desktop Software*. (2022). Retrieved from tightvnc.com: https://www.tightvnc.com/

23. mozilla. (2022). *Window.localStorage - Web APIs | MDN*. Retrieved from mozilla.org: https://developer.mozilla.org/en-US/docs/Web/API/Window/localStorage