Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Μεταπτυχιακή Διατριβή
Στην Ασφάλεια Υπολογιστών και Δικτύων

Machine Learning for Red Team Attacks in Cyber Range

Παναγιώτα Ιωάννου

Επιβλέπουσα Καθηγήτρια
Δρ. Αδαμαντίνη Περατικού

Μάιος 2023

Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Machine Learning for Red Team Attacks in Cyber Range

Παναγιώτα Ιωάννου

Επιβλέπουσα Καθηγήτριας
Δρ. Αδαμαντίνη Περατικού

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

Μάιος 2023

Περίληψη

Η ραγδαία ανάπτυξη της τεχνολογίας έχει συμβάλει στη βελτίωση σε διάφορους τομείς της ζωής των ανθρώπων οι οποίοι βασίζουν τις δραστηριότητες τους, την επεξεργασία και την αποθήκευση των δεδομένων στα πληροφοριακά συστήματα όπου αναπόφευκτα γίνονται συχνοί στόχοι κακόβουλων επιθέσεων στον κυβερνοχώρο. Η εισαγωγή της μηχανικής μάθησης έχει σαν κύριο μέλημα να βελτιώσει τη λειτουργία των υφιστάμενων συστημάτων σε διάφορους τομείς θέτοντας ως προτεραιότητα την αποτροπή πιθανών επιθέσεων από τους κυβερνοεγκληματίες. Η αποτροπή αυτή επιτυγχάνετε μέσο της διαδικασίας δοκιμής διείσδυσης, η οποία εκτελείται από τις διάφορες ομάδες «Red Teams» με σκοπό την διερεύνηση, τον εντοπισμό και την βελτίωση των διαφόρων ευάλωτων σημείων στα πληροφοριακά συστήματα. Συνεπώς η συνεχής εκπαίδευση των ομάδων αυτών σε νέες τεχνολογίες και η επίγνωση τους στα νέα διαθέσιμα εργαλεία είναι αναπόφευκτο στοιχείο ώστε να τους καθιστά εξίσου ευρηματικούς και επίδοξους όσο τους κυβερνοεγκληματίες.

Στόχος της παρούσας μεταπτυχιακής διατριβής είναι η εις βάθος διερεύνηση των υφιστάμενων εργαλείων μηχανικής μάθησης που χρησιμοποιούνται κατά τη διαδικασία δοκιμής διείσδυσης, η αξιολόγηση της λειτουργικότητας και της αποτελεσματικότητας τους στην συλλογή πληροφορίων και στον εντοπισμό των ευπαθειών των πληροφοριακών συστημάτων. Επιπρόσθετα, γίνεται χρήση των εργαλείων αυτών που έχουν επιλεγεί σε εικονικές επιθέσεις στο περιβάλλον «Cyber Range» ώστε να καταστεί εφικτή η εξοικείωση και εκπαίδευση των «Red Teams» στα εργαλεία αυτά.

Summary

The rapid development of technology has contributed to the improvement in various domains in people's lives who base their activities, the processing and storage of their data on information systems which they inevitably become frequent targets of malicious cyber-attacks. The introduction of Machine Learning has its main concern to improve the functionality of the existing systems in various sectors by prioritizing the prevention of potential attacks by cybercriminals. The prevention is achieved through the Penetration Testing process, which is performed by the "Red Teams" in order to investigate, identify and improve the vulnerabilities in the information systems. Therefore, the continuous training of these teams in new technologies and their awareness of the new available tools is inevitable in order to make them as resourceful and ambitious as cybercriminals.

The aim of this master's dissertation is the in-depth investigation of the existing Machine Learning tools that are used during the Penetration Testing process, the evaluation of their functionality and their effectiveness in information gathering and identifying the vulnerabilities of the information systems. Moreover, the tools that have been selected are used in virtual attacks in the "Cyber Range" environment to enable familiarization and training of the Red Teams in these tools.

Ευχαριστίες

Αρχικά θα ήθελα να ευχαριστήσω την επιβλέπουσα καθηγήτρια μου Δρ. Αδαμαντίνη Περατικού για τη στήριξη, την ενθάρρυνση και την καθοδήγηση της για την ολοκλήρωση της παρούσας Μεταπτυχιακής Διατριβής.

Επίσης θα ήθελα να ευχαριστήσω τα άτομα που με στήριξαν, μου συμπαραστάθηκαν και με βοήθησαν καθόλη την διάρκεια των σπουδών μου.

Πάνω από όλα θα ήθελα να ευχαριστήσω το άτομο που είναι πάντα δίπλα μου, με στηρίζει, με εμψυχώνει και με βοηθά να αντιμετωπίζω όλες τις δυσκολίες και τις αντιξοότητες που αντιμετωπίζω.

Περιεχόμενα

Κατάλογος Εικόνων / Πινάκων

Κεφάλαιο 1
Εισαγωγή

Στη σύγχρονη εποχή υπάρχει μια ραγδαία ανάπτυξη και χρήση του διαδικτύου, το οποίο έχει γίνει αναπόσπαστο κομμάτι της καθημερινότητας των ανθρώπων τόσο σε προσωπικό επίπεδο όσο και σε επαγγελματικό. Πλέον οι άνθρωποι και οι οργανισμοί βασίζουν τις δραστηριότητες, την αποθήκευση και την επεξεργασία των δεδομένων τους στα πληροφοριακά συστήματα όπου αναπόφευκτα γίνονται στόχος κακόβουλων επιθέσεων στον κυβερνοχώρο. Συνεπώς υπάρχει μια συνεχόμενη ανάγκη προστασίας των πληροφοριακών συστημάτων και των δεδομένων αυτών, κυριότερα στους οργανισμούς όπου βασίζουν τη λειτουργία τους στα συστήματα αυτά. Για το λόγο αυτό έχουν δημιουργηθεί διάφορες ομάδες ασφαλείας αποτελούμενες από εξειδικευμένο προσωπικό, όπως οι Κόκκινες και Μπλε ομάδες (Red and Blue Teams), όπου έχουν σκοπό να αξιολογούν, να προστατεύουν και να βελτιώνουν την ασφάλεια των πληροφοριακών συστημάτων και των δεδομένων ενός οργανισμού. Συνεπώς τα άτομα των ομάδων αυτών πρέπει να εκπαιδεύονται συνεχώς στις υφιστάμενες και νέες τεχνολογίες οι οποίες είναι πιθανόν να χρησιμοποιηθούν από εισβολείς κακόβουλα και να εισχωρήσουν στα συστήματα ενός οργανισμού προκαλώντας ζημιά είτε στα συστήματα αυτά είτε στα δεδομένα του οργανισμού.

Η Μηχανική Μάθησης (Machine Learning) είναι μια νέα τεχνολογία η οποία προσφέρει τεράστιες δυνατότητες στον κυβερνοχώρο και μπορεί να βελτιώσει τον τρόπο λειτουργίας των

υφιστάμενων συστημάτων σε διάφορους τομείς της καθημερινότητας των ανθρώπων όπως στην ιατρική, την εκπαίδευση, την οικονομία, την ψυχαγωγία κ.α. Παρόλα αυτά όμως μπορούν να χρησιμοποιηθούν κακόβουλα στον κυβερνοχώρο ώστε να βελτιώσουν τις τακτικές επιθέσεων από εισβολείς.

Συνεπώς, οι Red και Blue teams πρέπει να εκπαιδεύονται συνεχώς στην τεχνολογία του Machine Learning και στα νέα εργαλεία ώστε να είναι σε θέση να αποτρέψουν τις επιθέσεις και να προστατέψουν τα πληροφοριακά συστήματα και τα δεδομένα ενός οργανισμού. Ένα τέτοιο περιβάλλον εκπαίδευσης είναι το Cyber range στο οποίο μπορούν να δοκιμάζονται τα διάφορα εργαλεία που χρησιμοποιούν οι εισβολείς ώστε να προσομοιώσουν διάφορα σενάρια πραγματικών επιθέσεων με σκοπό να βελτιώσουν την ασφάλεια των πληροφοριακών συστημάτων και να προστατέψουν τα αγαθά ενός οργανισμού.

1.1 Αναγκαιότητα και σπουδαιότητα της έρευνας

Με την πάροδο του χρόνου η ραγδαία ανάπτυξη και χρήση του διαδικτύου τείνει να εδραιώνεται, καθιστώντας τα πληροφοριακά συστήματα όλο και πιο αναγκαία για τις καθημερινές δραστηριότητες των ανθρώπων, τόσο για τις προσωπικές τους δραστηριότητες όσο και για τις επαγγελματικές. Συνεπώς γίνεται επιτακτική η ανάγκη για προστασία των πληροφοριακών συστημάτων και των δεδομένων τους, τα οποία προσελκύουν ολοένα και περισσότερες κακόβουλες επιθέσεις. Οι εισβολείς στη προσπάθεια τους να πετύχουν το σκοπό τους και να αποκτήσουν πρόσβαση στα πληροφοριακά συστήματα ενός οργανισμού γίνονται ολοένα και πιο ευρηματικοί χρησιμοποιώντας πληθώρα νέων εργαλείων και τεχνολογιών. Για το λόγο αυτό η ανάγκη για εκπαίδευση των επαγγελματιών της κυβερνοασφάλειας στις νέες τεχνολογίες και τα εργαλεία γίνεται ακόμα πιο σημαντική. Συνεπώς κρίνεται αναγκαία η χρήση των εργαλείων Machine Learning στο περιβάλλον Cyber range όπου θα δημιουργούνται πιο έξυπνα και ρεαλιστικά σενάρια επιθέσεων αναπαριστώντας τους Red Teams. Η έρευνα αυτή θα συγκρίνει διάφορα εργαλεία Machine Learning στο περιβάλλον Cyber range δημιουργώντας σενάρια επιθέσεων των Red Team ώστε να αξιολογηθεί η αποτελεσματικότητα τους και κατ' επέκταση να βοηθήσει στην εκπαίδευση των επαγγελματιών της κυβερνοασφάλειας.

1.2 Σκοπός της Μεταπτυχιακής Διατριβής

Η παρούσα διατριβή έχει σκοπό να ερευνήσει υφιστάμενα εργαλεία Machine Learning που χρησιμοποιούνται από τις ομάδες Red Team για τον εντοπισμό ευπαθειών στα συστήματα ενός οργανισμού. Θα επικεντρωθεί στην εφαρμογή των εργαλείων αυτών σε περιβάλλον Cyber range ώστε να αξιολογηθεί η ικανότητα τους να συλλέγουν πληροφορίες από το περιβάλλον αυτό. Κατ' επέκταση θα ερευνηθεί κατά πόσο μπορούν να δημιουργηθούν διάφορα σενάρια επιθέσεων ώστε να μπορούν οι ομάδες Red Team να εξοικειωθούν και να εκπαιδευτούν στη χρήση των εργαλείων Machine Learning στο περιβάλλον Cyber range.

1.3 Βασικά Ερευνητικά Ερωτήματα

Τα ερευνητικά ερωτήματα που θα εξεταστούν στη παρούσα Μεταπτυχιακή Διατριβή είναι τα ακόλουθα:

- Κατά πόσο υπάρχουν εργαλεία Machine Learning για σκοπούς επιθέσεων Red Teaming
- Ποσό αποτελεσματικά είναι τα εργαλεία Machine Learning για Red Teaming σε περιβάλλον Cyber range
- Μπορούν να χρησιμοποιηθούν τα εργαλεία Machine Learning για εκπαιδευτικούς σκοπούς των ατόμων που απαρτίζουν τις Red Team
- Ποια εργαλεία Machine Learning είναι πιο αποδοτικά σε διάφορα σενάρια επιθέσεων Red Teaming

1.4 Οργάνωση της Μεταπτυχιακής Διατριβής

Η παρούσα Μεταπτυχιακή Διατριβή θα αποτελείται από 6 κεφάλαια ως ακολούθως:

Το κεφάλαιο 1 Εισαγωγή, θα περιλαμβάνει το σκοπό και τα ερευνητικά ερωτήματα καθώς και την αναγκαιότητα της μεταπτυχιακής διατριβής.

Έπειτα το κεφάλαιο 2 θα παρουσιάσει τη βιβλιογραφική ανασκόπηση όπου θα εμπεριέχει το υλικό που θα μελετηθεί.

Στο κεφάλαιο 3 θα περιγράφεται η μεθοδολογία που θα ακολουθηθεί κατά την εκπόνηση της μεταπτυχιακής διατριβής.

Ακολούθως στο κεφάλαιο 4 θα παρουσιάζεται η υλοποίηση όπου θα αναλύονται τα στάδια της εγκατάστασης και της λειτουργίας των εργαλείων Machine Learning που θα επιλεχτούν.

Στο κεφάλαιο 5 θα αναλυθούν τα συμπεράσματα έπειτα από την ολοκλήρωση της υλοποίησης και την λειτουργία των εργαλείων Machine Learning.

Ολοκληρώνοντας στο κεφάλαιο 6, ο επίλογος θα περιλαμβάνει σχόλια για την επίτευξη του σκοπού της μεταπτυχιακής διατριβής καθώς και τα μελλοντικά σχέδια.

Κεφάλαιο 2
Βιβλιογραφική Ανασκόπηση

Η ασφάλεια των πληροφοριακών συστημάτων και των δεδομένων ενός οργανισμού εναπόκειται στο πόσο ανθεκτικά και προστατευμένα είναι ώστε να εξασφαλιστεί η εμπιστευτικότητα, η ακεραιότητα και η διαθεσιμότητα (Confidentiality, Integrity and Availability (CIA)) τους. Αυτά αποτελούν τα βασικά χαρακτηριστικά της ασφάλειας πληροφοριακών συστημάτων και αποτελούν το κύριο στόχο των κακόβουλων επιθέσεων [1]. Για να εξασφαλιστεί η ασφάλεια τους επιβάλλεται ανά τακτά χρονικά διαστήματα να πραγματοποιούνται έλεγχοι ώστε να εντοπίζονται και να διορθώνονται τα κενά ασφαλείας και τυχόν λανθασμένες παραμετροποιήσεις. Για το λόγο αυτό οι οργανισμοί προσλαμβάνουν εξειδικευμένο προσωπικό, την Red Team [2], η οποία αποτελείται από άτομα με ηθικές αξίες και έχουν σκοπό να χρησιμοποιήσουν τα εργαλεία και τις τεχνικές που χρησιμοποιούν οι πραγματικοί εισβολείς και να προσομοιάσουν πραγματικές επιθέσεις. Με τις επιθέσεις αυτές εξετάζουν σε βάθος τα πληροφοριακά συστήματα ενός οργανισμού ώστε να εντοπίσουν ευπάθειες που θα τους επιτρέψουν να εισβάλουν στα συστήματα και να προκαλέσουν ζημιά στον οργανισμό. Συνεπώς οι Red Teams χρησιμοποιούν πληθώρα εργαλείων και μεθόδων και πρέπει να εκπαιδεύονται συνεχώς και να ενημερώνονται για τις νέες τεχνολογίες και τα νέα εργαλεία που είναι διαθέσιμα στο κυβερνοχώρο ώστε να μπορούν να τα εφαρμόζουν στις επιθέσεις που πραγματοποιούν προσομοιάζοντας τους εισβολείς.

Το Machine Learning είναι μια νέα τεχνολογία συνεχώς αναπτυσσόμενη με απεριόριστες δυνατότητες. Αποτελεί κομμάτι της τεχνητής νοημοσύνης (Artificial Intelligence (AI)) και βασίζεται στη λογική και τη λειτουργία της ανθρώπινης σκέψης η οποία εκπαιδεύεται από το περιβάλλον, συγκεντρώνει πληροφορίες και με βάση αυτές προσαρμόζονται οι ενέργειες των ανθρώπων. Αντίστοιχα το Machine Learning αποτελείται από αλγόριθμους οι οποίοι συλλέγουν και επεξεργάζονται δεδομένα ώστε να προσαρμόσουν τη λειτουργία τους μαθαίνοντας και βελτιώνουν την απόδοση τους με την πάροδο του χρόνου. Για το λόγο αυτό το Machine Learning έχει γίνει αρκετά διαδεδομένο στο χώρο της κυβερνοασφάλειας και χρησιμοποιείται ευρέως σε διάφορους τομείς τόσο για την προστασία των συστημάτων όσο και για κακόβουλες επιθέσεις όπως για παράδειγμα spamming, phishing attacks, malware attacks, Deep fake attacks, fuzzing κ.α. Υπάρχουν τέσσερις κύριες κατηγορίες στο Machine Learning ανάλογα με την μεθοδολογία τους; το Supervised Machine Learning, το Unsupervised Machine Learning, το Semi-Supervised Machine Learning και το Reinforcement Learning [3].

Συνεπώς οι Red Teams χρειάζονται ένα προστατευμένο περιβάλλον όπως το Cyber range, ώστε να μπορούν να δοκιμάζουν και να εκπαιδεύονται στα καινούργια εργαλεία και τεχνικές. Το Cyber range είναι ένα εικονικό περιβάλλον το οποίο αποτελείται από διάφορα πληροφοριακά συστήματα ώστε να δώσει την ευκαιρία στους επαγγελματίες της κυβερνοασφάλειας όπως τους Red Teams να χρησιμοποιήσουν διάφορα εργαλεία ώστε να προσομοιάσουν σενάρια πραγματικών επιθέσεων. Αυτό τους δίνει τη δυνατότητα τόσο να εκπαιδευτούν στις λειτουργίες και να αξιολογήσουν την απόδοση των εργαλείων όσο και για να βελτιώσουν τις μεθόδους επίθεσης που μπορούν να πραγματοποιήσουν στο πραγματικό περιβάλλον όταν τους ζητηθεί από κάποιο οργανισμό [4].

2.1 Red Team

Οι Red Teams αποτελούνται από άτομα με εξιδεικευμένες γνώσεις που έχουν σκοπό να εντοπίσουν κάποιο τρόπο ώστε να εισβάλουν στο πληροφοριακό σύστημα ενός οργανισμού προσομοιάζοντας πραγματικές επιθέσεις. Οι Red Teams κατέχουν εξειδικευμένες γνώσεις και δεξιότητες σε όλο το φάσμα των πληροφοριακών συστημάτων όπως λειτουργικά συστήματα, δίκτυα, εφαρμογές, βάσεις δεδομένων, Firewalls, κ.α. καθώς και στα υπάρχοντα εργαλεία που χρησιμοποιούνται από τους εισβολείς. Η διαφορά των Red Team από τους κακόβουλους εισβολείς είναι ότι ενεργούν ηθικά και κατόπιν οδηγιών του ίδιου του οργανισμού, για αυτό και ονομάζονται

ηθικοί εισβολείς (Ethical Hackers) ή White Hat Hackers. Απώτερος τους σκοπός δεν είναι να προκαλέσουν ζημιά στον οργανισμό αλλά να εντοπίσουν τις ευπάθειες, τα κενά ή και τις λανθασμένες παραμετροποιήσεις που υπάρχουν στο πληροφοριακό σύστημα, και να τις αναφέρουν στο τμήμα ασφάλειας του οργανισμού ώστε να προβούν στις διορθωτικές ενέργειες που απαιτούνται και να προστατέψουν τα αγαθά του οργανισμού από κυβερνοεπιθέσεις.

2.1.1 Μεθοδολογία των Red Teams

Η μεθοδολογία που ακολουθούν οι ομάδες Red Team βασίζεται στα πρότυπα του Penetration Testing Execution Standards (PTES), αλλά επεκτείνεται και πέραν από αυτό αφού έχουν ως στόχο όχι μόνο να εντοπίσουν τις ευπάθειες ενός οργανισμού αλλά και να τις αξιοποιήσουν για να πραγματοποιήσουν τις επιθέσεις τους. Συνεπώς συνδυάζουν και χρησιμοποιούν διάφορες τεχνικές και εργαλεία για να πετύχουν το σκοπό τους. Το Penetration Testing αποτελεί αναπόσπαστο κομμάτι της μεθοδολογίας των Red Team καθώς μέσω της μεθόδου αυτής εντοπίζουν τις ευπάθειες ενός οργανισμού. Η μεθοδολογία που χρησιμοποιούν οι Red Teams αποτελείται από επτά στάδια; Την Αναγνώριση του στόχου (Reconnaissance), την Εισχώρηση (Compromise), τη Διατήρηση της πρόσβασης (Persistence), τον Απομακρυσμένο έλεγχο (Command and Control), την Αναβάθμιση των προνομίων (Privilege Escalation), την Περιστροφή (Pivoting), την Αναφορά και τον Καθαρισμό (Reporting and Clean up) [5].

Στο πρώτο στάδιο, Reconnaissance, συλλέγονται όσες περισσότερες πληροφορίες είναι δυνατόν για το πληροφοριακό σύστημα ή το στόχο που θα πραγματοποιηθεί η επίθεση. Η συλλογή πληροφοριών χωρίζεται σε δυο κατηγορίες; Στην παθητική και την ενεργητική συλλογή πληροφοριών. Στην παθητική συλλογή πληροφοριών δεν γίνεται αλληλεπίδραση με το πληροφοριακό σύστημα ή το στόχο. Κατά τη διαδικασία της συλλογής πληροφοριών χρησιμοποιούνται εργαλεία που είναι ευρέως διαδεδομένα και ελεύθερα προς χρήση από τον οποιοδήποτε στο διαδίκτυο όπως για παράδειγμα το Facebook, το Google, το LinkedIn, η ιστοσελίδα ενός οργανισμού κ.α. Αντίθετα στην ενεργητική συλλογή πληροφοριών πραγματοποιείται αλληλεπίδραση με το στόχο μέσω διάφορων εργαλείων όπως το Nmap, Metasploit, Maltego κ.α. Έχει σκοπό την αναγνώριση των συστημάτων που υπάρχουν στον οργανισμό όπως για παράδειγμα εκδόσεις συστημάτων Windows και Linux, κατά πόσον υπάρχει εγκατεστημένο Firewall στο πληροφοριακό σύστημα, διευθύνσεις IP κ.α. Η διαδικασία αυτή αποσκοπεί στο να γίνει μια αρχική χαρτογράφηση του πληροφοριακού συστήματος και να

ανιχνευτούν ευπάθειες οι οποίες είναι δυνατόν να αξιοποιηθούν κατά την επίθεση των εισβολέων ώστε να εισχωρήσουν στο πληροφοριακό σύστημα.

Οι Red Teams δεν εστιάζονται μόνο στα φυσικά και τα εικονικά στοιχεία ενός οργανισμού αλλά και στο ανθρώπινο δυναμικό του οργανισμού με την τεχνική της κοινωνικής μηχανικής (Social Engineering) [6]. Η τεχνική του Social Engineering αποτελεί πολύτιμο εργαλείο καθώς ασχολείται με το χειρισμό της ανθρώπινης αλληλεπίδρασης για να εκμαιεύσει ευαίσθητες πληροφορίες όπως για παράδειγμα τους κωδικούς πρόσβασης του χρήστη. Επίσης χρησιμοποιείται για να εκμεταλλευτεί την άγνοια των ανθρώπων ενός οργανισμού και να αποκτήσει πρόσβαση στο πληροφοριακό σύστημα. Αυτό μπορεί να επιτευχθεί για παράδειγμα μέσω κακόβουλων ηλεκτρονικών μηνυμάτων (phishing emails) όπου οι ανυποψίαστοι χρήστες θα παραπεμφθούν σε κακόβουλες ιστοσελίδες που προσομοιάζουν τις πραγματικές, και θα αποκαλύψουν εν άγνοια τους προσωπικά τους στοιχεία όπως κωδικούς πρόσβασης και αριθμούς πιστωτικών καρτών. Επίσης μέσω των κακόβουλων ηλεκτρονικών μηνυμάτων οι ανυποψίαστοι χρήστες πιθανόν να εγκαταστήσουν κακόβουλα λογισμικά στα συστήματα ενός οργανισμού δίνοντας πρόσβαση στους εισβολείς [7]. Στο άρθρο [8] οι ερευνητές αναλύουν την ανθρώπινη συμπεριφορά και τα ευάλωτα στοιχεία της όπως ο φόβος, η ανθρωπιά, η επιθυμία να αισθάνονται χρήσιμοι, η περιέργεια, ο ενθουσιασμός, κ.α. Τα στοιχεία αυτά μπορούν να τα εκμεταλλευτούν κακόβουλα οι κυβερνοεγκληματίες και χρησιμοποιώντας τις τεχνικές του social engineering να επιτύχουν την επίθεση τους στα πληροφοριακά συστήματα ενός οργανισμού. Επιπλέον οι ερευνητές στο άρθρο [9] απέδειξαν ότι οι άνθρωποι μπορούν να εμπιστευτούν και να αποκαλύψουν προσωπικές πληροφορίες ακόμα και σε ένα ρομπότ επιβεβαιώνοντας ότι και τα ρομπότ αν χρησιμοποιηθούν κακόβουλα μπορούν να μετατραπούν σε ένα ισχυρά εργαλεία για τις τεχνικές του social engineering.

Στο δεύτερο στάδιο, compromise, πραγματοποιείται ανάλυση των πληροφοριών που συλλέχτηκα στο πρώτο στάδιο της μεθοδολογίας. Στόχος του σταδίου αυτού είναι να εντοπιστούν οι ευπάθειες του πληροφοριακού συστήματος που θα επιτρέψουν στους εισβολείς να εισχωρήσουν σε κάποιο από τα συστήματα ενός οργανισμού. Στο στάδιο αυτό μπορεί να συνδυαστεί μια επίθεση phishing κατά την οποία εν αγνοία του ο χρήστης θα επιτρέψει την εκτέλεση και την εγκατάσταση κακόβουλου λογισμικού στο σύστημα του και θα επιτρέψει την πρόσβαση στον εισβολέα.

Στο τρίτο στάδιο, persistence, η ομάδα των Red Team θα επιδιώξει να διατηρήσει την πρόσβαση και την επικοινωνία που απέκτησε στο σύστημα του οργανισμού. Αυτό γίνεται με την εγκατάσταση κάποιου εργαλείου Command and Control έτσι ώστε να μην χρειαστεί σε μελλοντικό στάδιο να επαναλάβει την διαδικασία εισχώρησης στο πληροφοριακό σύστημα.

Ακολούθως στο στάδιο privilege escalation, η ομάδα των Red Team θα επιχειρήσει να αναβαθμίσει την πρόσβαση που απέκτησε σε χρήστη με πλήρης δικαιώματα διατήρησης για παράδειγμα Administrator σε περιβάλλον Windows ή root σε περιβάλλον Linux.

Έπειτα στο στάδιο pivoting, θα επιδιώξει να εισβάλει σε άλλες μηχανές του πληροφοριακού συστήματος μέσω του συστήματος που έχει ήδη αποκτήσει πρόσβαση.

Στη συνέχεια θα διαγράψει τις καταγραφές των κινήσεων που έγιναν στα διάφορα αρχεία ιχνηλάτησης (log files) των συστημάτων ώστε να μην γίνει αντιληπτή η παρουσία των ατόμων Red Team από την ομάδα ασφαλείας του οργανισμού.

Τέλος η ομάδα Red Team θα συντάξει και θα αναφέρει τα αποτελέσματα του ελέγχου που πραγματοποιήθηκε. Η αναφορά αυτή περιλαμβάνει τις ευπάθειες που εντοπίστηκαν και χρησιμοποιήθηκαν για να επιτευχθεί η διείσδυση στο πληροφοριακό σύστημα, τα συστήματα που είναι ευάλωτα σε επιθέσεις καθώς και τη ζημιά που θα μπορούσε να προκληθεί στα αγαθά και τα συστήματα του οργανισμού από μια επιτυχή κακόβουλη επίθεση.

2.2 Penetration Testing

Το Penetration Testing είναι μια από τις τακτικές που χρησιμοποιούν οι Red Teams ώστε να εντοπίσουν τις ευπάθειες των πληροφοριακών συστημάτων οι οποίες θα μπορούσαν να θέσουν σε κίνδυνο τα αγαθά ενός οργανισμού [6]. Εστιάζεται στα φυσικά και τα εικονικά αγαθά του οργανισμού. Τα φυσικά αγαθά αποτελούνται από τις συσκευές του πληροφοριακού συστήματος όπως τους servers, routers, switches, κάμερες ασφαλείας κ.α. Τα εικονικά αγαθά αποτελούνται από τα λογισμικά και τις εφαρμογές του πληροφοριακού συστήματος όπως τα λειτουργικά συστήματα, οι εφαρμογές, οι Firewalls, οι βάσεις δεδομένων κ.α.

Επιπλέον υπάρχουν τρεις δημοφιλής στρατηγικές για τη διεξαγωγή του Penetration Testing. Αρχικά η στρατηγική του Black Box κατά την οποία τα άτομα που θα διεξάγουν τον έλεγχο, όπως παρόμοια με τους κυβερνοεγκληματίες, δεν έχουν καμία γνώση της αρχιτεκτονικής του πληροφοριακού συστήματος [6]. Αντίθετα στη στρατηγική του White Box υπάρχει πλήρη επίγνωση για το πληροφοριακό σύστημα που θα εξεταστεί. Στην στρατηγική αυτή συνήθως συνεργάζονται οι αναλυτές με τους προγραμματιστές του οργανισμού για να αξιολογηθεί μια ένα λογισμικό [6]. Επιπλέον υπάρχει και η στρατηγική του Gray Box κατά την οποία υπάρχει μερική γνώση για την αρχιτεκτονική του στόχου.

Πέραν από τις στρατηγικές που ακολουθούνται κατά την εκτέλεση του Penetration Testing, ο έλεγχος μπορεί να εστιαστεί είτε εξωτερικά είτε εσωτερικά του οργανισμού. Κατά τον εξωτερικό έλεγχο εξετάζονται τα στοιχεία που μπορούν να εντοπιστούν από εξωτερικούς παράγοντες όπως για παράδειγμα το διαδίκτυο και τις ευπάθειες που μπορούν να εντοπιστούν από άτομα εκτός του οργανισμού προσμοιάζοντας επίθεση από το διαδίκτυο. Στον εσωτερικό έλεγχο εξετάζονται τα στοιχεία και οι ευπάθειες στο εσωτερικό δίκτυο του πληροφοριακού συστήματος προσμοιάζοντας επίθεση που θα ήταν πιθανόν να πραγματοποιηθεί από εσωτερικούς χρήστες, και πιθανόν δυσαρεστημένους εργαζομένους [10].

2.2.1 Μεθοδολογία του Penetration testing

Ο έλεγχος Penetration Testing πραγματοποιείται σύμφωνα με προκαθορισμένα πρότυπα όπως για παράδειγμα το Open Web Application Security Project (OWASP), το Open Source Security Testing Methodology Manual (OSSTMM), το Information System Security Assessment Framework (ISSAF) κ.α. [5]. Η πιο διαδεδομένη μεθοδολογία που ακολουθείται κατά την εκτέλεση του Penetration Testing είναι το Penetration Testing Execution Standards (PTES). Η μεθοδολογία PTES αποτελείται από επτά στάδια; Την αλληλεπίδραση πριν την εκμετάλλευση (Pre-engagement Interaction), τη συλλογή πληροφοριών (Intelligence Gathering), τη μοντελοποίηση απειλών (Treat Modeling), την Ανάλυση Ευπαθειών (Vulnerability Analysis), την εκμετάλλευση (Exploitation), την μετά-εκμετάλλευση (Post-exploitation), και την αναφορά (Reporting) [5].

Στο πρώτο στάδιο, της αλληλεπίδρασης πριν την εκμετάλλευση, καθορίζεται ο σκοπός του ελέγχου που θα πραγματοποιηθεί. Στο στάδιο αυτό ανάλογα με τον τύπο του ελέγχου ενημερώνονται τα άτομα που θα πραγματοποιήσουν τον έλεγχο, επιλέγονται τα συστήματα που

θα εκλεχτούν, καθορίζονται οι ημερομηνίες διεξαγωγής του ελέγχου, καθορίζονται οι νομικές διαδικασίες κ.α.

Ακολούθως, στο επόμενο στάδιο συλλογής πληροφοριών, τα άτομα που θα πραγματοποιήσουν τον έλεγχο συγκεντρώνουν όσες περισσότερες πληροφορίες είναι δυνατόν για τα συστήματα του οργανισμού που πρόκειται να ελεγχτούν. Το στάδιο αυτό είναι το ίδιο με το προαναφερθέν στάδιο συλλογής πληροφοριών στην μεθοδολογία των Red Team.

Αφού συλλεχτούν οι πληροφορίες για το πληροφοριακό σύστημα και τον οργανισμό, πραγματοποιείται η μοντελοποίηση των απειλών. Στο στάδιο αυτό αναγνωρίζονται και καταγράφονται οι απειλές και ο βαθμός επικινδυνότητας τους είτε πρόκειται για συστήματα είτε για εφαρμογές.

Ακολούθως πραγματοποιείται η ανάλυση των ευπαθειών κατά την οποία εντοπίζονται οι ευπάθειες, οι λανθασμένες παραμετροποιήσεις, τα κενά και οι παραλήψεις που υπάρχουν στο πληροφοριακό σύστημα τις οποίες μπορούν να εκμεταλλευτούν οι κακόβουλοι εισβολείς για να εισχωρήσουν στο πληροφοριακό σύστημα του οργανισμού.

Στη συνέχεια στο στάδιο της εκμετάλλευσης γίνεται χρήση των ευπαθειών που εντοπίστηκαν στο προηγούμενο στάδιο. Ακολούθως στο στάδιο της μετά-εκμετάλλευσης αξιολογείται ο βαθμός κρισιμότητας και επικινδυνότητας της ευπάθειας είτε επιτεύχθηκε η χρήση του είτε όχι.

Αφού ολοκληρωθεί η διαδικασία για όλες τις ευπάθειες που εντοπίστηκαν τότε θα συνταχθεί μια αναφορά και θα παραδοθεί στο τμήμα ασφαλείας του οργανισμού. Η αναφορά αυτή θα περιλαμβάνει τις ευπάθειες που εντοπίστηκαν και την επικινδυνότητας τους, τα βήματα που πραγματοποιήθηκαν κατά τον έλεγχο των συστημάτων. Επίσης θα περιλαμβάνει εισηγήσεις προς την ομάδα ασφαλείας του οργανισμού για διορθωτικές ενέργειες που θα πρέπει να προβούν ώστε να αποφευχθούν πιθανές επιθέσεις λόγω των ευπαθειών που εντοπίστηκαν.

2.3 Red Team VS Penetration testing

Οι Red Teams και το Penetration Testing συχνά εκλαμβάνονται ως συνώνυμες έννοιες παρόλο που υπάρχουν κάποιες διαφορές μεταξύ τους.

Αρχικά το Penetration Testing εστιάζεται στον εντοπισμό των τρωτών σημείων στα πληροφοριακά συστήματα του οργανισμού και αφού τα εντοπίσει ενημερώνει το τμήμα ασφαλείας του οργανισμού ώστε να τα διορθώσει. Αντίθετα οι Red Teams όχι μόνο θα εντοπίσουν τα τρωτά σημεία αλλά θα επιδιώξουν να τα χρησιμοποιήσουν ώστε να προσομοιάσουν τις ενέργειες των εισβολέων και να εισχωρήσουν στο πληροφοριακό σύστημα. Συνεπώς ο σκοπός του Penetration Testing είναι απλά ο εντοπισμός όσων περισσοτέρων ευπαθειών είναι δυνατόν τη δεδομένη στιγμή και η αναφορά τους, ενώ ο σκοπός των Red Team είναι η διεξαγωγή μιας έρευνας σε βάθος, ο εντοπισμός και η εκμετάλλευση έστω και μιας ευπάθειας ώστε να εισχωρήσουν στα πληροφοριακά συστήματα και να ερευνήσουν πόση ζημιά είναι δυνατόν να προκαλέσουν όπως θα έκαναν και οι πραγματικοί εισβολείς.

Το Penetration Testing χρησιμοποιεί καθορισμένη μεθοδολογία όπως για παράδειγμα το PTES. Οι Red Teams χρησιμοποιούν τη μεθοδολογία του PTES ως βάση αλλά ενεργούν και πέραν από αυτή, συνδυάζοντας διάφορες τεχνικές και εργαλεία ώστε να πετύχουν το σκοπό τους.

Το Penetration Testing ασχολείται με τα φυσικά και τα εικονικά στοιχεία (virtual assets) του οργανισμού ενώ οι Red Teams ασχολούνται και με το ανθρώπινο δυναμικό του οργανισμού ώστε να εκμαιεύσουν περισσότερες πληροφορίες για τον οργανισμό και τα συστήματα του [6] με τεχνικές social engineering.

Η χρονική διάρκεια της κάθε αξιολόγησης είναι επίσης μια σημαντική διαφορά των δυο. Το Penetration Testing συνήθως διαρκεί μια ως δυο εβδομάδες σε αντίθεση με την αξιολόγηση της Red Team η οποία διαρκεί περισσότερο όπως για παράδειγμα 3-4 εβδομάδες ή και μήνες.

Κατά τη διάρκεια της διεξαγωγής του Penetration testing είναι ενημερωμένη η ομάδα ασφαλείας του οργανισμού σε αντίθεση με την αξιολόγηση της Red Team στην οποία είναι ενημερωμένος μόνο ο υπεύθυνος της ομάδας ασφαλείας ή/και τα διευθυντικά στελέχη του οργανισμού.

2.4 Machine Learning

Το Machine Learning αποτελεί ένα κλάδο του Artificial Intelligence το οποίο προσομοιάζει τη λειτουργία της ανθρώπινης σκέψης η οποία μαθαίνει από το περιβάλλον ώστε να προσαρμόσει τις μελλοντικές ενέργειες του ανθρώπου. Κατ' επέκταση το Machine Learning βασίζεται σε αλγόριθμους έτσι ώστε να συλλέγει και να επεξεργάζεται δεδομένα ώστε το σύστημα να εκπαιδεύεται και να βελτιώνει την απόδοση του με την πάροδο του χρόνου. Η τεχνολογία αυτή είναι ιδιαίτερα βοηθητική στη σύγχρονη εποχή όπου υπάρχει μεγάλος όγκος δεδομένων και υπολογιστικής ισχύος. Στη σύγχρονη εποχή χρησιμοποιείται ευρέως η τεχνολογία του Artificial Intelligence και του Machine Learning σε διάφορους τομείς ώστε να βοηθήσει και να βελτιώσει τη ζωή των ανθρώπων. Κάποια παραδείγματα είναι τα έξυπνα αυτοκίνητα όπου έχουν σκοπό να βοηθήσουν τους ανθρώπους στην οδήγηση και να μειώσουν τα δυστυχήματα, τα μέσα κοινωνικής δικτύωσης, όπως το Facebook, όπου φιλτράρουν και προτείνουν στους χρήστες παρόμοια θέματα που έχουν δείξει ενδιαφέρον στον παρελθόν. Ένα ακόμα παράδειγμα είναι η χρήση του Machine Learning σε διαδικτυακές πλατφόρμες αγοράς προϊόντων όπως για παράδειγμα το Amazon, ώστε να συστήσουν προϊόντα που πιθανόν να ενδιαφέρουν τους χρήστες ανάλογα με τις προηγούμενες αγορές τους.

Το Machine Learning χρησιμοποιείται επίσης και στο τομέα της κυβερνοασφάλειας για την προστασία των πληροφοριακών συστημάτων από κυβερνοεπιθέσεις όπως για παράδειγμα στα anti-virus, τα συστήματα ανίχνευσης και πρόληψης εισβολέων (Intrusion Detection and Prevention IDPS), τα Firewalls, τα συστήματα πληροφοριών ασφάλειας και διαχείριση συμβάντων (Security Information Event management SIEM) κ.α. [11].

Αναπόφευκτα και οι κυβερνοεγκληματίες τείνουν προς τη τεχνολογία του Machine Learning εφευρίσκοντας καινούργιους και πιο εξελιγμένους τρόπους και εργαλεία επίθεσης. Με αυτό το τρόπο επιδιώκουν είτε να εντοπίσουν ευπάθειες των συστημάτων που έχουν ξεφύγει από τους αναλυτές ασφαλείας, είτε να παραπλανήσουν τα σύγχρονα προστατευτικά εργαλεία που

βασίζονται στο Machine Learning και να εισχωρήσουν στα πληροφοριακά συστήματα των χρηστών και του οργανισμού. Συνεπώς αναπτύσσονται συνεχώς καινούργιες επιθέσεις βασισμένες στο Machine Learning όπως για παράδειγμα το spamming, οι επιθέσεις phishing, οι επιθέσεις malware, οι επιθέσεις deep fake, το fuzzing, επιθέσεις κωδικών ασφαλείας, επιθέσεις captcha κ.α. Αναπόφευκτα το Machine Learning βοηθά στην αντιμετώπιση των επιθέσεων αυτών αφού εκπαιδεύεται από προηγούμενες εμπειρίες επιθέσεων και μπορεί να ανταποκριθεί στις μελλοντικές καινούργιες επιθέσεις [3].

Επιπλέον οι ερευνητές έχουν στραφεί στην έρευνα πιθανών λύσεων έξυπνων αυτοματισμών με βάση το Machine Learning όπου θα μπορούν να ενσωματωθούν και στο τομέα του Penetration Testing. Αυτό θα μπορεί να βοηθήσει τους αναλυτές στα διάφορα στάδια του ελέγχου όπως την συλλογή πληροφοριών (Information Gathering), την Ανάλυση Ευπαθειών (Vulnerability Analysis), και την εκμετάλλευση (Exploitation). Επιπλέον θα έχει ως αποτέλεσμα την αποφόρτιση των αναλυτών από επαναλαμβανόμενες χρονοβόρες διαδικασίες, κυρίως σε μεγάλα δίκτυα, έτσι ώστε να μπορούν να επικεντρωθούν σε πιο απαιτητικά σημεία του ελέγχου [11]. Επίσης είναι ιδιαίτερα σημαντική η ενσωμάτωση της τεχνολογίας του Machine Learning στη διαδικασία του Penetration Testing και των ομάδων Red Team όπου μπορεί να βοηθήσει στην αποφυγή ανθρώπινων λαθών που οφείλονται στην κούραση, την υπερφόρτωση, το στρες και τις παραλήψεις των αναλυτών. Επιπλέον είναι εξίσου σημαντικό στο τομέα του επιθετικού ελέγχου που διεξάγεται από τους αναλυτές των Red Team ώστε να μπορεί να αξιολογηθεί το πληροφοριακό σύστημα του οργανισμού κατά πόσο είναι ανθεκτικό σε καινούργιες τεχνολογικά επιθέσεις. Συνεπώς πρέπει να αναπτύσσονται εργαλεία όπου θα αξιοποιούν τις δυνατότητες του Machine Learning και να εκπαιδεύονται τα άτομα των ομάδων Red Team στις νέες τάσεις και δυνατότητες της τεχνολογίας και των σύγχρονων επιθέσεων ώστε να μπορούν να προσομοιάζουν τις επιθέσεις της σύγχρονης εποχής.

Για να επιτευχθεί η αξιοποίηση των δυνατοτήτων της τεχνολογίας του Machine Learning είναι σημαντικό να ακολουθηθεί η κατάλληλη μεθοδολογία ώστε να επιφέρει το επιθυμητό αποτέλεσμα.

2.5 Κατηγορίες του Machine Learning

Ανάλογα με τη μεθοδολογία που ακολουθείται και τη χρήση του συστήματος το Machine Learning χωρίζεται σε τέσσερις κατηγορίες; η Επιβλεπόμενη Μηχανική Μάθησης (Supervised Machine Learning), η Μη Επιβλεπόμενη Μηχανική Μάθησης (Unsupervised Machine Learning), η Ημι-επιβλεπόμενη Μηχανική Μάθησης (Semi-Supervised Machine Learning) και η Ενίσχυση Μάθησης (Reinforcement Learning) [3]. Οι τρεις πρώτες κατηγορίες Machine Learning χρησιμοποιούνται στο τομέα των αμυντικών συστημάτων ασφαλείας ενώ αντίθετα το Reinforcement Learning χρησιμοποιείται στο τομέα των επιθετικών συστημάτων ασφαλείας.

2.5.1 Επιβλεπόμενη Μηχανική Μάθησης (Supervised Machine Learning)

Το Supervised Machine Learning είναι μια κατηγορία του Machine Learning η οποία εκπαιδεύεται με βάση κάποια παραδείγματα τα οποία αποτελούν το σύνολο δεδομένων εκπαίδευσης (training dataset). Το σύνολο δεδομένων εκπαίδευσης περιλαμβάνει δεδομένα εισόδου με ετικέτα (ή ένδειξη) και σωστά αποτελέσματα εξόδου. Με βάση την εκπαίδευση του ο αλγόριθμος του Supervised Machine Learning έχει ως στόχο, να προσδιορίσει το σωστό αποτέλεσμα εξόδου σε καινούργια δεδομένα εισόδου, ελαχιστοποιώντας το ποσοστό σφάλματος των αποτελεσμάτων του με την πάροδο του χρόνου. Σύμφωνα με τους συγγράφεις του άρθρου [12] το Supervised Machine Learning χωρίζεται σε δυο κατηγορίες ανάλογα με τα προβλήματα που καλείται να επιλύσει; την ταξινόμηση (Classification) και την οπισθοδρόμηση (Regression).

Στην ταξινόμηση ο αλγόριθμος με βάση την εμπειρία του από το σύνολο δεδομένων εκπαίδευσης προσπαθεί να συμπεράνει κατά πόσο τα δεδομένα εισόδου πληρούν κάποια κριτήρια έτσι ώστε να χωρίσει τα δεδομένα εξόδου σε δυο κατηγορίες. Για παράδειγμα διαχωρίζει την ανεπιθύμητη αλληλογραφία (spam email) από την επιθυμητή και καταχωρεί τα ηλεκτρονικά μηνύματα στους ανάλογους φακέλους. Εναπόκειται στο χρήστη να επιλέξει κατά πόσο ο διαχωρισμός που έγινε είναι σωστός ή όχι. Στην περίπτωση που λανθασμένα έχει τοποθετηθεί επιθυμητή αλληλογραφία στο φάκελο των ανεπιθύμητων ο χρήστης μπορεί να καθορίσει την αλλαγή που επιθυμεί. Συνεπώς με το τρόπο αυτό ο αλγόριθμος εκπαιδεύεται και σε μελλοντική παρόμοια αλληλογραφία δεν θα επαναλάβει το ίδιο σφάλμα. Οι πιο διαδεδομένοι αλγόριθμοι της κατηγορίας

αυτής του Supervised Machine Learning είναι το Naive Bayer, το Decision Tree και το Support Vector Machine (SVM) [3].

Οι αλγόριθμοι οπισθοδρόμησης χρησιμοποιούνται για να κάνουν προβλέψεις μέσω της σύνδεσης μεταξύ εξαρτημένων και ανεξάρτητων μεταβλητών. Κάποια παραδείγματα της χρήσης του αλγορίθμου αυτού είναι η πρόγνωση των καιρικών συνθηκών, η πρόβλεψη της κίνησης των μετοχών, η πρόβλεψη της αγοράς προϊόντων των καταναλωτών ώστε να μπορούν τα διαδικτυακά καταστήματα να διαφημίζουν και να προτείνουν προϊόντα στους καταναλωτές ανάλογα με τις προτιμήσεις τους και το ιστορικό τους, πρόβλεψη ύπαρξης κακόβουλου λογισμικού (malware) στο πληροφοριακό σύστημα κ.α. [12]. Είναι ιδιαίτερα σημαντικό για την ασφάλεια των πληροφοριακών συστημάτων οι προβλέψεις κακόβουλων λογισμικών να γίνονται με τη μεγαλύτερη ακρίβεια ώστε να μπορούν να προστατευτούν τα δεδομένα και πληροφοριακά συστήματα του οργανισμού. Οι ερευνητές του άρθρου [13] αναλύοντας διάφορους αλγόριθμους του Supervised Machine Learning έχουν καταδείξει ότι μπορεί να εντοπιστεί το κακόβουλο λογισμικό με ακρίβεια 99.1%. Οι πιο γνωστοί αλγόριθμοι της κατηγορίας αυτής του Supervised Machine Learning [3] είναι το Linear Regression, το Logistic Regression, το Polynomial Regression και το Support Vector Regression (SVR).

2.5.2 Μη-Επιβλεπόμενη Μηχανική Μάθησης (Unsupervised Machine Learning)

Το Unsupervised Machine Learning επίσης εκπαιδεύεται με βάση το σύνολο των δεδομένων εκπαίδευσης που θα του δοθεί. Αντίθετα όμως με το Supervised Machine Learning το σύνολο δεδομένων εκπαίδευσης περιλαμβάνει δεδομένα χωρίς ετικέτα. Σκοπός του αλγόριθμου είναι να ανακαλύψει μοτίβα με βάση τα δεδομένα εκπαίδευσης με λίγη ή και καθόλου ανθρώπινη βοήθεια, τα οποία θα το βοηθήσουν να εξάγει τα επιθυμητά σωστά αποτελέσματα εξόδου. Κάποια παραδείγματα χρήσης των αλγορίθμων της κατηγορίας αυτής είναι ο εντοπισμός ανωμαλιών στα δεδομένα και οι προτιμήσεις προϊόντων των καταναλωτών. Χωρίζεται σε δυο κατηγορίες [12] ανάλογα με τη μεθοδολογία που ακολουθείτε στην επίλυση των προβλημάτων; την ομαδοποίηση (Clustering) και τους κανόνες συσχέτισης (Association rules).

Στην ομαδοποίηση το μοτίβο που ακολουθείται είναι να ομαδοποιηθούν τα δεδομένα εισόδου βάση των χαρακτηριστικών τους για παράδειγμα το μέγεθος τους, το σχήμα τους, η τιμή τους κ.α. Οι αλγόριθμοι K-mean, Hierarchical Clustering και K-NN (K-nearest neighbors) είναι οι πιο

διαδεδομένοι αλγόριθμοι της κατηγορίας αυτής. Για παράδειγμα ο αλγόριθμος K-mean χρησιμοποιείται από τα εργαλεία πρόληψης κυβερνοεπιθεσέων όπως την ανίχνευση του κακόβουλου λογισμικού malware όταν πλημυρίζει το δίκτυο με πακέτα ώστε να προκαλέσει συμφόρηση [12], όπου τα πακέτα αυτά συνήθως έχουν κάποιο μοτίβο.

Στη κατηγορία κανόνες συσχέτισης ο αλγόριθμος έχει στόχο να κατανοήσει κάποιους κανόνες που συσχετίζουν τις διάφορες ομάδες δεδομένων. Ένα παράδειγμα του αλγόριθμου αυτού είναι οι προτιμήσεις προϊόντων των καταναλωτών. Τα διαδικτυακά καταστήματα χρησιμοποιούν τη μέθοδο αυτή για να κατανοήσουν ποια προϊόντα αγοράστηκαν ταυτόχρονα από τους καταναλωτές έτσι ώστε να είναι σε θέση να προτείνουν προϊόντα που πιθανόν να ενδιαφέρουν τους καταναλωτές που αγόρασαν ένα από αυτά τα προϊόντα [12]. Στη κατηγορία αυτή οι πιο γνωστοί αλγόριθμοι είναι ο Apriori, και ο FP-Growth.

2.5.3 Ημιεπιβλεπόμενη Μηχανική Μάθησης (Semi-Supervised Machine Learning)

Το Semi-Supervised Machine Learning είναι ένας συνδυασμός του Supervised Machine Learning και του Unsupervised Machine Learning. Στο Semi-Supervised Machine Learning εισάγονται δεδομένα με ετικέτες στο σύνολο δεδομένων εκπαίδευσης χωρίς ετικέτες. Με βάση τους ερευνητές [3] [12] αυτό βοηθά το σύστημα να κατανοήσει καλυτέρα τα μοτίβα αφού πλέον έχει δεδομένα με ετικέτες στο εκπαιδευτικό του υλικό. Έτσι επιτυγχάνεται η βελτίωση της ταχύτητας και της ακρίβειας της εκπαίδευσης των συστημάτων.

2.5.4 Ενίσχυση Μάθησης (Reinforcement Learning)

Το Supervised και το Unsupervised Machine Learning όμως δεν μπορούν να εφαρμοστούν σε περιβάλλοντα όπως στη περίπτωση του information gathering και του post-exploitation αφού δεν υπάρχουν εκπαιδευτικά δεδομένα για να δοθούν στο σύστημα. Αντίθετα με τους υπόλοιπους τύπους του Machine Learning, το Reinforcement Learning δεν απαιτεί να του δοθούν εκπαιδευτικά δεδομένα κάτι που το κάνει ιδανικό για τη χρήση του σε άγνωστα και περίπλοκα περιβάλλοντα. Συνεπώς το Reinforcement Learning επιλέχτηκε ως η πιο υποσχόμενη επιλογή μεταξύ των τύπων του Machine Learning ώστε να επιτρέψει την αυτοματοποίηση της διαδικασίας του penetration testing όπου αφενός θα συμπεριφερθεί όπως οι αναλυτές όπου

κερδίζουν εμπειρία και γνώσεις με την πάροδο του χρόνου και αφετέρου θα αποφορτιστούν οι αναλυτές από χρονοβόρες, επαναλαμβανόμενες και κουραστικές διαδικασίες και θα μπορούν να επικεντρωθούν σε πιο σημαντικά στοιχεία της ανάλυσης [11]. Σύμφωνα με τους ερευνητές στο άρθρο [14] το Reinforcement Learning επικεντρώνεται στο να εκπαιδευτεί μέσω της αλληλεπίδρασης του με το περιβάλλον του με απώτερο σκοπό να μεγιστοποιήσει όσο το δυνατό την ανταμοιβή του. Η φιλοσοφία του Reinforcement Learning είναι ο εκπαιδευόμενος (agent) να μαζέψει όσες περισσότερες ανταμοιβές (rewards) μπορεί μέσω των σωστών ενεργειών (actions) που θα πραγματοποιήσει ελαχιστοποιώντας ή αποφεύγοντας τις λανθασμένες ενέργειες του όπου του δίνονται αρνητικές ανταμοιβές. Σημαντικό στοιχείο του Reinforcement Learning είναι ότι δεν του δίνονται κατευθυντήριες γραμμές ως προς το ποιες ενέργειες θα πραγματοποιήσει ώστε να ανταμειφθεί. Αντίθετα καλείται να εξερευνήσει και να δοκιμάσει διάφορες ενέργειες μέχρι να εντοπίσει αυτές που θα του δώσουν τις περισσότερες θετικές ανταμοιβές.

Πέραν από τον agent και το περιβάλλον (environment) που θα αλληλοεπιδράσει, το Reinforcement Learning αποτελείται από ακόμα τρία βασικά στοιχεία [15]; Την πολιτική (policy), την ανταμοιβή και τη συνάρτηση τιμής (value function). Η πολιτική είναι η μέθοδος με την οποία ο agent θα επιλέξει ποια θα είναι η επόμενη ενέργεια που θα πραγματοποιήσει σε κάθε κατάσταση που βρίσκεται. Η ανταμοιβή είναι αυτό που θα καθορίσει κατά ποσό η ενέργεια που πραγματοποίησε ο agent είναι σωστή ή λανθασμένη. Συνεπώς όταν ο agent πραγματοποιήσει μια σωστή ενέργεια στο περιβάλλον τότε θα ανταμειφθεί με θετική ανταμοιβή. Αντίθετα όταν πραγματοποιήσει μια λανθασμένη ενέργεια τότε θα τιμωρηθεί με αρνητική ανταμοιβή. Η συνάρτηση τιμής καθορίζει την μελλοντική ανταμοιβή που θα ανταμειφθεί ο agent από ένα σύνολο ενεργειών. Για παράδειγμα είναι πιθανόν η ανταμοιβή που θα πάρει για την επόμενη ενέργεια του να έχει μικρότερη αξία από κάποια άλλη ενέργεια, όμως οι ενέργειες που ακολουθούν θα του δώσουν περισσότερη αξία ανταμοιβών.

Το Reinforcement Learning χρησιμοποιεί ως επί το πλείστων τη μεθοδολογία Markov Decision Process (MDP) [11] για να καθορίσει τη διαδικασία λήψης αποφάσεων με τον τρόπο αλληλεπίδρασης του agent στο περιβάλλον του αναφορικά με τις καταστάσεις στις οποίες βρίσκεται, στις ενέργειες που θα πραγματοποιήσει και τις ανταμοιβές που θα πάρει. Με βάση τη θεωρία του Markov Property, η οποία ορίζει ότι η παρούσα κατάσταση εξαρτάται μόνο από την προηγούμενη κατάσταση, το Markov Process καθορίζεται ως (S, P) όπου το S είναι η κατάσταση (state) και το P είναι η πιθανότητα μετάβασης σε άλλη κατάσταση (state transition probability). Συνεπώς για να μπορεί να εφαρμοστεί στο Reinforcement Learning, το Markov Process

συνδυάζεται με την ενέργεια και την ανταμοιβή. Συνεπώς το MDP καθορίζεται ως (S, A, P, R, γ) [15] όπου το R είναι η ανταμοιβή (reward) που πάρει ο agent και το A είναι οι ενέργειες (actions) που θα πραγματοποιήσει.

Απώτερος στόχος της χρήσης της μεθοδολογίας του MDP είναι να χρησιμοποιηθεί η πολιτική που θα επιφέρει τη μεγαλύτερη ανταμοιβή στον agent. Συνεπώς χρησιμοποιούνται διάφορες μέθοδοι για τον καθορισμό της πολιτικής αυτής όπως το Value Iteration και το Policy Iteration. Με βάση τους αναλυτές στο άρθρο [14], οι αλγόριθμοι που βασίζονται στη μέθοδο του Value Iteration επικεντρώνονται στο να χρησιμοποιήσουν την εμπειρία τους και να εντοπίσουν την ενέργεια με τη μεγαλύτερη ανταμοιβή όπως για παράδειγμα ο αλγόριθμος Q-Learning. Αντίθετα οι αλγόριθμοι που βασίζονται στη μέθοδο του Policy Iteration επικεντρώνονται στο να χρησιμοποιήσουν την εμπειρία τους και να βελτιώσουν τις πολίτικες τους. Ένα παράδειγμα της μεθόδου Policy-based είναι ο αλγόριθμος State-Action-Reward-State-Action (SARSA) [14]. Υπάρχουν όμως και αλγόριθμοι που χρησιμοποιούν και τις δυο μεθόδους [14] όπως για παράδειγμα ο αλγόριθμος Actor-Critic (AC) ο οποίος συνδυάζει τις δυο μεθόδους για να εξελίξει την εκπαίδευση του. Η συνδυαστική μέθοδος αυτή όμως είναι πιο χρονοβόρα στην εκπαίδευση συγκριτικά με τις άλλες μεθόδους αλλά επιφέρει πιο βάσιμα αποτελέσματα.

2.6 Machine Learning Επιθέσεις

Το Machine Learning χρησιμοποιείτε και από τους κυβερνοεγκληματίες οι οποίοι επινοούν και κατασκευάζουν καινούργιες, πιο εξελιγμένες, και πιο έξυπνες επιθέσεις σε σύγκριση με τις παραδοσιακές μεθόδους επιθέσεων. Είναι αναπόφευκτο να οδηγηθούν σε αυτή τη κατεύθυνση ώστε να μπορούν να ξεγελάσουν τα συστήματα προστασίας που πλέον βασίζονται στο Machine Learning για τον εντοπισμό και την αποτροπή των επιθέσεων. Συνεπώς και οι ομάδες των Red Team πρέπει να εκπαιδεύονται για τις δυνατότητες των επιθέσεων αυτών και να ενημερώνονται για τις νέες τεχνολογίες έτσι ώστε να μπορούν να τις ενσωματώσουν στις προσομοιάσεις επιθέσεων που πραγματοποιούν. Στη συνέχεια της μεταπτυχιακής διατριβής θα αναλυθούν επιθέσεις που χρησιμοποιούν το Machine Learning.

2.6.1 Spamming επιθέσεις

Οι επιθέσεις Spamming είναι η μέθοδος κατά την οποία στέλνονται μαζικά ηλεκτρονικά μηνύματα σε χιλιάδες άγνωστους χρήστες. Έχουν σκοπό είτε να διαφημίσουν προϊόντα, είτε να ξεγελάσουν τους χρήστες ώστε να εγκαταστήσουν κακόβουλο λογισμικό στο πληροφοριακό τους σύστημα, είτε για να εξαπατήσουν τους χρήστες παραπέμποντας τους σε κακόβουλες ιστοσελίδες όπου θα τους ζητηθεί η εισαγωγή προσωπικών τους στοιχείων όπως για παράδειγμα κωδικούς πρόσβασης, στοιχεία τραπεζικών λογαριασμών κ.α. Για να προστατευτούν οι χρήστες από τις επιθέσεις spamming εγκαθίστανται στους εξυπηρετητές ηλεκτρονικών ταχυδρομείων λογισμικά προστασίας όπου με τη χρήση του Machine Learning διαχωρίζουν την ηλεκτρονική αλληλογραφία των χρηστών σε spam (junk email) και σε επιθυμητή αλληλογραφία. Αντίστοιχα οι κυβερνοεγκληματίες μπορούν να χρησιμοποιήσουν το Machine Learning, σύμφωνα με τους αναλυτές του άρθρου [3], έτσι ώστε στέλνοντας αρκετά συχνά υλικό ηλεκτρονικών μηνυμάτων να μπορούν να ανασυνθέσουν το μοντέλο του Machine Learning λογισμικού που έχουν τα συστήματα προστασίας και πλέον να ρυθμίσουν την επίθεση τους παρακάμπτοντας τα μοντέλα των συστημάτων.

2.6.2 Phishing επιθέσεις

Οι επιθέσεις phishing είναι ηλεκτρονικά μηνύματα που στέλνονται από κυβερνοεκληματίες και έχουν σκοπό να εξαπατήσουν τους ανθρώπους ώστε να εισάγουν προσωπικά τους στοιχεία όπως για παράδειγμα αριθμούς πιστωτικών καρτών, κωδικούς πρόσβασης κ.α. αφού μιμούνται νόμιμες πήγες. Συνεπώς όσο πιο αληθοφανής είναι το ηλεκτρονικό μήνυμα τόσο περισσότερες πιθανότητες υπάρχουν ώστε να ξεγελαστεί ο χρήστης και να πιστέψει ότι πρόκειται για νόμιμη διαδικασία και κατ' επέκταση να παραχωρήσει τις προσωπικές του πληροφορίες. Το Machine Learning χρησιμοποιείται από τους κυβερνοεγκληματίες ώστε να βελτιώσουν το περιεχόμενο των ηλεκτρονικών μηνυμάτων και να το κάνουν πιο αληθοφανές. Για παράδειγμα προσθέτοντας ρεαλιστικές εικόνες, φωτογραφικό υλικό, λογότυπα, προφίλ από κοινωνικά δίκτυα, διορθώνοντας συντακτικά και γραμματικά λάθη που πιθανόν να κάνουν τους ανθρώπους να υποψιαστούν ότι πρόκειται για απατή [12].

2.6.3 DeepFakes επιθέσεις

Η επίθεση DeepFake είναι η μέθοδος κατά την οποία δημιουργούνται ψεύτικα βίντεο και φωτογραφίες ατόμων αλλάζοντας τα πρόσωπα τους με άλλα πρόσωπα. Η τεχνική αυτή όπως περιγράφεται από τους αναλυτές στο άρθρο [16] χρησιμοποιεί τη μέθοδο του Artificial Intelligence Deep Learning και οπτικοακουστικό υλικό, και επιτυγχάνει την ανταλλαγή των προσώπων των ατόμων έτσι ώστε να παρουσιάζεται το πρόσωπο και οι εκφράσεις του ατόμου λέγοντας και κάνοντας κάτι που ουσιαστικά δεν είναι πραγματικό με σκοπό να εξαπατηθεί ο αποδέχτης του οπτικοακουστικού υλικού. Για παράδειγμα μπορεί να ανταλλαχτεί το πρόσωπο κάποιου διάσημου ατόμου σε ένα χαρακτήρα από κάποιο πορνογραφικό υλικό και να παρουσιάζεται τόσο αληθοφανές ώστε να γίνει πιστευτό ότι όντως το άτομο αυτό πραγματικά συμμετείχε στη δημιουργία του υλικού αυτού. Η μέθοδος του DeepFake μπορεί να εφαρμοστεί και σε ψεύτικες ειδήσεις (fake news), σε φάρσες, σε οικονομικές απάτες, ως απειλητικά στοιχεία κ.α. σύμφωνα με το άρθρο [12] μπορεί επίσης να εφαρμοστεί για παράδειγμα για απάτες από κυβερνοεγκληματίες όπου μπορούν να μιμηθούν τη φωνή κάποιου διευθυντή και να ξεγελάσουν τον υπεύθυνο ασφαλείας ώστε να εξουσιοδοτήσει πρόσβαση στο πληροφοριακό σύστημα.

2.6.4 Επιθέσεις Malware

Το Malware είναι κακόβουλο λογισμικό το οποίο χρησιμοποιείται για να αποσπάσει πληροφορίες από το πληροφοριακό σύστημα ή και να προκαλέσει ζημιά σε δεδομένα ή πληροφοριακά συστήματα. Ο όρος Malware περιλαμβάνει διάφορες κατηγορίες κακόβουλων λογισμικών όπως τα viruses, τα worms, τα Trojan, τα Spyware, τα Adware, και τα Ransomware. Τα συστήματα προστασίας anti-malware των πληροφοριακών συστημάτων έχουν βελτιώσει σημαντικά τη λειτουργία τους αφού έχουν ενισχυθεί με την τεχνολογία των Machine Learning ώστε να μπορούν να εντοπίσουν τα κακόβουλα λογισμικά Malware και να τα αποτρέψουν από το να προκαλέσουν ζημιά. Αντίστοιχα όμως, σύμφωνα με τους ερευνητές στο άρθρο [17], χρησιμοποιώντας το Machine Learning οι κυβερνοεγκληματίες μπορούν να εξελίξουν τα κακόβουλα λογισμικά τους ώστε να αποφύγουν τον εντοπισμό τους από τα συστήματα προστασίας του πληροφοριακού συστήματος.

2.6.5 Παράκαμψη των CAPTCHA

Τα CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) δημιουργήθηκαν για να ελέγχεται κατά πόσο ο υπολογιστής λειτουργείται από κάποιο άνθρωπο ή από κάποιο ρομπότ. Με το τρόπο αυτό διαχωρίζεται κατά πόσο θα του εξουσιοδοτηθεί η πρόσβαση ή όχι. Συνεπώς προσφέρουν ένα επιπλέον επίπεδο ασφαλείας στα πληροφοριακά συστήματα έτσι ώστε να αποτραπούν οι επιθέσεις brute forcing ή η μαζική δημιουργία λογαριασμών για κακόβουλους σκοπούς. Η φιλοσοφία των CAPTCHA είναι ότι χρειάζεται η ανθρώπινη ευφυΐα για να λυθούν παρόλο που για τους ανθρώπους αποτελούν απλές προκλήσεις, κάτι όμως που για τα ρομπότ δεν ισχύει. Με την χρήση του Machine Learning όμως, με βάση τους αναλυτές [12], οι προκλήσεις CAPTCHA μπορούν να λυθούν και από υπολογιστικά συστήματα και συνεπώς να παρακαμφθεί η προστασία που προσφέρουν στο διαχωρισμό των ανθρώπων από τους υπολογιστές.

2.6.6 Επιθέσεις Brute Force

Η επίθεση Brute Force είναι η μέθοδος κατά την οποία οι κυβερνοεγκληματίες μέσω εξειδικευμένων εργαλείων δοκιμάζουν συνεχώς κωδικούς πρόσβασης για κάποιο λογαριασμό μέχρι να εντοπίσουν το σωστό κωδικό και να τους παραχωρηθεί η πρόσβαση στο πληροφοριακό σύστημα. Χρησιμοποιώντας το Machine Learning οι κυβερνοεκληματίες μπορούν να δημιουργήσουν λίστες με κωδικούς πρόσβασης πολύ πιο συνοπτικά και να έχουν καλύτερα αποτελέσματα κατά την επίθεση Brute Force. Παράλληλα είναι πιθανόν να εντοπίσουν το σωστό κωδικό σε μικρότερο χρονικό διάστημα με λιγότερες ανεπιτυχής προσπάθειες.

2.6.7 Επίθεση AI poisoning

Το Artificial Intelligence και το Machine Learning βασίζονται κυρίως στα εκπαιδευτικά δεδομένα που θα τους δοθεί έτσι ώστε να μπορούν να κάνουν τις σωστές προβλέψεις, όπως για παράδειγμα πρόβλεψη των καιρικών συνθήκων, και διαχωρισμός των δεδομένων όπως για παράδειγμα ο διαχωρισμός των spam ηλεκτρονικών μηνυμάτων από το νομιμά. Στη περίπτωση όμως που το εκπαιδευτικό υλικό τους είναι λανθασμένο αναπόφευκτα θα προβούν σε λανθασμένες αποφάσεις, προβλέψεις και διαχωρισμούς δεδομένων. Η επίθεση AI poisoning είναι η επίθεση

κατά την οποία οι κυβερνοεκληματίες εισάγουν πλαστά δεδομένα στο σύστημα AI. Τα AI συστήματα θεωρούν ότι πρόκειται για νόμιμα δεδομένα που προστέθηκαν στο εκπαιδευτικό τους υλικό οπόταν συνεχίζουν να εκπαιδεύονται με βάση τα νέα δεδομένα δίνοντας ουσιαστικά λανθασμένα αποτελέσματα [18], [19].

2.7 Υφιστάμενα εργαλεία Machine Learning

2.7.1 Intelligent Automated Penetration Testing System (IAPTS)

Το εργαλείο Intelligent Automated Penetration Testing System (IAPTS) [11] χρησιμοποιεί τη μέθοδο του Reinforcement Learning όπου ο agent αλληλοεπιδρά με το περιβάλλον του, μαθαίνοντας από αυτό βάση των ανταμοιβών που παίρνει για τις ενέργειες του. Η αξιολόγηση του Penetration testing μπορεί να αντιπροσωπευτεί από ένα περιβάλλον Partially Observable Markov Decision Process (POMDP) το οποίο χρησιμοποιεί τη μέθοδο του Reinforcement Learning για την επίλυση των προβλημάτων. Το εργαλείο IAPTS χρησιμοποιεί τον αλγόριθμο Generalized Incremental Pruning (GIP) ο οποίος σύμφωνα με τους ερευνητές [20] μειώνει σημαντικά το χρόνο και τη μνήμη που χρησιμοποιείται από την αλγόριθμο κατά την εκτέλεση ειδικότερα σε μεγάλα POMDP περιβάλλοντα.

Στο αρχικό στάδιο, όπου γίνεται η συλλογή πληροφοριών, το εργαλείο IAPTS χρησιμοποιεί πακέτα εντολών στη γλώσσα προγραμματισμού Python για να μετατρέψει τις πληροφορίες που συλλέχτηκαν από το εξεταζόμενο δίκτυο, σε μορφή POMDP προβλήματος ώστε να μπορεί να γίνει η επεξεργασία των δεδομένων από τον αλγόριθμο. Συνεπώς οι πληροφορίες για κάθε συσκευή του δικτύου που περιλαμβάνουν στοιχεία όπως το λειτουργικό σύστημα της συσκευής, τη θύρα, την υπηρεσία ή την εφαρμογή που εντοπίστηκαν μετατρέπονται στον εξής τρόπο: “Mi-OS1-Port80-ServiceXXX” όπου Mi αντιστοιχεί στο νούμερο που θα δοθεί στη συγκεκριμένη συσκευή. Επίσης περιλαμβάνονται πληροφορίες διασύνδεσης των συσκευών μεταξύ τους όπως το πρωτόκολλο που χρησιμοποιείται για την επικοινωνία των συσκευών, αν είναι μέρος κάποιου υποδικτύου ή εικονικού δικτύου και κατά πόσον υπάρχει αμυντικός περιορισμός. Οι πληροφορίες αυτές θα μετατραπούν στη μορφή “Mi-Mj-TCP-SSH-0”. Ο σκοπός του συγκεκριμένου τρόπου αντιπροσώπευσης των δεδομένων γίνεται αφενός για να μειωθεί το μέγεθος του αρχείου που

αποθηκεύονται τα δεδομένα αυτά και αφετέρου για να διατηρηθούν τα δεδομένα σε μορφή απλή, ευανάγνωστη και με ακρίβεια.

Το εργαλείο IAPTS λειτουργεί σε τέσσερις διαφορετικούς μεθόδους. Η πρώτη μέθοδος "Fully autonomous" επιτρέπει στο εργαλείο IAPTS να διεξάγει την αξιολόγηση του Penetration Testing αυτόνομα χωρίς την παρέμβαση του εμπειρογνώμονα αξιολογητή. Στη δεύτερη μέθοδο "Partially autonomous" το εργαλείο IAPTS διεξάγει τους ελέγχους του Penetration Testing υπό την συνεχή επίβλεψη του εμπειρογνώμονα αξιολογητή. Η τρίτη μέθοδος "Decision-making assistant" επιτρέπει στο εργαλείο IAPTS να βοηθήσει στον έλεγχο που διεξάγει ο εμπειρογνώμονας αξιολογητής υποδεικνύοντας του πιθανές λύσεις με βάση παρόμοια σενάρια που έχει αποθηκευμένα στη μνήμη του από προηγούμενους ελέγχους. Η τέταρτη μέθοδος "Expertise building" χρησιμοποιείται για να μπορέσει το εργαλείο να πραγματοποιεί τους ελέγχους παράλληλα με τον εμπειρογνώμονα αξιολογητή έτσι ώστε να μπορεί να αποκτήσει τη γνώση και την εμπειρία όπου θα αποθηκευτούν στη μνήμη τους για μελλοντική χρήση. Συνεπώς κατά τα αρχικά στάδιο της χρήσης του εργαλείου χρησιμοποιείται ο ανθρώπινος παράγοντας ώστε να μπορέσει να εκπαιδευτεί ο αλγόριθμος και να μπορεί σε μεταγενέστερο στάδιο να πραγματοποιήσει τους ελέγχους αυτόνομα.

Επιπλέον η μέθοδος της ανταμοιβής του εκπαιδευομένου αρχικά βασίζεται στην ανταμοιβή που δίνει ο εμπειρογνώμονας αξιολογητής, ανάλογα με τη δίκη του εμπειρία, κατά την επίβλεψη της αξιολόγησης που πραγματοποιείτε από το εργαλείο IAPTS. Στη συνέχεια αφού έχει παρέλθει το στάδιο της εκπαίδευσης του αλγορίθμου, η μέθοδος της ανταμοιβής καθορίζεται βάση κάποιων κριτηρίων όπως η επίτευξη του τελικού στόχου, η προσέγγιση μιας τερματικής κατάστασης και η αποτυχία επίτευξης κάποιου στόχου.

Το εργαλείο IAPTS έχει επίσης τη δυνατότητα να επαναλάβει την αξιολόγηση του δικτύου για παράδειγμα σε περίπτωση που προστεθούν συσκευές στο δίκτυο ή γίνει κάποια παραμετροποίηση στις υπάρχουσες συσκευές του δικτύου. Κατά την διαδικασία αυτή το εργαλείο IAPTS επαναχρησιμοποιεί τις υπάρχουσες πληροφορίες που έχει αποθηκευμένες στη μνήμη του από τον προηγούμενο έλεγχο. Με τον τρόπο αυτό γίνεται πιο αποτελεσματικό και γρήγορο στην νέα αξιολόγηση του υφιστάμενου δικτύου.

2.7.2 NDSPI-DQN

Ο αλγόριθμος NDSPI-DQL σχεδιάστηκε από τους ερευνητές [21] με σκοπό να αυτοματοποιήσει τη διαδικασία του Penetration Testing και να βελτιώσει την ταχύτητα και την αποτελεσματικότητα των ενεργειών των ομάδων Red Team. Οι ερευνητές παρουσίασαν την διαδικασία του Penetration Testing ως ένα μοντέλο προβλήματος Markov Decision Process και χρησιμοποίησαν τη μέθοδο του Reinforcement Learning για την επίλυση του προβλήματος σε μεγάλης κλίμακας δίκτυα.

Η ονομασία του αλγορίθμου NDSPI-DQL αποτελεί τα αρχικά των πέντε παραμέτρων του Deep Q-Network που επιλέχτηκαν να χρησιμοποιηθούν για την κατασκευή του αλγορίθμου. Οι πέντε παράμετροι είναι το Noisy nets, το Dueling network architectures, το Soft Q-learning, το Prioritized experience replay και το Intrinsic curiosity module. Οι παράμετροι αυτοί έχουν αποδεικτή [21] ότι ενισχύουν την εξερεύνηση του agent από διαφορετικές οπτικές γωνίες και βελτιώνουν την συνολική του απόδοση.

Ο στόχος του agent είναι να εισχωρήσει στην πιο πολύτιμη συσκευή του δικτύου και να αποκτήσει προνόμια διαχειριστή (admin) με τις λιγότερες επιβλαβής ενέργειες, προσομοιάζοντας την επίθεση του κυβερνοεγκληματία. Συνεπώς για να επιτευχθεί αυτός ο στόχος οι ερευνητές καθόρισαν στον αλγόριθμο να διαχωρίζει το δίκτυο και την επίλυση του προβλήματος σε δυο διαφορετικά μέτωπα. Στο ένα μέτωπο πραγματοποιείται η εκτίμηση της αξίας των συσκευών ενώ στο άλλο μέτωπο πραγματοποιείται η εκτίμηση της αξίας των ενεργειών που θα πραγματοποιηθούν. Αυτό έχει σαν αποτέλεσμα ο agent να μπορεί να επιλέξει ανεξάρτητα την συσκευή θύμα και την ενέργεια που πρέπει να πραγματοποιήσει εναντίον του θύματος. Συνεπώς με τον τρόπο αυτό μπορεί να μειωθεί ο χρόνος επίλυσης του προβλήματος σε μεγάλα δίκτυα όπου υπάρχουν εκατοντάδες συσκευές.

Επιπλέον η μέθοδος της αξιολόγησης των ενεργειών βασίζεται στο σύστημα CVSS (Common Vulnerability Scoring System) το οποίο θα αποτελεί και την ανταμοιβή του agent για τις ενέργειες που θα πραγματοποιήσει εναντίον του θύματος. Το σύστημα CVSS αποτελεί ένα ευρέος διαδεδομένο σύστημα που περιλαμβάνει το βαθμό επικινδυνότητας όλων των γνωστών ευπαθειών συνεπώς η αξία της ανταμοιβής του agent για τις ενέργειες του αποτελεί αξιόπιστη και ισοδύναμη με τον βαθμό επικινδυνότητας σε μια πραγματική επίθεση.

2.7.3 Hierarchical Agent - Deep Reinforcement Learning (HA-DRL)

Ο αλγόριθμος HA-DRL (Hierarchical Agent - Deep Reinforcement Learning) [22] αποτελεί μια ακόμα πρόταση για την αυτοματοποίηση της διαδικασίας του Penetration Testing. Χρησιμοποιεί τη μέθοδο του Reinforcement Learning ως μοντέλο για την επίλυση του προβλήματος Markov Decision Process.

Οι ερευνητές στο άρθρο [22] προτείνουν την χρήση πολλαπλών agent οι οποίοι είναι ομαδοποιημένοι σε ιεραρχική δομή για την αντιμετώπιση μεγάλου μήκους δικτύων. Με τον τρόπο αυτό μπορεί να χωριστεί το πεδίο δράσης των εκπαιδευομένων σε μικρότερα υποδίκτυα ώστε να είναι πιο διατηρήσιμο και να βελτίωση τη μάθηση και την απόδοση των εκπαιδευομένων συνολικά.

Η χρήση των πολλαπλών εκπαιδευομένων επιφέρει βασικά πλεονεκτήματα στην επίλυση του προβλήματος όπως για παράδειγμα επίτευξη γρηγορότερης εκπαίδευσης και αναγνώρισης των στοιχείων του δικτύου συγκριτικά με το χρόνο εκπαίδευσης ενός μεμονωμένου agent. Επίσης οι πολλαπλοί agents δεν χρειάζεται να μάθουν ολόκληρη την αρχιτεκτονική του δικτύου για να αποκτήσουν μια συνολική βέλτιστη πολιτική. Αντίθετα συνδυάζουν τη γνώση που απέκτησαν με τους υπολοίπους agents μειώνοντας το χρόνο και αυξάνοντας την απόδοση του αλγορίθμου.

2.7.4 DeepExploit

Το εργαλείο DeepExploit [23] είναι ένα εργαλείο αυτοματοποίησης της ανάλυσης Penetration Testing το οποίο είναι γραμμένο σε γλώσσα προγραμματισμού Python. Χρησιμοποιεί τους αλγόριθμους Keras και TensorFlow του μοντέλου Deep Reinforcement Learning για την επίλυση της ανάλυσης, τον εντοπισμό και την εκμετάλλευση του στόχου.

Το DeepExploit δίνει τη δυνατότητα στους αναλυτές να πραγματοποιήσουν συλλογή πληροφοριών για το στόχο, μοντελοποίηση απειλών, ανάλυση και εκμετάλλευση ευπαθειών και εν κατά κλείδι να εκδώσει την αναφορά των αποτελεσμάτων της ανάλυσης που πραγματοποιήθηκε.

Με τη χρήση του εργαλείου Nmap πραγματοποιείται έρευνα στις συσκευές του δικτύου για να εντοπιστούν πληροφορίες όπως τα λειτουργικά συστήματα των συσκευών του δικτύου, πρωτόκολλα που χρησιμοποιούνται από τις συσκευές και ενεργοποιημένες θύρες και υπηρεσίες. Επιπλέον με τη χρήση του εργαλείου Metasploit το οποίο συνδέετε με το εργαλείο DeepExploit γίνετε εκμετάλλευση των ευπαθειών που έχουν εντοπιστεί.

Τα εκπαιδευτικά δεδομένα του εργαλείου DeepExploit βασίζονται σε δεδομένα που συλλέχτηκαν από προηγούμενες επιτυχημένες επιθέσεις σε ευάλωτα συστήματα όπως το Metasploitable2 και Metaspoitable3 . Τα συστήματα αυτά είναι εκ προθέσεως ευάλωτες εικονικές μηχανές οι οποίες χρησιμοποιούνται για εκπαιδευτικούς σκοπούς ασφάλειας.

2.7.5 AutoPentest-DRL

Οι ερευνητές [24] δημιούργησαν το εργαλείο AutoPentest-DRL (Automated Penetration Testing – Deep Reinforcement Learning) κυρίως για εκπαιδευτικούς σκοπούς έτσι ώστε να μπορούν οι αναλυτές να εξοικειώνονται και να εκπαιδεύονται σε ελεγχόμενο περιβάλλον σε επιθέσεις και στρατηγικές που θα τους βοηθήσουν στην ανάλυση του πραγματικού περιβάλλοντος.

Το εργαλείο AutoPentest-DRL αποτελείται από δυο στάδια. Στο πρώτο στάδιο γίνεται η συλλογή των πληροφοριών και των ευπαθειών του δικτύου με τη χρήση του εργαλείου Shodan. Το εργαλείο Shodan είναι μια μηχανή αναζήτησης στο διαδίκτυο το οποίο περιλαμβάνει πληροφορίες όπως διευθύνσεις IP, ενεργοποιημένες υπηρεσίες και θύρες, και ευπάθειες των συσκευών, για περισσότερες από 500 εκατομμύρια πραγματικές συσκευές δικτύων. Χρησιμοποιείται από τους αναλυτές και τους κυβερνοεκλληματίες για τη συλλογή πληροφοριών των πιθανών στόχων επίθεσης. Οι ευπάθειες που συλλέγονται περιλαμβάνουν τον κωδικό Common Vulnerabilities and Exposures (CVE), τον τύπο της ευπάθειας και το βαθμό εκμετάλλευσης CVSS σύμφωνα με τις βάσεις δεδομένων National Vulnerability Database (NVD) και της Microsoft Database. Οι πληροφορίες των ευπαθειών θα χρησιμοποιούν κατά την επίθεση του δικτύου αλλά και ως μονάδες ανταμοιβής του αλγόριθμου κατά την επίθεση.

Ακολούθως χρησιμοποιώντας το εργαλείο MulVAL δημιουργείται το δέντρο επίθεσης (attack tree) της τοπολογίας του δικτύου με βάση τις πληροφορίες που συλλέχτηκαν. Το εργαλείο

MulVAL είναι εργαλείο ανοικτού κώδικα το οποίο δίνει τη δυνατότητα της δημιουργίας δέντρου επίθεσης με το οποίο μπορούν να μελετηθούν και να εντοπιστούν οι πιθανές διαδρομές προς τον επιθυμητό στόχο ώστε να επιτευχθεί η επιθυμητή επίθεση. Συνεπώς με βάση το δέντρο επίθεσης μπορούν να εντοπιστούν πιθανές διαδρομές προς τη συσκευή στόχου του δικτύου. Στη συνέχεια μετατρέπεται το δέντρο επίθεσης σε μορφή απλοποιημένου πίνακα με τη χρήση του αλγορίθμου Depth-First Search (DFS) ώστε αν μπορεί να εισαχθεί στη συνέχεια στον αλγόριθμο για επεξεργασία.

Στο δεύτερο στάδιο χρησιμοποιώντας αλγόριθμο του μοντέλου Deep Q-Learning Network (DQN) γίνεται επεξεργασία του εισαγόμενου πίνακα ώστε να καθοριστεί ο καταλληλότερος τρόπος και διαδρομή ώστε να επιτευχθεί η επίθεση του δικτύου χρησιμοποιώντας το εργαλείο Metasploit.

2.7.6 Mushikago-femto

Το εργαλείο Mushikago-femto [25] αποτελεί ακόμα ένα εργαλείο αυτοματοποίησης της ανάλυσης Penetration Testing το οποίο επικεντρώνεται κυρίως στην επαλήθευση της εκμετάλλευσης του στόχου. Χρησιμοποιεί την τεχνολογία του Goal-Oriented Action Planning (GOAP) το οποίο στο περιβάλλον των παιχνιδιών με τη χρήση της τεχνίτης νοημοσύνης γνωστό ως “game IA” χρησιμοποιείται για τους χαρακτήρες του παιχνιδιού που δεν τους χειρίζεται κάποιος άνθρωπος. Με αυτό το τρόπο μπορεί το εργαλείο Mushikago-femto να μιμηθεί τις επιθέσεις που πραγματοποιούν οι κυβερνοεκλήματίες και να πραγματοποιεί εικονικές επιθέσεις από τους αναλυτές του Penetration Testing.

Το εργαλείο Mushikago-femto έχει τη δυνατότητα να συλλέξει πληροφορίες για το στόχο όπως το λειτουργικό σύστημα και τις ενεργοποιημένες θύρες, να εντοπίσει το λογαριασμό και το κωδικό πρόσβασης των χρηστών, να συλλέξει πληροφορίες για τις ευπάθειες των συσκευών του δικτύου, να συλλέξει πληροφορίες για τα λογισμικά ασφαλείας που είναι εγκατεστημένα στις συσκευές και να εκμεταλλευτεί τις ευπάθειες των συσκευών.

Κεφάλαιο 3
Μεθοδολογία

Στη παρούσα μεταπτυχιακή διατριβή έχει επιλεχτεί η ποσοτική έρευνα ώστε να μελετηθούν και να συγκριθούν τα υφιστάμενα εργαλεία Machine Learning για αυτοματοποίηση της ανάλυσης penetration testing και η αποτελεσματικότητα τους στο περιβάλλον του Cyber Range.

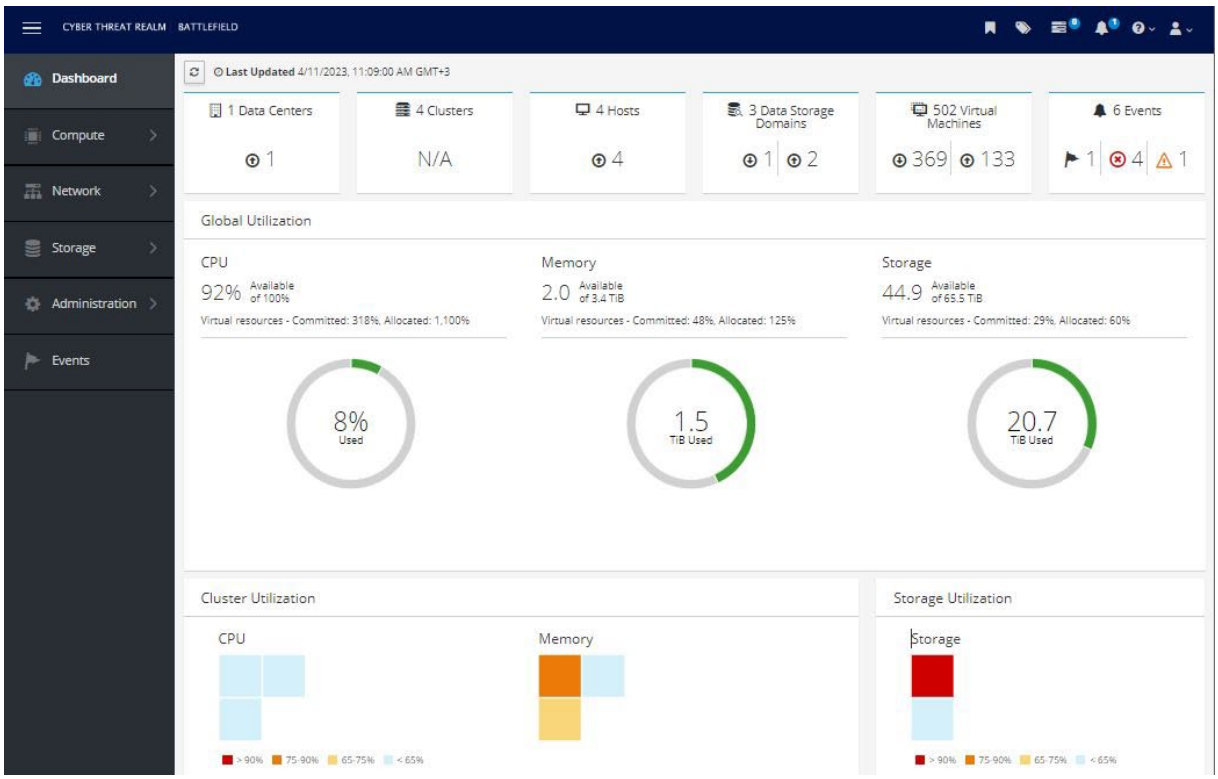
Η ποσοτική έρευνα, σε αντίθεση με την ποιοτική έρευνα, έχει σκοπό να μελετήσει και να συγκρίνει δυο ή και περισσότερες μεταβλητές ώστε να απαντηθούν τα ερευνητικά ερωτήματα που έχουν τεθεί. Εφόσον ένας από τους σκοπούς της παρούσας μεταπτυχιακής διατριβής είναι να συγκριθεί η αποτελεσματικότητα των υφιστάμενων εργαλείων Machine Learning, συνεπώς η ποσοτική έρευνα είναι η πιο κατάλληλη μέθοδος για την εκπόνηση της.

Αφού μελετήθηκαν οι τύποι του Machine Learning και τα υφιστάμενα εργαλεία που έχουν αναπτυχθεί από τους ερευνητές για αυτοματοποίηση της ανάλυσης Penetration Testing, στη συνέχεια της μεταπτυχιακής διατριβής θα πραγματοποιηθεί εγκατάσταση των εργαλείων ανοικτού κώδικα στο περιβάλλον Cyber Range. Ακολούθως θα εκτελεστούν τα εργαλεία αυτά ώστε να μελετηθεί η ευχρηστία και η αποτελεσματικότητα τους στον εντοπισμό των ευπαθειών του δικτύου. Επιπλέον θα μελετηθεί κατά πόσο τα εργαλεία αυτά είναι κατάλληλα ώστε να μπορούν να εξοικειωθούν και να εκπαιδευτούν οι αναλυτές των ομάδων Red Team στη χρήση των εργαλείων Machine Learning.

Στη συνέχεια θα αξιολογηθεί η ικανότητα τους να εντοπίζουν τις ευπάθειες των πληροφοριακών συστημάτων και να συλλέγουν πληροφορίες ώστε να επιτύχουν την εκμετάλλευση των ευπαθειών αυτών σε εικονική επίθεση στο σύστημα στόχου.

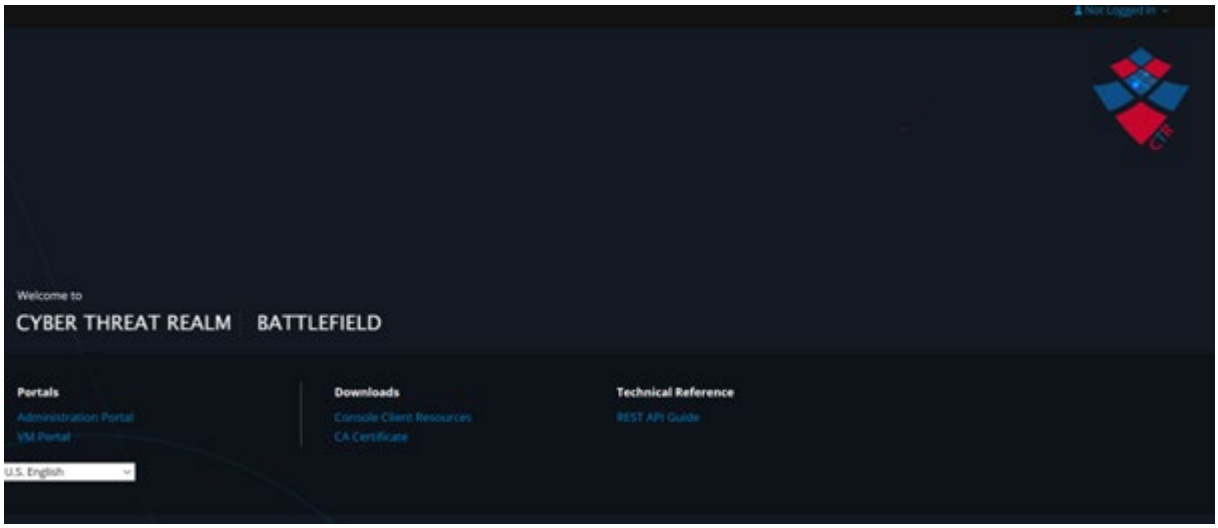
3.1 Περιβάλλον Cyber Range

Το περιβάλλον Cyber Range είναι ένα πειραματικό περιβάλλον το οποίο ανήκει στο Ανοικτό Πανεπιστήμιο Κύπρου και χρησιμοποιείται για εκπαιδευτικούς σκοπούς σε πειράματα, εργασίες και έρευνες της πανεπιστημιακής κοινότητας. Αποτελείται από ένα Data Center, τέσσερα Clusters, τέσσερα Hosts, τρεις τομείς αποθήκευσης δεδομένων (Data Storage Domains) και πάνω από 500 εικονικές μηχανές (Εικόνα 3.1). Τα τεχνικά χαρακτηριστικά του Cyber Range περιβάλλοντος περιλαμβάνουν επίσης μνήμη 3.4 TB και αποθηκευτικό χώρο 65.5 TB



Εικόνα 3. 1: Τεχνικά χαρακτηριστικά του Cyber Range περιβάλλοντος

Η είσοδος στο περιβάλλον επιτυγχάνεται μέσω της πύλης του Cyber Range (Εικόνα 3.2) όπου ο χρήστης μπορεί να επιλέξει ανάμεσα στη πύλη του διαχειριστή του περιβάλλοντος ή στο περιβάλλον των εικονικών μηχανών.



Εικόνα 3. 2: Η Πύλη του Cyber Range

Κεφάλαιο 4
Υλοποίηση

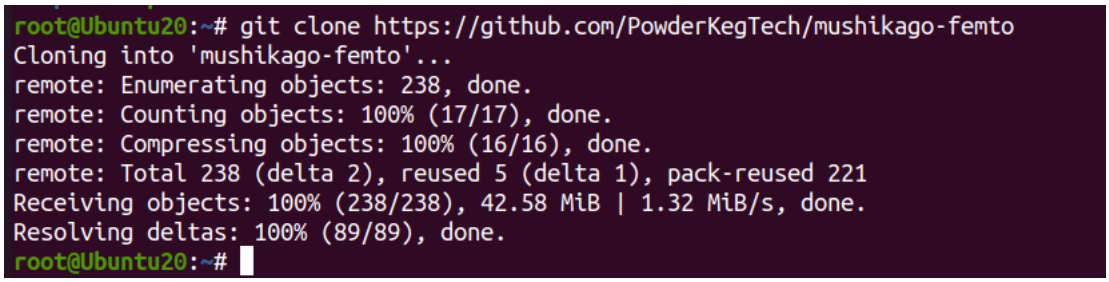
Για την υλοποίηση της μεταπτυχιακής διατριβής επιλέχτηκαν να εγκατασταθούν και να δοκιμαστούν τα εργαλεία Mushikago-femto και DeepExploit τα οποία είναι εργαλεία ανοικτού κώδικα και είναι διαθέσιμα στην ιστοσελίδα https://github.com. Αρχικά θα γίνει η εγκατάσταση των εργαλείων στο εικονικό περιβάλλον VirtualBox σε εκδόσεις μηχανών όπως προτείνονται από τους σχεδιαστές των εργαλείων και ακολούθως θα πραγματοποιηθούν επιθέσεις σε ευάλωτες μηχανές ώστε να αξιολογηθεί η λειτουργία και η αποτελεσματικότητα των εργαλείων.

4.1 Mushikago-femto

4.1.1 Εγκατάσταση εργαλείου Mushikago-femto

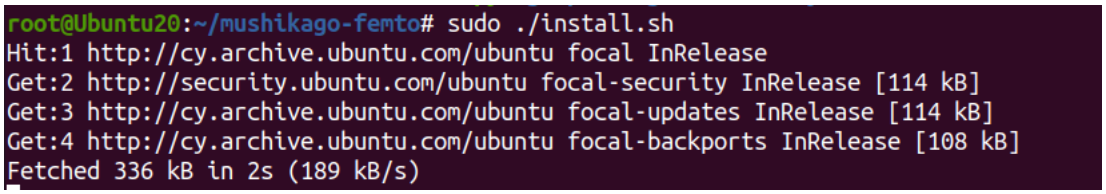
Το εργαλείο Mushikago-femto είναι ένα εργαλείο αυτοματοποίησης της διαδικασίας Penetration testing το οποίο εστιάζεται στην επαλήθευση του post-exploitation το οποίο αποτελεί ένα από τα βασικά βήματα της διαδικασίας αυτής. Η εγκατάσταση του εργαλείου Mushikago-femto [25] έγινε σε εικονική μηχανή Ubuntu 20.04 όπως προτείνεται από τον σχεδιαστή του.

Αρχικά γίνεται λήψη των απαραίτητων αρχείων του εργαλείου από την ιστοσελίδα [25] στο GitHub με τη χρήση της εντολής "git clone https://github.com/PowderKegTech/mushikago-femto" όπως παρουσιάζεται στην Εικόνα 4.1.



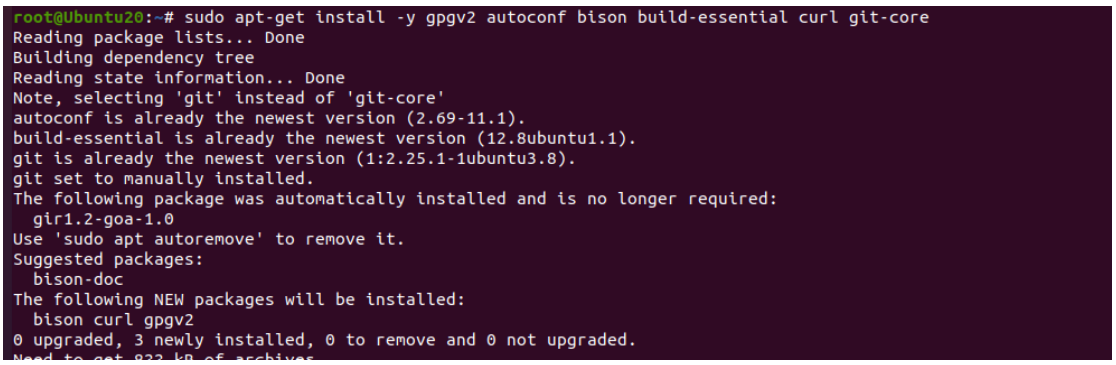
Εικόνα 4. 1: Λήψη αρχείων του εργαλείου Mushikago-femto

Στη συνέχεια εκτελείτε το αρχείο "install.sh" που περιέχεται στο φάκελο "Mushikago-femto" που έχει δημιουργηθεί (Εικόνα 4.2). Το αρχείο εκτελεί εγκαταστάσεις διάφορων εργαλείων που χρειάζονται για την εκτέλεση του εργαλείου Mushikago-femto όπως για παράδειγμα τα εργαλεία Nmap, arp-scan, pymetasploit3 έκδοση ίση ή μεγαλύτερη του 1.0.3, msgpack έκδοση ίση ή μεγαλύτερη του 1.0.2 κ.α.

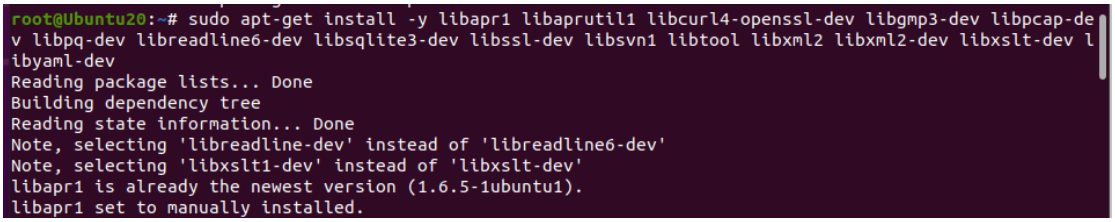


Εικόνα 4. 2: Εκτέλεση του αρχείου "install.sh"

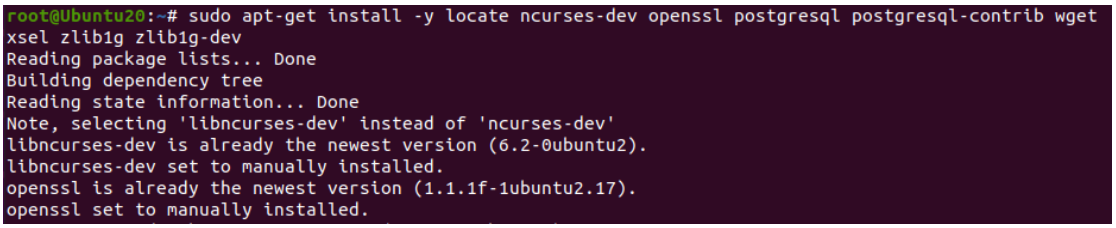
Αφού ολοκληρωθεί η εγκατάσταση των εργαλείων, το επόμενο εργαλείο που χρειάζεται να εγκατασταθεί είναι το εργαλείο Metasploit. Αρχικά πρέπει να εγκατασταθούν κάποια προ απαιτούμενα πακέτα. Τα πακέτα αυτά εγκαθιστόνται με τις παρακάτω εντολές (Εικόνες 4.3-4.5) "sudo apt-get install -y gpgv2 autoconf bison build-essential curl git-core", "sudo apt-get install -y libapr1 libaprutil1 libcurl4-opnssl-dev libgmp3-dev libpcap-dev libpq-dev libreadline6-dev libsqlite3-dev libssl-dev libsvn1 libtool libxml2 libxml2-dev libxslt-dev libyaml-dev" και " sudo apt-get install -y locate ncurses-dev openssl postgresql postgresql-contrib wget xsel zlib1g zlib1g-dev".



Εικόνα 4. 3: Εγκατάσταση προ-απαιτούμενων πακέτων για το εργαλείο Metasploit

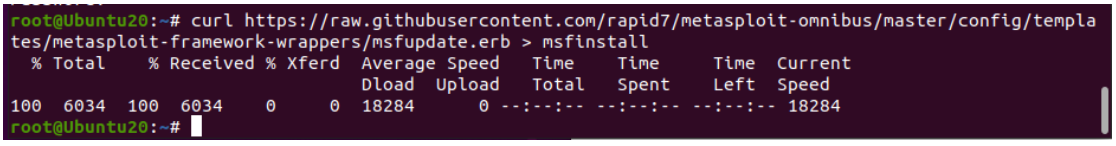


Εικόνα 4. 4: Εγκατάσταση προ-απαιτούμενων πακέτων για το εργαλείο Metasploit

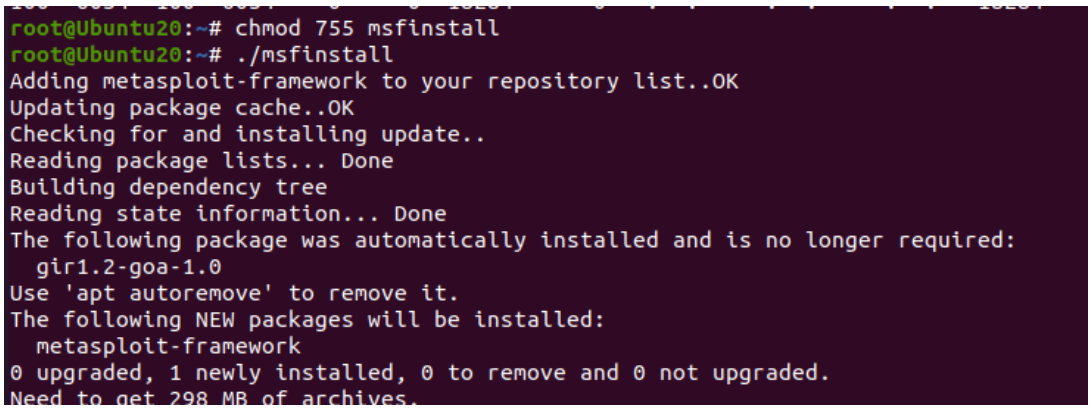


Εικόνα 4. 5: Εγκατάσταση προ-απαιτούμενων πακέτων για το εργαλείο Metasploit-Framework

Ακολούθως γίνεται εγκατάσταση του εργαλείου Metasploit-Framework χρησιμοποιώντας την εντολή "curl" για να αποθηκευτεί τοπικά ο κώδικας που απαιτείται για την εγκατάσταση (Εικόνα 4.6). Στη συνέχεια γίνεται διαφοροποίηση των δικαιωμάτων του εκτελούμενου κώδικα χρησιμοποιώντας την εντολή "chmod" (Εικόνα 4.7). Έπειτα εκτελείτε η εγκατάσταση του κώδικα του εργαλείου Metasploit-Framework με τη χρήση της εντολής "msfinstall" (Εικόνα 4.7).

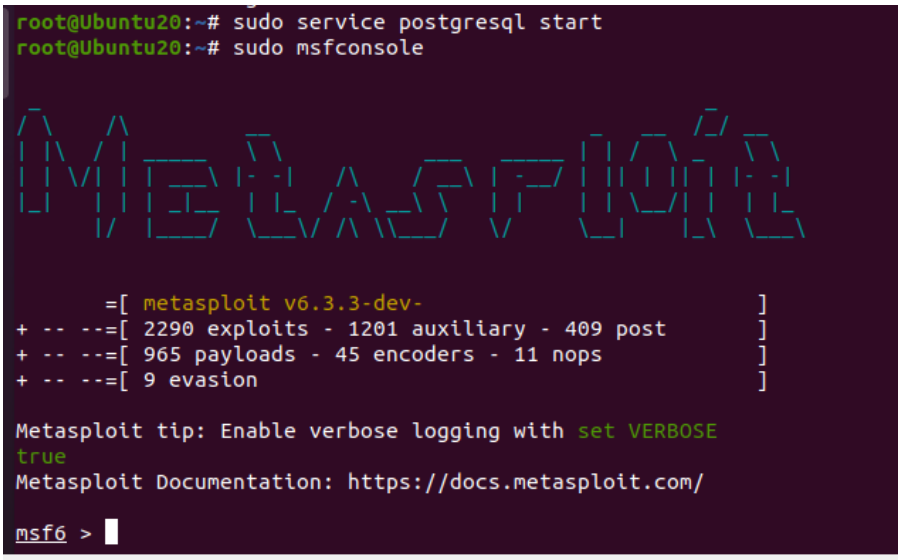


Εικόνα 4. 6: Αποθήκευση τοπικά του κώδικα εγκατάστασης



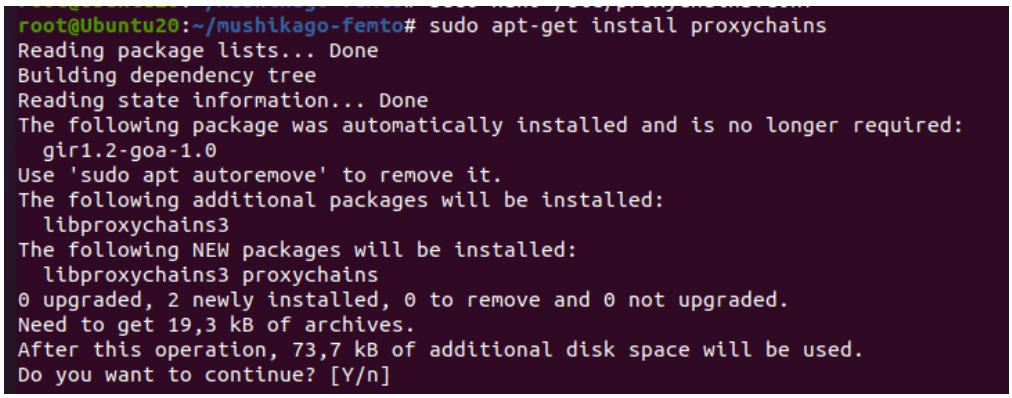
Εικόνα 4. 7: Διαφοροποίηση δικαιωμάτων και εγκατάσταση του εργαλείου Metasploit-Framework

Αφού ολοκληρωθεί η εγκατάσταση γίνεται έναρξη της υπηρεσίας "postgresql" και του εργαλείου Metasploit-Framework με τη χρήση της εντολής "msfconsole" (Εικόνα 4.8).



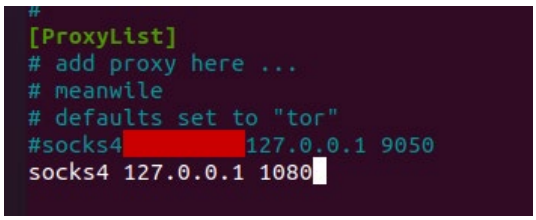
Εικόνα 4. 8: Έναρξη της υπηρεσίας postgresql και του εργαλείου Metasploit-Framework

Στη συνέχεια πραγματοποιείται εγκατάσταση του εργαλείου proxychains με τη χρήση της εντολής " sudo apt-get install proxychains" (Εικόνα 4.9).



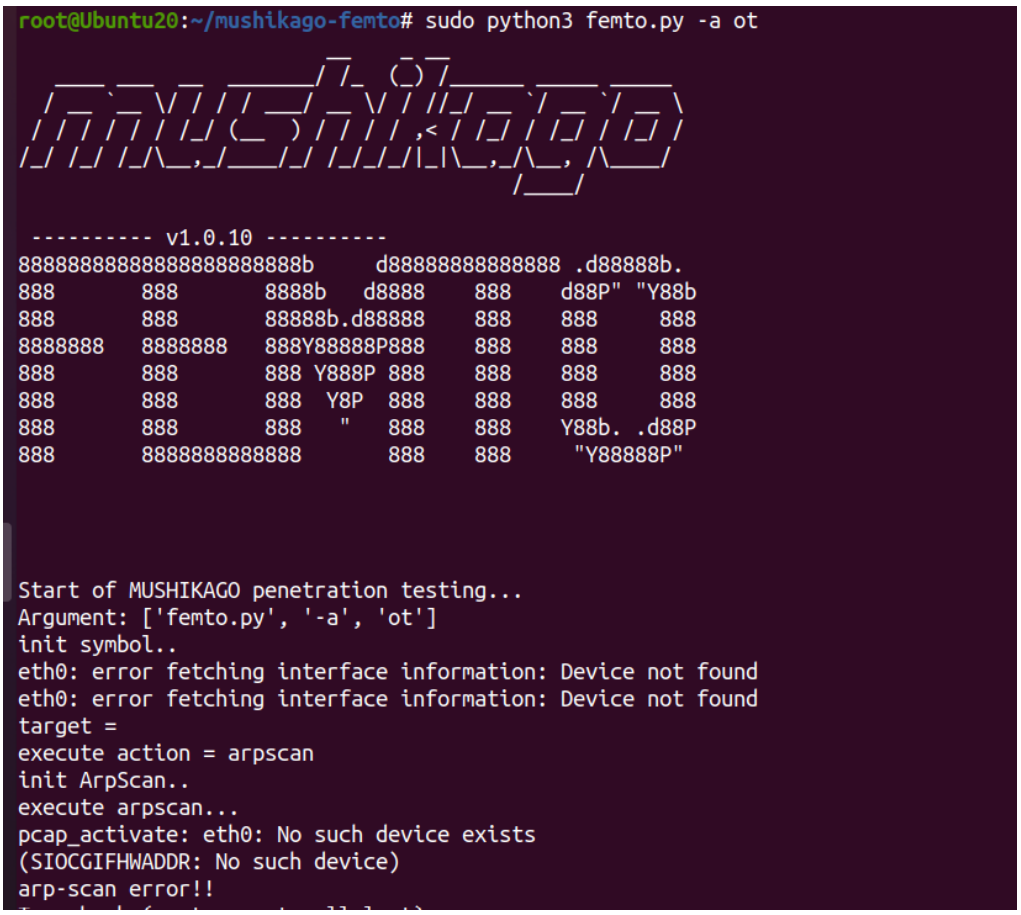
Εικόνα 4. 9: Εγκατάσταση του εργαλείου proxychains

Στη συνέχεια πραγματοποιείται διαμόρφωση των παραμέτρων του αρχείου /etc/proxychains.conf προσθέτοντας την διεύθυνση IP 127.0.0.1 και τη θύρα 1080 όπως παρουσιάζεται στην εικόνα 4.10.

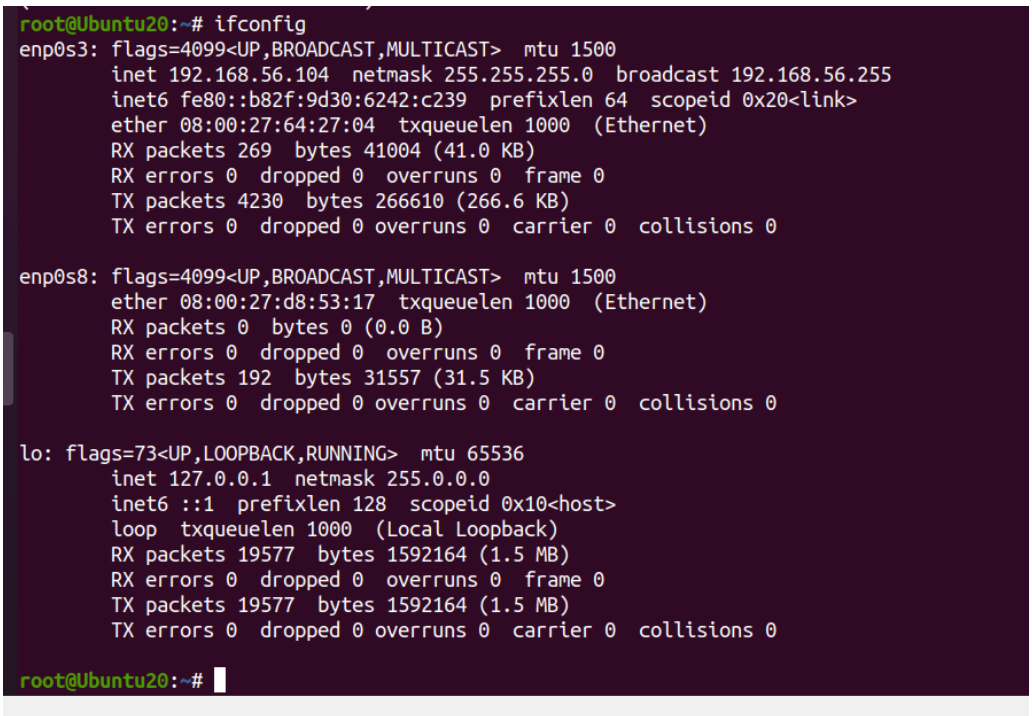


Εικόνα 4. 10: Παραμετροποίηση του αρχείου proxychains.conf

Κατά την εκτέλεση του εργαλείου Mushikago-femto παρουσιάζεται σφάλμα το οποίο σχετίζεται με την εκτέλεση του πακέτου arp-scan (Εικόνα 4.11). Το σφάλμα προκύπτει διότι στις καινούργιες εκδόσεις Ubuntu οι διεπαφές ορίζονται ως “enp0s” (Εικόνα 4.12) ενώ το πακέτο arp-scan σαρώνει το δίκτυο μέσω της διεπαφής “eth0”



Εικόνα 4. 11: Σφάλμα εκτέλεσης πακέτου arp-scan



Εικόνα 4. 12: Παρουσίαση υφιστάμενων διεπαφών της μηχανής Ubuntu

Συνεπώς θα πρέπει να διορθωθεί η ονοματολογία των διεπαφών ώστε να χρησιμοποιείται η ονομασία “eth0”. Η διαδικασία αλλαγής της ονοματολογίας των διεπαφών περιγράφεται στο παράρτημα Α1. Αφού ολοκληρωθεί η διαδικασία οι υφιστάμενες διεπαφές εμφανίζονται με την ονομασία “eth0” όπως παρουσιάζεται στην εικόνα 4.13.

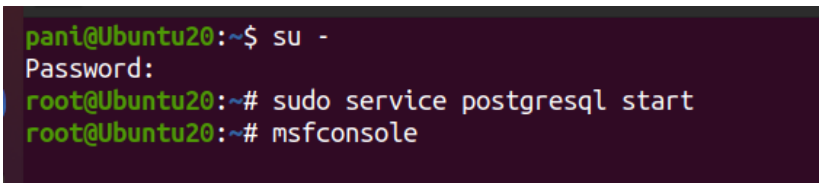
```
root@Ubuntu20:/# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.56.104  netmask 255.255.255.0  broadcast 192.168.56.255
        inet6 fe80::5b5d:8bc5:c951:bbc4  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:64:27:04  txqueuelen 1000  (Ethernet)
        RX packets 93  bytes 19059 (19.0 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 86  bytes 11833 (11.8 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.3.15  netmask 255.255.255.0  broadcast 10.0.3.255
        inet6 fe80::bb97:89f:35f1:830d  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:d8:53:17  txqueuelen 1000  (Ethernet)
        RX packets 28431  bytes 42737894 (42.7 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1518  bytes 123520 (123.5 KB)
        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
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 889  bytes 84578 (84.5 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 889  bytes 84578 (84.5 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Εικόνα 4. 13: Παρουσίαση διεπαφών μετά την αλλαγή της ονομασίας σε “eth0”

Στη συνέχεια ακολουθεί η εκτέλεση του εργαλείου Mushikago-femto

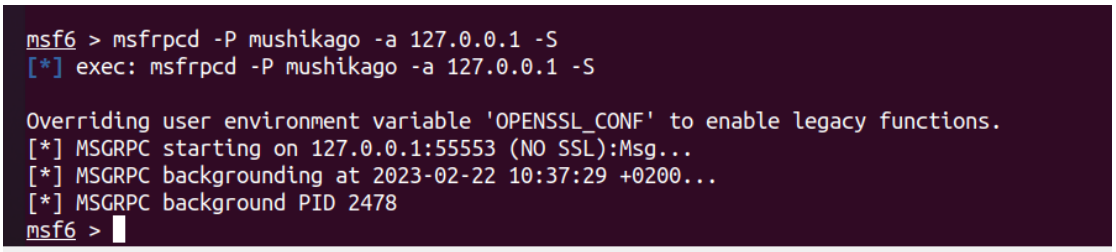
4.1.2 Λειτουργία εργαλείου Mushikago-femto

Για να γίνει εφικτή η λειτουργία του εργαλείου Mushikago-femto θα πρέπει να εκκινήσει πρώτα το εργαλείο Metasploit-Framework. Αρχικά εκτελείται η εντολή “sudo service postgresql start” για να ενεργοποιηθεί η υπηρεσία postgresql (Εικόνα 4.14) και ακολούθως με την εντολή sudo msfconsole γίνεται η εκκίνηση του εργαλείου Metasploit-Framework όπως παρουσιάζεται στην εικόνα 4.14.



Εικόνα 4. 14: Εκκίνηση υπηρεσίας postgresql και εργαλείου Metasploit-Framework

Ακολούθως εκτελείται η εντολή "msfrpcd -P mushikago -a 127.0.0.1 -S" (Εικόνα 4.15) με τις ανάλογες παραμέτρους ώστε να μπορεί το εργαλείο να εκμεταλλευτεί τις αδυναμίες του συστήματος στόχου. Οι παράμετροι που χρειάζεται να δηλωθούν είναι το -P όπου αντιπροσωπεύει το κωδικό ασφάλειας που χρειάζεται για την αυθεντικοποίηση, -a όπου αντιπροσωπεύει τη διεύθυνση IP της επιτιθέμενης μηχανής, και -S για την απενεργοποίηση της σύνδεσης SLL. Οι παράμετροι αυτοί έχουν εντοπιστεί έπειτα από σφάλματα που παρουσιάζονταν την εκτέλεση του εργαλείου. Τα σφάλματα αυτά παρουσιάζονται στα παραρτήματα Α2, Α3 και Α4.



Εικόνα 4. 15: Εκτέλεση της εντολής msfrpcd με τις ανάλογες παραμέτρους

Στη συνέχεια από ένα άλλο παράθυρο γραμμής εντολών πραγματοποιείται η εκκίνηση του εργαλείου Mushikago-femto. Η εντολή εκκίνησης του εργαλείου ποικίλει ανάλογα με το σύστημα στόχου. Στη συνέχεια της Μεταπτυχιακής Διατριβής παραθέτονται παραδείγματα εκτέλεσης του εργαλείου Mushikago-femto με τις διαθέσιμες επιλογές.

4.1.2.1 Επιλογή εκτέλεσης σε σύστημα στόχου IT (Information Technology)

Μια από τις επιλογές που προσφέρει το εργαλείο Mushikago-femto είναι η σάρωση και η εκτέλεση της διαδικασίας Penetration Testing σε συστήματα IT (Information Technology). Τα συστήματα IT περιλαμβάνουν συστήματα τεχνολογίας πληροφοριών και επικοινωνίας (Information and Communication Technology ICT). Στα συστήματα αυτά συγκαταλέγονται για παράδειγμα τα

πληροφοριακά συστήματα, οι εξυπηρετητές, συσκευές δικτύωσης κ.α. Συνεπώς με τη χρήση της επιλογής αυτής θα εκτελεστεί η διαδικασία Penetration Testing σε όλα τα πληροφορία συστήματα που θα εντοπιστούν στο δίκτυο.

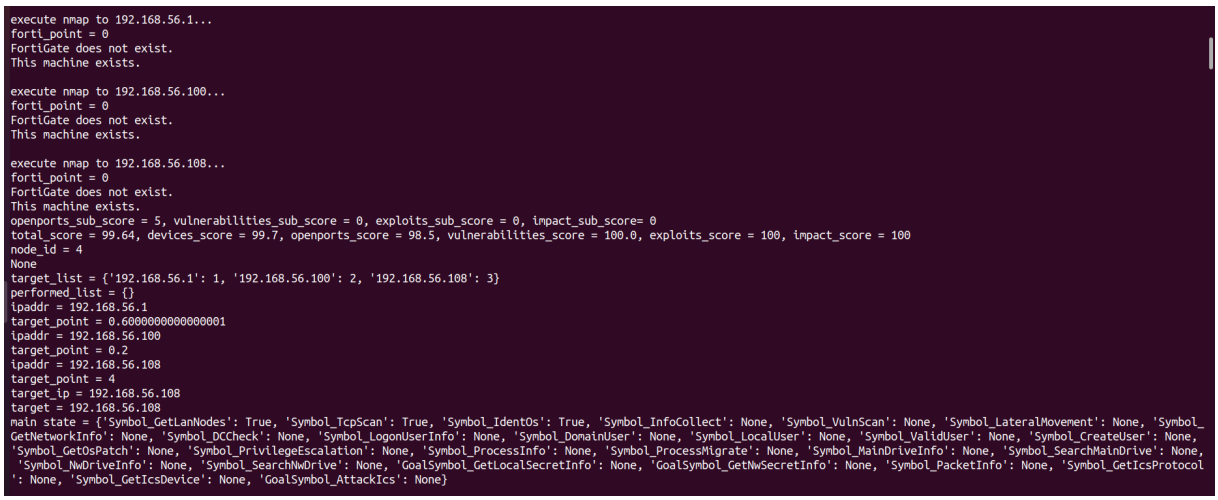
Χρησιμοποιώντας την εντολή “sudo python3 femto.py -a it” (Εικόνα 4.16) ξεκινά η σάρωση του δικτύου και η εκτέλεση της διαδικασίας Penetration Testing στα συστήματα που θα εντοπιστούν. Στιγμιότυπα της διαδικασίας παρουσιάζονται στις εικόνες 4.17-4.19 .

```
pani@Ubuntu20:~$ su -
Password:
root@Ubuntu20:~# cd mushikago-femto/
root@Ubuntu20:~/mushikago-femto# sudo python3 femto.py -a it
```

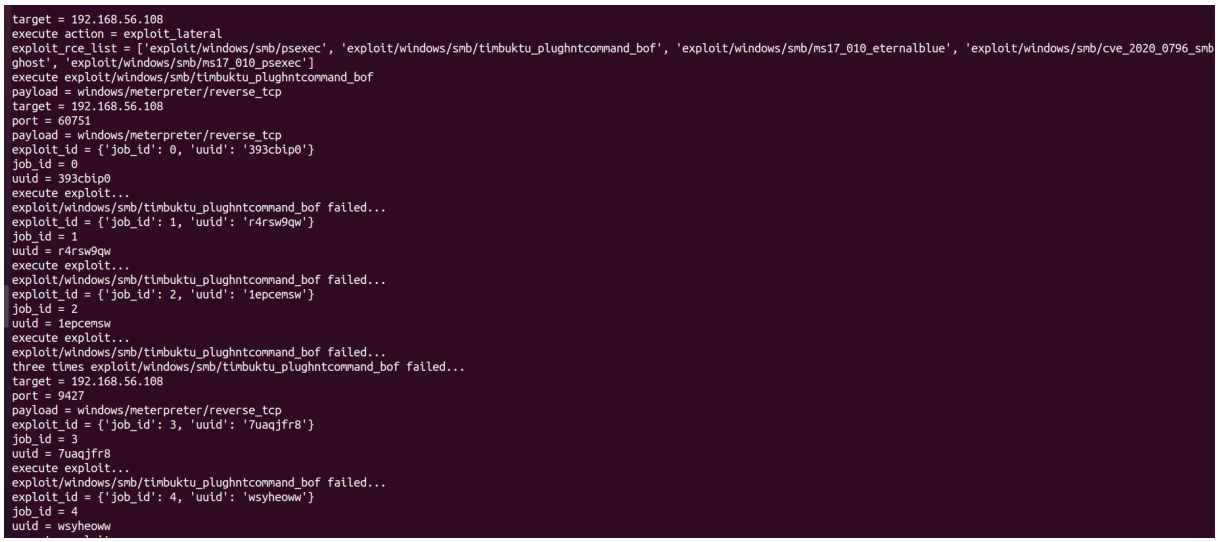
Εικόνα 4. 16: Εκκίνηση εργαλείου Mushikago-femto σε σύστημα στόχου IT

```
root@Ubuntu20:~/mushikago-femto# sudo python3 femto.py -a it
                                  __      _ __
   ____ ___  __  _____/ /_  (_) /_____ _____ _____
  / __ `__ \/ / / / ___/ __ \/ / //_/ __ `/ __ `/ __ \
 / / / / / / /_/ (__  ) / / / / ,< / /_/ / /_/ / /_/ /
/_/ /_/ /_/\__,_/____/_/ /_/_/_/|_|\__,_/\__, /\____/
                                        /____/

 ---------- v1.0.10 ----------
8888888888888888888888b     d88888888888888 .d88888b.
888       888       8888b   d8888    888    d88P" "Y88b
888       888       88888b.d88888    888    888     888
8888888   8888888   888Y88888P888    888    888     888
888       888       888 Y888P 888    888    888     888
888       888       888  Y8P  888    888    888     888
888       888       888   "   888    888    Y88b. .d88P
888       8888888888888       888    888     "Y88888P"



Start of MUSHIKAGO penetration testing...
Argument: ['femto.py', '-a', 'it']
init symbol..
target = 192.168.56.107
execute action = arpscan
init ArpScan..
execute arpscan...
192.168.56.1    0a:00:27:00:00:11       (Unknown: locally administered)
192.168.56.100  08:00:27:fb:b2:4b       PCS Systemtechnik GmbH
192.168.56.108  08:00:27:8b:a2:16       PCS Systemtechnik GmbH

init ICS Detect..
execute action = tcpscan
```

Εικόνα 4. 17: Στιγμιότυπα από τη διαδικασία εκτέλεσης του εργαλείου σε σύστημα στόχου IT



Εικόνα 4. 18: Στιγμιότυπα από τη διαδικασία εκτέλεσης του εργαλείου σε σύστημα στόχου IT



Εικόνα 4. 19: Στιγμιότυπα από τη διαδικασία εκτέλεσης του εργαλείου σε σύστημα στόχου IT

4.1.2.2 Επιλογή εκτέλεσης σε σύστημα στόχου OT (Operational Technology)

Το εργαλείο Mushikago-femto προσφέρει επίσης την επιλογή σάρωσης και εκτέλεσης της διαδικασίας Penetration Testing σε συστήματα OT (Operation Technology). Στα συστήματα OT συγκαταλέγονται βιομηχανικά συστήματα ελέγχου (Industrial Control Systems ICS) όπως για παράδειγμα το σύστημα SCADA (Supervisory Control and Data Acquisition System) τα οποία είναι υπεύθυνα για την παρακολούθηση και τον έλεγχο των συστημάτων και των πυλών IoT (Internet of Things). Συνεπώς κρίνεται χρήσιμη η διεξαγωγή του ελέγχου Penetration Testing και στα συστήματα αυτά.

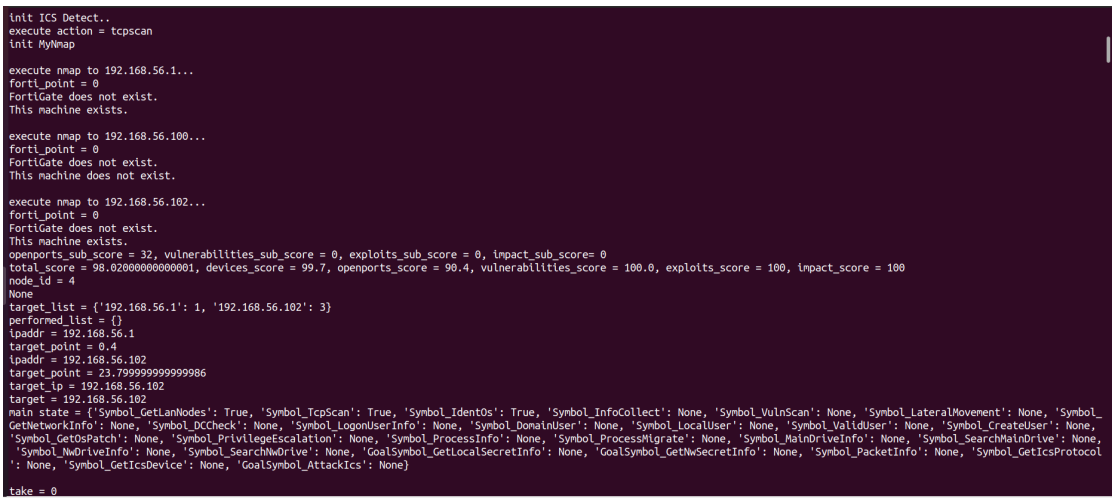
Χρησιμοποιώντας την εντολή “sudo python3 femto.py -a ot” (Εικόνα 4.20) ξεκινά η σάρωση του δικτύου και η εκτέλεση της διαδικασίας Penetration Testing στα συστήματα που θα εντοπιστούν. Στιγμιότυπα της διαδικασίας παρουσιάζονται στις εικόνες 4.21-4.24.

```
root@Ubuntu20:~# cd mushikago-femto/
root@Ubuntu20:~/mushikago-femto# sudo python3 femto.py -a ot
```

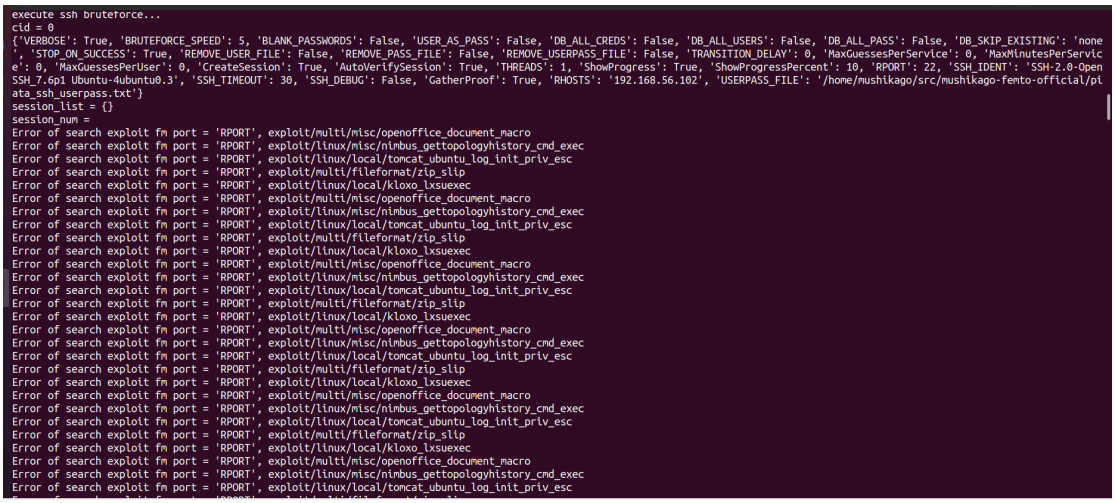
Εικόνα 4. 20: Εκκίνηση εργαλείου Mushikago-femto σε σύστημα στόχου OT

```
root@Ubuntu20:~# cd mushikago-femto/
root@Ubuntu20:~/mushikago-femto# sudo python3 femto.py -a ot
                    __      _ __
   ____ ___  __  _____/ /_  (_) /______ _____ _____
  / __ `__ \/ / / / ___/ __ \/ / //_/ __ `/ __ `/ __ \
 / / / / / / /_/ (__  ) / / / / ,< / /_/ / /_/ / /_/ /
/_/ /_/ /_/\__,_/____/_/ /_/_/_/|_|\__,_/\__, /\____/
                                        /____/

 ---------- v1.0.10 ----------
88888888888888888888888b     d88888888888888 .d88888b.
888       888       8888b   d8888    888    d88P" "Y88b
888       888       88888b.d88888    888    888     888
8888888   8888888   888Y88888P888    888    888     888
888       888       888 Y888P 888    888    888     888
888       888       888  Y8P  888    888    888     888
888       888       888   "   888    888    Y88b. .d88P
888       8888888888888       888    888     "Y88888P"



Start of MUSHIKAGO penetration testing...
Argument: ['femto.py', '-a', 'ot']
init symbol..
target = 192.168.56.107
execute action = arpscan
init ArpScan..
execute arpscan...
192.168.56.1    0a:00:27:00:00:11       (Unknown: locally administered)
192.168.56.100  08:00:27:f4:0d:68       PCS Systemtechnik GmbH
192.168.56.102  08:00:27:e1:3f:3a       PCS Systemtechnik GmbH

init ICS Detect..
execute action = tcpscan
init MyNmap
```

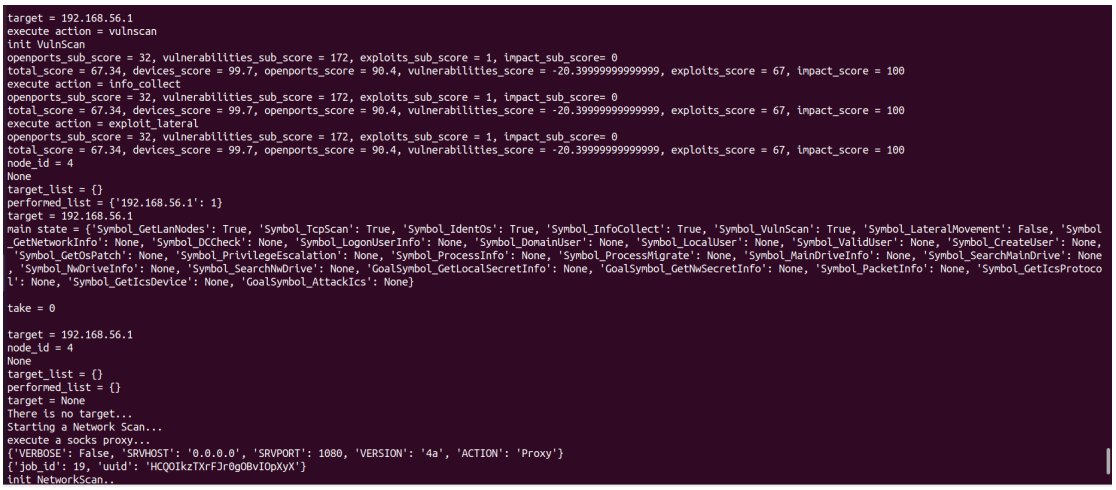
Εικόνα 4. 21: Στιγμιότυπα από τη διαδικασία εκτέλεσης του εργαλείου σε σύστημα στόχου OT



Εικόνα 4. 22: Στιγμιότυπα από τη διαδικασία εκτέλεσης του εργαλείου σε σύστημα στόχου OT



Εικόνα 4. 23: Στιγμιότυπα από τη διαδικασία εκτέλεσης του εργαλείου σε σύστημα στόχου OT



Εικόνα 4. 24: Στιγμιότυπα από τη διαδικασία εκτέλεσης του εργαλείου σε σύστημα στόχου OT

4.1.2.3 Επιλογή εκτέλεσης σε καθορισμένη διεύθυνση IP

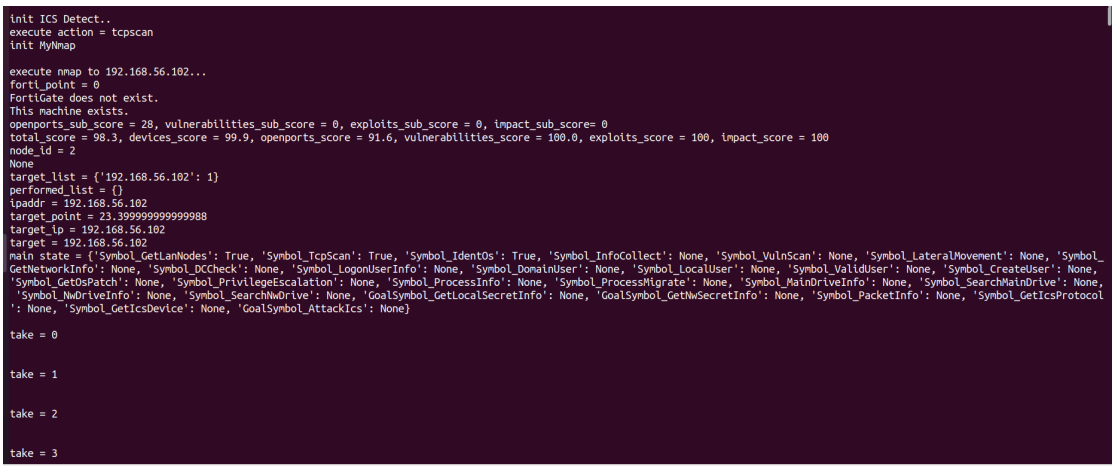
Επιπλέον το εργαλείο Mushikago-femto προσφέρει την επιλογή σάρωσης και εκτέλεσης της διαδικασίας Penetration Testing σε συσκευή με συγκεκριμένη διεύθυνση IP. Η επιλογή αυτή εκτελείται χρησιμοποιώντας την εντολή “sudo python3 femto.py -a it -ip 192.168.56.102” όπως παρουσιάζεται στο πιο κάτω παράδειγμα (Εικόνα 4.25). Στιγμιότυπα της διαδικασίας παρουσιάζονται στις εικόνες 4.26-4.29.

```
pani@Ubuntu20:~$ su -
Password:
root@Ubuntu20:~# cd mushikago-femto/
root@Ubuntu20:~/mushikago-femto# sudo python3 femto.py -a it -ip 192.168.56.102
```

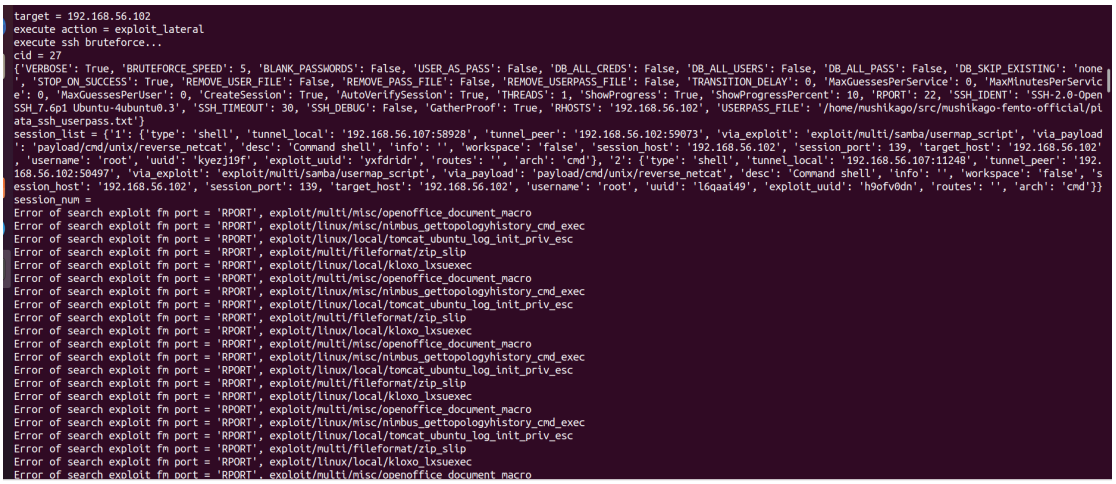
Εικόνα 4. 25: Εκκίνηση εργαλείου σε σύστημα στόχου με καθορισμένη διεύθυνση IP

```
pani@Ubuntu20:~$ su -
Password:
root@Ubuntu20:~# cd mushikago-femto/
root@Ubuntu20:~/mushikago-femto# sudo python3 femto.py -a it -ip 192.168.56.102


                        __      _ __
   ____ ___  __  _____/ /_  (_) /_____ _____ _____
  / __ `__ \/ / / / ___/ __ \/ / //_/ __ `/ __ `/ __ \
 / / / / / / /_/ (__  ) / / / / ,< / /_/ / /_/ / /_/ /
/_/ /_/ /_/\__,_/____/_/ /_/_/_/|_|\__,_/\__, /\____/
                                        /____/

 ---------- v1.0.10 ----------
888888888888888888888888b     d88888888888888 .d88888b.
888       888       8888b   d8888    888    d88P" "Y88b
888       888       88888b.d88888    888    888     888
8888888   8888888   888Y88888P888    888    888     888
888       888       888 Y888P 888    888    888     888
888       888       888  Y8P  888    888    888     888
888       888       888   "   888    888    Y88b. .d88P
888       8888888888888       888    888     "Y88888P"



Start of MUSHIKAGO penetration testing...
Argument: ['femto.py', '-a', 'it', '-ip', '192.168.56.102']
Check target IP address
192.168.56.102 is IP address
init symbol..
target = 192.168.56.102
execute action = arpscan
init ArpScan..
execute arpscan...
192.168.56.102  08:00:27:e1:3f:3a       PCS Systemtechnik GmbH

init ICS Detect..
```

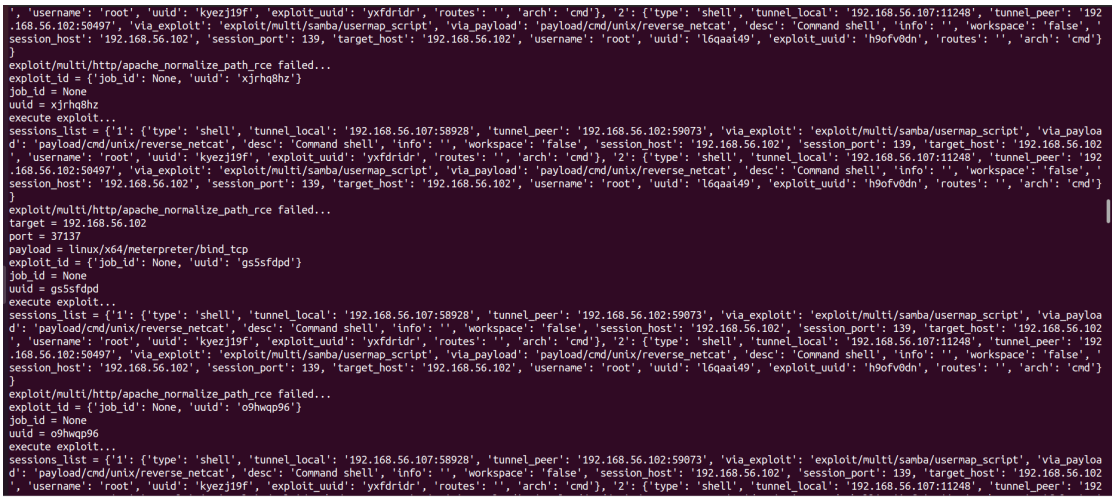
Εικόνα 4. 26: Στιγμιότυπα από τη διαδικασία εκτέλεσης του εργαλείου σε καθορισμένη διεύθυνση



Εικόνα 4. 27: Στιγμιότυπα από τη διαδικασία εκτέλεσης του εργαλείου σε καθορισμένη διεύθυνση



Εικόνα 4. 28: Στιγμιότυπα από τη διαδικασία εκτέλεσης του εργαλείου σε καθορισμένη διεύθυνση



Εικόνα 4. 29: Στιγμιότυπα από τη διαδικασία εκτέλεσης του εργαλείου σε καθορισμένη διεύθυνση

Κατά τη διάρκεια του ελέγχου παρουσιάζονται τα στάδια της εκτέλεσης του εργαλείου καθώς και τα αποτελέσματα των προσπαθειών εντοπισμού και εκμετάλλευσης των ευπαθειών. Παράλληλα τα αποτελέσματα αποθηκεύονται στο αρχείο Mushikago.log. Απόσπασμα του ελέγχου από το αρχείο αυτό παρουσιάζεται στην εικόνα 4.30. Συγκεκριμένα παρουσιάζεται η εκκίνηση του ελέγχου και ο εντοπισμός των διαθέσιμων ενεργών θυρών και υπηρεσιών του συστήματος στόχου.

```
2023-03-30 21:09:27,472     INFO Start of MUSHIKAGO penetration testing...
2023-03-30 21:09:27,487     INFO Argument: ['femto.py', '-a', 'it', '-ip', '192.168.56.102']
2023-03-30 21:09:27,488     INFO Check target IP address
2023-03-30 21:09:27,488     INFO 192.168.56.102 (target) is IP address.
2023-03-30 21:09:27,489     INFO MUSHIKAGO IT mode
2023-03-30 21:09:47,655     INFO target = 192.168.56.102
2023-03-30 21:09:47,657     INFO action plan = ['arpscan', 'tcpscan']
2023-03-30 21:09:47,657     INFO execute action = arpscan
2023-03-30 21:09:47,658     INFO execute arpscan...
2023-03-30 21:09:48,330     INFO arpscan result =
192.168.56.102    08:00:27:e1:3f:3a PCS Systemtechnik GmbH

2023-03-30 21:09:48,345     INFO execute action = tcpscan
2023-03-30 21:09:48,346     INFO execute nmap to 192.168.56.102
2023-03-30 21:12:29,834     INFO detect_ports = [{'number': '21/tcp', 'service': 'ftp', 'version': 'vsftpd 2.3.4'},
 {'number': '22/tcp',
  'service': 'ssh',
  'version': 'OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)'},
 {'number': '23/tcp', 'service': 'telnet', 'version': 'Linux telnetd'},
 {'number': '25/tcp', 'service': 'smtp', 'version': 'Postfix smtpd'},
 {'number': '53/tcp', 'service': 'domain', 'version': 'ISC BIND 9.4.2'},
 {'number': '80/tcp',
  'service': 'http',
  'version': 'Apache httpd 2.2.8 ((Ubuntu) DAV/2)'},
 {'number': '111/tcp', 'service': 'rpcbind', 'version': '2 (RPC #100000)'},
 {'number': '139/tcp',
  'service': 'netbios-ssn',
  'version': 'Samba smbd 3.X - 4.X (workgroup: WORKGROUP)'},
 {'number': '445/tcp',
  'service': 'netbios-ssn',
  'version': 'Samba smbd 3.X - 4.X (workgroup: WORKGROUP)'},
 {'number': '512/tcp', 'service': 'exec', 'version': 'netkit-rsh rexecd'},
 {'number': '513/tcp', 'service': 'login', 'version': ''},
 {'number': '514/tcp', 'service': 'shell', 'version': 'Netkit rshd'},
```

Εικόνα 4. 30: Απόσπασμα αποτελεσμάτων από το αρχείο Mushikago.log

Στην εικόνα 4.31 παρουσιάζεται ένα παράδειγμα επιτυχούς εκμετάλλευσης. Αντίστοιχα στο αρχείο Mushikago.log παρουσιάζονται το αποτέλεσμα της εκμετάλλευσης αυτής (Εικόνα 4.32).

```
execute exploit...
exploit/multi/http/apache_apisix_api_default_token_rce failed...
three times exploit/multi/http/apache_apisix_api_default_token_rce failed...
execute exploit/linux/http/piranha_passwd_exec
execute exploit/multi/samba/usermap_script
payload = cmd/unix/reverse_netcat
target = 192.168.56.102
port = 25694
payload = cmd/unix/reverse_netcat
exploit_id = {'job_id': 6, 'uuid': 'ooidnves'}
job_id = 6
uuid = ooidnves
execute exploit...
sessions_list = {'1': {'type': 'shell', 'tunnel_local': '192.168.56.107:25694', 'tunnel_peer': '192.168.56.102:58913', 'via_exploit': 'exploit/multi/samba/usermap_script', 'via_payloa
d': 'payload/cmd/unix/reverse_netcat', 'desc': 'Command shell', 'info': '', 'workspace': 'default', 'session_host': '192.168.56.102', 'session_port': 139, 'target_host': '192.168.56.1
02', 'username': 'pani', 'uuid': 'mtlrrji0', 'exploit_uuid': 'ooidnves', 'routes': '', 'arch': 'cmd'}}
match key = 1
exploit_uuid = ooidnves
exploit success...
Sessions avaiables :
['1']
openports_sub_score = 29, vulnerabilities_sub_score = 0, exploits_sub_score = 1, impact_sub_score= 0
total_score = 91.64, devices_score = 99.9, openports_score = 91.3, vulnerabilities_score = 100.0, exploits_score = 67, impact_score = 100
```

Εικόνα 4. 31: Επιτυχής εκμετάλλευση ευπάθειας

```
2023-03-30 21:46:39,497     INFO port =  25694
2023-03-30 21:46:39,497     INFO payload =  cmd/unix/reverse_netcat
2023-03-30 21:46:40,102     INFO execute exploit...
2023-03-30 21:47:30,150    DEBUG sessions_list = {'1': {'arch': 'cmd',
       'desc': 'Command shell',
       'exploit_uuid': 'ooidnves',
       'info': '',
       'routes': '',
       'session_host': '192.168.56.102',
       'session_port': 139,
       'target_host': '192.168.56.102',
       'tunnel_local': '192.168.56.107:25694',
       'tunnel_peer': '192.168.56.102:58913',
       'type': 'shell',
       'username': 'pani',
       'uuid': 'mtlrrji0',
       'via_exploit': 'exploit/multi/samba/usermap_script',
       'via_payload': 'payload/cmd/unix/reverse_netcat',
       'workspace': 'default'}}
2023-03-30 21:47:30,150     INFO exploit success...
2023-03-30 21:47:30,157     INFO execute action = get_dc_info
```

Εικόνα 4. 32: Επιτυχής εκμετάλλευση ευπάθειας από το αρχείο Mushikago.log

4.2 DeepExploit

4.2.1 Εγκατάσταση εργαλείου DeepExploit

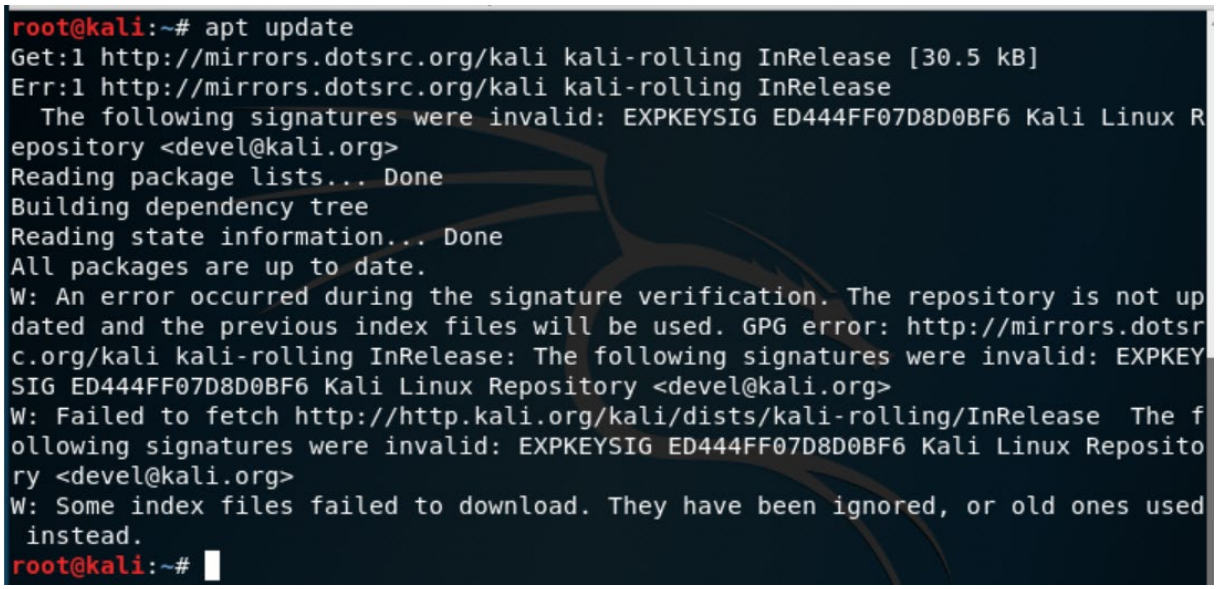
Το εργαλείο DeepExploit είναι ένα εργαλείο αυτοματοποίησης της διαδικασίας Penetration Testing το οποίο χρησιμοποιεί δεδομένα από προηγούμενες επιτυχημένες επιθέσεις ως εκπαιδευτικά δεδομένα. Η εγκατάσταση του εργαλείου DeepExploit [26] πραγματοποιήθηκε σε εικονική μηχανή Kali Linux 2019.2 όπως εισηγείται ο σχεδιαστής του.

Αρχικά γίνεται λήψη των απαραίτητων αρχείων του εργαλείου από την ιστοσελίδα [26] στο GitHub με τη χρήση της εντολής "git clone https://github.com/13o-bbr-bbq/machine_learning_security.git" όπως παρουσιάζεται στη εικόνα 4.33.

```
root@kali:~# git clone https://github.com/13o-bbr-bbq/machine_learning_security.git
Cloning into 'machine_learning_security'...
remote: Enumerating objects: 3623, done.
remote: Counting objects: 100% (80/80), done.
remote: Compressing objects: 100% (46/46), done.
remote: Total 3623 (delta 45), reused 57 (delta 30), pack-reused 3543
Receiving objects: 100% (3623/3623), 60.21 MiB | 9.64 MiB/s, done.
Resolving deltas: 100% (2252/2252), done.
root@kali:~#
```

Εικόνα 4. 33: Λήψη αρχείων του εργαλείου DeepExploit

Ακολούθως γίνεται ενημέρωση της λίστας των υφιστάμενων πακέτων χρησιμοποιώντας την εντολή “apt update”. Στο σημείο αυτό παρουσιάζεται σφάλμα στην εκτέλεση της ενημέρωσης (Εικόνα 4.34) για το λόγο ότι η έκδοση του λειτουργικού συστήματος Kali που χρησιμοποιήθηκε είναι απαρχαιωμένη. Η επίλυση του σφάλματος αυτού παρουσιάζεται στο παράρτημα Β1.

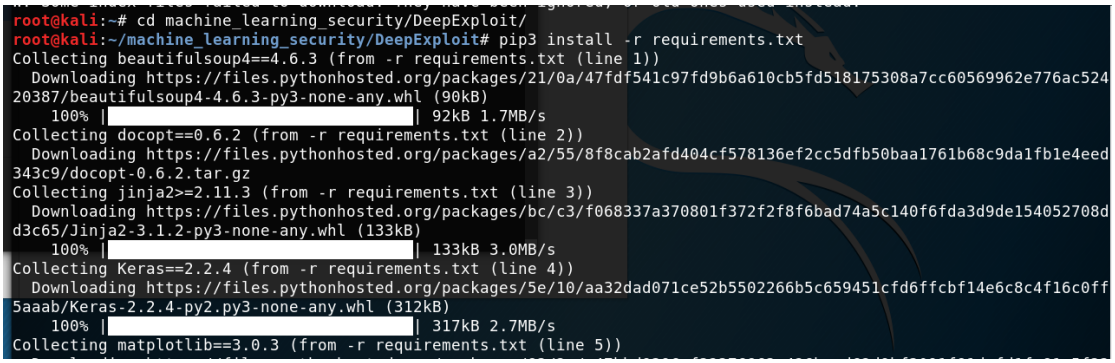


Εικόνα 4. 34: Σφάλμα εκτέλεσης ενημέρωσης της εντολής “apt update”

Στη συνέχεια σύμφωνα με τις οδηγίες που δόθηκαν από το σχεδιαστή του εργαλείου χρειάζεται να γίνει εγκατάσταση του πακέτου pip χρησιμοποιώντας την εντολή “apt-get install python3-pip”. Στην έκδοση του λειτουργικού συστήματος Kali Linux 2019.2 υπάρχει ήδη εγκατεστημένο τόσο το πακέτο python3 όσο και το πακέτο pip3. Η επαλήθευση για την ύπαρξη των εργαλείων αυτών μπορεί να γίνει με τις εντολές “python3 -V” και “pip3 -V" (Εικόνα 4.35) όπου θα παρουσιαστεί η έκδοση των πακέτων αυτών.

Εικόνα 4. 35: Επαλήθευση της έκδοσης των πακέτων python3 και pip3

Ακολούθως γίνεται μετάβαση στο φάκελο machine_learning_security/DeepExploit όπου θα πραγματοποιηθεί η εγκατάσταση των απαιτούμενων πακέτων της python χρησιμοποιώντας την εντολή " pip3 install -r requirements.txt" (Εικόνα 4.36).

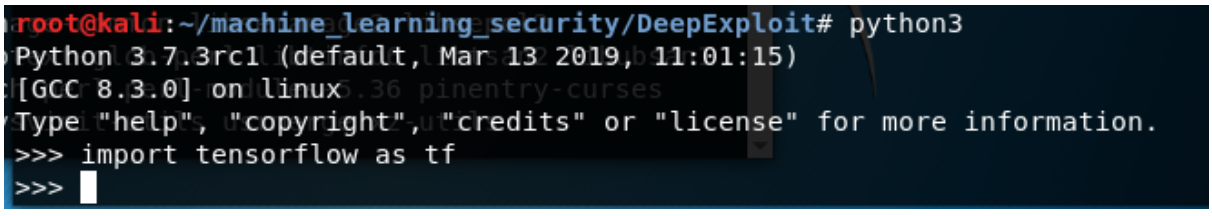


Εικόνα 4. 36: Εγκατάσταση των απαιτούμενων πακέτων της python

Κατά τη διάρκεια της εγκατάστασης παρουσιάστηκε σφάλμα με κάποια προ-απαιτούμενα πακέτα τα οποία χρειάζονται για τα εργαλεία που εγκαταστόνται. Η επίλυση του σφάλματος παρουσιάζεται στο παράρτημα Β2.

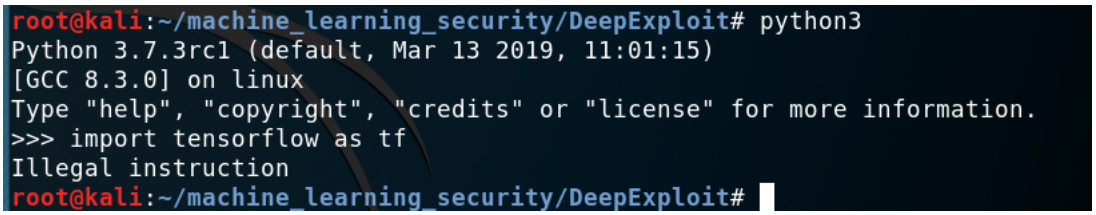
Αφού ολοκληρωθεί η εγκατάσταση των απαιτούμενων πακέτων γίνεται επαλήθευση της σωστής λειτουργίας των πακέτων και ειδικότερα της βιβλιοθήκης TensorFlow καθώς είναι ένα από τα σημαντικότερα πακέτα που χρησιμοποιεί το εργαλείο DeepExploit. Το TensorFlow είναι μια βιβλιοθήκη ανοικτού κώδικα που χρησιμοποιείται για machine learning και artificial intelligence καθώς δίνει ιδιαίτερη έμφαση στην εκπαίδευση των συστημάτων.

Η επαλήθευση της σωστής λειτουργίας της βιβλιοθήκης TensorFlow μπορεί να γίνει όταν εισάξουμε τη βιβλιοθήκη στη γλώσσα προγραμματισμού python3 χρησιμοποιώντας την εντολή "import TensorFlow as tf" όπως παρουσιάζεται στην εικόνα 4.37.



Εικόνα 4. 37: Εισαγωγή της βιβλιοθήκης TensorFlow στη γλώσσα προγραμματισμού python

Αν δεν παρουσιαστεί κάποιο σφάλμα όπως φαίνεται στην εικόνα 4.34 τότε η βιβλιοθήκη έχει εισαχθεί σωστά. Στη περίπτωση που παρουσιαστεί το σφάλμα "Illegal instruction" (Εικόνα 4.38) τότε το εργαλείο DeepExploit δεν μπορεί να εκτελεστεί (Εικόνα 4.39).



Εικόνα 4. 38: Σφάλμα "Illegal instruction" της βιβλιοθήκης TensorFlow

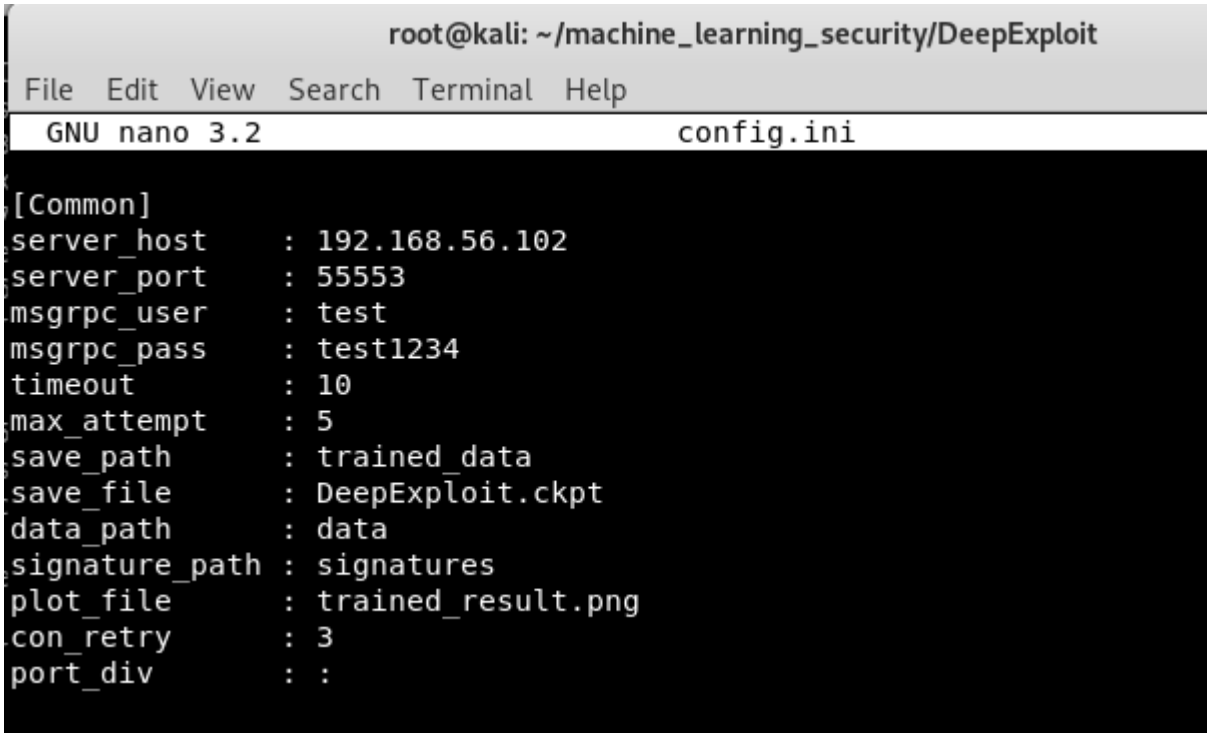
Εικόνα 4. 39: Σφάλμα "Illegal instruction" της βιβλιοθήκης TensorFlow

Το σφάλμα αυτό οφείλεται στη τεχνολογία των υπολογιστών, στην έκδοση της βιβλιοθήκης TensorFlow και στην έκδοση της γλώσσας προγραμματισμού python. Η βιβλιοθήκη TensorFlow μετά την έκδοση 1.5 χρησιμοποιεί την τεχνολογία Graphics Processing Unit (GPU) των υπολογιστών ενώ οι παλιότερες εκδόσεις του χρησιμοποιούσαν την τεχνολογία Central Processing Unit (CPU). Στον υπολογιστή που εκτελείται η τρέχουσα εγκατάσταση δεν υποστηρίζει την τεχνολογία GPU για τις εικονικές μηχανές. Συνεπώς θα πρέπει να εγκατασταθεί η έκδοση 1.5 της βιβλιοθήκης TensorFlow. Αυτό όμως επηρεάζει και τα υπόλοιπα πακέτα που έχουν εγκατασταθεί καθώς θα πρέπει να υποβαθμιστούν οι εκδόσεις τους οι οποίες όμως δεν είναι όλες συμβατές μεταξύ τους. Για την επίλυση του προβλήματος αυτού εκτελέστηκε η πιο πάνω εγκατάσταση των εργαλείων σε ένα άλλο υπολογιστή ο οποίος υποστηρίζει την τεχνολογία GPU για τις εικονικές μηχανές.

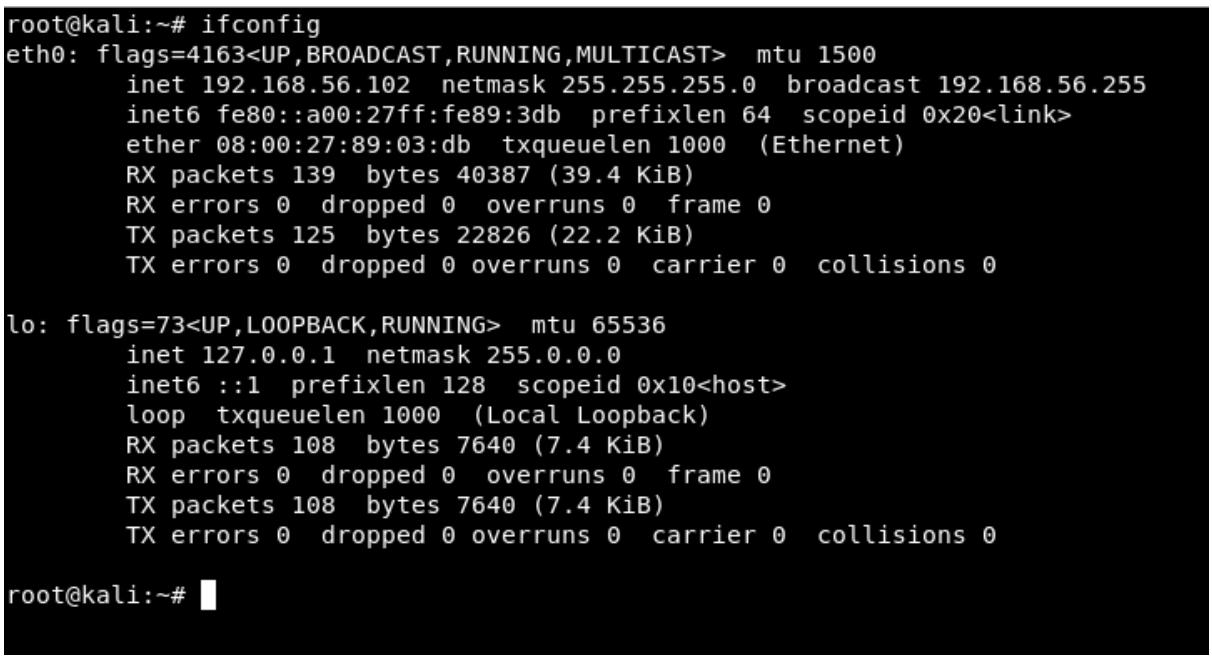
Ακολούθως εκτελείται επεξεργασία στο αρχείο "config.ini" χρησιμοποιώντας τον επεξεργαστή αρχείων "nano" (Εικόνα 4.40).

Εικόνα 4. 40: Χρήση του επεξεργαστή αρχείων nano για το αρχείο config.ini

Στο αρχείο αυτό γίνεται διόρθωση της διεύθυνσης IP στο πεδίο server_host (Εικόνα 4.41) έτσι ώστε να αναγράφεται η διεύθυνση IP 192.168.56.102 του λειτουργικού συστήματος Kali Linux όπως παρουσιάζεται στην εικόνα 4.42.



Εικόνα 4. 41: Επεξεργασία του πεδίου server_host στο αρχείο config.ini

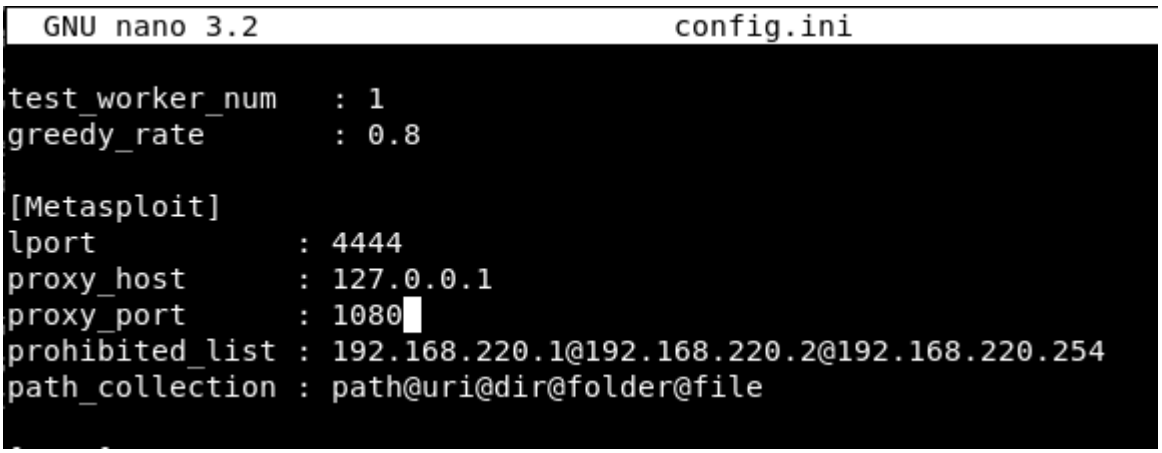


Εικόνα 4. 42: Διεύθυνση IP του λειτουργικού συστήματος Kali Linux

Στη συνέχεια εκτελείται επεξεργασία του αρχείου "/etc/proxychains.conf" χρησιμοποιώντας τον επεξεργαστή αρχείων "nano" (Εικόνα 4.43).

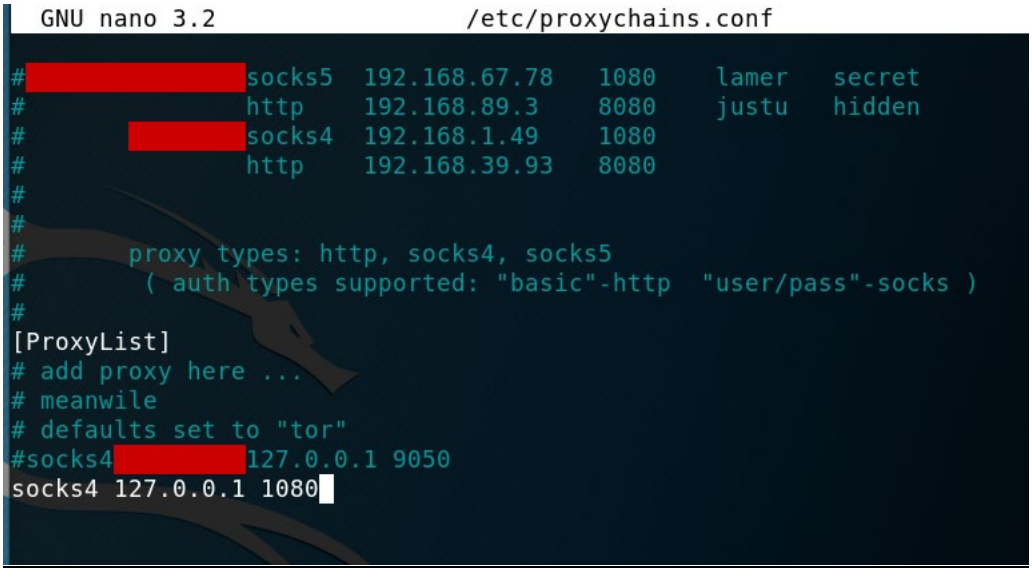
Εικόνα 4. 43: Χρήση του επεξεργαστή αρχείων nano για το αρχείο proxychains.conf

Στο αρχείο αυτό γίνεται προσθήκη στη περιοχή "ProxyList" οι πληροφορίες 127.0.0.1 και 1080 όπως αναγράφονται αντίστοιχα στα πεδία "proxy_host" και "proxy_port" στο αρχείο "config.ini" (Εικόνα 4.44). Οι πληροφορίες αυτές θα χρησιμοποιηθούν ως μεσολαβητής του εργαλείου DeepExploit.



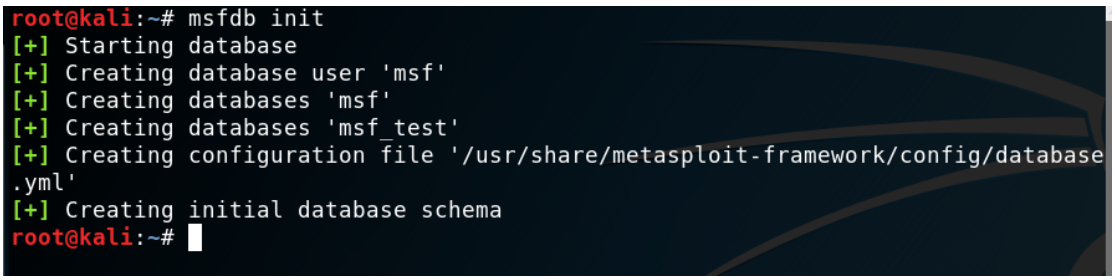
Εικόνα 4. 44: Πεδία "proxy_host" και "proxy_port" του αρχείου "config.ini"

Συνεπώς θα προστεθεί η διεύθυνσης IP και η θύρα χρησιμοποιώντας την εντολή "socks4 127.0.0.1 1080" στο αρχείο proxychains.conf όπως παρουσιάζεται στην εικόνα 4.45.



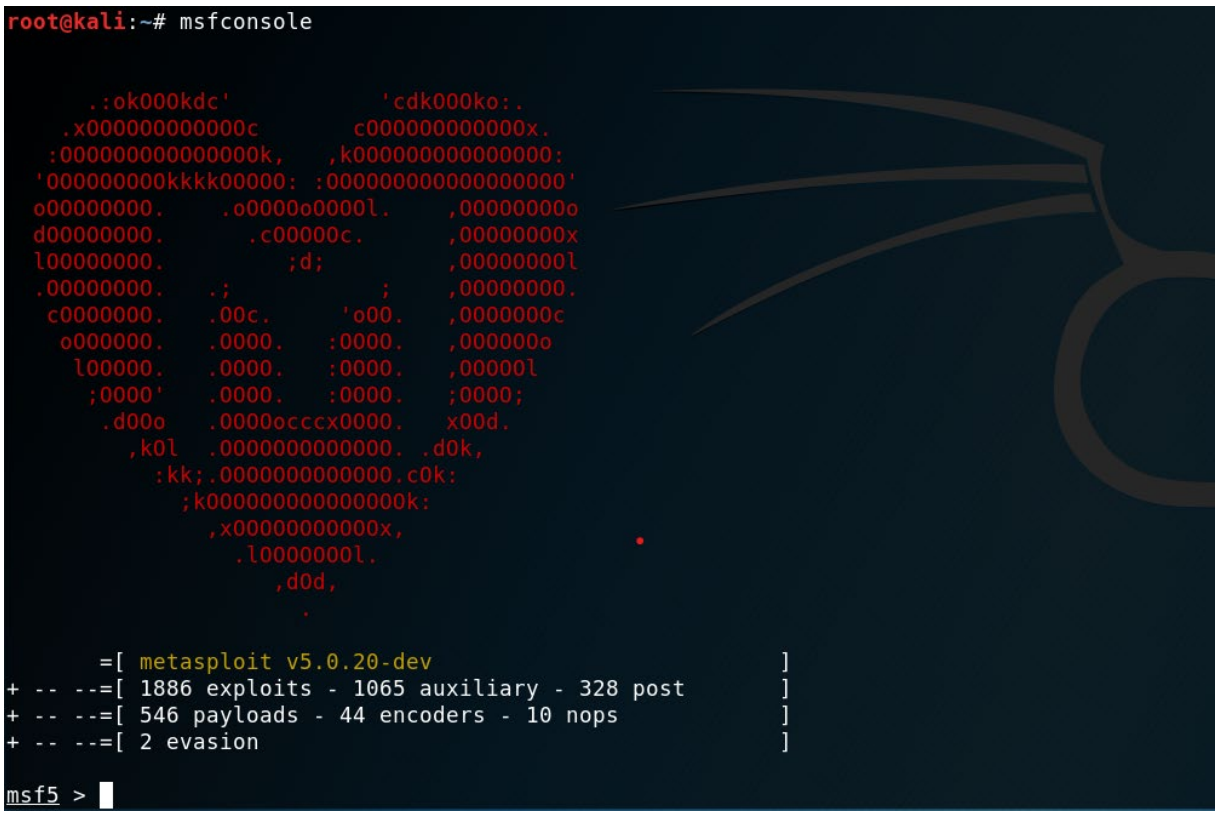
Εικόνα 4. 45: Επεξεργασία της λίστας proxy στο αρχείο proxychains.conf

Ακολούθως εκτελείται αρχικοποίηση της βάσης δεδομένων "postgreSQL" του εργαλείου Metasploit χρησιμοποιώντας την εντολή "msfdb init" όπως παρουσιάζεται στην εικόνα 4.46.



Εικόνα 4. 46: Αρχικοποίηση της βάσης δεδομένων του εργαλείου Metasploit

Αφού ολοκληρωθεί η αρχικοποίηση της βάσης δεδομένων εκτελείται εκκίνηση του εργαλείου Metasploit Framework με την εντολή "msfconsole" (Εικόνα 4.47).



Εικόνα 4. 47: Εκκίνηση του εργαλείου Metasploit-Framework

Έπειτα εκτελείται εκκίνηση του διακομιστή RPC του εργαλείου Metasploit χρησιμοποιώντας τις πληροφορίες που καθορίστηκαν στο αρχείο config.ini. Οι πληροφορίες αυτές όπως παρουσιάζονται στην εικόνα 4.48, είναι οι τιμές στα πεδία "server_host" όπου αντιπροσωπεύει τη διεύθυνση IP της μηχανής που είναι εγκατεστημένο το εργαλείο Metasploit, "server_port" όπου αντιπροσωπεύει τη θύρα η οποία θα χρησιμοποιηθεί από το εργαλείο Metasploit, "msgrpc_user"

το οποίο είναι ο χρήστης που θα χρησιμοποιηθεί για την αυθεντικοποίηση και "msgrpc_pass" είναι ο κωδικός ασφαλείας του χρήστη για την αυθεντικοποίηση.

```
root@kali:~/machine_learning_security/DeepExploit# cat config.ini
[Common]
server_host     : 192.168.56.109
server_port     : 55553
msgrpc_user     : test
msgrpc_pass     : test1234
timeout         : 10
max_attempt     : 5
```

Εικόνα 4. 48: Πληροφορίες από το αρχείο config.ini

Συνεπώς η εντολή με τις πληροφορίες όπως διαμορφώνεται και εκτελείται στο διακομιστή RPC είναι "load msgrpc ServerHost=192.168.56.102 ServerPort=55553 User=test Pass=test1234" (Εικόνα 4.49).

```
  .00000000.   .;           ;    ,00000000.
  c0000000.   .00c.      'o00.   ,0000000c
   o000000.   .0000.   :0000.   ,000000o
    l00000.   .0000.   :0000.   ,00000l
     ;0000'   .0000.   :0000.   ;0000;
      .d00o   .0000occcx0000.   x00d.
        ,k0l  .0000000000000. .d0k,
          :kk;.0000000000000.c0k:
            ;k000000000000000k:
              ,x0000000000x,
                .l00000000l.
                   ,d0d,
                     .

       =[ metasploit v5.0.20-dev                          ]
+ -- --=[ 1886 exploits - 1065 auxiliary - 328 post       ]
+ -- --=[ 546 payloads - 44 encoders - 10 nops            ]
+ -- --=[ 2 evasion                                       ]
msf5 > load msgrpc ServerHost=192.168.56.102 ServerPort=55553 User=test Pass=test1234
[*] MSGRPC Service:  192.168.56.102:55553
[*] MSGRPC Username: test
[*] MSGRPC Password: test1234
[*] Successfully loaded plugin: msgrpc
msf5 >
```

Εικόνα 4. 49: Εκκίνηση του διακομιστή RPC

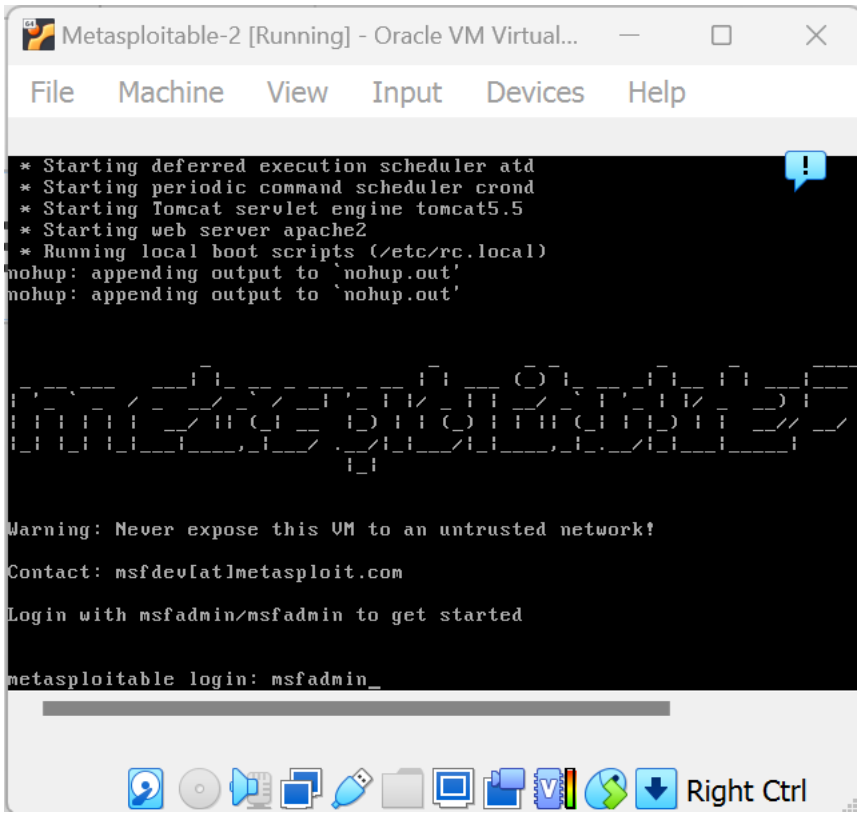
4.2.2 Λειτουργία εργαλείου DeepExploit

Για να γίνει εφικτή η λειτουργία του εργαλείου DeepExploit θα πρέπει να εκκινήσει πρώτα το εργαλείο Metasploit Framework και ο διακομιστής RPC όπως περιγράφηκε πιο πάνω. Συνεπώς αφού εκτελεστεί η εντολή " load msgrpc ServerHost=192.168.56.102 ServerPort=55553 User=test

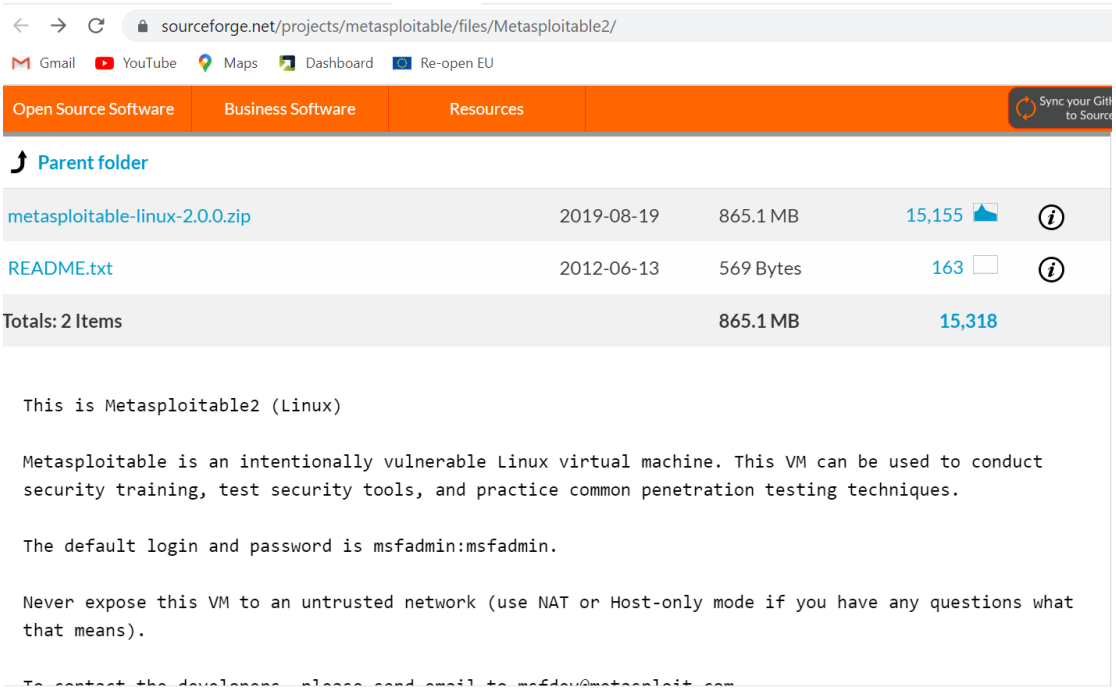
Pass=test1234" (Εικόνα 4.49) σε ένα άλλο παράθυρο γραμμής εντολών πραγματοποιείται η εκκίνηση του εργαλείου DeepExploit.

Αρχικά θα πρέπει να εκτελεστεί εκπαίδευση του αλγόριθμου του εργαλείου σε μια μηχανή η οποία είναι σκόπιμα ευάλωτη έτσι ώστε να μπορεί σε κατοπινό στάδιο να εντοπίσει τις ευπάθειες των άλλων μηχανών που θα καλεστεί να ερευνήσει.

Για το σκοπό αυτό εγκαταστάθηκε στο εικονικό περιβάλλον VirtualBox η ευάλωτη μηχανή Metasploitable2 (Εικόνα 4.50) η οποία λήφθηκε από την ιστοσελίδα https://sourceforge.net/projects/metasploitable/files/Metasploitable2/ (Εικόνα 4.51)

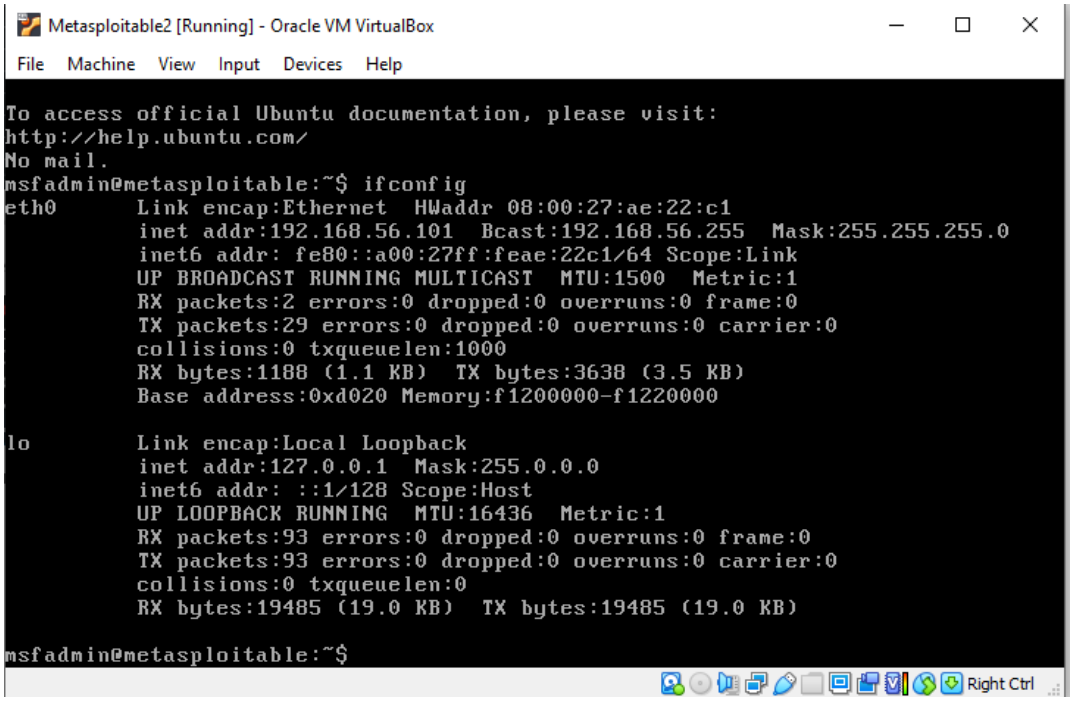


Εικόνα 4. 50: Εικονική μηχανή Metasploitable2



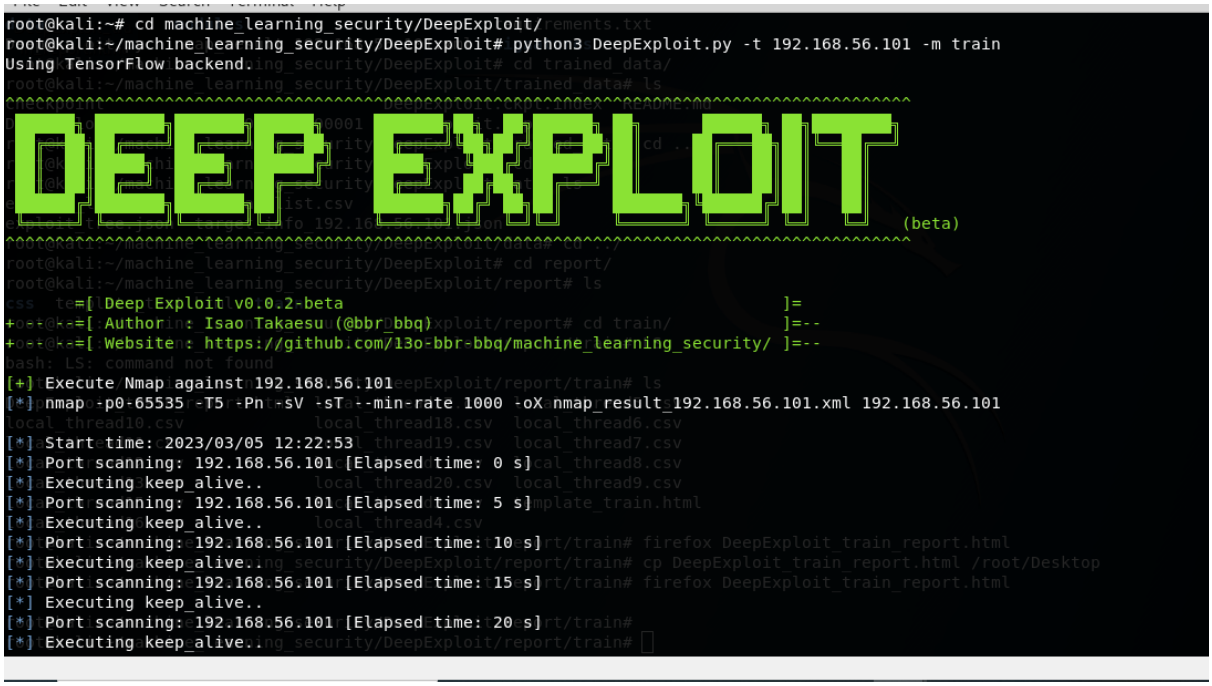
Εικόνα 4. 51: Λήψη της εικονικής μηχανής Metasploitable2

Αφού ολοκληρώθηκε η εγκατάσταση της εικονικής μηχανής Metasploitable2 ρυθμίστηκε να είναι στο ίδιο δίκτυο με την εικονική μηχανή Kali Linux που έχει εγκατεστημένο το εργαλείο DeepExploit. Αυτό μπορεί να επαληθευτεί από την διεύθυνση IP 192.168.56.101 της εικονικής μηχανής Metasploitable2 (Εικόνα 4.52).



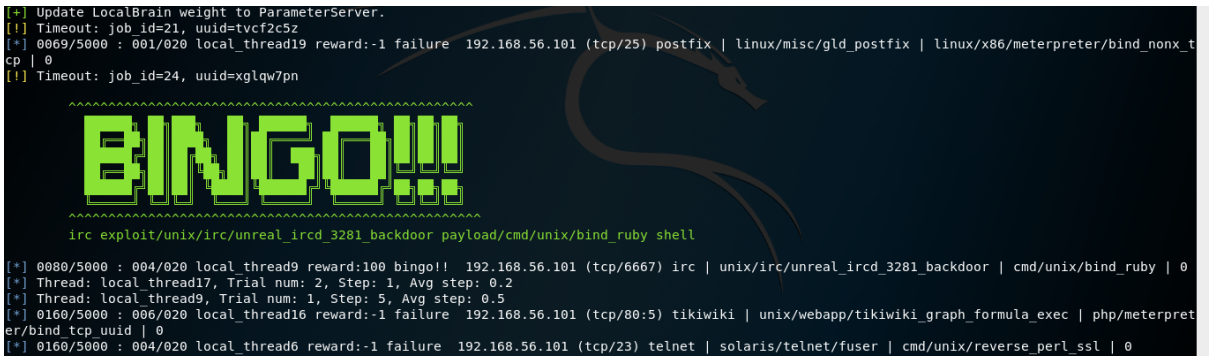
Εικόνα 4. 52: Διεύθυνση IP της εικονικής μηχανής Metasploitable2

Ακολούθως μπορεί να εκτελεστεί η εκπαίδευση του αλγόριθμου του εργαλείου DeepExploit χρησιμοποιώντας την εντολή “python3 DeepExploit.py -t 192.168.56.101 -m train” (Εικόνα 4.53)

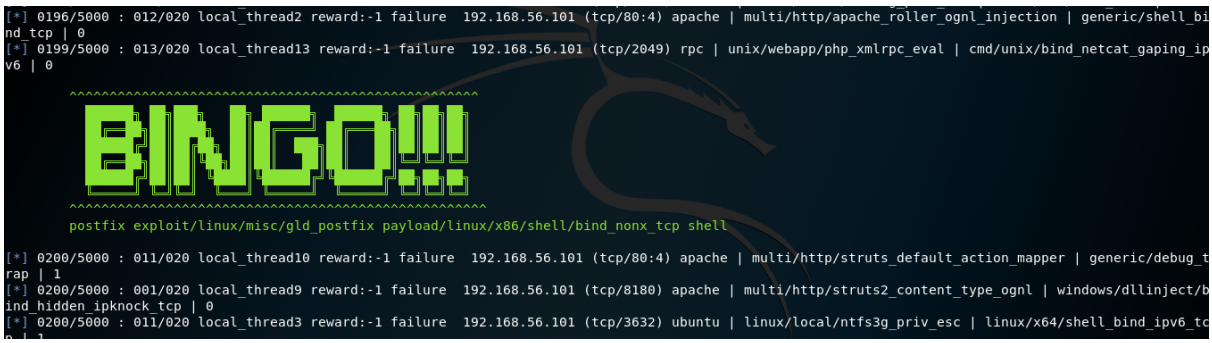


Εικόνα 4. 53: Εκκίνηση εκπαίδευσης του αλγόριθμου του εργαλείου DeepExploit

Κατά τη διάρκεια της εκπαίδευσης παρατηρείται σε αρκετές περιπτώσεις επιτυχής εκμετάλλευση των ευπαθειών που εντοπίστηκαν και υποδηλώνονται με τη λέξη “BINGO!!!” όπως παρουσιάζονται στις εικόνες 4.54-4.57.

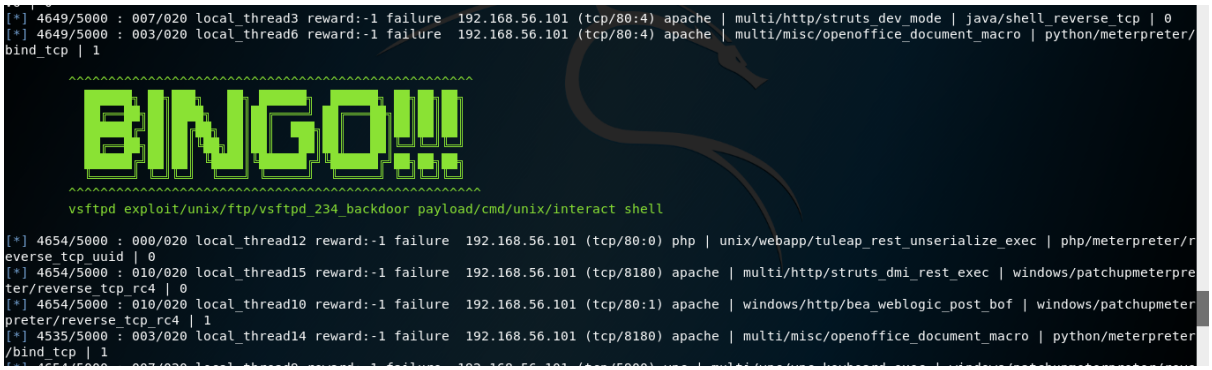


Εικόνα 4. 54: Εντοπισμός και εκμετάλλευση ευπάθειας



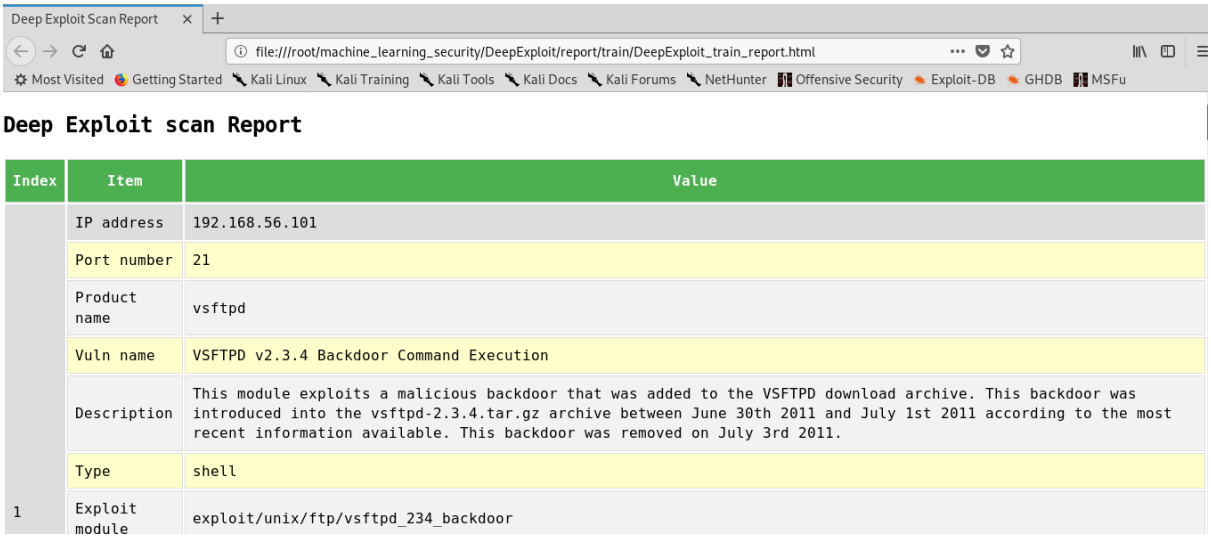
Εικόνα 4. 55: Εντοπισμός και εκμετάλλευση ευπάθειας

Εικόνα 4. 56: Εντοπισμός και εκμετάλλευση ευπάθειας



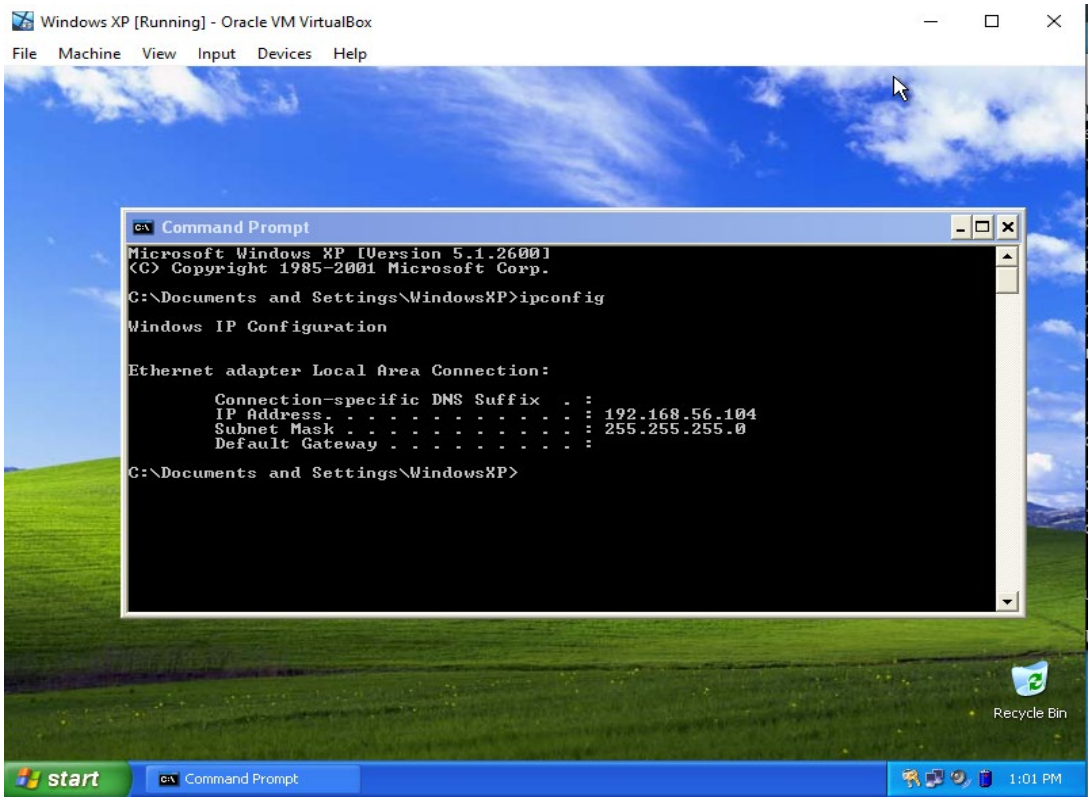
Εικόνα 4. 57: Εντοπισμός και εκμετάλλευση ευπάθειας

Τα αποτελέσματα των ευπαθειών που εντοπίστηκαν κατά την εκπαίδευση παρουσιάζονται στην αναφορά που εκδίδεται κατά το τέλος της διαδικασίας (Εικόνα 4.58)



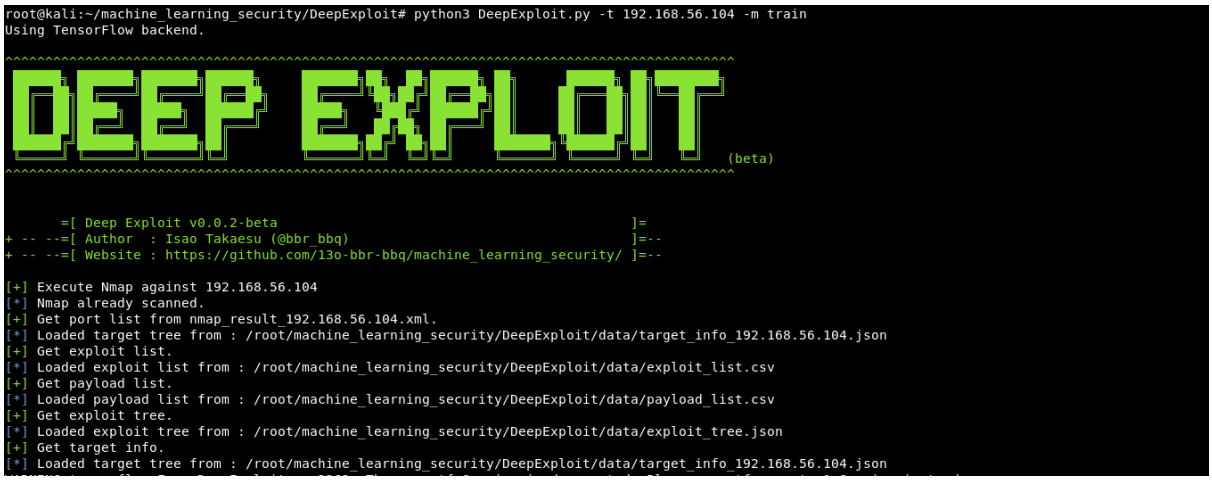
Εικόνα 4. 58: Αναφορά αποτελεσμάτων των ευπαθειών που εντοπίστηκαν.

Στη συνέχεια εγκαθίσταται μια ακόμα ευάλωτη μηχανή με λειτουργικό σύστημα Windows XP ώστε να εκτελεστεί περεταίρω εκπαίδευση του αλγορίθμου. Η εικονική μηχανή εγκαταστάθηκε και ρυθμίστηκε στο ίδιο δίκτυο με τις υπόλοιπες εικονικές μηχανές ώστε να έχει επικοινωνία με την εικονική μηχανή Kali Linux που έχει εγκατασταθεί το εργαλείο DeepExploit. Στην εικόνα 4.59 παρουσιάζεται η εικονική μηχανή Windows XP η οποία έχει διεύθυνση IP 192.168.56.104.



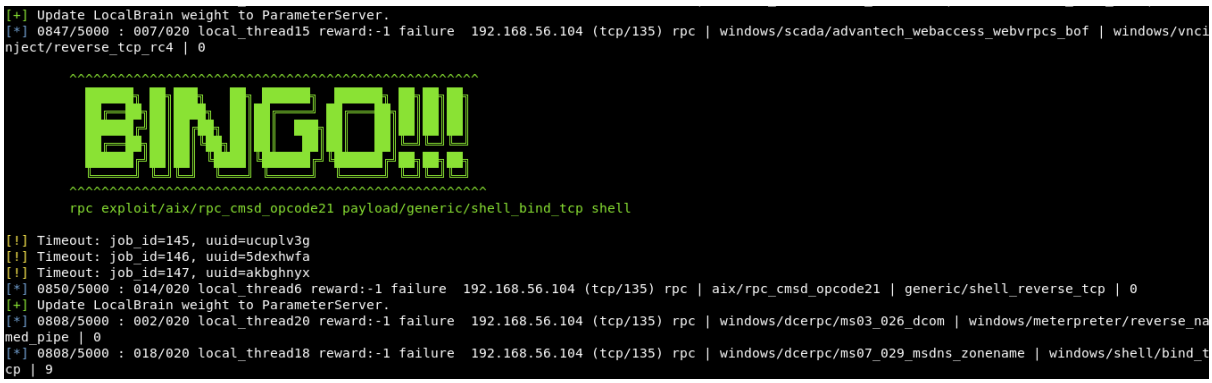
Εικόνα 4. 59: Εικονική μηχανή Windows XP

Η εκπαίδευση του αλγορίθμου του εργαλείου DeepExploit χρησιμοποιώντας την εικονική μηχανή Windows XP εκτελείται με την εντολή " python3 DeepExploit.py -t 192.168.56.104 -m train" όπως παρουσιάζεται στην εικόνα 4.60.

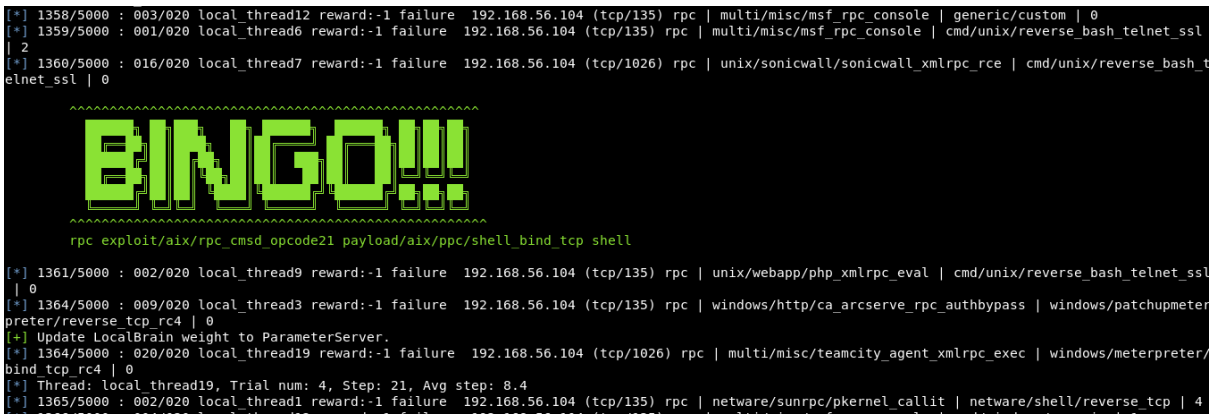


Εικόνα 4. 60: Εκκίνηση εκπαίδευσης του αλγορίθμου προς την ευάλωτη μηχανή Windows XP

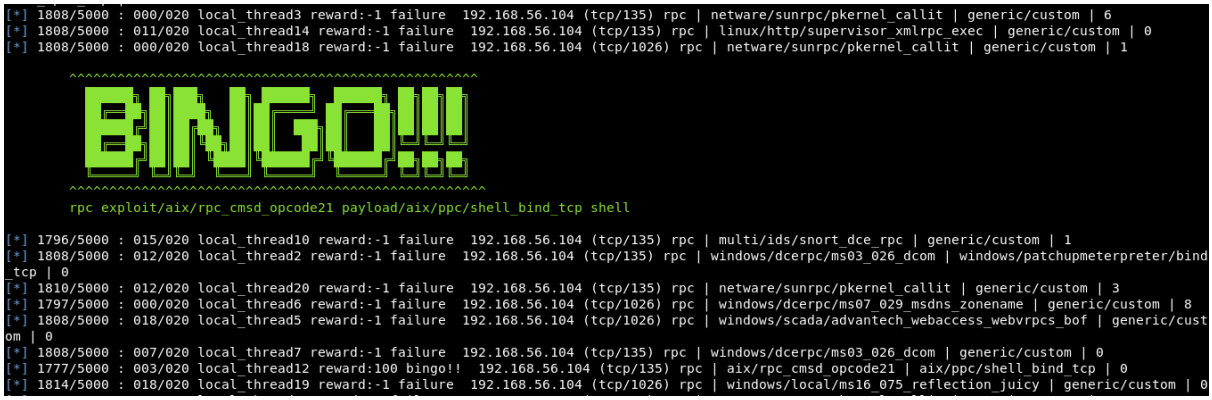
Ομοίως με την πρώτη εκπαίδευση που πραγματοποιήθηκε στη εικονική μηχανή Metasploitable2, εντοπίζονται οι ευπάθειες της μηχανής και παρουσιάζονται με την λέξη "BINGO!!!" Αποσπάσματα της εκπαίδευσης παρουσιάζονται στις εικόνες 4.61-4.64.



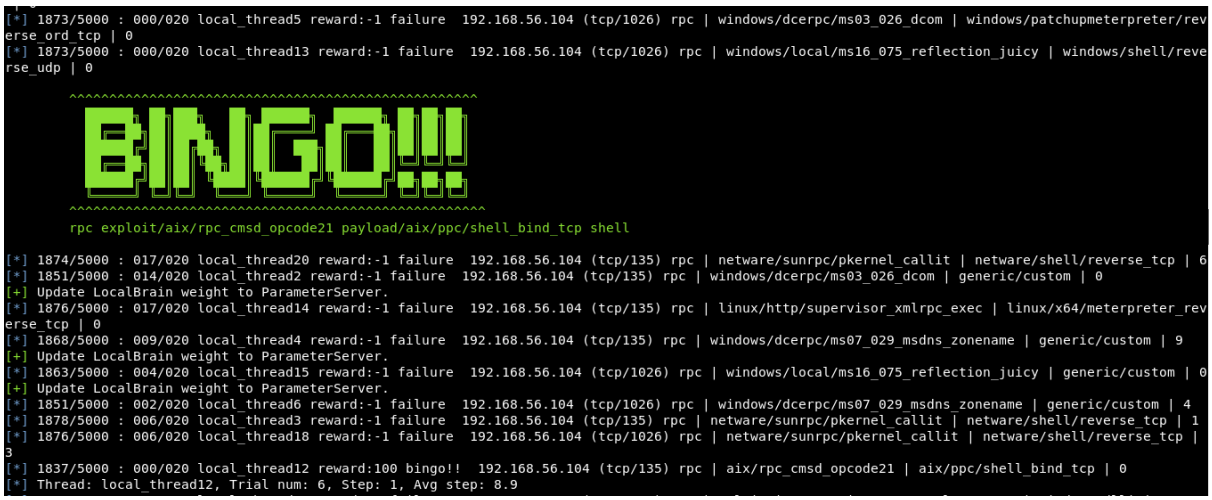
Εικόνα 4. 61: Εντοπισμός και εκμετάλλευση ευπάθειας



Εικόνα 4. 62: Εντοπισμός και εκμετάλλευση ευπάθειας



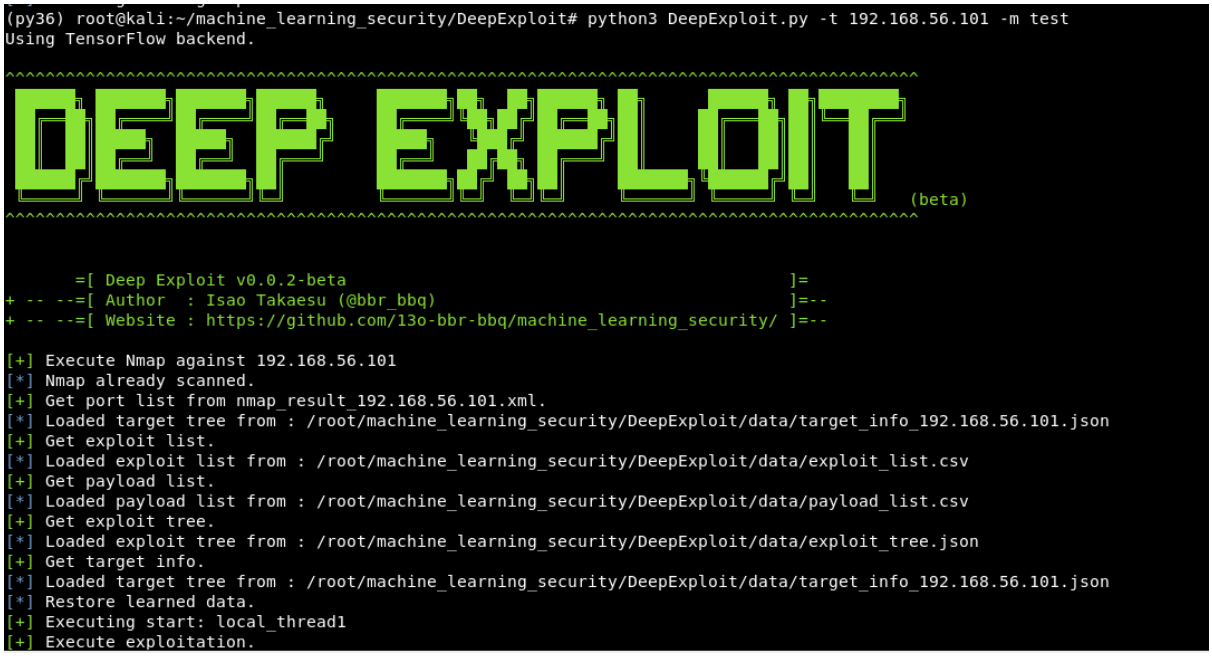
Εικόνα 4. 63: Εντοπισμός και εκμετάλλευση ευπάθειας



Εικόνα 4. 64: Εντοπισμός και εκμετάλλευση ευπάθειας

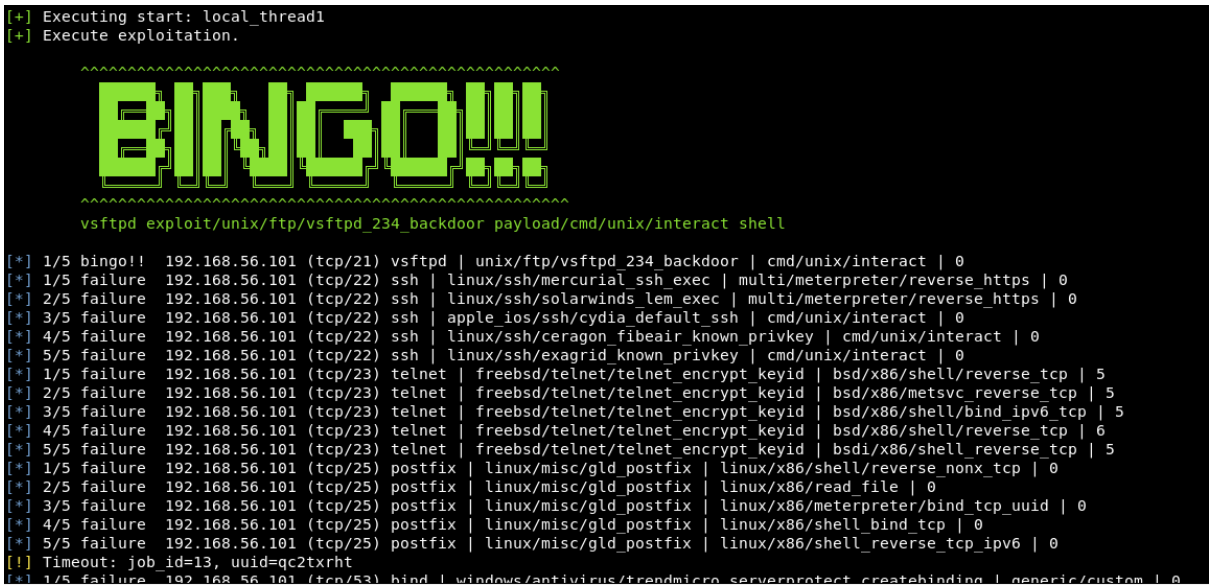
Αφού ολοκληρωθεί η εκπαίδευση του αλγορίθμου του εργαλείου DeepExploit στη συνέχεια μπορεί να εκτελεστεί ο έλεγχος Penetration Testing. Για την εκτέλεση του ελέγχου

χρησιμοποιήθηκε η εντολή “python3 DeepExploit.py -t 192.168.56.101 -m test” όπως παρουσιάζεται στην εικόνα 4.65.



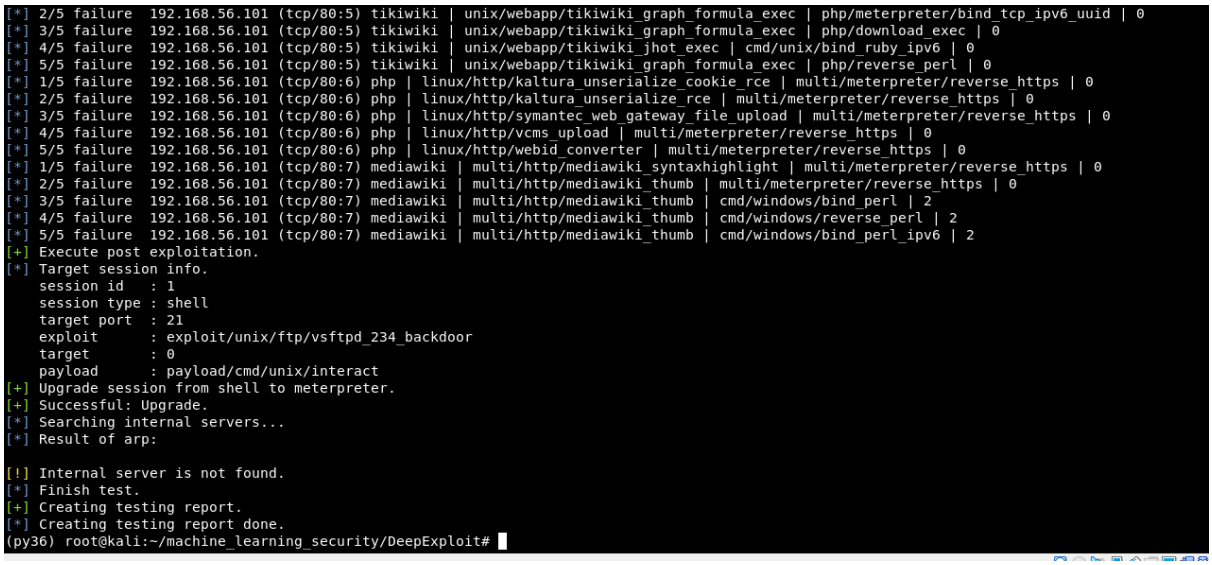
Εικόνα 4. 65: Εκτέλεση ελέγχου Penetration testing

Κατά τη διάρκεια του ελέγχου παρατηρείται ότι έχει εντοπιστεί ευπάθεια στο σύστημα η οποία μπορεί να χρησιμοποιηθεί για εκμετάλλευση του συστήματος στόχου (Εικόνα 4.66).



Εικόνα 4. 66: Εντοπισμός ευπάθειας κατά τον έλεγχο Penetration Testing

Το εργαλείο DeepExploit παρουσιάζει επίσης τις απαραίτητες πληροφορίες για την ευπάθεια που εντοπίστηκε και που μπορεί να αξιοποιηθεί καθώς επίσης και το κανάλι επικοινωνίας με το στόχο (Εικόνα 4.67).



Εικόνα 4. 67: Πληροφορίες της ευπάθειας που εντοπίστηκε κατά την εκτέλεση του ελέγχου

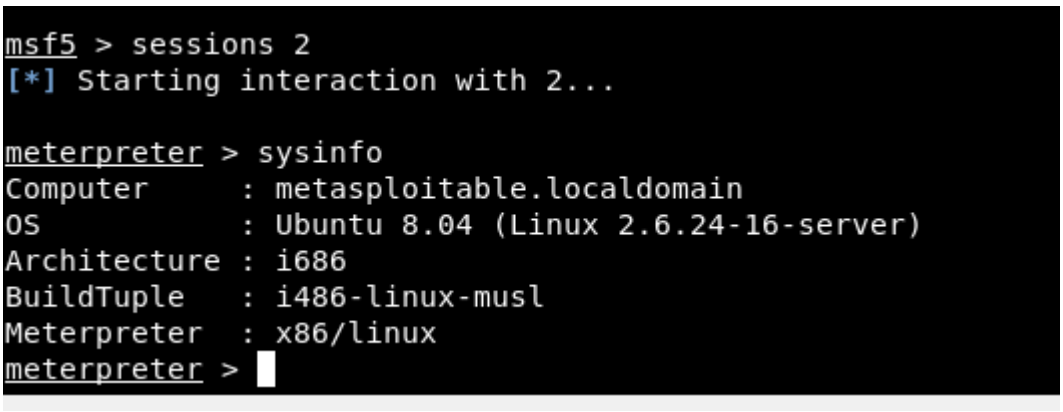
Παράλληλα στο εργαλείο Metasploit παρατηρείται ότι έχει ενεργοποιηθεί κανάλι επικοινωνίας (Shell session) σαν αποτέλεσμα της ευπάθειας που εντοπίστηκε και έχει επίσης αναβαθμιστεί σε κανάλι μετρητή (meterpreter session) όπως παρουσιάζεται στη εικόνα 4.68. Το meterpreter session παρέχει ένα διαδραστικό κέλυφος στον εισβολέα ώστε να μπορεί να εξερευνήσει τη μηχανή στόχο και να εκτελέσει τον κακόβουλο κώδικα του.

Εικόνα 4. 68: Ενεργοποίηση καναλιού επικοινωνίας και κανάλι μετρητή

Ακολούθως από το εργαλείο Metasploit επιλέγεται το κανάλι μετρητή με αριθμό 2 (Εικόνα 4.69) το οποίο θα επιτρέψει την πρόσβαση στη μηχανή στόχο.

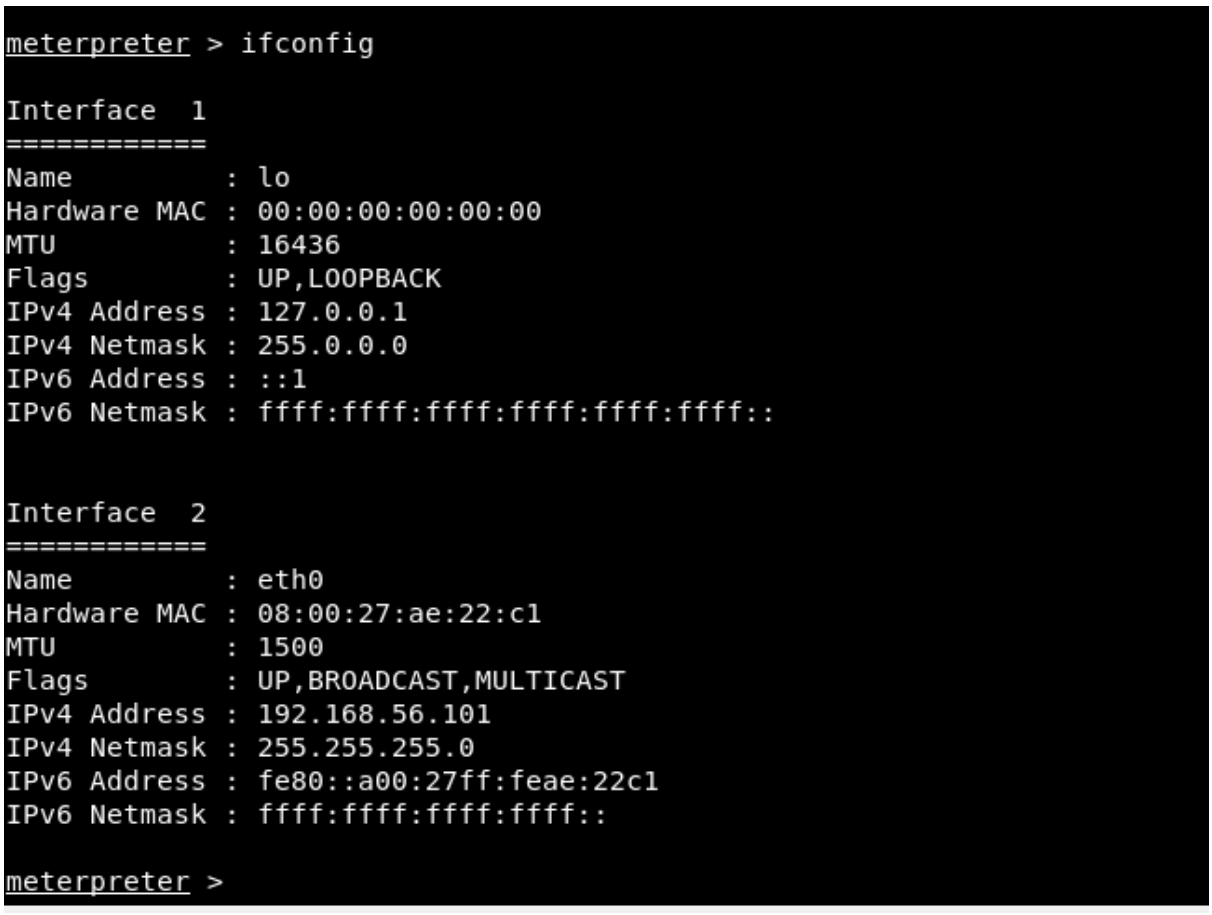
Εικόνα 4. 69: Επιλογή του καναλιού μετρητή 2

Στο σημείο αυτό μπορεί ο εισβολέας να εκτελέσει εντολές και κώδικα ομοίως με τον χειριστή της μηχανής αυτής. Για παράδειγμα με την εκτέλεση της εντολή “sysinfo” (Εικόνα 4.70) παρέχονται περισσότερες πληροφορίες για τη μηχανή αυτή.



Εικόνα 4. 70: Εκτέλεση εντολής “sysinfo”

Ένα ακόμα παράδειγμα είναι η εκτέλεση της εντολής “ifconfig” (Εικόνα 4.71) όπου παρουσιάζει και επιβεβαιώνει τα διαδικτυακά στοιχεία της μηχανής στόχου όπως είναι η διεύθυνση IP 192.168.56.101



Εικόνα 4. 71: Εκτέλεση της εντολής "ifconfig"

Στην εικόνα 4.72 παρουσιάζονται εντολές που έχουν εκτελεστεί στη μηχανή στόχου όπου πραγματοποιείται πλοήγηση στους φακέλους και τα αρχεία της μηχανής. Η επιβεβαίωση των διαδικτυακών στοιχείων καθώς και των φακέλων της μηχανής στόχου παρουσιάζεται στην εικόνα 4.73.

```
meterpreter > cd home
meterpreter > ls
Listing: /home
==============

Mode             Size  Type  Last modified              Name
----             ----  ----  -------------              ----
40755/rwxr-xr-x  4096  dir   2010-04-28 23:22:12 +0300  ftp
40755/rwxr-xr-x  4096  dir   2023-03-05 13:25:16 +0200  msfadmin
40755/rwxr-xr-x  4096  dir   2010-04-28 23:22:12 +0300  service
40755/rwxr-xr-x  4096  dir   2010-05-07 21:38:06 +0300  user

meterpreter > cd msfadmin
meterpreter > ls
Listing: /home/msfadmin
=======================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
20666/rw-rw-rw-   0     cha   2023-03-25 18:01:51 +0200  .bash_history
40755/rwxr-xr-x   4096  dir   2010-04-28 23:22:12 +0300  .distcc
40700/rwx------   4096  dir   2023-03-05 13:25:16 +0200  .gconf
40700/rwx------   4096  dir   2023-03-05 13:25:46 +0200  .gconfd
100600/rw-------  4174  fil   2012-05-14 09:01:49 +0300  .mysql_history
100644/rw-r--r--  586   fil   2010-04-28 23:22:27 +0300  .profile
100700/rwx------  4     fil   2012-05-20 21:24:45 +0300  .rhosts
40700/rwx------   4096  dir   2010-05-18 04:43:18 +0300  .ssh
100644/rw-r--r--  0     fil   2010-05-07 21:38:35 +0300  .sudo_as_admin_successful
40755/rwxr-xr-x   4096  dir   2010-04-28 23:22:27 +0300  vulnerable

meterpreter >
```

Εικόνα 4. 72: Πλοήγηση στους φακέλους της μηχανής στόχου

```
Metasploitable2 [Running] - Oracle VM VirtualBox
File  Machine  View  Input  Devices  Help
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:ae:22:c1
          inet addr:192.168.56.101  Bcast:192.168.56.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:feae:22c1/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:21072 errors:0 dropped:0 overruns:0 frame:0
          TX packets:15695 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:5606303 (5.3 MB)  TX bytes:2593844 (2.4 MB)
          Base address:0xd020 Memory:f1200000-f1220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:496 errors:0 dropped:0 overruns:0 frame:0
          TX packets:496 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:219849 (214.6 KB)  TX bytes:219849 (214.6 KB)

msfadmin@metasploitable:~$ pwd
/home/msfadmin
msfadmin@metasploitable:~$ ls
vulnerable
msfadmin@metasploitable:~$
```

Εικόνα 4. 73: Επιβεβαίωση στοιχείων από την μηχανής στόχου

Αφού ολοκληρωθεί ο έλεγχος Penetration Testing προς τη μηχανή στόχο, το εργαλείο DeepExploit δημιουργεί ένα αρχείο αναφοράς με τα αποτελέσματα του ελέγχου, παρέχοντας στοιχεία για την ευπάθεια που έχει εντοπιστεί. Το αρχείο αναφοράς αποθηκεύεται στο φάκελο report με την ονομασία DeepExploit_test_report.html και μπορεί να διαβαστεί χρησιμοποιώντας το πρόγραμμα περιήγησης Firefox (Εικόνα 4.74).

```
[!] Internal server is not found.
[*] Finish test.
[+] Creating testing report.
[*] Creating testing report done.
(py36) root@kali:~/machine_learning_security/DeepExploit# firefox report/DeepExploit_test_report.html
```

Εικόνα 4. 74: Αποθήκευση και άνοιγμα αρχείου αναφοράς DeepExploit_test_report.html

Στην εικόνα 4.75 παρουσιάζεται το περιεχόμενο του αρχείου αναφοράς με τα στοιχεία της ευπάθειας που εντοπίστηκε κατά τον έλεγχο Penetration Testing.

Εικόνα 4. 75: Αρχείο αναφοράς DeepExploit_test_report.html

Κεφάλαιο 5
Συμπεράσματα

Αφού ολοκληρώθηκε η εγκατάσταση και η λειτουργία των δυο εργαλείων στη συνέχεια της Μεταπτυχιακής διατριβής θα συγκριθούν τα εργαλεία αυτά ως προς τη λειτουργικότητα τους καθώς και ως προς την αποτελεσματικότητα τους.

5.1 Λειτουργικότητα

Αρχικά το εργαλείο DeepExploit λόγο του ότι αναπτύχθηκε το 2018 θεωρείται απαρχαιωμένο εφόσον η τεχνολογία αναπτύσσεται με ραγδαίους ρυθμούς, παρόλο που παρατηρούνται αναβαθμίσεις στο εργαλείο αυτό μέχρι και το 2021. Συνεπώς είναι δύσκολο στην εγκατάσταση του καθώς απαιτούνται συγκεκριμένες παλαιότερες εκδόσεις τόσο του λειτουργικού συστήματος όσο και των πακέτων που θα εγκατασταθούν όπως είναι για παράδειγμα η γλώσσα προγραμματισμού python και η βιβλιοθήκη TensorFlow. Επίσης χρειάζεται συμβατό υπολογιστικό σύστημα με τα εγκατεστημένα εργαλεία όπως για παράδειγμα με την βιβλιοθήκη TensorFlow ώστε να μπορούν να εκτελέσουν. Αντίθετα το εργαλείο Mushikago-femto αναπτύχθηκε το 2021 και εξακολουθεί να βελτιώνεται και να αναβαθμίζεται από τους σχεδιαστές του. Συνεπώς η εγκατάσταση του εργαλείου είναι εύκολη αφού τα απαιτούμενα πακέτα μπορούν να εγκατασταθούν σε καινούργιες εκδόσεις χωρίς να αντιμετωπίζονται ιδιαίτερα προβλήματα.

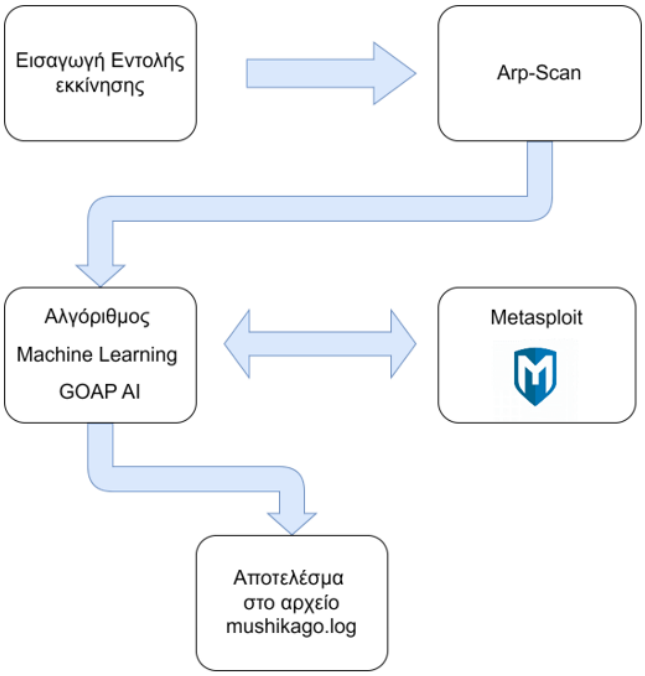
Παρόλα αυτά υπάρχουν κάποιες δυσκολίες στην εγκατάσταση. Λόγο των αναβαθμισμένων εκδόσεων του λειτουργικού συστήματος κάποια χαρακτηριστικά πρέπει να μετατραπούν ώστε να μπορεί να εκτελεστεί ο κώδικας του εργαλείου. Ένα παράδειγμα είναι η εμφάνιση των διεπαφών του δικτύου οι οποίες από "enp0s" θα πρέπει να μετατραπούν σε "eth".

Η εκτέλεση και των δυο εργαλείων γίνεται χρησιμοποιώντας περιβάλλον γραμμής εντολών (Command-line Interface CLI). Το εργαλείο DeepExploit μειονεκτεί έναντι του εργαλείου Mushikago-femto στο γεγονός ότι ο χρήστης του εργαλείου θα πρέπει να γνωρίζει και να καθορίσει την διεύθυνση IP του συστήματος στόχου κατά την έναρξη του ελέγχου. Αντίθετα το εργαλείο Mushikago-femto παρέχει μεν την επιλογή να καθοριστεί συγκεκριμένη διεύθυνση IP του συστήματος στόχου ώστε να εκτελέσει τον έλεγχο, αλλά μπορεί επίσης να σαρώσει το δίκτυο και να εντοπίσει τα συστήματα που υπάρχουν διαθέσιμα ώστε να εκτελέσει τον έλεγχο σε όλα τα συστήματα του δικτύου.

Αναφορικά με την εκπαίδευση των αλγορίθμων των εργαλείων, η μεθοδολογία που ακολουθείται από τα δυο εργαλεία είναι διαφορετική. Το εργαλείο DeepExploit πραγματοποιεί την εκπαίδευση του αλγορίθμου του χρησιμοποιώντας εικονικές μηχανές οι οποίες είναι εσκεμμένα ευάλωτες ώστε να βοηθήσουν στον αλγόριθμο του εργαλείου να εντοπίσει τις ευπάθειες και να εκπαιδευτεί στον εντοπισμό τους ούτως ώστε σε μελλοντικό στάδιο να είναι σε θέση να εντοπίσει και να παρέχει την ευκαιρία στους αναλυτές να εκμεταλλευτούν τις ευπάθειες αυτές. Αντίθετα το εργαλείο Mushikago-femto μειονεκτεί στο τομέα αυτό καθώς χρησιμοποιεί δεδομένα από την βάση δεδομένων του ώστε να μπορεί να εντοπίσει τις ευπάθειες των εικονικών μηχανών που καλείται να διερευνήσει. Συνεπώς θα πρέπει να επικαιροποιούνται συνεχώς τα δεδομένα των βάσεων αυτών ώστε να είναι σε θέση το εργαλείο να εντοπίζει και τις πιο καινούργιες ευπάθειες. Το εργαλείο DeepExploit χρησιμοποιεί τον αλγόριθμο A3C σε αντίθεση με το εργαλείο Mushikago-femto το οποίο χρησιμοποιεί την τεχνολογία του game AI και βασίζεται στη μέθοδο Goal-Oriented Action Planning (GOAP). Με βάση τη μέθοδο GOAP ο αλγόριθμος έχει συγκεκριμένο στόχο και δημιουργεί ένα σχέδιο δράσης για να επιτύχει το στόχο αυτό. Για παράδειγμα ο στόχος του αλγόριθμου στο εργαλείο Mushikago-femto είναι να εντοπίσει τις αδυναμίες του εικονικού συστήματος, συνεπώς επιλέγει τις ενέργειες που πρέπει να ακολουθήσει ώστε να επιτευχθεί ο στόχος αυτός. Οι σχεδιαστές του εργαλείου Mushikago-femto επισημαίνουν ότι σε μελλοντικό στάδιο θα προστεθούν και άλλοι αλγόριθμοι εκπαίδευσης.

Η ροή των ενεργειών που εκτελούνται από το εργαλείο Mushikago-femto παρουσιάζονται στην εικόνα 5.1. Αναλυτικά αφού γίνει εισαγωγή της κατάλληλης εντολής για εκκίνηση του εργαλείου

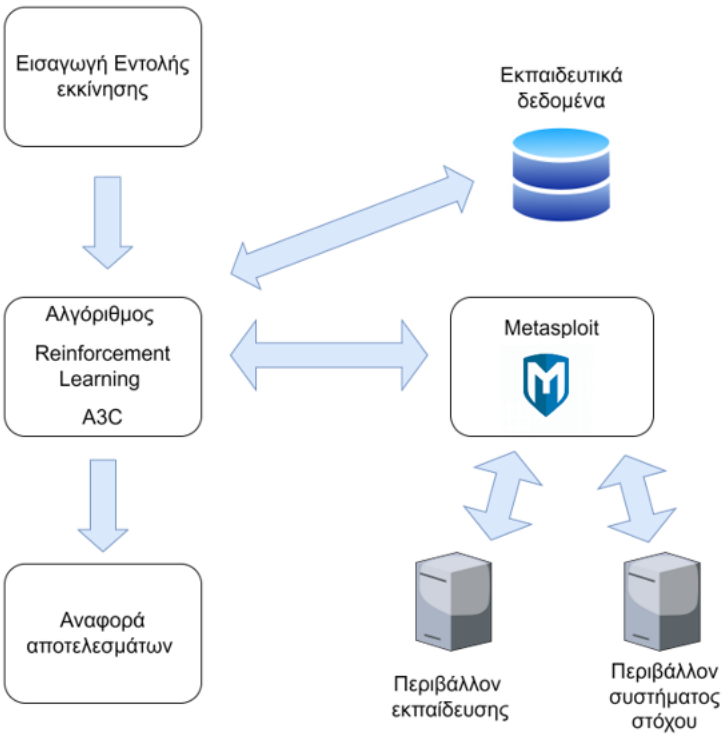
είτε με την διεύθυνση IP είτε χωρίς αυτή, εκτελείτε το εργαλείο Arp-scan όπου σαρώνει το δίκτυο για τον εντοπισμό της εικονικής μηχανής καθώς και τις ενεργείς υπηρεσίες και θύρες των εικονικών μηχανών που εντοπιστήκαν. Ακολούθως σύμφωνα με τα στοιχεία που εντοπίστηκαν εκτελείτε ο αλγόριθμος του Machine Learning σε συνδυασμό με το εργαλείο Metasploit-Framework ώστε να εντοπιστεί το κατάλληλο σχέδιο δράσης που θα επιτρέψει την εκμετάλλευση των ευπαθειών που εντοπίστηκαν. Τα αποτελέσματα της εκτέλεσης του εργαλείου αποθηκεύονται στο log αρχείο του εργαλείου ώστε να εξεταστούν περεταίρω από τους αναλυτές.



Εικόνα 5. 1 : Διάγραμμα ροής εργαλείου Mushikago-femto

Αντίστοιχα η ροή των ενεργειών που εκτελούνται από το εργαλείο DeepExploit παρουσιάζονται στην εικόνα 5.2. Αρχικά γίνεται η εισαγωγή της εντολής για την εκπαίδευση του αλγορίθμου όπου εντοπίζονται ενεργές υπηρεσίες και θύρες καθώς και ευπάθειες του συστήματος στόχου. Κατά την διάρκεια της εκπαίδευσης συλλέγονται εκπαιδευτικά δεδομένα και αποθηκεύονται ώστε να μπορούν να χρησιμοποιηθούν μελλοντικά κατά την διενέργεια της εξέτασης σε συστήματα στόχων. Αφού ολοκληρωθεί η εκπαίδευση το εργαλείο DeepExploit εκδίδει μια αναφορά με τα αποτελέσματα των ευπαθειών που έχει εντοπίσει κατά την εκπαίδευση του. Έπειτα εισάγεται η εντολή για την εκτέλεση της έρευνας σε συστήματα στόχου όπου επίσης θα εντοπιστούν ενεργές υπηρεσίες και θύρες καθώς και ευπάθειες του συστήματος στόχου ομοίως με την διαδικασία εκπαίδευσης. Κατά την διάρκεια της έρευνας το εργαλείο DeepExploit αλληλοεπιδρά με το

εργαλείο Metasploit-Framework ώστε να δημιουργηθούν τα ανάλογα κανάλια επικοινωνίας από τα οποία θα μπορεί να γίνει εκμετάλλευση των ευπαθειών που έχουν εντοπιστεί στο σύστημα στόχου. Ομοίως με την εκπαιδευτική διαδικασία, αφού ολοκληρωθεί η έρευνα το εργαλείο DeepExploit εκδίδει μια αναφορά με τα αποτελέσματα των ευπαθειών που έχουν εντοπιστεί στο σύστημα στόχου.



Εικόνα 5. 2: Διάγραμμα ροής εργαλείου DeepExploit

5.2 Αποτελεσματικότητα

Κατά την εκτέλεση των δυο εργαλείων παρατηρήθηκε ότι και τα δυο μπορούν να εντοπίσουν τις ευπάθειες του συστήματος στόχου. Το εργαλείο DeepExploit όμως προσφέρει πιο ολοκληρωμένη λύση από το εργαλείο Mushikago-femto αφού δίνει την ευκαιρία στους αναλυτές να εκμεταλλευτούν τις ευπάθειες του συστήματος αμέσως μετά την ολοκλήρωση του ελέγχου. Αυτό μπορεί να επιτευχθεί αφού χρησιμοποιεί το εργαλείο Metasploit σε πραγματικό χρόνο και δημιουργεί κανάλια επικοινωνίας (sessions) ώστε να επιτρέψει την άμεση εκμετάλλευση των ευπαθειών που έχουν εντοπιστεί. Αντίθετα το εργαλείο Mushikago-femto προσφέρει τον έλεγχο των ευπαθειών του συστήματος στόχου αλλά δεν εφαρμόζει ενέργειες εκμετάλλευσης τους. Ως

επί το πλείστων το εργαλείο Mushikago-femto μπορεί να χρησιμοποιηθεί σαν μέσο επαλήθευσης των ευπαθειών που μπορούν να εντοπιστούν στο σύστημα στόχου βοηθώντας τους αναλυτές να εντοπίσουν και να εκμεταλλευτούν τις ευπάθειες αυτές.

Επιπλέον μετά την ολοκλήρωση του ελέγχου το εργαλείο DeepExploit δημιουργεί μια αναφορά στην οποία καταγράφονται οι ευπάθειες που έχουν εντοπιστεί καθώς και σχετικές πληροφορίες για αυτές. Αντίθετα το εργαλείο Mushikago-femto δεν δημιουργεί αναφορά αλλά αποθηκεύει τις πληροφορίες του ελέγχου που πραγματοποιήθηκε σε ένα log αρχείο. Στο τομέα αυτό μειονεκτεί το εργαλείο Mushikago-femto καθώς η έκδοσης αναφοράς είναι ένα σημαντικό στοιχείο με την ολοκλήρωση του ελέγχου ώστε να παρουσιάζονται ξεκάθαρα τα αποτελέσματα και να μπορούν οι αναλυτές να αξιοποιήσουν τις πληροφορίες αυτές για να εκμεταλλευτούν το σύστημα στόχο.

Οι κύριες διαφορές των εργαλείων DeepExploit και Mushikago-femto παρουσιάζονται συνοπτικά στο Πίνακα 5.1.

Περιγραφή	DeepExploit	Mushikago-femto
Εγκατάσταση	Δύσκολο (χρειάζεται συγκεκριμένες εκδόσεις πακέτων)	Εύκολο (δεν χρειάζεται συγκεκριμένες εκδόσεις πακέτων)
Εντοπισμός ευπαθειών	✓	✓
Εκμετάλλευση ευπαθειών	✓	X
Έκδοση αναφοράς ευπαθειών που εντοπίστηκαν	✓	X (αποτελέσματα στο log αρχείο)
Εύκολο στη χρήση	✓	✓
Χρήση αλγορίθμων	Αλγόριθμος A3C	Τεχνολογία game AI

Πίνακας 5. 1: Σύγκριση εργαλείων DeepExploit και Mushikago-femto

Εν κατακλείδι το εργαλείο DeepExploit κρίνεται ως πιο αποτελεσματικό για αξιοποίηση από τους αναλυτές Red Team αφού ελέγχει το σύστημα στόχου, εντοπίζει τις ευπάθειες του και επιτρέπει την άμεση εκμετάλλευση τους από τους αναλυτές δημιουργώντας sessions στο εργαλείο Metasploit παράλληλα με την εκτέλεση του έλεγχο. Επιπλέον είναι εύκολο στη χρήση χωρίς να απαιτείται παρέμβαση από τους αναλυτές καθόλη τη διάρκεια της διαδικασίας, μέχρι την ολοκλήρωση του ελέγχου και την έκδοση της αναφοράς.

Κεφάλαιο 6
Επίλογος

Συνοψίζοντας, στη παρούσα μεταπτυχιακή διατριβή έγινε μια εκτεταμένη έρευνα αναφορικά με τις ομάδες Red Team, τη μεθοδολογία τους καθώς και τη διαδικασία ανάλυσης Penetration Testing. Επίσης έγινε διεξοδική μελέτη σχετικά με τους τύπους του Machine Learning εστιάζοντας στη μέθοδο Reinforcement Learning η οποία είναι η πιο κατάλληλη μέθοδος για την δημιουργία εργαλείων εκτέλεσης της διαδικασίας Penetration Testing.

Ακολούθως, διεξάχθηκε εκτεταμένη μελέτη της υπάρχουσας βιβλιογραφίας αναφορικά με τα υφιστάμενα εργαλεία Machine Learning αυτοματοποίησης της διαδικασίας Penetration Testing. Για την υλοποίηση της μεταπτυχιακής διατριβής, από τα εργαλεία που εντοπίστηκαν επιλέχτηκαν να αξιολογηθούν τα εργαλεία DeepExploit και Mushikago-femto, τα οποία είναι εργαλεία ανοικτού κώδικα και είναι διαθέσιμα στο διαδίκτυο. Τα εργαλεία αυτά εγκαταστάθηκαν και αξιολογήθηκαν για την λειτουργικότητα και την αποτελεσματικότητα τους στον εντοπισμό ευπαθειών των πληροφοριακών συστημάτων στόχου. Το εργαλείο DeepExploit υπερτερεί έναντι του εργαλείου Mushikago-femto στο γεγονός ότι αφού ολοκληρωθεί η έρευνα του εργαλείου DeepExploit δίνεται αμέσως η δυνατότητα στους αναλυτές να προβούν σε εκμετάλλευση των ευπαθειών που έχουν εντοπιστεί, μέσω του εργαλείου Metasploit το οποίο δημιουργεί κανάλια επικοινωνίας με το σύστημα στόχου. Αντίθετα το εργαλείο Mushikago-femto μπορεί να χρησιμοποιηθεί σαν μέσο

επαλήθευσης των ευπαθειών που μπορούν να εντοπιστούν στο σύστημα στόχου από τους αναλυτές.

Ένας από τους στόχους της παρούσας μεταπτυχιακής διατριβής ήταν να προσομοιάσει διάφορα σενάρια επιθέσεων στο περιβάλλον Cyber Range του πανεπιστήμιου ώστε να μπορούν τα άτομα των ομάδων Red Team να εξοικειωθούν και να εκπαιδευτούν στην χρήση των εργαλείων Machine Learning. Ωστόσο λόγο της κυβερνοεπίθεσης που δέχτηκε το Ανοικτό Πανεπιστήμιο Κύπρο αυτό δεν κατέστη δυνατό. Συνεπώς η εκτέλεση εικονικής επίθεσης έγινε με την χρήση εικονικών μηχανών σε περιορισμένη εμβέλεια για σκοπούς αξιολόγησης των εργαλείων. Παρόλα αυτά ακόμα και με την χρήση εικονικών μηχανών τα εργαλεία αυτά δίνουν την δυνατότητα στα άτομα των ομάδων Red Team να τα χρησιμοποιήσουν, να εξοικειωθούν και να εκπαιδευτούν με αυτά σε περιορισμένη εμβέλεια από άποψη σεναρίων επίθεσης.

6.1 Μελλοντικά Σχέδια

Όπως έχει προαναφερθεί, λόγο της κυβερνοεπίθεσης που δέχτηκε το Ανοικτό Πανεπιστήμιο Κύπρου δεν κατέστη εφικτό να διεξαχθούν σενάρια επιθέσεων στο περιβάλλον του Cyber Range του πανεπιστήμιου. Συνεπώς μελλοντικά θα μπορούσαν να σχεδιαστούν ρεαλιστικά σενάρια επιθέσεων στο περιβάλλον Cyber Range έτσι ώστε να μπορούν οι επαγγελματίες της κυβερνοασφάλειας να εξοικειώνονται με τα προαναφερθέντα εργαλεία του Machine Learning, τη χρησιμότητα τους και την ευελιξία που προσφέρουν στον εντοπισμό και την εκμετάλλευση των ευπαθειών των πληροφοριακών συστημάτων. Επιπλέον δίνεται η ευκαιρία στους επαγγελματίες της κυβερνοασφάλειας να εκπαιδεύονται σε νέες πτυχές της ραγδαία αναπτυσσόμενης τεχνολογίας και να εμπλουτίζουν τόσο τις γνώσεις τους όσο και τις δεξιότητες τους, αναφορικά με τις δυνατότητες που προσφέρει η τεχνολογία σε επίπεδο νέων μεθόδων επιθέσεων από κυβερνοεγκληματίες. Επιπλέον με τις γνώσεις που θα αποκομίσουν θα μπορούν να προσφέρουν την υποστήριξη που χρειάζεται για την όσο είναι δυνατό πιο βελτιωμένη προστασία των πληροφοριακών συστημάτων.

Βιβλιογραφία

[1] I. Rosenberg, A. Shabtai, Y. Elovici, and L. Rokach, “Adversarial Machine Learning Attacks and Defense Methods in the Cyber Security Domain,” *ACM Comput. Surv.*, vol. 54, no. 5, p. 108:1-108:36, May 2021, doi: 10.1145/3453158.

[2] S. Kraemer, P. Carayon, and R. Duggan, “Red Team Performance for Improved Computer Security,” *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, vol. 48, no. 14, pp. 1605–1609, Sep. 2004, doi: 10.1177/154193120404801410.

[3] K. Shaukat, S. Luo, V. Varadharajan, I. A. Hameed, and M. Xu, “A Survey on Machine Learning Techniques for Cyber Security in the Last Decade,” *IEEE Access*, vol. 8, pp. 222310–222354, 2020, doi: 10.1109/ACCESS.2020.3041951.

[4] M. M. Yamin, B. Katt, and V. Gkioulos, “Cyber ranges and security testbeds: Scenarios, functions, tools and architecture,” *Computers & Security*, vol. 88, p. 101636, Jan. 2020, doi: 10.1016/j.cose.2019.101636.

[5] H. Sharma and H. Singh, *Hands-on Red Team Tactics: A Practical Guide to Mastering Red Team Operations*. Packt Publishing Ltd, 2018.

[6] I. Yaqoob, S. Hussain, S. Mamoon, N. Naseer, J. Akram, and A. Rehman, “Penetration Testing and Vulnerability Assessment,” Aug. 2017.

[7] F. Salahdine and N. Kaabouch, “Social Engineering Attacks: A Survey,” *Future Internet*, vol. 11, no. 4, Art. no. 4, Apr. 2019, doi: 10.3390/fi11040089.

[8] Z. Wang, H. Zhu, and L. Sun, “Social Engineering in Cybersecurity: Effect Mechanisms, Human Vulnerabilities and Attack Methods,” *IEEE Access*, vol. 9, pp. 11895–11910, 2021, doi: 10.1109/ACCESS.2021.3051633.

[9] A. M. Aroyo, F. Rea, G. Sandini, and A. Sciutti, “Trust and Social Engineering in Human Robot Interaction: Will a Robot Make You Disclose Sensitive Information, Conform to Its Recommendations or Gamble?,” *IEEE Robotics and Automation Letters*, vol. 3, no. 4, pp. 3701–3708, Oct. 2018, doi: 10.1109/LRA.2018.2856272.

[10] S. V. Kumar, “Ethical Hacking and Penetration Testing Strategies,” *International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)*, vol. 11, no. 2, 2014.

[11] M. Ghanem and T. Chen, “Reinforcement Learning for Efficient Network Penetration Testing,” *Information*, vol. 11, p. 6, Dec. 2019, doi: 10.3390/info11010006.

[12] S. Halder and S. Ozdemir, *Hands on Machine Learning for Cybersecurity*. Packt Publishing Ltd, 2018.

[13] J. Singh and J. Singh, “Assessment of supervised machine learning algorithms using dynamic API calls for malware detection,” *International Journal of Computers and Applications*, vol. 44, no. 3, pp. 270–277, Mar. 2022, doi: 10.1080/1206212X.2020.1732641.

[14] R. Maeda and M. Mimura, “Automating post-exploitation with deep reinforcement learning,” *Computers & Security*, vol. 100, p. 102108, Jan. 2021, doi: 10.1016/j.cose.2020.102108.

[15] R. S. Sutton and A. G. Barto, *Reinforcement Learning: An Introduction*. MIT Press: Cambridge, MA, USA, 2018.

[16] R. Tolosana, R. Vera-Rodriguez, J. Fierrez, A. Morales, and J. Ortega-Garcia, “Deepfakes and beyond: A Survey of face manipulation and fake detection,” *Information Fusion*, vol. 64, pp. 131–148, Dec. 2020, doi: 10.1016/j.inffus.2020.06.014.

[17] Z. Fang, J. Wang, B. Li, S. Wu, Y. Zhou, and H. Huang, “Evading Anti-Malware Engines With Deep Reinforcement Learning,” *IEEE Access*, vol. 7, pp. 48867–48879, 2019, doi: 10.1109/ACCESS.2019.2908033.

[18] N. Khurana, S. Mittal, A. Piplai, and A. Joshi, “Preventing Poisoning Attacks On AI Based Threat Intelligence Systems,” in *2019 IEEE 29th International Workshop on Machine Learning for Signal Processing (MLSP)*, Oct. 2019, pp. 1–6. doi: 10.1109/MLSP.2019.8918803.

[19] C. Wang, J. Chen, Y. Yang, X. Ma, and J. Liu, “Poisoning attacks and countermeasures in intelligent networks: Status quo and prospects,” *Digital Communications and Networks*, vol. 8, no. 2, pp. 225–234, Apr. 2022, doi: 10.1016/j.dcan.2021.07.009.

[20] E. Walraven and M. T. J. Spaan, “Point-Based Value Iteration for Finite-Horizon POMDPs,” *Journal of Artificial Intelligence Research*, vol. 65, pp. 307–341, Jul. 2019, doi: 10.1613/jair.1.11324.

[21] S. Zhou, J. Liu, D. Hou, X. Zhong, and Y. Zhang, “Autonomous Penetration Testing Based on Improved Deep Q-Network,” *Applied Sciences*, vol. 11, no. 19, Art. no. 19, Jan. 2021, doi: 10.3390/app11198823.

[22] K. Tran *et al.*, “Deep hierarchical reinforcement agents for automated penetration testing.” arXiv, Sep. 14, 2021. doi: 10.48550/arXiv.2109.06449.

[23] T. Isao, “Metasploit Meets Machine Learning.” https://www.mbsd.jp/blog/20180228.html (accessed Jan. 15, 2023).

[24] Z. Hu, R. Beuran, and Y. Tan, “Automated Penetration Testing Using Deep Reinforcement Learning,” in *2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, Sep. 2020, pp. 2–10. doi: 10.1109/EuroSPW51379.2020.00010.

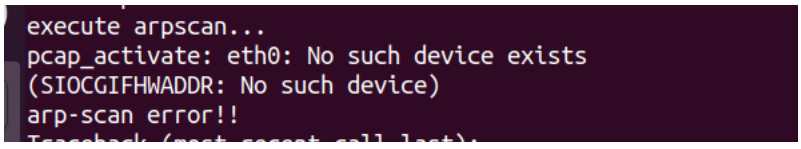
[25] PowderKegTech, “PowderKegTech/mushikago-femto.” Accessed: Dec. 17, 2022. [Online]. Available: https://github.com/PowderKegTech/mushikago-femto

[26] “machine_learning_security/DeepExploit at master · 13o-bbr-bbq/machine_learning_security.” Accessed: Dec. 17, 2022. [Online]. Available: https://github.com/13o-bbr-bbq/machine_learning_security

Παράρτημα Α
Σφάλματα κατά την εκτέλεση του εργαλείου Mushikago-femto

Α.1 Διαμόρφωση ονοματολογίας διεπαφών

Στις καινούργιες εκδόσεις Ubuntu η ονοματολογία των διεπαφών ορίζεται ως “enp0s3” κάτι το οποίο δημιουργεί σφάλμα κατά την εκτέλεση του εργαλείου arp-scan (Εικόνα Α.1) αφού η σάρωση του δικτύου γίνεται εφικτή μέσω της διεπαφής “eth0” η οποία δεν μπορεί να εντοπιστεί.



Εικόνα Α. 1: Σφάλμα κατά την εκτέλεση του εργαλείου arp-scan

Συνεπώς για την επίλυση του σφάλματος αυτού θα πρέπει να μετονομαστούν οι διεπαφές του συστήματος στην αρχική τους μορφή “eth0”. Αρχικά γίνεται εγκατάσταση των εργαλείων ifupdown και net-tools (Εικόνα Α.2) όπου θα βοηθήσουν στην διαμόρφωση της ονοματολογίας των διεπαφών.

```
root@Ubuntu20:/# sudo apt install ifupdown net-tools
Reading package lists... Done
Building dependency tree
Reading state information... Done
net-tools is already the newest version (1.60+git20180626.aebd88e-1ubuntu1).
The following package was automatically installed and is no longer required:
  gir1.2-goa-1.0
Use 'sudo apt autoremove' to remove it.
Suggested packages:
  rdnssd
The following NEW packages will be installed:
  ifupdown
0 upgraded, 1 newly installed, 0 to remove and 0 not upgraded.
Need to get 60,5 kB of archives.
After this operation, 234 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://cy.archive.ubuntu.com/ubuntu focal/universe amd64 ifupdown amd64 0.8.35ubuntu1 [60,5 kB]
Fetched 60,5 kB in 1s (67,3 kB/s)
Selecting previously unselected package ifupdown.
```

Εικόνα Α. 2: Εγκατάσταση εργαλείων για τη διαμόρφωση της ονοματολογίας των διεπαφών

Στη συνέχεια χρησιμοποιώντας το πρόγραμμα επεξεργασίας αρχείων και με δικαιώματα διαχειριστή γίνεται επεξεργασία του αρχείου /etc/default/grub (Εικόνα Α.3).

```
pani@Ubuntu20:~$ sudo nano /etc/default/grub
[sudo] password for pani:
```

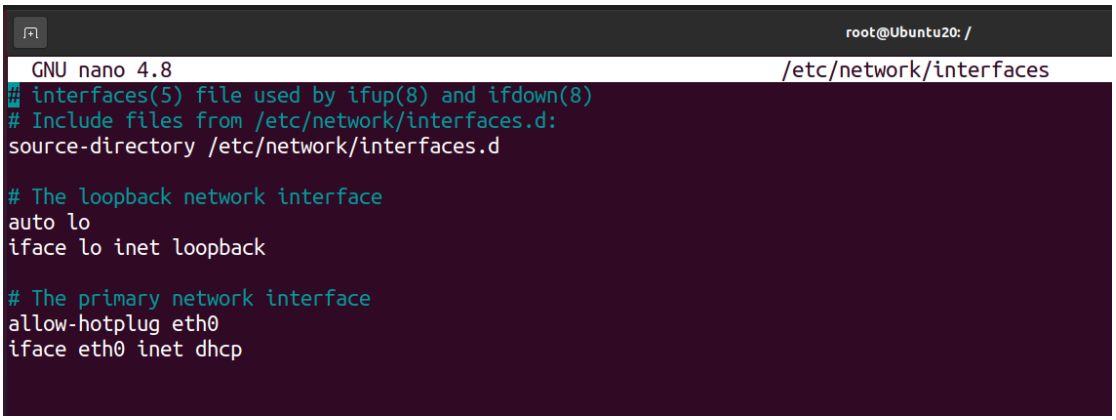
Εικόνα Α. 3: Διαμόρφωση του αρχείου /etc/default/grub

Στο αρχείο γίνεται αλλαγή της τιμής της παραμέτρου “GRUB_CMDLINE_LINUX” από κενό “ ” σε “net.ifnames=0 biosdevname=0“. Στην εικόνα Α.4 εμφανίζεται η τελική τιμή της παραμέτρου όπως έχει διαμορφωθεί στο αρχείο.

```
  GNU nano 4.8                                                /etc/default/grub
# If you change this file, run 'update-grub' afterwards to update
# /boot/grub/grub.cfg.
# For full documentation of the options in this file, see:
#   info -f grub -n 'Simple configuration'

GRUB_DEFAULT=0
GRUB_TIMEOUT_STYLE=hidden
GRUB_TIMEOUT=0
GRUB_DISTRIBUTOR=`lsb_release -i -s 2> /dev/null || echo Debian`
GRUB_CMDLINE_LINUX_DEFAULT="quiet splash"
GRUB_CMDLINE_LINUX="net.ifnames=0 biosdevname=0"
```

Εικόνα Α. 4: Διαμόρφωση της παραμέτρου “GRUB_CMDLINE_LINUX”

Στη συνέχεια γίνεται ανανέωση του grub χρησιμοποιώντας την εντολή " sudo update-grub " και επανεκκίνηση του λειτουργικού συστήματος. Ακολούθως χρησιμοποιώντας το πρόγραμμα επεξεργασίας αρχείων και με δικαιώματα διαχειριστή γίνεται επεξεργασία του αρχείου /etc/network/interfaces όπως παρουσιάζεται στην εικόνα Α.5 ώστε να μπορεί η διεπαφή του λειτουργικού συστήματος να αποκτά διεύθυνση IP μέσω του συστήματος DHCP.



Εικόνα Α. 5: Επεξεργασία του αρχείου /etc/network/interfaces

Στη συνέχεια γίνεται επανεκκίνηση της διεπαφής eth0 χρησιμοποιώντας τις εντολές " sudo ifdown --force eth0 " (Εικόνα Α.6) και " sudo ifup eth0 " (Εικόνα Α.7).

Εικόνα Α. 6: Επανεκκίνηση της διεπαφής eth0

```
root@Ubuntu20:/# sudo ifup eth0
Internet Systems Consortium DHCP Client 4.4.1
Copyright 2004-2018 Internet Systems Consortium.
All rights reserved.
For info, please visit https://www.isc.org/software/dhcp/

Listening on LPF/eth0/08:00:27:64:27:04
Sending on   LPF/eth0/08:00:27:64:27:04
Sending on   Socket/fallback
DHCPDISCOVER on eth0 to 255.255.255.255 port 67 interval 3 (xid=0xf03ce428)
DHCPOFFER of 192.168.56.107 from 192.168.56.100
DHCPREQUEST for 192.168.56.107 on eth0 to 255.255.255.255 port 67 (xid=0x28e43cf0)
DHCPACK of 192.168.56.107 from 192.168.56.100 (xid=0xf03ce428)
bound to 192.168.56.107 -- renewal in 240 seconds.
```

Εικόνα Α. 7: Επανεκκίνηση της διεπαφής eth0

Έπειτα γίνεται έλεγχος των διεπαφών για την επαλήθευση της ολοκλήρωση της διαδικασίας χρησιμοποιώντας την εντολή ifconfig όπου παρουσιάζονται οι διεπαφές του συστήματος με την ονοματολογία "eth" (Εικόνα Α.8)

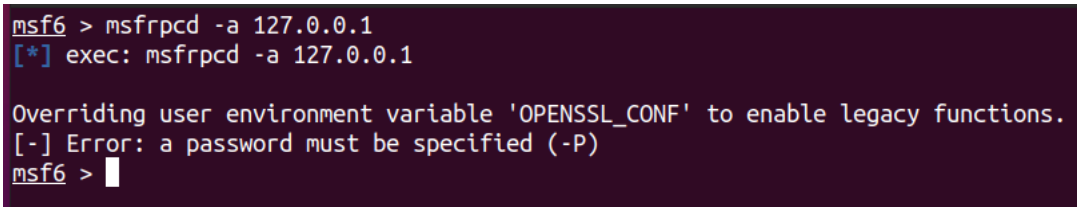
```
root@Ubuntu20:/# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.56.104  netmask 255.255.255.0  broadcast 192.168.56.255
        inet6 fe80::5b5d:8bc5:c951:bbc4  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:64:27:04  txqueuelen 1000  (Ethernet)
        RX packets 93  bytes 19059 (19.0 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 86  bytes 11833 (11.8 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.3.15  netmask 255.255.255.0  broadcast 10.0.3.255
        inet6 fe80::bb97:89f:35f1:830d  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:d8:53:17  txqueuelen 1000  (Ethernet)
        RX packets 28431  bytes 42737894 (42.7 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1518  bytes 123520 (123.5 KB)
        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
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 889  bytes 84578 (84.5 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 889  bytes 84578 (84.5 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Εικόνα Α. 8: Επαλήθευση διαμόρφωσης ονοματολογίας των διεπαφών

Α.2 Υποχρεωτική χρήση κωδικού ασφαλείας

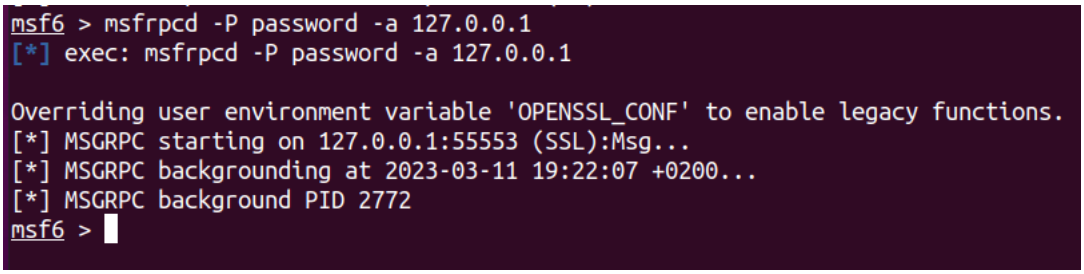
Στο εργαλείο Metasploit για να επιτευχθεί η εκμετάλλευση των ευπαθειών, εκτελέστηκε η εντολή "msfrpcd -a 127.0.0.1" με μοναδική παράμετρο την διεύθυνση IP της επιτιθέμενης μηχανής

(Εικόνα Α.9). Παρουσιάστηκε σφάλμα το οποίο παραπέμπει στη υποχρεωτική χρήση κωδικού ασφαλείας με την παράμετρο -P.



Εικόνα Α. 9: Εκτέλεση εντολής "msfrpcd -a 127.0.0.1"

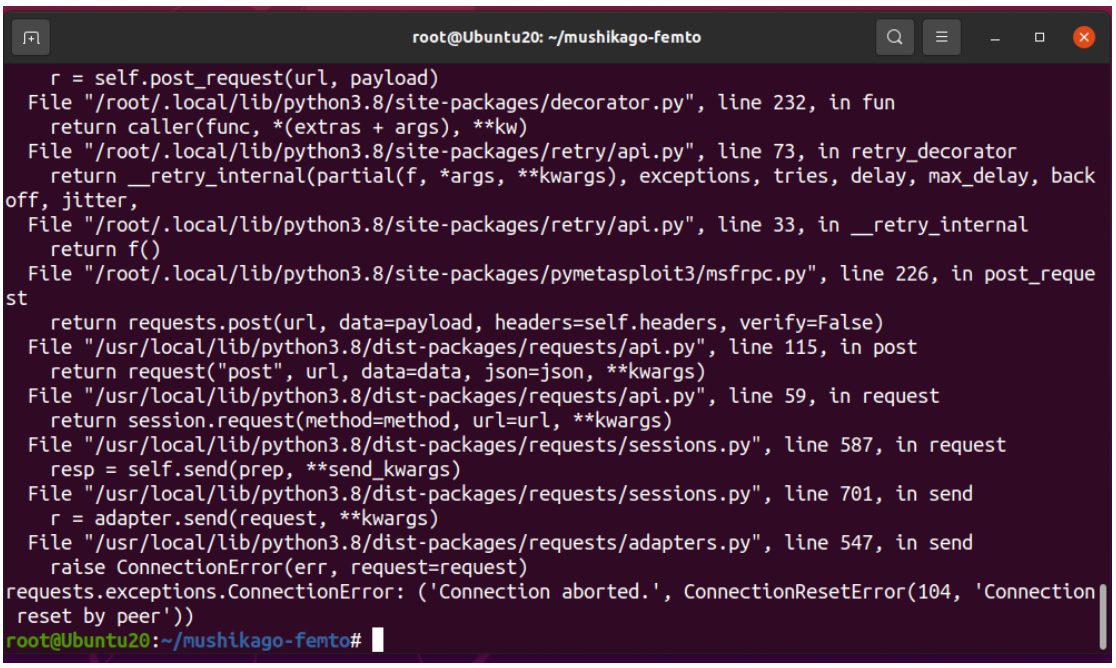
Για την επίλυση του σφάλματος δόθηκε εκ νέου η εντολή "msfrpcd –P password -a 127.0.0.1" (Εικόνα Α.10) με το τυχαίο κωδικό ασφαλείας "password" καθώς δεν ήταν γνωστός στη παρούσα στιγμή ο κωδικός ασφαλείας που θα έπρεπε να δοθεί.



Εικόνα Α. 10: Εκτέλεση εντολής "msfrpcd –P password -a 127.0.0.1"

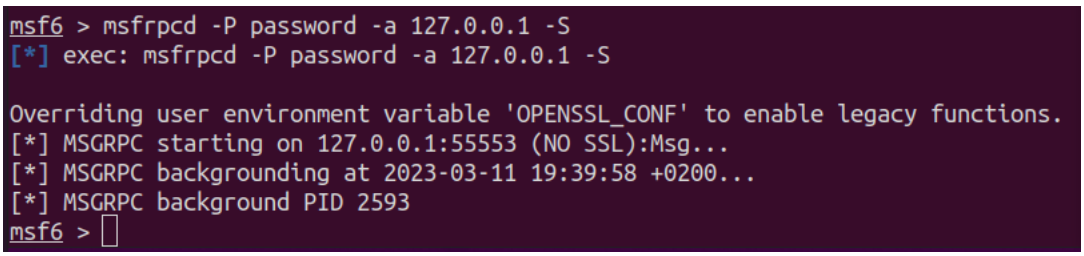
Α.3 Σφάλμα "Connection reset by peer"

Κατά την εκτέλεση του εργαλείου Mushikago-femto παρουσιάστηκε το σφάλμα "Connection reset by peer" (Εικόνα Α.11) το οποίο παραπέμπει σε σφάλμα κατά τη σύνδεση μεταξύ των μηχανών του επιτιθέμενου και του στόχου. Η σύνδεση πραγματοποιείται μέσω του εργαλείου Metasploit και τη χρήση της εντολής msfrpcd όπου η προκαθορισμένη ρύθμιση χρησιμοποιεί το πρωτόκολλο SSL.



Εικόνα Α. 11: Σφάλμα "Connection reset by peer"

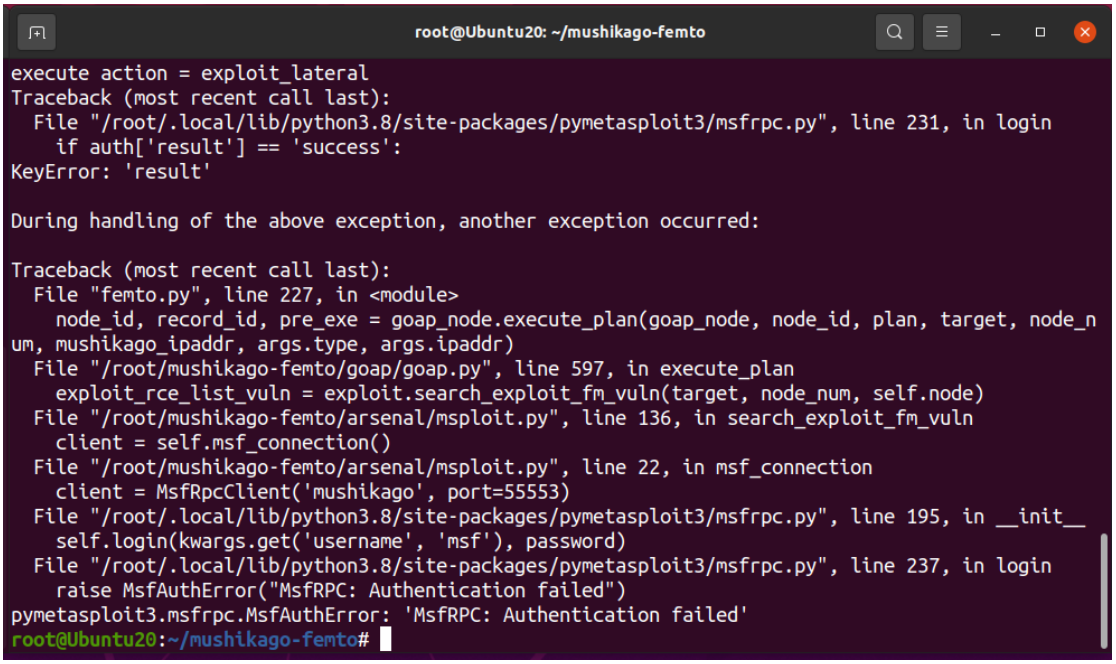
Για την επίλυση του σφάλματος προστέθηκε η παράμετρος -S (Εικόνα Α.12) κατά την εκτέλεση της εντολής msfrpcd όπου υποδηλώνει την απενεργοποίηση σύνδεσης με τη χρήση του πρωτοκόλλου SSL. Συνεπώς η νέα εντολή που δόθηκε στο εργαλείο Metasploit είναι "msfrpcd -P password -a 127.0.0.1 -S"



Εικόνα Α. 12: Εκτέλεση εντολής "msfrpcd -P password -a 127.0.0.1 -S"

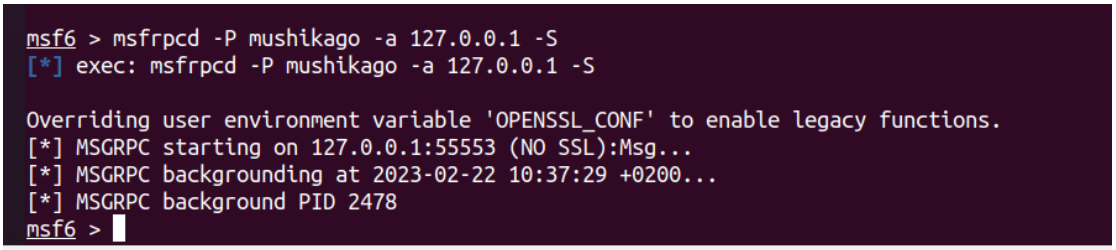
Α.1 Σφάλμα "MsfRPC: Authentication failed"

Κατά την εκτέλεση του εργαλείου Mushikago-femto παρουσιάστηκε το σφάλμα "MsfRPC: Authentication failed" (Εικόνα Α.13) το οποίο παραπέμπει σε σφάλμα αυθεντικοποίησης κατά τη σύνδεση μεταξύ των μηχανών του επιτιθέμενου και του θύματος.



Εικόνα Α. 13: Σφάλμα "MsfRPC: Authentication failed"

Έπειτα από ενδελεχή έρευνα που διεξάχθηκε στο κώδικα του εργαλείου διαφάνηκε ότι ο σωστός κωδικός ασφαλείας είναι η λέξη "mushikago". Συνεπώς στην εντολή σύνδεσης msfrpcd αντικαταστάθηκε ο τυχαίος κωδικός ασφαλείας που χρησιμοποιήθηκε αρχικά με τον σωστό κωδικό ασφαλείας. Η εντολή που διαμορφώθηκε είναι η "msfrpcd -P mushikago -a 127.0.0.1 -S" όπως παρουσιάζεται στην Εικόνα Α.14.

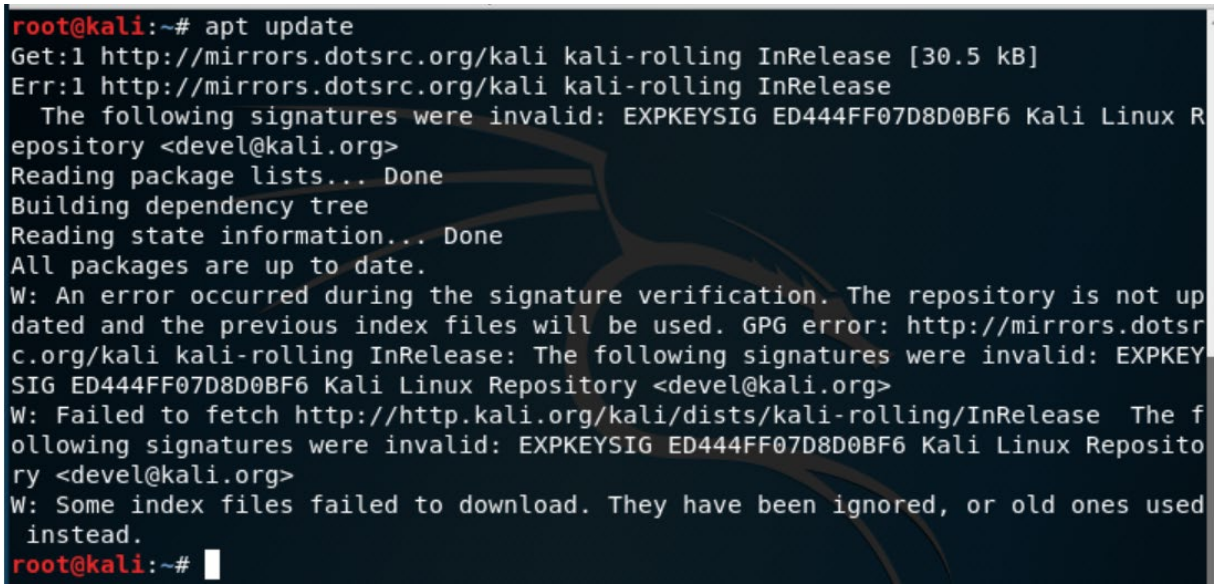


Εικόνα Α. 14: Εκτέλεση εντολής "msfrpcd -P mushikago -a 127.0.0.1 -S"

Παράρτημα Β
Σφάλματα κατά την εκτέλεση του εργαλείου DeepExploit

Β.1 Ενημέρωση της λίστας των υφιστάμενων πακέτων

Κατά την εκτέλεση της εντολής “apt update” που σχετίζεται με την ενημέρωση της λίστας των υφιστάμενων πακέτων παρουσιάστηκε το σφάλμα αναφορικά με άκυρες υπογραφές όπως παρουσιάζεται στην εικόνα Β.1. Ο λόγος που παρουσιάζεται το σφάλμα αυτό είναι διότι η έκδοση του λειτουργικού συστήματος Kali που χρησιμοποιήθηκε είναι απαρχαιωμένη.

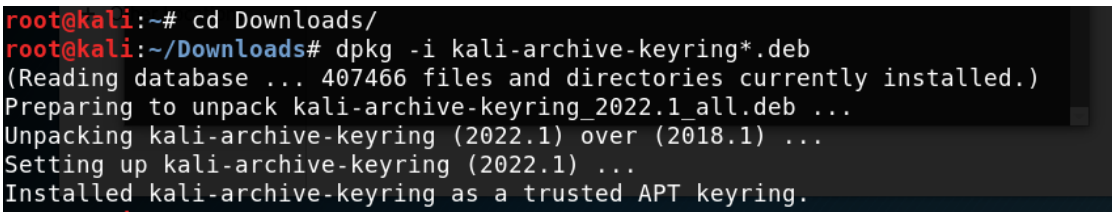


Εικόνα Β. 1: Σφάλμα κατά την εκτέλεση της εντολής "apt update"

Για την επίλυση του σφάλματος χρειάστηκε να εντοπιστεί το καινούργιο κλειδί από την επίσημη ιστοσελίδα https://http.kali.org/kali/pool/main/k/kali-archive-keyring/ Από την ιστοσελίδα έγινε λήψη του αρχείου "kali-archive-keyring_2022.1_all.deb" (Εικόνα Β.2).

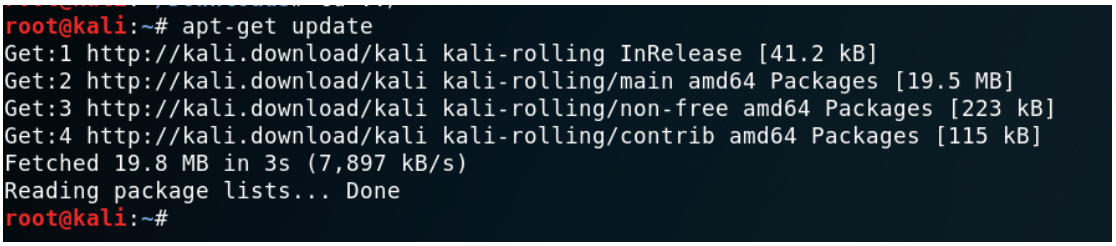
Εικόνα Β. 2: Λήψη του αρχείου "kali-archive-keyring_2022.1_all.deb"

Στη συνέχεια έγινε εγκατάσταση του κλειδιού χρησιμοποιώντας την εντολή "dpkg -i kali-archive-keyring*.deb" (Εικόνα Β.3)



Εικόνα Β. 3: Εγκατάσταση του καινούργιου κλειδιού

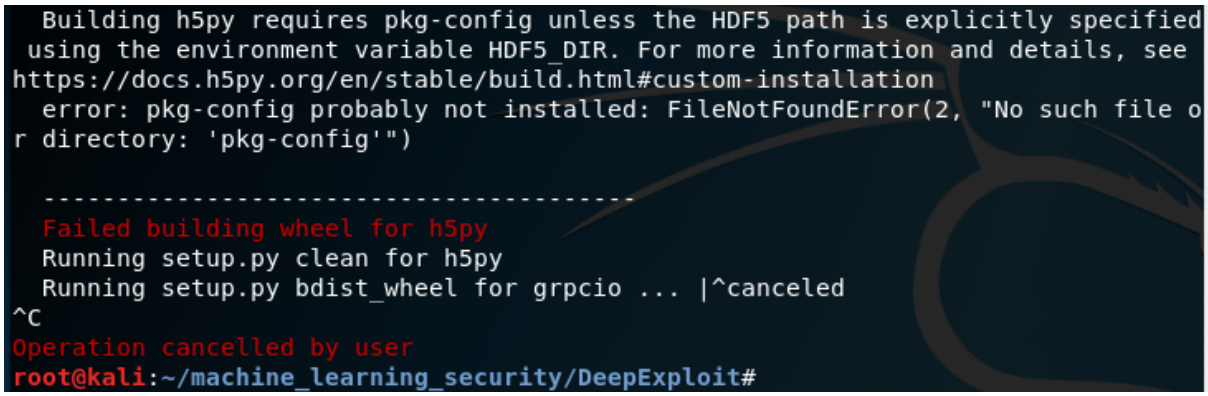
Έπειτα εκτελείτε ξανά η εντολή "apt update" όπου γίνεται επιτυχώς η ενημέρωση της λίστας των υφιστάμενων πακέτων (Εικόνα Β.4).



Εικόνα Β. 4: Επιτυχής εκτέλεση της εντολής "apt update"

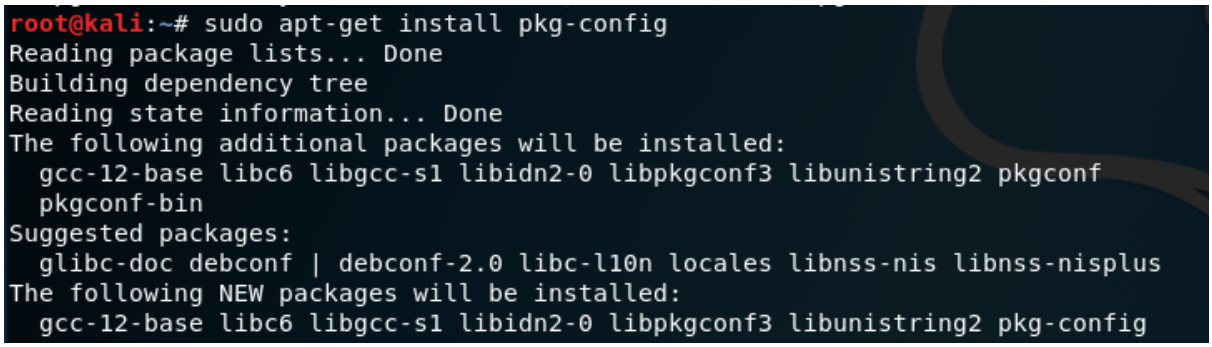
Β.2 Σφάλμα με προ-απαιτούμενα πακέτα

Κατά τη διάρκεια εγκατάστασης των απαιτούμενων πακέτων του εργαλείου DeepExploit παρουσιάστηκε σφάλμα για την έλλειψη κάποιων προ-απαιτούμενων πακέτων (Εικόνα Β.5) όπως για παράδειγμα των πακέτων "pkg-config" και "build-essential" .

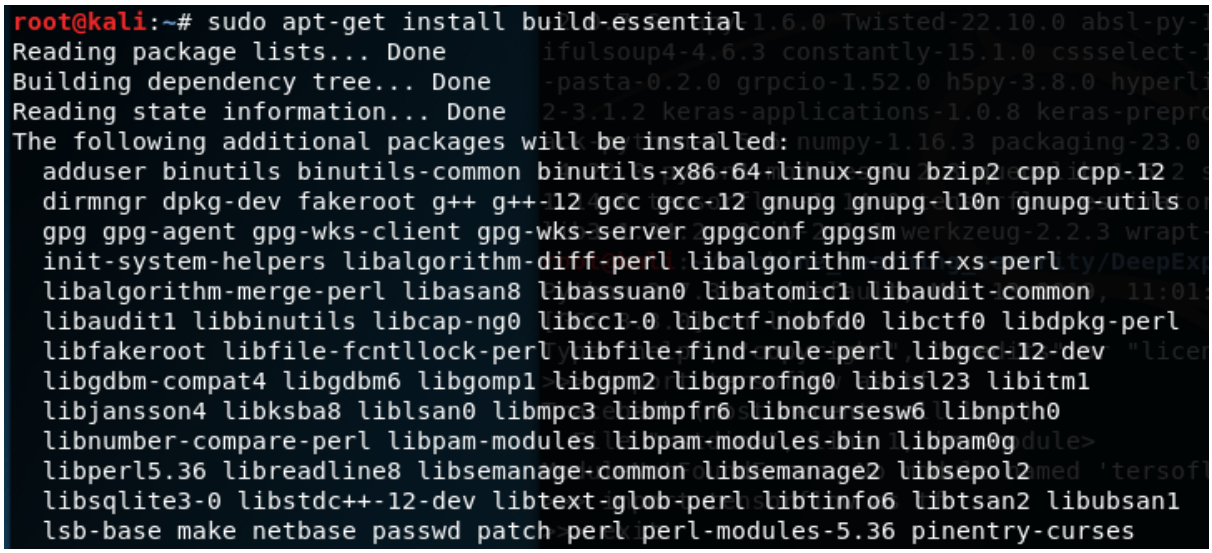


Εικόνα Β. 5: Σφάλμα έλλειψης προ-απαιτούμενων πακέτων

Για την επίλυση του σφάλματος έγινε εγκατάσταση των πακέτων “pkg-config” και “build-essential” χρησιμοποιώντας τις εντολές “sudo apt-get install pkg-config” και “sudo apt-get install build-essential” αντίστοιχα, όπως παρουσιάζονται στις εικόνες Β.6 και Β.7.



Εικόνα Β. 6: Εγκατάσταση του πακέτου pkg-config



Εικόνα Β. 7: Εγκατάσταση του πακέτου build-essential