ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ
ΣΧΟΛΗ ΤΕΧΝΟΛΟΓΙΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΩΝ
ΤΜΗΜΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Π.Μ.Σ. «Ασφάλεια Ψηφιακών Συστημάτων»

Χρήση αυτοματοποιημένης αξιολόγησης red teaming για τον έλεγχο των ρυθμίσεων και των συσκευών ασφαλείας καθώς και του προσωπικού προστασίας ενός δικτύου

ΜΕΤΑΠΤΥΧΙΑΚΗ ΔΙΑΤΡΙΒΗ

Αθανάσιος Παπαχαραλάμπους
ΜΤΕ 1730

Επιβλέπων Καθηγητής : Χριστόφορος Νταντογιάν

ΠΕΙΡΑΙΑΣ, ΙΟΥΝΙΟΣ 2019

Ευχαριστίες

Για τη διεκπεραίωση της παρούσας Πτυχιακής Εργασίας, πρώτα απ' όλα θα ήθελα να ευχαριστήσω τον επιβλέποντα καθηγητή, Δρ. Χριστόφορο Νταντογιάν, για την πολύτιμη βοήθεια και καθοδήγησή του κατά τη διάρκεια της πτυχιακής μου.

Επίσης θα ήθελα να ευχαριστήσω τον κ. Σπυρίδων Παπαγεωργίου για τη δυνατότητα που μου προσέφερε να ασχοληθώ με αυτό το ενδιαφέρον θέμα καθώς και για τη συνεργασία και την πολύτιμη συμβολή του στην ολοκλήρωση της εργασίας μου.

Τέλος πάνω απ' όλα, είμαι ευγνώμων στους γονείς μου και αφιερώνω αυτή την εργασία στην μητέρα μου και στον πατέρα μου για την ολόψυχη αγάπη και υποστήριξή τους όλα αυτά τα χρόνια.

Περίληψη

Στην σημερινή εποχή, οι χάκερς αποτελούν μια από τις πιο σημαντικές απειλές που έχουν ως στόχο τις πληροφορίες μας εκμεταλλευόμενοι τις ευπάθειες κάποιου κώδικα ή παρακάμπτοντας τα μέτρα ασφαλείας ενός συστήματος. Οι χάκερς χρησιμοποιούν μεγάλη ποικιλία από τεχνικές με διαφορετικές προθέσεις και στόχους κάθε φορά. Για το λόγο αυτό οι επαγγελματίες που ασχολούνται με την ασφάλεια και έχοντας ως κύριο στόχο την προστασία των διαφόρων συστημάτων από αυτές τις απειλές, προσπαθούν να αξιολογήσουν την ασφάλεια ενός δικτύου από την πλευρά του εισβολέα. Αυτή η τεχνική ονομάζεται Red Teaming ή Ethical Hacking, η οποία είναι μια διαδικασία που έχει σχεδιαστεί για τον εντοπισμό των τρωτών σημείων ενός δικτύου ή συστήματος και δοκιμάζει την ασφάλεια τους κάνοντας χρήση των γνώσεων και των δεξιοτήτων ενός υποθετικού επιτιθέμενου με απώτερο σκοπό την ενίσχυση ασφαλείας αυτών των συστημάτων.

Σε αυτή την εργασία θα περιγραφεί η μεθοδολογία που χρησιμοποιείται κατά την διαδικασία του Red Teaming καθώς και ο συνολικός ρόλος και η σπουδαιότητα της εν λόγω τεχνικής για την αξιολόγηση ασφαλείας του δικτύου ή του συστήματος. Θα γίνει επίσης περιγραφή και ανάλυση του MITRE’s Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK), το οποίο είναι ένα μοντέλο που χρησιμοποιείται για να περιγράψει την συμπεριφορά του αντιπάλου στον κυβερνοχώρο, αντικατοπτρίζοντας τις διάφορες φάσεις του κύκλου ζωής των επιθέσεων ενός αντίπαλου και τις πλατφόρμες στις οποίες είναι γνωστό ότι στοχεύουν. Επιπλέον θα γίνει εγκατάσταση και δοκιμή δύο εργαλείων που χρησιμοποιούνται για το Red Teaming του CALDERA και του Red Team Automation.

Abstact

Nowadays, hackers are one of the most important threats to our information infrastructure, by exploiting the vulnerabilities in code or bypassing a system's security measures. Hackers use a wide variety of techniques with different intentions and objectives. For this reason, security professionals to protect the various systems from these threats are trying to assess the security of a network from the attacker's side. This technique is called Red Teaming or Ethical Hacking, which is a process designed to identify vulnerabilities in a network or system that tests their security by making use of the knowledge and skills of a hypothetical attacker with the ultimate purpose of enhancing the security of these systems.
This thesis will describe the methodology used in the Red Teaming process, the overall role and the importance of this technique for network or system security evaluation. It will also describe and analyze MITRE's Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK), which is a model used to describe cyber adversary behavior, reflecting the various phases of an adversary's attack lifecycle and the platforms they are known to target. For this purpose, two tools used for Red Teaming, CALDERA and Red Team Automation, will be described, installed and tested.

Πίνακας περιεχομένων

Κατάλογος Εικόνων

Κατάλογος Πινάκων

Κεφάλαιο 1 Εισαγωγή

1.1 Τι είναι το Red Teaming

Το Red Teaming είναι μια πλήρης προσομοίωση επίθεσης και η οποία σχεδιάστηκε για να μετρήσει το πόσο καλά οι άνθρωποι και τα δίκτυα, οι εφαρμογές και οι έλεγχοι φυσικής ασφάλειας μιας εταιρείας ή ενός οργανισμού μπορούν να αντέξουν μια επίθεση από έναν πραγματικό αντίπαλο. Με άλλα λόγια είναι μια τεχνική «ethical hacking» δηλαδή ένας τρόπος για ανεξάρτητες ομάδες ασφαλείας να δοκιμάσουν πόσο καλά ένας οργανισμός μπορεί να ανταπεξέλθει για την αντιμετώπιση μιας πραγματικής επίθεσης. Ένα πρόγραμμα **vulnerability scanning** θα εντοπίσει μόνο επιφανειακά προβλήματα, και περιορίζεται στην αυτοματοποιημένη του εκτέλεση. Το **penetration test** θα δοκιμάσει ένα συστατικό του περιβάλλοντος ενός οργανισμού σε βάθος, αλλά δεν εξετάζει το πλαίσιο, τα κενά ασφαλείας γύρω από αυτό το στοιχείο ή τους πραγματικούς στόχους τους οποίους οι κακόβουλοι χρήστες θα προσπαθούν να προσβάλλουν. Το **Red Teaming** θέλει να απαντήσει στην ερώτηση, αν ο οργανισμός γίνει στόχος, μπορούν τα περιουσιακά στοιχεία (assets) που έχουν μεγάλη σημασία για τον οργανισμό αυτό (π.χ. προσωπικά δεδομένα) να διαρρεύσουν;
Μια εξονυχιστική δοκιμή από μια red team θα εκθέσει όλα τα τρωτά σημεία και τους κινδύνους που σχετίζονται με:

- Την τεχνολογία - Δίκτυα, εφαρμογές, δρομολογητές, switches, συσκευές κ.λπ.
- Τους ανθρώπους - Προσωπικό, ανεξάρτητοι εργολάβοι, τμήματα, επιχειρηματικοί εταίροι κ.λπ.
- Την φυσική ασφάλεια - Γραφεία, αποθήκες, υποσταθμούς, κέντρα δεδομένων, κτίρια κ.λπ.

Το red teaming βοηθά μια επιχείρηση να παραμείνει ανταγωνιστική, εξασφαλίζοντας παράλληλα τα επιχειρηματικά της συμφέροντα, αξιοποιώντας το social engineering και το penetration testing σε εφαρμογές και δίκτυα, για να βρει διάφορους τρόπους οι οποίοι θα προστατέψουν τις άμυνες της. Κατά τη διάρκεια εμπλοκής μιας red team, πολύ καλά εκπαιδευμένοι σύμβουλοι ασφαλείας καθορίζουν σενάρια επίθεσης για να αποκαλύψουν πιθανές αδυναμίες σχετικές με την φυσική ασφάλεια, το υλικό, το λογισμικό και τους ανθρώπους. Το εξειδικευμένο προσωπικό των red teams εντοπίζει επίσης κακόβουλους εισβολείς οι οποίοι μπορούν να θέσουν σε κίνδυνο τα συστήματα και τα δίκτυα της εταιρείας ή να επιτρέψουν παραβιάσεις δεδομένων.

1.2 Ποιος το χρειάζεται;

Εάν μια επιχείρηση είναι μεσαίου μεγέθους, τότε ίσως να πιστεύει ότι η red team δεν είναι για αυτήν. Συνήθως τέτοιου είδους επιχειρήσεις θεωρούν ότι : "Είμαι πολύ μικρός για να είμαι στόχος". Αλλά στην πραγματικότητα, αυτή είναι ακριβώς η γραμμή σκέψης που θέτει σε κίνδυνο έναν οργανισμό. Αν ήμασταν κάποιος κακόβουλος, δεν θα θέλαμε να επιτεθούμε σε κάποιον που δεν θα το περίμενε ποτέ; Παρόλο που μπορεί κάποιος να σκεφτεί ότι κανένας δεν θα ενδιαφερόταν

πραγματικά να «χακάρει» την επιχείρησή του, οι επιχειρήσεις όλων των μεγεθών, ακόμα και τα μεμονωμένα άτομα, είναι από τα πιο τακτικά θύματα. Και δεν πρόκειται μόνο για ευαίσθητες πληροφορίες. Οι κακόβουλοι προσπαθούν επίσης να αξιοποιήσουν τις τεχνολογίες που χρησιμοποιούμε στη ζωή μας. Για παράδειγμα, μπορεί να αναζητούν πρόσβαση στο δίκτυό μας για να αποκρύψουν καλύτερα τις δραστηριότητές τους, ενώ προσπαθούν να αναλάβουν κάποιο άλλο σύστημα ή δίκτυο κάπου αλλού στον κόσμο. Σε μια τέτοια περίπτωση τα δεδομένα μας δεν έχουν σημασία. Το μόνο που χρειάζονται είναι οι υπολογιστές μας τους οποίους θέλουν να μολύνουν με κάποιο κακόβουλο λογισμικό, ώστε να προσθέσουν το σύστημά μας σε ένα botnet γκρουπ.

1.3 RED TEAM VS PENETRATION TEST

Όσον αφορά το offensive security, η αξιολόγηση ασφαλείας ενός συστήματος για να βρεθούν οι ευπάθειές του, μπορεί να γίνει με :

α) το penetration test και
β) το red teaming.

Η κατανόηση των διαφορών μεταξύ των δύο αυτών τεχνικών είναι απαραίτητη όταν προσπαθούμε να εξετάσουμε την ασφάλεια μιας εφαρμογής, ενός δικτύου ή ενός οργανισμού.

1.3.1 PENETRATION TESTING

Το penetration test συχνά χωρίζεται σε μια σειρά από τύπους αξιολόγησης. Είτε πρόκειται για αξιολόγηση εφαρμογών, είτε για αξιολόγηση εσωτερικού ή εξωτερικού δικτύου ή κάτι πιο συγκεκριμένο ή πιο εσωτερικό. Το penetration test περιλαμβάνει έναν σύμβουλο ασφάλειας που είναι δυνατό να εκτελεί τόσο αυτοματοποιημένη όσο και μη ανάλυση ενός στόχου, προσπαθώντας να βρει όσο το δυνατόν περισσότερες ευπάθειες. Το penetration test επεκτείνεται πέρα από την αυτοματοποιημένη ανάλυση ευπάθειας, με τον σύμβουλο να κατανοεί την εφαρμογή ή το δίκτυο σε όλη τη διάρκεια της αξιολόγησης και να εντοπίζει χειροκίνητα συγκεκριμένες ευπάθειες.
Το penetration test θα αξιολογήσει την ασφάλεια μιας εφαρμογής ή δικτύου, συνήθως σε απομόνωση από το υπόλοιπο λειτουργικό περιβάλλον του οργανισμού. Για παράδειγμα, ένα penetration test στο εσωτερικό του δικτύου ενός οργανισμού θα αξιολογήσει το δίκτυο του, από την οπτική ενός κακόβουλου χρήστη, όπως για παράδειγμα ένα κακόβουλο μέλος του προσωπικού. Ο σύμβουλος για το penetration test θα φτάσει επιτόπου στις εγκαταστάσεις του οργανισμού, θα συνδέσει το φορητό του υπολογιστή στο δίκτυο των υπολογιστών του και θα ενεργήσει τους ελέγχους του από εκεί.
Ένας τέτοιος έλεγχος στο εσωτερικό του δικτύου θα αγνοήσει τα απαιτούμενα βήματα που θα χρειαζόταν να εκτελέσει ένας εισβολέας για να αποκτήσει αρχική πρόσβαση στο δίκτυο, και ο penetration tester προσπαθεί να βρει τις αδυναμίες από μια πιο προνομιακή θέση. Ο σύμβουλος θα προσπαθήσει να θέσει σε κίνδυνο τις συσκευές δικτύου και με τον τρόπο αυτό να αποκτήσει δικαιώματα διαχειριστή μέσα στο περιβάλλον που ενεργεί. Ένα report μετά από ένα penetration test στο εσωτερικό ενός δικτύου θα περιλαμβάνει συνήθως όλα τα «ευρήματα» σχετικά με τις διάφορες υπηρεσίες (services) που είναι εκτεθειμένες, διάφορα updates τα οποία

πρέπει να γίνουν για να λειτουργεί ορθά το σύστημα, κωδικούς πρόσβασης οι οποίοι έχουν ανακτηθεί από διακομιστές αρχείων, πρόσβαση με δικαιώματα διαχειριστή σε κάποιο domain και ούτω καθεξής. Αυτές οι πληροφορίες μπορούν στη συνέχεια να χρησιμοποιηθούν για την ενίσχυση του εσωτερικού δικτύου, αλλά το report δεν εξετάζει τα βήματα που θα χρειαστεί να κάνει ένας εισβολέας για να αποκτήσει πρόσβαση στο εσωτερικό δίκτυο.
Ένας έλεγχος των εφαρμογών θα παρέχει πληροφορίες σχετικά με τα τρωτά σημεία μιας συγκεκριμένης εφαρμογής και ο penetration tester θα εκτελέσει γενικά δοκιμές όπως θα εκτελούσε κανονικά και ένας επιτιθέμενος. Η έκθεση του report, όσον αφορά τις εφαρμογές, συνήθως περιλαμβάνει ζητήματα όπως η αδύναμη ασφάλεια των cookies, η απουσία λογαριασμών σε περίπτωση κλειδώματος μια εφαρμογής καθώς και τα τρωτά σημεία των εφαρμογών, όπως injection και cross-site scripting ευπάθειες. Ένα penetration test για έλεγχο των εφαρμογών θα αποκαλύψει ευπάθειες οι οποίες στις περισσότερες περιπτώσεις είναι άγνωστες μέχρι εκείνη την στιγμή.
Από τα παραπάνω μπορούμε να διαπιστώσουμε ότι κατά το penetration test εξετάζεται μόνο ένα μεμονωμένο στοιχείο το οποίο βρίσκεται συχνά σε απομόνωση από το υπόλοιπο δίκτυο. Τα penetration tests μπορούν να χρησιμοποιηθούν για να επαληθεύσουν την ασφάλεια μεμονωμένων δομικών στοιχείων ενός οργανισμού, αλλά τις περισσότερες φορές οι διάφορες ευπάθειες και οι επιθέσεις από αντίπαλους «παραμονεύουν» στις λεπτομέρειες του πώς αυτά τα δομικά στοιχεία αλληλοεπιδρούν μεταξύ τους μέσα σε ένα οργανισμό.

1.3.2 RED TEAMING

Από την άλλη μεριά το red teaming μπορεί να θεωρηθεί ως "εξομοίωση εισβολέα". Η αξιολόγηση είναι συνήθως καθορισμένη, με τέτοιο τρόπο ώστε στους συμβούλους ασφαλείας να παρέχονται ένας στόχος (π.χ. μια βάση δεδομένων πελατών ή ένα επίπεδο ελέγχου SCADA) και οι κανόνες εμπλοκής με αυτό τον στόχο (π.χ. δεν θα εμπλακούν τα πετροχημικά εργοστάσια, οι δοκιμές πρέπει να διεξαχθούν σε ωράριο εργασίας, κ.λπ.). Ο σύμβουλος ασφαλείας που θα εκτελέσει την εξομοίωση θα προσπαθήσει να επιτύχει τον τελικό στόχο και να αποφύγει την ανίχνευση. Το red teaming είναι ένας μηχανισμός που έχει σχεδιαστεί για να δώσει σε έναν οργανισμό να καταλάβει πως τα μέτρα ασφαλείας που εφαρμόζει σε συνάρτηση με τα μέτρα απόκρισης που έχει λάβει μπορούν να ανταπεξέλθουν ενάντια σε μια πραγματική απειλή. Οι τεχνικές του red teaming συνδυάζουν επιθέσεις ηλεκτρονικού "ψαρέματος" (phishing), social engineering, καθώς και επιθέσεις κατά των υποδομών πληροφορικής ενός οργανισμού για την επίτευξη των καθορισμένων στόχων.
Το report που θα προκύψει θα είναι περισσότερο σαν μια αφήγηση και θα αφορά την λίστα των ευρημάτων που αποκτήθηκαν κατά την διάρκεια της προσομοίωσης. Οι σύμβουλοι του ελέγχου αναφέρουν λεπτομερώς τα βήματα που έγιναν για να εκθέσουν τον οργανισμό και να επιτύχουν τον τελικό στόχο, περιγράφοντας όλα τα βήματα που εκτέλεσαν από την αρχική αναγνώριση μέχρι την τελική εξαγωγή (exfiltration) των δεδομένων. Οι σύμβουλοι χρησιμοποιούν παρόμοιες τεχνικές με τους επιτιθέμενους και ο οργανισμός που ελέγχεται θα πρέπει να αμυνθεί σε αυτές τις επιθέσεις, γεγονός που παρέχει μια ρεαλιστική εικόνα του τρόπου με τον οποίο μπορεί να τεθεί σε κίνδυνο ο οργανισμός.
Στον Πίνακα 1που ακολουθεί φαίνονται οι διαφορές των δυο αυτών τεχνικών

Penetration Test	Red Teaming
Το πεδίο εφαρμογής καθορίζεται και παρέχεται από τον πελάτη	Ολόκληρος ο οργανισμός είναι στο πεδίο εφαρμογής
Εύρεση, αξιολόγηση και εκμετάλλευση όλων των ευπαθειών	Εύρεση, αξιολόγηση και εκμετάλλευση μόνο των ευπαθειών που βοηθούν στην επίτευξη των στόχων
Παρέχεται αρχική πρόσβαση για δοκιμές στο εσωτερικό δίκτυο	Προσπαθεί να αποκτήσει πρόσβαση στο εσωτερικό δίκτυο
Οι εργαζόμενοι συνήθως γνωρίζουν τη δοκιμή	Περιορισμένος αριθμός υπαλλήλων γνωρίζει για τις δοκιμές
Οι δοκιμές πραγματοποιούνται κατά τις εργάσιμες ώρες	Οι δοκιμές πραγματοποιούνται όλο το 24ωρο
Οι κανόνες είναι σαφώς καθορισμένοι	Δεν υπάρχουν κανόνες
Το κάθε σύστημα ελέγχεται ανεξάρτητα	Αξιολογούνται μόνο οι επιτυχημένες επιθέσεις ως προς τις επιπτώσεις που έχουν για τον οργανισμό

Πίνακας 1 : Συγκριτικός πίνακας των δυο τεχνικών

1.4 Πως ενεργεί μια Red Team

Τα παρακάτω 3 χαρακτηριστικά βοηθούν να κατανοήσουμε πως ενεργεί μια red team:

1. Το πεδίο εφαρμογής μιας δοκιμής red teaming καθορίζεται από αντικειμενικούς στόχους και όχι από ένα περιορισμένο σύνολο IP διευθύνσεων, domain ή URL. Παραδείγματα αντικειμενικών στόχων που θέτουμε είναι να μπορούμε να αποκτήσουμε πρόσβαση στα προσωπικά δεδομένα των πελατών μιας επιχείρησης, να μπορούμε να επηρεάσουμε την διαθεσιμότητα ενός συστήματος της επιχείρησης ή αν μπορούμε να επηρεάσουμε την ακεραιότητα μια συναλλαγής μεταξύ ενός πελάτη Α και Β.

2. Να προσεγγίσουμε το στόχο όπως θα έκανε και ένας πραγματικός επιτιθέμενος. Η red team πρέπει να εξετάσει το περιβάλλον όπως ακριβώς θα έκανε και κάποιος επιτιθέμενος. Πώς δηλαδή αυτός θα συμπεριφερόταν, τι ενέργειες θα έκανε για να επιτύχει τους στόχους του κ.α.

3. Ευρύτερες πολιτικές της επιχείρησης και συστήματα ελέγχου εξετάζονται. Για παράδειγμα, εξετάζονται οι πολιτικές που αφορούν την φυσική πρόσβαση στο κτίριο, οί πολιτικές που εφαρμόζεται για τα updates, η διαδικασίες που εφαρμόζονται για την ανίχνευση και την αντιμετώπιση των διαφόρων περιστατικών καθώς και η αποτελεσματικότητα των υπόλοιπων μέτρων ασφαλείας.
Ο πρωταρχικός σκοπός της Red Team είναι να επικυρώσει την αποτελεσματικότητα ενός οργανισμού ενάντια σε αξιόπιστες και ρεαλιστικές απειλές που εμφανίζονται στον κυβερνοχώρο. Τα συστήματα ασφαλείας και ελέγχου που εφαρμόζονται από την υπάρχουσα στρατηγική ενός οργανισμού ενάντια στις κυβερνοαπειλές δοκιμάζονται σε τέτοιο βαθμό από την Red Team για να δουν πώς αυτά αντιδρούν και συμπεριφέρονται. Η Red Team στοχεύει στην εξομοίωση των πραγματικών

ενεργειών που θα εκτελούσε κάποιος εισβολέας και με τον τρόπο αυτό προσπαθούν να προσδιορίσουν αν τα υπάρχουσα επίπεδα ασφαλείας που εφαρμόζει ο οργανισμός είναι αξιόπιστα και αν απαιτείται να βελτιωθεί η αποτελεσματικότητα οποιασδήποτε μέτρου αντιμετώπισης απειλών σε διάφορα επίπεδα.

Μια άσκηση της ομάδας Red Team :

1. Θα προσομοιώσει μια πραγματική επίθεση από την θέση του πραγματικού επιτιθέμενου - Πώς θα αντιδράσει ένας οργανισμός κατά την διάρκεια μια επίθεσης; Το σημείο από το οποίο θα ξεκινήσει την επίθεση είναι και το πλεονέκτημα ενός εισβολέα.

2. Θα εστιάσει σε κρίσιμα περιουσιακά στοιχεία - Οι στόχοι καθορίζονται λόγω της σημασίας τους και την αξία που έχουν για την συγκεκριμένη επιχείρηση. Είναι σημαντικότερο να καθορίσουμε τον τρόπο με τον οποίο μπορούν αυτά να παραβιαστούν, παρά να εστιάσουμε στο τι επίδραση θα έχει μια ενδεχόμενη διαρροή.

3. Θα αφαιρέσει το προκαθορισμένο πεδίο εφαρμογής του ελέγχου που θα γίνει σε έναν οργανισμό – Ένα παραδοσιακό penetration test , ξεκινάει με ένα προκαθορισμένο πεδίο εφαρμογής. Αυτό θα καθοριστεί από τον ίδιο τον οργανισμό και μπορεί να επηρεαστεί από εσωτερικές προτιμήσεις σχετικά με το τι πρέπει / δεν πρέπει να συμπεριληφθεί στον έλεγχο. Το Red Teaming καταργεί αυτήν την προκατάληψη με την αφαίρεση τον περιορισμού που αφορά το πεδίο εφαρμογής του ελέγχου. Σε έναν τέτοιο έλεγχο το πεδίο εφαρμογής μπορεί να είναι ευρύτερο και η τεχνική της επίθεσης που θα εφαρμοστεί επιλέγεται με βάσει τα κενά ασφαλείας που θα εντοπιστούν κατά την διάρκεια της αναγνώρισης του οργανισμού.

4. Θα δοκιμάσει τις δυνατότητες εντοπισμού καθώς και των μέτρων αντιμετώπισης των απειλών - Μια άσκηση Red Teaming θα δοκιμάσει τις διαδικασίες και τα μέτρα ασφαλείας ενός οργανισμού. Πως δηλαδή θα εντοπίσουν, θα αντιδράσουν και θα συμπεριφερθούν τα διαφορετικά τμήματα ενός οργανισμού, καθώς επίσης και το πως αυτά θα λειτουργήσουν κατά την διάρκεια ενός πραγματικού σεναρίου.

5. Είναι ο πιο οικονομικός τρόπος για να δοκιμαστεί το επίπεδο ασφάλειας ενός οργανισμού – Στο να επενδύσει ένας οργανισμός σε αυτό το επίπεδο των δοκιμών είναι ο πιο καλός τρόπος για να επιτευχθεί ένα επίπεδο βεβαιότητας όσον αφορά την ασφάλεια, παρά να περιμένει μια πραγματική επίθεση να λάβει χώρα με τις οποιεσδήποτε συνέπειες.

6. Θα κάνει χρήση εξειδικευμένων εργαλείων - Οι πραγματικοί επιτιθέμενοι συχνά χρησιμοποιούν συνήθη εργαλεία και μια red team πρέπει να είναι σε θέση να μιμείται τους επιτιθέμενους με εξαιρετικά προχωρημένο και στοχευμένο τρόπο, όπως ακριβώς θα ενεργούσαν και οι αντίπαλοι. Αυτά τα εργαλεία επιτρέπουν στην red team να προσομοιώσει τις πραγματικές απειλές που αντιμετωπίζει κάποιος οργανισμός με τέτοιο τρόπο που να πλησιάζει ρεαλιστικά σε μια πραγματική επίθεση.

7. **Θα προσομοιάσει σενάρια επίθεσης που θα αφορούν τα περιουσιακά στοιχεία (assets) του οργανισμού και δεν θα επικεντρωθεί μόνο στο να παραβιάσει την περίμετρο ασφαλείας -** Μια red team θα δημιουργήσει σε βάθος μονοπάτια επίθεσης που μιμούνται ένα ευρύ φάσμα από προχωρημένα σενάρια. Αυτό θα βοηθήσει τις ομάδες ανίχνευσης και αντιμετώπισης των απειλών του οργανισμού να γνωρίζουν επακριβώς τι πρέπει να αναζητούν και να εντοπίζουν σε κάθε στάδιο της επίθεσης.

8. **Θα χρησιμοποιήσει πολλά «κόλπα» -** Οι Red Teams χρησιμοποιούν μια πληθώρα από εργαλεία και τεχνικές. Οι ικανότητες τους ειδικεύονται σε πολλούς τομείς, συμπεριλαμβανομένων των χρηματοπιστωτικών συστημάτων και υπηρεσιών, τις τραπεζικές υπηρεσίες, την ανάλυση και τη δημιουργία κακόβουλου λογισμικού και επίσης τεχνικές που σχετίζονται με το social engineering. Αυτά τα «κόλπα» θα προσαρμοστούν και θα δοκιμαστούν, ανάλογα με τον οργανισμό που θα γίνει ο έλεγχος, σε τέτοιο βαθμό ώστε να παραβιαστεί και να έχουμε διαρροή δεδομένων.

9. **Θα εκπαιδεύσει τον οργανισμό γύρω από τις δραστηριότητες των αντιπάλων –** Ο οργανισμός που θα δοκιμαστεί από Red Team θα μάθει πολλές πληροφορίες σχετικά με τους τύπους των απειλών που ενδεχομένως να αντιμετωπίσει και θα καταλάβει που υπάρχουν αδυναμίες όσον αφορά τους ανθρώπους, τις διαδικασίες και τις διάφορες τεχνολογίες που χρησιμοποιεί.

10. **Συνδυάσει τις τεχνικές και των αμυντικών και επιθετικών ομάδων -** Οι Red Teams συνδυάζουν τις τεχνικές τόσο των επιθετικών ομάδων (Red Teams) όσο και των αμυντικών (Blue Teams).

1.5 Σκοποί του Red Teaming

Ο σκοπός κάθε Red Team ποικίλλει. Χρησιμοποιώντας μια ευρεία ταξινόμηση που αναπτύχθηκε από τον Mateski (2004), οι κύριοι στόχοι της Red Teaming θα μπορούσαν να χωριστούν σε τέσσερις βασικές κατηγορίες: (1) στην κατανόηση, (2) την πρόβλεψη, (3) τη δοκιμή και (4) την εκπαίδευση, όπως περιγράφονται παρακάτω:

1. **Κατανόηση:** Σε αυτές τις δραστηριότητες η μπλε ομάδα επιχειρεί να καταλάβει την κόκκινη ομάδα και πώς αυτή τους αντιλαμβάνεται. Με την κατανόηση της κόκκινης ομάδας, οποιαδήποτε υπάρχουσες προκαταλήψεις ή ελαττώματα μπορούν να εκτεθούν. Μία εφαρμογή αυτού του είδους της δραστηριότητας αποτελεί μέρος της στρατιωτικής διαδικασίας συλλογής πληροφοριών.

2. **Πρόβλεψη:** Πολλές δραστηριότητες Red Teaming, ιδιαίτερα οι στρατιωτικές στοχεύουν στο να προβλέψουν το τι θα κάνει η αντίπαλη Red Team. Και πάλι, αυτές οι δραστηριότητες περιλαμβάνουν την εκτέλεση σεναρίων από την πλευρά του επιτιθέμενου και προσπαθούν να προβλέψουν τις πιθανές ενέργειες των επιτιθεμένων εξετάζοντας τα κίνητρά τους, τους πόρους και τις ικανότητές τους. Αυτές οι δραστηριότητες, αν γίνουν αποτελεσματικά, θα είναι σε θέση να μειώσουν την πιθανότητα να εμφανιστούν απρόβλεπτες ενέργειες του επιτιθέμενου και θα συμβάλλουν σε μεγάλο βαθμό στην ανάπτυξη ικανοποιητικών σχεδίων για τη

μείωση των ενδεχόμενων επιπτώσεων σε περίπτωση που ο επιτιθέμενος ενεργήσει όπως είχε προβλεφθεί ότι θα το κάνει. Μια εφαρμογή αυτού του τύπου δραστηριότητας είναι η αξιολόγηση απειλών, κίνδυνου και των ευπαθειών.

3. Δοκιμή: Οι ενέργειες που περιλαμβάνουν δοκιμές σε συστήματα συνήθως βασίζονται σε δραστηριότητες που έχουν ήδη προηγουμένως κατανοηθεί και υπάρχει δυνατότητα για πρόβλεψή τους. Με τη δοκιμή ενός συστήματος με μια μέθοδο Red Teaming, όλα τα ελαττώματα ή οι υπάρχουσες αδυναμίες του συστήματος θα είναι εκτεθειμένες. Σε πολλές περιπτώσεις δεν είναι δυνατό να εντοπιστούν οι τυχόν αδυναμίες κάποιου συστήματος χρησιμοποιώντας οποιαδήποτε άλλη μέθοδο ελέγχου. Μετά την διαδικασία εντοπισμού των διαφόρων αδυναμιών του συστήματος, είναι δυνατόν να γίνουν διάφορες τροποποιήσεις του ή των διαδικασιών που εφαρμόζονται προκειμένου να μετριαστούν οι απειλές από πιθανούς αντιπάλους. Τα συνηθισμένα παραδείγματα από δοκιμές που εφαρμόζονται είναι η προσομοίωση με σενάρια πραγματικών επιθέσεων (war-gaming) και τα penetration tests. Το war-gaming περιλαμβάνει τη δοκιμή των στρατηγικών και των τακτικών που εφαρμόζονται εναντίων μιας ανεξάρτητης Red Team, με σκοπό να τελειοποιηθούν αυτές πριν την εμφάνιση των συγκεκριμένων απειλών. Στην περίπτωση του penetration test, οι αδυναμίες στα διάφορα συστήματα ασφαλείας εξετάζονται και εντοπίζονται σε περιβάλλον που δεν υπάρχουν απειλές, με σκοπό μετριαστούν πριν την εμφάνισή τους.

4. Εκπαίδευση: Μια άσκηση από Red Teaming είναι με τέτοιο τρόπο σχεδιασμένη ώστε να είναι σε θέση να εκπαιδεύει τους συμμετέχοντες να κατανοήσουν τον τρόπο με τον οποίο σκέφτεται και θα μπορούσε ενδεχομένως να δράσει ένας επιτιθέμενος. Αυτό επίσης περιλαμβάνει εκπαίδευση σε διαδικασίες αντίδρασης στις αναμενόμενες ενέργειες της Red Team.
Η κατηγοριοποίηση αυτή έγινε από τον Mateski θεωρώντας αυτούς τους σκοπούς ως συσωρευτικούς, δεδομένου ότι κάθε διαδικασία βασίζεται στην προηγούμενη από αυτή. Για παράδειγμα, δεν είναι δυνατόν να προβλέψουμε πώς θα ενεργήσει η Red Team εάν αρχικά δεν την κατανοήσουμε. Επιπλέον, μια ορθή κατανόηση της Red Team, καθώς και η δυνατότητα πρόβλεψης του πως πιθανώς αυτή θα ενεργήσει, είναι απαραίτητη προϋπόθεση για την εκτέλεση μιας δοκιμής του συστήματος.
Εκτός από το σκοπό, κάθε δραστηριότητα μπορεί να ταξινομηθεί είτε ως παθητική είτε ως ενεργητική. Οι παθητικές δραστηριότητες δεν εκτελούν ενεργά καταστάσεις σε κάποιο πειραματικό ή επιχειρησιακό περιβάλλον, αλλά βοηθούν στην κατανόηση και στην πρόβλεψη των ενεργειών της Red Team. Οι ενεργητικές δραστηριότητες, από την άλλη πλευρά, γενικά βασίζονται σε ενέργειες που απαιτούν δράση καθώς και στην εκπαίδευση.

Κεφάλαιο 2 Η φιλοσοφία του μοντέλου ATT&CK

2.1 Εισαγωγή

MITRE's Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) είναι ένα μοντέλο για την συμπεριφορά του αντιπάλου στον κυβερνοχώρο, αντικατοπτρίζοντας τις διάφορες φάσεις του κύκλου ζωής των επιθέσεων του αντίπαλου και τις πλατφόρμες που είναι γνωστό ότι στοχεύουν. Το ATT&CK ξεκίνησε από ένα project για να απαριθμήσει και να κατηγοριοποιήσει τις τακτικές, τις τεχνικές και τις διαδικασίες εναντίον των συστημάτων Microsoft Windows με σκοπό τη βελτίωση της ανίχνευσης κακόβουλων δραστηριοτήτων. Από τότε έχει αναπτυχθεί για να συμπεριλάβει και τα λειτουργικά συστήματα Linux και MacOS, και έχει επεκταθεί για να καλύψει τις τακτικές και τεχνικές που εστιάζουν στην τεχνολογία όπως οι κινητές συσκευές. Το ATT&CK είναι ένα μοντέλο συμπεριφοράς που αποτελείται από τα ακόλουθα βασικά στοιχεία:

• Τακτικές, που υποδηλώνουν βραχυπρόθεσμα, στόχους των αντιπάλων κατά τη διάρκεια μιας επίθεσης (οι στήλες).

• Τεχνικές, που περιγράφουν τα μέσα με τα οποία οι αντίπαλοι επιτυγχάνουν τους στόχους (τα επιμέρους κελιά).

• Τεκμηριωμένη χρήση αντιπαράθεσης τεχνικών και άλλων μεταδεδομένων (που συνδέονται με τεχνικές).

2.2 Ιστορικό

Το μοντέλο ATT&CK δημιουργήθηκε από την ανάγκη συστηματικής κατηγοριοποίησης της συμπεριφοράς των αντιπάλων ως μέρος της διεξαγωγής προσομοιώσεων της συμπεριφοράς των αντιπάλων στο ερευνητικό περιβάλλον του MITRE. Το MITRE, το οποίο ιδρύθηκε το 2010, παρείχε τη δυνατότητα «ζωντανού εργαστηρίου» που επέτρεψε στους ερευνητές να αναπτύξουν εργαλεία, να δοκιμάσουν και να βελτιώσουν τις ιδέες τους για τον καλύτερο εντοπισμό των απειλών. Το MITRE άρχισε να ερευνά διάφορες πηγές δεδομένων και αναλυτικές διεργασίες που θα βοηθούσαν στην ταχύτερη ανίχνευση προχωρημένων απειλών (advanced persistent threats - APTs). Διάφορες ασκήσεις υπό μορφή παιχνιδιών στον κυβερνοχώρο διεξήχθησαν σε περιοδική βάση για να μιμηθούν τους αντιπάλους και δοκιμάστηκαν αναλυτικές υποθέσεις εναντίον των συλλεγόμενων δεδομένων. Ο στόχος ήταν να βελτιωθεί η ανίχνευση των απειλών που αντιμετωπίζουν τα διάφορα δίκτυα μέσω της τηλεμετρίας και των αναλύσεων συμπεριφοράς. Για να εργαστούμε αποτελεσματικά προς την επίτευξη αυτού του στόχου, είναι χρήσιμο να κατηγοριοποιήσουμε την παρατηρούμενη συμπεριφορά σε όλες τις σχετικές ομάδες αντιπάλων πραγματικού κόσμου και να χρησιμοποιήσουμε αυτές τις πληροφορίες για να διεξάγουμε ελεγχόμενες ασκήσεις που εξομοιώνουν αυτούς τους αντιπάλους μέσα στο περιβάλλον του MITRE. Το ATT&CK χρησιμοποιείται τόσο από την ομάδα που εξομοιώνει τους αντιπάλους (για

την ανάπτυξη σεναρίων) όσο και από την ομάδα των αμυνομένων (για αναλυτική μέτρηση της προόδου). Το πρώτο μοντέλο ATT&CK δημιουργήθηκε τον Σεπτέμβριο του 2013 και επικεντρώθηκε κυρίως στο περιβάλλον των Windows. Καθορίστηκε περαιτέρω μέσα από την εσωτερική έρευνα και ανάπτυξη και στη συνέχεια δημοσιεύθηκε δημοσίως το Μάιο του 2015 με 96 τεχνικές που οργανώθηκαν κάτω από 9 τακτικές. Έκτοτε, το μοντέλο αυτό παρουσίασε τεράστια αύξηση η οποία βασίζεται και στις συνεισφορές της cybersecurity κοινότητας. Από τον Απρίλιο του 2018, το μοντέλο ATT&CK περιλαμβάνει 219 τεχνικές σε Windows, Linux και Mac.

2.3 Περιπτώσεις χρήσης του μοντέλου ATT&CK

Adversary Emulation – Η διαδικασία αξιολόγησης της ασφάλειας ενός τεχνολογικού τομέα με την εφαρμογή πληροφοριών για απειλές στον κυβερνοχώρο σχετικά με συγκεκριμένους αντιπάλους και τον τρόπο με τον οποίο λειτουργούν για να εξομοιώσουν αυτήν την απειλή. Η προσομοίωση του αντιπάλου επικεντρώνεται στην ικανότητα ενός οργανισμού να επαληθεύει την ανίχνευση ή / και τον μετριασμό της δραστηριότητας του αντιπάλου σε όλα τα ισχύοντα σημεία του κύκλου ζωής τους. Το μοντέλο ATT&CK μπορεί να χρησιμοποιηθεί ως εργαλείο για τη δημιουργία σεναρίων εξομοίωσης των αντιπάλων με σκοπό τη δοκιμή και την επαλήθευση αμυντικών τεχνικών κατά των κοινών τεχνικών των αντιπάλων. Τα προφίλ για συγκεκριμένες ομάδες αντιπάλων μπορούν να κατασκευαστούν από τις πληροφορίες που τεκμηριώνονται στο ATT&CK. Αυτά τα προφίλ μπορούν επίσης να χρησιμοποιηθούν από τους αμυνόμενους για την βελτίωση των αμυντικών μέτρων που πρέπει να εφαρμόσουν.

Red Teaming – Είναι η εφαρμογή της νοοτροπίας του αντιπάλου χωρίς τη χρήση πληροφοριών για διάφορες απειλές με σκοπό τη σχεδίαση και την διεξαγωγή μιας άσκησης. Η κόκκινη ομάδα επικεντρώνεται στην επίτευξη του τελικού στόχου μιας επιχείρησης χωρίς να εντοπιστεί, με σκοπό να επιτύχει την αποστολή και να αποδείξει τον επιχειρησιακό αντίκτυπο μιας επιτυχούς παραβίασης**.**
Το μοντέλο ATT&CK μπορεί να χρησιμοποιηθεί ως εργαλείο για τη δημιουργία του σχεδίου δράσης των αντιπάλων και για την οργάνωση των ενεργειών τους, με σκοπό την αποφυγή των οποιοδήποτε αμυντικών μέτρων που ενδέχεται να υπάρχουν σε ένα δίκτυο. Μπορεί επίσης να χρησιμοποιηθεί ως ένα ερευνητικό σχέδιο δράσης για την ανάπτυξη νέων τεχνικών οι οποίες να μην εντοπίζονται από κοινές άμυνες.

Behavioral Analytics Development – Με την υπέρβαση των παραδοσιακών γνωστών υπογραφών των κακόβουλων δραστηριοτήτων, τα αναλυτικά στοιχεία ανίχνευσης συμπεριφοράς μπορούν να χρησιμοποιηθούν για τον εντοπισμό ενδεχομένως κακόβουλων δραστηριοτήτων μέσα σε ένα σύστημα ή ένα δίκτυο που μπορεί να μην βασίζονται σε προηγούμενη γνώση των εργαλείων που χρησιμοποιούν οι αντίπαλοι. Είναι ένας τρόπος αξιοποίησης του τρόπου με τον οποίο ένας αντίπαλος αλληλοεπιδρά με μια συγκεκριμένη πλατφόρμα για τον εντοπισμό και τη σύνδεση μιας ύποπτης δραστηριότητας η οποία είναι άγνωστη ή ανεξάρτητη από συγκεκριμένα εργαλεία που μπορούν να χρησιμοποιηθούν.
Το μοντέλο ATT&CK μπορεί να χρησιμοποιηθεί ως εργαλείο για την κατασκευή και τη δοκιμή αναλύσεων σύμφωνα με την συμπεριφορά με σκοπό την ανίχνευση της συμπεριφοράς των αντιπάλων μέσα σε ένα περιβάλλον. Το Cyber Analytics

Repository (CAR) είναι ένα παράδειγμα αναλυτικής ανάπτυξης που θα μπορούσε να χρησιμοποιηθεί ως σημείο εκκίνησης για έναν οργανισμό ώστε να δημιουργήσει αναλύσεις συμπεριφοράς με βάση το μοντέλο ATT&CK.

Defensive Gap Assessment – Μια αξιολόγηση ενός αμυντικού κενού ασφαλείας επιτρέπει σε έναν οργανισμό να προσδιορίσει ποια τμήματα της επιχείρησής του στερούνται υπεράσπισης ή / και ορατότητας. Αυτά τα κενά αντιπροσωπεύουν τυφλά σημεία και ενδεχομένως μπορεί να επιτρέψουν σε έναν αντίπαλο να αποκτήσει πρόσβαση στο δίκτυο ενός οργανισμού χωρίς να είναι δυνατόν να εντοπιστεί ή να μετριαστεί.
Το ATT&CK μπορεί να χρησιμοποιηθεί ως ένα κοινό μοντέλο βασισμένο στη συμπεριφορά των αντιπάλων, για την αξιολόγηση των διαφόρων εργαλείων, παρακολούθησης και μετριασμού των υφιστάμενων αμυντικών τεχνικών στο εσωτερικό ενός οργανισμού. Τα εντοπισμένα κενά είναι χρήσιμα ως ένας τρόπος για να δοθεί προτεραιότητα στις επενδύσεις για τη βελτίωση ενός προγράμματος ασφαλείας. Παρόμοια προϊόντα ασφαλείας μπορούν επίσης να συγκριθούν με ένα κοινό μοντέλο συμπεριφοράς των αντιπάλων για τον προσδιορισμό της κάλυψης πριν από την αγορά.

SOC Maturity Assessment – Το Κέντρο Επιχειρήσεων Ασφαλείας (Security Operations Center, SOC) ενός οργανισμού αποτελεί κρίσιμη συνιστώσα πολλών μεσαίων και μεγάλων επιχειρήσεων που παρακολουθούν συνεχώς τις ενεργές απειλές κατά του δικτύου. Η κατανόηση της ωριμότητας ενός SOC είναι σημαντική για τον προσδιορισμό της αποτελεσματικότητάς του.
Το μοντέλο ATT&CK μπορεί να χρησιμοποιηθεί ως ένα μέτρο για να προσδιοριστεί πόσο αποτελεσματικό είναι το SOC στην ανίχνευση, ανάλυση και σε ποιο βαθμό ανταποκρίνεται στις εισβολές. Παρόμοια με την αξιολόγηση του αμυντικού κενού, μια αξιολόγηση του βαθμού ωριμότητας ενός SOC πρέπει να επικεντρώνεται στις διαδικασίες που χρησιμοποιεί το SOC για την ανίχνευση, την κατανόηση και την ανταπόκριση του στις μεταβαλλόμενες απειλές στο εσωτερικό του δίκτυο με την πάροδο του χρόνου.

Cyber Threat Intelligence Enrichment – Η πληροφόρηση για τις απειλές του κυβερνοχώρου καλύπτει τη γνώση των απειλών στον κυβερνοχώρο και των ομάδων απειλών που επηρεάζουν την ασφάλεια σε αυτόν. Περιλαμβάνει πληροφορίες σχετικά με κακόβουλο λογισμικό (malware), εργαλεία, Tactics, Techniques and Procedures (TTPs), καθώς επίσης συμπεριφορές και άλλες ενδείξεις που σχετίζονται με απειλές.
Το μοντέλο ATT&CK είναι χρήσιμο για την κατανόηση και την καταγραφή του προφίλ των αντίπαλων ομάδων, βασιζόμενο σε μια συμπεριφορά που είναι άγνωστη στα διάφορα εργαλεία που μπορεί να χρησιμοποιεί ένας οργανισμός. Οι αναλυτές και οι αμυνόμενοι μπορούν να κατανοήσουν καλύτερα τις κοινές συμπεριφορές σε πολλές ομάδες και με αυτό τον τρόπο μπορούν να εφαρμόσουν πιο αποτελεσματικά τις αμυντικές τους ικανότητες. Κατανοώντας πως πολλαπλές διαφορετικές ομάδες χρησιμοποιούν την ίδια τεχνική συμπεριφορά, επιτρέπει στους αναλυτές να επικεντρωθούν σε πιο αποτελεσματικές άμυνες που καλύπτουν διαφορετικούς τύπους απειλών. Η δομημένη μορφή του ATT&CK μπορεί να προσθέσει αξία στην διαδικασία αναφοράς των απειλών, κατηγοριοποιώντας τη συμπεριφορά πέραν των τυποποιημένων δεικτών.

Πολλές ομάδες μέσα στο πρότυπο ATT&CK χρησιμοποιούν τις ίδιες τεχνικές. Για το λόγο αυτό, δεν συνιστάται ο προσδιορισμός της δραστηριότητας αποκλειστικά με βάση τις τεχνικές ATT&CK που χρησιμοποιήθηκαν.

2.4 Το μοντέλο ATT&CK

Η βάση του μοντέλου ATT&CK είναι το σύνολο των μεμονωμένων τεχνικών που αντιπροσωπεύουν τις ενέργειες που οι αντίπαλοι μπορούν να εκτελέσουν για την επίτευξη των στόχων. Αυτοί οι στόχοι αντιπροσωπεύονται από τις κατηγορίες των χρησιμοποιούμενων τακτικών στις οποίες εμπίπτουν οι τεχνικές αυτές. Αυτή η σχετικά απλή αναπαράσταση πετυχαίνει μια χρήσιμη ισορροπία μεταξύ των τεχνικών λεπτομερειών στο τεχνικό επίπεδο και του πλαισίου γύρω από το γιατί συμβαίνουν ενέργειες σε επίπεδο τακτικής.

2.4.1 Ο πίνακας του μοντέλου ATT&CK

Η σχέση μεταξύ τακτικής και τεχνικών μπορεί να απεικονιστεί στο πίνακα του ATT&CK. Για παράδειγμα, κάτω από το Persistence (αυτός είναι ο στόχος του αντιπάλου - να επιμείνει στο περιβάλλον στόχο), υπάρχει μια σειρά από τεχνικές που περιλαμβάνουν π.χ. AppInit DLL, New Service και Scheduled Task. Κάθε μία από αυτές είναι μια ενιαία τεχνική που οι αντίπαλοι μπορούν να χρησιμοποιήσουν για να επιτύχουν το στόχο αυτό. Η εικόνα 1 απεικονίζει τον πίνακα του μοντέλου ATT&CK για διάφορα συστήματα.

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Automated Exfiltration	Commonly Used Port
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	BITS Jobs	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Data Compressed	Communication Through Removable Media
Hardware Additions	Command-Line Interface	AppCert DLLs	AppCert DLLs	Binary Padding	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data	Data Encrypted	Connection Proxy
Replication Through Removable Media	Control Panel Items	AppInit DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	File and Directory Discovery	Exploitation of Remote Services	Data Staged	Data Transfer Size Limits	Custom Command and Control Protocol
Spearphishing Attachment	Dynamic Data Exchange	Application Shimming	Application Shimming	CMSTP	Credentials in Files	Network Service Scanning	Logon Scripts	Data from Information Repositories	Exfiltration Over Alternative Protocol	Custom Cryptographic Protocol
Spearphishing Link	Execution through API	Authentication Package	Bypass User Account Control	Clear Command History	Credentials in Registry	Network Share Discovery	Pass the Hash	Data from Local System	Exfiltration Over Command and Control Channel	Data Encoding
Spearphishing via Service	Execution through Module Load	BITS Jobs	DLL Search Order Hijacking	Code Signing	Exploitation for Credential Access	Password Policy Discovery	Pass the Ticket	Data from Network Shared Drive	Exfiltration Over Other Network Medium	Data Obfuscation
Supply Chain Compromise	Exploitation for Client Execution	Bootkit	Dylib Hijacking	Component Firmware	Forced Authentication	Peripheral Device Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Physical Medium	Domain Fronting
Trusted Relationship	Graphical User Interface	Browser Extensions	Exploitation for Privilege Escalation	Component Object Model Hijacking	Hooking	Permission Groups Discovery	Remote File Copy	Email Collection	Scheduled Transfer	Fallback Channels
Valid Accounts	InstallUtil	Change Default File Association	Extra Window Memory Injection	Control Panel Items	Input Capture	Process Discovery	Remote Services	Input Capture		Multi-Stage Channels
	LSASS Driver	Component Firmware	File System Permissions Weakness	DCShadow	Input Prompt	Query Registry	Replication Through Removable Media	Man in the Browser		Multi-hop Proxy
	Launchctl	Component Object Model Hijacking	Hooking	DLL Search Order Hijacking	Kerberoasting	Remote System Discovery	SSH Hijacking	Screen Capture		Multiband Communication
	Local Job Scheduling	Create Account	Image File Execution Options Injection	DLL Side-Loading	Keychain	Security Software Discovery	Shared Webroot	Video Capture		Multilayer Encryption
	Mshta	DLL Search Order Hijacking	Launch Daemon	Deobfuscate/Decode Files or Information	LLMNR/NBT-NS Poisoning	System Information Discovery	Taint Shared Content			Port Knocking
	PowerShell	Dylib Hijacking	New Service	Disabling Security Tools	Network Sniffing	System Network Configuration Discovery	Third-party Software			Remote Access Tools
		External Remote		Exploitation for Defense		System Network				

Εικόνα 1 : Ο πίνακας του μοντέλου ATT&CK

2.4.2 Τεχνολογικοί τομείς του μοντέλου ATT&CK

Το μοντέλο ATT&CK είναι οργανωμένο σε μια σειρά από «τεχνολογικούς τομείς» οι οποίοι παρέχουν στον αντίπαλο ένα σύνολο περιορισμών, τους οποίους πρέπει να παρακάμψει ή να εκμεταλλευτεί, για να επιτύχει ένα σύνολο στόχων. Μέχρι σήμερα, το πρότυπο έχει καθορίσει δύο τεχνολογικούς τομείς - Enterprise (που αντιπροσωπεύουν παραδοσιακά δίκτυα επιχειρήσεων) και Mobile (για συσκευές κινητής επικοινωνίας). Σε κάθε τεχνολογικό τομέα, το ATT&CK ορίζει πολλαπλές "πλατφόρμες" δηλαδή το σύστημα που ο αντίπαλος ενεργεί. Μια πλατφόρμα μπορεί να είναι ένα λειτουργικό σύστημα ή μια εφαρμογή (π.χ. Microsoft Windows). Οι τεχνικές μπορούν να εφαρμοστούν σε πολλές πλατφόρμες. Ο Πίνακας 2 παραθέτει τις πλατφόρμες που ορίζονται σήμερα για τους τεχνολογικούς τομείς του ATT&CK. Το πεδίο εφαρμογής του μοντέλου ATT&CK επεκτείνεται πέρα από τα πεδία τεχνολογίας με το μοντέλο PRE-ATT&CK. Το PRE-ATT&CK καλύπτει την τεκμηρίωση της συμπεριφοράς των αντιπάλων κατά τη συλλογή των απαιτήσεων και την αναγνώριση πριν από την πρόσβαση σε ένα δίκτυο. Είναι ανεξάρτητο από την τεχνολογία και μοντελοποιεί τη συμπεριφορά των αντιπάλων καθώς προσπαθούν να αποκτήσουν πρόσβαση σε έναν οργανισμό ή μια οντότητα μέσω της τεχνολογίας που χρησιμοποιούν, καλύπτοντας πολλαπλούς τομείς.

Technology Domain	Platform(s) defined
Enterprise	Linux, macOS, Windows
Mobile	Android, iOS

Πίνακας 2 : Τεχνολογικοί τομείς του μοντέλου ATT&CK

2.4.3 Τι αντιπροσωπεύουν οι τακτικές του μοντέλου ATT&CK

Οι τακτικές αντιπροσωπεύουν το "γιατί" μιας τεχνικής του ATT&CK. Είναι ο τακτικός στόχος του αντιπάλου, δηλαδή ο λόγος για την εκτέλεση μιας δράσης. Οι τακτικές χρησιμεύουν ως χρήσιμες κατηγορίες για μεμονωμένες τεχνικές και καλύπτουν τις τυποποιημένες μεθόδους για τις ενέργειες που κάνουν οι αντίπαλοι κατά τη διάρκεια μιας δράσης, όπως η εμμονή, η ανακάλυψη πληροφοριών, η εκτέλεση αρχείων και η απόσπαση δεδομένων. Οι τακτικές αντιμετωπίζονται ως "ετικέτες" εντός του μοντέλου ATT&CK όπου μια τεχνική σχετίζεται ή επισημαίνεται με μία ή περισσότερες κατηγορίες τακτικής, ανάλογα με τα διαφορετικά αποτελέσματα που μπορούν να επιτευχθούν χρησιμοποιώντας μια τεχνική.
Κάθε τακτική περιέχει έναν ορισμό που περιγράφει την κατηγορία και χρησιμεύει ως οδηγός για ποιες τεχνικές πρέπει να εφαρμοστούν για την τακτική αυτή. Για παράδειγμα, Execution ορίζεται ως μια τακτική που αντιπροσωπεύει τεχνικές που οδηγούν στην εκτέλεση κώδικα ελεγχόμενου από αντίπαλο σε τοπικό ή απομακρυσμένο σύστημα. Αυτή η τακτική χρησιμοποιείται συχνά σε συνδυασμό με την αρχική πρόσβαση, ώστε να είναι δυνατή η εκτέλεση κώδικα μόλις αποκτηθεί η πρόσβαση και στην συνέχεια εσωτερική μετακίνηση (lateral movement) για την επέκταση της πρόσβασης σε απομακρυσμένα συστήματα σε ένα δίκτυο.

2.4.4 Τι αντιπροσωπεύουν οι τεχνικές του μοντέλου ATT&CK

Οι τεχνικές αντιπροσωπεύουν το "πώς" ένας αντίπαλος επιτυγχάνει έναν τακτικό στόχο με την εκτέλεση μιας δράσης. Για παράδειγμα, ένας αντίπαλος μπορεί να αποσπάσει (dump) διαπιστευτήρια για να αποκτήσει πρόσβαση σε χρήσιμα διαπιστευτήρια εντός ενός δικτύου. Οι τεχνικές μπορεί επίσης να αντιπροσωπεύουν "τι" κερδίζει ένας αντίπαλος με την εκτέλεση μιας δράσης. Αυτή είναι μια χρήσιμη διάκριση για την τακτική Discovery, καθώς οι τεχνικές επισημαίνουν τι είδους πληροφορία αποσπά ένας αντίπαλος με μια συγκεκριμένη ενέργεια. Μπορεί να υπάρχουν πολλοί τρόποι ή τεχνικές για την επίτευξη των τακτικών στόχων, έτσι υπάρχουν πολλές διαφορετικές τεχνικές σε κάθε κατηγορία τακτικής.

2.4.4.1 Δομή της τεχνικής στο μοντέλο ATT&CK

Αυτοί οι όροι αντιπροσωπεύουν τμήματα και σημαντικές πληροφορίες που περιλαμβάνονται σε κάθε τεχνικής στο μοντέλο Enterprise του ATT&CK. Τα στοιχεία επισημαίνονται με **ετικέτα** (Tag) εάν το σημείο δεδομένων είναι μια ενημερωτική αναφορά στην τεχνική που μπορεί να χρησιμοποιηθεί και με το **πεδίο** (Field) εάν το αντικείμενο είναι ένα πεδίο κειμένου που χρησιμοποιείται για την λεπτομερή περιγραφή της τεχνική. Τα στοιχεία που σημειώνονται με **relationship** υποδεικνύουν πεδία που σχετίζονται με ομάδες και με λογισμικό που χρησιμοποιείται για την τεχνική. Παρακάτω ακολουθούν όλα τα στοιχεία των δεδομένων που ορίζονται σήμερα για τις διάφορες τεχνικές στο μοντέλο ATT&CK.

Data Item	Type	Description
Name	Field	Το όνομα της τεχνικής
ID	Tag	Μοναδικό αναγνωριστικό για την τεχνική. Μορφή : T####
Tactic	Tag	Οι τακτικοί στόχοι που μπορεί να επιτευχθούν την χρήση των διαφόρων τεχνικών. Οι τεχνικές μπορούν να χρησιμοποιηθούν για την εκτέλεση μιας ή πολλαπλών τακτικών
Description	Field	Πληροφορίες σχετικά με την τεχνική, τι είναι, για πιο λόγο χρησιμοποιείται συνήθως, πώς ένας αντίπαλος μπορεί να την εκμεταλλευτεί, και παραλλαγές για το πώς θα μπορούσε να χρησιμοποιηθεί. Συμπεριλάβετε αναφορές σε έγκυρα άρθρα που περιγράφουν επιπλέον τις τεχνικές πληροφορίες που σχετίζονται με την τεχνική αυτή καθώς και με τις αναφορές χρήσης, ανάλογα με την περίπτωση
Platform	Tag	Το σύστημα στο οποίο ο αντίπαλος λειτουργεί, μπορεί να είναι λειτουργικό σύστημα ή εφαρμογή (π.χ. Microsoft Windows). Οι διάφορες τεχνικές μπορούν να εφαρμοστούν σε πολλές πλατφόρμες
System Requirements	Field	Πρόσθετες πληροφορίες σχετικά με τις απαιτήσεις που πρέπει να πληροί ο αντίπαλος ή σχετικά με την κατάσταση του συστήματος που μπορεί να απαιτηθούν για την εργασία αυτή

Data Item	Type	Description
Permissions Required	Tag	Το χαμηλότερο επίπεδο των permission του αντιπάλου οι οποίες απαιτούνται για να εκτελέσει την τεχνική σε ένα σύστημα. Απαιτείται για privilege escalation
Effective Permissions	Tag	Το επίπεδο των permission που ο αντίπαλος θα επιτύχει με την εκτέλεση της τεχνικής. Ισχύει μόνο για τις τεχνικές κάτω από την τακτική του privilege escalation. Μπορεί να έχει πολλαπλές καταχωρήσεις εάν διαφορετικά permission μπορούν να ρυθμιστούν όταν εκτελείται τεχνική
Data Source	Tag	Πηγή πληροφοριών οι οποίες συλλέγονται από ένα αισθητήρα ή ένα σύστημα καταγραφής το οποίο μπορεί να χρησιμοποιηθεί για τη συλλογή πληροφοριών σχετικών με την αναγνώριση της ενέργειας που εκτελείται, της αλληλουχίας των ενεργειών ή των αποτελεσμάτων αυτών των ενεργειών από έναν αντίπαλο. Ο κατάλογος των πηγών δεδομένων μπορεί να ενσωματώνει διαφορετικές παραλλαγές του τρόπου με τον οποίο θα μπορούσε να εκτελεστεί η ενέργεια για μια συγκεκριμένη τεχνική. Αυτό το χαρακτηριστικό προορίζεται να περιορίζεται σε μια καθορισμένη λίστα, ώστε να επιτρέπεται η ανάλυση της τεχνικής κάλυψης βάσει μοναδικών πηγών δεδομένων. (Για παράδειγμα, "ποιες τεχνικές μπορώ να ανιχνεύσω εάν χρησιμοποιώ μια διαδικασία monitoring;")
Supports Remote	Tag	Εάν η τεχνική μπορεί να χρησιμοποιηθεί για να εκτελέσει κάτι σε ένα απομακρυσμένο σύστημα. Ισχύει μόνο για τεχνικές εκτέλεσης
Defense Bypassed	Tag	Εάν η τεχνική μπορεί να χρησιμοποιηθεί για να παρακάμψει ή να αποφύγει ένα συγκεκριμένο αμυντικό εργαλείο, μεθοδολογία ή διαδικασία. Ισχύει μόνο για τις τεχνικές defense evasion
CAPEC ID	Field	Υπερσύνδεση με τη σχετική καταχώρηση του CAPEC (Common Attack Pattern Enumeration and Classification) στον ιστότοπό του
Contributor	Tag	Κατάλογος συντελεστών που δεν συνεργάζονται με το MITRE (ιδιώτες ή / και οργανισμοί) που έχουν προσφέρει πληροφορίες ή έχουν υποστηρίξει την ανάπτυξη μια τεχνικής
Examples	Relationship / Field	Τα πεδία των παραδειγμάτων συμπληρώνονται σε μια τεχνική, όταν μια ομάδα ή μια οντότητα λογισμικού συσχετίζεται με μια τεχνική μέσω τεκμηριωμένης χρήσης. Περιγράφουν την ομάδα ή το λογισμικό με μια σύντομη περιγραφή του τρόπου με τον οποίο χρησιμοποιείται η τεχνική. Το παράδειγμα του τρόπου με τον οποίο ένας συγκεκριμένος αντίπαλος χρησιμοποιεί μια τεχνική

Data Item	Type	Description
		είναι μια άμεση αναφορά στις διαδικασίες που χρησιμοποιεί ή ένας ακριβής τρόπος με τον οποίο εκτελείται μια τεχνική σε ένα σύστημα
Detection	Field	Αναλυτική διαδικασία υψηλού επιπέδου, από αισθητήρες, δεδομένα και στρατηγικές ανίχνευσης που μπορεί να είναι χρήσιμες για τον εντοπισμό μιας τεχνικής η οποία έχει χρησιμοποιηθεί από έναν αντίπαλο. Αυτή η ενότητα έχει σκοπό να ενημερώσει αυτούς τους οποίους είναι υπεύθυνοι για την ανίχνευση της συμπεριφοράς των αντιπάλων (όπως οι αμυνόμενοι ενός δικτύου), ώστε να μπορούν να αναλάβουν δράση. Πρέπει να υπάρχουν αρκετές πληροφορίες και αναφορές που να δείχνουν χρήσιμες αμυντικές μεθοδολογίες. Θα μπορούσαν να υπάρχουν πολλοί τρόποι ανίχνευσης μιας τεχνικής, αλλά το μοντέλο ATT&CK και η MITRE δεν υποστηρίζουν καμία συγκεκριμένη εγγυημένη λύση. Συνεπώς, οι συστάσεις ανίχνευσης θα πρέπει να παραμείνουν άγνωστες, συνιστώντας μια πιο γενική μέθοδο και κατηγορία εργαλείων και όχι ένα μόνο συγκεκριμένο εργαλείο. Η ανίχνευση μπορεί να μην είναι πάντοτε δυνατή για μια συγκεκριμένη τεχνική και πρέπει να τεκμηριώνεται ως τέτοια
Mitigation	Field	Οι παράμετροι του συστήματος, τα εργαλεία ή οι διαδικασίες που εμποδίζουν μια τεχνική να λειτουργήσει ή να μην έχει το επιθυμητό αποτέλεσμα για έναν αντίπαλο. Σκοπός του παρόντος τμήματος είναι να ενημερώσει τους υπευθύνους για τον μετριασμό των αντιπάλων (όπως αμυνόμενοι ενός δικτύων ή οι υπεύθυνοι χάραξης πολιτικής ασφαλείας) για να τους επιτρέψουν να αναλάβουν δράση είτε με την αλλαγή πολιτικής ή η την ανάπτυξη κάποιου εργαλείου. Ο μετριασμός μπορεί να μην είναι πάντοτε εφικτός για μια συγκεκριμένη τεχνική και πρέπει να τεκμηριώνεται ως τέτοιος

Πίνακας 3 : Η δομή της τεχνικής του μοντέλου ATT&CK

2.4.5 Ομάδες του μοντέλου ATT&CK

Οι γνωστοί αντίπαλοι που παρακολουθούνται από δημόσιους και ιδιωτικούς οργανισμούς και αναφέρονται στις αναφορές πληροφοριών για απειλές παρακολουθούνται μέσα στο μοντέλο ATT&CK στο αντικείμενο του Group. Τα Group ορίζονται ως ονόματα από μια σειρά εισβολέων, ομάδες απειλών, ομάδες φορέων που τυπικά αντιπροσωπεύουν στοχοθετημένη, επίμονη δραστηριότητα απειλής. Το μοντέλο ATT&CK επικεντρώνεται κυρίως στις ομάδες APT (Advanced Persistent Threat Groups) αν και μπορεί να περιλαμβάνει και άλλες προηγμένες

ομάδες, όπως είναι οι οικονομικά παρακινημένες. Οι ομάδες μπορούν να χρησιμοποιούν τεχνικές απευθείας ή να χρησιμοποιούν λογισμικό που εφαρμόζει τεχνικές.

2.4.5.1 Δομή των ομάδων του μοντέλου ATT&CK

Τα στοιχεία επισημαίνονται με **tag** εάν το σημείο δεδομένων είναι μια ενημερωτική αναφορά στο Group που μπορεί να χρησιμοποιηθεί και **field** εάν το αντικείμενο είναι ένα πεδίο κειμένου που χρησιμοποιείται για την λεπτομερή περιγραφή της τεχνικής. Τα στοιχεία που σημειώνονται με **relationship** υποδεικνύουν πεδία που σχετίζονται με ομάδες και με λογισμικό που χρησιμοποιείται για την τεχνική.

Data Item	Type	Description
Name	Field	Το όνομα της ομάδας του αντιπάλου
ID	Tag	Μοναδικό αναγνωριστικό για την τεχνική. Μορφή : G####
Aliases	Tag	Εναλλακτικά ονόματα που αναφέρονται στην ίδια ομάδα αντιπάλων στην αναφορά πληροφοριών για απειλές
Description	Field	Περιγραφή της ομάδας σύμφωνα με τις δημόσια γνωστές αναφορές απειλών. Μπορεί να περιέχει ημερομηνίες δραστηριότητας, ύποπτες δραστηριότητες, στοχευμένες βιομηχανίες και αξιοσημεί-ωτα γεγονότα που αποδίδονται στις δραστηριότητες της ομάδας
Alias Descriptions	Field	Τμήμα που μπορεί να χρησιμοποιηθεί για να περιγράψει ψευδώνυμα ομάδων βασισμένο σε αναφορές που χρησιμοποιούνται για να συνδέσουν το ψευδώνυμο με το όνομα της ομάδας
Techniques Used	Relationship / Field	Κατάλογος τεχνικών που χρησιμοποιούνται από την ομάδα με ένα πεδίο το οποίο περιγράψει λεπτομέρειες σχετικά με τον τρόπο με τον οποίο χρησιμοποιείται η τεχνική. Αυτό αντιπροσωπεύει τη διαδικασία της ομάδας (στο πλαίσιο των TTP) για τη χρήση μιας τεχνικής. Κάθε τεχνική πρέπει να περιλαμβάνει μια αναφορά
Software	Relationship / Field	Λίστα λογισμικού που έχει αναφερθεί ότι η ομάδα χρησιμοποιεί με ένα πεδίο το οποίο περιγράψει λεπτομέρειες σχετικά με τον τρόπο χρήσης του λογισμικού

Πίνακας 4 : Η δομή των ομάδων στο μοντέλο ATT&CK

2.4.6 Λογισμικό που χρησιμοποιείται από το μοντέλο ATT&CK

Οι αντίπαλοι συνήθως χρησιμοποιούν διαφορετικούς τύπους λογισμικού κατά τη διάρκεια των επιθέσεων τους. Το λογισμικό μπορεί να προσδιορίζει μια τεχνική, οπότε είναι επίσης απαραίτητο να κατηγοριοποιηθεί μέσα στο μοντέλο ATT&CK, για παραδείγμα σχετικά με τον τρόπο με τον οποίο χρησιμοποιούνται οι τεχνικές. Το

λογισμικό χωρίζεται σε τρεις κατηγορίες υψηλού επιπέδου: εργαλεία (tools), βοηθητικά προγράμματα (utilities) και κακόβουλο λογισμικό(malware).

• **Tool -** Εμπορικό, λογισμικό ανοιχτού κώδικα ή διαθέσιμο στο κοινό, το οποίο θα μπορούσε να χρησιμοποιηθεί από έναν αμυνόμενο, από έναν pentester, έναν red teamer ή έναν αντίπαλο για κακόβουλους σκοπούς που γενικά δεν βρίσκεται σε ένα σύστημα. Παραδείγματα τέτοιων εργαλείων είναι PsExec, Metasploit, Mimikatz, κ.λπ.

• **Utility -** Λογισμικό γενικά διαθέσιμο ως μέρος ενός λειτουργικού συστήματος που είναι πιθανό να υπάρχει ήδη σε ένα περιβάλλον. Οι αντίπαλοι τείνουν να αξιοποιούν υπάρχων utilities στα συστήματα για τη συλλογή πληροφοριών και την εκτέλεση ενεργειών. Παραδείγματα τέτοιων προγραμμάτων των Windows είναι Net, netstat, Tasklist κ.λπ.

• **Malware –** Εμπορικό λογισμικό, κλειστού ή ανοιχτού κώδικα που προορίζεται για κακόβουλη χρήση από τους αντιπάλους. Παραδείγματα περιλαμβάνουν τα PlugX, CHOPSTICK κ.λπ.
Οι κατηγορίες λογισμικού θα μπορούσαν να αναλυθούν περαιτέρω, αλλά η ιδέα πίσω από την τρέχουσα κατηγοριοποίηση ήταν να δείξει πώς οι αντίπαλοι χρησιμοποιούν τα βοηθητικά προγράμματα και το νόμιμο λογισμικό για να εκτελούν ενέργειες παρόμοιες με τις παραδοσιακές κακόβουλες εφαρμογές.

2.4.6.1 Δομή του λογισμικού στο μοντέλο ATT&CK

Τα στοιχεία επισημαίνονται με **tag** εάν το σημείο δεδομένων είναι μια ενημερωτική αναφορά στο λογισμικό που μπορεί να χρησιμοποιηθεί και **field** εάν το στοιχείο είναι ένα πεδίο ελεύθερου κειμένου που χρησιμοποιείται για την λεπτομερή περιγραφή της τεχνικής. Τα στοιχεία που σημειώνονται με τη **relationship** υποδεικνύουν πεδία που σχετίζονται με τις σχέσεις της τεχνικής που χρησιμοποιείται με τις ομάδες.

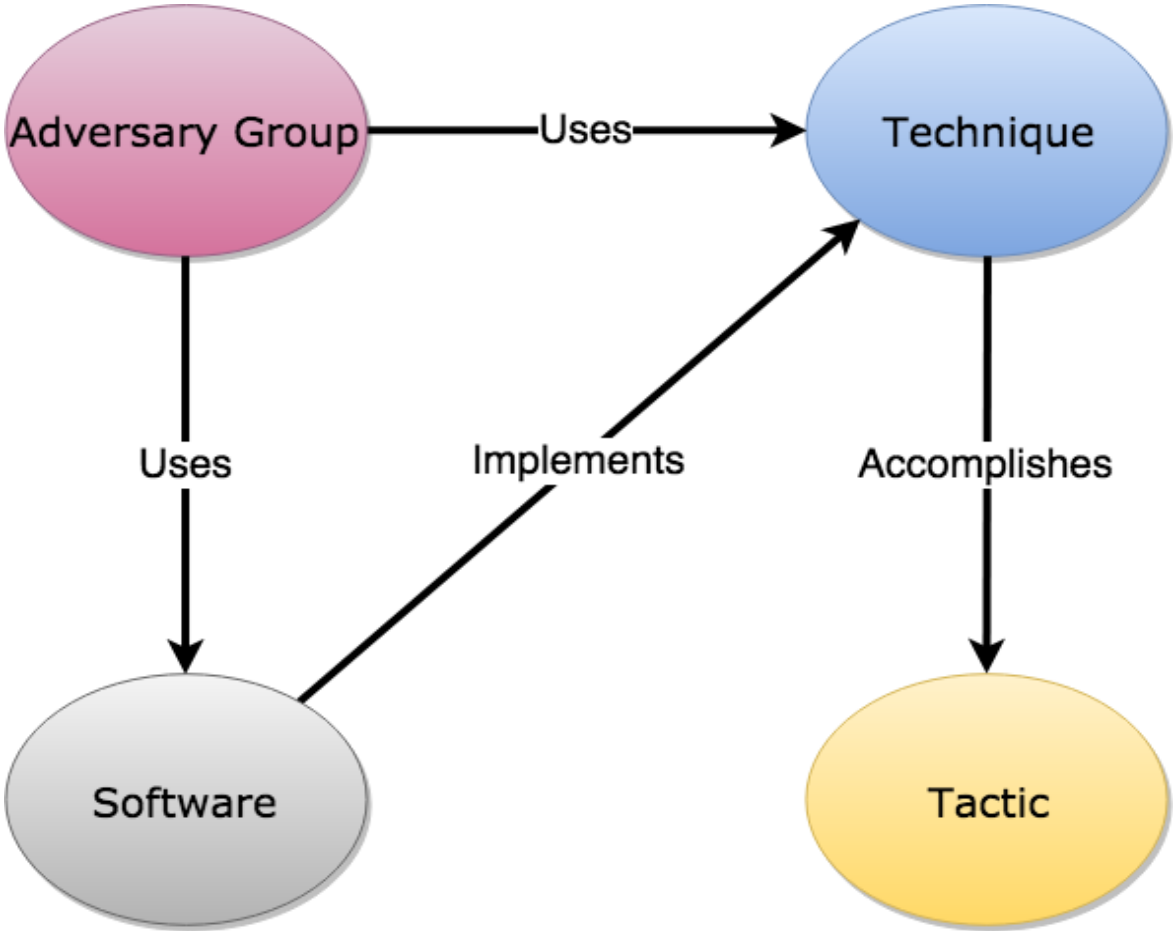
Data Item	Type	Description
Name	Field	Το όνομα του λογισμικού
ID	Tag	Μοναδικό αναγνωριστικό για την τεχνική. Μορφή : S####
Aliases	Tag	Εναλλακτικά ονόματα που αναφέρονται στο ίδιο λειτουργικό στην αναφορά πληροφοριών για απειλές
Type	Tag	Ο τύπος του λογισμικού που χρησιμοποιείται για την τεχνική : malware, tool, utility
Platform	Tag	Η πλατφόρμα πάνω στην οποία μπορεί να χρησιμοποιηθεί το λογισμικό π.χ. Windows, Linux, κ.λπ.
Description	Field	Περιγραφή του λογισμικού που βασίζεται σε τεχνικές αναφορές ή δημόσια αναφορά απειλών. Μπορεί να περιέχει δεσμούς με ομάδες που είναι γνωστό ότι χρησιμοποιούν το λογισμικό ή άλλες τεχνικές λεπτομέρειες με κατάλληλες αναφορές

Data Item	Type	Description
Alias Descriptions	Field	Τμήμα που μπορεί να χρησιμοποιηθεί για να περιγράψει τα ψευδώνυμα του λογισμικού με αναφορές στην αναφορά που χρησιμοποιείται για τη σύνδεση του ψευδωνύμου με το όνομα της ομάδας
Techniques Used	Relationship / Field	Κατάλογος των τεχνικών που εφαρμόζονται από το λογισμικό συνοδευόμενο με ένα πεδίο που περιγράφει λεπτομέρειες σχετικά με τον τρόπο με τον οποίο υλοποιείται ή χρησιμοποιείται η τεχνική. Κάθε τεχνική πρέπει να περιλαμβάνει μια αναφορά
Groups	Relationship / Field	Κατάλογος ομάδων για τις οποίες έχει αναφερθεί ότι το λογισμικό έχει χρησιμοποιηθεί συνοδευόμενο με ένα πεδίο που περιγράφει λεπτομέρειες σχετικά με τον τρόπο χρήσης του λογισμικού

Πίνακας 5 : Η δομή του λογισμικού στο μοντέλο ATT&CK

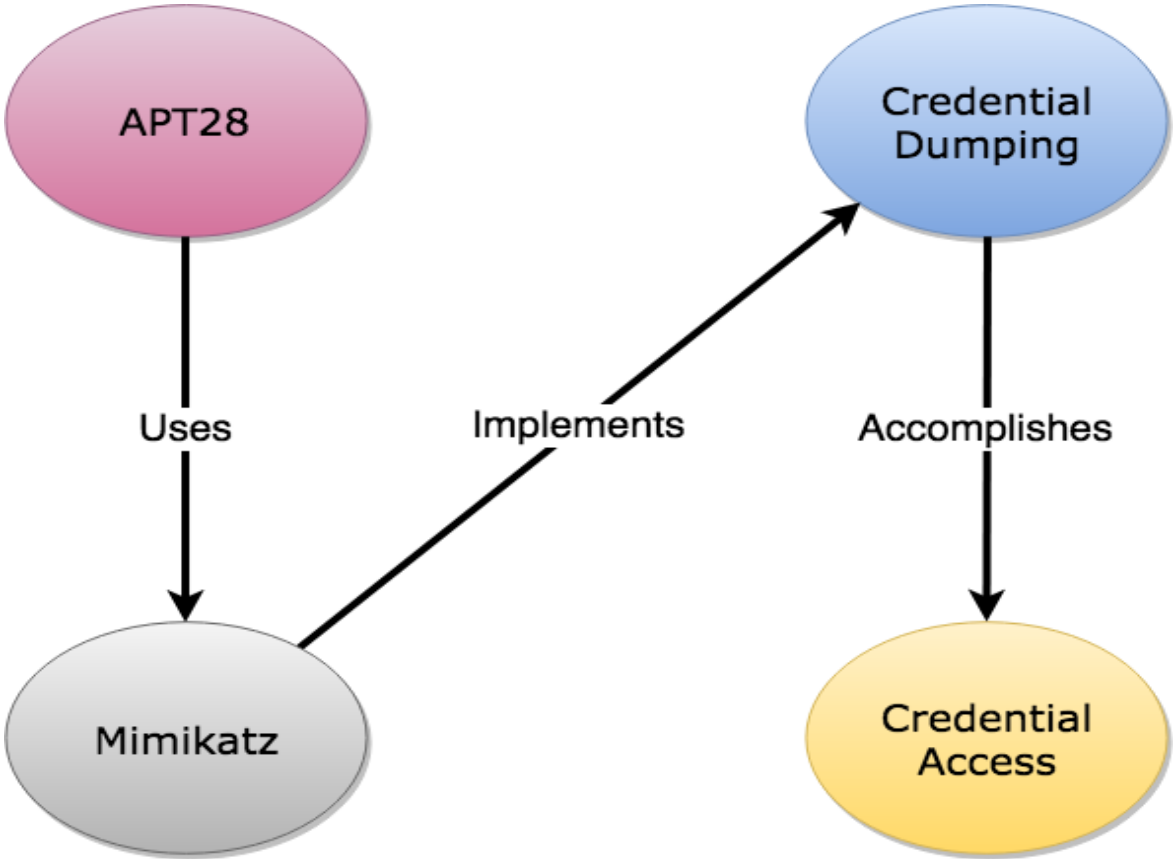
2.4.7 Σχέσεις μεταξύ των αντικειμένων στο μοντέλο ATT&CK

Κάθε συστατικό υψηλού επιπέδου του μοντέλου ATT&CK σχετίζεται με άλλα στοιχεία με κάποιο τρόπο. Οι σχέσεις που περιγράφονται στα πεδία περιγραφής στην προηγούμενη ενότητα μπορούν να απεικονιστούν στο παρακάτω διάγραμμα:



Εικόνα 2 : Σχέσεις μεταξύ των αντικειμένων στο μοντέλο ATT&CK

Ένα παράδειγμα που εφαρμόζεται σε μια συγκεκριμένη persistent threat ομάδα, όπου το APT28 χρησιμοποιεί το Mimikatz για credential dumping:



Εικόνα 3 : Σχέσεις μεταξύ των αντικειμένων στο μοντέλο ATT&CK (Παράδειγμα)

2.5 Μεθοδολογία στο μοντέλο ATT&CK

Οι προηγούμενες παραγράφους περιγράφουν και καθορίζουν τον σκοπό του μοντέλου ATT&CK. Σε αυτή την ενότητα θα περιγράψουμε την μεθοδολογία που χρησιμοποιείται για τη δημιουργία και τη συντήρηση του μοντέλου αυτού. Περιγράφεται επίσης τη διαδικασία που συνιστάται για να προσδιοριστεί εάν και πότε πρέπει να προστεθούν νέες τεχνικές στο μοντέλο και πώς χρησιμοποιείται η απειλή για τη διαμόρφωση των προφίλ της ομάδας και του λογισμικού της τεχνικής. Οι πληροφορίες εντός του μοντέλου ATT&CK έχουν εξελιχθεί με την πάροδο του χρόνου, όπως επίσης και οι εκτιμήσεις που χρησιμοποιούνται για το ποιες πληροφορίες συμπεριλαμβάνονται και πώς είναι αυτές δομημένες. Η διαδικασία παραμένει επικεντρωμένη σε μια ακριβή αναπαράσταση του τρόπου με τον οποίο οι αντίπαλοι διεξάγουν τις επιχειρήσεις με έναν τρόπο που είναι εύκολο να κατηγοριοποιήσουμε τις ενέργειες που εκτελούν και να συνδέσουμε αυτές τις ενέργειες με αισθητήρες, τους παραμέτρους των συστημάτων (system configurations) και τα αντίμετρα τα οποία οι αμυνόμενοι μπορούν να χρησιμοποιήσουν για την ανίχνευση και / ή τη διακοπή αυτών των ενεργειών.

2.5.1 Φιλοσοφία του μοντέλου ATT&CK

Υπάρχουν τρεις εννοιολογικές ιδέες που είναι βασικές για τη φιλοσοφία του μοντέλου ATT&CK:

- Διατηρεί την οπτική του αντιπάλου.

- Ακολουθεί τις δραστηριότητες όπως στον πραγματικό κόσμο χρησιμοποιώντας εμπειρικά παραδείγματα.

- Το επίπεδο της χρήσης των αφηρημένων εννοιών είναι κατάλληλο για τη γεφύρωση της επιθετικής δράσης με πιθανά αντίμετρα.

2.5.1.1 Η οπτική του επιτιθέμενου

Το μοντέλο ATT&CK χρησιμοποιεί την οπτική ενός αντιπάλου στην ορολογία και τις περιγραφές για τις τακτικές και τις τεχνικές που περιγράφονται στο μοντέλο. Αντιθέτως, τα πιο πολλά μοντέλα ασφαλείας περιγράφουν την επιθυμητή ασφάλεια από την πλευρά του αμυνόμενου χρησιμοποιώντας μια προσέγγιση από πάνω προς τα κάτω. Η χρήση της οπτικής ενός αντιπάλου, στο μοντέλο ATT&CK διευκολύνει περισσότερο την κατανόηση των ενεργειών και των πιθανών αντιμέτρων που χρειάζονται να υλοποιηθούν, από το αν κοιτάγαμε μόνο την πλευρά του αμυνομένου. Η χρήση της οπτικής αυτής αλλάζει την ερώτηση από αυτό που θα μπορούσε να συμβεί βάσει ενός καταλόγου διαθέσιμων πόρων σε αυτό που θα μπορούσε να συμβεί με ένα γενικό πλαίσιο για την σύνδεση μιας αμυντικής στρατηγικής με την στρατηγική («κόλπα») που ακολουθεί ο αντίπαλος. Εν μέρει, το μοντέλο ATT&CK παρέχει ένα πιο ακριβές πλαίσιο αναφοράς για τον τρόπο προσέγγισης της εκτίμησης της αμυντικής κάλυψης. Εκφράζει τις σχέσεις και τις εξαρτήσεις μεταξύ των ενεργειών του αντιπάλου και των πληροφοριών με τέτοιο τρόπο που είναι άγνωστος για οποιοδήποτε συγκεκριμένο αμυντικό εργαλείο ή μέθοδο συλλογής δεδομένων. Οι αμυνόμενοι είναι στη συνέχεια σε θέση να ακολουθήσουν το κίνητρο του αντιπάλου για μεμονωμένες ενέργειες και να κατανοήσουν πώς οι ενέργειες αυτές σχετίζονται με συγκεκριμένες κατηγορίες αμυνών που μπορούν να αναπτυχθούν σε ένα περιβάλλον.

2.5.1.2 Εμπειρική χρήση

Η δραστηριότητα που περιγράφεται από το μοντέλο ATT&CK προέρχεται σε μεγάλο βαθμό από δημοσιευμένα περιστατικά σχετικά με την ύποπτη δραστηριότητα των αντιπάλων, η οποία παρέχει γνώσεις έτσι ώστε να απεικονίζεται με ακρίβεια η δραστηριότητα που συμβαίνει ή ενδέχεται να συμβεί στο πραγματικό περιβάλλον. Η σύνδεση με τις δραστηριότητες αυτές διατηρεί το μοντέλο ενημερωμένο σε αληθινές απειλές που είναι πιθανόν να συμβούν και όχι θεωρητικές τεχνικές που είναι απίθανο να επιτευχθούν.

2.5.1.2.1 Πηγές Πληροφοριών

Νέες πληροφορίες σχετικά με τις τεχνικές του μοντέλου ATT&CK μπορούν να προέρχονται από πολλές διαφορετικές πηγές. Αυτές οι πηγές είναι δυνατόν να προέρχονται από :

- Αναφορές πληροφοριών απειλών (Threat intelligence reports)

- Παρουσιάσεις συνεδρίων

- Μέσα κοινωνικής δικτύωσης

- Blogs
- Αποθετήρια ανοιχτού κώδικα
- Δείγματα κακόβουλου λογισμικού

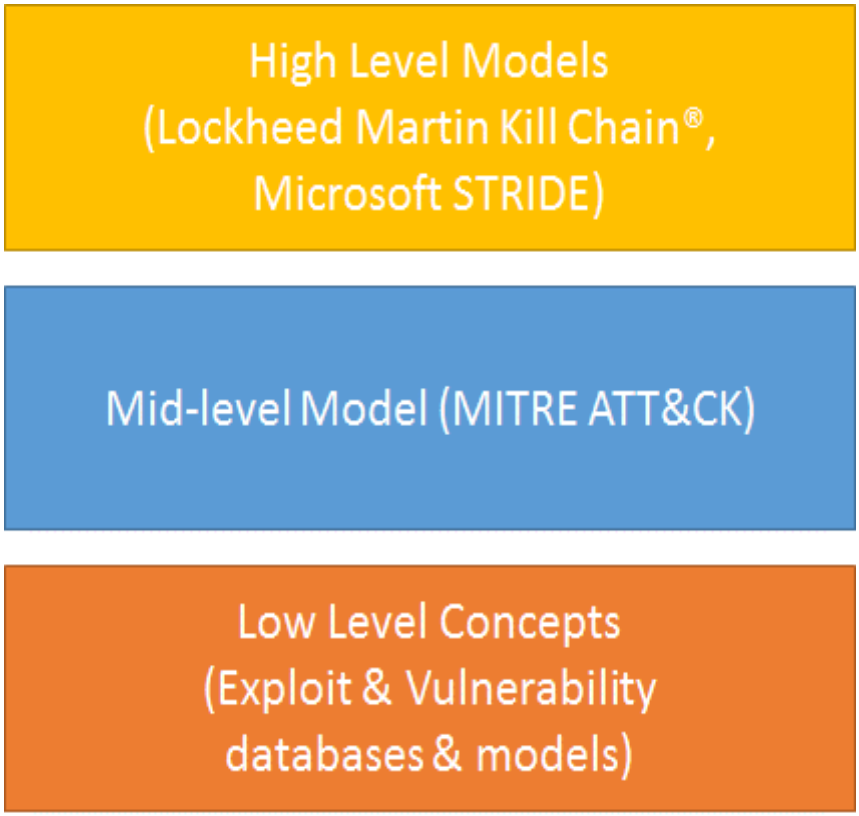
2.5.1.2.2 Μη δημοσιευμένα περιστατικά ασφαλείας

Η μεγάλη πλειονότητα των περιστατικών που ανακαλύφθηκαν δεν αναφέρονται δημοσίως. Μη ή ανεπαρκώς αναφερόμενα συμβάντα μπορούν να περιέχουν πολύτιμες πληροφορίες σχετικά με τον τρόπο συμπεριφοράς των αντιπάλων και την εμπλοκή τους σε διάφορες ενέργειες. Συχνά, οι χρησιμοποιούμενες τεχνικές μπορούν να βοηθήσουν στην αποκάλυψη νέων τεχνικών καθώς και παραλλαγών αυτών, όπως επίσης και στη δημιουργία στατιστικών στοιχείων που δείχνουν μια εκτίμηση όσον αφορά την συχνότητα της χρήσης αυτών των τεχνικών. Αυτός ο τύπος έμμεσων ενδείξεων χρήσης είναι πολύτιμος και λαμβάνεται υπόψη ως δεδομένα σχετικά με την εμπειρική χρήση κατά την προσθήκη νέων πληροφοριών στο μοντέλο ATT&CK.

2.5.1.3 Τα διάφορα επίπεδα των μοντέλων

Το επίπεδο των αφηρημένων τακτικών και τεχνικών που εφαρμόζουν οι αντίπαλοι μέσα στο ATT&CK είναι μια σημαντική διαφορά μεταξύ αυτού του μοντέλου και των άλλων υπαρχόντων παρόμοιων μοντέλων απειλής. Τα διάφορα μοντέλα υψηλού επιπέδου, είναι χρήσιμα στην κατανόηση των διαδικασιών υψηλού επιπέδου και των στόχων των αντιπάλων. Εντούτοις, αυτά τα μοντέλα δεν είναι αποτελεσματικά για να δείξουν ποια είναι τα αποτελέσματα των μεμονωμένων ενεργειών των αντιπάλων, πώς μια δράση σχετίζεται με μια άλλη, πώς διάφορες αλληλουχίες ενεργειών σχετίζονται με αντικειμενικούς σκοπούς των αντιπάλων και πώς οι διάφορες ενέργειες συσχετίζονται με αμυντικές τεχνικές και άλλα αντίμετρα που χρησιμοποιούνται για την ασφάλεια μιας πλατφόρμας και ενός domain.
Αντίθετα, οι βάσεις δεδομένων και τα διάφορα μοντέλα περιγράφουν συγκεκριμένες περιπτώσεις λογισμικού που χρησιμοποιείται, οι οποίες είναι συχνά διαθέσιμες για χρήση με παραδείγματα κώδικα, αλλά απέχουν πολύ από τις συνθήκες στις οποίες θα μπορούσαν ή θα έπρεπε να χρησιμοποιηθούν καθώς επίσης και από τη δυσκολία χρήσης τους. Παρομοίως, υπάρχουν επίσης βάσεις δεδομένων κακόβουλων προγραμμάτων, αλλά συνήθως δεν υπάρχει πλαίσιο σχετικά με το πώς χρησιμοποιείται το κακόβουλο αυτό λογισμικό και από ποιον. Δεν λαμβάνουν επίσης υπόψη πως κάποιο νόμιμο λογισμικό μπορεί να χρησιμοποιηθεί για κακόβουλους σκοπούς.
Ένα μοντέλο αντιπάλων μεσαίου επιπέδου (mid-level) όπως το ATT&CK είναι απαραίτητο για τη σύνδεση αυτών των διαφόρων συνιστωσών. Οι τακτικές και οι τεχνικές στο μοντέλο ATT&CK ορίζουν τις συμπεριφορές των αντιπάλων σε τέτοιο βαθμό όπου μπορούν να σχεδιαστούν πιο αποτελεσματικά οι διάφορες αμυντικές τεχνικές. Οι έννοιες υψηλού επιπέδου, όπως ο Έλεγχος (Control), η Εκτέλεση(Execute) και η Διατήρηση (Maintain), αναλύονται περαιτέρω σε πιο περιγραφικές κατηγορίες, στις οποίες μπορούν να οριστούν και να κατηγοριοποιηθούν μεμονωμένες ενέργειες σε ένα σύστημα. Ένα μοντέλο μεσαίου επιπέδου είναι επίσης χρήσιμο για την ενσωμάτωση των εννοιών του κατώτερου

επιπέδου. Τα exploits και το κακόβουλο λογισμικό (malware) είναι χρήσιμα σε έναν αντίπαλο, αλλά για να κατανοήσουμε πλήρως τη χρησιμότητά τους, είναι απαραίτητο να κατανοήσουμε το πλαίσιο εντός του οποίου μπορούν να χρησιμοποιηθούν για την επίτευξη ενός στόχου. Το μοντέλο μεσαίου επιπέδου είναι επίσης ένα χρήσιμο εργαλείο που συνδέει τα στοιχεία της απειλής και των περιστατικών για να δείξει ποιος κάνει τι καθώς και τα αποτελέσματα από την επικράτηση της χρήσης μιας συγκεκριμένης τεχνικής. Η εικόνα 4 δείχνει μια σύγκριση του αφηρημένου επιπέδου μεταξύ μοντέλων υψηλού, μεσαίου και χαμηλού επιπέδου και βάσεων γνώσεων απειλών:



Εικόνα 4 : Τα επίπεδα των μοντέλων

2.5.2 Τακτικές στο μοντέλο ATT&CK

Δεδομένου ότι οι τακτικές αντιπροσωπεύουν τους τακτικούς στόχους ενός αντιπάλου, αυτές παραμένουν σχετικά στατικές με την πάροδο του χρόνου, επειδή οι στόχοι των αντιπάλων είναι απίθανο να αλλάξουν. Οι τακτικές αντιπροσωπεύουν το τι προσπαθεί να επιτύχει ο αντίπαλος ανάλογα με την πλατφόρμα και τον τομέα στον οποίο δραστηριοποιείται. Συχνά, αυτοί οι στόχοι είναι παρόμοιοι σε όλες τις πλατφόρμες, για το λόγο αυτό και οι τακτικές του μοντέλου ATT&CK μπορούν να εφαρμοστούν σε όλα τα λειτουργικά συστήματα (Windows, MacOS και Linux). Στα σημεία στα οποία διαφέρουν είναι εκείνα όπου οι στόχοι των αντιπάλων και οι τεχνολογίες των διάφορων πλατφόρμων ή τομέων διαφέρουν. Μπορεί να υπάρχουν περιπτώσεις όπου οι τακτικές πρέπει να αναλυθούν παραπάνω για τον καλύτερο ορισμό των ενεργειών που συμβαίνουν. Στην αρχική του μορφή το μοντέλο ATT&CK για Επιχειρήσεις, η Τακτική Collection για το λειτουργικό σύστημα των Windows δεν υπήρχε, αλλά είχε συμπεριληφθεί ως τμήμα της τακτικής Exfiltration. Αυτή η

αντιπροσώπευση ταίριαζε επαρκώς για εκείνη την εποχή, καθώς θεωρήθηκε σε μεγάλο βαθμό ως μία ενέργεια κατά την οποία ένας αντίπαλος αποσπάει πληροφορίες αλλά δεν αντιπροσώπευε με ακρίβεια τα ξεχωριστά κίνητρα και τις ενέργειες που είναι απαραίτητες για την επιτυχή απόσπαση αυτών των πληροφοριών. Από πού προέρχονται τα δεδομένα αυτά καθώς επίσης και πώς αποκτώνται είναι εξίσου σημαντικά όπως επίσης και πως ένας αντίπαλος απομακρύνει τα δεδομένα από ένα περιβάλλον. Υπάρχει επίσης μια χρονική διαφορά μεταξύ του πότε ένας αντίπαλος μπορεί να συλλέξει τις πληροφορίες και πότε μπορεί να τις αποσπάσει. Έτσι, αποφασίστηκε στο μοντέλο σε νεότερη έκδοση του να σπάσει αυτή η τακτική σε δύο και να περιγραφεί ξεχωριστά η Συλλογή (Collection).

2.5.3 Τεχνικές στο μοντέλο ATT&CK

Οι τεχνικές αποτελούν τα θεμέλια του μοντέλου ATT&CK και αντιπροσωπεύουν τις μεμονωμένες ενέργειες που κάνουν οι αντίπαλοι ή τις πληροφορίες που ο αντίπαλος μαθαίνει κάνοντας μια ενέργεια.

2.5.3.1 Πως δημιουργείται μια τεχνική

Υπάρχουν διάφοροι παράγοντες σε μια τεχνική εντός του μοντέλου ATT&CK. Όλοι οι παράγοντες ζυγίζονται κατά τη διαδικασία λήψης αποφάσεων για να δημιουργηθεί μια τεχνική και με τον τρόπο αυτό να συμβάλουν στη συλλογή πληροφοριών που αντιπροσωπεύει αυτή η τεχνική με σκοπό τη δημιουργία μιας βάσης με αυτές τις πληροφορίες.

2.5.3.1.1 Ονομασία

Τα ονόματα των Τεχνικών επικεντρώνονται στο χαρακτηριστικό της τεχνικής που την καθιστά μοναδική, δηλαδή σε αυτό που ο αντίπαλος επιτυγχάνει με την χρήση αυτής της τεχνικής. Ένα παράδειγμα είναι αυτό της τεχνικής Credential Dumping για την τακτική Credential Access, όπου η τεχνική αυτή είναι μια μέθοδος απόκτησης πρόσβασης σε νέα διαπιστευτήρια τα οποία μπορούν να αποκτηθούν με διάφορους τρόπους. Ένα ακόμα παράδειγμα (ίδια τεχνική για διαφορετικές τακτικές) είναι το Rundll32, το οποίο αντιπροσωπεύει μια τεχνική που μπορεί να χρησιμοποιηθεί σε περισσότερες από μία τακτικές όπως Execution και Defense Evasion. Η ορολογία που είναι αποδεκτή για τις διάφορες τεχνικές τείνει να χρησιμοποιείται εάν έχει ήδη καθιερωθεί και τεκμηριωθεί μέσω παρουσιάσεων σε διάφορα συνέδρια, σε δημοσιεύσεις σε διάφορα blogs, σε άλλα άρθρα κ.λπ.

2.5.3.1.2 Τύποι των τεχνικών στο μοντέλο του ATT&CK

Οι τεχνικές γενικά εμπίπτουν σε τρία επίπεδα αφαιρετικότητας:

1. Γενικές τεχνικές που εφαρμόζονται σε πολλαπλές πλατφόρμες με γενικό τρόπο (π.χ. Obfuscated Files and Information).

2. Γενικές τεχνικές που εφαρμόζονται σε πολλαπλές πλατφόρμες με συγκεκριμένους τρόπους (π.χ. Process Injection).

3. Ειδικές τεχνικές που ισχύουν μόνο για μια πλατφόρμα (π.χ. Rundll32)

Για το πρώτο επίπεδο, ξεφεύγοντας από τον τρόπο με τον οποίο εφαρμόζεται αυτή η τεχνική σε πολλαπλές πλατφόρμες, επειδή η τεχνική περιγράφει μια γενική άγνωστη συμπεριφορά, όπως ένα μεγάλο μέρος της τακτικής Command and Control. Η γενική περιγραφή και οι λεπτομέρειες παρέχονται με παραπομπές σε παραδείγματα από τις διάφορες πλατφόρμες ανάλογα με τις ανάγκες.

Οι τεχνικές που μπορούν να εκτελεσθούν με διαφορετικούς τρόπους για να επιτευχθούν τα ίδια ή παρόμοια αποτελέσματα ομαδοποιούνται κάτω από μια γενική κατηγορία τεχνικών, όπως το Credential Dumping. Αυτές οι τεχνικές μπορούν να εφαρμοστούν σε πολλαπλές πλατφόρμες με συγκεκριμένους τρόπους, οι οποίοι περιγράφονται στην τεχνική περιγραφή και οι οποίοι είναι κατανεμημένοι σε ειδικά τμήματα για την πλατφόρμα. Πολλές φορές αυτές οι τεχνικές θα περιέχουν παραλλαγές για τον τρόπο με τον οποίο εφαρμόζονται σε μια συγκεκριμένη πλατφόρμα, όπως το Process Injection.

Περισσότερες ατομικές τεχνικές είναι γενικά οι συγκεκριμένοι τρόποι με τους οποίους ο αντίπαλος ενεργεί ενάντια σε μια συγκεκριμένη πλατφόρμα. Το Rundll32 είναι ένα παράδειγμα το οποίο μπορεί να εφαρμοστεί μόνο για τα συστήματα των Windows. Αυτές οι τεχνικές περιγράφουν το πώς τα ατομικά συστατικά της πλατφόρμας μπορούν να χρησιμοποιηθούν από τους αντιπάλους για να μας βλάψουν. Μερικές φορές οι τεχνικές μπορεί να απαιτούν περισσότερα από ένα βήματα για να υλοποιηθούν. Επομένως υπάρχει περίπτωση μερικά από αυτά τα βήματα να συνδέονται με άλλες υπάρχουσες τεχνικές ή κάποια βήματα θα μπορούσαν να αποτελούν μεμονωμένες τεχνικές.

2.5.3.1.3 Τεχνικές αναφορές

Παρέχονται τεχνικές αναφορές στους χρήστες προς περαιτέρω έρευνα ή για να δώσουν περισσότερες λεπτομέρειες σχετικά με τις τεχνικές. Περιοχές όπου οι τεχνικές αναφορές είναι χρήσιμες περιλαμβάνουν: το υπόβαθρο της τεχνικής, την αναμενόμενη χρήση σε αβλαβής περιπτώσεις, γενικά παραδείγματα χρήσης των τεχνικών αυτών, τις παραλλαγές μιας τεχνικής, τα σχετικά εργαλεία και τα αποθετήρια ανοιχτού κώδικα, παραδείγματα ανίχνευσης και βέλτιστων πρακτικών, παραδείγματα μετριασμού των τεχνικών αυτών.

2.5.3.1.4 Κατηγορίες πληροφοριών για τις τεχνικές

Το μοντέλο ATT&CK περιλαμβάνει επίσης πληροφορίες σχετικά με το εάν (και από ποιον) χρησιμοποιείται μια τεχνική καθώς και τις αναφερόμενες επιπτώσεις από την χρήση της. Όπως αναφέρεται στην ενότητα εμπειρικής χρήσης, υπάρχουν πολλές πηγές αυτών των πληροφοριών. Καθώς το πεδίο εφαρμογής του μοντέλου ATT&CK έχει επεκταθεί και έχει βελτιωθεί, υπάρχουν και τα απαραίτητα κριτήρια για την προσθήκη πληροφοριών. Υπάρχουν επίσης λιγότερα persistent threat περιστατικά που έχουν αναφερθεί κατά των συστημάτων Linux και Mac από ό,τι των συστημάτων Windows, που έχει σαν αποτέλεσμα να υπάρχουν σημαντικά λιγότερα διαθέσιμα δεδομένα απειλών. Υπάρχουν διάφορες γενικές κατηγορίες

πληροφοριών που βασίζονται στην εμπειρική χρήσης και μπορούν να χρησιμοποιηθούν όπως παρακάτω:

• **Reported -** Η χρήση της τεχνικής αναφέρεται μέσω δημόσιων πηγών.

• **Reported, non-public –** Η χρήση της τεχνικής αναφέρεται σε μη δημόσιες πηγές, αλλά η γνώση της υπάρχουσας τεχνικής υπάρχει σε δημόσιες πηγές.

• **Underreported –** Τεχνικές που πιθανόν να χρησιμοποιηθούν αλλά δεν αναφέρονται για κάποιο λόγο. Μπορεί επίσης να υπάρχουν περιπτώσεις στις οποίες υπάρχει έμμεση πληροφορία ότι χρησιμοποιείται μια τεχνική, αλλά είναι γενικά δύσκολο να συγκεντρωθούν περισσότερες πληροφορίες. Η διάκριση γίνεται με βάση την αξιοπιστία της πηγής.

• **Unreported –** Δεν υπάρχει δημόσια ή μη δημόσια πληροφορία που να λέει ότι χρησιμοποιείται μια τεχνική. Αυτή η κατηγορία μπορεί να περιέχει νέες τεχνικές που χρησιμοποιούνται από τις red teams και μπορεί να έχουν δημοσιευθεί, αλλά στις αντίπαλες ομάδες είναι άγνωστες. Η διάκριση χρησιμοποιείται με βάση τη χρησιμότητα της τεχνικής και την πιθανότητα χρήσης.

2.5.3.1.5 Διαφοροποίηση των τεχνικών

Αρκετοί παράγοντες λαμβάνονται υπόψιν όταν συμπεριλαμβάνονται νέες πληροφορίες για να προσδιοριστεί το πού και πώς μπορούν να ενταχθούν στο μοντέλο:

• **Στόχος (Objective) -** Τι επιτελεί η τεχνική. Παρόμοιες τεχνικές μπορούν να εκτελεσθούν με τον ίδιο τρόπο για την επίτευξη διαφορετικών τακτικών. Ομοίως, διαφορετικές τεχνικές μπορούν να επιτύχουν την ίδια τακτική με διάφορους τρόπους.

• **Ενέργειες (Actions) -** Πώς εκτελείται μια τεχνική. Είναι η εκτέλεση διαφορετική μεταξύ των τεχνικών η οποία τις διακρίνει, παρόλο που το αποτέλεσμα μπορεί να είναι το ίδιο ή παρόμοιο;

• **Χρήση (Use) -** Ποιος την χρησιμοποιεί; Υπάρχουν πολλές ομάδες; Εάν ναι, πώς η χρήση της τεχνικής είναι ίδια ή διαφορετική;¨

• **Απαιτήσεις (Requirements) -** Τα συστατικά που χρειάζονται για να χρησιμοποιήσουν μια τεχνική ή αυτά που επηρεάζονται από τη χρήση μιας τεχνικής. Για παράδειγμα, αρχεία, τοποθεσίες, αλλαγές στη registry, δικαιώματα κ.λπ.

• **Ανίχνευση (Detection) -** Τι εργαλεία χρειάζονται για την ανίχνευση της τεχνικής; Αυτό έχει σχέση με τις απαιτήσεις και τις ενέργειες που χρειάζονται να γίνουν, αλλά μπορεί να διαφέρει μεταξύ των τεχνικών που σχετίζονται μεταξύ τους.

• **Αντιμετώπιση (Mitigation) -** Ποιες εναλλακτικές επιλογές αντιμετώπισης υπάρχουν για την τεχνική; Είναι παρόμοιες ή διαφορετικές από άλλες τεχνικές που εκτελούνται με τον ίδιο τρόπο ή έχουν το ίδιο αποτέλεσμα;

Ορισμένες τεχνικές είναι αποτέλεσμα γενικότερων μεθόδων. Για παράδειγμα, το PowerShell είναι ένα υποσύνολο του scripting, αλλά υπάρχουν και άλλοι μηχανισμοί scripting που μπορούν να χρησιμοποιηθούν και θα χρειαστεί να αναλυθούν ξεχωριστά. Για το λόγο αυτό το PowerShell διαχωρίστηκε επειδή είναι μια πολύ διαδεδομένη μέθοδος scripting και execution που χρησιμοποιούνται από πολλές ομάδες αντιπάλων. Επιπλέον λόγω της ευρείας χρήσης του έχουν δημιουργηθεί ξεχωριστοί μηχανισμοί καταγραφής καθώς και ξεχωριστά αμυντικά μέτρα γύρω από αυτό.

Κεφάλαιο 3 Εύρεση απειλών στον κυβερνοχώρο με το μοντέλο ATT&CK

3.1 Αρχές κατά την προσέγγιση ασφαλείας του μοντέλου ATT&CK

Η προσέγγιση που βασίζεται στο μοντέλο του MITRE και η οποία αφορά στην ανίχνευση παραβίασης ασφάλειας δικτύου χρησιμοποιεί μια μεθοδολογία που βασίζεται στην συμπεριφορά και καθοδηγείται από πέντε αρχές που αναπτύχθηκαν ύστερα από έρευνα. Αυτές οι αρχές περιγράφουν κατά προσέγγιση ένα αποτελεσματικό μοντέλο απειλών όσον αφορά την ασφάλεια του δικτύου.

Εικόνα 5 : Αρχές κατά την προσέγγιση ασφαλείας του μοντέλου ATT&CK

Αρχή 1: **Include Post-Compromise Detection** (Ανίχνευση μετά την αρχική πρόσβαση ασφαλείας) - Με την πάροδο του χρόνου, οι προηγούμενες αποτελεσματικές και προληπτικές άμυνες στην περίμετρο μπορεί να αποτύχουν να κρατήσουν τις απειλές από ένα δίκτυο. Μετά την παραβίαση οι δυνατότητες ανίχνευσης είναι απαραίτητες όταν η απειλή παρακάμπτει τις καθιερωμένες άμυνες ή κάνει χρήση νέων τεχνικών για να εισέλθει σε ένα δίκτυο.

Αρχή 2: Focus on Behavior (Εστίαση στη συμπεριφορά) - Οι υπογραφές είναι χρήσιμες μαζί με μια εκ των προτέρων γνώση των υποδομών και των εργαλείων που ενδεχομένως χρησιμοποιεί ο αντίπαλος, αλλά αυτά τα αμυντικά εργαλεία που βασίζονται σε γνωστές υπογραφές συχνά καθίστανται αναξιόπιστα όταν οι υπογραφές μένουν στάσιμες σε σχέση με μια μεταβαλλόμενη απειλή. Οι εξεζητημένες αμυντικές τεχνικές θα πρέπει επίσης να ενσωματώνουν εκτός από την ανίχνευση και την μάθηση από την συμπεριφορά του αντιπάλου μετά την παραβίαση.

Αρχή 3: Use a Threat-based Model (Χρήση μοντέλου βασιζόμενο σε απειλή) – Ένα ακριβές και καλά ορισμένο μοντέλο απειλής είναι απαραίτητο για να εξασφαλιστεί ότι οι δραστηριότητες ανίχνευσης είναι αποτελεσματικές κατά των ρεαλιστικών και σχετικών συμπεριφορών των αντιπάλων.

Αρχή 4: Iterate by Design (Επαναλαμβανόμενη μεθοδολογία ελέγχου από τον σχεδιασμό) – Τα εργαλεία και οι τεχνικές που χρησιμοποιούν οι αντίπαλοι συνεχώς εξελίσσονται. Μια επιτυχημένη προσέγγιση όσον αφορά την ασφάλεια απαιτεί μια σταθερή και επαναλαμβανόμενη εξέλιξη και βελτίωση των μοντέλων ασφαλείας, καθώς επίσης των τεχνικών και των εργαλείων που χρησιμοποιούνται τα οποία δικαιολογούν την αλλαγή της συμπεριφοράς των αντιπάλων και εξηγούν πώς παραβιάζονται τα δίκτυα από μια απειλή.

Αρχή 5: Develop and Test in a Realistic Environment (Ανάπτυξη και δοκιμή σε πραγματικό περιβάλλον) – Η αναλυτική ανάπτυξη και βελτίωση πρέπει να πραγματοποιούνται σε περιβάλλον το οποίο να ταιριάζει όσο το δυνατόν καλύτερα σε ρεαλιστικές συνθήκες δικτύου. Η συμπεριφορά που παράγεται από πραγματικούς χρήστες του δικτύου θα πρέπει να υπάρχει για να είναι ρεαλιστική η πραγματική χρήση του δικτύου. Επιπλέον όποτε είναι δυνατόν, οι δυνατότητες ανίχνευσης θα πρέπει να δοκιμάζονται με την εξομοίωση της συμπεριφορά των αντιπάλων μέσα σε αυτό το περιβάλλον.

3.1.1 Αρχή 1η : Include Post-Compromise Detection

Υπάρχει πάντα η πιθανότητα οι αντίπαλοι να διεισδύσουν ακόμη και στην καλύτερα οργανωμένη αμυντική περίμετρο ενός δικτύου. Για παράδειγμα, προς το παρόν δεν υπάρχει κάποιος αποτελεσματικός τρόπος για την παρεμπόδιση της εκμετάλλευσης μιας zero-day ευπάθειας, δεν υπάρχει μέθοδος για την στιγμιαία εγκατάσταση κάποιου λογισμικού (patch) όταν διαπιστωθεί κάποιο κενό ασφαλείας και επίσης δεν υπάρχει κάποιος τρόπος ο οποίος να αποτρέπει τον άνθρωπο από το να εκθέτει τους κωδικούς πρόσβασης του. Επιπλέον το μέγεθος και η πολυπλοκότητα ενός δικτύου που θα δεχθεί μια επίθεση έχει ως αποτέλεσμα ότι οι επιτιθέμενοι θα βρίσκουν διαρκώς τρόπους για να παρακάμψουν τις κοινές πρακτικές ασφάλειας και να διεισδύσουν στο δίκτυο μιας επιχείρησης για να επιτύχουν τους στόχους τους. Ως εκ τούτου, οποιαδήποτε αποτελεσματική ασφάλεια δικτύου θα πρέπει να λαμβάνει υπόψη την συμπεριφορά των αντιπάλων μετά την παραβίαση, προκειμένου να ελαχιστοποιηθούν οι «ζημίες» που ενδεχομένως θα προκληθούν από έναν αντίπαλο ο οποίος θα καταφέρει επιτυχώς να διαπεράσει τις αρχικές άμυνες του δικτύου.

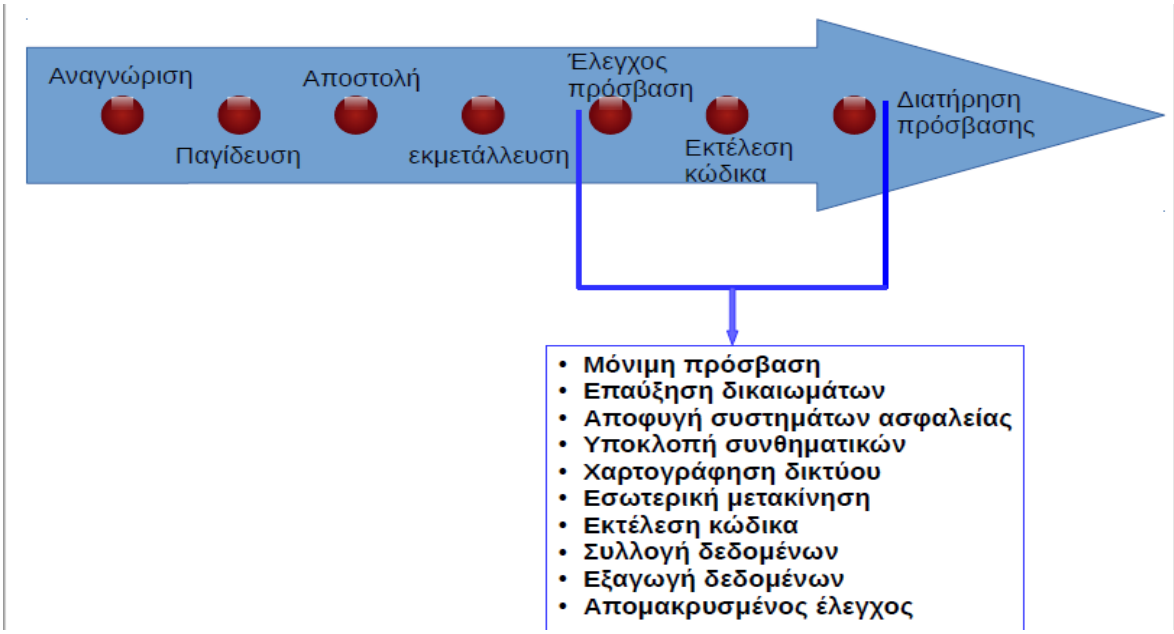
3.1.2 Αρχή 2η : Focus on Behavior

Πολλές σύγχρονες αμυντικές τεχνικές είναι στατικές και επικεντρώνονται σε υπογραφές, «signatured based» τακτικές άμυνας ή σε ενδείκτες προσβολής (indicators of compromise - IOCs). Οι ενδείκτες προσβολής (IOCs) αφορούν σε στοιχεία εγκληματολογικής ερευνάς (forensics artifacts) που μπορούν να αναγνωριστούν σε ένα τερματικό υπολογιστή ή δίκτυο και υποδεικνύουν μεγάλη πιθανότητα προσβολής από κακόβουλο λογισμικό. Τα IOC μπορεί να είναι υπογραφές διαφόρων τύπων που αφήνουν τα κακόβουλα λογισμικά, διευθύνσεις

IP, MD5 συναρτήσεις κατακερματισμού, URL, Domain Names. Σε πολλές περιπτώσεις αυτοί οι ενδείκτες είναι εύθραυστοι και πολύ εύκολο για τους επιτιθεμένους να τους παρακάμψουν με τροποποίηση του κακόβουλου λογισμικού. Ενδείκτες όπως αρχεία κατακερματισμού, διευθύνσεις IP και Domain Names έχουν γίνει το επίκεντρο για πολλούς αμυνόμενους ενός δικτύου, αλλά από την άλλη αυτοί οι ενδείκτες είναι εύκολος τρόπος για έναν αντίπαλο να τους τροποποιήσει προκειμένου να αποφευχθεί η ανίχνευση τους. Επιπλέον, ο οργανισμός που αμύνεται πρέπει να έχει πρόσβαση σε σχετικούς και ενημερωμένους ενδείκτες μέσω προγράμματος ανταλλαγής ενδεικτών απειλής ή εμπορικές πηγές δεδομένων, οι οποίες όμως δεν μπορούν να διασφαλίσουν ότι οι αμυνόμενοι μπορούν να συμβαδίσουν με τις τεχνικές των επιτιθεμένων. Ένα πρόγραμμα ανίχνευσης εισβολής (intrusion detection program) το οποίο ενσωματώνει αναλύσεις από ανίχνευση συμπεριφοράς είναι πιο ανθεκτικό στις προσπάθειες των αντιπάλων να αποφύγουν την ανίχνευση με βάση την υπογραφή μέσω της τροποποίησης των ενδεικτών. Οι προσεγγίσεις όσον αφορά την ανίχνευση της συμπεριφοράς βοηθούν στον εντοπισμό των κοινών συμπεριφορών που είναι πολύ πιθανό να εφαρμόσουν πολλές ομάδες αντιπάλων κατά τη διάρκεια μιας εισβολής και είναι ανεξάρτητες από συγκεκριμένες αλλαγές στους ενδείκτες που κάνουν οι αντίπαλοι. Αυτή είναι η αρχή που οδήγησε στην ανάπτυξη του μοντέλου ATT&CK.

3.1.3 Αρχή 3η : Use a Threat-based Model

Η χρήση ενός μοντέλου απειλής είναι το θεμέλιο μιας ισχυρής διαδικασίας ασφάλειας. Η συγκέντρωση των ενεργειών και της συμπεριφοράς των αντιπάλων σε ένα πρότυπο μοντέλο απειλών επιτρέπει στους αμυνόμενους να σχεδιάζουν επαρκώς και να αξιολογούν τις άμυνες τους. Σύμφωνα με τις αρχές 1 και 2, το μοντέλο απειλής ενθυλακωμένο στο πρότυπο ATT&CK περιγράφει τις συμπεριφορές των επιτιθέμενων όταν αποκτήσουν πρόσβαση στο εσωτερικό ενός δικτύου. Η εικόνα 6 δείχνει πώς το μοντέλο ATT&CK παίρνει τα τρία post-compromise (μετά την παραβίαση) στάδια του κύκλου ζωής των επιθέσεων στον κυβερνοχώρο και τα επεκτείνει σε 10 ξεχωριστές τακτικές οι οποίες χρησιμοποιούνται από τους επιτιθέμενους.



Εικόνα 6 : Τεχνική και τακτικές επιτιθέμενων του ATT&CK

3.1.4 Αρχή 4η : Iterate by Design

Μια επαναλαμβανόμενη διαδικασία δοκιμών και ελέγχων κρίνεται κρίσιμη για τη δημιουργία ενός αποτελεσματικού μοντέλου ανάλυσης και ανίχνευσης συμπεριφοράς, που μπορεί να εφαρμοστεί σε ένα σύστημα το οποίο συμβαδίζει με το μοντέλο ATT&CK. Ένα σημαντικό μέρος αυτής της διαδικασίας αφορά δοκιμές όσον αφορά τις αναλύσεις συμπεριφοράς σε τακτά χρονικά διαστήματα από μια Red team η οποία θα εξομοίωνε γνωστές συμπεριφορές επιτιθεμένων τεκμηριωμένες σύμφωνα με το μοντέλο ATT&CK. Ένα από τα οφέλη της χρήσης μιας επαναλαμβανόμενης διαδικασίας από ελέγχους είναι η γρήγορη ανατροφοδότηση που παρέχεται στους υπεύθυνους ανάπτυξης αμυντικών τεχνικών. Με τη χρήση μόνο μερικών αναλυτικών στοιχείων από μια τέτοια διαδικασία και στη συνέχεια την επικύρωσή τους μέσω ενός μοντέλου προσομοίωσης απειλών όπως θα γινόταν σε ένα πραγματικό δίκτυο, οι αναλυτές μπορούν να δουν γρήγορα ποια από αυτά τα στοιχεία είναι χρήσιμα και πρέπει να αναπτυχθούν περαιτέρω και ποια πρέπει να απορριφθούν. Αυτή η προσέγγιση παρέχει πολλές ευκαιρίες σε έναν προγραμματιστή να δοκιμάσει υποθετικά τον καλύτερο τρόπο για την ανίχνευση καθορισμένων συμπεριφορών σε ένα πραγματικό δίκτυο. Ένα άλλο όφελος αυτής της διαδικασίας είναι η ικανότητα των αμυντικών συστημάτων των δικτύων να προσαρμόζονται σε μια μεταβαλλόμενη απειλή. Όπως αναφέρθηκε προηγουμένως, μια προσεγγιστική ανίχνευση αλλαγής συμπεριφοράς παρέχει μια αποτελεσματική μέθοδο για την αντιμετώπιση των επιτιθεμένων οι οποίοι αλλάζουν συχνά τη συμπεριφορά τους για να ξεπεράσουν τα διάφορα αμυντικά εμπόδια που θα συναντήσουν κατά την επίθεση τους σε ένα δίκτυο. Οι αντίπαλοι χρησιμοποιούν νόμιμες υπηρεσίες ιστού και ισχυρή κρυπτογράφηση για να παρακάμψουν την ανίχνευση υπογραφής του πρωτοκόλλου δικτύου και τις μαύρες λίστες, αλλά θα χρειαστεί να αλληλοεπιδράσουν με το endpoint σύστημα με τέτοιο τρόπο ώστε να συμβαδίζει με τον τρόπο λειτουργίας του συστήματος. Επιπλέον ένας απομακρυσμένος χρήστης θα κάνει χρήση μια νέας υπηρεσίας των Windows για την εγκατάσταση επίμονου κακόβουλου λογισμικού. Ωστόσο, ανεξάρτητα από το

είδος του κακόβουλου λογισμικού το οποίο ο εισβολέας θα προσπαθήσει να τρέξει, η παρουσία του θα φαίνεται κάτι σαν μια νέα υπηρεσία των Windows και αυτό ακριβώς είναι μία από τις συμπεριφορές των επιτιθέμενων που περιγράφει το μοντέλο ATT&CK και μπορεί να συνδυαστεί με άλλα συμβάντα τα οποία αναγνωρίζουν ξεχωριστά πρότυπα συμπεριφορών των αντιπάλων. Η ανίχνευση συμπεριφοράς δυσκολεύει τους αντιπάλους να αποφύγουν την ανίχνευση. Ωστόσο, οι αντίπαλοι θα εξακολουθούν να συνεχίζουν να αλλάζουν τη συμπεριφορά τους με την πάροδο του χρόνου αλλά η γρήγορη ανατροφοδότηση από μια επαναλαμβανόμενη διαδικασία ελέγχων θα βοηθήσει αποτελεσματικά τις αμυντικές ικανότητες ενός δικτύου και θα ανιχνεύσει τις τελευταίες αλλαγές συμπεριφοράς μιας απειλής.

3.1.5 Αρχή 5η : Develop and Test in a Realistic Environment

Είναι σημαντικό για την επαναλαμβανόμενη διαδικασία αναλύσεων και ελέγχων όσον αφορά τις δυνατότητες ανίχνευσης να εκτελείται σε ένα περιβάλλον που να προσομοιάζει με το πραγματικό ή να είναι όσο το δυνατόν πιο ρεαλιστικό. Για να γίνει αυτό εφικτό η Red Team προσομοιώνει την συμπεριφορά των αντιπάλων με βάση τις τελευταίες καταγεγραμμένες απειλές του μοντέλου ATT&CK. Η πραγματική εκτέλεση των δοκιμών και η συλλογή των αναλυτικών στοιχείων πραγματοποιείται σε ένα κανονικό εταιρικό δίκτυο, με πραγματικούς χρήστες οι οποίοι εκτελούν τις καθημερινές τους εργασίες για να είναι δυνατόν να εξασφαλιστεί όσο γίνεται πιο ρεαλιστικά ο πραγματικός «θόρυβος» του συστήματος. Εάν τα αναλυτικά στοιχεία είχαν συλλεχθεί και δοκιμαστεί σε εργαστηριακό περιβάλλον χωρίς πραγματικούς χρήστες για την εκτέλεση πραγματικής εργασίας οι οποίοι χρησιμοποιούσαν πραγματικές εφαρμογές, η συμπεριφορά των αντιπάλων που θα ανιχνευόταν μπορεί να είχε θεωρηθεί ως συμπεριφορά την οποία θα εκτελούσαν οι κανονικοί χρήστες ή οι διαχειριστές του συστήματος, με αποτέλεσμα να είναι δύσκολο να ανιχνευτεί κάποια απειλή.

3.2 Περιγραφή του μοντέλου ATT&CK

Το ATT&CK είναι ένα μοντέλο που χρησιμοποιείται για να περιγράψει τις ενέργειες που θα εκτελέσει ένας αντίπαλος ο οποίος έχει αποκτήσει πρόσβαση στο εσωτερικό δίκτυο ενός οργανισμού. Οι Τακτικές, οι Τεχνικές και οι Διαδικασίες (Tactics, Techniques and Procedures - TTPs) που περιγράφονται στο μοντέλο ATT&CK επιλέχθηκαν με βάση τις παρατηρούμενες ενέργειες των επιτιθεμένων οι οποίες είναι καταγεγραμμένες σε δημόσιες αναφορές και περιλαμβάνονται στο μοντέλο σε επίπεδο αφαιρετικότητας (δηλαδή μπορεί να βρει εφαρμογή σε πολλαπλά περιβάλλοντα και ομάδες χρηστών), το οποίο είναι απαραίτητο για την αποτελεσματική ιεράρχηση των αμυντικών τεχνικών που χρειάζονται να εφαρμοστούν.

3.2.1 Post-Compromise Threat-Based Modeling

Το μοντέλο ATT&CK αντιμετωπίζει ένα κενό όσον αφορά στην κατανόηση λεπτομερειών σχετικά με την ανίχνευση μετά την παραβίαση. Οι δημόσιες αναφορές αναφέρουν συχνά λεπτομέρειες υψηλού επιπέδου για τη συμπεριφορά των

αντιπάλων και εισβολέων, χωρίς να διαθέτουν κρίσιμες πληροφορίες που θα μπορούσαν να χρησιμοποιηθούν για την αποτελεσματική αντιμετώπισή τους. Για παράδειγμα, οι αναφορές που αναφέρονται σε lateral movement χρησιμοποιούν πολύ γενικούς όρους χωρίς να παρέχουν συγκεκριμένες λεπτομέρειες για το πώς ένας αντίπαλος μπορεί να εκτελέσει αυτές τις κινήσεις, με αποτέλεσμα να μην βοηθούν έναν οργανισμό να αμυνθεί από αυτή τη συγκεκριμένη τακτική. Η MITRE δημιούργησε το μοντέλο ATT&CK για να αντιμετωπίσει την ανάγκη ώστε να δοθούν πρόσθετες λεπτομέρειες για το πως μπορεί να προστατευτεί ένας οργανισμός. Για την καλύτερη ενημέρωσή του το μοντέλο αυτό χρησιμοποίησε πληροφορίες από πηγές που συμπεριλαμβάνουν δημόσιες αναφορές για απειλές, από δοκιμές penetration testing και Red teaming καθώς και από έρευνες που έχουν γίνει πάνω στον τομέα της ασφάλειας. Οι τεχνικές στο μοντέλο ATT&CK επικεντρώνονται σε μεγάλο βαθμό στα συστήματα με λειτουργικό Windows, λόγω του μεγάλου αριθμού των χρηστών τους, καθώς υπάρχουν δημόσια στο κοινό πολλές εκθέσεις παραβίασης οι οποίες περιέχουν αρκετές λεπτομέρειες και εργαλεία που χρησιμοποιούν οι αντίπαλοι που επιτίθενται ενάντια στα Windows, υποδηλώνοντας ότι οι επιτιθέμενοι του δικτύου των επιχειρήσεων τείνουν να επικεντρωθούν σε αυτούς τους τύπους των συστημάτων. Ωστόσο, επειδή οι στόχοι των αντιπάλων τείνουν να παραμείνουν οι ίδιοι, ανεξάρτητα από το λειτουργικό σύστημα που χρησιμοποιεί ένας οργανισμός, το μοντέλο ATT&CK μπορεί να επεκταθεί σε μη Windows λειτουργικά συστήματα, ωστόσο αυτό θα απαιτούσε επιπρόσθετες πληροφορίες για τις τεχνικές των αντιπάλων σε αυτές τις πλατφόρμες ώστε να διατηρηθεί το επιθυμητό επίπεδο ρεαλισμού. Το μοντέλο ATT&CK χωρίζεται σε υψηλού επιπέδου κατηγορίες από τακτικές που χρησιμοποιούν οι αντίπαλοι καθώς και σε μεμονωμένες τεχνικές τις οποίες μπορούν οι επιτιθέμενοι να χρησιμοποιήσουν για καθεμία από τις κατηγορίες αυτές. Οι τακτικές περιγράφουν γιατί ένας αντίπαλος εκτελεί μια ενέργεια και οι τεχνικές περιγράφουν τον τρόπο με τον οποίο το κάνουν. Οι τεχνικές περιγράφονται στο μοντέλο του ATT&CK τόσο από την επιθετική όσο και από την αμυντική πλευρά, και με τον τρόπο αυτό αποτελούν ένα χρήσιμο σημείο αναφοράς και μπορούν να βοηθήσουν έναν οργανισμό ώστε να αμυνθεί κατάλληλα. Επιπλέον οι τεχνικές του ATT&CK περιέχουν αναφορές σε γνωστά παραδείγματα τόσο του τρόπου με τον οποίο έχει χρησιμοποιηθεί αυτή η τεχνική καθώς και την σύνδεση των διάφορων τεχνικών με ομάδες αντιπάλων που είναι γνωστό ότι τις χρησιμοποιούν.

3.2.2 Κατηγορίες των τακτικών του μοντέλου ATT&CK

Οι τακτικές αντιπροσωπεύουν το υψηλότερο επίπεδο αφαιρετικότητας μέσα στο μοντέλο ATT&CK. Είναι οι τακτικοί στόχοι που επιδιώκει να επιτύχει ένας αντίπαλος κατά τη διάρκεια μιας επιχείρησης. Οι κατηγορίες των τακτικών του μοντέλου ATT&CK είναι:

• **Persistence** (Μόνιμη πρόσβαση) – Κάθε πρόσβαση, δράση ή αλλαγή των παραμέτρων ενός συστήματος τα οποία δίνουν σε έναν αντίπαλο μια επίμονη παρουσία στο σύστημα αυτό. Οι αντίπαλοι θα πρέπει συχνά να διατηρούν την πρόσβαση στα συστήματα αυτά η οποία μπορεί να χάνεται μετά από μια επανεκκίνηση του συστήματος, η απώλεια διαπιστευτηρίων ή άλλες ενέργειες.

• **Privilege Escalation** (Επαύξηση δικαιωμάτων) –Το αποτέλεσμα των τεχνικών που έχουν σαν αποτέλεσμα ένας αντίπαλος να αποκτήσει υψηλότερο επίπεδο δικαιωμάτων σε ένα σύστημα ή δίκτυο. Ορισμένα εργαλεία ή ενέργειες απαιτούν υψηλότερο επίπεδο δικαιωμάτων από αυτά του απλού χρήστη για να μπορούν να εκτελεστούν και για το λόγο αυτό τα δικαιώματα αυτά είναι απαραίτητα κατά την απομακρυσμένη λειτουργία ενός συστήματος.

• **Defense Evasion** (Αποφυγή συστημάτων ασφαλείας) – Τεχνικές που ένας αντίπαλος μπορεί να χρησιμοποιήσει με απώτερο σκοπό να αποφύγει την ανίχνευση ή τα διάφορα συστήματα ασφαλείας.

• **Credential Access** (Υποκλοπή συνθηματικών) –Τεχνικές που έχουν ως αποτέλεσμα την πρόσβαση ή τον έλεγχο του συστήματος, του τομέα, ή μιας υπηρεσίας με την πρόσβαση και την υποκλοπή των διαπιστευτηρίων που χρησιμοποιούνται σε ένα περιβάλλον μιας επιχείρησης.

• **Discovery** (Χαρτογράφηση δικτύου) –Τεχνικές που επιτρέπουν σε έναν αντίπαλο να αποκτήσει γνώσεις σχετικά με ένα σύστημα καθώς και του εσωτερικού του δικτύου.

• **Lateral Movement** (Εσωτερική μετακίνηση) – Τεχνικές που επιτρέπουν σε έναν αντίπαλο να έχει πρόσβαση και να ελέγχει απομακρυσμένα συστήματα σε ένα δίκτυο. Συχνά το επόμενο βήμα μετά την εσωτερική μετακίνηση είναι η απομακρυσμένη εκτέλεση διάφορων εργαλείων και προγραμμάτων τα οποία έχουν εισήχθη στο δίκτυο από τον αντίπαλο.

• **Execution** (Εκτέλεση κώδικα) – Τεχνικές που έχουν ως αποτέλεσμα την εκτέλεση κώδικα ο οποίος ελέγχεται από τον αντίπαλο τόσο σε ένα τοπικό ή σε ένα απομακρυσμένο σύστημα.

• **Collection** (Συλλογή δεδομένων) – Τεχνικές που χρησιμοποιούνται για τον εντοπισμό και τη συλλογή πληροφοριών, όπως είναι τα ευαίσθητα αρχεία, από το δίκτυο - στόχο πριν από την εξαγωγή τους στο επόμενο βήμα.

• **Exfiltration** (Εξαγωγή δεδομένων) – Τεχνικές και χαρακτηριστικά που έχουν ως αποτέλεσμα ή βοηθούν έναν αντίπαλο να κάνει εξαγωγή των αρχείων και των πληροφοριών από το δίκτυο - στόχο. Αυτή η κατηγορία συμπεριλαμβάνει επίσης τις τοποθεσίες ενός συστήματος ή δικτύου στις οποίες ο αντίπαλος μπορεί να αναζητήσει πληροφορίες για να εξάγει.

• **Command and Control** (Διοίκηση και έλεγχος) – Τεχνικές και χαρακτηριστικά του τρόπου επικοινωνίας των αντιπάλων με τα συστήματα που έχουν υπό τον έλεγχό τους στο εσωτερικό του δικτύου - στόχου. Παραδείγματα περιλαμβάνουν τη χρήση νόμιμων πρωτόκολλα όπως το HTTP για τη μεταφορά πληροφοριών διοίκησης και ελέγχου (C2).

3.2.3 Τεχνικές και νόμιμες λειτουργίες του Λειτουργικού συστήματος

Οι τεχνικές στο μοντέλο ATT&CK περιγράφουν τις ενέργειες που εκτελούν οι αντίπαλοι για να πετύχουν τους τακτικούς στόχους τους. Μέσα σε κάθε κατηγορία τακτικής υπάρχει ένας πεπερασμένος αριθμός ενεργειών με τις οποίες μπορεί να επιτευχθεί αυτός ο στόχος. Καθ 'όλη τη διάρκεια των ενεργειών που λαμβάνουν χώρα μετά την παραβίαση, ο αντίπαλος λαμβάνει συνεχώς αποφάσεις σχετικά με την τεχνική την οποία πρέπει να χρησιμοποιήσει βασιζόμενος στις γνώσεις του, στις πληροφορίες που αποκτά για το περιβάλλον - στόχο, στις πληροφορίες που απαιτούνται για τις μελλοντικές δράσεις και στις ικανότητες που διαθέτει. Οι τεχνικές περιγράφουν τις ενέργειες που θα εκτελέσει ο αντίπαλος με τέτοιο τρόπο οι οποίες να είναι ανεξάρτητες από κακόβουλο λογισμικό ή εργαλεία που θα χρησιμοποιήσει ο αντίπαλος. Το όφελος από αυτή την προσέγγιση είναι ότι καλύπτει τη συμπεριφορά που εκτίθεται από έναν αντίπαλο μέσω της χρήσης εργαλείων απομακρυσμένης πρόσβασης, σεναρίων ή αλληλεπίδρασης με την γραμμή εντολών χωρίς να προσπαθεί να αμυνθεί σε ένα συγκεκριμένο κακόβουλο λογισμικό ή εργαλείο τα οποία ενδέχεται να αλλάξουν στο πέρασμα του χρόνου.
Στο μοντέλο ATT&CK πολλές από τις τεχνικές που χρησιμοποιούνται είναι νόμιμες λειτουργίες του λειτουργικού συστήματος οι οποίες μπορούν να χρησιμοποιηθούν για κακόβουλους σκοπούς από τους αντιπάλους. Για παράδειγμα, μια προγραμματισμένη εργασία των Windows που κάνει χρήση του schtasks.exe είναι μια τεχνική που μπορεί να χρησιμοποιηθεί για την μόνιμη πρόσβαση ή την εκτέλεση ενός αρχείου εξ αποστάσεως ως μέρος της εσωτερικής μετακίνησης. Η εμφάνιση του schtasks.exe σε ένα σύστημα δεν μπορεί να θεωρηθεί ως κακόβουλη πράξη επειδή αποτελεί ένα νόμιμο χαρακτηριστικό του λειτουργικού συστήματος. Οι αντίπαλοι γνωρίζουν αυτό όπως επίσης και άλλα νόμιμα χαρακτηριστικά του λειτουργικού συστήματος καθώς επίσης και τον τρόπο με τον οποίο μπορούν να τα χρησιμοποιήσουν προς όφελός τους.
Οι τεχνικές που περιγράφονται στο μοντέλο ATT&CK δεν πρέπει να αντιμετωπίζονται ως μεμονωμένες ενέργειες που ενδεχομένως να εκτελέσουν οι αντίπαλοι αλλά ως ένα κομμάτι μιας στρατηγικής των αντιπάλων το οποίο χαρτογραφεί μια κακόβουλη συμπεριφορά πάνω στην οποία τα αμυντικά συστήματα πρέπει να κατασκευαστούν ώστε να την ανιχνεύσουν. Δεδομένα από κάθε ενέργεια που θα εκτελέσει ο αντιπάλος μπορούν να χρησιμοποιηθούν για να βοηθήσουν να δημιουργηθεί μια ακριβέστερη πρόβλεψη για το αν μια σειρά ενεργειών συνιστά κακόβουλη ή καλοήθη συμπεριφορά.
Το μοντέλο ATT&CK δεν προσπαθεί να απαριθμήσει όλες τις πιθανές τεχνικές που μπορούν να εφαρμοστούν σε μια δεδομένη κατηγορία τακτικής, αλλά βασίζεται στην γνώση που έχει αποκτηθεί από τις ενέργειες που οι αντίπαλοι έχουν χρησιμοποιήσει για να επιτύχουν ένα συγκεκριμένο σκοπό, καθώς και στο πώς οι ενέργειες αυτές σχετίζονται μεταξύ τους για να σχηματίσουν αναγνωρίσιμες συμπεριφορές των αντιπάλων.

3.2.4 Περιπτώσεις λειτουργίας του μοντέλου

Το μοντέλο ATT&CK έχει δείξει τη δυνατότητα πολλαπλών εφαρμογών τόσο για την εκτέλεση επιθέσεων όσο και για δημιουργία αποτελεσματικών αμυνών. Για

παράδειγμα, στις ασκήσεις κυβερνοχώρου του MITRE, το μοντέλο ATT&CK χρησιμοποιείται ως μοντέλο για την εξομοίωση αντιπάλων (red team). Επιπλέον χρησιμοποιείται από την μπλε ομάδα (blue team) με σκοπό την δημιουργία αποτελεσματικών αμυνών εναντίων των σεναρίων των αντιπάλων. Με τον τρόπο αυτό κατασκευάζονται σενάρια που προσομοιάζουν τις πραγματικών επιθέσεων οι οποίες βασίζονται σε συμπεριφορές και ενέργειες όπως αυτές περιγράφονται στο μοντέλο αυτό για τη δοκιμή συγκεκριμένων αμυντικών συστημάτων και την συγκέντρωση αναλυτικών στοιχείων. Το μοντέλο παρέχει μια κοινή γλώσσα μεταξύ τόσο των μελών της red όσο και της blue team, ώστε να δοκιμαστούν διάφορες ενέργειες στο εσωτερικό περιβάλλον του δικτύου, που θα οδηγήσουν στο να βγουν διάφορα συμπεράσματα πως αυτές οι ενέργειες είναι δυνατόν να εντοπιστούν ή όχι κατά τη διάρκεια της προσομοίωσης ενός αντιπάλου. Το μοντέλο αυτό βοηθάει επίσης στο να έχουμε μια εκτίμηση της αποτελεσματικότητας τόσο των υπαρχόντων όσο και των νέων αμυντικών εργαλείων και υπηρεσιών που χρησιμοποιούνται. Με βάση αυτές τις εκτιμήσεις καθορίζεται πόσο καλά τα αμυντικά εργαλεία ανιχνεύουν ή εμποδίζουν ένα γνωστό σύνολο τεχνικών που χρησιμοποιούν οι αντίπαλοι και δίνεται μια προτεραιότητα με βάση τη συχνότητα χρήσης τους από τους αντιπάλους.

3.3 Βήματα που χρησιμοποιούνται στο μοντέλο ATT&CK

Η χρήση του μοντέλου ATT&CK έγινε με σκοπό να δημιουργηθεί, να αξιολογηθεί και να αναθεωρηθεί η ακριβέστερη μέθοδος ανίχνευσης σχετικά με την συμπεριφορά των αντιπάλων στον κυβερνοχώρο. Από το 2012 που ξεκίνησαν τα παιχνίδια τον κυβερνοχώρο, το μοντέλο αυτό έχει υποστεί αρκετές βελτιώσεις χρησιμοποιώντας την εμπειρία που έχει αποκτηθεί πάνω στην συμπεριφορά των αντιπάλων, την κατασκευή αισθητήρων για την απόκτηση δεδομένων και την ανάλυση αυτών των δεδομένων για την ανίχνευση της συμπεριφοράς των αντιπάλων. Για την περιγραφή και λειτουργία αυτού του μοντέλου χρησιμοποιούνται οι ακόλουθοι ρόλοι:

• **White Team –** Χρησιμοποιούνται για την ανάπτυξη των διαφόρων σεναρίων απειλής με τα οποία θα δοκιμαστούν τα αμυντικά συστήματα. Συνεργάζονται τόσο με την κόκκινη όσο και με την μπλε ομάδα για την αντιμετώπιση ζητημάτων που θα προκύψουν κατά τη διάρκεια των δοκιμών ώστε να εξασφαλιστεί ότι οι αντικειμενικοί στόχοι ικανοποιούνται. Αυτή η ομάδα είναι ο συνδετικός κρίκος με τους διαχειριστές του δικτύου που δοκιμάζεται.

• **Red Team –** Χρησιμοποιούνται για τον ρόλο του αντίπαλου σε αυτό το παιχνίδι του κυβερνοχώρου. Εκτελούν το προγραμματισμένο σενάριο για την ρεαλιστικότερη προσομοίωση της συμπεριφοράς των αντιπάλων και συνεργάζονται με την White Team όταν απαιτείται. Οποιεσδήποτε ευπάθειες του συστήματος ή του δικτύου οι οποίες ανακαλύπτονται αναφέρονται άμεσα στην White Team.

• **Blue Team –** Χρησιμοποιούνται για τον ρόλο του υπερασπιστή (αμυνόμενου) του δικτύου και προσπαθούν να εντοπίσουν τις δραστηριότητες της Red team.

Το μοντέλο κυβερνοάμυνας του ATT&CK βασιζόμενο στην απειλή περιέχει επτά βήματα που εμφανίζονται στην εικόνα 7.

Εικόνα 7 : Βήματα στο μοντέλο ATT&CK

1. Identify Behaviors (Εντοπισμός συμπεριφοράς) – Σε αυτό το βήμα προσδιορίζονται και δίνονται προτεραιότητες στις συμπεριφορές των αντιπάλων από το μοντέλο απειλής για να επιτευχθεί η ανίχνευση.

2. Acquire Data (Συλλογή πληροφοριών / Ανάπτυξη αισθητήρων) –Σε αυτό το βήμα προσδιορίζονται τα δεδομένα τα οποία είναι απαραίτητα για την ανίχνευση της επιθυμητής συμπεριφοράς των αντιπάλων. Εάν δεν υπάρχει η δυνατότητα απόκτησης αυτών των δεδομένων, τότε πρέπει να αναπτυχθούν κατάλληλοι αισθητήρες για τη συλλογή τους.

3. Develop Analytics (Ανάπτυξη ερωτημάτων) – Σε αυτό το βήμα δημιουργούνται αναλυτικά στοιχεία από τα συλλεγμένα δεδομένα για την ανίχνευση αναγνωρισμένων συμπεριφορών.

4. Develop an Adversary Emulation Scenario (Ανάπτυξη σεναρίου προσομοίωσης αντιπάλου) – Σε αυτό το βήμα η Λευκή ομάδα αναπτύσσει έναν αντίπαλο προσομοίωσης, βάσει του μοντέλου ATT&CK, το οποίο περιλαμβάνει τις συμπεριφορές που προσδιορίζονται στο Βήμα 1 (Εντοπισμός συμπεριφοράς). Το σενάριο αυτό περιλαμβάνει συγκεκριμένες τεχνικές οι οποίες θα πρέπει να χρησιμοποιηθούν από το Κόκκινη ομάδα.

5. Emulate Threat (Προσομοίωση της απειλής) – Σε αυτό το βήμα η Κόκκινη Ομάδα προσπαθεί να επιτύχει τους στόχους που περιγράφονται από τη Λευκή ομάδα κάνοντας χρήση των συμπεριφορών και των τεχνικών που περιγράφονται στο μοντέλο ATT&CK.

6. Investigate Attack (Διερεύνηση της επίθεσης) – Σε αυτό το βήμα η μπλε ομάδα επιχειρεί να αναπαραστήσει το χρονοδιάγραμμα των δραστηριοτήτων της Κόκκινης κάνοντας χρήση των αναλυτικών στοιχείων και των δεδομένων που αναπτύχθηκαν στο Βήμα 3 (Ανάπτυξη ερωτημάτων).

7. Evaluate Performance (Αξιολόγηση της απόδοσης) – Σε αυτό το βήμα η Λευκή, η Κόκκινη και η Μπλε ομάδες κάνουν μια κριτική όσον αφορά τον βαθμό εμπλοκής της Μπλε ομάδας, για να αξιολογήσουν κατά πόσο αυτή μπόρεσε να χρησιμοποιήσει επιτυχώς όλα τα δεδομένα της ανάλυσης που συλλέχθηκαν από τους αισθητήρες για την ανίχνευση της συμπεριφοράς των αντιπάλων. Μετά από αυτή την αξιολόγηση, ο κύκλος επαναλαμβάνεται και επιστρέφει Βήμα 1.

3.4 Ανάλυση Βημάτων

Βήμα 1: Identify Behaviors (Εντοπισμός συμπεριφοράς)

Η διαδικασία της αναλυτικής ανάπτυξης αρχίζει με τον εντοπισμό της συμπεριφοράς των αντιπάλων με σκοπό την ανίχνευσή τους. Αρκετοί παράγοντες πρέπει να λαμβάνονται υπόψη πριν πάρουμε απόφαση για το πώς να ιεραρχήσουμε τις συμπεριφορές αυτές:

• Ποιες συμπεριφορές είναι πιο συνηθισμένες;

Η ιεράρχηση των Τακτικών, των Τεχνικών και των Διαδικασιών (Tactics, Techniques and Procedures - TTPs) που χρησιμοποιούνται πιο συχνά από τους αντιπάλους παρουσιάζει μεγαλύτερο ενδιαφέρον κατά τον σχεδιασμό ασφάλειας ενός οργανισμού ο οποίος θα προσπαθήσει να αντιμετωπίσει τις απειλές οι οποίες είναι πιο διαδεδομένες και ως εκ τούτου είναι πιο πιθανό να συναντηθούν. Με αυτό τον τρόπο ένας οργανισμός μπορεί να ενημερωθεί σχετικά για τις τακτικές και τεχνικές του μοντέλου πάνω στις οποίες θα πρέπει να επικεντρωθεί.

• Ποιες συμπεριφορές έχουν τις πιο αρνητικές επιπτώσεις;

Οι οργανισμοί πρέπει να εξετάσουν ποιες Τακτικές, Τεχνικές και Διαδικασίες θα έχουν τις μεγαλύτερες πιθανές επιπτώσεις για τον οργανισμό. Αυτές οι επιπτώσεις μπορεί να έχουν τη μορφή της φυσικής καταστροφής, της απώλειας πληροφοριών, την απόκτηση πρόσβασης στο σύστημα καθώς επίσης και άλλες αρνητικές συνέπειες.

• Για ποιες συμπεριφορές υπάρχουν άμεσα διαθέσιμα δεδομένα;

Οι συμπεριφορές για τις οποίες υπάρχουν ήδη διαθέσιμα δεδομένα θα διευκολύνουν τη δημιουργία αμυντικών σχεδίων σε σχέση με εκείνες που απαιτούν την ανάπτυξη νέων αισθητήρων ή νέων πηγών δεδομένων.

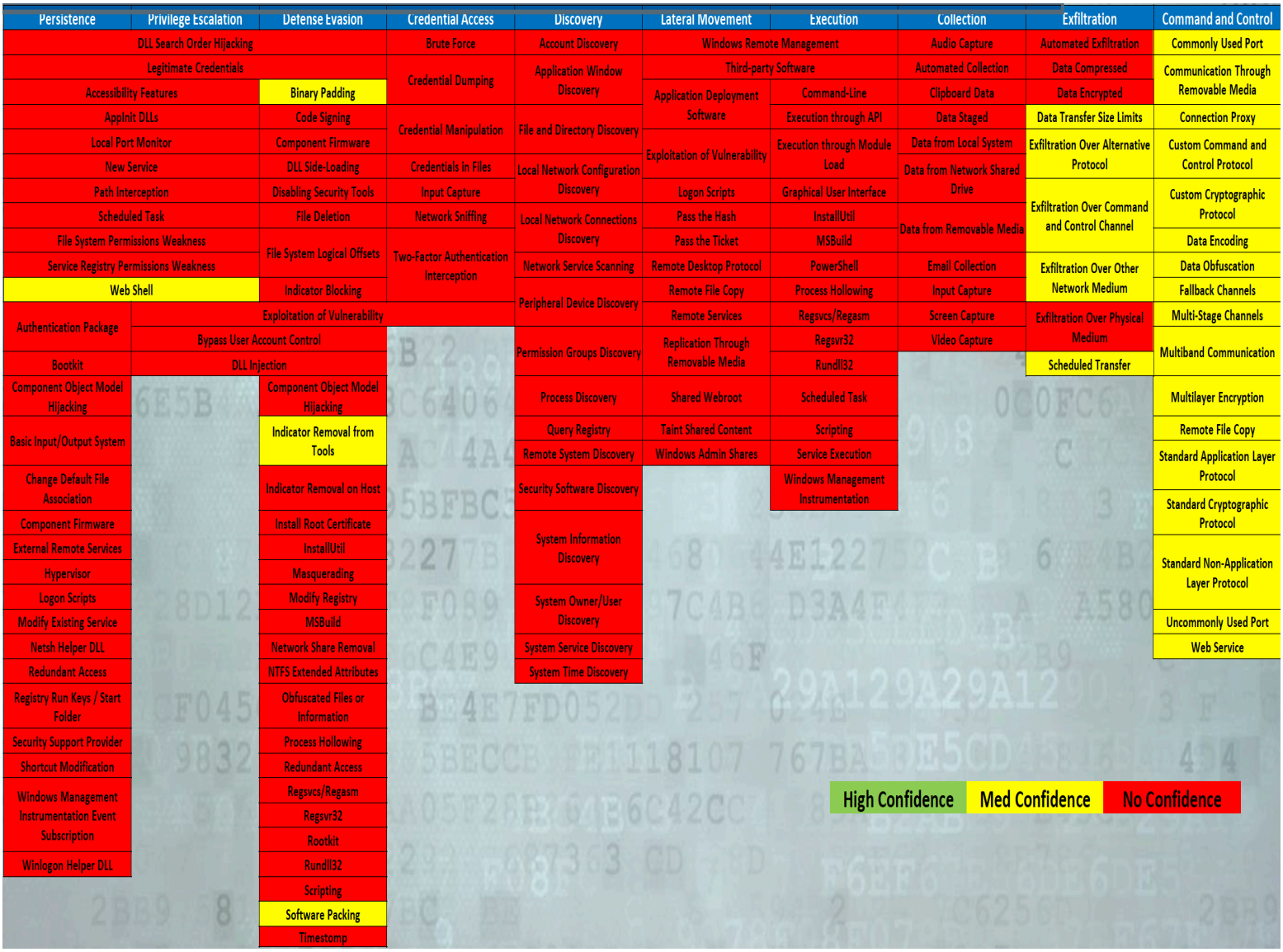
• Ποιες συμπεριφορές είναι πιο πιθανό να υποδεικνύουν κακόβουλη συμπεριφορά;

Οι συμπεριφορές που συνήθως προκύπτουν μόνο από τους αντιπάλους και όχι από τους νόμιμους χρήστες είναι οι πιο χρήσιμες για τους αμυνόμενους επειδή έχουν ως αποτέλεσμα λιγότερα false positives.

Βήμα 2: Acquire Data (Συλλογή πληροφοριών / Ανάπτυξη αισθητήρων)

Κατά την προετοιμασία για τη δημιουργία αναλυτικών στοιχείων, οι οργανισμοί πρέπει να εντοπίζουν, να συλλέγουν και να αποθηκεύουν τα δεδομένα τα οποία είναι απαραίτητα για την ανάλυση των δεδομένων. Για να καταφέρει να εντοπίσει ένας αναλυτής ποια δεδομένα χρειάζεται να συλλέξει για να δημιουργήσει τα δεδομένα που χρειάζεται, είναι σημαντικό να κατανοήσει ποια δεδομένα συλλέγονται ήδη από υπάρχοντες αισθητήρες και τους διάφορους μηχανισμούς καταγραφής. Σε ορισμένες περιπτώσεις, αυτά τα δεδομένα ενδέχεται να πληρούν τις απαιτήσεις δεδομένων για ένα καθορισμένο σύνολο αναλυτικών στοιχείων. Σε πολλές περιπτώσεις, ωστόσο, μπορεί να χρειαστεί να γίνουν ρυθμίσεις ή να οριστούν διάφοροι κανόνες για τους υπάρχοντες αισθητήρες και εργαλεία ώστε να τροποποιηθούν καταλληλά για να αρχίσουν να συλλέγουν τα απαιτούμενα δεδομένα. Επίσης σε άλλες περιπτώσεις μπορεί να χρειαστεί να εγκατασταθούν νέα εργαλεία τα οποία θα βοηθήσουν στη συλλογή των απαιτούμενων δεδομένων.
Πολλές επιχειρήσεις βασίζονται στην ανίχνευση παραβίασης του δικτύου στην περίμετρο λόγω της ευκολίας ανάπτυξης αισθητήρων στα σημεία εισόδου και εξόδου του δικτύου. Ωστόσο, αυτό περιορίζει την ορατότητα μόνο στην κίνηση του δικτύου η οποία εισέρχεται ή εξέρχεται από το δίκτυο και δεν βοηθά τους αμυνόμενους να αποκτήσουν μια πλήρη άποψη για το τι συμβαίνει μέσα στο δικτύου τους και μεταξύ των συστημάτων τους. Οι αμυνόμενοι στο πλαίσιο ανάπτυξης αισθητήρων στην περίμετρο, βασίζονται στην δέσμευση πακέτων (packet capture), σε firewalls, σε proxies, σε network-based intrusion detection συστήματα καθώς και σε άλλα συστήματα που βασίζονται στην ανάλυσης των διακινούμενων πακέτων του δικτύου. Σε αυτή την περίπτωση αν ένας αντίπαλος είναι σε θέση να αποκτήσει επιτυχώς πρόσβαση σε ένα σύστημα εντός της παρακολουθούμενης περιμέτρου και με τις κατάλληλες ενέργειες να παρακάμψει τις προστασίες του δικτύου, τότε ο αμυνόμενος θα είναι «τυφλός» και δεν θα μπορεί να εντοπίσει την δραστηριότητα του αντιπάλου στο εσωτερικό του δικτύου του.
Για να εντοπίσουμε την τακτική, τις τεχνικές, τις διαδικασίες και τα εργαλεία των επιτιθέμενων μετά την αρχική παραβίαση, θα πρέπει να αναπτύξουμε αισθητήρες συλλογής πληροφοριών σε επίπεδο προσωπικού υπολογιστή και όχι μόνο στην περίμετρο. Αυτό οφείλεται διότι στα τερματικά συστήματα, μέσα στην περίμετρο του δικτύου, μπορούμε να συγκεντρώσουμε περισσότερες πληροφορίες όσον αφορά τις δράσεις του επιτιθεμένου. Η εικόνα 8 δείχνει μια μήτρα του μοντέλου ATT&CK που αντιπροσωπεύει την κάλυψη με βάση μόνο την χρησιμοποίηση αισθητήρων στην περίμετρο του δικτύου. Τα κελιά με το κόκκινο χρώμα αντιπροσωπεύουν τις τεχνικές τις οποίες δεν υπάρχει δυνατότητα ανίχνευσης συμπεριφοράς, ενώ με το κίτρινο χρώμα υποδηλώνεται ότι υπάρχει μερική ικανότητα ανίχνευσης. Χωρίς την ανάπτυξη αισθητήρων σε επίπεδο προσωπικού υπολογιστή, οι οποίοι να ανιχνεύουν τα περιστατικά του δικτύου, όπως την εκκίνηση μιας διαδικασίας (process) καθώς και την δημιουργία νέων συνδέσεων στο εσωτερικό του δικτύου, είναι δύσκολο να ανιχνευτούν σε αποτελεσματικό βαθμό πολλές από τις συμπεριφορές που περιγράφονται από το μοντέλο, με βάση τις οποίες θα είναι δυνατόν να εντοπιστεί μια παραβίαση χωρίς να υπάρχει κάποια εκ των προτέρων γνώση για τον αντίπαλο και χωρίς να υπάρχουν ορισμένες εγκατεστημένες

αμυντικές ικανότητες οι οποίες θα συμβάλλουν στον έγκαιρο προσδιορισμό των ενεργειών του.



Εικόνα 8 : Κάλυψη με την χρήση μόνο αισθητήρων στην περίμετρο

Βήμα 3: Develop Analytics (Ανάπτυξη ερωτημάτων)

Μόλις οι οργανισμοί διαθέτουν τους απαιτούμενους αισθητήρες και δεδομένα, μπορούν στη συνέχεια να αναπτύξουν τα αναλυτικά στοιχεία. Η ανάπτυξη αναλυτικών στοιχείων απαιτεί μια πλατφόρμα υλικού και λογισμικού πάνω στην οποία θα σχεδιαστούν και θα δοκιμαστούν τα αναλυτικά αυτά στοιχεία. Αυτό συχνά γίνεται μέσω μιας πλατφόρμας SIEM (Security Information and Event Management). Η βασική τους λειτουργία, είναι να συλλέγουν data logs ασφαλείας από ένα μεγάλο εύρος πηγών εντός του οργανισμού, όπως συστήματα ελέγχου ασφαλείας, λειτουργικά συστήματα και εφαρμογές. Όταν το SIEM αποκτήσει τα log δεδομένα, τα επεξεργάζεται για να τα προσαρμόσει σε συγκεκριμένη μορφή, κάνει ανάλυση των μορφοποιημένων δεδομένων, εκδίδει ειδοποιήσεις όταν ανιχνεύσει ύποπτες δραστηριότητες και παράγει αναφορές όταν ζητηθούν από τους

διαχειριστές του SIEM. Οι ερευνητές του MITRE ταξινόμησαν τα αναλυτικά στοιχεία που σχετίζονται με το μοντέλο σε τέσσερις κύριους τύπους:

• **Behavioral** (Που σχετίζεται με την συμπεριφορά)– Τα αναλυτικά στοιχεία σχεδιάζονται με σκοπό να ανιχνεύουν μια συγκεκριμένη συμπεριφορά αντιπάλου, όπως π.χ. τη δημιουργία μιας νέας υπηρεσίας των Windows. Η συμπεριφορά αυτή από μόνη της μπορεί να είναι είτε κακόβουλη είτε όχι. Αυτές οι συμπεριφορές θα πρέπει να αντιστοιχίζονται στις τεχνικές που προσδιορίζονται από μοντέλο αυτό.

• **Situational Awareness** (Επίγνωση κατάστασης) – Τα αναλυτικά στοιχεία προσανατολίζονται προς μια γενική κατανόηση του τι συμβαίνει μέσα σε ένα περιβάλλον δικτύου σε μια δεδομένη στιγμή. Δεν είναι απαραίτητο όλα αυτά τα στοιχεία να προσανατολίζονται στο να παράγουν ειδοποιήσεις σχετικά με κακόβουλη συμπεριφορά. Αντίθετα, αυτά τα στοιχεία μπορεί να αποδειχθούν πολύτιμα για ένα οργανισμό όταν παρέχουν γενικές πληροφορίες σχετικά με την κατάσταση του περιβάλλοντος. Μια πληροφορία για τον χρόνο σύνδεσης ενός χρήστη δεν υπονοεί κάποια κακόβουλη δραστηριότητα, αλλά σε συνδυασμό με άλλους ενδείκτες, ακόμη και αυτός ο τύπος δεδομένων μπορεί να παρέχει τις απαραίτητες πληροφορίες σχετικά την συμπεριφορά του αντιπάλου. Τα στοιχεία που έχουν να κάνουν με την επίγνωση της κατάστασης του δικτύου μπορούν επίσης να βοηθήσουν στην παρακολούθηση της «υγείας» του περιβάλλοντος του δικτύου (για παράδειγμα μπορεί να προσδιοριστεί σε ποιους υπολογιστές οι αισθητήρες δεν λειτουργούν σωστά).

• **Anomaly / Outlier** (Στατιστική παρακολούθηση, εντοπισμός ανωμαλιών) – Τα αναλυτικά στοιχεία μπορεί πολλές φορές να εντοπίσουν συμπεριφορές που δεν είναι κακόβουλες, αλλά να είναι ασυνήθιστες και μπορεί να φαίνονται ύποπτες. Μερικά παραδείγματα θα ήταν η ανίχνευση κάποιων εκτελέσιμων αρχείων που δεν έχουν ξαναεκτελεστεί ή να αναγνωριστούν διαδικασίες που εκτελούνται στο δίκτυο και οι οποίες συνήθως δεν το κάνουν. Με την στατιστική παρακολούθηση, αυτοί οι τύποι αναλύσεων δεν υποδεικνύουν απαραίτητα μια επίθεση.

• **Forensic** (Συλλογή δεδομένων ψηφιακής σήμανσης) – Αναλυτικά στοιχεία που είναι πολύ χρήσιμα κατά τη διεξαγωγή έρευνας σχετικά με ένα περιστατικό. Για παράδειγμα, εάν ένας αναλυτής διαπιστώσει ότι χρησιμοποιήθηκε ένα πρόγραμμα για υποκλοπή διαπιστευτηρίων σε έναν κεντρικό υπολογιστή, η διαδικασία forensic θα αποκαλύψει όλους τους χρήστες των οποίων τα διαπιστευτήρια έχουν παραβιαστεί.

Βήμα 4: Develop an Adversary Emulation Scenario (Ανάπτυξη σεναρίου προσομοίωσης αντιπάλου)

Υπάρχουν πολλοί ορισμοί σχετικά με τις δραστηριότητες και τους τύπους των ελέγχων που καλύπτονται κάτω από την ομπρέλα των επιθετικών δοκιμών ασφαλείας που γίνονται στον κυβερνοχώρο. Τα παραδοσιακά penetration tests επικεντρώνονται στην επισήμανση τα τρωτών σημείων – αδυναμιών που εμφανίζονται σε διαφορετικούς τύπους συστημάτων τα οποία ένας αντίπαλος μπορεί να αξιοποιήσει για να προκαλέσει κάποια ενέργεια. Οι Κόκκινες ομάδες μπορεί να επικεντρωθούν σε ένα πιο μακροπρόθεσμο και επιζήμιο στόχο στο εσωτερικό ενός δικτύου - στόχου, όπως η ανάληψη του ελέγχου ενός κρίσιμου

συστήματος. Κατά τη διάρκεια ενός ελέγχου από την Κόκκινη ομάδα το πιο πιθανό είναι να ανακαλύψουν τρωτά σημεία τα οποία θα πρέπει να διορθωθούν, αλλά το πεδίο εφαρμογής της ομάδας περιορίζεται στο να επιτύχει τον τελικό της αντικειμενικό σκοπό.
Η προσέγγιση του μοντέλου για την εξομοίωση των αντιπάλων διαφέρει από τις υπόλοιπες παραδοσιακές προσεγγίσεις. Ο στόχος για τα μέλη της Red team είναι να εκτελέσουν συμπεριφορές και τεχνικές οι οποίες να βασίζονται σε συγκεκριμένες ή στις πιο γνωστές που χρησιμοποιούν οι αντίπαλοι με σκοπό να ελέγξουν συγκεκριμένες πτυχές ενός συστήματος ή δικτύου. Οι ασκήσεις προσομοίωσης που εκτελούν οι αντίπαλοι αποτελούνται από μικρής κλίμακας, επαναλαμβανόμενες συμπλοκές οι οποίες έχουν σχεδιαστεί με τέτοιο τρόπο ώστε να βελτιώνουν και να δοκιμάζουν τις άμυνες σε ένα «ζωντανό» περιβάλλον μέσω της συστηματικής εισαγωγής μιας σειράς νέων κακόβουλων συμπεριφορών στο δίκτυο. Η Red team η οποία προσομοιώνει την απειλή, συνεργάζεται στενά με την Μπλε ομάδα (συχνά αναφέρεται ως purple team) για να εξασφαλίσουν ανοιχτές γραμμές επικοινωνίας και αυτό είναι πολύ σημαντικό για την ταχεία χάραξη της αποτελεσματικής άμυνας ενός οργανισμού, έτσι ώστε αυτή να δοκιμαστεί προτού ένας πραγματικός αντίπαλος αρχίζει να ενεργεί στοχευμένα στο εσωτερικό περιβάλλον του δικτύου. Για τον σκοπό αυτό, οι δοκιμασίες προσομοίωσης αντιπάλου συχνά διεξάγονται με ταχύτερο και πιο εστιασμένο τρόπο από ότι τα penetration tests.
Καθώς αναπτύσσονται νέες μέθοδοι ανίχνευσης, οι οποίες χρησιμοποιούνται από ολόκληρη την κοινότητα του κυβερνοχώρου, η έρευνα στον τομέα της ασφάλειας θα επικεντρωθεί στο να βρει τρόπους παράκαμψης πριν το καταφέρουν οι πραγματικοί αντίπαλοι. Πρέπει να αναπτυχθούν σενάρια αντιμετώπισης των αντιπάλων μέσω προσομοίωσης γύρω από αυτή την ιδέα και θα πρέπει πάντα να έχουμε στο μυαλό μας ότι οι περισσότεροι πραγματικοί αντίπαλοι έχουν συγκεκριμένους στόχους, όπως για παράδειγμα η απόκτηση πρόσβασης σε ευαίσθητες πληροφορίες. Κατά τη διάρκεια των δοκιμαστικών διαδικασιών, η Κόκκινη Ομάδα μπορεί να έχει συγκεκριμένους στόχους αλλά όλες οι ενέργειες τις οποίες θα προσομοιώσουν θα πρέπει να επικεντρωθούν στον τρόπο με τον οποίο θα προσπαθήσουν να επιτύχουν τους στόχους τους αυτούς και όχι εάν θα τους επιτύχουν ή όχι.

Ανάπτυξη σεναρίων

Κατά την ανάπτυξη ενός σεναρίου εξομοίωσης αντιπάλων για τους σκοπούς της δοκιμής άμυνας ενός δικτύου, μπορεί να απαιτηθεί ένα σχέδιο υψηλού επιπέδου για την επίτευξη των επιχειρησιακών στόχων, χωρίς να δίνουν τις λεπτομέρειες του σεναρίου των δοκιμών τόσο στην Κόκκινη όσο και στην Μπλε ομάδα. Η Λευκή ομάδα θα πρέπει να σχεδιάσει αυτό το σενάριο, έχοντας γνώση των αισθητήρων που χρησιμοποιεί η Μπλε ομάδα καθώς και τα κενά ανίχνευσης που έχουν εντοπιστεί ενάντια στη συμπεριφορά απειλής, όπως επίσης και τις αλλαγές που έχει κάνει η Μπλε ομάδα για την βελτίωση αυτών των «κενών» ασφαλείας οι οποίες θα πρέπει να αξιολογηθούν. Η Λευκή ομάδα πρέπει επίσης να καθορίσει εάν η Κόκκινη ομάδα έχει αρκετές ικανότητες ώστε να προσομοιώσει κατάλληλα τη συμπεριφορά των αντιπάλων. Εάν όχι, τότε η Λευκή ομάδα θα πρέπει να συνεργαστεί με την Κόκκινη ομάδα για την αντιμετώπιση οποιωνδήποτε κενών, συμπεριλαμβανομένης της ανάπτυξης, της απόκτησης και της δοκιμής συγκεκριμένων εργαλείων που μπορεί να απαιτούνται. Ο υψηλού επιπέδου σχεδιασμός μπορεί να χρησιμοποιηθεί ως βάση για την πλήρη ανάπτυξη σεναρίου προσομοίωσης ώστε να καλυφθούν

όλες οι απαιτήσεις καθώς και για τον αποτελεσματικότερο συντονισμό όλων των ενδιαφερόμενων μερών.

Οι λεπτομέρειες σχεδιασμού ενός υψηλού επιπέδου σεναρίου μπορεί να περιλαμβάνουν:

1. Τους αισθητήρες καθώς και το ποιες αμυντικές δυνατότητες θα δοκιμαστούν κατά την διάρκεια της προσομοίωσης.
2. Ποια συμπεριφορά αντιπάλου θα πρέπει να χρησιμοποιηθεί.
3. Τις ακολουθίες των ενεργειών οι οποίες προτείνονται για την δοκιμή και επαλήθευση των αμυντικών δυνατοτήτων.
4. Τα συστήματα, το δίκτυο ή άλλους πόρους που απαιτούνται για το παιχνίδι - δοκιμή στον κυβερνοχώρο.

Το σενάριο προσομοίωσης των αντιπάλων μπορεί να είναι, αλλά αυτό δεν είναι απαραίτητο, ένα λεπτομερές command - by command script. Αυτό θα πρέπει να είναι αρκετά λεπτομερές ώστε να δώσει τις κατάλληλες κατευθύνσεις στην Κόκκινη ομάδα για να δοκιμάσει και να επαληθεύσει τις ικανότητες του αμυνομένου αλλά επιπλέον πρέπει να είναι αρκετά ευέλικτες ώστε να δώσουν ένα βαθμό ελευθερίας στην Κόκκινη ομάδα, με σκοπό να προσαρμόσει κατάλληλα τις δραστηριότητές της, οποτεδήποτε αυτό χρειαστεί κατά τη διάρκεια της άσκησης, ώστε να δοκιμάσει διάφορες παραλλαγές συμπεριφοράς οι οποίες ενδεχομένως να μην έχουν εξεταστεί από η Μπλε ομάδα. Αυτό γίνεται για το σκοπό του ότι σχεδιασμός των αμυντικών τεχνικών, από την Μπλε ομάδα, έχει γίνε ώστε να καλύπτει γνωστές συμπεριφορές απειλών, επομένως η Κόκκινη ομάδα πρέπει να είναι ελεύθερη να δοκιμάσει παραλλαγές αυτών των συμπεριφορών. Χρησιμοποιώντας την Λευκή ομάδα στο να αποφασίσει ποιες νέες συμπεριφορές θα πρέπει να δοκιμαστούν, η Μπλε ομάδα δεν έχει καμία πληροφορία ως προς τι θα δοκιμαστεί και η Κόκκινη ομάδα θα παραμείνει ελεύθερη να δοκιμάσει τις ικανότητες της.

Βήμα 5: Emulate Threat (Προσομοίωση της απειλής)

Αφού σχεδιαστεί το σενάριο και συγκεντρωθούν τα αναλυτικά στοιχεία, είναι καιρός να γίνει χρήση αυτού του σεναρίου για την προσομοίωση του αντιπάλου ώστε να γίνει έλεγχος όσον αφορά την λειτουργικότητα του. Για να υλοποιηθεί αυτό το σενάριο απαιτείται μια Κόκκινη ομάδα η οποία θα προσομοιώσει την απειλητική συμπεριφορά και θα εκτελέσει διάφορες τεχνικές οι οποίες έχουν καθοριστεί από την Λευκή ομάδα. Αυτές οι ασκήσεις προσομοίωσης επιτρέπουν στους αναλυτές να επαληθεύσουν την αποτελεσματικότητα των αμυντικών τεχνικών που χρησιμοποιούνται. Επειδή οι τεχνικές αυτές εστιάζουν στις δυνατότητες εντοπισμού της συμπεριφοράς του αντιπάλου, μετά την αρχική παραβίαση, η Κόκκινη ομάδα ξεκινά τις ενέργειές της έχοντας αρχική πρόσβαση στο εσωτερικό του δικτύου μέσω ενός εργαλείου απομακρυσμένης πρόσβασης σε ένα συγκεκριμένο περιβάλλον. Αυτή η πρόσβαση επιταχύνει την διαδικασία της αξιολόγησης και διασφαλίζει ότι οι μετά την αρχική παραβίαση οι άμυνες ελέγχονται επαρκώς. Η Κόκκινη ομάδα ακολουθεί πιστά το σχέδιο και τις κατευθυντήριες γραμμές που έχουν δοθεί από την Λευκή ομάδα.

Βήμα 6: Investigate Attack (Διερεύνηση της επίθεσης)

Μόλις οι ενέργειες της Κόκκινης ομάδας κατά την διάρκεια των δοκιμών του δικτύου ολοκληρωθούν, η Μπλε ομάδα θα συγκεντρωθεί για να προσπαθήσει να ανακαλύψει τι ακριβώς έκανε η Κόκκινη ομάδα. Η δοκιμή με αυτόν τον τρόπο βοηθά να διασφαλιστεί ότι η επιτυχία της Μπλε ομάδας εξαρτάται στο ότι τα αναλυτικά στοιχεία είναι ευκολονόητα για όλους τους χρήστες, όχι μόνο για εκείνους που τα ανέπτυξαν.
Η μπλε ομάδα ξεκινά τις προσπάθειες της για την ανακάλυψη των ενεργειών της Κόκκινης ομάδας χρησιμοποιώντας ένα σύνολο αναλυτικών στοιχείων τα οποία εάν είναι σωστά, θα τους βοηθήσει για να αποκαλύψουν για το πού και πότε η Κόκκινη ομάδα μπορεί να ήταν ενεργή. Αυτό είναι σημαντικό, καθώς η Μπλε ομάδα δεν λαμβάνει καμία πληροφορία σχετικά με τη δραστηριότητα της Κόκκινης, εκτός από ένα αόριστο χρονικό παράθυρο, συνήθως της τάξης ενός μήνα. Τα αποτελέσματα από την εφαρμογή αυτών των αναλυτικών στοιχείων οδηγούν την Μπλε ομάδα για περαιτέρω διερεύνηση μεμονωμένων υπολογιστών χρησιμοποιώντας τους άλλους τύπους των αναλυτικών στοιχείων που περιεγράφηκαν προηγουμένως (Επίγνωση κατάστασης, στατιστική παρακολούθηση και εντοπισμός ανωμαλιών, συλλογή δεδομένων ψηφιακής σήμανσης). Όλες οι διαδικασίες τις Μπλε ομάδας κάνουν χρήση της εξόδου ενός αναλυτικού στοιχείου που έχει συλλεχθεί για τη βελτίωση κάποιου άλλου και όλη αυτή η διαδικασία είναι επαναληπτική και επαναλαμβάνεται καθ' όλη τη διάρκεια της άσκησης καθώς συλλέγονται νέες πληροφορίες.
Τελικά, καθώς αυτά τα γεγονότα αναγνωρίζονται ότι ανήκουν σε δραστηριότητες της Κόκκινης ομάδας, ένα χρονοδιάγραμμα ξεκινάει να σχηματίζεται. Η κατανόηση αυτού του χρονοδιαγράμματος των γεγονότων είναι σημαντική και μπορεί να βοηθήσει τους αναλυτές να συλλέξουν πληροφορίες οι οποίες δεν θα μπορούσαν να αποκτηθούν αποκλειστικά και μόνο από τα αναλυτικά στοιχεία. Τα κενά των δραστηριοτήτων στο χρονοδιάγραμμα αυτό μπορούν να βοηθήσουν ώστε να εντοπιστούν τα χρονικά παράθυρα όπου απαιτείται περαιτέρω διερεύνηση. Επίσης, εξετάζοντας τα δεδομένα με αυτόν τον τρόπο, τα μέλη της Μπλε ομάδας μπορεί να εξάγουν διάφορα συμπεράσματα ως προς το που μπορεί να βρεθεί δραστηριότητα, ακόμη και χωρίς να υπάρχουν άλλα αποδεικτικά στοιχεία για τη δραστηριότητα αυτή. Για παράδειγμα, αν διαπιστώσουν ότι κάποιο εκτελέσιμο πρόγραμμα εκτελείται, αλλά δεν έχουν κάποιες ενδείξεις για το πως αυτό τοποθετήθηκε στο μηχάνημα, τότε αυτή η συμπεριφορά προειδοποιεί τους αναλυτές σχετικά με πιθανή συμπεριφορά της Κόκκινης ομάδας και μπορεί να παράσχει επιπλέον λεπτομέρειες για το πώς η Κόκκινη Ομάδα πέτυχε την εσωτερική μετακίνηση (lateral movement). Αυτές οι ενδείξεις μπορούν επίσης να οδηγήσουν σε ιδέες για νέες αναλύσεις που πρέπει να γραφτούν για την επόμενη ενημέρωση του πίνακα του μοντέλου ATT&CK.
Καθώς η Μπλε ομάδα συνεχίζει να διερευνά την δραστηριότητα της Κόκκινης ομάδας, προσπαθεί να διαμορφώσει μια εικόνα και να συλλέξει πληροφορίες για την δραστηριότητα αυτή, όπως:

• **Hosts Involved/Compromised** – Αυτό απεικονίζεται συχνά κατά τη διάρκεια της άσκησης ως μια λίστα που περιέχει τους υπολογιστές καθώς επίσης και τους λόγους για του οποίους έχουν προσδιοριστεί ως ύποπτοι. Αυτές οι πληροφορίες θεωρούνται ως κρίσιμες όταν προσπαθούμε να αντιμετωπίσουμε ένα περιστατικό.

• **Accounts Compromised** – Είναι πολύ σημαντικό να μπορεί η Μπλε ομάδα να εντοπίσει όλους τους λογαριασμούς που έχουν παραβιαστεί σε ένα δίκτυο. Εάν δεν το γίνει αυτό, τότε επιτρέπουμε στην Κόκκινη ομάδα ή σε έναν πραγματικό επιτιθέμενο, να ανακτήσει ξανά την πρόσβαση στο δίκτυο.

• **Objective –** Η Μπλε ομάδα θα πρέπει επίσης να προσπαθήσει να ανακαλύψει ποιοι πιθανόν να ήταν οι στόχοι της Κόκκινης ομάδας καθώς επίσης και αν τους πέτυχαν ή όχι. Αυτό είναι συχνά μια από τις πιο δύσκολες εργασίες που πρέπει να γίνουν καθώς για να το ανακαλύψει αυτό η Μπλε ομάδα με βεβαιότητα απαιτείται να έχει στην κατοχή της ένα μεγάλο σύνολο δεδομένων από την συμπεριφορά της Κόκκινης ομάδας.

• **TTPs Used** – Είναι σημαντικό με το τέλος της άσκησης να σημειωθούν όλες οι Τακτικές, οι Τεχνικές και οι Διαδικασίες οι οποίες χρησιμοποιήθηκαν από την Κόκκινη ομάδα. Αυτό γίνεται για τον λόγο ότι η Κόκκινη ομάδα μπορεί να έχει εκμεταλλευτεί λανθασμένες ρυθμίσεις σε ένα δίκτυο τις οποίες θα πρέπει να αντιμετωπίσουμε ή να έχει ανακαλύψει μια νέα τεχνική την οποία η Μπλε ομάδα δεν μπορεί να εντοπίσει επί του παρόντος χωρίς περαιτέρω ανίχνευση. Τα TTPs που η Μπλε ομάδα έχει εντοπίσει ότι χρησιμοποιήθηκαν πρέπει να συγκριθούν με τον κατάλογο των TTPs που ισχυρίζεται η Κόκκινη ομάδα ότι χρησιμοποίησε για να εντοπιστούν τυχόν αμυντικά κενά.

Βήμα 7: Evaluate Performance (Αξιολόγηση της απόδοσης)

Αφού ολοκληρωθούν οι δραστηριότητες της ομάδας Μπλε και Κόκκινης ομάδας, η Λευκή ομάδα συγκρίνει τη δραστηριότητα της Κόκκινης ομάδας με την αναφορά που έχει λάβει από την Μπλε ομάδα. Με αυτό τον τρόπο επιτυγχάνεται μια ολοκληρωμένη εικόνα για το πόσο οι πληροφορίες που ανακάλυψε η Μπλε ομάδα ήταν επιτυχημένες όσον αφορά την ανακάλυψη των ενεργειών της Κόκκινης. Χρησιμοποιώντας αυτές πληροφορίες, η Μπλε ομάδα βελτιώνει τις υπάρχουσες αμυντικές τεχνικές και επιπλέον εντοπίζει για το ποιες συμπεριφορές των αντιπάλων πρέπει να αναπτύξουν ή να εγκαταστήσουν νέους αισθητήρες, ώστε να συλλέξουν νέα σύνολα δεδομένων ή να δημιουργήσουν νέα αναλυτικά στοιχεία.

Κεφάλαιο 4 Σύστημα προσομοίωσης αντιπάλων CALDERA

4.1 Η φιλοσοφία του CALDERA

Το CALDERA είναι ένα αυτοματοποιημένο σύστημα το οποίο προσομοιώνει τις ενέργειες των αντιπάλων και έχει κατασκευαστεί από την εταιρία MITRE. Έχει σχεδιαστεί για να λειτουργεί σε δίκτυα με λειτουργικό σύστημα Windows. Δημιουργεί διάφορα σενάρια κατά τη λειτουργία του, χρησιμοποιώντας ένα προ ρυθμισμένο μοντέλο προσομοίωσης αντιπάλων βασισμένο στο μοντέλο Adversarial Tactics, Techniques & Common Knowledge (ATT&CK). Αυτά τα χαρακτηριστικά επιτρέπουν στο CALDERA να λειτουργεί δυναμικά σε ένα σύνολο συστημάτων που χρησιμοποιούν μεταβλητές συμπεριφορές, το οποίο αντιπροσωπεύει καλύτερα τον τρόπο με τον οποίο οι ανθρώπινοι αντίπαλοι εκτελούν λειτουργίες σε σχέση με τα συστήματα που είναι ρυθμισμένα να ακολουθούν προκαθορισμένες ακολουθίες ενεργειών.
Το CALDERA είναι χρήσιμο για τους αμυνόμενους ενός δικτύου οι οποίοι θέλουν να αποκτήσουν πραγματικά δεδομένα, που αντιπροσωπεύουν πώς ένας αντίπαλος θα συμπεριφερόταν μέσα στα δίκτυά τους. Δεδομένου ότι οι γνώσεις του CALDERA σχετικά με ένα δίκτυο συγκεντρώνονται κατά τη διάρκεια της λειτουργίας του, οι οποίες στην συνέχεια χρησιμοποιούνται για την επιλογή των κατάλληλων τεχνικών για την επίτευξη ενός στόχου, οι αμυνόμενοι μπορούν να δουν πώς οι εσωτερικές εξαρτήσεις ασφάλειας του δικτύου τους, θα επιτρέψουν οι ενέργειες που θα εφαρμόσει ένας αντίπαλος να είναι επιτυχής. Το CALDERA είναι χρήσιμο για τον εντοπισμό νέων πηγών δεδομένων, για τη δημιουργία και βελτίωση των τεχνικών για την ανίχνευσης εισβολών που βασίζονται στη συμπεριφορά, για την δοκιμή των αμυντικών τεχνικών και για την ρύθμιση των παραμέτρων ασφαλείας καθώς επίσης και για την απόκτηση εμπειρίας την εκπαίδευση του προσωπικού το οποίο είναι υπεύθυνο για την ασφάλεια.

4.2 Γιατί προσομοίωση αντιπάλου

Η προσομοίωση του αντιπάλου είναι ένα τμήμα του Red teaming. Σκοπός της είναι να προσεγγίσει ένα πρόβλημα ή ένα σύστημα, όπως θα έκανε και ένας αντίπαλος, με το σκοπό να το παρενοχλήσει με κακόβουλο τρόπο. Το Red team χρησιμοποιείται συνήθως ως μια μέθοδος η οποία θα δοκιμάσει και θα βελτιώσει την ασφάλεια ενός συστήματος, εφαρμόζοντας τις ενέργειες που θα εκτελούσε και ένας επιτιθέμενος και έχει ως απώτερο σκοπό τον μετριασμό των επιθέσεων αυτών. Η Red team επικεντρώνεται συχνά στην επίδειξη του αντίκτυπου που θα έχει η επίθεση ενός αντιπάλου σε έναν οργανισμό. Οι ενέργειες αυτές μπορεί να διαρκέσουν εβδομάδες ή ακόμα και μήνες και ένας από τους κύριους στόχους της κόκκινης ομάδας είναι ότι δεν πρέπει να εντοπιστεί.
Η προσομοίωση του αντιπάλου είναι το επίκεντρο της κόκκινης ομάδας, αλλά αντί να χρησιμοποιεί τη γενική νοοτροπία ενός εισβολέα, υιοθετεί τις μεθοδολογίες ενός συγκεκριμένου επιτιθέμενου του πραγματικού κόσμου, συμπληρώνοντας τες με τους στόχους, τις μεθόδους και τις τεχνικές οι οποίες είναι γνωστό ότι θα χρησιμοποιήσει ο αντίπαλος για να ενεργήσει. Το πλεονέκτημα των ενεργειών αυτών είναι ότι η ομάδα που προσομοιώνει τους αντιπάλους και η ομάδα η οποία αμύνεται, εργάζονται μαζί για τη βελτίωση της ασφάλειας των συστημάτων, του δικτύου και των αμυντικών διαδικασιών που εφαρμόζονται, για την καλύτερη

ανίχνευση των τεχνικών που χρησιμοποιούνται από τον αντίπαλο κατά την διάρκεια μιας επίθεσης. Η κόκκινη ομάδα εστιάζεται σε απειλές οι οποίες είναι αποδεδειγμένα πραγματικές και με αυτό τον τρόπο οι αμυντικές βελτιώσεις που θα εφαρμοστούν μπορούν να μετρηθούν και να επαληθευτούν.
Η πρακτική της προσομοίωσης του αντιπάλου σχεδιάστηκε για να απαντήσει στην ερώτηση: "Είναι ασφαλές το δίκτυό μου;". Ή πιο συγκεκριμένα: "Είναι ασφαλές το δίκτυο μου ενάντια σε γνωστές απειλές;". Για τον λόγο αυτό ο καλύτερος τρόπος για να μάθουμε κάτι είναι να το δοκιμάσουμε. Το ίδιο ισχύει και για τα δίκτυα: ο καλύτερος τρόπος για να διαπιστώσουμε εάν ένα δίκτυο είναι ανθεκτικό στην επίθεση των αντιπάλων είναι να το δοκιμάσουμε εφαρμόζοντας τις ίδιες ενέργειες σε αυτό το δίκτυο και να παρατηρήσουμε πώς αυτό αντιδρά.

Αυτοματοποιημένη προσομοίωση αντιπάλων

Το CALDERA αυτοματοποιεί την προσομοίωση των αντιπάλων και αυτό γιατί περιέχει πολλές ενσωματωμένες τεχνικές τις οποίες χρησιμοποιούν οι αντίπαλοι και οι οποίες προέρχονται από το μοντέλο ATT&CK. Για κάθε τεχνική των αντιπάλων, το CALDERA περιέχει μια κωδικοποίηση σύμφωνα με την οποία περιγράφονται οι απαιτήσεις καθώς και τα αποτελέσματα των τεχνικών.
Το CALDERA επικεντρώνεται στην προσομοίωση των αντιπάλων "μετά την παραβίαση" (post compromise). Με άλλα λόγια, το CALDERA υποθέτει ότι ένας αντίπαλος έχει ήδη αποκτήσει αρχική πρόσβαση σε ένα δίκτυο. Το CALDERA προσομοιώνει τις ενέργειες που θα εκτελέσει ένας επιτιθέμενος μετά την είσοδο του στο δίκτυο. Αυτή η έννοια του " post compromise " έχει αρκετές σημαντικές επιπτώσεις: Το CALDERA δεν επικεντρώνεται στο τι θα κάνει ένας αντίπαλος για να «εισέλθει». Οι τεχνικές όπως vulnerability scanning, penetration testing, intelligence gathering, and spearphising, που συμβαίνουν συνήθως ως προάγγελοι σε μια επίθεση, είναι εκτός πεδίου δράσης για το CALDERA.
Η συμπεριφορά του CALDERA αντικατοπτρίζει το τι κάνουν οι επιτιθέμενοι αφού αρχικά εισέλθουν σε ένα δίκτυο, το οποίο διαφέρει σημαντικά από το πώς συμπεριφέρονται πριν, κατά την προσπάθεια τους να αποκτήσουν πρόσβαση σε αυτό. Υποθέτοντας ότι ένας εισβολέας έχει ήδη αποκτήσει πρόσβαση σε ένα δίκτυο, το CALDERA δοκιμάζει τρόπους άμυνας οι οποίοι έχουν αδυναμίες σε ένα δίκτυο και δεν έχουν δοκιμαστεί. Σημαντική έμφαση από τους σχεδιαστές των δικτύων δίνεται συνήθως στις περιμετρικές άμυνες όπως είναι τα firewalls, ή μία Demilitarized Zone (DMZ). Με άλλα λόγια, επενδύονται πολλά σε άμυνες που αποσκοπούν στην αποφυγή της αρχικής πρόσβασης, συχνά εις βάρος των αμυντικών τεχνικών που έχουν σχεδιαστεί για την πρόληψη ή την ανίχνευση μιας δραστηριότητας μετά την παραβίαση του δικτύου. Η μετά την παραβίαση λογική που χρησιμοποιεί το CALDERA σημαίνει ότι δοκιμάζει τους τομείς ασφάλειας που συνήθως παραμελούνται κατά τον σχεδιασμό της ασφάλειας ενός δικτύου.
Το CALDERA υποστηρίζει μόνο δίκτυα με λειτουργικό σύστημα Windows τα οποία έχουν ρυθμιστεί ως Windows Domain. Αυτό συμβαίνει επειδή οι τεχνικές και οι τακτικές που ενσωματώνονται μέχρι αυτή την στιγμή στο CALDERA είναι μοναδικές για Windows Domain. Παρ 'όλα αυτά, ο διακομιστής (server) του CALDERA μπορεί να εγκατασταθεί σε Linux ή Windows.

4.3 Αρχιτεκτονική

CALDERA αποτελείται από:

Server

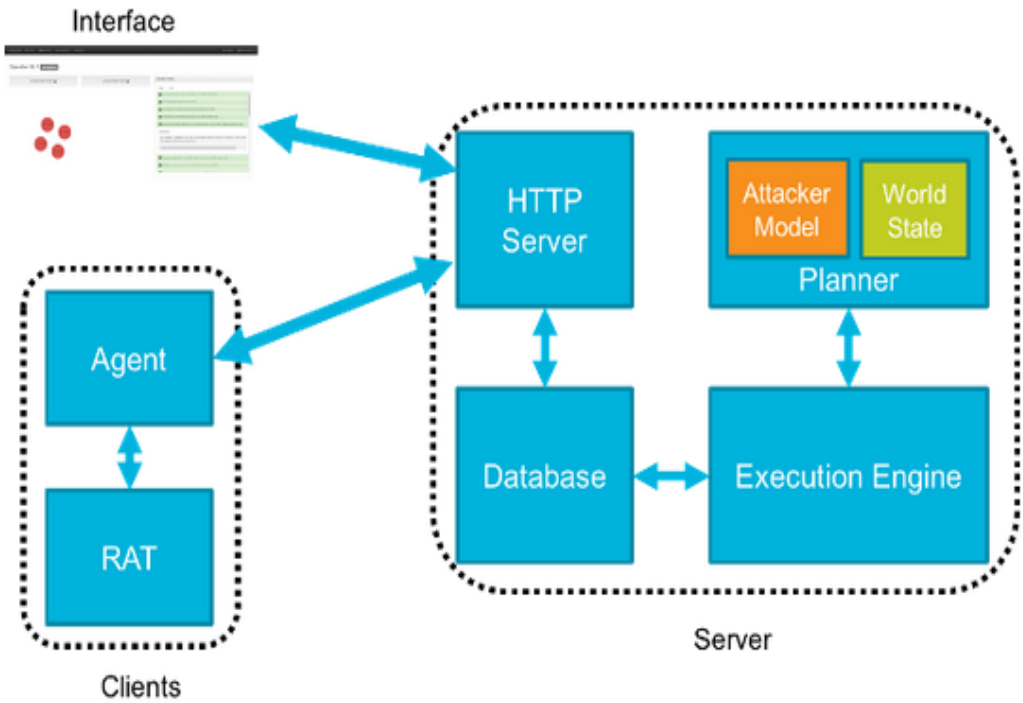
Planner – Μηχανισμός απόφασης που επιτρέπει στο CALDERA να επιλέξει δράσεις

Attacker Model – Δράσεις διαθέσιμες βασισμένες στο μοντέλο ATT&CK
World Model – Το οποίο αντιπροσωπεύει το περιβάλλον

Execution Engine – Ενεργοποιεί τις τεχνικές και ενημερώνει τη βάση δεδομένων
Database – Αποθηκεύει τις γνώσεις οι οποίες αποκτώνται από το περιβάλλον
HTTP Server

Clients

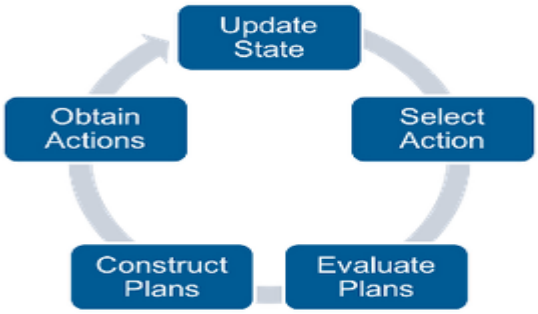
Agent – Client στα τερματικά συστήματα ο οποίος χρησιμοποιείται για την επικοινωνία
RAT – Εργαλείο απομακρυσμένης πρόσβασης που χρησιμοποιείται κατά τη διάρκεια των δοκιμών για να προσομοιώσει τη συμπεριφορά των αντιπάλων



Εικόνα 9 : Αρχιτεκτονική του CALDERA

Planning System

Το σύστημα σχεδιασμού του CALDERA του επιτρέπει να "αποφασίσει" για την επόμενη καλύτερη δράση που πρέπει να αναλάβει με βάση τις τρέχουσες γνώσεις που έχει αποκτήσει για το περιβάλλον και τις διαθέσιμες ενέργειες στο συγκεκριμένο χρονικό σημείο. Το μοντέλο εισβολέα του CALDERA αντιπροσωπεύεται από τις τεχνικές οι οποίες έχουν διαμορφωθεί από πριν και βασίζονται στο μοντέλο ATT&CK, οι οποίες επιτρέπουν στο CALDERA να συνδέσει μαζί τις ακολουθίες των ενεργειών που πρέπει να εφαρμοστούν για να φτάσει σε μια αντικειμενική κατάσταση.



Εικόνα 10 : Σύστημα Σχεδιασμού του CALDERA

Νέες τεχνικές μπορούν να προστεθούν στο CALDERA και αυτό είναι θετικό γιατί βοηθάει στο να αναπτυχθούν νέες τεχνικές καθώς και παραλλαγές αυτών και με τον τρόπο αυτό είναι δυνατόν να αντιπροσωπευτούν και να αντιμετωπιστούν πιο αποτελεσματικά οι τρόποι συμπεριφοράς των αντιπάλων.

4.4 Απαιτήσεις και περιορισμοί

Οι δοκιμές που έχει σχεδιαστεί για να εκτελέσει το CALDERA για να εντοπίσει συμπεριφορές αντιπάλων είναι εξονυχιστικές σε βάθος. Ενώ ο διακομιστής του CALDERA δεν διαθέτει κάποιες απαιτήσεις σε hardware, υπάρχουν περιορισμοί στον αριθμό των συστημάτων που μπορεί να λειτουργήσει το CALDERA, ώστε ο χρόνος που απαιτείται μεταξύ των ενεργειών να μην προκαλέσει σημαντικές καθυστερήσεις ή να οδηγήσει το σύστημα στο να αποτύχει. Για το λόγο αυτό δεν συνιστάται η χρήση του CALDERA έναντι ομάδων συστημάτων μεγαλύτερων από 20 υπολογιστών.
Το CALDERA εκτελεί πραγματικές ενέργειες στα συστήματα κατά τη διάρκεια της λειτουργία του. Για το λόγο αυτό εάν χρησιμοποιείται σε ένα πραγματικό δίκτυο και όχι σε ένα απομονωμένο εργαστηριακό δίκτυο, θα πρέπει να ληφθεί μέριμνα ώστε να ενημερωθεί οπωσδήποτε το προσωπικό ασφάλειας δικτύων, οι διαχειριστές ή χρήστες που μπορεί να επηρεαστούν από την χρήση του CALDERA ώστε να αποκατασταθούν τυχόν ζητήματα που ενδεχομένως να προκύψουν.
Το CALDERA χρησιμοποιεί επιπλέον και εργαλεία ανοιχτού κώδικα τα οποία χρησιμοποιούνται και την εκτέλεση των διαφόρων τεχνικών. Ορισμένα από αυτά τα εργαλεία κατηγοριοποιούνται ως penetration testing εργαλεία ή εργαλεία ελέγχου ασφάλειας και ενδεχομένως μερικά antivirus να τα θεωρήσουν ως επιβλαβές λογισμικό.

Το CALDERA δεν χρησιμοποιεί κάποιο εργαλείο το οποίο να θεωρείται κακόβουλο και να το χρησιμοποιούν οι αντίπαλοι. Επικεντρώνεται στη χρήση κακόβουλης συμπεριφοράς των αντιπάλων η οποία είναι τεκμηριωμένη σύμφωνα με τοι μοντέλο ATT&CK και η οποία μπορεί να χρησιμοποιηθεί με πολλούς διαφορετικούς τρόπους ανεξάρτητα από την χρήση κακόβουλου λογισμικού που ενδεχομένως να χρησιμοποιήσει ένας αντίπαλος.
Το CALDERA επίσης δεν χρησιμοποιεί κάποιο λογισμικό για εκμετάλλευση (exploitation). Υπάρχουν πολλά ελεύθερα και εμπορικά εργαλεία που μπορούν να χρησιμοποιηθούν για να εκτιμηθεί η αδυναμία και η δυνατότητα εκμετάλλευσης ενός λογισμικού. Το CALDERA όμως δεν είναι σχεδιασμένο για να χρησιμοποιείται για το σκοπό αυτό.

4.5 Εγκατάσταση και χρήση του CALDERA

ΠΕΡΙΒΑΛΛΟΝ ΔΟΚΙΜΩΝ

HARDWARE

Το hardware που χρησιμοποιήθηκε για την ανάπτυξη δικτύου των δοκιμών αποτελείται από σταθερό υπολογιστή με τα παρακάτω χαρακτηριστικά:

- Επεξεργαστής : i7 – 3770
- Κάρτα Γραφικών : Nvidia GeForce GT 620
- Μνήμη : 32 Gb

SOFTWARE

Το λειτουργικό σύστημα που χρησιμοποιήθηκε στον συγκεκριμένο σταθερό υπολογιστή είναι Windows 10. Επιπλέον για τις ανάγκες των δοκιμών δημιουργήθηκαν σε εικονικές μηχανές (VMs) σε VMware Workstation Pro τα παρακάτω :

- Ένα VM με λειτουργικό σύστημα Windows 2016 Server
- Δύο VMs με λειτουργικό σύστημα Windows 10
- Ένα VM με λειτουργικό σύστημα Windows 10 για την εγκατάσταση του Caldera Server

Σκοπός είναι η δημιουργία ενός δοκιμαστικού δικτύου που θα αποτελείται από δυο VMs με Windows 10 συνδεδεμένοι σε ένα domain με όνομα test.net που έχουμε δημιουργήσει με το Windows 2016 Server. Στο συγκεκριμένο δίκτυο θα δοκιμαστούν τα εργαλεία του Red Teaming, Caldera και Red Team Automation. Η δημιουργία και η διαμόρφωση ενός Windows Domain καθώς και η σύνδεση σταθμών εργασίας στο συγκεκριμένο Domain δεν εμπίπτει στα πλαίσια της συγκεκριμένης εργασίας και για το λόγο αυτό δεν θα γίνει περιγραφή της διαδικασίας που ακολουθήθηκε για τη δημιουργία του.

Εγκατάσταση CALDERA

Το CALDERA αποτελείται από τρία ξεχωριστά «κομμάτια» λογισμικού :

- **CALDERA server**

Ο server ελέγχει την εκτέλεση του CALDERA και περιέχει web interface για τη διαχείρισή του.

- **CALDERA agent**

Μια υπηρεσία των Windows που επικοινωνεί με τον server του CALDERA. Ο CALDERA agent είναι εγκατεστημένος σε κάθε υπολογιστή που συμμετέχει σε δραστηριότητες εξομοίωσης αντιπάλων.

- **Crater**

Ένα εκτελέσιμο των Windows που χρησιμοποιείται για τις ασκήσεις εξομοίωσης αντιπάλων.

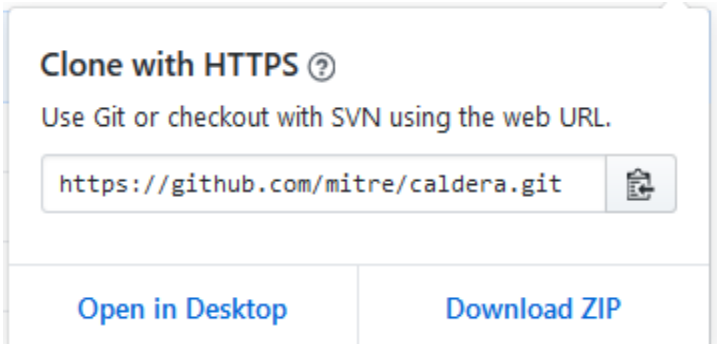
Στην αρχή θα γίνει περιγραφή της διαδικασίας εγκατάστασης του CALDERA Server μαζί με το Crater και στην συνέχεια της διαδικασίας εγκατάστασης του CALDERA Agent σε κάθε υπολογιστή που συμμετέχει στο δίκτυο των δοκιμών.

CALDERA Server Installation

Ο CALDERA Server είναι εγκατεστημένος σε έναν κεντρικό εξυπηρετητή. Θα πρέπει να είναι προσβάσιμος μέσω του δικτύου σε όλους τους υπολογιστές που συμμετέχουν στη λειτουργία προσομοίωσης αντίπαλων. Μπορεί να εγκατασταθεί σε συστήματα με λειτουργικό σύστημα τόσο Windows όσο και Linux. Στα πλαίσια της εργασίας θα περιγραφεί η διαδικασία εγκατάστασης σε Windows.

ΒΗΜΑ 1ο :

Από την σελίδα https://github.com/mitre/caldera κατεβάζουμε το αρχείο ZIP του CALDERA και το κάνουμε UNZIP στον υπολογιστή.



Εικόνα 11 : Κατέβασμα του αρχείου zip από github

ΒΗΜΑ 2ο :
Από την σελίδα https://www.python.org/downloads/ κατεβάζουμε και κάνουμε εγκατάσταση την έκδοση της Python 3.5.4 ή και νεότερη.

ΒΗΜΑ 3ο :

Με την εντολή **pip install --upgrade setuptools** κάνουμε αναβάθμιση το πακέτο setuptools της Python.

ΒΗΜΑ 4ο :

Κάνουμε εγκατάσταση το Visual C++ 2015 Build Tools και επιλέγουμε τις επιλογές Windows 8.1 SDK and Windows 10 SDK όπως στην εικόνα 12.

Εικόνα 12 : Εγκατάσταση του Visual C++ 2015 Build Tools

ΒΗΜΑ 5ο :

Στο folder caldera-master/caldera με την εντολή **pip install -r requirements.txt** κατεβάζουμε και κάνουμε εγκατάσταση τις βιβλιοθήκες της Python οι οποίες είναι απαραίτητες για να λειτουργήσει ο CALDERA Server.

ΒΗΜΑ 6ο :

Κάνουμε εγκατάσταση της MongoDB 3.0 ή νεότερης έκδοσης από την σελίδα https://www.mongodb.com/download-center/community. Στη συνέχεια ξεκινάμε την MongoDB με την εντολή **mongod.exe --bind_ip 127.0.0.1 --replSet caldera** (εικόνα 13)

```
C:\Program Files\MongoDB\Server\3.4\bin>mongod.exe --bind_ip 127.0.0.1 --replSet caldera
2019-01-25T02:42:22.148-0800 I CONTROL  [initandlisten] MongoDB starting : pid=7584 port=27017 dbpa
th=C:\data\db\ 64-bit host=victim1
2019-01-25T02:42:22.148-0800 I CONTROL  [initandlisten] targetMinOS: Windows 7/Windows Server 2008
R2
2019-01-25T02:42:22.148-0800 I CONTROL  [initandlisten] db version v3.4.18
2019-01-25T02:42:22.150-0800 I CONTROL  [initandlisten] git version: 4410706bef6463369ea2f42399e984
3903b31923
2019-01-25T02:42:22.150-0800 I CONTROL  [initandlisten] OpenSSL version: OpenSSL 1.0.2o-fips  27 Ma
r 2018
2019-01-25T02:42:22.150-0800 I CONTROL  [initandlisten] allocator: tcmalloc
```

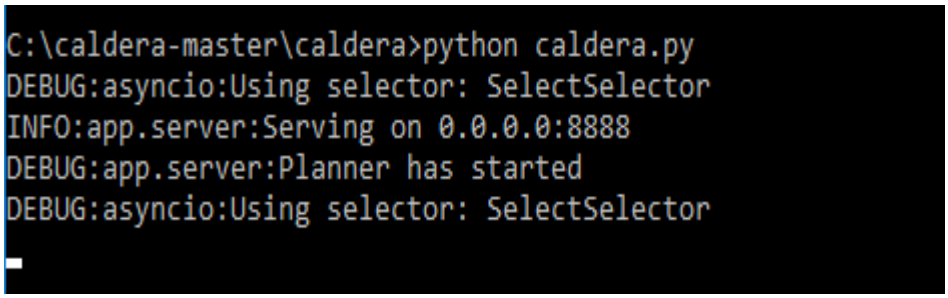
Εικόνα 13 : Εκκίνηση της MongoDB

ΒΗΜΑ 7ο :

Κατεβάζουμε το Crater από την σελίδα https://github.com/mitre/caldera-crater/releases και το κάνουμε εγκατάσταση στο folder : caldera-master\dep\crater\crater

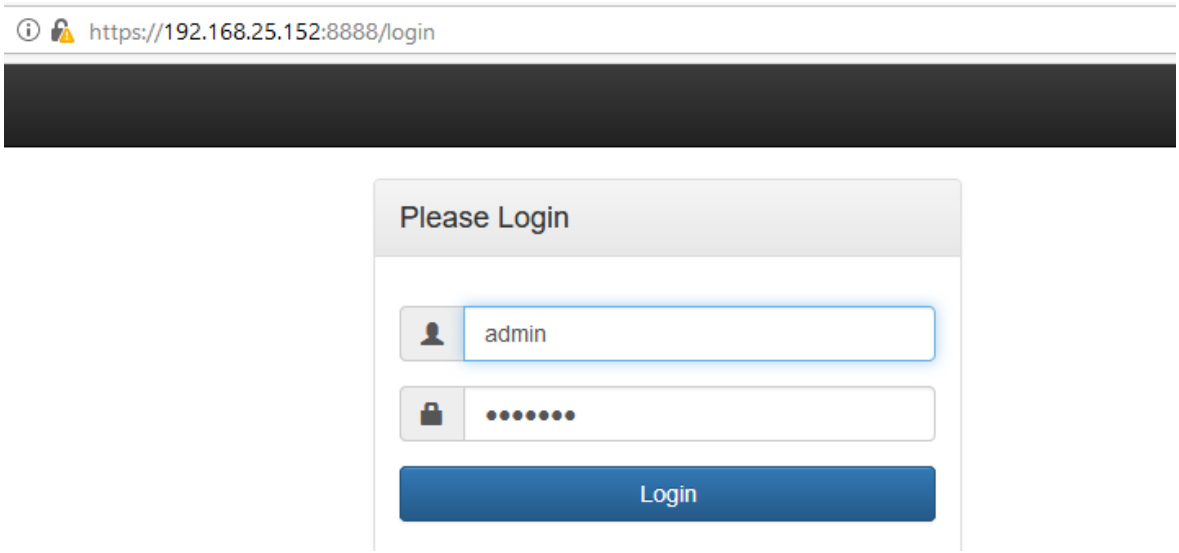
ΒΗΜΑ 8ο :

Στο folder caldera-master/caldera ξεκινάμε τον CALDERA Server με την εντολή **python caldera.py** (εικόνα 14)



Εικόνα 14 : Εκκίνηση του CALDERA Server

Μετά την εκκίνηση του Server από ένα browser ανοίγουμε το web interface του https://localhost:8888 όπως στην εικόνα 15 και χρησιμοποιούμε **username: admin password : caldera**.



Εικόνα 15 : Είσοδος στο CALDERA Server

ΒΗΜΑ 9ο :

Κατεβάζουμε και εγκαθιστούμε από την σελίδα https://www.microsoft.com/en-us/download/details.aspx?id=48145 το Visual C++ Redistributable for Visual Studio 2015 σε κάθε υπολογιστή του δικτύου και στην συνέχεια από την σελίδα https://github.com/mitre/caldera-agent/releases κατεβάζουμε το cagent.exe και το τοποθετούμε σε ένα folder στην τοποθεσία **C:\Program Files\cagent.** Στο ίδιο folder τοποθετούμε και το **conf.yml** το οποίο το κατεβάζουμε από τον CALDERA

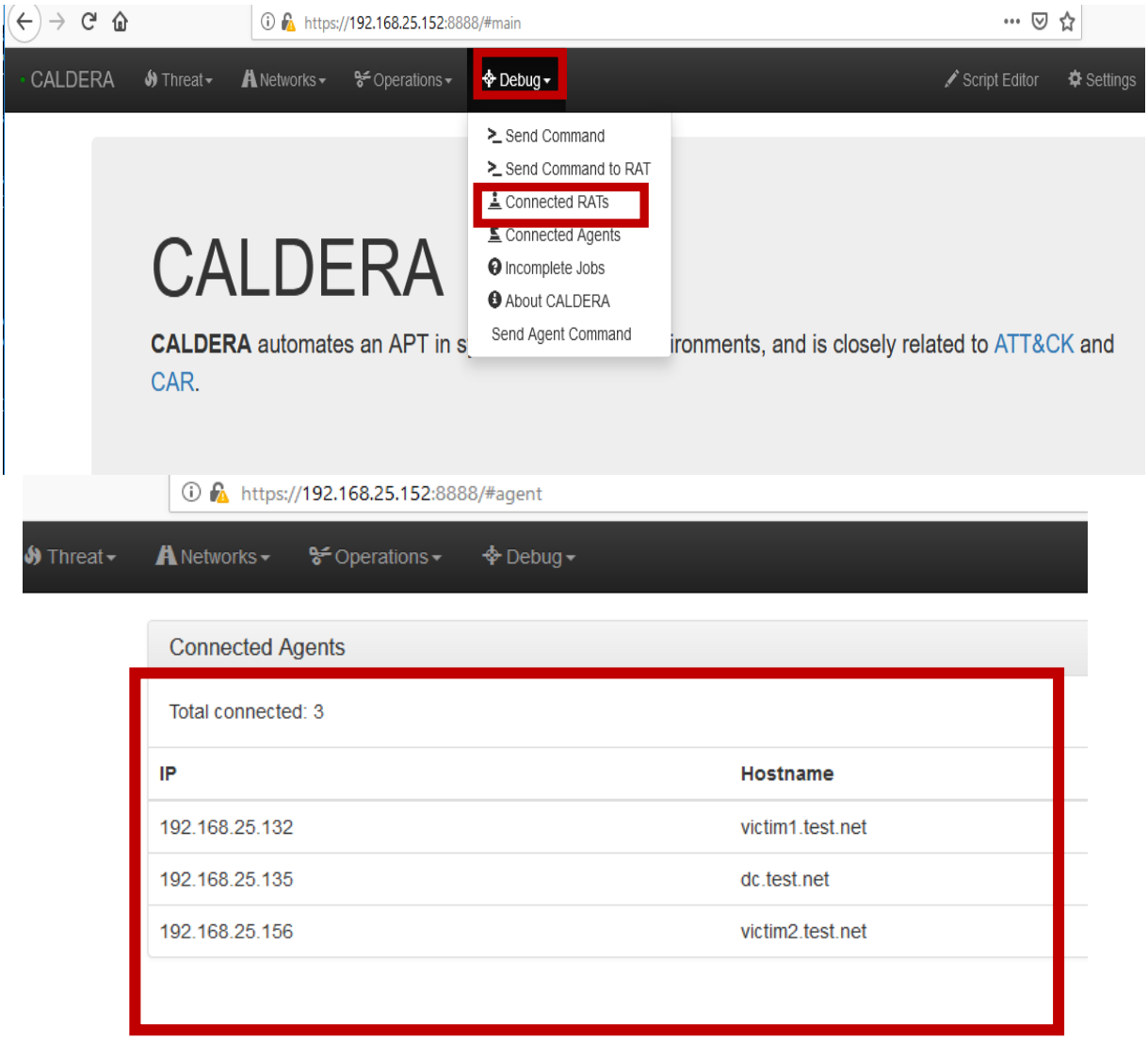
server https://192.168.25.152:8888/conf.yml. Στην συνέχεια με δικαιώματα Administrator από το command prompt κάνουμε εγκατάσταση και εκκινούμε την υπηρεσία του cagent (εικόνα 16).

```
C:\Program Files\cagent>cagent.exe --startup auto install
Installing service cagent
Changing service configuration
Service updated

C:\Program Files\cagent>cagent.exe start
Starting service cagent
```

Εικόνα 16 : Εγκατάσταση και εκκίνηση υπηρεσίας cagent

Η διαδικασία αυτή πρέπει να γίνει σε κάθε υπολογιστή ο οποίος συμμετέχει στην προσομοίωση του αντιπάλου. Οι Agents οι οποίοι είναι συνδεδεμένοι με τον CALDERA server είναι ορατοί επιλέγοντας την καρτέλα **Debug>Connected Agents** όπως φαίνεται στην εικόνα 17:

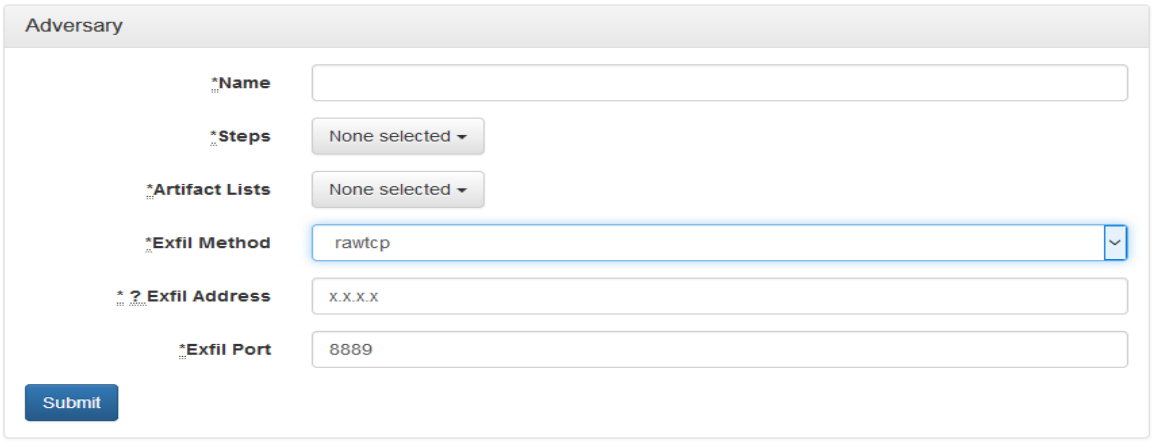


Εικόνα 17 : Συνδεδεμένοι Agents στον CALDERA server

Πραγματοποιώντας την πρώτη λειτουργία

Δημιουργία ενός αντιπάλου

Για να εκτελεστεί μια λειτουργία, το CALDERA χρειάζεται να προσομοιώσει έναν αντίπαλο. Στο CALDERA, ένας αντίπαλος αντιπροσωπεύει τις τακτικές και τις τεχνικές ενός πραγματικού αντιπάλου. Όταν δημιουργούμε μια λειτουργία, θα επιλέξουμε έναν αντίπαλο ο οποίος θα χρησιμοποιηθεί για να υπαγορεύει ποιες τεχνικές θα εκτελεί το CALDERA κατά τη διάρκεια της λειτουργίας. Μέσα από το μενού **Threat > Create Adversary** θα οδηγηθούμε στην σελίδα δημιουργίας αντιπάλου όπως στην εικόνα 18.



Εικόνα 18 : Δημιουργία αντιπάλου στο CALDERA

Name

Σε αυτό το πεδίο θα δώσουμε το όνομα στον αντίπαλο που θα δημιουργήσουμε. Θα δώσουμε το όνομα all_test για να εκτελέσουμε όλα τα βήματα που περιέχονται στο επόμενο πεδίο.

Steps

Σε αυτό το πεδίο ορίζουμε τις ατομικές ενέργειες που επιτρέπεται στον αντίπαλο να εκτελέσει. Τα βήματα είναι ο κύριος τρόπος με τον οποίο μπορούμε να αλλάξουμε τη συμπεριφορά του αντιπάλου. Κάθε βήμα δίνει στον αντίπαλο νέες ικανότητες για να εκτελέσει. Τα βήματα έχουν ένα όνομα και επιπλέον συνδέονται με το ATT&CK ID και την τακτική του μοντέλου ATT&CK. Μερικά από τα βήματα και ο τρόπος εμφάνισης τους φαίνεται παρακάτω:

- copy_file: [T1105, Lateral Movement]
- get_creds: [T1003, Credential Access]
- get_admin: [T1086, Execution | T1069 & T1087, Discovery]
- get_computers: [T1086, Execution | T1018, Discovery]
- get_domain: [T1016, Discovery]
- net_use: [T1077, Lateral Movement]
- remote_process(WMI): [T1047, Execution]

Artifact Lists

Οι λίστες αυτές επιτρέπουν να προσαρμόσουμε τα αντικείμενα που αφήνει ο αντίπαλός που δημιουργήσαμε. Αυτά τα αντικείμενα περιλαμβάνουν τα ονόματα αρχείων και υπηρεσιών. Αφήνουμε αυτό το πεδίο κενό για να χρησιμοποιήσουμε την προεπιλεγμένη λίστα Artifact.

Exfil Method

Αυτό το πεδίο καθορίζει τον τρόπο με τον οποίο ο αντίπαλος θα κάνει εξαγωγή των δεδομένων. Οι επιλογές είναι οι παρακάτω :

- **raw_tcp** – εξαγωγή δεδομένων χρησιμοποιώντας tcp πρωτόκολλο
- **http** – εξαγωγή δεδομένων χρησιμοποιώντας http πρωτόκολλο
- **https** – εξαγωγή δεδομένων χρησιμοποιώντας https πρωτόκολλο

Exfil Address

Σε αυτό το πεδίο δηλώνεται η διεύθυνση IP που θα χρησιμοποιηθεί για την εξαγωγή των δεδομένων από το CALDERA. Αφήνοντας το με την τιμή x.x.x.x θα χρησιμοποιηθεί αυτόματα η διεύθυνση IP του CALDERA.

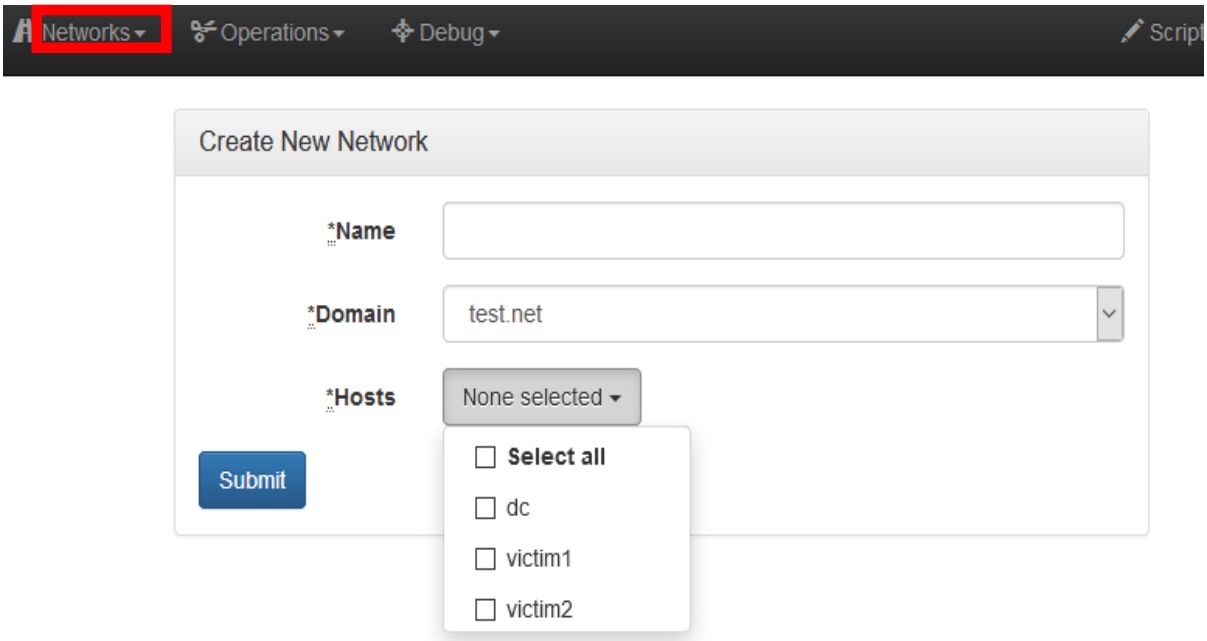
Exfil Port

Στο πεδίο αυτό δηλώνεται η θύρα TCP την οποία θα χρησιμοποιήσει για να κάνει εξαγωγή των δεδομένων το CALDERA. Χρησιμοποιούμε την προεπιλεγμένη τιμή.

Όταν συμπληρώσουμε τα πεδία αυτά επιλέγοντας το «Submit» βλέπουμε να δημιουργείται ο νέος αντίπαλος.

Δημιουργία δικτύου

Στην καρτέλα **Networks > Create Network** θα δούμε την σελίδα όπου θα δημιουργήσουμε το δίκτυο στο οποίο θα δοκιμάσουμε την προσομοίωση του αντιπάλου. Υπάρχουν μερικά πεδία που θα συμπληρώσουμε όπως στην εικόνα 19 όπου θα ρυθμίσουμε τις παραμέτρους του δικτύου.



Εικόνα 19 : Δημιουργία δικτύου στο CALDERA server

Name

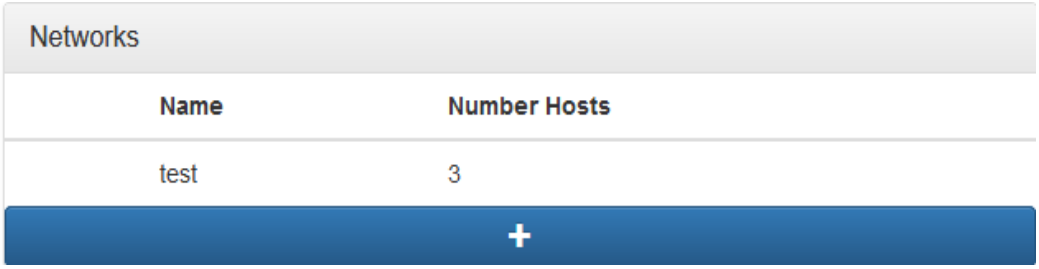
Σε αυτό το πεδίο μπορούμε να ονομάσουμε το δίκτυο που θέλουμε να δημιουργήσουμε. Για αυτό το παράδειγμα το δίκτυο θα το ονομάσουμε test.

Domain

Σε αυτό το πεδίο μπορούμε να επιλέξουμε το όνομα του domain των υπολογιστών που θέλουμε να συμπεριλάβουμε σε αυτή την άσκηση. Κάθε υπολογιστής σε ένα δίκτυο πρέπει να προέρχεται από το ίδιο domain. Για αυτό το παράδειγμα, επιλέγουμε το domain test.net το οποίο εμφανίζεται ως διαθέσιμο.

Hosts

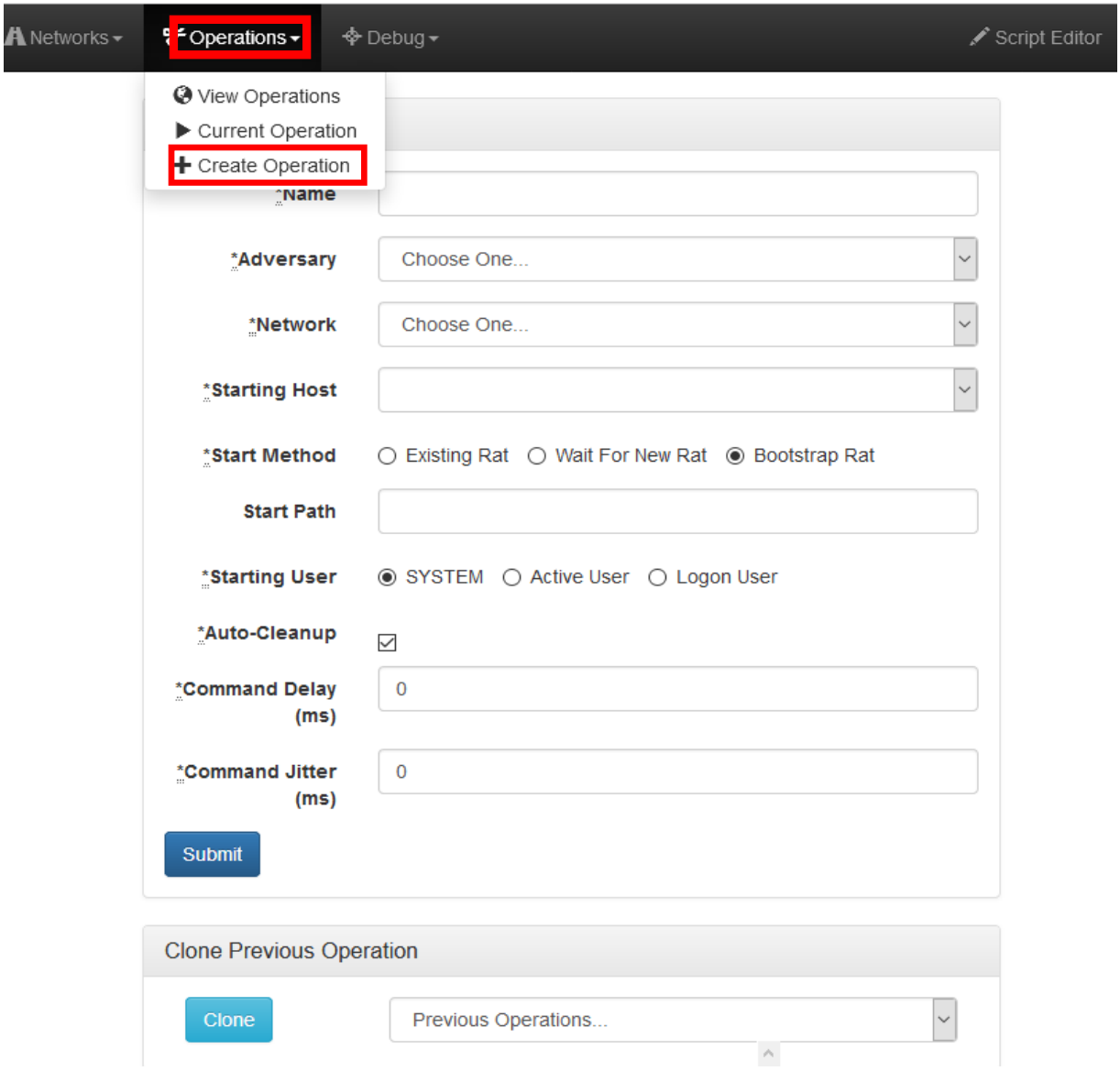
Μόλις επιλέξουμε το domain, στο πεδίο Hosts θα εμφανιστούν οι υπολογιστές του δικτύου στους οποίους είναι εγκατεστημένοι οι cagents. Επιλέγουμε όσους από τους εμφανιζόμενους υπολογιστές θέλουμε να συμμετάσχουν στην προσομοίωση. Για αυτό το παράδειγμα επιλέγουμε την επιλογή **Select all** και πατάμε την επιλογή Submit και δημιουργούμε το δίκτυο της εικόνας 20.



Εικόνα 20 : Δημιουργία δικτύου με το όνομα test

ΔΗΜΙΟΥΡΓΙΑ ΜΙΑΣ ΔΙΑΔΙΚΑΣΙΑΣ

Σε αυτή την στιγμή αφού έχουμε δημιουργήσει έναν αντίπαλο και ένα δίκτυο μπορούμε να δημιουργήσουμε την πρώτη διαδικασία. Στην καρτέλα **Operations > Create Operation** εμφανίζεται το περιεχόμενο της εικόνας 21 με τα αντίστοιχα πεδία που πρέπει να συμπληρωθούν και τα οποία θα αναλυθούν στην συνέχεια.



Εικόνα 21 : Δημιουργία διαδικασίας στο CALDERA

Name

Σε αυτό το πεδίο δίνουμε το όνομα της διαδικασίας που θα δημιουργήσουμε

Adversary

Σε αυτό το πεδίο θα επιλέξουμε τον αντίπαλο που δημιουργήσαμε προηγουμένως και ο οποίος θα εκτελέσει τα βήματα που του έχουμε καθορίσει κατά την διάρκεια

της διαδικασίας. Σε αυτό το παράδειγμα θα επιλέξουμε τον επιτιθέμενο με το όνομα **all_tests**.

Network

Σε αυτό το πεδίο θα επιλέξουμε το δίκτυο για αυτή την συγκεκριμένη διαδικασία, το οποίο θα περιορίσει το πεδίο της λειτουργίας της στους υπολογιστές που περιέχονται στο συγκεκριμένο δίκτυο. Επιλέγουμε το δίκτυο που δημιουργήσαμε νωρίτερα με το όνομα **test**.

Starting Host

Στο πεδίο αυτό επιλέγουμε τον υπολογιστή που θέλουμε να ξεκινήσει η διαδικασία και στις επιλογές που εμφανίζονται επιλέγουμε τον υπολογιστή με το όνομα **dc** που είναι ο server που έχουμε δημιουργήσει.

Start Method

Στο πεδίο αυτό έχουμε την επιλογή διαμορφώσουμε τον τρόπο δημιουργίας του αρχικού RAT (Remote Access Tool). Επειδή το CALDERA υποθέτει ότι ένα δίκτυο έχει ήδη παραβιαστεί, ξεκινά με ένα RAT που εκτελείται στον αρχικό κεντρικό υπολογιστή. Οι επιλογές που μας επιτρέπει να ρυθμίσουμε για τον τρόπο δημιουργίας του RAT είναι οι παρακάτω :

- **Existing Rat** - Αν ένα RAT είναι ήδη συνδεδεμένο με το CALDERA, μπορούμε να το χρησιμοποιήσετε ως RAT εκκίνησης. Αν επιλέξουμε αυτήν την επιλογή, θα εμφανιστεί ένα επιπλέον πεδίο που ονομάζεται " Starting Rat" που θα μας επιτρέψει να επιλέξουμε το RAT με τον οποίο θα θέλουμε να ξεκινήσουμε.

- **Wait For New Rat** - Αν θέλουμε να ξεκινήσουμε το RAT χειροκίνητα, μπορούμε να επιλέξουμε αυτήν την επιλογή και το CALDERA να περιμένει ένα Rat να συνδεθεί.

- **Bootstrap Rat** - Το CALDERA μπορεί να ξεκινήσει αυτόματα ένα RAT στον υπολογιστή που έχουμε επιλέξει να ξεκινήσει η διαδικασία. Στη διαδικασία που θα δημιουργήσουμε θα επιλέξουμε αυτήν την επιλογή.

Start Path

Στο πεδίο αυτό μπορούμε να πούμε στο CALDERA πού θέλουμε να τοποθετηθεί το εκτελέσιμο αρχείο Rat. Στη διαδικασία που θα δημιουργήσουμε αφήνουμε αυτό το πεδίο κενό για να χρησιμοποιήσουμε την προεπιλεγμένη θέση.

Starting User

Το Rat μπορεί να ξεκινήσει σε πολλά διαφορετικά περιβάλλοντα χρηστών. Αυτό το πεδίο μας επιτρέπει να επιλέξουμε το χρήστη που θα θέλαμε να ξεκινήσει το Rat.

- **System** - Αυτός είναι ο λογαριασμός του συστήματος. Στο παράδειγμα μας χρησιμοποιούμε αυτή την επιλογή.

- **Active User** – Αυτή η επιλογή θα ξεκινήσει το Rat στο λογαριασμό του χρήστη ο οποίος έχει συνδεθεί. Εάν επιλέξουμε αυτή την επιλογή, θα εμφανιστεί ένα πεδίο που ονομάζεται "Parent Process" που θα μας επιτρέψει να εισαγάγουμε μια διαδικασία που θα χρησιμοποιηθεί για το Rat.

- **Logon User** – Αυτή η επιλογή θα μας επιτρέψει να εισάγουμε έναν συγκεκριμένο λογαριασμό χρήστη που θα χρησιμοποιήσουμε. Εάν επιλέξουμε αυτήν την επιλογή, θα εμφανιστούν δύο πεδία για να εισαγάγουμε το όνομα χρήστη και τον κωδικό πρόσβασης του λογαριασμού στον οποίο θέλουμε να εκτελεστεί το Rat.

Auto-Cleanup

Το CALDERA έχει την ικανότητα να «καθαρίζει» τις τεχνικές που χρησιμοποιήθηκαν μετά από το τέλος της κάθε διαδικασίας. Με λίγες εξαιρέσεις, κάθε τεχνική που εκτελεί το CALDERA μπορεί να καθαριστεί. Επιλέγοντας αυτό το πεδίο θα πραγματοποιηθεί αυτόματα η εκκαθάριση όταν ολοκληρωθεί η διαδικασία στο CALDERA. Αν δεν επιλέξουμε αυτό το πεδίο μας δίνεται η δυνατότητα να ενεργοποιήσουμε χειροκίνητα την εκκαθάριση μετά την ολοκλήρωση της διαδικασίας.

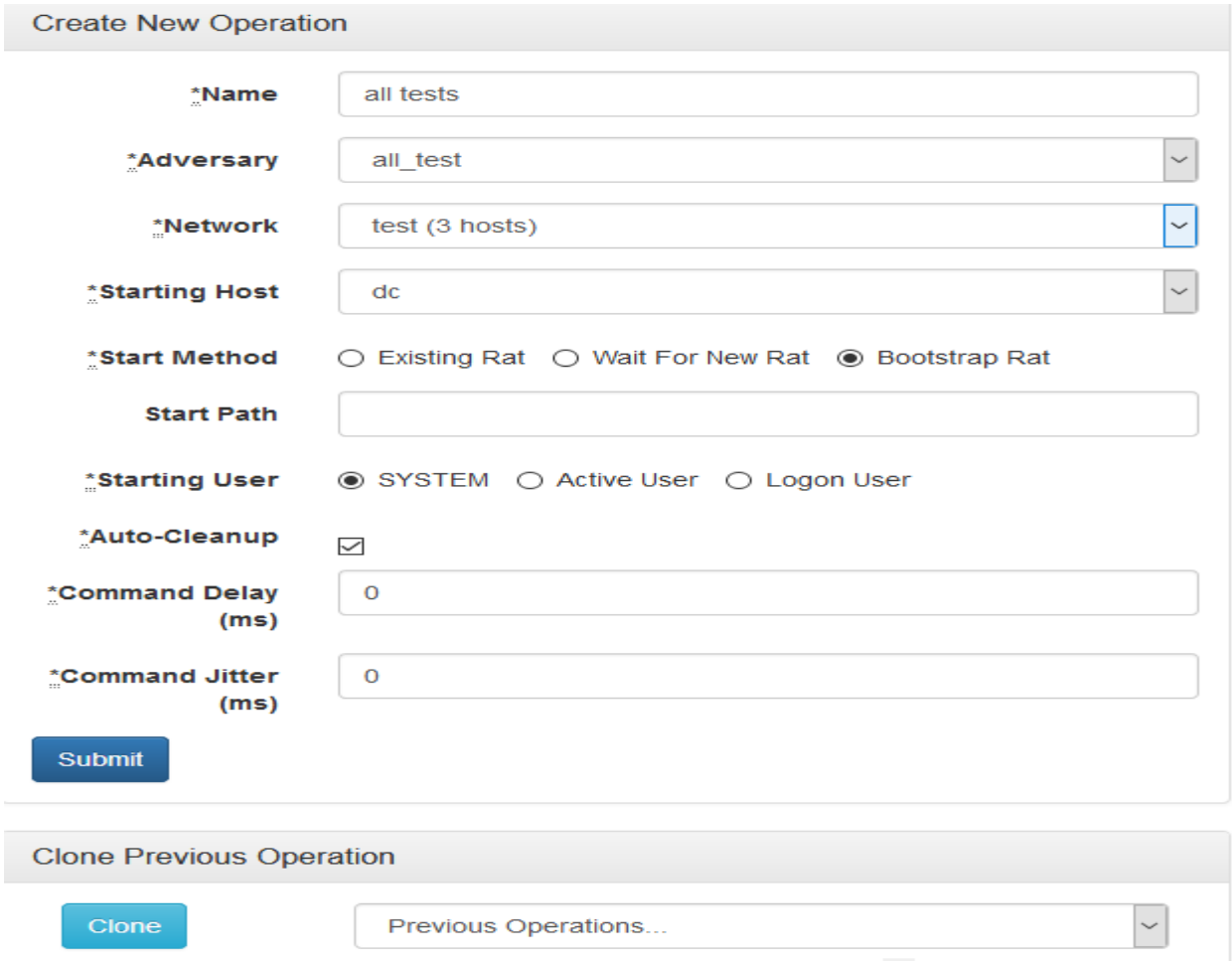
Command Delay (ms) & Command Jitter (ms)

Το CALDERA συνήθως εκτελεί τις τεχνικές πολύ γρήγορα. Εάν θέλουμε να εισάγουμε κάποια διαφοροποίηση στο πόσο γρήγορα θα λειτουργεί το CALDERA, μπορούμε να το επιβραδύνουμε τεχνητά προσθέτοντας καθυστέρηση και διακύμανση. Στο παράδειγμα μας στα πεδία αυτά θα αφήσουμε την τιμή 0.

Clone Previous Operation

Επιπλέον υπάρχει μια επιλογή για την κλωνοποίηση μιας προηγούμενης διαδικασίας. Αυτή η επιλογή μας επιτρέπει να αντιγράψουμε γρήγορα τις ρυθμίσεις από μια προηγούμενη διαδικασία.

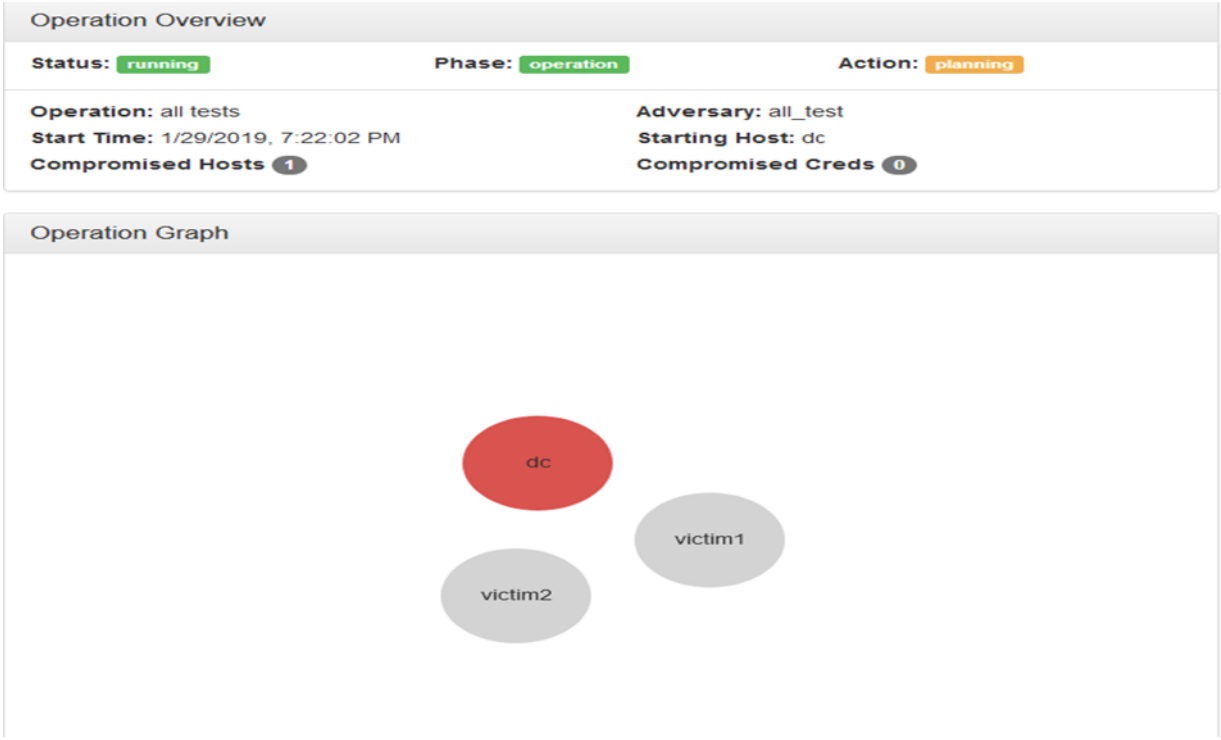
Αφού έχουμε συμπληρώσει όλα τα πεδία για το παράδειγμα μας η διαδικασία μας θα εμφανίζεται όπως την εικόνα 22 και πατώντας την επιλογή Submit δημιουργείται και εκτελείται η διαδικασία της εικόνας 23.



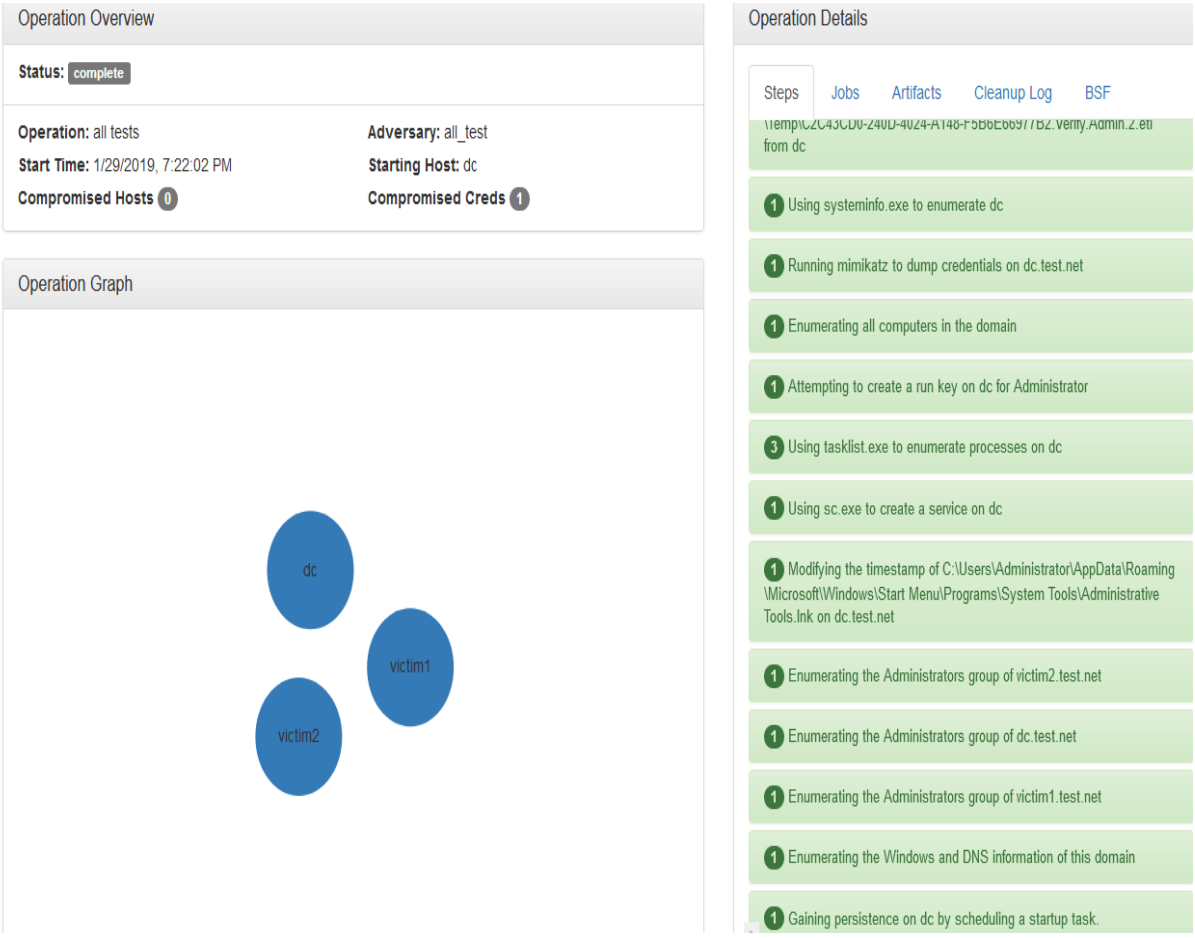
Εικόνα 22 : Συμπλήρωση πεδίων κατά την δημιουργία της διαδικασίας

Παρατηρώντας την διαδικασία

Στην προβολή της διαδικασίας, μπορούμε να δούμε την πρόοδο που έχει κάνει το CALDERA κατά την διάρκεια της. Η κατάσταση της διαδικασίας εμφανίζεται στο επάνω μέρος της οθόνης δίπλα στο όνομα της διαδικασίας όπως φαίνεται στην εικόνα 24. Κάτω από την κατάσταση, υπάρχει ένα γράφημα της διαδικασίας στο οποίο έγχρωμες φυσαλίδες υποδεικνύουν τον αριθμό των υπολογιστών οι οποίοι έχουν παραβιαστεί κατά τη διάρκεια αυτής της διαδικασίας. Οι φυσαλίδες αλλάζουν χρώμα σύμφωνα με την πρόοδο της διαδικασίας του CALDERA όσον αφορά την υπονόμευση του δικτύου. Κάθε φυσαλίδα αντιπροσωπεύει έναν υπολογιστή στο εσωτερικό του δικτύου. Οι φυσαλίδες ξεκινούν με γκρι χρώμα. Όταν το CALDERA ανακαλύψει έναν υπολογιστή, η φυσαλίδα του υπολογιστή γίνεται μπλε. Όταν το CALDERA τοποθετεί ένα Rat στον υπολογιστή, τότε η φυσαλίδα γίνεται κόκκινη.
Στα δεξιά υπάρχει παράθυρο που ονομάζεται "Operation Details" όπως φαίνεται στην εικόνα 24. Αυτό έχει πολλές καρτέλες που μας επιτρέπουν δούμε διάφορες λεπτομέρειες όσον αφορά την διαδικασία.



Εικόνα 23 : Δημιουργημένη διαδικασία στο CALDERA



Εικόνα 24 : Επισκόπηση της διαδικασίας

Προσθήκη νέας τεχνικής στο CALDERA

Το CALDERA έχει σχεδιαστεί για να είναι πλήρως αυτοματοποιημένο. Για τη δημιουργία ενός εντελώς αυτοματοποιημένου συστήματος, υπάρχει μια τάση ανάμεσα στο να αφήσουμε το σύστημα να αποφασίσει το τι θα κάνει ή να πούμε εμείς στο σύστημα το τι πρέπει να κάνει. Ο σχεδιασμός του CALDERA δίνει έμφαση στο πρώτο, δηλαδή το CALDERA αποφασίζει από μόνο του το τι πρέπει να κάνει. Το CALDERA παίρνει τις διάφορες αποφάσεις με βάση μια εσωτερική τιμή που του επιτρέπει πιθανές δράσεις. Το CALDERA μπορεί να προσαρμοστεί, προσαρμόζοντας αυτή την εσωτερική τιμή. Προς το παρόν, αυτό μπορεί να γίνει μόνο με την επεξεργασία του πηγαίου κώδικα. Ο σχεδιασμός του CALDERA είναι απλός, κάθε βήμα έχει μια αριθμητική τιμή που ονομάζεται value. Οι υψηλότερες τιμές υποδεικνύουν ένα υψηλότερο βήμα προτεραιότητας. Τα βήματα με υψηλότερη τιμή στο value έχουν προτεραιότητα σε σχέση με βήματα με χαμηλότερη. Οι ενσωματωμένες τιμές των βημάτων του CALDERA μπορούν να τροποποιηθούν με επεξεργασία του κώδικα του αρχείου που βρίσκεται στο : */caldera/caldera/app/operation/ operation_steps.py*.
Στο CALDERA η μικρότερη εκτελέσιμη δράση ενός αντιπάλου ονομάζεται βήμα (step). Το CALDERA χρησιμοποιεί μεμονωμένα βήματα μαζί για να σχηματίσει μια ακολουθία δραστηριότητας που αντιπροσωπεύει έναν αντίπαλο. Οι νέες τεχνικές μπορούν να προστεθούν στο CALDERA με την προσθήκη ενός νέου βήματος στο αρχείο *operation_steps.py*.

Κεφάλαιο 5 Red Team Automation (RTA)

5.1 Εισαγωγή

Οι οργανισμοί και οι αμυνόμενοι συχνά χρησιμοποιούν πρακτικούς τρόπους για την αξιολόγηση της αποτελεσματικότητας των προϊόντων πρόληψης και εντοπισμού. Ο πίνακας του μοντέλου ATT&CK του MITRE εντοπίζει περίπου 200 διαφορετικά είδη συμπεριφοράς των αντιπάλων. Καθώς οι αμυνόμενοι αναγνωρίζουν την ανάγκη να προχωρήσουν πέρα από τις δοκιμές εναντίον κακόβουλου λογισμικού, το μοντέλο ATT&CK, γίνεται όλο και περισσότερο το πρότυπο το οποίο χρησιμοποιείται για την αξιολόγηση της συμπεριφοράς των αντιπάλων. Ωστόσο, είναι σημαντικό οι οργανισμοί να συνειδητοποιήσουν ότι η κάλυψή τους εναντίον των τεχνικών από το μοντέλο ATT&CK είναι μια διαδικασία η οποία πρέπει να επαναλαμβάνεται, δεδομένου ότι προστίθενται συχνά νέες τακτικές.
Οι οργανισμοί και οι αμυνόμενοι πρέπει ακόμα να δοκιμάσουν τις άμυνές τους εναντίον κάθε μιας από τις συμπεριφορές οι οποίες περιγράφονται λεπτομερώς στο μοντέλο ATT&CK. Αυτό το μοντέλο μπορεί να είναι αποτελεσματικό λόγω της ευρείας γκάμας τεχνικών τις οποίες περιγράφει καθώς επίσης αναλύει με ποιους τρόπους ο αντίπαλος μπορεί να εφαρμόσει τις τεχνικές αυτές.
Η Red Team Automation (RTA) της Endgame ενώνει ένα μικρό αριθμό από παρόμοια χρήσιμα εργαλεία προσομοίωσης αντιπάλων, όπως το Atomic Red του Red Canary, το πρότζεκτ Metta της Uber καθώς και το Caldera του MITRE. Η ερευνητική ομάδα της Endgame δημιούργησε το πλαίσιο RTA για εσωτερικούς πειραματισμούς και αυτοματοποιημένους ελέγχους ανίχνευσης συμπεριφοράς αντιπάλων, το οποίο το μοιράστηκε δημοσίως για να βοηθήσει τους οργανισμούς να εντοπίσουν τα κενά ασφαλείας που ενδεχομένως να έχουν.

5.2 Περιγραφή του RTA

Το RTA αποτελείται από ένα σετ 42 σεναρίων και υποστηρίζει εκτελέσιμα αρχεία που δημιουργούν αξιόπιστα αντικείμενα τα οποία στην συνέχεια αντιστοιχούν σε τεχνικές στο μοντέλο του ATT&CK. Αρχικά, το μοντέλο RTA παρέχει κάλυψη 49 τεχνικών του πίνακα ATT&CK το οποίο όμως θα επεκταθεί με την πάροδο του χρόνου. Το RTA έχει δομηθεί με τέτοιο τρόπο ώστε να βοηθάει τις αμυντικές δυνατότητες να χρησιμοποιούνται αποτελεσματικά καθώς και να υποστηρίζει την ευρύτερη κοινότητα ανοιχτού κώδικα. Για το σκοπό αυτό, ο καθένας μπορεί να συνεισφέρει προσθέτοντας νέες τεχνικές στο RTA μέσω του αποθετηρίου GitHub
Το RTA διαφέρει από άλλα εργαλεία προσομοίωσης των αντιπάλων και αυτό γιατί όταν σχεδιάστηκε κανένα από τα άλλα πλαίσια δεν υπήρχε δημοσίως. Συνεχίστηκε να αναπτύσσεται αντί να υιοθετηθεί ένα άλλο πλαίσιο επειδή το RTA της Endgame έχει χαμηλό κόστος, είναι πολύ απλό στη χρήση και μπορεί να επεκταθεί σχετικά εύκολα.
Για να αρχίσουμε να χρησιμοποιούμε το RTA, είναι σημαντικό να κατανοήσουμε μερικά από τα βασικά χαρακτηριστικά του. Ορισμένα σενάρια λειτουργούν με ένα εκτελέσιμο αρχείο, το "myapp.exe", το οποίο είναι ικανό να δημιουργήσει έναν τοπικό web server για τη φιλοξενία κακόβουλων αρχείων καθώς και για την παραποίηση χρονοσημάνσεων σε ένα αρχείο. Επίσης περιλαμβάνει δεκάδες σενάρια που βασίζονται σε γλώσσα προγραμματισμού Python με τις εξής δυνατότητες:

- Μπορούν να κάνουν χρήση εργαλείων για τη λήψη και την εκτέλεση απομακρυσμένων αρχείων.

- Μπορούν να εκτελέσουν ενέργειες για την κάλυψη των ιχνών τους (anti-forensics operations).

- Μπορούν να εκτελέσουν πλευρική μετακίνηση (lateral movement) σε ένα σύστημα στόχο και να εκτελέσουν διάφορες ενέργειες σε αυτό.

- Μπορούν να εκτελέσουν μία από τις πολλές τεχνικές παράκαμψης του User Account Control (UAC).

Το αποθετήριο RTA της Endgame έχει μέχρι σήμερα 42 σενάρια ενεργειών εκτός από το εκτελέσιμο αρχείο "myapp.exe". Μελλοντικά η εταιρεία έχει ως σκοπό να προσθέσει επιπλέον σενάρια ώστε να μπορέσει να καλύψει ακόμη μεγαλύτερο μέρος του πίνακα του προτύπου ATT&CK. Στην εικόνα 25 φαίνεται η κάλυψη του μοντέλου RTA.

Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Execution	Command and Control
Accessibility Features	Accessibility Features	Bypass user Account Control	Credentials in Files	Account Discovery	Remote Services	Execution through Module Load	Commonly Used Port
AppInit DLLs	AppInit DLLs	Code Signing		Query Registry		InstallUtil	Remote File Copy
Component Object Model Hijacking	Bypass User Account Control	Component Object Model Hijacking		System Time Discovery		PowerShell	Web Service
File System Permissions Weaknesses	File System Permissions Weakness	Deobfuscate/ Decode Files or Information				Regsvcs/Regasm	
Modify Existing Service	New Service	Disabling Security Tools				Rundll32	
New Service	Scheduled Task	File Deletion				Scheduled Task	
Registry Run Keys/Start Folder		Hidden Files and Directories				Scripting	
Scheduled Task		Install Root Certificate				Service Execution	
Create Account		InstallUtil				Trusted Developer Utilities	
		Masquerading				Windows Management Instrumentation	
		Modify Registry					
		Obfuscated Files or Information					
		Regsvcs/Regasm					
		Regsver32					
		Rundll32					
		Scripting					
		Timestamp					
		Trusted Developer Utilities					

Εικόνα 25 : Τρέχουσα κάλυψη του πίνακα ATT&CK χρησιμοποιώντας το μοντέλο RTA της Endgame

Το RTA repo περιλαμβάνει επίσης ένα αρχείο που περιέχει τις συνολικές ρυθμίσεις διαμόρφωσης και λειτουργίες χρησιμότητας, το οποίο ονομάζεται "common.py". Αυτό μπορεί να εισαχθεί σε ένα νέο σενάριο και να επωφεληθεί από τις διάφορες μεταβλητές ή λειτουργίες, καθώς και να τροποποιηθεί για να δημιουργήσει νέες μεταβλητές ή δυνατότητες. Με την ενημέρωση της μεταβλητής LOCAL_IP, η οποία έχει οριστεί από προεπιλογή στο localhost (127.0.0.1), τα σενάρια του RTA μπορούν να εκτελούνται από απομακρυσμένο σύστημα. Αυτό το αρχείο Python περιέχει επίσης λειτουργίες που αναγνωρίζονται σε παγκόσμιο επίπεδο, όπως η καταγραφή μηνυμάτων κατά την εκτέλεση των διαφόρων δοκιμών που μπορούν να εμφανίζονται και στο χρήστη, αξιολογώντας εάν ένα σύστημα είναι 32 ή 64 bit. ή την αναγνώριση εγγράψιμων καταλόγων. Αυτή τη στιγμή, το RTA έχει πολύ λίγες απαιτήσεις για να εκτελεστεί με την μόνη προϋπόθεση ότι χρειάζεται να είναι εγκατεστημένη η έκδοση της Python 2.7. Επιπλέον για να γίνει αξιοποίηση στο

έπακρο του μοντέλου RTA, προτείνουμε στους χρήστες να κάνουν λήψη και εξαγωγή της σουίτα Sysinternals καθώς επίσης και το πρόγραμμα της Microsoft, "msxsl.exe".

5.3 Εγκατάσταση του Red Team Automation

Από την σελίδα https://github.com/endgameinc/RTA κατεβάζουμε το zip αρχείο στον υπολογιστή μας και το κάνουμε extract στο φάκελο c:\RTA.
Επιπλέον ορισμένα από τα σενάρια του RTA απαιτούν πρόσθετα εργαλεία τρίτων για να εκτελεστούν σωστά. Μπορούμε να εκτελέσουμε πολλά RTA χωρίς πρόσθετα εργαλεία, αλλά για να χρησιμοποιήσουμε την πλήρη σουίτα από την σελίδα https://docs.microsoft.com/en-us/sysinternals/downloads/sysinternals-suite κατεβάζουμε το Sysinternals Suite και το κάνουμε extract στον φάκελο C:\RTA\red_ttp\bin.
Από την σελίδα https://www.microsoft.com/en-us/download/details.aspx?id=21714 κατεβάζουμε και κάνουμε εγκατάσταση το πρόγραμμα Command Line Transformation Utility (msxsl.exe).

5.4 Εκτέλεση των σεναρίων

Για να εκτελέσουμε κάποιο σενάριο χρησιμοποιούμε την εντολή python μαζί με το όνομα του σεναρίου μέσα από τον φάκελο red_ttp. Για παράδειγμα αν θέλουμε να τρέξουμε το σενάριο με όνομα *enum_commands.py* θα χρησιμοποιήσουμε την εντολή ***python enum_commands.py*** όπως φαίνεται στην εικόνα 26.

```
C:\RTA\red_ttp>python enum_commands.py
[+] Running 25 out of 25 enumeration commands

[+] About to call ipconfig /all
dc > ipconfig /all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : dc
   Primary Dns Suffix  . . . . . . . : test.net
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No
   DNS Suffix Search List. . . . . . : test.net
                                       localdomain

Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . : localdomain

[+] About to call net localgroup administrators
dc > net localgroup administrators
Alias name     administrators
Comment        Administrators have complete and unrestricted access to the computer/domain

Members

-------------------------------------------------------------------------------
Administrator
Domain Admins
Domain Computers

[+] About to call net user
dc > net user

User accounts for \\DC

-------------------------------------------------------------------------------
Administrator            DefaultAccount           Guest
krbtgt                   victim1                  victim2
The command completed successfully.
```

Εικόνα 26 : Εκτέλεση σεναρίου RTA

Η εντολή αυτή θα εκτελέσει τις εντολές που φαίνονται στην εικόνα 27 και θα εμφανίζει τα αντίστοιχα αποτελέσματα

```
commands = [
    "ipconfig /all",
    "net localgroup administrators",
    "net user",
    "net user administrator",
    "net user /domain"
    "tasklist",
    "net view",
    "net view /domain",
    "net view \\\\%s" % common.LOCAL_IP,
    "netstat -nao",
    "whoami",
    "hostname",
    "net start",
    "tasklist /svc",
    "net time \\\\%s" % common.LOCAL_IP,
    "net use",
    "net view",
    "net start",
    "net accounts",
    "net localgroup",
    "net group",
    "net group \"Domain Admins\" /domain",
    "net share",
    "net config workstation",
```

Εικόνα 27 : Εντολές σεναρίου enum_commands.py

Στο μοντέλο RTA υπάρχει η δυνατότητα να εκτελέσουμε όλα τα σενάρια αυτόματα με την εντολή ***python run_all.py*** μέσα από το φάκελο C:\RTA λαμβάνοντας τα αντίστοιχα αποτελέσματα κάθε φορά.

Συμπεράσματα

Στην παρούσα εργασία συζητήθηκαν τα κίνητρα για τη δημιουργία του μοντέλου ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge), η φιλοσοφία σχεδιασμού του όσον αφορά τις τακτικές και τις τεχνικές, η πρόοδος του έχει κάνει το συγκεκριμένο μοντέλο καθώς και πώς μπορεί αυτό να χρησιμοποιηθεί από τις red teams. Επιπλέον έγινε περιγραφή του μοντέλου ATT&CK και αναλύθηκαν οι αρχές στις οποίες βασίζεται το μοντέλο κατά την προσέγγιση ασφαλείας για την εύρεση απειλών στο κυβερνοχώρο. Επίσης έγινε αναφορά και σύγκριση μεταξύ των τεχνικών red teaming kai penetration test, οι οποίες χρησιμοποιούνται για την αξιολόγηση ασφαλείας ενός συστήματος με σκοπό να βρεθούν οι ευπάθειές του, ώστε να γίνει η κατανόηση των διαφορών τους.
Στο πρακτικό μέρος της εργασίας δοκιμάστηκαν δύο εργαλεία που χρησιμοποιούνται για την τεχνική red teaming, το Caldera και το RTA (Red Team Automation). Από τα δύο αυτά εργαλεία το RTA είχε ελάχιστες απαιτήσεις όσον αφορούσε στην εγκατάστασή του, διότι αποτελείται μόνο από python scripts. Οι ελάχιστες απαιτήσεις ήταν ότι για την εκτέλεση των σεναρίων χρειάζεται να είναι εγκατεστημένη η Python 2.7 και όχι κάποια νεότερη έκδοση καθώς επίσης και η εγκατάσταση των Sysinternals Suite και του προγράμματος msxsl.exe.
Για την χρήση του εργαλείου Caldera χρειαζόταν να γίνει εγκατάσταση του server. Στην αρχή τον εγκατέστησα με vm με λειτουργικό Ubuntu 18.04, αλλά κατά την εκτέλεση των σεναρίων διαπίστωσα ότι εμφανίζει δυσλειτουργίες κατά την εκτέλεση κάποιον σεναρίων. Συγκεκριμένα κατά την εκτέλεση της τεχνικής για Credential Dumping με την χρήση του εργαλείου Mimikatz δεν εμφάνιζε τα αναμενόμενα αποτελέσματα και για τον λόγο αυτό δοκίμασα την εγκατάσταση του σε vm με λειτουργικό Windows 10, οπού λειτουργούσαν κανονικά όλα τα σενάρια χωρίς πρόβλημα.
Μελλοντικά θα μπορούσε να δοκιμαστεί το εργαλείο Caldera σε περιβάλλον με παραπάνω από 20 συστήματα, πράγμα που δεν ήταν δυνατόν να δοκιμαστεί στα πλαίσια της εργασίας αυτής λόγω περιορισμών σε hardware του υπολογιστή. Επιπλέον στο μέλλον θα μπορούσαν να προστεθούν και να δοκιμαστούν , στις ήδη υπάρχουσες, νέες τεχνικές, με την προσθήκη νέων βημάτων στο αρχείο **operation_steps.py**.

Βιβλιογραφία

- Dalziel, Henry-Next Generation Red Teaming-Elsevier_Syngress (2015)
- https://blog.nettitude.com/red-team-testing-10-reasons-why-you-should-be-doing-it
- https://en.wikipedia.org/wiki/Red_team
- https://www.redteamsecure.com/what-is-red-teaming-and-why-do-i-need-it-2
- https://pulsesecurity.co.nz/articles/pentest-vs-redteam
- https://blog.contentsecurity.com.au/red-teaming-vs-penetration-testing-whats-the-difference-0
- A Simple Handbook for Non-Traditional Red Teaming
- MITRE ATT&CK™ : Design and Philosophy
- Finding Cyber Threats with ATT&CK™-Based Analytics
- https://caldera.readthedocs.io/en/latest/philosophy.html
- https://github.com/mitre/caldera
- https://caldera.readthedocs.io/en/latest/installation.html
- https://caldera.readthedocs.io/en/latest/environment_setup.html
- https://caldera.readthedocs.io/en/latest/first_operation.html
- https://www.csoonline.com/article/3268545/data-breach/4-open-source-mitre-attandck-test-tools-compared.html?nsdr=true&cid=cso_nlt_cso_update_2018-04-12
- https://www.endgame.com/blog/technical-blog/introducing-endgame-red-team-automation
- https://github.com/endgameinc/RTA