Χρήση του εργαλείου Sysmon για τον εντοπισμό επιθέσεων εσωτερικής μετακίνησης ενός επιτιθέμενου

Πανεπιστήμιο Πειραιώς – Τμήμα Ψηφιακών Συστημάτων
Πρόγραμμα Μεταπτυχιακών Σπουδών
«Ασφάλεια Ψηφιακών Συστημάτων»

Στεφανία Κλώντζα

Επιβλέπων Καθηγητής Χρήστος Ξενάκης

Μάρτιος 2022

Περίληψη
Στην παρούσα διπλωματική εργασία παρουσιάζεται το εργαλείο Sysmon καθώς και ο τρόπος εγκατάστασης και παραμετροποίησης του ώστε να μπορεί να εντοπιστεί η εσωτερική μετακίνηση ενός επιτιθέμενου μέσα στο δίκτυο. Το Sysmon είναι ένα εργαλείο παρακολούθησης συστημάτων Windows το οποίο παρέχει λεπτομερείς πληροφορίες σχετικά με τις δημιουργίες διεργασιών, τις συνδέσεις δικτύου και τις αλλαγές στον χρόνο δημιουργίας αρχείων. Μέσα από την συλλογή των συμβάντων που δημιουργούνται από το Windows Event Collection agent, μπορεί να εντοπιστεί η κακόβουλη δραστηριότητα και να κατανοηθεί πως λειτουργούν οι επιτιθέμενοι μέσα στο δίκτυο. Αρχικά, αναλύεται η έννοια της εσωτερικής μετακίνησης, χρησιμοποιώντας τη στήλη Lateral Movement σύμφωνα με την κατηγοριοποίηση του MITRE ATT&CK και έπειτα με τη βοήθεια του Sysmon θα παρουσιαστούν τα καταγεγραμμένα συμβάντα που εντοπίστηκαν κατά τη διαδικασία της εσωτερικής μετακίνησης ανάμεσα σε δύο (2) Windows συστήματα. Τέλος, θα αναπτυχθούν οι τεχνικές παραμετροποίησης του εργαλείου για την σωστή καταγραφή αρχείων καθώς και τα διάφορα εργαλεία που θα χρησιμοποιηθούν κατά την διάρκεια αυτής της διαδικασίας. Ως τελικό αποτέλεσμα, θα υπάρχει ένας ταξινομημένος πίνακας με όλα τα ευρήματα από την συγκεκριμένη έρευνα.

Abstract
This thesis presents the Sysmon tool as well as how to install and configure it so that the lateral movement of an attacker within the network can be detected. Sysmon is a Windows system monitoring tool that provides detailed information about process creations, network connections, and changes in file generation time. Through the event collection displayed by the Windows Event Collection agent, malware activity can be detected and the attacker's activity within the network. First, the meaning of lateral movement is analyzed, using the Lateral Movement column according to the categorization of MITER ATT&CK and then with the help of Sysmon will be presented the recorded events identified during the process of lateral movement between two (2) Windows systems. Finally, the tool configuration techniques for the correct file logging will be developed as well as the various tools that will be used during this process. As a final result, there will be a sorted table with all the findings from this research.

ΠΕΡΙΕΧΟΜΕΝΑ

Περιεχόμενο Πινάκων

1 Εισαγωγή

1.1 Η διάσταση της ασφάλειας Πληροφοριακών Συστημάτων σήμερα

Η παρούσα διπλωματική αποτελεί μια έρευνα στον τομέα της ασφάλειας πληροφοριακών συστημάτων σε συνδυασμό με την ραγδαία αύξηση των προηγμένων απειλών. Το βασικό πρόβλημα είναι ότι λόγω της πληθώρας των Πληροφοριακών Συστημάτων δεν είναι πάντα εφικτή η έγκαιρη διάγνωση μίας επίθεσης. Για το λόγο αυτό, η ασφάλεια των Πληροφοριακών Συστημάτων έχει τώρα περισσότερο την ανάγκη να ανιχνεύει και να αντιδρά γρήγορα σε κάθε πιθανή επίθεση.
Σε μία επίθεση υπάρχει η αρχική φάση όπου ο επιτιθέμενος προσπαθεί να βρει τις κατάλληλες τεχνικές για να εισβάλει στο δίκτυο αλλά και η τελική φάση όπου έχει αποκτήσει πρόσβαση σε δεδομένα και σε συστήματα.
Η πιο κρίσιμη όμως φάση είναι η μεσαία όπου ο επιτιθέμενος κινείται σιωπηλά στα συστήματα και στα δίκτυα με τελικό σκοπό να αποκτήσει πρόσθετα προνόμια και να υποκλέψει τα δεδομένα. Η φάση αυτή ονομάζεται εσωτερική μετακίνηση και είναι το πιο σημαντικό κομμάτι της επίθεσης καθώς ο επιτιθέμενος ξοδεύει πολύ χρόνο στο στάδιο αυτό και ταυτόχρονα πρέπει να κινηθεί αργά και μυστικά ώστε να μην γίνει αντιληπτός.

1.2 Αντικείμενο διπλωματικής

Σκοπός της παρούσας διπλωματικής είναι η ανίχνευση της εσωτερικής μετακίνησης ενός επιτιθέμενου στο δίκτυο μέσω του εργαλείου Sysmon καθώς και η κατάλληλη παραμετροποίηση τόσο του Sysmon όσο και των event logs που παράγει ένα σύστημα Windows.
Η διπλωματική εστιάζει στις τεχνικές και στα εργαλεία εσωτερικής μετακίνησης από τη στήλη Lateral Movement του πίνακα MITRE ATT&CK, που σχετίζονται με επιθέσεις σε συστήματα με λειτουργικό σύστημα Windows.

1.3 Δομή διπλωματικής

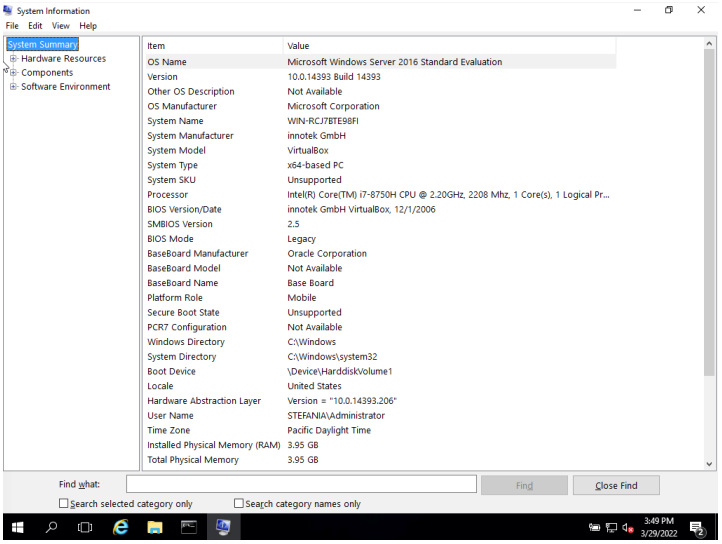
Το Κεφάλαιο 2 περιγράφει την αρχιτεκτονική που δημιουργήθηκε για την υλοποίηση της διπλωματικής. Στο Κεφάλαιο 3 αναλύεται η έννοια της εσωτερικής μετακίνησης και οι τεχνικές και τα εργαλεία που υπάρχουν σύμφωνα με το MITRE ATT&CK Framework. Στο Κεφάλαιο 4 παρουσιάζεται το εργαλείο Sysmon και στο Κεφάλαιο 5 τα αρχεία καταγραφής των Windows. Το Κεφάλαιο 6 περιλαμβάνει τα αποτελέσματα της έρευνας και το Κεφάλαιο 7 τα συμπεράσματα.

2 Περιβάλλον Έρευνας

Για την υλοποίηση της διπλωματικής δημιουργήθηκε ένα εικονικό περιβάλλον με ένα ζεύγος πελάτη και διακομιστή με τα παρακάτω συστήματα:

Πελάτης
- Windows 10

Διακομιστής
- Windows Server 2016



ΕΙΚΟΝΑ 1: WINDOWS SERVER 2016

3 Εσωτερική Μετακίνηση (Lateral Movement)

3.1 MITRE ATT&CK Framework

Το MITRE ATT&CK είναι μια παγκοσμίως βάση γνώσεων σχετικά με τις τακτικές και τις τεχνικές που χρησιμοποιούν οι επιτιθέμενοι βασισμένες σε παρατηρήσεις που πηγάζουν από τον πραγματικό κόσμο.

Το ATT&CK, το οποίο σημαίνει Adversarial Tactics, Techniques και Common Knowledge, είναι στην ουσία ένας δομημένος κατάλογος γνωστών συμπεριφορών κακόβουλων χρηστών όπου κατηγοριοποιεί και περιγράφει τις κακόβουλες συμπεριφορές για την ανάπτυξη συγκεκριμένων μοντέλων και μεθοδολογιών απειλών εναντίον εταιρικών συστημάτων, εφαρμογών cloud, φορητών συσκευών και συστημάτων βιομηχανικού ελέγχου.

Με αυτόν τον τρόπο, το ATT&CK επιλύει προβλήματα για μια πιο αποτελεσματική ασφάλεια στον κυβερνοχώρο βοηθώντας στην κατανόηση για το πώς σκέφτονται και λειτουργούν οι επιτιθέμενοι. Το ATT&CK είναι ανοιχτό και διαθέσιμο σε οποιοδήποτε άτομο ή οργανισμό για χρήση χωρίς χρέωση.

3.2 Ανάλυση εσωτερικής μετακίνησης

Οι επιθέσεις που θα χρησιμοποιηθούν εστιάζουν στην στήλη Lateral Movement του MITRE ATT&CK Framework, όπου σύμφωνα με την κατηγοριοποίηση του MITRE ο επιτιθέμενος προσπαθεί να αποκτήσει πρόσβαση και έλεγχο στα απομακρυσμένα συστήματα ενός δικτύου.

Πρωταρχικός στόχος του επιτιθέμενου είναι η εξερεύνηση του δικτύου για την εύρεση του στόχου του και στην συνέχεια η απόκτηση πρόσβασης σ' αυτόν. Η επίτευξη του στόχου τους συχνά περιλαμβάνει περιστροφή μέσω πολλαπλών συστημάτων και λογαριασμών καθώς οι επιτιθέμενοι ενδέχεται να εγκαταστήσουν τα δικά τους εργαλεία απομακρυσμένης πρόσβασης για να επιτύχουν την εσωτερική μετακίνηση ή να χρησιμοποιήσουν τα νόμιμα διαπιστευτήρια με εγγενή εργαλεία δικτύου και λειτουργικού συστήματος, τα οποία μπορεί να είναι πιο κρυφά.

Με πιο απλά λόγια, η εσωτερική μετακίνηση αποτελείται από τρείς (3) φάσεις:

- Αναγνώριση στόχου

Ο επιτιθέμενος παρατηρεί, εξερευνά και χαρτογραφεί το δίκτυο, τους χρήστες και τις συσκευές τους.

- Συλλογή διαπιστευτηρίων

Ο επιτιθέμενος χρησιμοποιεί τακτικές κοινωνικής μηχανικής όπως είναι η επίθεση ηλεκτρονικού «ψαρέματος» ώστε να εξαπατήσει τους χρήστες και να συλλέξει τα διαπιστευτήρια τους. Έτσι, μπορεί να χρησιμοποιήσει όσα διαπιστευτήρια μπόρεσε να αποκτήσει για να υποδυθεί το θύμα και να συνδεθεί σε άλλα μηχανήματα.

- Απόκτηση πρόσβασης

Μόλις ο επιτιθέμενος αποκτήσει πρόσβαση στον υπολογιστή, μπορεί να επαναλάβει την τακτική του αναζητώντας πρόσθετα στοιχεία, διαπιστευτήρια ή και προνόμια που μπορεί να εκμεταλλευτεί με τελικό στόχο την εγκατάσταση μιας απομακρυσμένης σύνδεσης.

Σε αυτό το σημείο αξίζει να αναφέρουμε ότι πολλές φορές μπορεί να είναι πολύ δύσκολο να εντοπιστεί η εσωτερική μετακίνηση ενός επιτιθέμενου στο δίκτυο καθώς μπορεί να φαίνεται ότι είναι «κανονική» κίνηση δικτύου. Για παράδειγμα, μπορεί τα τερματικά να πραγματοποιούν ασυνήθιστες διεργασίες χωρίς την άδεια του εκάστοτε διαχειριστή και να αλληλοεπιδρούν με τερματικά ή υπηρεσίες που συνήθως δεν αλληλοεπιδρούν.

3.3 Τεχνικές εσωτερικής μετακίνησης

Σύμφωνα με το Mitre Attack Framework, η στήλη Lateral Movement αποτελείται από τις παρακάτω βασικές τεχνικές:

- Αξιοποίηση Απομακρυσμένων Υπηρεσιών (Exploitation of Remote Services)

Οι επιτιθέμενοι ενδέχεται να εκμεταλλευτούν απομακρυσμένες υπηρεσίες για να αποκτήσουν μη εξουσιοδοτημένη πρόσβαση στα εσωτερικά συστήματα του δικτύου. Η αξιοποίηση ενός ευπαθούς λογισμικού συμβαίνει όταν ο επιτιθέμενος εκμεταλλεύεται ένα προγραμματιστικό λάθος του προγράμματος, της υπηρεσίας ή εντός του ίδιου του λογισμικού για να εκτελέσει κώδικα ελεγχόμενο από τον ίδιο. Μετά την πρώτη εκμετάλλευση, Ένας κοινός στόχος για την αξιοποίηση των απομακρυσμένων υπηρεσιών είναι η εσωτερική μετακίνηση για την πρόσβαση σε απομακρυσμένο σύστημα.
Ο επιτιθέμενος μπορεί να χρειαστεί να προσδιορίσει εάν το απομακρυσμένο σύστημα βρίσκεται σε ευάλωτη κατάσταση μέσω μιας υπηρεσίας σάρωσης δικτύου ή άλλων μεθόδων εξερεύνησης για ευάλωτο λογισμικό ή έλλειψη ορισμένων ενημερώσεων κώδικα με σκοπό τον εντοπισμό της απομακρυσμένης πρόσβασης.
Οι διακομιστές είναι στόχος υψηλής αξίας για την εκμετάλλευση της εσωτερικής μετακίνησης αλλά και τα συστήματα τελικού σημείου ενδέχεται επίσης να διατρέχουν κίνδυνο εάν παρέχουν πρόσβαση σε πρόσθετους πόρους.

- Internal Spearphishing

Οι επιτιθέμενοι ενδέχεται να χρησιμοποιήσουν την τεχνική «ψαρέματος» μέσα στον οργανισμό με σκοπό να αποκτήσουν επιπρόσθετες πληροφορίες για άλλους χρήστες ή συστήματα. Το εσωτερικό «ψάρεμα» είναι από τις πιο γνωστές επιθέσεις όπου ο επιτιθέμενος εγκαθιστά κακόβουλο λογισμικό ώστε να διακυβεύσει τα διαπιστευτήρια του λογαριασμού του χρήστη και να ελέγχει την συσκευή του. Με αυτόν τον τρόπο, οι επιτιθέμενοι προσπαθούν να συλλέξουν έναν αξιόλογο αριθμό εσωτερικών λογαριασμών ώστε να αυξήσουν τις πιθανότητες εξαπάτησης στην απόπειρα phishing.
Στην περίπτωση phishing, οι επιτιθέμενοι αποστέλλουν μέσω ηλεκτρονικού ταχυδρομείου ένα συνημμένο αρχείο ή έναν σύνδεσμο με κακόβουλο λογισμικό στους χρήστες με σκοπό να τους εξαπατήσουν και να συλλέξουν διαπιστευτήρια.

- Lateral Tool Transfer

Οι επιτιθέμενοι ενδέχεται να μεταφέρουν εργαλεία ή αρχεία μεταξύ των εσωτερικών συστημάτων που έχουν παραβιαστεί ώστε να υποστηρίξουν την εσωτερική μετακίνηση χρησιμοποιώντας πρωτόκολλα κοινής χρήσης αρχείων όπως το SMB που συνδέει κοινόχρηστα αρχεία μέσω δικτύου ή πρωτόκολλο απομακρυσμένης επιφάνειας εργασίας.

- Remote Service Session Hijacking

Οι επιτιθέμενοι μπορούν να πάρουν τον έλεγχο των συνεδριών που ήδη υπάρχουν με απομακρυσμένες υπηρεσίες για να μετακινηθούν εσωτερικά στο δίκτυο. Οι χρήστες μπορούν να χρησιμοποιήσουν έγκυρα διαπιστευτήρια για να συνδεθούν σε μια υπηρεσία ειδικά σχεδιασμένη για απομακρυσμένες συνδέσεις όπως το telnet, SSH (Secure Shell) και RDP (Remote Desktop Protocol). Όταν συνδεθεί ο χρήστης στην υπηρεσία, θα δημιουργηθεί μια περίοδος λειτουργίας που θα του επιτρέψει την συνεχή αλληλεπίδραση με αυτήν.
Η τεχνική αυτή συμπεριλαμβάνει δύο (2) υποκατηγορίες:

- SSH Hijacking
- RDP Hijacking

Σε κάθε κατηγορία ο επιτιθέμενος προσπαθεί να παραβιάσει τη συνεδρία SSH ή την περίοδο λειτουργίας απομακρυσμένης εργασίας ενός νόμιμου χρήστη.

- Απομακρυσμένες Υπηρεσίες (Remote Services)

Ο επιτιθέμενος μπορεί να χρησιμοποιήσει τους έγκυρους λογαριασμούς για να συνδεθεί σε μια υπηρεσία ειδικά σχεδιασμένη για να δέχεται απομακρυσμένες συνδέσεις όπως το telnet, SSH και VNC. Ο αντίπαλος μπορεί στην συνέχεια να εκτελέσει ενέργειες ως συνδεδεμένος χρήστης.
Η τεχνική αυτή συμπεριλαμβάνει έξι (6) υποκατηγορίες:

- Remote Desktop Protocol
- SMB/Windows Admin Shares
- Distributed Component Object Model
- SSH
- VNC
- Windows Remote Management

Σε κάθε κατηγορία ο επιτιθέμενος χρησιμοποιεί έγκυρους λογαριασμούς με τελικό σκοπό την εκτέλεση εντολών ως συνδεδεμένος χρήστης.

- Αντιγραφή μέσω αφαιρούμενων μέσων (Replication Through Removable Media)

Οι επιτιθέμενοι μπορούν να μετακινηθούν σε συστήματα ή και σε αποσυνδεδεμένα δίκτυα, αντιγράφοντας κακόβουλο λογισμικό σε αφαιρούμενα μέσα. Στην περίπτωση της εσωτερικής μετακίνησης, αυτό μπορεί να πραγματοποιηθεί μέσω τροποποίησης εκτελέσιμων αρχείων που είναι αποθηκευμένα σε αφαιρούμενα μέσα ή αντιγραφής του κακόβουλου λογισμικού και μετονομασίας του για να μοιάζει με ένα νόμιμο αρχείο και να εξαπατήσει τους χρήστες να το εκτελέσουν.

- Εργαλεία Ανάπτυξης Λογισμικού (Software Deployment Tools)

Οι επιτιθέμενοι μπορούν να αποκτήσουν πρόσβαση και να χρησιμοποιήσουν συστήματα ανάπτυξης εφαρμογών τρίτων κατασκευαστών εγκατεστημένα σε ένα δίκτυο. Οι εφαρμογές τρίτων και τα συστήματα ανάπτυξης λογισμικού ενδέχεται να χρησιμοποιούνται στο περιβάλλον δικτύου για σκοπούς διαχείρισης (π.χ. SSCM, HBSS, Altiris, κ.λπ.). Η πρόσβαση σε αυτά τα συστήματα, δίνει στον επιτιθέμενο τη δυνατότητα να έχει απομακρυσμένο έλεγχο για την εκτέλεση κώδικα σε όλα τα συστήματα που είναι συνδεδεμένα σε ένα τέτοιο σύστημα ώστε να χρησιμοποιηθεί για την εσωτερική μετακίνηση.

- Κοινόχρηστο Περιεχόμενο (Taint Shared Content)

Το περιεχόμενο που είναι αποθηκευμένο σε μονάδες δικτύου ή σε άλλες κοινόχρηστες τοποθεσίες ενδέχεται να παραβιαστεί τοποθετώντας κακόβουλα προγράμματα σε έγκυρα αρχεία. Μόλις ένας χρήστης ανοίξει το κοινόχρηστο μολυσμένο αρχείο, το κακόβουλο τμήμα θα εκτελέσει τον κώδικα του επιτιθέμενου σε ένα απομακρυσμένο σύστημα. Ο

επιτιθέμενος μπορεί να χρησιμοποιήσει το πλαστό κοινόχρηστο περιεχόμενο για να μετακινηθεί εσωτερικά.

- Μέθοδος Ελέγχου Ταυτότητας (Use Alternate Authentication Material)

Οι επιτιθέμενοι μπορούν να χρησιμοποιήσουν εναλλακτική μέθοδο ελέγχου ταυτότητας όπως ο κατακερματισμός κωδικών πρόσβασης, τα εισιτήρια Kerberos και τα access tokens προκειμένου να μετακινηθούν εσωτερικά και να παρακάμψουν τον έλεγχο πρόσβασης του συστήματος.
Η τεχνική αυτή συμπεριλαμβάνει τέσσερις (4) υποκατηγορίες:

- Application Access Token
- Pass the Hash
- Pass the Ticket
- Web Session Cookie

Κάθε κατηγορία είναι μια μέθοδος παράκαμψης αυθεντικοποίησης και ο επιτιθέμενος τις χρησιμοποιεί ανάλογα με τις ανάγκες για εσωτερική μετακίνηση στο δίκτυο.

3.4 Ανίχνευση Εσωτερικής Μετακίνησης

Στην ενότητα **3.2** αναφέραμε πως η ανίχνευση της εσωτερικής μετακίνησης είναι πολλές φορές δύσκολη. Παρόλα αυτά, υπάρχουν κάποιες μέθοδοι παρακολούθησης για το πως μπορεί κάποιος να ανιχνεύσει τεχνικές εσωτερικής μετακίνησης στο δίκτυο του και αυτές θα περιγράψουμε παρακάτω:

- Παρακολούθηση απομακρυσμένων υπηρεσιών

Η αναζήτηση εκμετάλλευσης απομακρυσμένων υπηρεσιών όπως είναι το λογισμικό είναι αρκετά δύσκολη. Η αναγνώριση της μη φυσιολογικής συμπεριφοράς των διεργασιών είναι το πιο σημαντικό. Αυτό μπορεί να περιλαμβάνει ύποπτα αρχεία που έχουν εγγραφεί στο δίσκο, αποδεικτικά στοιχεία διεργασίας για προσπάθειες απόκρυψης εκτέλεσης ή ακόμη και ασυνήθιστη κίνηση δικτύου που μπορεί να υποδεικνύει πρόσθετα εργαλεία που έχουν μεταφερθεί στο σύστημα.

- Παρακολούθηση για μεταφορά αρχείων

Η παρακολούθηση για τη δημιουργία αρχείων που μεταφέρονται στο δίκτυο χρησιμοποιώντας πρωτόκολλα όπως το SMB μπορεί να επιφέρει ασυνήθιστες διαδικασίες με εσωτερικές συνδέσεις που δημιουργούν αρχεία στο σύστημα. Σε αυτή την περίπτωση, ενδείκνυται η εξέταση παρακολούθησης για μη φυσιολογική χρήση βοηθητικών προγραμμάτων και γραμμών εντολών που μπορούν να χρησιμοποιηθούν για την υποστήριξη της απομακρυσμένης μεταφοράς αρχείων.

- Παρακολούθηση εσωτερικής επίθεσης ηλεκτρονικού ταχυδρομείου

Τα συστήματα ανίχνευσης εισβολής δικτύου καθώς και οι πύλες ηλεκτρονικού ταχυδρομείου συχνά δεν σαρώνουν τα εσωτερικά μηνύματα ηλεκτρονικού ταχυδρομείου. Για αυτό το λόγο, οι ενσωματωμένες λύσεις σε on-premise υπηρεσίες ή η αποστολή αντίγραφου των μηνυμάτων σε υπηρεσίες ασφάλειας για ανάλυση, βοηθούν στην ανίχνευση εσωτερικών επιθέσεων spearphishing.

- Παρακολούθηση της πρόσβασης αρχείων σε αφαιρούμενα μέσα

Ο εντοπισμός διεργασιών που εκτελούνται από τα αφαιρούμενα μέσα κατά την τοποθέτηση ή την εκκίνηση από τον χρήστη. Εάν ένα εργαλείο απομακρυσμένης πρόσβασης χρησιμοποιείται με αυτόν τον τρόπο για εσωτερική μετακίνηση, τότε είναι πιθανό να προκύψουν πρόσθετες ενέργειες μετά την εκτέλεση όπως το άνοιγμα συνδέσεων δικτύου για πληροφορίες συστήματος και δικτύου.

- Remote Service Session Hijacking

Η χρήση των SSH και RDP μπορεί να είναι νόμιμη ανάλογα με το περιβάλλον δικτύου και τον τρόπο χρήσης τους αλλά υπάρχουν παράγοντες που μπορεί να υποδηλώνουν την ύποπτη ή κακόβουλη συμπεριφορά τους. Η παρακολούθηση των λογαριασμών των χρηστών που είναι συνδεδεμένοι σε συστήματα στα οποία κανονικά δεν θα είχαν πρόσβαση καθώς και η παρακολούθηση για διεργασίες και γραμμές εντολών που σχετίζονται με υπηρεσίες hijacking, βοηθάει στην καλύτερη ανίχνευση της τεχνικής.

- Παρακολούθηση εργαλείων λογισμικού

Οι μέθοδοι ανίχνευσης διαφέρουν ανάλογα με τον τύπο λογισμικού των κατασκευαστών και τον τρόπο χρήσης τους.
Συχνά οι εφαρμογές τρίτων έχουν δικά τους αρχεία καταγραφής που μπορούν να συλλέξουν δεδομένα και να τα συσχετίσουν με άλλα δεδομένα στο δίκτυο. Για την διεκπεραίωση της παρακολούθησης, ενδείκνυται η ενσωμάτωση των αρχείων καταγραφής στο εταιρικό σύστημα καταγραφής ώστε να ελέγχονται τακτικά για μη εξουσιοδοτημένη δραστηριότητα όπως είναι οι συνδέσεις λογαριασμού στο σύστημα.

- Παρακολούθηση κοινόχρηστων φακέλων

Οι διεργασίες που εγγράφουν ή αντικαθιστούν πολλά αρχεία σε κοινόχρηστο κατάλογο δικτύου μπορεί να είναι ύποπτες. Σε αυτή την περίπτωση, ενδείκνυται η συχνή σάρωση των κοινόχρηστων καταλόγων για κακόβουλα αρχεία.

- Παρακολούθηση Ελέγχου Ταυτότητας

Διαμόρφωση ισχυρών πολιτικών ελέγχου δραστηριότητας λογαριασμού σε όλα τα εσωτερικά συστήματα.
Η αναζήτηση ύποπτης συμπεριφοράς σε υπηρεσίες ή λογαριασμούς όπως η σύνδεση λογαριασμών σε πολλά συστήματα ταυτόχρονα ή πολλαπλοί λογαριασμοί που έχουν συνδεθεί στο ίδιο μηχάνημα ταυτόχρονα.

3.5 Αντιμετώπιση των τεχνικών

Στη συνέχεια θα αναλύσουμε τις τεχνικές αντιμετώπισης των παραπάνω τεχνικών εσωτερικής μετακίνησης:

Τεχνική	Μετρίαση	Περιγραφή
Αξιοποίηση Απομακρυσμένων Υπηρεσιών (Exploitation of Remote Services)	Απομόνωση εφαρμογών και Sandboxing	Περιορίζουμε την εκτέλεση κώδικα σε ένα εικονικό περιβάλλον στο τελικό τερματικό. Καταστούμε δύσκολο για τον επιτιθέμενο να προωθήσει τη λειτουργία του μέσω της εκμετάλλευσης ανεξερεύνητων ή μη ενημερωμένων τρωτών σημείων χρησιμοποιώντας sandboxing.
	Απενεργοποίηση ή κατάργηση των δυνατοτήτων ή του προγράμματος	Καταργούμε ή αποκλείουμε την πρόσβαση σε ευάλωτα λογισμικά για να αποτρέψουμε την κατάχρηση τους από τον

Τεχνική	Μετρίαση	Περιγραφή
		επιτιθέμενο. Ελαχιστοποιούμε τις διαθέσιμες υπηρεσίες μόνο σε εκείνες που είναι απαραίτητες.
	Απόκτηση προστασίας	Χρησιμοποιούμε τις δυνατότητες για την ανίχνευση και την παρεμπόδιση των συνθηκών που μπορεί να οδηγήσουν στην εκμετάλλευση δυναμικού. Οι εφαρμογές ασφάλειας που αναζητούν συμπεριφορά που χρησιμοποιείτε κατά την εκμετάλλευση όπως το Windows Defender Exploit Guard (WDEG) και το Enhanced Mitigation Experience Toolkit (EMET) μπορούν να χρησιμοποιηθούν για να μετριάσουν κάποια συμπεριφορά εκμετάλλευσης.
	Τμηματοποίηση δικτύου	Τμηματοποιούμε τα δίκτυα και τα συστήματα κατάλληλα ώστε να μειώσουμε την πρόσβαση σε κρίσιμα συστήματα και υπηρεσίες ώστε να έχουμε ελεγχόμενες μεθόδους.
	Διαχείριση προνομίων λογαριασμού	Ελαχιστοποιούμε τα δικαιώματα και την πρόσβαση σε λογαριασμούς υπηρεσίας για να περιορίσουμε τις επιπτώσεις της εκμετάλλευσης.
	Πρόγραμμα ακεραιότητας απειλών	Δημιουργούμε μια ισχυρή καταγραφή πληροφοριών σχετικά με τις απειλές στον κυβερνοχώρο για να καθορίσουμε ποιοι τύποι και ποια επίπεδα απειλής μπορούν να χρησιμοποιούν τα προγράμματα εκμετάλλευσης λογισμικού.
	Ενημέρωση λογισμικού	Ενημερώνουμε τακτικά το λογισμικό χρησιμοποιώντας τη διαχείριση των ενημερώσεων κώδικα για εσωτερικά τερματικά και τους διακομιστές.
	Σαρώσεις για ευπάθειες	Ελέγχουμε τακτικά το εσωτερικό δίκτυο για τον εντοπισμό νέων ενδεχομένως ευάλωτων υπηρεσιών.
Internal Spearphishing	Αυτός ο τύπος τεχνικής δεν μπορεί να μετριαστεί εύκολα με προληπτικά μέτρα καθώς βασίζεται στην κατάχρηση των χαρακτηριστικών του συστήματος	-
Lateral Tool Transfer	Φιλτράρισμα κίνησης δικτύου	Εξετάστε το ενδεχόμενο χρήσης τείχους προστασίας για να περιορίσετε τις επικοινωνίες για

Τεχνική	Μετρίαση	Περιγραφή
		κοινή χρήση αρχείων όπως το SMB.
	Πρόληψη εισβολής δικτύου	Τα συστήματα ανίχνευσης εισβολής δικτύου που χρησιμοποιούν υπογραφές δικτύου για την αναγνώριση κακόβουλου λογισμικού μέσω γνωστών εργαλείων και πρωτοκόλλων όπως το FTP, μπορούν να χρησιμοποιηθούν για τον μετριασμό της δραστηριότητας στο δίκτυο.
Remote Service Session Hijacking	Απενεργοποίηση ή κατάργηση προγραμμάτων	Απενεργοποίηση των απομακρυσμένων υπηρεσιών όπως το SSH και το RDP εάν δεν είναι απαραίτητη.
	Τμηματοποίηση δικτύου	Ενεργοποίηση των κανόνων για το τείχος προστασίας για τον αποκλεισμό της περιττής κίνησης μεταξύ των ζωνών ασφαλείας στο δίκτυο.
	Διαχείριση λογαριασμού	Μη επιτρεπτή πρόσβαση σε απομακρυσμένες υπηρεσίες ως λογαριασμός με δικαιώματα εκτός αν είναι απαραίτητο.
	Διαχείριση λογαριασμού χρήστη	Περιορισμός των δικαιωμάτων χρήστη εάν είναι απαραίτητη η απομακρυσμένη πρόσβαση.
Απομακρυσμένες Υπηρεσίες (Remote Services)	Έλεγχος ταυτοποίησης πολλαπλών παραγόντων	Χρήση ελέγχου ταυτότητας πολλαπλών παραγόντων σε συνδέσεις απομακρυσμένης υπηρεσίας όπου είναι δυνατόν.
	Διαχείριση λογαριασμού χρήστη	Περιορισμός των λογαριασμών χρηστών που ενδέχεται να χρησιμοποιούν απομακρυσμένες υπηρεσίες. Περιορισμός των δικαιωμάτων για λογαριασμούς ώστε οι χρήστες να μπορούν να εκτελούν μόνο συγκεκριμένα προγράμματα.
Αντιγραφή μέσω αφαιρούμενων μέσων (Replication Through Removable Media)	Απενεργοποίηση ή κατάργηση προγραμμάτων	Απενεργοποίηση του Autorun και αποκλεισμός ή περιορισμός των αφαιρούμενων μέσων εάν δεν απαιτούνται από τις διεργασίες.
	Περιορισμός της εγκατάστασης υλικού	Περιορισμός της χρήσης αφαιρούμενων μέσων εντός ενός δικτύου.
Εργαλεία Ανάπτυξης Λογισμικού (Software Deployment Tools)	Διαμόρφωση καταλόγου Active Directory	Ρύθμιση του καταλόγου Active Directory για την αποτροπή της χρήσης ορισμένων τεχνικών. Διασφάλιση της σωστής απομόνωσης των συστημάτων και της πρόσβασης για συστήματα δικτύου μέσω πολιτικών.

Τεχνική	Μετρίαση	Περιγραφή
	Έλεγχος ταυτοποίησης πολλαπλών παραγόντων	Διασφάλιση της σωστής απομόνωσης των συστημάτων και της πρόσβασης για συστήματα δικτύου μέσω της χρήσης ελέγχου ταυτότητας πολλαπλών παραγόντων.
	Τμηματοποίηση δικτύου	Διασφάλιση της σωστής απομόνωσης των συστημάτων και της πρόσβασης για συστήματα δικτύου μέσω της χρήσης τείχους προστασίας.
	Πολιτική κωδικών πρόσβασης	Διασφάλιση ότι τα διαπιστευτήρια λογαριασμού που μπορούν να χρησιμοποιηθούν για την πρόσβαση σε συστήματα είναι μοναδικά και δεν χρησιμοποιούνται σε όλο το δίκτυο.
	Διαχείριση εξουσιοδοτημένων λογαριασμών	Δικαίωμα πρόσβασης σε συστήματα ανάπτυξης εφαρμογών μόνο σε περιορισμένο αριθμό εξουσιοδοτημένων λογαριασμών.
	Απομακρυσμένη αποθήκευση δεδομένων	Χρήση του αρχείου απομακρυσμένης καταγραφής ενεργειών ασφάλειας και αποθήκευσης ευαίσθητων αρχείων, όπου η πρόσβαση μπορεί να ελεγχθεί καλύτερα ώστε να αποφευχθεί η έκθεση των δεδομένων καταγραφής ανίχνευσης εισβολής ή ευαίσθητων πληροφοριών.
	Ενημέρωση λογισμικού	Εγκατάσταση τακτικών ενημερώσεων εκδόσεων στα συστήματα για την αποτροπή πιθανών απομακρυσμένων προσβάσεων.
	Διαχείριση λογαριασμού χρήστη	Διαχείριση της δημιουργίας, της τροποποίησης, της χρήσης και των αδειών που σχετίζονται με τους λογαριασμούς χρηστών. Διασφάλιση ότι οι λογαριασμοί που χρησιμοποιούνται για την πρόσβαση σε συστήματα, δεν χρησιμοποιούνται σε όλο το δίκτυο.
	Εκπαίδευση χρηστών	Εκπαίδευση χρηστών ώστε να γνωρίζουν τις τεχνικές επίθεσης και χειραγώγησης από τον επιτιθέμενο ώστε να μειωθεί ο κίνδυνος πρόσβασης στα συστήματα.
Κοινόχρηστο Περιεχόμενο (Taint Shared Content)	Αποτροπή εκτελέσεων	Αποκλεισμός εκτέλεσης κώδικα σε ένα σύστημα μέσω της παραμετροποίησης της λίστας

Τεχνική	Μετρίαση	Περιγραφή
		προσβάσεων των εφαρμογών (white and black lists) και τον αποκλεισμό άγνωστων προγραμμάτων.
	Απόκτηση προστασίας	Χρήση βοηθητικών προγραμμάτων που ανιχνεύουν ή μετριάζουν τα χαρακτηριστικά που χρησιμοποιούνται στην εκμετάλλευση.
	Περιορισμός στα δικαιώματα αρχείων	Προστασία των κοινόχρηστων φακέλων ελαχιστοποιώντας τους χρήστες που έχουν πρόσβαση εγγραφής.
Μέθοδος Ελέγχου Ταυτότητας (Use Alternate Authentication Material)	Διαχείριση λογαριασμού	Περιορισμός των ίδιων διαπιστευτηρίων μεταξύ των συστημάτων για την αποτροπή συλλογής τους από τον επιτιθέμενο κατά την εσωτερική μετακίνηση.
	Διαχείριση λογαριασμού χρήστη	Διαχείριση της δημιουργίας, της τροποποίησης, της χρήσης και των αδειών που σχετίζονται με τους λογαριασμούς χρηστών. Αποτροπή του χρήστη από συστήματα με δικαιώματα διαχειριστή.

ΠΙΝΑΚΑΣ 1: ΑΝΤΙΜΕΤΩΠΙΣΗ ΤΩΝ ΤΕΧΝΙΚΩΝ ΕΣΩΤΕΡΙΚΗΣ ΜΕΤΑΚΙΝΗΣΗΣ

3.6 Εργαλεία εσωτερικής μετακίνησης

1. Psexec

Βοηθητικά προγράμματα όπως το Telnet και τα προγράμματα απομακρυσμένου ελέγχου, όπως το PC Anywhere της Symantec, επιτρέπουν να εκτελέσουμε προγράμματα σε απομακρυσμένα συστήματα. Παρόλα αυτά, η εγκατάσταση μπορεί να γίνει περίπλοκη και να απαιτηθεί η εγκατάσταση λογισμικού πελάτη στα απομακρυσμένα συστήματα στα οποία επιθυμεί κάποιος να έχει πρόσβαση. Το PsExec είναι μια αντικατάσταση του telnet που επιτρέπει την εκτέλεση διαδικασιών σε άλλα συστήματα, με πλήρη αλληλεπίδραση για εφαρμογές κονσόλας, χωρίς χρειάζεται η εγκατάσταση λογισμικού πελάτη. Οι πιο ισχυρές χρήσεις του PsExec περιλαμβάνουν την εκκίνηση διαδραστικών εντολών σε απομακρυσμένα συστήματα και την εκκίνηση εργαλείων απομακρυσμένης ενεργοποίησης όπως το IpConfig που διαφορετικά δεν θα είχαν τη δυνατότητα να εμφανίζουν πληροφορίες σχετικά με τα απομακρυσμένα συστήματα.
Ορισμένοι ανιχνευτές προστασίας από ιούς θα αναφέρουν ότι ένα ή περισσότερα από τα εργαλεία έχουν μολυνθεί από ιό απομακρυσμένης διαχείρισης. Κανένα όμως από τα PsTools δεν περιέχει ιούς, αλλά έχουν χρησιμοποιηθεί από ιούς, γι 'αυτό και προκαλούν ειδοποιήσεις για ιούς.
Όσον αφορά την εγκατάσταση, αντιγράφουμε το PsExec στην εκτελέσιμη διαδρομή πληκτρολογώντας "psexec".

Παραδείγματα:

- Η ακόλουθη εντολή εκκινεί μια διαδραστική εντολή για την εντολή \\ marklap:
    - psexec \\ marklap cmd

- Η εντολή αυτή εκτελεί το IpConfig στο απομακρυσμένο σύστημα με την επιλογή / all και εμφανίζει την έξοδο τοπικά: psexec \\ marklap ipconfig / all
- Αυτή η εντολή αντιγράφει το πρόγραμμα test.exe στο απομακρυσμένο σύστημα και το εκτελεί διαδραστικά: psexec \\ marklap -c test.exe
- Καθορίζει την πλήρη διαδρομή προς ένα πρόγραμμα που είναι ήδη εγκατεστημένο σε ένα απομακρυσμένο σύστημα αν δεν είναι στη διαδρομή του συστήματος:
    - psexec \\ marklap c: \ bin \ test.exe
- Εκτελεί το Regedit διαδραστικά στο λογαριασμό System για να γίνει προβολή των περιεχόμενων των κλειδιών SAM και SECURITY :: psexec -i -d -s c: \ windows \ regedit.exe
- Για να γίνει εκτέλεση του Internet Explorer όπως και για τα δικαιώματα περιορισμένων
    - χρηστών, γίνεται χρήση της παρακάτω εντολής:
    - psexec -l -d "c: \ αρχεία προγράμματος \ internet explorer \ iexplore.exe"

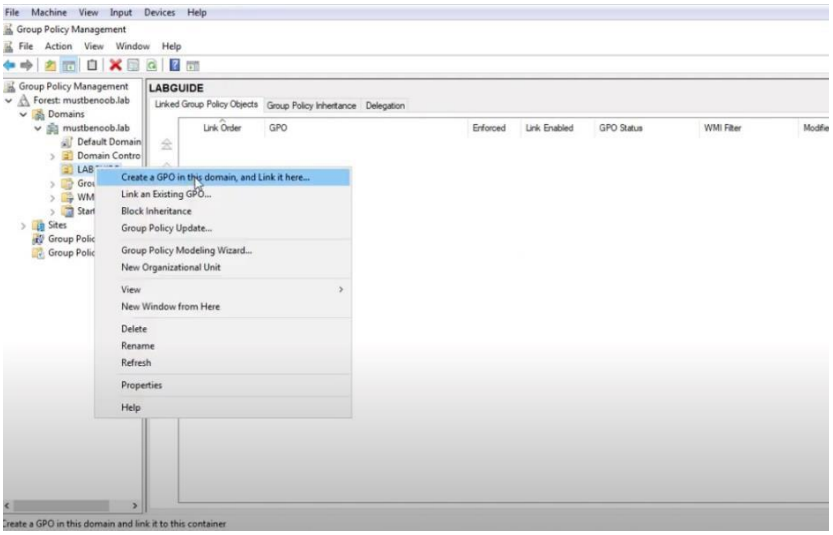
2. Wmiexec

Το Msiexec είναι το πρόγραμμα εγκατάστασης των Windows της Microsoft. Εμφανίζεται συχνά ως msiexec.exe στη Διαχείριση εργασιών των Windows. Χρησιμοποιείται για την εγκατάσταση, τη διατήρηση καθώς και την αφαίρεση προγραμμάτων που είναι ενσωματωμένα στη μορφή εγκατάστασης MSI. Αυτά τα αρχεία έχουν την επέκταση .MSI ή .msi στο τέλος του ονόματος αρχείου. Όταν ένα από αυτά τα αρχεία ανοίγεται, το msiexec φορτώνεται αυτόματα και ξεκινάει τη διαδικασία εγκατάστασης.

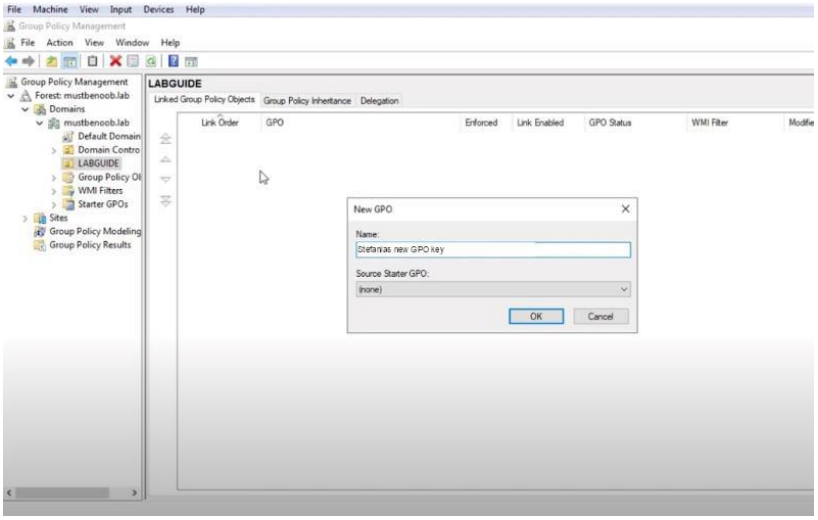
3. WinRM

Το Windows Remote Management (WinRm) είναι ένα πρωτόκολλο απομακρυσμένης διαχείρισης ενσωματωμένο στα Windows στην απλούστερη μορφή του που χρησιμοποιεί το πρωτόκολλο Simple Access Protocol για τη διασύνδεση με αποκαρυσμένους υπολογιστές και διακομιστές καθώς και σε λειτουργικά συστήματα και εφαρμογές.
Το WinRm είναι ένα εργαλείο γραμμής εντολών που χρησιμοποιείται για την απομακρυσμένη επικοινωνία με κεντρικούς υπολογιστές εντός του δικτύου και υποστηρίζει την εκτέλεση εντολών από απόσταση σε συστήματα που είναι απομακρυσμένα αλλά έχουν πρόσβαση στο δίκτυο.
Προκειμένου να λειτουργήσει το WinRm, πρέπει να ολοκληρωθούν τα παρακάτω βήματα:

- Δημιουργία GPO
- Διαμόρφωση του ακροατή WinRm
- Αυτόματη εκκίνηση της υπηρεσίας WinRm

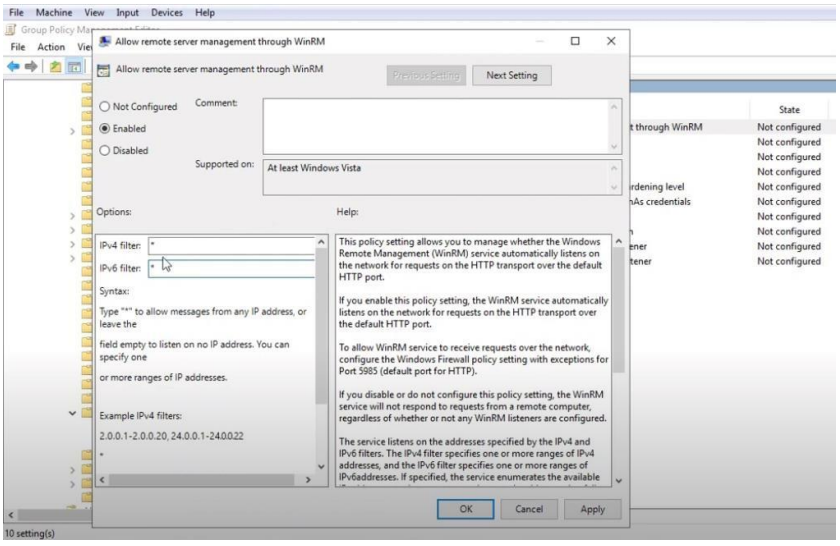


ΕΙΚΟΝΑ 2: ΔΗΜΙΟΥΡΓΙΑ GPO 1



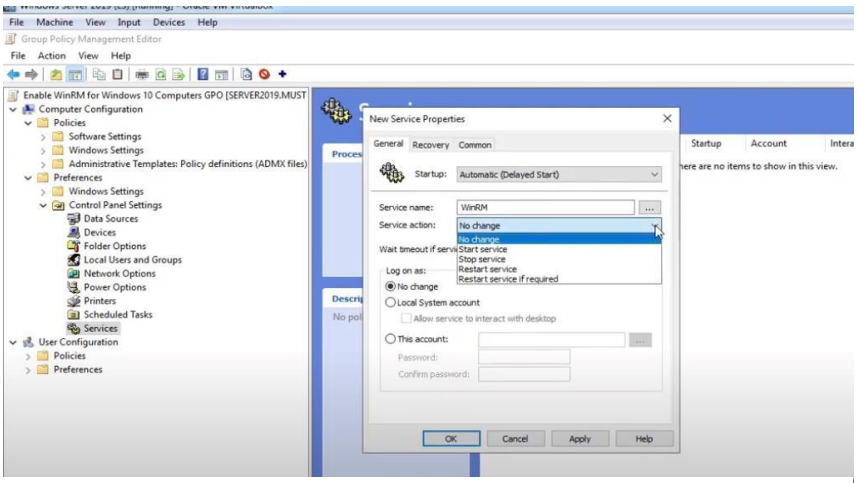
ΕΙΚΟΝΑ 3: ΔΗΜΙΟΥΡΓΙΑ GPO 2

Αφού έχουμε δημιουργήσουμε με επιτυχία το Group Policy Object, θα χρειαστεί να ενεργοποιήσουμε από τις ρυμίσεις πολιτικής την επιλογή «Να επιτρέπεται η αυτόματη ρύθμιση των ακροατών». Εδώ θα καθορίσουμε και τις IP διευθύνσεις που θα ακούσει η υπηρεσία WinRM.



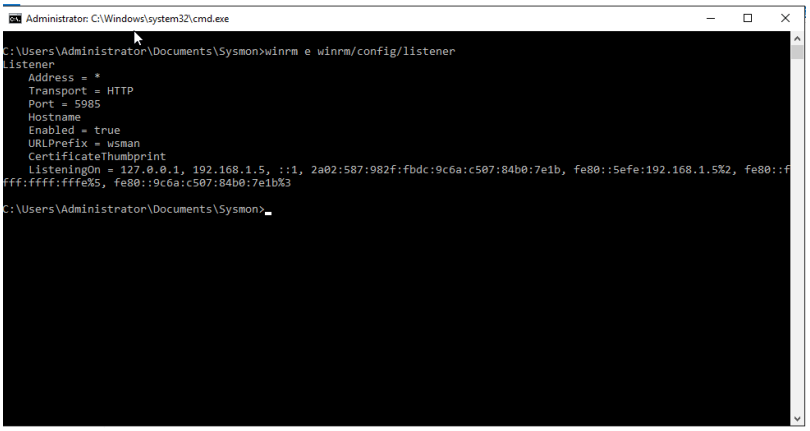
ΕΙΚΟΝΑ 4: ΔΙΑΜΟΡΦΩΣΗ ΤΟΥ ΑΚΡΟΑΤΗ WINRM

Στη συνέχεια θα χρειαστεί να βεβαιωθούμε ότι η υπηρεσία WinRM ξεκινά αυτόματα σε όλα τα μηχανήματα. Αυτό θα γίνει μέσα από τις ρυθμίσεις των παραμέτρων.



ΕΙΚΟΝΑ 5: ΑΥΤΟΜΑΤΗ ΕΚΚΙΝΗΣΗ ΤΟΥ WINRM

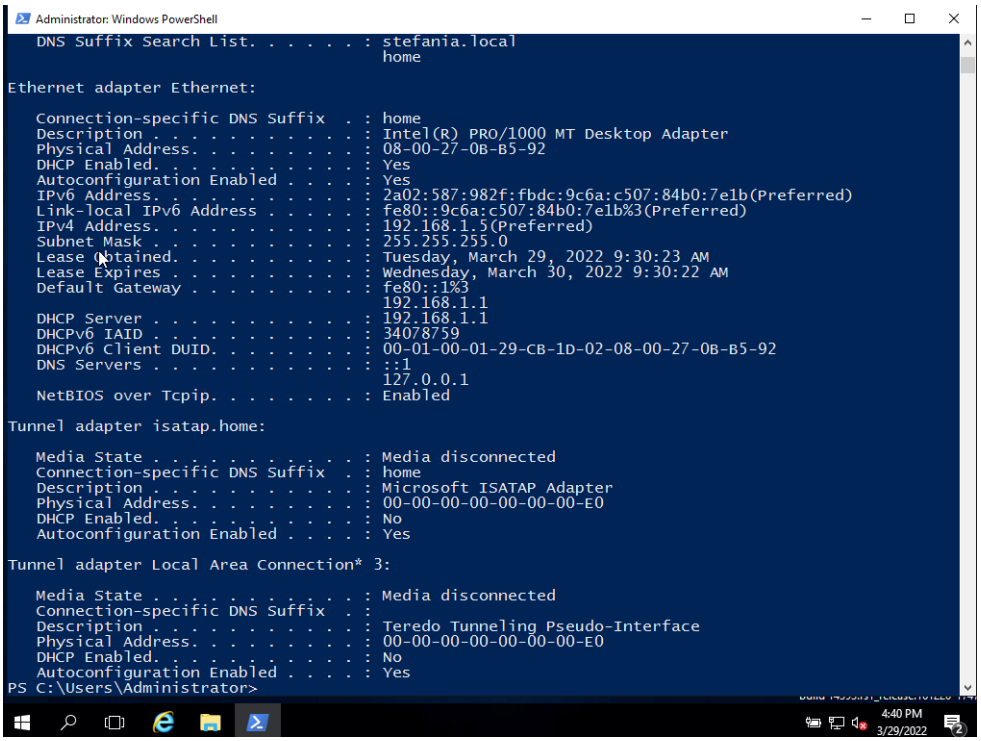
Αφού έχουμε διαμορφώσει με επιτυχία το Group Policy Object, θα πληκτρολογήσουμε την εντολή “winrm e winrm/config/listener” ώστε να δούμε τις ρυθμίσεις του ακροατή.



ΕΙΚΟΝΑ 6: ΠΡΟΒΟΛΗ ΡΥΘΜΙΣΕΩΝ ΑΚΡΟΑΤΗ

Προκειμένου να γίνει δοκιμή μιας σύνδεσης, ανοίγουμε ένα PowerShell για την δημιουργία διαπιστευτηρίων ώστε να συνδεθούμε στο απομακρυσμένο μηχάνημα. Χρησιμοποιούμε ένα λογαριασμό με επαρκή δικαιώματα:
PS> $cred = New-Object System.Management.Automation.PSCredential -ArgumentList @(‘USERNAME’,(ConvertTo-SecureString-String’PASSWORD’ -AsPlainText -Force))

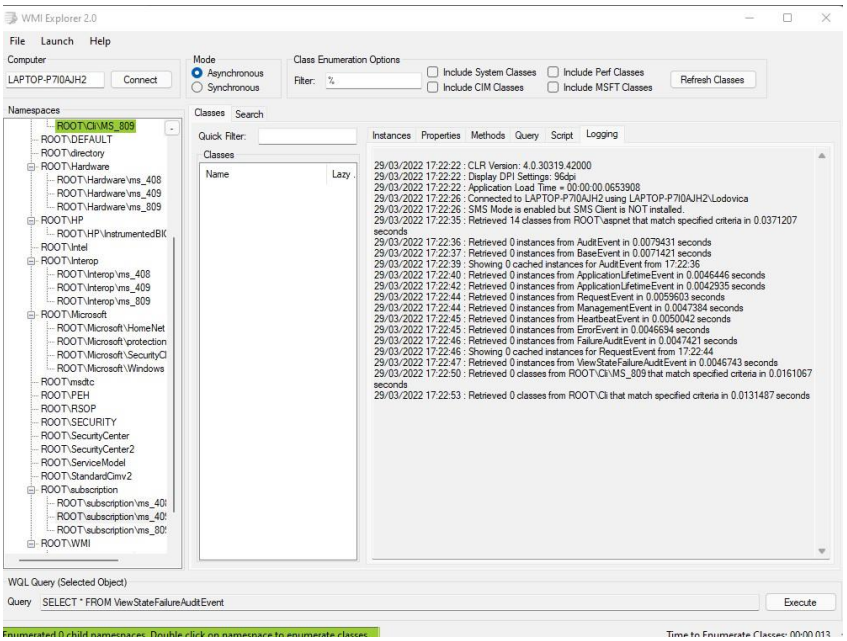
Αντικαθιστούμε το USERNAME και το PASSWORD με τα στοιχεία της σύδεσης μας και στη συνέχεια καλούμε μια απομακρυσμένη εντολή σε ένα απομακρυσμένο μηχάνημα. Στο δικό μας παράδειγμα, θα τρέξουμε το ‘ipconfig/all’ και θα πρέπει να επαληθεύσουμε οτι στην έξοδο είναι όλα καλά.



ΕΙΚΟΝΑ 7: ΔΟΚΙΜΗ ΣΥΝΔΕΣΗΣ ΤΟΥ WINRM

4. Wmic

Το WMIC είναι ένα πρόγραμμα λογισμικού που επιτρέπει στους χρήστες να εκτελούν λειτουργίες με τη γραμμή εντολών. Το WMI είναι η υλοποίηση της Microsoft για το Web Based Enterprise Management (WEBEM), το οποίο έχει βασιστεί στο Common Information Model (CIM), ένα πρότυπο βιομηχανίας υπολογιστών για τον καθορισμό των χαρακτηριστικών των συσκευών και των εφαρμογών, έτσι ώστε οι διαχειριστές συστήματος και τα προγράμματα διαχείρισης να μπορούν να ελέγχουν συσκευές και εφαρμογές από πολλές πολλές πηγές με τον ίδιο τρόπο.
Το WMIC παρέχει στους χρήστες πληροφορίες σχετικά με την κατάσταση των τοπικών ή απομακρυσμένων συστημάτων και υποστηρίζει ενέργειες όπως διαμόρφωση ρυθμίσεων ασφαλείας, ρύθμιση και αλλαγή των ιδιοτήτων του συστήματος και αλλαγή αδειών για εξουσιοδοτημένους χρήστες, δημιουργία αντιγράφων ασφαλείας και ενεργοποίηση ή απενεργοποίηση του error logging.
Το WMIC λειτουργεί με δύο τρόπους. Ο πρώτος είναι ο διαδραστικός που επιτρέπει την εισαγωγή εντολών σε μία γραμμή κάθε φορά και ο μη διαδραστικός που επιτρέπει τη δέσμευση εντολών για χρήση σε αρχεία.



ΕΙΚΟΝΑ 8: WMIC EXPLORER

4 Παρουσίαση του εργαλείου Sysmon

4.1 Εισαγωγή

Το Sysmon (System Monitor) είναι ένα εργαλείο παρακολούθησης συστημάτων Windows και αναπτύχθηκε από τους Mark Russinovich and Thomas Garnier. Το Sysmon είναι στην ουσία μια υπηρεσία συστήματος, η οποία αφού εγκατασταθεί σε ένα σύστημα, παραμένει ενεργό σε όλες τις επανεκκινήσεις του συστήματος για να παρακολουθεί και να καταγράφει τη δραστηριότητα του συστήματος στο αρχείο καταγραφής συμβάντων των Windows.
Παρέχει λεπτομερείς πληροφορίες σχετικά με την δημιουργία νέων διεργασιών, τις συνδέσεις δικτύου και τις αλλαγές στον χρόνο δημιουργίας των αρχείων. Μέσα από την συλλογή συμβάντων που παράγει το Sysmon, χρησιμοποιώντας το Windows Event Collector ή agent κάποιου SIEM, γίνεται η συγκεντρωτική συλλογή των events και στη συνέχεια αναλύοντας τα, είναι δυνατός ο εντοπισμός κακόβουλης δραστηριότητας και η κατανόηση του πως λειτουργούν οι επιτιθέμενοι ή κάποιο κακόβουλο λογισμικό στο σύστημα ή στο δίκτυο.

4.2 Βασικά Χαρακτηριστικά του Sysmon

Το Sysmon διαθέτει τα παρακάτω χαρακτηριστικά:

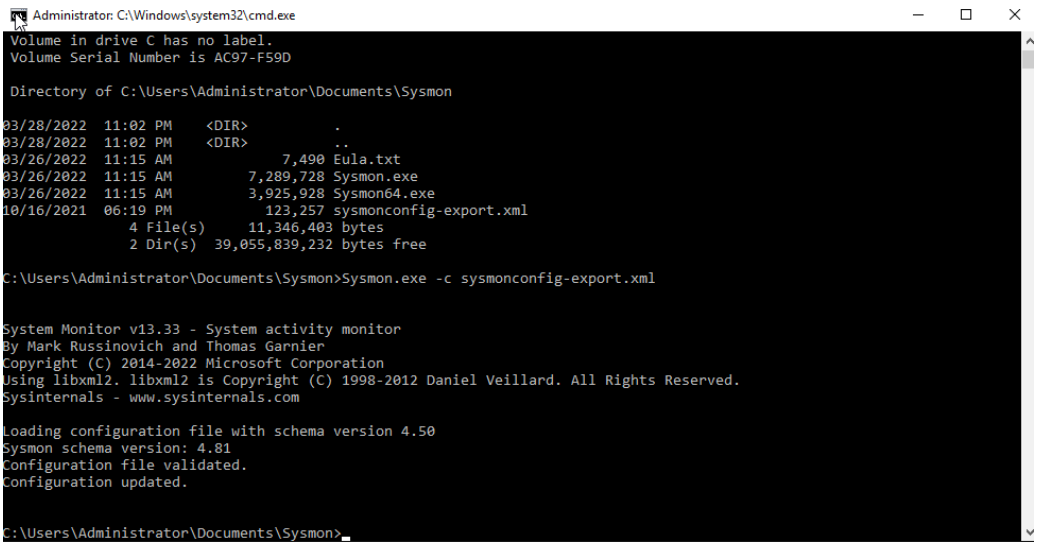
- Καταγράφει τη διαδικασία δημιουργίας διεργασιών από τη γραμμή εντολών είτε για PID είτε για PPID.
- Καταγράφει το hash μιας διεργασίας χρησιμοποιώντας SHA1(προεπιλογη), MD5, SHA256 ή IMPHASH.
- Μπορεί να χρησιμοποιήσει ταυτόχρονα πολλά hashes.
- Περιλαμβάνει ένα περιβάλλον GUID σε κάθε γεγονός και επιτρέπει τη συσχέτιση των συμβάντων στην ίδια σύνοδο.
- Καταγράφει την εκκίνηση προγραμμάτων οδήγησης ή των DLL με τις υπογραφές και τα hashes τους.
- Καταγράφει προσβάσεις σε δίσκους και μονάδες εγγραφής.
- Προαιρετικά καταγράφει συνδέσεις δικτύου συμπεριλαμβανόμενης της διεργασίας από την οποία προέρχεται κάθε σύνδεση, των διευθύνσεων IP, των αριθμών θυρών, των ονομάτων κεντρικών υπολογιστών και των ονομάτων των θυρών.

- Εντοπίζει αλλαγές στο χρόνο δημιουργίας αρχείων για να καταλάβει πότε δημιουργήθηκε ένα αρχείο. Η τροποποίηση του αρχείου δημιουργίας timestamps είναι μια τεχνική που συνήθως χρησιμοποιείται από κακόβουλο λογισμικό για να καλύψει τα ίχνη του.
- Επαναφορτώνει αυτόματα το αρχείο config ακόμα και αν αλλάξει η registry.
- Επιτρέπει τη δημιουργία κανόνων για να συμπεριληφθούν ή να αποκλειστούν δυναμικά ορισμένα συμβάντα.
- Δημιουργεί συμβάντα από την αρχή της διαδικασίας εκκίνησης για τη λήψη δραστηριότητας ακόμη και από ένα εξελιγμένο κακόβουλο λογισμικό πυρήνα.

Σημειώνεται ότι το Sysmon δεν παρέχει ανάλυση των συμβάντων που δημιουργεί το ίδιο, ούτε προσπαθεί να προστατευτεί ή να κρυφτεί από τους επιτιθέμενους.

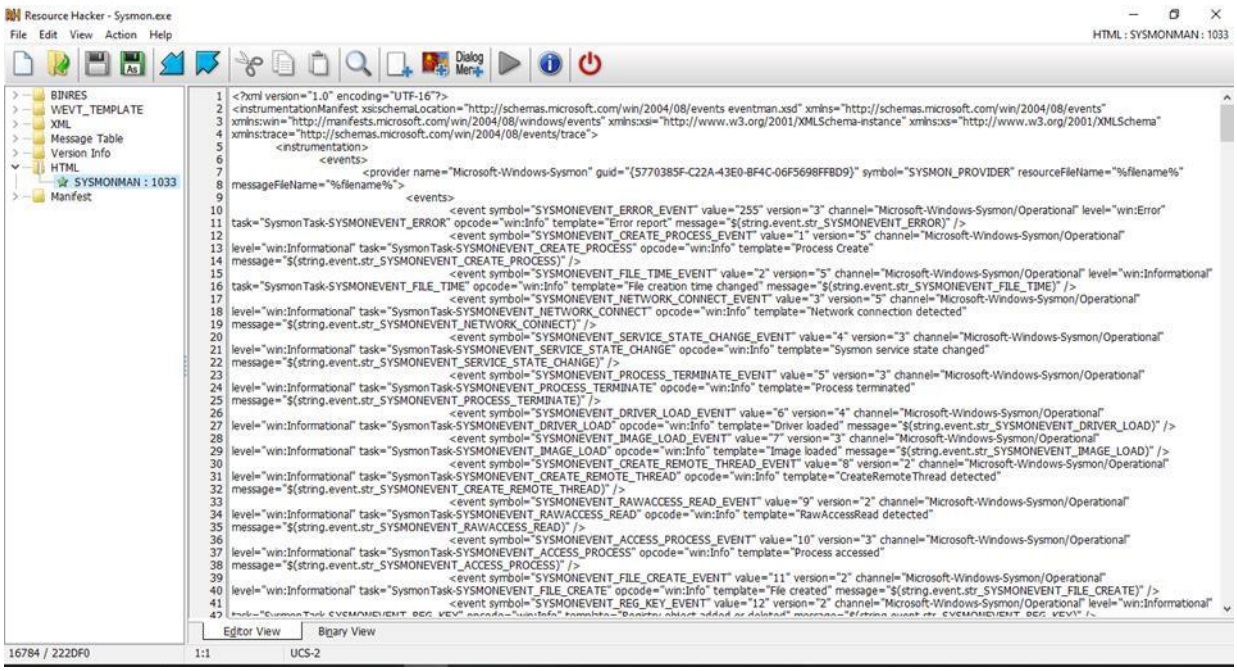
4.3 Ρυθμίσεις και Χρήση του εργαλείου Sysmon

Όπως φαίνεται στην Εικόνα 9, χρησιμοποιήθηκε το προ-ρυθμισμένο config file το οποίο θεωρείται ένα από τα πιο ολοκληρωμένα αρχεία ρύιμισης του Sysmon γιατί ακολουθεί την κατηγοριοποίηση του MITRE ATT&CK προκειμένου να αναγνωρίσει κακόβουλη συμπεριφορά.



ΕΙΚΟΝΑ 9: ΧΡΗΣΗ ΤΟΥ ΑΡΧΕΙΟΥ ΡΥΘΜΙΣΗΣ ΚΑΙ ΕΚΚΙΝΗΣΗ ΤΟΥ SYSMON

Για να μπορέσει κάποιος να αντιληφθεί πλήρως τον τρόπο με τον οποίο το Sysmon δουλεύει θα πρέπει να κατανοήσει πρώτα τον τρόπο με τον οποίο το Sysmon προσεγγίζει την κάθε καταγραφή την οποια επρόκειτω να προσθέσει. Για παράδειγμα στο παρακάτω Εικόνα, εμφανίζεται όλο το περιεχόμενο του Sysmon μαζί με τις υλοποιημένες ρουτίνες τις οποίες έχουμε προσθέσει μέσα από το configuration file.



ΕΙΚΟΝΑ 10: ΠΡΟΒΟΛΗ ΤΩΝ ΠΕΡΙΕΧΟΜΕΝΩΝ ΤΟΥ SYSMON

Στην παραπάνω εικόνα μπορεί κάποιος εύκολα να διακρίνει οτι το Sysmon αποτελείται απο πολλαπλές ρουτίνες οι οποίες προσθέτουν στο αρχείο καταγραφής πληροφορίες όπως η αλλαγή χρόνου δημιουργίας ενός αρχείου, η παρακολούθηση μιας διεργασίας με σκοπό την καταγραφή της λειτουργικότητας της, ο τερματισμός μια διεργασίας αλλά και η ανίχνευση σύνδεσης μέσα στο δίκτυο.

Με αφορμή τις πληροφορίες που έχουμε αναφερθεί παραπάνω, έχουμε δημιουργήσει ένα φίλτρο στο οποίο καταγράφουμε την εκτέλεση ενός msi αρχείου ως service (wmiprvse.exe). Τα αρχεία MSI ονομάζονται επίσης αρχεία πακέτων εγκατάστασης των Windows, τα οποία χρησιμοποιούνται για τη διανομή ενημερώσεων των Windows και προγραμμάτων εγκατάστασης τρίτων που αναπτύχθηκαν για συστήματα που βασίζονται σε Windows.
Με την ενεργοποίηση αυτών των αρχείων MSI, αρχικοποιείται η διαδικασία εγκατάστασης για τη σχετική εφαρμογή ή την ενημέρωση των Windows, προκειμένου να εκτελεστούν οι απαραίτητες λειτουργίες για την εγκατάσταση της εφαρμογής ή της ενημέρωσης στον υπολογιστή που βασίζεται στα Windows. Το περιεχόμενο αυτών των αρχείων MSI είναι συνήθως αρχεία στοιχείων και βιβλιοθήκες πόρων μιας εφαρμογής ή ενημέρωσης των Windows, τα οποία εκφορτώνονται στο σύστημα κατά τη διαδικασία εγκατάστασης, ακολουθώντας τις εντολές εγκατάστασης και τις οδηγίες που είναι επίσης συσκευασμένες σε αυτά τα αρχεία MSI.

Η Microsoft (για Windows Update) και οι προγραμματιστές τρίτων δημιουργούν και διανέμουν αυτά τα πακέτα εγκατάστασης των Windows ως αρχεία που επισυνάπτονται με την επέκταση .msi, η οποία μπορεί επίσης να αποσυμπιεστεί χρησιμοποιώντας το λογισμικό 7-Zip.

Σχετικά με τον φίλτρο το οποίο έχουμε δημιουργήσει μπορούμε να αντιληφθούμε ότι το Sysmon δεν θα αναφέρει μόνο τις περιπτώσεις που θα καταγράψει σχετικά με την δημιουργία ενός process wmiprvse.exe. Το εργαλείο μας δίνει την δυνατότητα να καταγράψουμε κανόνες συμβάντων τύπου pipe έτσι ώστε να καταγραφούν ακόμα και μικροαλλαγές ή η αθέμιτη χρήση του wmi process.

```
<Sysmon schemaversion="10.4">
<HashAlgorithms>md5,sha256</HashAlgorithms>
<CheckRevocation/>
<EventFiltering>
<ProcessCreate onmatch="include">
<Image condition="contains">wmiprvse.exe</Image>
</ProcessCreate>
</EventFiltering>
</Sysmon>
```

ΕΙΚΟΝΑ 11: ΔΗΜΙΟΥΡΓΙΑ ΚΑΝΟΝΩΝ ΣΤΟ ΑΡΧΕΙΟ ΡΥΘΜΙΣΕΩΝ

Δεν χρειάζεται να ρυθμίσει κανείς τα πάντα, μπορεί να διαμορφώσει μόνο μερικά πράγματα, περιλαμβάνοντας ορισμένα γεγονότα είτε εξαιρώντας τα.

Για την περίπτωση σύνδεσης στο δίκτυο, γίνεται παρακολούθηση όλων των τύπων συμβάντων.

Είναι όμως αυτό αρκετά περίπλοκο ώστε να μην μπορεί κάποιος να παρακολουθήσει διαδικασίες οι οποίες δεν είναι τοσο γνωστές;
Η απάντηση δεν είναι ξεκάθαρη και γι αυτό το λόγο θα χρειαστεί να γίνουν κάποιες παραμετροποιήσεις στα αρχεία.

sysmon_swift.xml - Notepad

File Edit Format View Help

```
<Sysmon schemaversion="3.30">
        <HashAlgorithms>md5,sha256</HashAlgorithms>
        <EventFiltering>

        <!--SYSMON EVENT ID 1 : PROCESS CREATION-->
                <!--DATA: UtcTime, ProcessGuid, ProcessID, Image, CommandLine, CurrentDirector
TerminalSessionId, IntegrityLevel, Hashes, ParentProcessGuid, ParentProcessId, ParentImage, Pa
                <ProcessCreate onmatch="exclude">
                <!--COMMENT:    All process launched will be included, except for what matches
specific as possible, to
                                avoid user-mode executables imitating other process names to a
in an existing directory.
                                Ultimately, you must weigh CPU time checking many detailed rul
exploiting the blindness created.-->
                        <!--SECTION: Microsoft Windows-->
                        <CommandLine condition="begin with">C:\Windows\system32\DllHost.exe /P
Microsoft:Windows-->
                        <CommandLine condition="is">C:\Windows\system32\SearchIndexer.exe /Emb
Microsoft:Windows: Search Indexer-->
                        <Image condition="end with">C:\Windows\System32\CompatTelRunner.exe</I
Experience Improvement-->
                        <Image condition="is">C:\Windows\System32\MusNotification.exe</Image>
                        <Image condition="is">C:\Windows\System32\MusNotificationUx.exe</Image
```

ΕΙΚΟΝΑ 12: ΠΑΡΑΜΕΤΡΟΠΟΙΗΣΗ ΤΩΝ ΑΡΧΕΙΩΝ ΤΟΥ SYSMON

Όπως βλέπουμε στην παραπάνω Εικόνα, έχουν αναφερθεί διαφορετικοί τύποι διαδικασιών που δεν χρήζουν παρακολούθησης. Γίνεται λοιπόν απόκλιση όλων των ονομάτων των γνωστών διαδικασιών και αυτό μπορεί να δημιουργήσει κάποιο πρόβλημα καθώς μπορεί να κρύβεται κακόβουλο λογισμικό ως ένα από αυτά τα γνωστά αρχεία.
Για το λόγο αυτό πρέπει να δημιουργούνται διαφορετικές συνθήκες στο αρχείο για αυτές τις διαδικασίες οι οποίες όμως δημιουργούν ένα πραγματικά μεγάλο αρχείο.
Μια καλή λύση για το παράπάνω πρόβλημα είναι η εξαίρεση όλων των διαδικασιών που δεν μας ενδιαφέρουν στο δίκτυο όπως για παράδειγμα να εξαιρείται οτιδήποτε μπορεί να σημιουργήσει επικονωνία δικτύου μέσα στο C: \users.

Παρόλα αυτά, η σύνδεση δικτύου που δημιουργείται από διαφορετικούς τύπους αρχείων δεν ενδείκνυται συνήθως καθώς είναι εκτός της νομικής διαμόρφωσης του λειτουργικού συτήματος.
Ακόμα και με την εντολή exclude, δεν αποκλείονται πολλά πράγματα, απλά εξαιρούμε διάφορους τύπους οδηγών εγκατάστασης από τα Windows και της Intel.

4.4 Αρχείο Παραμετροποίησης του Sysmon

- Βασική διαμόρφωση
  Υπάρχει η γρήορη ρύθμιση του Sysmon για την παρακολούθηση επιλεγμένων συμβάντων στη γραμμή εντολών. Πιο συγκεκριμένα:
  - -h [hash, …] = Καθορίζει τους τύπους κατακερματισμού που πρέπει να καταγραφούν. Χρήση του “*” για καταγραφή όλων ή των -h SHA256 και IMPHASH.
  - -n [process, …] = Ενεργοποίηση καταγραφής των συνδέσεων δικτύου. Μπορεί να οριστεί και μία ενιαία διαδικασία χρησιμοποιώντας ένα όνομα διαδικασίας όπως -n cmd.exe
  - -l [process, …] = Ενεργοποίηση καταγραφής συμβάντων που έχουν φορτωθεί με Εικόνα. Μπορεί να οριστεί και μία ενιαία διαδικασία χρησιμοποιώντας ένα όνομα διαδικασίας όπως -n cmd.exe

Να σημειωθεί ότι έαν γίνει χρήση των εντολών για την ενεργοποίηση και την απανεργοποίηση του Sysmon, οι επιλογές αυτεές δεν είναι πρόσθετες και πρέπει να καθοριστούν όλες οι επιθυμητές επιλογές ταυτόχρονα. Η εντολή Sysmon -c θα επαναφέρει την προεπιλογή.

- Προηγμένη διαμόρφωση
  Οι προηγμένοι κανόνες για το Sysmon δημιουργούνται σε μορφή XML που είναι ο προτεινόμενος τρόπος για διαμόρφωση του Sysmon. Ένας σκελετός για ένα αρχείο XML Sysmon είναι ο ακόλουθος:

```
<Sysmon schemaversion=”3.20”>
        <!—Capture all hash types-->
        <HashAlgorithms>*</HashAlgorithms>
        <EventFiltering>
        …conditions go here…
        </EventFiltering>
</Sysmon>
```

Οι συνθήκες καθορίζουν τον έλεγχο για το τι θα εγγραφεί και τι οχι. Ορίζονται οι λίστες των κανόνων χρησιμοποιώντας τις οδηγίες “include” και “exclude” και με βάση αυτές, όλα τα υπόλοιπα θα αντιστοιχούν ή οχι στον κατάλογο. Ουσιαστικά γίνεται ένα είδος whitelist/blacklist των συνθηκών που θα καταγραφούν, όπως για παράδειγμα την καταγραφή μόνο των προγραμμάτων οδήγησης που δεν έχουν υπογραφεί από τα Microsoft Windows. Αυτό μπορεί να γίνει με τη χρήση του παρακάτω κανόνα με μια συνθήκη υπογραφής:

```
<DriverLoad onmatch=”exclude”>
        <Signature condition=”is”>Microsoft Windows</Signature>
</DriverLoad>
```

Ένας παρόμοιος κανόνας που θα περιλαμβάνει την καταγραφή της κίνησης στη θύρα 80, IP 1.1.1.1 είναι ο παρακάτω:

```
<NetworkConnect onmatch=”include”>
        <DestinationPort condition=”is”>80</DestinationPort>
        <DestinationIp condition=”is”>1.1.1.1</DestinationIp>
</NetworkConnect>
```

Οι διαθέσιμες συνθήκες για τις καταχωρίσεις πεδίου είναι οι εξής:

- is - Οι τιμές είναι ίσες (προεπιλογή)
- is not - Οι τιμές είναι διαφορετικές
- contains – Το πεδίο περιέχει αυτή την τιμή
- excludes - Το πεδίο δεν περιέχει αυτή την τιμή
- begin with - Το πεδίο αρχίζει με αυτή την τιμή
- end with - Το πεδίο τελειώνει με αυτή την τιμή
- less than – Η σύγκριση είναι μικρότερη από το μηδέν
- more than – Η σύγκριση είναι μεγαλύτερη από το μηδέν
- image – Ταιριάζει με διαδρομή Εικόνας (είτε το όνομα Εικόνας ή πλήρης διαδρομή)

5 Αρχεία Καταγραφής των Windows

5.1 Ανάλυση των αρχείων καταγραφής

Το αρχείο καταγραφής συμβάντων των Windows (Event Viewer) είναι μια λεπτομερής καταγραφή των ειδοποιήσεων συστήματος, ασφάλειας και εφαρμογών που έχουν αποθηκευτεί από το λειτουργικό σύστημα των Windows για τη διάγνωση προβλημάτων του συτήματος αλλά και την πρόβλεψη μελλοντικών σφαλμάτων.
Το λειτουργικό σύστημα Windows παρακολουθεί συγκεκριμένα συμβάντα στα αρχεία καταγραφής του, όπως είναι οι εφαρμογές εγκατάστασης, η διαχείριση ασφάλειας, οι λειτουργίες ρύθμισης συστήματος κατά την αρχική εκκίνηση και τα προβλήματα ή τα σφάλματα.
Κάθε συμβάν σε καταχώρηση αρχείου καταγραφής περιέχει τις ακόλουθες πληροφορίες:

- Ημερομηνία: Η ημερομηνία εμφάνισης του συμβάντος.
- Ώρα: Ο χρόνος που συνέβη το συμβάν.
- Χρήστης: Το όνομα χρήστη που καταγράφηκε στο μηχάνημα όταν συνέβη το συμβάν.
- Υπολογιστής: Το όνομα του υπολογιστή.
- Αναγνωριστικό συμβάντος: Αριθμός αναγνώρισης των Windows που καθορίζει τον τύπο συμβάντος.
- Πηγή: Το πρόγραμμα ή το στοιχείο που προκάλεσε το συμβάν.
- Τύπος: Ο τύπος συμβάντος, συμπεριλαμβανομένων πληροφοριών, προειδοποίησης, σφάλματος, ελέγχου επιτυχίας ασφαλείας ή ελέγχου αποτυχίας ασφαλείας.

Το λειτουργικό σύστημα Windows καταγράφει συμβάντα σε πέντε τομείς:

- Εφαρμογή
- Ασφάλεια
- Ρύθμιση
- Σύστημα
- Προωθούμενα συμβάντα

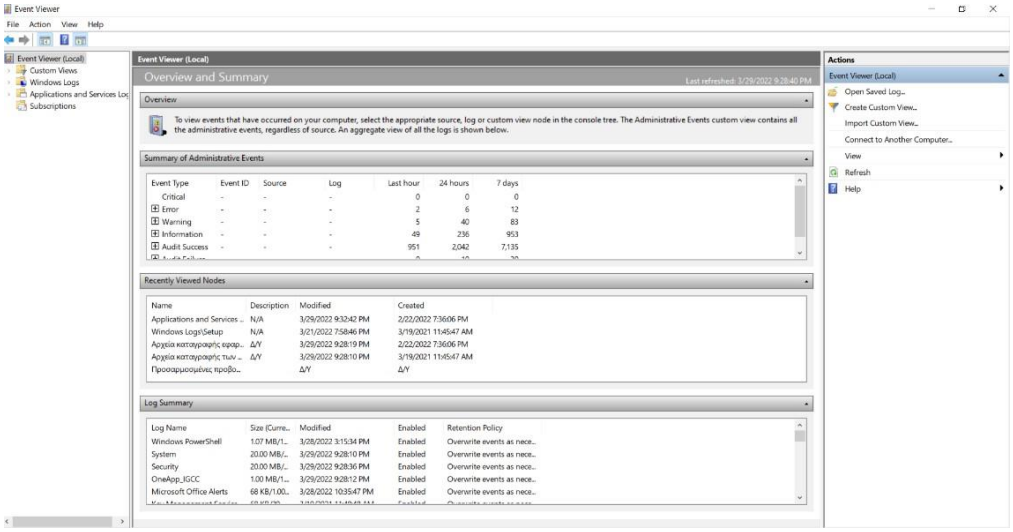
Τα Windows αποθηκεύουν τα αρχεία καταγραφής συμβάντων στο φάκελο C: \ WINDOWS \ system32 \ config \.

1. Τα συμβάντα εφαρμογής αφορούν σε συμβάντα με το λογισμικό που είναι εγκατεστημένο
   στον τοπικό υπολογιστή. Εάν μια εφαρμογή όπως το Microsoft Word διακοπεί, τότε το αρχείο καταγραφής συμβάντων των Windows θα δημιουργήσει μια καταχώρηση ημερολογίου σχετικά με το ζήτημα, το όνομα της εφαρμογής και γιατί διακόπηκε.
2. Τα συμβάντα ασφαλείας αποθηκεύουν πληροφορίες βάσει των πολιτικών ελέγχου του συστήματος των Windows και τα τυπικά αποθηκευμένα συμβάντα περιλαμβάνουν τις προσπάθειες σύνδεσης και την πρόσβαση σε πόρους. Για παράδειγμα, το αρχείο καταγραφής ασφαλείας αποθηκεύει μια εγγραφή όταν ο υπολογιστής επιχειρεί να επαληθεύσει τα διαπιστευτήρια λογαριασμού όταν ένας χρήστης προσπαθεί να συνδεθεί σε ένα μηχάνημα.

3. Τα συμβάντα ρύθμισης περιλαμβάνουν συμβάντα σχετικά με τον έλεγχο τομέων, όπως η
   θέση των αρχείων καταγραφής μετά από μια διαμόρφωση δίσκου.
4. Τα συμβάντα του συστήματος σχετίζονται με συμβάντα σε συγκεκριμένα συστήματα των Windows, όπως η κατάσταση των προγραμμάτων οδήγησης συσκευών.
5. Τα προωθούμενα συμβάντα φτάνουν από άλλα μηχανήματα στο ίδιο δίκτυο όταν ένας διαχειριστής θέλει να χρησιμοποιήσει έναν υπολογιστή που συγκεντρώνει πολλαπλά αρχεία καταγραφής.

5.2 Χρήση του εργαλείου καταγραφής συμβάντων

Η Microsoft περιλαμβάνει το πρόγραμμα προβολής συμβάντων στο λειτουργικό σύστημα Windows Server και πελάτη για την προβολή των αρχείων καταγραφής. Οι χρήστες έχουν εύκολη πρόσβαση στο πρόγραμμα κάνοντας κλικ στο κουμπί Έναρξη και έτσι μπορούν να επιλέξουν το επιθυμητή επιλογή.



ΕΙΚΟΝΑ 13: ΠΡΟΒΟΛΗ ΤΟΥ EVENT VIEWER

Όπως βλέπουμε και παραπάνω, τα Windows κατηγοριοποιούν κάθε συμβάν με ένα επίπεδο σοβαρότητας. Υπάρχουν πέντε τύποι συμβάντων που μπορούν να καταγραφούν. Όλα αυτά έχουν καλά καθορισμένα κοινά δεδομένα και μπορούν προαιρετικά να περιλαμβάνουν δεδομένα για συγκεκριμένα συμβάντα.

Η εφαρμογή υποδεικνύει τον τύπο συμβάντος όταν αναφέρει ένα συμβάν. Κάθε συμβάν πρέπει να είναι ενός μόνο τύπου. Το Event Viewer εμφανίζει ένα διαφορετικό εικονίδιο για κάθε τύπο στην προβολή λίστας του αρχείου καταγραφής συμβάντων.

Ο παρακάτω πίνακας περιγράφει τους πέντε τύπους συμβάντων που χρησιμοποιούνται στην καταγραφή συμβάντων.

Συμβάν (Event)	Περιγραφή
Σφάλμα	Ένα συμβάν που υποδεικνύει ένα σημαντικό πρόβλημα, όπως απώλεια δεδομένων ή απώλεια λειτουργικότητας. Για παράδειγμα, εάν μια υπηρεσία αποτύχει να φορτώσει κατά την εκκίνηση, καταγράφεται ένα συμβάν σφάλματος.
Προειδοποίηση	Ένα γεγονός που δεν είναι απαραίτητα σημαντικό, αλλά μπορεί να υποδηλώνει ένα πιθανό μελλοντικό πρόβλημα. Για παράδειγμα, όταν ο χώρος στο δίσκο είναι χαμηλός,

Συμβάν (Event)	Περιγραφή
	καταγράφεται ένα συμβάν προειδοποίησης. Εάν μια εφαρμογή μπορεί να ανακτήσει από ένα συμβάν χωρίς απώλεια λειτουργικότητας ή δεδομένων, μπορεί γενικά να ταξινομήσει το συμβάν ως συμβάν προειδοποίησης.
Πληροφορία	Ένα συμβάν που περιγράφει την επιτυχή λειτουργία μιας εφαρμογής, προγράμματος οδήγησης ή υπηρεσίας. Για παράδειγμα, όταν ένα πρόγραμμα οδήγησης δικτύου φορτώνεται με επιτυχία, μπορεί να είναι σκόπιμο να καταγράψετε ένα συμβάν πληροφοριών. Σημειώστε ότι είναι γενικά ακατάλληλο για μια εφαρμογή επιτραπέζιου υπολογιστή να καταγράφει ένα συμβάν κάθε φορά που ξεκινά.
Επιτυχία ελέγχου	Ένα συμβάν που καταγράφει μια ελεγμένη προσπάθεια πρόσβασης ασφαλείας που είναι επιτυχής. Για παράδειγμα, η επιτυχημένη προσπάθεια ενός χρήστη να συνδεθεί στο σύστημα καταγράφεται ως συμβάν επιτυχούς ελέγχου.
Αποτυχία ελέγχου	Ένα συμβάν που καταγράφει μια ελεγμένη προσπάθεια πρόσβασης ασφαλείας που αποτυγχάνει. Για παράδειγμα, εάν ένας χρήστης προσπαθήσει να αποκτήσει πρόσβαση σε μια μονάδα δίσκου δικτύου και αποτύχει, η προσπάθεια καταγράφεται ως συμβάν ελέγχου αποτυχίας.

ΠΙΝΑΚΑΣ 2: ΠΕΡΙΓΡΑΦΗ ΣΥΜΒΑΝΤΩΝ

Οι επιλεγμένες δραστηριότητες των χρηστών μπορούν να παρακολουθούνται ελέγχοντας συμβάντα ασφαλείας και στη συνέχεια τοποθετώντας καταχωρήσεις στο αρχείο καταγραφής ασφαλείας ενός υπολογιστή.

5.3 Ανάλυση του εργαλείου καταγραφής συμβάντων

Το πρόγραμμα καταγραφής συμβάντων παραθέτει τα αρχεία καταγραφής ως εξής:

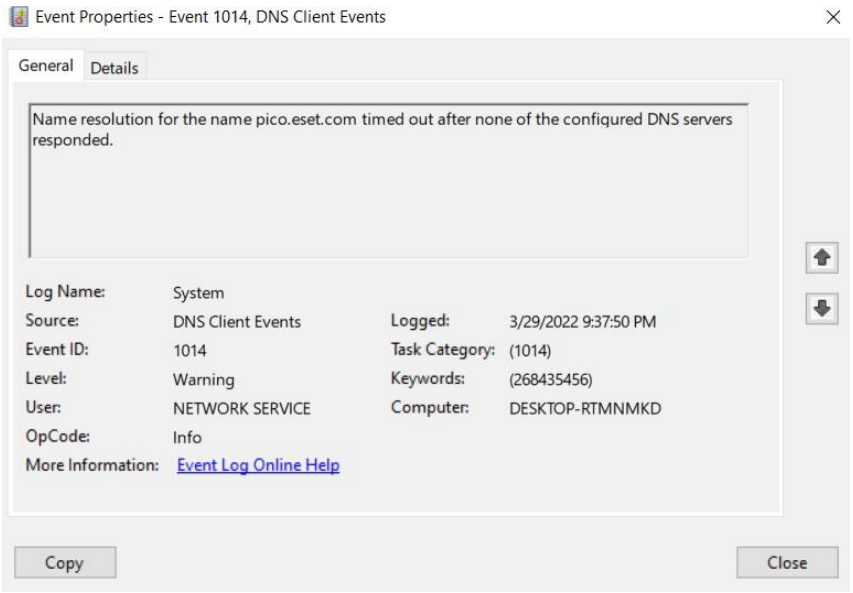
- Επίπεδο
  - Τύπος συμβάντος
- Ημερομηνία & Ώρα
  - Την ημερομηνία και την ώρα που συνέβη το συμβάν.
- Πηγή
  - Η πηγή που δημιούργησε το συμβάν π.χ. στοιχείο του συστήματος.
- Αναγνωριστικό συμβάντος
  - Αριθμός συμβάντος που προσδιορίζει τον τύπο συμβάντος.
- Κατηγορία
  - Κάθε συμβάν μπορεί να ορίσει τις δικές του αριθμημένες κατηγορίες στις οποίες αντιστοιχίζεται. Το πρόγραμμα καταγραφής συμβάντων μπορεί να χρησιμοποιήσει την κατηγορία για να φιλτράρει συμβάντα στο αρχείο καταγραφής.

System Number of events: 32,168

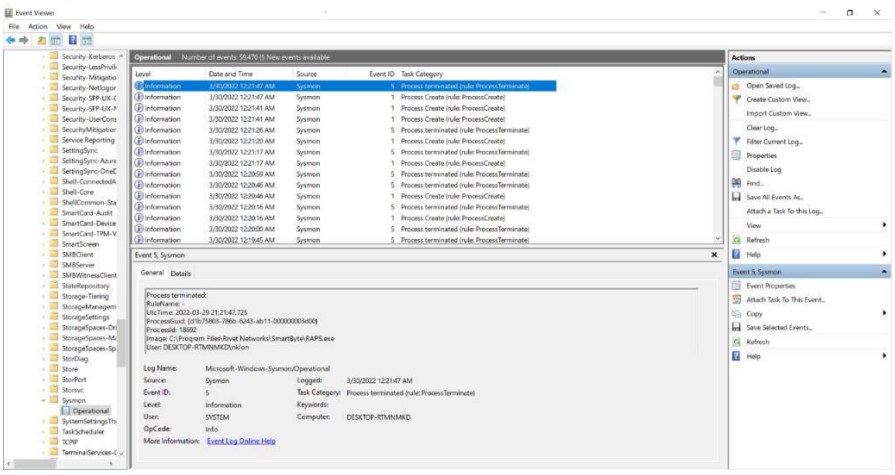
Level	Date and Time	Source	Event ID	Task Category
Information	3/29/2022 10:10:02 PM	Kernel-Power	107	(102)
Information	3/29/2022 10:10:01 PM	Kernel-Power	42	(64)
Warning	3/29/2022 9:50:55 PM	WHEA-Logger	17	None
Warning	3/29/2022 9:41:57 PM	WHEA-Logger	17	None
Warning	3/29/2022 9:37:50 PM	DNS Client Events	1014	(1014)
Error	3/29/2022 9:28:04 PM	WindowsUpdateClient	20	Windows Update Agent
Information	3/29/2022 9:28:01 PM	WindowsUpdateClient	43	Windows Update Agent
Warning	3/29/2022 9:27:56 PM	DNS Client Events	1014	(1014)
Warning	3/29/2022 9:27:54 PM	DNS Client Events	1014	(1014)
Warning	3/29/2022 9:27:53 PM	BTHUSB	34	None
Information	3/29/2022 9:27:53 PM	BTHUSB	18	None
Warning	3/29/2022 9:27:52 PM	DNS Client Events	1014	(1014)
Information	3/29/2022 9:27:52 PM	Power-Troubleshooter	1	None
Information	3/29/2022 9:27:50 PM	Kernel-Boot	27	(33)
Information	3/29/2022 9:27:50 PM	Kernel-Boot	25	(32)

ΕΙΚΟΝΑ 14: ΠΡΟΒΟΛΗ ΤΩΝ ΣΥΜΒΑΝΤΩΝ

Κάνοντας διπλό κλικ σε ένα συμβάν, προβάλλονται οι λεπτομέρειες:



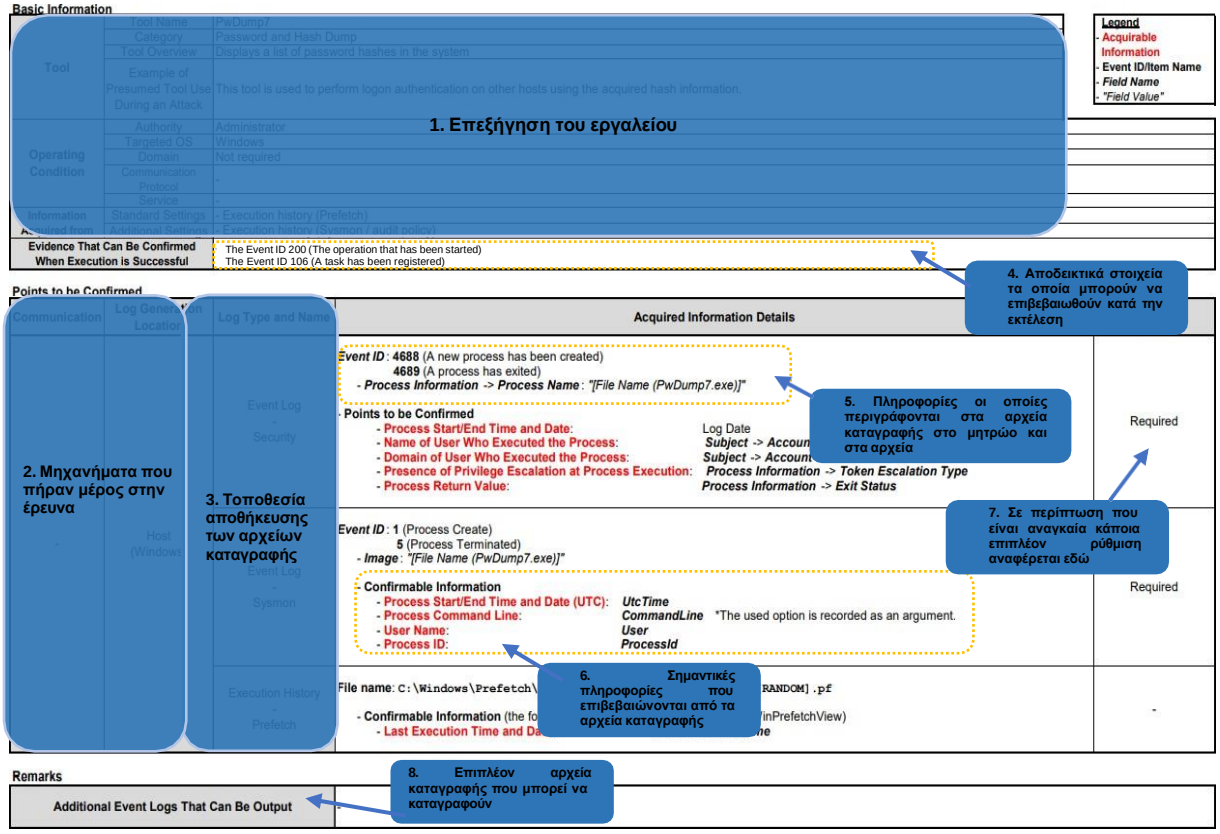
ΕΙΚΟΝΑ 15: ΠΡΟΒΟΛΗ ΛΕΠΤΟΜΕΡΕΙΩΝ ΕΝΟΣ ΣΥΜΒΑΝΤΟΣ



ΕΙΚΟΝΑ 16: ΠΡΟΓΡΑΜΜΑ ΠΡΟΒΟΛΗΣ ΣΥΜΒΑΝΤΩΝ ΜΕΣΩ ΤΟΥ SYSMON

6 Αποτελέσματα έρευνας

Συνοψίζοντας όλες τις βασικές πληροφορίες συμπεριλαμβανομένης της λειτουργικότητας των εργαλείων που δοκιμάστηκαν σε αυτή την έρευνα και των αρχείων καταγραφής κατά την εκτέλεση τους, δημιουργήθηκε ένας πίνακας με τα αποτελέσματα της έρευνας όπου περιγράφει αναλυτικά τις λεπτομέρειες των αρχείων καταγραφής οι οποίες μπορούν να αποκτηθούν με τις κατάλληλες ρυθμίσεις.



ΕΙΚΟΝΑ 17: ΕΠΕΞΗΓΗΣΗ ΠΙΝΑΚΑ ΜΕ ΤΑ ΑΠΟΤΕΛΕΣΜΑΤΑ ΤΗΣ ΕΡΕΥΝΑΣ

Από τον παραπάνω πίνακα προκύπτουν οχτώ (8) στοιχεία τα οποία περιγράφουν το περιεχόμενο του εκάστοτε στοιχείου. Πιο συγκεκριμένα:

1. Περιγραφή του εργαλείου
   - Οι επιπτώσεις απο τη χρήση του εργαλείου, τα προνόμια χρήσης του εργαλείου, το πρωτόκολλο επικοινωνίας και οι σχετικές υπηρεσίες.
2. Περιβάλλον δοκιμής
   - Πληροφορίες για το λειτουργικό σύστημα των κεντρικών υπολογιστών
3. Χώρος αποθήκευσης αρχείου καταγραφής
   - Θέση αποθήκευσης μητρώων και αρχείων καταγραφής
4. Στοιχεία που μπορούν να επιβεβαιωθούν εάν η εκτέλεση είναι επιτυχής
   - Η μέθοδος επιβεβαίωσης της επιτυχούς εκτέλεσης του εργαλείου.
5. Πληροφορίες που περιγράφονται στα αρχεία καταγραφής συμβάντων, στα μητρώα και στα αρχεία
   - Εάν η εγγραφή σε ένα αρχείο καταγραφής συμβάντων ταιριάζει με την περιγραφή αυτού του στοιχείου, τότε είναι πιθανό ότι το αρχείο έγινε με την εκτέλεση του σχετικού εργαλείου και συνεπώς απαιτείται έρευνα.
6. Σημαντικές πληροφορίες που μπορούν να επιβεβαιωθούν σε ενα αρχείο καταγραφής
   - Σημαντικές πληροφορίες που μπορούν να χρησιμοποιηθούν για τη διερεύνηση αρχείων στα αρχεία καταγραφής.

7. Το αν απαιτείται ή οχι πρόσθετη ρύθμιση για την απόκτηση του σχετικού αρχείου καταγραφής
    - Αναφέρεται ως “-” όταν το αρχείο καταγραφής μπορεί να δημιουργηθεί στην τυπική ρύθμιση ή ως “Απαιτείται” όταν χρειάζεται πρόσθετη ρύθμιση.
8. Πρόσθετα αρχεία καταγραφής συμβάντων που μπορεί να καταγραφούν
    - Κάθε αρχείο που μπορεί να καταγραφεί επιπρόσθετα.

6.1 Πίνακας αποτελεσμάτων για τα εργαλεία εσωτερικής μετακίνησης

Δεδομένου ότι έχει γίνει κατανοητός ο παραπάνω πίνακας και τα στοιχεία που εμπεριέχει, ας προχωρήσουμε με τα αποτελέσματα από τα εργαλεία εσωτερικής μετακίνησης που αναπτύξαμε σε προηγούμενη ενότητα.

6.1.1 Psexec

Βασικές Πληροφορίες

Εργαλείο	Όνομα Εργαλείου	**psexec**
	Κατηγορία	Εκτελεση εντολών
	Περιγραφή εργαλείου	Εκτέλεση διεργασιών σε ένα απομακρυσμένο σύστημα
	Παράδειγμα υποτιθέμενης χρήσης του εργαλείου σε περίπτωση επίθεσης	Αυτό το εργαλείο μπορεί να χρησιμοποιηθεί για να εκτελεστούν απομακρυσμένες εντολές σε ένα πελάτη ή σε ένα διακομιστή στον τομέα ενός δικτύου. • Κεντρικός υπολογιστής πηγής: Psexec πηγή εκτέλεσης εντολών • Κεντρικός υπολογιστής προορισμού: Ο προορισμός που έχει συνδεθεί με την εντολή Psexec.
Κατάσταση λειτουργίας	Εξουσιοδότηση	• Κεντρικός υπολογιστής πηγής: Βασικός χρήστης • Κεντρικός υπολογιστής προορισμού: Διαχειριστής
	Στοχευμένο Λογισμικό	Windows
	Τομέας	Δεν απαιτείται
	Πρωτόκολλο επικοινωνίας	135/TCP, 445/TCP, μία τυχαία μεγάλη πόρτα. Όταν εκτελείται σε ένα περιβάλλον τομέα, πραγματοποιείται επικοινωνία για έλεγχο ταυτότητας Kerberos με τον ελεγκτή τομέα.
	Υπηρεσία	-

Απαιτούμενη πληροφορία	Ρυθμίσεις	• Κεντρικός υπολογιστής πηγής: Έχει καταχωρηθεί ένα μητρώο με το οποίο έχει εισαχθεί η Άδεια Χρήσης του PsExec. • Κεντρικός υπολογιστής προορισμού: Έχει καταχωρηθεί το γεγονός ότι έχει εγκατασταθεί, ξεκινήσει ή τελειώσει η υπηρεσία PsExec.
	Επιπλέον ρυθμίσεις	• Ιστορικό εκτέλεσης: (Sysmon/πολιτική ελέγχου) • Κεντρικός υπολογιστής πηγής: Το γεγονός ότι η διαδικασία PsExec εκτελέστηκε και έγινε σύνδεση στον προορισμό μέσω του δικτύου, καθώς και το όνομα της εντολής και το όρισμα για μια εντολή που εκτελέστηκε εξ 'αποστάσεως καταγράφονται. • Κεντρικός υπολογιστής προορισμού: Το γεγονός ότι το δυαδικό αρχείο PSEXESVC δημιουργήθηκε και προσπεράστηκε και ότι η σύνδεση έγινε από την πηγή μέσω του δικτύου, καθώς και το όνομα εντολής και το όρισμα για μια εντολή που εκτελέστηκε εξ 'αποστάσεως καταγράφονται.
Αποδεικτικά τα οποία μπορούν να επαληθευτούν όταν η εκτέλεση είναι επιτυχής		Εάν κάποιο από τα παρακάτω παραιτηθεί τότε είναι πιθανόν να έχει εκτελεστεί το Psexec. • Κεντρικός υπολογιστής πηγής: Εάν υπάρχει η παρακάτω καταγραφή στις καταγραφές γεγονότων ○ Event ID 4689 (μία διεργασία εξήλθε) από το Psexec.exe έχει καταγραφεί στις καταγραφές γεγονότων «Security» με τιμή αποτελέσματος εκτέλεσης 0x0. • Κεντρικός υπολογιστής προορισμού: Το Psexesvc.exe έχει εγκατασταθεί.

ΠΙΝΑΚΑΣ 3: PSEXEC

Στοιχεία που μπορούν να επαληθευτούν

Επικοινωνία	Τοποθεσία δημιουργίας των αρχείων καταγραφής	Τύπος και όνομα αρχείου καταγραφής	Απαιτούμενες Πληροφορίες	Επιπλέον ρυθμίσεις
Λειτουρικό σύτημα : Χρήστης	Πηγή	Αρχείο καταγραφής -	**Event ID: 4688 (νέα διεργασία δημιουργήθηκε)**	Απαιτείται

Windows ↓ Λειτουργικό σύτημα : Χρήστης Windows		Ασφάλεια	**Event ID: 4689 (μία διεργασία εξήλθε)** **-Πληροφορίες διεργασίας → Όνομα διεργασίας: '[Αρχείο εκτέλεσης (psexec.exe)])'** **Πληροφορίες Επιβεβαίωσης:** • **Όνομα και ημερομηνία έναρξης/τερματισμού διεργασίας: Ημερομηνία καταγραφής** • **Όνομα χρήστη που εκτέλεσε τη διεργασία: Subject →Account Name** • **Τομέας του χρήστη που εκτέλεσε τη διεργασία: Subject →Account Domain** • **Προβολή των προνομίων που είχε κατά την εκτέλεση της διεργασίας.: Process Information → Token Escalation Type** • **Τιμή που επέστρεψε η διεργασία. : Process Information →Exit Status**	
		Αρχείο καταγραφής - Sysmon	**Event ID: 1 (Δημιουργία διεργασίας)** **Event ID: 2 (Η διεργασία εξήλθε)** **-Image: '[Αρχείο εκτέλεσης(psexec.exe)]'** **Πληροφορίες Επιβεβαίωσης:** • **Ημερομηνία και ώρα έναρξης/τερματισμού της διεργασίας (UTC): UTCTime** • **Διεργασία στη γραμμή εντολών: Γραμμή εντολών 'Η εντολή που εκτελέστηκε απομακρυσμένα καταγράφτηκε στο στοιχείο της γραμμής εντολών.'** • **Όνομα χρήστη: Χρήστης** • **Αναγνωριστικό διεργασίας: ProcessId**	Απαιτείται

		Ιστορικό Εκτέλεσης - Προετοιμασία	**Καταγραφή στο αρχείο μητρώου: HKEY_USERS\[SID]\Software \Sysinternals\PsExec - EulaAccepted ‘Εάν το αρχείο PsExec δεν εκτελέστηκε στο παρελθόν, εκδίδεται το μητρώο με την ένδειξη ότι έχει τεθεί η συμφωνία άδειας χρήσης. (Εάν η υπηρεσία εκτελέστηκε στο παρελθόν, το μητρώο θα παραμείνει αμετάβλητο.)’**	Απαιτείται
	Προορισμός	Αρχείο καταγραφής - Σύστημα	Event ID: 7045 (Μία υπηρεσία εγκαταστάθηκε στο σύστημα) **Πληροφορίες Επιβεβαίωσης**: • Όνομα διεργασίας: ‘Psexesvc’ • Μονοπάτι: "%SystemRoot%\PSEXESVC.exe"	Απαιτείται
			Event ID: 7036 (Η κατάσταση της υπηρεσίας άλλαξε) * Η υπηρεσία "PSEXESVC" εισέρχεται στην κατάσταση "Executing" πριν εκτελέσει μια απομακρυσμένη διαδικασία και στην κατάσταση "Stopped" μετά την εκτέλεση.	
		Αρχείο καταγραφής - Ασφάλεια	Event ID: 5156 (Η πλατφόρμα φιλτραρίσματος των Windows έχει επιτρέψει μια σύνδεση) ‘Η επικοινωνία γίνεται από τον κεντρικό υπολογιστή προέλευσης στον κεντρικό υπολογιστή προορισμού με πόρτες προορισμού 135 και 445,’ (Παράδειγμα: Η πλατφόρμα φιλτραρίσματος Windows επέτρεψε την επικοινωνία από 192.168.0.10:49210 έως 192.168.0.2: 445) * Η επικοινωνία γίνεται από τον κεντρικό υπολογιστή προέλευσης στον κεντρικό υπολογιστή προορισμού με τυχαία υψηλή θύρα ως θύρα προορισμού. (1024 και πάνω)	Απαιτείται
			Event ID 5140 (Πρόσβαση σε αντικείμενο κοινόχρηστου δικτύου)	Απαιτείται

			Πληροφορίες Επιβεβαίωσης: • Ώρα και ημερομηνία σύνδεσης: Ημερομηνία καταγραφής 'Η ημερομηνία και η ώρα πριν την έναρξη του Psexesvc.exe' Ο χρήστης που χρησιμοποιήθηκε για τη δύνδεση: Subject→Security ID και Account Name • Κεντρικός υπολογιστής πηγής: Πληροφορίες διαδυκτίου→Διεύθυνση πηγής και πόρτες πηγής. • Κοινόχρηστη σύνδεση: "\??\C:\Windows" (administrative share)	
			Event ID: 4672 (Ειδικά προνόμια ανατέθηκαν κατά τη σύνδεση): 'Πριν από αυτό το γεγονός, εμφανίζεται το γεγονός 4624. Ένας λογαριασμός που έχει συνδεθεί κατά την εμφάνιση του συμβάντος 4624 έχει ανατεθειμένα δικαιώματα.' Πληροφορίες Επιβεβαίωσης: • Ο λογαριασμός που χρησιμοποιήθηκε για τη σύνδεση: Subject→Security ID και Account Name • Ανατεθειμένα προνόμια: Privileges	
			Event ID: 4656 (Ζητήθηκε μια χειραγώγηση σε ένα αντικείμενο) Event ID: 4663 (Έγινε προσπάθεια πρόσβασης σε ένα αντικείμενο) • Object -> Object Name :"C:\Windows\PSEXESVC.exe"	Απαιτείται
			Event ID: 5140 (Ένα κοινόχρηστο αντικείμενο στο δίκτυο προσπελάστηκε) Πληροφορίες Επιβεβαίωσης: • Λογαριασμός που χρησιμοποιήθηκε για τη	Απαιτείται

			σύνδεση: Security ID και Account Name • Κεντρικός υπολογιστής πηγής; Πληροφορίες διαδικτύου →Διεύθυνση πηγής και πόρτες πηγής • Κοινόχρηστη σύνδεση: *\IPC$ (administrative share)	
			Event ID: 5145 (Έχει επιλεγεί ένα αντικείμενο κοινής χρήσης δικτύου για να διαπιστωθεί εάν μπορεί να αποκτηθεί η επιθυμητή πρόσβαση από τον πελάτη) Το αναγνωριστικό του γεγονότος καταγράφετε πολλές φόρες. Πληροφορίες Επιβεβαίωσης: • Λογαριασμός που χρησιμοποιήθηκε για τη σύνδεση: Security ID και Account Name • Κεντρικός υπολογιστής πηγής; Πληροφορίες διαδυκτίου →Διεύθυνση πηγής και πόρτες πηγής • Κοινόχρηστος στόχος: Κοινόχρηστη πληροφορία → Κοινόχρηστο μονοπάτι Η διαδρομή κοινής χρήσης περιέχει "PSEXESVC" και "\\ ?? \ C: \ Windows".	Απαιτείται
			Event ID: 4656 (Ζητήθηκε μια χειραγώγηση σε ένα αντικείμενο) Event ID: 4660 (Ένα αντικείμενο διαγράφτηκε) Event ID: 4658 (Η χειραγώγηση του αντικειμένου τερματίστηκε) Πληροφορίες διεργασίας→Αναγνωριστικό διεργασίας: ‘0x4’ (System) Πληροφορίες Επιβεβαίωσης: • Στοχευμένο αρχείο: Object Object Name ("C:\Windows\PSEXESVC.exe") • Αναγνωριστικό χειραγώγησης: Object → Handle ID (Χρησιμοποιείται για	Απαιτείται

			συσχέτιση με άλλες καταγραφές) • Λεπτομέρειες διεργασίας: Access Request Information → Accces (‘Delete’,’ReadAttributes’) • Επιτυχία ή Αποτυχία: Keywords (‘Επιτυχία ελέγχου’)	
		Αρχείο καταγραφής - Sysmon	Event ID: 1 (Δημιουργία διεργασίας) Event ID: 5 (Τερματισμός διεργασίας) **Πληροφορίες Επιβεβαίωσης:** • Πρόοδος απομακρυσμένης εκτέλεσης: Image • Επιχειρηματολογία: CommandLine • Ημερομηνία και ώρα έναρξης/τερματισμού της διεργασίας (UTC): UtcTime ‘Η ημερομηνία και η ώρα μετά την έναρξη του PSEXESVC.exe και πριν από το τέλος του’ • Λογαριασμός χρήστη που χρησιμοποιήθηκε για την πομακρυσμένη εκτέλεση: User	Απαιτείται

Παρατηρήσεις

Επιπλέον στοιχεία καταγραφής που μπορεί να εξαχθούν	Πληροφορίες σχετικά με την εκτέλεση της διαδικασίας χρησιμοποιώντας PsExec μπορεί να καταγραφούν στον "Destination Host".

6.1.2 Wmiexec

Βασικές πληροφορίες

Εργαλείο	Όνομα Εργαλείου	**Wmiexec**
	Κατηγορία	Εκτελεση εντολών
	Περιγραφή εργαλείου	Εργαλείο διαχείρισης του συστήματος των Windows
	Παράδειγμα υποτιθέμενης χρήσης του εργαλείου σε περίπτωση επίθεσης	Αυτό το εργαλείο εκτελεί μια δέσμη ενεργειών για άλλους κεντρικούς υπολογιστές. • Κεντρικός υπολογιστής πηγής: Η πηγή που εκτελεί το wmiexec.vbs

		• Κεντρικός υπολογιστής προορισμού: Το μηχάνημα που έχει πρόσβαση από το wmiexec.vbs
Κατάσταση λειτουργίας	Εξουσιοδότηση	Απλός χρήστης
	Στοχευμένο Λογισμικό	Windows
	Τομέας	Δεν απαιτείται
	Πρωτόκολλο επικοινωνίας	135/TCP, 445/TCP
	Υπηρεσία	-
Απαιτούμενη πληροφορία	Ρυθμίσεις	Ιστορικό εκτέλεσης (Prefetch)
	Επιπλέον ρυθμίσεις	• Ιστορικό δημιουργίας / διαγραφής αρχείου (Πολιτική ελέγχου) • Ιστορικό εκτέλεσης (Sysmon)
Αποδεικτικά τα οποία μπορούν να επαληθευτούν όταν η εκτέλεση είναι επιτυχής		Κεντρικός υπολογιστής πηγής: Το κοινόχρηστο στοιχείο "WMI_SHARE" έχει δημιουργηθεί και διαγράφτηκε.

ΠΙΝΑΚΑΣ 4: WMIEXEC

Στοιχεία που μπορούν να επαληθευτούν

Επικοινωνία	**Τοποθεσία δημιουργίας των αρχείων καταγραφής**	**Τύπος και όνομα αρχείου καταγραφής**	**Απαιτούμενες Πληροφορίες**	**Επιπλέον ρυθμίσεις**
Λειτουργικό σύτημα : Χρήστης Windows ↓ Λειτουργικό σύτημα : Χρήστης Windows	Πηγή	Αρχείο καταγραφής - Ασφάλεια	Event ID: 4688 (νέα ιεργασία δημιουργήθηκε) Event ID: 4689 (μία διεργασία εξήλθε) -Πληροφορίες διεργασίας → Όνομα διεργασίας: '[Αρχείο εκτέλεσης (psexec.exe)])' **Πληροφορίες Επιβεβαίωσης:** • Όνομα και ημερομηνία έναρξης/τερματισμού διεργασίας: Ημερομηνία καταγραφής • Όνομα χρήστη που εκτέλεσε τη διεργασία: Subject →Account Name • Τομέας του χρήστη που εκτέλεσε τη διεργασία: Subject	Απαιτείται

			→Account Domain • Προβολή των προνομίων που είχε κατά την εκτέλεση της διεργασίας.: Process Information → Token Escalation Type • Τιμή που επέστρεψε η διεργασία. : Process Information →Exit Status	
			Event ID: 5156 (Η πλατφόρμα φιλτραρίσματος των Windows έχει επιτρέψει μια σύνδεση) -Πληροφορίες διεργασίας →Όνομα διεργασίας: "C:\Windows\System32\cscript.exe" **Πληροφορίες Επιβεβαίωσης:** • Port πηγής: Πληροφορίες διαδικτύου →Port προορισμού "Ένας αριθμός θύρας μπορεί να αλλάξει καθορίζοντάς τον στον προορισμό"	Απαιτείται
		Αρχείο καταγραφής - Sysmon	Event ID: 1 (Μία διεργασία δημιουργήθηκε) Event ID: 5 (Μία διεργασία τερματίστηκε) -Image: "C:\Windows\System32\cscript.exe" **Πληροφορίες Επιβεβαίωσης:** • Ημερομηνία και ώρα έναρξης/τερματισμού διεργασίας (UTC)→UtcTime	Απαιτείται

			• Διεργασία στη γραμμή εντολών→Γραμμή εντολών • Όνομα χρήστη→User • Αναγνωριστικό διεργασίας→ProcessId	
		Ιστορικό Εκτέλεσης - Προετοιμασία	Όνομα αρχείου: C:\Windows\Prefetch\CSCRIPT.EXE-D1EF4768.pf **Πληροφορίες Επιβεβαίωσης:** Η επιβεβαίωση μπορεί να γίνει χρησιμοποιώντας το εργαλείο WinPrefetchView • Ημερομηνία και ώρα τελευταίας εκτέλεσης→ Last Execution Time	Απαιτείται
	Προορισμός	Αρχείο καταγραφής - Ασφάλεια	Event ID: 4656 (Ζητήθηκε ο χειρισμός ενός αντικειμένου) Event ID: 4663 (Έγινε προσπάθεια προσπέλασης ενός αντικειμένου) Event ID: 4658 (Η χειραγώγηση του αντικειμένου τελείωσε) -Αντικείμενο→Object Name "(C:\Windows\Temp\wmi.dll)" -Πληροφορίες αιτήματος πρόσβασης→Access / Reason for Access: ("WriteData (ή AddFile)", "AppendData (ή AddSubdirectory ή CreatePipeInstance)") **Πληροφορίες Επιβεβαίωσης:** • Όνομα διεργασίας: "C:\Windows\System32\cmd.exe" • Αναγνωριστικό χειραγώγησης: Object -> Handle	Απαιτείται

			ID Χρησιμοποιείται για σύνδεση με άλλα αρχεία καταγραφής	
			Event ID: 5142 (Προστέθηκε ένα κοινόχρηστο αντικείμενο στο δίκτυο) **Πληροφορίες Επιβεβαίωσης:** • Ημερομηνία και ώρα έναρξης/τερματισμού της διεργασίας: Log Date • Όνομα χρήστη που εκτέλεσε την διεργασία: Subject→Account Name • Τομέας του χρήστη που εκτέλεσε τη διεργασία: Subject→ Account Domain • Κοινόχρηστο όνομα: Share Information→ Share name: ("*\WMI_SHARE") • Κοινόχρηστη διαδρομή: Share Information→Share Path: ("C:\Windows\Temp")	Απαιτείται
			Event ID: 5145 (Έχει επιλεγεί ένα αντικείμενο κοινόχρηστου δικτύου για να διαπιστωθεί εάν ο πελάτης μπορεί να λάβει την επιθυμητή πρόσβαση) **Πληροφορίες Επιβεβαίωσης:** • Ημερομηνία και ώρα έναρξης/τερματισμού της	Απαιτείται

			διεργασίας: Log Date • Όνομα χρήστη που εκτέλεσε την διεργασία: Subject→Account Name • Τομέας του χρήστη που εκτέλεσε τη διεργασία: Subject→ Account Domain • Κοινόχρηστο όνομα: Share Information→ Share name: ("*\WMI_SHARE") • Κοινόχρηστη διαδρομή: Share Information→Share Path: ("C:\Windows\Temp") • Κοινόχρηστη διαδρομή: Share Information→Relative Target Name: (“wmi.dll”)	
			Event ID: 4656 (Ζητήθηκε ο χειρισμός ενός αντικειμένου) Event ID: 4660 (Το αντικείμενο διαγράφτηκε) Event ID: 4658 (Η χειραγώγηση του αντικειμένου τελείωσε) -Αντικείμενο→Object Name: "(C:\Windows\Temp\wmi.dll)" -Πληροφορίες Αίτησης Πρόσβασης→ Access/Reason for Access: "DELETE **Πληροφορίες Επιβεβαίωσης:** • Όνομα διεργασίας: "(C:\Windows\System32\cmd.exe)"	Απαιτείται

			Event ID: 5144 (Ένα κοινόχρηστο με το δίκτυο αντικείμενο διαγράφτηκε) **Πληροφορίες Επιβεβαίωσης:** • Κοινόχρηστο όνομα: Share Information →Share name: ("*\WMI_SHARE") • Κοινόχρηστη διαδρομή: Share Information→Share Path: ("C:\Windows\Temp")	Απαιτείται
		Αρχείο καταγραφής - Sysmon	Event ID: 1 (Μία διεργασία δημιουργήθηκε) Event ID: 5 (Μία διεργασία τερματίστηκε) -Image: "C:\Windows\System32\wbem\WmiPrvSE.exe" "C:\Windows\System32\cmd.exe" **Πληροφορίες Επιβεβαίωσης:** • Ημερομηνία και ώρα έναρξης/τερματισμού διεργασίας (UTC)→UtcTime • Διεργασία στη γραμμή εντολών→Γραμμή εντολών • Όνομα χρήστη→User • Αναγνωριστικό διεργασίας→ProcessId	Απαιτείται
		Ιστορικό Εκτέλεσης - Προετοιμασία	Όνομα αρχείου: C:\Windows\Prefetch\CSCRIPT.EXE-D1EF4768.pf **Πληροφορίες Επιβεβαίωσης:** Η επιβεβαίωση μπορεί να γίνει	Απαιτείται

			χρησιμοποιώντας το εργαλείο WinPrefetchView • Last Execution Time and Date: Last Execution Time	

Παρατηρήσεις

Επιπλέον στοιχεία καταγραφής που μπορεί να εξαχθούν	**.....**

6.1.3 WinRm

Βασικές Πληροφορίες

Εργαλείο	Όνομα Εργαλείου	**winrm**
	Κατηγορία	Εκτελεση εντολών
	Περιγραφή εργαλείου	Απομακρυσμένη εκτέλεση εντολών σε ένα κεντρικό υπολογιστή
	Παράδειγμα υποτιθέμενης χρήσης του εργαλείου σε περίπτωση επίθεσης	Αυτό το εργαλείο χρησιμοποιείται για μια έρευνα πριν από την εκτέλεση μιας απομακρυσμένης εντολής. • Κεντρικός υπολογιστής πηγής: Πηγή εκτέλεσης εντολών WinRM • Κεντρικό υπολογιστής προορισμού: Το μηχάνημα που έχει πρόσβαση από την εντολή WinRM
Κατάσταση λειτουργίας	Εξουσιοδότηση	Διαχειριστής
	Στοχευμένο Λογισμικό	Windows
	Τομέας	-
	Πρωτόκολλο επικοινωνίας	5985/tcp (HTTP) or 5986/tcp (HTTPS)
	Υπηρεσία	Κεντρικός υπολογιστής προορισμού: Απομακρυσμένη διαχείριση των Windows (WS-Management)
Απαιτούμενη πληροφορία	Ρυθμίσεις	Ιστορικό εκτέλεσης (Prefetch)
	Επιπλέον ρυθμίσεις	• Κεντρικός υπολογιστής πηγής: Ιστορικό εκτέλεσης (Sysmon) • Κεντρικός υπολογιστής προορισμού: Σύνδεση από τον κεντρικό υπολογιστή πηγής.
Αποδεικτικά τα οποία μπορούν να επαληθευτούν όταν η εκτέλεση είναι επιτυχής		Κεντρικός υπολογιστής πηγής: Εάν υπάρχει το ακόλουθο

	αρχείο καταγραφής, είναι δυνατό να εκτελεστεί το WinRM. • Καταγράφεται ένα γεγονός που υποδεικνύει ότι το cscript.exe έχει πρόσβαση στον κεντρικό υπολογιστή προορισμού με αναγνωριστικά συμβάντων 1 και 5 του αρχείου καταγραφής συμβάντων "Sysmon"

ΠΙΝΑΚΑΣ 5: WINRM

Στοιχεία που μπορούν να επαληθευτούν

Επικοινωνία	Τοποθεσία δημιουργίας των αρχείων καταγραφής	Τύπος και όνομα αρχείου καταγραφής	Απαιτούμενες Πληροφορίες	Επιπλέον ρυθμίσεις
Λειτουργικό σύτημα : Χρήστης Windows ↓ Λειτουργικό σύτημα : Χρήστης Windows	Πηγή	Αρχείο καταγραφής - Ασφάλεια	Event ID: 4688 (νέα ιεργασία δημιουργήθηκε) Event ID: 4689 (μία διεργασία εξήλθε) -Πληροφορίες διεργασίας → Όνομα διεργασίας: '[Αρχείο εκτέλεσης (psexec.exe)])' **Πληροφορίες Επιβεβαίωσης:** • Όνομα και ημερομηνία έναρξης/τερματισμού διεργασίας: Ημερομηνία καταγραφής • Όνομα χρήστη που εκτέλεσε τη διεργασία: Subject →Account Name • Τομέας του χρήστη που εκτέλεσε τη διεργασία: Subject →Account Domain • Προβολή των προνομίων που είχε κατά την εκτέλεση της διεργασίας.: Process Information → Token Escalation Type	Απαιτείται

			• Τιμή που επέστρεψε η διεργασία. : Process Information →Exit Status	
			Event ID: 5156 (Η πλατφόρμα φιλτραρίσματος των Windows έχει επιτρέψει μια σύνδεση) -Πληροφορίες διεργασίας→ Όνομα διεργασίας: "C:\Windows\System32\cscript.exe" **Πληροφορίες Επιβεβαίωσης**: • Port πηγής: Πληροφορίες διαδικτύου→Port προορισμού "Ένας αριθμός θύρας μπορεί να αλλάξει καθορίζοντάς τον στον προορισμό"	Απαιτείται
		Αρχείο καταγραφής - Sysmon	Event ID: 1 (Μία διεργασία δημιουργήθηκε) Event ID: 5 (Μία διεργασία τερματίστηκε) -Image: "C:\Windows\System32\cscript.exe" **Πληροφορίες Επιβεβαίωσης:** • Ημερομηνία και ώρα έναρξης/τερματισμού διεργασίας (UTC)→UtcTime • Διεργασία στη γραμμή εντολών→Γραμμή εντολών • Όνομα χρήστη→User • Αναγνωριστικό διεργασίας→ProcessId	Απαιτείται
		Αρχείο καταγραφής -	Event ID: 166 (Ο επιλεγμένος μηχανισμός ελέγχου	Απαιτείται

		Εφαρμογές και υπηρεσίες Microsoft\Windows \Windows Remote Management	ταυτότητας είναι διαπραγματεύσιμος) **Πληροφορίες Επιβεβαίωσης:** • Μέθοδος αυθεντικοποίησης: Authentication Mechanism (ο επιλεγμένος μηχανισμός ελέγχου ταυτότητας είναι Kerberos)	
			Event ID: 80 (Αποστολή της αίτησης για λειτουργία λήψης στον κεντρικό υπολογιστή προορισμού και τη θύρα) **Πληροφορίες Επιβεβαίωσης:** • Αποστολή υπολογιστή προορισμού και θύρα: "[Host Name]:[Port]"	Απαιτείται
			Event ID: 143 (Λήψη απάντησης από το επίπεδο δικτύου) **Πληροφορίες Επιβεβαίωσης:** • Κατάσταση: Status (200 (HTTP_STATUS_OK))	Απαιτείται
			Event ID: 132 (Η λειτουργία WSMan εντοπίζεται επιτυχώς) **Πληροφορίες Επιβεβαίωσης:** • Χρόνος και ημερομηνία ολοκλήρωσης (UTC): UTCTime	Απαιτείται

		Ιστορικό Εκτέλεσης - Προετοιμασία	Όνομα αρχείου: C:\Windows\Prefetch\CSCRIPT.EXE-D1EF4768.pf **Πληροφορίες Επιβεβαίωσης:** • Χρόνος και ημερομηνία τελευταίας εκτέλεσης: Last Execution Time	Απαιτείται
	Προορισμός	Αρχείο καταγραφής - Ασφάλεια	Event ID: 5156 (Το φιλτράρισμα των Windows επέτρεψε μία σύνδεση) -Πληροφορίες εφαρμογής→Όνομα εφαρμογής: “System” -Πληροφορίες διαδικτύου→ Προορισμός: “Inbound” -Πληροφορίες διαδικτύου→Port πηγής: "5985" (HTTP) ή "5986" (HTTPS) -Πληροφορίες διαδικτύου→ Πρωτόκολλο: "6" (TCP) **Πληροφορίες Επιβεβαίωσης:** • Κεντρικός υπολογιστής πηγής Πληροφορίες διαδικτύου→ Διεύθυνση προορισμού • Κεντρικός υπολογιστής προορισμού: Πληροφορίες διαδικτύου→Port προορισμού	Απαιτείται
			Event ID: 4624 (Ένας λογαριασμός συνδέθηκε επιτυχώς) -Τύπος εισόδου: “3” **Πληροφορίες Επιβεβαίωσης:** • Αναγνωριστικό ασφαλείας: New	Απαιτείται

			Logon→Security ID • Αναγνωριστικό σύνδεσης: Subject→Logon ID • Λογαριασμός: Account Name→ Account Domain	
			Event ID: 4656 (Ζητήθηκε ο χειρισμός ενός αντικειμένου) Event ID: 4658 (Η χειραγώγηση του αντικειμένου τελείωσε) -Πληροφορίες διεργασίας→Όνομα διεργασίας: "C:\Windows\System32\svchost.exe" -Αντικείμενο→Όνομα αντικειμένου: "\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\WSMAN\Client" -Αντικείμενο→ Όνομα αντικειμένου: "\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\WSMAN\Service" **Πληροφορίες Επιβεβαίωσης:** • Αναγνωριστικό χειρισμού: Object→Handle ID • Λεπτομέρειες αίτησης πρόσβασης: Access request information→Access ("READ_CONTROL", "Query key value", "Enumerate sub-keys", "Notify about changes to keys") * Αυτή η διαδικασία εκτελείται πολλές φορές.	Απαιτείται
	Active Directory	Αρχείο καταγραφής	Event ID: 5156 (Η πλατφόρμα	Απαιτείται

	Domain Controller	- Ασφάλεια	φιλτραρίσματος των Windows επέτρεψε μία σύνδεση) -Πληροφορίες εφαρμογής→ Όνομα εφαρμογής: "\device\harddiskvolume2 \windows\system32\lsass.exe" -Πληροφορίες διαδικτύου→ Κατεύθυνση: "Inbound" **Πληροφορίες Επιβεβαίωσης:** • Κεντρικός υπολογιστής πηγής: Network Information→Destination Address	
			Event ID: 4769 (Ζητήθηκε εισιτήριο υπηρεσίας Kerberos) -Πληροφορίες διαδικτύου→ Διεύθυνση πελάτη:"[Source Host]" **Πληροφορίες Επιβεβαίωσης:** • Χρήστης που χρησιμοποιήθηκε: Account Information→ Account Name	Απαιτείται

Παρατηρήσεις

Επιπλέον στοιχεία καταγραφής που μπορεί να εξαχθούν	**.....**

6.1.4 Wmic

Βασικές Πληροφορίες

Εργαλείο	Όνομα Εργαλείου	**winrm**
	Κατηγορία	Εκτελεση εντολών
	Περιγραφή εργαλείου	Ένα εργαλείο που χρησιμοποιείται για τη διαχείριση συστημάτων των Windows
	Παράδειγμα υποτιθέμενης χρήσης του εργαλείου σε περίπτωση επίθεσης	Αυτό το εργαλείο χρησιμοποιείται για μια έρευνα πριν από την εκτέλεση μιας απομακρυσμένης εντολής με το WMI. • Κεντρικός υπολογιστής πηγής: Πηγή εκτέλεσης εντολών wmic.

		• Κεντρικό υπολογιστής προορισμού: Το μηχάνημα που έχει πρόσβαση από την εντολή wmic.
Κατάσταση λειτουργίας	Εξουσιοδότηση	Απλός χρήστης “Ανάλογα με την εντολή που εκτελείται στην στην απομακρυσμένη πλευρά, ενδέχεται να απαιτούνται δικαιώματα διαχειριστή.”
	Στοχευμένο Λογισμικό	Windows
	Τομέας	Δεν απαιτείται
	Πρωτόκολλο επικοινωνίας	135 / tcp, 445 / tcp, μια τυχαία επιλεγμένη θύρα TCP 1024 ή μεγαλύτερη
	Υπηρεσία	Μέσα διαχείρισης παραθύρων, κλήση απομακρυσμένης διαδικασίας (RPC)
Απαιτούμενη πληροφορία	Ρυθμίσεις	Ιστορικό εκτέλεσης (Prefetch)
	Επιπλέον ρυθμίσεις	Λεπτομέρειες εκτέλεσης διεργασίας (το όρισμα στο wmic) και η κατάσταση εκτέλεσης επιτυχία ή αποτυχία (η τιμή επιστροφής) (Sysmon και πολιτική ελέγχου)
Αποδεικτικά τα οποία μπορούν να επαληθευτούν όταν η εκτέλεση είναι επιτυχής		Εάν τα ακόλουθα αρχεία καταγραφής που έχουν τον ίδιο χρόνο καταγραφής βρίσκονται στο "host source" και "host destination", είναι πιθανό να γίνει μια απομακρυσμένη σύνδεση -Κεντρικός υπολογιστής πηγής: Εάν υπάρχει η παρακάτω εγγραφή στις καταγραφές συμβάντων: • Event ID: 4689 (μία διεργασία εξήλθε) -Κεντρικός υπολογιστής προορισμού: Εάν υπάρχει η παρακάτω εγγραφή στο Sysmon • Event ID: Καταγράφεται στο αρχείο καταγραφής συμβάντων "Sysmon" ότι εκτελέστηκε το αρχείο WmiPrvSE.exe με τα αναγνωριστικά συμβάντων 1 και 5

ΠΙΝΑΚΑΣ 6: WMIC

Στοιχεία που μπορούν να επαληθευτούν

Επικοινωνία	**Τοποθεσία δημιουργίας των αρχείων καταγραφής**	**Τύπος και όνομα αρχείου καταγραφής**	**Απαιτούμενες Πληροφορίες**	**Επιπλέον ρυθμίσεις**
Λειτουργικό σύτημα : Χρήστης Windows ↓ Λειτουργικό σύτημα : Χρήστης	Πηγή	Αρχείο καταγραφής - Ασφάλεια	Event ID: 4688 (νέα ιεργασία δημιουργήθηκε) Event ID: 4689 (μία διεργασία εξήλθε) -Πληροφορίες διεργασίας → Όνομα διεργασίας:	Απαιτείται

Windows			'[Αρχείο εκτέλεσης (psexec.exe)])' **Πληροφορίες Επιβεβαίωσης:** • Όνομα και ημερομηνία έναρξης/τερματισμού διεργασίας: Ημερομηνία καταγραφής • Όνομα χρήστη που εκτέλεσε τη διεργασία: Subject →Account Name • Τομέας του χρήστη που εκτέλεσε τη διεργασία: Subject →Account Domain • Προβολή των προνομίων που είχε κατά την εκτέλεση της διεργασίας.: Process Information → Token Escalation Type • Τιμή που επέστρεψε η διεργασία. : Process Information →Exit Status	
		Αρχείο καταγραφής - Sysmon	Event ID: 1 (Μία διεργασία δημιουργήθηκε) Event ID: 5 (Μία διεργασία τερματίστηκε) -Image: "C:\Windows\System32\wbem\WMIC.exe" **Πληροφορίες Επιβεβαίωσης:** • Ημερομηνία και ώρα έναρξης/τερματισμού διεργασίας (UTC) → UtcTime • Διεργασία στη γραμμή	Απαιτείται

			εντολών→Γραμμή εντολών ("C:\Windows\System32\wmiprvse.exe -secured -Embedding") • Όνομα χρήστη→User ("NT AUTHORITY\NETWORK SERVICE") • Αναγνωριστικό διεργασίας→ProcessId	
		Ιστορικό Εκτέλεσης - Προετοιμασία	Όνομα αρχείου: C:\Windows\Prefetch\WMIC.EXE-98223A30.pf **Πληροφορίες Επιβεβαίωσης:** (τα παρακάτω μπορούν να επιβεβαιωθούν χρησιμοποιώντας αυτό το εργαλείο: WinPrefetchView) • Ημερομηνία και ώρα τελευταίας εκτέλεσης: Last Executed Time	

	Προορισμός	Αρχείο καταγραφής - Sysmon	Event ID: 1 (Μία διεργασία δημιουργήθηκε) Event ID: 5 (Μία διεργασία τερματίστηκε) -Image: "C:\Windows\System32\wbem\WmiPrvSE.exe" **Πληροφορίες Επιβεβαίωσης:** • Ημερομηνία και ώρα έναρξης/τερματισμού διεργασίας (UTC) → UtcTime • Διεργασία στη γραμμή εντολών→Γραμμή εντολών ("C:\Windows\System32\wmiprvse.exe - secured -Embedding") • Όνομα χρήστη→User ("NT AUTHORITY\NETWORK SERVICE") • Αναγνωριστικό διεργασίας→ProcessId	Απαιτείται
		Ιστορικό Εκτέλεσης - Προετοιμασία	Όνομα αρχείου: C:\Windows\Prefetch\WMIPRVSE.EXE-1628051C.pf **Πληροφορίες Επιβεβαίωσης:** (τα παρακάτω μπορούν να επιβεβαιωθούν χρησιμοποιώντας αυτό το εργαλείο: WinPrefetchView) • Ημερομηνία και ώρα τελευταίας εκτέλεσης: Last Executed Time	Απαιτείται

Παρατηρήσεις

Επιπλέον στοιχεία καταγραφής που μπορεί να εξαχθούν	-Ανάλογα με τη διαδικασία που ονομάζεται wmic, τα συμβάντα για τη συγκεκριμένη διαδικασία μπορούν να καταγραφούν. -Εάν ο χρήστης υπάρχει στην υπηρεσία καταλόγου Active Directory, το αίτημα ελέγχου ταυτότητας μπορεί να καταγραφεί στον ελεγκτή τομέα -Ωστόσο, δεν είναι δυνατό να προσδιοριστεί εάν ένα τέτοιο αίτημα ελέγχου ταυτότητας έγινε από wmic ή άλλους.

7 Συμπεράσματα

Κατά την υλοποίηση και εκπόνηση αυτής της διπλωματικής, αναγνωρίζουμε οτι για την καλύτερη καταγραφή συμβάντων τα οποία έχουν πραγματοποιηθεί στο δίκτυο μας και έχουν αναγνωριστεί ως lateral movement, αποτελούνε ένα πολυ μεγάλο και σοβαρό κίνδυνο στην Ασφάλεια Πληροφοριακών Συστημάτων.

Στις περιπτώσεις επιθέσεων οι οποίες χαρακτηρίζονται ως lateral movement, ένα από τα εργαλεία που χρησιμοποιούμε είναι το Sysmon το οποίο με τις κατάλληλες ρυθμίσεις μπορεί να ανιχνεύσει τέτοια συμβάντα.

Για την ανάγκη αυτή χρειάστηκε να δοκιμάσουμε και να πραγματοποιήσουμε οι ίδιοι μια προσομοίωση τέτοιας επίθεσης με τη χρήση ειδικών εργαλείων απομακρυσμένου ελέγχου και χειραγώγησης λειτουργικών συστημάτων έτσι ώστε να μπορέσουμε να αποδείξουμε στην αναφορά μας τη λειτουργικότητα του προγράμματος (Sysmon) αλλά και την αποτελεσματικότητά του στην εύρεση τέτοιου είδους συμβάντων.

Σύμφωνα με τα αποτελέσματα από τα αρχεία συμβάντων, έγινε μια πλήρης καταγραφή και ανάλυση των εργαλείων που ενεργοποίησαν τις συνθήκες αυτές έτσι ώστε να εντοπιστεί η εσωτερική μετακίνηση στο δίκτυο.

Τέλος, θεωρούμε ότι το Sysmon αποτελεί ένα εξαιρετικά αποτελεσματικό εργαλείο το οποίο προσφέρει μεγαλη ποικιλία πληροφοριών σε τέτοιου είδους συμβάντα το οποίο καθιστά τη χρήση του αναγκαία σε κάθε είδους σύστημα.

Βιβλιογραφία-Πηγές

1) SwiftOnSecurity, (2018). Sysmon-Configuration (Github)
2) The MITRE Corporation, (2018). Lateral Movement
3) Mark Russinovich and Thomas Garnier, (2022). Sysmon Configuration
4) Mark Russinovich, (2020). Sysinternals
5) Detecting Lateral Movement through Tracking Event Logs, (2015). JPCERT Coordination Center
6) Malware Archaeology, (2019). Windows Sysmon Logging Cheat Sheet
7) Malware Archaeology, (2019). Windows Advanced Logging Cheat Sheet
8) Nader Shalabi, (2018). Utilities for Sysmon tools
9) Mark Russinovich, (2021). Psexec
10) William Ballenthin, Matthew Graeber and Claudiu Teodorescu, (2015). Windows Management Instrumentation (WMI) Offense, Defense, and Forensics
11) Chris Truncer (2018). WMImplant
12) Microsoft Official Documentation, (2021). Installation and configuration for Windows Remote Management
13) Jon Martindale, (2021). How to Use Event Viewer in Windows 10
14) Papadopoulos, (2019). Windows Sysmon tool for lateral movement alerts