ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΙΓΑΙΟΥ
ΠΟΛΥΤΕΧΝΙΚΗ ΣΧΟΛΗ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ

ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Μεταπτυχιακή Διπλωματική Εργασία
ΘΕΜΑ:
«Ανακατασκευή μιας εγκληματικής ενέργειας μέσω του Windows Event Viewer»

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

του

Χρήστου ΒΟΥΛΓΑΡΗ [19006, icsdm319006 @icsd.aegean.gr]

Επιβλέπουσα : Κωνσταντία Μπαρμπάτσαλου

Μέλη εξεταστικής επιτροπής:

Σάμος, 02/2022

Η σελίδα αυτή είναι σκόπιμα λευκή.

Πρόλογος και ευχαριστίες

του/της
[ΒΟΥΛΓΑΡΗ ΧΡΗΣΤΟΥ]
Τμήμα Μηχανικών Πληροφοριακών και Επικοινωνιακών Συστημάτων
ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΙΓΑΙΟΥ

Η σελίδα αυτή είναι σκόπιμα λευκή.

Πίνακας περιεχομένων

Λίστα Εικόνων

Λίστα Πινάκων

Ακρωνύμια

TCP	Transmission Control Protocol
IP	Internet Protocol
VM	Virtual Machine

Περίληψη

Η άμεση κατανόηση της φύσης των απειλών είναι ίσως το σημαντικότερο κομμάτι στην έγκαιρη αντίδρασης απέναντι σε κακόβουλες ενέργειες. Ο Event Viewer είναι ένα πρόγραμμα του λειτουργικού συστήματος Microsoft Windows, το οποίο επιτρέπει στους διαχειριστές και τους χρήστες του συστήματος να προβάλλουν αρχεία καταγραφής συμβάντων. Αυτή η κεντρική υπηρεσία καταγραφής μπορεί να χρησιμοποιηθεί από εφαρμογές και λοιπά στοιχεία του λειτουργικού συστήματος για την αναφορά συμβάντων που έχουν συμβεί, όπως η αποτυχία εκκίνησης ενός στοιχείου ή η ολοκλήρωση μιας ενέργειας. Στόχος της παρούσας διπλωματικής εργασίας είναι η προσπάθεια οπτικής αναπαράστασης μιας κακόβουλης ενέργειας σε ένα τερματικό, βασισμένη στο αρχείο καταγραφής του Event Viewer. Συγκεκριμένα έγινε προσπάθεια να απεικονιστούν τα συμβάντα που δημιουργούνται στα αρχεία καταγραφής μετά την εκτέλεση κακόβουλης ενέργειας. Για της ανάγκες του σεναρίου υλοποιήθηκε επίθεση με εκτέλεση reverse_tcp σε ένα μηχάνημα με λειτουργικό σύστημα Windows XP. Μετά την εκτέλεση της κακόβουλης ενέργειας συλλέχθηκαν τα κυριότερα στοιχεία από τα αρχεία καταγραφής τα οποία αποτυπώθηκαν σε έναν πίνακα. Η μελέτη των ιχνών που αφήνει το κάθε είδος επίθεσης στο σύστημα μπορεί να υποβοηθήσει σημαντικά τη διαδικασία εντοπισμού μιας κακόβουλης ενέργειας.

Λέξεις Κλειδιά: Windows Event Viewer, Windows XP, ανακαταστευή κακόβουλης ενέργειας

Abstract

Immediate understanding of the nature of the threats is perhaps the most important part of responding in a timely manner to malicious actions. Event Viewer is a Microsoft Windows operating system program that allows system administrators and users to view event logs. This central logging service can be used by applications and other operating system components to report events that have occurred, such as a component failing to start or completing an action. The aim of this thesis is to attempt a visual representation of a malicious action which is performed against a computer, based on the Event Viewer log. More specifically, an attempt was made to depict the events that are created in the logs after the execution of a malicious action. For the purposes of the scenario, a reverse tcp attack was performed on a machine running Windows XP. After the malicious action was performed, the data were collected from the logs which were recorded in a table. Studying the traces left by each type of attack on the system can greatly aid in the process of detecting a malicious action.

Keywords: Windows Event Viewer, Windows XP, reconstruction, malicious activity

1

Εισαγωγή

1.1 Η σημασία της ασφάλειας των πληροφοριακών συστημάτων σήμερα

Η ασφάλεια των πληροφοριακών συστημάτων αποτελεί βασικό κομμάτι στον γενικότερο χώρο της πληροφορικής. Λόγω του ότι στις μέρες μας αφορά τεράστιο πλήθος δικτύων υπολογιστών ή μεμονωμένων συσκευών, αποτελεί τεράστια πρόκληση. Συνεπώς, αν και έχουν αναπτυχθεί αποτελεσματικές τεχνικές και μηχανισμοί για την προστασία τους, το πλήθος τους και μόνο προσθέτει πολυπλοκότητα στο έργο της προστασίας τους από κακόβουλες ενέργειες. Βασικό πρόβλημα στην αντιμετώπιση των απειλών είναι η έγκαιρη ανίχνευση της κακόβουλης ενέργειας, ώστε να ληφθούν τα κατάλληλα μέτρα για την αντιμετώπισή της.

1.2 Αντικείμενο διπλωματικής

Σκοπός της παρούσας διπλωματικής διατριβής είναι η προσπάθεια οπτικοποίησης των στοιχείων καταγραφής του Event Viewer έπειτα από κακόβουλη ενέργεια σε ένα τερματικό βασισμένη στα event ids των αρχείων καταγραφής (logfiles), που παράγονται από το σύστημα αυτό, με στόχο την ανακατασκευή του χρονικού της επίθεσης.

1.3 Δομή της διπλωματικής

Παρούσα διπλωματική εργασία, κινείται σε δύο άξονες. Στο πρώτο κομμάτι αναλύονται τα βασικά χαρακτηριστικά και ο τρόπος λειτουργίας του Event Viewer των Windows. Γίνεται μια σύντομη περιγραφή των επιμέρους λειτουργιών του, καθώς και των βασικών σημείων ελέγχου.

Στο δεύτερο κομμάτι, υπλοποιείται μία επίθεση από ένα τερματικό σε ένα άλλο, και γίνεται προσπάθεια να οπτικοποιηθεί το χρονικό της επίθεσης αυτής μέσω γραφικής παράστασης. Συγκεκριμένα, περιγράφεται και αναλύεται η μεθοδολογία και το μέσο με το οποίο πραγματοποιηείται η επίθεση και στη συνέχεια περιγράφεται η μεθοδολογία της γραφικής απεικόνισης της.

Τέλος, πραγματοποιείται η σύνοψη και η εξαγωγή των συμπερασμάτων.

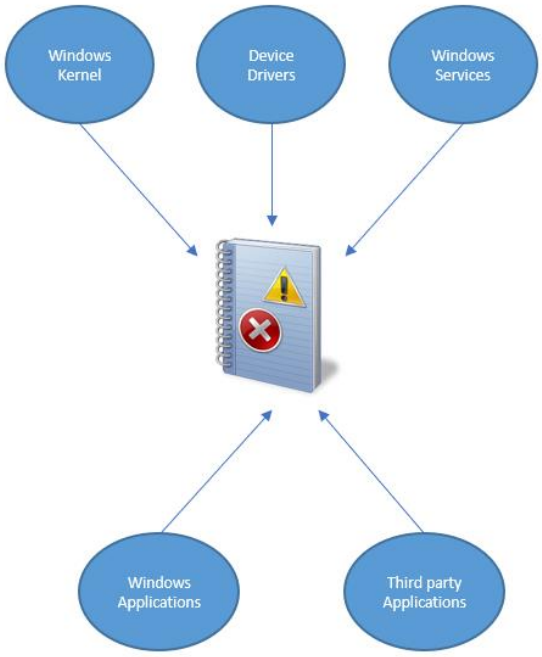
2

WINDOWS EVENT VIEWER

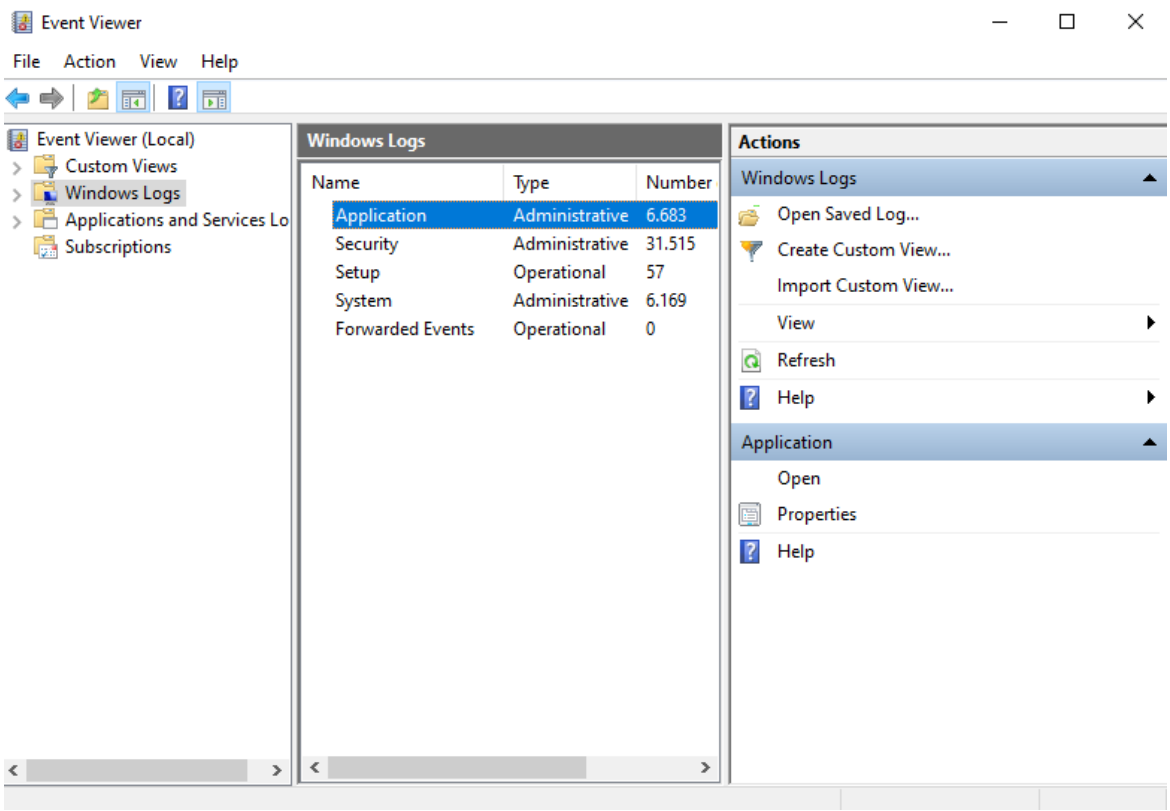
2.1 Εισαγωγή

Ο Event Viewer είναι μια εφαρμογή των Windows η οποία επιτρέπει στους διαχειριστές και τους χρήστες να προβάλλουν τα αρχεία καταγραφής συμβάντων αρχεία καταγραφής μηνυμάτων (logfiles) εφαρμογής (application) και συστήματος (system), συμπεριλαμβανομένων σφαλμάτων, μηνυμάτων πληροφοριών και προειδοποιήσεων. Οι εφαρμογές και τα επιμέρους στοιχεία του λειτουργικού συστήματος μπορούν να χρησιμοποιήσουν αυτήν την κεντρική υπηρεσία καταγραφής για να αναφέρουν συμβάντα που έχουν λάβει χώρα, όπως αποτυχία εκκίνησης ενός στοιχείου ή ολοκλήρωσης μιας ενέργειας. Συνοπτικά, πρόκειται για ένα εργαλείο που αποσκοπεί στην αντιμετώπιση διαφορετικών προβλημάτων κάθε είδους, τα οποία αφορούν το λειτουργικό σύστημα των Windows.

Αξίζει να σημειωθεί ότι ακόμη και ένα σύστημα που λειτουργεί σωστά θα εμφανίζει διάφορες προειδοποιήσεις και σφάλματα στα αρχεία καταγραφής του Event Viewer. Κακόβουλοι χρήστες ενδέχεται να χρησιμοποιήσουν ακόμη και αυτό το γεγονός σε ορισμένες περιπτώσεις για να εξαπατήσουν τους νόμιμους χρήστες και να πιστέψουν ότι το σύστημά τους έχει πρόβλημα. Κατά κανόνα, στην περίπτωση που ο υπολογιστής λειτουργεί σωστά, τα σφάλματα και οι προειδοποιήσεις που εμφανίζονται στον Event Viewer μπορούν να αγνοηθούν. Συνεπώς, απαιτούνται κάποιες βασικές γνώσεις πάνω στο συγκεκριμένο εργαλείο ώστε να μπορεί να φανεί πραγματικά χρήσιμο. Τα Windows παρέχουν αυτόν τον κεντρικό μηχανισμό καταγραφής που μπορούν να χρησιμοποιήσουν οι εφαρμογές και το λειτουργικό σύστημα για την αποθήκευση των συμβάντων τους. Ο Event Viewer, μπορεί να χρησιμοποιηθεί για την προβολή και την εξαγωγή αυτών των αρχείων καταγραφής. Ο Windows Event Viewer εισήχθη στα Windows NT και αποτελεί μέρος όλων των εκδόσεων των Windows από τότε και στο εξής.



Εικόνα 2:Architecture



Εικόνα 1:Event Viewer

Τα αρχεία καταγραφής συμβάντων των Windows περιέχουν συνήθως τις ακόλουθες πληροφορίες:

• Επίπεδο σοβαρότητας (Log level) – υποδεικνύει τη σοβαρότητα του καταγεγραμμένου συμβάντος. Παρακάτω συνοψίζοται τα επίπεδα σοβαρόητητας που είναι διαθέσιμα στα αρχεία καταγραφής συμβάντων των Windows:

Πίνακας 1: Log levels

Level	**Description**
Verbose	Detailed output of the event log entry
Information	Generally used by applications and operating system components to denote successful execution of an operation
Warning	Not an error, but a possible source of issues in future
Error	Failure of an operation. It may indicate the source of a problem in an operating system service, component or application.
Critical	The major issue that should be addressed immediately

Τα επίπεδα σοβαρότητας στο αρχείο καταγραφής συμβάντων αποφασίζονται ανάλογα με την επίπτωση που ενδέχεται να υπάρχει στο σύστημα. Τα επίπεδα "Verbose" και "Information" περιέχουν γενικά ενημερωτικά μηνύματα όπως η επιτυχής ολοκλήρωση εργασιών οι οποίες εκτελούνται στο παρασκήνιο. Τα επίπεδα, “Warning”, “Error”, “Critical” είναι βαθμοί κρισιμότητας και αναφέρονται σε περιπτώσεις σφάλματος και αποτυχίας.

Τα υπόλοιπα πεδία που καταγράφονται είναι τα ακόλουθα:
Το πεδίο “Date and Time” Αναφέρεται στο χρόνο της καγραφής ενός συμβάντος.
Η εφαρμογή ή η υπηρεσία που δημιούργησε το συμβάν μπορεί να περιλαμβάνει υπηρεσίες ή εφαρμογές του λειτουργικού συστήματος.
Αναγνωριστικό συμβάντος (Event ID): ένα μοναδικό αναγνωριστικό του συμβάντος που καταγράφεται. Το ίδιο αναγνωριστικό αναμένεται να χρησιμοποιείται σε όλες τις περιπτώσεις του συμβάντος που καταγράφεται.
Κατηγορία εργασιών (Task Category) – οι εφαρμογές που έχουν δημιουργήσει το συμβάν, μπορούν να κατηγοριοποιήσουν περαιτέρω το συμβάν δίνοντας στο συμβάν έναν αριθμό και μια ετικέτα. Αυτό το πεδίο βοηθά τους χρήστες του Windows Event Viewer να φιλτράρουν συμβάντα.

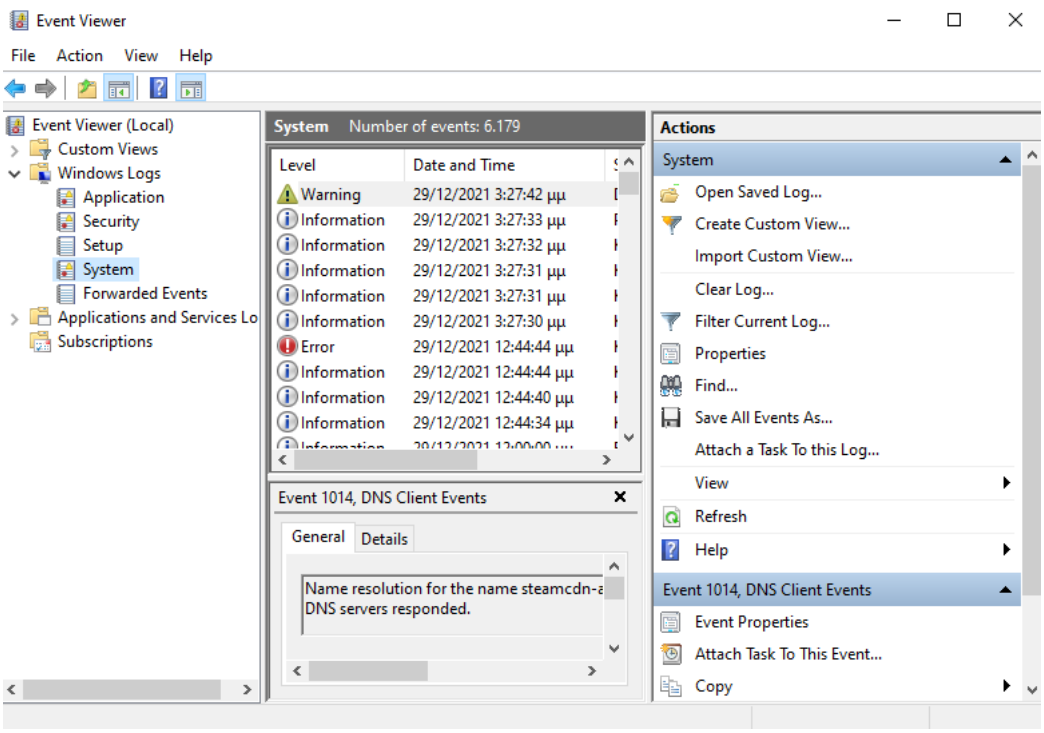
2.2 Κατηγορίες Συμβάντων

Τα συμβάντα κατηγοριοποιούνται από το πρόγραμμα σε διαφορετικές κατηγορίες, καθεμία από τις οποίες σχετίζεται με ένα αρχείο καταγραφής(logfile) που διατηρεί συμβάντα σχετικά με αυτήν την κατηγορία. Αν και υπάρχουν πολλές κατηγορίες, ο κυριότερος όγκος προβλημάτων που πιθανότατα χρίζουν αντιμετώπισης, αφορά τρεις από αυτές:

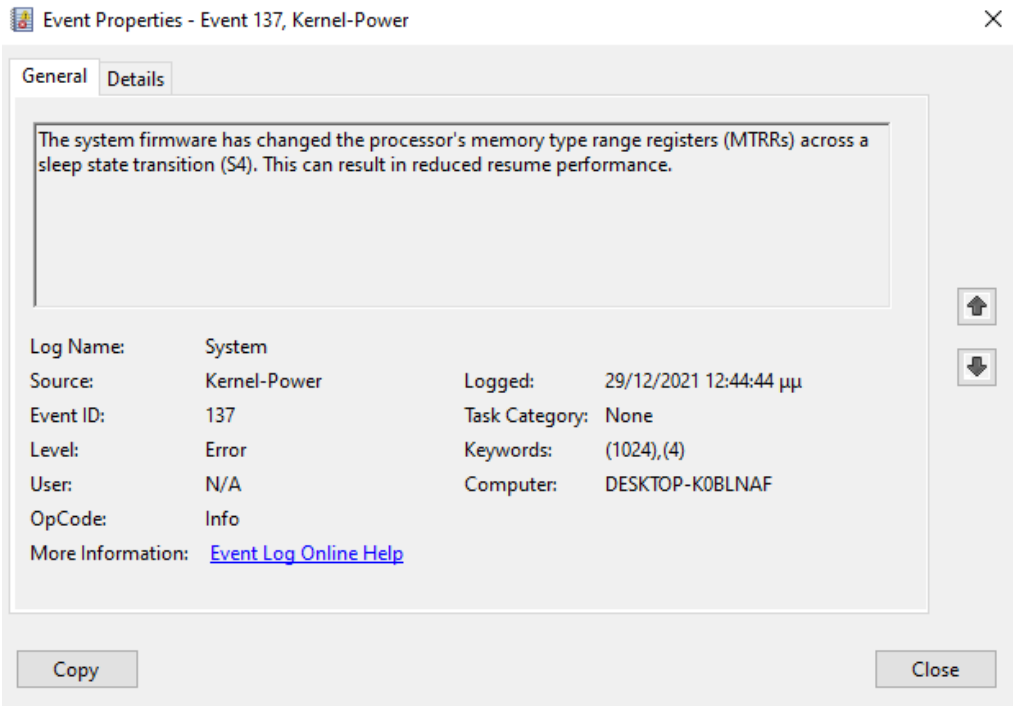
Εφαρμογή (Application): Το αρχείο καταγραφής εφαρμογής καταγράφει συμβάντα που σχετίζονται με στοιχεία του συστήματος των Windows, όπως προγράμματα οδήγησης και ενσωματωμένα στοιχεία διεπαφής.

Σύστημα (System): Το αρχείο καταγραφής συστήματος καταγράφει συμβάντα που σχετίζονται με προγράμματα που είναι εγκατεστημένα στο σύστημα.

Ασφάλεια (Security): Όταν η καταγραφή ασφαλείας είναι ενεργοποιημένη , αυτό το αρχείο καταγραφής καταγράφει συμβάντα που σχετίζονται με την ασφάλεια, όπως προσπάθειες σύνδεσης και πρόσβαση σε πόρους.



Εικόνα 3:System



Εικόνα 4:Event properties

2.3 Τα αρχεία καταγραφής συμβάντων των Windows και οι χρήσεις τους στα Digital Forensics:

Τα αρχεία καταγραφής συμβάντων των Windows περιέχουν αρχεία καταγραφής που δημιουργούνται από συμβάντα σε εφαρμογές και στο λειτουργικό σύστημα εν γένει. Αυτές οι εγγραφές στην εφαρμογή, μπορούν να συσχετιστούν με ενέργειες χρήστη, όπως συνδέσεις χρηστών, εφαρμογές που χρησιμοποιούνται σε διάφορα χρονικά σημεία, χρονικές περιόδους κατά τις οποίες το σύστημα ήταν σε χρήση κ.α.
Θα πρέπει να σημειωθεί ότι τα αρχεία καταγραφής συμβάντων των Windows δεν περιέχουν λεπτομέρειες των ενεργειών που εκτελούνται από τον χρήστη σε εφαρμογές. Για παράδειγμα, οι εφαρμογές συνήθως δεν αποθηκεύουν συμβάντα, όπως την τελευταία φορά που ο χρήστης είχε πρόσβαση σε ένα συγκεκριμένο μενού ή μία εφαρμογή. Για την καταγραφή τέτοιων ενεργειών, οι εφαρμογές διατηρούν ξεχωριστά αρχεία καταγραφής και αυτά δεν συνδέονται με αρχεία καταγραφής συμβάντων των Windows.
Τα αρχεία καταγραφής συμβάντων των Windows περιέχουν συνήθως συμβάντα εφαρμογών ή λειτουργικού συστήματος χαμηλού επιπέδου. Μερικά από τα πιο συχνά παραδείγματα συμβάντων που καταγράφονται από το λειτουργικό σύστημα είναι τα παρακάτω:

- Είσοδος χρήστη
- Αποσύνδεση χρήστη
- Διακοπή εφαρμογής
- Εγκατάσταση εφαρμογών
- Εγκατάσταση υλικού

Όπως αναφέρθηκε και παραπάνω, οι εγγραφές του αρχείου καταγραφής συμβάντων δεν περιέχουν αρχεία καταγραφής σχετικά με συγκεκριμένες ενέργειες των χρηστών σε επίπεδο εφαρμογών. Ωστόσο, κάποιος ερευνητής, θα πρέπει να προσπαθήσει να συσχετίσει τις ενέργειες που εκτελούνται από τους χρήστες του συστήματος, με τις αντίστοιχες καταχωρίσεις του Event Viewer των Windows. Σε ορισμένες περιπτώσεις, όταν δεν υπάρχουν καταγραφές για χρήση συγκεκριμένων εφαρμογών ή τα δεδομένα που υπάρχουν δεν επαρκούν, καταχωρήσεις αρχείου καταγραφής συμβάντων του Event Viewer, όπως ο χρόνος σύνδεσης του χρήστη, η έναρξη μιας υπηρεσίας κλπ, μπορούν να βοηθήσουν έναν ερευνητή να τεκμηριώσει τα ευρήματά του και να παγιώσει το πορισμά του σχετικά με το συμβάν που εξετάζει. Τα αρχεία καταγραφής συμβάντων των Windows βοηθούν πολύ στη συσχέτιση ενεργειών που εκτελούνται από τον χρήστη σε εφαρμογές και υπηρεσίες, σε επίπεδο λειτουργικού συστήματος όπως οι χρόνοι σύνδεσης και αποσύνδεσης ή η έναρξη και ο τερματισμός υπηρεσιών.

3

ΣΧΕΔΙΑΣΜΟΣ ΚΑΙ ΥΛΟΠΟΙΗΣΗ ΚΑΚΟΒΟΥΛΗΣ ΕΝΕΡΓΕΙΑΣ

3.1 Συστήματα που χρησιμοποιήθηκαν

Για της ανάγκες του σεναρίου χρησιμοποιήθηκαν τα παρακάτω:

- Το λογισμικό VirtualBox το οποίο φιλοξένησε τα vms που χρησιμοποιήθηκαν στο σενάριο
- VM με λειτουργικό σύστημα Kali Linux 2019.1, από το οποίο πραγματοποιήθηκε η κακόβουλη ενέργεια
- VM με λειτουργικό σύστημα Windows XP SP1, το οποίο χρησιμοποιήθηκε ως "στόχος"
- VM με λειτουργικό σύστημα Windows 10, το οποίο χρησιμοποιήθηκε ως "στόχος"

Η αρχιτεκτονική του συστήματος ήταν η εξής: Τα δύο VMs ήταν συνδεδεμένα στο ίδιο δίκτυο με bridged connection και οι IP που απέκτησαν ήταν οι παρακάτω:

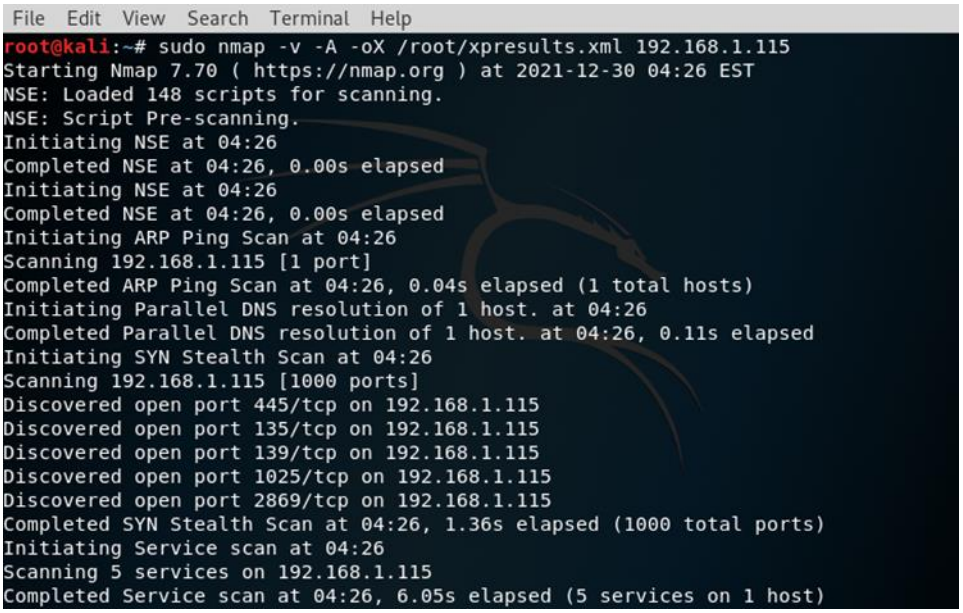
VM	IP
Kali Linux 2019.1	192.168.1.15
Windows XP SP1	192.168.1.115
Windows 10	192.168.1.25

3.2 Μεθοδολογία επίθεσης

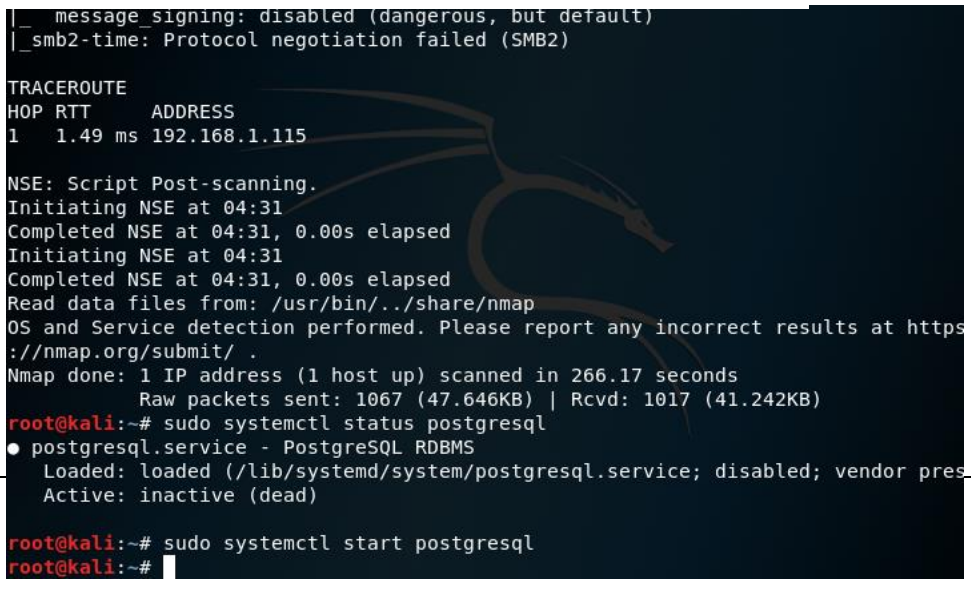
Η μέθοδολογία που αποφασίστηκε να χρησιμοποιηθεί για της ανάγκες της διπλωματικής διατριβής, στο κομμάτι της πραγματοποίησης της κακόβουλης ενέργειας είναι η λεγόμενη Reverse_tcp. Το πρωτόκολλο TCP/IP ή Transmission Control Protocol/Internet Protocol είναι η πρωτόκολλο επικοινωνίας του Διαδικτύου. Το TCP/IP χρησιμοποιείται για να επιτρέπει σε έναν υπολογιστή να επικοινωνεί με έναν άλλο υπολογιστή μέσω Διαδικτύου, με τη μεταγλώττιση πακέτων δεδομένων και αποστολή τους στο σωστό αποδέκτη. Ένα τείχος προστασίας λειτουργεί συνήθως για τον αποκλεισμό τέτοιου είδους εισερχόμενων συνδέσε ων. Ένα Reverse_tcp είναι όταν ο εισβολέας κάνει τον κεντρικό υπολογιστή να ξεκινήσει τη σύνδεση με τον εισβολέα. Συνοπτικά, η παραπάνω είναι η βασική ιδέα ενός reverse tcp.

3.2.1 Κακόβουλη επίθεση σε Windows XP

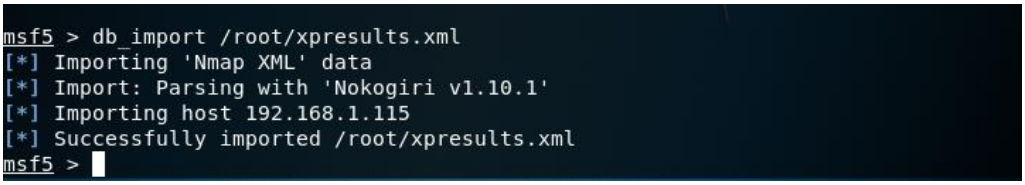
Παρακάτω παρατείθενται εικόνες από την επίθεση που πραγματοποιήθηκε στο μηχάνημα-στόχο με λειτουργικό σύστημα Windows XP.



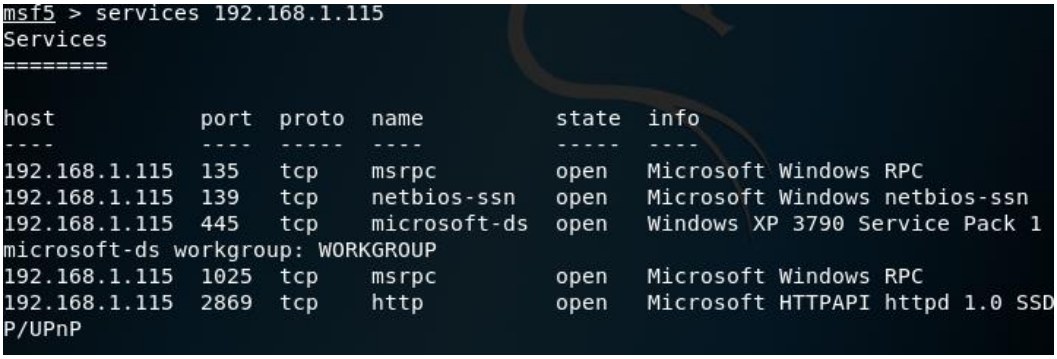
Εικόνα 5:nmap



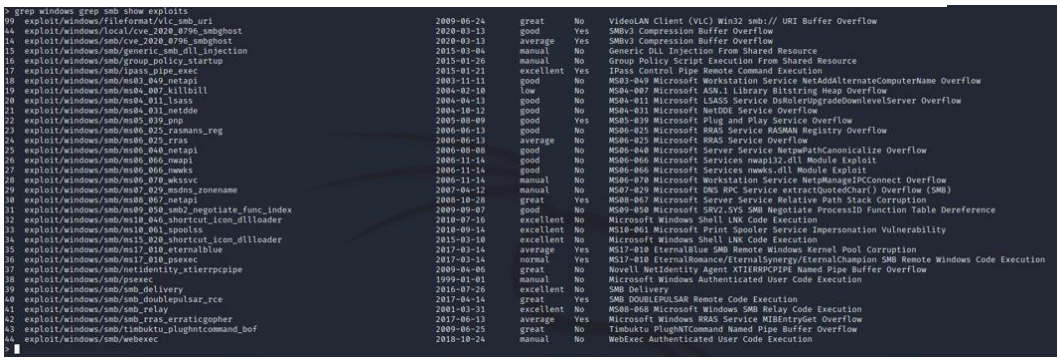
Εικόνα 7:Postgresql



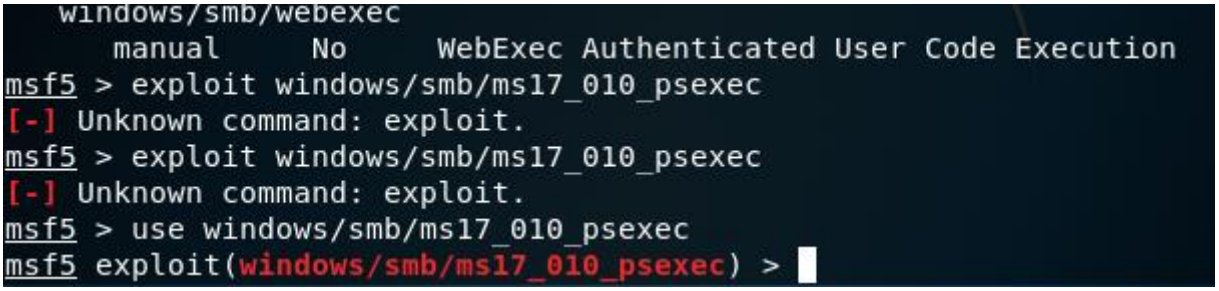
Εικόνα 8:db import



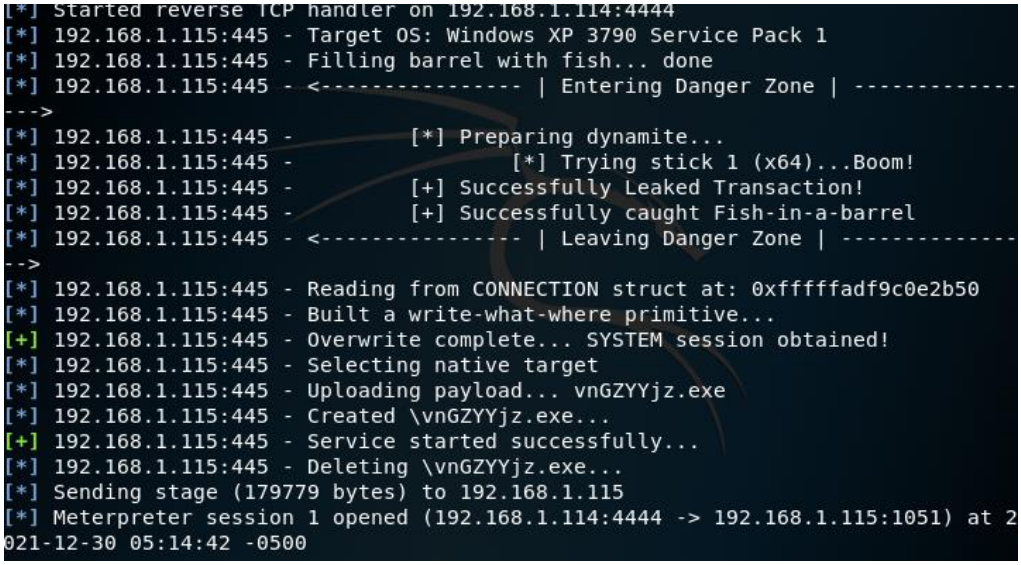
Εικόνα 11:Services



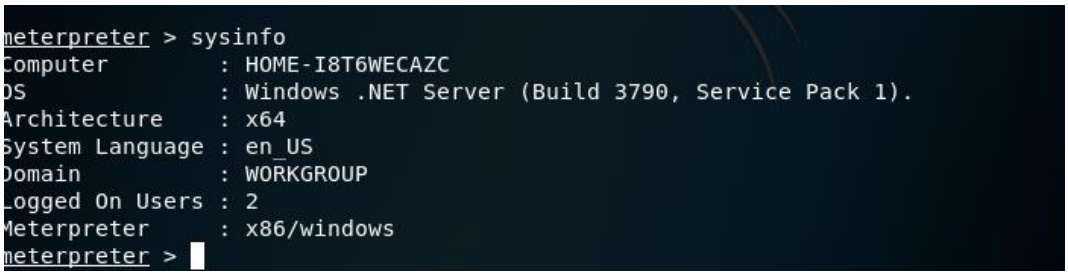
Εικόνα 10:Exploits



Εικόνα 9:Psexec



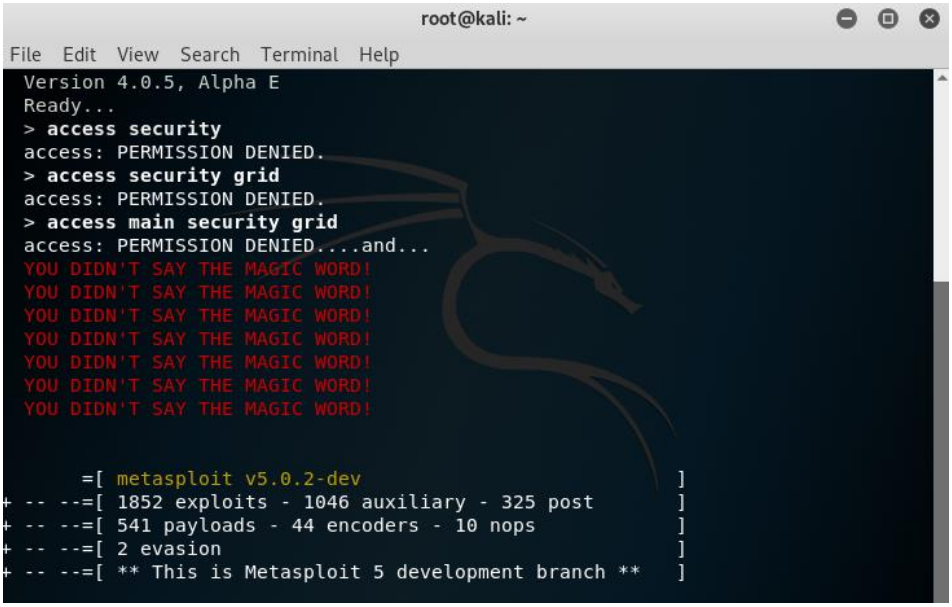
Εικόνα 12:Remote Session



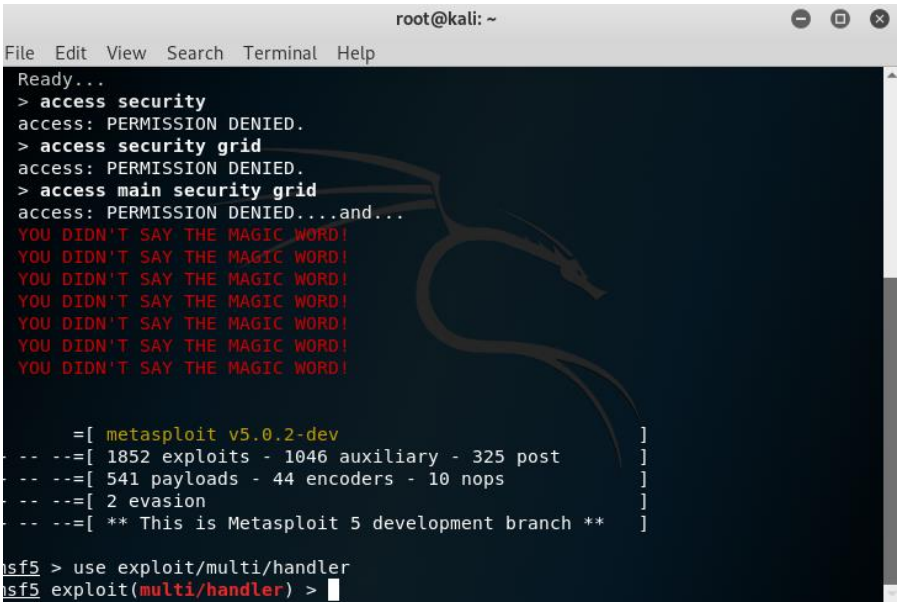
Εικόνα 13:Sysinfo

3.2.2 Κακόβουλη ενέργεια σε Windows 10

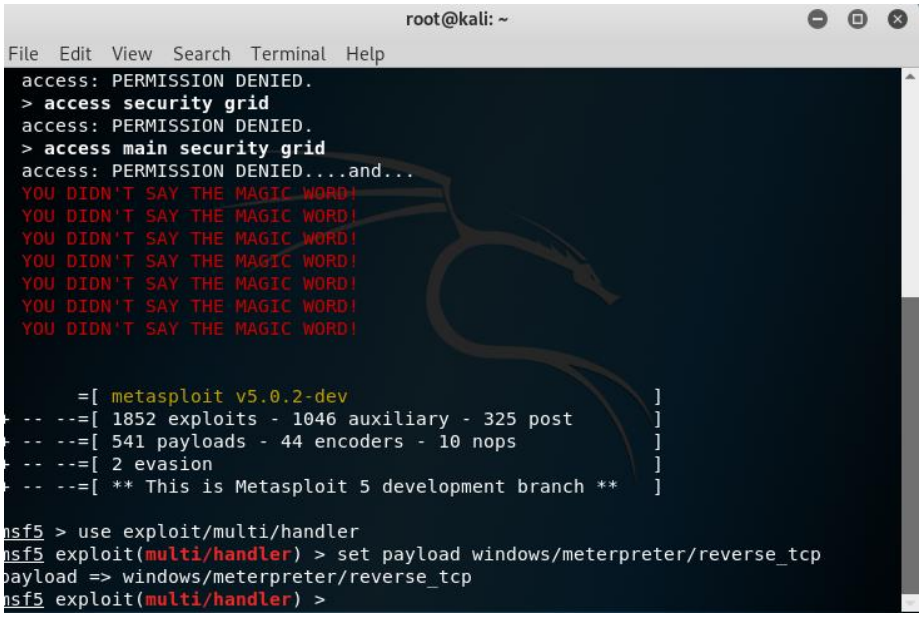
Παρακάτω παρατείθενται εικόνες από την επίθεση που πραγματοποιήθηκε στο μηχάνημα-στόχο με λειτουργικό σύστημα Windows XP.



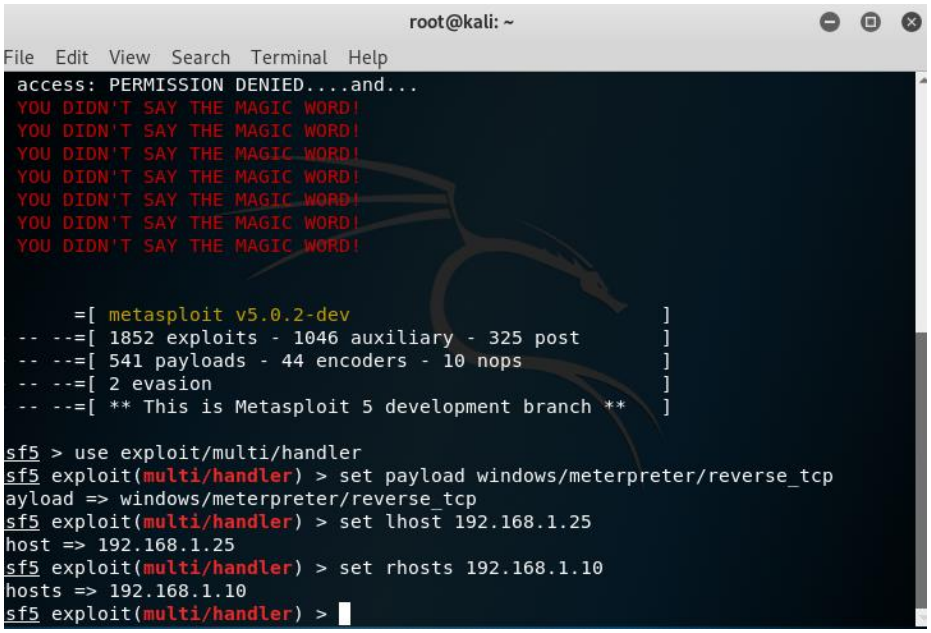
Εικόνα 14:win10_msfconsole



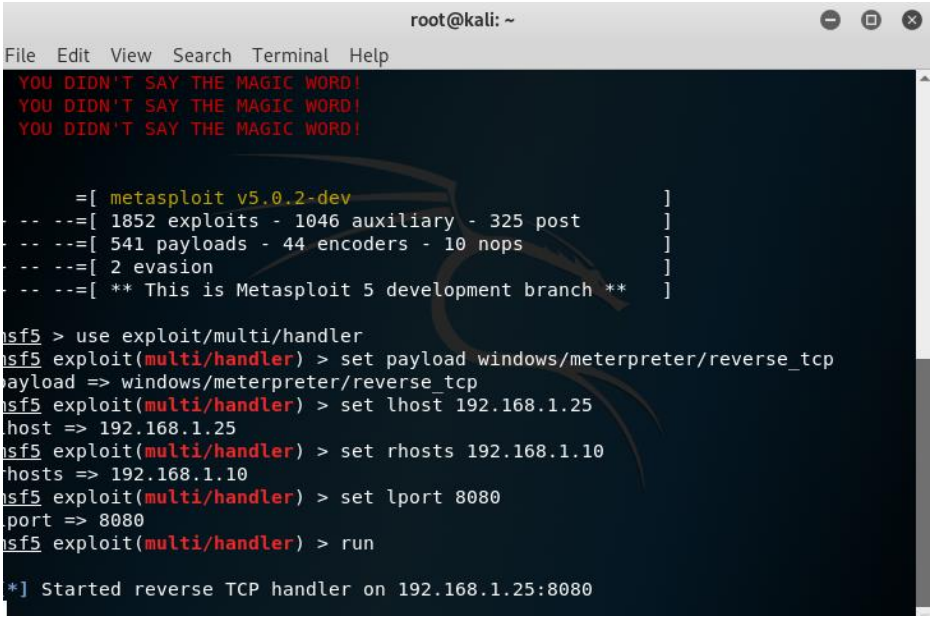
Εικόνα 15:win10_exploit



Εικόνα 16:win10_payload



Εικόνα 17: win10_hosts



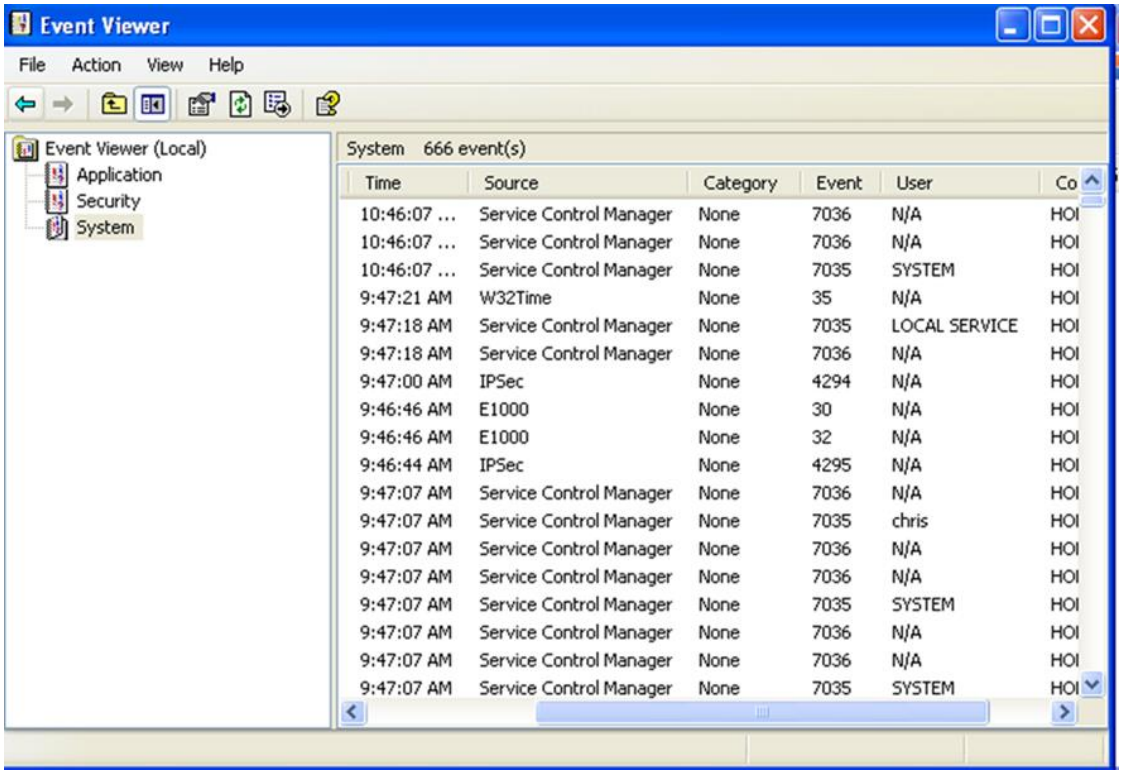
Εικόνα 18:win10_run_exploit

Σε αυτό το σημείο αξίζει να σημειωθεί ότι η επίθεση αυτή εν τέλει απετράπη από τους μηχανισμούς των windows. Συνεπώς, το μηχάνημα-στόχος σε αυτή την περίπτωση δεν επιρρεάστηκε από τον κακόβουλο χρήστη. Στο παρακάτω κεφάλαιο θα αξιολογηθούν τα συμπεράσματα που μπορούν να εξαχθούν από τις εγγραφές του Event Viewer σαε αυτή την περίπτωση.

3.3 EVENT VIEWER LOGS

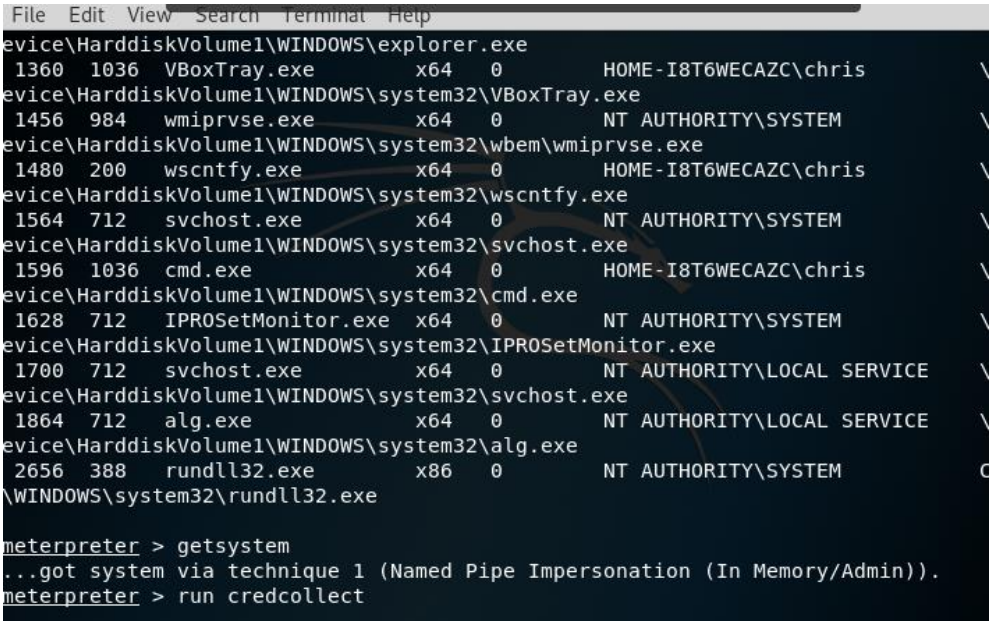
3.3.1 Event logs Windows XP

Ανοίγοντας τον Event Viewer των Windows XP φαίνεται ότι την ώρα της επίθεσης, δημιουργούνται κάποια events στην κατηγορία system. Τα event IDs είναι τα 7035 και 7036.

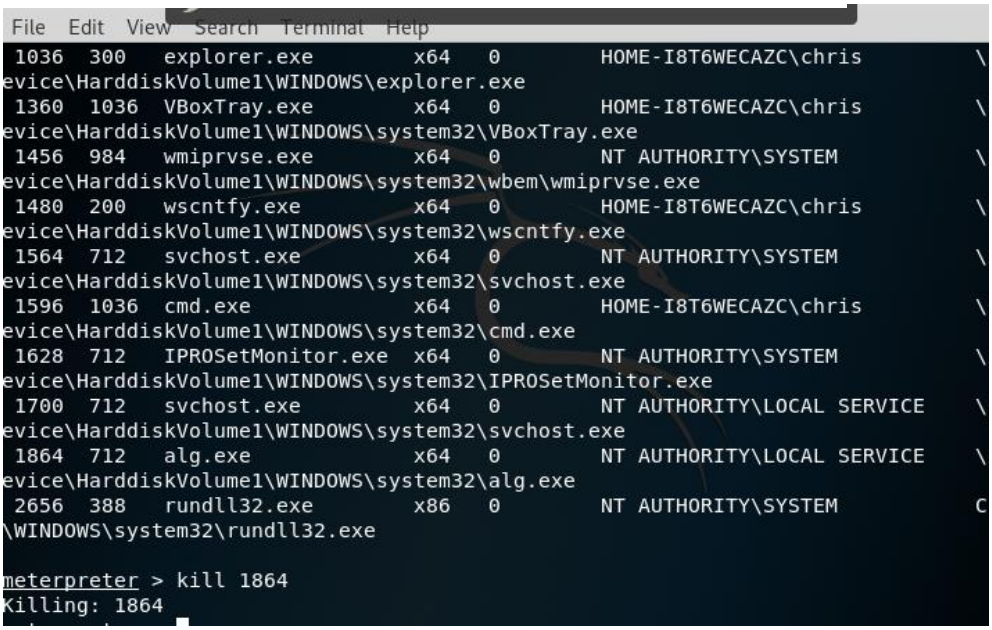


Εικόνα 19:Event Viewer Logs

Όπως φαίνεται παρακάτω έπειτα από την πραγματοποίηση της επίθεσης, ο επιτειθέμενος αφού απέκτησε πρόσβαση στο μηχάνημα-στόχο, προσπάθησε να εκτελέσει απομακρυσμένα εντολές στο μηχάνημα. Κάποιες από τις εντολές αυτές εκτελέστηκαν με επιτυχία στο μηχάνημα-στόχο και κάποιες απέτυχαν, με αποτέλεσμα να υπάρξουν νέες εγγραφές στον Event Viewer όπως θα αναλυθεί αργότερα.

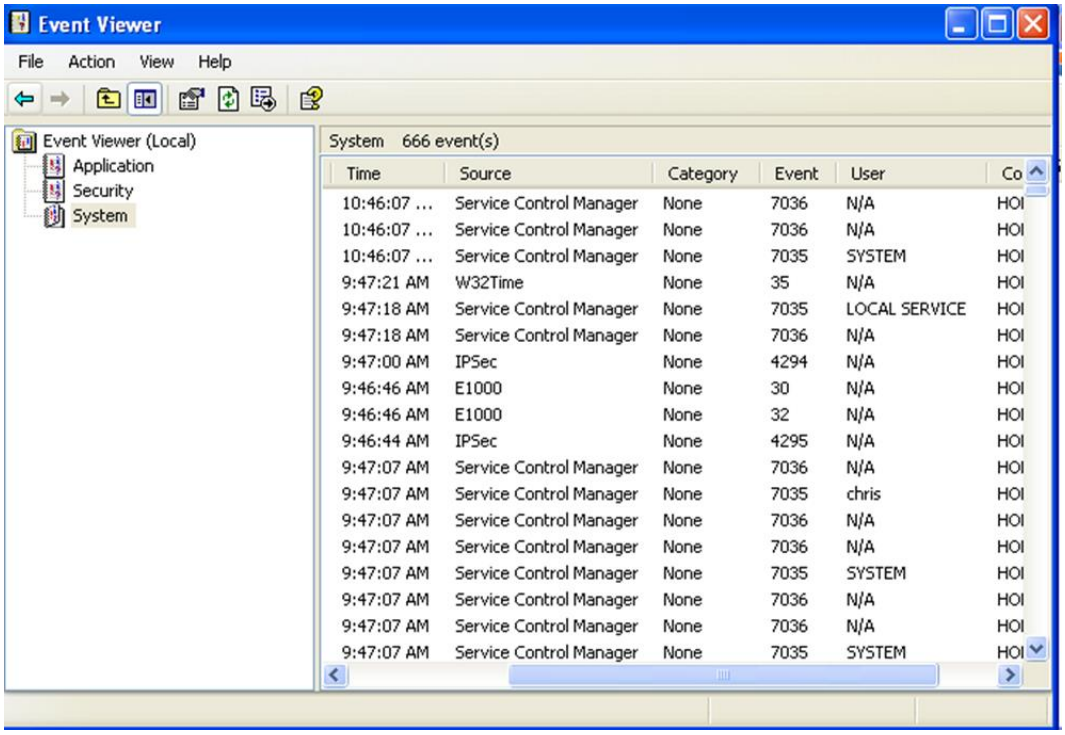


Εικόνα 20:Getsystem

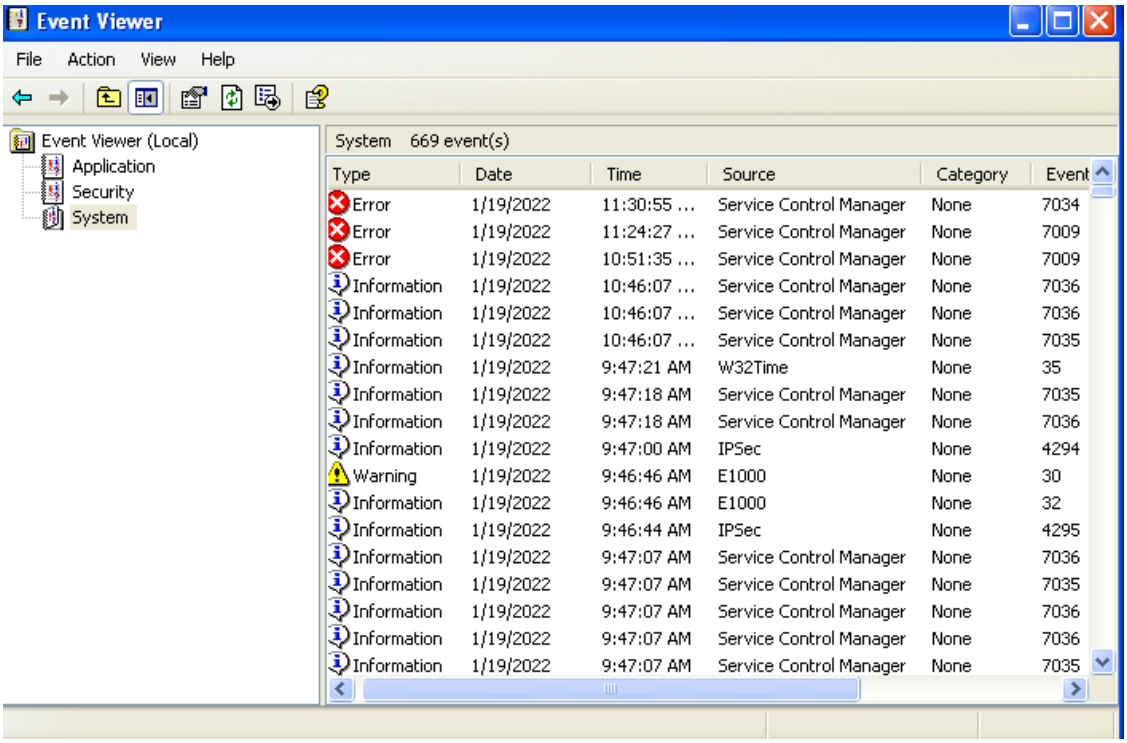


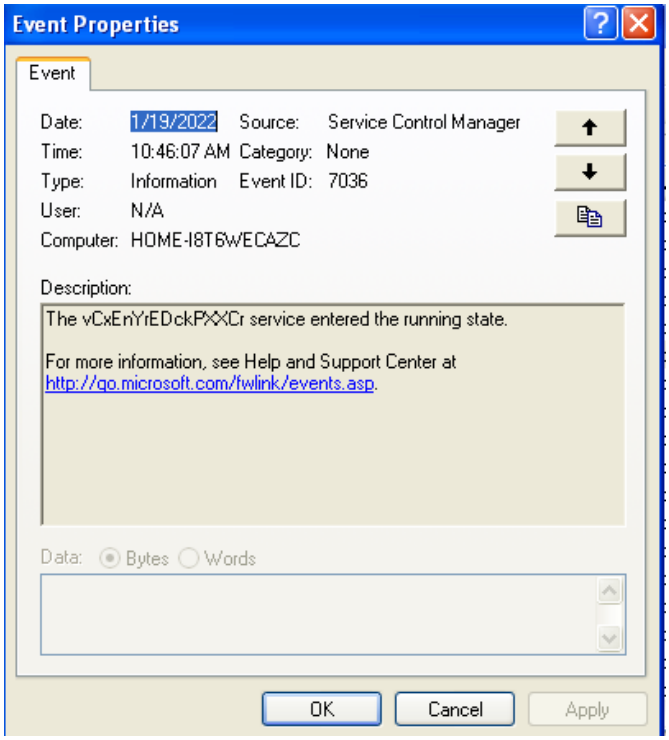
Εικόνα 21:Kill

Ανοίγοντας εκ νέου τον Event Viewer των Windows φαίνεται ότι την ώρα της επίθεσης, δημιουργούνται κάποια ακόμη events στην κατηγορία system. Τα νέα Event Ids στην περίπτωση αυτή είναι τα 7009 και 7034.

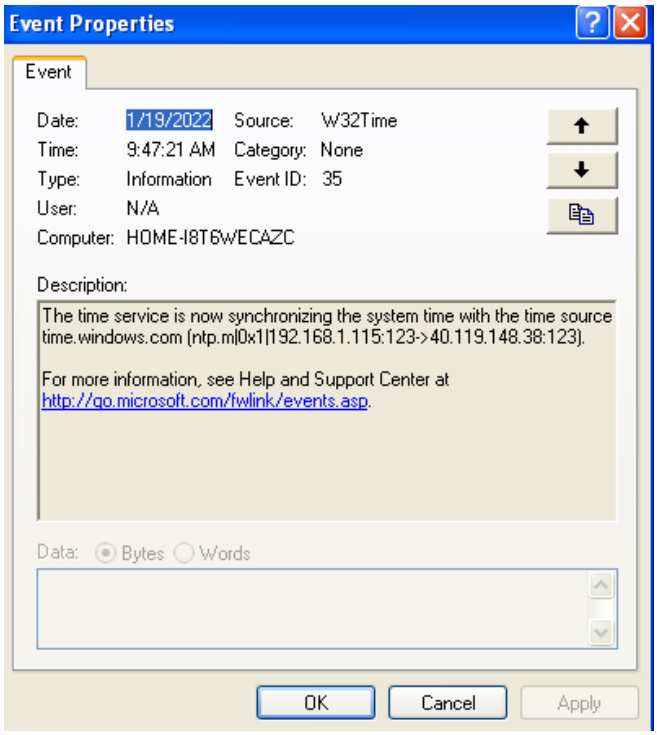


Εικόνα 22:Sysyem Logs

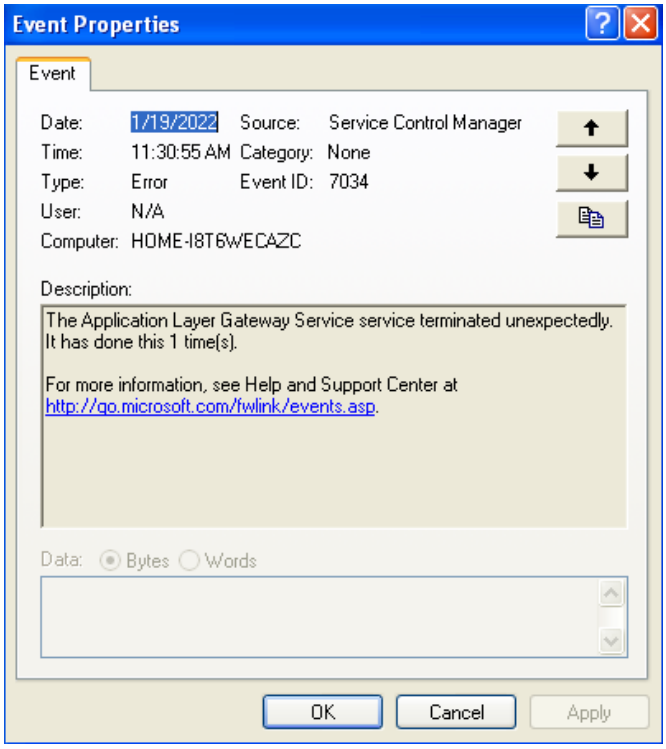




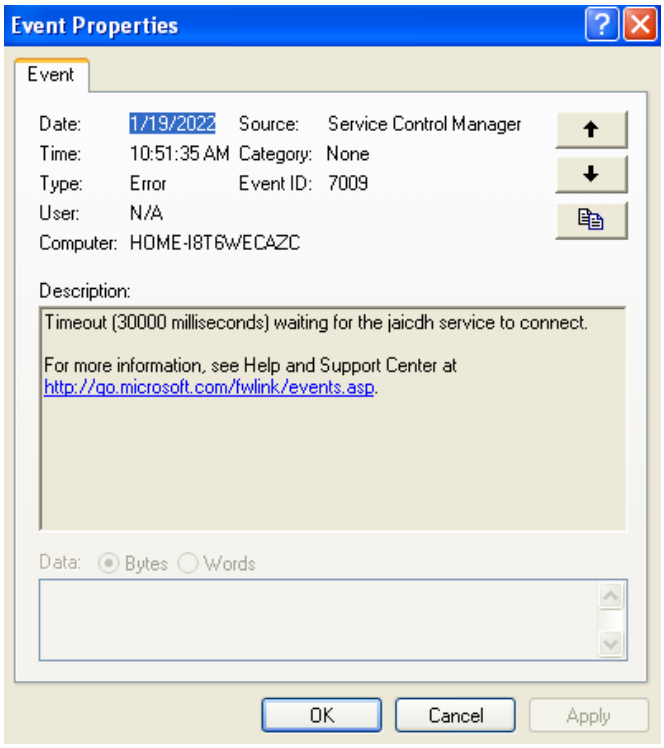
Εικόνα 23: Event 7036



Εικόνα 24:Event 35



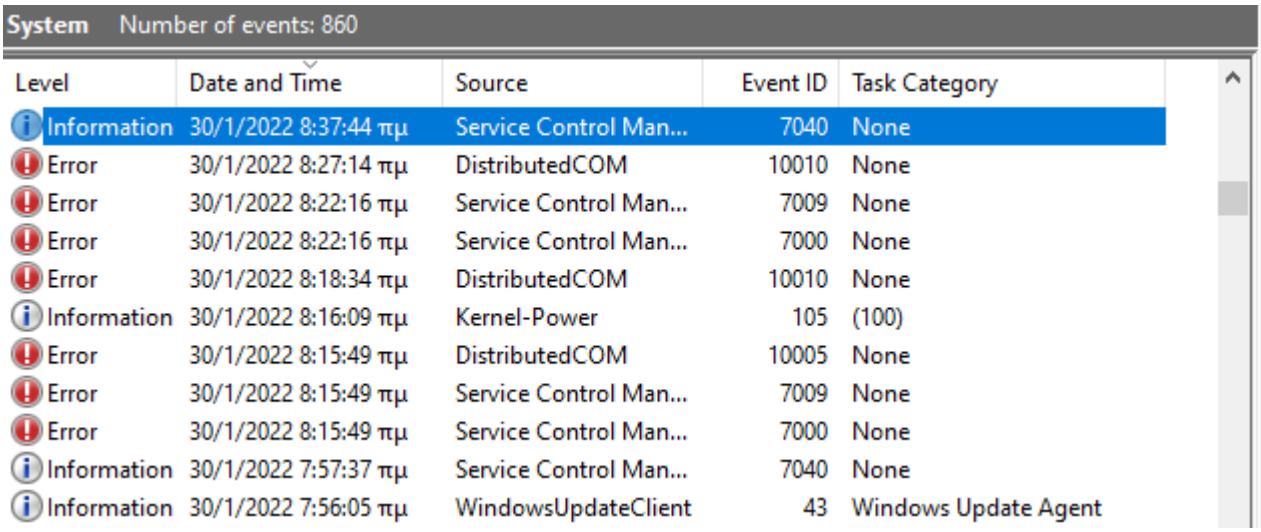
Εικόνα 25:Event 7034



Εικόνα 26:Event 7009

3.3.2 Event logs Windows 10

Ανοίγοντας τον Event Viewer των Windows 10, φαίνεται ότι την ώρα της επίθεσης, δημιουργούνται κάποια events στην κατηγορία system. Όπως φαίνεται στον παρακάτω πίνακα, τα IDs των εγγραφών που δημιουργούνται είναι τα εξής: 7040, 10010, 7009,7000, 105



System Number of events: 860

Level	Date and Time	Source	Event ID	Task Category
Information	30/1/2022 8:37:44 πμ	Service Control Man...	7040	None
Error	30/1/2022 8:27:14 πμ	DistributedCOM	10010	None
Error	30/1/2022 8:22:16 πμ	Service Control Man...	7009	None
Error	30/1/2022 8:22:16 πμ	Service Control Man...	7000	None
Error	30/1/2022 8:18:34 πμ	DistributedCOM	10010	None
Information	30/1/2022 8:16:09 πμ	Kernel-Power	105	(100)
Error	30/1/2022 8:15:49 πμ	DistributedCOM	10005	None
Error	30/1/2022 8:15:49 πμ	Service Control Man...	7009	None
Error	30/1/2022 8:15:49 πμ	Service Control Man...	7000	None
Information	30/1/2022 7:57:37 πμ	Service Control Man...	7040	None
Information	30/1/2022 7:56:05 πμ	WindowsUpdateClient	43	Windows Update Agent

Εικόνα 27:win10_event_logs

4

4

ΑΝΑΚΑΤΑΣΚΕΥΗ ΚΑΚΟΒΟΥΛΗΣ ΕΝΕΡΓΕΙΑΣ

Η ανακατασκευή του χρονικού της κακόβουλης ενέργειας, αποφασίστηκε να γίνει αποτυπώνοντας τα Events που προκύπτουν από τον event viewer σε γραφική παράσταση.

4.1 PYTHON και Βιβλιοθήκες

Η ανακατασκευή του χρονικού της κακόβουλης ενέργειας, αποφασίστηκε να γίνει χρησιμοποιώντας τη γλώσσα Python και συγκεκριμένα τη βιβλιοθήκη Pandas. Η βιβλιοθήκη Pandas είναι το ένα εργαλείο το οποίο χρησιμοποιείται για την πραγματοποίηση ανάλυσης δεδομένων στην Python. Επιπλέον, είναι ένα από τα ισχυρότερα και πιο ευέλικτα εργαλεία ανάλυσης / χειρισμού δεδομένων ανοιχτού κώδικα διαθέσιμο σε οποιαδήποτε γλώσσα.

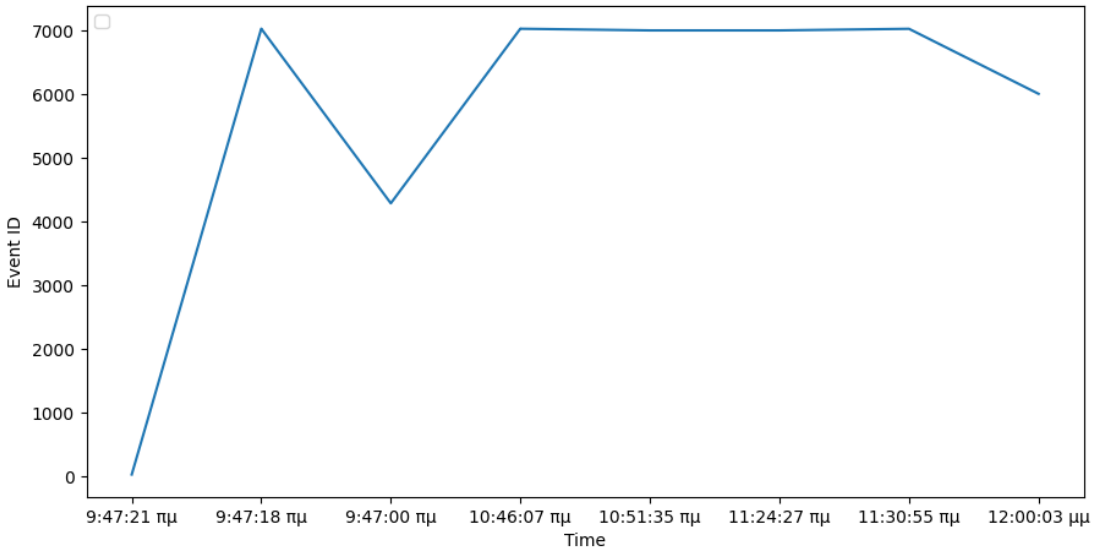
4.2 ΜΕΘΟΔΟΛΟΓΙΑ

Έχοντας αποθηκεύσει όλα τα αποτελέσματα του event viewer στο αρχείο xpresults.xml στο οποίο καταγράφονται όλες οι εγγραφές, οι στήλες που ενδιαφέρουν, μπορούν να αποθηκευθούν σε ένα αρχείο xlsx.

Οι 2 διαστάσεις που επιλέθηκαν να χρησιμοποιηθούν είναι το Time και το Event ID, τα οποία αντιπροσωπεύουν το χρόνο της εγγραφής και το ID του κάθε event, αντίστοιχα. Τα γραφήματα που προκύπτουν έπειτα από την εκτέλεση του κώδικα Python για κάθε μία από τις δύο περιπτώσεις κακόβουλων ενεργειών είναι τα παρακάτω:

4.3 ΑΝΑΛΥΣΗ ΓΡΑΦΗΜΑΤΟΣ

4.3.1 Ανάλυση γραφήματος μηχανήματος Windows XP

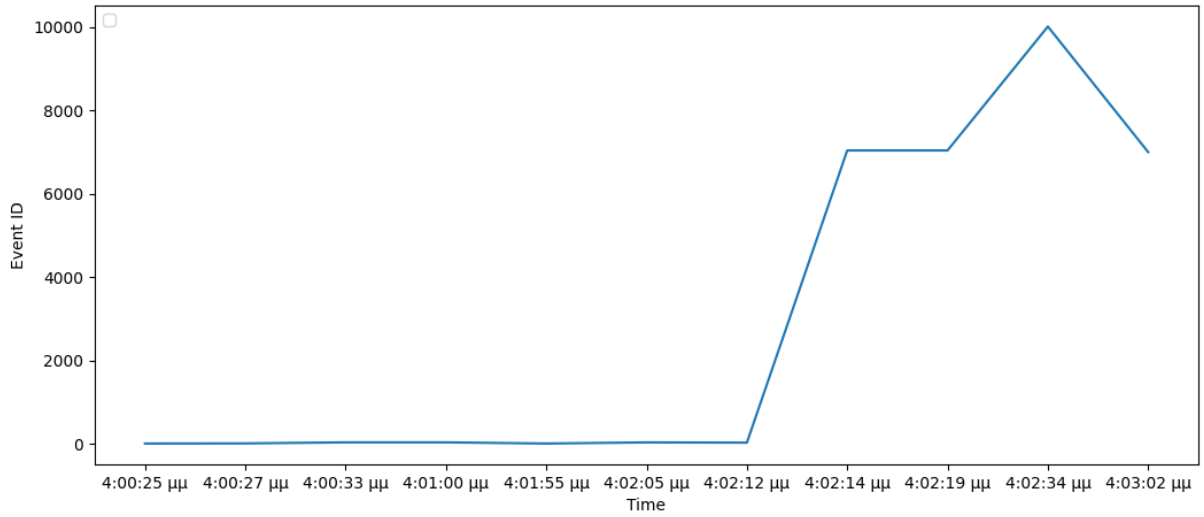


Εικόνα 29:Windows XP graph

Time	9:47:21 πμ	9:47:18 πμ	9:47:18 πμ	9:47:00 πμ	10:46:07 πμ	10:46:07 πμ	10:46:07 πμ	10:51:35 πμ	11:24:27 πμ	11:30:55 πμ	12:00:03 μμ
EventID	35	7035	7036	4294	7036	7036	7035	7009	7009	7034	6013

Αρχικά παρατηρείται ότι την ώρα που το μηχάνημα-στόχος ενεργοποιείται ο Event viewer καταγράφει ID 7035 και 7036.
Event ID: 7036 (The service state has changed)
Την ώρα της κακόβουλης ενέρχειας, που τρέχει η απομακρυσμένη πρόσβαση και ο κακόβουλος χρήστης έχει πάρει πρόσβαση στο μηχάνημα-στόχο, εμφανίζονται ξανά τα ID 7035, 7036. Βλέπουμε επίσης ότι η υπηρεσία "PSEXESVC" μπαίνει σε status "Executing" κατα τή διάρκεια της εκτέλεσης μιας απομακρυσμένης διαδικασίας και στη συνέχεια σε status "Stopped" μετά την εκτέλεση.
Έπειτα και όσο ο επιτηθέμενος πραγματοποιεί απομακρυσμένες εντολές ο Event viewer καταγράφει “errors” με IDs 7009, 7034.
Event ID: 7009 (Service Error - Timeout)
Event ID: 7034 (Service Terminated)

4.3.2 Ανάλυση γραφήματος μηχανήματος Windows 10



Εικόνα 30:Windows 10 graph

4:00:25 μμ	4:00:27 μμ	4:00:33 μμ	4:01:00 μμ	4:01:55 μμ	4:02:05 μμ	4:02:12 μμ	4:02:14 μμ	4:02:19 μμ	4:02:34 μμ	4:03:02 μμ
16	19	44	44	16	43	37	7040	7040	10010	7000

Τα Event IDs που καταγράφονται την ώρα της προσπάθειας επίθεσης στο μηχάνημα-στόχο, είναι τα Παρακάτω:

Event ID: 16 When Automatic Updates tries to download updates, the download doesn't succeed, and Event ID 16 is recorded in the system log

Event ID: 19 Windows successfully installed the update

Event ID: 44 Remote users cannot log on to a Windows Server 2012-based Remote Desktop Session Host (RD Session Host) server

Event ID: 43 This event is logged when the time provider returned an error when notified of a network configuration change

Event ID: 7040 Remote users cannot log on to a Windows Server 2012-based Remote Desktop Session Host (RD Session Host) server

Event ID: 10010 This event is logged when the server did not register with DCOM within the required time-out period

Event ID: 7000 The service did not start due to a logon failure.

5

ΕΠΙΛΟΓΟΣ -

ΣΥΜΠΕΡΑΣΜΑΤΑ

5.1 Συμπεράσματα κακόβουλης επίθεσης σε Windows XP

Καθώς είναι προφανές ότι πολλα τερματικά έχουν υποστεί ζημιές λόγω στοχευμένων επιθέσεων, η σημασία των ερευνών πάνω στα συμβάντα αυτά για την περαιτέρω εξέταση τέτοιων ζημιών αυξάνεται. Στα πλαίσια της παρούσας διπλωματικής εργασίας συνοψίζονται και παρουσιάζονται στοιχεία που συσχετίζουν την εκτέλεση εντολών με πιθανές κακόβουλες ενέργειες. Με μία πρώτη ματιά, πολλά εργαλεία/ εντολές δεν αφήνουν αποδείξεις ότι δεν έχουν εκτελεστεί με κακόβουλο σκοπό, κάτι που μπορεί να έχει ως αποτέλεσμα να παραμείνουν άλυτες οι έρευνες συμβάντων. Για να αναλυθεί λεπτομερώς τι έκανε κάποιος πιθανός εισβολέας, πρέπει να προετοιμαστεί εκ των προτέρων ένα περιβάλλον που επιτρέπει την συλλογή αρχείων καταγραφής και την οπτικοποίηση τους.
Η κατ'επανάληψη πραγματοποίηση του πειράματος με πιθανή κακόβουλη δραστηριότητα οδήγησαν στο εξής συμπέρασμα. Βασικό χαρακτηριστικό είναι αφενός η δημιουργία των ίδιων Event IDs κάθε φορά που ένας κακόβουλος χρήστης αποκτά απομακρυσμένη πρόσβαση στο μηχάνημα-στόχο. Επίσης δημιουργούνται συγκεκριμένα IDs, όπως φαίνεται στον παρακάτω πίνακα τα οποία μπορούν να υποδηλώσουν την ύπαρξη κακόβουλης δραστηριότητας, λόγω των μη αναμενόμενων υπηρεσιών που δημιουργούνται και τερματζίζονται. Ο συνδυασμός των παραπάνω σε συνδυασμό με την περαιτέρω ανάλυση των logfiles του Event Viewer μπορεί να οδηγήσει κάποιον αναλυτή σε ένα ασφαλές συμπέρασμα οτι έχει πραγματοποιηθεί παραβίαση στο σύστημα και να προβεί στις ανάλογες ενέργειες.

Πίνακας 2: Windows XP Event IDs Explanations

Event ID	**Explanation**
7035	The service was successfully sent a start control
7036	The service state has changed
7009	Service Error - Timeout
7034	Service Terminated

5.2 Συμπεράσματα κακόβουλης επίθεσης σε Windows 10

Στην περίπτωση της αποτυχημένης επίθεσης στο μηχάνημα το οποίο διέθεται λειτουργικό σύστημα Windows 10, παρατηρείται μια πιο λεπτομερής και ξεκάθαρη περιγραφή των events που καταγράφει ο Event Viewer. Τα IDs που έχουν ενδιαφέρον εδώ είναι τα 7040, 10010 και 7000. Μετα από διερεύνηση των παρακάτω IDs, μπορούμε να οδηγηθούμε στην υπόθεση οτι κάποιος κακόβουλος χρήστης προσπάθησε να αποκτήσει απομακρυσμένο έλεγχο στο μηχάνημα, αλλα εν τέλει δεν κατάφερε να πετύχει η επίθεσή του Ο συνδυασμός των παραπάνω events σε συνδυασμό με την περαιτέρω ανάλυση των logfiles του Event Viewer μπορεί να οδηγήσει κάποιον αναλυτή σε ένα ασφαλές συμπέρασμα οτι έχει πραγματοποιηθεί παραβίαση στο σύστημα και να προβεί στις ανάλογες ενέργειες. Το σημαντικό σε αυτή την περίπτωση, σε σχέση με το μηχάνημα που διέθεται λειτουργικό σύστημα Windows XP, είναι οτι στην περίπτωση των Windows 10, ο Event Viewer καταγράφει ακόμη και IDs τα οποία είναι πιθανό να συσχετιστούν με πιθανές αποτυχημένες κακόβουλες ενέργειες. Αντιθέτως αυτό δεν παρατηρήθηκε στην περίπτωση των Windows XP.

Πίνακας 3: Windows XP Event IDs Explanations

Event ID	**Explanation**
16	When Automatic Updates tries to download updates, the download doesn't succeed, and Event ID 16 is recorded in the system log
19	Windows successfully installed the update
44	Remote users cannot log on to a Windows Server 2012-based Remote Desktop Session Host (RD Session Host) server
43	This event is logged when the time provider returned an error when notified of a network configuration change
7040	Remote users cannot log on to a Windows Server 2012-based Remote Desktop Session Host (RD Session Host) server
10010	This event is logged when the server did not register with DCOM within the required time-out period
7000	The service did not start due to a logon failure.

Βιβλιογραφία [παράδειγμα]

[1] Detecting Lateral Movement through Tracking Event Logs (2017) JPCERT Coordination Center

[2] Nurudeen Ibrahim Universiti Teknologi Malaysia, A. Al-Nemrat University of East London, Hamid Jahankhani Northumbria University London Campus (2012), Sufficiency of Windows Event Log as Evidence in Digital Forensics

[3] Rich Murphey, Applied Cognitive Solutions, Houston, TX, United States (2007) Automated Windows event log forensics

[4] Nagendar Rao Koppolu Inspector of Police (In-charge State Cyber Vertical), Telangana Police Department (2021), Utilizing Event Logs of Windows Operating System in Digital Crime Investigations

[5] J. Dwyer and T. M. Truta, "Finding anomalies in windows event logs using standard deviation," 9th IEEE International Conference on Collaborative Computing: Networking, Applications and Worksharing, 2013, pp. 563-570, doi: 10.4108/icst.collaboratecom.2013.254136.

Παράρτημα Ι Κώδικας που χρησιμοποιήθηκε

Παρακάτω παρατείθενται οι εντολές που χρησιμοποιήθηκαν για την πραγματοποίηση της επίθεσης από το Kali Linux στο Windows XP μηχάνημα.

-sudo nmap –v –A –oX /root/xpresults.xml IP του win XP VM
-sudo systemctl status postgresql
-sudo systemctl start postgresql
-sudo msfdb init
-sudo msfconsole
-db_import /root/xpresults.xml
-services 192.168.1.115
-grep windows grep smb show exploits
-exploit windows/smb/ms17_010_psexec
-info windows/smb/ms17_010_psexec
-exploit windows/smb/ms17_010_psexec
-show options
-set RHOSTS 192.168.1.115
-set LHOST 192.168.1.15
-exploit
-sysinfo
-getsystem
-kill 1864

Παρακάτω παρατείθενται οι εντολές που χρησιμοποιήθηκαν για την πραγματοποίηση της επίθεσης από το Kali Linux στο Windows 10 μηχάνημα.

-services 192.168.1.10
-sudo systemctl status postgresql
-sudo systemctl start postgresql
-sudo msfdb init
-sudo msfconsole
-use exploit/multi/handler
-set payload windows/meterpreter/reverse_tcp
-set rhosts 192.168.1.10
- set lhost 192.168.1.25
-run

Παρακάτω παρατείθεται ο κώδικας Python, ο οποίος χρησιμοποιήθηκε για την γραφική αναπαράσταση του χρονικού της επίθεσης.

```
import pandas as pd
import matplotlib.pyplot as plt
import tkinter as tk

from tkinter import filedialog
root = tk.Tk()
root.withdraw()

file_path = filedialog.askopenfilename()

file1 = pd.read_excel(file_path)
file1.head()

plt.plot(file1['Time'],file1['EventID'])
plt.xlabel('Time')
plt.ylabel('Event ID')
plt.legend(loc='upper left')


plt.show()
```