



**ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ**  
**ΣΧΟΛΗ ΤΕΧΝΟΛΟΓΙΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ**  
**ΕΠΙΚΟΙΝΩΝΙΩΝ ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ**

**Πτυχιακή Εργασία**

Τίτλος Πτυχιακής Εργασίας	Ενίσχυση των δυνατοτήτων ανίχνευσης απειλών σε περιβάλλοντα Windows και CentOS μέσω της ανάλυσης συστημικών και firewall logs από το QRadar  Enhancing Threat Detection Capabilities in Windows and Centos Environments through QRadar Analysis of System and Firewall Logs
Όνοματεπώνυμο Φοιτητή	Ναπολέων Ανδριώτης
Πατρώνυμο	Θεόδωρος Ανδριώτης
Αριθμός Μητρώου	Π14009
Επιβλέπων	Ευθύμιος Αλέπης, Καθηγητής

Ημερομηνία Παράδοσης

Σεπτέμβριος  
2024

---

**Copyright ©**

Απαγορεύεται η αντιγραφή, αποθήκευση και διανομή της παρούσας εργασίας, εξ ολοκλήρου ή τμήματος αυτής, για εμπορικό σκοπό. Επιτρέπεται η ανατύπωση, αποθήκευση και διανομή για σκοπό μη κερδοσκοπικό, εκπαιδευτικής ή ερευνητικής φύσης, υπό την προϋπόθεση να αναφέρεται η πηγή προέλευσης και να διατηρείται το παρόν μήνυμα. Οι απόψεις και τα συμπεράσματα που περιέχονται σε αυτό το έγγραφο εκφράζουν αποκλειστικά τον συγγραφέα και δεν αντιπροσωπεύουν τις επίσημες θέσεις του Πανεπιστημίου Πειραιώς. Ως συγγραφέας της παρούσας εργασίας δηλώνω πως η παρούσα εργασία δεν αποτελεί προϊόν λογοκλοπής και δεν περιέχει υλικό από μη αναφερόμενες πηγές.

## ΠΕΡΙΛΗΨΗ

Ο σκοπός της εργασίας είναι να αναδυχθεί η τέχνη του εντοπισμού και αντιμετώπισης κινδύνων σε ένα Security Operation Center(SOC). Για τη δημιουργία του χρησιμοποιώντας το IBM QRadar, η διαδικασία ξεκίνησε με την εγκατάσταση του VMware σε έναν windows 10 υπολογιστή και την ανάπτυξη ενός εικονικού μηχανήματος QRadar Community Edition 7.5.0 από ένα αρχείο ISO. Το QRadar λειτουργεί ως κεντρική πλατφόρμα παρακολούθησης και ανάλυσης. Στη συνέχεια, δημιουργήθηκαν αρκετά εικονικά μηχανήματα: ένας υπολογιστής με Windows 10 Pro, ένας υπολογιστής με Kali Linux και ένα honeypot με CentOS 8. Κάθε υπολογιστής ρυθμίστηκε για τη δημιουργία και την αποστολή καταγραφών στο QRadar, όπου παραμετροποιήθηκαν τα αντίστοιχα Log Sources για την εισαγωγή και την ερμηνεία αυτών των δεδομένων.

Μόλις η υποδομή ήταν έτοιμη, καθορίστηκαν εννέα Use Cases για να προσομοιώσουν διάφορα σενάρια επίθεσης, με στόχο να δοκιμαστεί και να επικυρωθεί το Rule Correlation Engine του QRadar. Η μεθοδολογία περιλάμβανε την εκτέλεση επιθέσεων κατά των εικονικών μηχανημάτων, την παρακολούθηση και την ανάλυση των καταγραφών που δημιουργήθηκαν μέσα στο QRadar. Βασιζόμενοι στα παρατηρούμενα πρότυπα και συμπεριφορές, δημιουργήθηκαν και εφαρμόστηκαν προσαρμοσμένοι κανόνες συσχέτισης στο QRadar για την ανίχνευση και την αντιμετώπιση αυτών των προσομοιωμένων απειλών. Στη συνέχεια, η αποτελεσματικότητα αυτών των κανόνων επικυρώθηκε με την επανεκτέλεση των επιθέσεων για να εξασφαλιστεί ότι το QRadar αναγνώρισε σωστά και ανταποκρίθηκε σε κάθε σενάριο. Αυτή η ολοκληρωμένη εγκατάσταση εργαστηρίου και διαδικασία δοκιμής αναπαριστά αποτελεσματικά τη ροή εργασίας και τις δυνατότητες ενός πραγματικού SOC, επιδεικνύοντας πώς οι προσαρμοσμένοι κανόνες μπορούν να ενισχύσουν την προστασία δικτύου με την ανίχνευση και την απόκριση ενεργειών ασφαλείας.

## SUMMARY

The purpose of this work is to explore the art of identifying and addressing risks within a Security Operations Center (SOC). For its creation using IBM QRadar, the process began with the installation of VMware on a Windows 10 computer and the deployment of a QRadar Community Edition 7.5.0 virtual machine from an ISO file. QRadar functions as a central monitoring and analysis platform. Subsequently, several virtual machines were created: a Windows 10 Pro computer, a Kali Linux computer, and a honeypot running CentOS 8. Each machine was configured to generate and send logs to QRadar, where the respective Log Sources were configured for the ingestion and interpretation of this data.

Once the infrastructure was ready, nine use cases were defined to simulate various attack scenarios, aiming to test and validate QRadar's Rule Correlation Engine. The methodology involved executing attacks against the virtual machines, monitoring, and analyzing the logs generated within QRadar. Based on the observed patterns and behaviors, custom correlation rules were created and implemented in QRadar to detect and respond to these simulated threats. The effectiveness of these rules was then validated by re-executing the attacks to ensure that QRadar accurately recognized and responded to each scenario. This comprehensive lab setup and testing process effectively represent the workflow and capabilities of a real SOC, demonstrating how custom rules can enhance network protection through the detection and response to security incidents.

## ΠΕΡΙΕΧΟΜΕΝΑ

Copyright © .....	1
ΠΕΡΙΛΗΨΗ.....	2
SUMMARY.....	3
ΠΕΡΙΕΧΟΜΕΝΑ.....	4
ΚΑΤΑΛΟΓΟΣ ΕΙΚΟΝΩΝ.....	5
ΠΡΟΛΟΓΟΣ.....	6
ΕΙΣΑΓΩΓΗ.....	7
1. Qradar Installation Steps.....	7
2. Configuration Windows Host.....	7
3. Configuration Centos8 Host.....	10
Use Cases.....	13
4. Use Case 1: New Administrator Was Added.....	14
5. Use Case 2: SMB Anonymous Logon.....	17
6. Use Case 3: SSH BruteForce was Detected.....	20
7. Use Case 4: SSH BruteForce Centos Host.....	22
8. Use Case 5: Critical: Successful Login After BruteForce Attack.....	24
9. Use Case 6: SSH to Honeypot Detected.....	27
10. Use Case 7: Username Enumeration Detected.....	30
11. Use Case 8: Port Scan Detected.....	32
12. Use Case 9: SMB Scan on the Network was Detected.....	35
ΣΥΜΠΕΡΑΣΜΑΤΑ.....	39
ΠΙΝΑΚΑΣ ΟΡΟΛΟΓΙΑΣ.....	40
ΣΥΝΤΜΗΣΕΙΣ – ΑΡΚΤΙΚΟΛΕΞΑ – ΑΚΡΩΝΥΜΙΑ.....	41

## ΚΑΤΑΛΟΓΟΣ ΕΙΚΟΝΩΝ

Εικόνα 1	Windows Audit Policy Enable Logging .....	8
Εικόνα 2	Firewall Logging .....	8
Εικόνα 3	Windows log Source Configuration .....	9
Εικόνα 4	Windows Service Log source .....	10
Εικόνα 5	SSH Change level To Enable Logging .....	11
Εικόνα 6	Centos Syslog Forward Events to Qradar .....	12
Εικόνα 7	Centos Log Source Configuration .....	13
Εικόνα 8	Administrator Creation and Addition to Administrator group .....	14
Εικόνα 9	Event Created .....	15
Εικόνα 10	New Administrator Was Added Rule .....	15
Εικόνα 11	New Administrator Was Added RuleRest .....	16
Εικόνα 12	After Adding User Again Rule Created An Event.....	17
Εικόνα 13	SMB Anonymous Logon Attack .....	17
Εικόνα 14	SMB Anonymous Logon Event Created .....	18
Εικόνα 15	SMB Anonymous Logon Rule .....	18
Εικόνα 16	SMB Anonymous Logon Dispatched Event .....	19
Εικόνα 17	SSH Bruteforce Attack .....	20
Εικόνα 18	SSH Bruteforce Logs .....	20
Εικόνα 19	SSH Bruteforce Building Block.....	21
Εικόνα 20	SSH Bruteforce Rule .....	21
Εικόνα 21	SSH Bruteforce Offence.....	21
Εικόνα 22	SSH Bruteforce on Centos Host .....	22
Εικόνα 23	Password Check Failed Event .....	22
Εικόνα 24	SSH Bruteforce on Centos Host Rule .....	23
Εικόνα 25	SSH Bruteforce Centos Host Offence Triggered .....	23
Εικόνα 26	Bruteforce Reference Set Creation .....	24
Εικόνα 27	Enable Add to Reference Set Attribute .....	24
Εικόνα 28	Successful SSH Login Event .....	25
Εικόνα 29	Successfull Login After BruteForce Attack Rule .....	25
Εικόνα 30	Successfull Login After BruteForce Attack Offence .....	26
Εικόνα 31	Honeypot Reference Set.....	27
Εικόνα 32	Honeypot SSH Centos Event.....	27
Εικόνα 33	SSH custom property regex .....	28
Εικόνα 34	SSH custom property regex 2 .....	28
Εικόνα 35	SSH to Honeypot Rule .....	29
Εικόνα 36	SSH to Honeypot Offense.....	29
Εικόνα 37	Username Enumeration Logs .....	30
Εικόνα 38	Event used for Rule.....	30
Εικόνα 39	Username Enumeration Rule.....	31
Εικόνα 40	Username Enumeration Offence.....	31
Εικόνα 41	Nmap Scan to trigger logs.....	32
Εικόνα 42	Log Detection .....	32
Εικόνα 43	Event 5152 .....	33
Εικόνα 44	Event 5156 .....	34
Εικόνα 45	Port Scan Rule Building Block .....	34
Εικόνα 46	Port Scan Rule .....	34
Εικόνα 47	Port Scan Triggered Offence .....	35
Εικόνα 48	Scan Including SMB port.....	36
Εικόνα 49	Events Detected From Windows Host .....	36
Εικόνα 50	Windows Event Used .....	37
Εικόνα 51	Centos Logs .....	37

Εικόνα 52 Centos 445 Event.....	37
Εικόνα 53 Windows Building Block .....	38
Εικόνα 54 Centos Building Block .....	38
Εικόνα 55 SMB Scan Rule .....	38
Εικόνα 56 SMB Scan Offence.....	38

## ΠΡΟΛΟΓΟΣ

Η παρούσα εργασία εστιάζει στην εφαρμογή και αξιολόγηση της τέχνης της ανίχνευσης και διαχείρισης κινδύνων στον τομέα της ψηφιακής ασφάλειας. Το πλαίσιο της εργασίας περιλαμβάνει τη δημιουργία ενός εικονικού περιβάλλοντος που αναπαριστά ένα Security Operation Center (SOC), με στόχο τη δοκιμή και επικύρωση της αποτελεσματικότητας των εργαλείων ανάλυσης και παρακολούθησης.

Η διαδικασία αυτή περιλάμβανε τη δημιουργία και προσομοίωση διαφόρων σεναρίων απειλών, ώστε να εξεταστεί η ικανότητα του συστήματος να εντοπίζει και να διαχειρίζεται επικίνδυνες καταστάσεις. Μέσα από τις δοκιμές και την ανάλυση των αποτελεσμάτων, επιδιώχθηκε η ενίσχυση των διαδικασιών ασφαλείας και η καλύτερη κατανόηση των πρακτικών που ακολουθούνται σε ένα SOC.

Με την ολοκλήρωση της διαδικασίας, αναδείχθηκε η σημασία της συνεχούς αναβάθμισης και βελτίωσης των εργαλείων ασφαλείας, προσφέροντας πολύτιμα διδάγματα για την ενίσχυση της προστασίας των ψηφιακών συστημάτων.

## ΕΙΣΑΓΩΓΗ

### 1. Qradar Installation Steps

Για να εγκαταστήσετε το QRadar 7.5.0, ξεκινήστε δημιουργώντας ένα νέο εικονικό μηχάνημα στο VMware Workstation. Επιλέξτε "I will install the operating system later" και ορίστε το guest OS ως Linux με "Other Linux 4.x kernel 64-bit".

Βεβαιωθείτε ότι ο αποθηκευτικός χώρος του δίσκου ρυθμίζεται ως single file και προσαρμόστε το υλικό για να πληροί τις ελάχιστες απαιτήσεις που ορίζει η IBM δηλαδή στη συγκεκριμένη περίπτωση 24GB RAM, 4 cores και 250GB disk minimum. Στην καρτέλα Network Adapter, επιλέξτε "Bridged: connected to physical network". Σημειώστε ότι πρέπει να ενεργοποιήσετε το Bridged Protocol του VMware από τις ethernet adapter settings στον Windows .

Στη συνέχεια, φορτώστε το αρχείο ISO του QRadar 7.5.0 και συνεχίστε με την εγκατάσταση. Ο installer θα εγκαταστήσει πρώτα το RHEL (Red Hat Enterprise Linux), ενώ στη συνέχεια θα ακολουθήσει η αυτόματη εγκατάσταση του QRadar. Κατά την εγκατάσταση του RHEL, συνδεθείτε ως "root" χωρίς κωδικό πρόσβασης και αποδεχτείτε τη Συμφωνία Χρήστη Τελικού Χρήστη (EULA) πληκτρολογώντας "yes".

Αφού ολοκληρωθεί η εγκατάσταση του RHEL, θα ξεκινήσει το Wizard Εγκατάστασης του QRadar. Επιλέξτε "Software Install" και συνεχίστε με το "All-in-One Console". Επιλέξτε την εγκατάσταση "Normal", ρυθμίστε τις ρυθμίσεις ώρας, επιλέξτε τη σωστή ζώνη ώρας και ρυθμίστε τα πρωτόκολλα δικτύου. Καθορίστε το Management NIC και ρυθμίστε τις ρυθμίσεις δικτύου, βεβαιωθείτε ότι το hostname είναι το Fully Qualified Domain Name (FQDN).

Καταχωρίστε νέους κωδικούς διαχειριστή και root με προσοχή, χρησιμοποιώντας το πλήκτρο tab για πλοήγηση και έπειτα enter για επιβεβαίωση, προκειμένου να αποφευχθούν προβλήματα ρύθμισης κωδικού που θα μπορούσαν να οδηγήσουν σε κλείδωμα. Ολοκληρώστε τη διαδικασία εγκατάστασης για να ρυθμίσετε επιτυχώς το QRadar σε δίσκο SATA, καθώς οι δίσκοι NVME δεν είναι συμβατοί με την εγκατάσταση.

Ακολουθώντας αυτά τα βήματα εξασφαλίζετε μια ομαλή εγκατάσταση του QRadar 7.5.0, προσαρμοσμένη για να πληροί τις απαιτήσεις των προδιαγραφών.

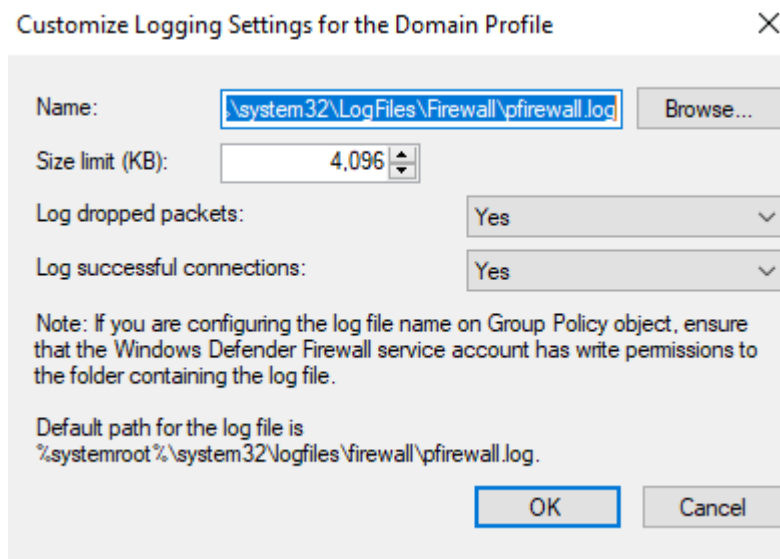
### 2. Configuration Windows Host

Αρχικά, ενεργοποιήσαμε καταγραφές μέσω του local audit policy για να διασφαλίσουμε την ολοκληρωμένη κάλυψη των καταγραφών στο περιβάλλον των Windows. Ταυτόχρονα, ενεργοποιήσαμε όλες τις καταγραφές του Windows Firewall και ενεργοποιήσαμε συγκεκριμένους κανόνες ώστε να επιτρέψουμε την εξερχόμενη κίνηση προς τη θύρα 514, η οποία είναι αφιερωμένη για την επικοινωνία με το QRadar.



Policy	Security Setting
Audit account logon events	Success, Failure
Audit account management	Success, Failure
Audit directory service access	Success, Failure
Audit logon events	Success, Failure
Audit object access	Success, Failure
Audit policy change	Success, Failure
Audit privilege use	Success, Failure
Audit process tracking	Success, Failure
Audit system events	Success, Failure


Εικόνα 1 Windows Audit Policy Enable Logging



Εικόνα 2 Firewall Logging

Μετά τις παραπάνω προετοιμασίες, προχωρήσαμε στην εγκατάσταση του WinCollect έκδοσης 7.3.1-22x86.exe στον υπολογιστή με Windows σε standalone configuration, καθώς το Qradar CE δεν υποστηρίζει managed configuration. Μετά την ολοκλήρωση της εγκατάστασης, επανεκκινήσαμε την υπηρεσία WinCollect για να εξασφαλίσουμε την ορθή αρχικοποίηση και συγχρονισμό με το QRadar.

Στη συνέχεια, στην κονσόλα του QRadar, διαμορφώσαμε ένα νέο log source, παρέχοντας τις απαραίτητες λεπτομέρειες για τον Windows υπολογιστή προκειμένου να ολοκληρωθεί το integration. Να σημειώσουμε ότι έχει δημιουργηθεί ένα ακόμα log source που περιχει καταγραφές από το service wincollect που εγκαταστήσαμε στον host. Με αυτές τις καταγραφές θα μπορούσαμε να κάνουμε troubleshoot σε ένα ενδεχόμενο error μέσω του Qradar.



**Beast @ 192.168.1.48**

Microsoft Windows Security Event Log

Status: OK

Last Update

Overview

Protocol

<b>ID</b>	163
<b>Name</b>	Beast @ 192.168.1.48
<b>Description</b>	
<b>Enabled</b>	Yes
<b>Log Source Type</b>	Microsoft Windows Security Event Log
<b>Protocol Type</b>	Forwarded
<b>Groups</b>	<span style="border: 1px solid #ccc; border-radius: 10px; padding: 2px 5px; background-color: #f0f0f0;">Other</span>
<b>Extension</b>	
<b>Language</b>	English
<b>Target Event Collector</b>	eventcollector0 :: Logger
<b>Disconnected Log Collector</b>	Not Set
<b>Credibility</b>	5
<b>Internal</b>	No
<b>Deployed</b>	Yes
<b>Coalescing Events</b>	Yes
<b>Store Event Payloads</b>	Yes

**Εικόνα 3 Windows log Source Configuration**

**WinCollect @ BEAST**

WinCollect

Status: OK

**Overview**

## Protocol

<b>ID</b>	162
<b>Name</b>	WinCollect @ BEAST
<b>Description</b>	WinCollect device
<b>Enabled</b>	Yes
<b>Log Source Type</b>	WinCollect
<b>Protocol Type</b>	Syslog
<b>Groups</b>	<span>Other</span>
<b>Extension</b>	
<b>Language</b>	English
<b>Target Event Collector</b>	eventcollector0 :: Logger
<b>Disconnected Log Collector</b>	Not Set
<b>Credibility</b>	5
<b>Internal</b>	No
<b>Deployed</b>	Yes
<b>Coalescing Events</b>	Yes
<b>Store Event Payloads</b>	Yes

Εικόνα 4 Windows Service Log source

Το Qradar δέχεται πλέον με επιτυχία καταγραφές και το correlation ξεκίνησε.

### 3. Configuration Centos8 Host

Για την διαμόρφωση ενός CentOS μηχανήματος και την αποστολή των καταγραφών του στο QRadar, ξεκινήσαμε ενεργοποιώντας τη δυνατότητα καταγραφής στο σύστημα. Επιπλέον, ενεργοποιήσαμε την καταγραφή συνδέσεων SSH, εξασφαλίζοντας ότι όλες οι απόπειρες σύνδεσης μέσω SSH καταγράφονται και αποστέλλονται για ανάλυση. Στη συνέχεια, διαμορφώσαμε το σύστημα να αποστέλλει τα αρχεία καταγραφής στο QRadar χρησιμοποιώντας

την θύρα 514, η οποία είναι αφιερωμένη για τέτοιου είδους επικοινωνία. Αυτό επιτεύχθηκε με την προσαρμογή των ρυθμίσεων του syslog ώστε να προωθεί τις καταγραφές στο QRadar.

```
HostKey /etc/ssh/ssh_host_rsa_key
HostKey /etc/ssh/ssh_host_ecdsa_key
HostKey /etc/ssh/ssh_host_ed25519_key

# Ciphers and keying
#RekeyLimit default none

# This system is following system-wide crypto policy. The changes to
# crypto properties (Ciphers, MACs, ...) will not have any effect here.
# They will be overridden by command-line options passed to the server
# on command line.
# Please, check manual pages for update-crypto-policies(8) and sshd_config(5).

# Logging
#SyslogFacility AUTH
SyslogFacility AUTHPRIV
LogLevel INFO

# Authentication:

#LoginGraceTime 2m
PermitRootLogin yes
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10

#PubkeyAuthentication yes

# The default is to check both .ssh/authorized_keys and .ssh/authorized_keys2
# but this is overridden so installations will only check .ssh/authorized_keys
AuthorizedKeysFile .ssh/authorized_keys
```

Εικόνα 5 SSH Change level To Enable Logging

```
##### GLOBAL DIRECTIVES #####  
  
# Where to place auxiliary files  
global(workDirectory="/var/lib/rsyslog")  
  
# Use default timestamp format  
module(load="builtin:omfile" Template="RSYSLOG_TraditionalFileFormat")  
  
# Include all config files in /etc/rsyslog.d/  
include(file="/etc/rsyslog.d/*.conf" mode="optional")  
  
##### RULES #####  
  
# Log all kernel messages to the console.  
# Logging much else clutters up the screen.  
#kern.* /dev/console  
  
# Log anything (except mail) of level info or higher.  
# Don't log private authentication messages!  
*.info;mail.none;authpriv.none;cron.none /var/log/messages  
  
# The authpriv file has restricted access.  
authpriv.* /var/log/secure  
  
# Log all the mail messages in one place.  
mail.* -/var/log/maillog  
  
# Log cron stuff  
cron.* /var/log/cron  
  
# Everybody gets emergency messages  
*.emerg :omusrmsg:*  
  
# Save news errors of level crit and higher in a special file.  
uucp,news.crit /var/log/spooler  
  
# Save boot messages also to boot.log  
local7.* /var/log/boot.log  
  
*.*@192.168.1.123:514
```

Εικόνα 6 Centos Syslog Forward Events to Qradar

Μετά την ολοκλήρωση αυτών των βημάτων, δημιουργήσαμε ένα νέο log source στην κονσόλα του QRadar για τον CentOS υπολογιστή, παρέχοντας όλες τις απαραίτητες πληροφορίες σχετικά με το σύστημα και διασφαλίζοντας ότι το QRadar μπορεί να λαμβάνει και να επεξεργάζεται τα καταγεγραμμένα δεδομένα από τον συγκεκριμένο υπολογιστή.



## LinuxServer @ centos8

Linux OS

Status: **Error**

Events have not been received from this Log Source in over 720 minutes.

### Overview

### Protocol

<b>ID</b>	212
<b>Name</b>	LinuxServer @ centos8
<b>Description</b>	LinuxServer device
<b>Enabled</b>	Yes
<b>Log Source Type</b>	Linux OS
<b>Protocol Type</b>	Syslog
<b>Groups</b>	Other
<b>Extension</b>	
<b>Language</b>	English
<b>Target Event Collector</b>	eventcollector0 :: Logger
<b>Disconnected Log Collector</b>	Not Set
<b>Credibility</b>	5
<b>Internal</b>	No
<b>Deployed</b>	Yes
<b>Coalescing Events</b>	Yes
<b>Store Event Payloads</b>	Yes

Εικόνα 7 Centos Log Source Configuration

## Use Cases

#### 4. Use Case 1: New Administrator Was Added

Ο κανόνας αυτός θα υποδείξει σε έναν πιθανό αναλυτή ασφαλείας ότι ένας καινούργιος χρήστης προστέθηκε στο Administrators group το οποίο του δίνει admin privileges. Η κίνηση αυτή πρέπει να καταγράφεται ειδικά σε ένα domain περιβάλλον. Εμείς δημιουργήσαμε το κανόνα ώστε να ειδοποιεί για τον Local administrator καθώς δεν δημιουργήσαμε domain. Με το Event ID και το Group Name δημιουργήσαμε τον κανόνα και επαναλάβαμε την διαδικασία ώστε να τεστάrouμε αν δουλεύει ο κανόνας που δημιουργήσαμε.

```
Microsoft Windows [Version 10.0.19045.4651]
(c) Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>net localgroup administrators
Alias name      administrators
Comment        Administrators have complete and unrestricted access to the computer/domain

Members

-----
Administrator
Napoleon
The command completed successfully.

C:\WINDOWS\system32>

C:\WINDOWS\system32>net user Kali kali123!@# /add
The command completed successfully.

C:\WINDOWS\system32>net localgroup administrators Kali /add
The command completed successfully.

C:\WINDOWS\system32>net localgroup administrators
Alias name      administrators
Comment        Administrators have complete and unrestricted access to the compu

Members

-----
Administrator
Kali
Napoleon
The command completed successfully.
```

Εικόνα 8 Administrator Creation and Addition to Administrator group

Event Name	Success Audit: A member was added to a security-enabled local group		
Low Level Category	Group Member Added		
Event Description	Success Audit: A member was added to a security-enabled local group.		
Magnitude		(4) Relevance	6
Username	Napoleon		
Start Time	Jul 16, 2024, 6:44:23 PM	Storage Time	Jul 16, 2024, 6:44:23 PM
Account Name (custom)	-		
Event ID (custom)	4732		
Group ID (custom)	N/A		
Group Name (custom)	Administrators		
Logon Type (custom)	N/A		
Object Type (custom)	N/A		
Source Workstation (custom)	N/A		
Target Username (custom)	Kali		
User Domain (custom)	BEAST		
Domain	Default Domain		

Source and Destination Information			
Source IP	192.168.1.48	Destination IP	192.168.1.48
Source Asset Name	N/A	Destination Asset Name	N/A

Εικόνα 9 Event Created

Type to filter

- when the local network is one of the following networks
- when the destination network is one of the following networks
- when the IP protocol is one of the following protocols
- when the Event Payload contains this string
- when the source port is one of the following ports
- when the destination port is one of the following ports
- when the local port is one of the following ports
- when the remote port is one of the following ports
- when the source IP is one of the following IP addresses
- when the destination IP is one of the following IP addresses

Rule (Click on an underlined value to edit it)  
 Invalid tests are highlighted and must be fixed before rule can be saved.

Apply  on events which are detected by the Local system

- and when the event matches Event ID (custom) is any of 4732
- and when the event matches Group Name (custom) is any of Administrators

Please select any groups you would like this rule to be a member of:

- Anomaly
- Asset Reconciliation Exclusion
- Authentication
- Botnet
- Category Definitions

Notes (Enter your notes about this rule)

Performance Analysis

This rule has not yet had a detailed analysis.

Εικόνα 10 New Administrator Was Added Rule



<input checked="" type="checkbox"/> Severity	Set to	10
<input checked="" type="checkbox"/> Credibility	Set to	10
<input checked="" type="checkbox"/> Relevance	Set to	10
<input type="checkbox"/> Ensure the detected event is part of an offense		
<input type="checkbox"/> Annotate event		
<input type="checkbox"/> Bypass further rule correlation event		

**Rule Response**  
Choose the response(s) to make when an event triggers this rule

Dispatch New Event

Enter the details of the event to dispatch

Event Name: Administrator Added

Event Description: Administrator Added

**Event Details:**

Severity 5    Credibility 10    Relevance 10

High-Level Category: Access    Low-Level Category: Access Denied

Annotate this offense: Administrator Added

Ensure the dispatched event is part of an offense

Index offense based on Source IP

Include detected events by Source IP from this point forward, in the offense, for: 300 second(s)

**Offense Naming**

This information should contribute to the name of the associated offense(s)

This information should set or replace the name of the associated offense(s)

This information should not contribute to the naming of the associated offense(s)

Εικόνα 11 New Administrator Was Added RuleRest

Event Information			
Event Name	Administrator Added		
Low Level Category	Access Denied		
Event Description	Administrator Added		
Magnitude		(6) Relevance	6
Severity	Severit		
Username	Napoleon		
Start Time	Jul 16, 2024, 6:49:37 PM	Storage Time	Jul 16, 2024, 6:49:37 PM
Log So	Log So		
CRE Description (custom)	Administrator Added		
CRE Name (custom)	Administrator Added		
Domain	Default Domain		

Source and Destination Information			
Source IP	192.168.1.48	Destination IP	192.168.1.48
Source Asset Name	N/A	Destination Asset Name	N/A
Source Port	0	Destination Port	0
Pre NAT Source IP		Pre NAT Destination IP	
Pre NAT Source Port	0	Pre NAT Destination Port	0
Post NAT Source IP		Post NAT Destination IP	
Post NAT Source Port	0	Post NAT Destination Port	0
Source IPv6	0:0:0:0:0:0:0:0	Destination IPv6	0:0:0:0:0:0:0:0
Source MAC	00:00:00:00:00:00	Destination MAC	00:00:00:00:00:00

Payload Information	
Encoding	utf hex base64
Wrap Text	<input checked="" type="checkbox"/>
Content	Administrator Added Administrator Added

Εικόνα 12 After Adding User Again Rule Created An Event

### 5. Use Case 2: SMB Anonymous Logon

Το δεύτερο use case που τεστάρουμε είναι το SMB Anonymous Logon καθώς είναι μία από τις πρώτες ευπάθειες που θα προσπαθήσει να εκμεταλευτεί ένας κακόβουλος όταν εισέρχεται σε ένα δίκτυο. Το SMB Anonymous Logon αναφέρεται στη δυνατότητα πρόσβασης σε πόρους δικτύου χωρίς την παροχή ονόματος χρήστη και κωδικού πρόσβασης.

```

enum4linux 192.168.1.48
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Wed Jul 17 14:00:07 2024

----- ( Target Information ) -----
Target ..... 192.168.1.48
RID Range ..... 500-550,1000-1050
Username ..... ''
Password ..... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none

----- ( Enumerating Workgroup/Domain on 192.168.1.48 ) -----

[+] Got domain/workgroup name: WORKGROUP

----- ( Nbtstat Information for 192.168.1.48 ) -----

Looking up status of 192.168.1.48
No reply from 192.168.1.48

----- ( Session Check on 192.168.1.48 ) -----

[E] Server doesn't allow session using username '', password ''. Aborting remainder of tests.
    
```

Εικόνα 13 SMB Anonymous Logon Attack

Event Information			
Event Name	Success Audit: An account was successfully logged on		
Low Level Category	User Login Success		
Event Description	Success Audit: An account was successfully logged on.		
Magnitude	(0)	Relevance	0
Username	ANONYMOUS LOGON		
Start Time	Jul 17, 2024, 9:19:21 PM	Storage Time	Jul 17, 2024, 9:19:21 PM
Account Name (custom)	ANONYMOUS		
Event ID (custom)	4624		
Group ID (custom)	N/A		
Logon Type (custom)	3		
Machine Identifier (custom)	CHILLIKOS		
Object Type (custom)	N/A		
Process Name (custom)	-		
Source Workstation (custom)	CHILLIKOS		
Target Username (custom)	ANONYMOUS LOGON		
User Domain (custom)	-		
Domain	Default Domain		

Εικόνα 14 SMB Anonymous Logon Event Created

Test Group [Full]
Export to Summary Screen

Type to filter
 

- + when the local network is one of the following networks
- + when the destination network is one of the following networks
- + when the IP protocol is one of the following protocols
- + when the Event Payload contains this string
- + when the source port is one of the following ports
- + when the destination port is one of the following ports
- + when the local port is one of the following ports
- + when the remote port is one of the following ports
- + when the source IP is one of the following IP addresses
- + when the destination IP is one of the following IP addresses

Rule (Click on an underlined value to edit it)  
 Invalid tests are highlighted and must be fixed before rule can be saved.

Apply SMB ANONYMOUS LOGON on events which are detected by the Local system
 

- ⊘ ↔ and when the event matches Event ID (custom) is any of 4624
- ⊘ ↔ and when the event matches Logon Type (custom) is any of 3
- ⊘ ↔ and when the event matches Username is any of ANONYMOUS LOGON

Please select any groups you would like this rule to be a member of:

- Anomaly
- Asset Reconciliation Exclusion
- Authentication
- Botnet
- Category Definitions


Notes (Enter your notes about this rule)

SMB ANONYMOUS LOGON Shouldnt be open

Performance Analysis

This rule has not yet had a detailed analysis.

Εικόνα 15 SMB Anonymous Logon Rule

Event Information			
Event Name	ANONYMOUS LOGON ATTEMPT		
Low Level Category	Access Denied		
Event Description	ANONYMOUS LOGON		
Magnitude		(6)	Relevance
Severity	6		
Username	ANONYMOUS LOGON		
Start Time	Jul 17, 2024, 9:19:22 PM	Storage Time	Jul 17, 2024, 9:19:22 PM
Log Source Time			
CRE Description (custom)	ANONYMOUS LOGON		
CRE Name (custom)	ANONYMOUS LOGON ATTEMPT		
Domain	Default Domain		

Source and Destination Information			
Source IP	192.168.1.135	Destination IP	192.168.1.48
Source Asset Name	N/A	Destination Asset Name	N/A
Source Port	45078	Destination Port	0
Pre NAT Source IP		Pre NAT Destination IP	
Pre NAT Source Port	0	Pre NAT Destination Port	0
Post NAT Source IP		Post NAT Destination IP	
Post NAT Source Port	0	Post NAT Destination Port	0
Source IPv6	0:0:0:0:0:0:0:0	Destination IPv6	0:0:0:0:0:0:0:0
Source MAC	00:00:00:00:00:00	Destination MAC	00:00:00:00:00:00

Payload Information	
<div style="display: flex; border: 1px solid #ccc; padding: 2px;"> <span style="border: 1px solid #ccc; padding: 2px 5px;">utf</span> <span style="border: 1px solid #ccc; padding: 2px 5px;">hex</span> <span style="border: 1px solid #ccc; padding: 2px 5px;">base64</span> </div> <div style="border: 1px solid #ccc; padding: 2px;"> <input checked="" type="checkbox"/> Wrap Text                 </div>	ANONYMOUS LOGON ATTEMPT ANONYMOUS LOGON

**Εικόνα 16 SMB Anonymous Logon Dispatched Event**

## 6. Use Case 3: SSH Bruteforce was Detected

Μια επίθεση brute-force στην SSH υπηρεσία είναι μια απειλή ασφαλείας, όπου ένας επιτιθέμενος προσπαθεί να αποκτήσει μη εξουσιοδοτημένη πρόσβαση σε ένα σύστημα, δοκιμάζοντας συστηματικά συνδυασμούς ενός ονόματος χρήστη και πολλαπλών κωδικών πρόσβασης. Ο εντοπισμός περιλαμβάνει συνήθως την παρακολούθηση για επανειλημμένες αποτυχημένες προσπάθειες σύνδεσης από την ίδια διεύθυνση IP ή για ασυνήθιστες συμπεριφορές σύνδεσης, όπως προσπάθειες από μη αναμενόμενες γεωγραφικές τοποθεσίες. Εάν η επίθεση επιτύχει, ο επιτιθέμενος μπορεί να παραβιάσει λογαριασμούς και πιθανόν να αποκτήσει τον έλεγχο του συστήματος. Στην συγκεκριμένη περίπτωση χρησιμοποιούμε το event id 4625 και το Process Name "sshd.exe" για τον εντοπισμό της σωστής καταγραφής και τα τοποθετούμε σε ένα Building Block. Στο επόμενο βήμα δημιουργούμε κανόνα ώστε αν εντοπίσει το συγκεκριμένο pattern 5 φορές σε ένα λεπτό να ενεργοποιηθεί το offence.

```
msf6 auxiliary(scanner/ssh/ssh_login) > set VERBOSE true
VERBOSE => true
msf6 auxiliary(scanner/ssh/ssh_login) > run

[*] 192.168.1.48:22 - Starting bruteforce
[-] 192.168.1.48:22 - Failed: 'root:123456'
[!] No active DB -- Credential data will not be saved!
[-] 192.168.1.48:22 - Failed: 'root:12345'
[-] 192.168.1.48:22 - Failed: 'root:123456789'
[-] 192.168.1.48:22 - Failed: 'root:password'
[-] 192.168.1.48:22 - Failed: 'root:iloveyou'
[-] 192.168.1.48:22 - Failed: 'root:princess'
[-] 192.168.1.48:22 - Failed: 'root:1234567'
[-] 192.168.1.48:22 - Failed: 'root:rockyou'
[-] 192.168.1.48:22 - Failed: 'root:12345678'
```

Εικόνα 17 SSH Bruteforce Attack

Original Filters:  
 Source IP is not 192.168.1.123 (Clear Filter) Process Path (custom) is any of C:\Windows\System32\OpenSSH\sshd.exe (Clear Filter)

Current Filters:  
 Event Name is Failure Audit: An account failed to log on (Clear Filter)

► Current Statistics

Event Name	Log Source	Event Count	Time	Low Level Category	Source IP	Source Port	Destination IP
Failure Audit: An account failed to log on	Beast @ 192.168.1.48	14	Jul 15, 2024, 7:41:26 PM	User Login Failure	192.168.1.48	0	192.168.1.48
Failure Audit: An account failed to log on	Beast @ 192.168.1.48	34	Jul 15, 2024, 7:41:08 PM	User Login Failure	192.168.1.48	0	192.168.1.48
Failure Audit: An account failed to log on	Beast @ 192.168.1.48	46	Jul 15, 2024, 7:40:58 PM	User Login Failure	192.168.1.48	0	192.168.1.48
Failure Audit: An account failed to log on	Beast @ 192.168.1.48	8	Jul 15, 2024, 7:40:47 PM	User Login Failure	192.168.1.48	0	192.168.1.48
Failure Audit: An account failed to log on	Beast @ 192.168.1.48	41	Jul 15, 2024, 7:40:37 PM	User Login Failure	192.168.1.48	0	192.168.1.48
Failure Audit: An account failed to log on	Beast @ 192.168.1.48	49	Jul 15, 2024, 7:40:26 PM	User Login Failure	192.168.1.48	0	192.168.1.48
Failure Audit: An account failed to log on	Beast @ 192.168.1.48	46	Jul 15, 2024, 7:40:13 PM	User Login Failure	192.168.1.48	0	192.168.1.48
Failure Audit: An account failed to log on	Beast @ 192.168.1.48	59	Jul 15, 2024, 7:39:58 PM	User Login Failure	192.168.1.48	0	192.168.1.48
Failure Audit: An account failed to log on	Beast @ 192.168.1.48	46	Jul 15, 2024, 7:39:46 PM	User Login Failure	192.168.1.48	0	192.168.1.48
Failure Audit: An account failed to log on	Beast @ 192.168.1.48	45	Jul 15, 2024, 7:39:34 PM	User Login Failure	192.168.1.48	0	192.168.1.48
Failure Audit: An account failed to log on	Beast @ 192.168.1.48	41	Jul 15, 2024, 7:39:22 PM	User Login Failure	192.168.1.48	0	192.168.1.48
Failure Audit: An account failed to log on	Beast @ 192.168.1.48	45	Jul 15, 2024, 7:39:10 PM	User Login Failure	192.168.1.48	0	192.168.1.48
Failure Audit: An account failed to log on	Beast @ 192.168.1.48	51	Jul 15, 2024, 7:38:58 PM	User Login Failure	192.168.1.48	0	192.168.1.48
Failure Audit: An account failed to log on	Beast @ 192.168.1.48	46	Jul 15, 2024, 7:38:46 PM	User Login Failure	192.168.1.48	0	192.168.1.48
Failure Audit: An account failed to log on	Beast @ 192.168.1.48	43	Jul 15, 2024, 7:38:34 PM	User Login Failure	192.168.1.48	0	192.168.1.48
Failure Audit: An account failed to log on	Beast @ 192.168.1.48	53	Jul 15, 2024, 7:38:22 PM	User Login Failure	192.168.1.48	0	192.168.1.48
Failure Audit: An account failed to log on	Beast @ 192.168.1.48	41	Jul 15, 2024, 7:38:10 PM	User Login Failure	192.168.1.48	0	192.168.1.48
Failure Audit: An account failed to log on	Beast @ 192.168.1.48	43	Jul 15, 2024, 7:37:58 PM	User Login Failure	192.168.1.48	0	192.168.1.48

Εικόνα 18 SSH Bruteforce Logs

### Rule


Apply SSH Bruteforce Detected Building Block on events which are detected by the Local system and when the event matches Event ID is any of 4625 and when the event matches Process Name (custom) is any of sshd.exe

Εικόνα 19 SSH Bruteforce Building Block

### Rule

Apply SSH Bruteforce was Detected on events which are detected by the Local system and when SSH Bruteforce Detected Building Block match at least 5 times in 1 minutes

Εικόνα 20 SSH Bruteforce Rule

Event Information			
Event Name	BRUTE FORCE DETECTED		
Low Level Category	Access Denied		
Event Description	Multiple ssh failed attempts were detected Actions Block IP of the attacker Stop ssh Service on host		
Magnitude		(6)	Relevance 6
Severity			
Username	NOUSER		
Start Time	Jul 15, 2024, 8:11:17 PM	Storage Time	Jul 15, 2024, 8:11:17 PM
Log Source			
CRE Description (custom)	Multiple ssh failed attempts were detected		
CRE Name (custom)	BRUTE FORCE DETECTED		
Domain	Default Domain		
Source and Destination Information			
Source IP	192.168.1.48	Destination IP	192.168.1.48
Source Asset Name	N/A	Destination Asset Name	N/A
Source Port	0	Destination Port	0
Pre NAT Source IP		Pre NAT Destination IP	
Pre NAT Source Port	0	Pre NAT Destination Port	0
Post NAT Source IP		Post NAT Destination IP	
Post NAT Source Port	0	Post NAT Destination Port	0
Source IPv6	0:0:0:0:0:0:0:0	Destination IPv6	0:0:0:0:0:0:0:0
Source MAC	00:00:00:00:00:00	Destination MAC	00:00:00:00:00:00
Payload Information			

Εικόνα 21 SSH Bruteforce Offence


## 7. Use Case 4: SSH Bruteforce Centos Host

Καθώς το event 4625 είναι για windows μηχανήματα πως θα μπορούσε να εντοπιστεί η ίδια επίθεση σε ένα CentOS λειτουργικό; Κάνοντας την επίθεση και αναλύοντας τις καταγραφές βρίσκουμε το event “Password Check Failed” το οποίο χρησιμοποιούμε στο Building block του κανόνα μας μέσω του QID του. Στον κανόνα προσθέτουμε την συχνότητα που θέλουμε και ξανατρέχουμε την επίθεση. Ο κανόνας δουλεύει και δημιουργεί καινούργιο event από το “custom rule engine”.

```

[-] 192.168.1.166:22 - Failed: 'centos:hello'
[-] 192.168.1.166:22 - Failed: 'centos:elizabeth'
[-] 192.168.1.166:22 - Failed: 'centos:hottie'
[-] 192.168.1.166:22 - Failed: 'centos:tinkerbell'
[-] 192.168.1.166:22 - Failed: 'centos:charlie'
[-] 192.168.1.166:22 - Failed: 'centos:samantha'
[-] 192.168.1.166:22 - Failed: 'centos:barbie'
[-] 192.168.1.166:22 - Failed: 'centos:chelsea'
[-] 192.168.1.166:22 - Failed: 'centos:lovers'
[-] 192.168.1.166:22 - Failed: 'centos:teamo'
[-] 192.168.1.166:22 - Failed: 'centos:jasmine'
[-] 192.168.1.166:22 - Failed: 'centos:brandon'
[-] 192.168.1.166:22 - Failed: 'centos:666666'
[-] 192.168.1.166:22 - Failed: 'centos:shadow'
[-] 192.168.1.166:22 - Failed: 'centos:melissa'
    
```

Εικόνα 22 SSH Bruteforce on Centos Host

Event Name	Password Check Failed		
Low Level Category	Notice		
Event Description	Password Check Failed		
Magnitude		(5)	Relevance 6
Severity			
Username	centos		
Start Time	Sep 2, 2024, 3:55:44 PM	Storage Time	Sep 2, 2024, 3:55:44 PM
Log Source			
Application (custom)	unix_chkpwd		
Machine Identifier (custom)	N/A		
Process ID (custom)	5588		
Process Name (custom)	N/A		
User ID (custom)	N/A		
Domain	Default Domain		

### Source and Destination Information


Source IP	192.168.1.166	Destination IP	192.168.1.166
Source Asset Name	N/A	Destination Asset Name	N/A

Εικόνα 23 Password Check Failed Event

### Rule

Apply SSH Bruteforce Centos Host on events which are detected by the Local system and when SSH Bruteforce Centos Host Building Block match at least 10 times in 1 minutes

Εικόνα 24 SSH Bruteforce on Centos Host Rule

Event Information			
Event Name	SSH Bruteforce Centos Host		
Low Level Category	Access Denied		
Event Description	SSH Bruteforce Centos Host		
Magnitude	 (6)	Relevance	6
Severity			
Username	centos		
Start Time	Sep 2, 2024, 3:54:53 PM	Storage Time	Sep 2, 2024, 3:54:53 PM
Domain	Default Domain		
Log Source			
Source and Destination Information			
Source IP	192.168.1.166	Destination IP	192.168.1.166
Source Asset Name	N/A	Destination Asset Name	N/A
Source Port	0	Destination Port	0
Pre NAT Source IP		Pre NAT Destination IP	
Pre NAT Source Port	0	Pre NAT Destination Port	0
Post NAT Source IP		Post NAT Destination IP	
Post NAT Source Port	0	Post NAT Destination Port	0
Source IPv6	0:0:0:0:0:0:0:0	Destination IPv6	0:0:0:0:0:0:0:0
Source MAC	00:00:00:00:00:00	Destination MAC	00:00:00:00:00:00
Payload Information			
<div style="display: flex; border: 1px solid #ccc; padding: 2px;"> <span style="border: 1px solid #ccc; padding: 2px 5px;">utf</span> <span style="border: 1px solid #ccc; padding: 2px 5px; margin-left: 5px;">hex</span> <span style="border: 1px solid #ccc; padding: 2px 5px; margin-left: 5px;">base64</span> </div> <input checked="" type="checkbox"/> Wrap Text			
SSH Bruteforce Centos Host    SSH Bruteforce Centos Host			

Εικόνα 25 SSH Bruteforce Centos Host Offence Triggered



## 8. Use Case 5: Critical: Successful Login After BruteForce Attack

Ακολούθως μπορούμε να δημιουργήσουμε έναν ακόμα κανόνα για τους centos Host που έχουμε. Με μια μικρή παραμετροποίηση του use case 4 μπορούμε να εντοπίσουμε ένα Successful Login μετά το bruteforce και να δημιουργήσουμε ένα καινούργιο use case μεγαλύτερης κρισιμότητας. Το σενάριο είναι ότι ο επιτιθέμενος έκανε μία επιτυχημένη bruteforce επίθεση. Για να εντοπίσουμε το παραπάνω θα πρέπει η IP του επιτιθέμενου να έχει αποθηκευτεί σε ένα Reference Set το οποίο θα χρησιμοποιήσουμε στον κανόνα μας ώστε να ενεργοποιηθεί. Το event "systemd-logind: New Session." μας βοηθάει να εντοπίσουμε το επιτυχημένο login μετά την επίθεση.

### Edit Reference Data

---

Name:

Type:

Description:

Time to Live of elements: (YY:MM:DD:hh:mm:ss)

<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="30"/>	<input type="text" value="0"/>
--------------------------------	--------------------------------	--------------------------------	--------------------------------	---------------------------------	--------------------------------

Since first seen  
 Since last seen

Lives Forever

When elements expire:

Log each element in a separate log entry  
 Log elements in one log entry  
 Do not log elements


Εικόνα 26 BruteForce Reference Set Creation

Email  
 Send to Local Syslog  
 Send to Forwarding Destinations  
 Notify  
 Add to a Reference Set












Add the  of the event or flow payload to the Reference Set:

Add to Reference Data  
 Remove from a Reference Set  
 Remove from Reference Data  
 Execute Custom Action

Εικόνα 27 Enable Add to Reference Set Attribute

Event Information			
Event Name	systemd-logind: New session		
Low Level Category	Session Opened		
Event Description	systemd-logind: New session.		
Magnitude		(9)	Relevance 8
Username	centos		
Start Time	Sep 2, 2024, 3:56:24 PM	Storage Time	Sep 2, 2024, 3:56:24 PM
Application (custom)	logind		
Machine Identifier (custom)	N/A		
Process ID (custom)	892		
Process Name (custom)	N/A		
User ID (custom)	N/A		
Domain	Default Domain		


Εικόνα 28 Successful SSH Login Event

Performance	Rule Name	Group	Rule Category
	SMB Scan on the Network was Detected	Anomaly	Custom Rule
	SSH to Honeypot Detected	Anomaly	Custom Rule
	Username Enumeration Detected	Anomaly	Custom Rule
	Critical: Successfull Login After BruteForce Attack	Anomaly	Custom Rule
	SSH Bruteforce Centos Host	Anomaly	Custom Rule
	SMB ANONYMOUS LOGON	Anomaly	Custom Rule
	New Administrator was Added	Anomaly	Custom Rule
	Port Scan Detected	Anomaly	Custom Rule
	SSH Bruteforce was Detected	Anomaly	Custom Rule
	User Load Basic Building Blocks	System	Custom Rule
	First-Time User Access to Critical Asset	Anomaly, Authenti...	Custom Rule
	Load Basic Building Blocks	System	Custom Rule
	Vulnerabilities: Vulnerability Reported by Scanner	Exploit	Custom Rule
	Policy: New Service Discovered	Policy	Custom Rule

**Rule**

Apply Critical: Successfull Login After BruteForce Attack on events which are detected by the Local system and when the event matches QID Number is 4,750,241 and when any of Source IP are contained in any of SSH Bruteforced IPs - IP

Εικόνα 29 Successfull Login After BruteForce Attack Rule

<b>Event Name</b>	Critical: Successful Login After BruteForce Attack		
<b>Low Level Category</b>	Access Denied		
<b>Event Description</b>	Critical: Successful Login After BruteForce Attack		
<b>Magnitude</b>	 (6)	<b>Relevance</b>	6
<b>Username</b>	centos		
<b>Start Time</b>	Sep 2, 2024, 3:56:24 PM	<b>Storage Time</b>	Sep 2, 2024, 3:56:24 PM
<b>Domain</b>	Default Domain		

**Source and Destination Information**

<b>Source IP</b>	192.168.1.166	<b>Destination IP</b>	192.168.1.166
<b>Source Asset Name</b>	N/A	<b>Destination Asset Name</b>	N/A
<b>Source Port</b>	0	<b>Destination Port</b>	0
<b>Pre NAT Source IP</b>		<b>Pre NAT Destination IP</b>	
<b>Pre NAT Source Port</b>	0	<b>Pre NAT Destination Port</b>	0
<b>Post NAT Source IP</b>		<b>Post NAT Destination IP</b>	
<b>Post NAT Source Port</b>	0	<b>Post NAT Destination Port</b>	0
<b>Source IPv6</b>	0:0:0:0:0:0:0:0	<b>Destination IPv6</b>	0:0:0:0:0:0:0:0
<b>Source MAC</b>	00:00:00:00:00:00	<b>Destination MAC</b>	00:00:00:00:00:00

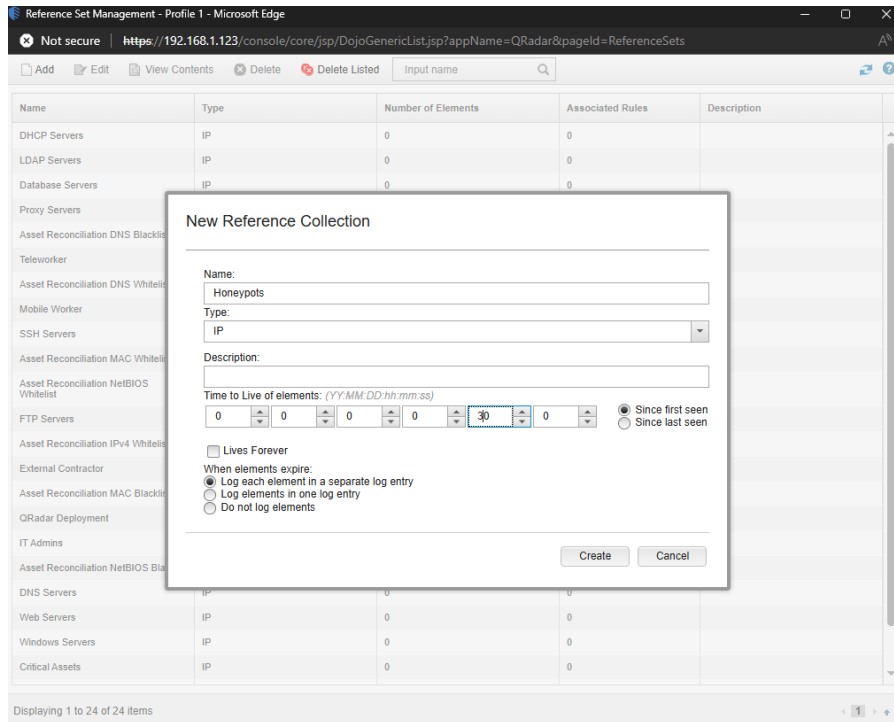
**Payload Information**

<input checked="" type="radio"/> utf <input type="radio"/> hex <input type="radio"/> base64
<input checked="" type="checkbox"/> Wrap Text
Critical: Successful Login After BruteForce Attack    Critical: Successful Login After BruteForce Attack

Εικόνα 30 Successful Login After BruteForce Attack Offence

## 9. Use Case 6: SSH to Honeypot Detected

Ένα honeypot είναι ένας μηχανισμός που σχεδιάζεται για να προσελκύει και να παγιδεύει επιτιθέμενους, προσομοιώνοντας ένα ευάλωτο σύστημα ή δίκτυο. Λειτουργεί ως δόλωμα, επιτρέποντας στις ομάδες ασφαλείας να παρακολουθούν και να αναλύουν κακόβουλες δραστηριότητες χωρίς να διακινδυνεύουν πραγματικά περιουσιακά στοιχεία. Εδώ χρησιμοποιώντας Reference set θα ορίσουμε ποια είναι τα συστήματα που είναι honeypots και έτσι οποιαδήποτε κίνηση προς αυτά είναι άξια διερεύνησης. Θα δημιουργήσουμε το reference set και στο event που εντοπίσαμε θα φτιάξουμε καινούργιο custom property ώστε να χρησιμοποιήσουμε την πόρτα 22 για τον κανόνα μας. Θα μπορούσαμε να φτιάξουμε πολλαπλούς κανόνες χρησιμοποιώντας την πόρτα. Όπως SMB, RDP to Honeypot κλπ ή κάποιον γενικότερο όπως Traffic to Honeypot Detected.



Εικόνα 31 Honeypot Reference Set

Original Filters:  
Log Source is LinuxServer @ centos8 (Clear Filter)

Current Statistics

Start Time	Log Source	Payload
Jul 17 2024 7:35	LinuxServer @ centos8	<86-Jul 17 12:35:26 centos8 sudo(49990): pam_unix(sudo:session): session opened for user root by centos(uid=0)
Jul 17 2024 7:35	LinuxServer @ centos8	<89-Jul 17 12:35:26 centos8 sudo(49990): pam_unix(sudo:session): session closed for user root
Jul 17 2024 7:35	LinuxServer @ centos8	<87-Jul 17 12:35:26 centos8 sudo(49990): pam_systemd(sudo:session): Cannot create session: Already running in a session or user slice
Jul 17 2024 7:35	LinuxServer @ centos8	<85-Jul 17 12:35:26 centos8 sudo(49990): centos: TTY=pts/0; PWD=/home/centos; USER=root; COMMAND=/bin/grep SSH /var/log/messages
Jul 17 2024 7:30	LinuxServer @ centos8	<86-Jul 17 12:30:16 centos8 sudo(49955): pam_unix(sudo:session): session opened for user root by centos(uid=0)
Jul 17 2024 7:30	LinuxServer @ centos8	<89-Jul 17 12:30:16 centos8 sudo(49955): pam_unix(sudo:session): session closed for user root
Jul 17 2024 7:30	LinuxServer @ centos8	<87-Jul 17 12:30:16 centos8 sudo(49955): pam_systemd(sudo:session): Cannot create session: Already running in a session or user slice
Jul 17 2024 7:30	LinuxServer @ centos8	<85-Jul 17 12:30:16 centos8 sudo(49955): centos: TTY=pts/0; PWD=/home/centos; USER=root; COMMAND=/bin/grep SSH /var/log/messages
Jul 17 2024 7:30	LinuxServer @ centos8	<9-Jul 17 12:30:10 centos8 kernel: <b>SSH-LDPS</b> [N=periph] OUT: MAC=08:00:27:12:38:25 20:14:88:20:8a:1c:08:00 SRC=192.168.1.135 DST=192.168.1.166 LEN=60 TOS=0x00 PREC=0x00 TTL=64 ID=7509 DF PROTO=TCP SPT=41824 DPT=
Jul 17 2024 7:24	LinuxServer @ centos8	<87-Jul 17 12:23:43 centos8 sudo(49950): pam_systemd(sudo:session): Cannot create session: Already running in a session or user slice
Jul 17 2024 7:24	LinuxServer @ centos8	<86-Jul 17 12:23:43 centos8 sudo(49950): pam_unix(sudo:session): session opened for user root by centos(uid=0)
Jul 17 2024 7:24	LinuxServer @ centos8	<85-Jul 17 12:23:43 centos8 sudo(49950): centos: TTY=pts/0; PWD=/home/centos; USER=root; COMMAND=/bin/telnetd -cmd -list-all
Jul 17 2024 7:24	LinuxServer @ centos8	<86-Jul 17 12:23:43 centos8 sudo(49950): pam_unix(sudo:session): session closed for user root

Εικόνα 32 Honeypot SSH Centos Event

**Test Field**

```
<@=3= 17 15:59:42 centos@ kernel: SSH-LOG-IN: IN=ensp0e3 OUT= MAC=08:00:27:f2:38:a5:20:1e:88:c0b:9e:1c:08:00 SRC=192.168.1.135 DST=192.168.1.166 LEN=60 TOS=0x10 PREC=0x00 TTL=64 ID=65424 DF PROTO=TCP SPT=47910 DPT=22 WINDOW=32120 RES=0x00 SYN (SEQ=)
```

**Property Definition**

Existing Property:

New Property:  Please enter a property name.

Enable for use in Rules, Forwarding Profiles and Search Indexing:

Field Type:

Description:

**Property Expression Definition**

Enabled:

Selection

Log Source Type:

Log Source:

Event Name:  Kernel Message

High Level Category:

Low Level Category:

Category:

Extraction using:

Regex:

Capture Group:

Εικόνα 33 SSH custom property regex

<b>Event Name</b>	Kernel Message		
<b>Low Level Category</b>	Messages		
<b>Event Description</b>	This event was recognized as an kernel log message		
<b>Magnitude</b>	<div style="width: 100%; height: 10px; background: linear-gradient(to right, yellow, orange, red);"></div>	(4)	Relevance 6
<b>Username</b>	N/A		
<b>Start Time</b>	Jul 17, 2024, 11:00:00 PM	<b>Storage Time</b>	Jul 17, 2024, 11:00:00 PM
<b>Application (custom)</b>	N/A		
<b>CentosPort (custom)</b>	22		
<b>Machine Identifier (custom)</b>	N/A		
<b>Process ID (custom)</b>	N/A		
<b>Process Name (custom)</b>	N/A		
<b>User ID (custom)</b>	N/A		
<b>Domain</b>	Default Domain		
<b>Source and Destination Information</b>			
<b>Source IP</b>	192.168.1.166	<b>Destination IP</b>	192.168.1.166
<b>Source Asset Name</b>	N/A	<b>Destination Asset Name</b>	N/A
<b>Source Port</b>	0	<b>Destination Port</b>	0
<b>Pre NAT Source IP</b>		<b>Pre NAT Destination IP</b>	
<b>Pre NAT Source Port</b>	0	<b>Pre NAT Destination Port</b>	0
<b>Post NAT Source IP</b>		<b>Post NAT Destination IP</b>	
<b>Post NAT Source Port</b>	0	<b>Post NAT Destination Port</b>	0
<b>Source IPv6</b>	0:0:0:0:0:0:0:0	<b>Destination IPv6</b>	0:0:0:0:0:0:0:0
<b>Source MAC</b>	00:00:00:00:00:00	<b>Destination MAC</b>	00:00:00:00:00:00
<b>Payload Information</b>			
<input checked="" type="checkbox"/> utf	<input type="checkbox"/> hex	<input type="checkbox"/> base64	
<input checked="" type="checkbox"/> Wrap Text			

Εικόνα 34 SSH custom property regex 2

Which tests do you wish to perform on incoming events?

Test Group  ▼

[Export as Building Block](#)

refe

- + when any of these event properties are contained in any of these reference set(s)
- + when any of these event properties is the key and any of these event properties is the value in any of these reference maps
- + when any of these event properties is the key and any of these event properties is the value in any of these reference map of sets
- + when any of these event properties is the key of the first map and any of these event properties is the key of the second map and any of these event properties is the value in any of these reference map of maps
- + when Reference Table Key data matches any/all selected event properties and selected reference table column Select operator the value of selected event property

Rule (Click on an underlined value to edit it)  
 Invalid tests are highlighted and must be fixed before rule can be saved.

Apply  on events which are detected by the  system

- ⊖ ⊕ and when the event matches QID Number is 44,251,261
- ⊖ ⊕ and when the event matches CentosPort (custom) is any of 22
- ⊖ ⊕ and when any of Source IP are contained in any of Honeypots - IP

Please select any groups you would like this rule to be a member of:

- Anomaly
- Asset Reconciliation Exclusion
- Authentication
- Botnet
- Category Definitions

Notes (Enter your notes about this rule)

Honeypot device is used to trap attackers. Anyone contacting the specific host is considered suspicious

Performance Analysis

This rule has not yet had a detailed analysis.

Εικόνα 35 SSH to Honeypot Rule

Event Information			
Event Name	SSH to Honeypot Detected		
Low Level Category	Access Denied		
Event Description	SSH to Honeypot Detected		
Magnitude	<div style="width: 100%; height: 10px; background: linear-gradient(to right, yellow, orange, red);"></div>	(6)	Relevance 6
Severity			
Username	N/A		
Start Time	Jul 18, 2024, 12:31:01 AM	Storage Time	Jul 18, 2024, 12:31:01 AM
Log Source Time			
CRE Description (custom)	SSH to Honeypot Detected		
CRE Name (custom)	SSH to Honeypot Detected		
Domain	Default Domain		
Source and Destination Information			
Source IP	192.168.1.166	Destination IP	192.168.1.166
Source Asset Name	N/A	Destination Asset Name	N/A
Source Port	0	Destination Port	0
Pre NAT Source IP		Pre NAT Destination IP	
Pre NAT Source Port	0	Pre NAT Destination Port	0
Post NAT Source IP		Post NAT Destination IP	
Post NAT Source Port	0	Post NAT Destination Port	0
Source IPv6	0:0:0:0:0:0:0:0	Destination IPv6	0:0:0:0:0:0:0:0
Source MAC	00:00:00:00:00:00	Destination MAC	00:00:00:00:00:00
Payload Information			
Encoding	<input checked="" type="radio"/> utf <input type="radio"/> hex <input type="radio"/> base64		
Wrap Text	<input checked="" type="checkbox"/>		
Raw	SSH to Honeypot Detected		
Decoded	SSH to Honeypot Detected		


Εικόνα 36 SSH to Honeypot Offense

## 10. Use Case 7: Username Enumeration Detected

Ακολουθώντας την προσπάθεια μας να θωρακίσουμε το δίκτυο από κακόβουλες επιθέσεις θα δημιουργήσουμε κανόνα για τον εντοπισμό του username enumeration. Την προσπάθεια ενός κακόβουλου δηλαδή χρησιμοποιώντας πολλαπλά ονόματα χρήστη να αποκτήσει πρόσβαση σε λογαριασμούς με τον ίδιο κωδικό.

Bad Username	LinuxServer @ centos8	1	Sep 16, 2024, 1:44:...	SSH Login Failed	192.168.1.135	0	192.168.1.166
Failed SSH Login Method	LinuxServer @ centos8	1	Sep 16, 2024, 1:44:...	Information	192.168.1.135	40085	192.168.1.166
Bad Username	LinuxServer @ centos8	1	Sep 16, 2024, 1:44:...	SSH Login Failed	192.168.1.135	0	192.168.1.166
Failed SSH Login Method	LinuxServer @ centos8	1	Sep 16, 2024, 1:44:...	Information	192.168.1.135	35881	192.168.1.166
Failed SSH Login Method	LinuxServer @ centos8	1	Sep 16, 2024, 1:44:...	Information	192.168.1.135	38643	192.168.1.166
Failed SSH Login Method	LinuxServer @ centos8	1	Sep 16, 2024, 1:44:...	Information	192.168.1.135	37269	192.168.1.166
Bad Username	LinuxServer @ centos8	1	Sep 16, 2024, 1:44:...	SSH Login Failed	192.168.1.135	0	192.168.1.166
Bad Username	LinuxServer @ centos8	1	Sep 16, 2024, 1:44:...	SSH Login Failed	192.168.1.135	0	192.168.1.166
Failed SSH Login Method	LinuxServer @ centos8	1	Sep 16, 2024, 1:44:...	Information	192.168.1.135	46023	192.168.1.166
Multiple Login Failures to the Same Destination	Custom Rule Engine-8 :: Logger	1	Sep 16, 2024, 1:44:...	Remote Access Login Failed	192.168.1.135	0	192.168.1.166
Multiple Login Failures from the Same Source	Custom Rule Engine-8 :: Logger	1	Sep 16, 2024, 1:44:...	Misc Login Failed	192.168.1.135	0	192.168.1.166
Bad Username	LinuxServer @ centos8	1	Sep 16, 2024, 1:44:...	SSH Login Failed	192.168.1.135	0	192.168.1.166
Bad Username	LinuxServer @ centos8	1	Sep 16, 2024, 1:44:...	SSH Login Failed	192.168.1.135	0	192.168.1.166

Εικόνα 37 Username Enumeration Logs

Event Information	
<b>Event Name</b>	Failed SSH Login Method
<b>Low Level Category</b>	Information
<b>Event Description</b>	Failed SSH Login Method
<b>Magnitude</b>	
<b>Username</b>	tech
<b>Start Time</b>	Sep 16, 2024, 1:44:22 PM
<b>Application (custom)</b>	sshd
<b>Machine Identifier (custom)</b>	N/A
<b>Process ID (custom)</b>	1649
<b>Process Name (custom)</b>	N/A
<b>User ID (custom)</b>	N/A
<b>Domain</b>	Default Domain


Εικόνα 38 Event used for Rule

**Rule**

Apply Username Enumeration Detected on events which are detected by the Local system and when the event matches QID Number is 44,251,216 and when at least 10 events are seen with the same Source IP, Destination IP and different Username in 1 minutes

Εικόνα 39 Username Enumeration Rule

**Event Information**

<b>Event Name</b>	Username Enumeration Detected
<b>Low Level Category</b>	Access Denied
<b>Event Description</b>	Username Enumeration Detected
<b>Magnitude</b>	
<b>Username</b>	supervisor
<b>Start Time</b>	Sep 16, 2024, 1:44:22 PM
<b>Domain</b>	Default Domain

**Source and Destination Information**

<b>Source IP</b>	192.168.1.135
<b>Source Asset Name</b>	N/A
<b>Source Port</b>	38643
<b>Pre NAT Source IP</b>	

Εικόνα 40 Username Enumeration Offence



## 11. Use Case 8: Port Scan Detected

Ο κανόνας που δημιουργήσαμε για την ανίχνευση του Port Scan λειτουργεί με βάση την καταγραφή 100 ή περισσότερων συμβάντων από την ίδια διεύθυνση πηγής (Source IP) προς διαφορετικές θύρες προορισμού (Destination Ports) εντός δύο λεπτών. Αυτός ο κανόνας στοχεύει στην ανίχνευση πιθανής κακόβουλης δραστηριότητα σε windows περιβάλλοντα, όπως είναι η σάρωση θυρών (port scanning), που χρησιμοποιείται συχνά από επιτιθέμενους για να εντοπίσουν ανοιχτές θύρες και υπηρεσίες σε ένα σύστημα. Όταν πληρούνται αυτά τα κριτήρια, το σύστημα ενεργοποιεί το συμβάν "Port Scan Detected", το οποίο σηματοδοτεί ότι ενδέχεται να υπάρχει ύποπτη δραστηριότητα δικτύου.


Με την ενεργοποίηση του κανόνα, η τοπική ομάδα ασφαλείας μπορεί να λάβει ειδοποίηση και να προχωρήσει σε περαιτέρω έρευνα ή άμεση αντίδραση. Η έγκαιρη ανίχνευση τέτοιων μοτίβων επιτρέπει την αναχαίτιση επιθέσεων πριν αυτές κλιμακωθούν, ενώ παράλληλα παρέχει πολύτιμες πληροφορίες για την κίνηση στο δίκτυο. Σε περίπτωση ανάγκης, μπορεί να ληφθούν επιπρόσθετα μέτρα, όπως ο αποκλεισμός της ύποπτης διεύθυνσης IP ή η εντατικοποίηση της παρακολούθησης.

```
(root@Chillikos)-[~/home/chill/Downloads]
# nmap -T4 192.168.1.48 -Pn
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-16 11:03 EDT
Nmap scan report for Beast.home (192.168.1.48)
Host is up (0.0063s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE
135/tcp   open  msrpc
445/tcp   open  microsoft-ds
6881/tcp  open  bittorrent-tracker
MAC Address: B0:48:7A:BF:30:E5 (TP-Link Technologies)
Nmap done: 1 IP address (1 host up) scanned in 4.70 seconds
```

Εικόνα 41 Nmap Scan to trigger logs

Time	Source IP	Destination IP	Event	Source Port	Destination Port	Direction	Protocol	Service	Severity	Count
1900	192.168.1.135	192.168.1.48	Multiple (2)	Multiple (2)	Multiple (2)	Out	TCP	None	None	5
135	192.168.1.135	192.168.1.48	Success Audit: The Windows Filtering Platform has allowed a connection	Beast @ 192.168.1.48	Multiple (2)	In	TCP	None	None	3
2095	192.168.1.135	192.168.1.48	Multiple (2)	Multiple (2)	Multiple (2)	Out	TCP	None	None	5
646	192.168.1.135	192.168.1.48	Multiple (2)	Multiple (2)	Multiple (2)	Out	TCP	None	None	5
49152	192.168.1.135	192.168.1.48	Failure Audit: The Windows Filtering Platform blocked a packet	Beast @ 192.168.1.48	Access Denied	In	TCP	None	None	5
32768	192.168.1.135	192.168.1.48	Failure Audit: The Windows Filtering Platform blocked a packet	Beast @ 192.168.1.48	Access Denied	In	TCP	None	None	5
32769	192.168.1.135	192.168.1.48	Failure Audit: The Windows Filtering Platform blocked a packet	Beast @ 192.168.1.48	Access Denied	In	TCP	None	None	5
49153	192.168.1.135	192.168.1.48	Failure Audit: The Windows Filtering Platform blocked a packet	Beast @ 192.168.1.48	Access Denied	In	TCP	None	None	5
49154	192.168.1.135	192.168.1.48	Failure Audit: The Windows Filtering Platform blocked a packet	Beast @ 192.168.1.48	Access Denied	In	TCP	None	None	5
32770	192.168.1.135	192.168.1.48	Failure Audit: The Windows Filtering Platform blocked a packet	Beast @ 192.168.1.48	Access Denied	In	TCP	None	None	5
49155	192.168.1.135	192.168.1.48	Failure Audit: The Windows Filtering Platform blocked a packet	Beast @ 192.168.1.48	Access Denied	In	TCP	None	None	5
32771	192.168.1.135	192.168.1.48	Failure Audit: The Windows Filtering Platform blocked a packet	Beast @ 192.168.1.48	Access Denied	In	TCP	None	None	5
32772	192.168.1.135	192.168.1.48	Failure Audit: The Windows Filtering Platform blocked a packet	Beast @ 192.168.1.48	Access Denied	In	TCP	None	None	5
49156	192.168.1.135	192.168.1.48	Failure Audit: The Windows Filtering Platform blocked a packet	Beast @ 192.168.1.48	Access Denied	In	TCP	None	None	5
49157	192.168.1.135	192.168.1.48	Failure Audit: The Windows Filtering Platform blocked a packet	Beast @ 192.168.1.48	Access Denied	In	TCP	None	None	5
32773	192.168.1.135	192.168.1.48	Failure Audit: The Windows Filtering Platform blocked a packet	Beast @ 192.168.1.48	Access Denied	In	TCP	None	None	5
32774	192.168.1.135	192.168.1.48	Failure Audit: The Windows Filtering Platform blocked a packet	Beast @ 192.168.1.48	Access Denied	In	TCP	None	None	5
49158	192.168.1.135	192.168.1.48	Failure Audit: The Windows Filtering Platform blocked a packet	Beast @ 192.168.1.48	Access Denied	In	TCP	None	None	5
32775	192.168.1.135	192.168.1.48	Failure Audit: The Windows Filtering Platform blocked a packet	Beast @ 192.168.1.48	Access Denied	In	TCP	None	None	5
49161	192.168.1.135	192.168.1.48	Failure Audit: The Windows Filtering Platform blocked a packet	Beast @ 192.168.1.48	Access Denied	In	TCP	None	None	5
32777	192.168.1.135	192.168.1.48	Failure Audit: The Windows Filtering Platform blocked a packet	Beast @ 192.168.1.48	Access Denied	In	TCP	None	None	5
32778	192.168.1.135	192.168.1.48	Failure Audit: The Windows Filtering Platform blocked a packet	Beast @ 192.168.1.48	Access Denied	In	TCP	None	None	5
32779	192.168.1.135	192.168.1.48	Failure Audit: The Windows Filtering Platform blocked a packet	Beast @ 192.168.1.48	Access Denied	In	TCP	None	None	5
32780	192.168.1.135	192.168.1.48	Failure Audit: The Windows Filtering Platform blocked a packet	Beast @ 192.168.1.48	Access Denied	In	TCP	None	None	5
32781	192.168.1.135	192.168.1.48	Failure Audit: The Windows Filtering Platform blocked a packet	Beast @ 192.168.1.48	Access Denied	In	TCP	None	None	5
32782	192.168.1.135	192.168.1.48	Failure Audit: The Windows Filtering Platform blocked a packet	Beast @ 192.168.1.48	Access Denied	In	TCP	None	None	5
49167	192.168.1.135	192.168.1.48	Failure Audit: The Windows Filtering Platform blocked a packet	Beast @ 192.168.1.48	Access Denied	In	TCP	None	None	5
32783	192.168.1.135	192.168.1.48	Failure Audit: The Windows Filtering Platform blocked a packet	Beast @ 192.168.1.48	Access Denied	In	TCP	None	None	5
32784	192.168.1.135	192.168.1.48	Failure Audit: The Windows Filtering Platform blocked a packet	Beast @ 192.168.1.48	Access Denied	In	TCP	None	None	5
32785	192.168.1.135	192.168.1.48	Failure Audit: The Windows Filtering Platform blocked a packet	Beast @ 192.168.1.48	Access Denied	In	TCP	None	None	5
18176	192.168.1.135	192.168.1.48	Failure Audit: The Windows Filtering Platform blocked a packet	Beast @ 192.168.1.48	Access Denied	In	TCP	None	None	5
49400	192.168.1.135	192.168.1.48	Failure Audit: The Windows Filtering Platform blocked a packet	Beast @ 192.168.1.48	Access Denied	In	TCP	None	None	5
18113	192.168.1.135	192.168.1.48	Failure Audit: The Windows Filtering Platform blocked a packet	Beast @ 192.168.1.48	Access Denied	In	TCP	None	None	5
18080	192.168.1.135	192.168.1.48	Failure Audit: The Windows Filtering Platform blocked a packet	Beast @ 192.168.1.48	Access Denied	In	TCP	None	None	5
18018	192.168.1.135	192.168.1.48	Failure Audit: The Windows Filtering Platform blocked a packet	Beast @ 192.168.1.48	Access Denied	In	TCP	None	None	5
18012	192.168.1.135	192.168.1.48	Failure Audit: The Windows Filtering Platform blocked a packet	Beast @ 192.168.1.48	Access Denied	In	TCP	None	None	5
18001	192.168.1.135	192.168.1.48	Failure Audit: The Windows Filtering Platform blocked a packet	Beast @ 192.168.1.48	Access Denied	In	TCP	None	None	5


Εικόνα 42 Log Detection

<b>Event Name</b>	Failure Audit: The Windows Filtering Platform blocked a packet		
<b>Low Level Category</b>	Access Denied		
<b>Event Description</b>	Failure Audit: The Windows Filtering Platform blocked a packet.		
<b>Magnitude</b>		(5)	<b>Relevance</b> 6
<b>Username</b>	N/A		
<b>Start Time</b>	Sep 19, 2024, 4:50:59 PM	<b>Storage Time</b>	Sep 19, 2024
<b>Account Name (custom)</b>	N/A		
<b>Event ID (custom)</b>	5152		
<b>Group ID (custom)</b>	N/A		
<b>Logon Type (custom)</b>	N/A		
<b>Object Type (custom)</b>	N/A		
<b>Source Workstation (custom)</b>	N/A		
<b>User Domain (custom)</b>	N/A		
<b>Domain</b>	Default Domain		

**Source and Destination Information**

<b>Source IP</b>	192.168.1.135
<b>Source Asset Name</b>	N/A
<b>Source Port</b>	50882

Εικόνα 43 Event 5152

<b>Event Name</b>	Success Audit: The Windows Filtering Platform has allowed a connection		
<b>Low Level Category</b>	Access Permitted		
<b>Event Description</b>	Success Audit: The Windows Filtering Platform has allowed a connection.		
<b>Magnitude</b>	 (3)	<b>Relevance</b>	6
<b>Username</b>	N/A		
<b>Start Time</b>	Sep 19, 2024, 4:50:53 PM	<b>Storage Time</b>	Sep 19, 2024, 4:50:53 PM
<b>Account Name (custom)</b>	N/A		
<b>Event ID (custom)</b>	5156		
<b>Group ID (custom)</b>	N/A		
<b>Logon Type (custom)</b>	N/A		
<b>Object Type (custom)</b>	N/A		
<b>Source Workstation (custom)</b>	N/A		

Εικόνα 44 Event 5156

**Rule**


Apply Port Scan BuildingBlock on events which are detected by the Local system and when the event matches Event ID (custom) is any of [5152 or 5156]

Εικόνα 45 Port Scan Rule Building Block

**Rule**

Apply Port Scan Detected on events which are detected by the Local system and when Port Scan BuildingBlock match at least 100 times with the same Source IP and different Destination Port in 2 minutes

Εικόνα 46 Port Scan Rule

Event Name	Port Scan Event		
Low Level Category	Access Denied		
Event Description	Port Scan Event was detected		
Magnitude	 (6)	Relevance	6
Severity			
Username	N/A		
Start Time	Sep 19, 2024, 4:50:53 PM	Storage Time	Sep 19, 2024, 4:50:53 PM
Domain	Default Domain		

**Source and Destination Information**

Source IP	192.168.1.135	Destination IP	192.168.1.48
Source Asset Name	N/A	Destination Asset Name	N/A
Source Port	50880	Destination Port	10243
Pre NAT Source IP		Pre NAT Destination IP	
Pre NAT Source Port	0	Pre NAT Destination Port	0
Post NAT Source IP		Post NAT Destination IP	
Post NAT Source Port	0	Post NAT Destination Port	0
Source IPv6	0:0:0:0:0:0:0:0	Destination IPv6	0:0:0:0:0:0:0:0
Source MAC	00:00:00:00:00:00	Destination MAC	00:00:00:00:00:00

**Εικόνα 47 Port Scan Triggered Offence**

**12. Use Case 9: SMB Scan on the Network was Detected**

Ο παραπάνω κανόνας θα συνδυασει καταγραφές από windows και centos hosts στην προσπάθεια να εντοπίσει κάποιο ενδεχόμενο SMB scan στο δικτυο. Αρχικά θα ξεκινήσουμε με τον εντοπισμό των καταγραφών που μας δείχνουν πιθανή επικοινωνία με την πόρτα 445. Οι windows με τους centos host παράγουν διαφορετικά event οπότε θα πρέπει να τα εντοπίσουμε ξεχωριστά. Ακολούθως θα φτιάξουμε για το κάθε περιβάλλον από ένα building block και θα τα συνδυάσουμε στον κανόνα μας.

```
Nmap scan report for wlan0-30.home (192.168.1.102)
Host is up (0.0056s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
5668/tcp  open  irc
MAC Address: A0:92:08:BE:E9:43 (Tuya Smart)

Nmap scan report for 192.168.1.123
Host is up (0.0089s latency).
Not shown: 929 filtered tcp ports (no-response), 67 filtered tcp ports (port-unreach)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    closed http
443/tcp   open  https
514/tcp   open  shell
MAC Address: B0:48:7A:BF:30:E5 (TP-Link Technologies)

Nmap scan report for AndriotisPC.home (192.168.1.140)
Host is up (0.0085s latency).
Not shown: 995 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp   filtered msrpc
139/tcp   filtered netbios-ssn
445/tcp   filtered microsoft-ds
3389/tcp  filtered ms-wbt-server
5357/tcp  filtered wsddapi
MAC Address: 20:1E:88:CB:9A:21 (Intel Corporate)

Nmap scan report for centos8.home (192.168.1.166)
Host is up (0.069s latency).
Not shown: 913 filtered tcp ports (no-response), 83 filtered tcp ports (admin-prohibited)
PORT      STATE SERVICE
22/tcp    open  ssh
139/tcp   closed netbios-ssn
445/tcp   closed microsoft-ds
9090/tcp  closed zeus-admin
MAC Address: D8:C0:A6:AA:0E:EF (AzureWave Technology)

Nmap scan report for wlan0.home (192.168.1.180)
Host is up (0.0060s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
5668/tcp  open  irc
MAC Address: A0:92:08:BE:EC:B6 (Tuya Smart)

Nmap scan report for LAPTOP-721LS6VB.home (192.168.1.246)
Host is up (0.10s latency).
All 1000 scanned ports on LAPTOP-721LS6VB.home (192.168.1.246) are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: D8:C0:A6:AA:0E:EF (AzureWave Technology)

Nmap scan report for Chillikos.home (192.168.1.135)
Host is up (0.0000010s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
7070/tcp  open  realserver
```

**Εικόνα 48 Scan Including SMB port**

Failure Audit: The Windows Filtering Platform blocked a packet	Beast @ 192.168.1.48	2 Sep 19, 2024, 6:26...	Access Denied	192.168.1.135	44779	192.168.1.48	3404
Failure Audit: The Windows Filtering Platform blocked a packet	Beast @ 192.168.1.48	2 Sep 19, 2024, 6:26...	Access Denied	192.168.1.135	44779	192.168.1.48	55555
Failure Audit: The Windows Filtering Platform blocked a packet	Beast @ 192.168.1.48	2 Sep 19, 2024, 6:26...	Access Denied	192.168.1.135	44779	192.168.1.48	1080
Failure Audit: The Windows Filtering Platform blocked a packet	Beast @ 192.168.1.48	2 Sep 19, 2024, 6:26...	Access Denied	192.168.1.135	44779	192.168.1.48	1236
Failure Audit: The Windows Filtering Platform blocked a packet	Beast @ 192.168.1.48	2 Sep 19, 2024, 6:26...	Access Denied	192.168.1.135	44779	192.168.1.48	7443
Failure Audit: The Windows Filtering Platform blocked a packet	Beast @ 192.168.1.48	2 Sep 19, 2024, 6:26...	Access Denied	192.168.1.135	44779	192.168.1.48	2005
Success Audit: The Windows Filtering Platform has allowed a c...	Beast @ 192.168.1.48	1 Sep 19, 2024, 6:26...	Access Permitted	192.168.1.135	44852	192.168.1.48	445
Failure Audit: The Windows Filtering Platform blocked a packet	Beast @ 192.168.1.48	2 Sep 19, 2024, 6:26...	Access Denied	192.168.1.135	44779	192.168.1.48	16993
Failure Audit: The Windows Filtering Platform blocked a packet	Beast @ 192.168.1.48	2 Sep 19, 2024, 6:26...	Access Denied	192.168.1.135	44779	192.168.1.48	20222
Failure Audit: The Windows Filtering Platform blocked a packet	Beast @ 192.168.1.48	2 Sep 19, 2024, 6:26...	Access Denied	192.168.1.135	44779	192.168.1.48	1088
Failure Audit: The Windows Filtering Platform blocked a packet	Beast @ 192.168.1.48	2 Sep 19, 2024, 6:26...	Access Denied	192.168.1.135	44779	192.168.1.48	5405
Failure Audit: The Windows Filtering Platform blocked a packet	Beast @ 192.168.1.48	2 Sep 19, 2024, 6:26...	Access Denied	192.168.1.135	44779	192.168.1.48	13
Failure Audit: The Windows Filtering Platform blocked a packet	Beast @ 192.168.1.48	2 Sep 19, 2024, 6:26...	Access Denied	192.168.1.135	44779	192.168.1.48	9929
Failure Audit: The Windows Filtering Platform blocked a packet	Beast @ 192.168.1.48	2 Sep 19, 2024, 6:26...	Access Denied	192.168.1.135	44779	192.168.1.48	8082
Failure Audit: The Windows Filtering Platform blocked a packet	Beast @ 192.168.1.48	2 Sep 19, 2024, 6:26...	Access Denied	192.168.1.135	44779	192.168.1.48	6101
Failure Audit: The Windows Filtering Platform blocked a packet	Beast @ 192.168.1.48	2 Sep 19, 2024, 6:26...	Access Denied	192.168.1.135	44779	192.168.1.48	8022
Failure Audit: The Windows Filtering Platform blocked a packet	Beast @ 192.168.1.48	2 Sep 19, 2024, 6:26...	Access Denied	192.168.1.135	44779	192.168.1.48	1029
Failure Audit: The Windows Filtering Platform blocked a packet	Beast @ 192.168.1.48	2 Sep 19, 2024, 6:26...	Access Denied	192.168.1.135	44779	192.168.1.48	9999

**Εικόνα 49 Events Detected From Windows Host**

Event Information			
Event Name	Success Audit: The Windows Filtering Platform has allowed a connection		
Low Level Category	Access Permitted		
Event Description	Success Audit: The Windows Filtering Platform has allowed a connection.		
Magnitude		(3) Relevance	6 Severity
Username	N/A		
Start Time	Sep 19, 2024, 6:26:17 PM	Storage Time	Sep 19, 2024, 6:26:17 PM Log Source T
Account Name (custom)	N/A		
Event ID (custom)	5156		
Group ID (custom)	N/A		
Logon Type (custom)	N/A		
Object Type (custom)	N/A		
Source Workstation (custom)	N/A		
User Domain (custom)	N/A		
Domain	Default Domain		

Source and Destination Information			
Source IP	192.168.1.135	Destination IP	192.168.1.48
Source Asset Name	N/A	Destination Asset Name	N/A
Source Port	44852	Destination Port	445

**Εικόνα 50 Windows Event Used**

Kernel Message	LinuxServer @ centos8	1	Sep 19, 2024, 6:25:...	Messages	192.168.1.166	0	192.168.1.1...
Kernel Message	LinuxServer @ centos8	1	Sep 19, 2024, 6:25:...	Messages	192.168.1.166	0	192.168.1.1...
Kernel Message	LinuxServer @ centos8	1	Sep 19, 2024, 6:23:...	Messages	192.168.1.166	0	192.168.1.1...
Kernel Message	LinuxServer @ centos8	5	Sep 19, 2024, 6:22:...	Messages	192.168.1.166	0	192.168.1.1...
Kernel Message	LinuxServer @ centos8	1	Sep 19, 2024, 6:20:...	Messages	192.168.1.166	0	192.168.1.1...
Kernel Message	LinuxServer @ centos8	1	Sep 19, 2024, 6:16:...	Messages	192.168.1.166	0	192.168.1.1...
Kernel Message	LinuxServer @ centos8	1	Sep 19, 2024, 6:16:...	Messages	192.168.1.166	0	192.168.1.1...
Kernel Message	LinuxServer @ centos8	3	Sep 19, 2024, 6:16:...	Messages	192.168.1.166	0	192.168.1.1...
Kernel Message	LinuxServer @ centos8	1	Sep 19, 2024, 6:11:0...	Messages	192.168.1.166	0	192.168.1.1...

**Εικόνα 51 Centos Logs**

Event Information			
Event Name	Kernel Message		
Low Level Category	Messages		
Event Description	This event was recognized as an kernel log message		
Magnitude		(4) Relevance	6 Severity 1 Credib
Username	N/A		
Start Time	Sep 19, 2024, 6:11:05 PM	Storage Time	Sep 19, 2024, 6:11:05 PM Log Source Time Sep 19, 2024, 11:10:
Application (custom)	N/A		
CentosPort (custom)	445		
Machine Identifier (custom)	N/A		
Process ID (custom)	N/A		
Process Name (custom)	N/A		
User ID (custom)	N/A		
Domain	Default Domain		

Source and Destination Information			
Source IP	192.168.1.166	Destination IP	192.168.1.166
Source Asset Name	N/A	Destination Asset Name	N/A

**Εικόνα 52 Centos 445 Event**

Apply Windows SMB Building Block on events which are detected by the Local system and when the event matches QID Number is 5,001,114 and when the event matches Destination Port is 445


**Εικόνα 53 Windows Building Block**

Apply Centos SMB Building Block on events which are detected by the Local system and when the event matches QID Number is 44,251,261 and when the event matches CentosPort (custom) is any of 445

**Εικόνα 54 Centos Building Block**

Apply SMB Scan on the Network was Detected on events which are detected by the Local system and when Centos SMB Building Block, Windows SMB Building Block match at least 2 times with the same Source IP in 1 minutes

**Εικόνα 55 SMB Scan Rule**

<b>Event Name</b>	SMB Scan Detected
<b>Low Level Category</b>	Access Denied
<b>Event Description</b>	SMB Scan Detected
<b>Magnitude</b>	
<b>Username</b>	N/A
<b>Start Time</b>	Sep 19, 2024, 6:22:43 PM
<b>Domain</b>	Default Domain

**Source and Destination Information**

<b>Source IP</b>	192.168.1.166
<b>Source Asset Name</b>	N/A
<b>Source Port</b>	0
<b>Pre NAT Source IP</b>	
<b>Pre NAT Source Port</b>	0
<b>Post NAT Source IP</b>	
<b>Post NAT Source Port</b>	0
<b>Source IPv6</b>	0:0:0:0:0:0:0:0
<b>Source MAC</b>	00:00:00:00:00:00

**Εικόνα 56 SMB Scan Offence**

## ΣΥΜΠΕΡΑΣΜΑΤΑ

Η ολοκλήρωση του έργου έδειξε ότι η χρήση του IBM QRadar ήταν εξαιρετικά αποτελεσματική για την ανάλυση των logs από συστήματα Windows και CentOS, προσφέροντας αξιόπιστη ανίχνευση απειλών, όπως brute force επιθέσεις, ανώνυμες συνδέσεις SMB και σάρωση θυρών. Η εφαρμογή των "use cases" ενίσχυσε σημαντικά την ασφάλεια του οργανισμού, επιτρέποντας έγκαιρη ανίχνευση και αντιμετώπιση ύποπτων δραστηριοτήτων. Επιπλέον, η διαλειτουργικότητα μεταξύ των δύο πλατφορμών απέδειξε ότι το QRadar μπορεί να παρέχει ολοκληρωμένη προστασία σε διάφορα περιβάλλοντα, ενισχύοντας τη συνολική ασφάλεια του δικτύου.

Με τους μηχανισμούς ανίχνευσης να αυτοματοποιούν τη διαδικασία, ο χρόνος αντίδρασης μειώθηκε αισθητά, ενώ η ακρίβεια στην ανίχνευση πραγματικών απειλών αυξήθηκε. Η ικανότητα του QRadar να εντοπίζει επιτυχείς συνδέσεις μετά από brute force επιθέσεις, καθώς και άλλες ύποπτες δραστηριότητες, έδειξε ότι το σύστημα λειτουργεί προληπτικά, θωρακίζοντας τους οργανισμούς από εξελισσόμενες απειλές. Το έργο παρείχε σημαντικές γνώσεις για τη συνεχή βελτιστοποίηση των μηχανισμών ανίχνευσης, εξασφαλίζοντας ότι η ασφάλεια μπορεί να προσαρμόζεται στις νέες κυβερνοαπειλές, ενισχύοντας την ανθεκτικότητα και την ασφάλεια των συστημάτων μακροπρόθεσμα.



**ΠΙΝΑΚΑΣ ΟΡΟΛΟΓΙΑΣ**

<b>Ξενόγλωσσος όρος</b>	<b>Ελληνικός Όρος</b>
Firewall	Τείχος προστασίας
Standalone configuration	Αυτόνομη ρύθμιση
Managed configuration	Διαχειριζόμενη ρύθμιση
WinCollect	WinCollect
Host	Φιλοξενούμενος
Intergration	Ενοποίηση
Service	Υπηρεσία
Troubleshoot	Αντιμετώπιση προβλημάτων
Error	Σφάλμα
Administrator	Διαχειριστές
Admin privileges	Δικαιώματα διαχειριστή
Domain	Τομέας
Local administrator	Τοπικός διαχειριστής
Event	Γεγονός
Group Name	Όνομα ομάδας
Anonymous Logon	Ανώνυμη σύνδεση
Event ID	ID Γεγονότος
Process Name	Όνομα διεργασίας
Building Block	Μπλοκ Δόμησης
Pattern	Μοτίβο
Offence	Επίθεση
Password Check Failed	Αποτυχία ελέγχου κωδικού πρόσβασης
Custom rule engine	Μηχανισμός προσαρμοσμένων κανόνων
Use case	
Successful Login	Επιτυχής σύνδεση
Reference Set	Σύνολο αναφορών
New Session	Νέα συνεδρία
Login	Σύνδεση
Custom property	Προσαρμοσμένη ιδιότητα
Traffic	Κυκλοφορία
Hoeynot detected	Ανίχνευση honeypot
Username enumeration	Καταμέτρηση ονομάτων χρήστη
Port Scan	Σάρωση θυρών
Source IP	Διεύθυνση IP προέλευσης
Destination Ports	Θύρες προορισμού
Port Scanning	Σάρωση θυρών
Port Scan Detected	Ανίχνευση σάρωσης θυρών

**ΣΥΝΤΜΗΣΕΙΣ – ΑΡΚΤΙΚΟΛΕΞΑ – ΑΚΡΩΝΥΜΙΑ**

SOC	Security Operations Center
IBM	International Business Machines Corporation
ISO	International Organization for Standardization
SSH	Secure Shell
SMB	Server Message Block
BB	Building Block
OS	Operating System
RAM	Random Access Memory
BIT	Binary Digit
GB	Gigabyte
RHEL	Red Hat Enterprise Linux
EULA	End User License Agreement
NIC	Network Interface Card
FQDN	Fully Qualified Domain Name
SATA	Serial Advanced Technology Attachment
NVME	Non-Volatile Memory Express
EXE	Executable (file extension)
CE	Community Edition
SSHD	Secure Shell Daemon
QID	QRadar Identifier
IP	Internet Protocol
RDP	Remote Desktop Protocol