Industry Project

Report

On

Security Operation Center (SOC)

Developed By: -
Vraj Patel (20162171034)

Guided By:-
Prof. Sonam Singh (Internal)
Janvi Sharma (External – Heritage Cyberworld)

Submitted to

Faculty of Engineering and Technology

Institute of Computer Technology

Ganpat University

Year – 2024

CERTIFICATE

This is to certify that the **Industry** Project work entitled **"SOC"** by Vraj Patel (EnrolmentNo. 20162171034) and of Ganpat University, towards the partial fulfillment of requirements of the degree of Bachelor of Technology – Computer Science and Engineering, carried out by them in the CSE(CS) Department at Heritage Cyberworld LLP The results/findings contained in this Project have not been submitted in part or full to any other University / Institute for award of any other Degree/Diploma.

Name & Signature of Internal Guide

Name & Signature of Head

Place: ICT - GUNI

Date

Registerd Office
504-Santorini Square,
Opp. Star Bazaar, Jodhpur,
Ahmedabad-380015,
Gujarat, INDIA.

Corporate Office
504, 505 Aarohi Verve,
Near Vakil Bridge, Bopal,
Ahmedabad-380058,
Gujarat, INDIA.

Integrated Cyber Security Command Control Center
605-606 Solaris Business Hub,
Opp. Parshwanath Jain Mandir BRTS,
Bhuyangdev, Ahmedabad-380013,
Gujarat, INDIA.

HERITAGE
CYBERWORLD LLP

INTERNSHIP COMPLETION CERTIFICATE

DATE: 27th April 2024

This is to certify that Vraj Patel has successfully completed a four month SOC analyst internship with Heritage Cyberworld.

During this internship, he has demonstrated exceptional dedication, enthusiasm, and a strong willingness to learn. Vraj Patel actively participated in gaining knowledge about SOC infrastructure, log analysis, implementation, and integration of different SIEM tools such as Wazuh and Splunk, as well as expertise in threat hunting, threat intelligence, and incident response also in Final Project deployed virtual SOC with AD created demo users to stimulate a working office and consistently contributed valuable insights to our team.

Date of Starting: 1st January 2024
Date of Completion: 30th April 2024

This internship has provided him with valuable hands-on experience in SIEM Tools, Analytical skills, problem solving skills, Knowledge of security tools and Incident response experience. enhancing his knowledge and skills in Cyber Security & IT Industry.

We commend Vraj Patel for his outstanding performance and commitment throughout the duration of the internship. We believe that he has a bright future ahead and wish him continued success in his academic and professional endeavour's.

HERITAGE
CYBERWORLD LLP

AUTHORIZED SIGNATURE

Vraj Patel.

INTERN SIGNATURE

ACKNOWLEDGEMENT

IBM/Industry Internship project is a golden opportunity for learning and self-development. I consider myself very lucky and honored to have so many wonderful people lead me through in completion of this project. First and foremost, I would like to thank Dr. Rohit Patel, Principal, ICT, and Prof. Dharmesh Darji , Head, ICT who gave us an opportunity to undertake this project. My grateful thanks to Prof. Sonam Singh & Mr. Anoj Dixit (Internal & External Guides) for their guidance in project work, who despite being extraordinarily busy with academics, took time out to hear, guide and keep us on the correct path. We do not know where we would have been without his/her help. CSE department monitored our progress and arranged all facilities to make life easier. We choose this moment to acknowledge their contribution gratefully.

VRAJ PATEL (Enrollment No:20162171034)

ABSTRACT

Security Operations Center (SOC) serves as a pivotal entity within modern cybersecurity infrastructures, tasked with the continuous monitoring, detection, analysis, and response to potential security threats and incidents. This abstract provides an overview of SOC's fundamental components, functions, and methodologies aimed at safeguarding organizational assets and data integrity. It explores the role of SOC in proactively identifying and mitigating security risks through advanced technologies such as intrusion detection systems (IDS), security information and event management (SIEM) platforms, threat intelligence, and incident response frameworks. Additionally, the abstract highlights the significance of collaboration between SOC analysts, threat hunters, and incident responders to ensure swift and effective remediation of security incidents. Emphasis is placed on the evolving landscape of cyber threats and the imperative for SOC to adapt and innovate in order to maintain resilience against sophisticated adversaries. Through constant refinement of processes, adoption of best practices, and integration of automation and artificial intelligence (AI), SOC endeavors to fortify organizational defenses and uphold the integrity of digital assets in an increasingly complex threat landscape.

INDEX

CHAPTER: 1 INTRODUCTION

CHAPTER 1 INTRODUCTION

In an era marked by ubiquitous digital connectivity and pervasive cyber threats, the Security Operations Center (SOC) emerges as a cornerstone in the defense against malicious actors and cyber attacks. With organizations facing an ever-expanding array of sophisticated threats, ranging from malware and phishing scams to advanced persistent threats (APTs) and ransomware, the role of SOC has become increasingly vital in safeguarding sensitive data, preserving operational continuity, and mitigating financial and reputational risks.

The introduction of this discourse sets the stage for understanding the multifaceted role of SOC within the broader context of cybersecurity operations. It delineates the escalating nature of cyber threats and the imperative for organizations across industries to fortify their defenses and bolster their incident response capabilities. As technology evolves and threat vectors become more diverse and elusive, the SOC stands as a bastion of vigilance, equipped with the requisite tools, technologies, and expertise to detect, analyze, and mitigate security incidents in real-time.

This introduction provides a glimpse into the foundational principles and operational paradigms that underpin the SOC's mission, emphasizing the symbiotic relationship between proactive threat detection, rapid incident response, and continuous improvement. As organizations contend with an ever-shifting threat landscape characterized by novel attack vectors and sophisticated adversaries, the efficacy of the SOC hinges on its ability to adapt, innovate, and collaborate across organizational silos to confront emerging challenges head-on.

In the subsequent sections, we delve deeper into the core components, operational workflows, and technological innovations that define contemporary SOC operations. Through a comprehensive exploration of SOC's functions, methodologies, and best practices, this discourse seeks to illuminate the pivotal role that SOC plays in fortifying organizational resilience and safeguarding critical assets against the relentless tide of cyber threats

CHAPTER: 2 PROJECT SCOPE

CHAPTER 2 PROJECT SCOPE

The scope of this discussion encompasses the multifaceted dimensions of Security Operations Center (SOC) operations, focusing on its primary functions, methodologies, technologies, and best practices within the realm of cybersecurity.

The scope also acknowledges the dynamic nature of the cybersecurity landscape and the evolving threat landscape, which necessitates ongoing adaptation, innovation, and knowledge sharing within SOC environments. While the focus is primarily on traditional SOC models, consideration may also be given to emerging trends such as managed SOC services, cloud-based SOC solutions, and the integration of artificial intelligence (AI) and machine learning (ML) technologies within SOC operations.

Overall, the scope aims to provide a comprehensive understanding of the role, functions, and operational dynamics of SOC within modern cybersecurity ecosystems, with a view towards fostering resilience, agility, and proactive threat mitigation strategies in the face of evolving cyber threats.

CHAPTER: 3 HARDWARE REQUIREMENTS

CHAPTER: 3 HARDWARE REQUIREMENTS

CPU: Multi-core processors (e.g., Intel Xeon, AMD EPYC) with sufficient processing power to handle concurrent tasks and data analysis.

RAM: Depending on the size of the organization and the volume of data being processed, servers may require anywhere from 32GB to 256GB or more of RAM.

Storage: High-speed SSDs or SAS drives for storing security logs, event data, and application databases. Storage capacity requirements will vary based on data retention policies and the volume of data generated.

Network Appliances:

Firewalls, routers, switches, and other network appliances typically have their own hardware specifications provided by the manufacturer. These specifications should be aligned with the organization's network throughput requirements and security policies.

Endpoint Devices:

Workstations or laptops used by SOC analysts should have modern CPUs (e.g., Intel Core i7 or equivalent), sufficient RAM (16GB or more), and fast SSD storage for responsiveness during analysis tasks.

CHAPTER: 4 SOFTWARE REQUIREMENTS

CHAPTER: 4 SOFTWARE REQUIREMENTS

Security Information and Event Management (SIEM) Platform:

Examples: Splunk Enterprise Security, IBM QRadar, LogRhythm, Elastic SIEM.

Description: SIEM platforms collect, analyze, and correlate security event data from various sources to provide real-time threat detection, incident response, and compliance reporting.

Intrusion Detection System/Intrusion Prevention System (IDS/IPS):

Examples: Snort, Suricata, Cisco Firepower, Palo Alto Networks IDS/IPS.

Description: IDS/IPS solutions monitor network traffic for signs of malicious activity or policy violations and can either alert SOC analysts or take automated action to block suspicious traffic.

Endpoint Detection and Response (EDR) Software:

Examples: CrowdStrike Falcon, Carbon Black, Microsoft Defender for Endpoint, Symantec Endpoint Detection and Response.

Description: EDR solutions provide visibility into endpoint activities, detect and respond to threats in real-time, and offer capabilities for investigation and remediation of security incidents on endpoints.

Threat Intelligence Platforms (TIPs):

Examples: ThreatConnect, Anomali ThreatStream, Recorded Future, ThreatQ

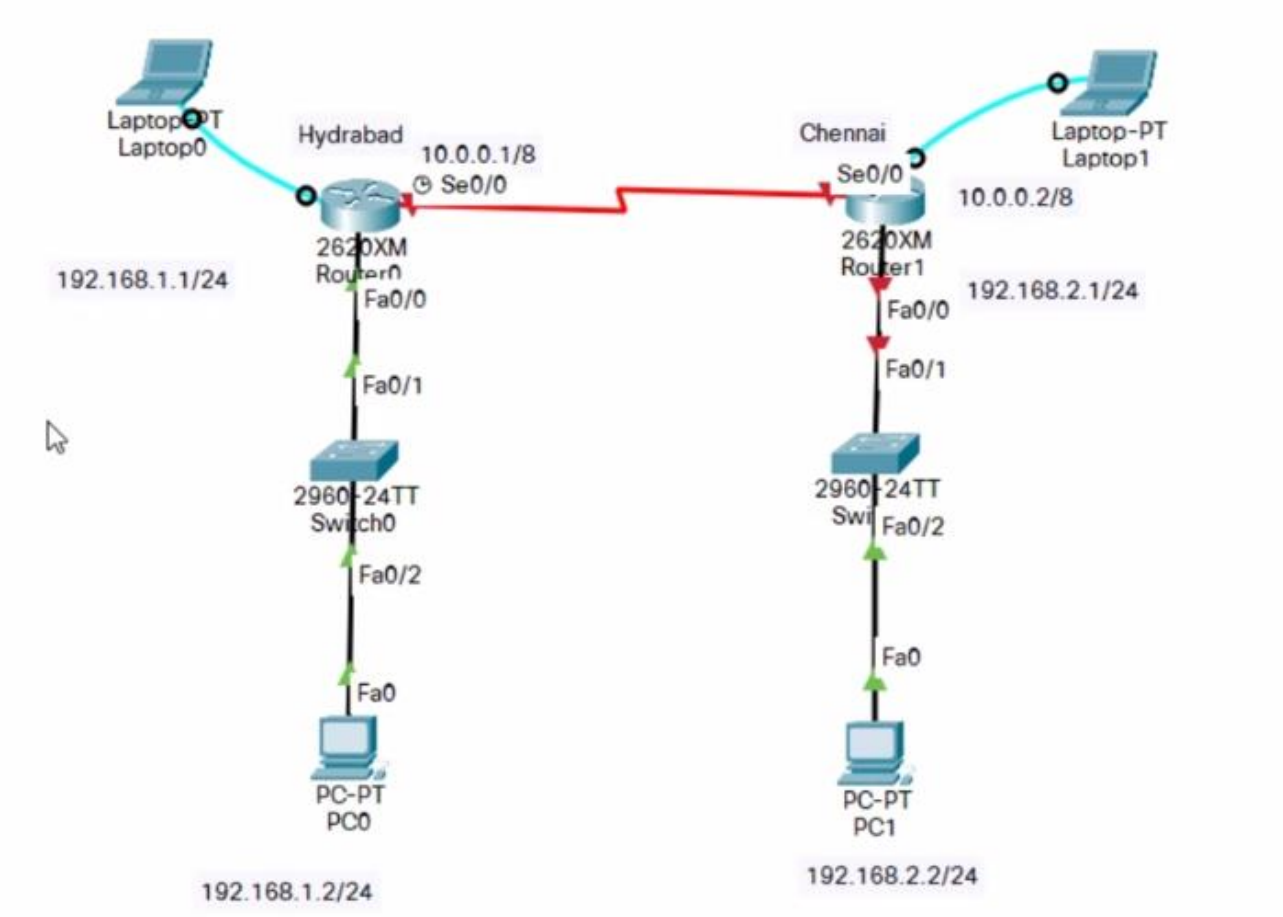
CHAPTER: 5 WEEKLY TASKS

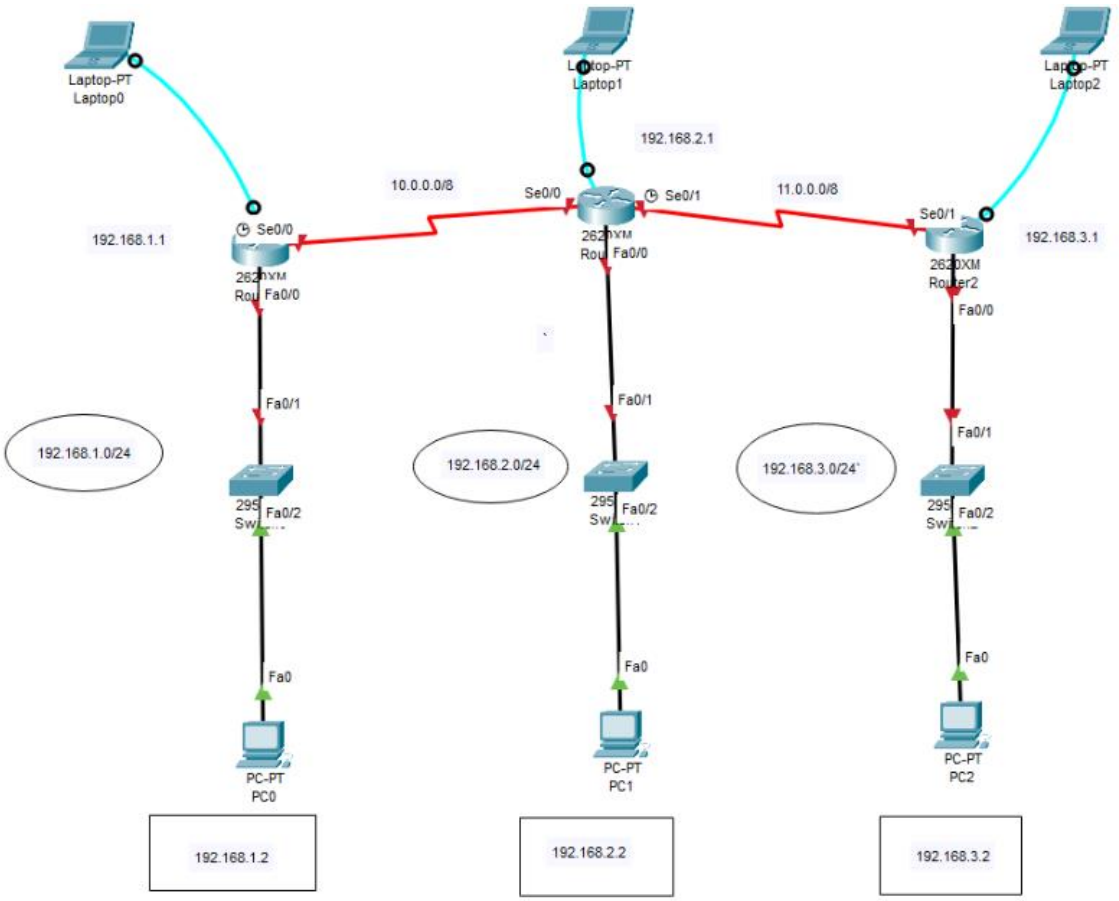
CHAPTER: 5 WEEKLY TASKS

5.1 WEEK – 1

- Basics of Computer Networks
- Practical on Cisco Packet Tracer

Routing protocols –

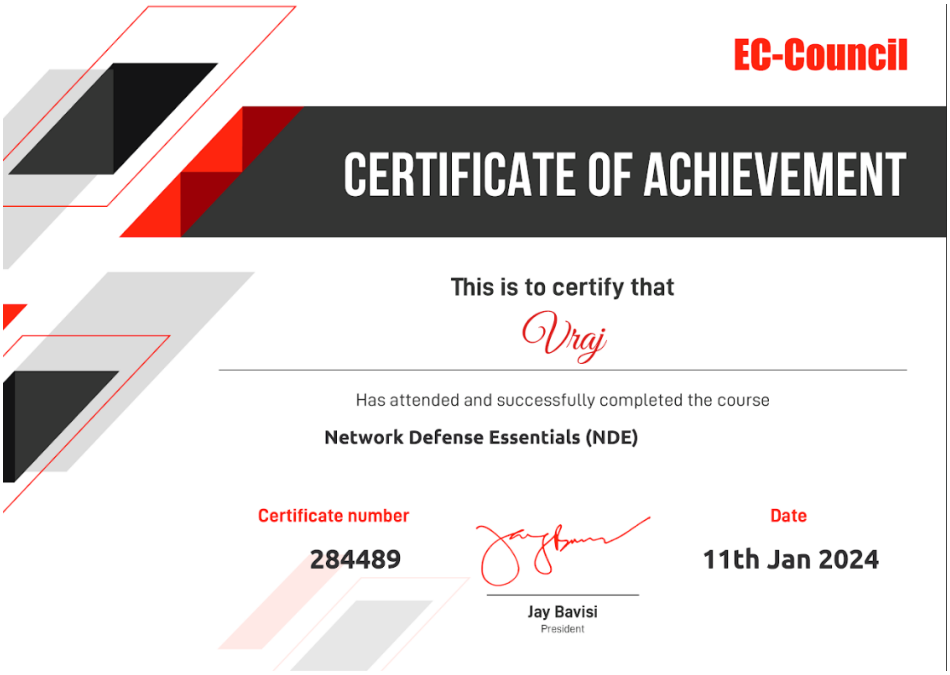




- Practical on Wireshark

5.2 WEEK – 2

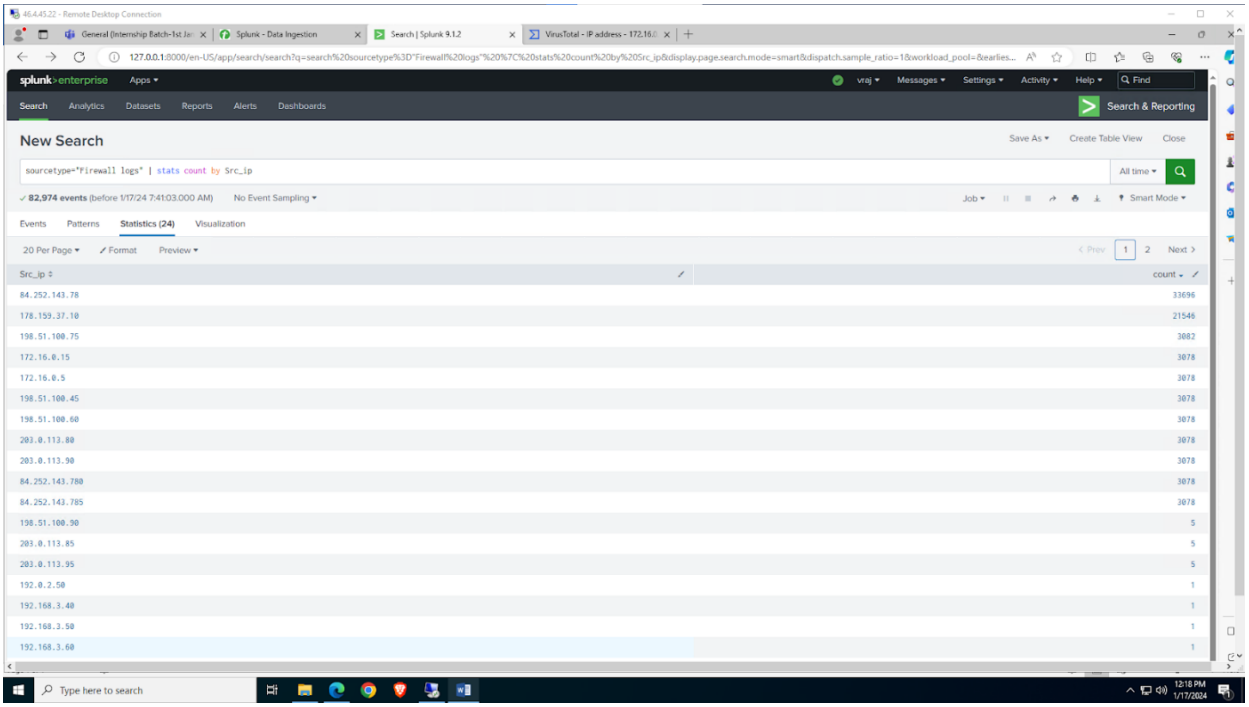
- Certified course of EC-Council

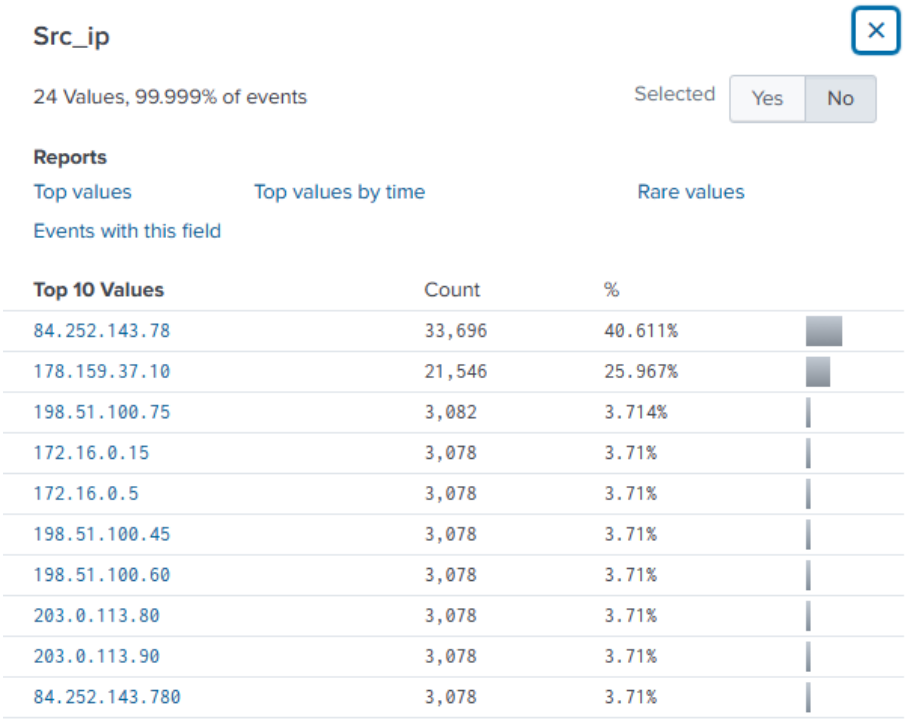


- Certified course of Splunk

5.3 WEEK – 3

- Practical on Splunk
- Analyzing Logs on Splunk





Destination_ip

9 Values, 99.999% of events

Selected Yes No

Reports

Top values | Top values by time | Rare values

Events with this field

Values	Count	%
8.8.8.8	18,474	22.265%
192.168.1.200	12,318	14.846%
10.0.0.1	12,156	14.65%
10.0.0.2	9,240	11.136%
10.10.0.5	9,239	11.135%
192.168.2.200	9,234	11.129%
192.168.2.100	6,156	7.419%
10.0.0.5	3,078	3.71%
10.10.0.10	3,078	3.71%

Destination_port

5 Values, 99.999% of events

Selected Yes No

Reports

Average over time | Maximum value over time | Minimum value over time

Top values | Top values by time | Rare values

Events with this field

Avg: 130.88087691176648 **Min:** 0 **Max:** 443 **Std Dev:** 169.4878643130313

Values	Count	%
53	21,557	25.981%
0	21,547	25.969%
443	18,474	22.265%
80	18,317	22.076%
22	3,078	3.71%

- Report & Presentation on Qradar – Vraj

CONTENT

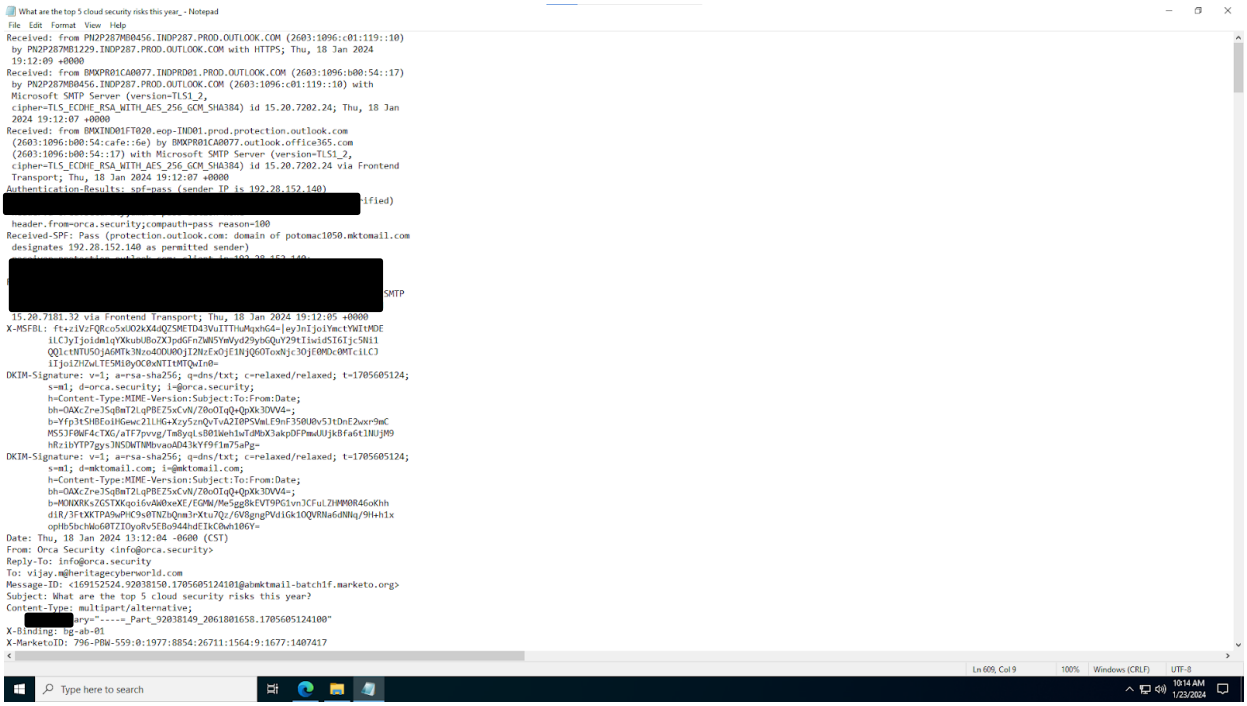
- ABOUT
- TOP 10 FEATURES OF IBM QRADAR
- DEPLOYMENT OPTIONS
- COMPLIANCE
- SYSTEM REQUIREMENTS
- USE CASES
- PRICE COMPARISION WITH OTHER SIEM TOOLS
- DEMO

PRICE COMPARISION WITH OTHER SIEM TOOLS

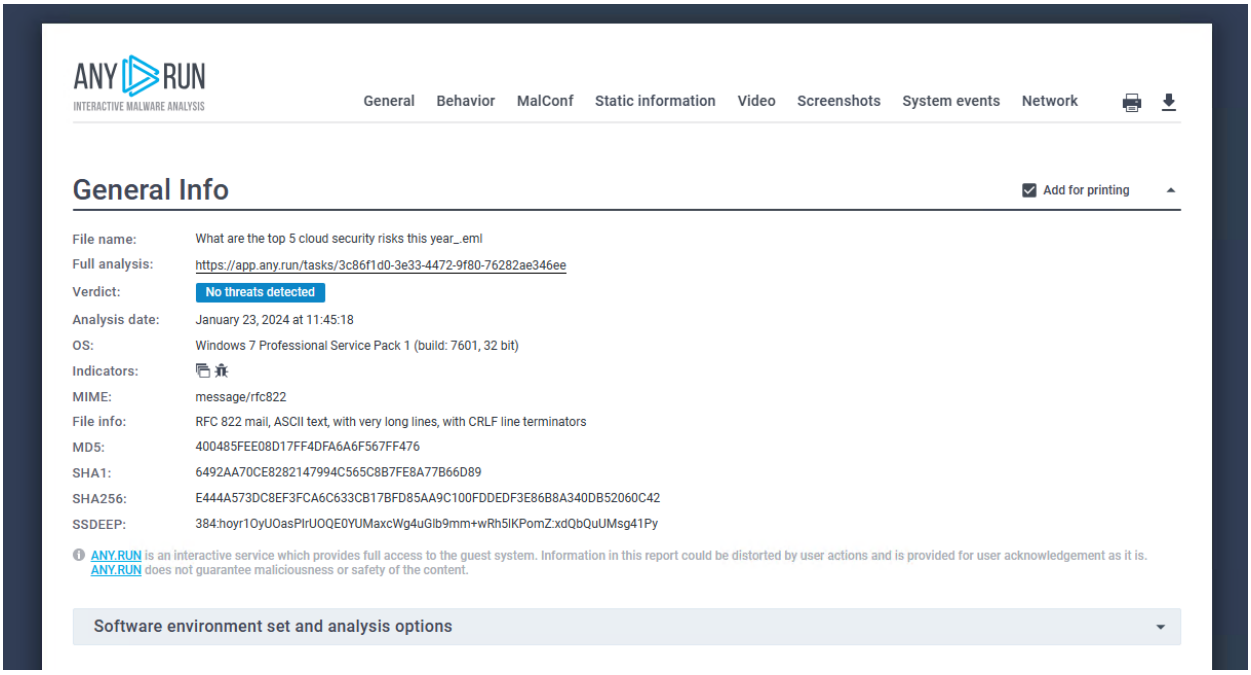
IBM QRADAR	SPLUNK
QRadar which is priced based on the events per second.	Splunk is priced based on the amount of data ingested on daily basis or the number of Splunk Virtual Compute (SVCs) units consumed (Workload Pricing), which can be more expensive than **QRadar**
$740–$1050 per month for 500 employees in organization(Software Based) $2300-$3100 per month for 500 employees in organization(SaaS)	Pricing starts at $150 per ingested GB of data per month.

5.4 WEEK – 4

- Email logs & Header Analysis



```
What are the top 5 cloud security risks this year_ - Notepad
File  Edit  Format  View  Help
Received: from PN2P287MB0456.INDP287.PROD.OUTLOOK.COM (2603:1096:c01:119::10)
 by PN2P287MB1229.INDP287.PROD.OUTLOOK.COM with HTTPS; Thu, 18 Jan 2024
 19:12:09 +0000
Received: from BMXPR01CA0077.INDPRD01.PROD.OUTLOOK.COM (2603:1096:b00:54::17)
 by PN2P287MB0456.INDP287.PROD.OUTLOOK.COM (2603:1096:c01:119::10) with
 Microsoft SMTP Server (version=TLS1_2,
 cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.7202.24; Thu, 18 Jan
 2024 19:12:07 +0000
Received: from BMXIND01FT020.eop-IND01.prod.protection.outlook.com
 (2603:1096:b00:54:cafe::6e) by BMXPR01CA0077.outlook.office365.com
 (2603:1096:b00:54::17) with Microsoft SMTP Server (version=TLS1_2,
 cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.7202.24 via Frontend
 Transport; Thu, 18 Jan 2024 19:12:07 +0000
Authentication-Results: spf=pass (sender IP is 192.28.152.140)
[redacted]
 header.from=orca.security;compauth=pass reason=100
Received-SPF: Pass (protection.outlook.com: domain of potomac1050.mktomail.com
 designates 192.28.152.140 as permitted sender)
[redacted]
 15.20.7181.32 via Frontend Transport; Thu, 18 Jan 2024 19:12:05 +0000
X-MSFBL: ft+zIVzFQRco5xUO2kX4dQZSMTD4JVuITThuMqxhG4=[eyJnIjoiYmctYWItMDE
        iLCJyIjoidmlqYXkubUBoZXJpdGFnZWN5YmVyd29ybGQuY29tIiwidSI6Ijc5Ni1
        QQ1ctNTU5OjA6MTk3Nzo4ODU0OjI2NzExOjE1NjQ6OToxNjc3OjE0MDc0MTciLCJ
        iIjoiZHZwLTE5Mi0yOC0xNTItMTQwIn0=
DKIM-Signature: v=1; a=rsa-sha256; q=dns/txt; c=relaxed/relaxed; t=1705605124;
        s=m1; d=orca.security; i=@orca.security;
        h=Content-Type:MIME-Version:Subject:To:From:Date;
        bh=OAXcZre3SqBmT2LqPBEZ5xCvN/Z0xOIqQ+QpXk3DVV4=;
        b=Yfp3tSHBEoiHGewc21LHG+XzySznQvTvA2I0PSVmLE9nF350U0v5JtDnE2wxr9mC
        MS5JF0WF4cTXG/aTF7pvvg/Tm8yqlsB01Weh1wTdMbX3akpDFPmwUUjkBfa6t1NUjM9
        hRzibYTP7gysJNSOWTNMbvaoAD43kYf9f1m75aPg=
DKIM-Signature: v=1; a=rsa-sha256; q=dns/txt; c=relaxed/relaxed; t=1705605124;
        s=m1; d=mktomail.com; i=@mktomail.com;
        h=Content-Type:MIME-Version:Subject:To:From:Date;
        bh=OAXcZre3SqBmT2LqPBEZ5xCvN/Z0xOIqQ+QpXk3DVV4=;
        b=MONXRKsZGSTXKqoi6vAW0xeXE/EGMW/Me5gg8kEVT9PG1vnJCFuLZHMM0R4GoKhh
        dlR/3FtKKTPA9wPnC9s0TNZbQnm3rXtu7Qz/6V8gngPVdiGk1OQVRNa6dNNq/9H+h1x
        opHb5bchWo60TZIOyoRv5EBo944hdEIkC0wh106Y=
Date: Thu, 18 Jan 2024 13:12:04 -0600 (CST)
From: Orca Security <info@orca.security>
Reply-To: info@orca.security
To: vijay.m@heritagecyberworld.com
Message-ID: <169152524.92038150.1705605124101@abmktmail-batch1f.marketo.org>
Subject: What are the top 5 cloud security risks this year?
Content-Type: multipart/alternative;
 [redacted]ary="----=_Part_92038149_2061801658.1705605124100"
X-Binding: bg-ab-01
X-MarketoID: 796-PBW-559:0:1977:8854:26711:1564:9:1677:1407417
```



ANY RUN
INTERACTIVE MALWARE ANALYSIS

General Behavior MalConf Static information Video Screenshots System events Network

General Info

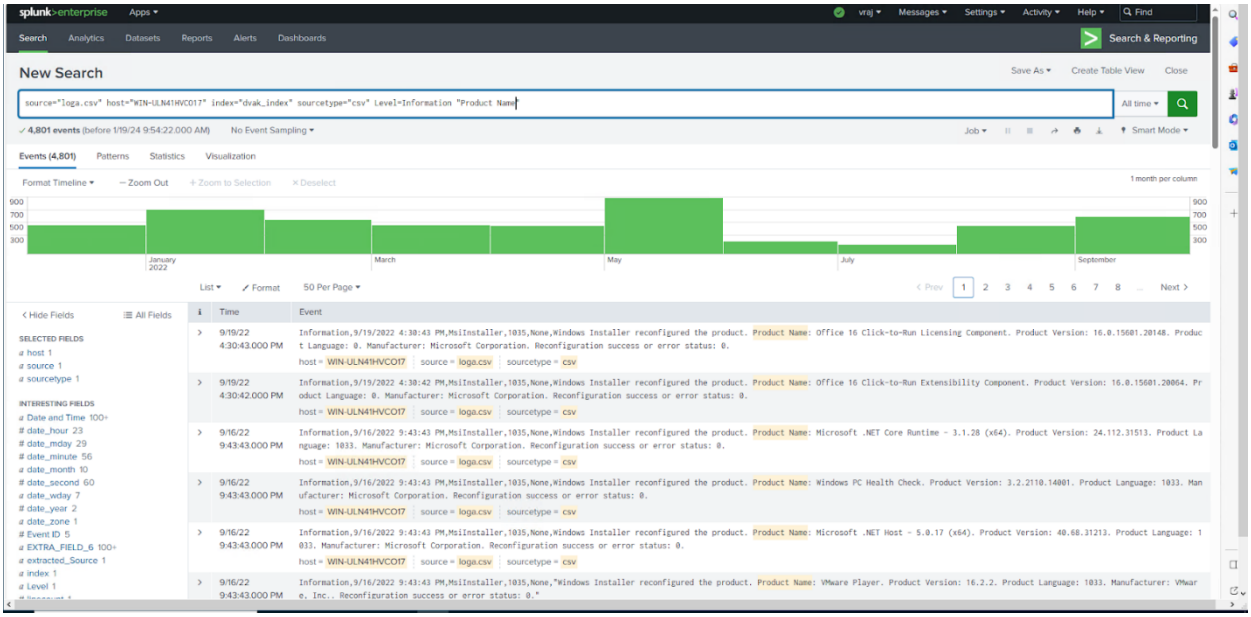
Add for printing

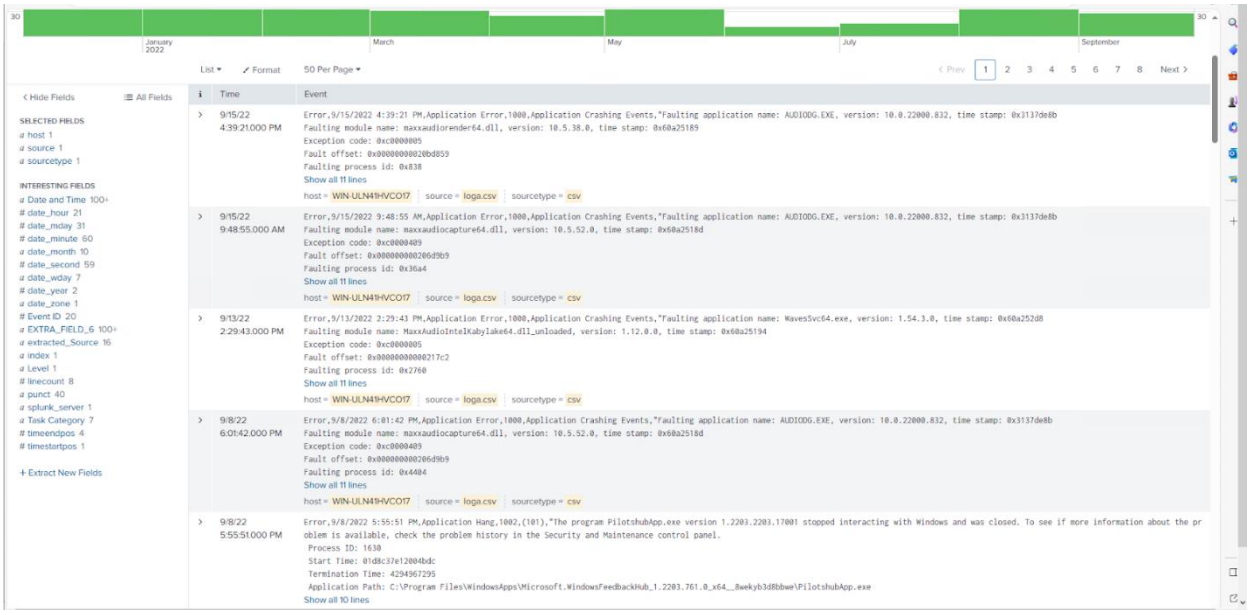
File name:	What are the top 5 cloud security risks this year_.eml
Full analysis:	https://app.any.run/tasks/3c86f1d0-3e33-4472-9f80-76282ae346ee
Verdict:	No threats detected
Analysis date:	January 23, 2024 at 11:45:18
OS:	Windows 7 Professional Service Pack 1 (build: 7601, 32 bit)
Indicators:	
MIME:	message/rfc822
File info:	RFC 822 mail, ASCII text, with very long lines, with CRLF line terminators
MD5:	400485FEE08D17FF4DFA6A6F567FF476
SHA1:	6492AA70CE8282147994C565C8B7FE8A77B66D89
SHA256:	E444A573DC8EF3FCA6C633CB17BFD85AA9C100FDDEDF3E86B8A340DB52060C42
SSDEEP:	384:hoyr1OyUOasPlrUOQE0YUMaxcWg4uGlb9mm+wRh5lKPomZ:xdQbQuUMsg41Py

ANY.RUN is an interactive service which provides full access to the guest system. Information in this report could be distorted by user actions and is provided for user acknowledgement as it is. ANY.RUN does not guarantee maliciousness or safety of the content.

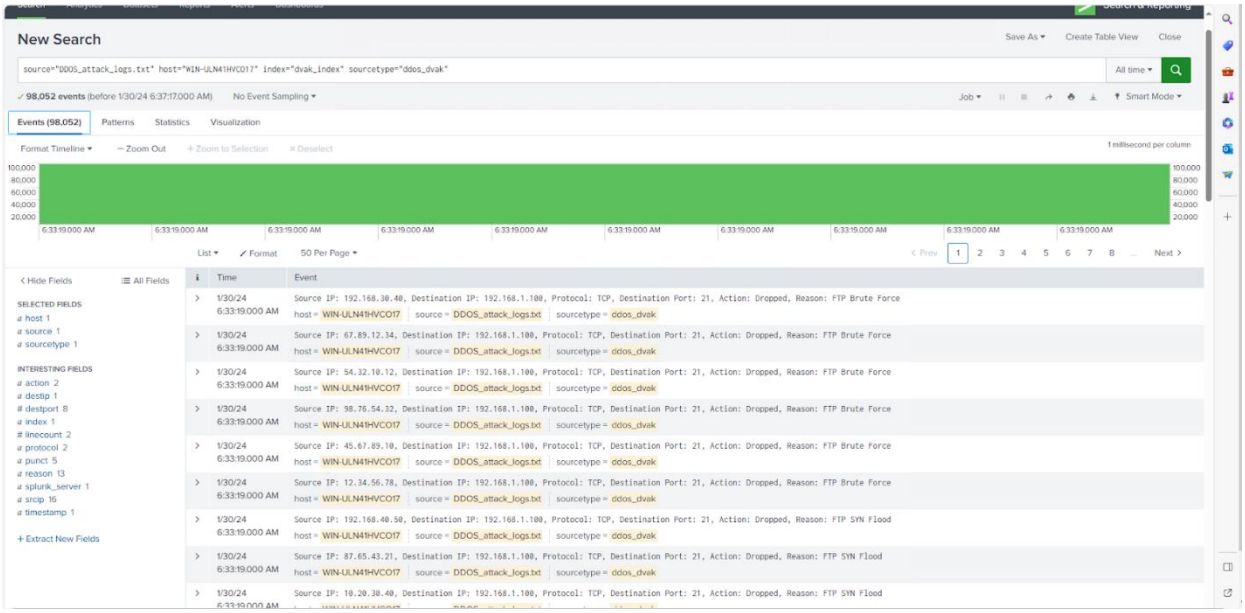
Software environment set and analysis options

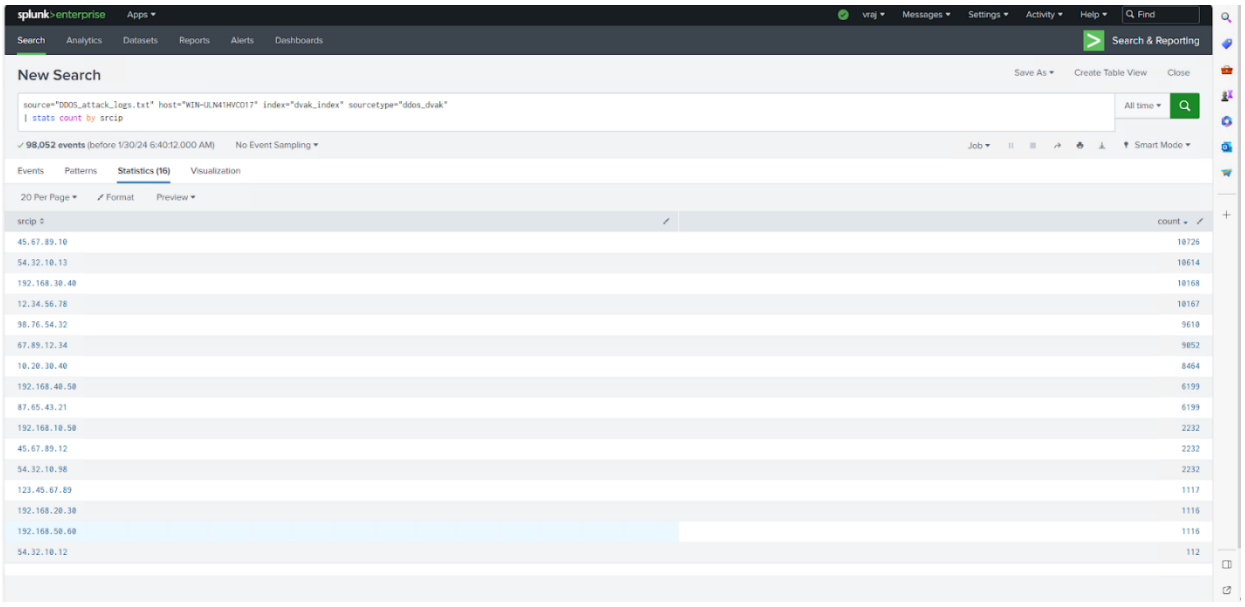
- Firewall Logs





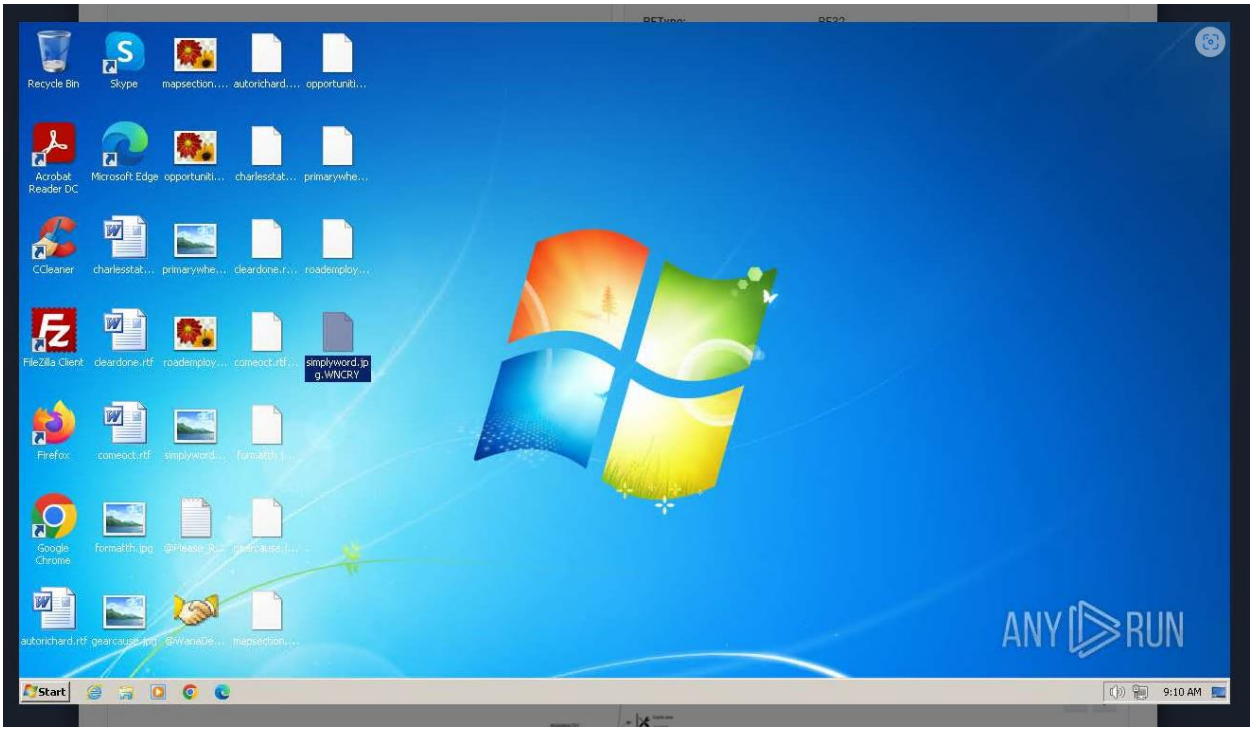
- DDoS Logs

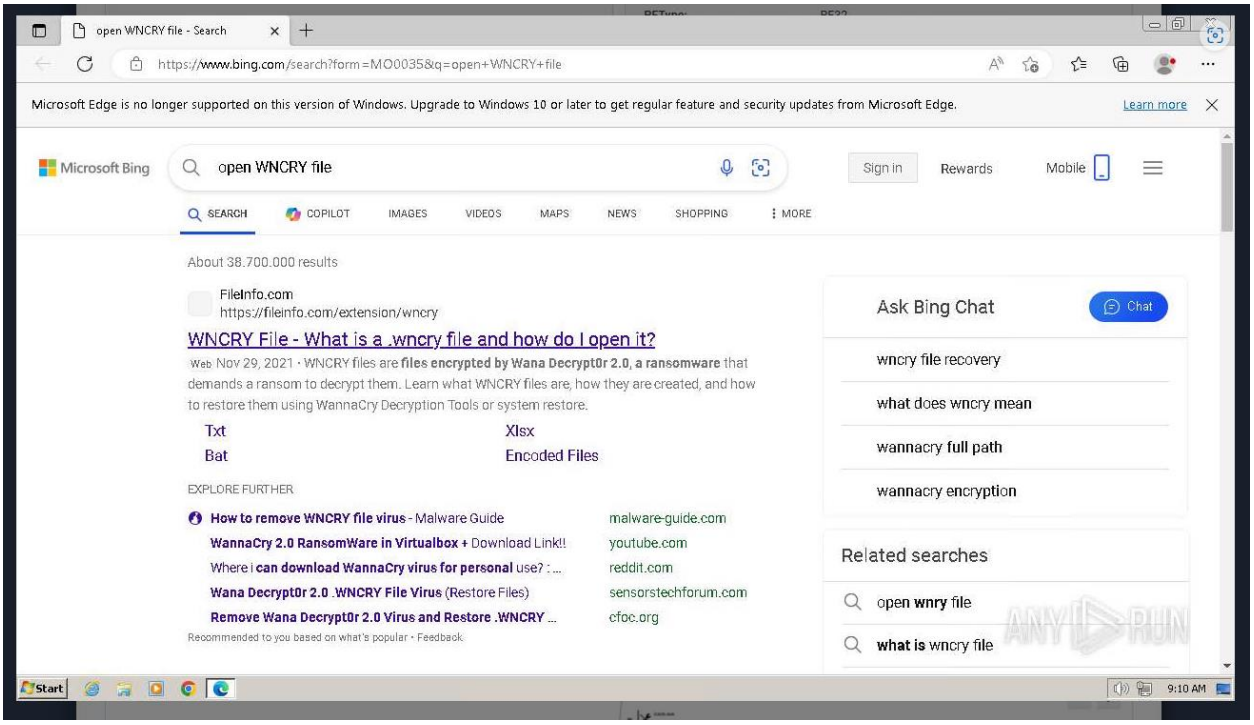

New Search
source="DDOS_attack_logs.txt" host="WIN-ULN41HVCO17" index="dvak_index" sourcetype="ddos_dvak"
98,052 events (before 1/30/24 6:37:17.000 AM)
Events (98,052)
Patterns
Statistics
Visualization
Time
Event
Source IP: 192.168.30.40, Destination IP: 192.168.1.100, Protocol: TCP, Destination Port: 21, Action: Dropped, Reason: FTP Brute Force
Source IP: 67.89.12.34, Destination IP: 192.168.1.100, Protocol: TCP, Destination Port: 21, Action: Dropped, Reason: FTP Brute Force
Source IP: 54.32.10.12, Destination IP: 192.168.1.100, Protocol: TCP, Destination Port: 21, Action: Dropped, Reason: FTP Brute Force
Source IP: 98.76.54.32, Destination IP: 192.168.1.100, Protocol: TCP, Destination Port: 21, Action: Dropped, Reason: FTP Brute Force
Source IP: 45.67.89.10, Destination IP: 192.168.1.100, Protocol: TCP, Destination Port: 21, Action: Dropped, Reason: FTP Brute Force
Source IP: 12.34.56.78, Destination IP: 192.168.1.100, Protocol: TCP, Destination Port: 21, Action: Dropped, Reason: FTP Brute Force
Source IP: 192.168.40.50, Destination IP: 192.168.1.100, Protocol: TCP, Destination Port: 21, Action: Dropped, Reason: FTP SYN Flood
Source IP: 87.65.43.21, Destination IP: 192.168.1.100, Protocol: TCP, Destination Port: 21, Action: Dropped, Reason: FTP SYN Flood
Source IP: 10.20.30.40, Destination IP: 192.168.1.100, Protocol: TCP, Destination Port: 21, Action: Dropped, Reason: FTP Brute Force


New Search
source="DDOS_attack_logs.txt" host="WIN-ULN41HVCO17" index="dvak_index" sourcetype="ddos_dvak"
| stats count by srcip
98,052 events (before 1/30/24 6:40:12.000 AM)
Events
Patterns
Statistics (16)
Visualization
srcip
count
45.67.89.10 10726
54.32.10.13 10614
192.168.30.40 10168
12.34.56.78 10167
98.76.54.32 9610
67.89.12.34 9052
10.20.30.40 8464
192.168.40.50 6199
87.65.43.21 6199
192.168.10.50 2232
45.67.89.12 2232
54.32.10.98 2232
123.45.67.89 1117
192.168.20.30 1116
192.168.50.60 1116
54.32.10.12 112

5.5 WEEK – 5

- Malware Analysis

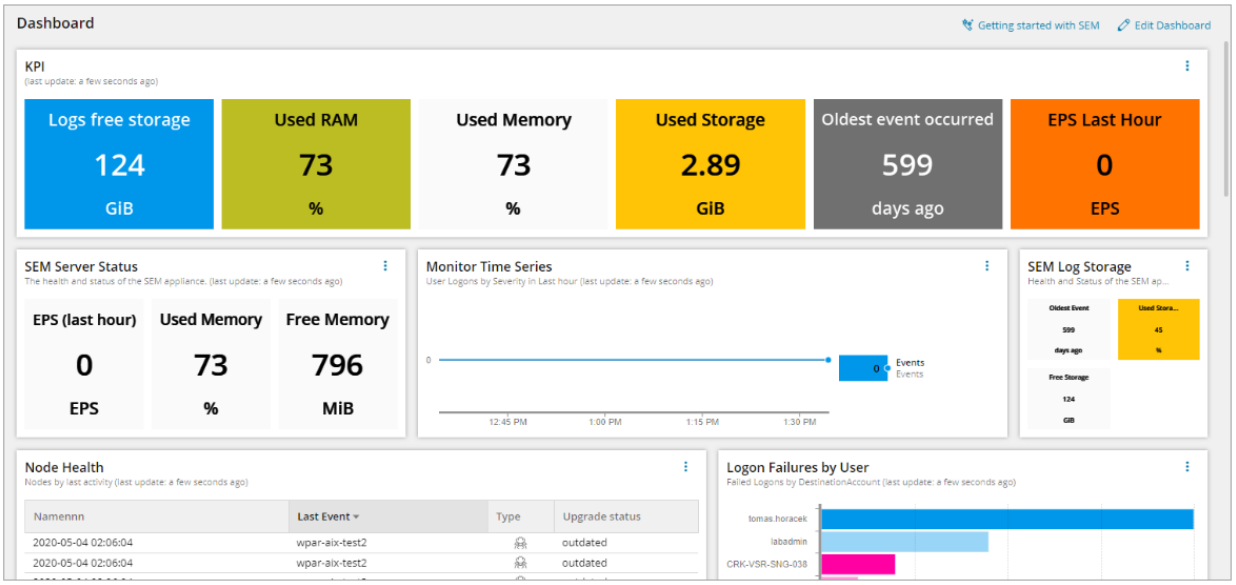


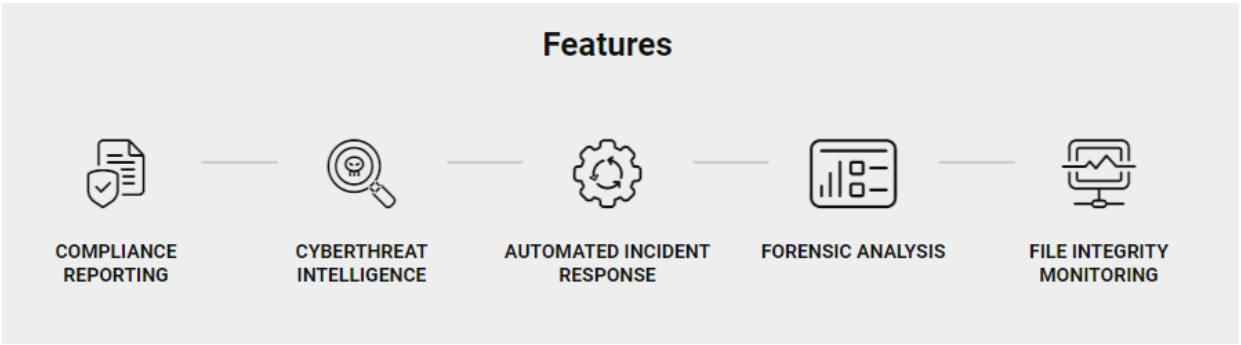


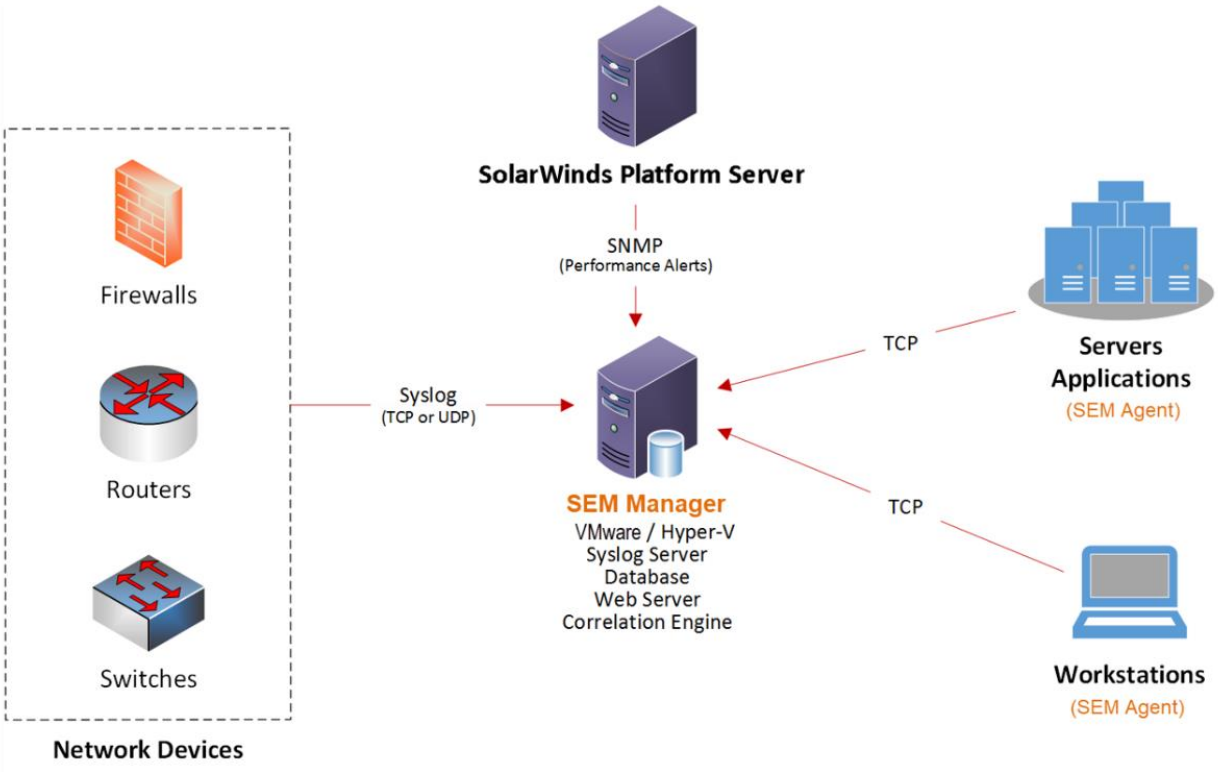

Wana Decrypt0r 2.0
Ooops, your files have been encrypted!
English
What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.
Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.
How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am
Payment will be raised on
1/4/1970 00:00:00
Time Left
Your files will be lost on
1/8/1970 00:00:00
Time Left
About bitcoin
How to buy bitcoins?
Contact Us
Send $600 worth of bitcoin to this address:
bitcoin ACCEPTED HERE
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw
Copy
Check Payment
Decrypt
ANY RUN


Ooops, your important files are encrypted.
If you see this text, but don't see the "Wana Decrypt0r" window,
then your antivirus removed the decrypt software or you deleted
it from your computer.
If you need your files you have to run the decrypt software.
Please find an application file named "@WanaDecryptor@.exe" in
any folder or restore from the antivirus quarantine.
Run and follow the instructions!
ANY RUN

- Report on OEM
- Solarwinds – Vraj

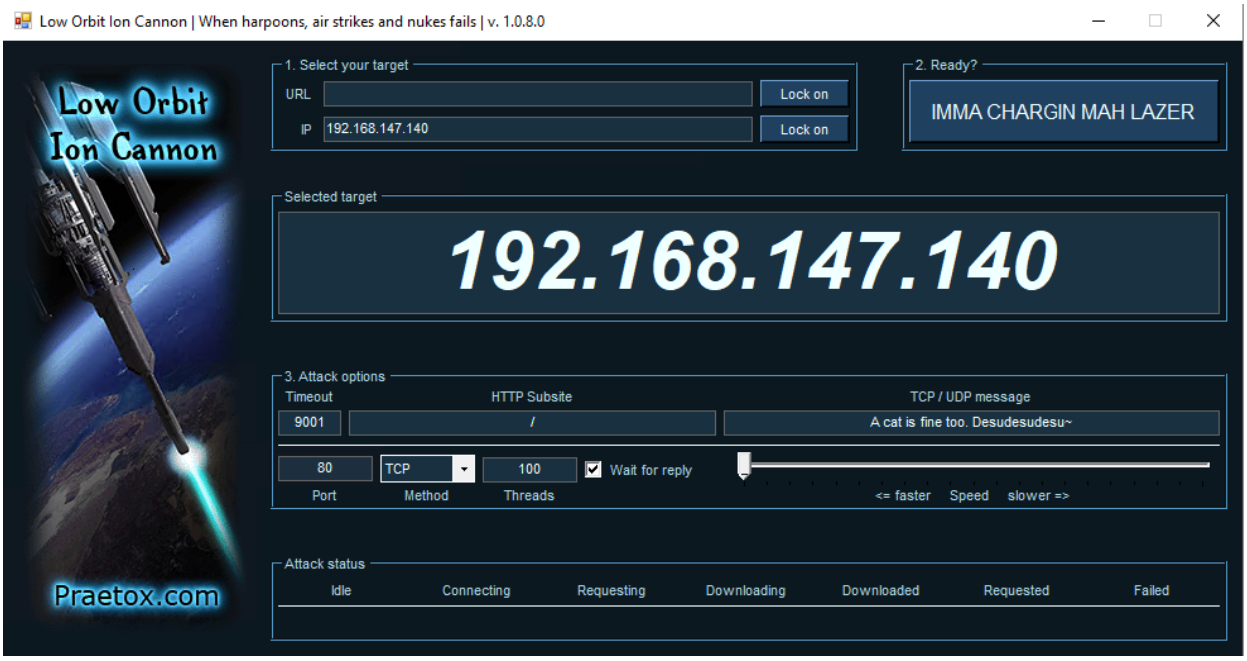


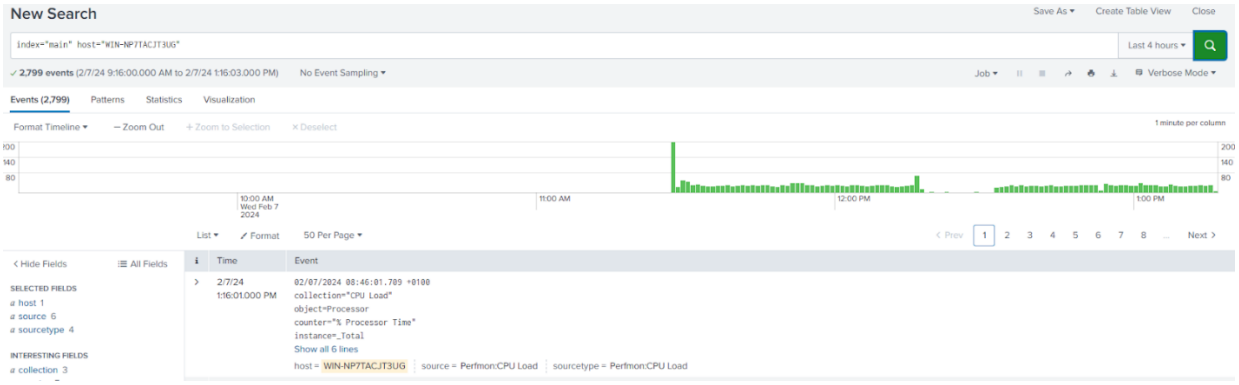



SolarWinds Platform Server
SNMP
(Performance Alerts)
Firewalls
Routers
Switches
Network Devices
Syslog
(TCP or UDP)
SEM Manager
VMware / Hyper-V
Syslog Server
Database
Web Server
Correlation Engine
TCP
Servers
Applications
(SEM Agent)
TCP
Workstations
(SEM Agent)

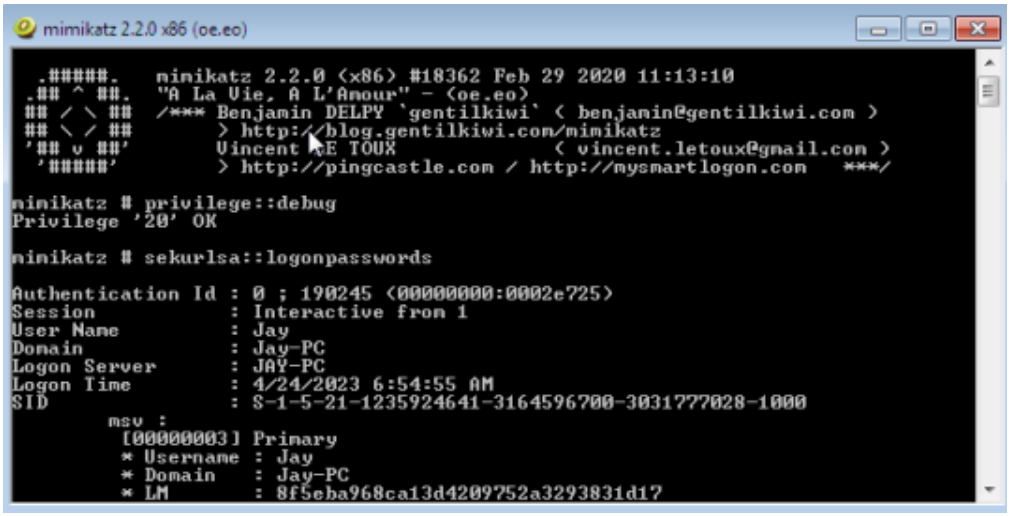
5.6 WEEK – 6

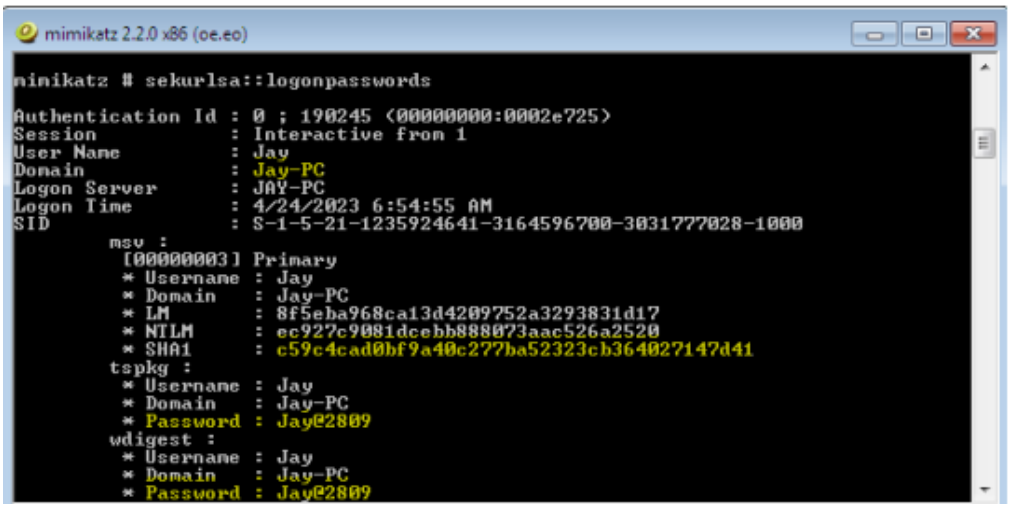
- DDoS attack practical & Logs collection





- Mimikatz attack practical & Logs collection



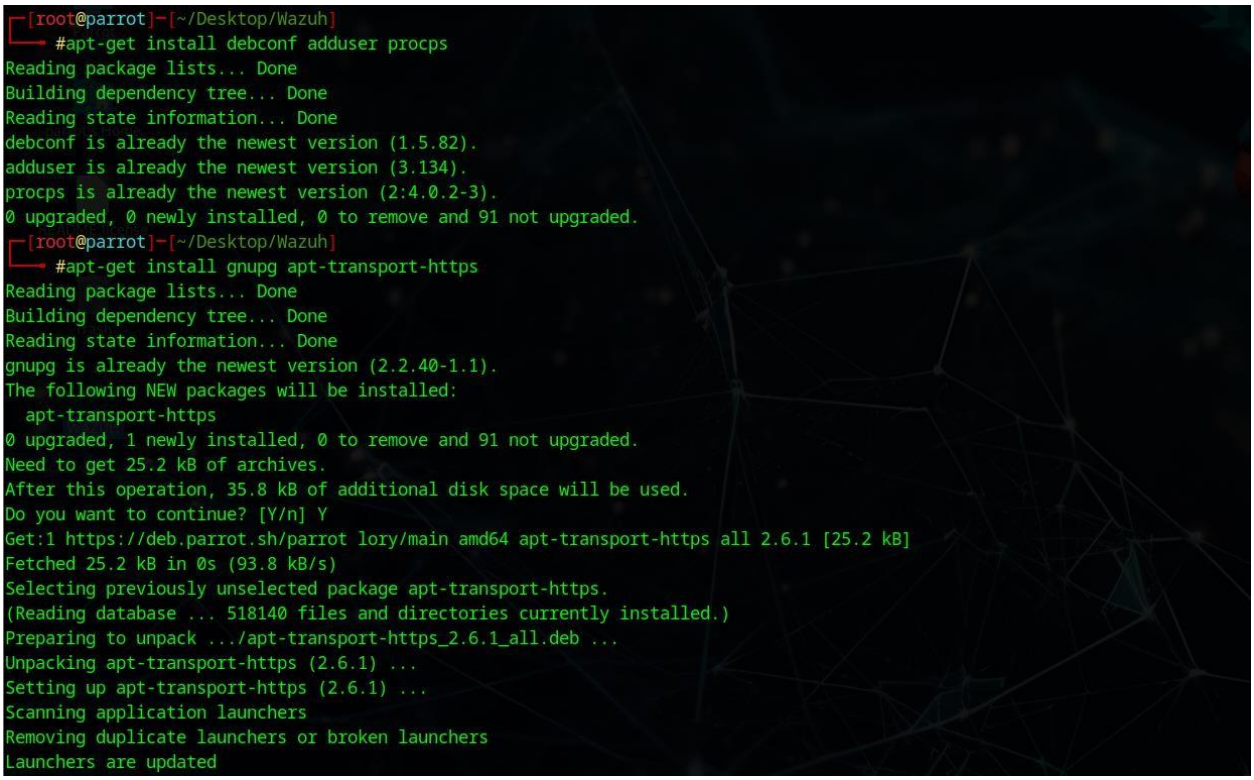


CHAPTER: 6 WAZUH DEPLOYMENT

CHAPTER: 6 WAZUH DEPLOYMENT

WAZUH Indexer –

Wazuh Indexer Install
Install Prerequisites
apt-get install debconf adduser procps apt-get install gnupg apt-transport-https



Install GPG Key and Add repo –
curl -s https://packages.wazuh.com/key/GPG-KEY-WAZUH | gpg --no-default-keyring --keyring gnupg-ring:/usr/share/keyrings/wazuh.gpg --import && chmod 644 /usr/share/keyrings/wazuh.gpg
echo "deb [signed-by=/usr/share/keyrings/wazuh.gpg] https://packages.wazuh.com/4.x/apt/ stable main" | tee -a /etc/apt/sources.list.d/wazuh.list

Install
apt-get update
apt-get -y install wazuh-indexer

```
┌──[root@parrot]─[~/Desktop/Wazuh]
└─── #apt-get update
Hit:1 https://deb.parrot.sh/parrot lory InRelease
Hit:2 https://deb.parrot.sh/direct/parrot lory-security InRelease
Hit:3 https://deb.parrot.sh/parrot lory-backports InRelease
Get:4 https://packages.wazuh.com/4.x/apt stable InRelease [17.3 kB]
Get:5 https://packages.wazuh.com/4.x/apt stable/main amd64 Packages [39.0 kB]
Fetched 56.3 kB in 1s (42.0 kB/s)
Reading package lists... Done
```

```
┌──[root@parrot]─[~/Desktop/Wazuh]
└─── #apt-get -y install wazuh-indexer
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
  wazuh-indexer
0 upgraded, 1 newly installed, 0 to remove and 91 not upgraded.
Need to get 686 MB of archives.
After this operation, 969 MB of additional disk space will be used.
Get:1 https://packages.wazuh.com/4.x/apt stable/main amd64 wazuh-indexer amd64 4.7.2-1 [686 MB]
Fetched 686 MB in 21s (32.5 MB/s)
Selecting previously unselected package wazuh-indexer.
(Reading database ... 518144 files and directories currently installed.)
Preparing to unpack .../wazuh-indexer_4.7.2-1_amd64.deb ...
Creating wazuh-indexer group... OK
Creating wazuh-indexer user... OK
Unpacking wazuh-indexer (4.7.2-1) ...
Setting up wazuh-indexer (4.7.2-1) ...
Created opensearch keystore in /etc/wazuh-indexer/opensearch.keystore
Scanning application launchers
Removing duplicate launchers or broken launchers
Launchers are updated
```

Certificate Deployment
Deploy certificates for encryption and security.
wget https://raw.githubusercontent.com/socfortress/Wazuh-Rules/main/wazuh-certstool.sh -q -O /tmp/wazuh-certs-tool.sh wget https://raw.githubusercontent.com/socfortress/Wazuh-Rules/main/config.yml -q -O /tmp/config.yml

```
┌──[root@parrot]─[~/Desktop/Wazuh]
└─── #wget https://raw.githubusercontent.com/socfortress/Wazuh-Rules/main/wazuh-certs-tool.sh -q -O /tmp/wazuh-certs-tool.sh
┌──[root@parrot]─[~/Desktop/Wazuh]
└─── #wget https://raw.githubusercontent.com/socfortress/Wazuh-Rules/main/config.yml -q -O /tmp/config.yml
```

2. Update the /tmp/config.yml file to fit your hostname and IP.

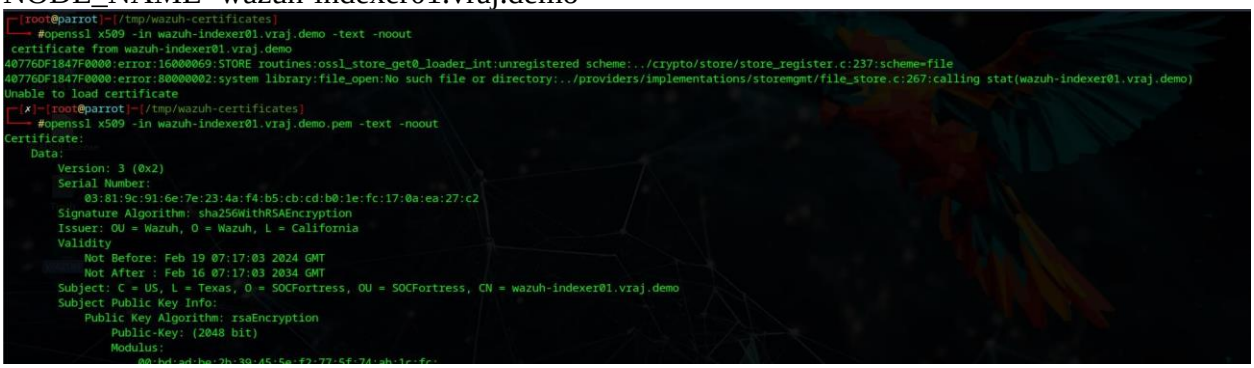
```
 GNU nano 7.2                                  /tmp/config.yml
nodes:
  # Wazuh indexer nodes
  indexer:
    - name: wazuh-indexer01.vraj.demo
      ip: 10.10.9.130
    #- name: node-2
    #  ip: <indexer-node-ip>
    #- name: node-3
    #  ip: <indexer-node-ip>

  # Wazuh server nodes
  # If there is more than one Wazuh server
  # node, each one must have a node_type
  server:
    - name: wazuh-indexer01.vraj.demo
      ip: 10.10.9.130
    #  node_type: master
    #- name: wazuh-2
    #  ip: <wazuh-manager-ip>
    #  node_type: worker
    #- name: wazuh-3
    #  ip: <wazuh-manager-ip>
    #  node_type: worker

  # Wazuh dashboard nodes
  dashboard:
    - name: wazuh-indexer01.vraj.demo
      ip: 10.10.9.130
                                [ line  1/29 ( 3%), col  1/ 7 ( 14%), char   0/655 ( 0%) ]
^G Help      ^O Read File  ^R Replace   ^K Paste     ^C Go To Line  ^Y Redo      M-6 Copy      ^Q Where Was  M-W Next      ^← Forward   ^→ Next Word
^X Exit      ^W Where Is   ^\ Cut       ^U Execute   ^Z Undo        M-A Set Mark  M-] To Bracket M-Q Previous  ^B Back      ^A Home
```

3. Run the /tmp/wazuh-certs-tool.sh -A script to generate the certificates.

4. Obtain the the value of the CN of the hostname.pem certificate.

openssl x509 -in wazuh-indexer01.vraj.demo -text -noout

NODE_NAME=wazuh-indexer01.vraj.demo



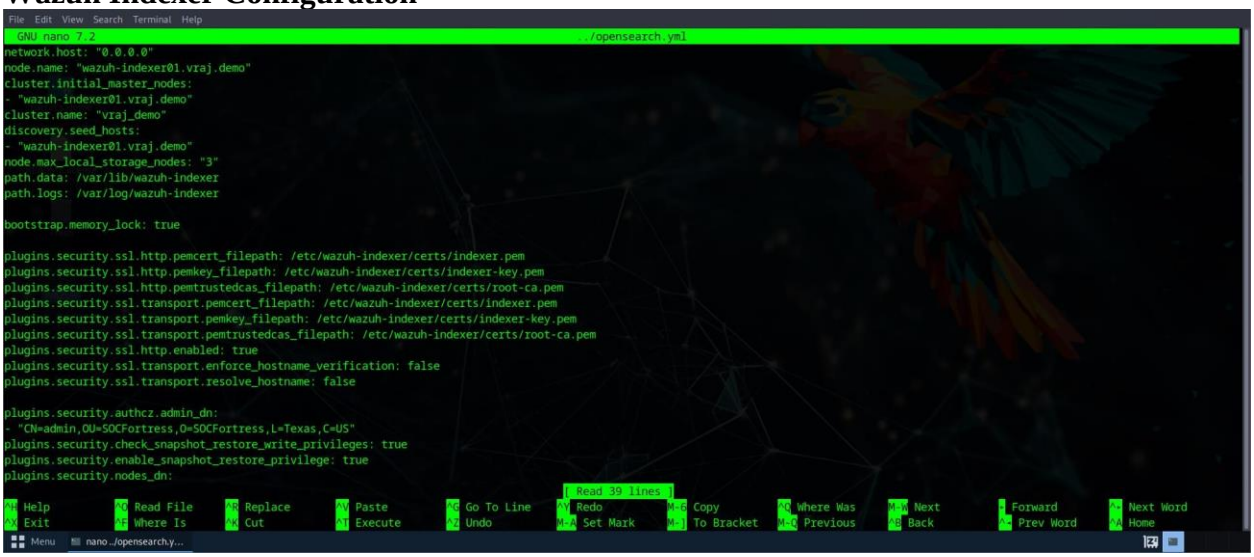
5. Copy certs into /etc/wazuh-indexer/certs

mkdir /etc/wazuh-indexer/certs cd /tmp/wazuh-certificates cp ./$NODE_NAME.pem ./$NODE_NAME-key.pem ./admin.pem ./admin-key.pem ./rootca.pem /etc/wazuh-indexer/certs/ mv -n /etc/wazuh-indexer/certs/$NODE_NAME.pem /etc/wazuhindexer/certs/indexer.pem mv -n /etc/wazuh-indexer/certs/$NODE_NAME-key.pem /etc/wazuhindexer/certs/indexer-key.pem

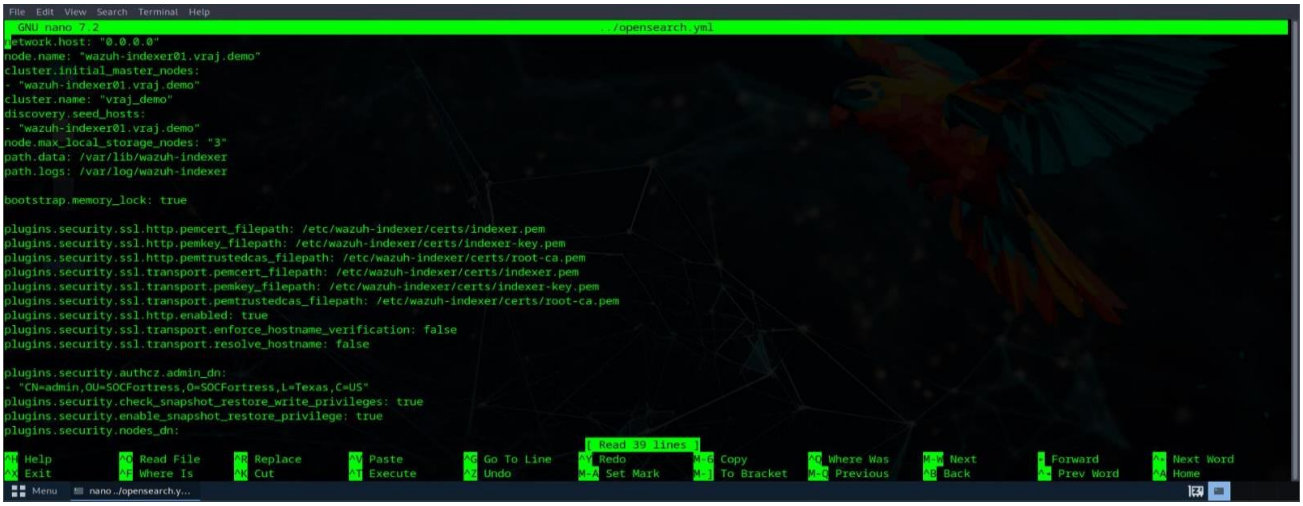
6. Set ownership and permissions

chmod 500 /etc/wazuh-indexer/certs chmod 400 /etc/wazuh-indexer/certs/* chown -R wazuh-indexer:wazuh-indexer /etc/wazuh-indexer/certs

Wazuh Indexer Configuration



Memory Locking
Uncomment or add this line to the /etc/wazuh-indexer/opensearch.yml file:
bootstrap.memory_lock: true



2. Edit the limit of system resources:

nano /usr/lib/systemd/system/wazuh-indexer.service

Place under [Service] block LimitMEMLOCK=infinity

3. Set JVM Options to 50% of total memory available

nano /etc/wazuh- indexer/jvm.options

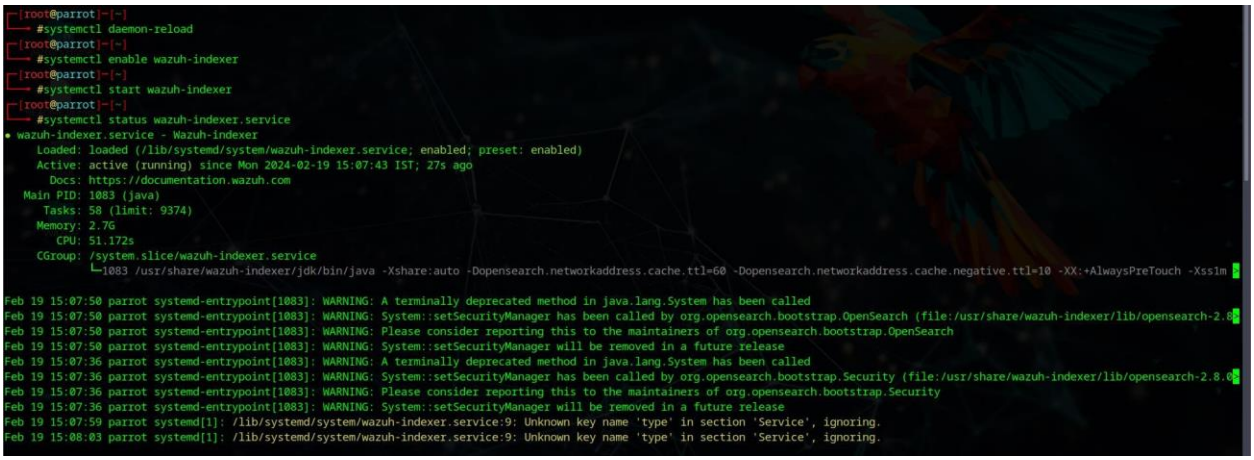
change Xms1g to Xms2g.

Start the Service

systemctl daemon-reload

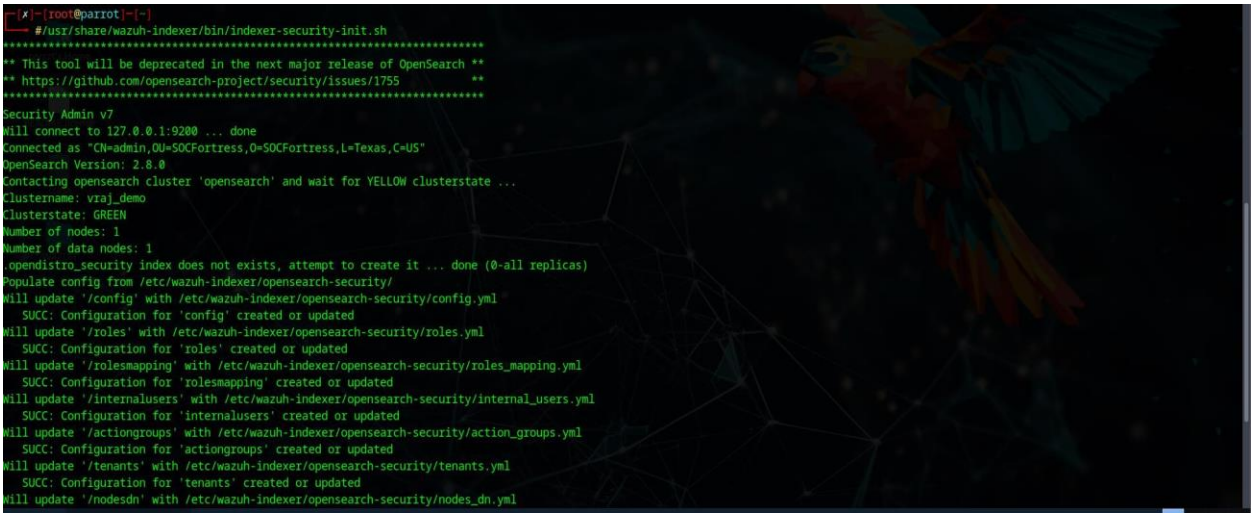
systemctl enable wazuh-indexer

systemctl start wazuh-indexer



Cluster Initialization

/usr/share/wazuh-indexer/bin/indexer-security-init.sh

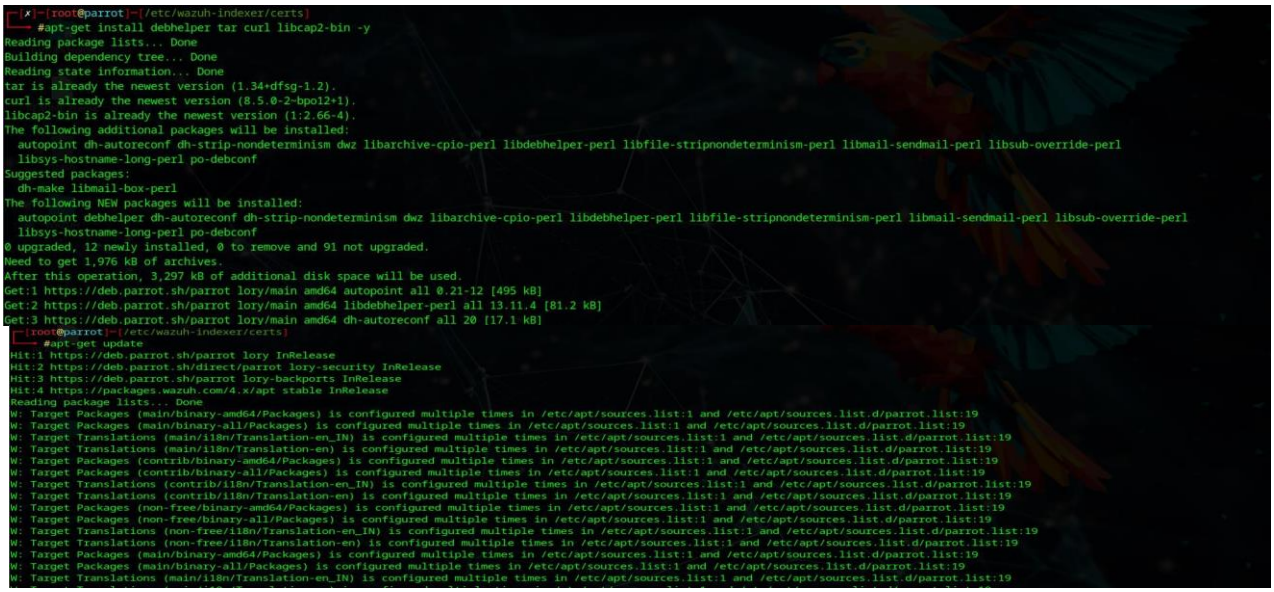


Install Wazuh-Dashboard

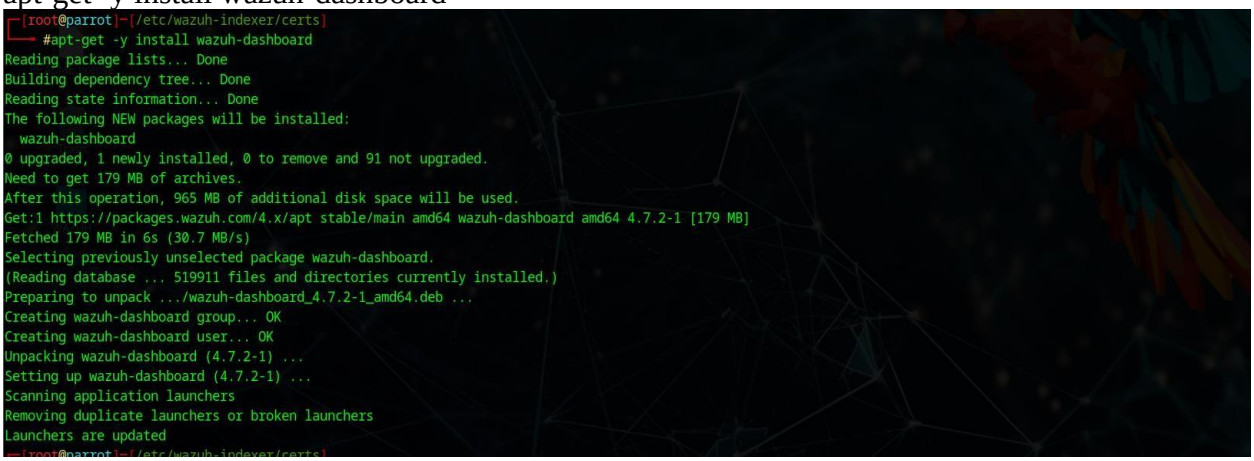
Only needs to be installed on Wazuh-Indexer Node 01

Install Prerequisites:

apt-get install debhelper tar curl libcap2-bin -y apt-get update

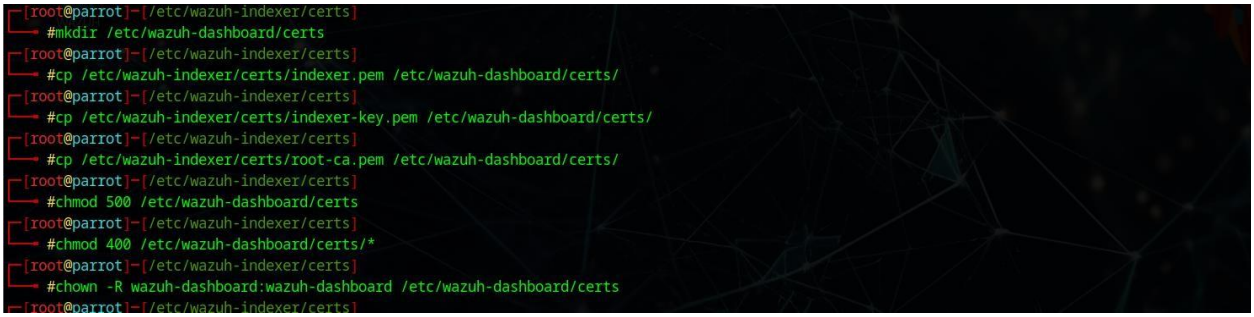


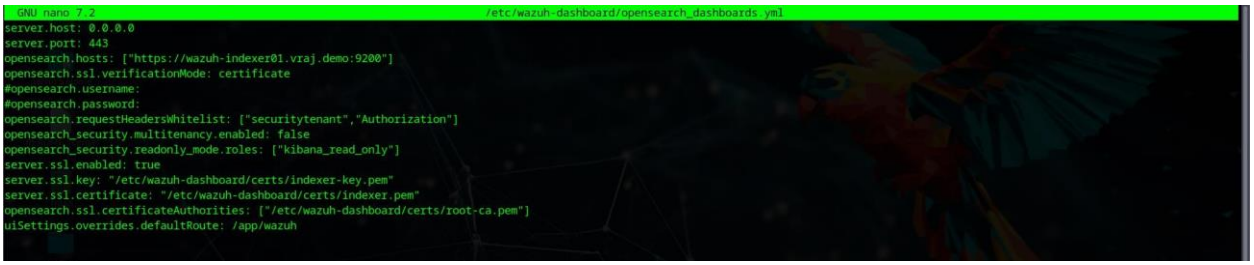
2. Install:
apt-get -y install wazuh-dashboard



Configure Wazuh-Dashboard

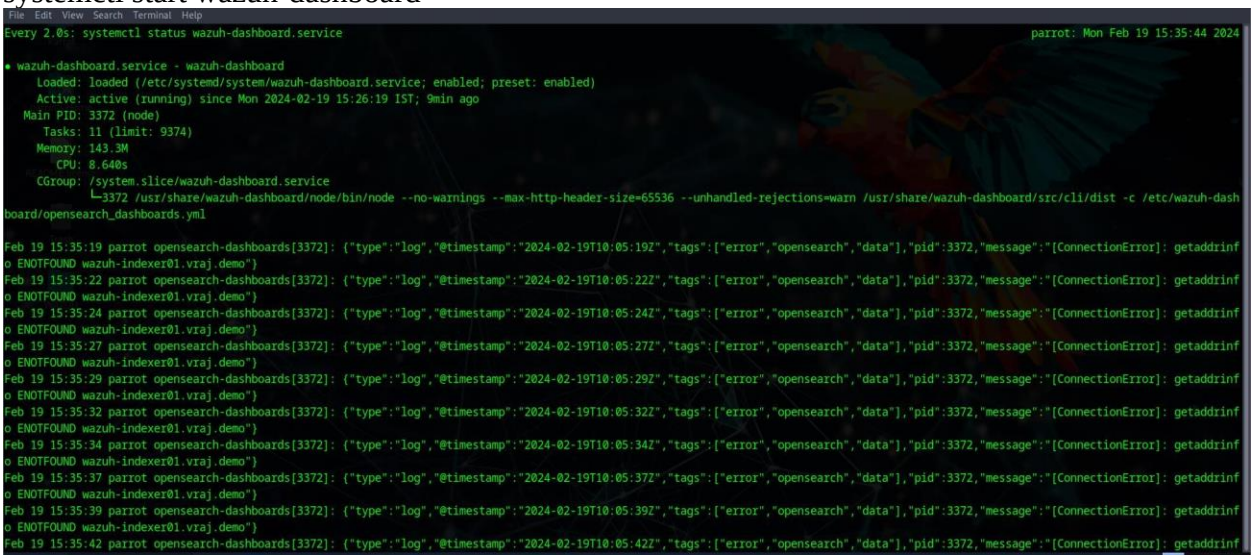
Configure certificates so that Wazuh-Dashboard service can connect to the Wazuh-Indexer cluster. mkdir /etc/wazuh-dashboard/certs cp /etc/wazuh-indexer/certs/indexer.pem /etc/wazuh-dashboard/certs/ cp /etc/wazuh-indexer/certs/indexer-key.pem /etc/wazuh-dashboard/certs/ cp /etc/wazuh-indexer/certs/root-ca.pem /etc/wazuh-dashboard/certs/ chmod 500 /etc/wazuh-dashboard/certs chmod 400 /etc/wazuh-dashboard/certs/*
chown -R wazuh-dashboard:wazuh-dashboard /etc/wazuh-dashboard/certs





Start Wazuh-Dashboard

systemctl daemon-reload
systemctl enable wazuh-dashboard
systemctl start wazuh-dashboard



Securing The Cluster

Update the default passwords of the admin and wazuh-dashboard users.

On the Wazuh Indexer Node 01, use the Wazuh passwords tool to change the passwords of the Wazuh indexer users.

Run Script

/usr/share/wazuh-indexer/plugins/opensearch-security/tools/wazuh-passwordstool.sh --change-all

```
┌──[root@parrot]─[/etc/wazuh-indexer/certs]
└─── #/usr/share/wazuh-indexer/plugins/opensearch-security/tools/wazuh-passwords-tool.sh --change-all
19/02/2024 15:39:39 INFO: Wazuh API admin credentials not provided, Wazuh API passwords not changed.
19/02/2024 15:39:52 INFO: The password for user admin is f3nSmfp93fej3UF7tkLVn+RtfVSNm5*T
19/02/2024 15:39:52 INFO: The password for user kibanaserver is 2OwH?uuYx*Vz+NLzUcH1iWKFSDyI2l*W
19/02/2024 15:39:52 INFO: The password for user kibanaro is 2jFx4Mk8+RmGkH6yH1?29jKJCkrOqmcN
19/02/2024 15:39:52 INFO: The password for user logstash is Ep8yrxELnXJ41SsPZ?ZMQ1E0c2buvmX+
19/02/2024 15:39:52 INFO: The password for user readall is hPV1qJZcpMZvy0*NT5jc5?Z6ACpGi5CO
19/02/2024 15:39:52 INFO: The password for user snapshotrestore is +PbOZ2TivyvK8VD2SRr4loLE4.Zr4sqH
19/02/2024 15:39:52 WARNING: Wazuh indexer passwords changed. Remember to update the password in the Wazuh dashboard and Filebeat nodes if necessary, and restart the services.
┌──[root@parrot]─[/etc/wazuh-indexer/certs]
```

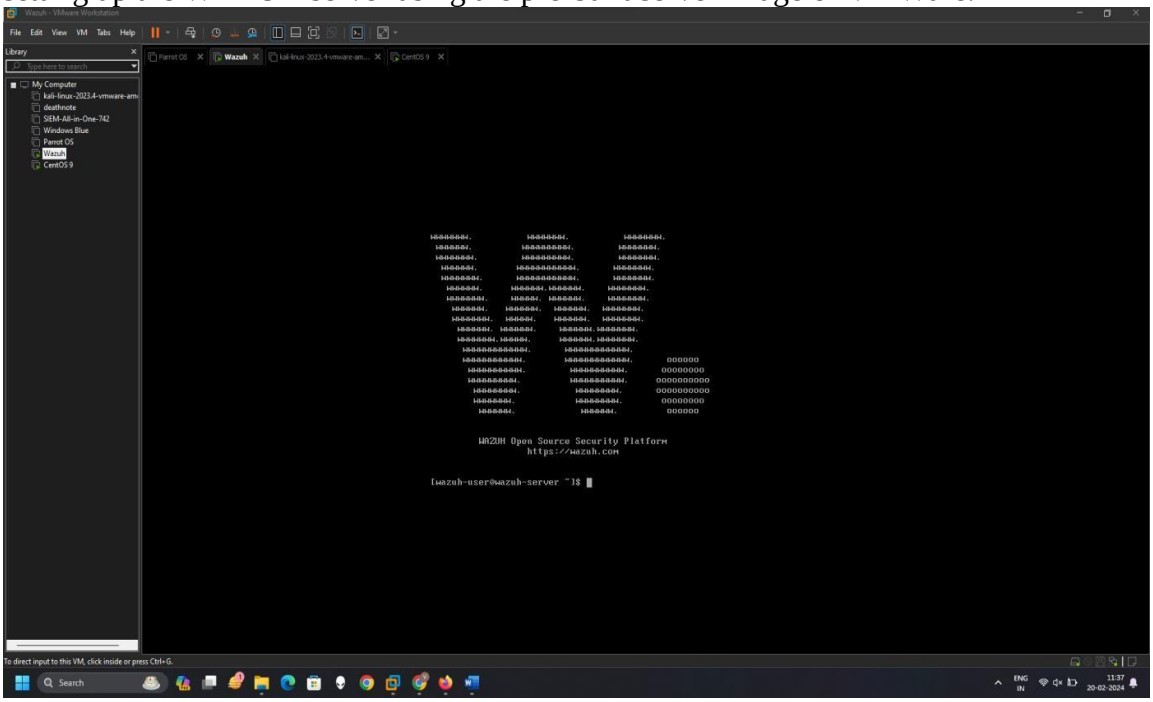
2. Change Wazuh Dashboard Password:

On your Wazuh dashboard node, run the following command to update the kibanaserver password in the Wazuh dashboard keystore. Replace <kibanaserver-password> with the random password generated in the first step. echo <kibanaserver-password> | /usr/share/wazuh-dashboard/bin/opensearchdashboards-keystore --allow-root add -f --stdin opensearch.password

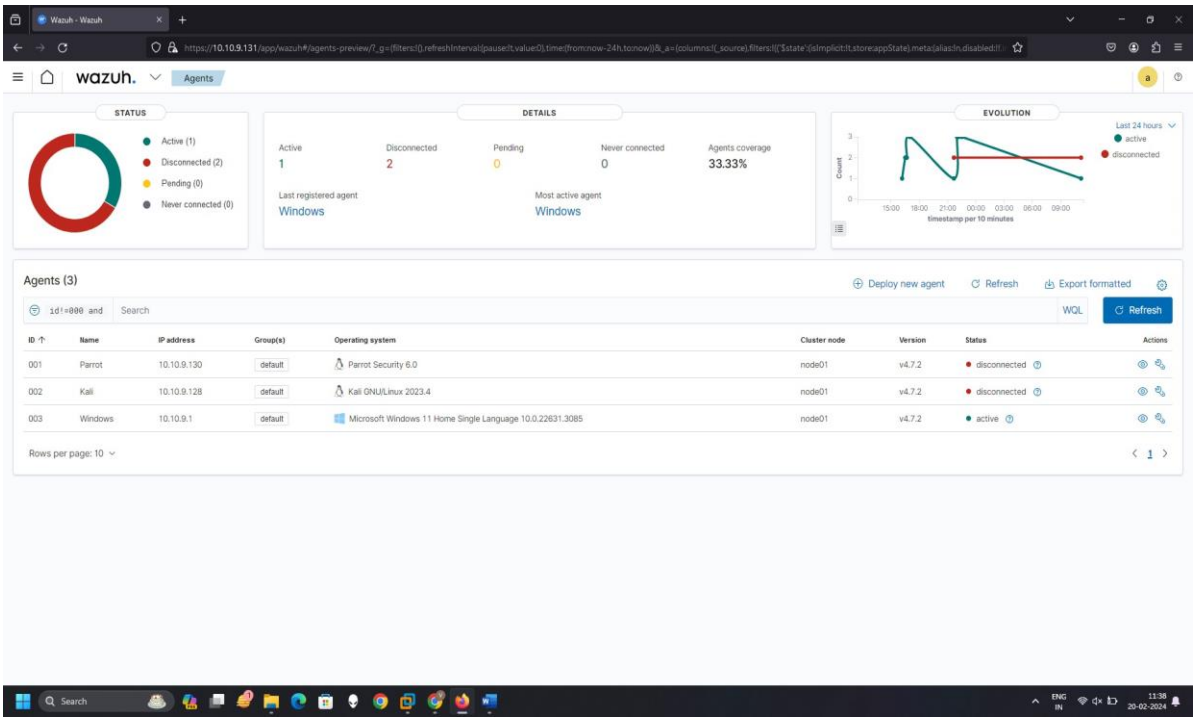
```
┌──[root@parrot]─[/etc/wazuh-indexer/certs]
└─── #echo 2OwH?uuYx*Vz+NLzUcH1iWKFSDyI2l*W | /usr/share/wazuh-dashboard/bin/opensearch-dashboards-keystore --allow-root add -f --stdin opensearch.password
v16.20.0
```

3. Restart the service systemctl restart wazuh-dashboard

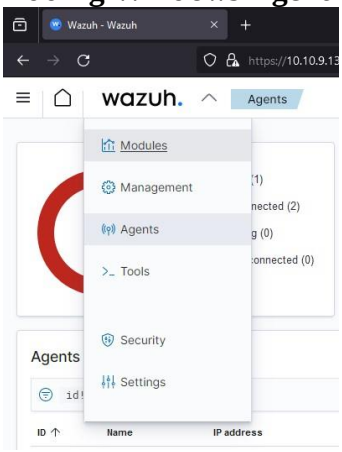
Got some connection error for dashboard tried to troubleshoot it but not getting the solution so setting up the WAZUH server using the pre-built server image of VMWare.



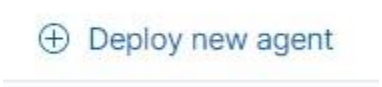
WAZUH Dashboard –



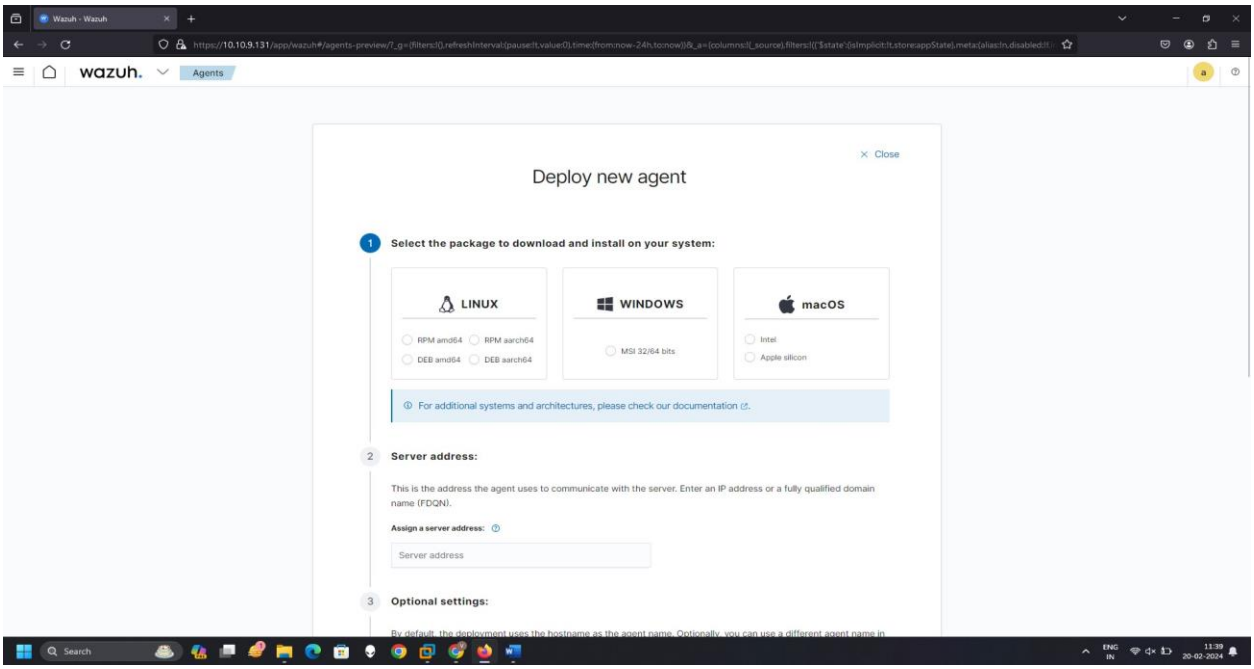
Adding Windows Agent –



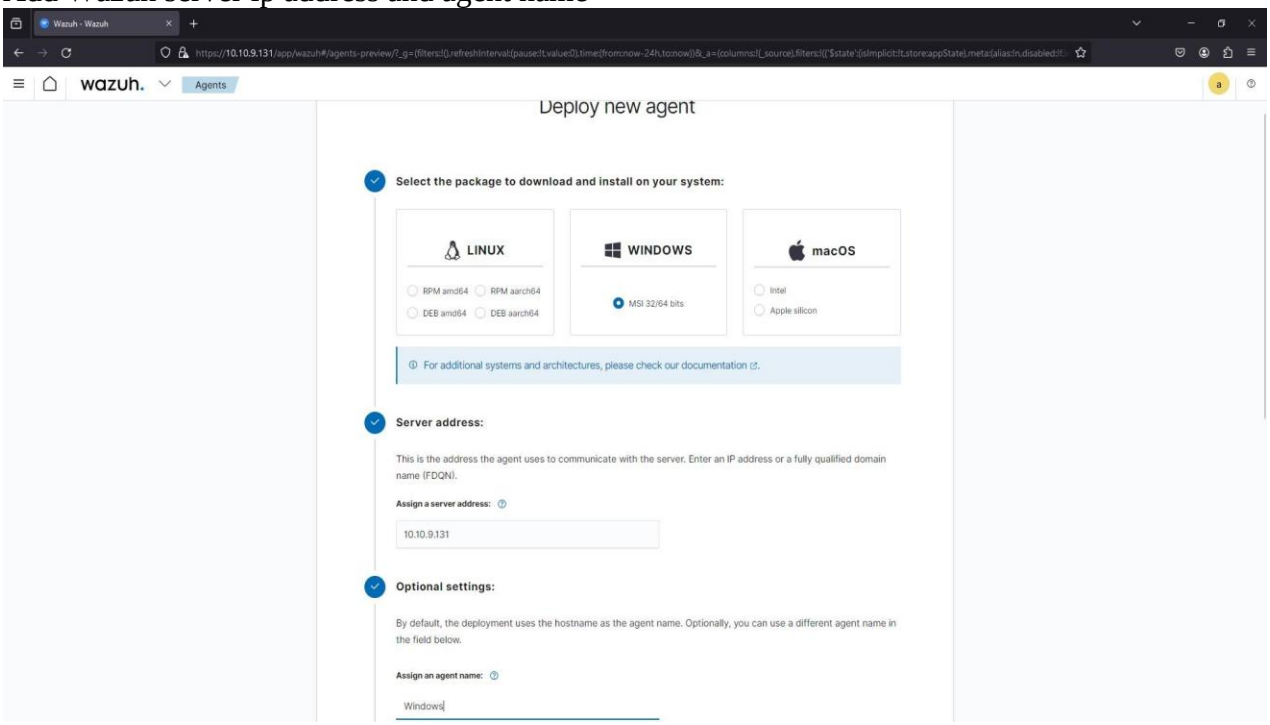
Goto –



Select the source –



Add Wazuh server ip address and agent name –



Run the following commands in windows powershell.

4 **Run the following commands to download and install the agent:**

```
Invoke-WebRequest -Uri https://packages.wazuh.com/4.x/windows/wazuh-agent-4.7.2-1.msi -OutFile $
{env.tmp}\wazuh-agent; msiexec.exe /i ${env.tmp}\wazuh-agent /q WAZUH_MANAGER='10.10.9.131'
WAZUH_AGENT_GROUP='default' WAZUH_AGENT_NAME='Windows' WAZUH_REGISTRATION_SERVER='10.10.9.131'
```

ⓘ Requirements

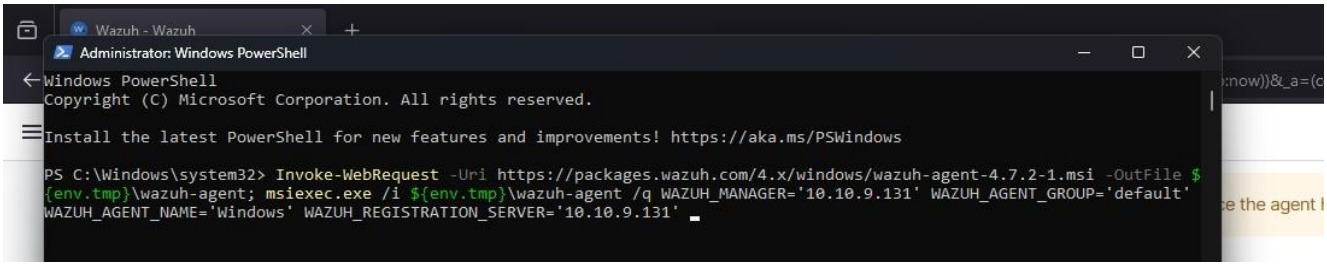
- You will need administrator privileges to perform this installation.
- PowerShell 3.0 or greater is required.

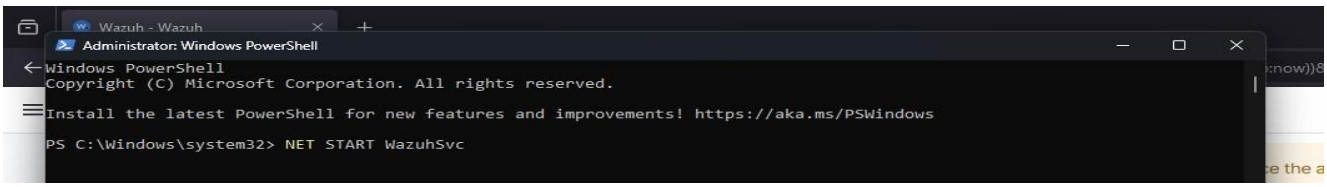
Keep in mind you need to run this command in a Windows PowerShell terminal.

5 **Start the agent:**

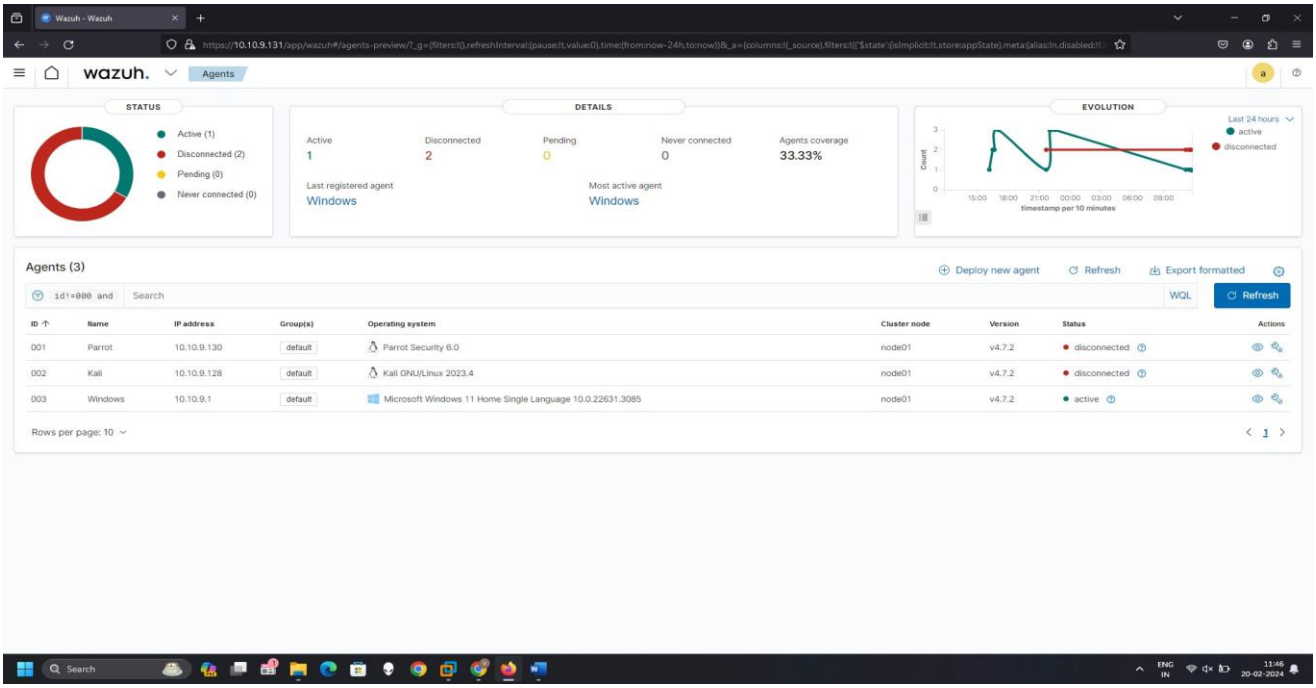
```
NET START WazuhSvc
```

Run the command –



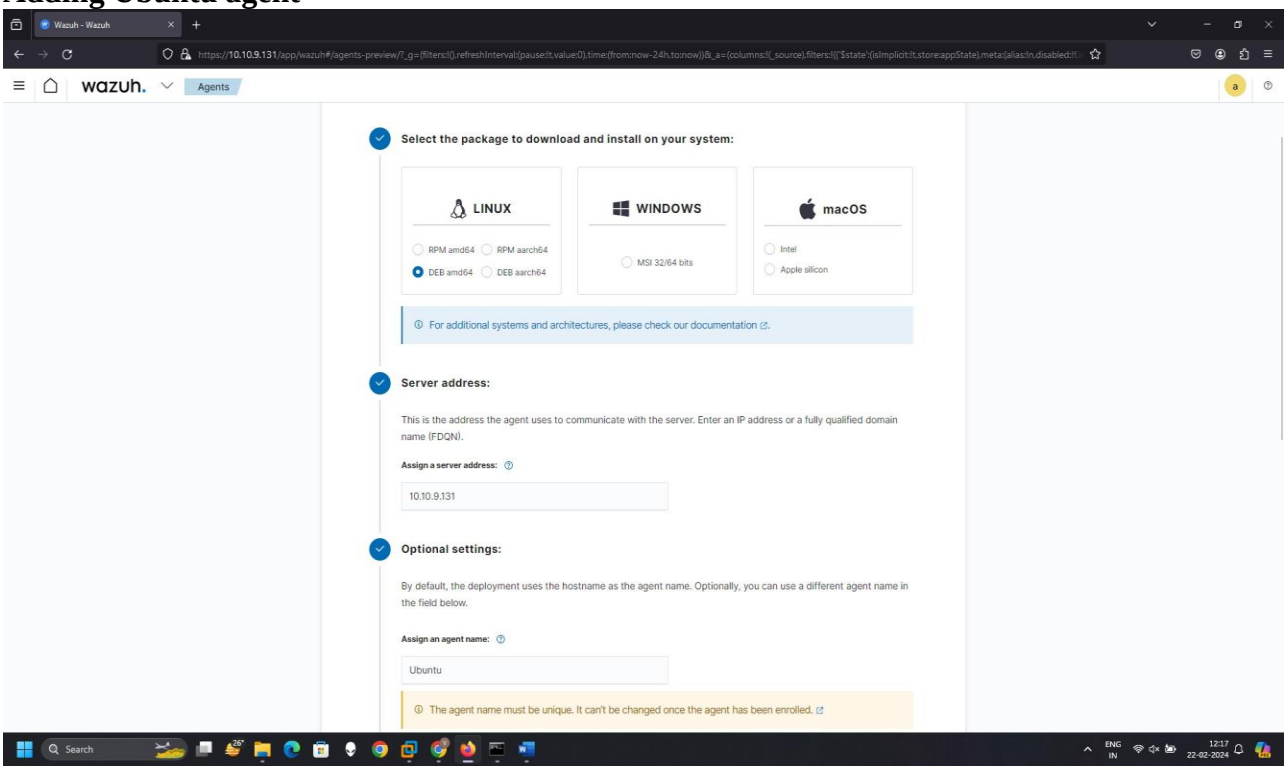


Agent added Successfully –



Windows agent added and status is active.

Adding Ubuntu agent –



Run the following commands to download and install the agent:

```
wget https://packages.wazuh.com/4.x/apt/pool/main/w/wazuh-agent/wazuh-agent_4.7.2-1_amd64.deb &&
sudo WAZUH_MANAGER='10.10.9.131' WAZUH_AGENT_GROUP='linux' WAZUH_AGENT_NAME='Ubuntu' dpkg -i ./
wazuh-agent_4.7.2-1_amd64.deb
```

Requirements

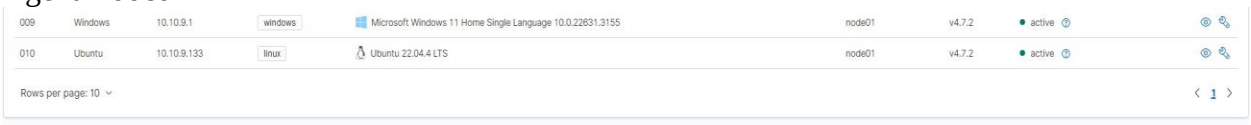
- You will need administrator privileges to perform this installation.
- Shell Bash is required.

Keep in mind you need to run this command in a Shell Bash terminal.

5 Start the agent:

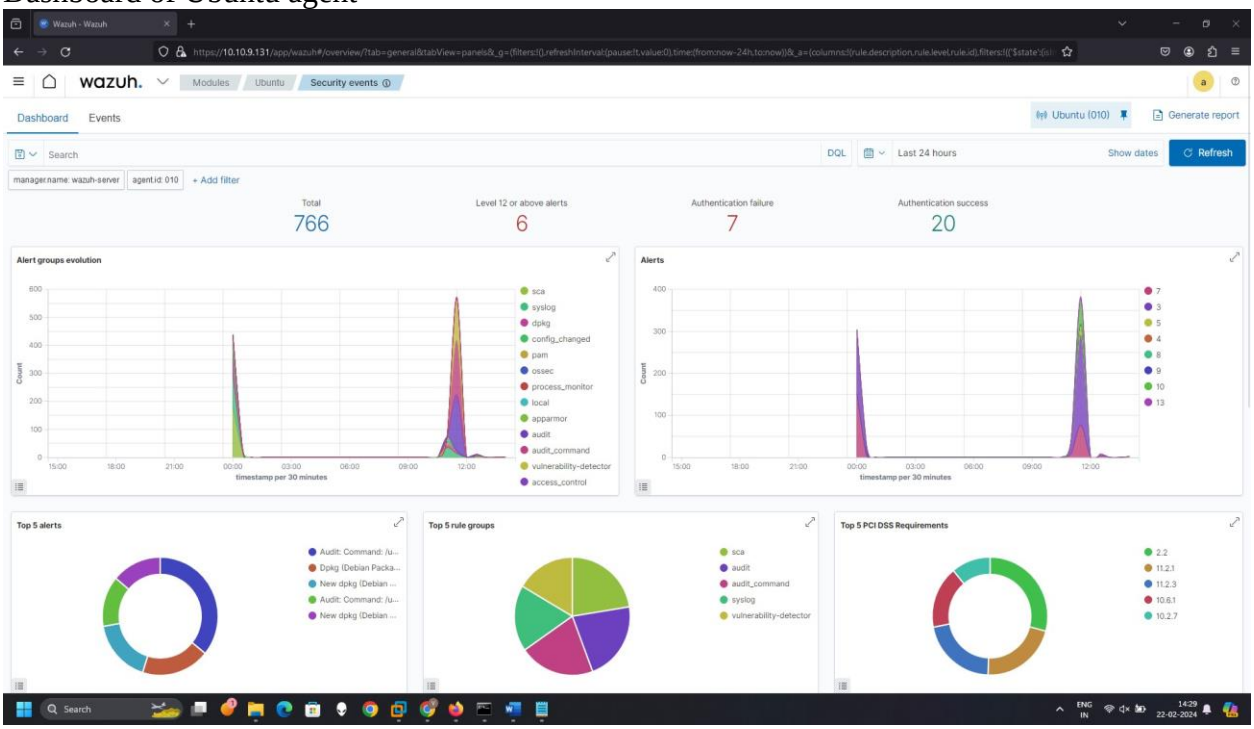
```
sudo systemctl daemon-reload
sudo systemctl enable wazuh-agent
sudo systemctl start wazuh-agent
```

Running the following commands in ubuntu.
Agent Added –

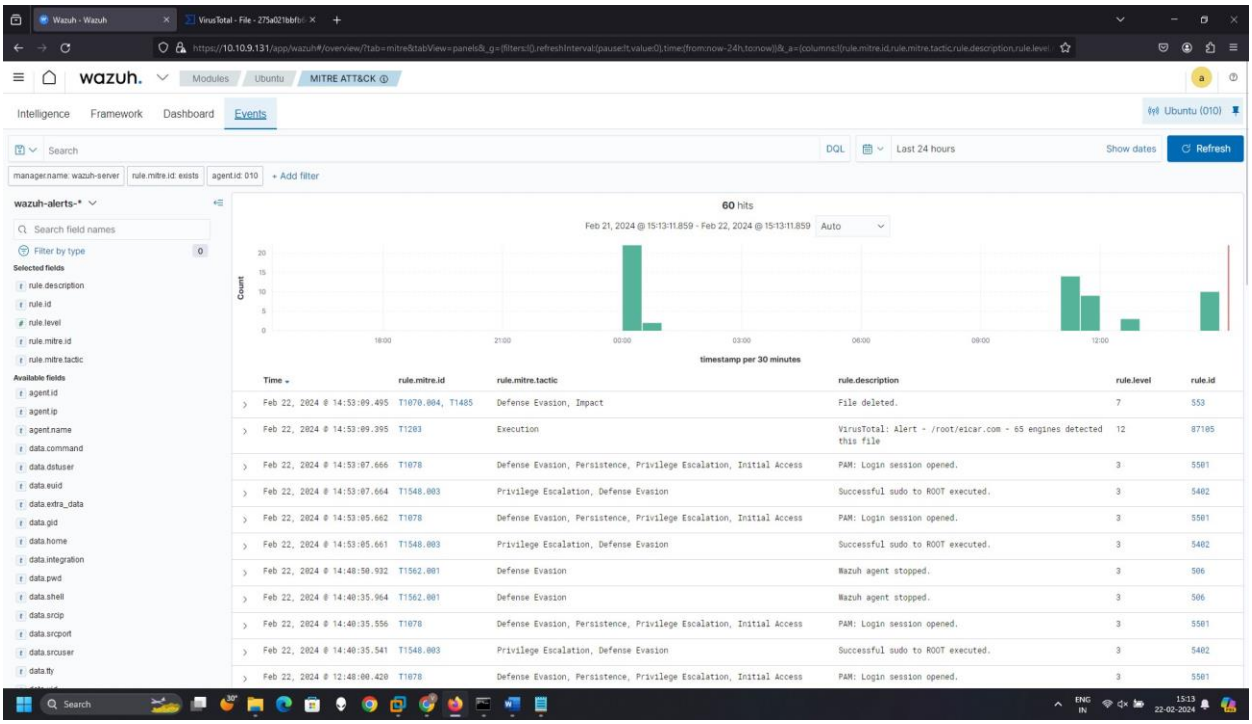


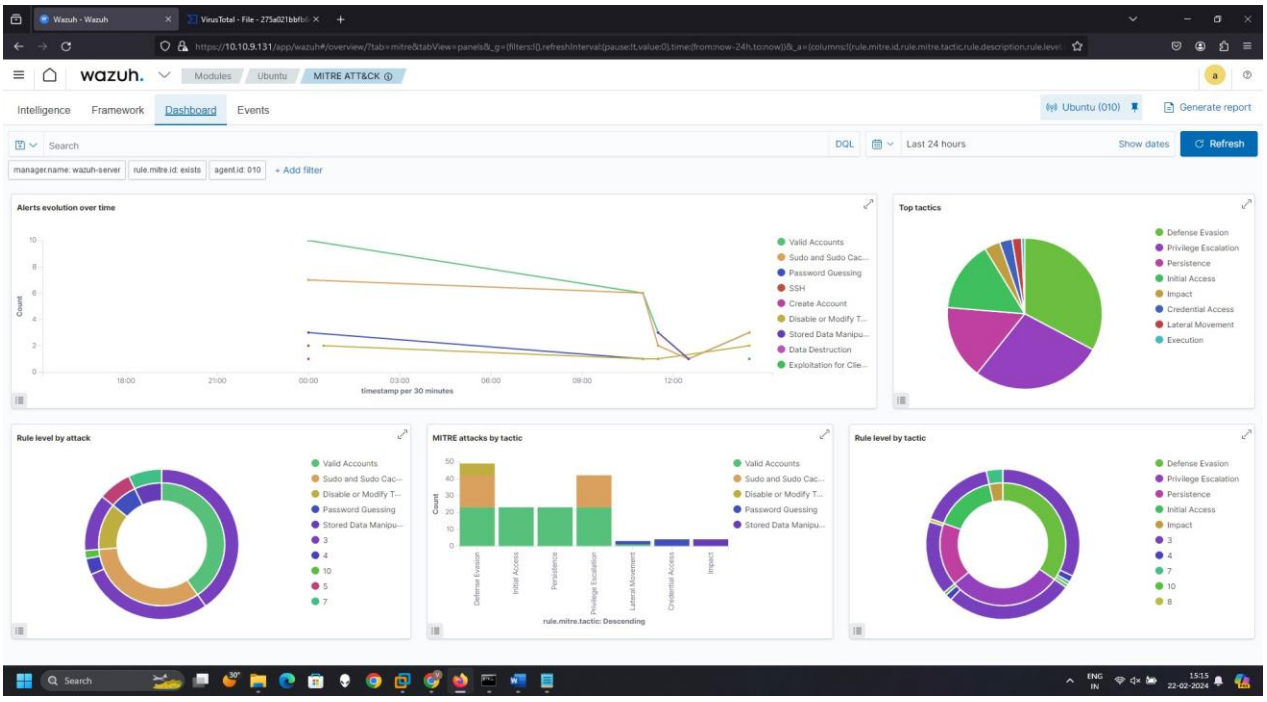
Looking at the basic logs –

Dashboard of Ubuntu agent

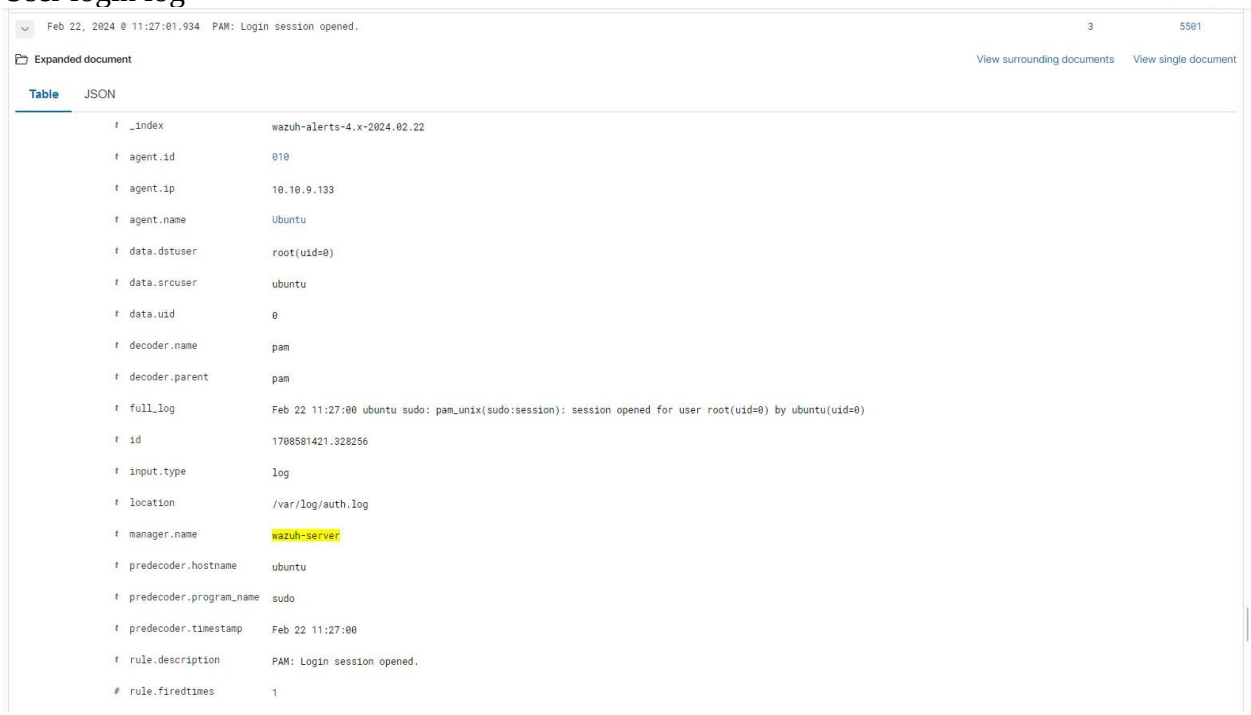


MITRE ATT&CK

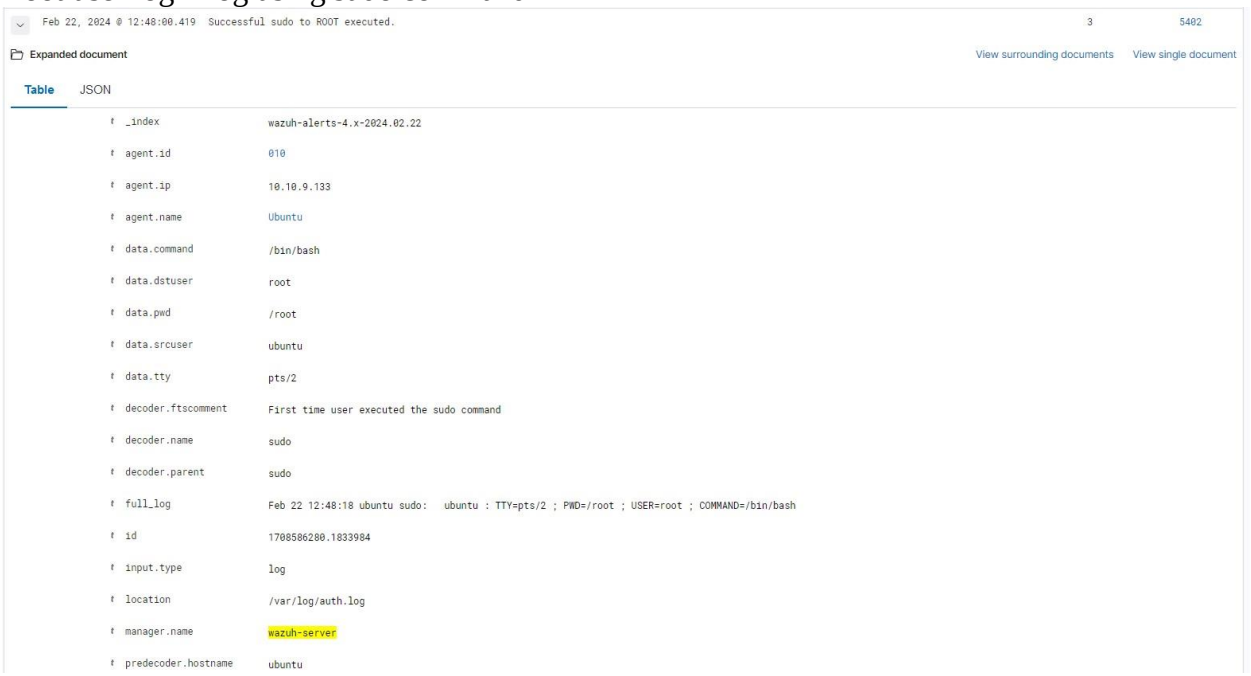

wazuh.
Modules
Ubuntu
MITRE ATT&CK
Intelligence
Framework
Dashboard
Events
Ubuntu (010)
Search
DQL
Last 24 hours
Show dates
Refresh
manager.name: wazuh-server
rule.mitre.id: exists
agent.id: 010
+ Add filter
wazuh-alerts-*
Search field names
Filter by type
Selected fields
rule.description
rule.id
rule.level
rule.mitre.id
rule.mitre.tactic
Available fields
agent.id
agent.ip
agent.name
data.command
data.dstuser
data.euid
data.extra_data
data.gid
data.home
data.integration
data.pwd
data.shell
data.srcip
data.srcport
data.srcuser
data.tty
60 hits
Feb 21, 2024 @ 15:13:11.859 - Feb 22, 2024 @ 15:13:11.859
Auto
Count
timestamp per 30 minutes
Time
rule.mitre.id
rule.mitre.tactic
rule.description
rule.level
rule.id
Feb 22, 2024 @ 14:53:09.495 T1070.004, T1485 Defense Evasion, Impact File deleted. 7 553
Feb 22, 2024 @ 14:53:09.395 T1203 Execution VirusTotal: Alert - /root/eicar.com - 65 engines detected this file 12 87105
Feb 22, 2024 @ 14:53:07.666 T1078 Defense Evasion, Persistence, Privilege Escalation, Initial Access PAM: Login session opened. 3 5501
Feb 22, 2024 @ 14:53:07.664 T1548.003 Privilege Escalation, Defense Evasion Successful sudo to ROOT executed. 3 5402
Feb 22, 2024 @ 14:53:05.662 T1078 Defense Evasion, Persistence, Privilege Escalation, Initial Access PAM: Login session opened. 3 5501
Feb 22, 2024 @ 14:53:05.661 T1548.003 Privilege Escalation, Defense Evasion Successful sudo to ROOT executed. 3 5402
Feb 22, 2024 @ 14:48:50.932 T1562.001 Defense Evasion Wazuh agent stopped. 3 506
Feb 22, 2024 @ 14:40:35.964 T1562.001 Defense Evasion Wazuh agent stopped. 3 506
Feb 22, 2024 @ 14:40:35.556 T1078 Defense Evasion, Persistence, Privilege Escalation, Initial Access PAM: Login session opened. 3 5501
Feb 22, 2024 @ 14:40:35.541 T1548.003 Privilege Escalation, Defense Evasion Successful sudo to ROOT executed. 3 5402
Feb 22, 2024 @ 12:48:00.420 T1078 Defense Evasion, Persistence, Privilege Escalation, Initial Access PAM: Login session opened. 3 5501


wazuh.
Modules
Ubuntu
MITRE ATT&CK
Intelligence
Framework
Dashboard
Events
Ubuntu (010)
Generate report
Search
DQL
Last 24 hours
Show dates
Refresh
manager.name: wazuh-server
rule.mitre.id: exists
agent.id: 010
+ Add filter
Alerts evolution over time
Count
timestamp per 30 minutes
Valid Accounts
Sudo and Sudo Cac...
Password Guessing
SSH
Create Account
Disable or Modify T...
Stored Data Manipu...
Data Destruction
Exploitation for Clie...
Top tactics
Defense Evasion
Privilege Escalation
Persistence
Initial Access
Impact
Credential Access
Lateral Movement
Execution
Rule level by attack
Valid Accounts
Sudo and Sudo Cac...
Disable or Modify T...
Password Guessing
Stored Data Manipu...
3
4
10
5
7
MITRE attacks by tactic
Count
Defense Evasion
Initial Access
Persistence
Privilege Escalation
Lateral Movement
Credential Access
Impact
rule.mitre.tactic: Descending
Rule level by tactic
Defense Evasion
Privilege Escalation
Persistence
Initial Access
Impact
3
4
7
10
8

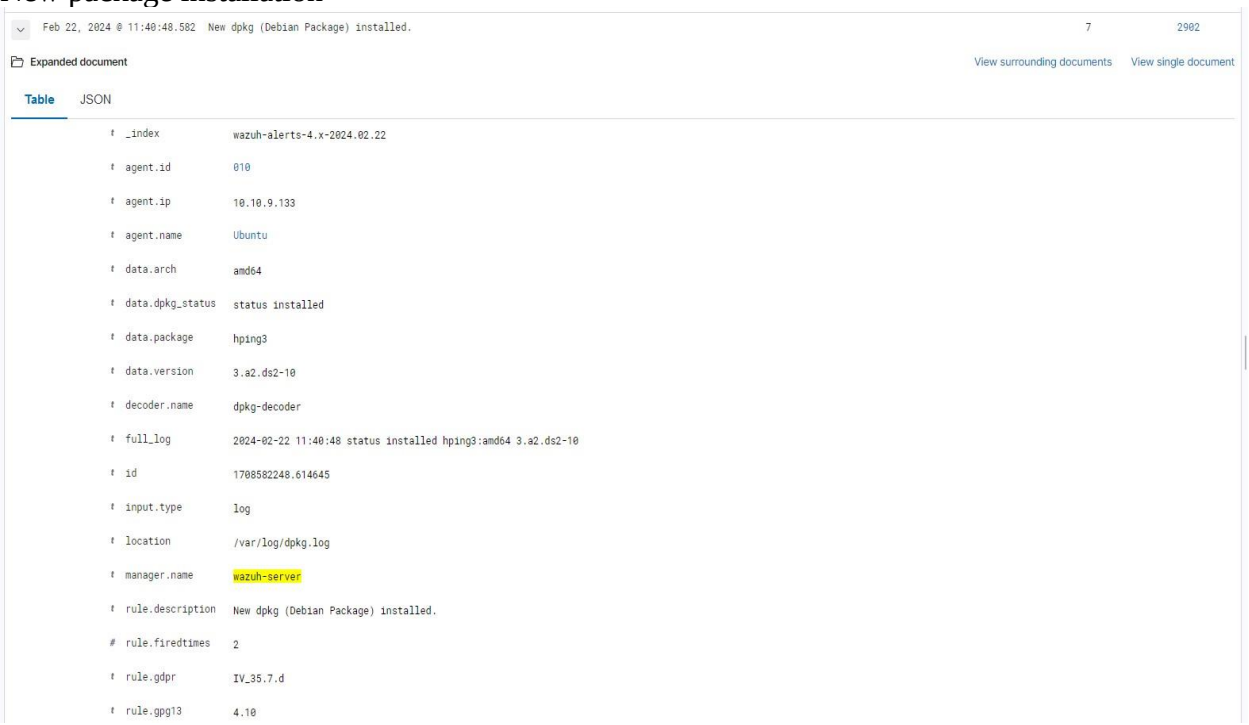
User login log



Root user login log using sudo command



New package installation



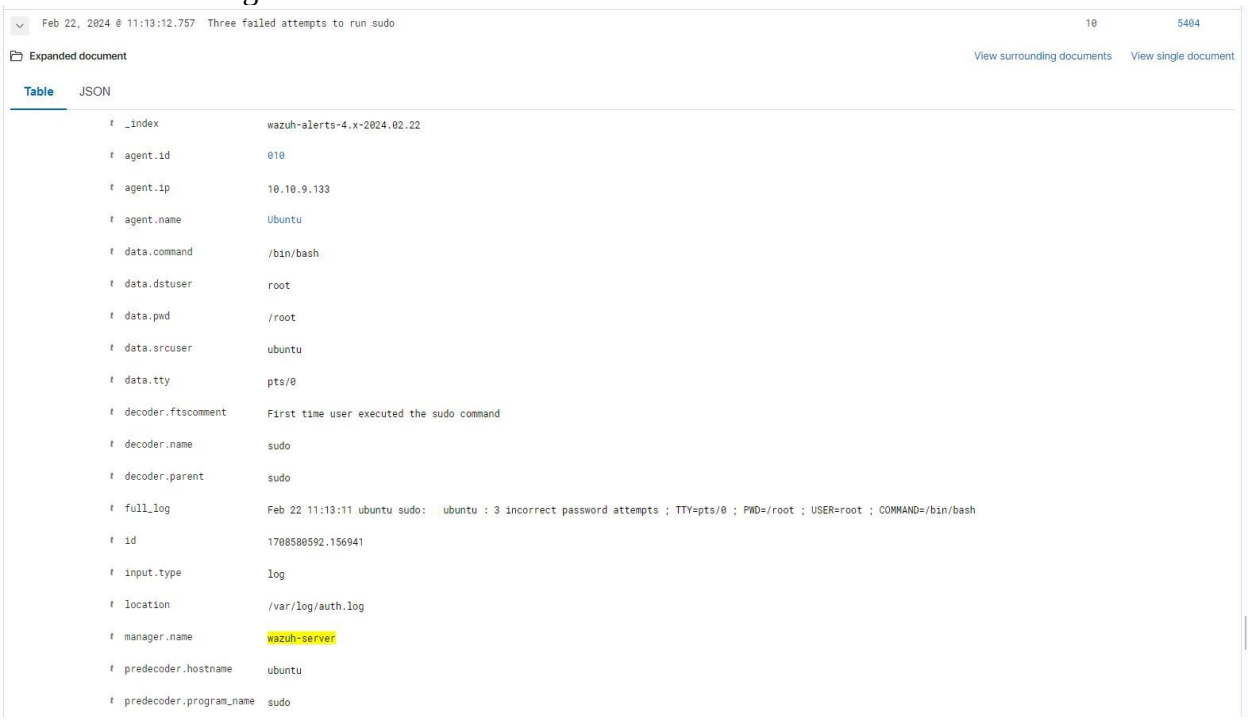
Feb 22, 2024 @ 11:40:48.582 New dpkg (Debian Package) installed. 7 2902

Expanded document View surrounding documents View single document

Table JSON

t _index	wazuh-alerts-4.x-2024.02.22
t agent.id	010
t agent.ip	10.10.9.133
t agent.name	Ubuntu
t data.arch	amd64
t data.dpkg_status	status installed
t data.package	hping3
t data.version	3.a2.ds2-10
t decoder.name	dpkg-decoder
t full_log	2024-02-22 11:40:48 status installed hping3:amd64 3.a2.ds2-10
t id	1708582248.614645
t input.type	log
t location	/var/log/dpkg.log
t manager.name	wazuh-server
t rule.description	New dpkg (Debian Package) installed.
# rule.firedtimes	2
t rule.gdpr	IV_35.7.d
t rule.gpg13	4.10

Failed sudo user login –



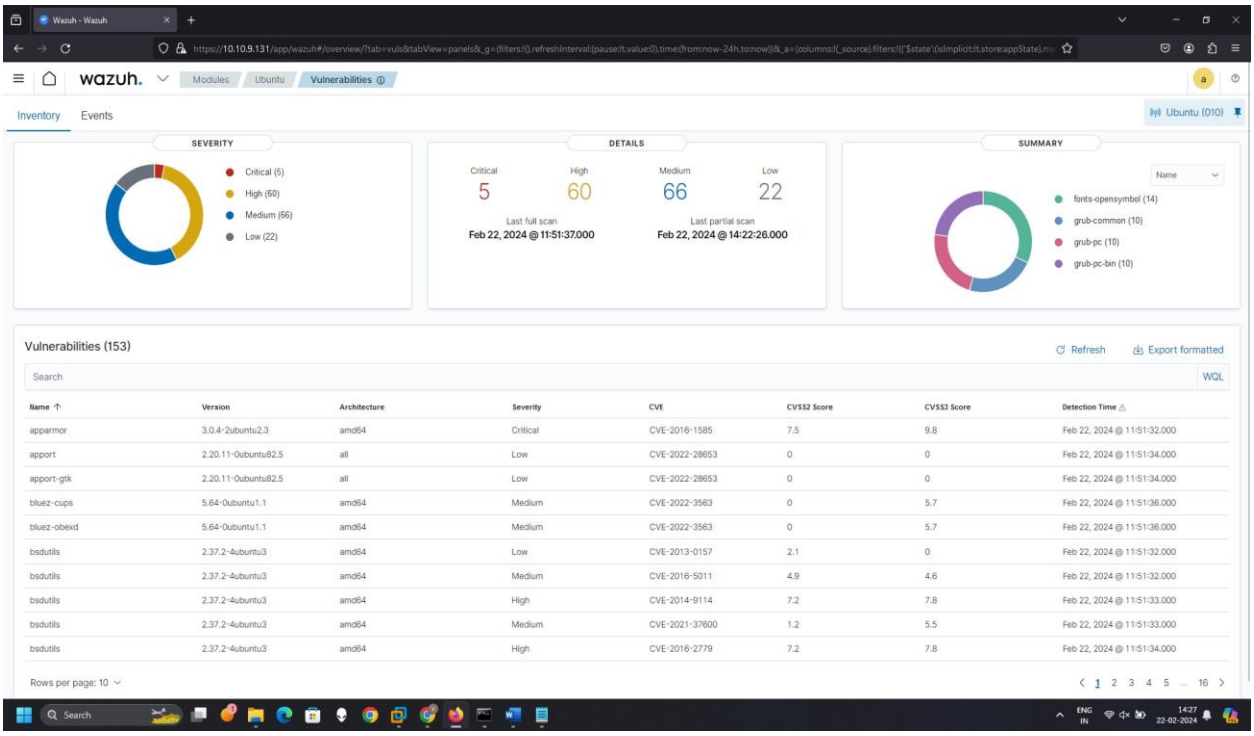
Feb 22, 2024 @ 11:13:12.757 Three failed attempts to run sudo 10 5404

Expanded document View surrounding documents View single document

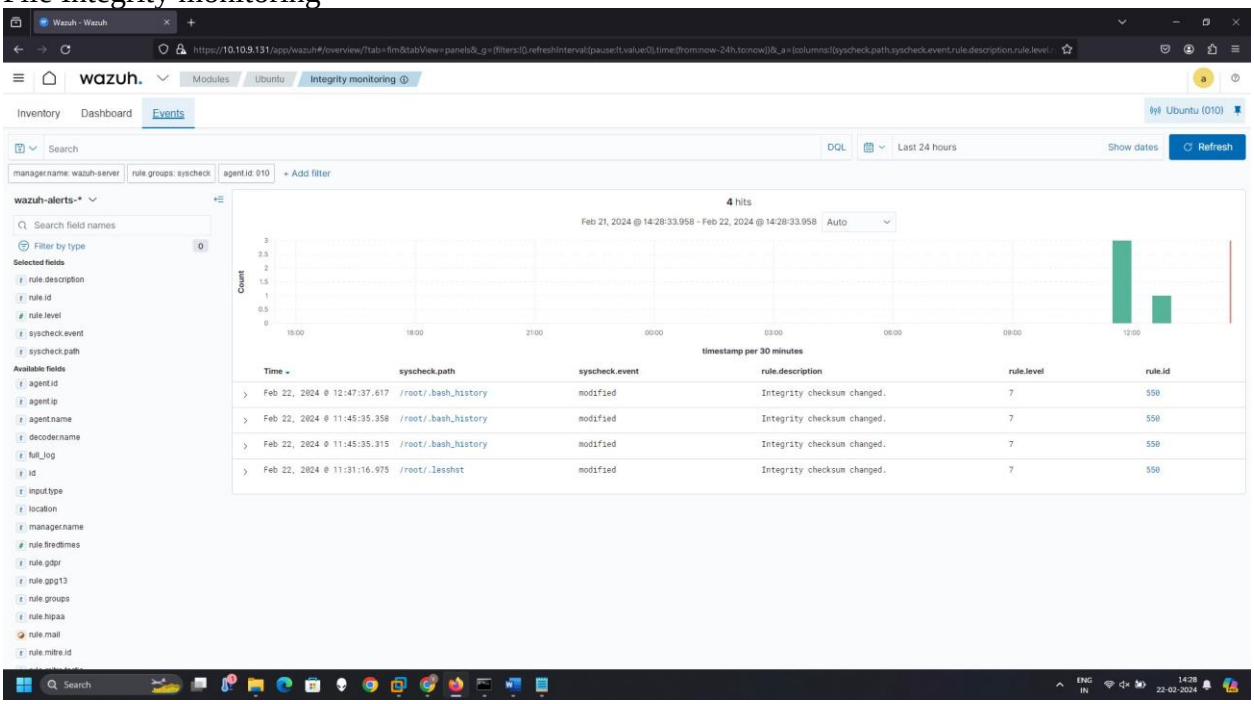
Table JSON

t _index	wazuh-alerts-4.x-2024.02.22
t agent.id	010
t agent.ip	10.10.9.133
t agent.name	Ubuntu
t data.command	/bin/bash
t data.dstuser	root
t data.pwd	/root
t data.srcuser	ubuntu
t data.tty	pts/0
t decoder.ftscomment	First time user executed the sudo command
t decoder.name	sudo
t decoder.parent	sudo
t full_log	Feb 22 11:13:11 ubuntu sudo: ubuntu : 3 incorrect password attempts ; TTY=pts/0 ; PWD=/root ; USER=root ; COMMAND=/bin/bash
t id	1708580592.156941
t input.type	log
t location	/var/log/auth.log
t manager.name	wazuh-server
t predecoder.hostname	ubuntu
t predecoder.program_name	sudo

Vulnerabilities



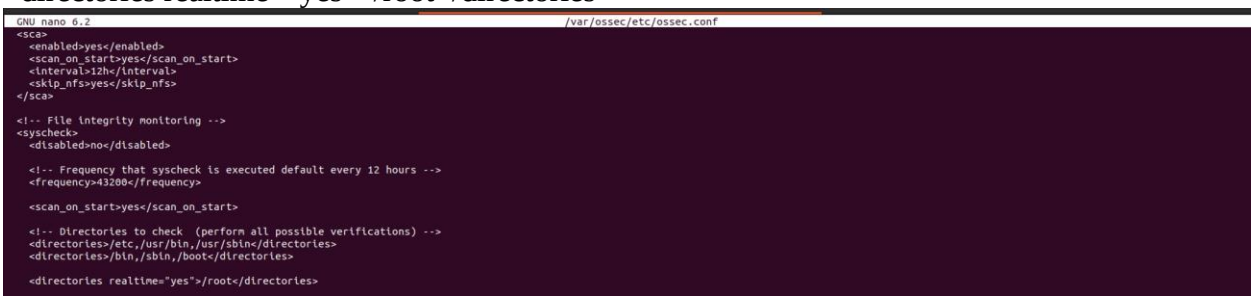
File Integrity monitoring



CHAPTER: 7 INTEGRATING VIRUSTOTAL

CHAPTER: 7 INTEGRATING VIRUSTOTAL

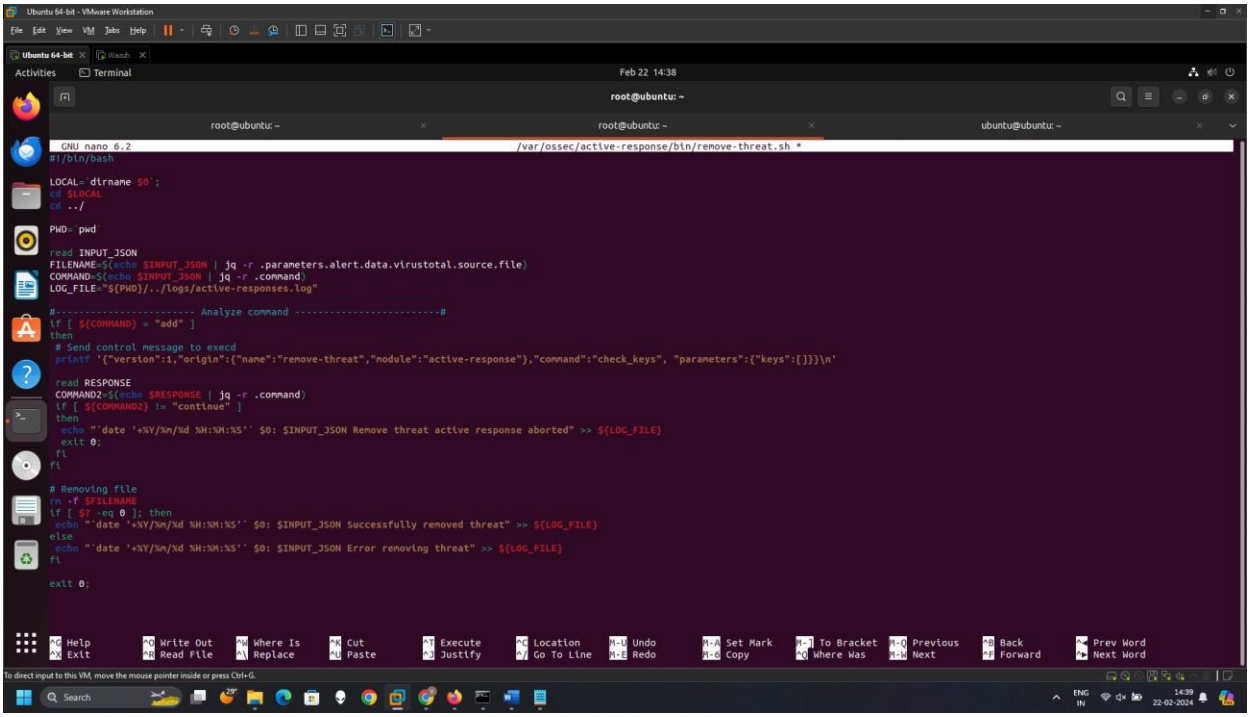
Search for the <syscheck> block in the Wazuh agent configuration file /var/ossec/etc/ossec.conf. Make sure that <disabled> is set to no. This enables the Wazuh FIM to monitor for directory changes.
Add an entry within the <syscheck> block to configure a directory to be monitored in near real-time. In this case, you are monitoring the /root directory:
<directories realtime="yes">/root</directories>



Install jq, a utility that processes JSON input from the active response script.
sudo apt update sudo apt -y install jq

```
root@ubuntu:~# apt -y install jq
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  libjq1 libonig5
The following NEW packages will be installed:
  jq libjq1 libonig5
0 upgraded, 3 newly installed, 0 to remove and 0 not upgraded.
Need to get 357 kB of archives.
After this operation, 1,087 kB of additional disk space will be used.
Get:1 http://in.archive.ubuntu.com/ubuntu jammy/main amd64 libonig5 amd64 6.9.7.1-2build1 [172 kB]
Get:2 http://in.archive.ubuntu.com/ubuntu jammy/main amd64 libjq1 amd64 1.6-2.1ubuntu3 [133 kB]
Get:3 http://in.archive.ubuntu.com/ubuntu jammy/main amd64 jq amd64 1.6-2.1ubuntu3 [52.5 kB]
Fetched 357 kB in 1s (299 kB/s)
Selecting previously unselected package libonig5:amd64.
(Reading database ... 203534 files and directories currently installed.)
Preparing to unpack .../libonig5_6.9.7.1-2build1_amd64.deb ...
Unpacking libonig5:amd64 (6.9.7.1-2build1) ...
Selecting previously unselected package libjq1:amd64.
Preparing to unpack .../libjq1_1.6-2.1ubuntu3_amd64.deb ...
Unpacking libjq1:amd64 (1.6-2.1ubuntu3) ...
Selecting previously unselected package jq.
Preparing to unpack .../jq_1.6-2.1ubuntu3_amd64.deb ...
Unpacking jq (1.6-2.1ubuntu3) ...
Setting up libonig5:amd64 (6.9.7.1-2build1) ...
Setting up libjq1:amd64 (1.6-2.1ubuntu3) ...
Setting up jq (1.6-2.1ubuntu3) ...
Processing triggers for man-db (2.10.2-1) ...
Processing triggers for libc-bin (2.35-0ubuntu3.6) ...
root@ubuntu:~#
```

Create the /var/ossec/active-response/bin/remove-threat.sh active response script to remove malicious files from the endpoint:



Change the /var/ossec/active-response/bin/remove-threat.sh file ownership, and permissions:
sudo chmod 750 /var/ossec/active-response/bin/remove-threat.sh sudo chown root:wazuh /var/ossec/active-response/bin/remove-threat.sh

```
root@ubuntu:~# chmod 750 /var/ossec/active-response/bin/remove-threat.sh
root@ubuntu:~# chown root:wazuh /var/ossec/active-response/bin/remove-threat.sh
root@ubuntu:~#
```

Restart the Wazuh agent to apply the changes:
sudo systemctl restart wazuh-agent

```
root@ubuntu:~# sudo systemctl restart wazuh-agent
root@ubuntu:~#
```

Wazuh server

Perform the following steps on the Wazuh server to alert for changes in the endpoint directory and enable the VirusTotal integration. These steps also enable and trigger the active response script whenever a suspicious file is detected.
Add the following rules to the /var/ossec/etc/rules/local_rules.xml file on the Wazuh server. These rules alert about changes in the /root directory that are detected by FIM scans:

```
<group name="syscheck,pci_dss_11.5,nist_800_53_SI.7,">
  <!-- Rules for Linux systems -->
  <rule id="100200" level="7">
    <if_sid>550</if_sid>
    <field name="file">/root</field>
    <description>File modified in /root directory.</description>
  </rule>
  <rule id="100201" level="7">
    <if_sid>554</if_sid>
```

```
    <field name="file">/root</field>
    <description>File added to /root directory.</description>
  </rule>
</group>
```

```
<group name="syscheck,pci_dss_11.5,nist_800_53_SI.7,">
    <!-- Rules for Linux systems -->
    <rule id="100200" level="7">
        <if_sid>550</if_sid>
        <field name="file">/root</field>
        <description>File modified in /root directory.</description>
    </rule>
    <rule id="100201" level="7">
        <if_sid>554</if_sid>
        <field name="file">/root</field>
        <description>File added to /root directory.</description>
    </rule>
</group>
```

Add the following configuration to the Wazuh server /var/ossec/etc/ossec.conf file to enable the Virustotal integration. Replace <YOUR_VIRUS_TOTAL_API_KEY> with your VirusTotal API key. This allows to trigger a VirusTotal query whenever any of the rules 100200 and 100201 are triggered:

```
<ossec_config>
  <integration>
    <name>virustotal</name>
    <api_key><YOUR_VIRUS_TOTAL_API_KEY></api_key> <!-- Replace with your VirusTotal API key -->
    <rule_id>100200,100201</rule_id>
    <alert_format>json</alert_format>
  </integration>
</ossec_config>
```

```
<ossec_config>
  <integration>
    <name>virustotal</name>
    <api_key>196a8d525e15c1f01d4a397272af2076a8803ed0591dc7a72c9c9c6ee4211c00</api_key> <!-- Replace with your Virus$
    <rule_id>100200,100201</rule_id>
    <alert_format>json</alert_format>
  </integration>
</ossec_config>
```

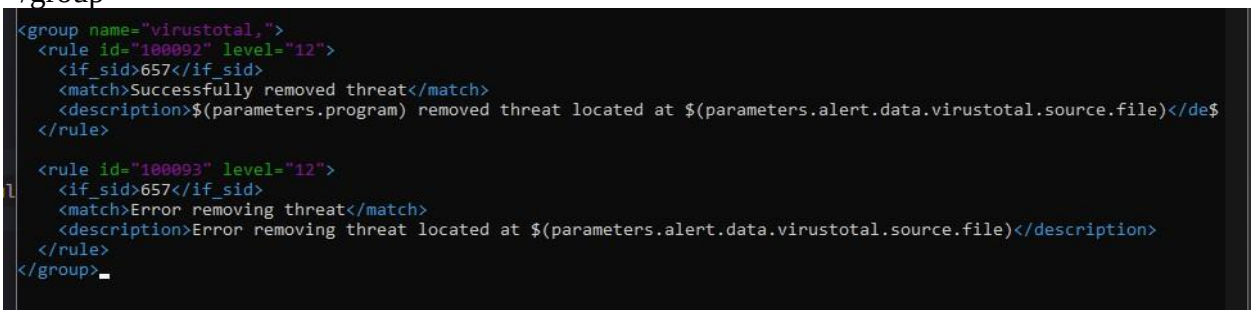
Append the following blocks to the Wazuh server /var/ossec/etc/ossec.conf file. This enables active response and triggers the remove-threat.sh script when VirusTotal flags a file as malicious:

```
<ossec_config>
  <command>
    <name>remove-threat</name>
    <executable>remove-threat.sh</executable>     <timeout_allowed>no</timeout_allowed>
  </command>
```

```
  <active-response>
    <disabled>no</disabled>
    <command>remove-threat</command>
    <location>local</location>
    <rules_id>87105</rules_id>
  </active-response>
</ossec_config>
```

Add the following rules to the Wazuh server /var/ossec/etc/rules/local_rules.xml file to alert about the active response results:

```
<group name="virustotal,">
  <rule id="100092" level="12">
    <if_sid>657</if_sid>
    <match>Successfully removed threat</match>
    <description>$(parameters.program) removed threat located at
$(parameters.alert.data.virustotal.source.file)</description>
  </rule>

  <rule id="100093" level="12">
    <if_sid>657</if_sid>
    <match>Error removing threat</match>
    <description>Error removing threat located at
$(parameters.alert.data.virustotal.source.file)</description>
  </rule>
</group>
```

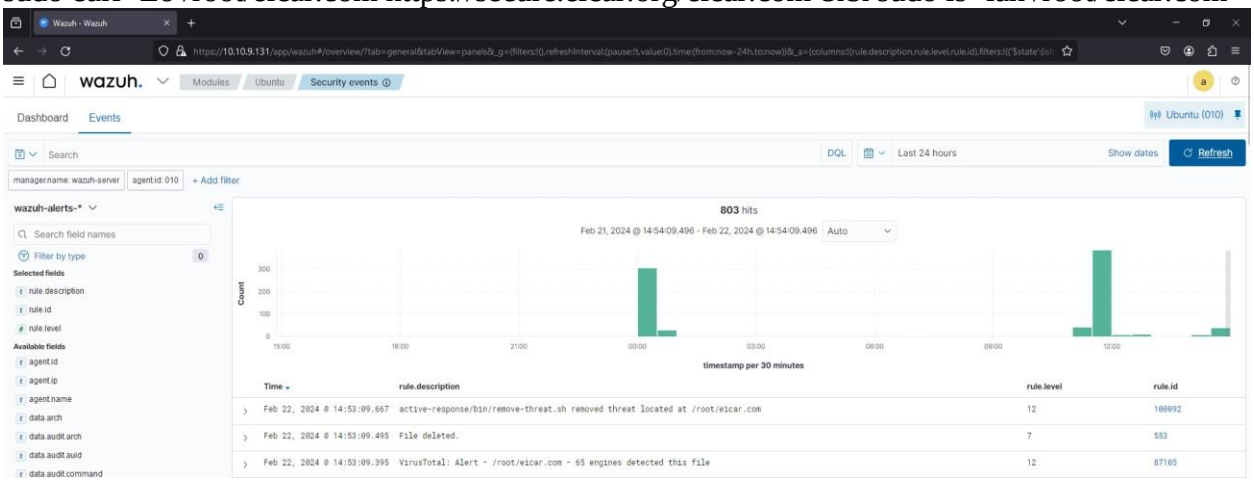


Restart the Wazuh manager to apply the configuration changes:
sudo systemctl restart wazuh-manager

```
[root@wazuh-server ~]# systemctl restart wazuh-manager
[root@wazuh-server ~]#
```

Attack emulation

Download an EICAR test file to the /root directory on the Ubuntu endpoint:
sudo curl -Lo /root/eicar.com https://secure.eicar.org/eicar.com && sudo ls -lah /root/eicar.com



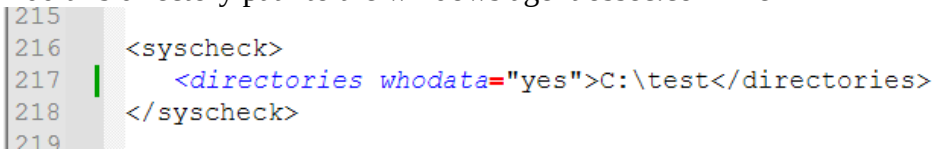
CHAPTER: 8 WAZUH POC

CHAPTER: 8 WAZUH POC

➔ File Integrity monitoring –

Creating rule file –

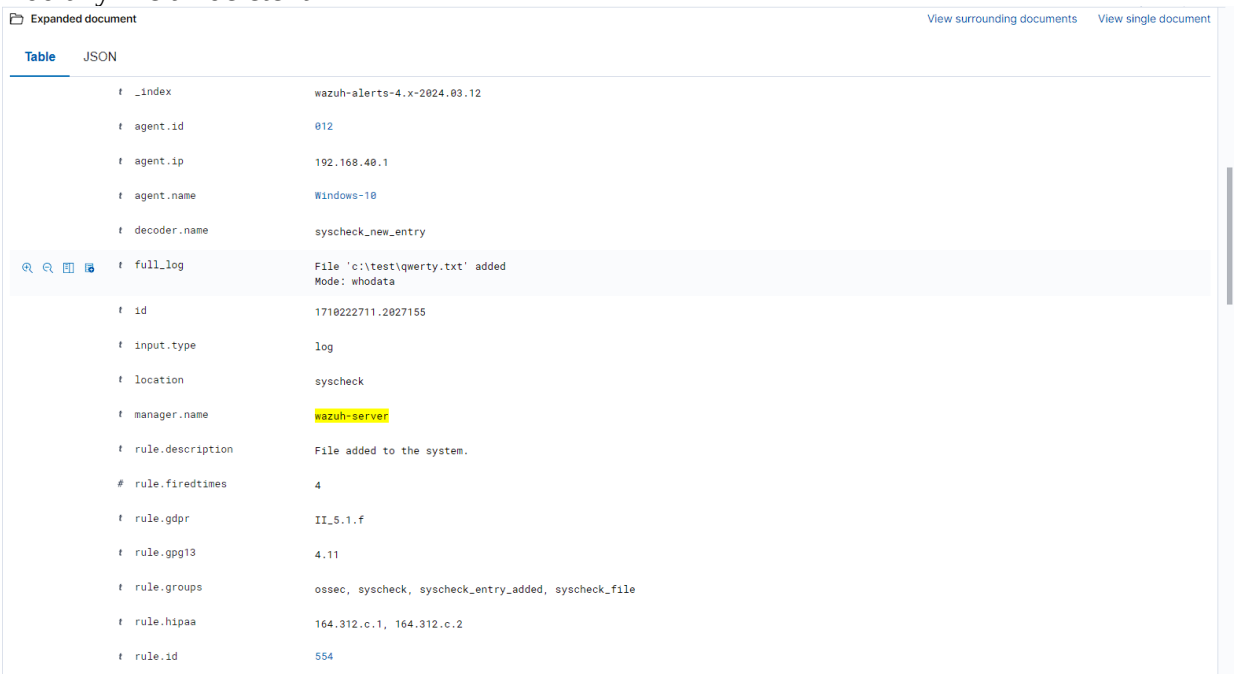
Add this directory path to the windows agent ossec.conf file –

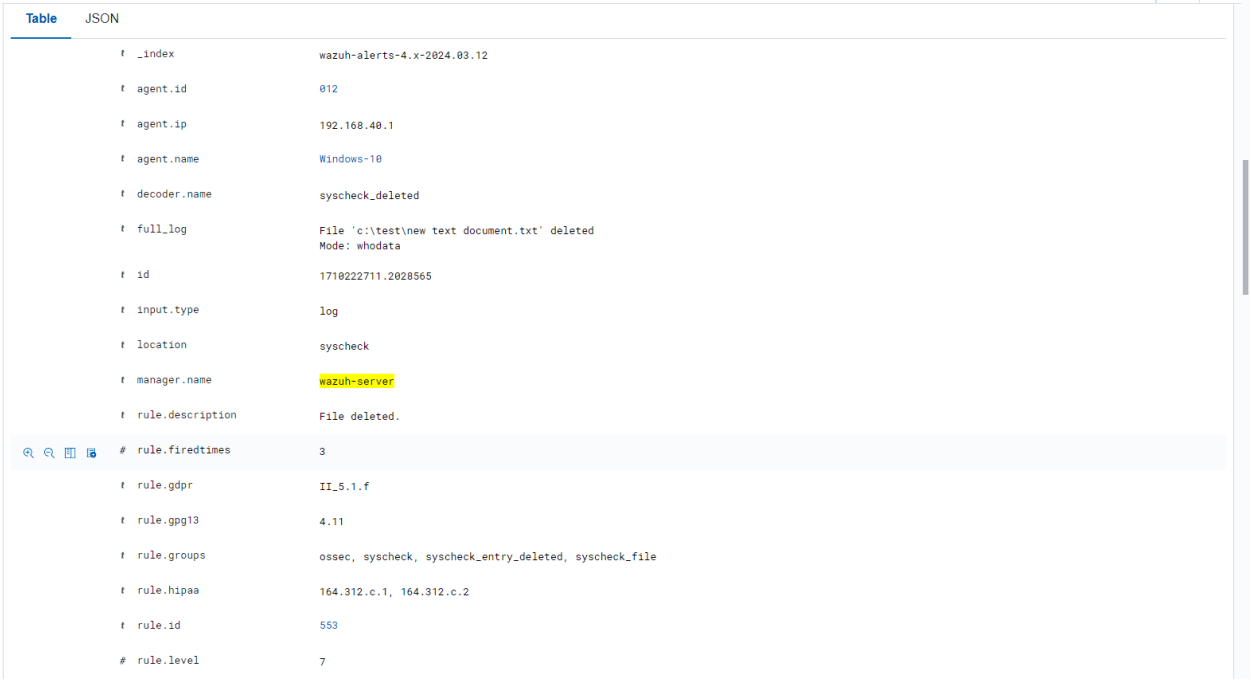


Testing the rule –

Create a folder in name test in C:\ -

Add any file an delete it –





➔ Detecting Malware Persistence –

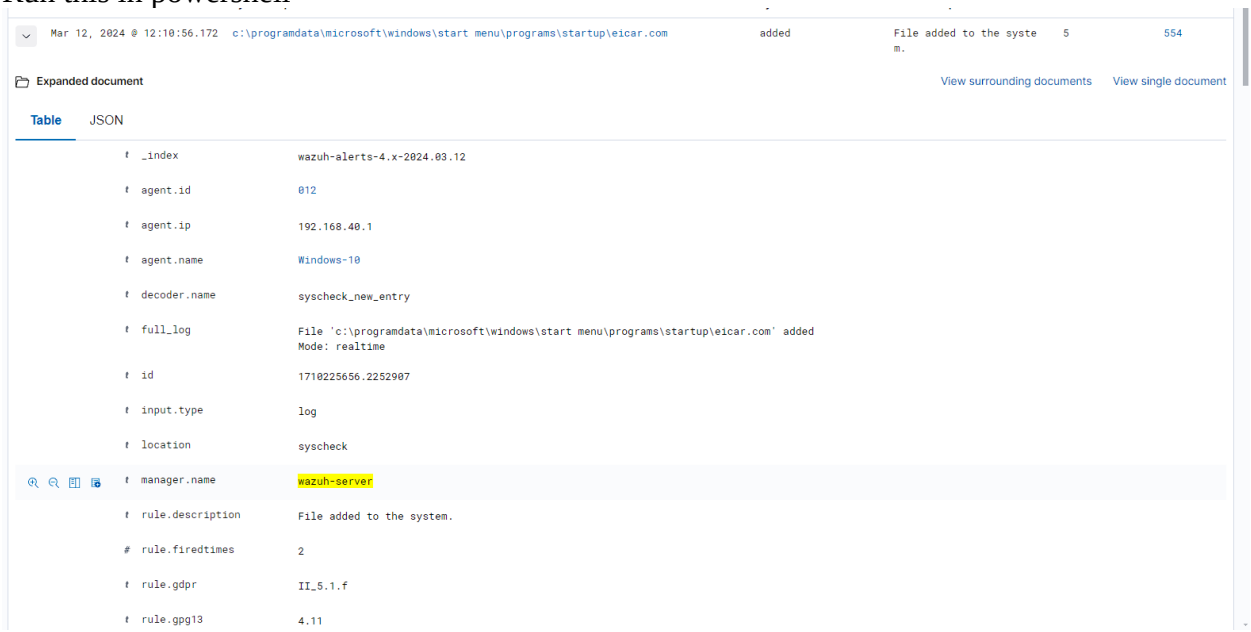
Add this the configuration file of wazuh agent – ossec.conf –

```
<syscheck>
  <directories realtime="yes">%PROGRAMDATA%\Microsoft\Windows\Start Menu\Programs\Startup</directories>
</syscheck>
```

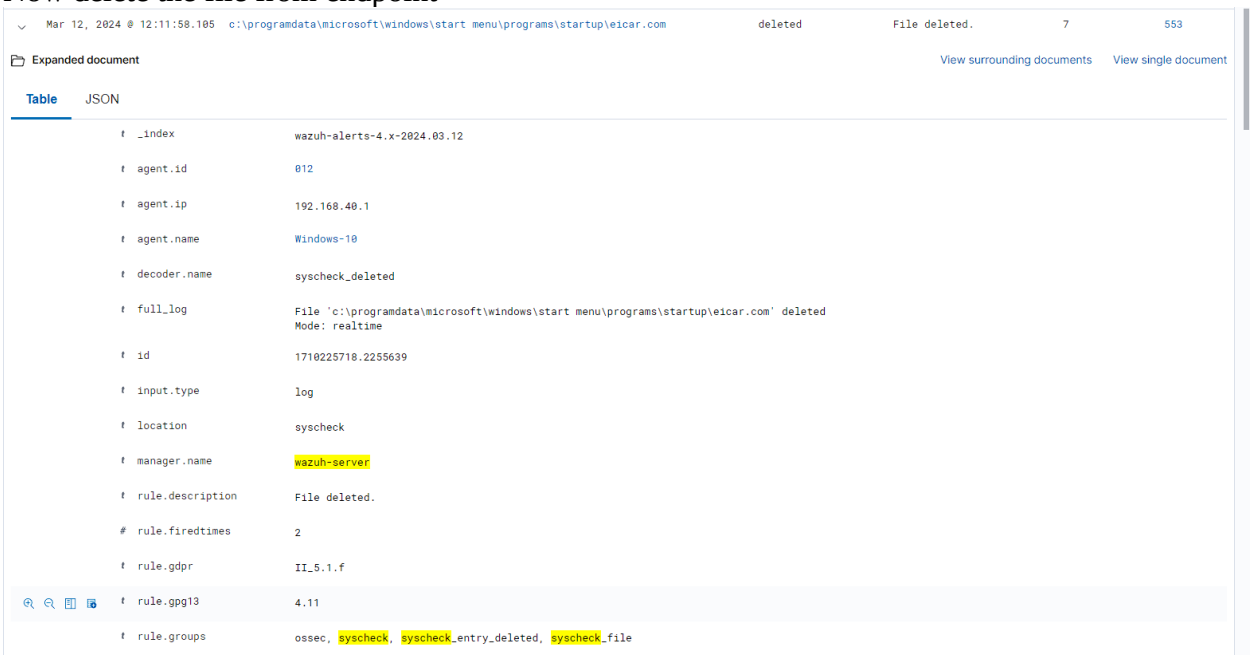
Testing the configuration –

Employ PowerShell to acquire the EICAR test file and save it to the C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup folder.

Run this in powershell –

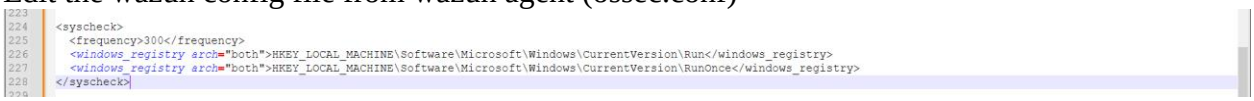


Now delete the file from endpoint –



➔ Detecting malware persistence in windows registry –

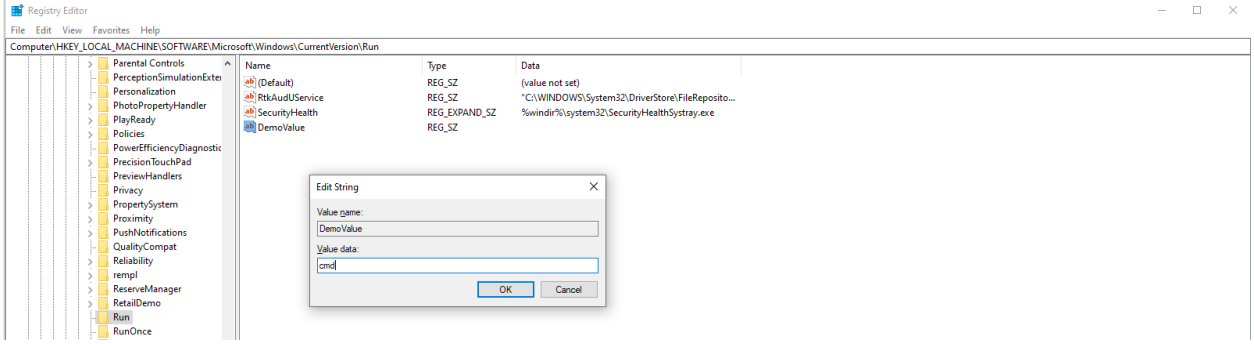
Edit the wazuh config file from wazuh agent (ossec.conf) –

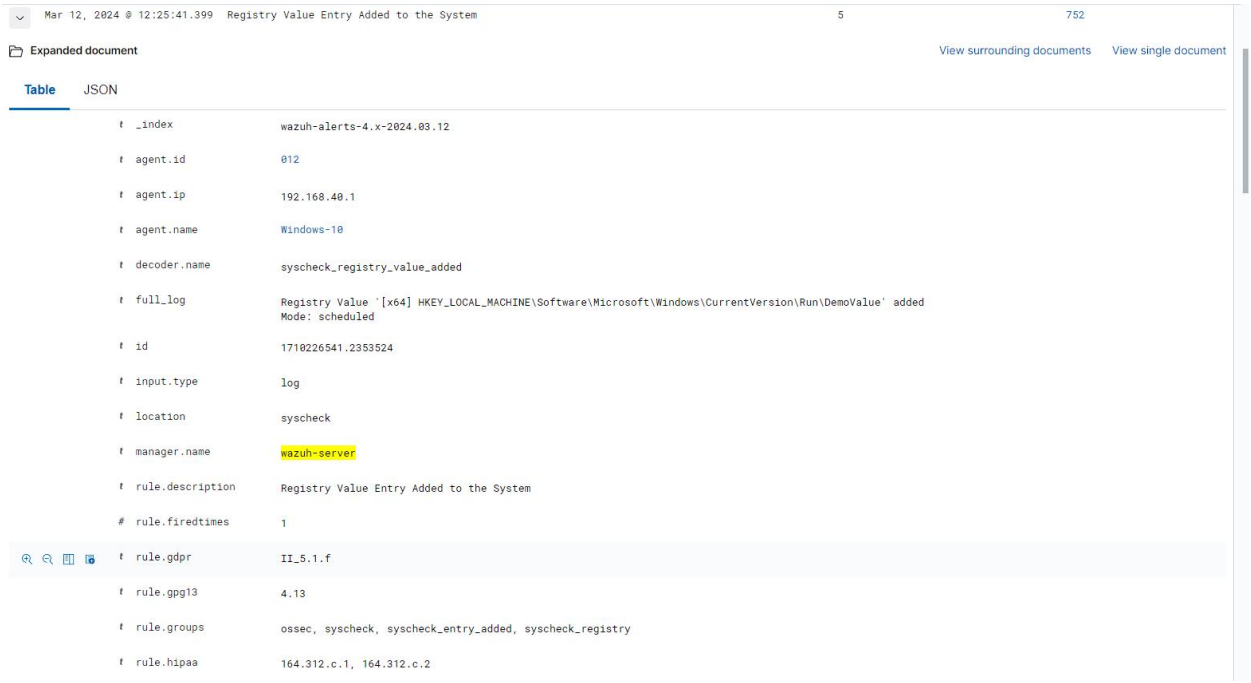


Restart the Wazuh Agent –

Test the configuration –

Add the registry value name DemoValue and registry value data cmd to the HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run key.

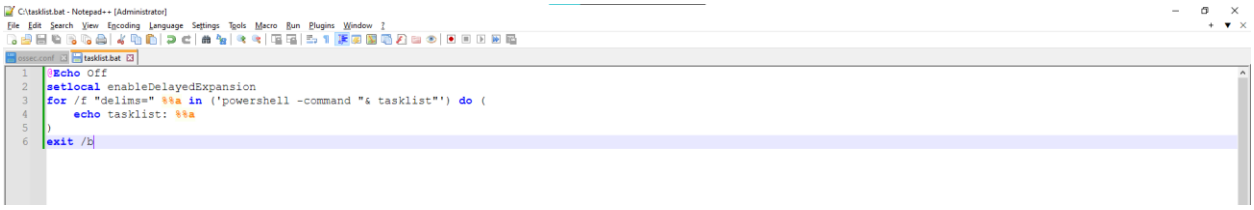




Time	syscheck.path	syscheck.event	rule.description	rule.level	rule.id
Mar 12, 2024 @ 12:25:41.399	HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run	added	Registry Value Entry Added to the System	5	752
Mar 12, 2024 @ 12:25:41.398	HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run	modified	Registry Key Integrity Checksum Changed	5	594

➔ Notepad –

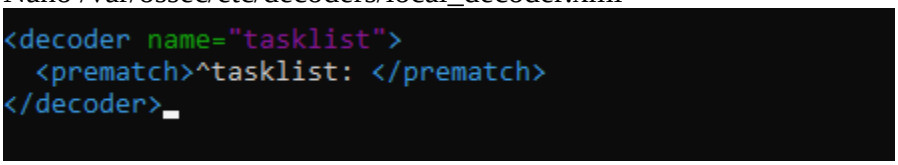
Create a bat file – tasklist.bat in C Drive –



Edit ossec.conf –

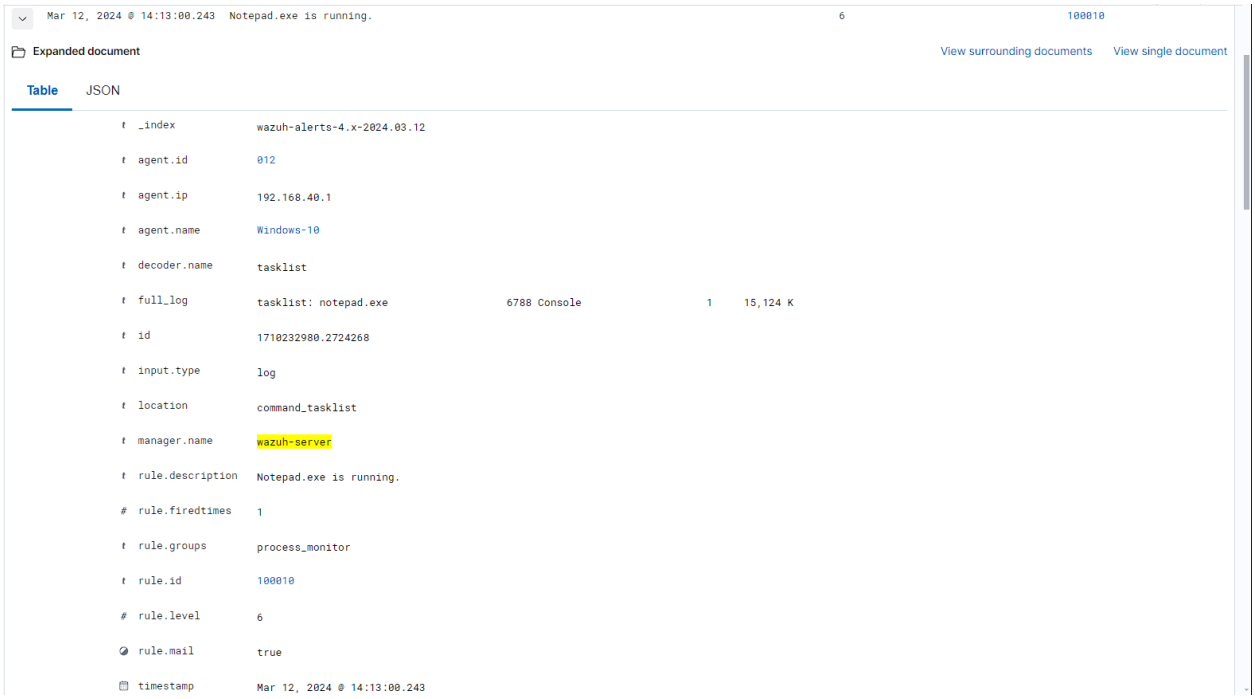
Edit this file in Wazuh Server –

Nano /var/ossec/etc/decoders/local_decoder.xml –



Nano /var/ossec/etc/rules/local_rules.xml –

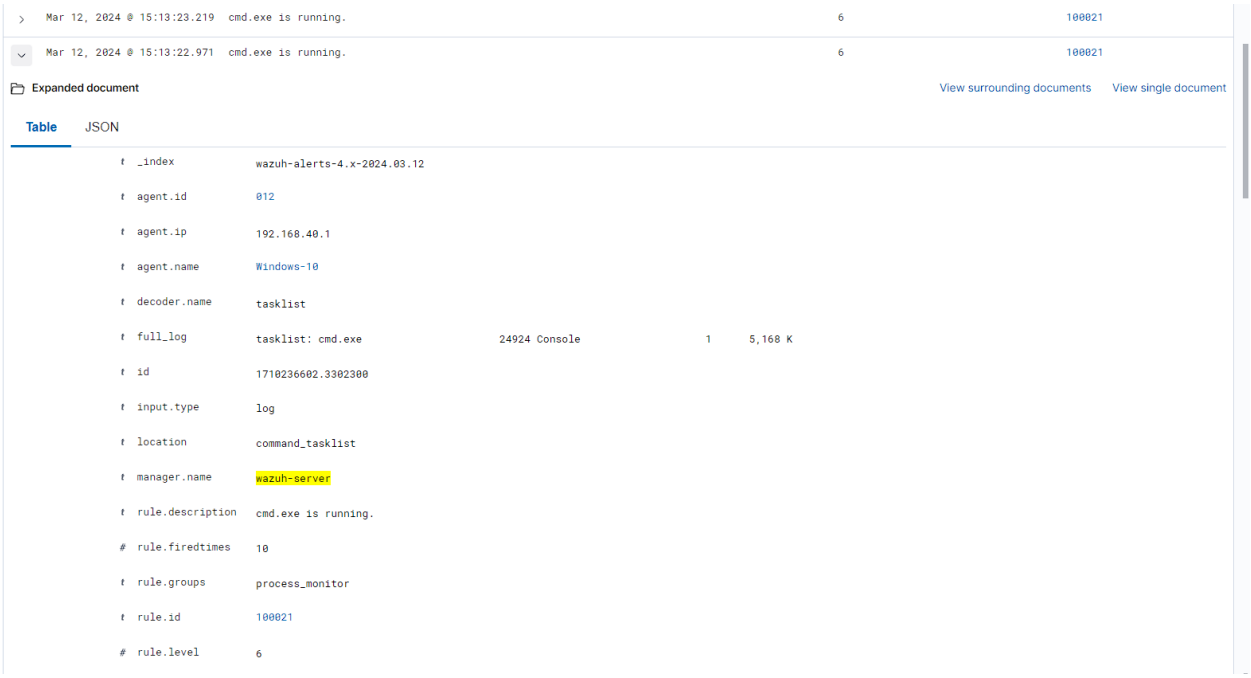
```
<group name="process_monitor,">
  <rule id="100010" level="6">
    <decoded_as>tasklist</decoded_as>
    <regex type="pcre2">(?i)notepad.exe</regex>
    <description>Notepad.exe is running.</description>
  </rule>
</group>
```



➔ CMD –

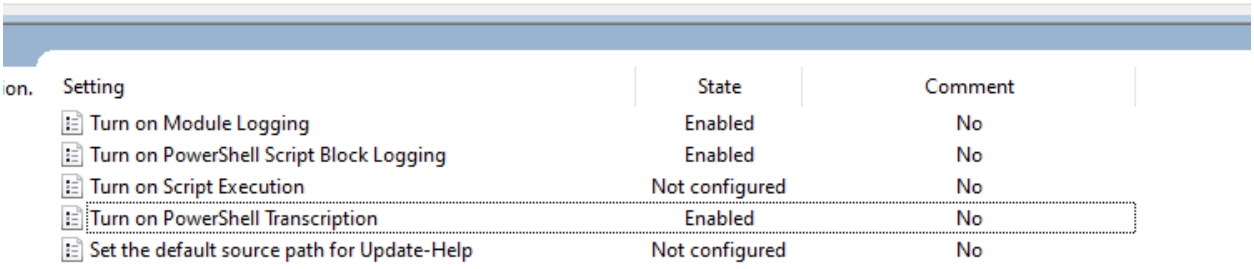
```
<group name="process_monitor,">
  <rule id="100021" level="6">
    <decoded_as>tasklist</decoded_as>
    <regex type="pcre2">(?i)cmd.exe</regex>
    <description>cmd.exe is running.</description>
  </rule>
</group>
```

Edit the local_rules.xml file and add the above code.
Alert -



➔ Logging the command of powershell in wazuh –

Press Windows + R keys on your keyboard to open the run dialog box.
Type gpedit.msc in the search box and click OK to open the local group policy editor.
Navigate to Computer Configuration > Administrative Templates > Windows Components > Windows PowerShell > Turn on PowerShell Script Block Logging.



Enable the following settings.

Open ossec.conf file in windows agent and append this –

```
<localfile>
  <location>Microsoft-Windows-PowerShell/Operational</location>
  <log_format>eventchannel</log_format>
</localfile>
```

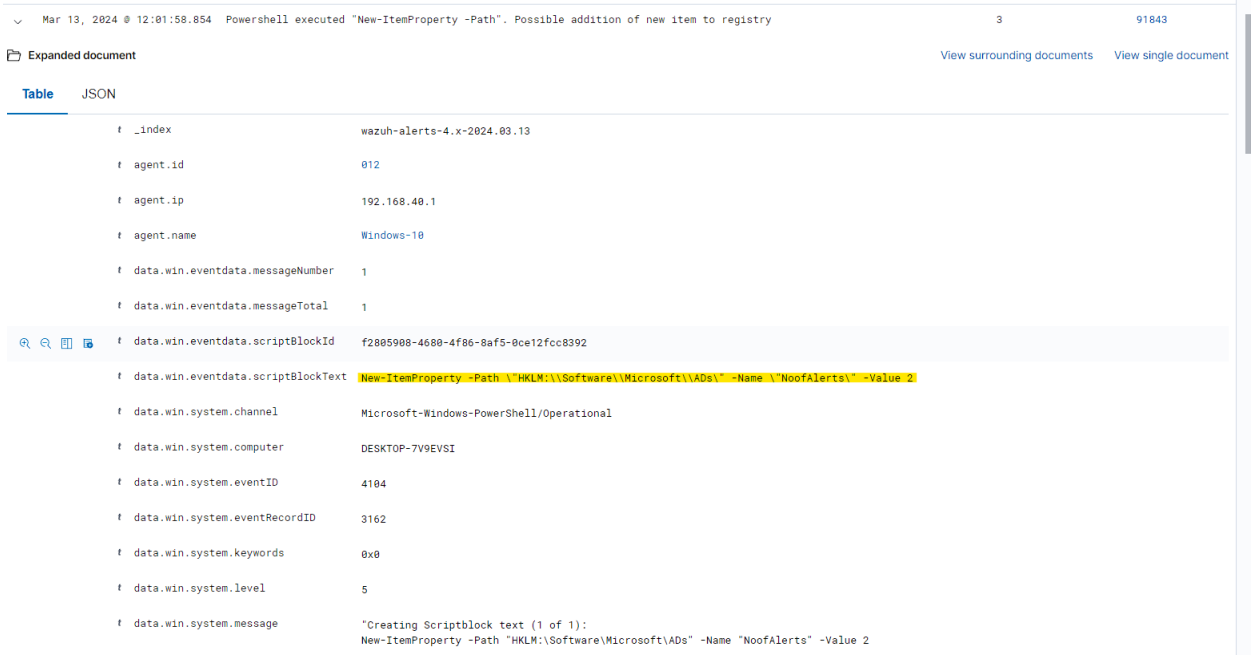
Restart the wazuh agent –

```
> Restart-Service -Name wazuh
```

Test the configuration –
On the Windows endpoint, run the following command via PowerShell with administrator privileges to add a registry entry NoofAlerts to the HKLM\Software\Microsoft\ADs registry key, and set the value to 2:

```
> New-ItemProperty -Path "HKLM:\Software\Microsoft\ADs" -Name "NoofAlerts" -Value 2
```

```
PS C:\WINDOWS\system32> New-ItemProperty -Path "HKLM:\Software\Microsoft\ADs" -Name "NoofAlerts" -Value 2


NoofAlerts    : 2
PSPath        : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\Software\Microsoft\ADs
PSParentPath  : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\Software\Microsoft
PSChildName   : ADs
PSDrive       : HKLM
PSProvider    : Microsoft.PowerShell.Core\Registry


PS C:\WINDOWS\system32>
```



➔ Windows Defender logs –

Add the following configuration in the ossec.conf file in the windows agent –

```
<!-- Windows Defender -->
<localfile>
  <location>Microsoft-Windows-Windows Defender/Operational</location>
  <log_format>eventchannel</log_format>
</localfile>
```

Testing the configuration –

Turn off the windows defender.

➔ Monitoring Downloads directory using virustotal for malicious file download and delete–

Add the directory you want to monitor using virustotal in ossec.conf file of agent –

```
<syscheck>
   <directories whodata="yes">C:\test</directories>
<!-- Virustotal integration windows -->
<directories realtime="yes">C:\Users\vrajp\Downloads</directories>
</syscheck>
```

Create a python file (remove-threat.py) –

```
#!/usr/bin/python3
# Copyright (C) 2015-2022, Wazuh Inc.
# All rights reserved.

import os
import sys
import json
import datetime

if os.name == 'nt':
    LOG_FILE = "C:\\Program Files (x86)\\ossec-agent\\active-response\\active-responses.log"
else:
```

```
    LOG_FILE = "/var/ossec/logs/active-responses.log"

ADD_COMMAND = 0
DELETE_COMMAND = 1
CONTINUE_COMMAND = 2
ABORT_COMMAND = 3

OS_SUCCESS = 0
OS_INVALID = -1

class message:
    def __init__(self):
        self.alert = ""
        self.command = 0

def write_debug_file(ar_name, msg):
    with open(LOG_FILE, mode="a") as log_file:
        log_file.write(str(datetime.datetime.now().strftime('%Y/%m/%d %H:%M:%S')) + " " +
ar_name + ": " + msg +"\n")

def setup_and_check_message(argv):

    # get alert from stdin
    input_str = ""
    for line in sys.stdin:
        input_str = line
        break


    try:
        data = json.loads(input_str)
    except ValueError:
        write_debug_file(argv[0], 'Decoding JSON has failed, invalid input format')
        message.command = OS_INVALID
        return message

    message.alert = data

    command = data.get("command")

    if command == "add":
        message.command = ADD_COMMAND
    elif command == "delete":
        message.command = DELETE_COMMAND
    else:
        message.command = OS_INVALID
```

```
        write_debug_file(argv[0], 'Not valid command: ' + command)

    return message


def send_keys_and_check_message(argv, keys):

    # build and send message with keys
    keys_msg = json.dumps({"version": 1,"origin":{"name": argv[0],"module":"active-
response"},"command":"check_keys","parameters":{"keys":keys}})

    write_debug_file(argv[0], keys_msg)

    print(keys_msg)
    sys.stdout.flush()

    # read the response of previous message
    input_str = ""
    while True:
        line = sys.stdin.readline()
        if line:
            input_str = line
            break

    # write_debug_file(argv[0], input_str)

    try:
        data = json.loads(input_str)
    except ValueError:
        write_debug_file(argv[0], 'Decoding JSON has failed, invalid input format')
        return message

    action = data.get("command")

    if "continue" == action:
        ret = CONTINUE_COMMAND
    elif "abort" == action:
        ret = ABORT_COMMAND
    else:
        ret = OS_INVALID
        write_debug_file(argv[0], "Invalid value of 'command'")

    return ret

def main(argv):
```

```
    write_debug_file(argv[0], "Started")

    # validate json and get command
    msg = setup_and_check_message(argv)

    if msg.command < 0:
        sys.exit(OS_INVALID)

    if msg.command == ADD_COMMAND:
        alert = msg.alert["parameters"]["alert"]
        keys = [alert["rule"]["id"]]
        action = send_keys_and_check_message(argv, keys)

        # if necessary, abort execution
        if action != CONTINUE_COMMAND:

            if action == ABORT_COMMAND:
                write_debug_file(argv[0], "Aborted")
                sys.exit(OS_SUCCESS)
            else:
                write_debug_file(argv[0], "Invalid command")
                sys.exit(OS_INVALID)

        try:
            file_path = msg.alert["parameters"]["alert"]["data"]["virustotal"]["source"]["file"]
            if os.path.exists(file_path):
                os.remove(file_path)
            write_debug_file(argv[0], json.dumps(msg.alert) + " Successfully removed threat")
        except OSError as error:
            write_debug_file(argv[0], json.dumps(msg.alert) + "Error removing threat")


    else:
        write_debug_file(argv[0], "Invalid command")

    write_debug_file(argv[0], "Ended")

    sys.exit(OS_SUCCESS)

if __name__ == "__main__":
    main(sys.argv)
```

Convert the active response Python script remove-threat.py to a Windows executable application. Run the following PowerShell command as an administrator to create the executable:

```
pyinstaller -F \path_to_remove-threat.py
```

Take note of the path where pyinstaller created remove-threat.exe.
Move the executable file remove-threat.exe to the C:\Program Files (x86)\ossec-agent\active-response\bin directory.
Restart the Wazuh agent to apply the changes.
Restart-Service -Name wazuh

Add the virustotal api key in ossec.conf file of wazuh manager –

```
<ossec_config>
  <integration>
    <name>virustotal</name>
    <api_key>5db16355483f100aa03869c48791c964982556c2896e2a6012a05b85f6a047c8</api_key> <!-- Replace with your VirusTotal API key -->
    <group>syscheck</group>
    <alert_format>json</alert_format>
  </integration>
</ossec_config>
```

Append the following blocks to the Wazuh server /var/ossec/etc/ossec.conf file. This enables active response and trigger the remove-threat.exe executable when the VirusTotal query returns positive matches for threats

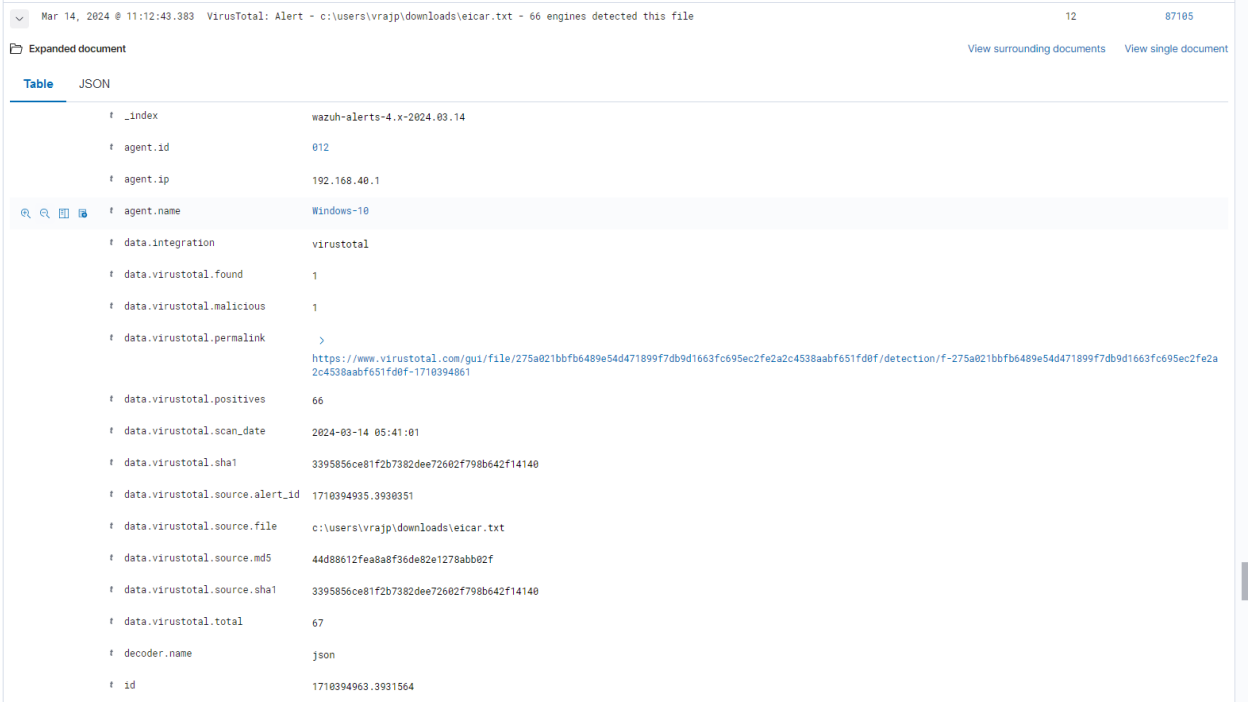
```
<ossec_config>
  <command>
    <name>remove-threat</name>
    <executable>remove-threat.exe</executable>
    <timeout_allowed>no</timeout_allowed>
  </command>

  <active-response>
    <disabled>no</disabled>
    <command>remove-threat</command>
    <location>local</location>
    <rules_id>87105</rules_id>
  </active-response>
</ossec_config>
```

Add the following rules to the Wazuh server /var/ossec/etc/rules/local_rules.xml file to alert about the active response results

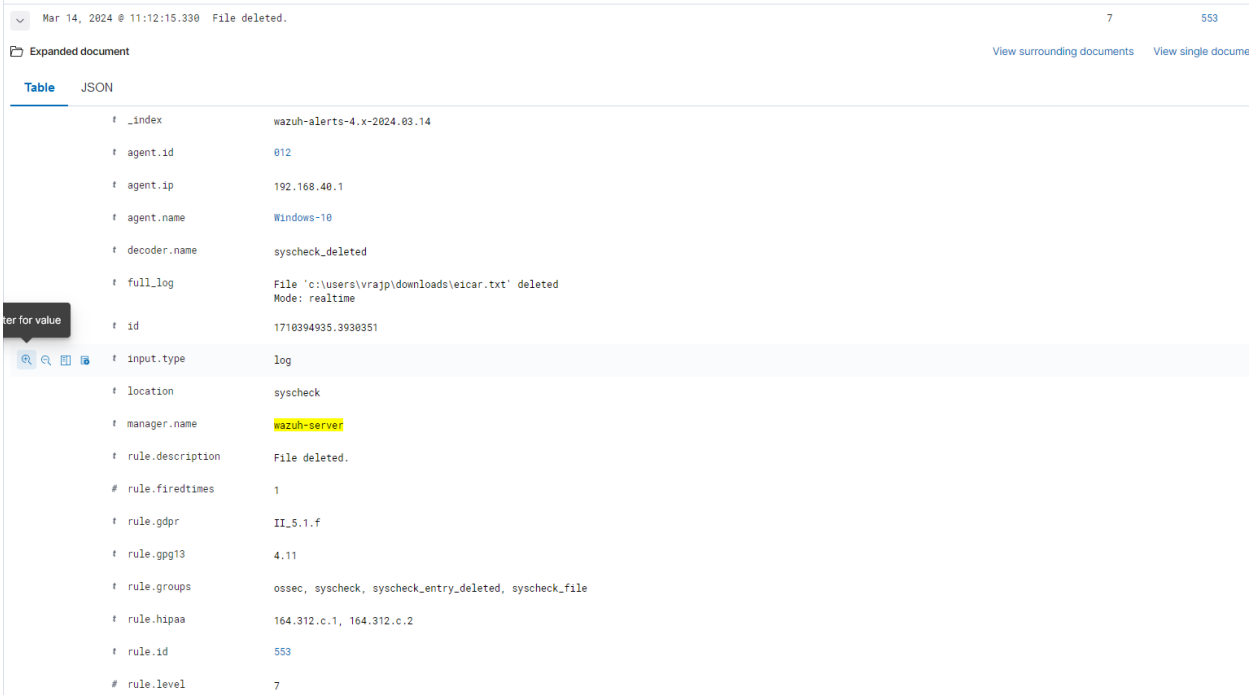
```
<!-- Virustotal Windows -->
<group name="virustotal,">
  <rule id="100092" level="12">
      <if_sid>657</if_sid>
      <match>Successfully removed threat</match>
      <description>$(parameters.program) removed threat located at $(parameters.alert.data.virustotal.source.file)</description>
  </rule>

  <rule id="100093" level="12">
    <if_sid>657</if_sid>
    <match>Error removing threat</match>
    <description>Error removing threat located at $(parameters.alert.data.virustotal.source.file)</description>
  </rule>
</group>
```

Restart the Wazuh manager to apply the configuration changes:
sudo systemctl restart wazuh-manager

Downloading the malicious file in Downloads Folder –



File deleted –



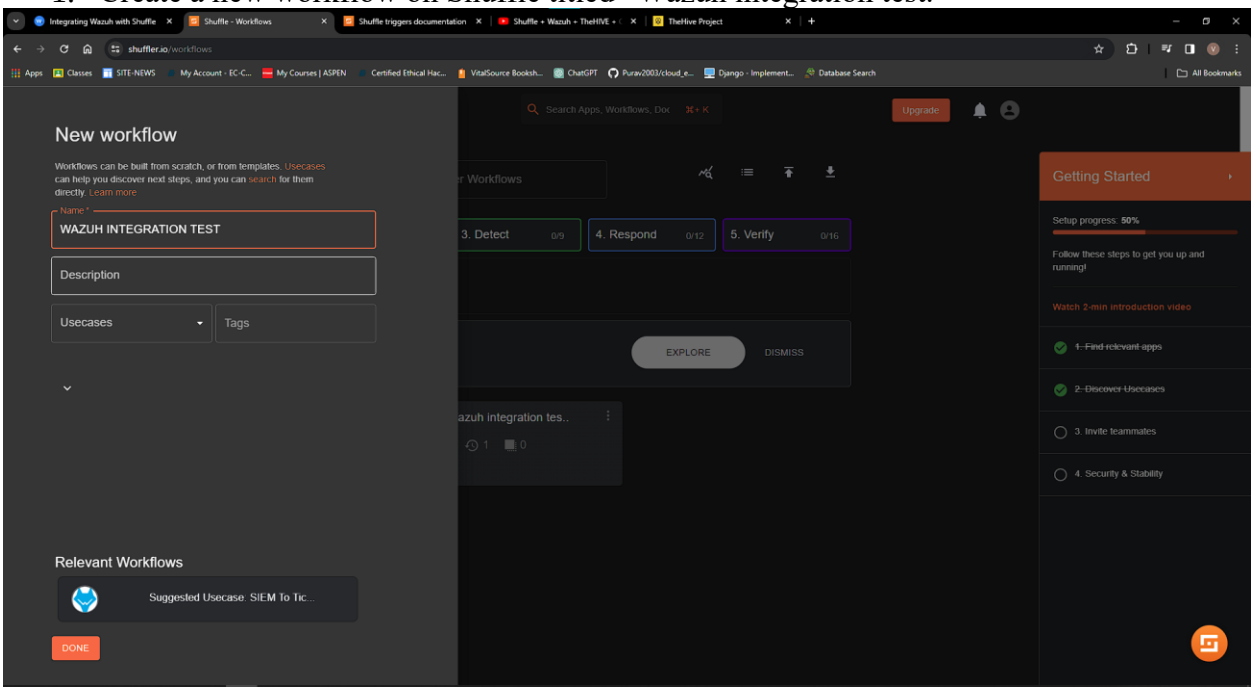
CHAPTER: 9 WAZUH AND SOAR INTEGRATION

CHAPTER: 9 WAZUH AND SOAR INTEGRATION

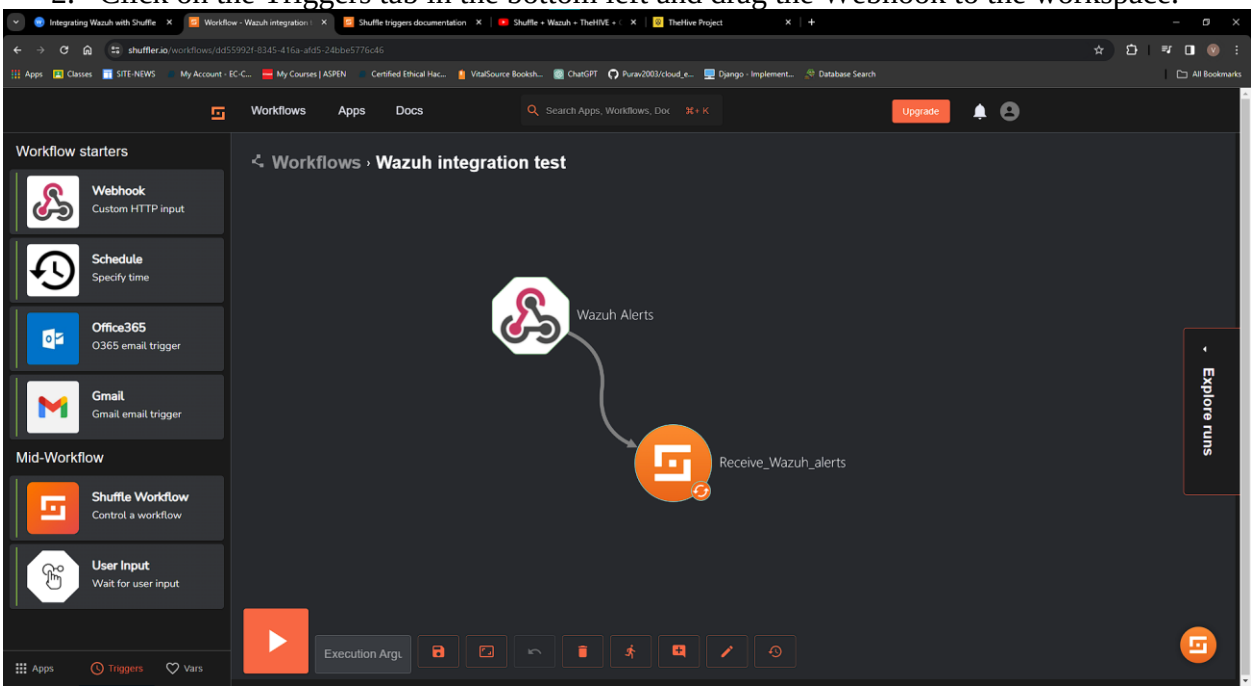
WAZUH & SHUFFLE SOAR INTEGRATION

Perform the steps below on the Shuffle dashboard to create a new workflow and extract the webhook URI.

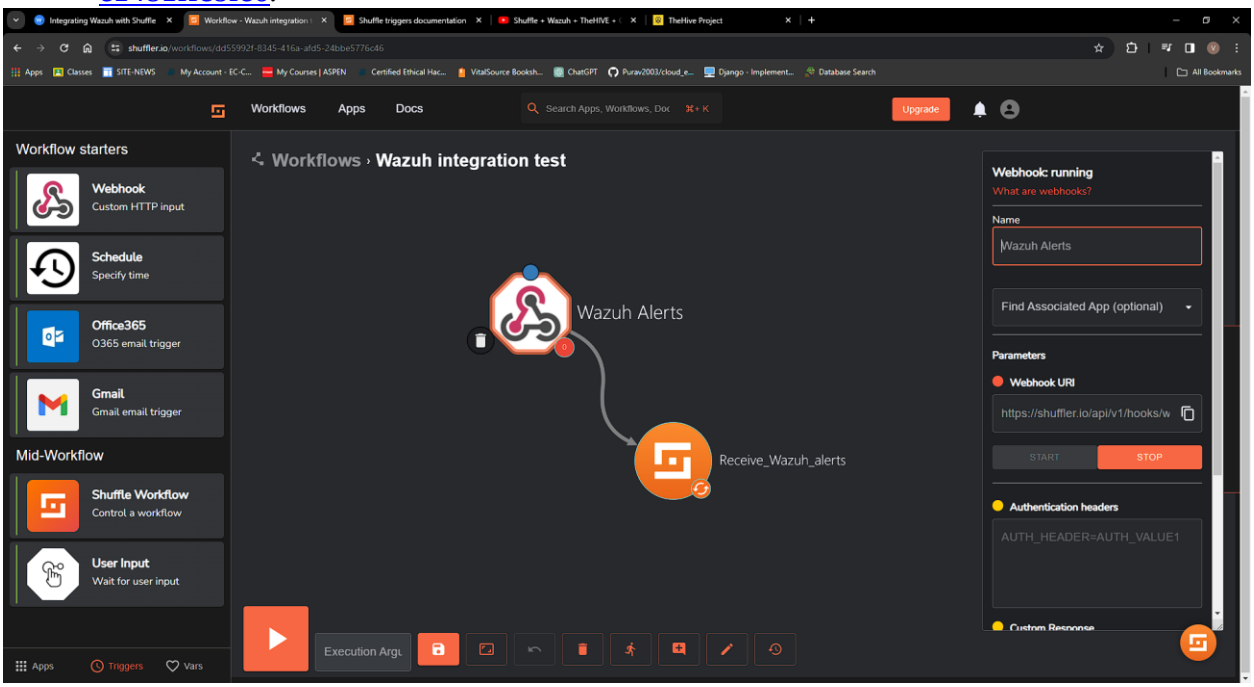
1. Create a new workflow on Shuffle titled “Wazuh integration test.”



2. Click on the Triggers tab in the bottom left and drag the Webhook to the workspace.



3. Click on the webhook and rename it to Wazuh alerts. Copy and save the webhook URI because we use it when configuring the Wazuh server. Start the webhook. The webhook URI looks like the following: https://<YOUR_SHUFFLE_URL>/api/v1/hooks/webhook_18cdc939-5e7b-428e-b82f-e1481ffc8fe6.



WAZUH SERVER

Perform the steps below on the Wazuh server to configure Wazuh to send alerts to Shuffle for analysis.

1. Add the following configuration in between the <ossec_config> block of the Wazuh server /var/ossec/etc/ossec.conf file:

```
<integration>
  <name>shuffle</name>
  <hook_url><YOUR_SHUFFLE_URL>/api/v1/hooks/<HOOK_ID></hook_url>
  <level>3</level>
  <alert_format>json</alert_format>
</integration>
```

Where:
<name>: This is the name of the integration.
<hook_url>: This is the webhook URI copied from the Shuffle webhook. Your Shuffle URL depends on your deployment, for example, http://<SHUFFLE_IP>:3001 for a Shuffle on-premise deployment and https://shuffler.io for Shuffle Cloud.
<level>: This is used to forward a specific alert level.
<alert_format>: This forwards alerts to Shuffle in JSON format.
For more information on available options, check out this guide.

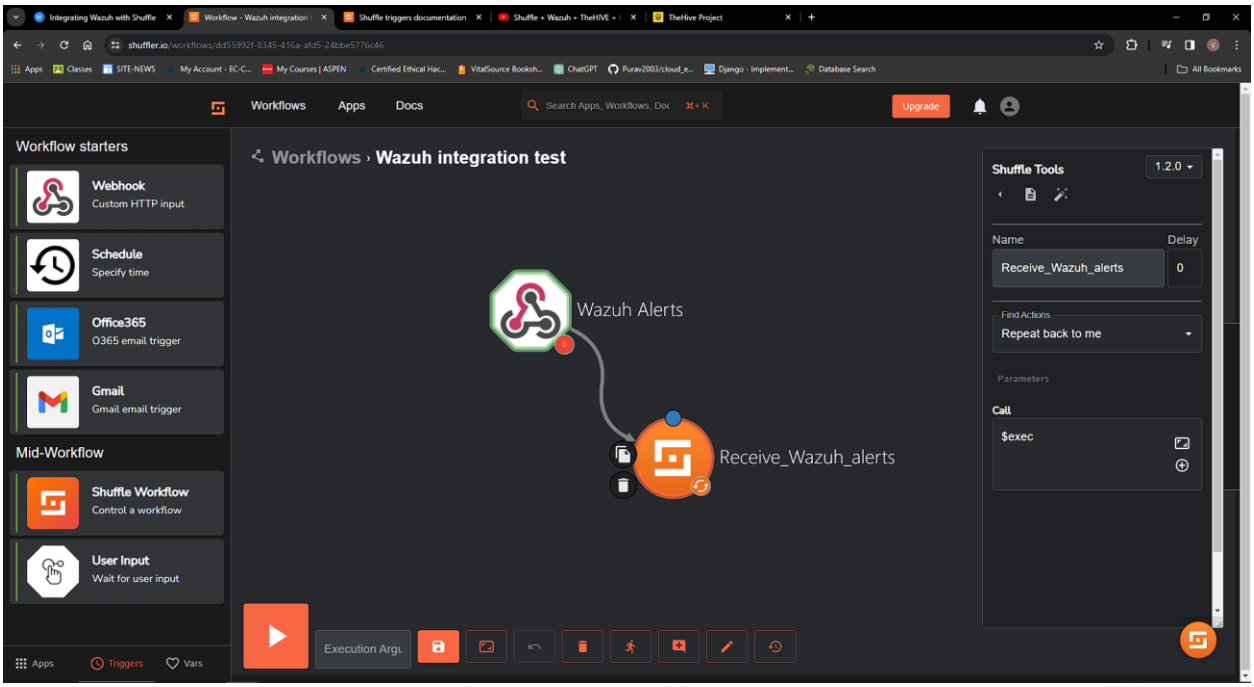
```
<!-- Shuffle SOAR -->
<integration>
  <name>shuffle</name>
  <hook_url>https://shuffler.io/api/v1/hooks/webhook_0ed0f798-02d4-40e5-893a-842170df7059</hook_url>
  <level>3</level>
  <alert_format>json</alert_format>
</integration>
```

2. Restart the Wazuh manager service to apply changes:
sudo systemctl restart wazuh-manager

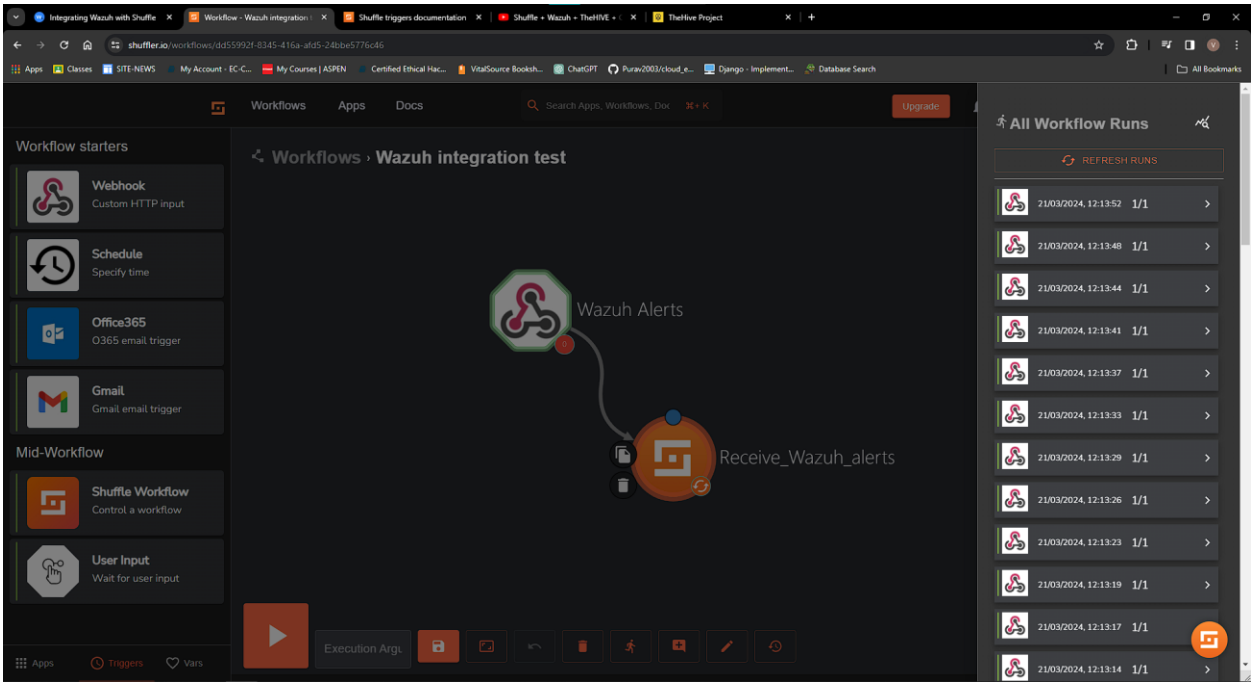
```
[root@wazuh-server ~]# sudo systemctl restart wazuh-manager
[root@wazuh-server ~]# sudo systemctl status wazuh-manager
● wazuh-manager.service - Wazuh manager
   Loaded: loaded (/usr/lib/systemd/system/wazuh-manager.service; enabled; vendor preset: disabled)
   Active: active (running) since Thu 2024-03-21 06:06:00 UTC; 14s ago
  Process: 22738 ExecStop=/usr/bin/env /var/ossec/bin/wazuh-control stop (code=exited, status=0/SUCCESS)
  Process: 22896 ExecStart=/usr/bin/env /var/ossec/bin/wazuh-control start (code=exited, status=0/SUCCESS)
   CGroup: /system.slice/wazuh-manager.service
           ├─22956 /var/ossec/framework/python/bin/python3 /var/ossec/api/scripts/wazuh-apid.py
           ├─22957 /var/ossec/framework/python/bin/python3 /var/ossec/api/scripts/wazuh-apid.py
           ├─22960 /var/ossec/framework/python/bin/python3 /var/ossec/api/scripts/wazuh-apid.py
           ├─22963 /var/ossec/framework/python/bin/python3 /var/ossec/api/scripts/wazuh-apid.py
           ├─22988 /var/ossec/bin/wazuh-integratord
           ├─23008 /var/ossec/bin/wazuh-authd
           ├─23025 /var/ossec/bin/wazuh-db
           ├─23050 /var/ossec/bin/wazuh-execd
           ├─23062 /var/ossec/bin/wazuh-maild
           ├─23068 /var/ossec/bin/wazuh-analysisd
           ├─23089 /var/ossec/bin/wazuh-syscheckd
           ├─23106 /var/ossec/bin/wazuh-remoted
           ├─23140 /var/ossec/bin/wazuh-logcollector
```

Shuffle SOAR

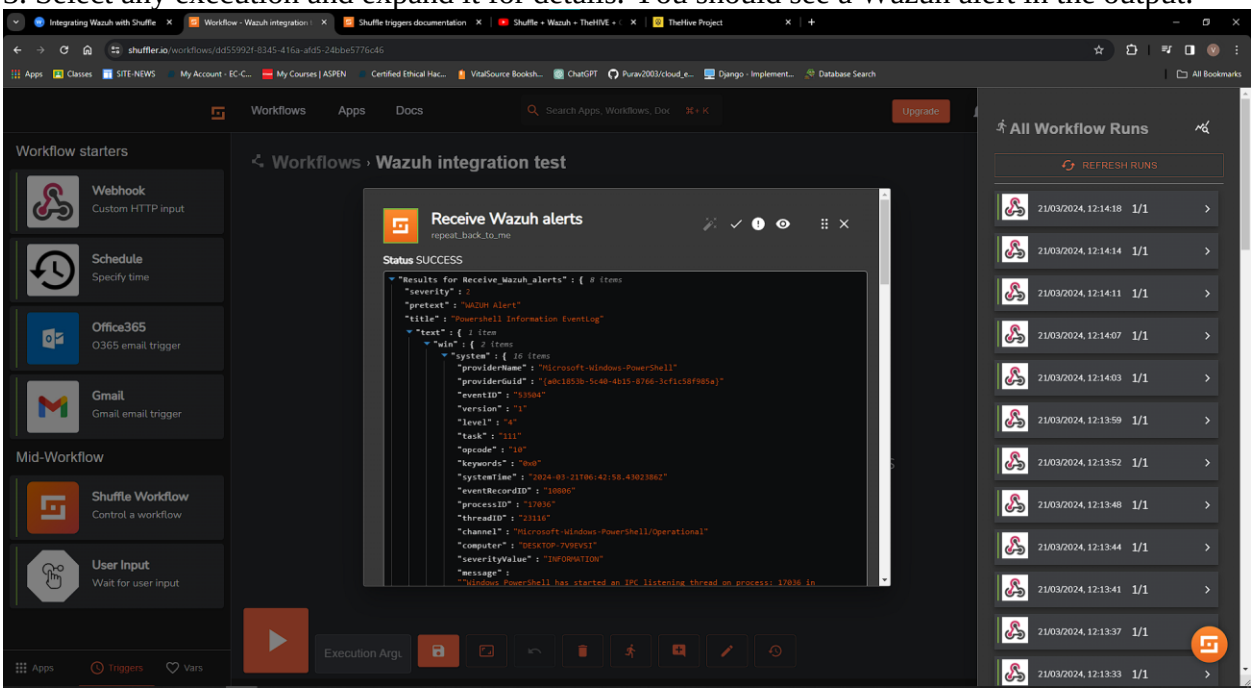
1. Click on the Shuffle Tools app named “Change me” and rename it to Receive_Wazuh_alerts. Set the call option to “$exec”, and save the workflow. This Shuffle app now repeats the events that are received by the Wazuh alerts webhook. This allows us to test that Shuffle can receive Wazuh alerts.



2. Click on the show executions button.



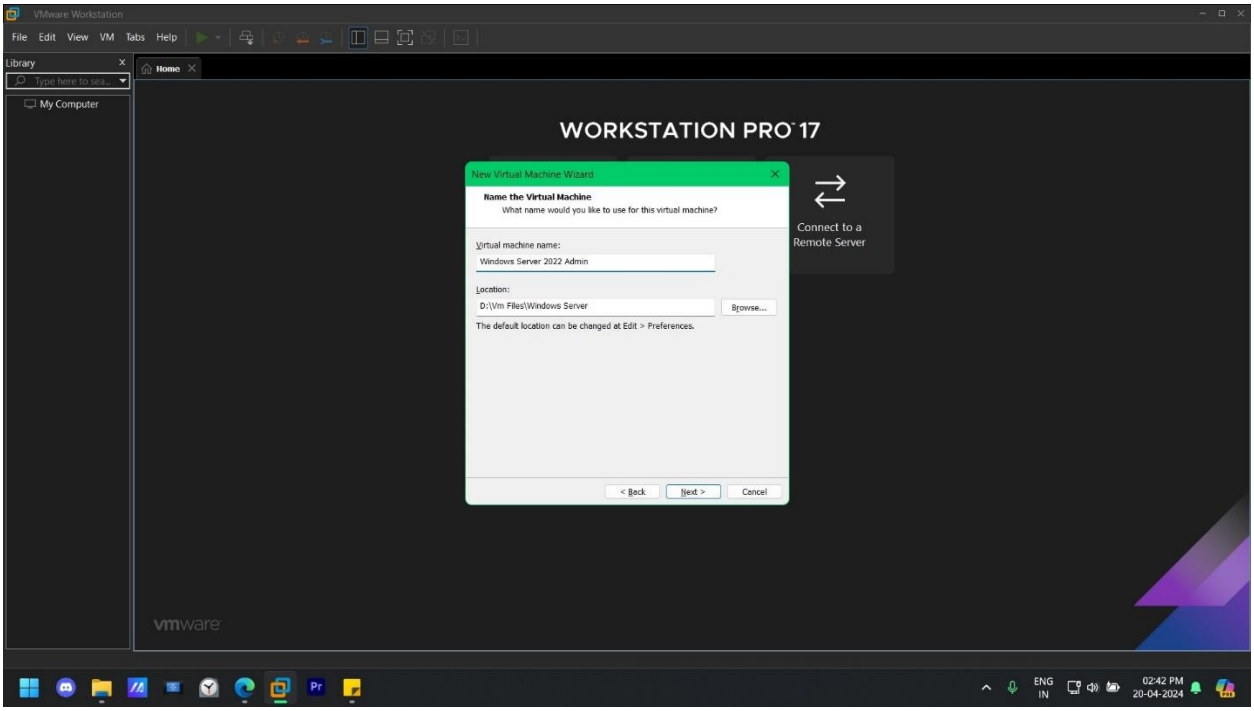
3. Select any execution and expand it for details. You should see a Wazuh alert in the output.



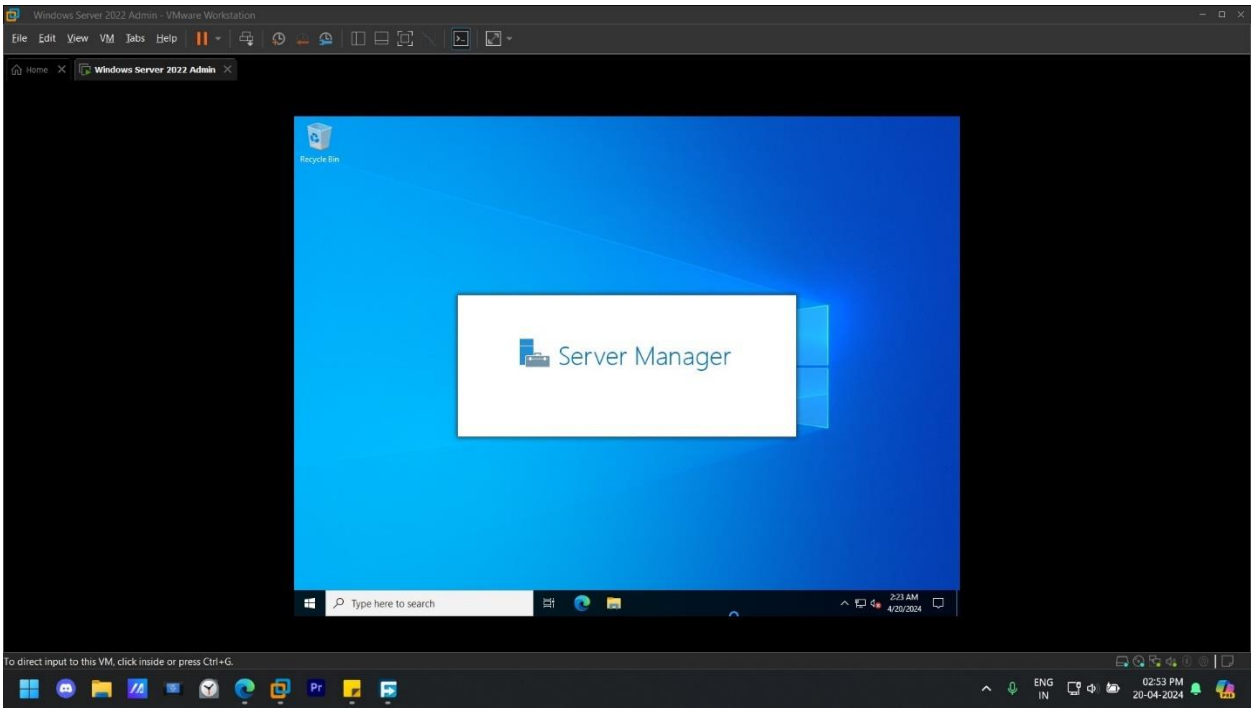
CHAPTER: 10 WINDOWS AD CREATION

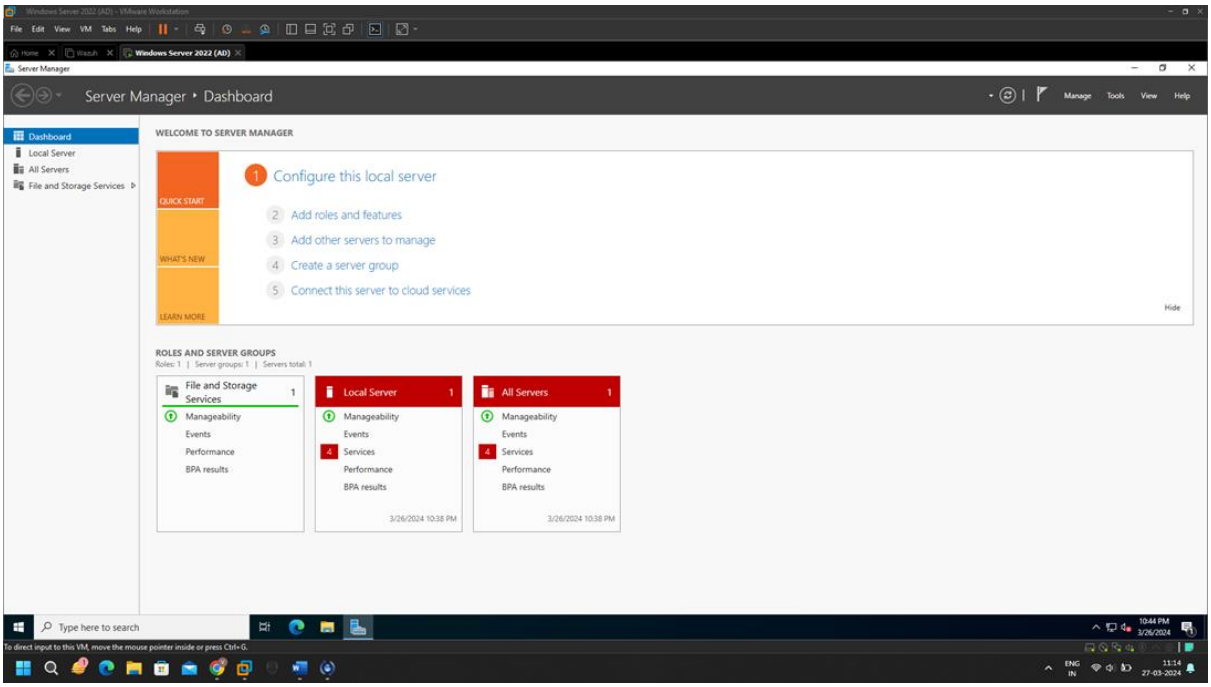
CHAPTER: 10 WINDOWS AD CREATION

Installing windows server 2022 in VM –

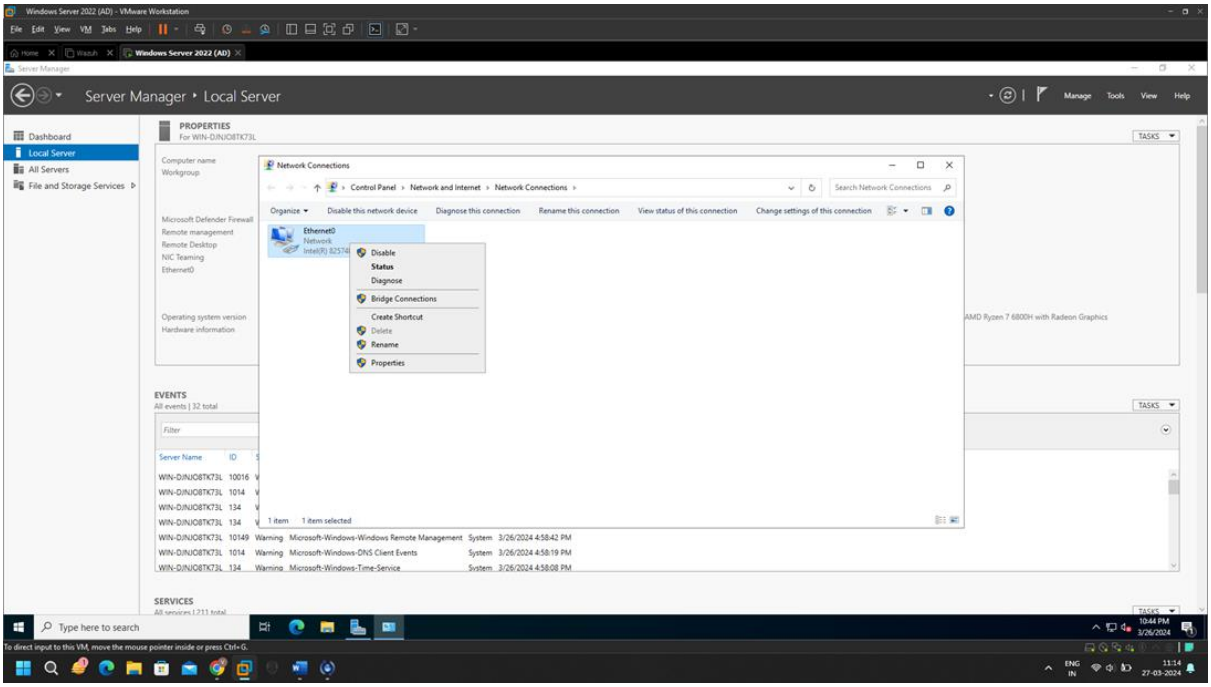


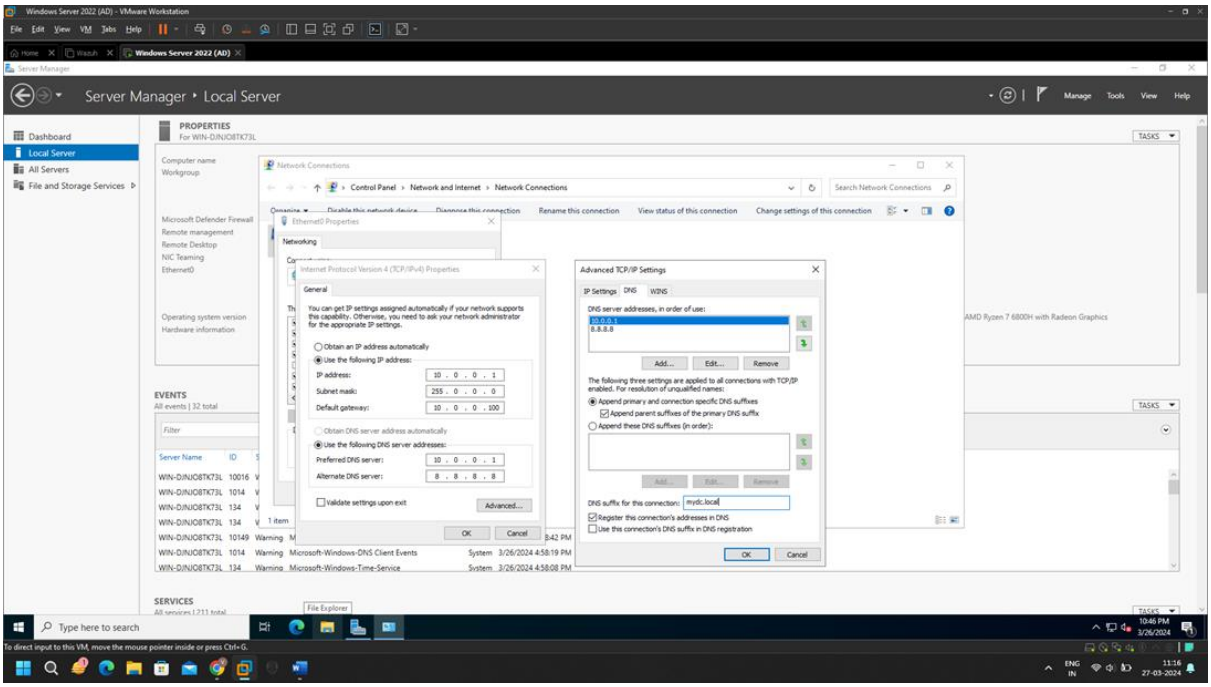
Start Server Manager after installation –



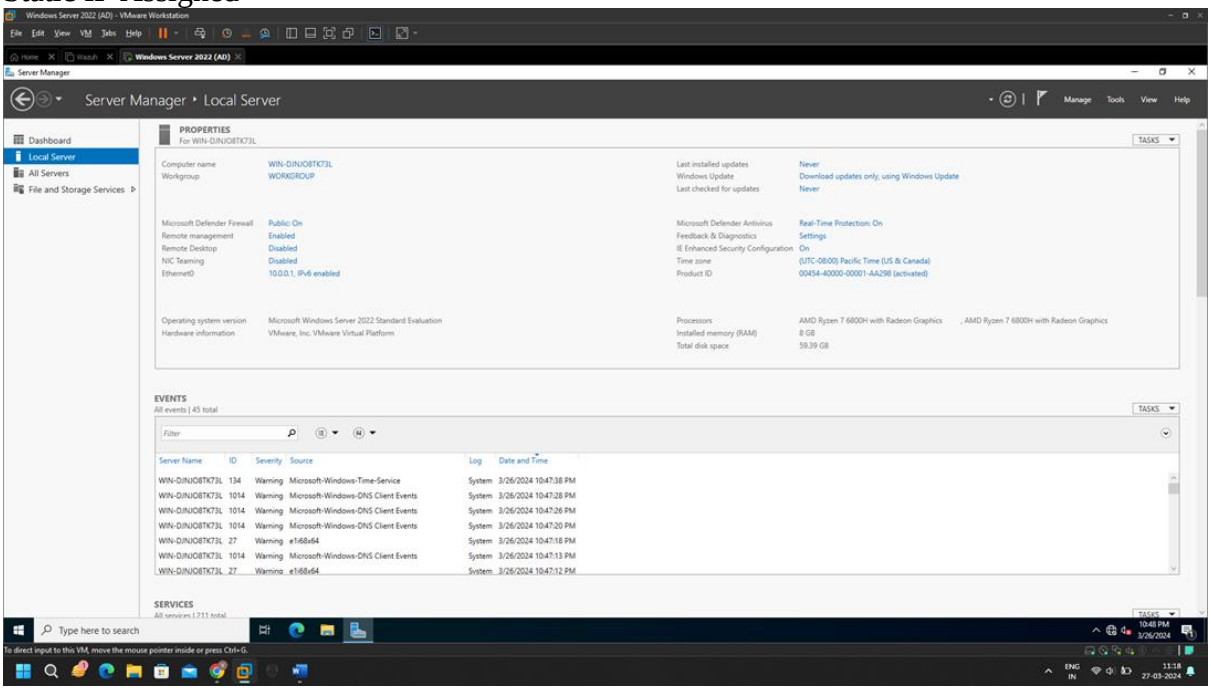


Goto Local Server and Configure IP –

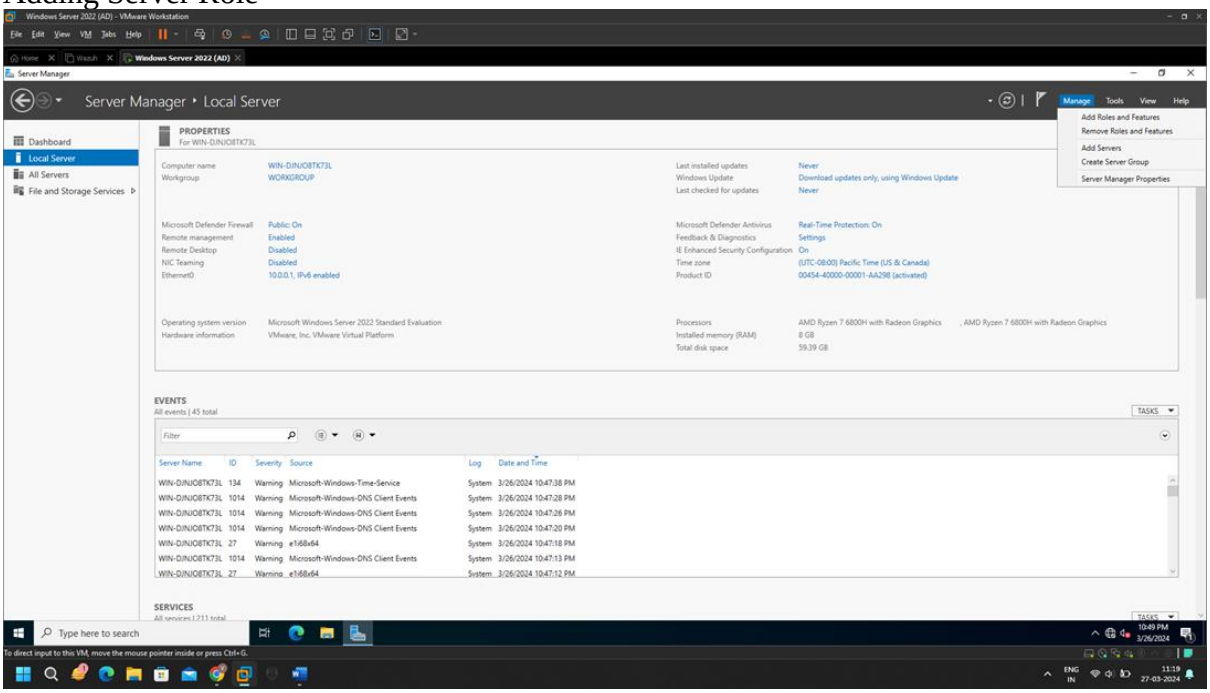




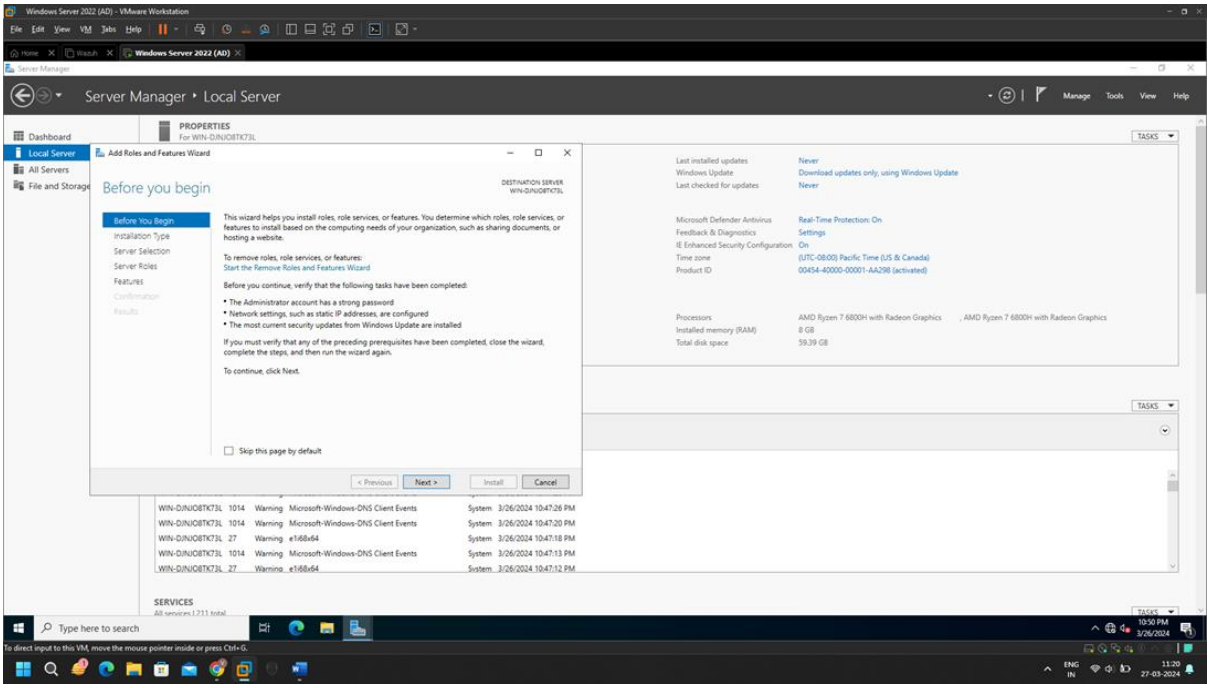
Static IP Assigned –



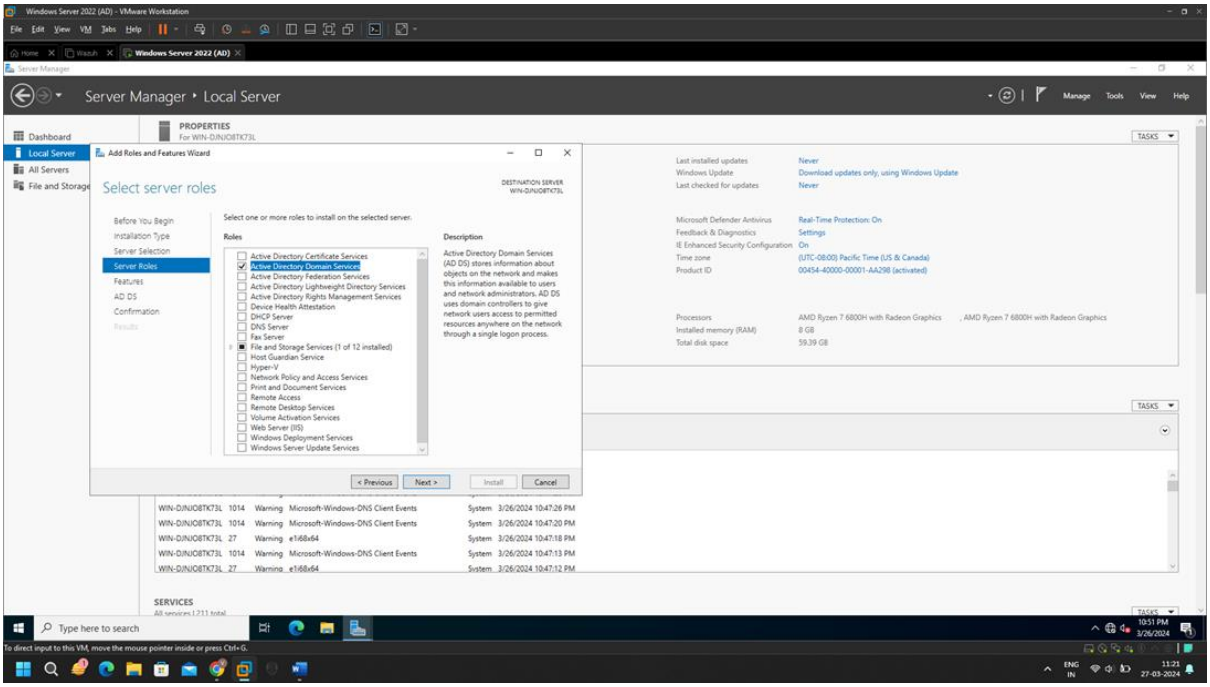
Adding Server Role –



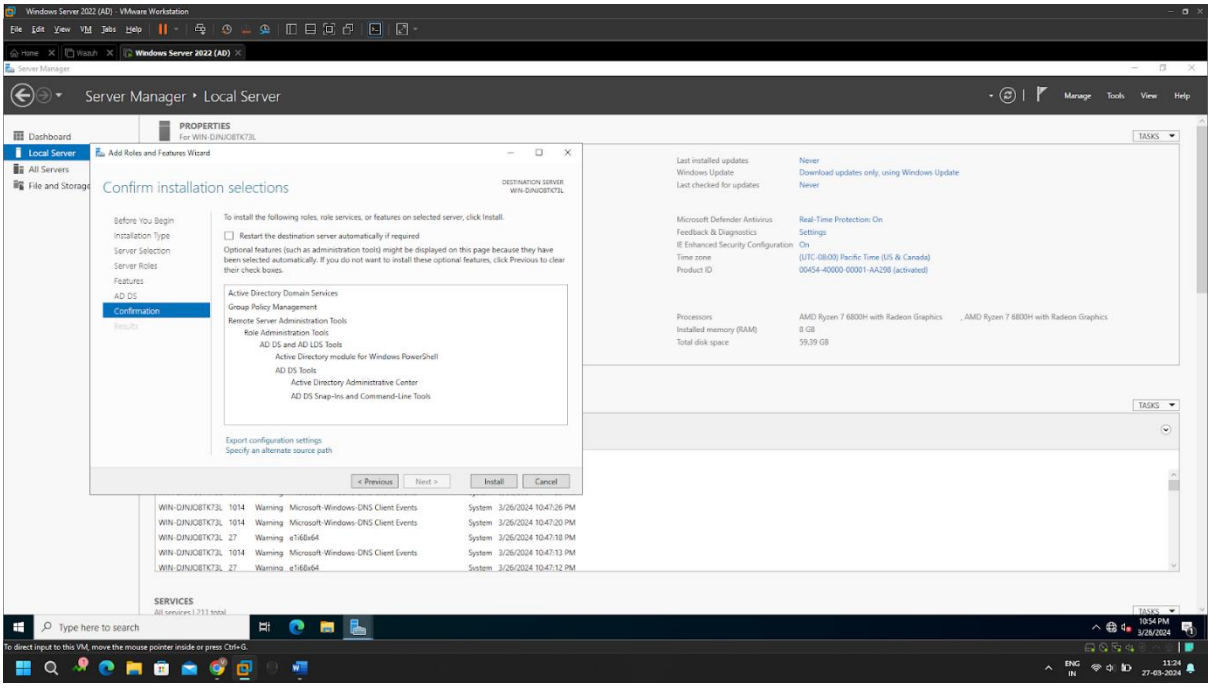
Click Next,



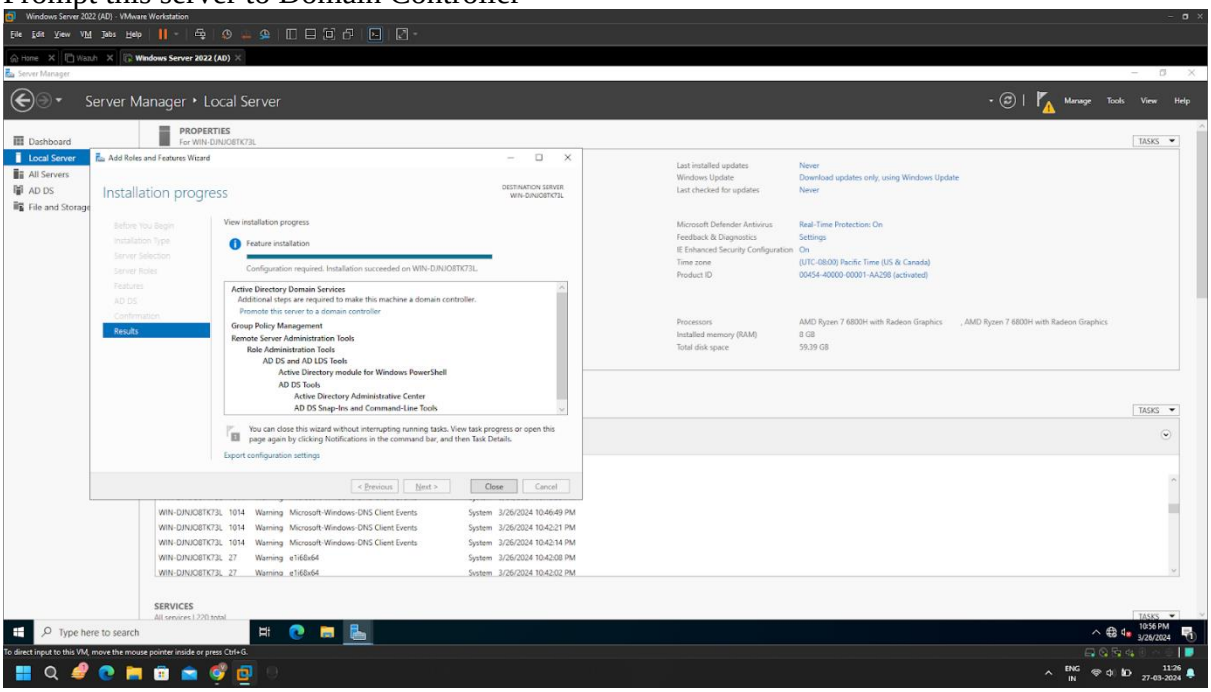
Select – Active Directory Domain Services and Click Next,



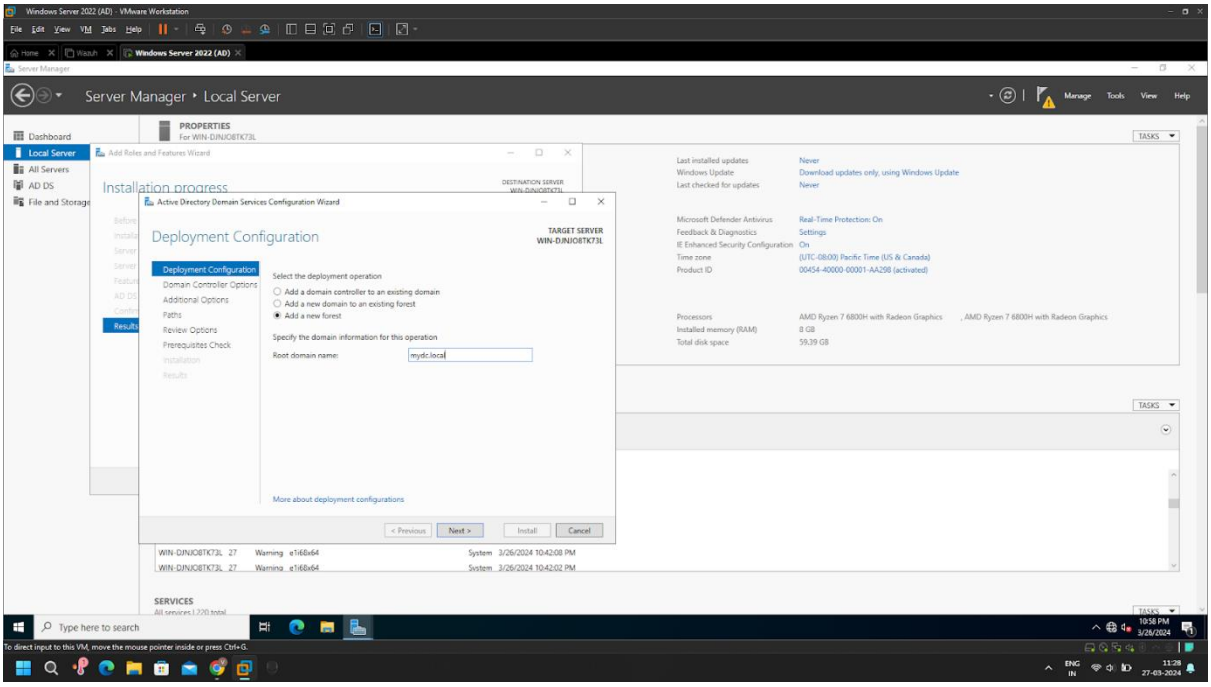
Next Install –

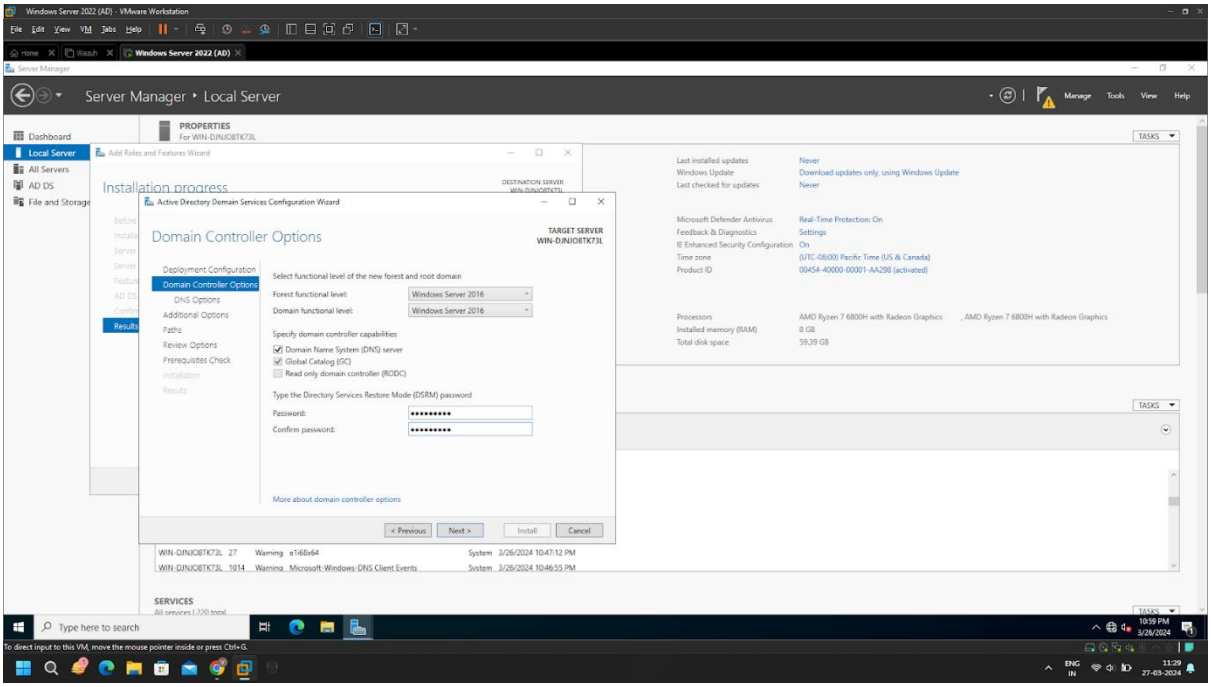


Prompt this server to Domain Controller

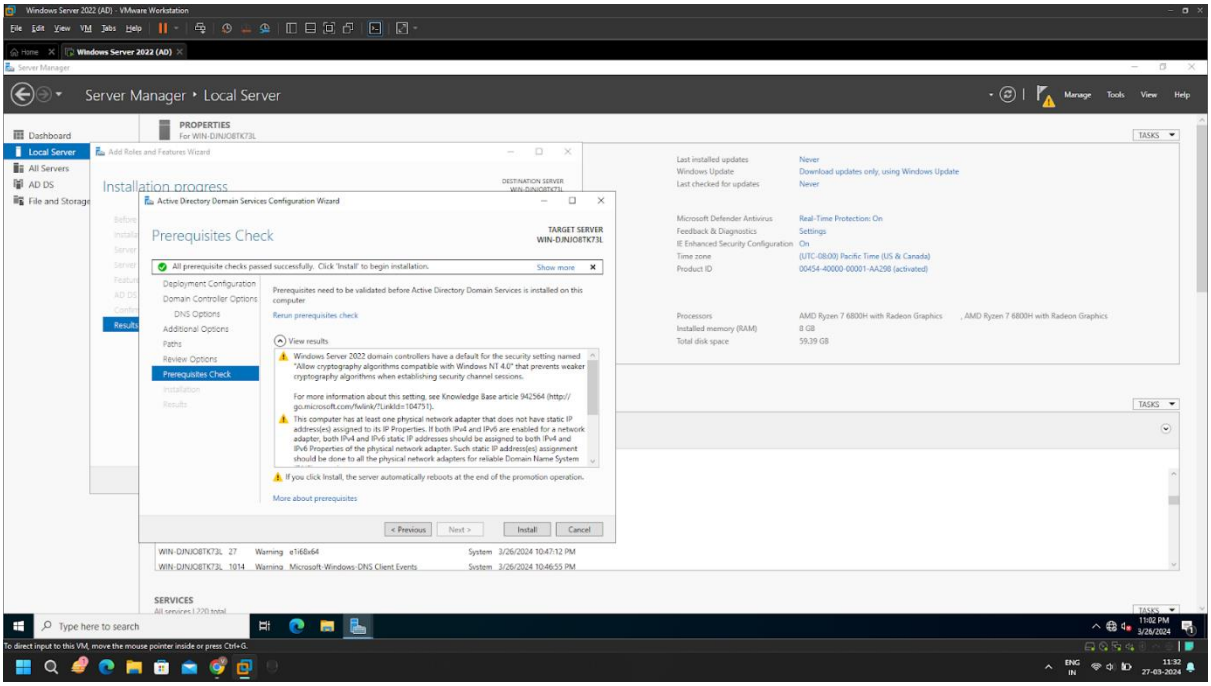


Add New Forest –

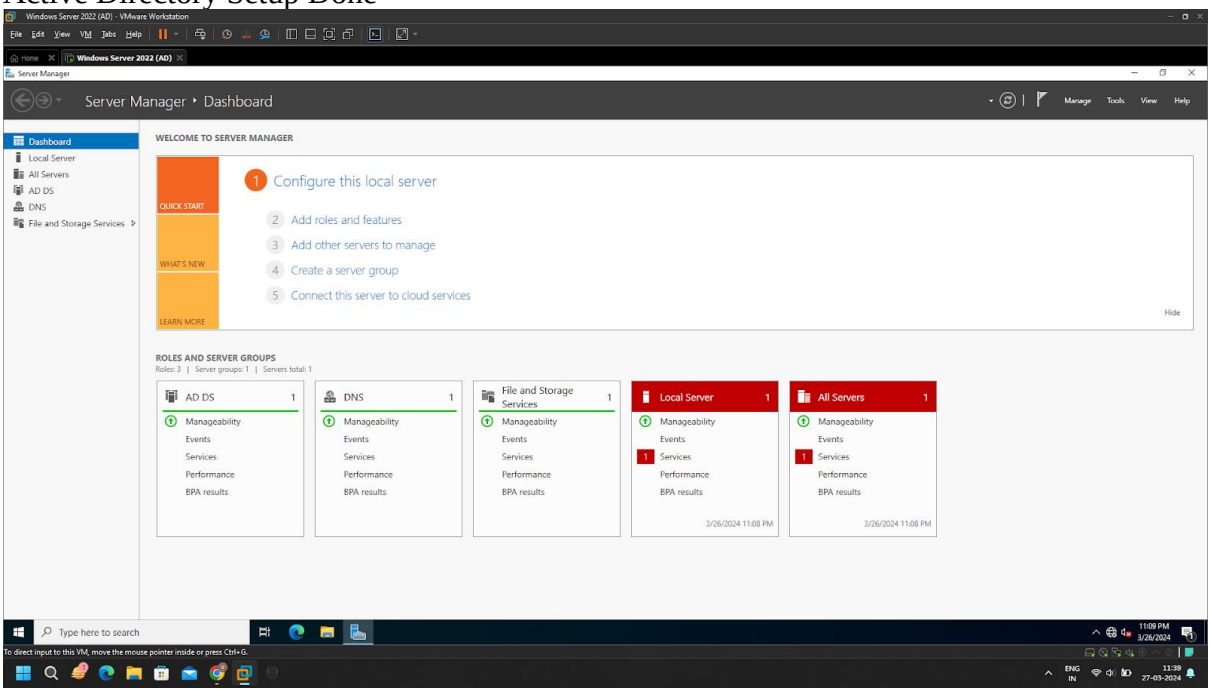




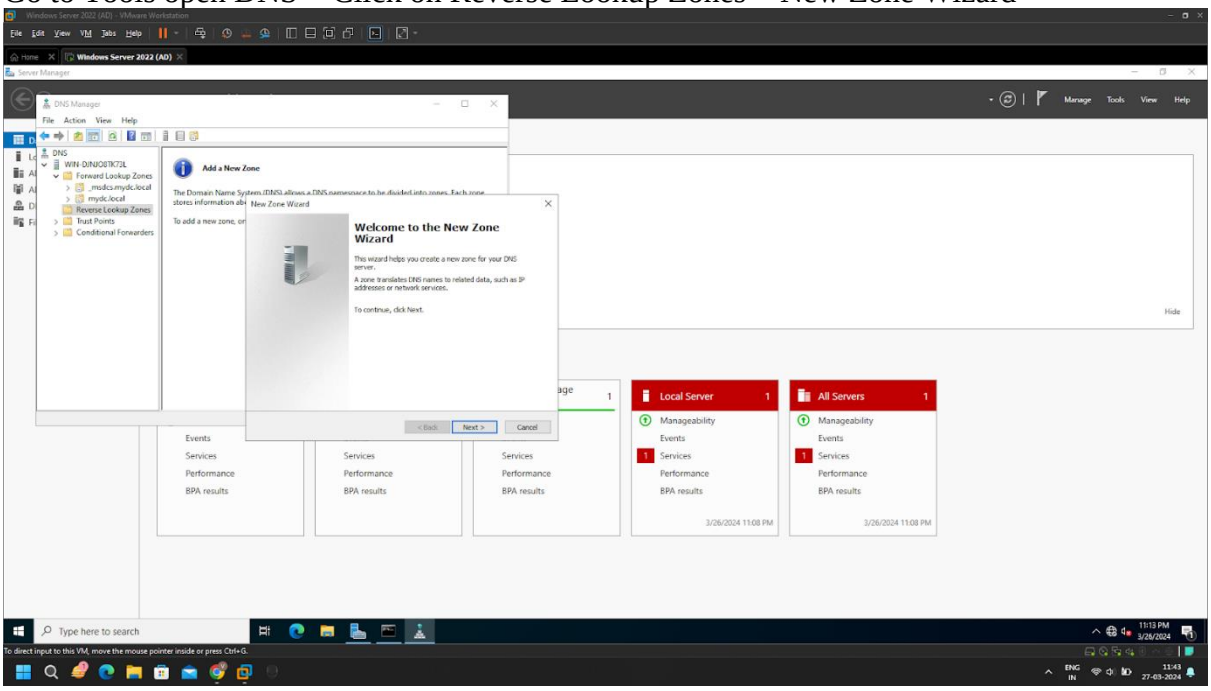
Next Install –



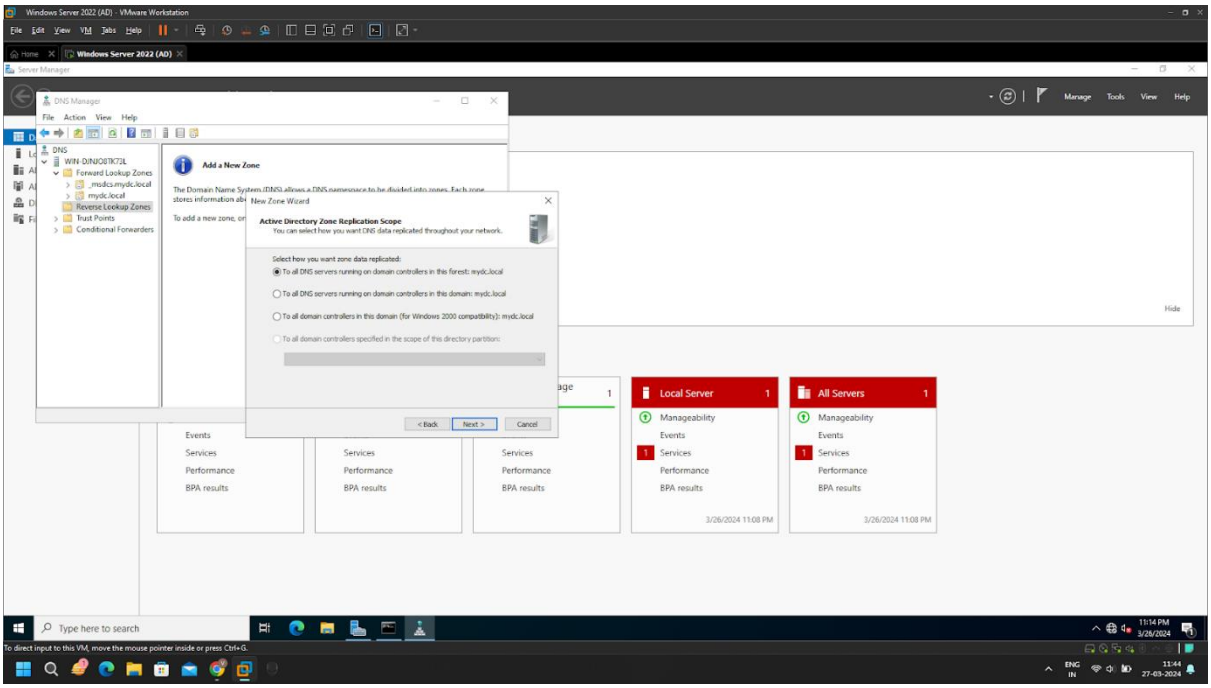
Active Directory Setup Done



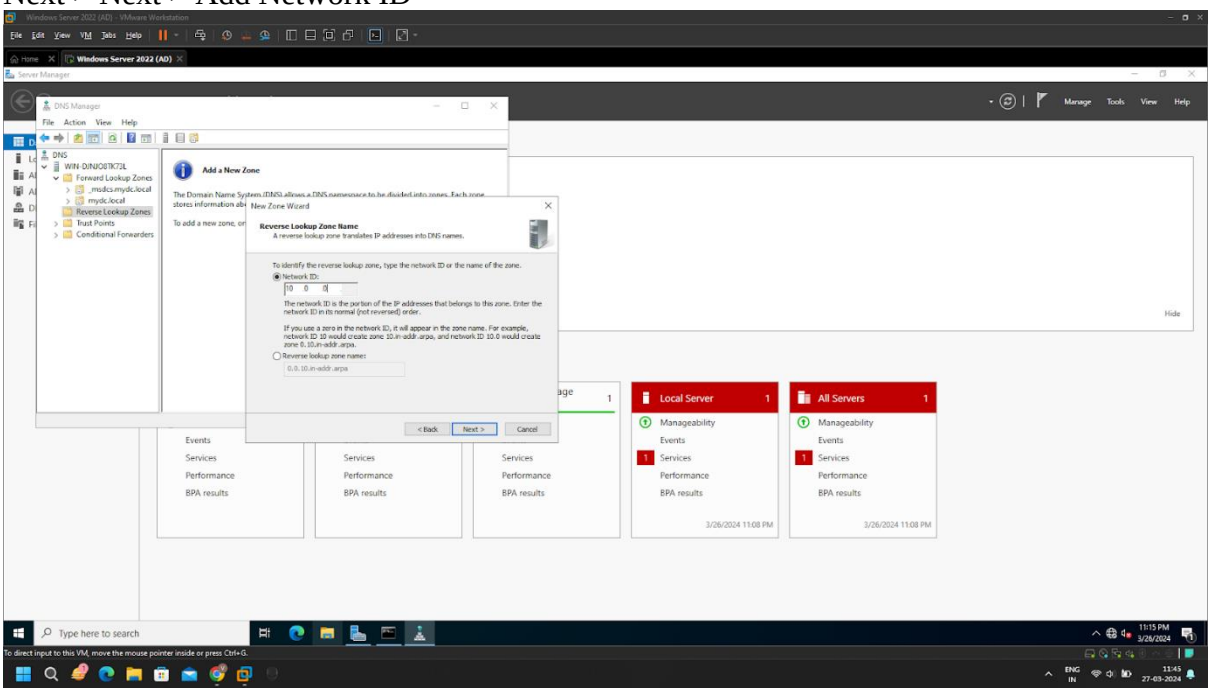
Go to Tools open DNS > Click on Reverse Lookup Zones > New Zone Wizard



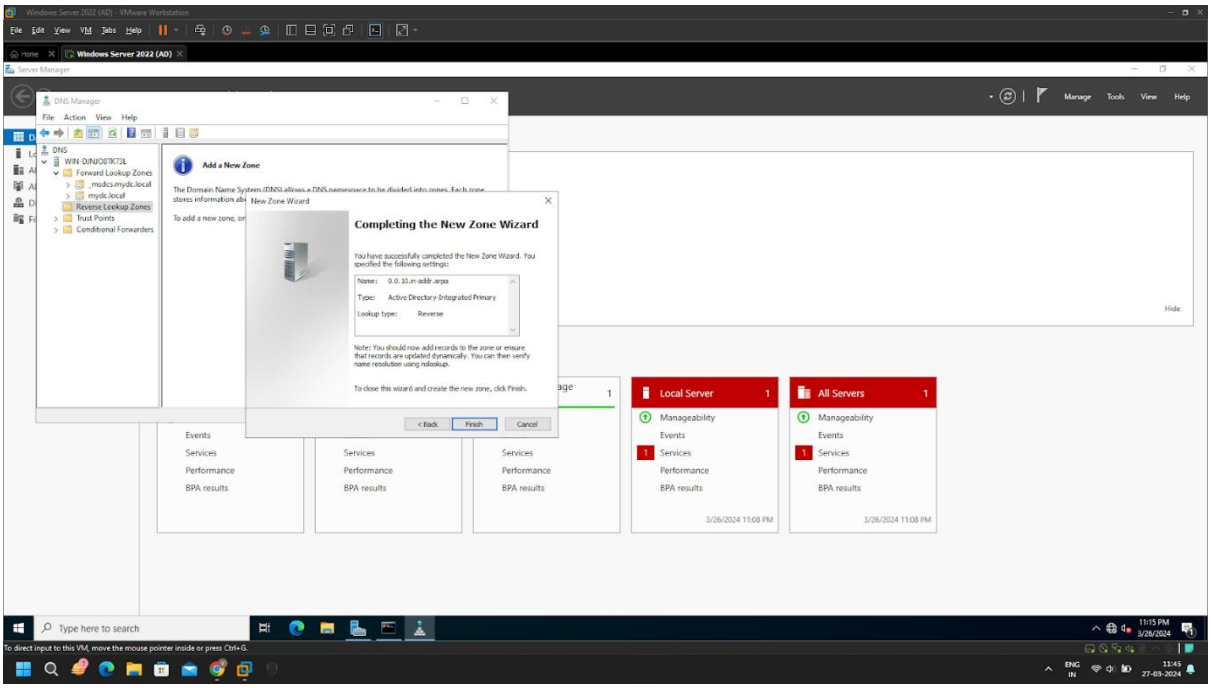
Click Next –



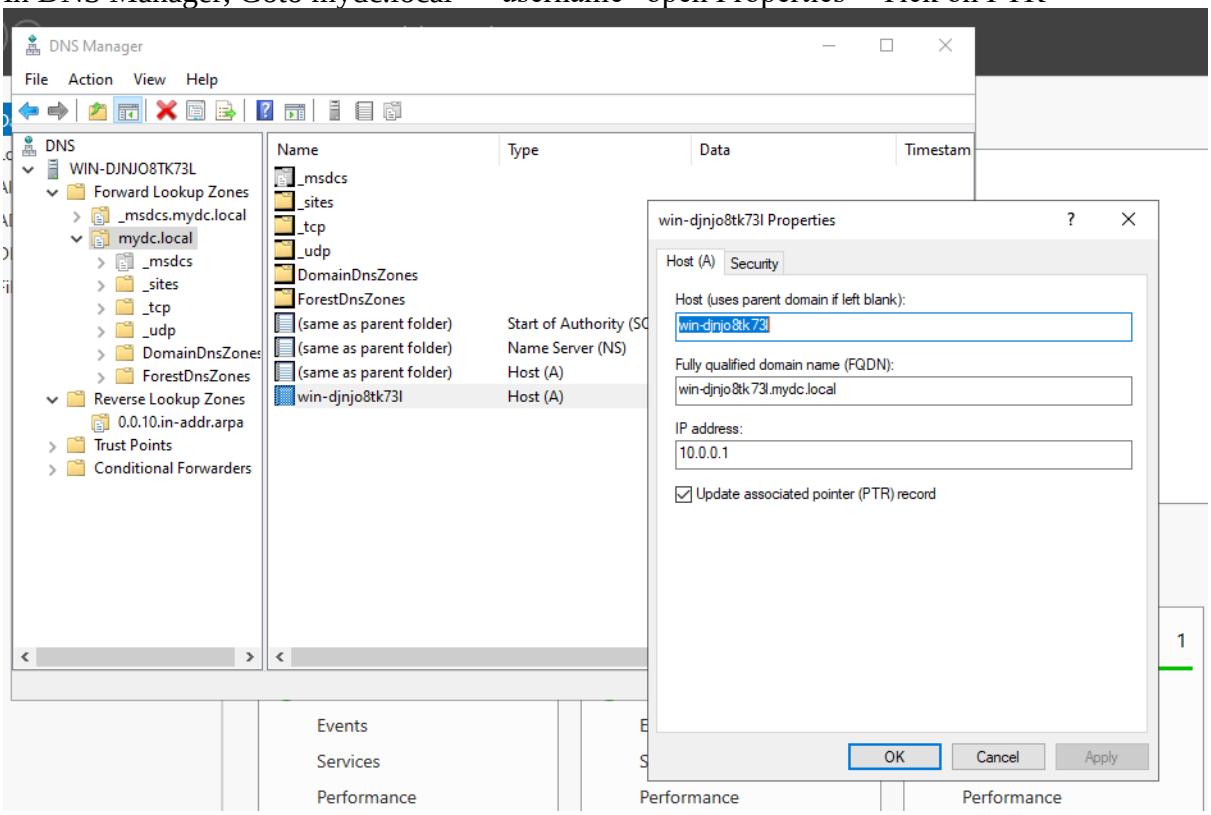
Next > Next > Add Network ID –



Next > Finish

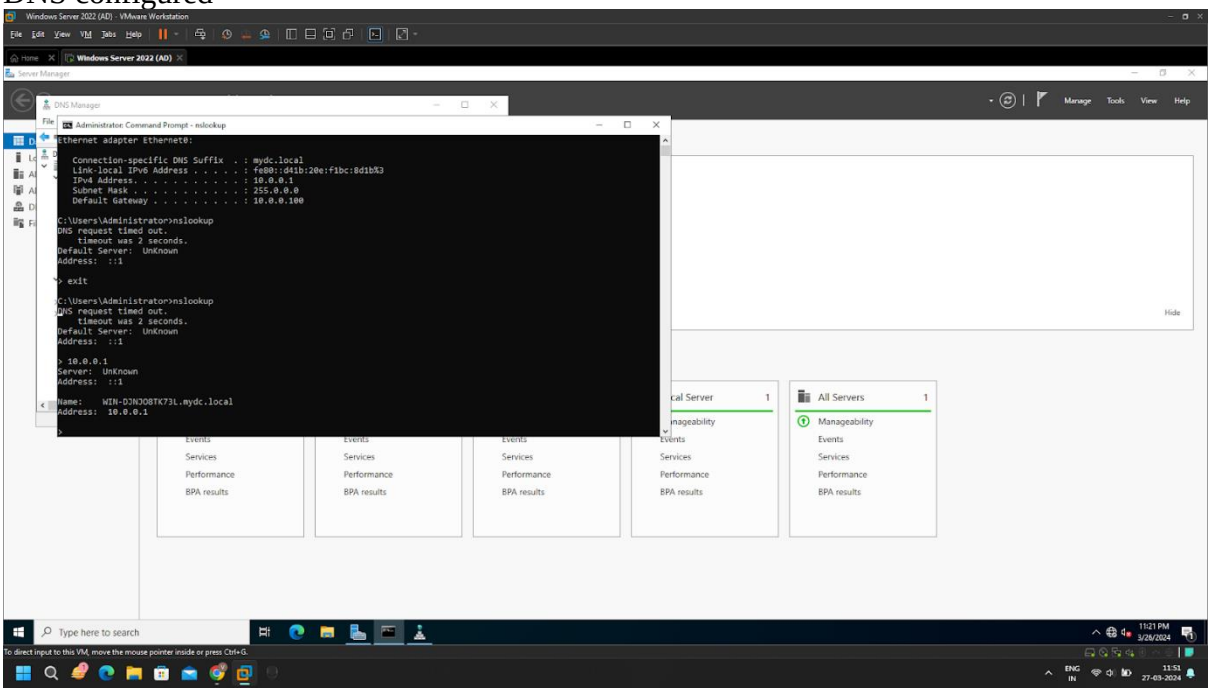


In DNS Manager, Goto mydc.local > “username” open Properties > Tick on PTR

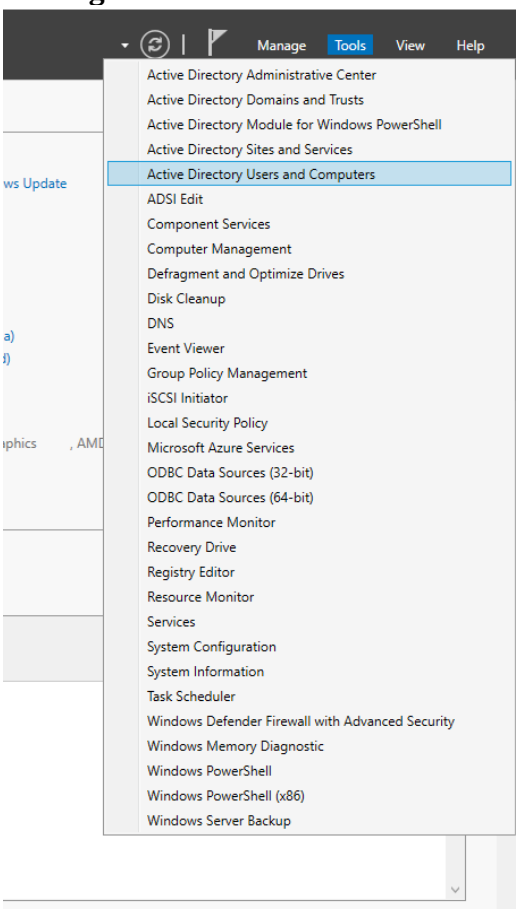


Click OK.

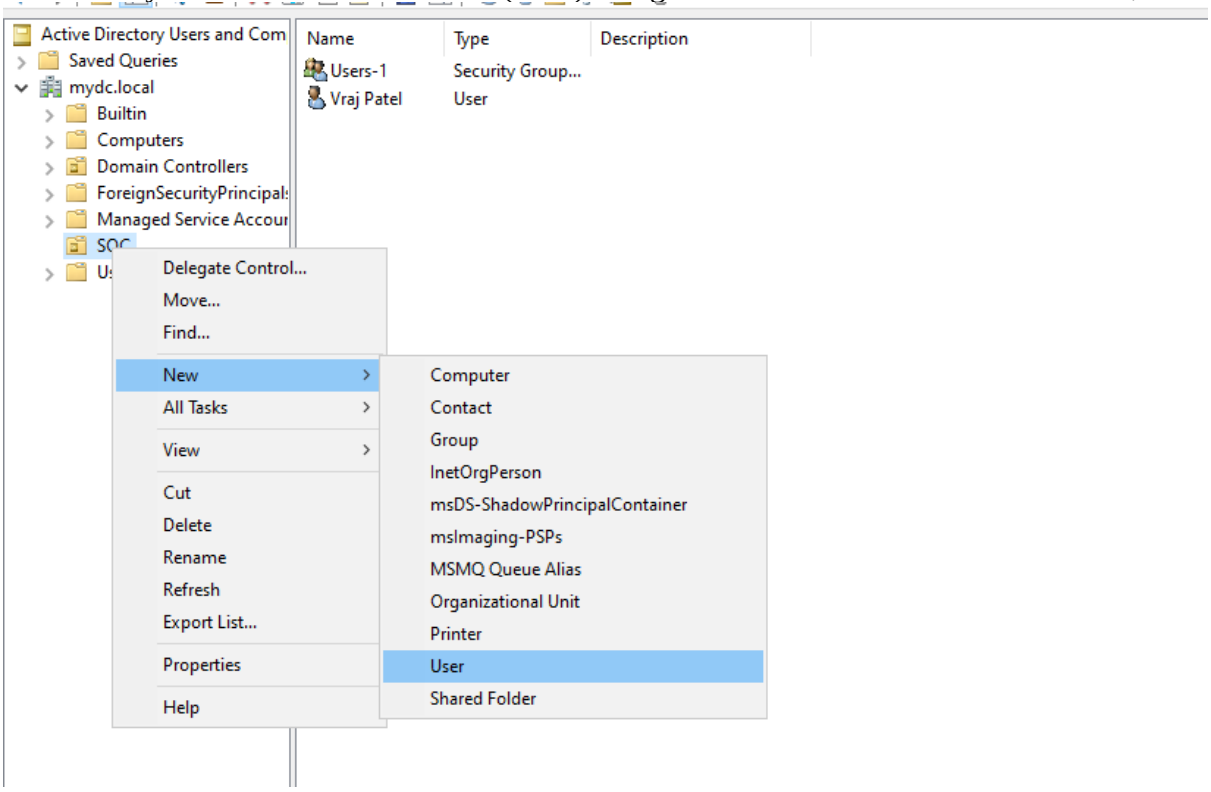
DNS configured –

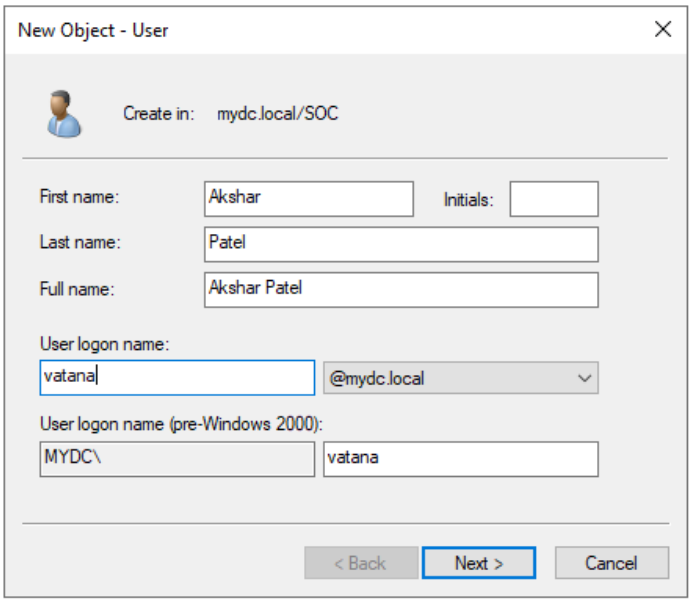


Adding Users –

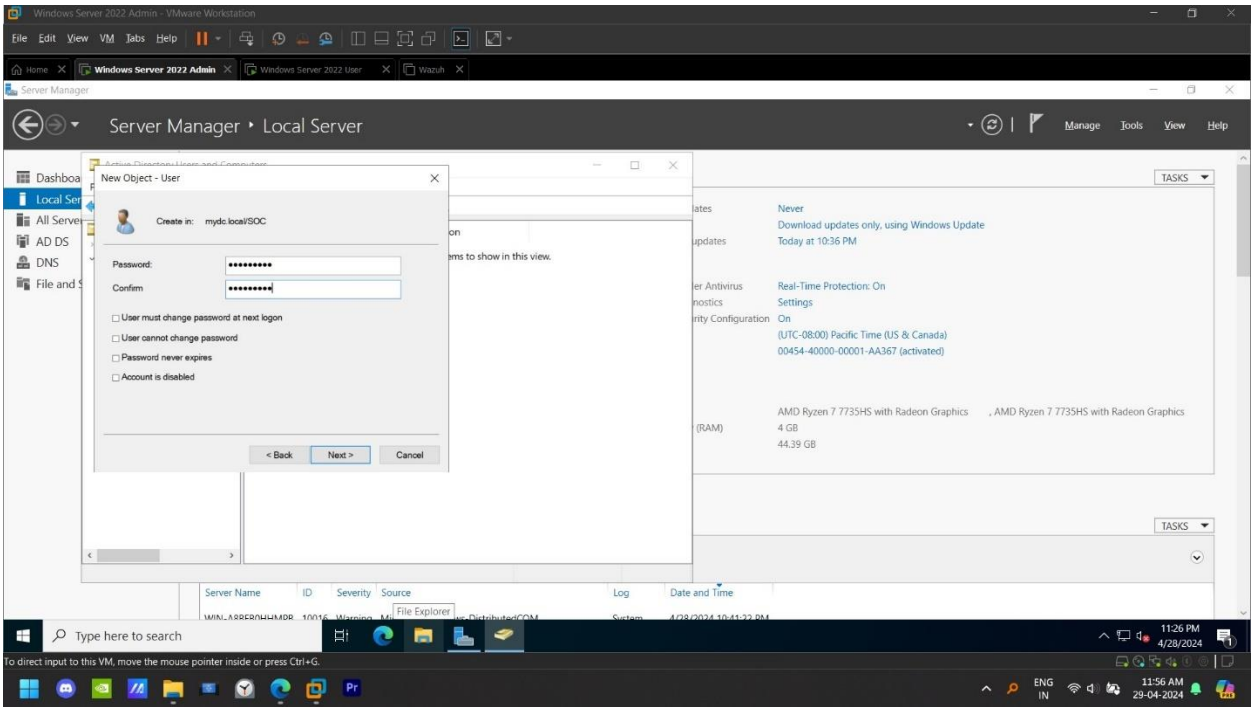


Click on mydc.local > Create New OU(SOC) > Right click on that and create New User,

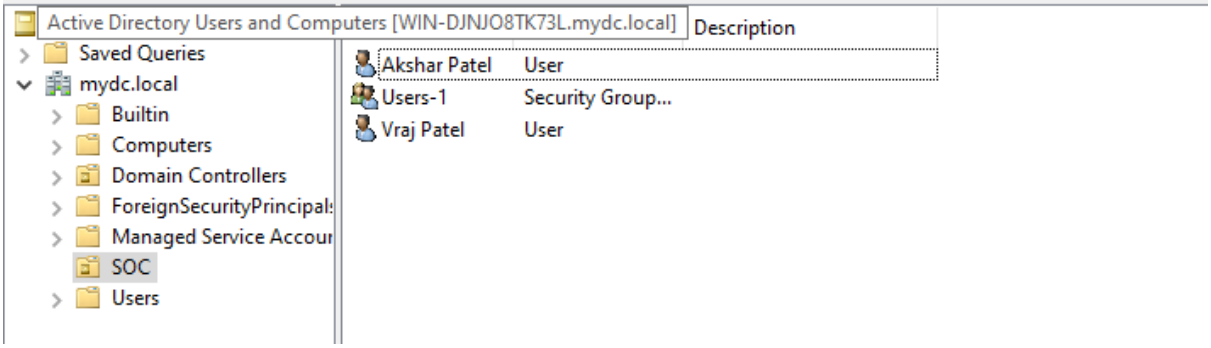




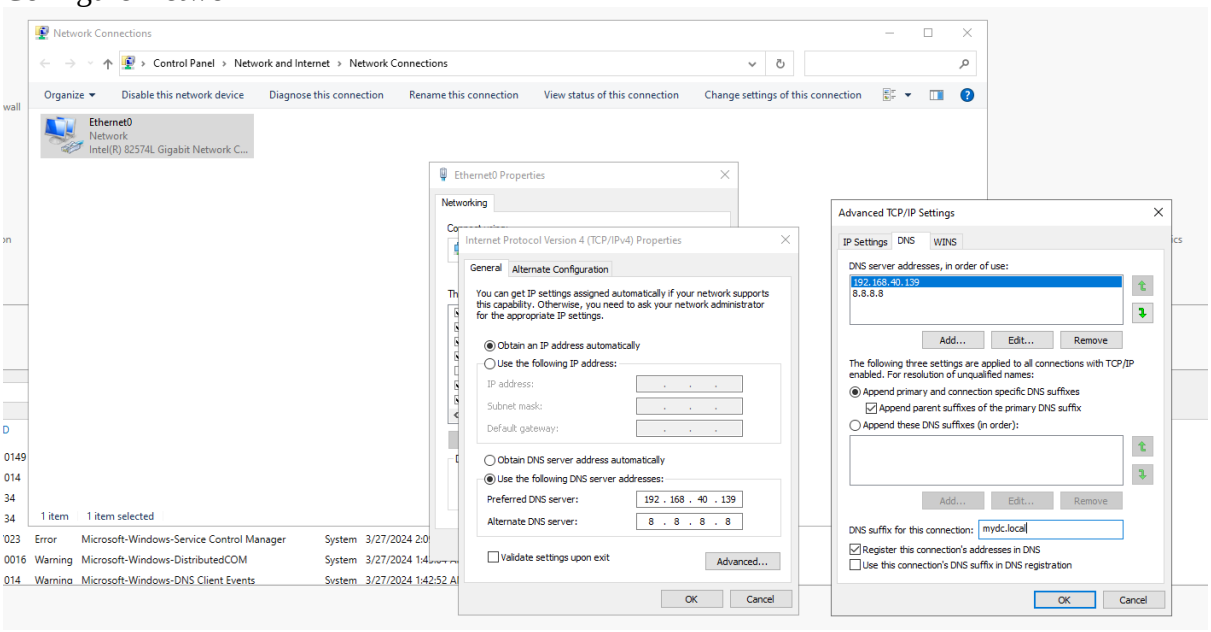
Add Password –



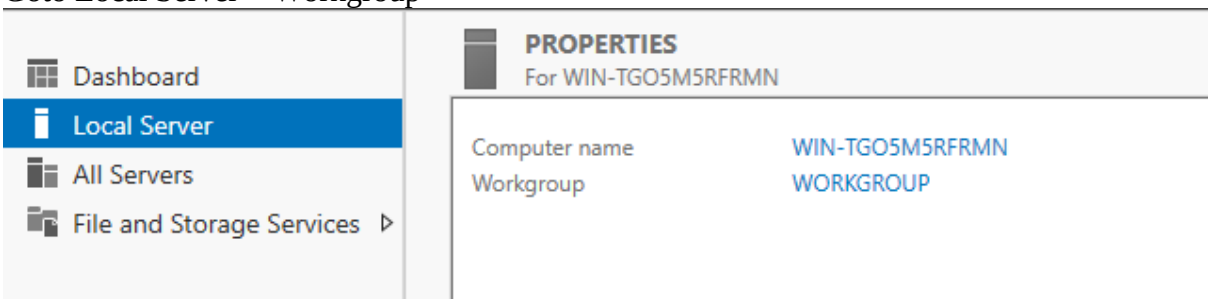
User created –



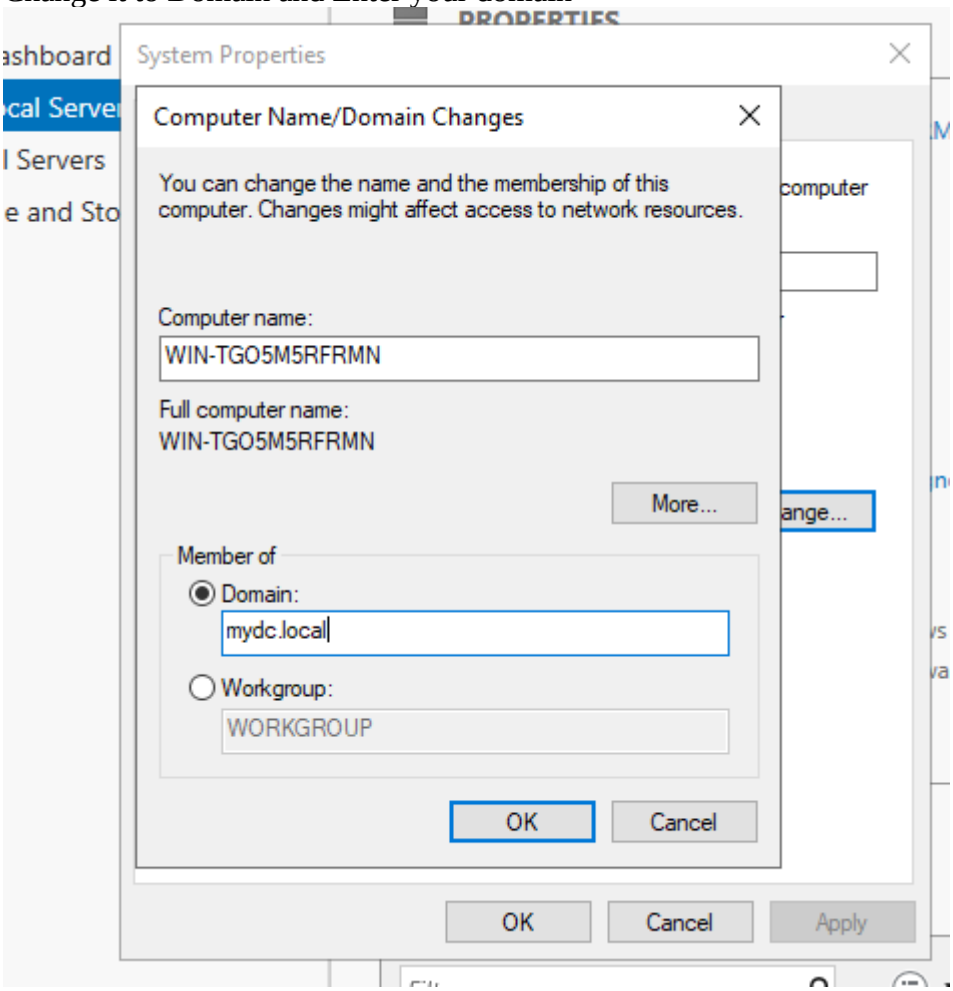
Create new VM to login with the created credentials
Configuring another pc to add it in the workgroup mydc.local
Configure Network



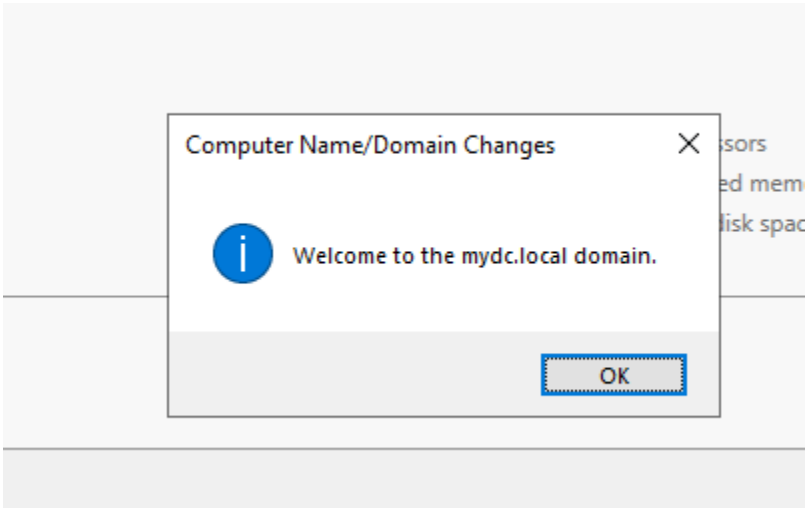
Goto Local Server > Workgroup



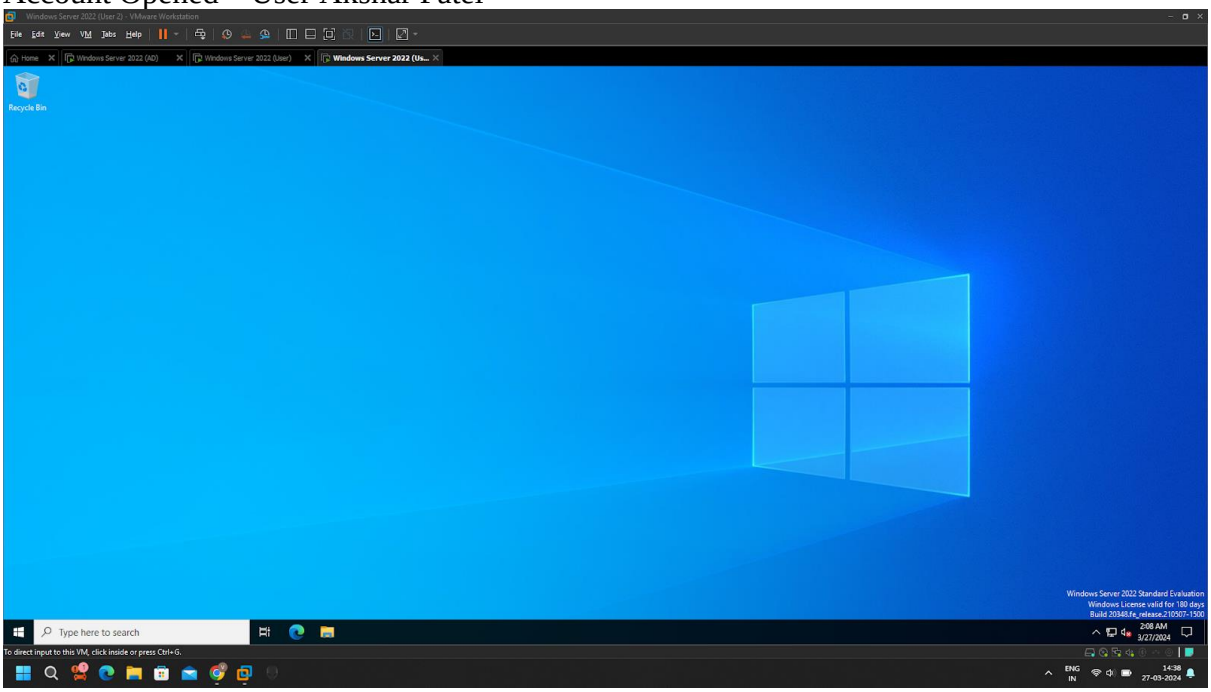
Change it to Domain and Enter your domain



Click OK.



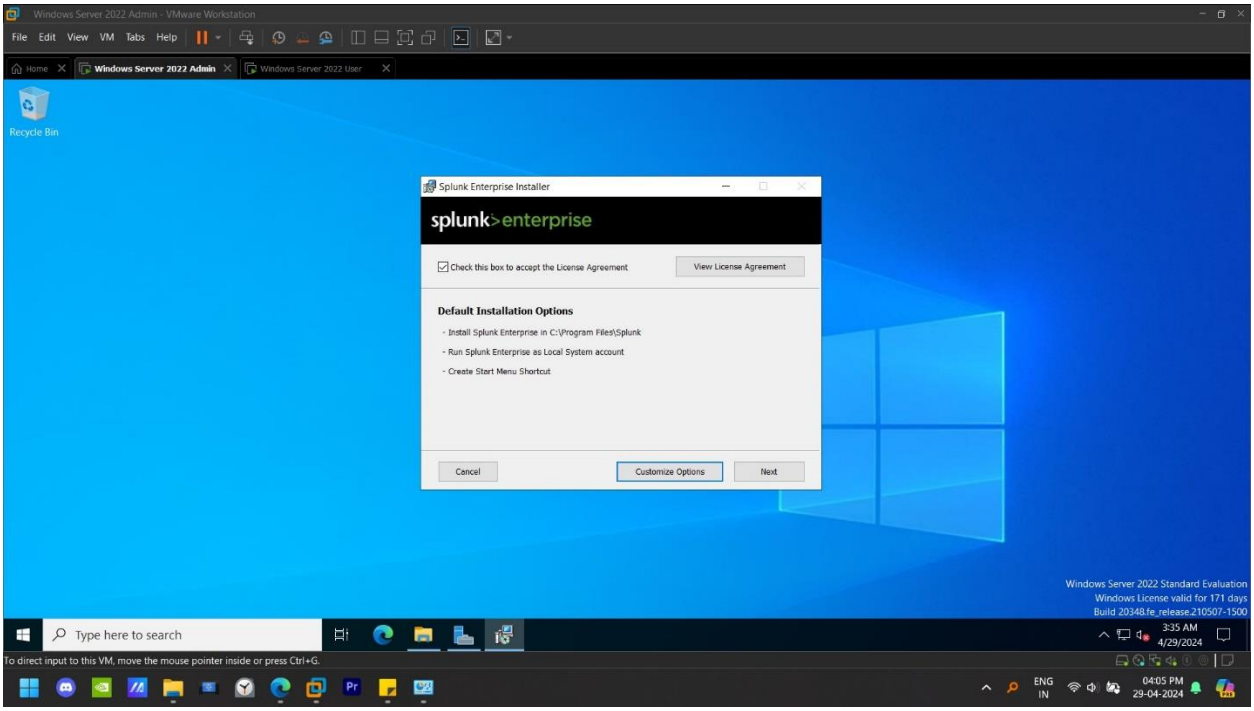
Account Opened – User Akshar Patel



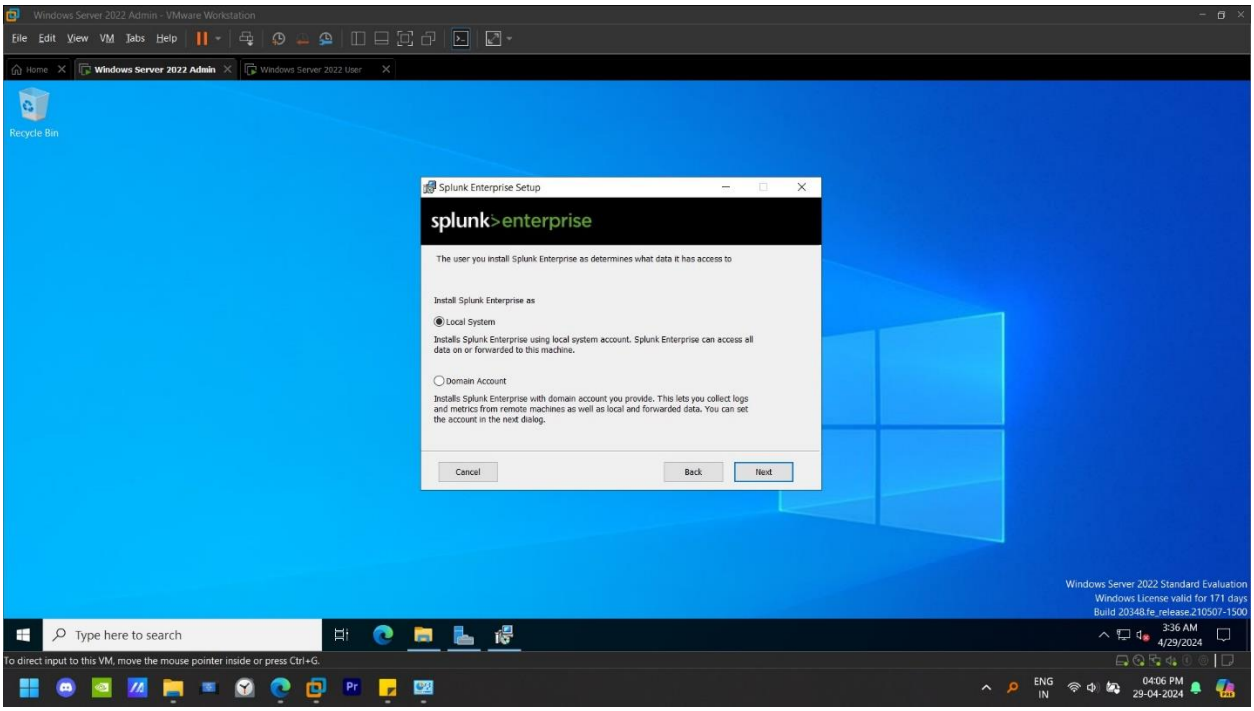
CHAPTER: 11 INSTALLING SPLUNK

CHAPTER: 11 INSTALLING SPLUNK

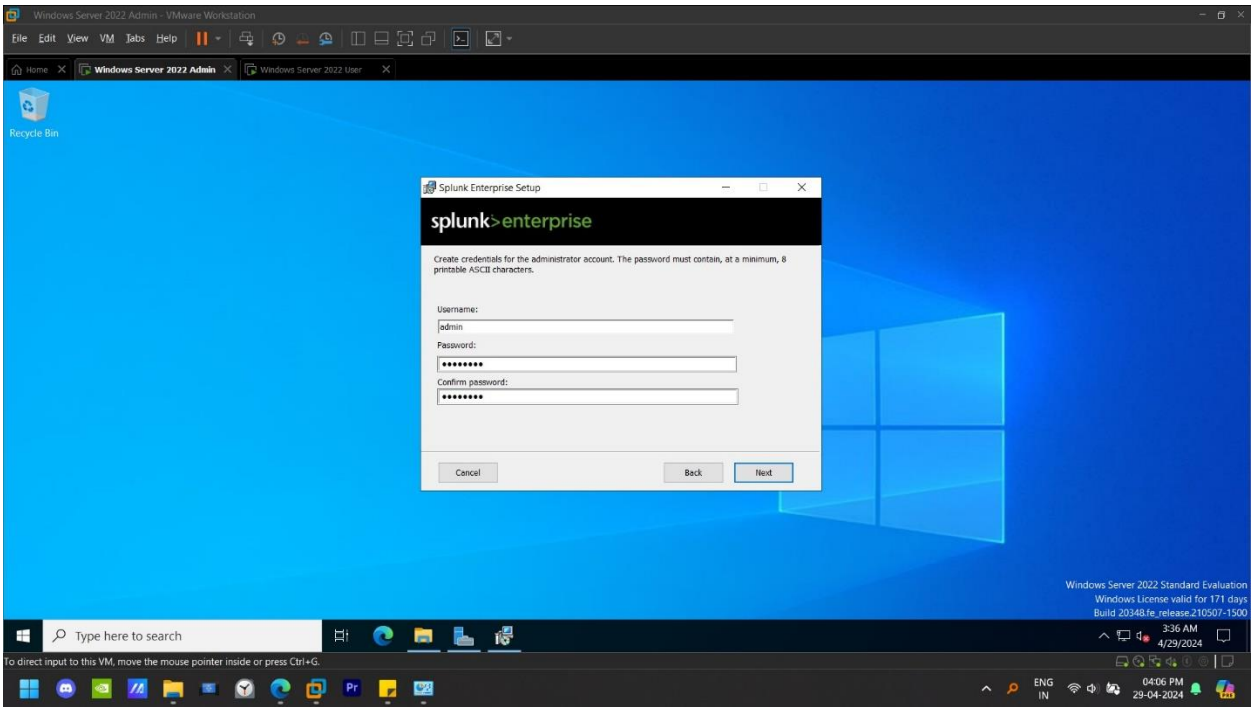
Installing Splunk Enterprise in Windows Server 2022 Admin Account



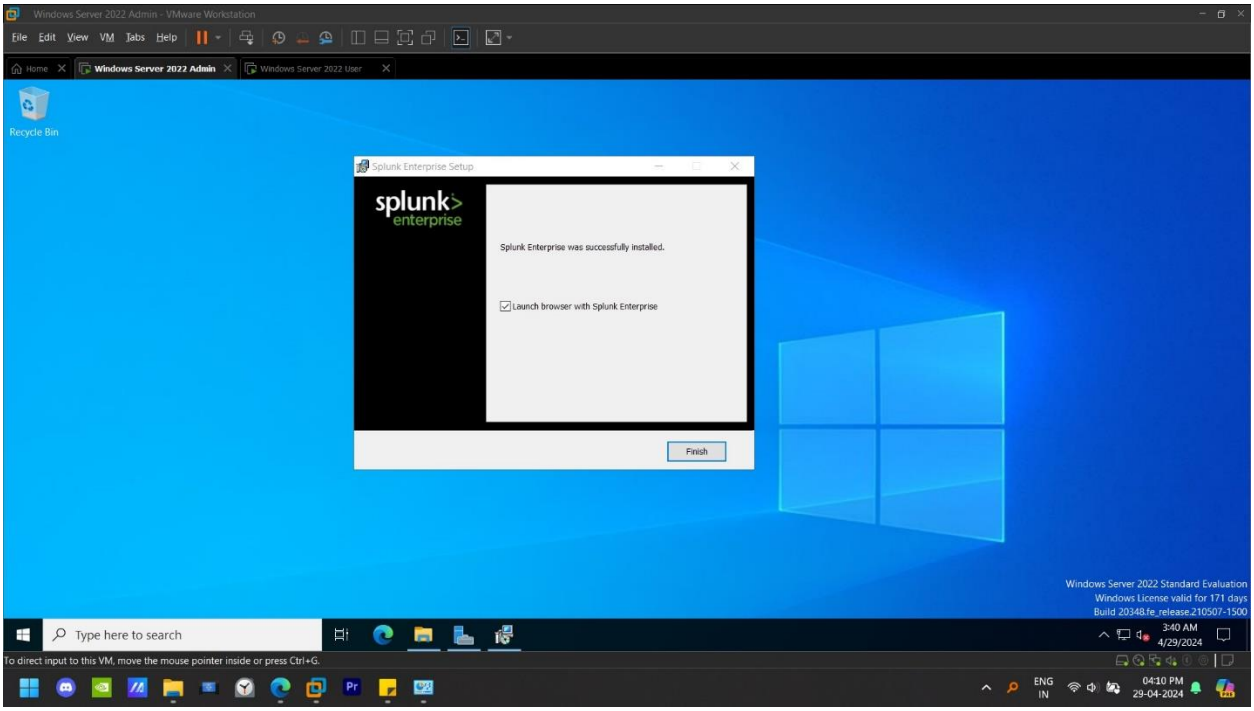
Select Local Account –



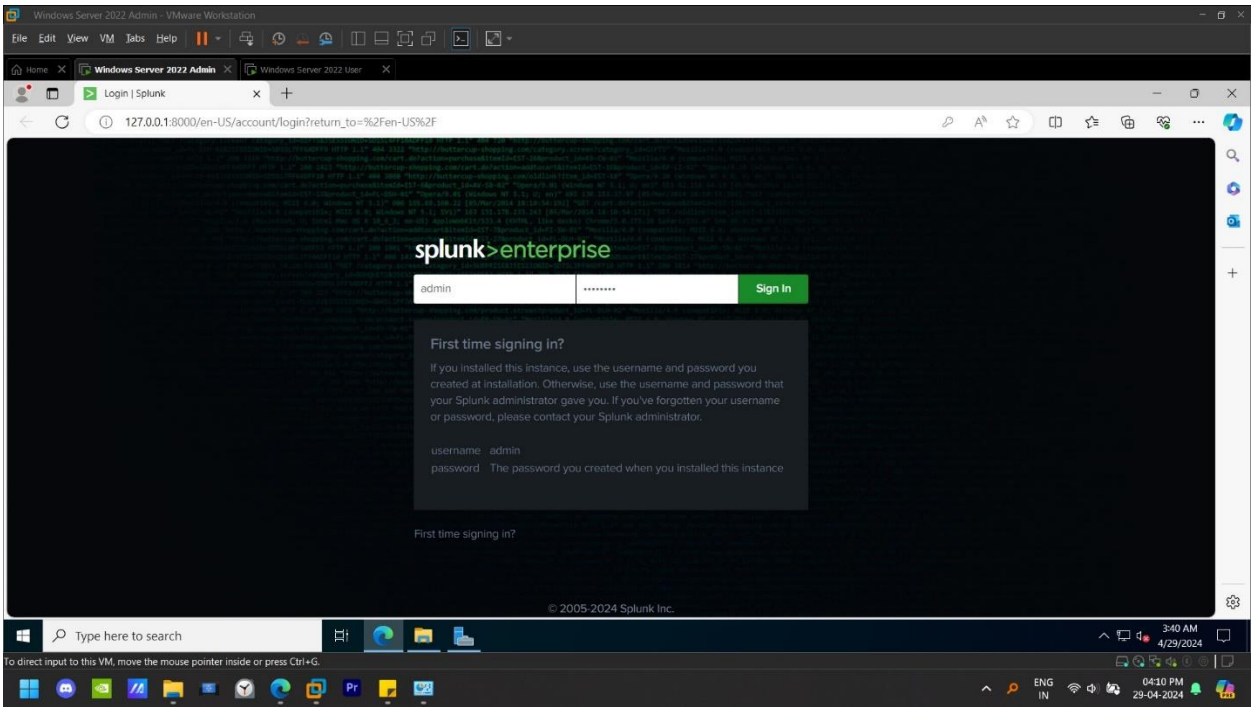
Enter Login credentials –



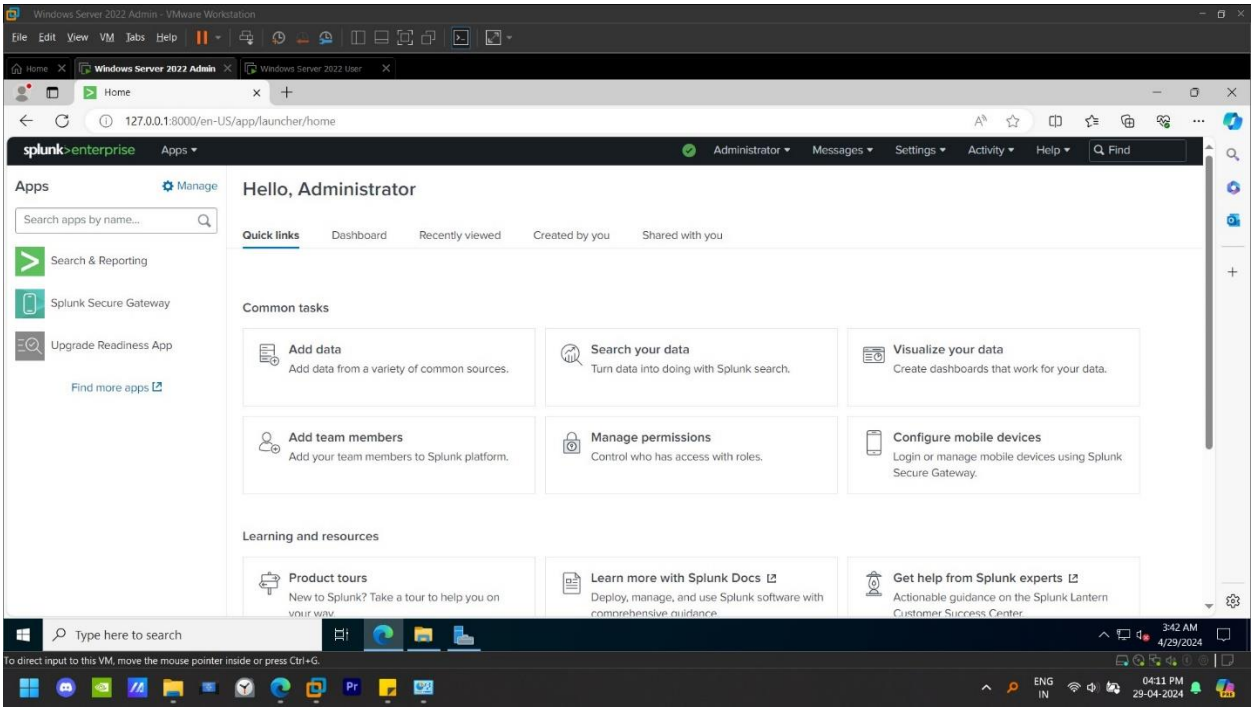
Installation Done –



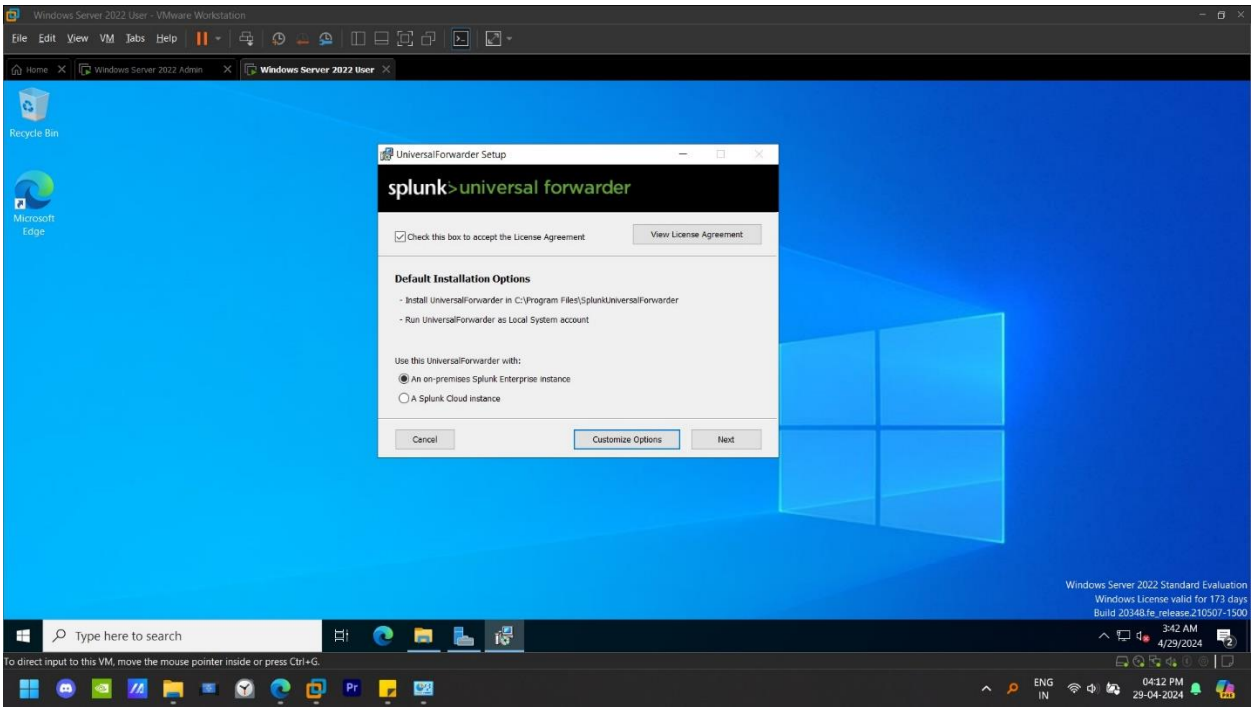
Open Splunk Enterprise from Start Menu –



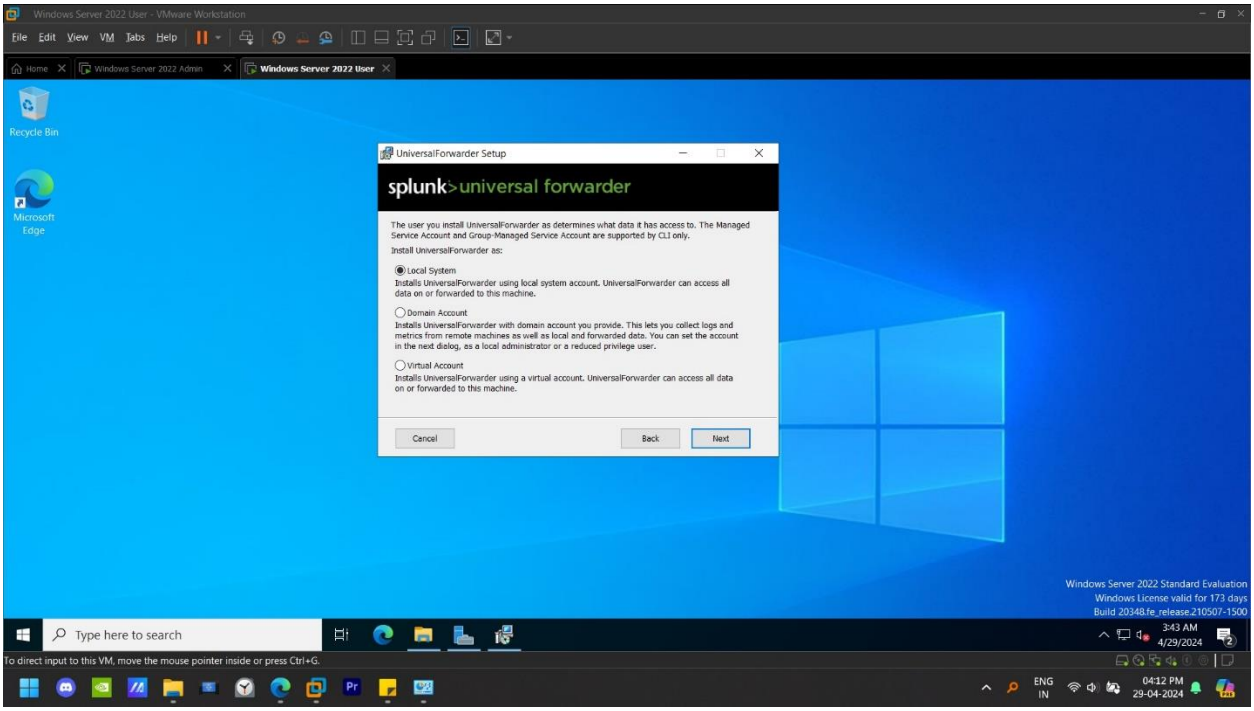
Enter Login Credentials –



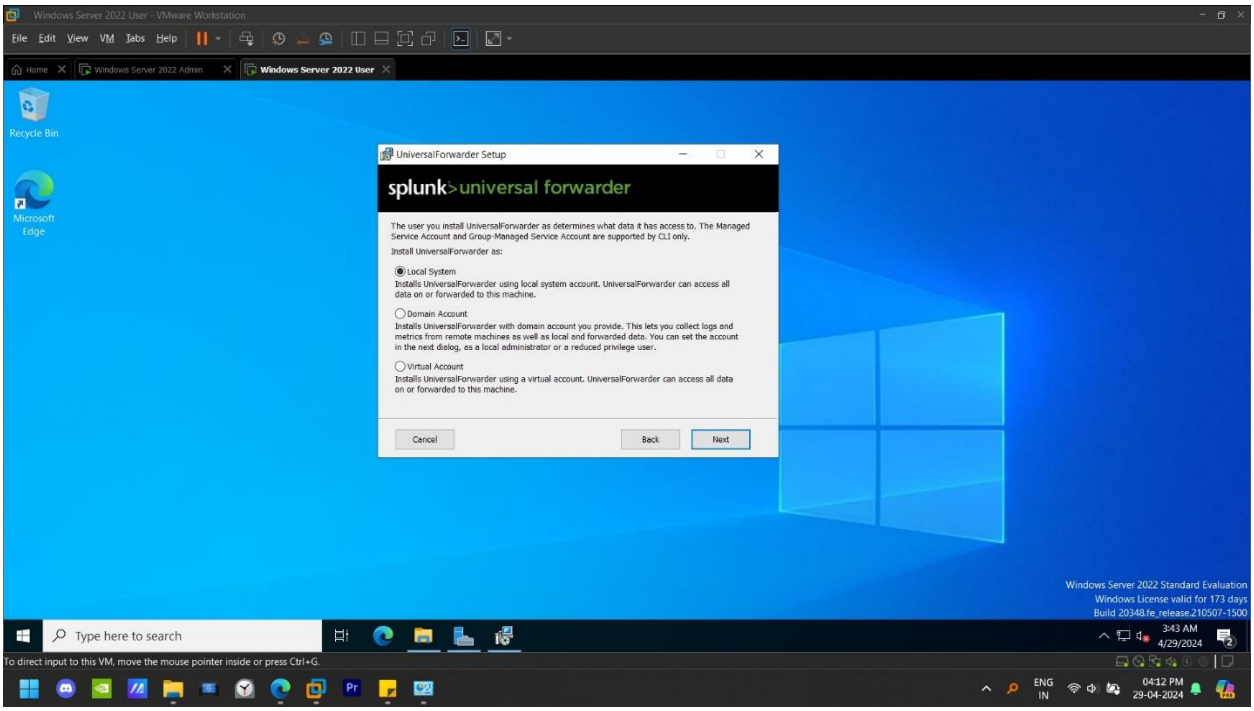
Installing Splunk Forwarder in Windows Server 2022 User Account –



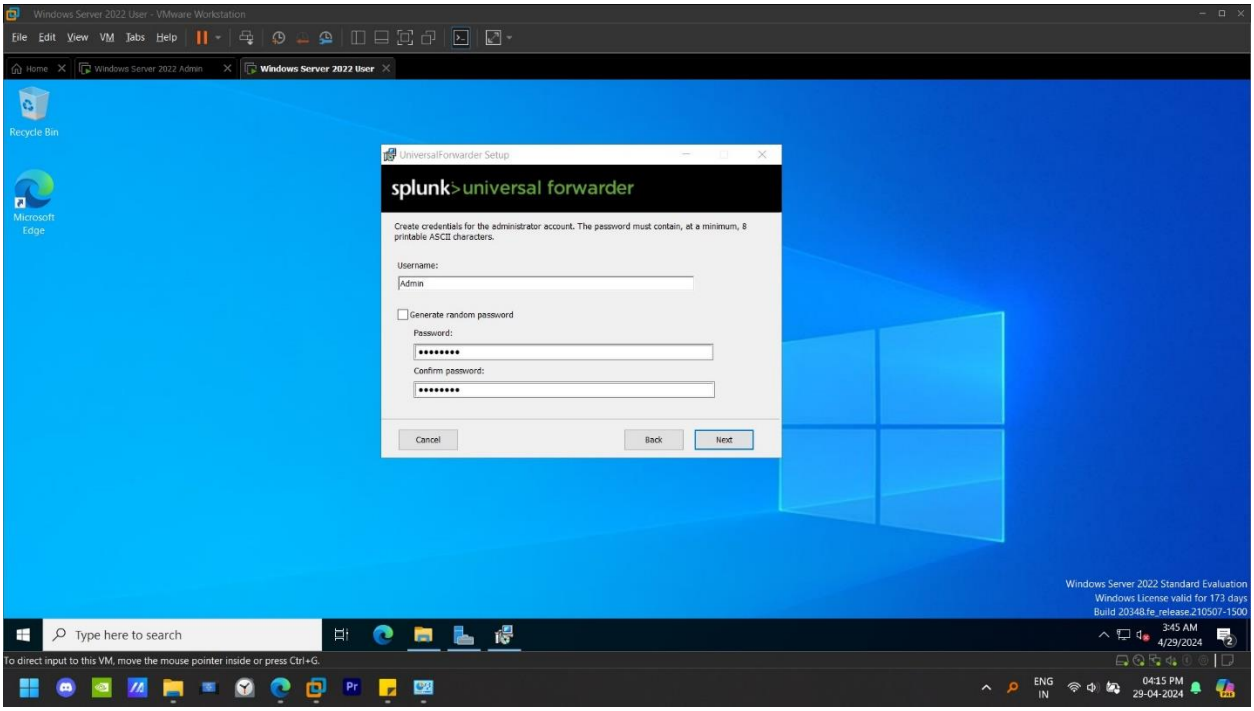
Select Local System –



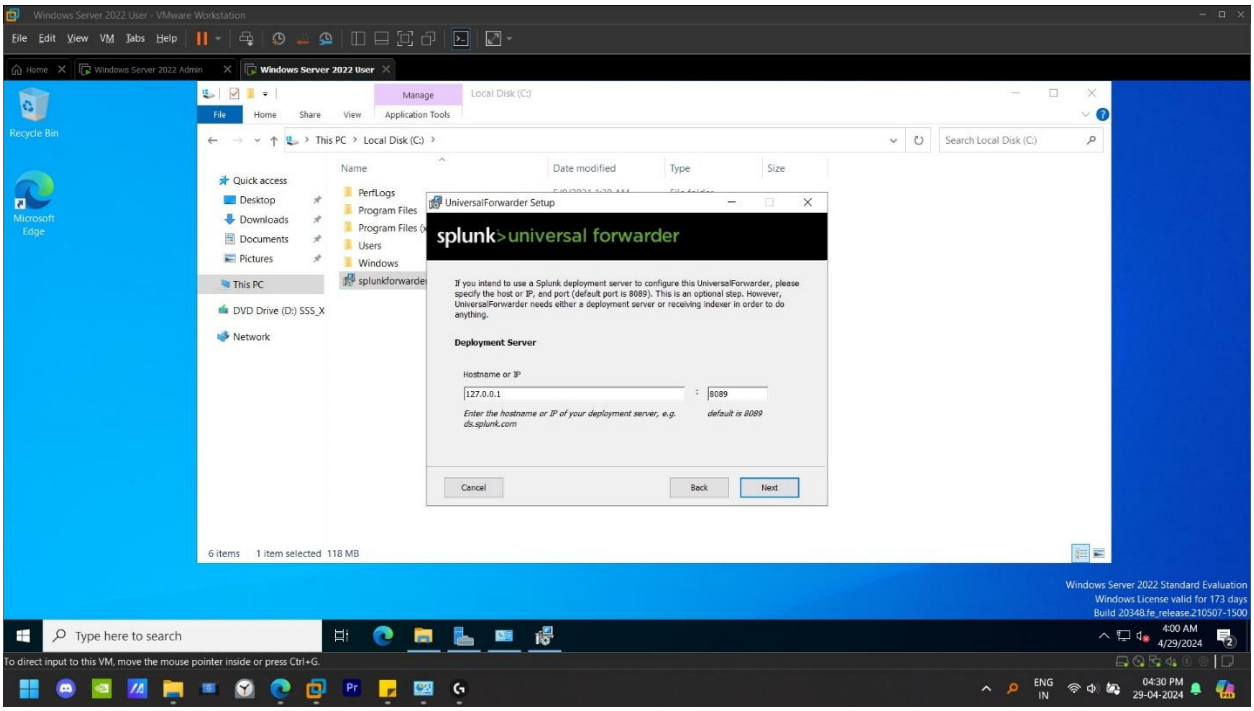
Select All Logs –



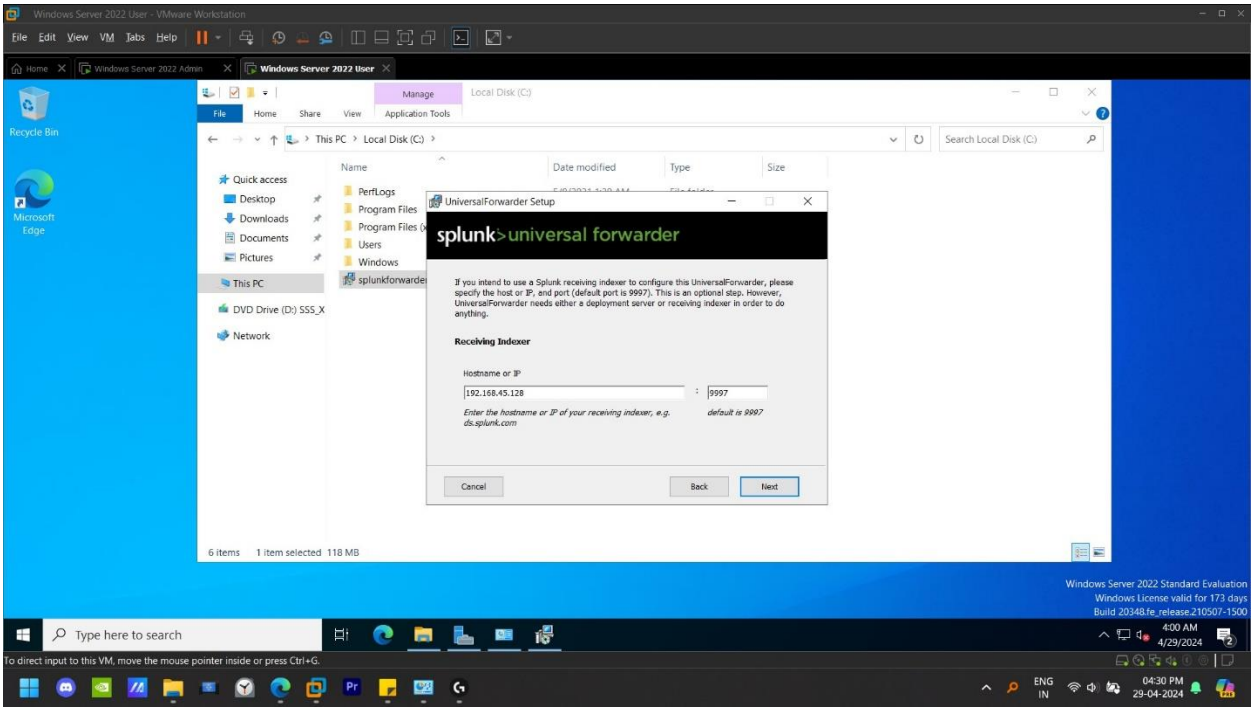
Add admin Credentials –



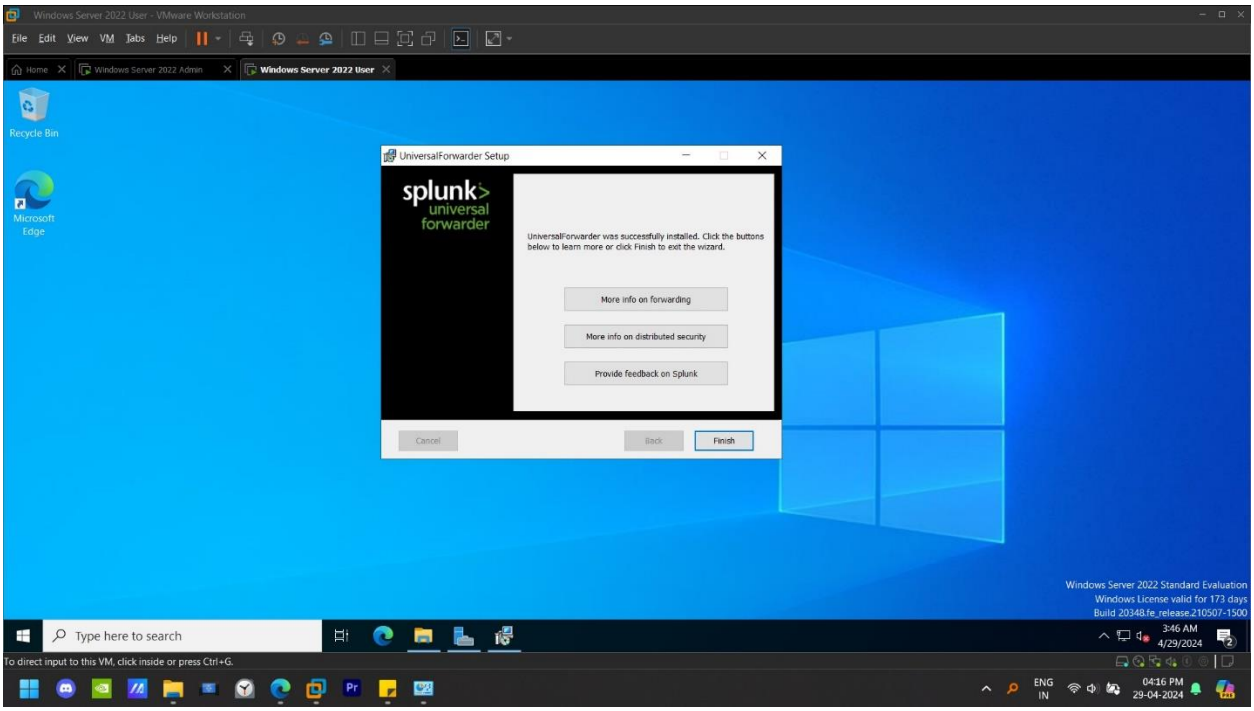
Enter Localhost IP and Port Number(8089) in Deployment Server –



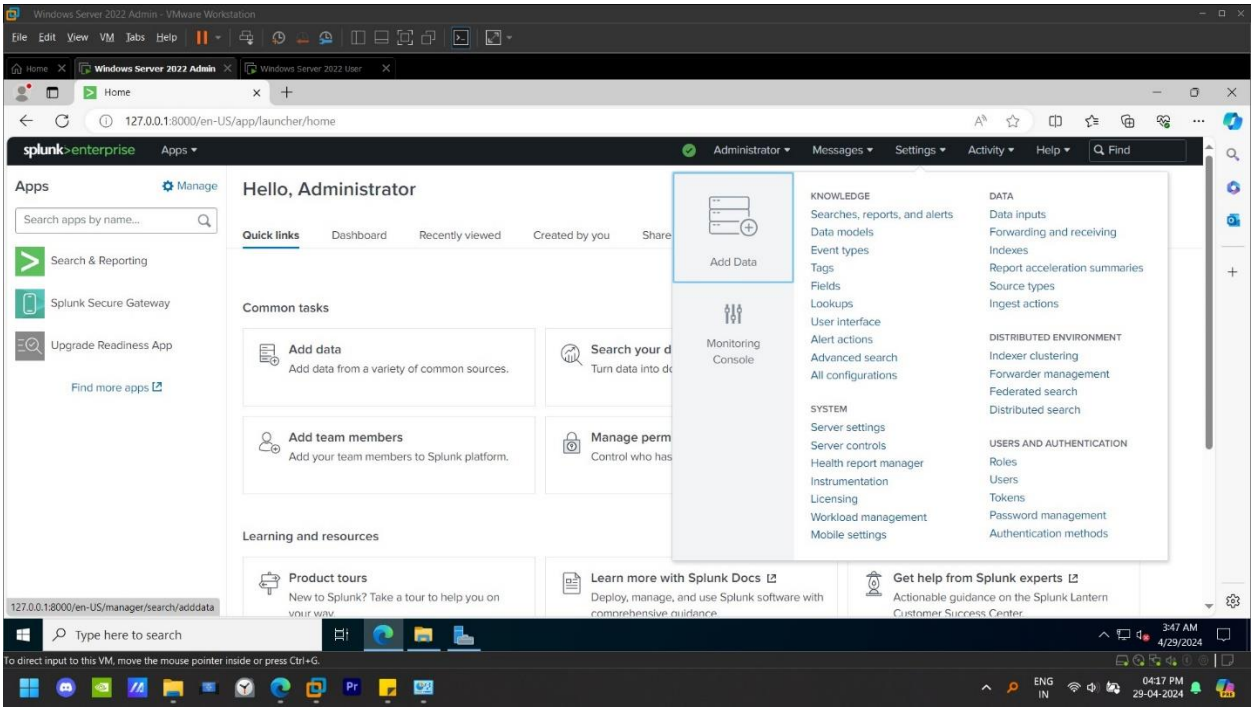
Enter the IP of Enterprise Server Machine and Port Number(9997) in Receiving Indexer –



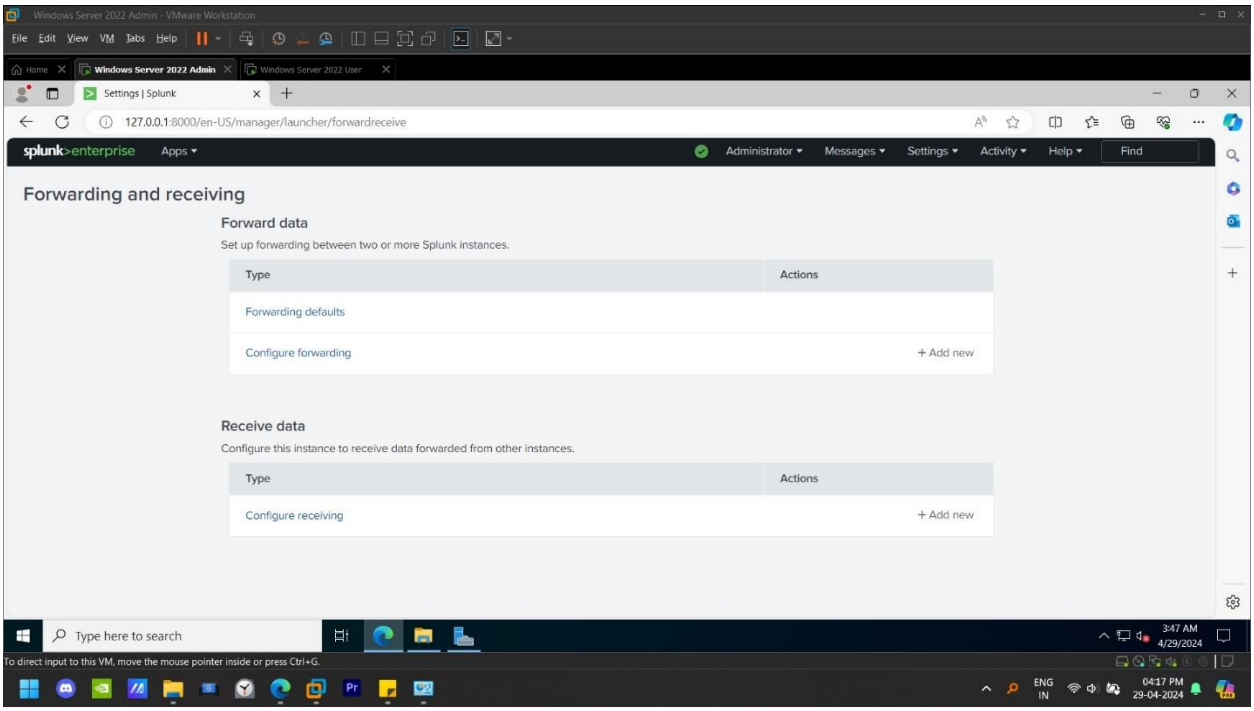
Installation Done –



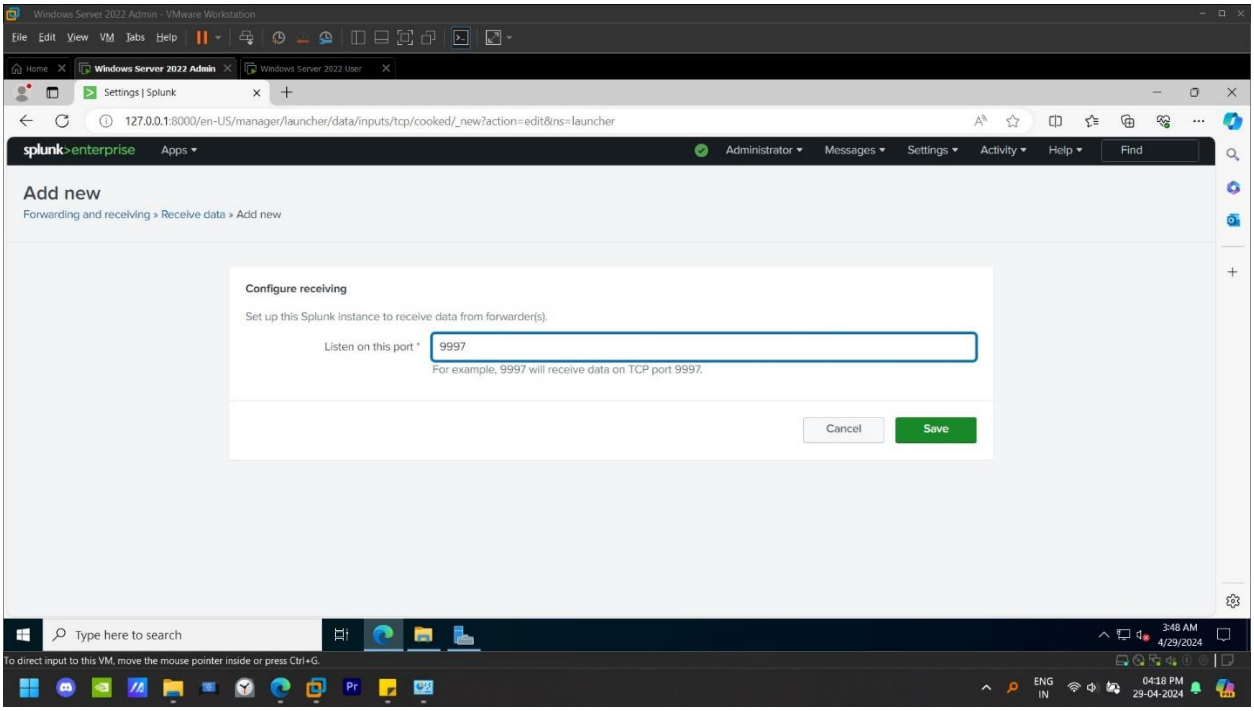
Now Open Splunk and Goto Administrator option and add Forwarding and Receiving Data –

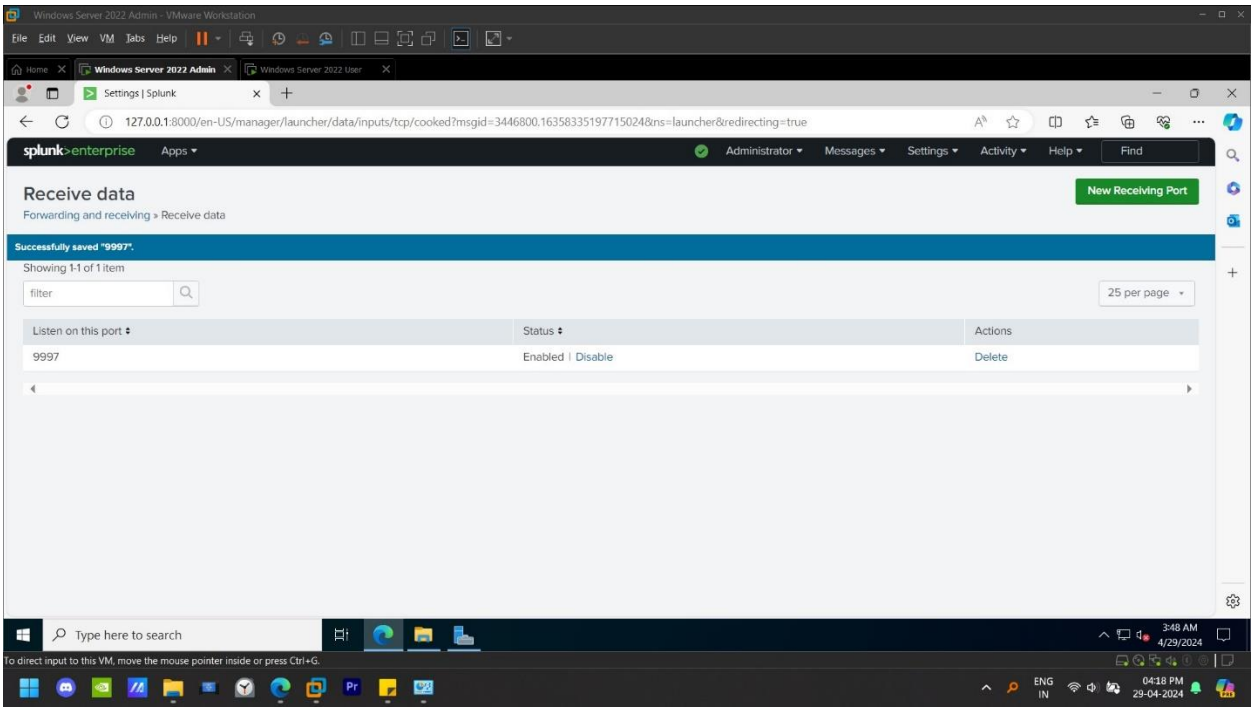


Click on Add Data in Receive Data –

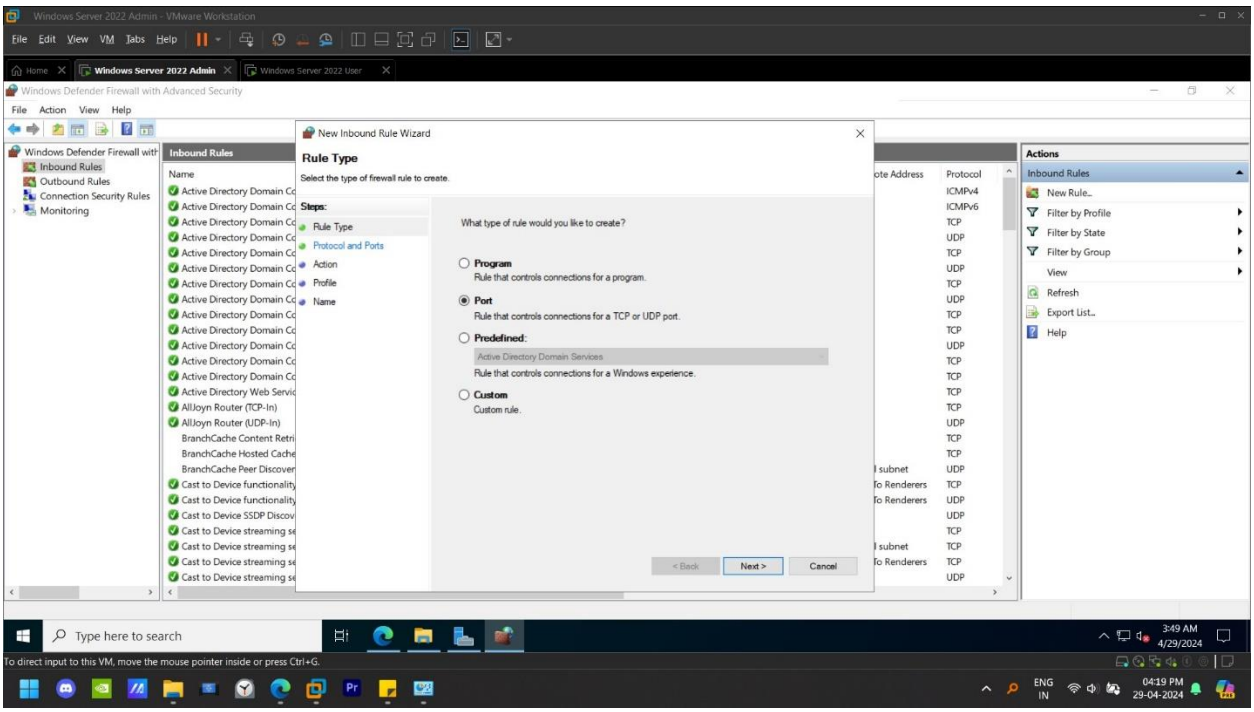


Add Port 9997 –



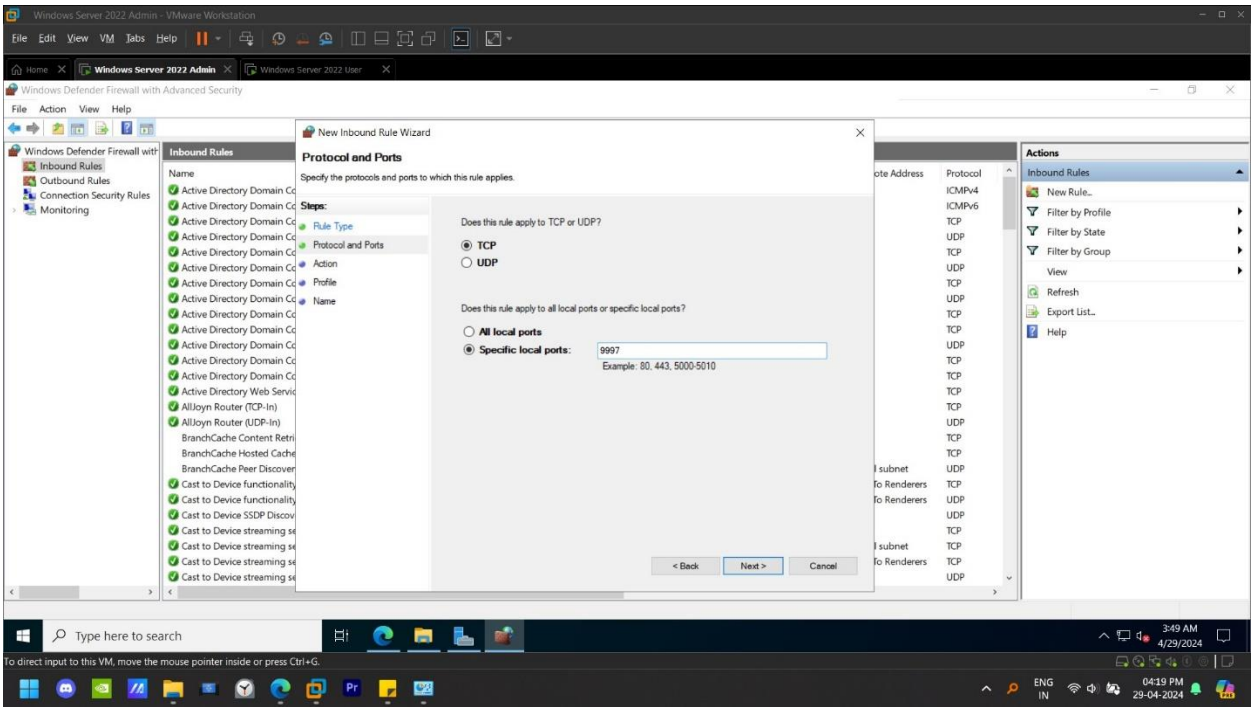


Now goto windows firewall and and create inbound and outbound rule –

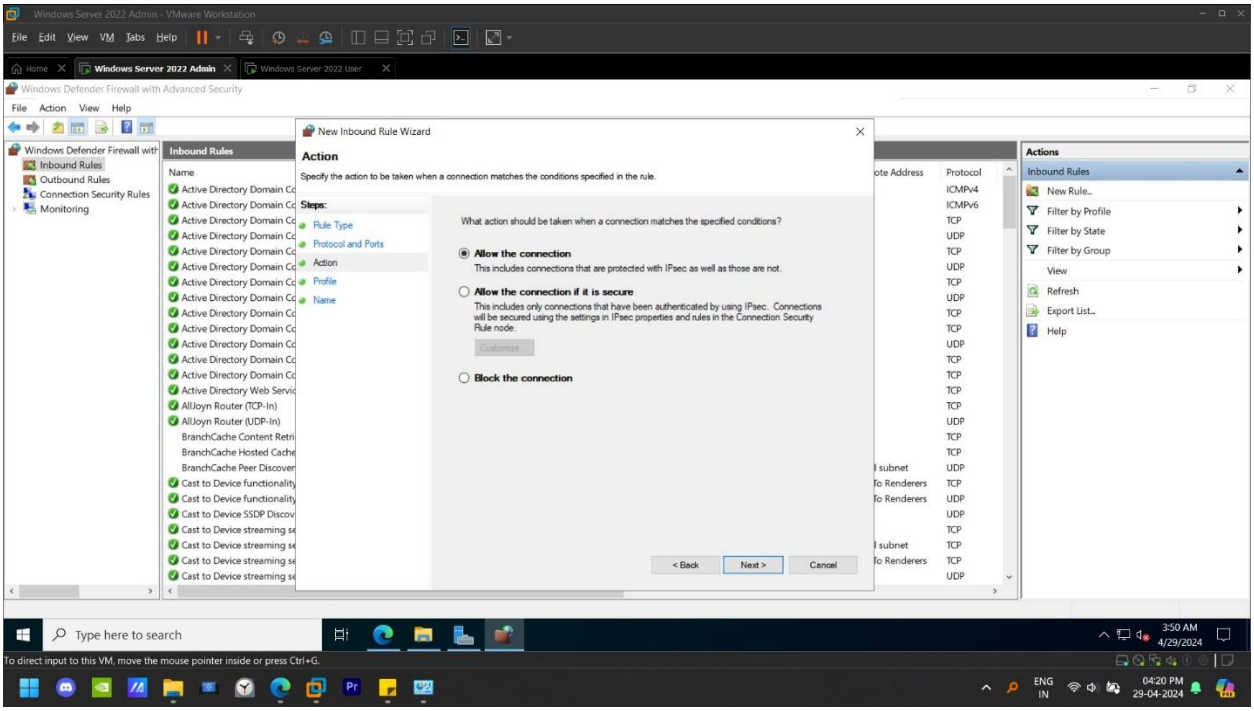


Select Port

Specify the port number 9997.

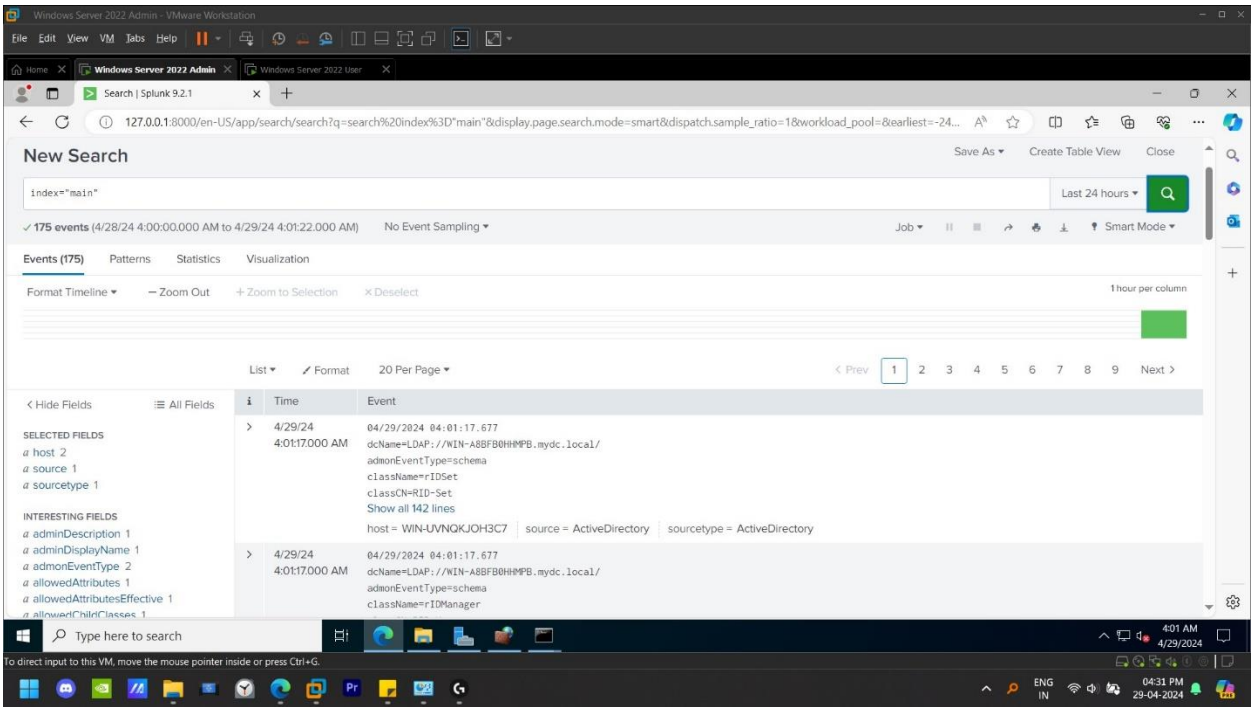


Allow the connection –



Do same for Outbound Rule in both the Admin Account and user Account.

Logs of User Account –



CHAPTER: 12 CONCLUSION

CHAPTER: 12 CONCLUSION

The implementation of Wazuh, coupled with the successful Proof of Concept (POC) and the integration of Shuffle SOAR, marks a significant advancement in our cybersecurity infrastructure. By leveraging multiple operating systems within Wazuh, we have enhanced our ability to detect and respond to a diverse range of threats effectively. Furthermore, the integration of VirusTotal enriches our threat intelligence capabilities, enabling more comprehensive analysis and informed decision-making.

This comprehensive approach not only strengthens our defensive posture but also streamlines incident response processes. The successful integration of these tools showcases our commitment to proactive cybersecurity measures and underscores our readiness to mitigate emerging threats effectively.

Moving forward, continual refinement and optimization of these integrations will be essential to ensure ongoing efficacy and adaptability in the face of evolving cyber threats. Additionally, exploring further synergies between Wazuh and other complementary security solutions could yield additional benefits, enhancing our overall resilience against cyberattacks.

Overall, the successful deployment and integration of Wazuh, coupled with the strategic utilization of additional tools and resources, position us well to navigate the dynamic landscape of cybersecurity threats confidently.

CHAPTER: 13 REFRENCES

CHAPTER: 13 REFRENCES

1. https://docs.splunk.com/Documentation/Splunk/latest/Admin/Inputsconf
2. https://documentation.wazuh.com/current/getting-started/index.html
3. https://learn.microsoft.com/en-us/windows-server/
4. https://www.youtube.com/watch?v=6ig5vTzME20&pp=ygUVc2V0dGluZyB1cCB3aW5kb3dzIGFk