CareerTiQ
CHOOSE THE BEST

PROJECT TITLE

SECURITY OPERATIONS WITH WAZUH SIEM AND XDR

TABLE OF CONTENTS

ABSTRACT

This engineering final year project focuses on the configuration and deployment of a Wazuh server, integrated with a Windows 11 agent system to monitor and analyze security threats. Wazuh, an open-source security monitoring tool, offers extensive capabilities for threat detection, integrity monitoring, incident response, and compliance management. In this project, we set up a Wazuh server and connect it to an agent system running on Windows 11. To simulate a real-world cyber threat scenario, we deliberately introduce a system infected with malware. The malicious activities are then monitored and analyzed through the Wazuh dashboard, providing comprehensive insights into the nature and behavior of the malware attack. This project demonstrates Wazuh's effectiveness in identifying and responding to security incidents, with a particular focus on detecting unauthorized processes, mitigating malware threats using VirusTotal integration, and uncovering hidden processes. By showcasing these capabilities, the project highlights Wazuh's crucial role in enhancing proactive security management and maintaining robust cybersecurity defenses.

PROJECT SCOPE

OBJECTIVES

1. Configure and Deploy Wazuh Server:

- Set up a Wazuh server to establish a centralized security monitoring and management platform.
- Ensure proper installation and configuration of the server for optimal performance and security.

2.Integrate Windows 11 Agent System:

- Connect a Windows 11 system as an agent to the Wazuh server.
- Verify successful communication and data transfer between the agent and the server.

3. Simulate Malware Attack:

- Introduce a controlled malware infection on the Windows 11 agent system.
- Ensure the malware is safely contained and does not pose a risk to other systems or networks.

4. Monitor and Analyse Threats:

- Utilize the Wazuh dashboard to monitor the agent system in real-time.
- Detect and analyse unauthorized processes, malware

activities, and hidden processes.

5. Utilize VirusTotal Integration:

- Leverage VirusTotal integration within Wazuh to enhance malware detection capabilities.
- Analyse the results and verify the detection and mitigation of malware threats.

6. Generate Comprehensive Reports:

- Create detailed reports reflecting the malware activities detected and the corresponding analysis.
- Document the process and findings to provide insights into the effectiveness of the Wazuh platform.

7. Evaluate Wazuh's Effectiveness:

- Assess the Wazuh platform's ability to detect, analyse, and respond to the simulated malware attack.
- Identify strengths and areas for improvement in using Wazuh for proactive security management.

8. Enhance Proactive Security Management:

- Demonstrate the utility of Wazuh in maintaining robust cybersecurity defenses.
- Provide recommendations for integrating Wazuh into broader security strategies for enhanced protection.

REQUIREMENTS

The successful execution of this project involves a set of hardware, software, and security requirements essential for configuring and deploying the Wazuh server, integrating the Windows 11 agent system, and simulating a malware attack. These requirements ensure the project environment is adequately prepared for seamless installation, configuration, monitoring, and analysis.

A. Hardware Requirements

1. Server Hardware:

- A physical or virtual server with sufficient CPU, RAM, and storage to host the Wazuh server.
- Recommended: At least 4 CPU cores, 8 GB of RAM, and 100 GB of storage.

2. Agent Hardware:

- A Windows 11 system with adequate resources to run the Wazuh agent and simulate malware.
- Recommended: At least 2 CPU cores, 4 GB of RAM, and 50 GB of storage.

3. Networking:

- Stable and secure network connections between the Wazuh server and the Windows 11 agent.
- Network infrastructure that supports necessary communication protocols (e.g., HTTP, HTTPS).

B. Software Requirements

1. Operating Systems:

- Wazuh Server: Compatible with various Linux distributions such as Ubuntu, CentOS, or Debian.
- Windows 11: Latest version with up-to-date security patches and updates.

2. Wazuh Software:

- Wazuh server software, including the Wazuh manager, API, and Wazuh agent software for Windows.
- Elasticsearch, Logstash, and Kibana (ELK Stack) for data storage, processing, and visualization.

3. Additional Software:

- VirtualBox or any other virtualization software for setting up the virtual environments if using virtual machines.
- Malware samples for the controlled simulation of malware attacks, ensuring they are handled securely.

C. Security Requirements

1. Secure Environment:

- Isolated network environment to safely conduct malware simulations without risking other systems.
- Use of virtual machines or sandboxed environments for testing and analysis.

2. Access Controls:

- Proper user permissions and access controls to restrict access to critical components of the Wazuh server and agent systems.
- Secure SSH access for remote management of the Wazuh

server.

3. Data Protection:

- Encryption of communication channels between the Wazuh server and agent using TLS/SSL.
- Regular backups of configuration files and collected data to prevent data loss.

4. Compliance and Legal Considerations:

- Adherence to relevant legal and compliance requirements for handling and storing security data.
- Ensure that malware samples used for simulations are legal and obtained from trusted sources.

By meeting these requirements, the project will have a robust foundation for effectively configuring the Wazuh server, integrating the Windows 11 agent system, and conducting the malware simulation. This preparation will enable comprehensive monitoring and analysis

PROBLEM STATEMENT

This project aims to configure and deploy a robust security monitoring solution using the Wazuh platform. The primary objective is to set up a Wazuh server and connect it to an agent system running Windows 11. By simulating a malware attack on the agent system, the project seeks to evaluate the effectiveness of Wazuh in detecting unauthorized processes, identifying and mitigating malware using VirusTotal integration, and uncovering hidden processes. The project will demonstrate Wazuh's

capability to provide detailed insights into the nature and behaviour of cyber threats, thereby enhancing proactive security management and fortifying cybersecurity defences.
Despite the availability of various security tools, there is a lack of cohesive platforms that integrate multiple security functions into a single, unified interface. This project addresses this gap by leveraging Wazuh's comprehensive features to offer an all-encompassing security monitoring and incident response solution. The outcomes of this project will provide valuable insights into the practical implementation and effectiveness of Wazuh in real-world scenarios, contributing to the broader field of cybersecurity.

PROJECT SOLUTIONS

This project provides a comprehensive solution for enhancing cybersecurity defenses through the configuration and deployment of a Wazuh server and the integration of a Windows 11 agent system. The solution is designed to simulate a real-world malware attack, allowing for the effective monitoring, detection, and analysis of security threats using the Wazuh platform. The key components of the solution are outlined below:

A. Wazuh Server Configuration

1. **Installation of Wazuh Server**:
    - Set up a dedicated or virtual server environment compatible with Linux distributions such as Ubuntu.
    - Install the Wazuh manager, API, and necessary

dependencies following the official Wazuh installation guide.
    - Integrate Elasticsearch, Logstash, and Kibana (ELK Stack) to facilitate data storage, processing, and visualization.
2. **Server Configuration**:
    - Configure the Wazuh manager to handle incoming data from agent systems.
    - Set up necessary security measures, including TLS/SSL for encrypted communication and access controls for secure management.
    - Ensure the server is optimized for performance, including appropriate allocation of system resources.

B. Windows 11 Agent Integration

1. **Agent Installation**:
    - Install the Wazuh agent software on the Windows 11 system.
    - Configure the agent to communicate with the Wazuh server, ensuring proper connection and data transfer.
2. **Agent Configuration**:
    - Set up monitoring configurations on the agent system to collect relevant log data, including system events, file integrity monitoring, and security alerts.
    - Ensure the agent is configured to detect unauthorized processes, malware activities, and hidden processes.

C. Malware Attack Simulation

1. **Controlled Malware Introduction**:
    - Introduce a controlled malware sample into the Windows 11 agent system to simulate a real-world cyber-attack.

- Ensure the malware is contained within a secure, isolated environment to prevent any unintended spread or damage.

2. **Monitoring and Analysis**:
   - Use the Wazuh dashboard to monitor the Windows 11 agent system in real-time.
   - Detect and analyse the activities of the malware, focusing on unauthorized processes, malware detection through VirusTotal integration, and hidden processes.
3. **VirusTotal Integration**:
   - Leverage Wazuh's integration with VirusTotal to enhance malware detection capabilities.
   - Analyse the results from VirusTotal to verify the identification and classification of the malware sample.

D. Data Collection and Reporting

1. **Log Collection**:
   - Collect logs generated by the Windows 11 agent system during the malware simulation.
   - Store and manage the logs on the Wazuh server for further analysis.
2. **Report Generation**:
   - Use the Wazuh dashboard and ELK Stack to create detailed reports reflecting the detected malware activities and corresponding analysis.
   - Document the entire process, findings, and results to provide insights into the effectiveness of the Wazuh platform.

E. Evaluation and Recommendations

1. **Effectiveness Assessment**:

- Evaluate the performance and effectiveness of the Wazuh platform in detecting, analysing, and responding to the simulated malware attack.
- Identify any strengths and areas for improvement in the setup and configuration.

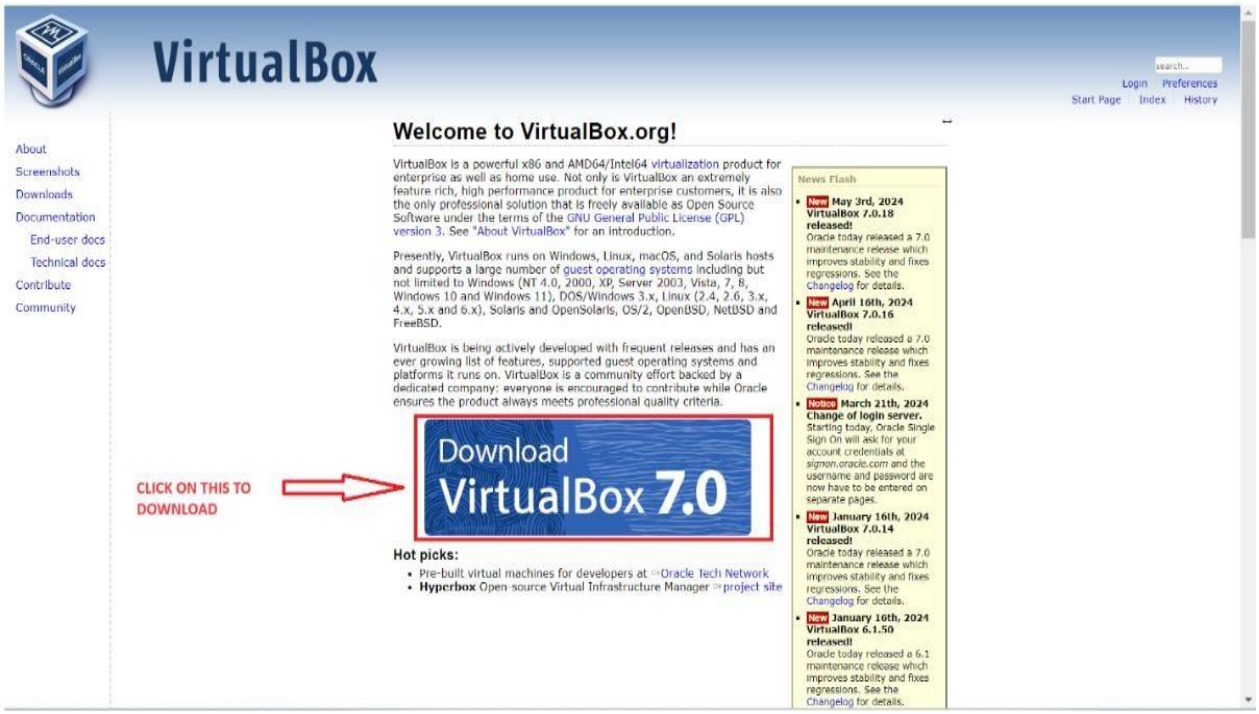
2. **Recommendations**:
   - Provide recommendations for enhancing the implementation of Wazuh in real-world security environments.
   - Suggest best practices for integrating Wazuh into broader cybersecurity strategies to improve proactive security management.

SETUP AND CONFIGURATION

VIRTUAL MACHINE INSTALLATION

STEP 1:

Go to the Virtual Box Official Website: https://www.virtualbox.org/ (Or can also use the VMWare Workstation) and download it



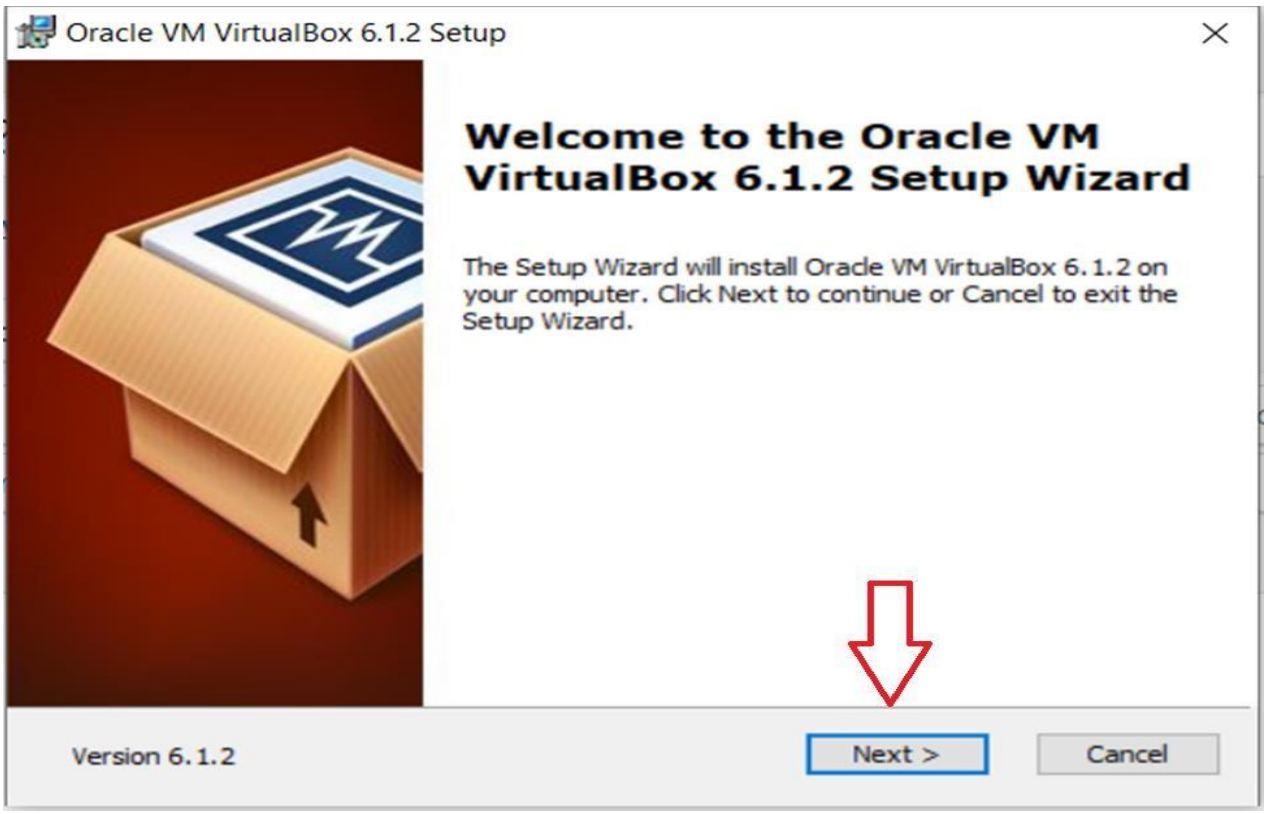
STEP 2:

Select VirtualBox as per your Operating System.


https://www.virtualbox.org/wiki/Downloads
VirtualBox
search...
Login
Preferences
Start page
Index
History
About
Screenshots
Downloads
Documentation
End-user docs
Technical docs
Contribute
Community
Download VirtualBox
Here you will find links to VirtualBox binaries and its source code.
VirtualBox binaries
By downloading, you agree to the terms and conditions of the respective license.
VirtualBox 7.0.20 platform packages
Windows hosts
macOS / Intel hosts
Linux distributions
Solaris hosts
Solaris 11 IPS hosts
The binaries are released under the terms of the GPL version 3.
See the changelog for what has changed.
You might want to compare the checksums to verify the integrity of downloaded packages. The SHA256 checksums should be favored as the MD5 algorithm must be treated as insecure!

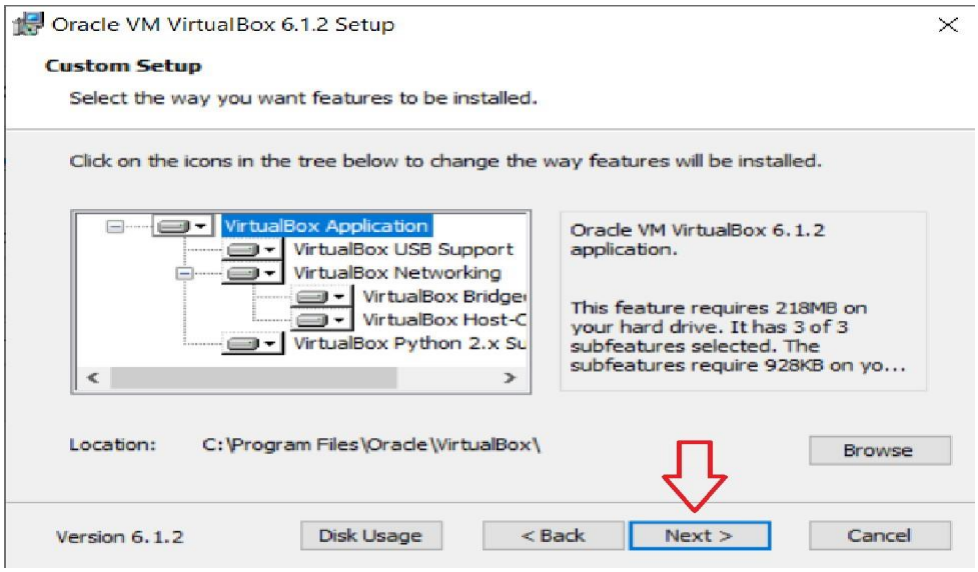
STEP 3:

Install the VirtualBox



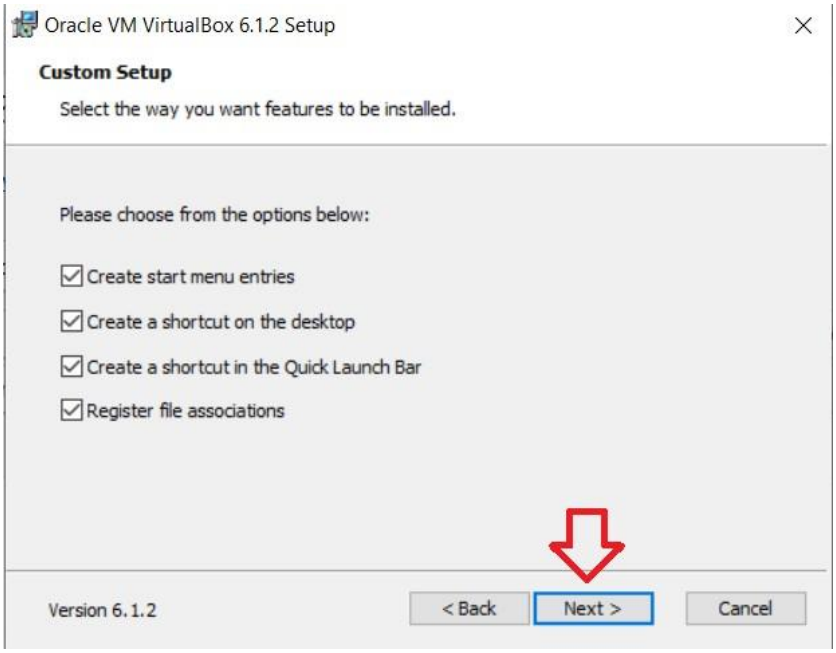
STEP 4:

Select Installation Location


Oracle VM VirtualBox 6.1.2 Setup
Custom Setup
Select the way you want features to be installed.
Click on the icons in the tree below to change the way features will be installed.
VirtualBox Application
VirtualBox USB Support
VirtualBox Networking
VirtualBox Bridge
VirtualBox Host-C
VirtualBox Python 2.x Su
Oracle VM VirtualBox 6.1.2 application.
This feature requires 218MB on your hard drive. It has 3 of 3 subfeatures selected. The subfeatures require 928KB on yo...
Location:
C:\Program Files\Oracle\VirtualBox\
Browse
Version 6.1.2
Disk Usage
< Back
Next >
Cancel

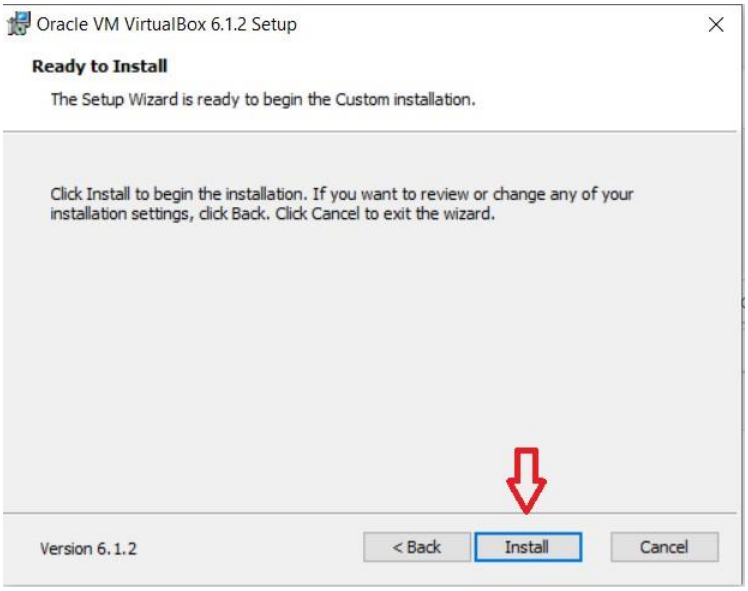
STEP 5:

Creating Entries and Shortcuts



STEP 6:

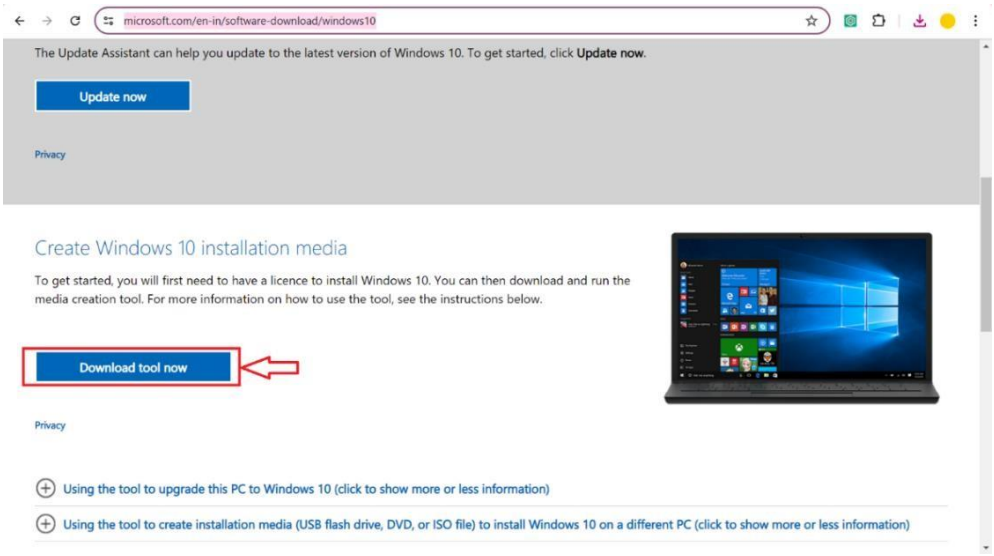
Ready To Install


Oracle VM VirtualBox 6.1.2 Setup
Ready to Install
The Setup Wizard is ready to begin the Custom installation.
Click Install to begin the installation. If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.
Version 6.1.2
< Back
Install
Cancel

WINDOWS10 IN VIRTUAL MACHINE INSTALLATION

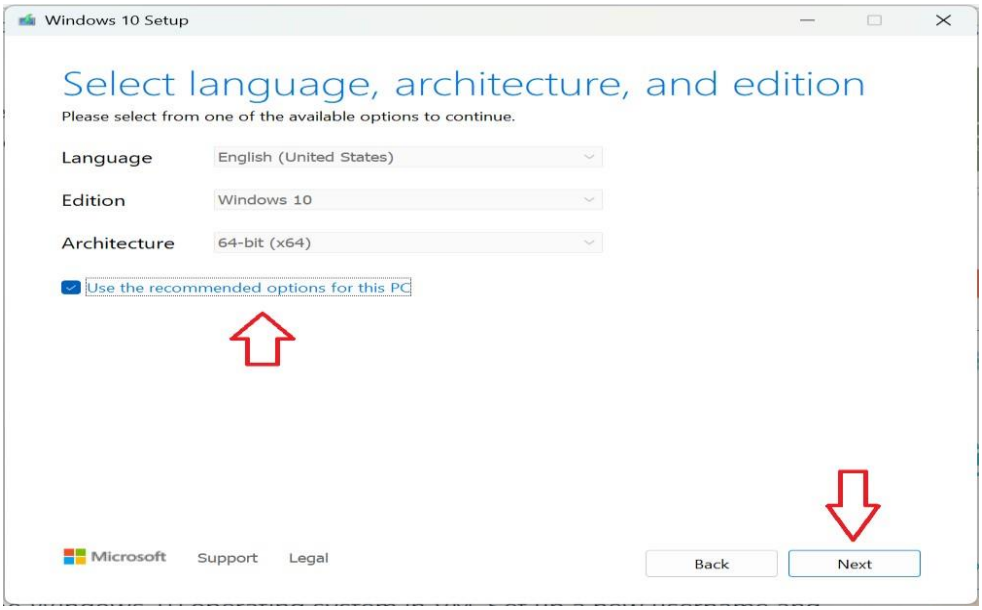
STEP 1:

Go to the windows: https://www.microsoft.com/en-in/software-download/windows10 and download the tool



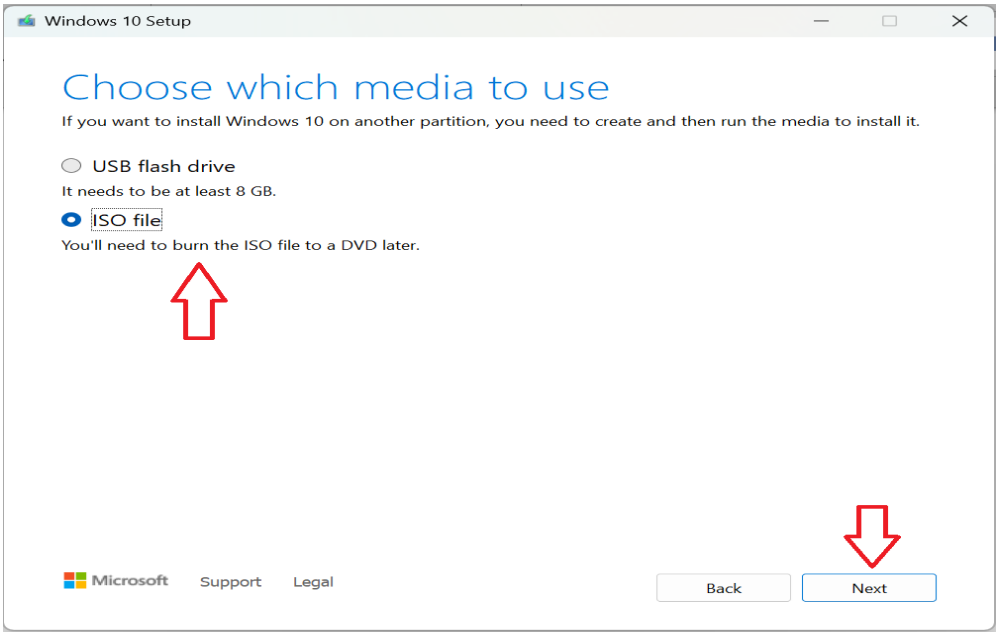
STEP 2:

Select the option shown bellow


Windows 10 Setup
Select language, architecture, and edition
Please select from one of the available options to continue.
Language
English (United States)
Edition
Windows 10
Architecture
64-bit (x64)
Use the recommended options for this PC
Microsoft
Support
Legal
Back
Next

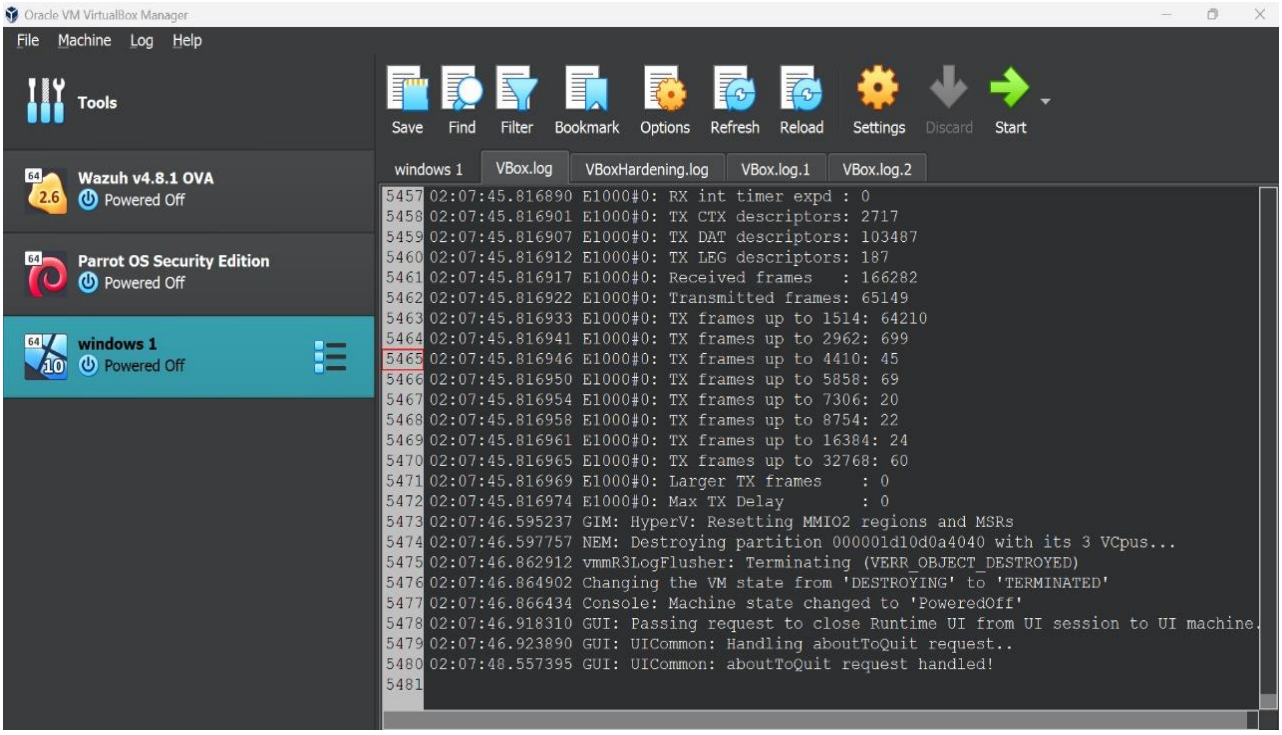
STEP 3:

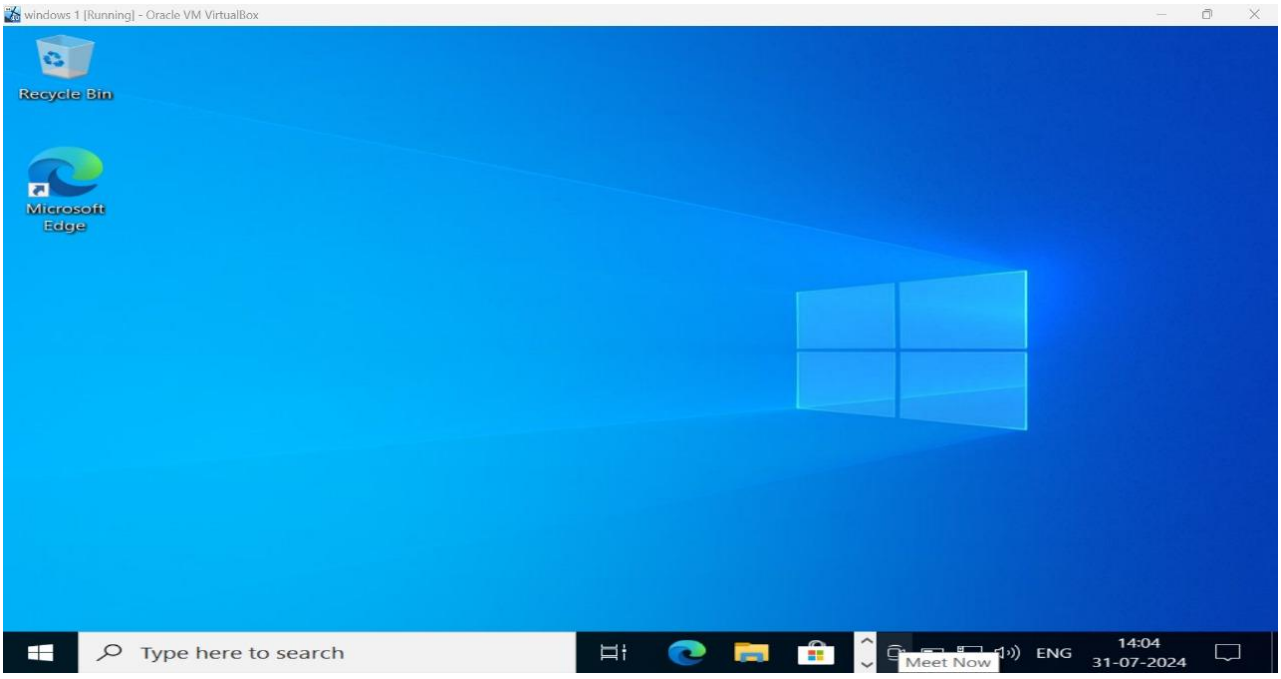
Select the iso file



STEP 4:

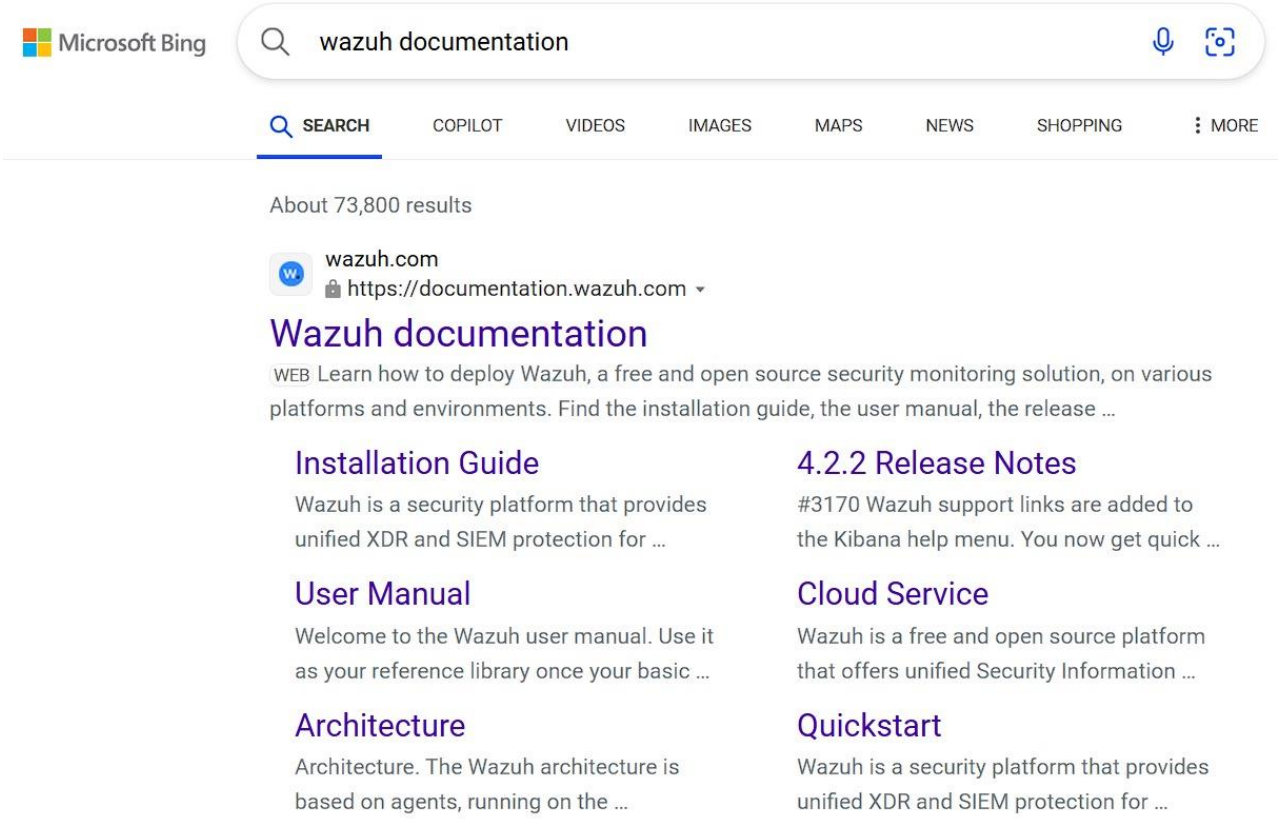
Select on file destination and click next to download the file


Oracle VM VirtualBox Manager
File Machine Log Help
Tools
Wazuh v4.8.1 OVA
Powered Off
Parrot OS Security Edition
Powered Off
windows 1
Powered Off
Save Find Filter Bookmark Options Refresh Reload Settings Discard Start
windows 1 VBox.log VBoxHardening.log VBox.log.1 VBox.log.2
5457 02:07:45.816890 E1000#0: RX int timer expd : 0
5458 02:07:45.816901 E1000#0: TX CTX descriptors: 2717
5459 02:07:45.816907 E1000#0: TX DAT descriptors: 103487
5460 02:07:45.816912 E1000#0: TX LEG descriptors: 187
5461 02:07:45.816917 E1000#0: Received frames : 166282
5462 02:07:45.816922 E1000#0: Transmitted frames: 65149
5463 02:07:45.816933 E1000#0: TX frames up to 1514: 64210
5464 02:07:45.816941 E1000#0: TX frames up to 2962: 699
5465 02:07:45.816946 E1000#0: TX frames up to 4410: 45
5466 02:07:45.816950 E1000#0: TX frames up to 5858: 69
5467 02:07:45.816954 E1000#0: TX frames up to 7306: 20
5468 02:07:45.816958 E1000#0: TX frames up to 8754: 22
5469 02:07:45.816961 E1000#0: TX frames up to 16384: 24
5470 02:07:45.816965 E1000#0: TX frames up to 32768: 60
5471 02:07:45.816969 E1000#0: Larger TX frames : 0
5472 02:07:45.816974 E1000#0: Max TX Delay : 0
5473 02:07:46.595237 GIM: HyperV: Resetting MMIO2 regions and MSRs
5474 02:07:46.597757 NEM: Destroying partition 00001d10d0a4040 with its 3 VCpus...
5475 02:07:46.862912 vmmR3LogFlusher: Terminating (VERR_OBJECT_DESTROYED)
5476 02:07:46.864902 Changing the VM state from 'DESTROYING' to 'TERMINATED'
5477 02:07:46.866434 Console: Machine state changed to 'PoweredOff'
5478 02:07:46.918310 GUI: Passing request to close Runtime UI from UI session to UI machine.
5479 02:07:46.923890 GUI: UICommon: Handling aboutToQuit request..
5480 02:07:48.557395 GUI: UICommon: aboutToQuit request handled!
5481

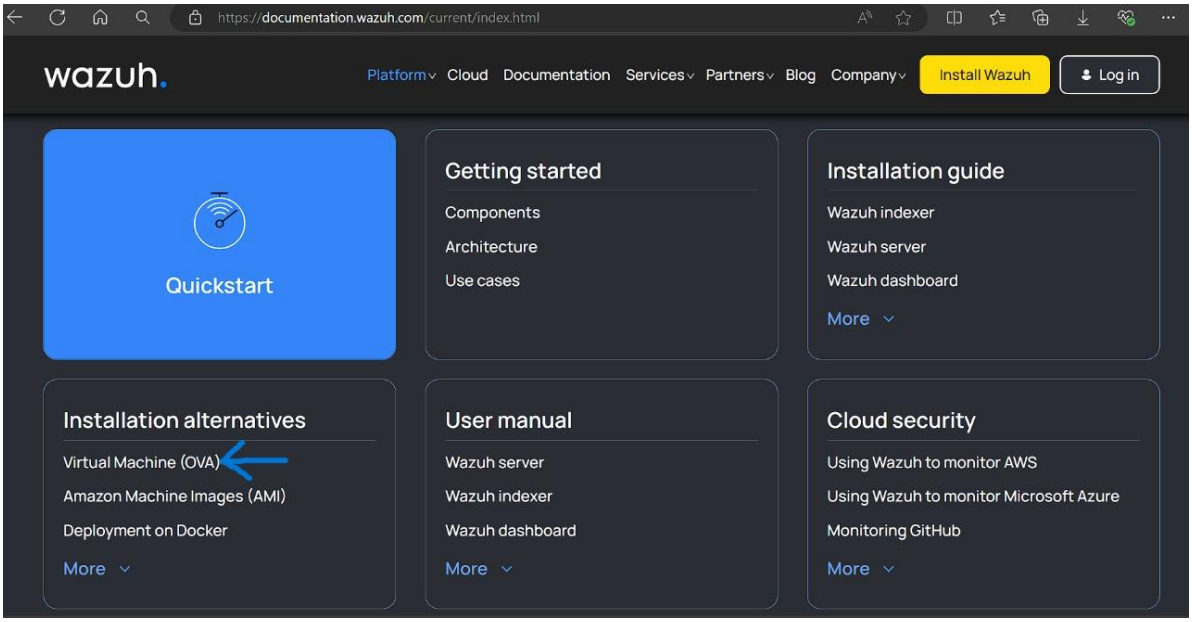

windows 1 [Running] - Oracle VM VirtualBox
Recycle Bin
Microsoft Edge
Type here to search
Meet Now
ENG
14:04
31-07-2024

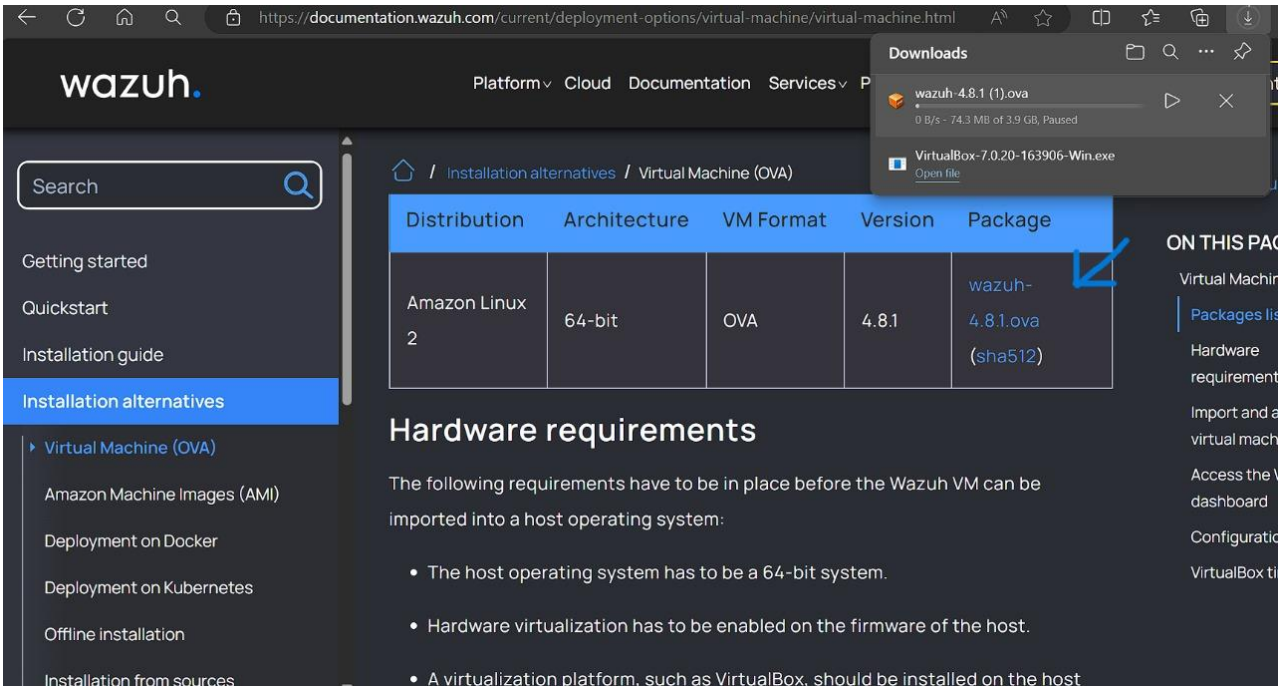
WAZUH INSTALLATION AND CONFIGURATION

STEP 1: Navigate to the official website of wazuh and and click on alternative installation ovi file of wazuh VM. Which acts as the wazuh server which comes will pre-installed requirements.

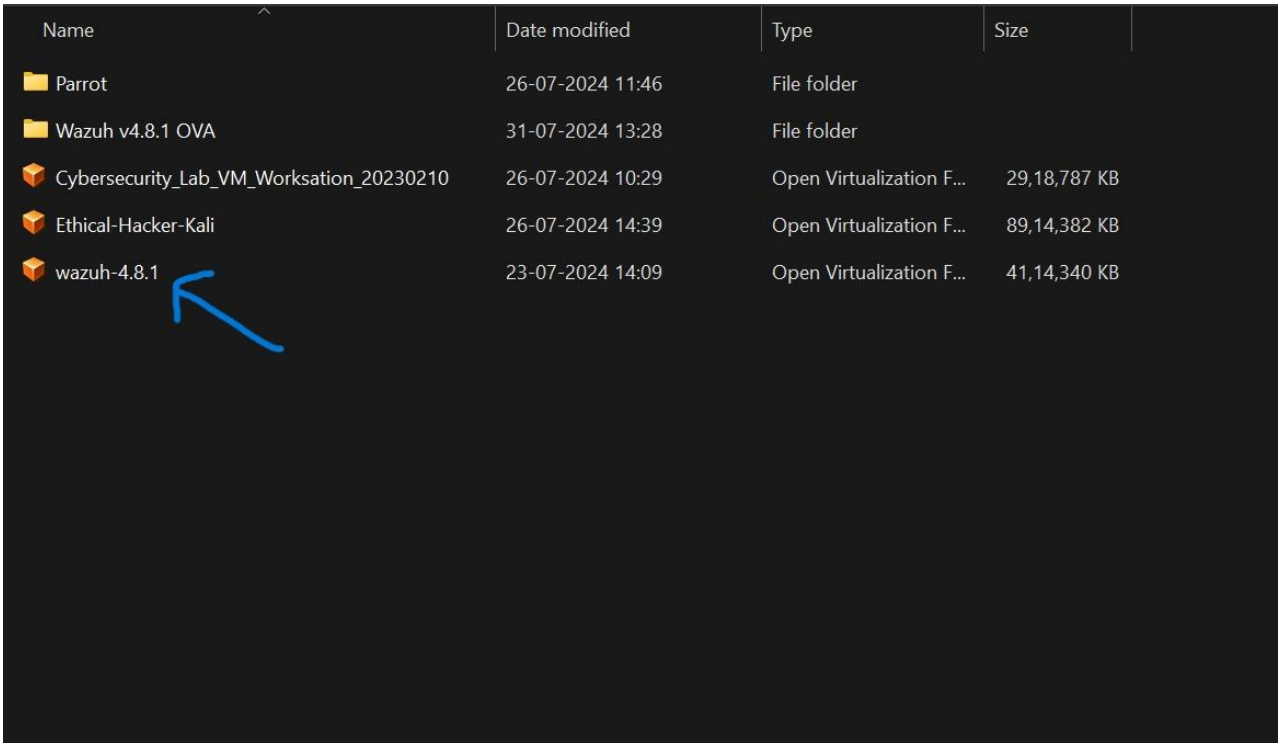


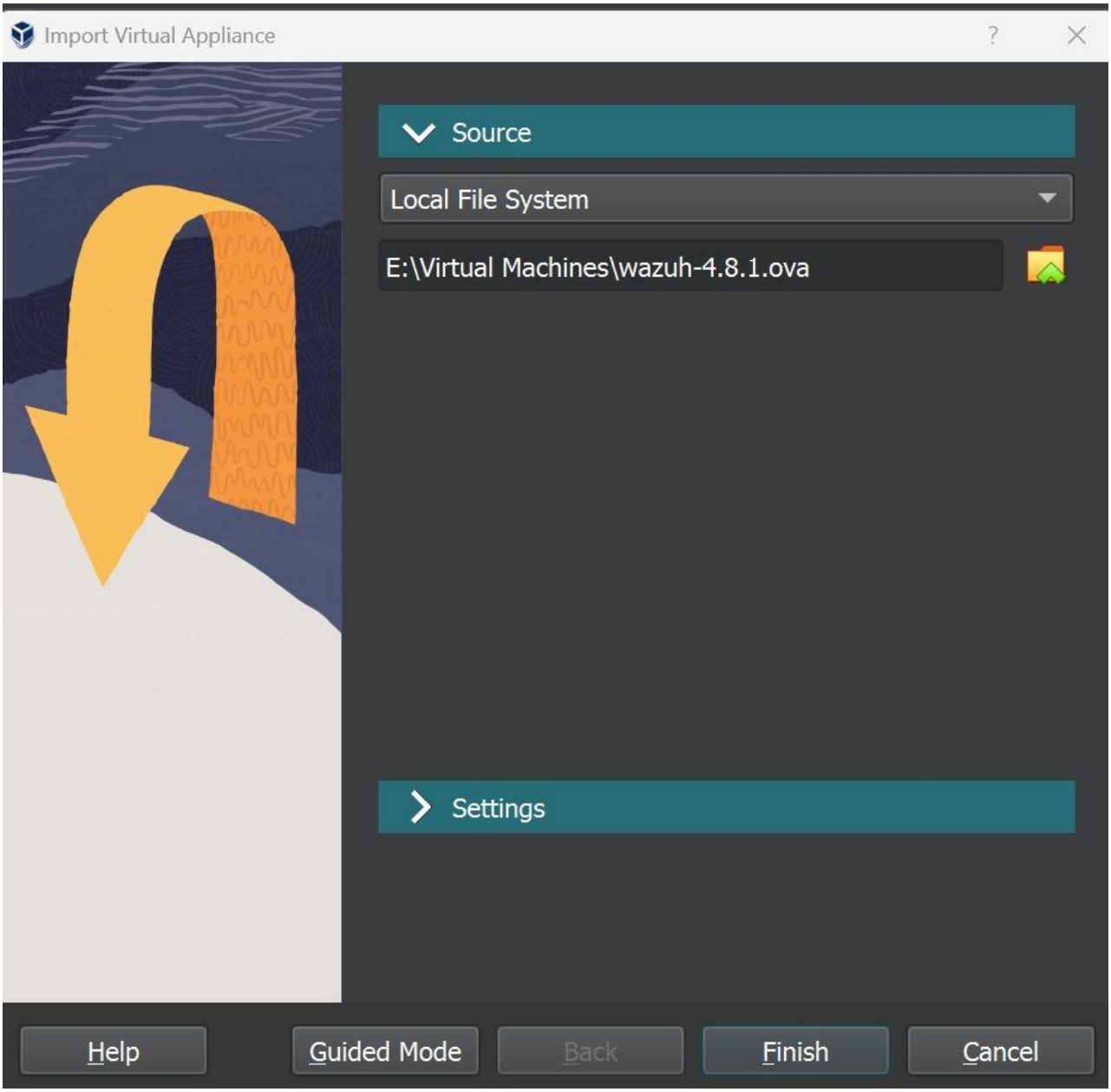
STEP 2: Go to virtual machine OVA and click on the file called Wazuh 4.8.1



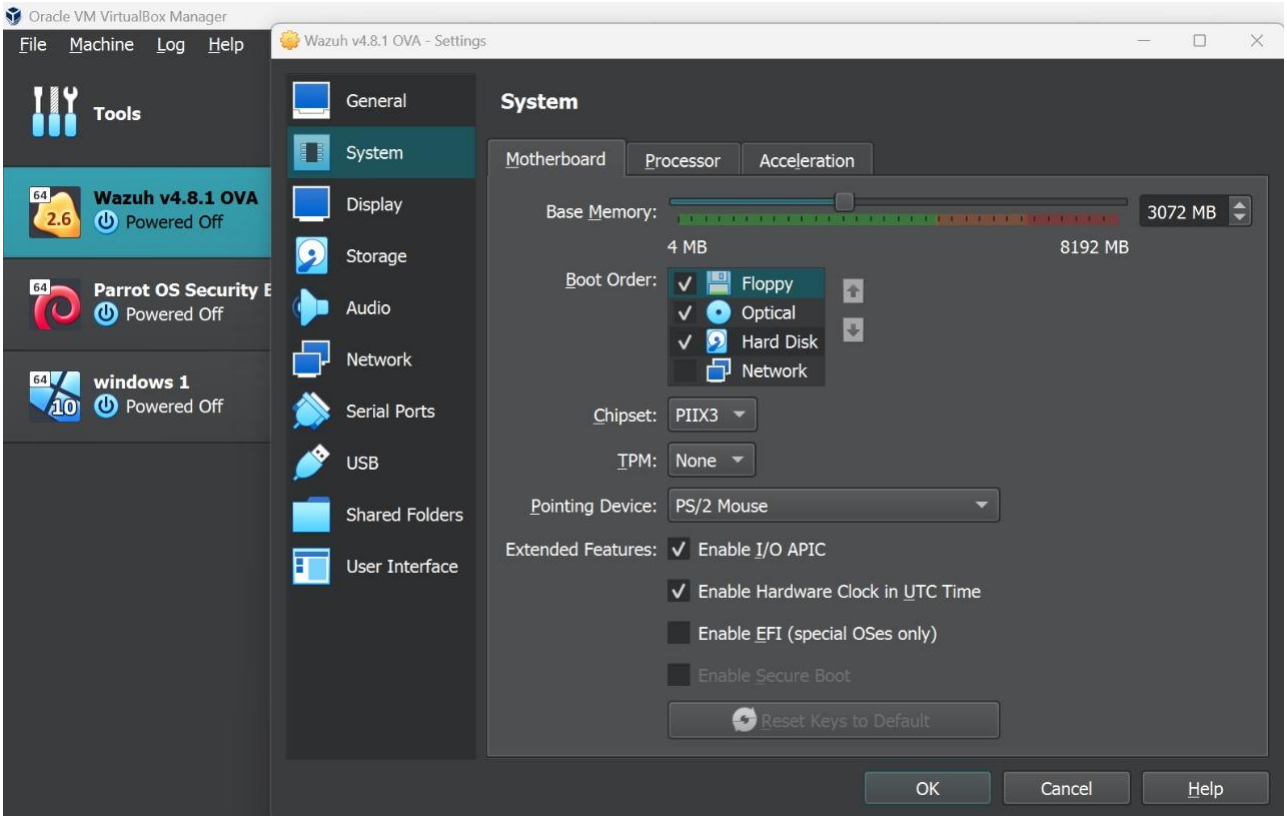


STEP 3: Click on the downloaded file it will get opened in virtual machine and some settings should be configured to make sure the server runs continuously without getting frozen.

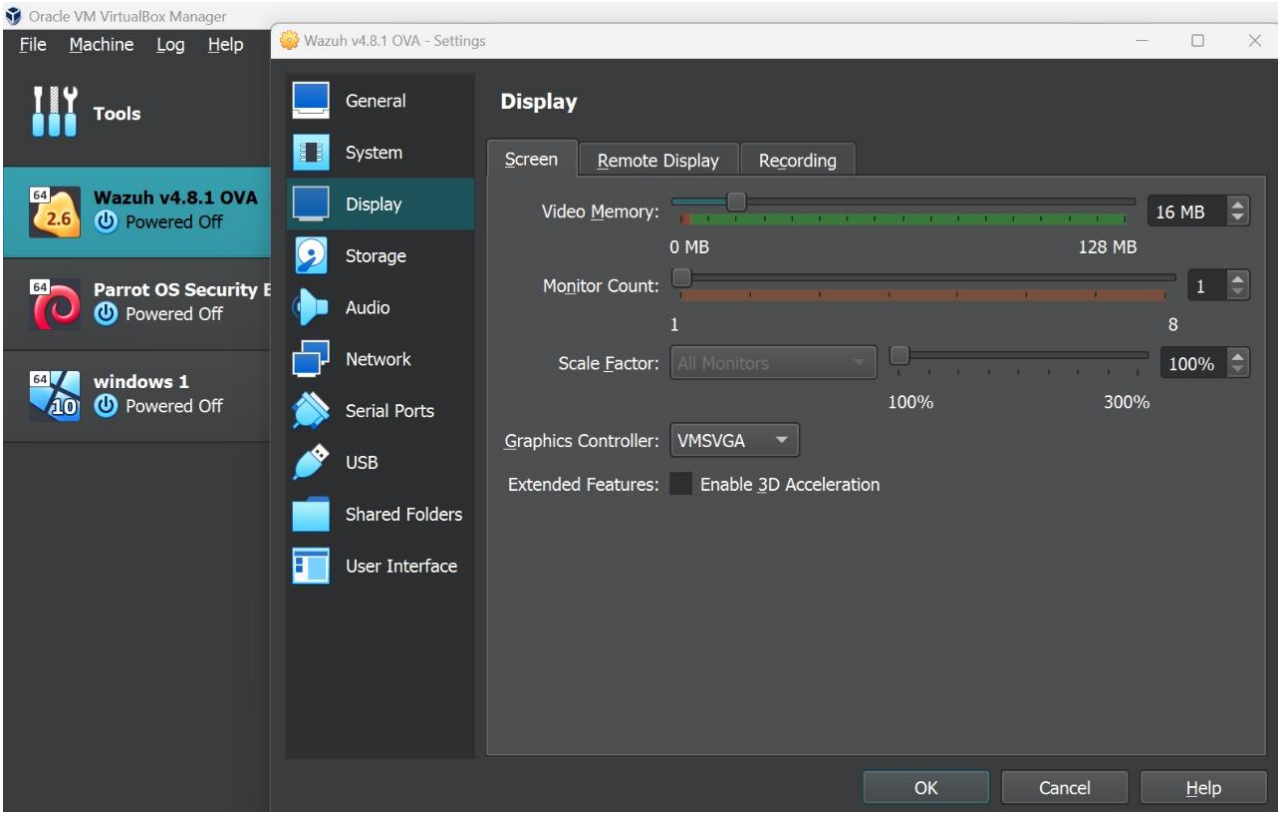

Name
Date modified
Type
Size
Parrot
26-07-2024 11:46
File folder
Wazuh v4.8.1 OVA
31-07-2024 13:28
File folder
Cybersecurity_Lab_VM_Worksation_20230210
26-07-2024 10:29
Open Virtualization F...
29,18,787 KB
Ethical-Hacker-Kali
26-07-2024 14:39
Open Virtualization F...
89,14,382 KB
wazuh-4.8.1
23-07-2024 14:09
Open Virtualization F...
41,14,340 KB



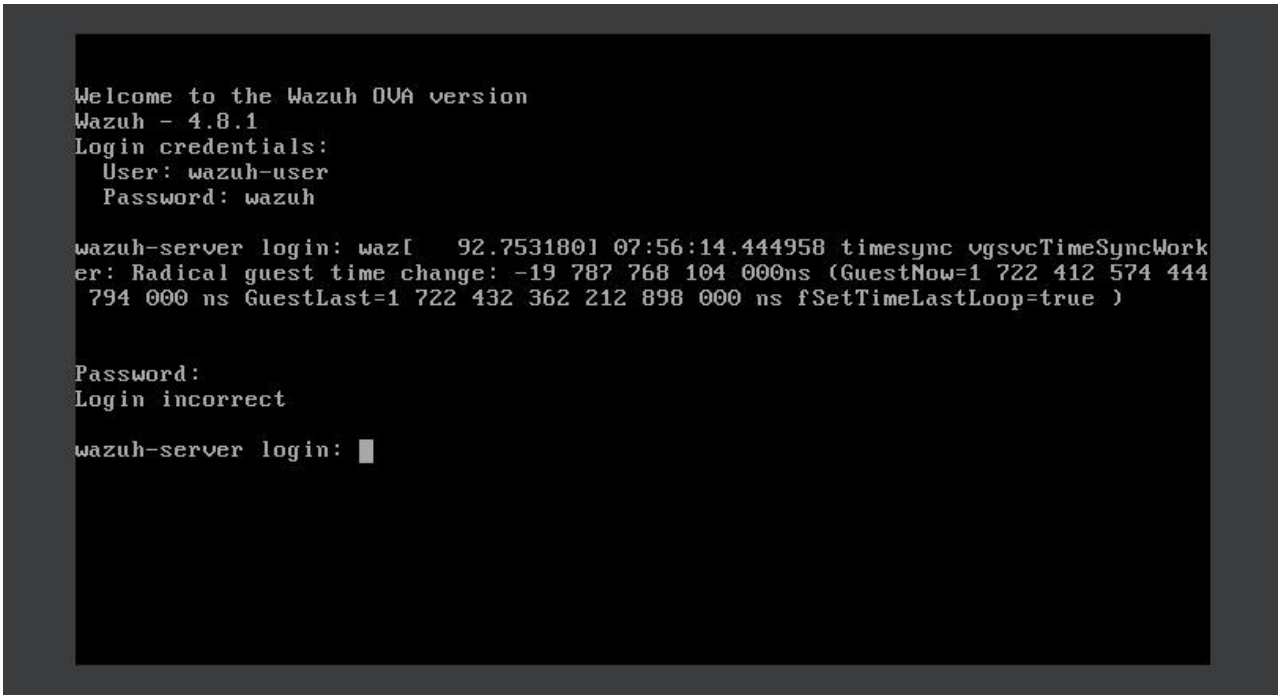
STEP 4: Make necessary configuration. First click on wazuh vm settings and go to system and check the " ENABLE HARDWARE CLOCK IN UTC TIME " is checked.



STEP 5: Also make sure the graphics setting is configured correctly. Go to display settings and change the graphic controller to " VMSVGA ".



STEP 6: Boot the Wazuh VM and wait for it to load the files until it throws the login page. Enter the default credentials and login as root by giving the username as root and password as wazuh.


Welcome to the Wazuh OVA version
Wazuh - 4.8.1
Login credentials:
User: wazuh-user
Password: wazuh
wazuh-server login: waz[92.753180] 07:56:14.444958 timesync vgsvcTimeSyncWork
er: Radical guest time change: -19 787 768 104 000ns (GuestNow=1 722 412 574 444
794 000 ns GuestLast=1 722 432 362 212 898 000 ns fSetTimeLastLoop=true)
Password:
Login incorrect
wazuh-server login:


WAZUH Open Source Security Platform
https://wazuh.com
[wazuh-user@wazuh-server ~]$

STEP 7: It is important to set a static IP address to any server. If you use DHCP your server could receive a different IP address and your hosts would not be able to communicate with it. This is especially true with the Wazuh server because the configuration and agents are dependent on the IP address to send logs.

You can set the static IP address with a few simple commands. While it is best practice to set it before configuring Wazuh, it can still done after Wazuh is configured as long as the VM still has the same IP address that it had when you configured it.

You do not have to change the IP address from the original IP address assigned to it. The first thing you need to do is confirm the IP address and the netmask.

You can discover the default gateway by using the command below.

ip r

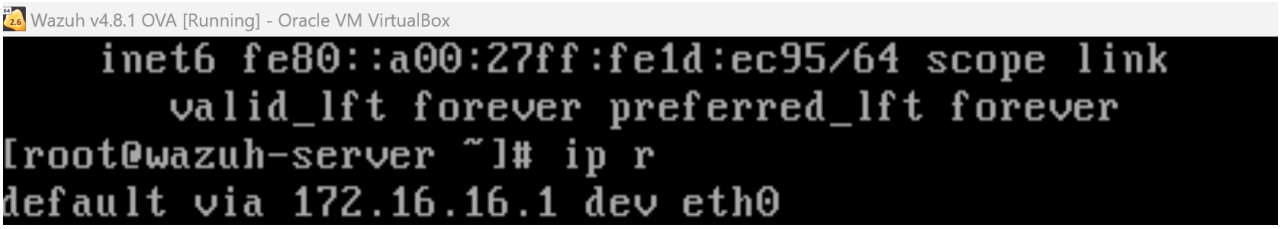
You can make that IP address static by using the following command:

sudo ifconfig eth0 192.168.137.20 netmask 255.255.255.0

Set the default gateway using the following command:

sudo route add default gw 192.168.137.1 eth0

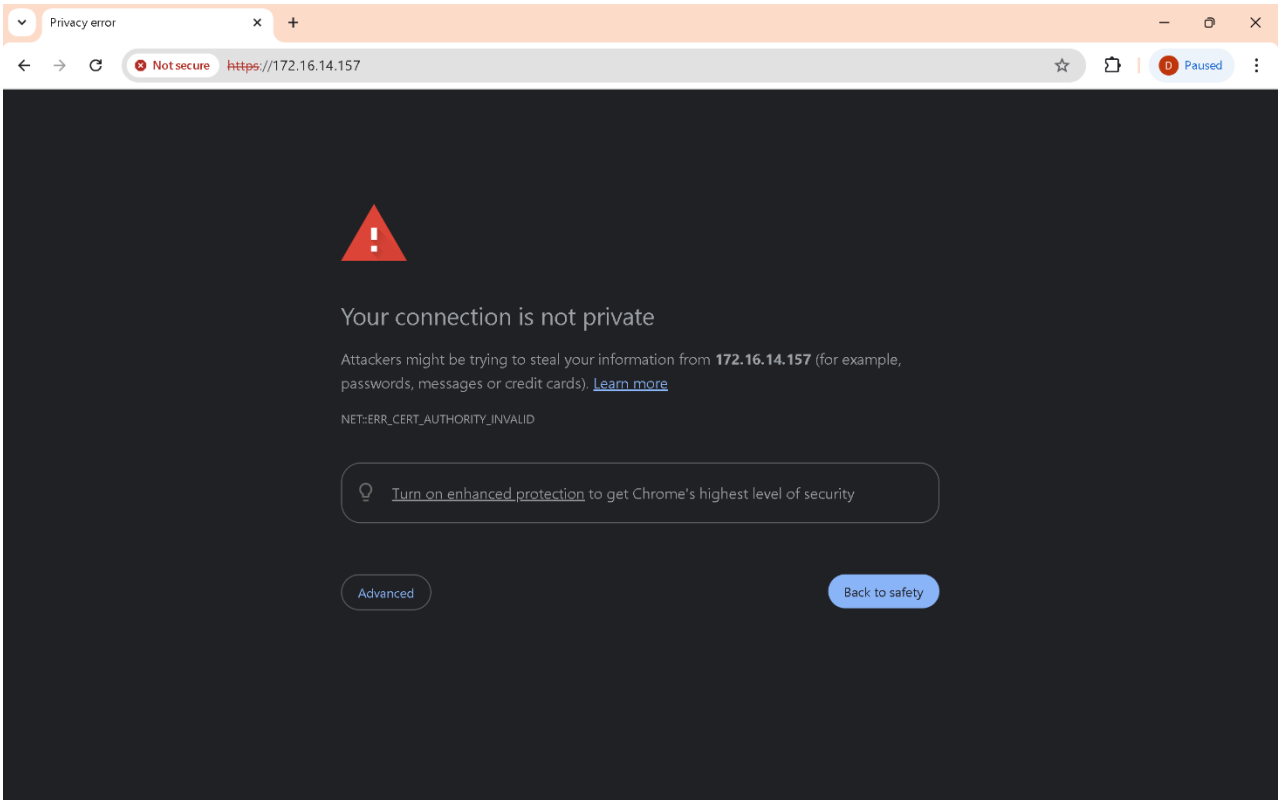
Thus set the static IP to the server and the default gateway.

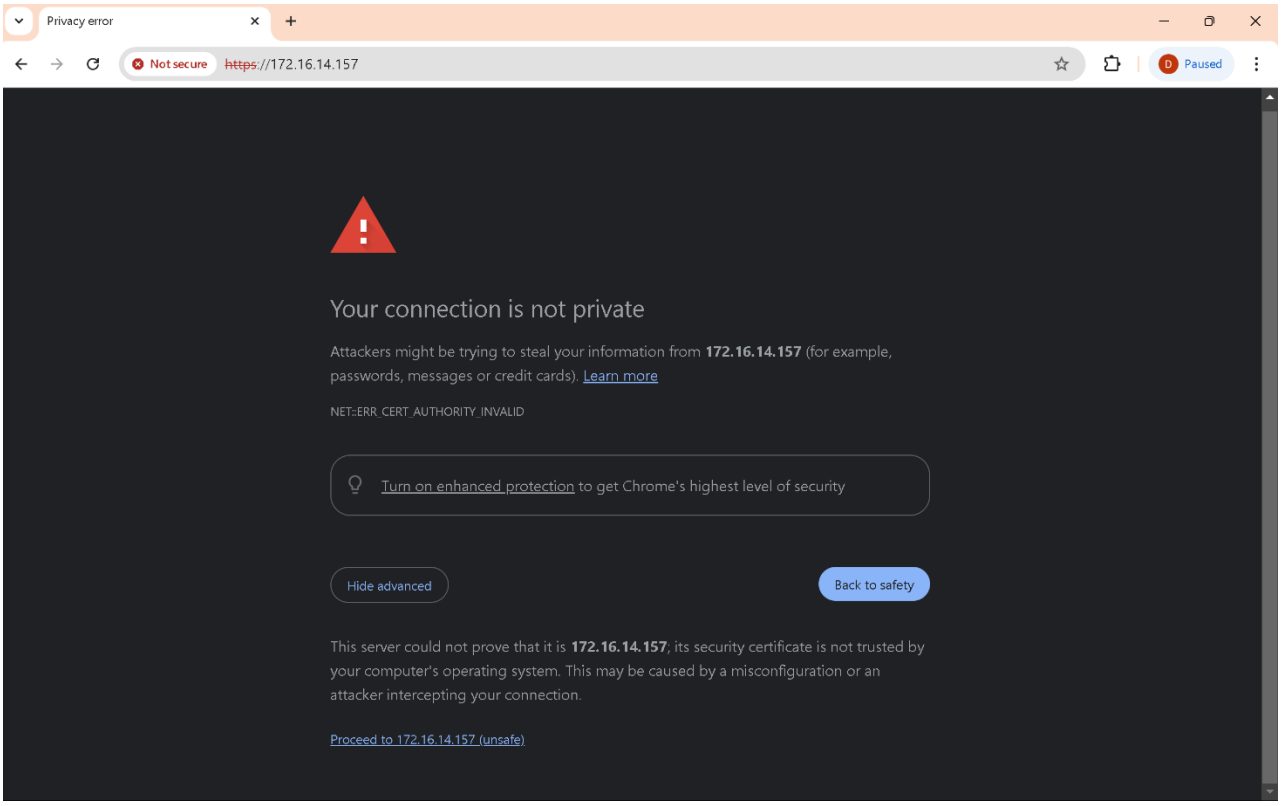


ACCESSING THE WAZUH DASHBOARD

STEP 1: Go to a web browser (chrome is recommended) and enter the IP Address of the wazuh server to access the dashboard

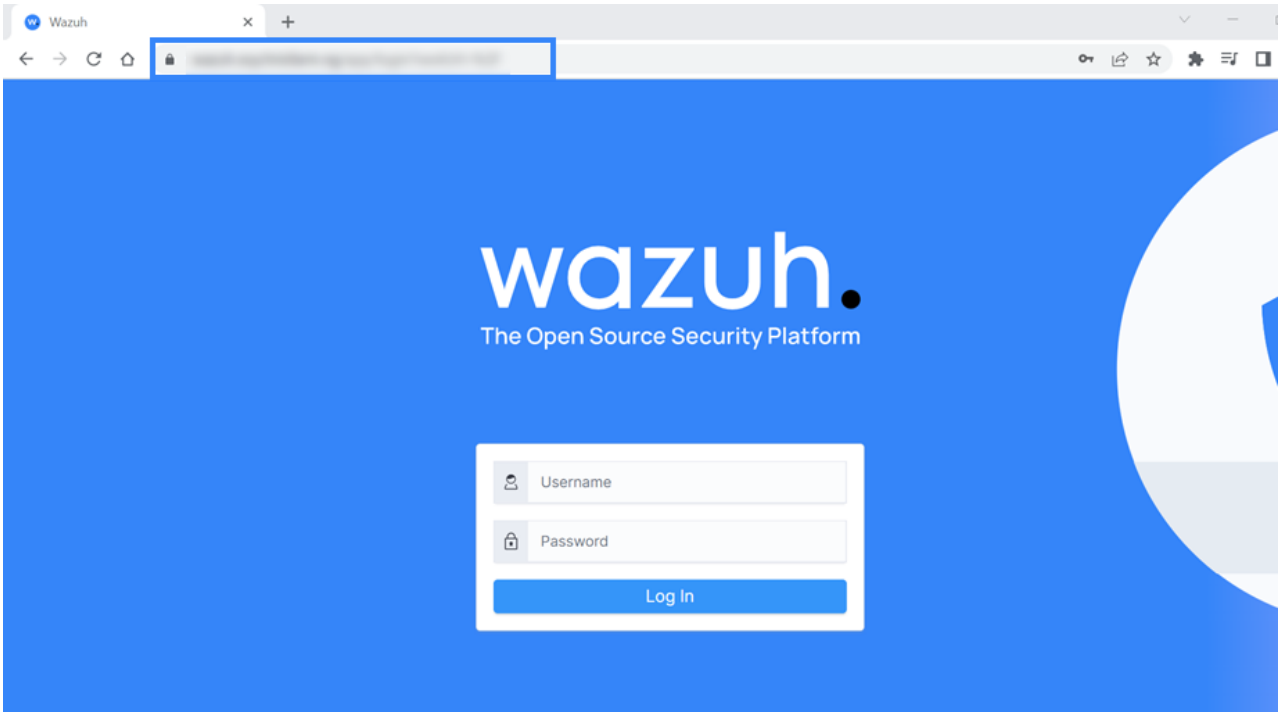
It will throw a warning and this can be ignored and go to the advanced settings and click on proceed to the IP Address.

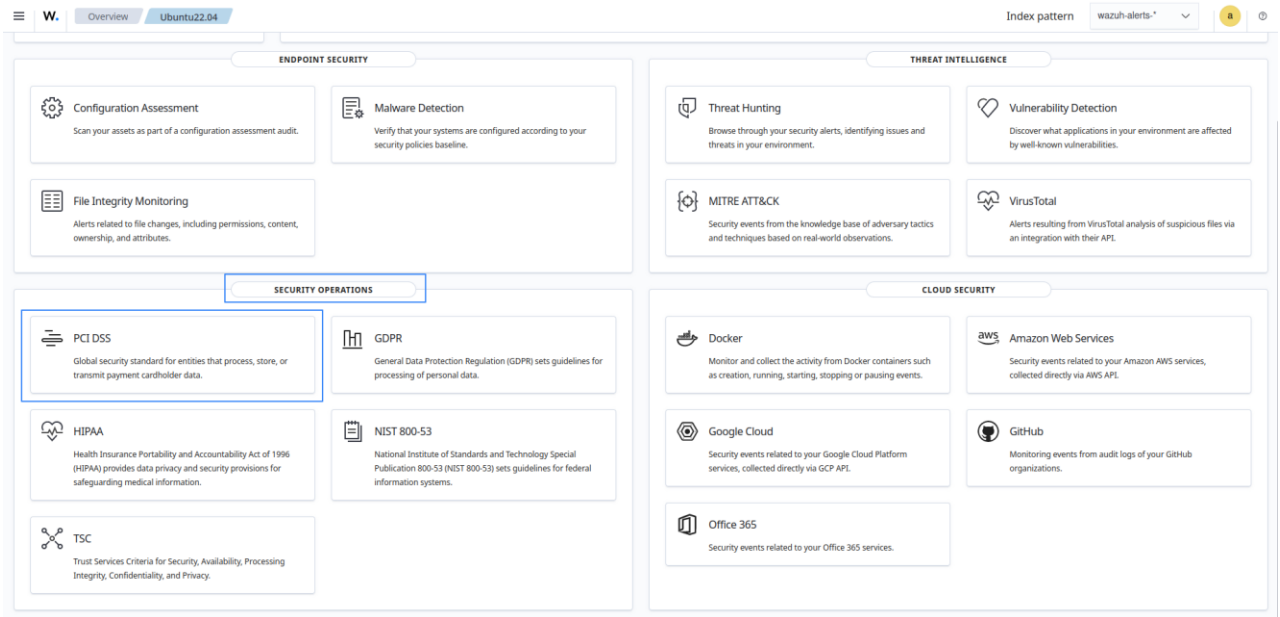

Privacy error
Not secure
https://172.16.14.157
Paused
Your connection is not private
Attackers might be trying to steal your information from 172.16.14.157 (for example, passwords, messages or credit cards). Learn more
NET::ERR_CERT_AUTHORITY_INVALID
Turn on enhanced protection to get Chrome's highest level of security
Advanced
Back to safety


Privacy error
Not secure
https://172.16.14.157
Paused
Your connection is not private
Attackers might be trying to steal your information from 172.16.14.157 (for example, passwords, messages or credit cards). Learn more
NET::ERR_CERT_AUTHORITY_INVALID
Turn on enhanced protection to get Chrome's highest level of security
Hide advanced
Back to safety
This server could not prove that it is 172.16.14.157; its security certificate is not trusted by your computer's operating system. This may be caused by a misconfiguration or an attacker intercepting your connection.
Proceed to 172.16.14.157 (unsafe)

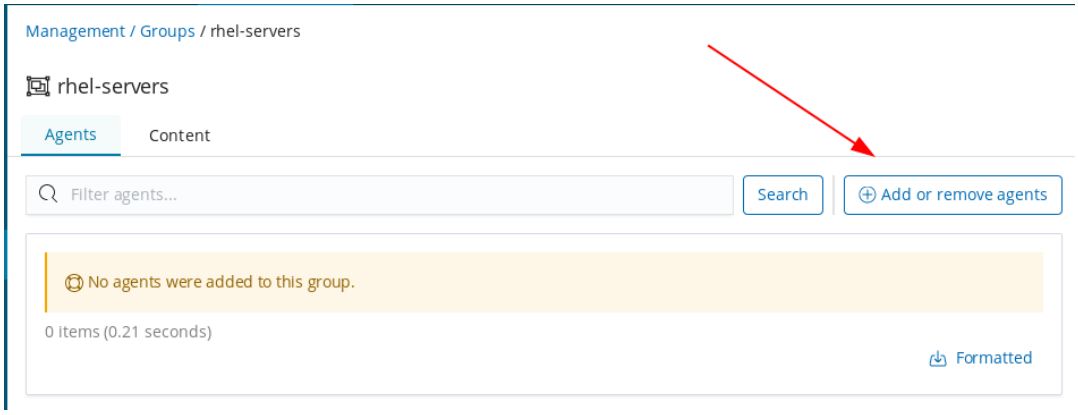
Now after this the wazuh login page will show up. Enter the default credentials where the username is admin and the password is also admin.

And the dashboard will appear.

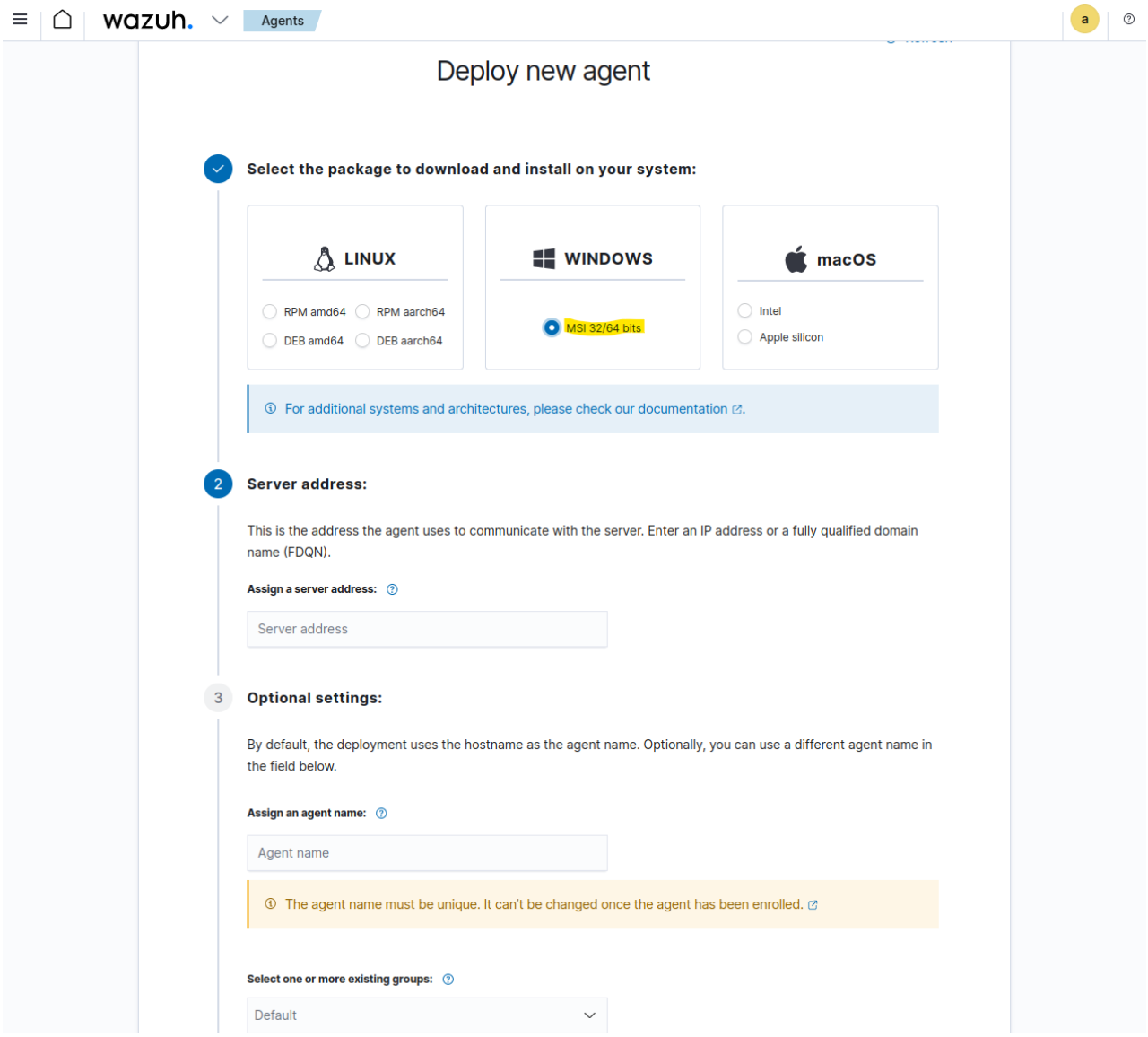


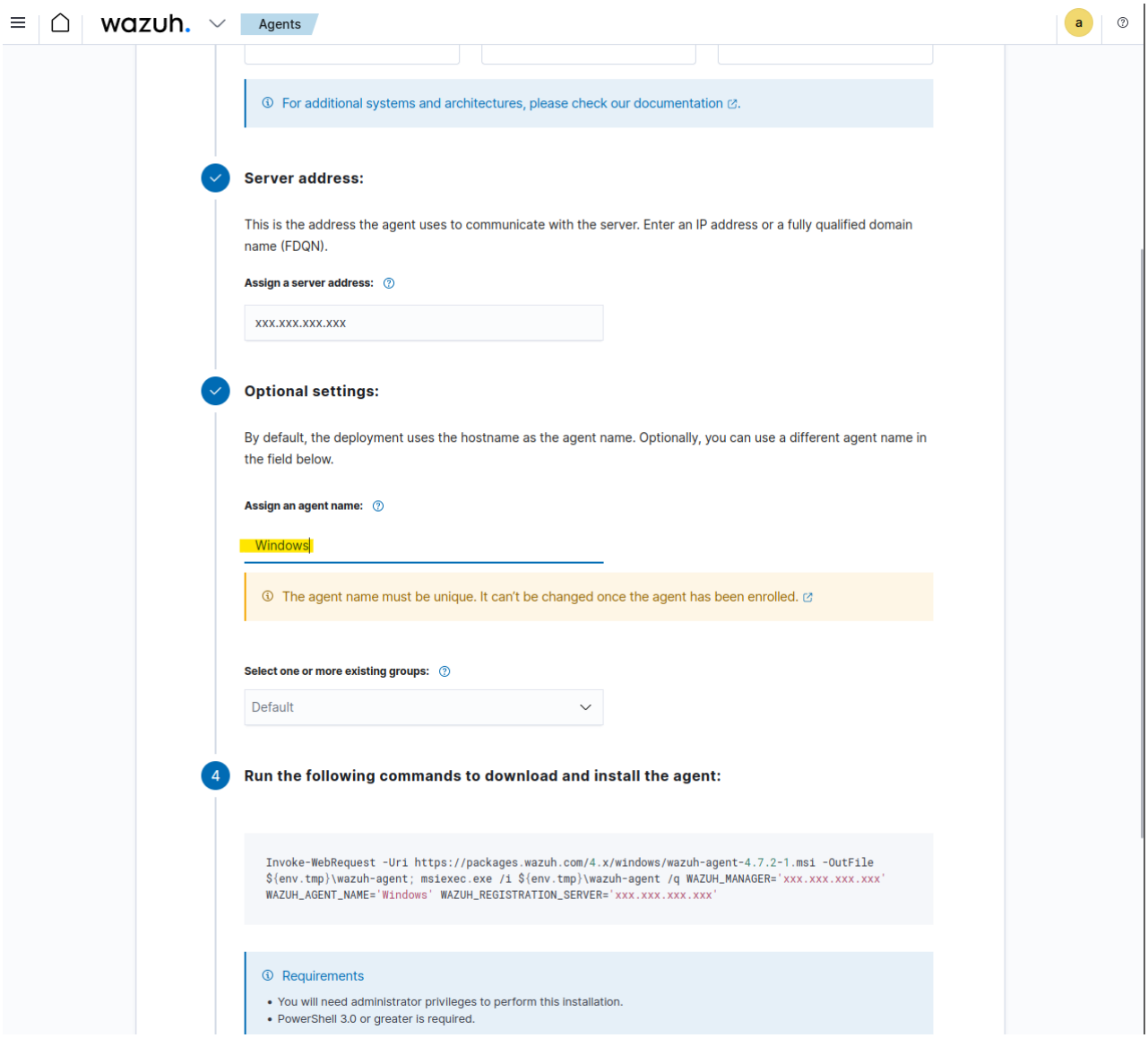


The next step is to add new agents to the wazuh server. It can be either Linux, Windows or any other given OS.



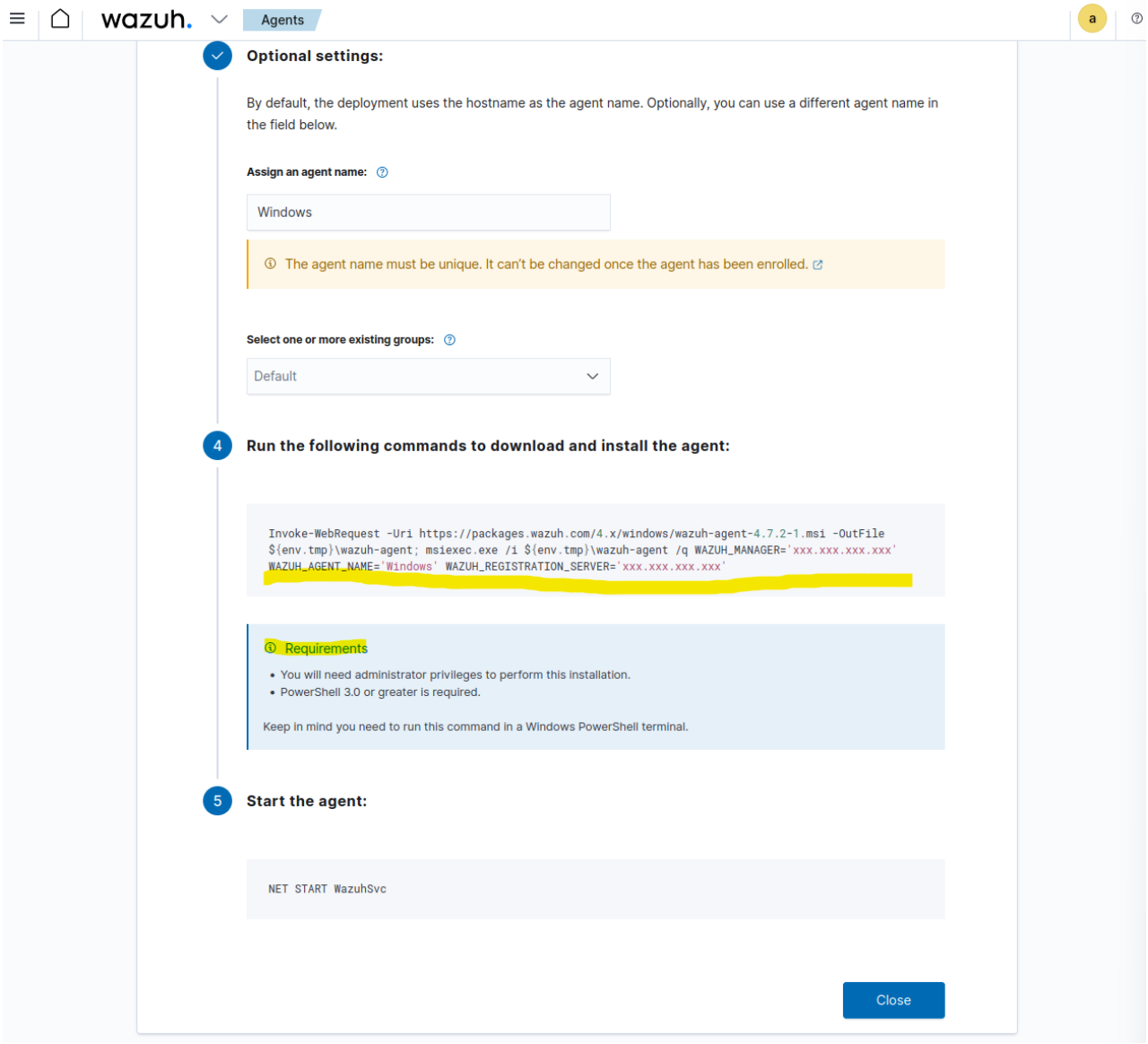
Click on the required agent OS type and fill up the necessary details, the IP should be the servers IP and you can give any name to the agent and the commands will be automatically generated as per the OS. And this should be proceeded in the agent system.


wazuh.
Agents
a
Deploy new agent
Select the package to download and install on your system:
LINUX
RPM amd64
RPM aarch64
DEB amd64
DEB aarch64
WINDOWS
MSI 32/64 bits
macOS
Intel
Apple silicon
For additional systems and architectures, please check our documentation.
2
Server address:
This is the address the agent uses to communicate with the server. Enter an IP address or a fully qualified domain name (FDQN).
Assign a server address:
Server address
3
Optional settings:
By default, the deployment uses the hostname as the agent name. Optionally, you can use a different agent name in the field below.
Assign an agent name:
Agent name
The agent name must be unique. It can't be changed once the agent has been enrolled.
Select one or more existing groups:
Default

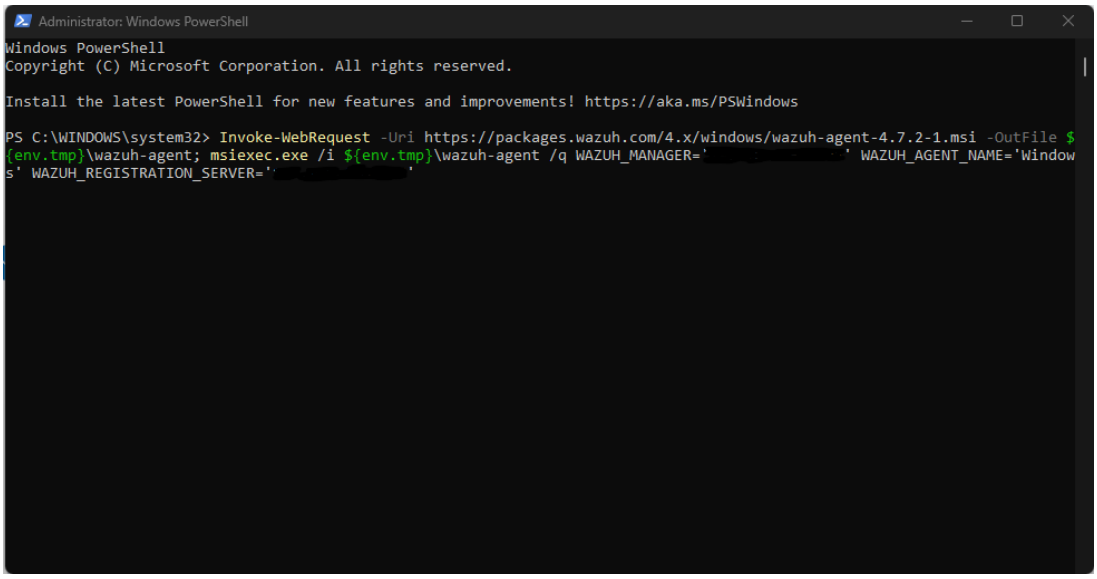


For the next step we simple have to copy and run the command the Wazuh Manager created for us on the desired end point. If you look at the command, you will see all the fields we filled out were conveniently compiled into this command for us. If you hover over the command box, there is a button that allows you to copy the entire command. Easy!

Note to run this command you will need administrator privileges on the end point and PowerShell 3.0 or greater. Run the command in Windows PowerShell, not Command Prompt.

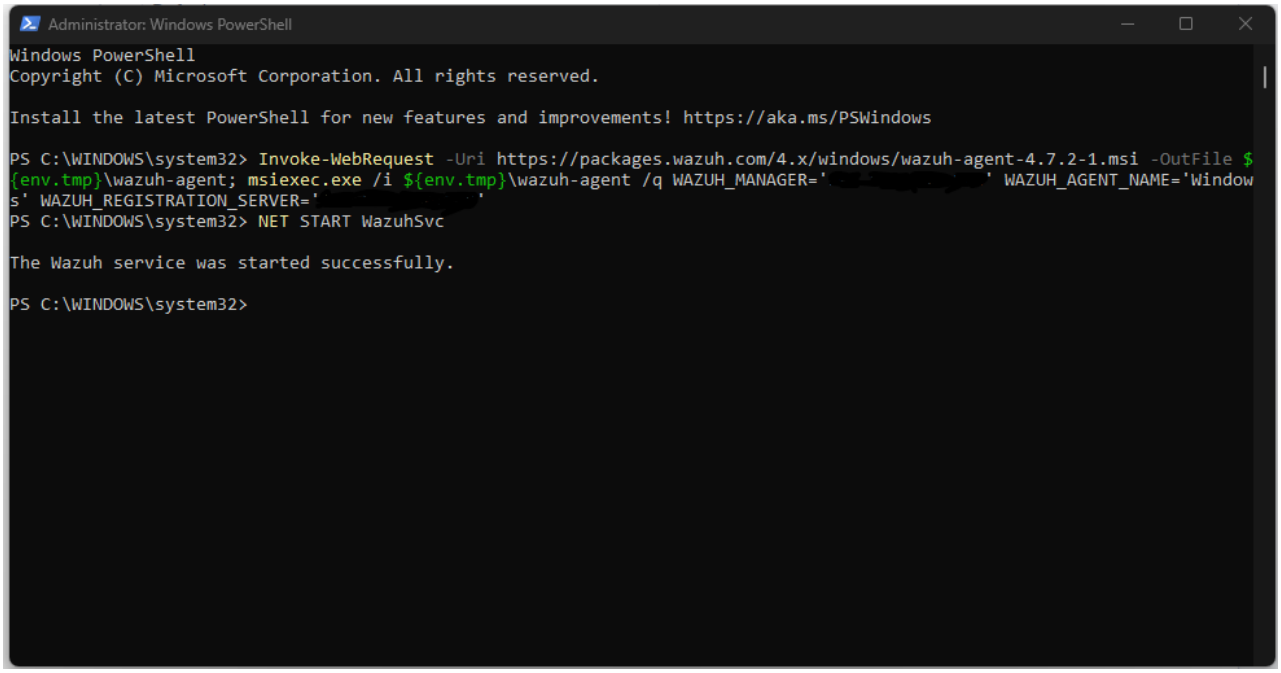

wazuh.
Agents
a
Optional settings:
By default, the deployment uses the hostname as the agent name. Optionally, you can use a different agent name in the field below.
Assign an agent name:
Windows
The agent name must be unique. It can't be changed once the agent has been enrolled.
Select one or more existing groups:
Default
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='xxx.xxx.xxx.xxx' WAZUH_AGENT_NAME='Windows' WAZUH_REGISTRATION_SERVER='xxx.xxx.xxx.xxx'
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
Close

Now go to windows VM and enter these commands in the powershell with administrator priviliges.



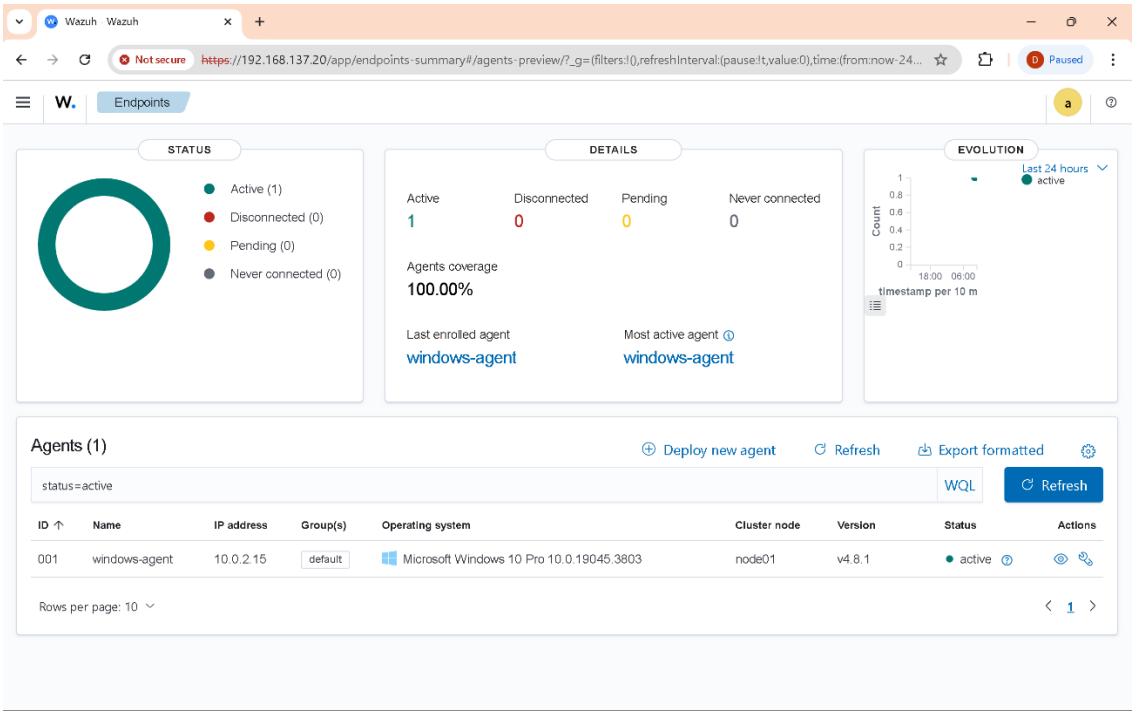
Press Enter and the Wazuh Agent will automatically download and install to the Windows machine. A progress counter will display until it is installed. You will know it is finished installing when the command prompt returns.

Next we need to start the Agent now that we have it installed. Copy the command provided by Wazuh Manager, paste it in your Windows PowerShell window, and press Enter. This will start the Wazuh Agent service.

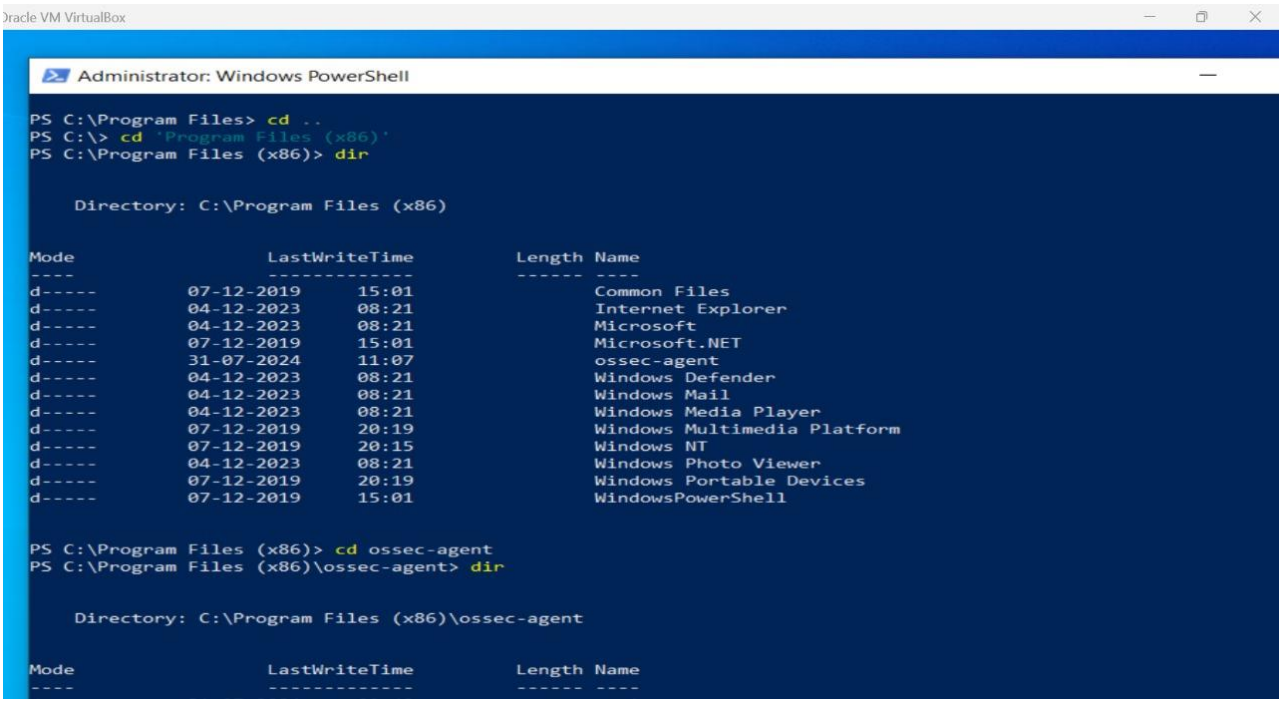


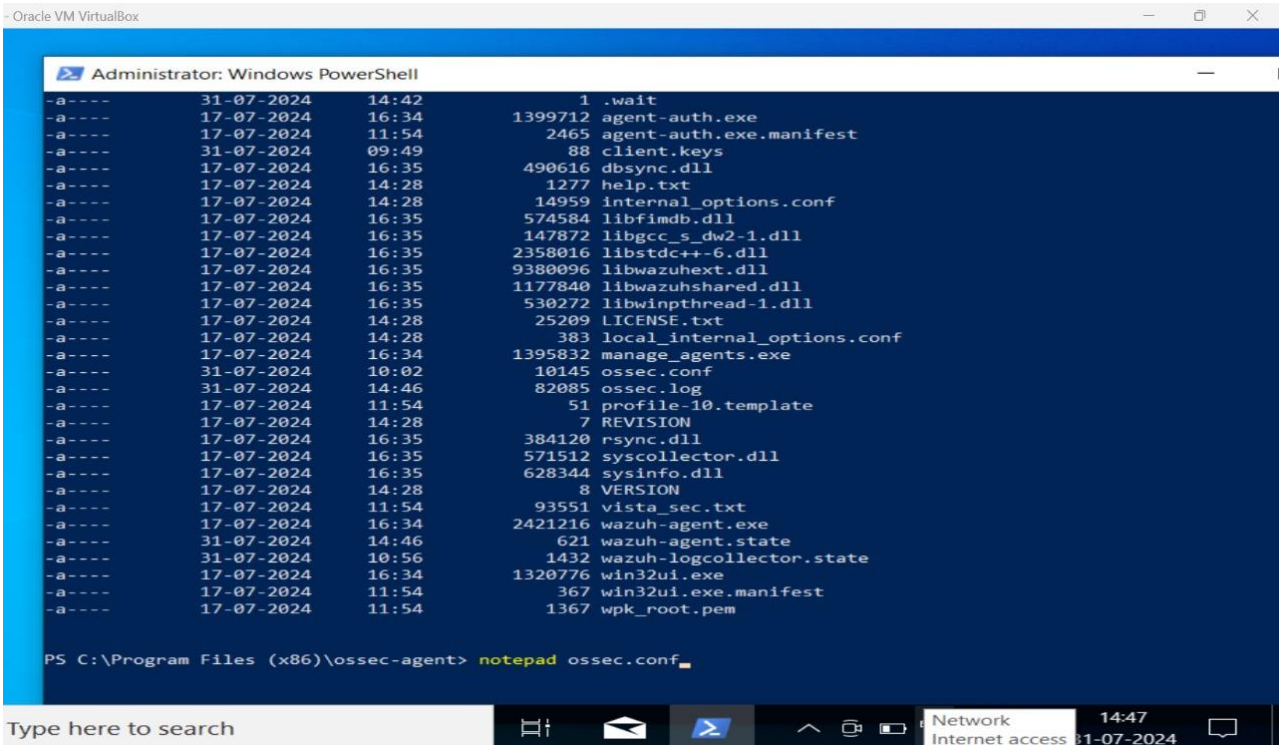
Navigate back to your Wazuh Manager home page and you will see the Total agents and Active agents counts are now ‘one’.

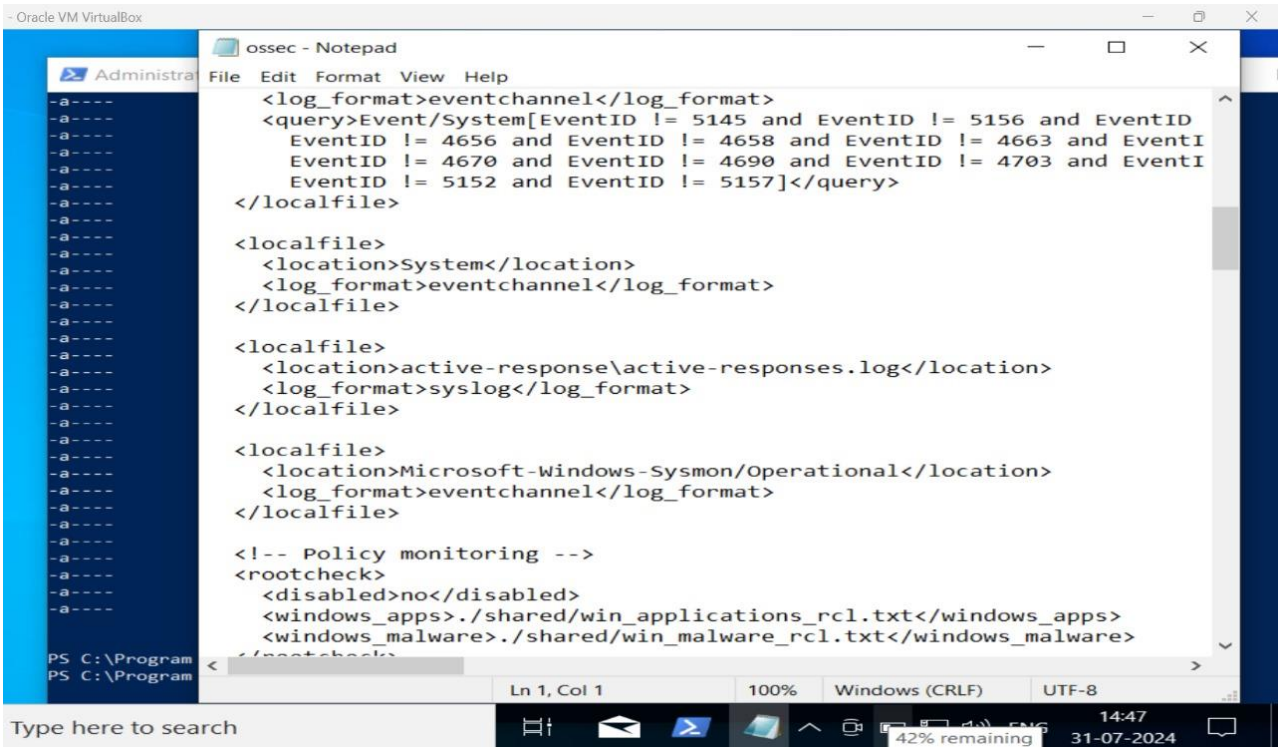
Congratulations! You have successfully added your first agent to the Wazuh Manager! Select the number ‘one’ and you will be directed to the dashboard for your agent. Feel free to poke around the dashboard and explore.



On the Windows VM: Use a text editor (notepad++ or notepad) as an Administrator and edit the C:\\\\Program Files (x86)\\\\ossec-agent\\\\ossec.conf file and add the following entries:

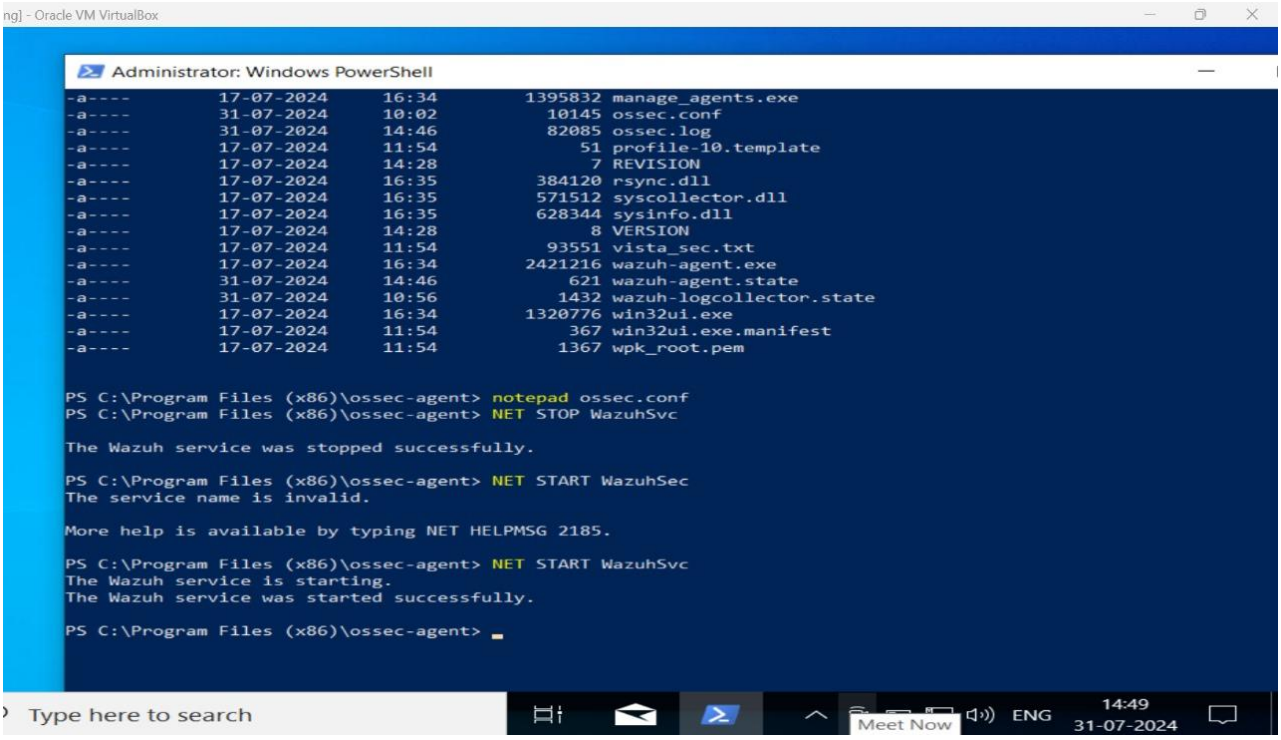



Oracle VM VirtualBox
Administrator: Windows PowerShell
-a---- 31-07-2024 14:42 1 .wait
-a---- 17-07-2024 16:34 1399712 agent-auth.exe
-a---- 17-07-2024 11:54 2465 agent-auth.exe.manifest
-a---- 31-07-2024 09:49 88 client.keys
-a---- 17-07-2024 16:35 490616 dbsync.dll
-a---- 17-07-2024 14:28 1277 help.txt
-a---- 17-07-2024 14:28 14959 internal_options.conf
-a---- 17-07-2024 16:35 574584 libfimdb.dll
-a---- 17-07-2024 16:35 147872 libgcc_s_dw2-1.dll
-a---- 17-07-2024 16:35 2358016 libstdc++-6.dll
-a---- 17-07-2024 16:35 9380096 libwazuhext.dll
-a---- 17-07-2024 16:35 1177840 libwazuhshared.dll
-a---- 17-07-2024 16:35 530272 libwinpthread-1.dll
-a---- 17-07-2024 14:28 25209 LICENSE.txt
-a---- 17-07-2024 14:28 383 local_internal_options.conf
-a---- 17-07-2024 16:34 1395832 manage_agents.exe
-a---- 31-07-2024 10:02 10145 ossec.conf
-a---- 31-07-2024 14:46 82085 ossec.log
-a---- 17-07-2024 11:54 51 profile-10.template
-a---- 17-07-2024 14:28 7 REVISION
-a---- 17-07-2024 16:35 384120 rsync.dll
-a---- 17-07-2024 16:35 571512 syscollector.dll
-a---- 17-07-2024 16:35 628344 sysinfo.dll
-a---- 17-07-2024 14:28 8 VERSION
-a---- 17-07-2024 11:54 93551 vista_sec.txt
-a---- 17-07-2024 16:34 2421216 wazuh-agent.exe
-a---- 31-07-2024 14:46 621 wazuh-agent.state
-a---- 31-07-2024 10:56 1432 wazuh-logcollector.state
-a---- 17-07-2024 16:34 1320776 win32ui.exe
-a---- 17-07-2024 11:54 367 win32ui.exe.manifest
-a---- 17-07-2024 11:54 1367 wpk_root.pem
PS C:\Program Files (x86)\ossec-agent> notepad ossec.conf
Type here to search
Network
Internet access
14:47
31-07-2024



Restart the Wazuh service:

NET STOP WazuhSvc
NET START WazuhSvc



CONFIGURING WAZUH FOR SYSMON EVENTS

Enable the ability to ssh as a root from our Windows VM:

Enable root SSH access:

In the Wazuh VM, edit the SSH configuration file:

sudo nano /etc/ssh/sshd_config

Change ##PermitRootLogin no to PermitRootLogin yes

```
# Authentication:

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

#PubkeyAuthentication yes
```

- Save and exit
- Restart the SSH service: service sshd restart

service sshd restart

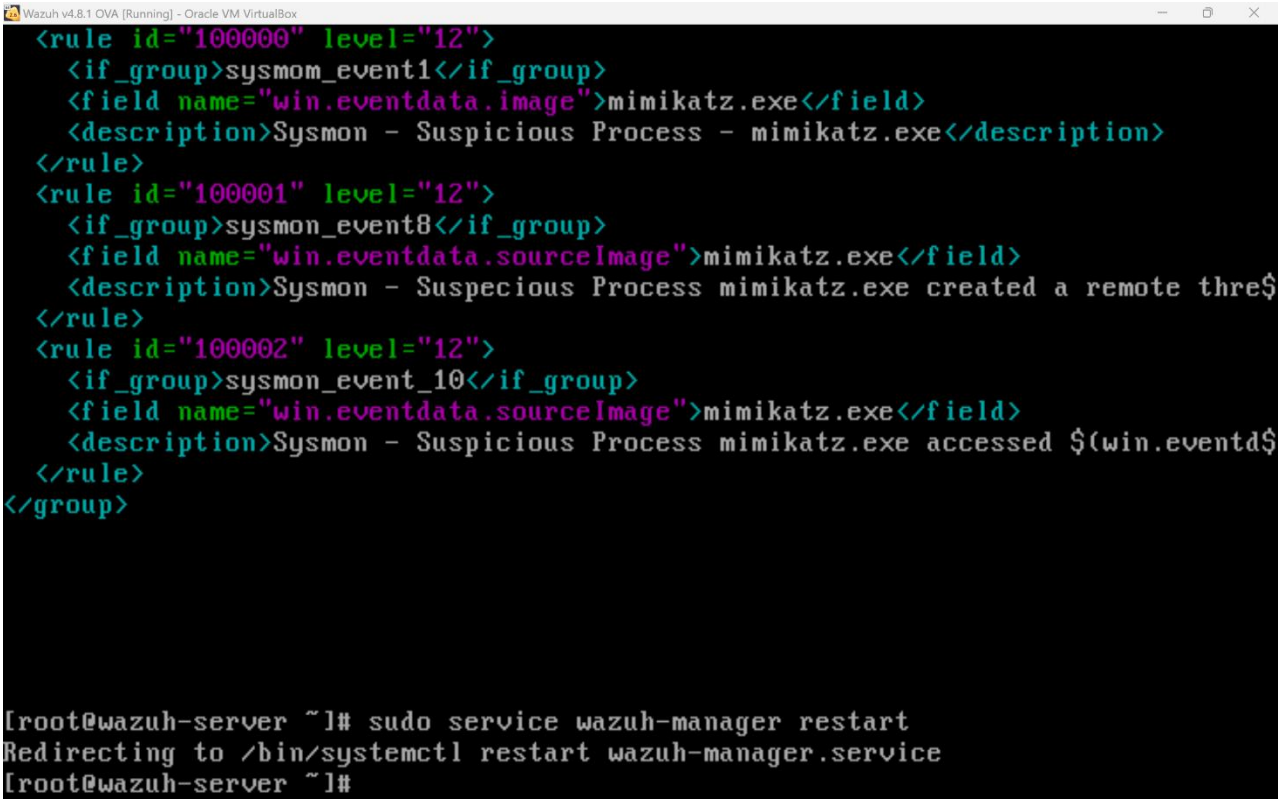
```
[root@wazuh-server ~]# service sshd restart
Redirecting to /bin/systemctl restart sshd.service
[root@wazuh-server ~]#
```

CONFIGURING SERVER TO DETECT THE SIMULATED MALWARE

Test it by writing some rules for detecting suspicious events related to the mimikatz.exe process. Mimikatz is a well-known tool for extracting Windows credentials.

Write the security rules:

- Edit the Wazuh rules file:
- sudo nano /var/ossec/etc/rules/local_rules.xml



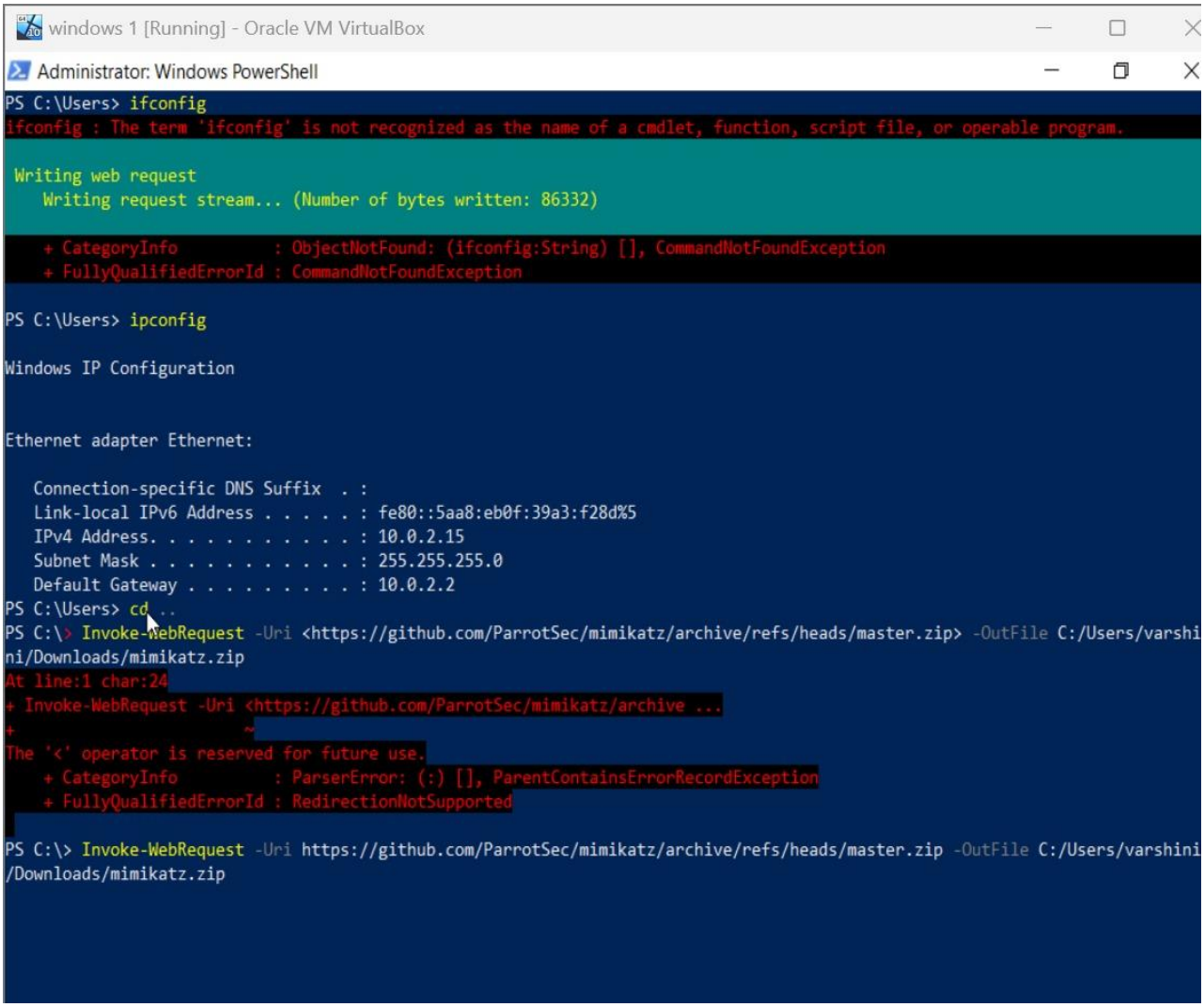
Restart the Wazuh Manager:

sudo service wazuh-manager restart

INSTALLING THE SIMULATED MALWARE FILE IN THE AGENT SYSTEM

Extract the previously downloaded Mimikatz .zip file.

Open PowerShell as administrator and navigate to the extracted Mimikatz folder.


windows 1 [Running] - Oracle VM VirtualBox
Administrator: Windows PowerShell
PS C:\Users> ifconfig
ifconfig : The term 'ifconfig' is not recognized as the name of a cmdlet, function, script file, or operable program.
Writing web request
Writing request stream... (Number of bytes written: 86332)
+ CategoryInfo : ObjectNotFound: (ifconfig:String) [], CommandNotFoundException
+ FullyQualifiedErrorId : CommandNotFoundException
PS C:\Users> ipconfig
Windows IP Configuration
Ethernet adapter Ethernet:
Connection-specific DNS Suffix . :
Link-local IPv6 Address . . . . . : fe80::5aa8:eb0f:39a3:f28d%5
IPv4 Address. . . . . : 10.0.2.15
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 10.0.2.2
PS C:\Users> cd ..
PS C:\> Invoke-WebRequest -Uri <https://github.com/ParrotSec/mimikatz/archive/refs/heads/master.zip> -OutFile C:/Users/varshi
ni/Downloads/mimikatz.zip
At line:1 char:24
+ Invoke-WebRequest -Uri <https://github.com/ParrotSec/mimikatz/archive ...
+ ~
The '<' operator is reserved for future use.
+ CategoryInfo : ParserError: (:) [], ParentContainsErrorRecordException
+ FullyQualifiedErrorId : RedirectionNotSupported
PS C:\> Invoke-WebRequest -Uri https://github.com/ParrotSec/mimikatz/archive/refs/heads/master.zip -OutFile C:/Users/varshini
/Downloads/mimikatz.zip

Run the following commands:

.\\mimikatz.exe

.\\mimikatz.exe: This command executes the Mimikatz executable file. The **.** at the beginning specifies that the file is located in the current directory.

privilege::debug

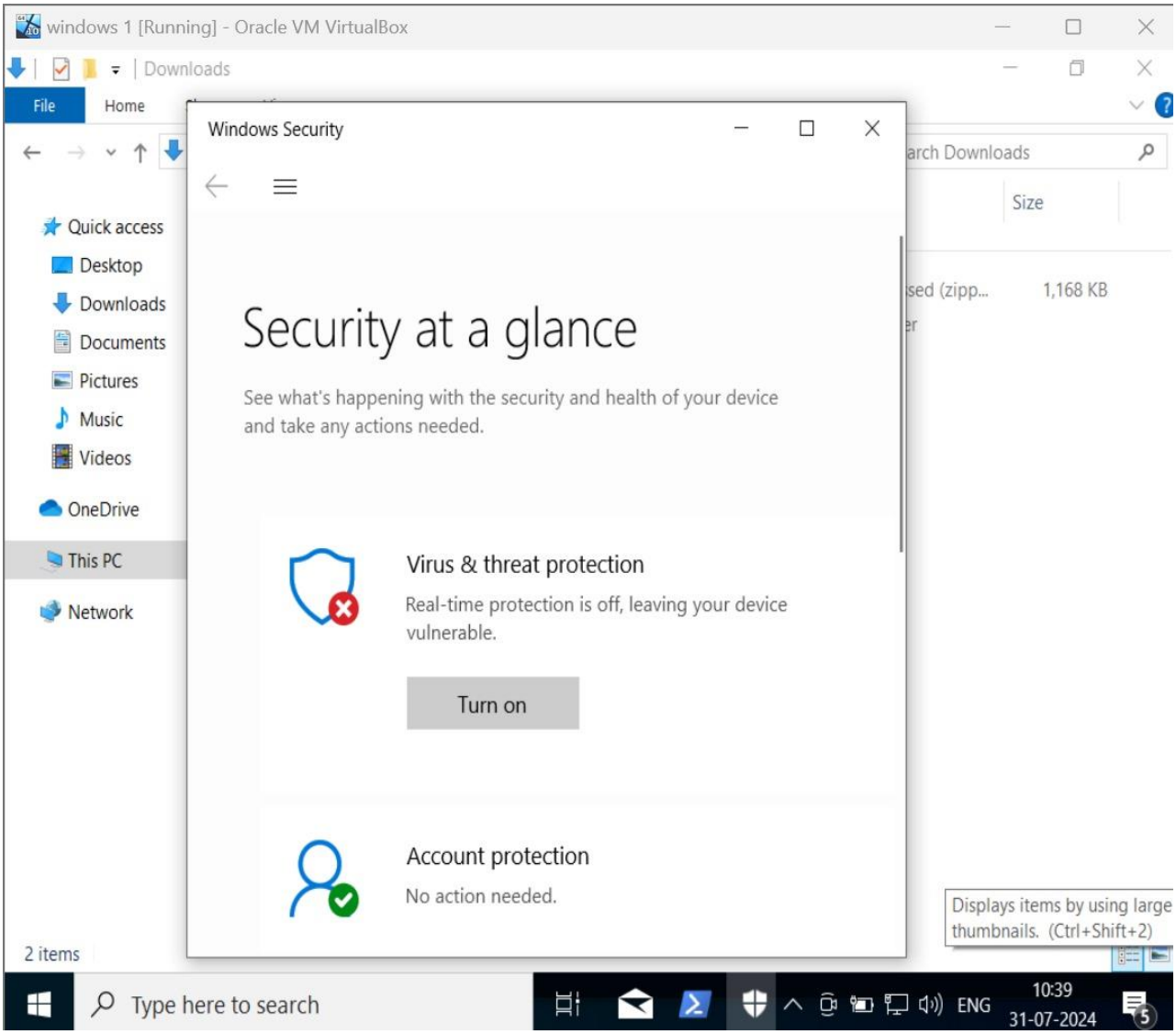
privilege::debug: This command instructs Mimikatz to enable debug privileges. Debug privileges are powerful permissions that allow a user to interact directly with system processes and memory, potentially bypassing security mechanisms.

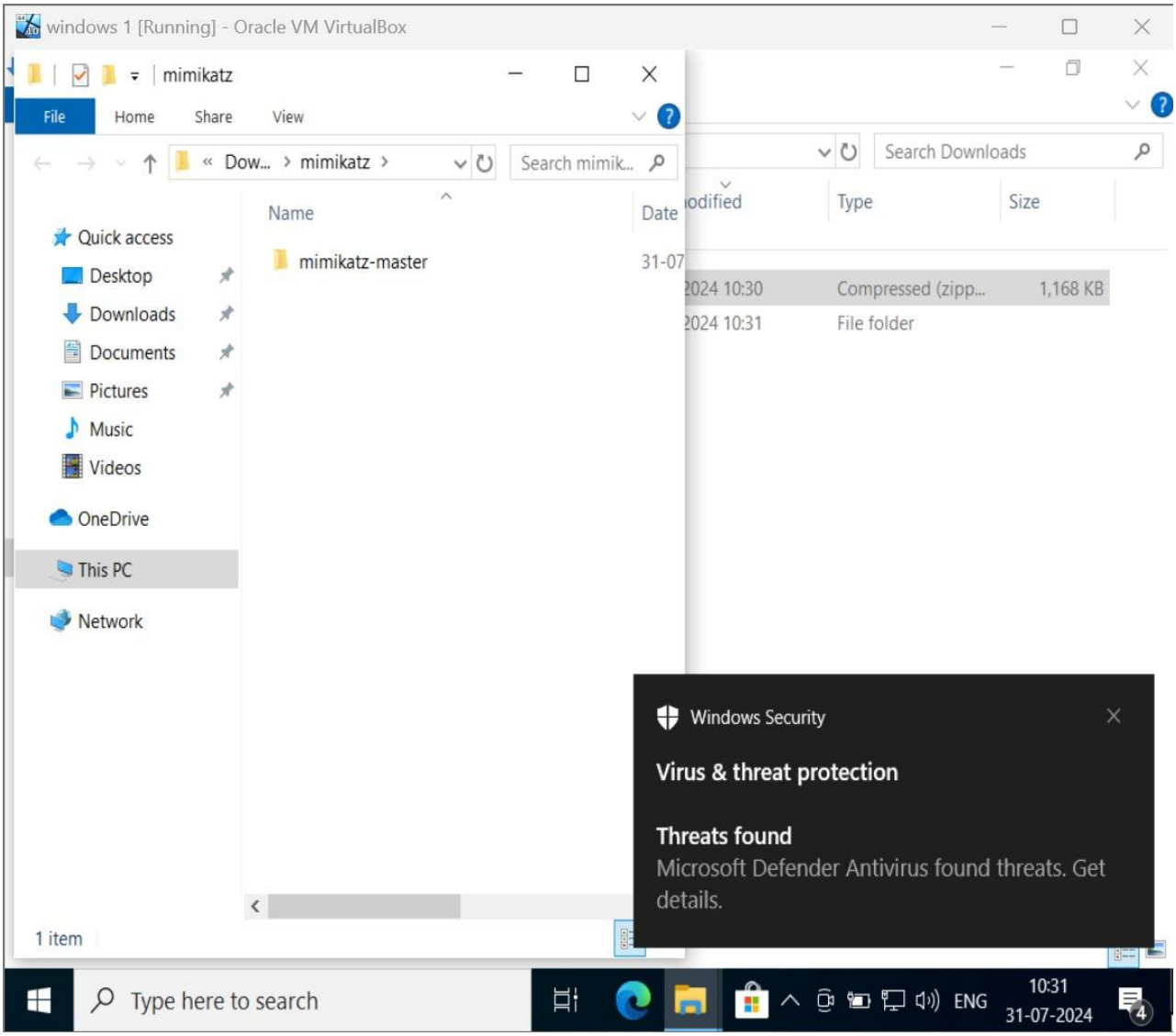
log mimikatz.log

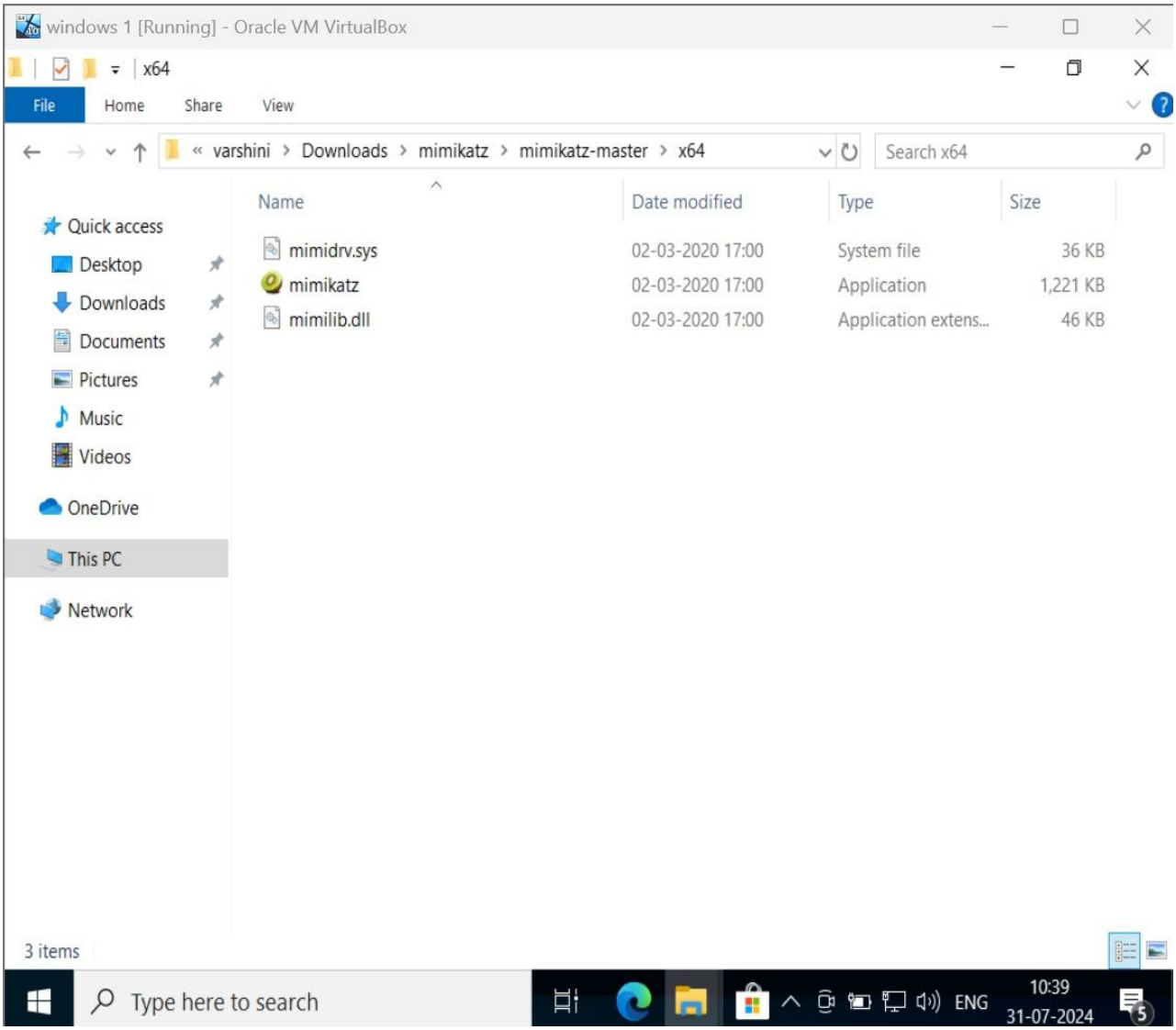
log mimikatz.log: This command sets up logging, directing the output of Mimikatz commands to a file named **mimikatz.log**. This can be useful for later analysis or auditing purposes.

sekurlsa::logonpasswords

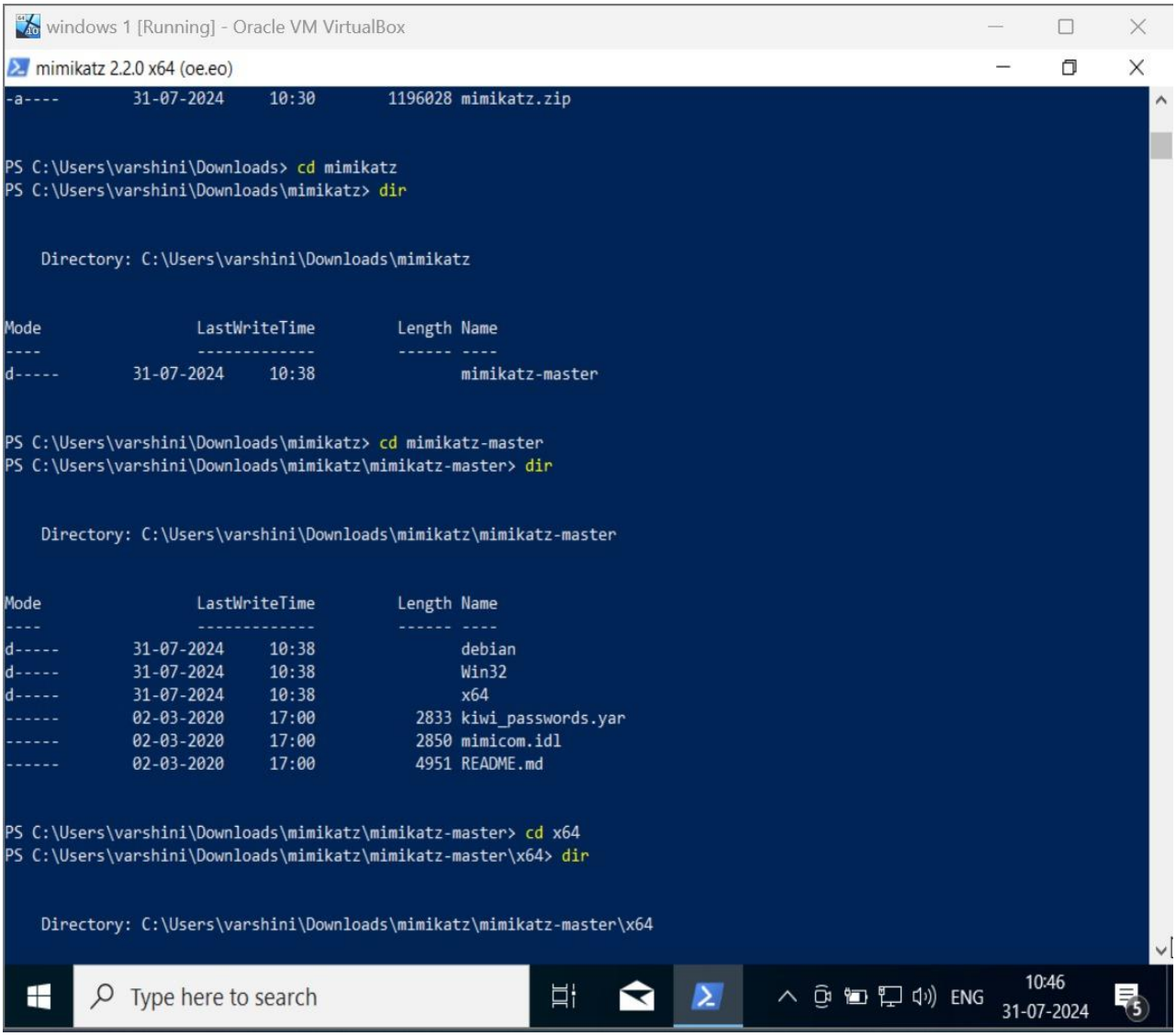
sekurlsa::logonpasswords: This command instructs Mimikatz to retrieve and display plaintext passwords from the Windows Security Account Manager (SAM) database, which contains user account information including passwords.
Mimikatz's **sekurlsa** module specifically deals with credentials.


windows 1 [Running] - Oracle VM VirtualBox
Downloads
File
Home
Windows Security
Security at a glance
See what's happening with the security and health of your device and take any actions needed.
Virus & threat protection
Real-time protection is off, leaving your device vulnerable.
Turn on
Account protection
No action needed.
Quick access
Desktop
Downloads
Documents
Pictures
Music
Videos
OneDrive
This PC
Network
Size
1,168 KB
2 items
Displays items by using large thumbnails. (Ctrl+Shift+2)
Type here to search
ENG
10:39
31-07-2024

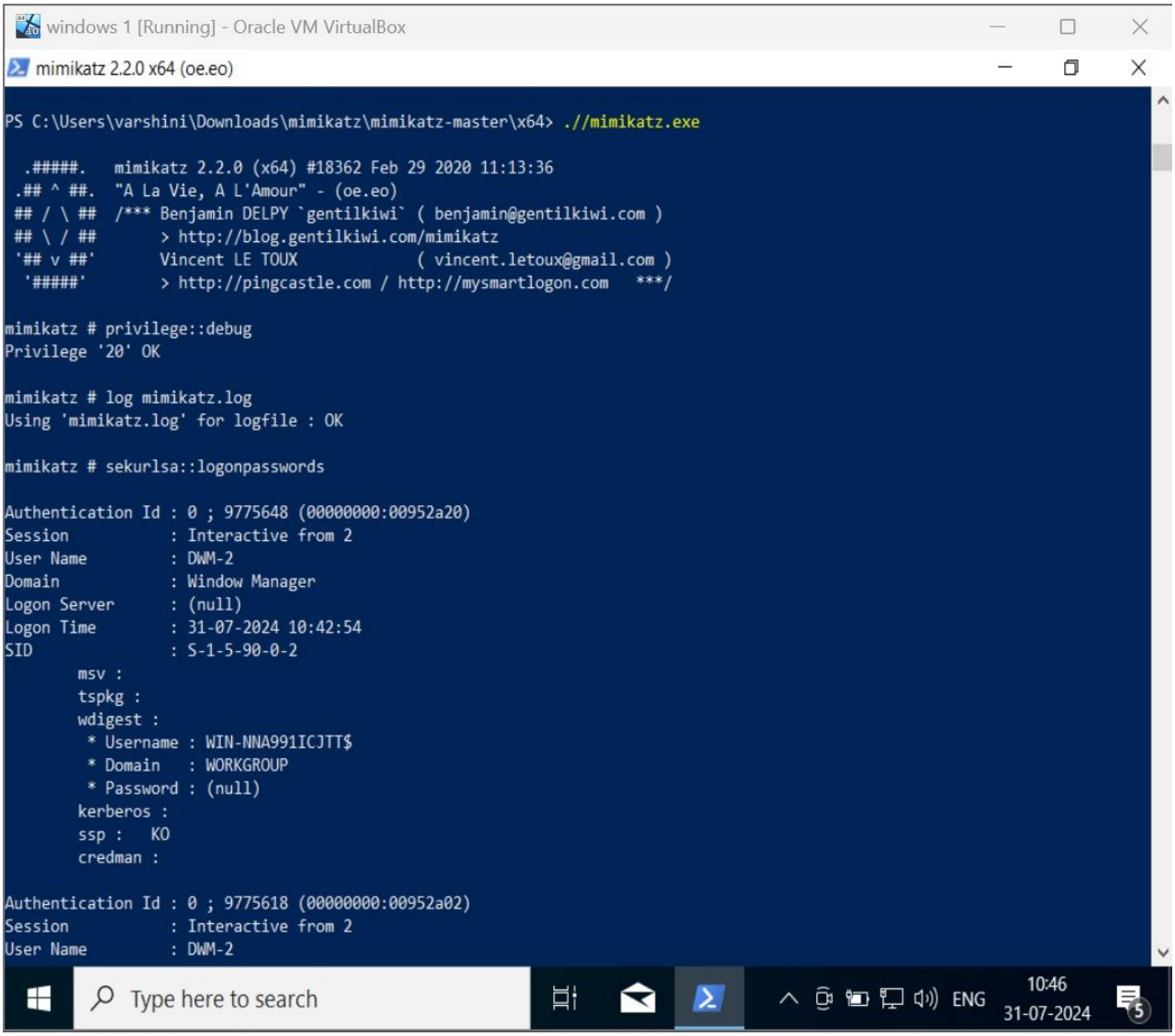

windows 1 [Running] - Oracle VM VirtualBox
mimikatz
File
Home
Share
View
Dow... › mimikatz ›
Search mimik...
Quick access
Desktop
Downloads
Documents
Pictures
Music
Videos
OneDrive
This PC
Network
Name
Date
mimikatz-master
31-07
1 item
Search Downloads
Type
Size
Compressed (zipp...
1,168 KB
File folder
Windows Security
Virus & threat protection
Threats found
Microsoft Defender Antivirus found threats. Get details.
Type here to search
ENG
10:31
31-07-2024

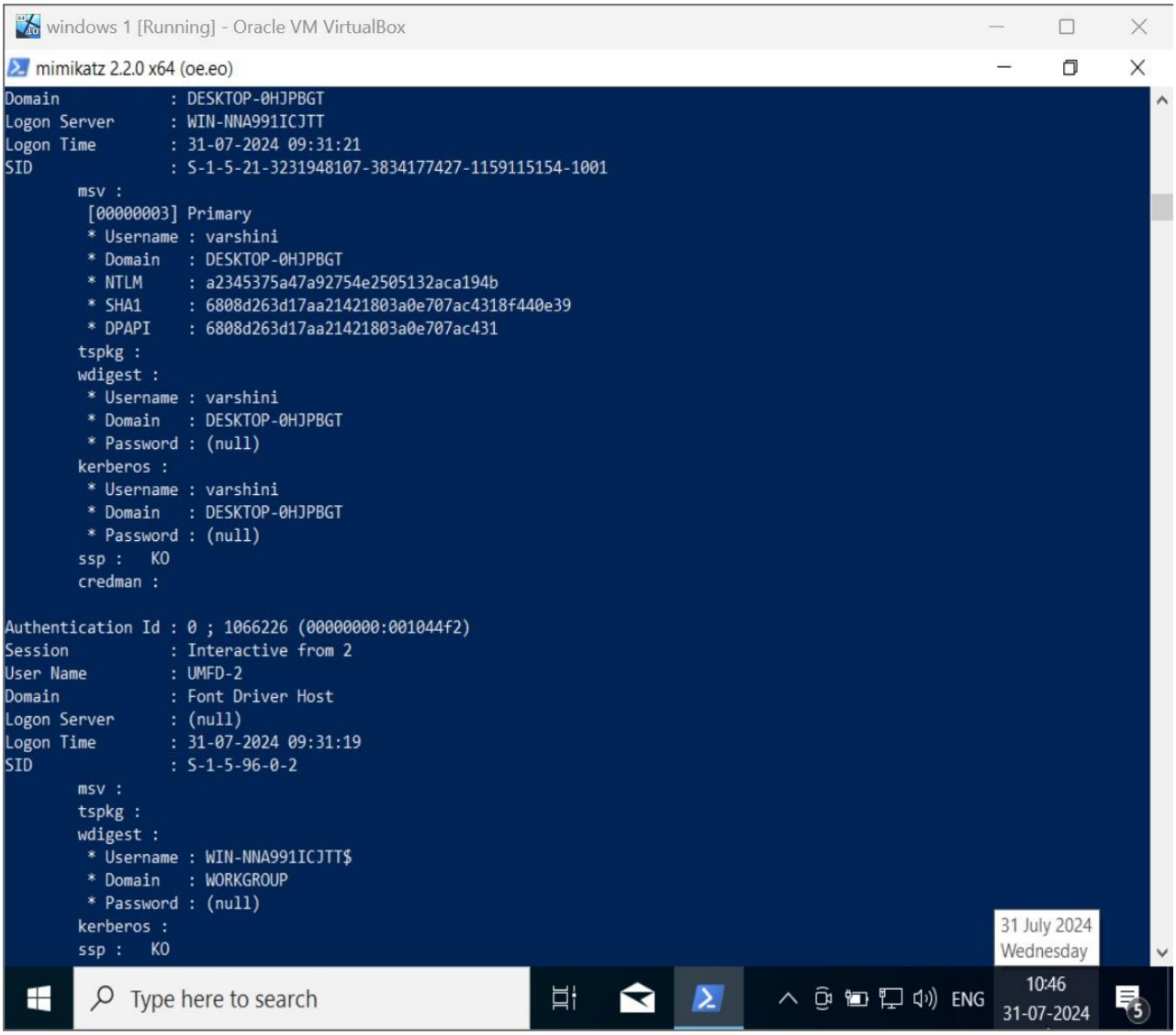


Open PowerShell as administrator and navigate to the extracted Mimikatz folder.



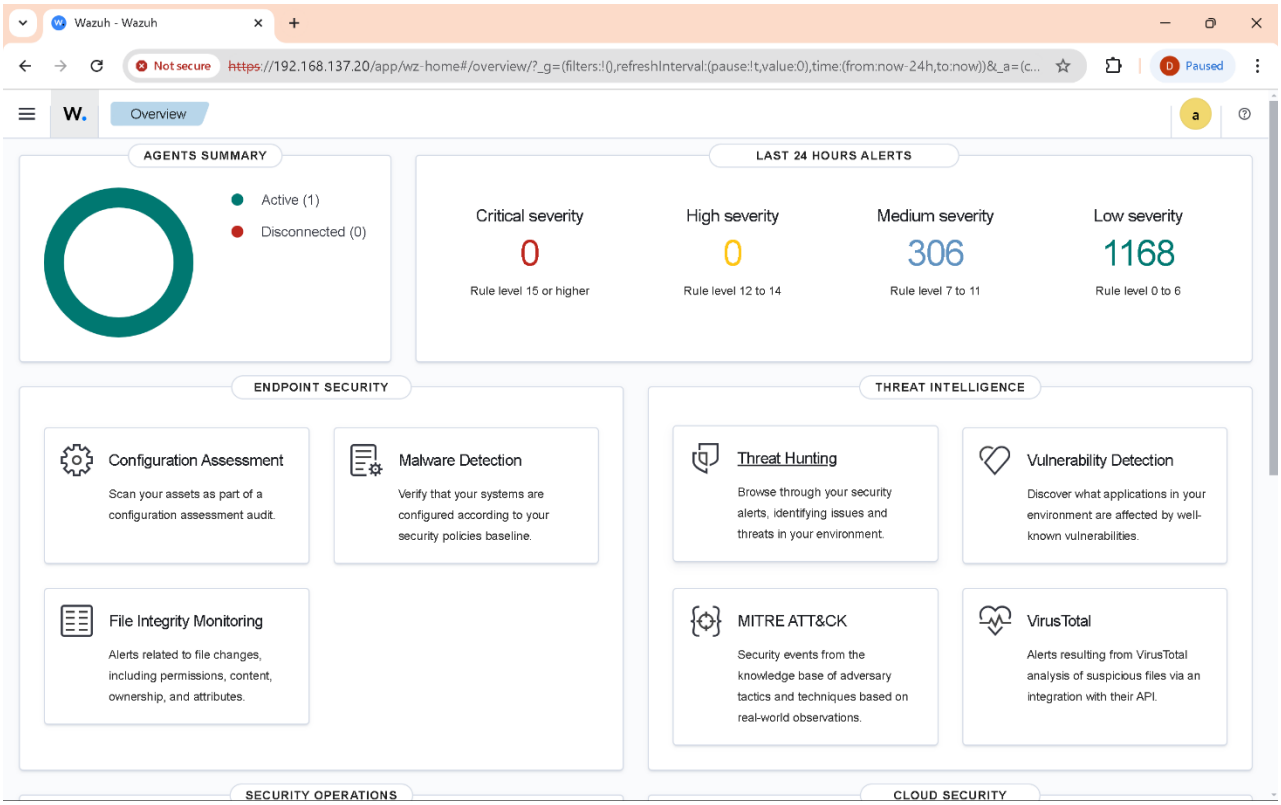
EXECUTING THE MALWARE FILE

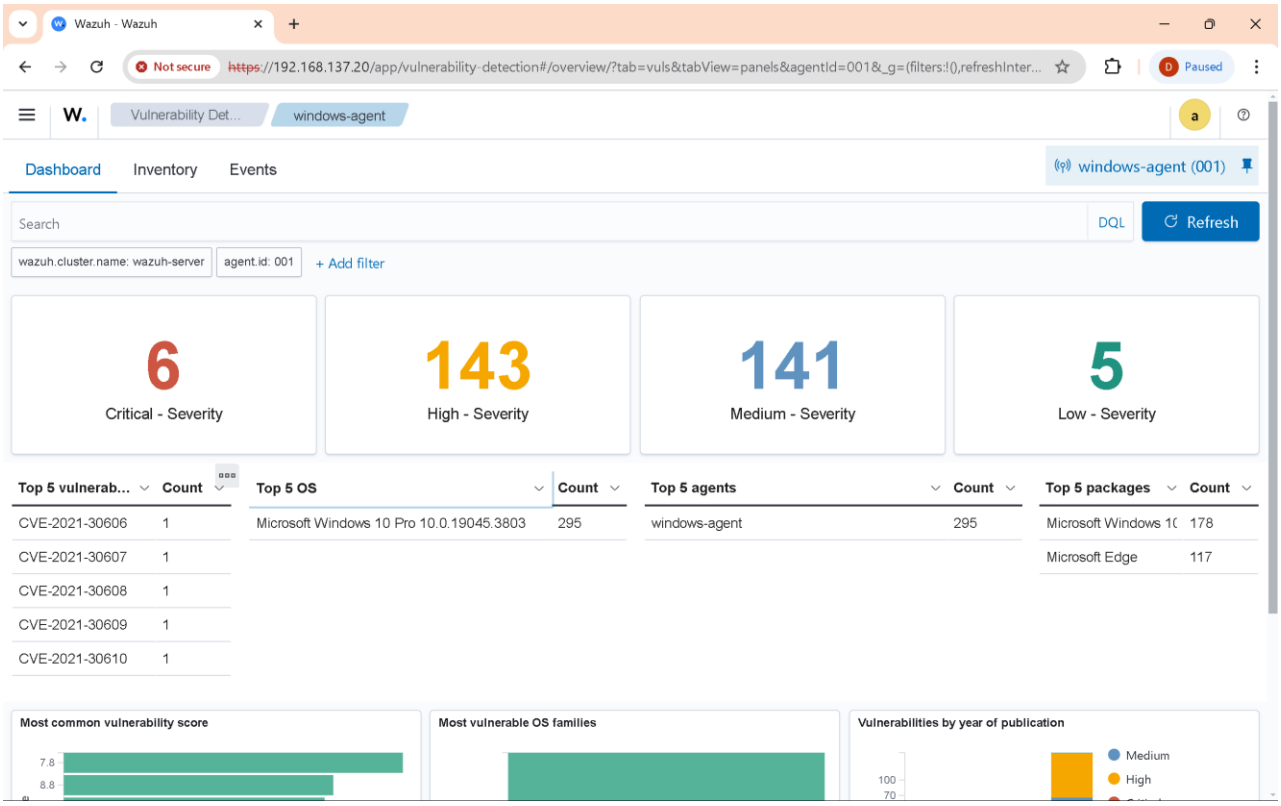

windows 1 [Running] - Oracle VM VirtualBox
mimikatz 2.2.0 x64 (oe.eo)
PS C:\Users\varshini\Downloads\mimikatz\mimikatz-master\x64> .//mimikatz.exe
.#####. mimikatz 2.2.0 (x64) #18362 Feb 29 2020 11:13:36
.## ^ ##. "A La Vie, A L'Amour" - (oe.eo)
/ \ ## /*** Benjamin DELPY `gentilkiwi` (benjamin@gentilkiwi.com)
\ / ## > http://blog.gentilkiwi.com/mimikatz
'## v ##' Vincent LE TOUX (vincent.letoux@gmail.com)
'#####' > http://pingcastle.com / http://mysmartlogon.com ***/
mimikatz # privilege::debug
Privilege '20' OK
mimikatz # log mimikatz.log
Using 'mimikatz.log' for logfile : OK
mimikatz # sekurlsa::logonpasswords
Authentication Id : 0 ; 9775648 (00000000:00952a20)
Session : Interactive from 2
User Name : DWM-2
Domain : Window Manager
Logon Server : (null)
Logon Time : 31-07-2024 10:42:54
SID : S-1-5-90-0-2
msv :
tspkg :
wdigest :
* Username : WIN-NNA991ICJTT$
* Domain : WORKGROUP
* Password : (null)
kerberos :
ssp : KO
credman :
Authentication Id : 0 ; 9775618 (00000000:00952a02)
Session : Interactive from 2
User Name : DWM-2
Type here to search
ENG
10:46
31-07-2024

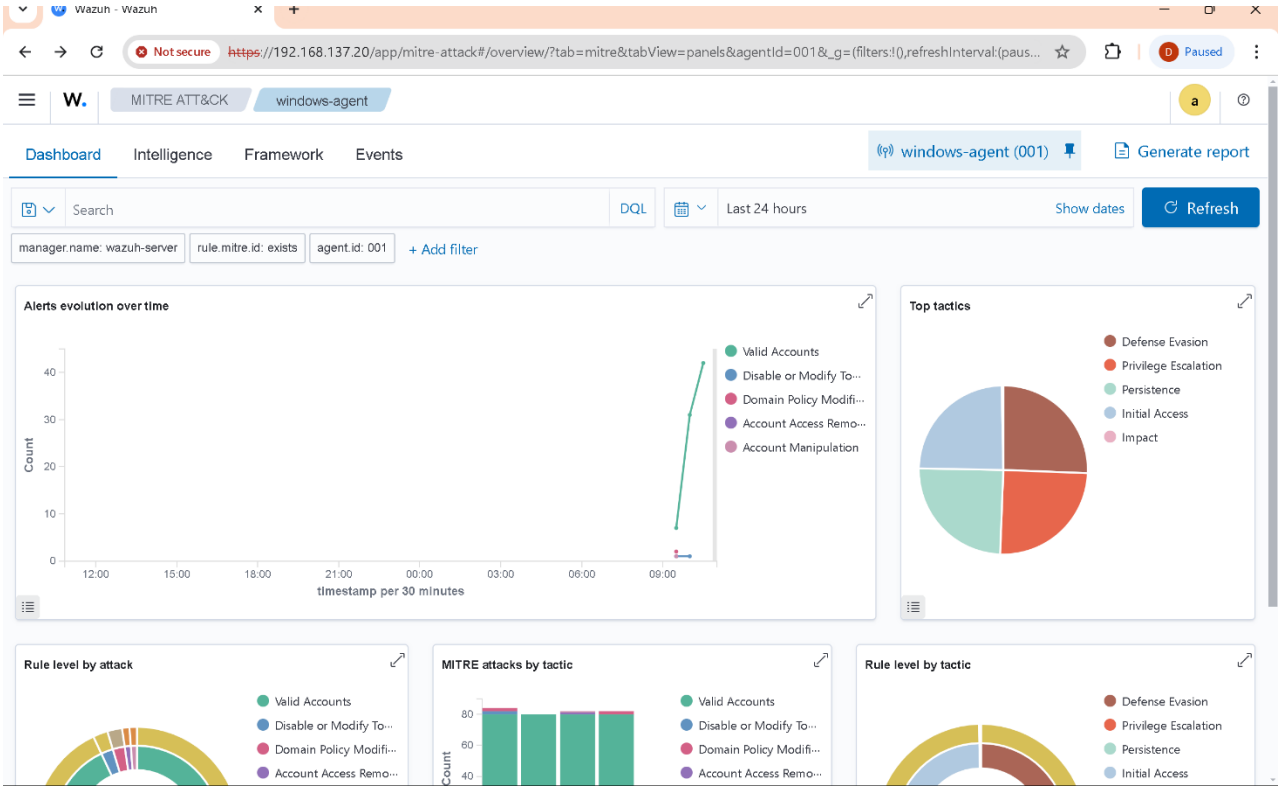


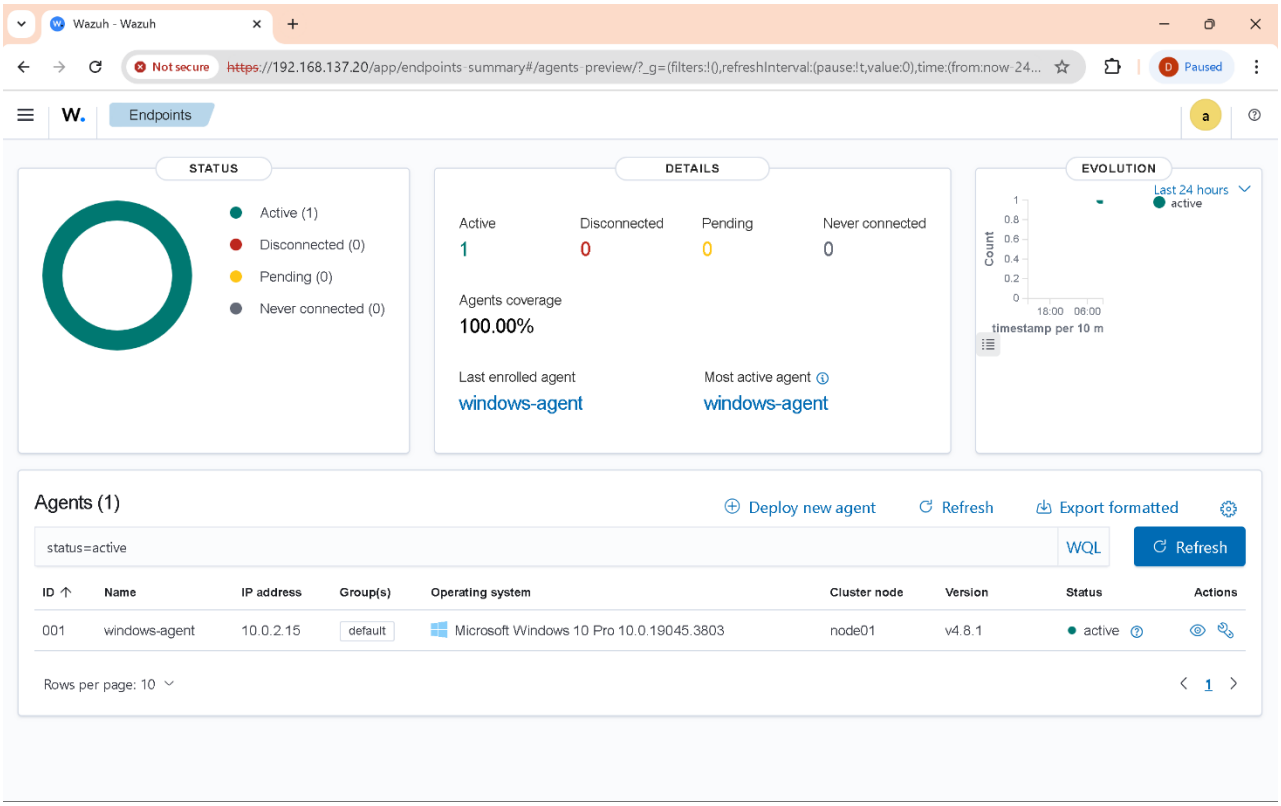
MONITORING MALWARE USING WAZUH SIEM AND XDR

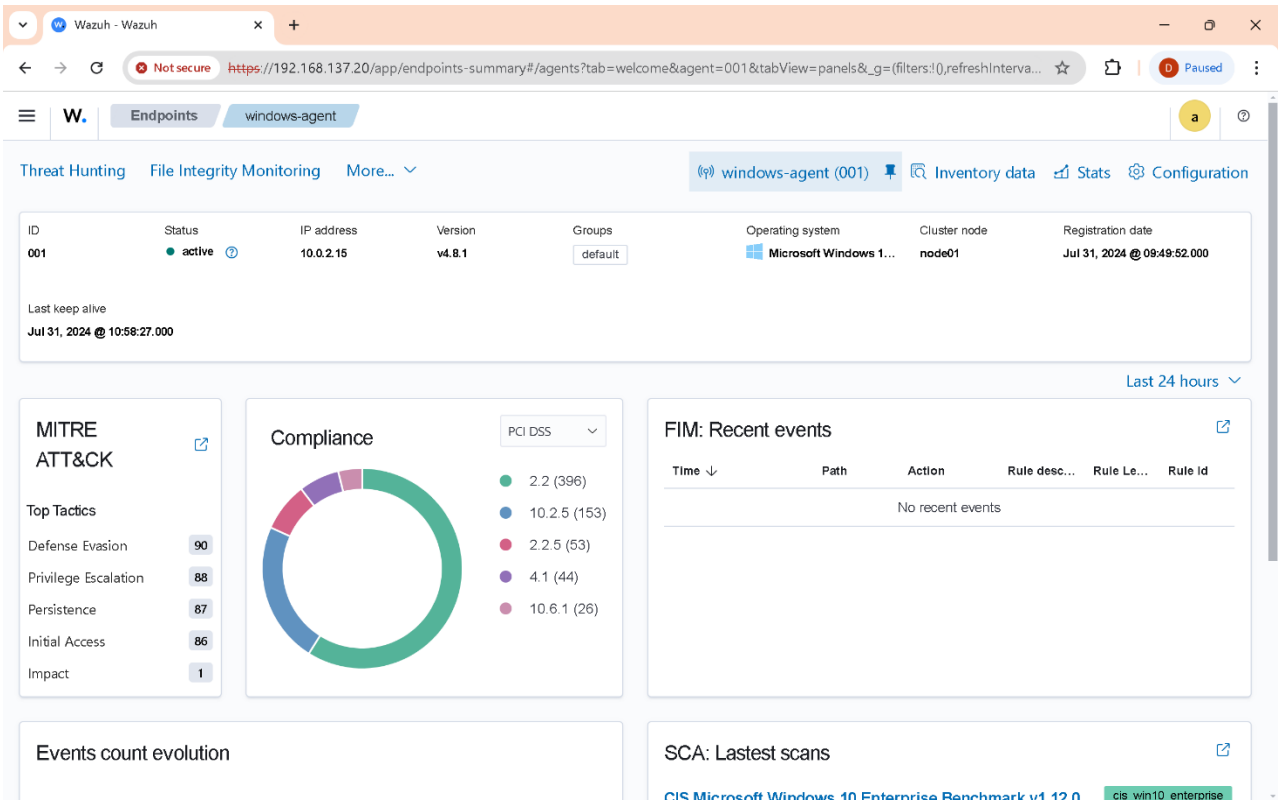
On the Wazuh dashboard, navigate to “Security information management → Security events → Level 12 or above alerts” and you will be able to see alerts related to the Mimikatz activities.

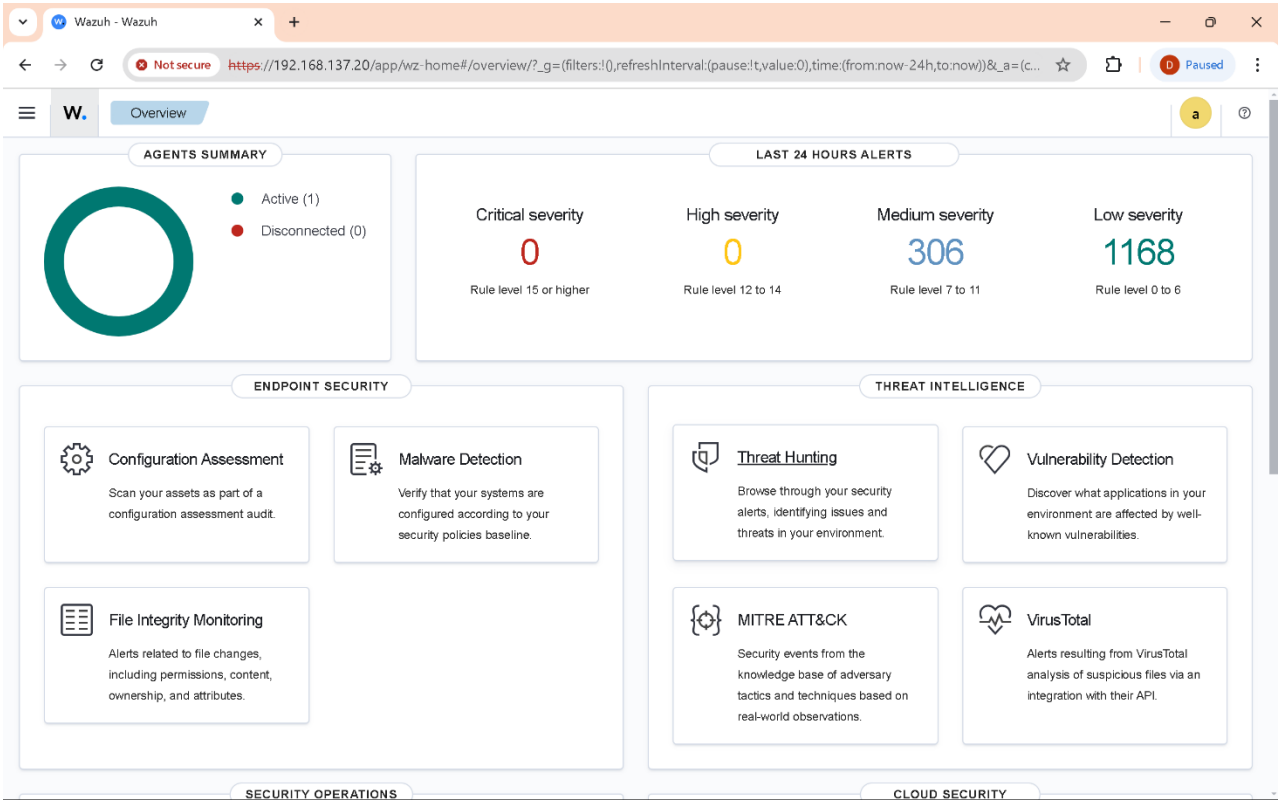

Wazuh - Wazuh
Not secure
https://192.168.137.20/app/wz-home#/overview/?_g=(filters:!(),refreshInterval:(pause:!t,value:0),time:(from:now-24h,to:now))&_a=(c...
Paused
Overview
AGENTS SUMMARY
Active (1)
Disconnected (0)
LAST 24 HOURS ALERTS
Critical severity
0
Rule level 15 or higher
High severity
0
Rule level 12 to 14
Medium severity
306
Rule level 7 to 11
Low severity
1168
Rule level 0 to 6
ENDPOINT SECURITY
Configuration Assessment
Scan your assets as part of a configuration assessment audit.
Malware Detection
Verify that your systems are configured according to your security policies baseline.
File Integrity Monitoring
Alerts related to file changes, including permissions, content, ownership, and attributes.
THREAT INTELLIGENCE
Threat Hunting
Browse through your security alerts, identifying issues and threats in your environment.
Vulnerability Detection
Discover what applications in your environment are affected by well-known vulnerabilities.
MITRE ATT&CK
Security events from the knowledge base of adversary tactics and techniques based on real-world observations.
VirusTotal
Alerts resulting from VirusTotal analysis of suspicious files via an integration with their API.
SECURITY OPERATIONS
CLOUD SECURITY

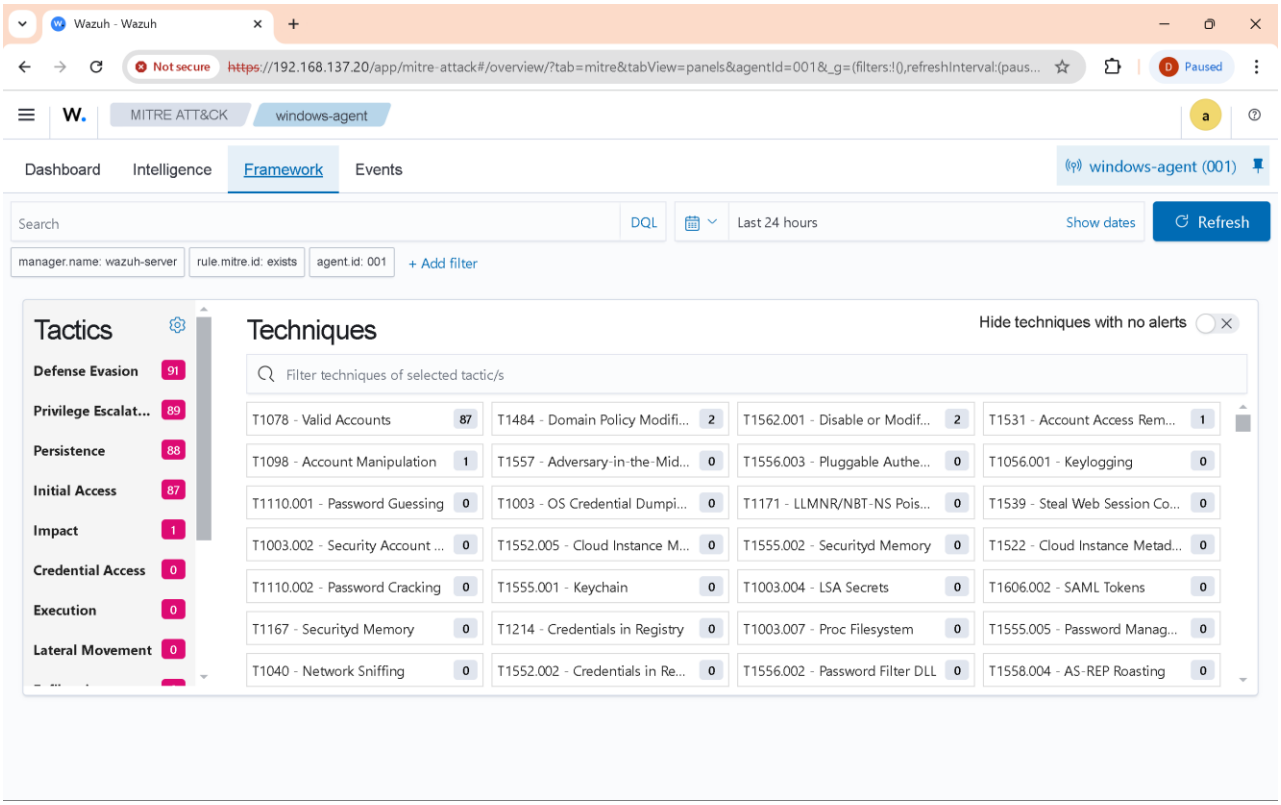

Wazuh - Wazuh
Not secure
https://192.168.137.20/app/vulnerability-detection#/overview/?tab=vuls&tabView=panels&agentId=001&_g=(filters:!(),refreshInter...
Paused
Vulnerability Det...
windows-agent
Dashboard
Inventory
Events
windows-agent (001)
Search
DQL
Refresh
wazuh.cluster.name: wazuh-server
agent.id: 001
+ Add filter
6
Critical - Severity
143
High - Severity
141
Medium - Severity
5
Low - Severity
Top 5 vulnerab...
Count
CVE-2021-30606 1
CVE-2021-30607 1
CVE-2021-30608 1
CVE-2021-30609 1
CVE-2021-30610 1
Top 5 OS
Count
Microsoft Windows 10 Pro 10.0.19045.3803 295
Top 5 agents
Count
windows-agent 295
Top 5 packages
Count
Microsoft Windows 1(178
Microsoft Edge 117
Most common vulnerability score
Most vulnerable OS families
Vulnerabilities by year of publication
Medium
High

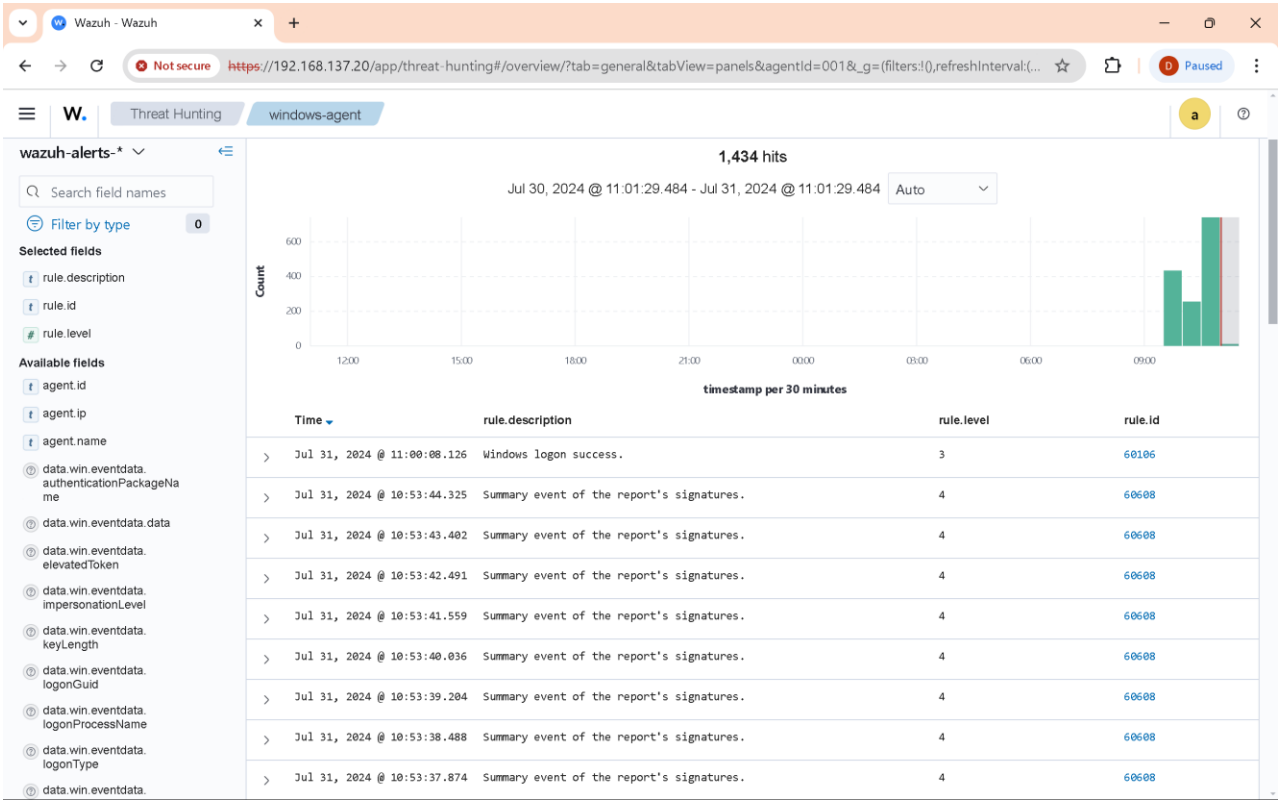

Wazuh - Wazuh
Not secure
https://192.168.137.20/app/mitre-attack#/overview/?tab=mitre&tabView=panels&agentId=001&_g=(filters:!(),refreshInterval:(paus...
Paused
MITRE ATT&CK
windows-agent
Dashboard
Intelligence
Framework
Events
windows-agent (001)
Generate report
Search
DQL
Last 24 hours
Show dates
Refresh
manager.name: wazuh-server
rule.mitre.id: exists
agent.id: 001
+ Add filter
Alerts evolution over time
Count
timestamp per 30 minutes
Valid Accounts
Disable or Modify To···
Domain Policy Modifi···
Account Access Remo···
Account Manipulation
Top tactics
Defense Evasion
Privilege Escalation
Persistence
Initial Access
Impact
Rule level by attack
MITRE attacks by tactic
Rule level by tactic

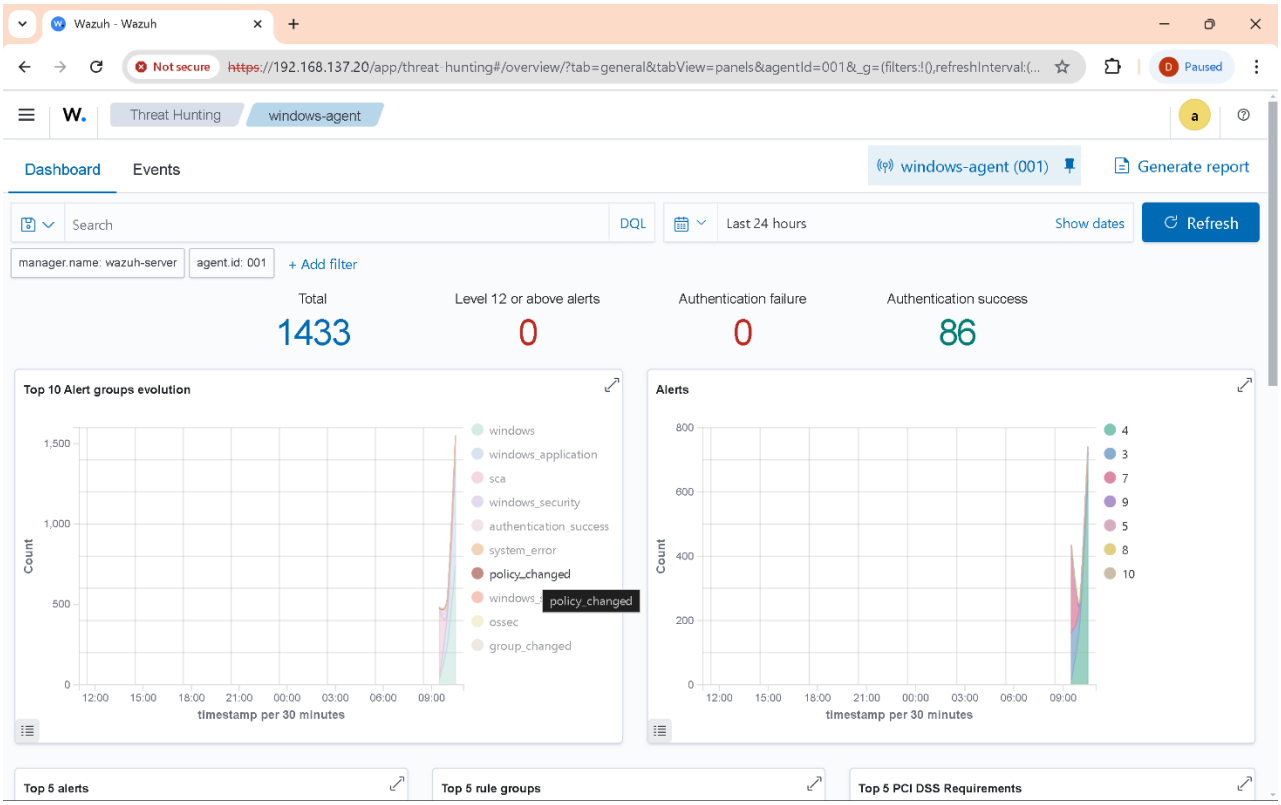

Wazuh - Wazuh
Not secure
https://192.168.137.20/app/endpoints-summary#/agents-preview/?_g=(filters:!(),refreshInterval:(pause:!t,value:0),time:(from:now-24...
Paused
Endpoints
STATUS
Active (1)
Disconnected (0)
Pending (0)
Never connected (0)
DETAILS
Active
1
Disconnected
0
Pending
0
Never connected
0
Agents coverage
100.00%
Last enrolled agent
windows-agent
Most active agent
windows-agent
EVOLUTION
Last 24 hours
active
Count
timestamp per 10 m
Agents (1)
Deploy new agent
Refresh
Export formatted
status=active
WQL
Refresh
ID
Name
IP address
Group(s)
Operating system
Cluster node
Version
Status
Actions
001
windows-agent
10.0.2.15
default
Microsoft Windows 10 Pro 10.0.19045.3803
node01
v4.8.1
active
Rows per page: 10
1

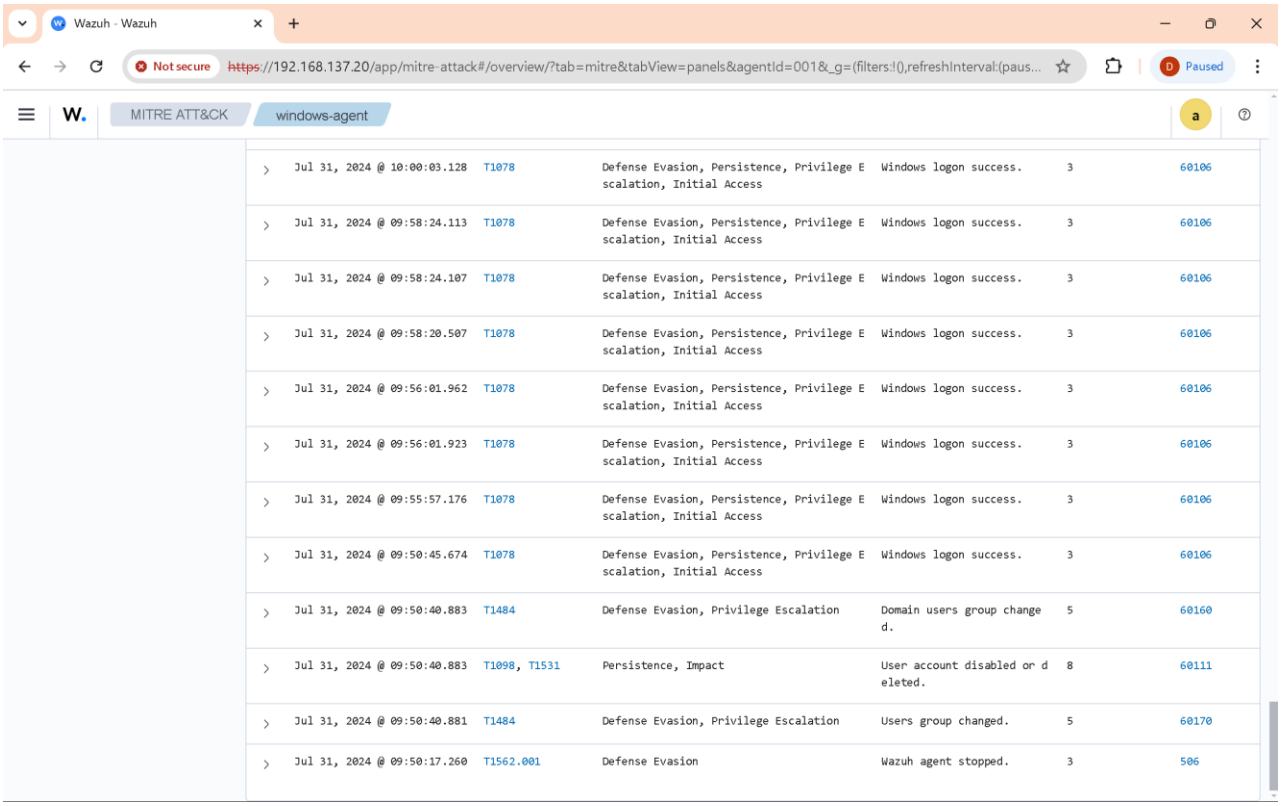

Wazuh - Wazuh
Not secure
https://192.168.137.20/app/endpoints-summary#/agents?tab=welcome&agent=001&tabView=panels&_g=(filters:!(),refreshInterva...
Paused
Endpoints
windows-agent
Threat Hunting
File Integrity Monitoring
More...
windows-agent (001)
Inventory data
Stats
Configuration
ID
001
Status
active
IP address
10.0.2.15
Version
v4.8.1
Groups
default
Operating system
Microsoft Windows 1...
Cluster node
node01
Registration date
Jul 31, 2024 @ 09:49:52.000
Last keep alive
Jul 31, 2024 @ 10:58:27.000
Last 24 hours
MITRE ATT&CK
Top Tactics
Defense Evasion 90
Privilege Escalation 88
Persistence 87
Initial Access 86
Impact 1
Compliance
PCI DSS
2.2 (396)
10.2.5 (153)
2.2.5 (53)
4.1 (44)
10.6.1 (26)
FIM: Recent events
Time
Path
Action
Rule desc...
Rule Le...
Rule Id
No recent events
Events count evolution
SCA: Lastest scans
CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0
cis_win10_enterprise


Wazuh - Wazuh
Not secure
https://192.168.137.20/app/wz-home#/overview/?_g=(filters:!(),refreshInterval:(pause:!t,value:0),time:(from:now-24h,to:now))&_a=(c...
Paused
Overview
AGENTS SUMMARY
Active (1)
Disconnected (0)
LAST 24 HOURS ALERTS
Critical severity
0
Rule level 15 or higher
High severity
0
Rule level 12 to 14
Medium severity
306
Rule level 7 to 11
Low severity
1168
Rule level 0 to 6
ENDPOINT SECURITY
Configuration Assessment
Scan your assets as part of a configuration assessment audit.
Malware Detection
Verify that your systems are configured according to your security policies baseline.
File Integrity Monitoring
Alerts related to file changes, including permissions, content, ownership, and attributes.
THREAT INTELLIGENCE
Threat Hunting
Browse through your security alerts, identifying issues and threats in your environment.
Vulnerability Detection
Discover what applications in your environment are affected by well-known vulnerabilities.
MITRE ATT&CK
Security events from the knowledge base of adversary tactics and techniques based on real-world observations.
VirusTotal
Alerts resulting from VirusTotal analysis of suspicious files via an integration with their API.
SECURITY OPERATIONS
CLOUD SECURITY

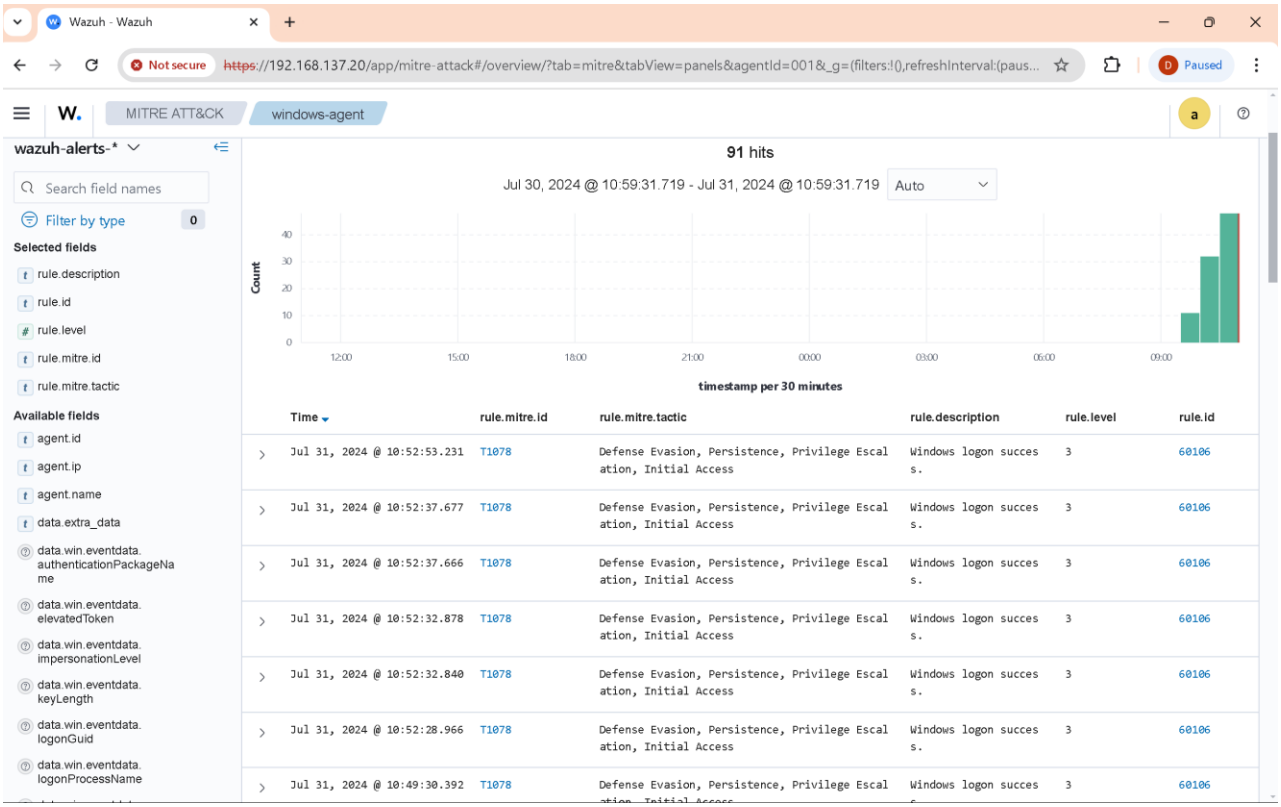

Wazuh - Wazuh
Not secure
https://192.168.137.20/app/mitre-attack#/overview/?tab=mitre&tabView=panels&agentId=001&_g=(filters:!(),refreshInterval:(paus...
Paused
MITRE ATT&CK
windows-agent
Dashboard
Intelligence
Framework
Events
windows-agent (001)
Search
DQL
Last 24 hours
Show dates
Refresh
manager.name: wazuh-server
rule.mitre.id: exists
agent.id: 001
+ Add filter
Tactics
Defense Evasion 91
Privilege Escalat... 89
Persistence 88
Initial Access 87
Impact 1
Credential Access 0
Execution 0
Lateral Movement 0
Techniques
Hide techniques with no alerts
Filter techniques of selected tactic/s
T1078 - Valid Accounts 87
T1484 - Domain Policy Modifi... 2
T1562.001 - Disable or Modif... 2
T1531 - Account Access Rem... 1
T1098 - Account Manipulation 1
T1557 - Adversary-in-the-Mid... 0
T1556.003 - Pluggable Authe... 0
T1056.001 - Keylogging 0
T1110.001 - Password Guessing 0
T1003 - OS Credential Dumpi... 0
T1171 - LLMNR/NBT-NS Pois... 0
T1539 - Steal Web Session Co... 0
T1003.002 - Security Account ... 0
T1552.005 - Cloud Instance M... 0
T1555.002 - Securityd Memory 0
T1522 - Cloud Instance Metad... 0
T1110.002 - Password Cracking 0
T1555.001 - Keychain 0
T1003.004 - LSA Secrets 0
T1606.002 - SAML Tokens 0
T1167 - Securityd Memory 0
T1214 - Credentials in Registry 0
T1003.007 - Proc Filesystem 0
T1555.005 - Password Manag... 0
T1040 - Network Sniffing 0
T1552.002 - Credentials in Re... 0
T1556.002 - Password Filter DLL 0
T1558.004 - AS-REP Roasting 0

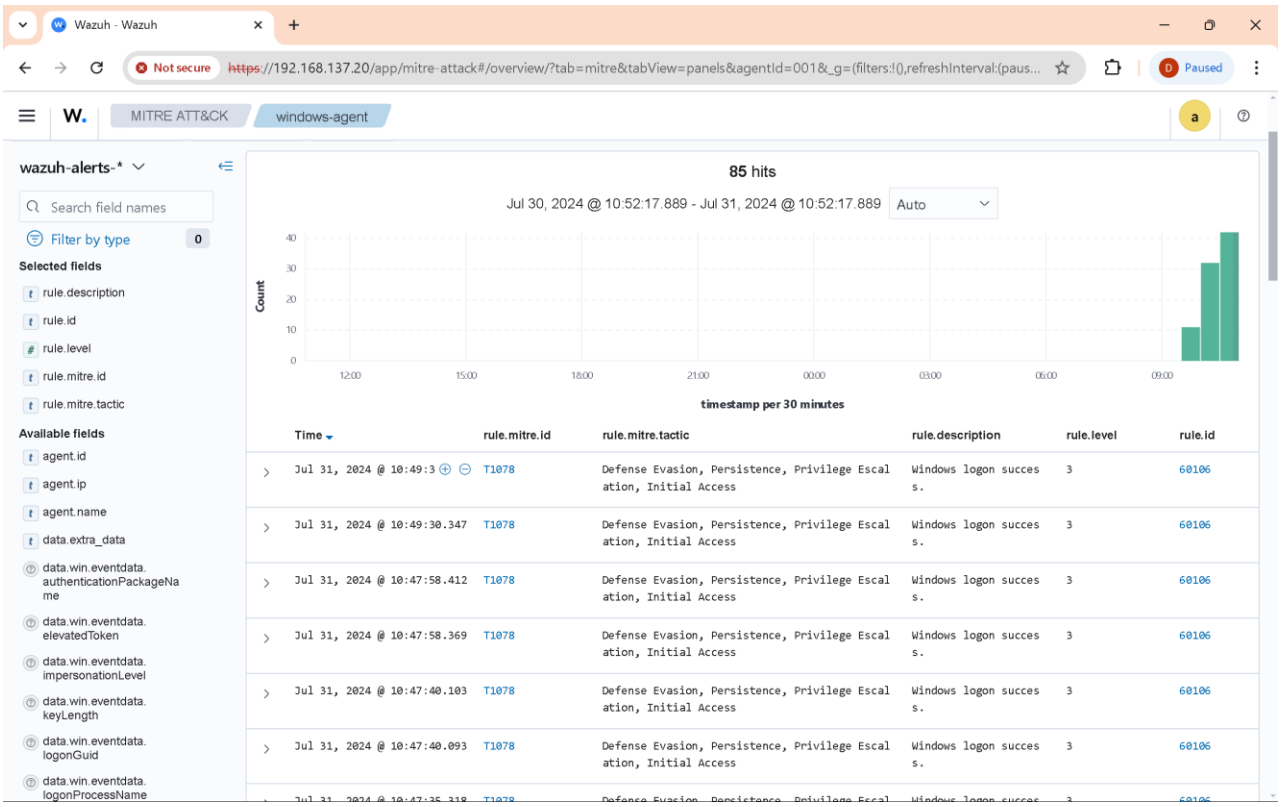

Wazuh - Wazuh
Not secure
https://192.168.137.20/app/threat-hunting#/overview/?tab=general&tabView=panels&agentId=001&_g=(filters:!(),refreshInterval:(...
Paused
Threat Hunting
windows-agent
wazuh-alerts-*
Search field names
Filter by type
0
Selected fields
rule.description
rule.id
rule.level
Available fields
agent.id
agent.ip
agent.name
data.win.eventdata.authenticationPackageName
data.win.eventdata.data
data.win.eventdata.elevatedToken
data.win.eventdata.impersonationLevel
data.win.eventdata.keyLength
data.win.eventdata.logonGuid
data.win.eventdata.logonProcessName
data.win.eventdata.logonType
data.win.eventdata.
1,434 hits
Jul 30, 2024 @ 11:01:29.484 - Jul 31, 2024 @ 11:01:29.484
Auto
Count
600
400
200
0
12:00
15:00
18:00
21:00
00:00
03:00
06:00
09:00
timestamp per 30 minutes
Time
rule.description
rule.level
rule.id
Jul 31, 2024 @ 11:00:08.126 Windows logon success. 3 60106
Jul 31, 2024 @ 10:53:44.325 Summary event of the report's signatures. 4 60608
Jul 31, 2024 @ 10:53:43.402 Summary event of the report's signatures. 4 60608
Jul 31, 2024 @ 10:53:42.491 Summary event of the report's signatures. 4 60608
Jul 31, 2024 @ 10:53:41.559 Summary event of the report's signatures. 4 60608
Jul 31, 2024 @ 10:53:40.036 Summary event of the report's signatures. 4 60608
Jul 31, 2024 @ 10:53:39.204 Summary event of the report's signatures. 4 60608
Jul 31, 2024 @ 10:53:38.488 Summary event of the report's signatures. 4 60608
Jul 31, 2024 @ 10:53:37.874 Summary event of the report's signatures. 4 60608

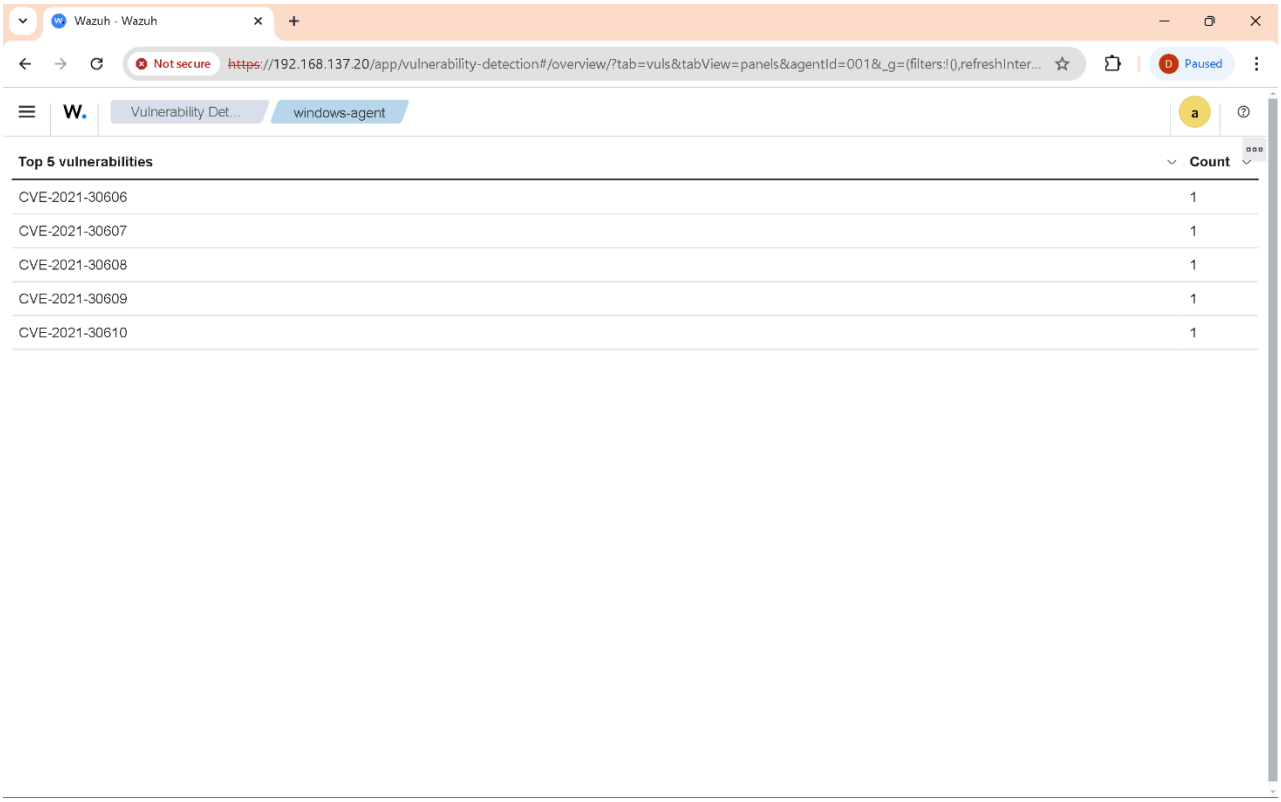

Wazuh - Wazuh
Not secure
https://192.168.137.20/app/threat-hunting#/overview/?tab=general&tabView=panels&agentId=001&_g=(filters:!(),refreshInterval:(...
Paused
Threat Hunting
windows-agent
Dashboard
Events
windows-agent (001)
Generate report
Search
DQL
Last 24 hours
Show dates
Refresh
manager.name: wazuh-server
agent.id: 001
+ Add filter
Total
1433
Level 12 or above alerts
0
Authentication failure
0
Authentication success
86
Top 10 Alert groups evolution
Count
timestamp per 30 minutes
windows
windows_application
sca
windows_security
authentication_success
system_error
policy_changed
ossec
group_changed
policy_changed
Alerts
Count
timestamp per 30 minutes
Top 5 alerts
Top 5 rule groups
Top 5 PCI DSS Requirements



Jul 31, 2024 @ 10:00:03.128	T1078	Defense Evasion, Persistence, Privilege Escalation, Initial Access	Windows logon success.	3	60106
Jul 31, 2024 @ 09:58:24.113	T1078	Defense Evasion, Persistence, Privilege Escalation, Initial Access	Windows logon success.	3	60106
Jul 31, 2024 @ 09:58:24.107	T1078	Defense Evasion, Persistence, Privilege Escalation, Initial Access	Windows logon success.	3	60106
Jul 31, 2024 @ 09:58:20.507	T1078	Defense Evasion, Persistence, Privilege Escalation, Initial Access	Windows logon success.	3	60106
Jul 31, 2024 @ 09:56:01.962	T1078	Defense Evasion, Persistence, Privilege Escalation, Initial Access	Windows logon success.	3	60106
Jul 31, 2024 @ 09:56:01.923	T1078	Defense Evasion, Persistence, Privilege Escalation, Initial Access	Windows logon success.	3	60106
Jul 31, 2024 @ 09:55:57.176	T1078	Defense Evasion, Persistence, Privilege Escalation, Initial Access	Windows logon success.	3	60106
Jul 31, 2024 @ 09:50:45.674	T1078	Defense Evasion, Persistence, Privilege Escalation, Initial Access	Windows logon success.	3	60106
Jul 31, 2024 @ 09:50:40.883	T1484	Defense Evasion, Privilege Escalation	Domain users group changed.	5	60160
Jul 31, 2024 @ 09:50:40.883	T1098, T1531	Persistence, Impact	User account disabled or deleted.	8	60111
Jul 31, 2024 @ 09:50:40.881	T1484	Defense Evasion, Privilege Escalation	Users group changed.	5	60170
Jul 31, 2024 @ 09:50:17.260	T1562.001	Defense Evasion	Wazuh agent stopped.	3	506


Wazuh - Wazuh
Not secure https://192.168.137.20/app/mitre-attack#/overview/?tab=mitre&tabView=panels&agentId=001&_g=(filters:!(),refreshInterval:(paus...
Paused
MITRE ATT&CK
windows-agent
wazuh-alerts-*
Search field names
Filter by type
0
Selected fields
rule.description
rule.id
rule.level
rule.mitre.id
rule.mitre.tactic
Available fields
agent.id
agent.ip
agent.name
data.extra_data
data.win.eventdata.authenticationPackageName
data.win.eventdata.elevatedToken
data.win.eventdata.impersonationLevel
data.win.eventdata.keyLength
data.win.eventdata.logonGuid
data.win.eventdata.logonProcessName
91 hits
Jul 30, 2024 @ 10:59:31.719 - Jul 31, 2024 @ 10:59:31.719
Auto
Count
timestamp per 30 minutes
Time
rule.mitre.id
rule.mitre.tactic
rule.description
rule.level
rule.id
Jul 31, 2024 @ 10:52:53.231 T1078 Defense Evasion, Persistence, Privilege Escalation, Initial Access Windows logon success. 3 60106
Jul 31, 2024 @ 10:52:37.677 T1078 Defense Evasion, Persistence, Privilege Escalation, Initial Access Windows logon success. 3 60106
Jul 31, 2024 @ 10:52:37.666 T1078 Defense Evasion, Persistence, Privilege Escalation, Initial Access Windows logon success. 3 60106
Jul 31, 2024 @ 10:52:32.878 T1078 Defense Evasion, Persistence, Privilege Escalation, Initial Access Windows logon success. 3 60106
Jul 31, 2024 @ 10:52:32.840 T1078 Defense Evasion, Persistence, Privilege Escalation, Initial Access Windows logon success. 3 60106
Jul 31, 2024 @ 10:52:28.966 T1078 Defense Evasion, Persistence, Privilege Escalation, Initial Access Windows logon success. 3 60106
Jul 31, 2024 @ 10:49:30.392 T1078 Defense Evasion, Persistence, Privilege Escalation, Initial Access Windows logon success. 3 60106


Wazuh - Wazuh
Not secure https://192.168.137.20/app/mitre-attack#/overview/?tab=mitre&tabView=panels&agentId=001&_g=(filters:!(),refreshInterval:(paus...
Paused
MITRE ATT&CK
windows-agent
wazuh-alerts-*
Search field names
Filter by type
0
Selected fields
rule.description
rule.id
rule.level
rule.mitre.id
rule.mitre.tactic
Available fields
agent.id
agent.ip
agent.name
data.extra_data
data.win.eventdata.authenticationPackageName
data.win.eventdata.elevatedToken
data.win.eventdata.impersonationLevel
data.win.eventdata.keyLength
data.win.eventdata.logonGuid
data.win.eventdata.logonProcessName
85 hits
Jul 30, 2024 @ 10:52:17.889 - Jul 31, 2024 @ 10:52:17.889
Auto
Count
timestamp per 30 minutes
Time
rule.mitre.id
rule.mitre.tactic
rule.description
rule.level
rule.id
Jul 31, 2024 @ 10:49:3 T1078 Defense Evasion, Persistence, Privilege Escalation, Initial Access Windows logon success. 3 60106
Jul 31, 2024 @ 10:49:30.347 T1078 Defense Evasion, Persistence, Privilege Escalation, Initial Access Windows logon success. 3 60106
Jul 31, 2024 @ 10:47:58.412 T1078 Defense Evasion, Persistence, Privilege Escalation, Initial Access Windows logon success. 3 60106
Jul 31, 2024 @ 10:47:58.369 T1078 Defense Evasion, Persistence, Privilege Escalation, Initial Access Windows logon success. 3 60106
Jul 31, 2024 @ 10:47:40.103 T1078 Defense Evasion, Persistence, Privilege Escalation, Initial Access Windows logon success. 3 60106
Jul 31, 2024 @ 10:47:40.093 T1078 Defense Evasion, Persistence, Privilege Escalation, Initial Access Windows logon success. 3 60106



SUMMARY

Simulating Mimikatz Malware on a Windows 10 Machine for Detection by Wazuh SIEM and XDR

Mimikatz is a powerful post-exploitation tool often used by attackers to extract credentials and perform other malicious activities on Windows systems. To ensure your security infrastructure can detect and respond to such threats, simulating Mimikatz activity in a controlled environment is crucial. This simulation can help evaluate the effectiveness of your Wazuh SIEM (Security Information and Event Management) and XDR (Extended Detection and Response) solutions.

Setup and Preparation:

1. **Environment Preparation:** Create a controlled Windows 10 virtual machine (VM) for the simulation. Ensure this VM is isolated from your production network to prevent any accidental spread of the simulated threat.

2. Install Security Tools: Make sure Wazuh agents are installed and properly configured on the Windows 10 machine. Additionally, ensure your XDR solution is operational and integrated with Wazuh for comprehensive monitoring and response.

Simulating Mimikatz:

1. **Obtain Mimikatz**: Download the Mimikatz tool from a reputable source (such as GitHub) or from the official Mimikatz website. Use only the latest and verified version to reflect current threats accurately.

2. Execute Mimikatz: Run Mimikatz on the Windows 10 VM with specific commands that mimic real-world attack scenarios. Common commands include:

- privilege::debug to elevate privileges.
- sekurlsa::logonpasswords to dump credentials from memory.
- kerberos::ptt to manipulate Kerberos tickets.

Ensure you execute these commands under conditions similar to what attackers would use, such as running them from a

command prompt with administrative privileges.

Monitoring and Detection:

1. **Wazuh SIEM:** Wazuh should be configured to monitor the Windows event logs, particularly for signs of suspicious activities associated with Mimikatz. Look for event IDs related to privilege escalation, credential dumping, and process creations that are abnormal. Wazuh's rules and decoders can help in detecting these activities.

2. XDR Analysis: The XDR solution should be set up to correlate data from various sources, including endpoint activities, network traffic, and log data. It should generate alerts for anomalous behaviors indicative of Mimikatz usage, such as unusual credential access patterns or abnormal process behavior.

Validation and Response:

1. **Verify Detection:** Check if Wazuh and XDR systems successfully detect and alert on the simulated Mimikatz activities. Ensure that alerts are generated and are actionable.

2. Review Logs and Alerts: Analyze the generated logs and alerts to verify that the detection rules are effective and that any false positives or negatives are identified.

Conclusion:

Simulating Mimikatz on a Windows 10 machine provides

valuable insights into the effectiveness of your Wazuh SIEM and XDR solutions. By carefully analyzing the detection capabilities and response actions, you can fine-tune your security measures to better protect against real-world threats. Regular simulations and updates to detection rules are essential to stay ahead of evolving attack techniques.

PROJECT REVIEW 100% COMPLETED

TRAINER : ZEESHAN FAROOQ