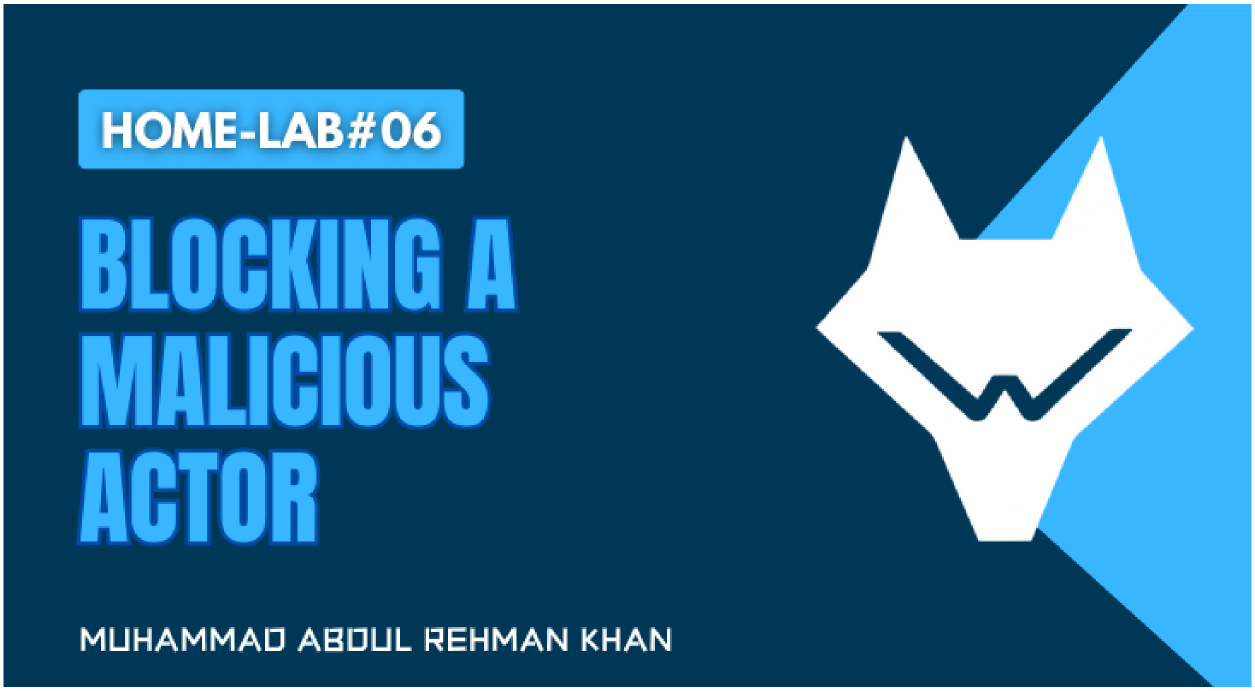
PREPARED BY: MUHAMMAD ABDUL REHMAN KHAN



LAB OUTLINE:

- Who is a Malware Actor?
- Requirement
- Setting up Wazuh Manager
- Adding Windows Agent to Wazuh
- Setting up Malware Actor
- Visualization
- Conclusion

Who is a MALICIOUS ACTOR?

A malicious actor is an individual, group, or entity that deliberately engages in harmful activities aimed at disrupting systems, stealing sensitive information, or causing damage to organizations or individuals. These actors may use various techniques such as hacking, phishing, deploying malware, exploiting vulnerabilities, or launching attacks like ransomware or denial-of-service (DoS). Malicious actors can include cybercriminals seeking financial gain, hacktivists pushing political agendas, insider threats with access to critical systems, or nation-state groups conducting cyber espionage or warfare. Their actions often pose significant risks to system security, data integrity, and organizational reputation.

REQUIREMENTS:

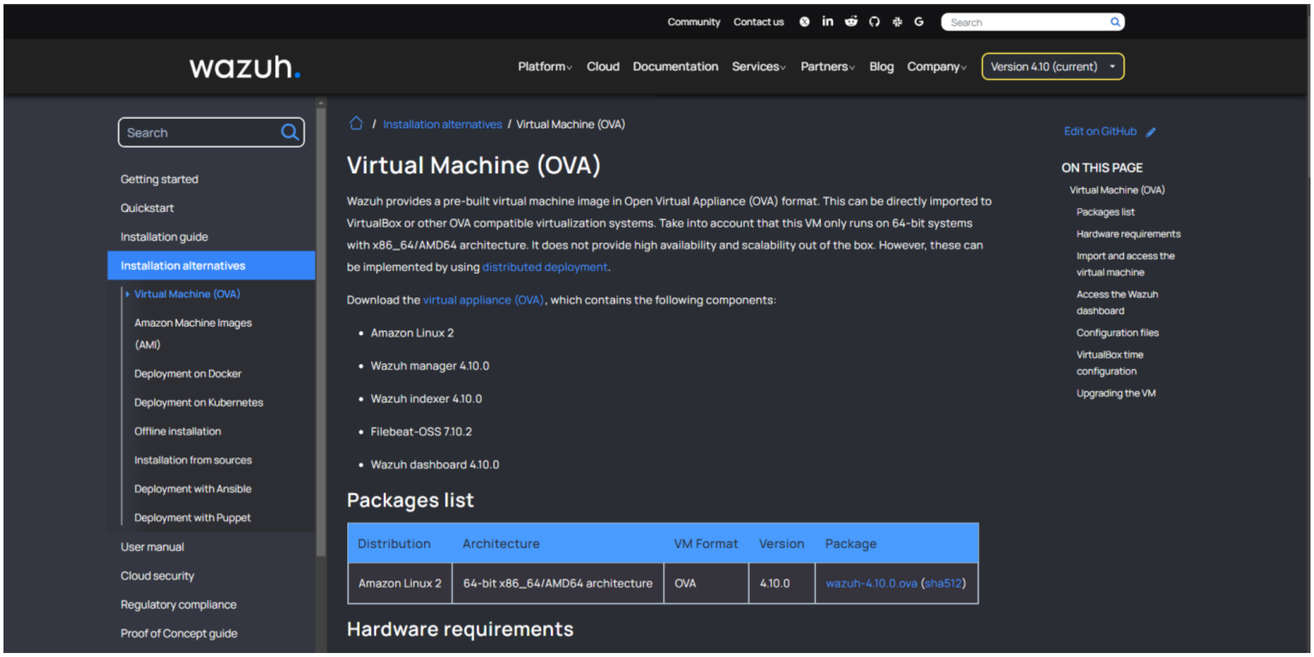
To set up our Home-lab, we need platforms and tools as mentioned below:

- VirtualBox
- Windows 10VM
- Kali Linux VM
- Wazuh OVA File

SETTING UP WAZUH MANAGER:

For Home-lab, it is convenient to use Wazuh OVA file. Visit their official website the file

(*https://documentation.wazuh.com/current/deployment-options/virtual-machine/virtual-machine.html*)



Virtual Machine (OVA)

Wazuh provides a pre-built virtual machine image in Open Virtual Appliance (OVA) format. This can be directly imported to VirtualBox or other OVA compatible virtualization systems. Take into account that this VM only runs on 64-bit systems with x86_64/AMD64 architecture. It does not provide high availability and scalability out of the box. However, these can be implemented by using distributed deployment.

Download the virtual appliance (OVA), which contains the following components:

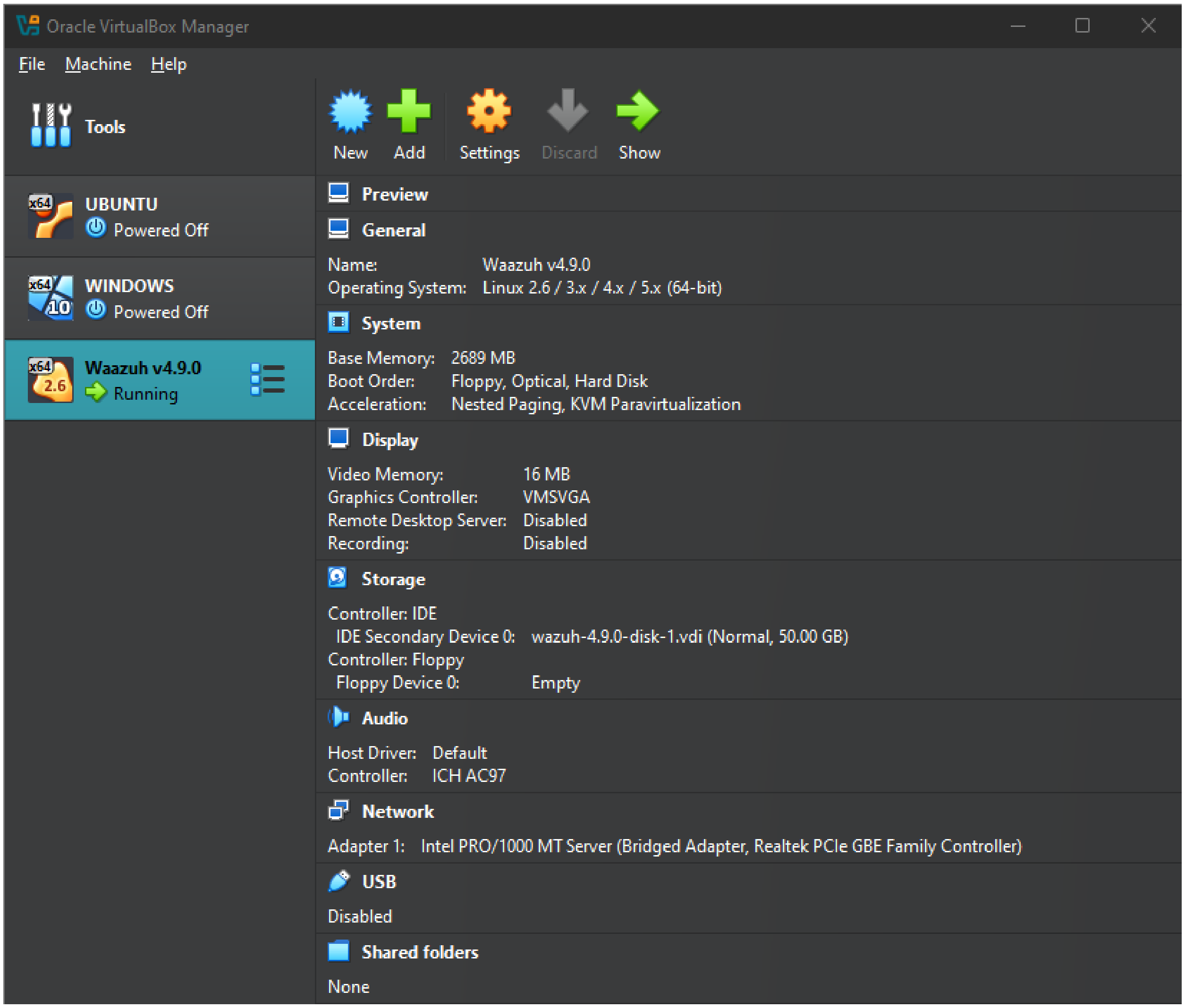
- Amazon Linux 2
- Wazuh manager 4.10.0
- Wazuh indexer 4.10.0
- Filebeat-OSS 7.10.2
- Wazuh dashboard 4.10.0

Packages list

Distribution	Architecture	VM Format	Version	Package
Amazon Linux 2	64-bit x86_64/AMD64 architecture	OVA	4.10.0	wazuh-4.10.0.ova (sha512)

Hardware requirements

Open the file in VirtualBox and start the Virtual Machine



General

Name: Waazuh v4.9.0
Operating System: Linux 2.6 / 3.x / 4.x / 5.x (64-bit)

System

Base Memory: 2689 MB
Boot Order: Floppy, Optical, Hard Disk
Acceleration: Nested Paging, KVM Paravirtualization

Display

Video Memory: 16 MB
Graphics Controller: VMSVGA
Remote Desktop Server: Disabled
Recording: Disabled

Storage

Controller: IDE
 IDE Secondary Device 0: wazuh-4.9.0-disk-1.vdi (Normal, 50.00 GB)
Controller: Floppy
 Floppy Device 0: Empty

Audio

Host Driver: Default
Controller: ICH AC97

Network

Adapter 1: Intel PRO/1000 MT Server (Bridged Adapter, Realtek PCIe GBE Family Controller)

USB

Disabled

Shared folders

None

Now, log in to Wazuh CLI and run ***ifconfig*** to get the IP address. The default Wazuh CLI credential is:

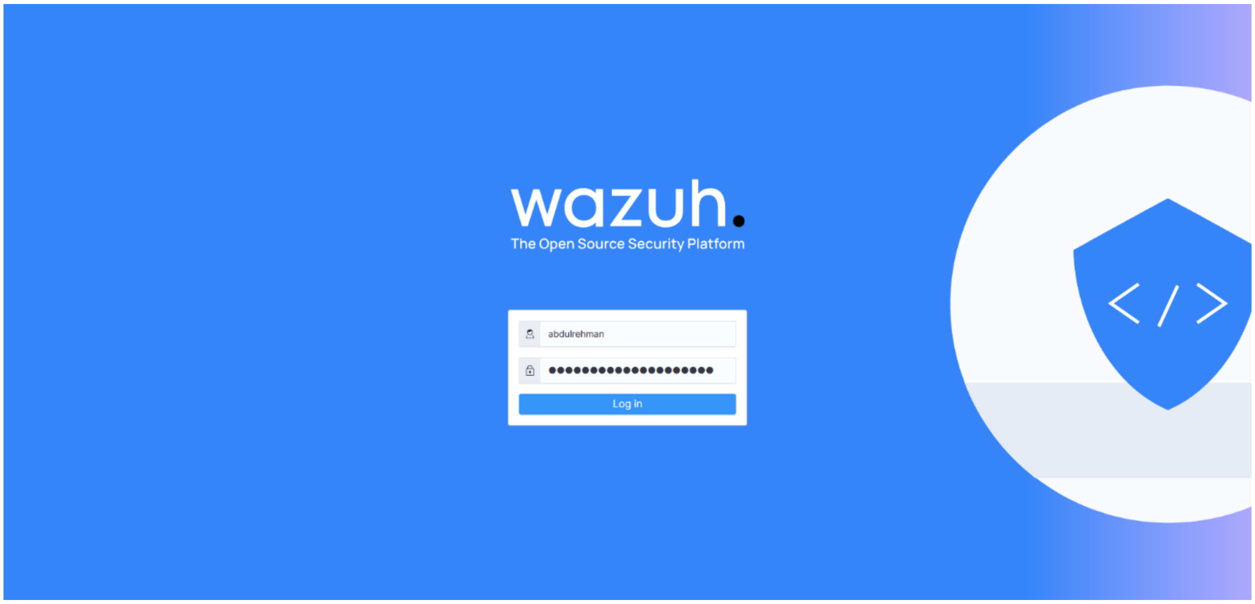
> **username:** *wazuh-user*
>
> **password:** *wazuh*

Once, you have the IP address, open your favourite browser and submit the URL:

> ***https://<WAZUH_IP_ADDRESS>***

Next, enter the Wazuh GUI credential as shown below

> **username:** *admin*
>
> **password:** *admin*



abdulrehman

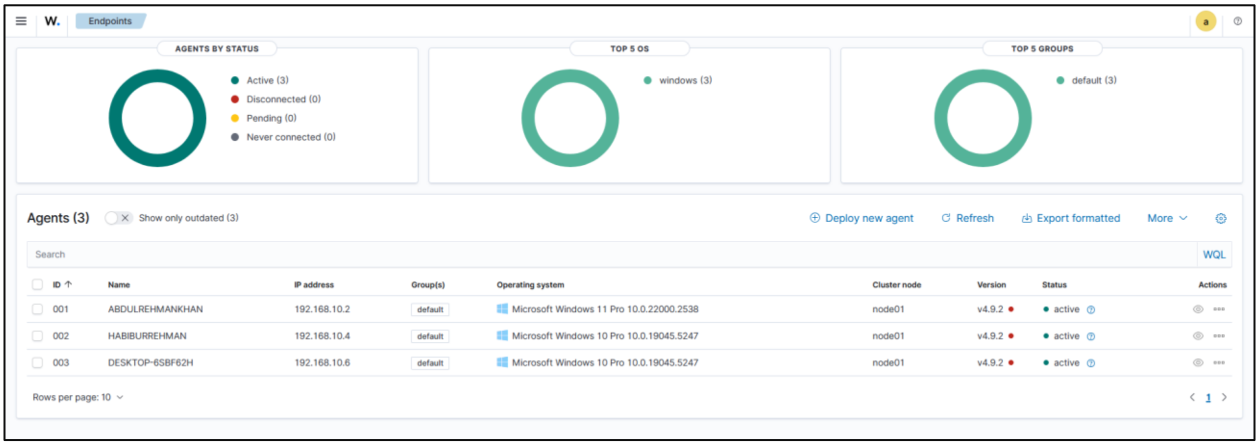
●●●●●●●●●●●●●●●●●●●●●

You are successfully logged-in to your WAZUH dashboard.

ADDING WINDOWS MACHINE TO WAZUH:

If your host OS is Windows, you can go for installing locally or else you can download the Windows 10/11 Virtual Edition from Microsoft's official ***website***.

Step1: Once your Windows 10 machine is ready, visit the Wazuh platform using GUI. Go to Agents and click on Deploy new agent, as shown below.

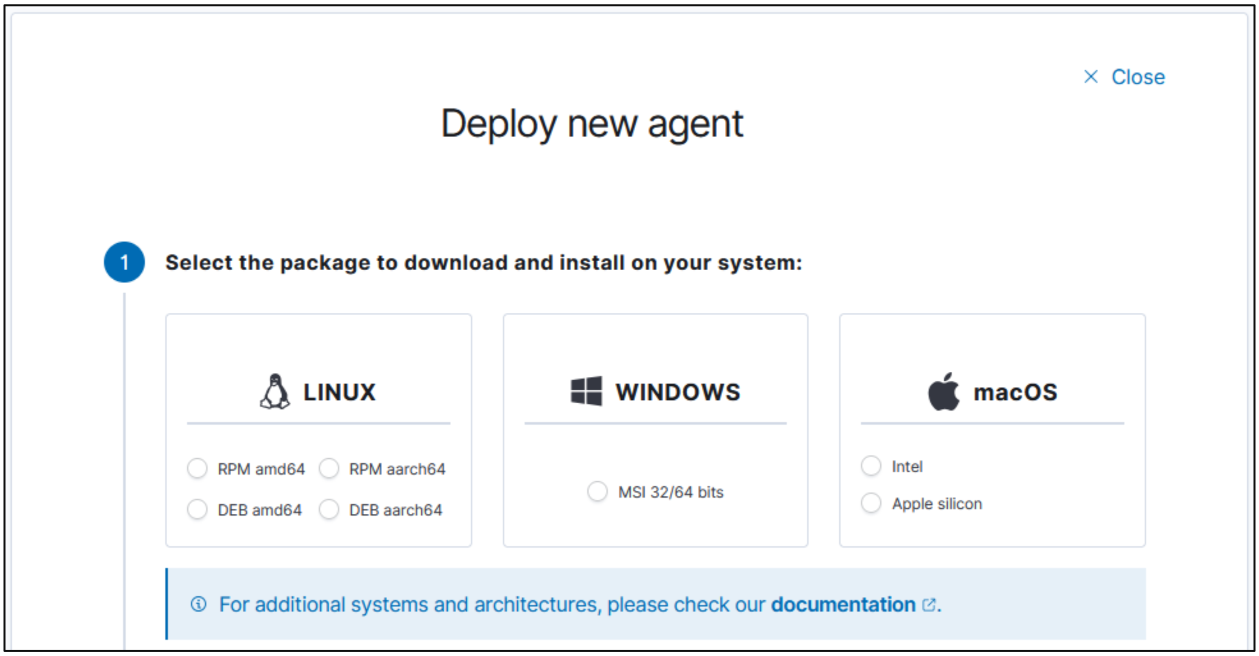


Agents (3) Show only outdated (3)

ID ↑	Name	IP address	Group(s)	Operating system	Cluster node	Version	Status	Actions
001	ABDULREHMANKHAN	192.168.10.2	default	Microsoft Windows 11 Pro 10.0.22000.2538	node01	v4.9.2 ●	● active	
002	HABIBURREHMAN	192.168.10.4	default	Microsoft Windows 10 Pro 10.0.19045.5247	node01	v4.9.2 ●	● active	
003	DESKTOP-6SBF62H	192.168.10.6	default	Microsoft Windows 10 Pro 10.0.19045.5247	node01	v4.9.2 ●	● active	

Rows per page: 10

Step2: Next, select an Operating system, enter your Wazuh Server address, and set your agent name as shown below.



Deploy new agent

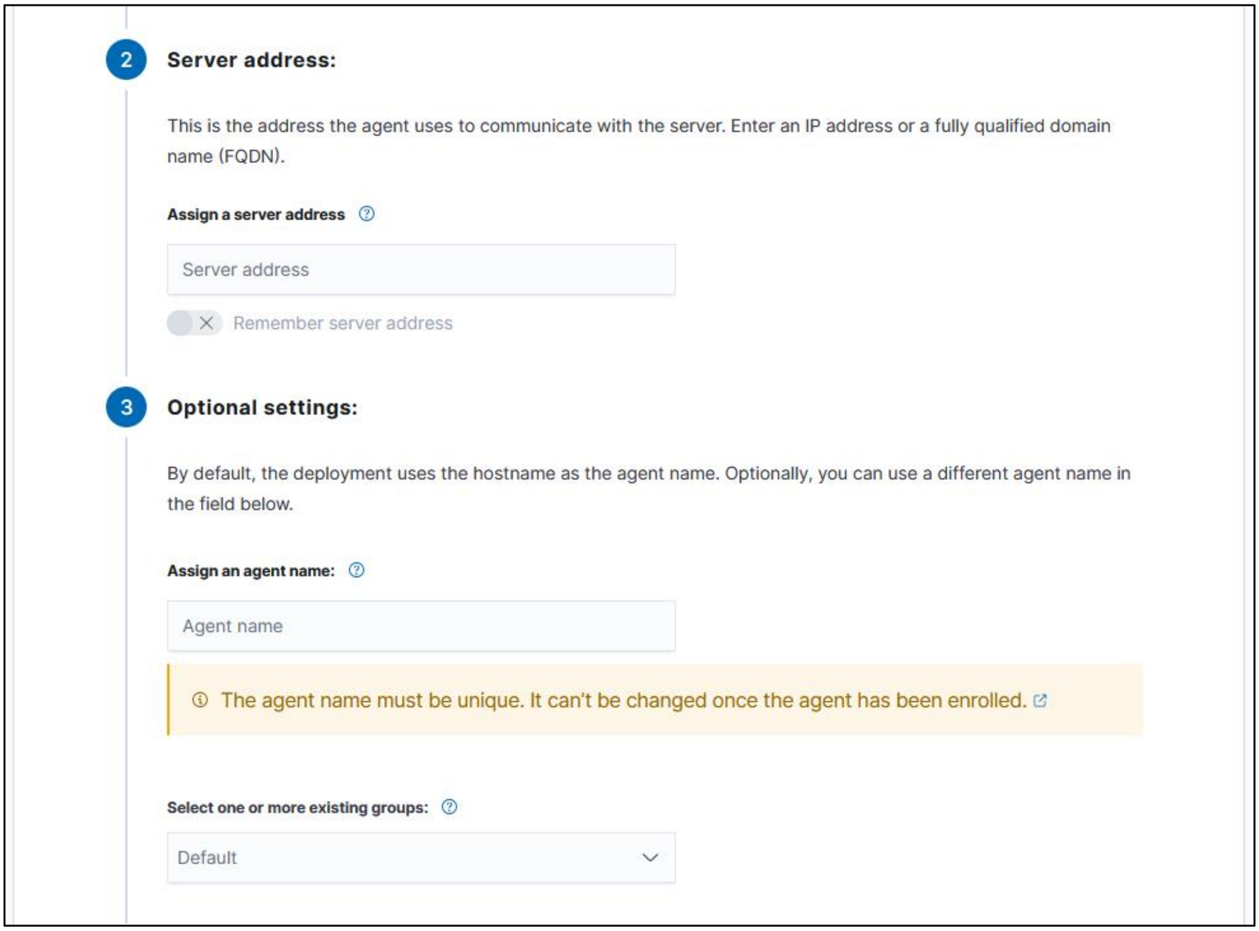
1 Select the package to download and install on your system:

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 (FQDN).

Assign a 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.

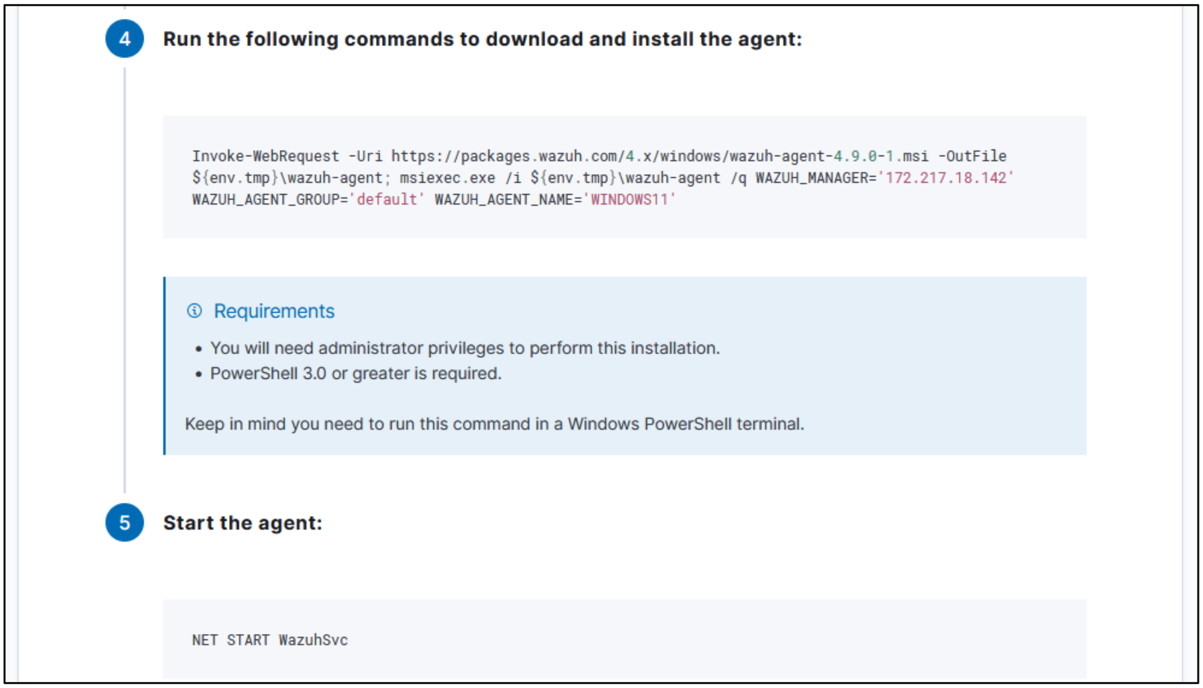
Assign an agent name: ⓘ

ⓘ The agent name must be unique. It can't be changed once the agent has been enrolled.

Select one or more existing groups: ⓘ

Default

Step3: In the end, you will get a PowerShell script & a command to start the Wazuh service on your agent, as shown below.



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

```
Invoke-WebRequest -Uri https://packages.wazuh.com/4.x/windows/wazuh-agent-4.9.0-1.msi -OutFile
${env.tmp}\wazuh-agent; msiexec.exe /i ${env.tmp}\wazuh-agent /q WAZUH_MANAGER='172.217.18.142'
WAZUH_AGENT_GROUP='default' WAZUH_AGENT_NAME='WINDOWS11'
```

ⓘ Requirements

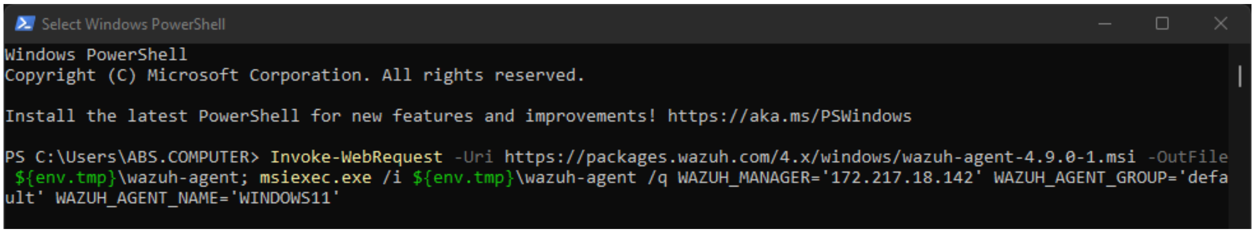
- You will need administrator privileges to perform this installation.
- PowerShell 3.0 or greater is required.

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

5 **Start the agent:**

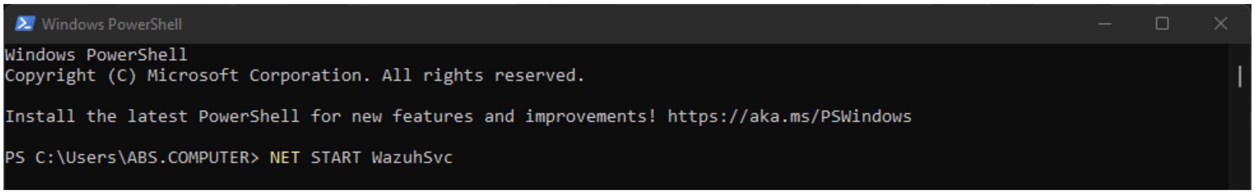
```
NET START WazuhSvc
```

Step4: Next, go to your Windows 10 Machine and the script in your PowerShell command prompt.



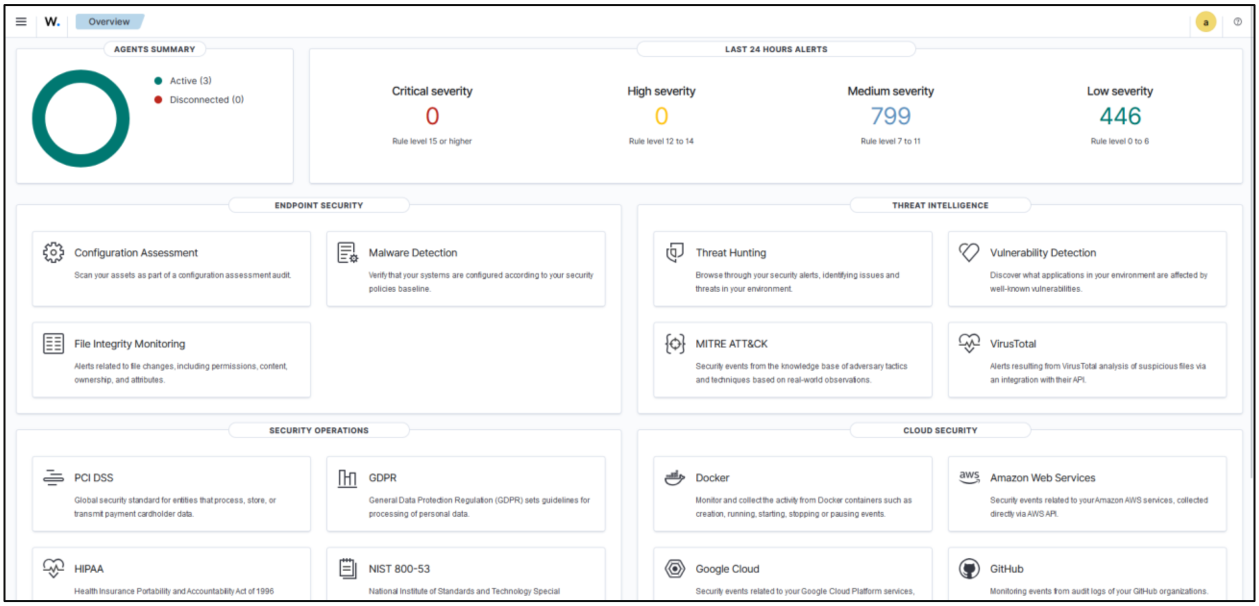
```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\ABS.COMPUTER> Invoke-WebRequest -Uri https://packages.wazuh.com/4.x/windows/wazuh-agent-4.9.0-1.msi -OutFile
 ${env.tmp}\wazuh-agent; msiexec.exe /i ${env.tmp}\wazuh-agent /q WAZUH_MANAGER='172.217.18.142' WAZUH_AGENT_GROUP='defa
ult' WAZUH_AGENT_NAME='WINDOWS11'
```

Step5: Next, start the Wazuh service.



```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\ABS.COMPUTER> NET START WazuhSvc
```

Step6: Finally, come back to your Wazuh platform and go to Agents; you should see your newly on boarded Windows agent here.



AGENTS SUMMARY

Active (3)
Disconnected (0)

LAST 24 HOURS ALERTS

Critical severity	High severity	Medium severity	Low severity
0	0	799	446
Rule level 15 or higher	Rule level 12 to 14	Rule level 7 to 11	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

PCI DSS
Global security standard for entities that process, store, or transmit payment cardholder data.

GDPR
General Data Protection Regulation (GDPR) sets guidelines for processing of personal data.

HIPAA
Health Insurance Portability and Accountability Act of 1996

NIST 800-53
National Institute of Standards and Technology Special

CLOUD SECURITY

Docker
Monitor and collect the activity from Docker containers such as creation, running, starting, stopping or pausing events.

Amazon Web Services
Security events related to your Amazon AWS services, collected directly via AWS API.

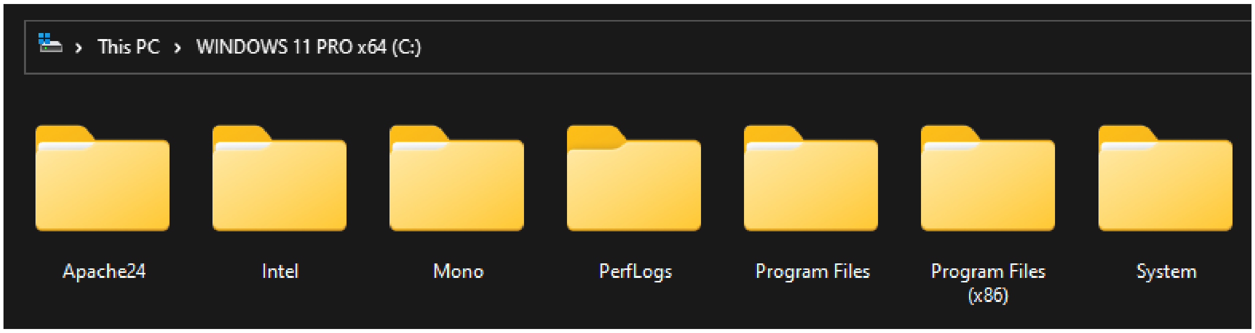
Google Cloud
Security events related to your Google Cloud Platform services,

GitHub
Monitoring events from audit logs of your GitHub organizations.

You have successfully boarded a new WINDOWS agent on your WAZUH dashboard.

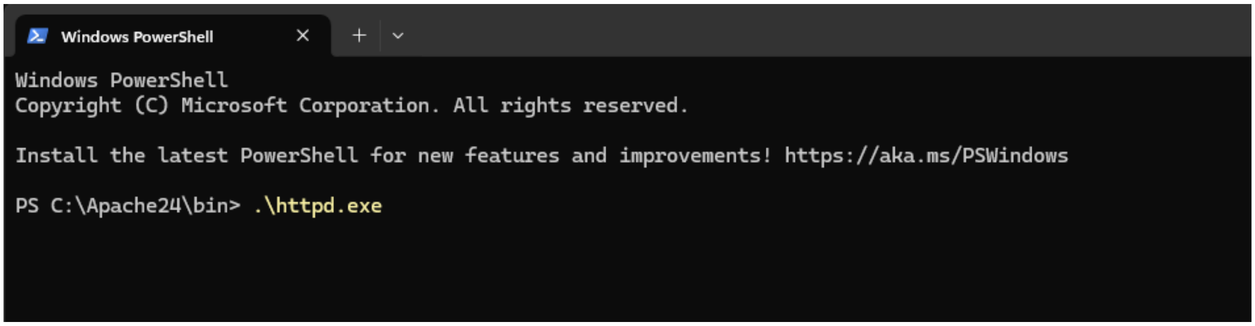
SETTING UP MALICIOUS ACTOR:

First, we create a Apache web server, for this install *Visual C++ Redistributable package* and Download the *Apache web server Win64 ZIP* installation file. Unzip the contents of the Apache web server zip file and copy the extracted Apache24 folder to the C: directory.



Navigate to the (*C:\Apache24\bin*) folder and run the following command in a PowerShell terminal with administrator privileges.

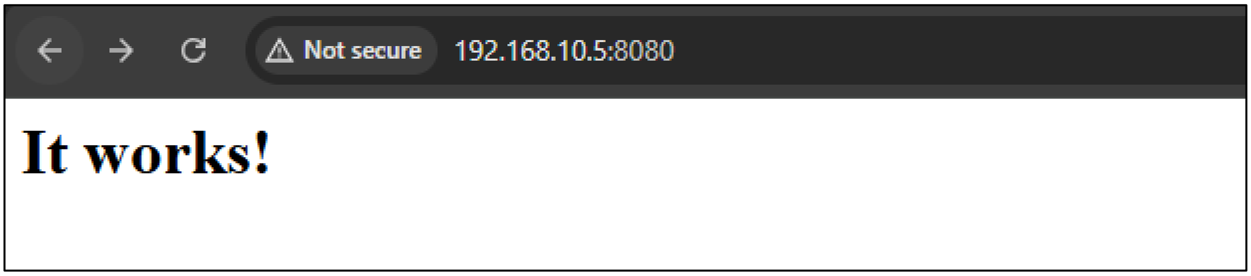
> **.\httpd.exe**



```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Apache24\bin> .\httpd.exe
```

Open (*http://<WINDOWS_IP>)* in a browser to view the Apache landing page and verify the installation. Also, verify that this URL can be reached from the attacker endpoint.

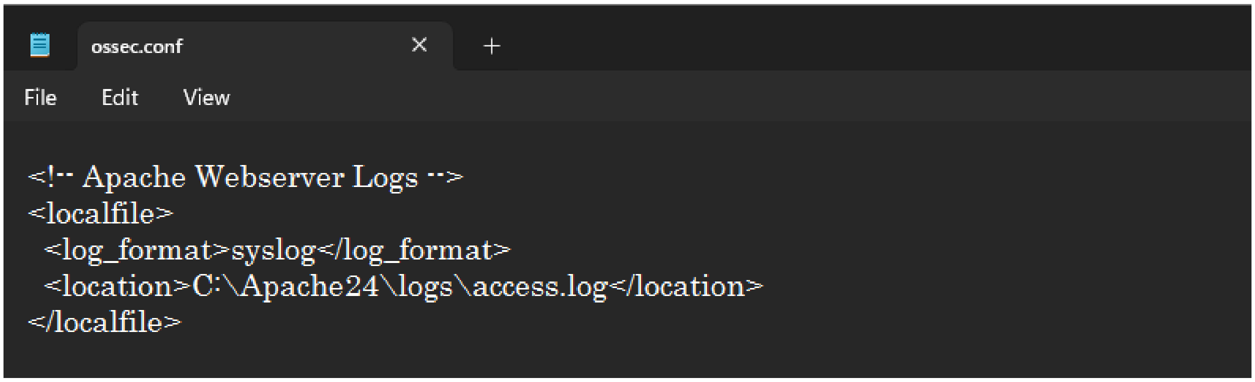
> ***https://< WINDOWS_IP_ADDRESS>***



It works!

Now, open (*ossec.conf*) file located at (*C:\Program Files (x86)\ossec-agent\ossec.conf*) and add the following block of configuration to configure the Wazuh agent and monitor the Apache access logs.

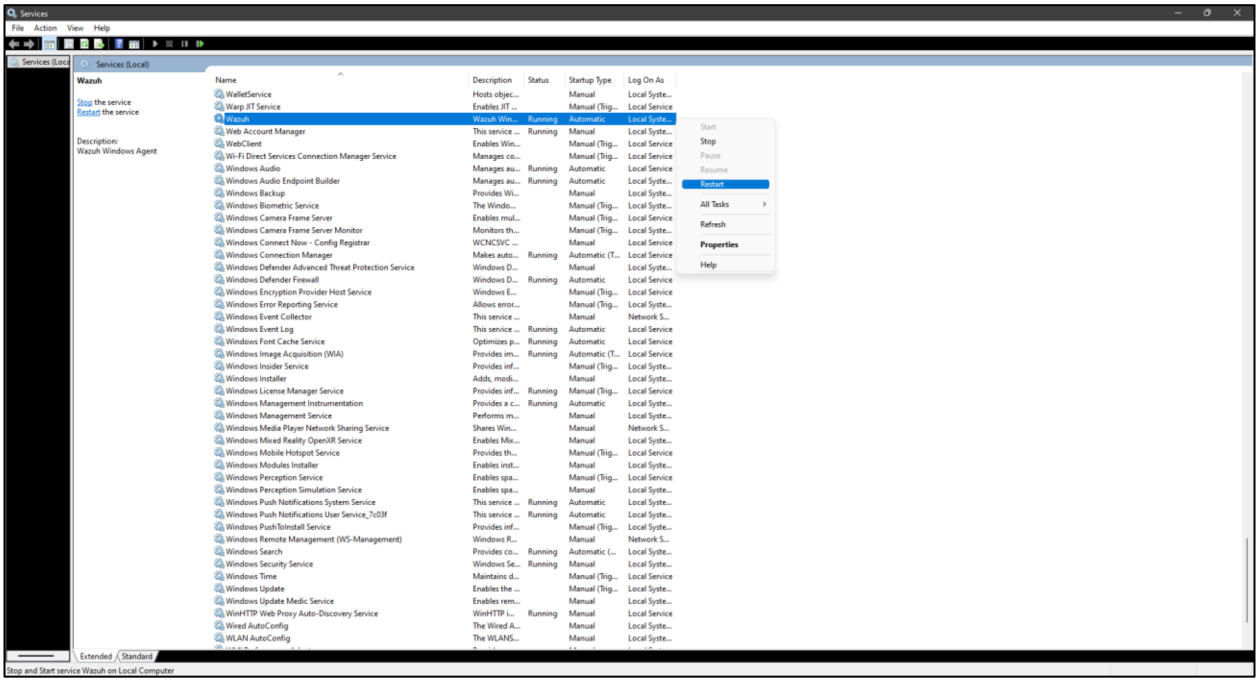
```
<localfile>
<log_format>syslog</log_format>
<location>C:\Apache24\logs\access.log</location>
</localfile>
```



```
<!-- Apache Webserver Logs -->
<localfile>
  <log_format>syslog</log_format>
  <location>C:\Apache24\logs\access.log</location>
</localfile>
```

Now, Go to (*Start>Services>Wazuh*), Right click on wazuh service and click on restart. OR, Simply type the following command in PowerShell terminal with administrator privileges to apply the changes.

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



Wazuh

Stop the service
Restart the service

Description:
Wazuh Windows Agent

Name	Description	Status	Startup Type	Log On As
WalletService	Hosts objec...		Manual	Local Syste...
Warp JIT Service	Enables JIT ...		Manual (Trig...	Local Service
Wazuh	Wazuh Win...	Running	Automatic	Local Syste...
Web Account Manager	This service ...	Running	Manual	Local Syste...
WebClient	Enables Win...		Manual (Trig...	Local Service
Wi-Fi Direct Services Connection Manager Service	Manages co...		Manual (Trig...	Local Service
Windows Audio	Manages au...	Running	Automatic	Local Service
Windows Audio Endpoint Builder	Manages au...	Running	Automatic	Local Syste...
Windows Backup	Provides Wi...		Manual	Local Syste...
Windows Biometric Service	The Windo...		Manual (Trig...	Local Syste...
Windows Camera Frame Server	Enables mul...		Manual (Trig...	Local Service
Windows Camera Frame Server Monitor	Monitors th...		Manual (Trig...	Local Syste...
Windows Connect Now - Config Registrar	WCNCSVC ...		Manual	Local Service
Windows Connection Manager	Makes auto...	Running	Automatic (T...	Local Service
Windows Defender Advanced Threat Protection Service	Windows D...		Manual	Local Syste...
Windows Defender Firewall	Windows D...	Running	Automatic	Local Service
Windows Encryption Provider Host Service	Windows E...		Manual (Trig...	Local Service
Windows Error Reporting Service	Allows error...		Manual (Trig...	Local Syste...
Windows Event Collector	This service ...		Manual	Network S...
Windows Event Log	This service ...	Running	Automatic	Local Service
Windows Font Cache Service	Optimizes p...	Running	Automatic	Local Service
Windows Image Acquisition (WIA)	Provides im...	Running	Automatic (T...	Local Service
Windows Insider Service	Provides inf...		Manual (Trig...	Local Syste...
Windows Installer	Adds, modi...		Manual	Local Syste...
Windows License Manager Service	Provides inf...	Running	Manual (Trig...	Local Service
Windows Management Instrumentation	Provides a c...	Running	Automatic	Local Syste...
Windows Management Service	Performs m...		Manual	Local Syste...
Windows Media Player Network Sharing Service	Shares Win...		Manual	Network S...
Windows Mixed Reality OpenXR Service	Enables Mix...		Manual	Local Syste...
Windows Mobile Hotspot Service	Provides th...		Manual (Trig...	Local Service
Windows Modules Installer	Enables inst...		Manual	Local Syste...
Windows Perception Service	Enables spa...		Manual (Trig...	Local Service
Windows Perception Simulation Service	Enables spa...		Manual	Local Syste...
Windows Push Notifications System Service	This service ...	Running	Automatic	Local Syste...
Windows Push Notifications User Service_7c03f	This service ...	Running	Automatic	Local Syste...
Windows PushToInstall Service	Provides inf...		Manual (Trig...	Local Syste...
Windows Remote Management (WS-Management)	Windows R...		Manual	Network S...
Windows Search	Provides co...	Running	Automatic (...	Local Syste...
Windows Security Service	Windows Se...	Running	Manual	Local Syste...
Windows Time	Maintains d...		Manual (Trig...	Local Service
Windows Update	Enables the ...		Manual (Trig...	Local Syste...
Windows Update Medic Service	Enables rem...		Manual	Local Syste...
WinHTTP Web Proxy Auto-Discovery Service	WinHTTP i...	Running	Manual	Local Service
Wired AutoConfig	The Wired A...		Manual	Local Syste...
WLAN AutoConfig	The WLANS...		Manual	Local Syste...

Stop and Start service Wazuh on Local Computer

Now, Go WAZUH Server and run the following commands to download the utilities and configure the CDB list.

Install the wget utility to download the necessary artifacts using the command line interface.

> **sudo yum update && sudo yum install -y wget**

Download the Alienvault IP reputation database.

> **sudo wget https://raw.githubusercontent.com/firehol/blocklist-ipsets/master/alienvault_reputation.ipset -O /var/ossec/etc/lists/alienvault_reputation.ipset**

Append the IP address of the attacker endpoint to the IP reputation database. Replace <ATTACKER_IP> with the RHEL IP address in the command below.

```
sudo echo "<ATTACKER_IP>" >> /var/ossec/etc/lists/alienvault_reputation.ipset
```

Download a script to convert from the .ipset format to the .cdb list format.

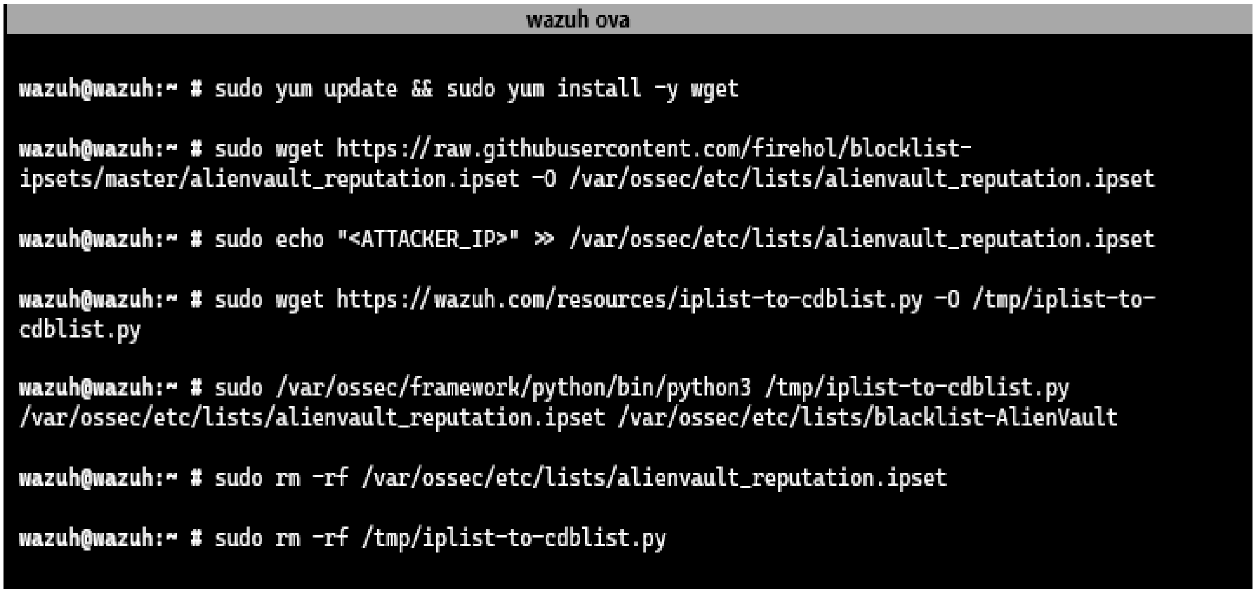
```
sudo wget https://wazuh.com/resources/iplist-to-cdblist.py -O /tmp/iplist-to-cdblist.py
```

Convert the alienvault_reputation.ipset file to a .cdb format using the previously downloaded script.

```
sudo /var/ossec/framework/python/bin/python3 /tmp/iplist-to-cdblist.py /var/ossec/etc/lists/alienvault_reputation.ipset /var/ossec/etc/lists/blacklist-alienvault
```

Optional: Remove the *alienvault_reputation.ipset* file and the *iplist-to-cdblist.py* script, as they are no longer needed.

```
sudo rm -rf /var/ossec/etc/lists/alienvault_reputation.ipset
sudo rm -rf /tmp/iplist-to-cdblist.py
```



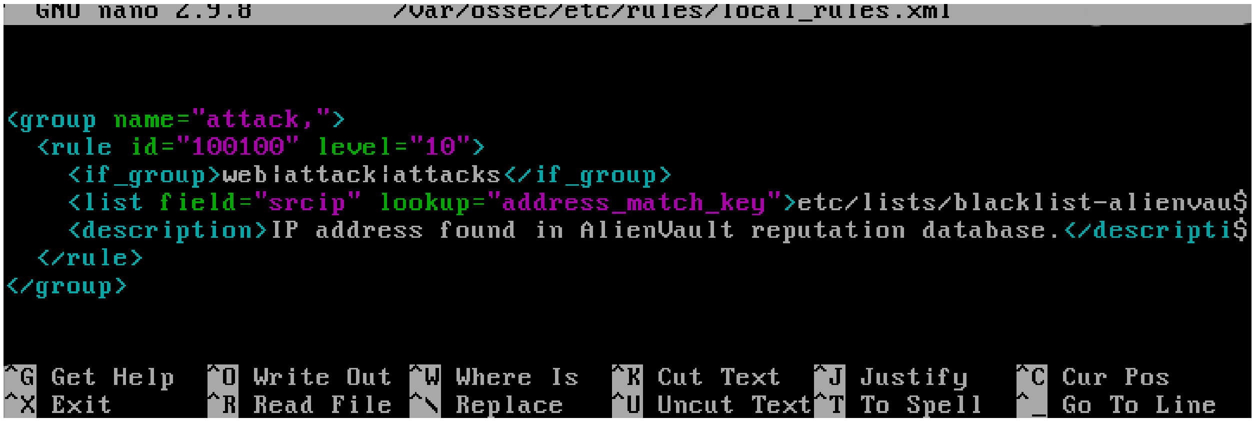
wazuh ova

```
wazuh@wazuh:~ # sudo yum update && sudo yum install -y wget

wazuh@wazuh:~ # sudo wget https://raw.githubusercontent.com/firehol/blocklist-
ipsets/master/alienvault_reputation.ipset -O /var/ossec/etc/lists/alienvault_reputation.ipset

wazuh@wazuh:~ # sudo echo "<ATTACKER_IP>" >> /var/ossec/etc/lists/alienvault_reputation.ipset

wazuh@wazuh:~ # sudo wget https://wazuh.com/resources/iplist-to-cdblist.py -O /tmp/iplist-to-
cdblist.py

wazuh@wazuh:~ # sudo /var/ossec/framework/python/bin/python3 /tmp/iplist-to-cdblist.py
/var/ossec/etc/lists/alienvault_reputation.ipset /var/ossec/etc/lists/blacklist-AlienVault

wazuh@wazuh:~ # sudo rm -rf /var/ossec/etc/lists/alienvault_reputation.ipset

wazuh@wazuh:~ # sudo rm -rf /tmp/iplist-to-cdblist.py
```

To Configure the Active Response module to block the malicious IP address, add a custom rule to trigger a Wazuh active response script.

Do this in the Wazuh server (*/var/ossec/etc/rules/local_rules.xml*) custom ruleset file.

> **<group name="attack,">**
> **<rule id="100100" level="10">**
> **<if_group>web|attack|attacks</if_group>**
> **<list field="srcip" lookup="address_match_key">etc/lists/blacklist-alienvault</list>**
> **<description>IP address found in AlienVault reputation database.</description>**
> **</rule>**
> **</group>**

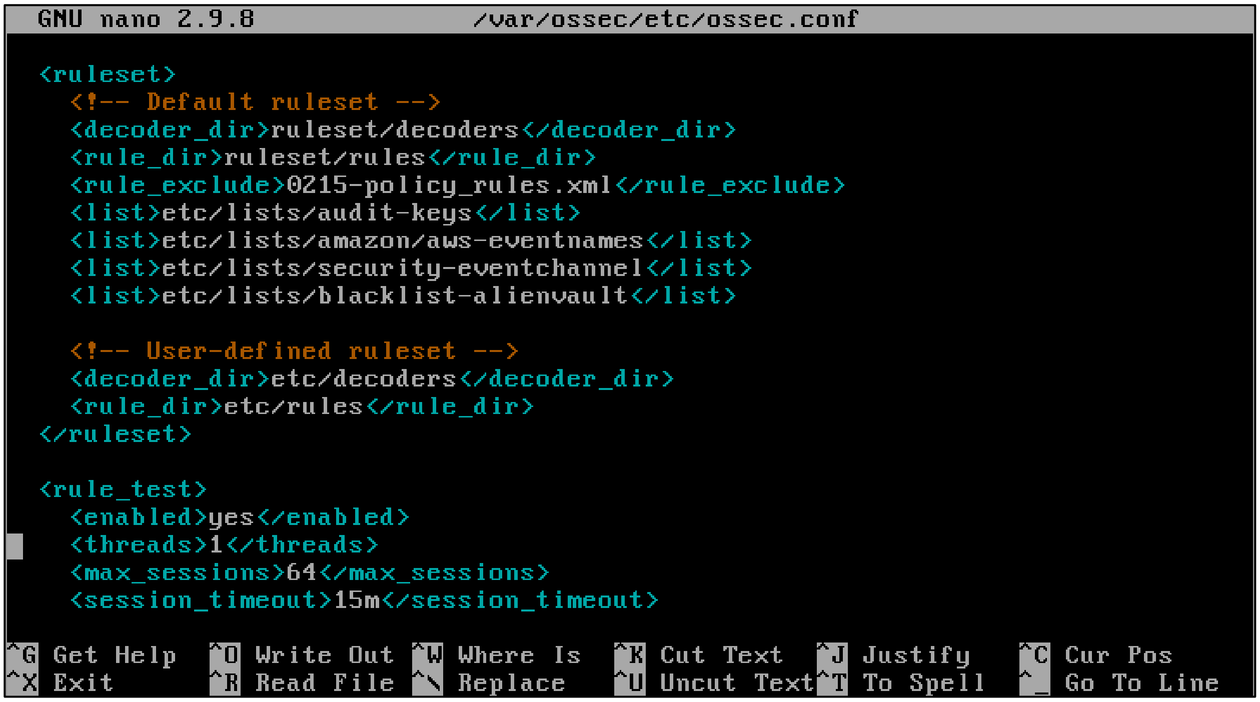


```
  GNU nano 2.9.8          /var/ossec/etc/rules/local_rules.xml


<group name="attack,">
  <rule id="100100" level="10">
    <if_group>web|attack|attacks</if_group>
    <list field="srcip" lookup="address_match_key">etc/lists/blacklist-alienvau$
    <description>IP address found in AlienVault reputation database.</descripti$
  </rule>
</group>


^G Get Help   ^O Write Out  ^W Where Is   ^K Cut Text   ^J Justify    ^C Cur Pos
^X Exit       ^R Read File  ^\ Replace    ^U Uncut Text^T To Spell    ^_ Go To Line
```

Now, edit the Wazuh server (*/var/ossec/etc/ossec.conf*) configuration file and add the (*etc/lists/blacklist-alienvault*) list to the <*ruleset*> section.

> **<ruleset>**
> **<decoder_dir>ruleset/decoders</decoder_dir>**
> **<rule_dir>ruleset/rules</rule_dir>**
> **<rule_exclude>0215-policy_rules.xml</rule_exclude>**

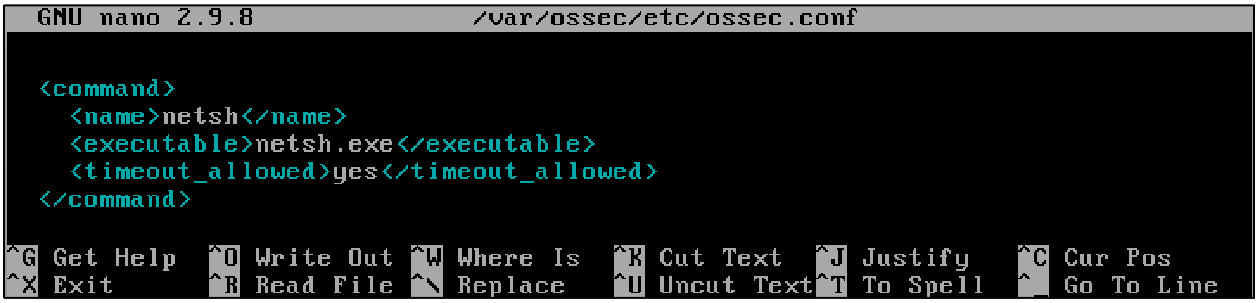
```
<list>etc/lists/audit-keys</list>
<list>etc/lists/amazon/aws-eventnames</list>
<list>etc/lists/security-eventchannel</list>
<list>etc/lists/blacklist-alienvault</list>
```



```
  GNU nano 2.9.8                /var/ossec/etc/ossec.conf

  <ruleset>
    <!-- Default ruleset -->
    <decoder_dir>ruleset/decoders</decoder_dir>
    <rule_dir>ruleset/rules</rule_dir>
    <rule_exclude>0215-policy_rules.xml</rule_exclude>
    <list>etc/lists/audit-keys</list>
    <list>etc/lists/amazon/aws-eventnames</list>
    <list>etc/lists/security-eventchannel</list>
    <list>etc/lists/blacklist-alienvault</list>

    <!-- User-defined ruleset -->
    <decoder_dir>etc/decoders</decoder_dir>
    <rule_dir>etc/rules</rule_dir>
  </ruleset>

  <rule_test>
    <enabled>yes</enabled>
    <threads>1</threads>
    <max_sessions>64</max_sessions>
    <session_timeout>15m</session_timeout>

^G Get Help   ^O Write Out  ^W Where Is   ^K Cut Text   ^J Justify    ^C Cur Pos
^X Exit       ^R Read File  ^\ Replace    ^U Uncut Text ^T To Spell   ^_ Go To Line
```

Now, add the Active Response block to the Wazuh server (*/var/ossec/etc/ossec.conf*) file. For the Windows endpoint, the active response script uses the *netsh* command to block the attacker's IP address on the Windows endpoint. It runs for 60 seconds.

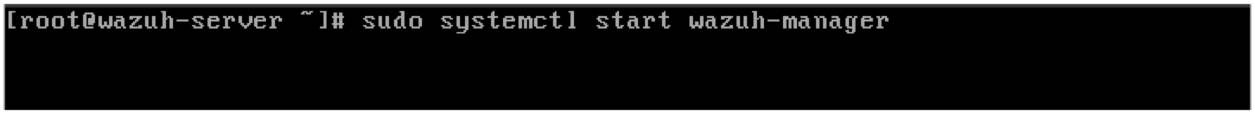
```
<active-response>
<command>netsh</command>
<location>local</location>
<rules_id>100100</rules_id>
<timeout>60</timeout>
</active-response>
```



```
  GNU nano 2.9.8                    /var/ossec/etc/ossec.conf

  <command>
    <name>netsh</name>
    <executable>netsh.exe</executable>
    <timeout_allowed>yes</timeout_allowed>
  </command>
```

Restart the Wazuh manager to apply the changes.

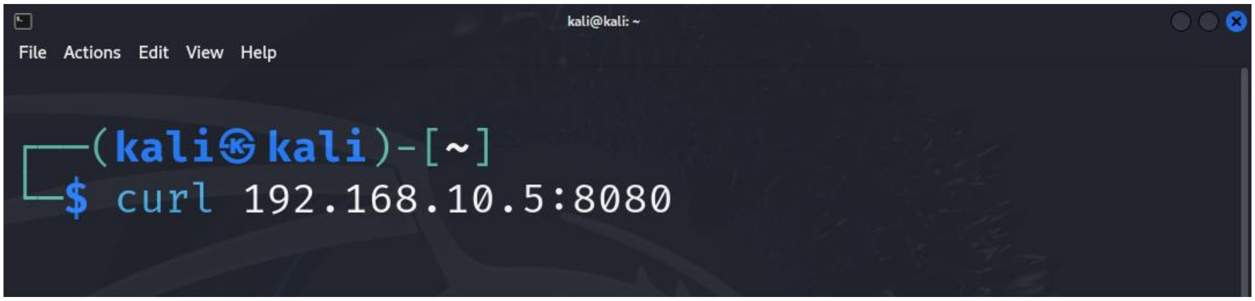
```
sudo systemctl restart wazuh-manager
```



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

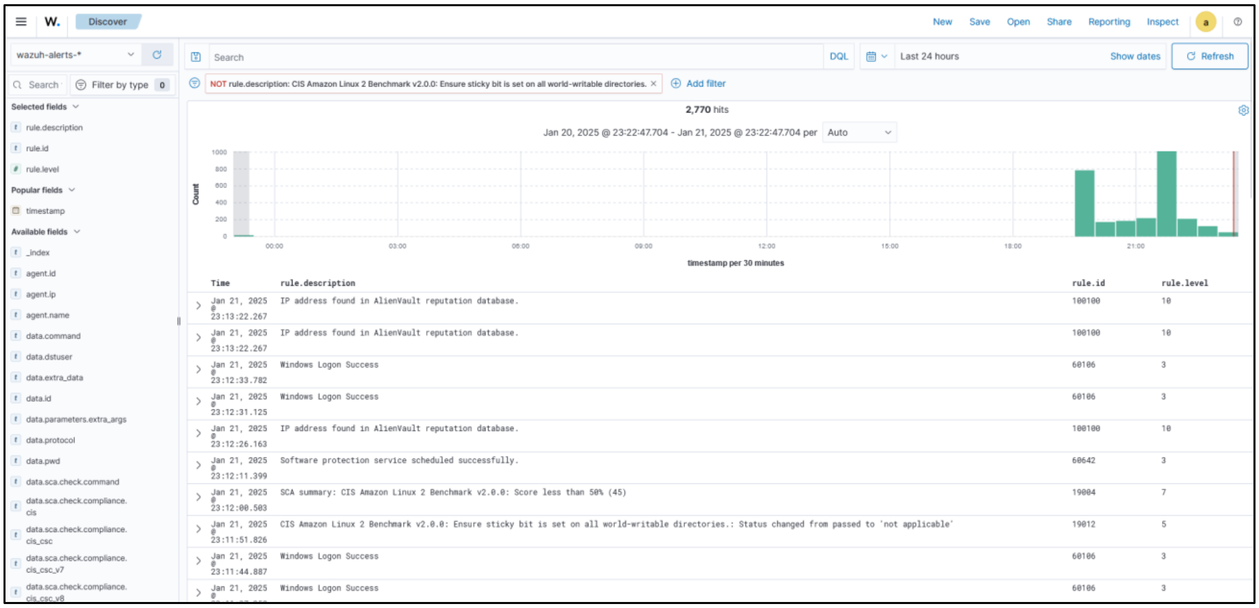
To emulate the attack, access any of the web servers from the RHEL endpoint using the corresponding IP address. Replace <WEBSERVER_IP> with the appropriate value and execute the following command from the attacker endpoint.

```
curl http://<WEBSERVER_IP>
```



```
┌──(kali㉿kali)-[~]
└─$ curl 192.168.10.5:8080
```

The attacker endpoint connects to the victim's web servers the first time. After the first connection, the Wazuh Active Response module temporarily blocks any successive connection to the web servers for 60 seconds.

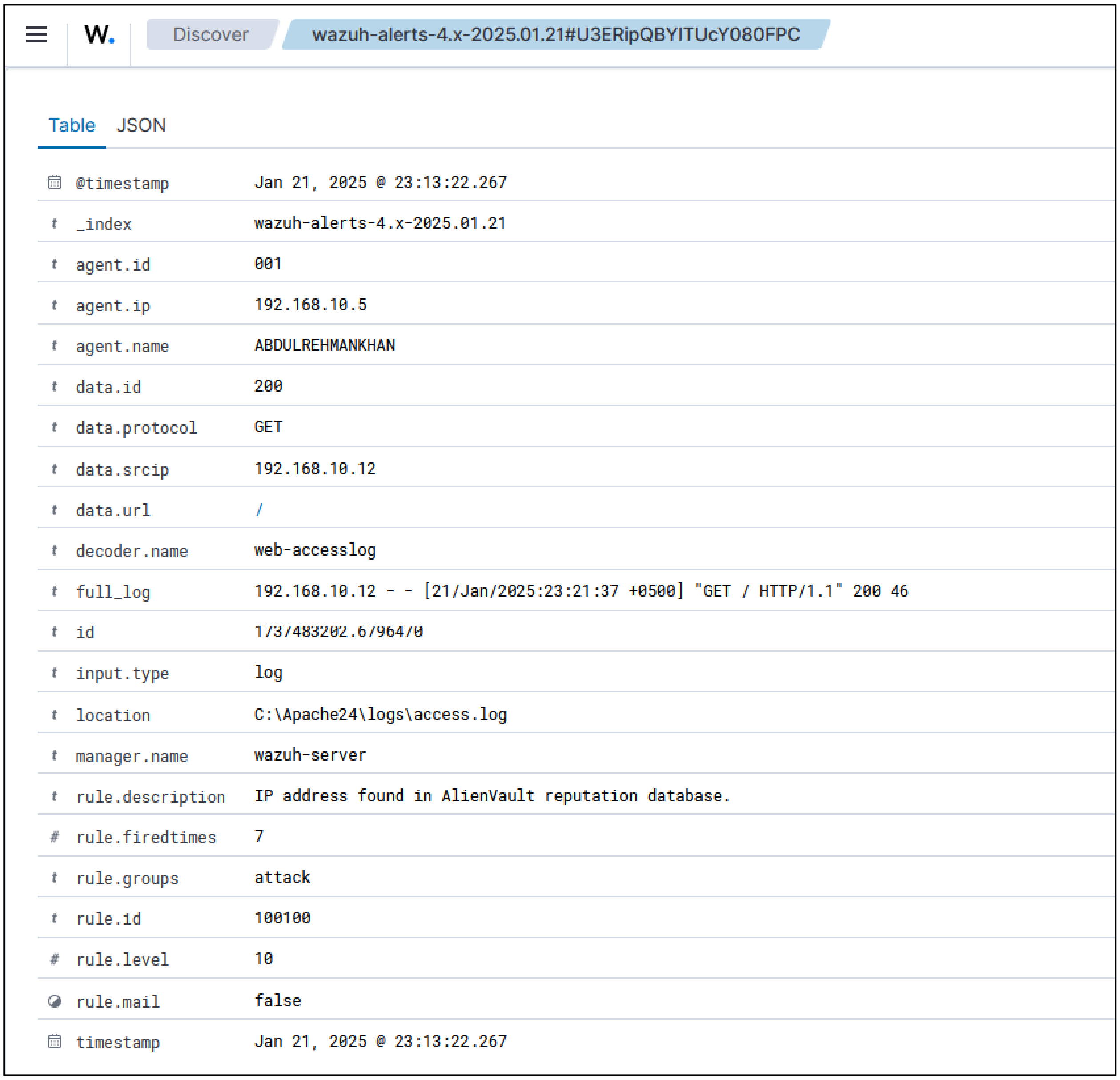


NOT rule.description: CIS Amazon Linux 2 Benchmark v2.0.0: Ensure sticky bit is set on all world-writable directories.

2,770 hits

Jan 20, 2025 @ 23:22:47.704 - Jan 21, 2025 @ 23:22:47.704 per Auto

Time	rule.description	rule.id	rule.level
Jan 21, 2025 @ 23:13:22.267	IP address found in AlienVault reputation database.	100100	10
Jan 21, 2025 @ 23:13:22.267	IP address found in AlienVault reputation database.	100100	10
Jan 21, 2025 @ 23:12:33.782	Windows Logon Success	60106	3
Jan 21, 2025 @ 23:12:31.125	Windows Logon Success	60106	3
Jan 21, 2025 @ 23:12:26.163	IP address found in AlienVault reputation database.	100100	10
Jan 21, 2025 @ 23:12:11.399	Software protection service scheduled successfully.	60642	3
Jan 21, 2025 @ 23:12:00.503	SCA summary: CIS Amazon Linux 2 Benchmark v2.0.0: Score less than 50% (45)	19004	7
Jan 21, 2025 @ 23:11:51.826	CIS Amazon Linux 2 Benchmark v2.0.0: Ensure sticky bit is set on all world-writable directories.: Status changed from passed to 'not applicable'	19012	5
Jan 21, 2025 @ 23:11:44.887	Windows Logon Success	60106	3
Jan 21, 2025 @	Windows Logon Success	60106	3



@timestamp	Jan 21, 2025 @ 23:13:22.267
_index	wazuh-alerts-4.x-2025.01.21
agent.id	001
agent.ip	192.168.10.5
agent.name	ABDULREHMANKHAN
data.id	200
data.protocol	GET
data.srcip	192.168.10.12
data.url	/
decoder.name	web-accesslog
full_log	192.168.10.12 - - [21/Jan/2025:23:21:37 +0500] "GET / HTTP/1.1" 200 46
id	1737483202.6796470
input.type	log
location	C:\Apache24\logs\access.log
manager.name	wazuh-server
rule.description	IP address found in AlienVault reputation database.
rule.firedtimes	7
rule.groups	attack
rule.id	100100
rule.level	10
rule.mail	false
timestamp	Jan 21, 2025 @ 23:13:22.267

BLOCKING A KNOWN MALICIOUS ACTOR

OVERVIEW:

A malicious actor is an entity, such as a cybercriminal or hacker that engages in harmful activities like data theft, system compromise, or disruption of services. Blocking known malicious actors is a critical step in protecting systems and networks from ongoing or future threats. Wazuh plays an essential role in identifying and mitigating threats by analyzing logs and detecting suspicious activities associated with malicious actors. By leveraging threat intelligence feeds and defining custom rules, Wazuh can identify IP addresses, domains, or activities linked to known malicious entities and take action to block them. This process ensures that potential threats are neutralized before they can cause significant harm.

CONCLUSION:

In this lab, we demonstrated how to block a known malicious actor using Wazuh. By analyzing threat intelligence and log data, Wazuh identified activities associated with malicious entities and initiated measures to prevent their access to the system. This lab highlights the importance of using proactive detection and prevention tools like Wazuh to protect systems against ongoing threats, reduce attack surfaces, and maintain a robust security posture.