Building a SIEM Tool Using Wazuh

Contents

Chapter 1

Introduction

This Project Involved in building a functional SIEM environment using Wazuh, with the goal of learning how centralised log monitoring and threat detection work in practice. I built and deployed a Wazuh Manager on an Ubuntu server and then connected my main Windows machine as an agent to collect system logs, analyse security events and generate alerts.

Chapter 2

System Requirements & VM Setup

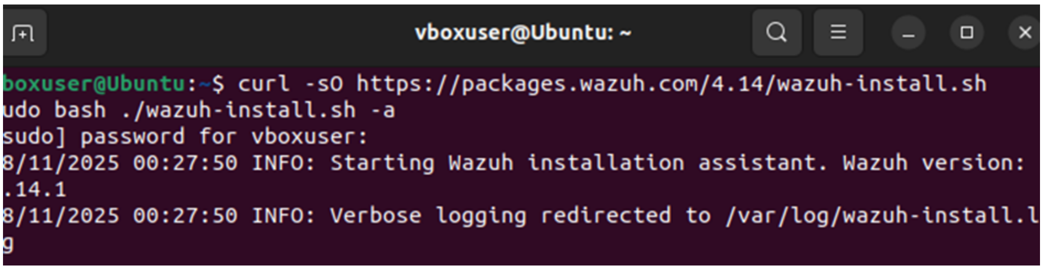
Firstly, I went to the Wazuh Page and under “Documentation” I found the system requirements to deploy Wazuh, According the documentation for 1 - 25 agents, The server required 4vCPU 8GB RAM and 50GB storage. So I built an Ubuntu virtual machine with the require settings.

Chapter 3

Wazuh Manager Installation (Ubuntu)

Then using the provided installation command in the documentation, I ran this on the command line as the root user:

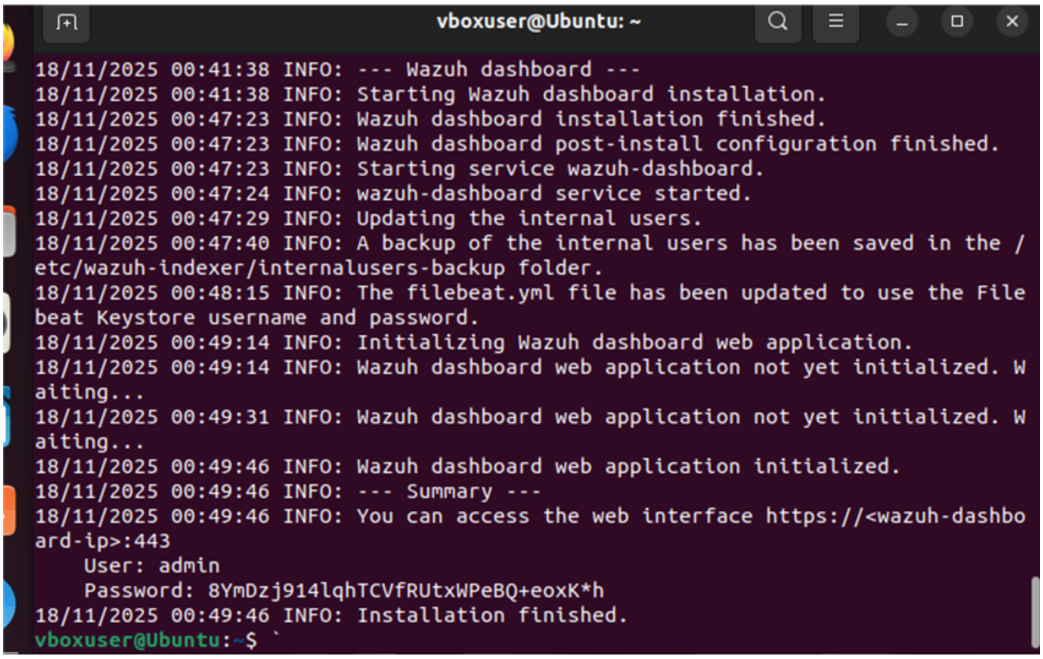
```
curl -sO https://packages.wazuh.com/4.14/wazuh-install.sh
&& sudo bash ./wazuh-install.sh -a
```



```
boxuser@Ubuntu:~$ curl -sO https://packages.wazuh.com/4.14/wazuh-install.sh
udo bash ./wazuh-install.sh -a
sudo] password for vboxuser:
8/11/2025 00:27:50 INFO: Starting Wazuh installation assistant. Wazuh version:
.14.1
8/11/2025 00:27:50 INFO: Verbose logging redirected to /var/log/wazuh-install.l
g
```

Figure 3.1:

Once the installation was finished, I was now given a username and a password to access my Wazuh Dashboard.



```
18/11/2025 00:41:38 INFO: --- Wazuh dashboard ---
18/11/2025 00:41:38 INFO: Starting Wazuh dashboard installation.
18/11/2025 00:47:23 INFO: Wazuh dashboard installation finished.
18/11/2025 00:47:23 INFO: Wazuh dashboard post-install configuration finished.
18/11/2025 00:47:23 INFO: Starting service wazuh-dashboard.
18/11/2025 00:47:24 INFO: wazuh-dashboard service started.
18/11/2025 00:47:29 INFO: Updating the internal users.
18/11/2025 00:47:40 INFO: A backup of the internal users has been saved in the /
etc/wazuh-indexer/internalusers-backup folder.
18/11/2025 00:48:15 INFO: The filebeat.yml file has been updated to use the File
beat Keystore username and password.
18/11/2025 00:49:14 INFO: Initializing Wazuh dashboard web application.
18/11/2025 00:49:14 INFO: Wazuh dashboard web application not yet initialized. W
aiting...
18/11/2025 00:49:31 INFO: Wazuh dashboard web application not yet initialized. W
aiting...
18/11/2025 00:49:46 INFO: Wazuh dashboard web application initialized.
18/11/2025 00:49:46 INFO: --- Summary ---
18/11/2025 00:49:46 INFO: You can access the web interface https://<wazuh-dashbo
ard-ip>:443
    User: admin
    Password: 8YmDzj914lqhTCVfRUtxWPeBQ+eoxK*h
18/11/2025 00:49:46 INFO: Installation finished.
vboxuser@Ubuntu:~$ `
```

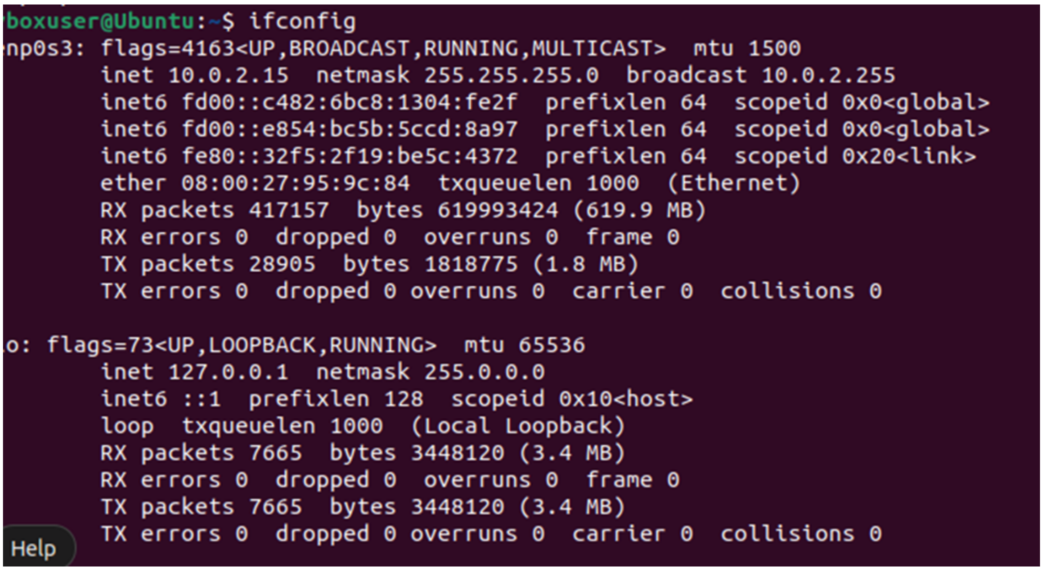
Figure 3.2:

Chapter 4

Dashboard Access & Network Configuration

Now in order to access this dashboard I had to find my network using Ifconfig in the CLI.

From the screenshot below I can see that my Ip address is at 10.0.2.15, this would pose to be an issue as this will only work if both my agent device and manager device is on the same network.

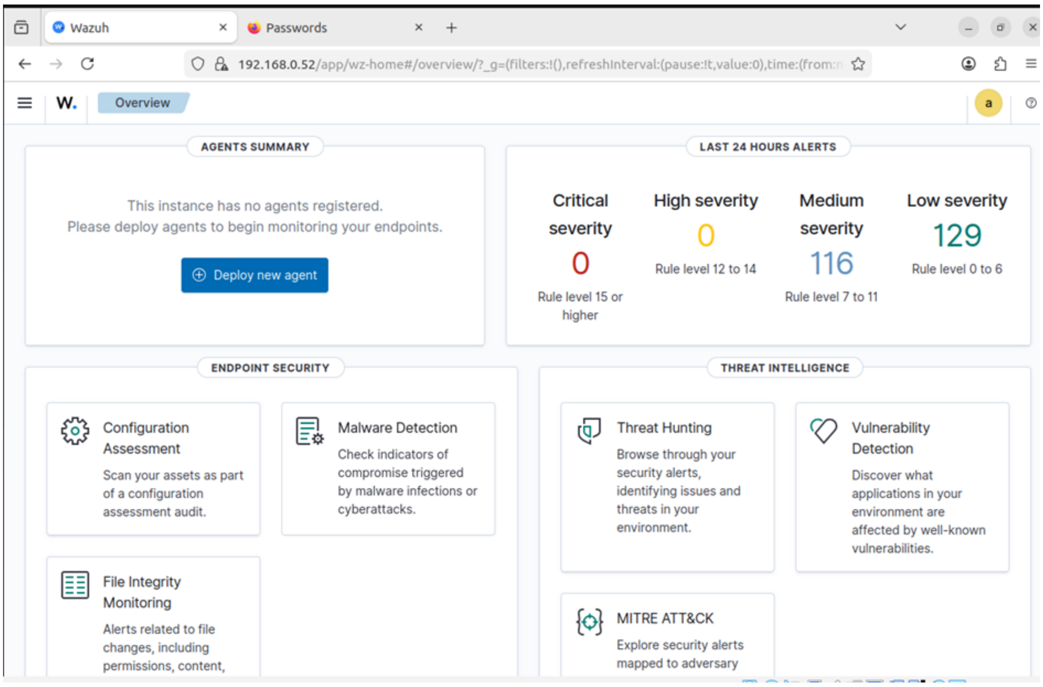


```
boxuser@Ubuntu:~$ ifconfig
np0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
       inet 10.0.2.15  netmask 255.255.255.0  broadcast 10.0.2.255
       inet6 fd00::c482:6bc8:1304:fe2f  prefixlen 64  scopeid 0x0<global>
       inet6 fd00::e854:bc5b:5ccd:8a97  prefixlen 64  scopeid 0x0<global>
       inet6 fe80::32f5:2f19:be5c:4372  prefixlen 64  scopeid 0x20<link>
       ether 08:00:27:95:9c:84  txqueuelen 1000  (Ethernet)
       RX packets 417157  bytes 619993424 (619.9 MB)
       RX errors 0  dropped 0  overruns 0  frame 0
       TX packets 28905  bytes 1818775 (1.8 MB)
       TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

o: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
       inet 127.0.0.1  netmask 255.0.0.0
       inet6 ::1  prefixlen 128  scopeid 0x10<host>
       loop  txqueuelen 1000  (Local Loopback)
       RX packets 7665  bytes 3448120 (3.4 MB)
       RX errors 0  dropped 0  overruns 0  frame 0
       TX packets 7665  bytes 3448120 (3.4 MB)
       TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Figure 4.1:

And I know that by running ipconfig on windows PowerShell my network was at 192.168.0.

To fix this I changed the settings of my ubuntu device from “NAT” to “Bridged Adapter” and then when I restarted ubuntu I received an Ip address with 192.168.0.52 and this was now possible to use to deploy the SIEM tool.


Wazuh
Passwords
192.168.0.52/app/wz-home#/overview/?_g=(filters:!(),refreshInterval:(pause:!t,value:0),time:(from:n
W.
Overview
a

AGENTS SUMMARY

This instance has no agents registered.
Please deploy agents to begin monitoring your endpoints.

Deploy new agent

LAST 24 HOURS ALERTS

Critical severity	High severity	Medium severity	Low severity
0	0	116	129
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
Check indicators of compromise triggered by malware infections or cyberattacks.

File Integrity Monitoring
Alerts related to file changes, including permissions, content,

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.

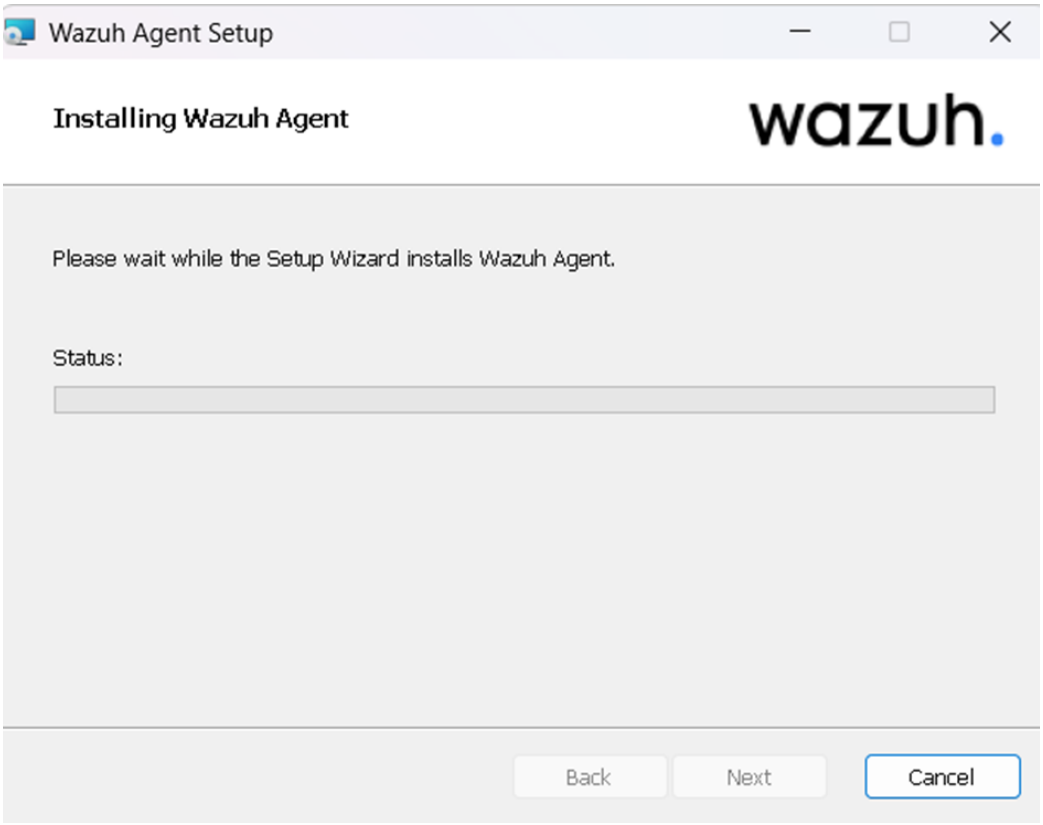
MITRE ATT&CK
Explore security alerts mapped to adversary

Figure 4.2:

Chapter 5

Windows Agent Deployment

Once the dashboard was set up now it was time to deploy the agent on Windows device.



Wazuh Agent Setup

Installing Wazuh Agent

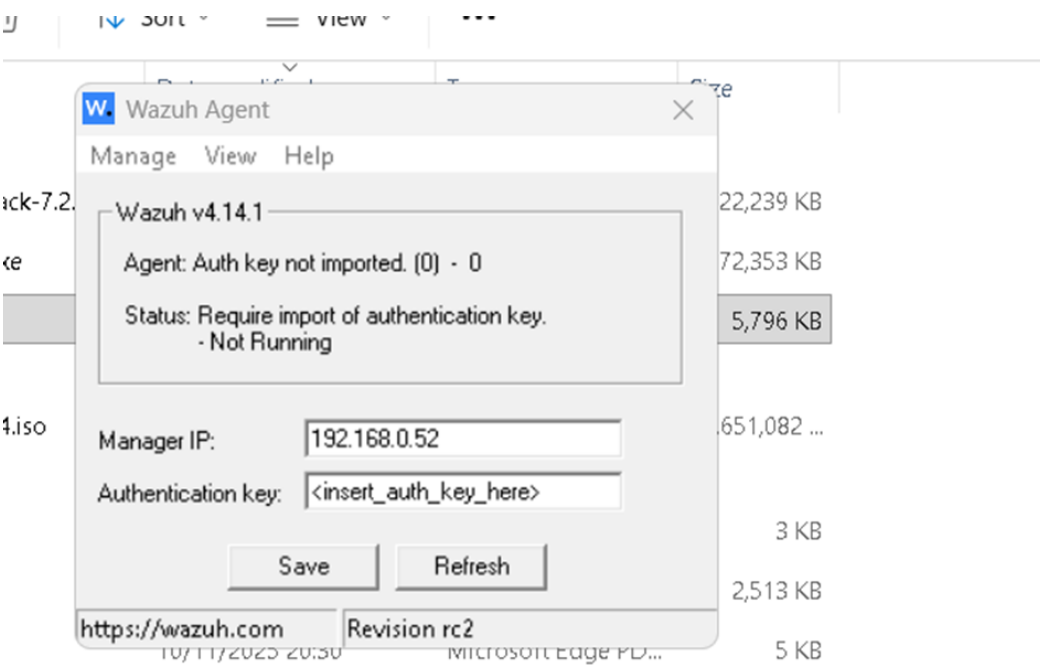
Please wait while the Setup Wizard installs Wazuh Agent.

Status:

Figure 5.1:

Using the documentation from Wazuh once again found the windows installer for the Agent. I set this up normally.

After the agent was finished installing I had to insert the managers IP Address and the key to finish the process.



Wazuh v4.14.1

Agent: Auth key not imported. (0) - 0

Status: Require import of authentication key.
- Not Running

Manager IP: 192.168.0.52

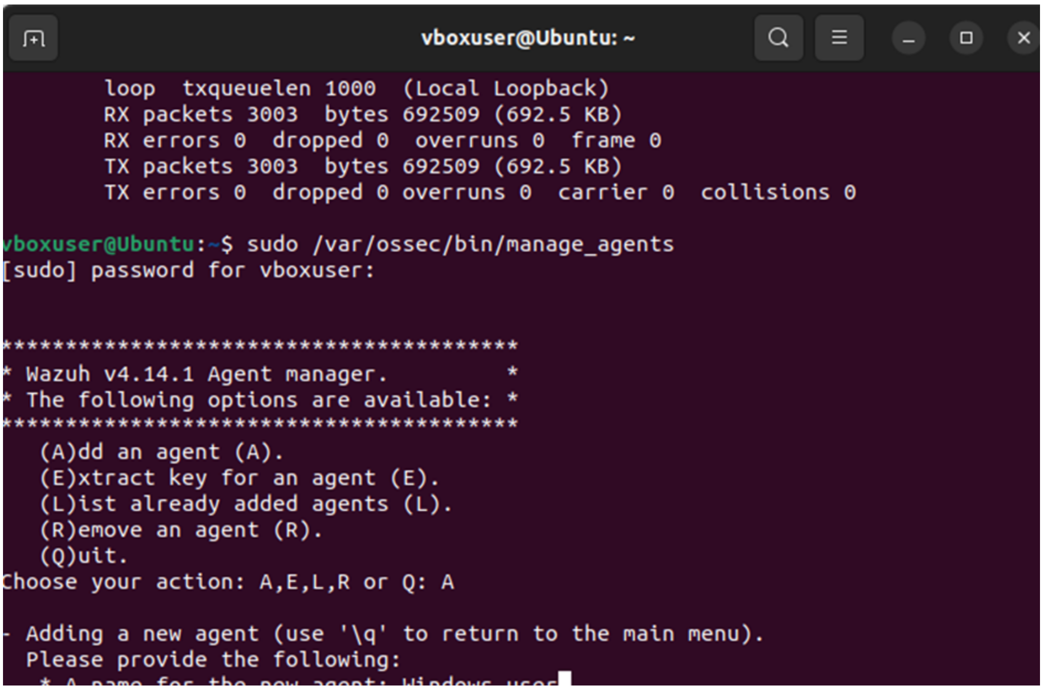
Authentication key: <insert_auth_key_here>

https://wazuh.com

Revision rc2

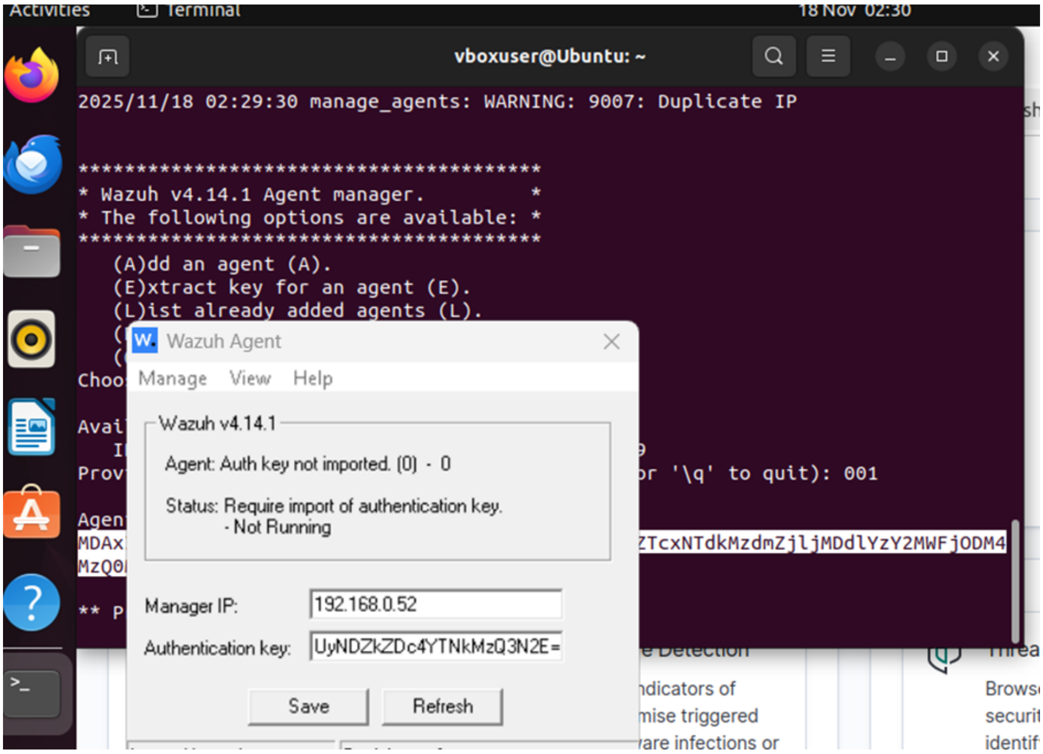
Figure 5.2:

To Find the key I had to go back to the Ubuntu Server and access the manage agents option and from there I added the agent and generated my key.



```
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 3003  bytes 692509 (692.5 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 3003  bytes 692509 (692.5 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

vboxuser@Ubuntu:~$ sudo /var/ossec/bin/manage_agents
[sudo] password for vboxuser:


****************************************
* Wazuh v4.14.1 Agent manager.         *
* The following options are available: *
****************************************
   (A)dd an agent (A).
   (E)xtract key for an agent (E).
   (L)ist already added agents (L).
   (R)emove an agent (R).
   (Q)uit.
Choose your action: A,E,L,R or Q: A

- Adding a new agent (use '\q' to return to the main menu).
  Please provide the following:
   * A name for the new agent: Windows user
```

Figure 5.3:



```
2025/11/18 02:29:30 manage_agents: WARNING: 9007: Duplicate IP


****************************************
* Wazuh v4.14.1 Agent manager.         *
* The following options are available: *
****************************************
   (A)dd an agent (A).
   (E)xtract key for an agent (E).
   (L)ist already added agents (L).
   (
   (
Choo

Avai
   I                                                    9
Prov                                                    or '\q' to quit): 001

Agen
MDAx                                                    ZTcxNTdkMzdmZjljMDdlYzY2MWFjODM4
MzQ0

** P
```

Wazuh v4.14.1

Agent: Auth key not imported. (0) - 0

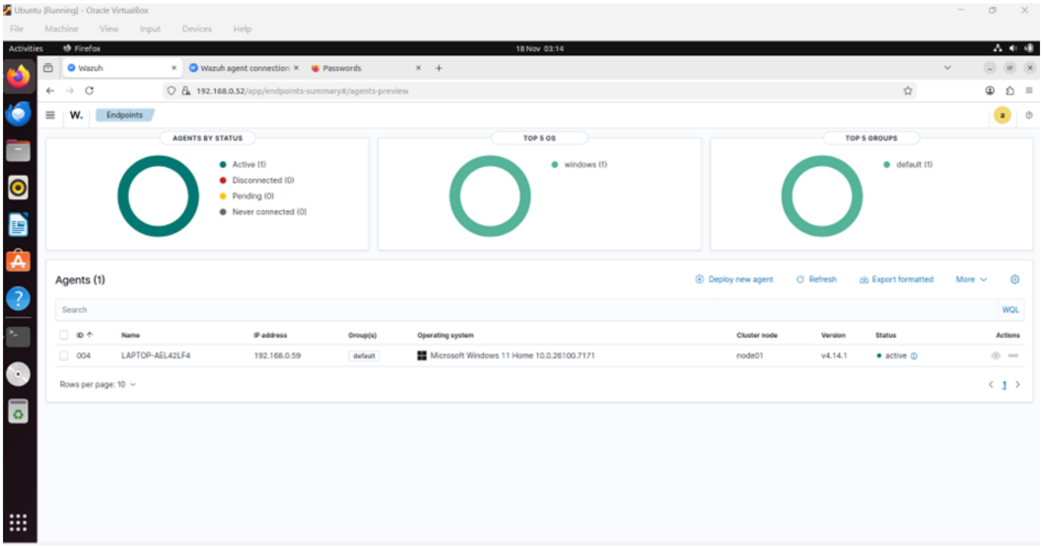
Status: Require import of authentication key.
- Not Running

Manager IP: 192.168.0.52

Authentication key: UyNDZkZDc4YTNkMzQ3N2E=

Figure 5.4:

Once this was finished, in Windows Terminal I restarted the Net Wazuh and then when I went to the Ubuntu Server I was now connected to the Windows Server and was ready to analyze logs and test detection capabilities.



Agents (1)

ID	Name	IP address	Group(s)	Operating system	Cluster node	Version	Status	Actions
004	LAPTOP-AEL42LF4	192.168.0.59	default	Microsoft Windows 11 Home 10.0.26100.7171	node01	v4.14.1	active	

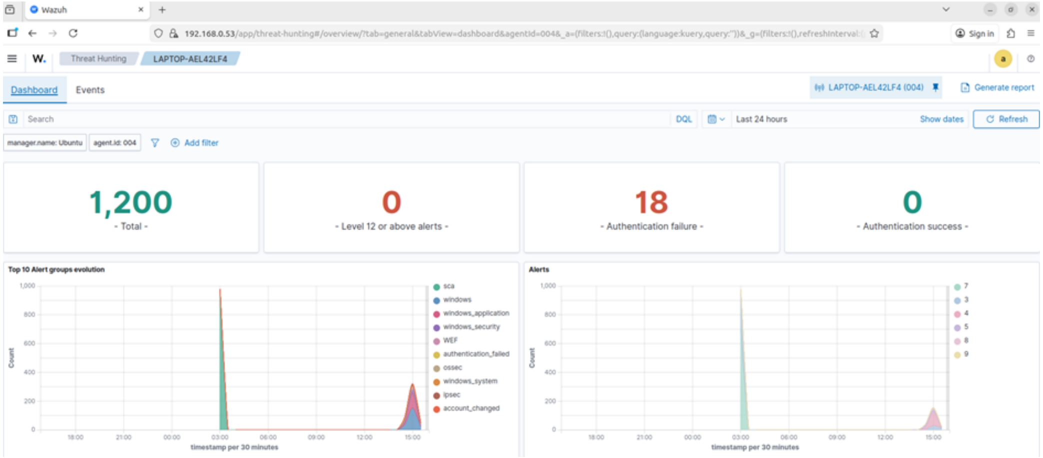
Figure 5.5:

Chapter 6

Testing & Detection

6.1 Failed RDP Login Attempts

Next we will be testing failed RDP login attempts. To begin this test we first have to see how Wazuh tracks authentication failures. In the dashboard, under the threat hunting section, we are able to see a tab named “Authentication failure” which displays a number, in my instance 18. This keeps track of all the failed logins on my Windows device. To test this feature, we will press Windows button + L at the same time to lock the screen, we will then enter the password incorrectly twice and then login correctly on the third try.



192.168.0.53/app/threat-hunting#/overview/?tab=general&tabView=dashboard&agentId=004&_a=(filters:!(),query:(language:kuery,query:''))&_g=(filters:!(),refreshInterval:(

manager.name: Ubuntu   agent.id: 004

Last 24 hours

1,200 - Total -

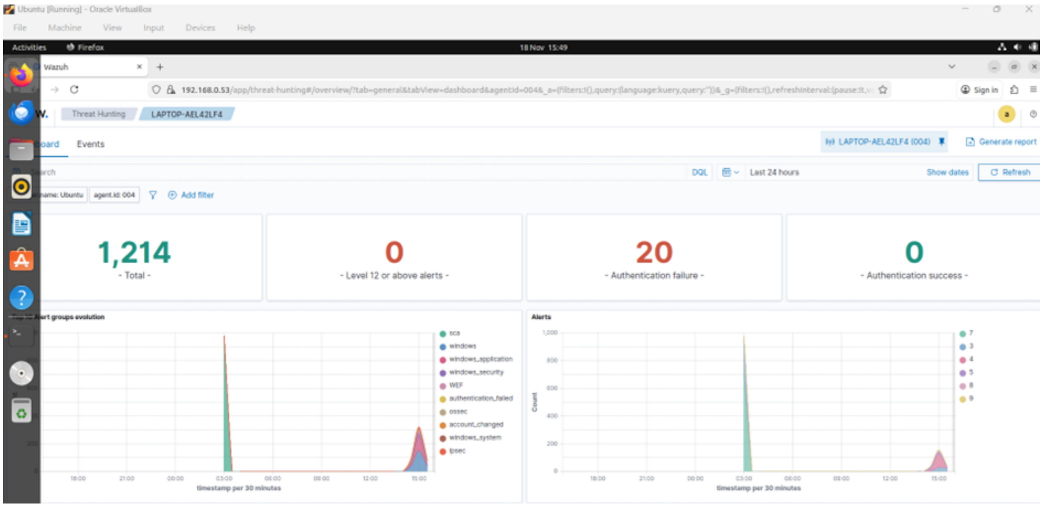
0 - Level 12 or above alerts -

18 - Authentication failure -

0 - Authentication success -

Figure 6.1:

Once we have logged in correctly, we can see that the system has updated the “Authentication failure” to 20. This demonstrates that the SIEM is correctly monitoring Windows login activity and is capable of identifying potential brute-force or unauthorized access attempts.



1,214 - Total -

0 - Level 12 or above alerts -

20 - Authentication failure -

0 - Authentication success -

Figure 6.2:

6.2 File Integrity Monitoring

File integrity monitoring on Windows is also a feature within Wazuh, with this feature we are able to see if any changes have been brought to a file to uphold integrity. To do this, we will create a folder named secret folder on the Desktop and remember its path.

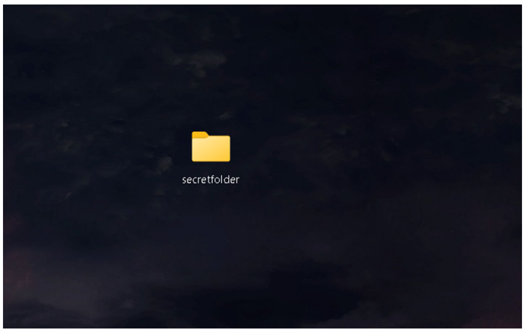
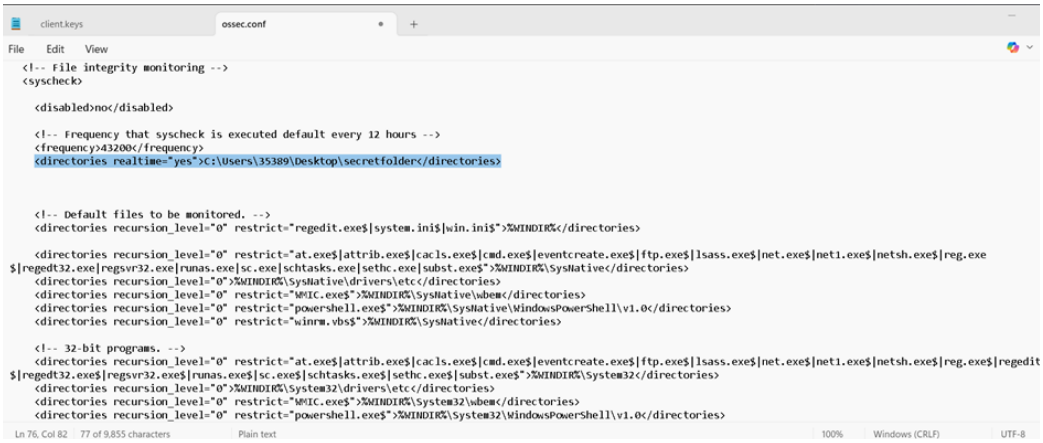


Figure 6.3:

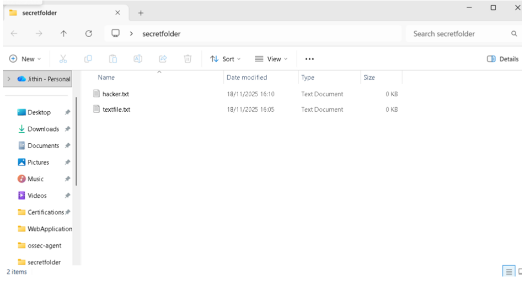
Then we have to access the ossec.conf file of the Wazuh file, which is the main configuration file for both the Wazuh manager and Wazuh agents. To access this we need to run Notepad as administrator. The file is situated in `C:\Program Files (x86)\ossec-agent`.Once you are in the file, scroll down to "File Integrity Monitoring" and we will add the text in the picture below to monitor activity in the folder we created earlier, with the path of the folder. Now we will save this.



```
  <!-- File integrity monitoring -->
  <syscheck>

    <disabled>no</disabled>

    <!-- Frequency that syscheck is executed default every 12 hours -->
    <frequency>43200</frequency>
    <directories realtime="yes">C:\Users\35389\Desktop\secretfolder</directories>



    <!-- Default files to be monitored. -->
    <directories recursion_level="0" restrict="regedit.exe$|system.ini$|win.ini$">%WINDIR%</directories>

    <directories recursion_level="0" restrict="at.exe$|attrib.exe$|cacls.exe$|cmd.exe$|eventcreate.exe$|ftp.exe$|lsass.exe$|net.exe$|net1.exe$|netsh.exe$|reg.exe
$|regedt32.exe|regsvr32.exe|runas.exe|sc.exe|schtasks.exe|sethc.exe|subst.exe$">%WINDIR%\SysNative</directories>
    <directories recursion_level="0">%WINDIR%\SysNative\drivers\etc</directories>
    <directories recursion_level="0" restrict="WMIC.exe$">%WINDIR%\SysNative\wbem</directories>
    <directories recursion_level="0" restrict="powershell.exe$">%WINDIR%\SysNative\WindowsPowerShell\v1.0</directories>
    <directories recursion_level="0" restrict="winrm.vbs$">%WINDIR%\SysNative</directories>

    <!-- 32-bit programs. -->
    <directories recursion_level="0" restrict="at.exe$|attrib.exe$|cacls.exe$|cmd.exe$|eventcreate.exe$|ftp.exe$|lsass.exe$|net.exe$|net1.exe$|netsh.exe$|reg.exe$|regedit
$|regedt32.exe$|regsvr32.exe$|runas.exe$|sc.exe$|schtasks.exe$|sethc.exe$|subst.exe$">%WINDIR%\System32</directories>
    <directories recursion_level="0">%WINDIR%\System32\drivers\etc</directories>
    <directories recursion_level="0" restrict="WMIC.exe$">%WINDIR%\System32\wbem</directories>
    <directories recursion_level="0" restrict="powershell.exe$">%WINDIR%\System32\WindowsPowerShell\v1.0</directories>
```

Figure 6.4:

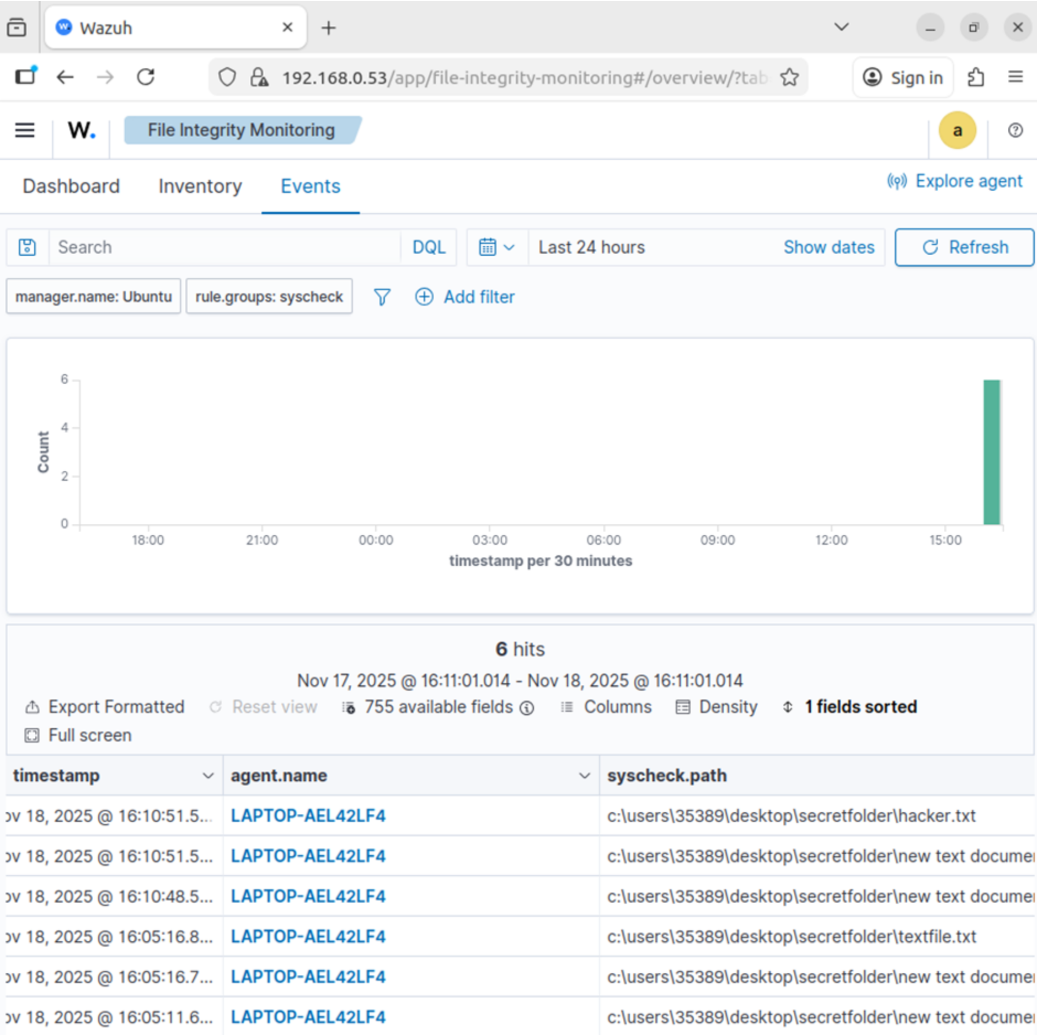
Now to test if this works, we will access the folder and add two new documents.



Name	Date modified	Type	Size
hacker.txt	18/11/2025 16:10	Text Document	0 KB
textfile.txt	18/11/2025 16:05	Text Document	0 KB

Figure 6.5:

Now if we head back to the Wazuh server and go to File Integrity Monitoring, we can switch to the events tab and now we can see the changes made to the folder.



192.168.0.53/app/file-integrity-monitoring#/overview/?tab

Last 24 hours

manager.name: Ubuntu

rule.groups: syscheck

6 hits

Nov 17, 2025 @ 16:11:01.014 - Nov 18, 2025 @ 16:11:01.014

timestamp	agent.name	syscheck.path
ov 18, 2025 @ 16:10:51.5...	LAPTOP-AEL42LF4	c:\users\35389\desktop\secretfolder\hacker.txt
ov 18, 2025 @ 16:10:51.5...	LAPTOP-AEL42LF4	c:\users\35389\desktop\secretfolder\new text docume
ov 18, 2025 @ 16:10:48.5...	LAPTOP-AEL42LF4	c:\users\35389\desktop\secretfolder\new text docume
ov 18, 2025 @ 16:05:16.8...	LAPTOP-AEL42LF4	c:\users\35389\desktop\secretfolder\textfile.txt
ov 18, 2025 @ 16:05:16.7...	LAPTOP-AEL42LF4	c:\users\35389\desktop\secretfolder\new text docume
ov 18, 2025 @ 16:05:11.6...	LAPTOP-AEL42LF4	c:\users\35389\desktop\secretfolder\new text docume

Figure 6.6:

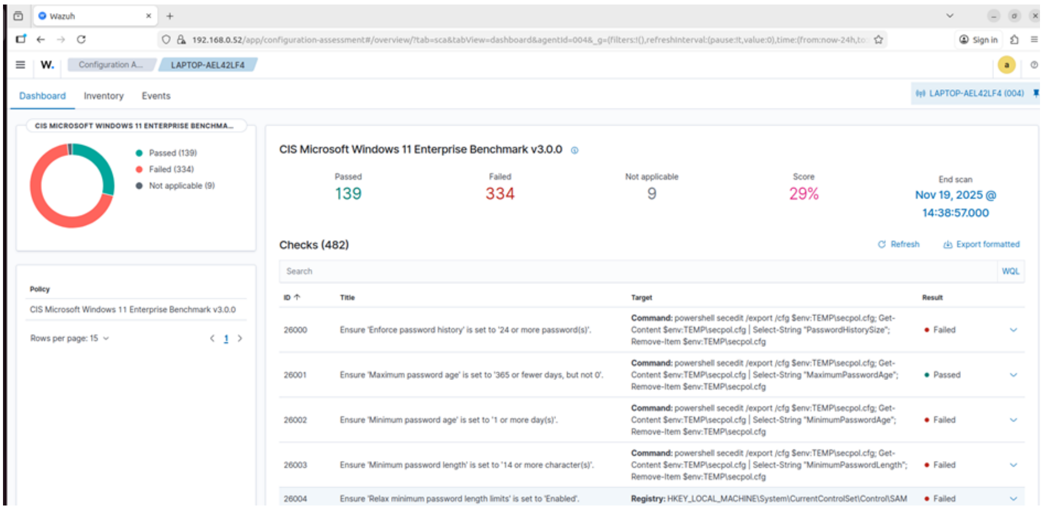
6.3 CIS Benchmark

One of the important features used by Wazuh is its CIS Benchmark feature, it can be found in the Security Configuration Assessment. The CIS Benchmark allows you to see a full security compliance audit of the machine, it does this by checking the system against the official CIS hardening rules.

Wazuh goes through every configuration of your machine to show its misconfigurations and gives you a percentage total based on everything. Along with this, Wazuh also tells you how to fix each failed configuration.

Wazuh shows a summary:

- Total rules checked
- Total passed
- Total failed
- Compliance percentage



Wazuh
192.168.0.52/app/configuration-assessment#/overview/?tab=sca&tabView=dashboard&agentId=004&_g=(filters:!(),refreshInterval:(pause:!t,value:0),time:(from:now-24h,to
Sign in
W.
Configuration A...
LAPTOP-AEL42LF4
Dashboard
Inventory
Events
LAPTOP-AEL42LF4 (004)
CIS MICROSOFT WINDOWS 11 ENTERPRISE BENCHMA...
Passed (139)
Failed (334)
Not applicable (9)
Refresh
Export formatted
Search
WQL

Policy

CIS Microsoft Windows 11 Enterprise Benchmark v3.0.0

Rows per page: 15

CIS Microsoft Windows 11 Enterprise Benchmark v3.0.0

Passed	Failed	Not applicable	Score	End scan
139	334	9	29%	Nov 19, 2025 @ 14:38:57.000

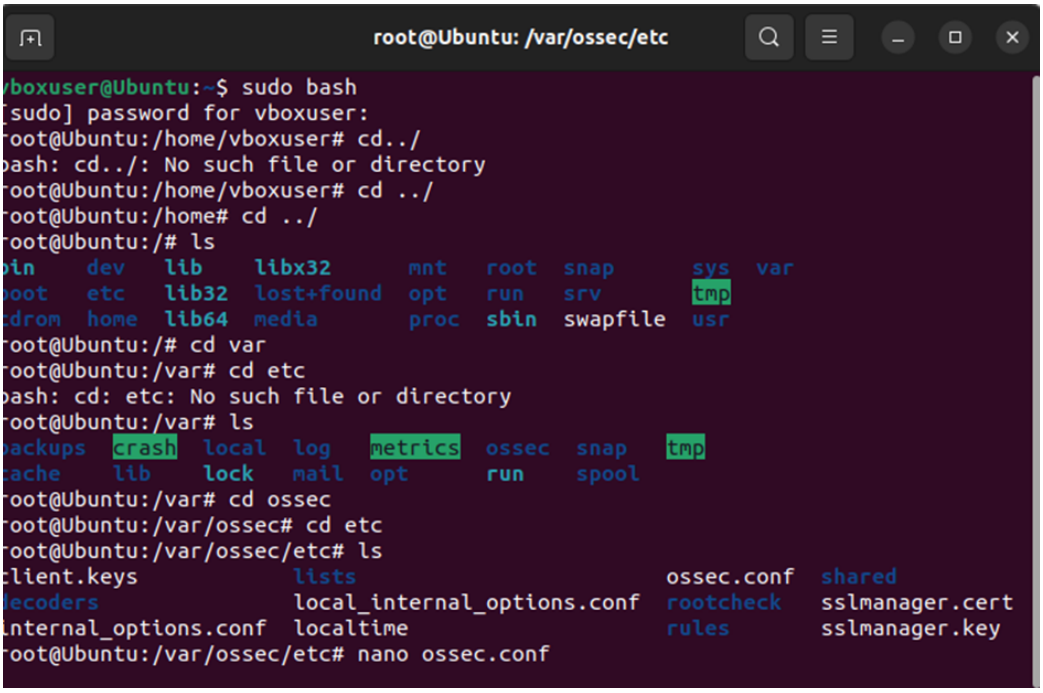
Checks (482)

ID	Title	Target	Result
26000	Ensure 'Enforce password history' is set to '24 or more password(s)'.	**Command:** powershell secedit /export /cfg $env:TEMP\secpol.cfg; Get-Content $env:TEMP\secpol.cfg | Select-String "PasswordHistorySize"; Remove-Item $env:TEMP\secpol.cfg	● Failed
26001	Ensure 'Maximum password age' is set to '365 or fewer days, but not 0'.	**Command:** powershell secedit /export /cfg $env:TEMP\secpol.cfg; Get-Content $env:TEMP\secpol.cfg | Select-String "MaximumPasswordAge"; Remove-Item $env:TEMP\secpol.cfg	● Passed
26002	Ensure 'Minimum password age' is set to '1 or more day(s)'.	**Command:** powershell secedit /export /cfg $env:TEMP\secpol.cfg; Get-Content $env:TEMP\secpol.cfg | Select-String "MinimumPasswordAge"; Remove-Item $env:TEMP\secpol.cfg	● Failed
26003	Ensure 'Minimum password length' is set to '14 or more character(s)'.	**Command:** powershell secedit /export /cfg $env:TEMP\secpol.cfg; Get-Content $env:TEMP\secpol.cfg | Select-String "MinimumPasswordLength"; Remove-Item $env:TEMP\secpol.cfg	● Failed
26004	Ensure 'Relax minimum password length limits' is set to 'Enabled'.	**Registry:** HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\SAM	● Failed

Figure 6.7:

6.4 Vulnerability Detection

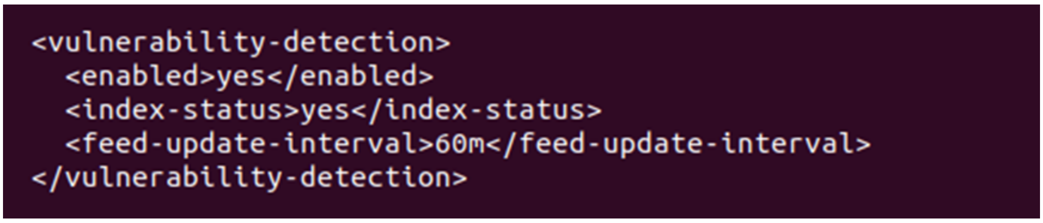
To enable vulnerability detection we have to access the ossec.conf from the Ubuntu server, down below you can see the path to the folder.



```
boxuser@Ubuntu:~$ sudo bash
sudo] password for vboxuser:
oot@Ubuntu:/home/vboxuser# cd../
ash: cd../: No such file or directory
oot@Ubuntu:/home/vboxuser# cd ../
oot@Ubuntu:/home# cd ../
oot@Ubuntu:/# ls
in    dev   lib    libx32      mnt   root  snap      sys  var
oot   etc   lib32  lost+found  opt   run   srv       tmp
drom  home  lib64  media       proc  sbin  swapfile  usr
oot@Ubuntu:/# cd var
oot@Ubuntu:/var# cd etc
ash: cd: etc: No such file or directory
oot@Ubuntu:/var# ls
ackups  crash  local  log   metrics  ossec  snap   tmp
ache    lib    lock   mail  opt      run    spool
oot@Ubuntu:/var# cd ossec
oot@Ubuntu:/var/ossec# cd etc
oot@Ubuntu:/var/ossec/etc# ls
lient.keys            lists                        ossec.conf  shared
ecoders               local_internal_options.conf  rootcheck   sslmanager.cert
nternal_options.conf  localtime                    rules       sslmanager.key
oot@Ubuntu:/var/ossec/etc# nano ossec.conf
```

Figure 6.8:

We will now go to the section that says vulnerability detection and change the ”no” to a ”yes”.

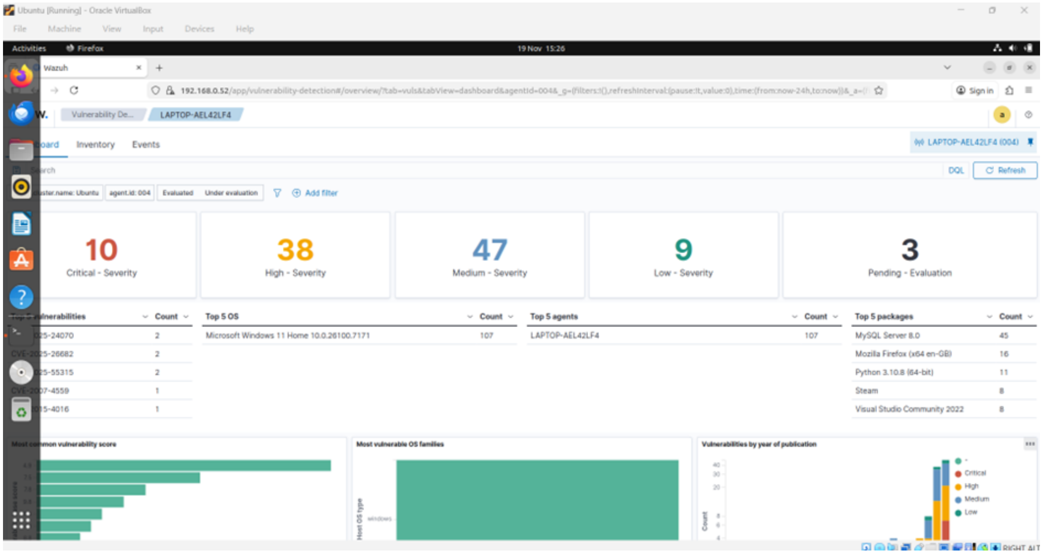


```
<vulnerability-detection>
  <enabled>yes</enabled>
  <index-status>yes</index-status>
  <feed-update-interval>60m</feed-update-interval>
</vulnerability-detection>
```

Figure 6.9:

When we now go to the vulnerability detection tab of the dashboard, we can now see a whole list of vulnerabilities. Each one shows:

CVE ID (e.g., CVE-2023-XXXX) , Severity (Low, Medium, High, Critical), Affected software, Installed version, Safe version, Description of the vulnerability, Links to the official CVE page



Ubuntu [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Activities Firefox
19 Nov 15:26
Wazuh
192.168.0.52/app/vulnerability-detection#/overview/?tab=vuls&tabView=dashboard&agentId=004&_g=(filters:!(),refreshInterval:(pause:!t,value:0),time:(from:now-24h,to:now))&_a=(
Sign in
Vulnerability De...
LAPTOP-AEL42LF4
board
Inventory
Events
LAPTOP-AEL42LF4 (004)
Search
DQL
Refresh
cluster.name: Ubuntu
agent.id: 004
Evaluated
Under evaluation
Add filter

10 Critical - Severity

38 High - Severity

47 Medium - Severity

9 Low - Severity

3 Pending - Evaluation

Top 5 vulnerabilities	Count
025-24070	2
CVE-2025-26682	2
025-55315	2
CVE-2007-4559	1
2015-4016	1

Top 5 OS	Count
Microsoft Windows 11 Home 10.0.26100.7171	107

Top 5 agents	Count
LAPTOP-AEL42LF4	107

Top 5 packages	Count
MySQL Server 8.0	45
Mozilla Firefox (x64 en-GB)	16
Python 3.10.8 (64-bit)	11
Steam	8
Visual Studio Community 2022	8

Most common vulnerability score
Most vulnerable OS families
Host OS type
windows
Vulnerabilities by year of publication
Count
40
30
20
8
6
4
-
Critical
High
Medium
Low
RIGHT ALT

Figure 6.10: