

VISUAL REPORT OF TASK-1

1) Wazuh Installation .

```
sudo apt update && sudo apt upgrade -y
```

```
sudo apt install curl apt-transport-https lsb-release gnupg -y
```

```
curl -sO https://packages.wazuh.com/4.12/wazuh-install.sh
```

```
sudo bash ./wazuh-install.sh -a
```

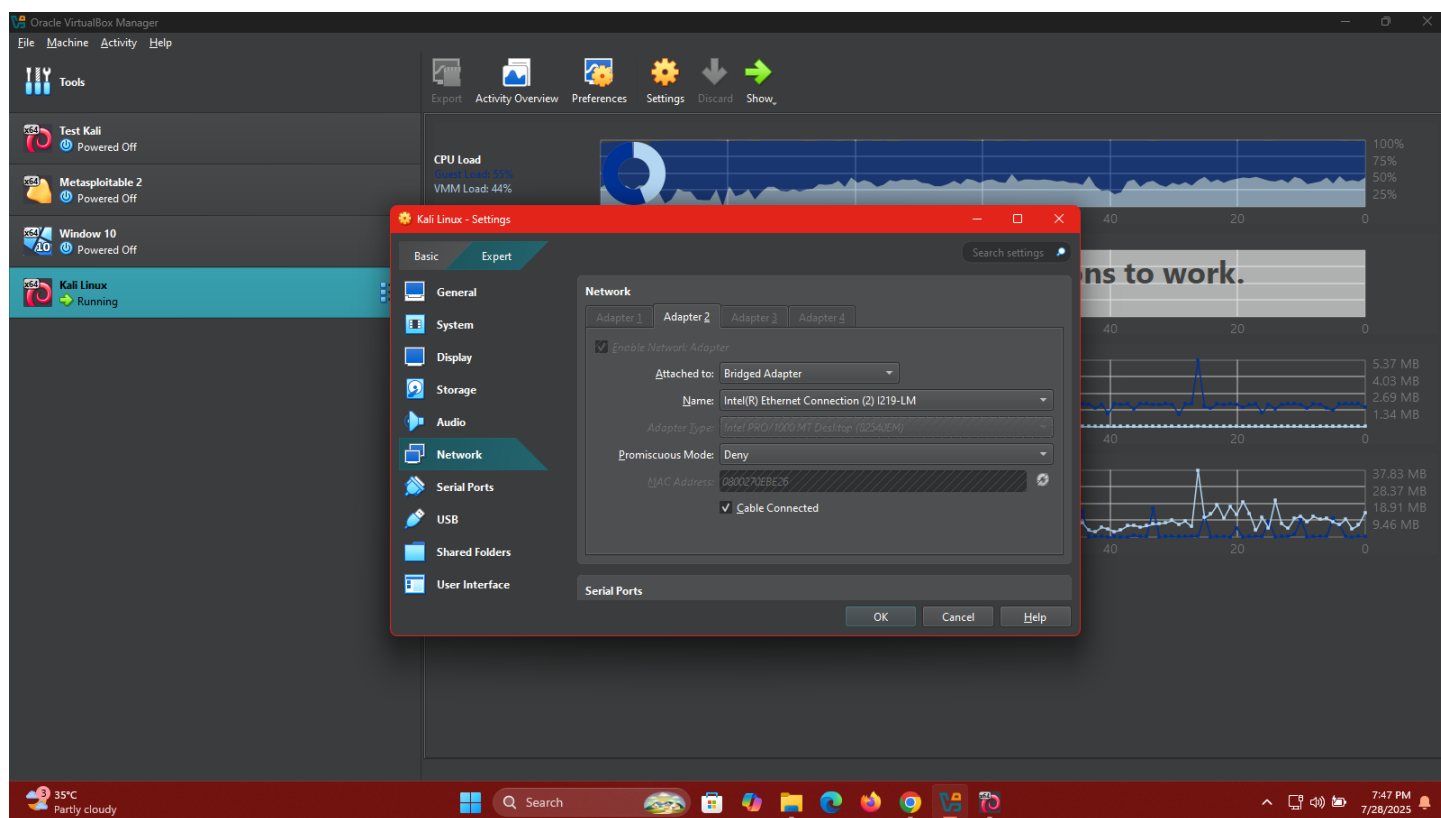
```
sudo ufw allow 1515/tcp
```

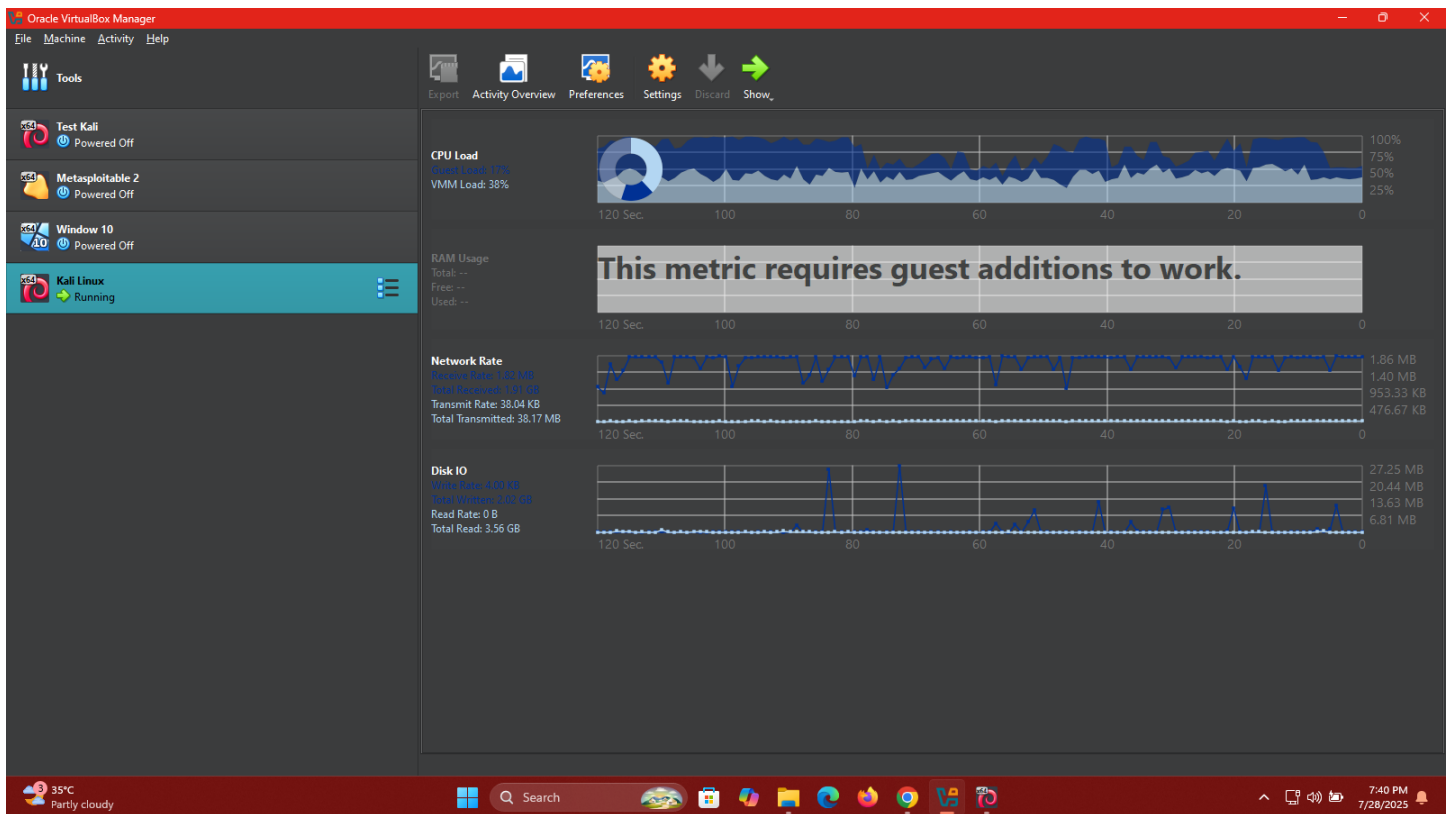
```
sudo ufw allow 1514/tcp
```

```
sudo ufw allow 443/tcp
```

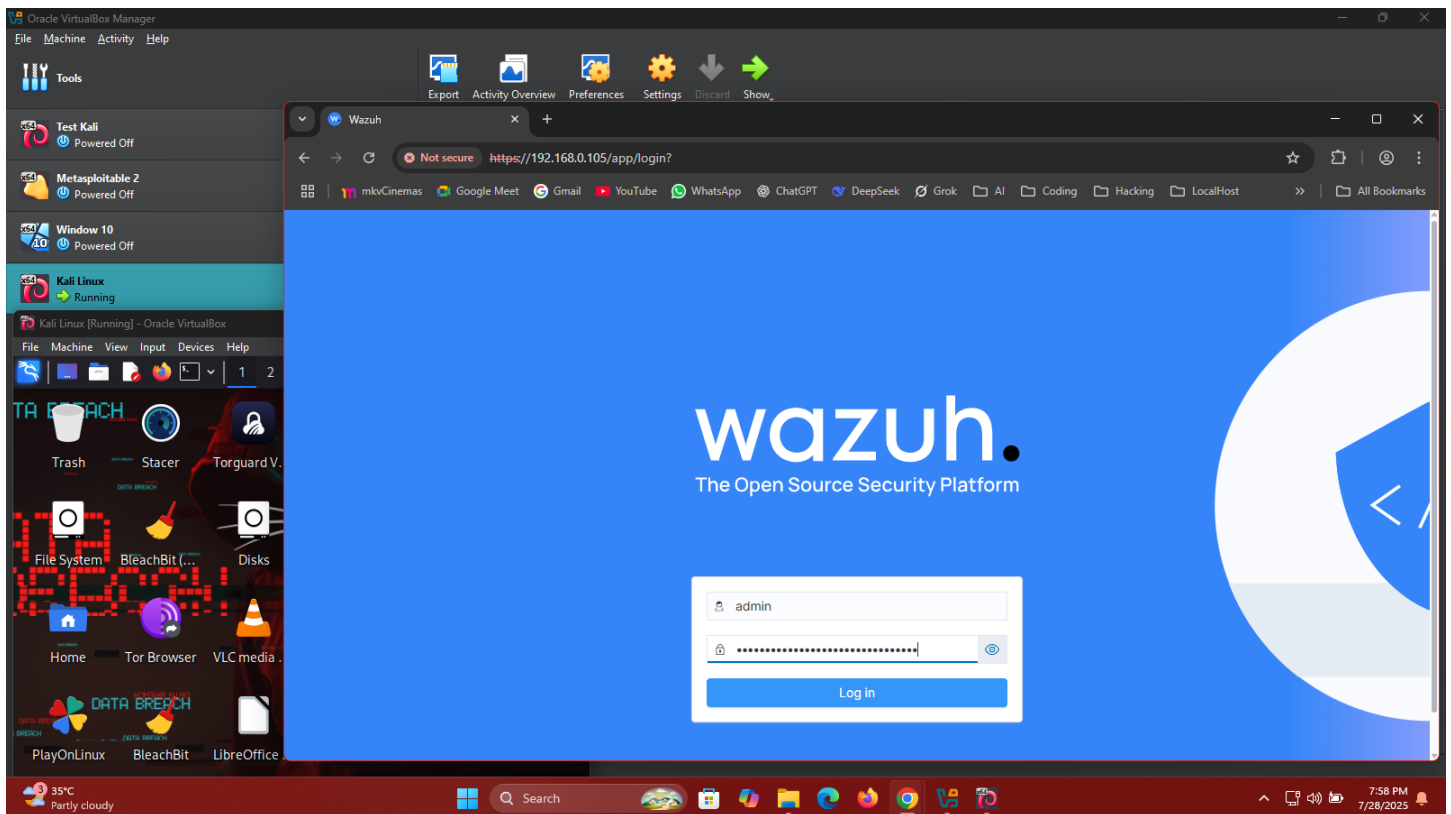
```
sudo ufw reload
```

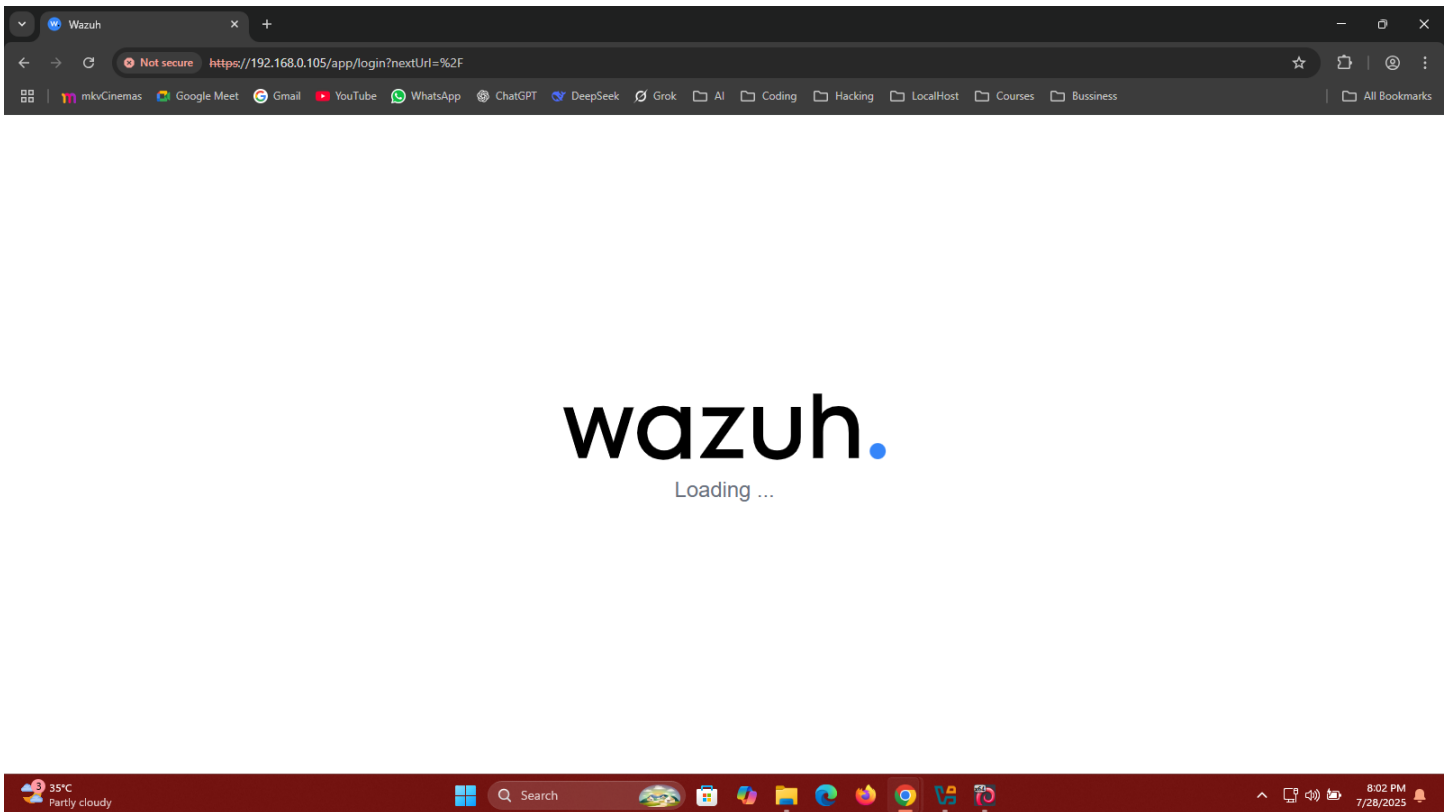
```
sudo ufw status
```



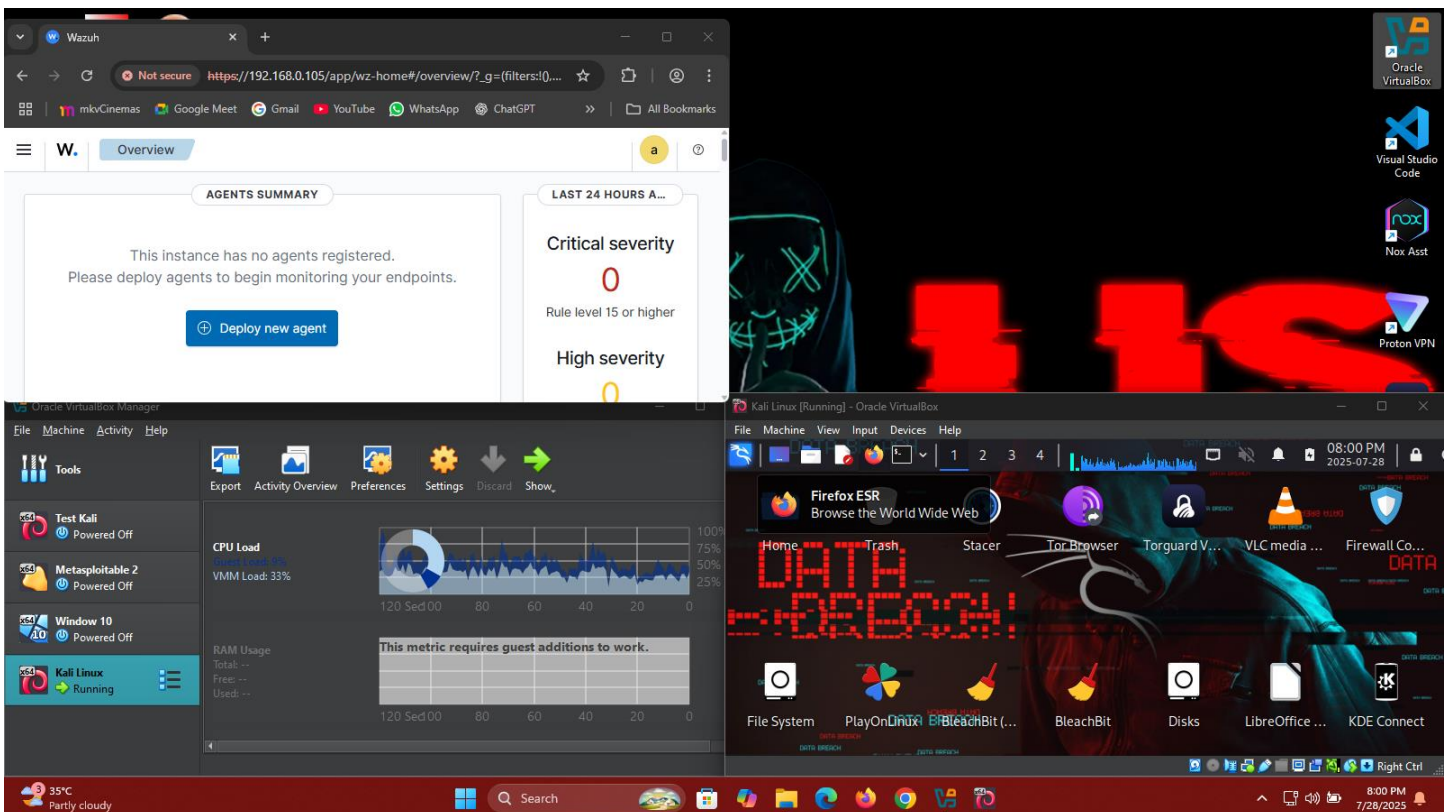


Accessing From Host !





Wazuh server on linux & Access Dashboard From Host Window .



Access With in linux as a whole system .

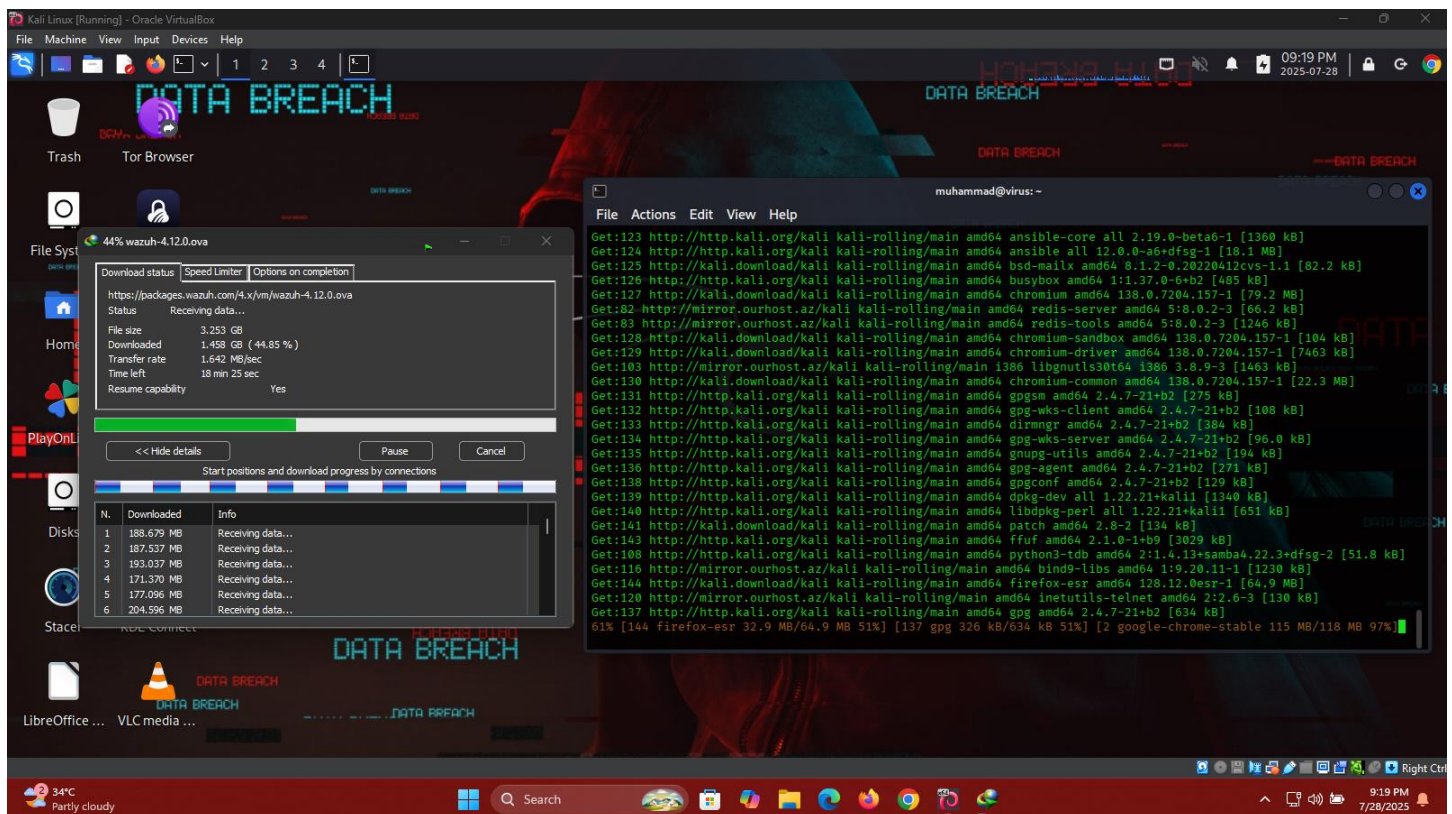
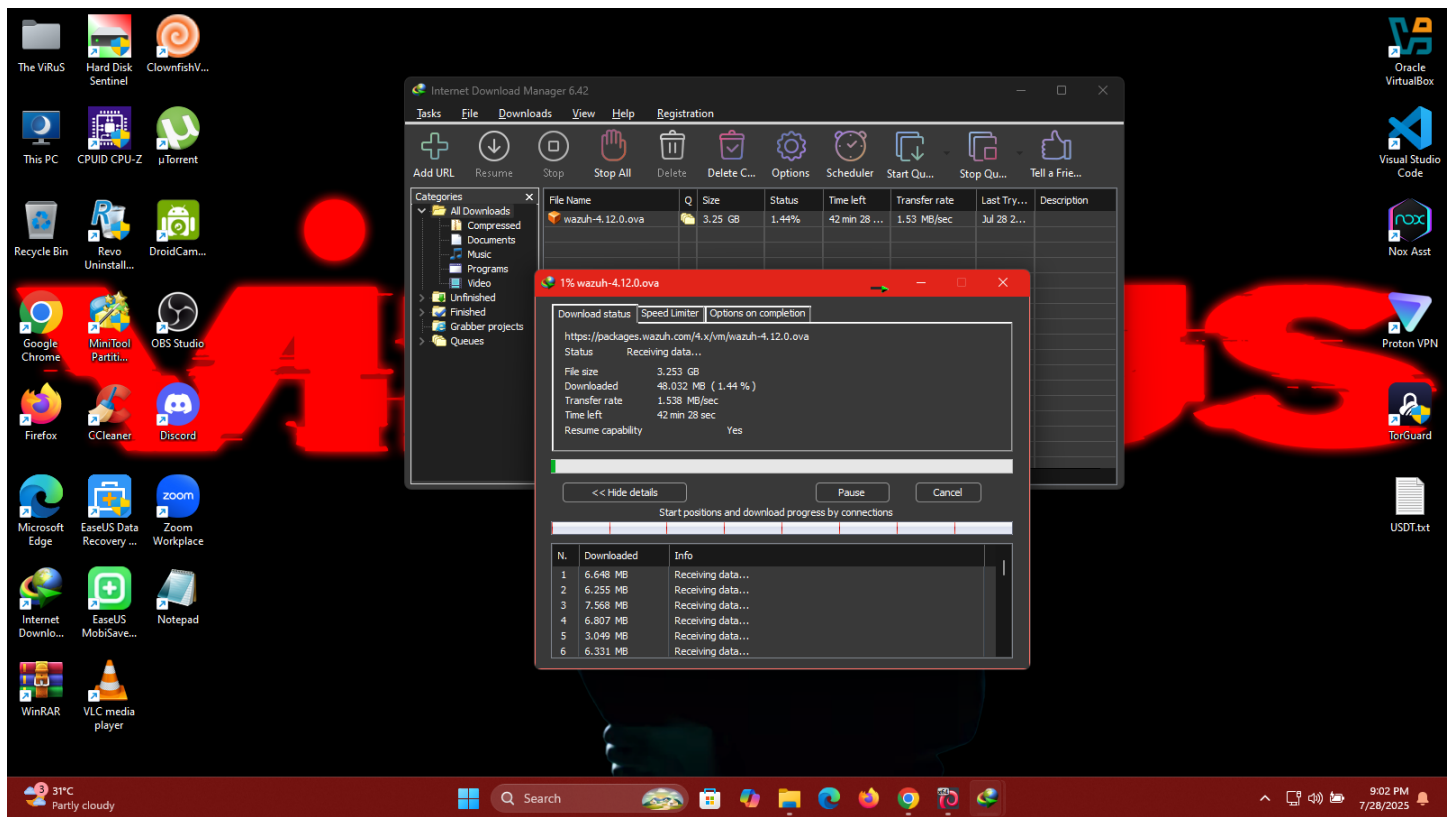
The screenshot shows the Wazuh dashboard interface. The top navigation bar includes a menu icon, the Wazuh logo, and the 'Overview' tab. The main content area is divided into several sections:

- AGENTS SUMMARY:** A box indicating that no agents are currently registered, with a 'Deploy new agent' button.
- LAST 24 HOURS ALERTS:** A summary of alerts by severity level:
 - Critical severity: 0 (Rule level 15 or higher)
 - High severity: 0 (Rule level 12 to 14)
 - Medium severity: 131 (Rule level 7 to 11)
 - Low severity: 112 (Rule level 0 to 6)
- ENDPOINT SECURITY:** A section with three sub-items:
 - 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, ownership, and attributes.
- THREAT INTELLIGENCE:** A section with two sub-items:
 - Threat Hunting:** Browse through your security alerts, identifying issues and threats in your environment.
 - MITRE ATT&CK:** Explore security alerts mapped to adversary tactics and techniques for better threat understanding.

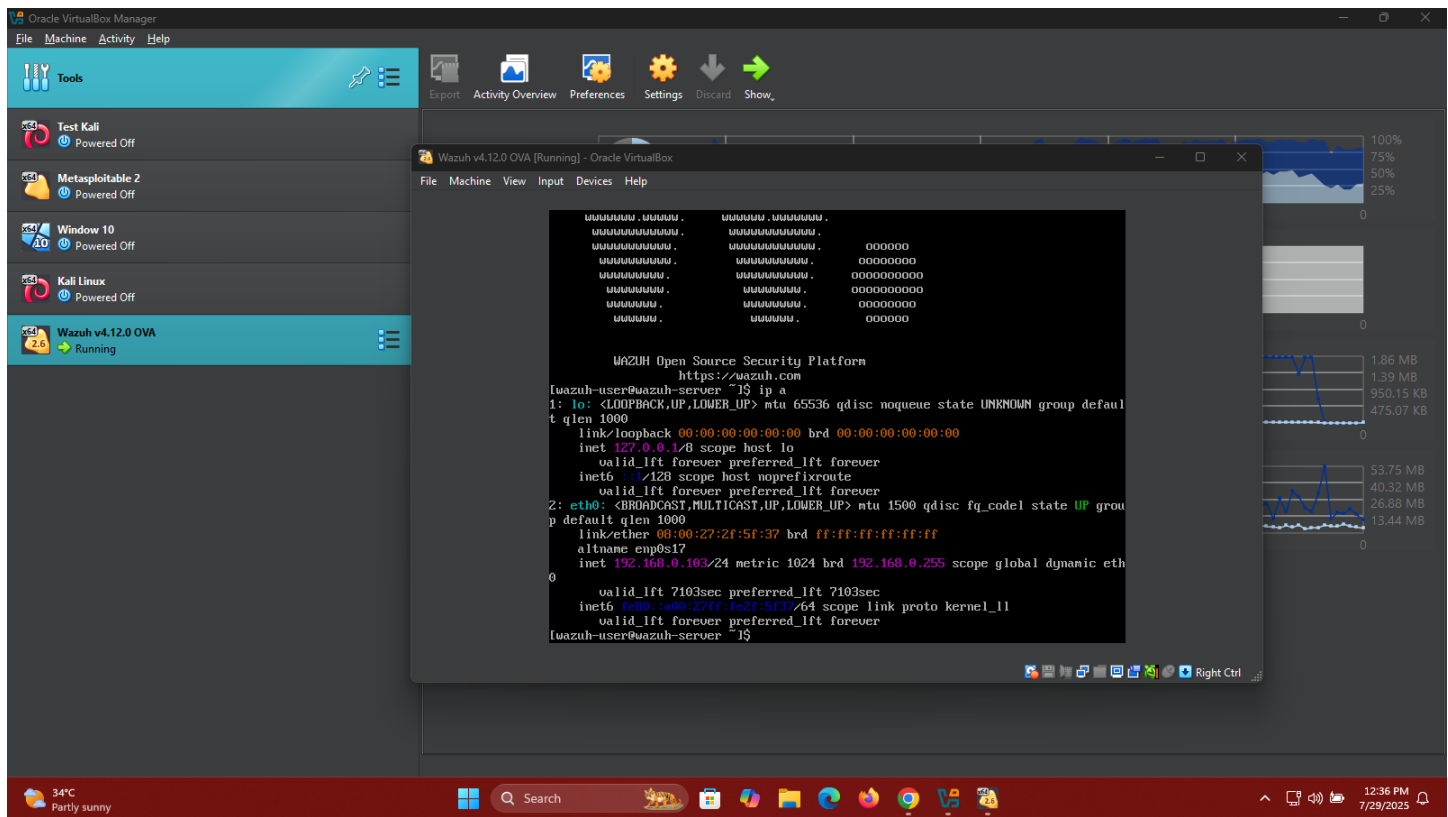
The bottom of the dashboard features a 'Recently viewed' sidebar on the left, listing various sections like Home, Explore, Endpoint security, Threat intelligence, Security operations, Cloud security, Agents management, Server management, Indexer management, and Dashboard management. The main content area below the overview section is partially visible, showing 'SECURITY OPERATIONS' and 'CLOUD SECURITY' sections.

The browser's address bar shows the URL: `https://192.168.0.105/app/wz-home#/overview/?_g=(filters:[]&refreshInterval:(pause:1t,value:0);time:(from:now-24h,to:now))&a=(filters:[]&query:(language:query,query:'))`. The browser's taskbar at the bottom shows various open applications and the system clock indicating 8:02 PM on 7/28/2025.

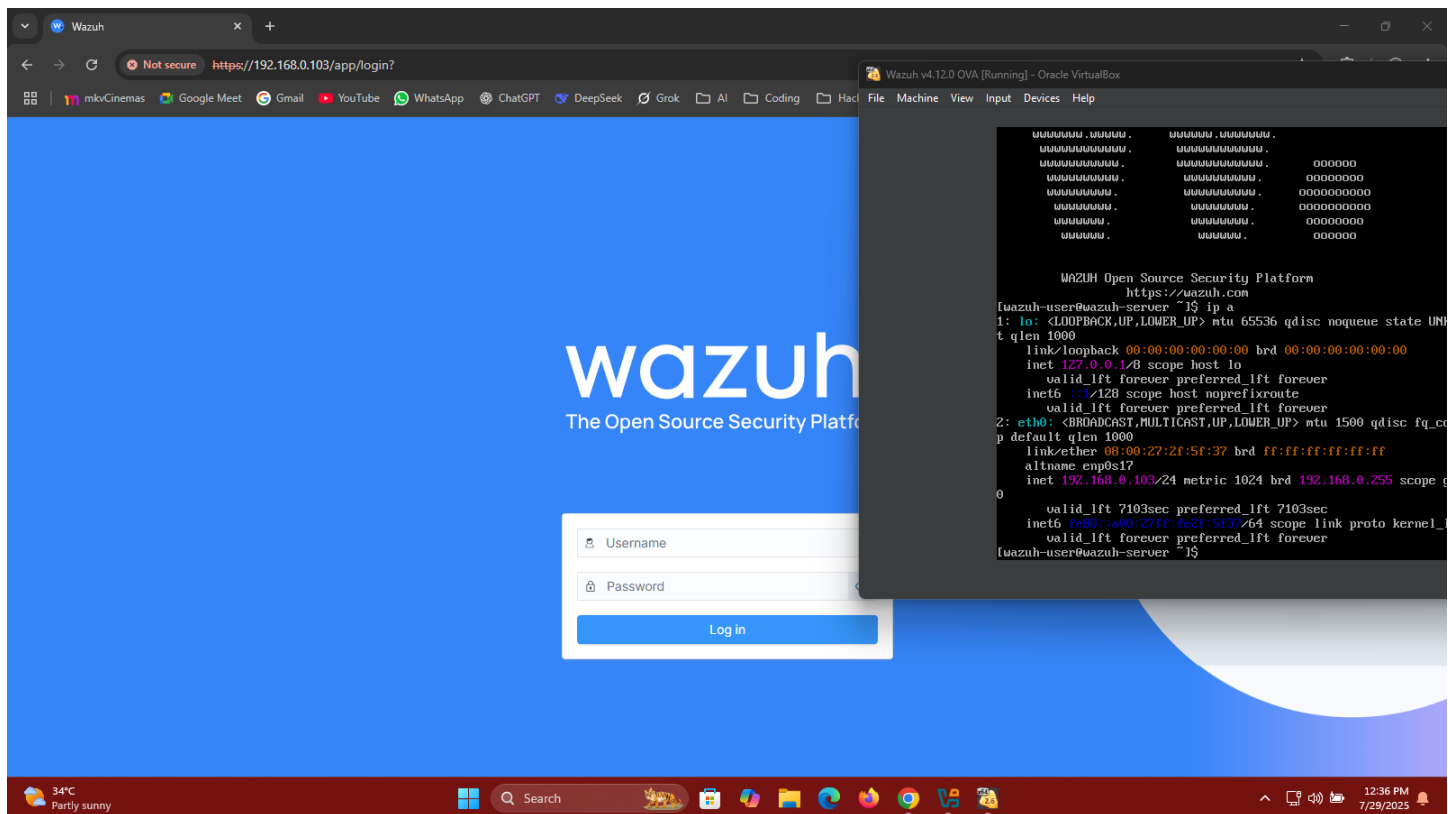
Installing wazuh as a separate server machine due to slow down of kali .



Running the OVA machine , separate full system . works perfect for me !



Accessing with Host , better & smoother then Kali .



The screenshot shows the Wazuh Open Source Security Platform interface in a web browser. The browser address bar shows the URL: `https://192.168.0.103/app/wz-home#/overview/?_g=(filters:[{}],refreshInterval:(pause:1,value:0),time:(from:now-24h,to:now))&a=(filters:[{}],query:(language:query,query:'))`. The interface has a sidebar with 'Overview' selected. The main content area shows 'AGENTS SUMMARY' with a message: 'This instance has no agents registered. Please deploy agents to begin monitoring your endpoints.' and a 'Deploy new agent' button. To the right, 'LAST 24 HOURS ALERTS' shows severity counts: Critical severity (0), High severity (0), Medium severity (2), and Low severity (8). Below this, there are sections for 'ENDPOINT' (Configuration Assessment and File Integrity Monitoring) and 'SECURITY'. A terminal window titled 'Wazuh v4.12.0 OVA [Running] - Oracle VirtualBox' is overlaid on the interface, displaying network configuration details for the 'wazuh-user@wazuh-server' machine, including IP addresses, MAC addresses, and interface names.

2) Installing Wazuh Agent and Configuration !

```
curl -s https://packages.wazuh.com/key/GPG-KEY-WAZUH | gpg --dearmor | sudo tee
/usr/share/keyrings/wazuh.gpg > /dev/null
```

```
echo "deb [signed-by=/usr/share/keyrings/wazuh.gpg] https://packages.wazuh.com/4.x/apt/ stable
main" | sudo tee /etc/apt/sources.list.d/wazuh.list
```

```
deb [signed-by=/usr/share/keyrings/wazuh.gpg] https://packages.wazuh.com/4.x/apt/ stable main
```

```
sudo apt install wazuh-agent
```

now ,

```
sudo gedit /var/ossec/etc/ossec.conf
```

adding server ,

```
<client>
```

```
<server>
```

```
<address>192.168.0.100</address>
```

```
<port>1514</port>
```

```
sudo systemctl enable wazuh-agent
```

```
sudo systemctl start wazuh-agent
```

```
sudo systemctl status wazuh-agent
```

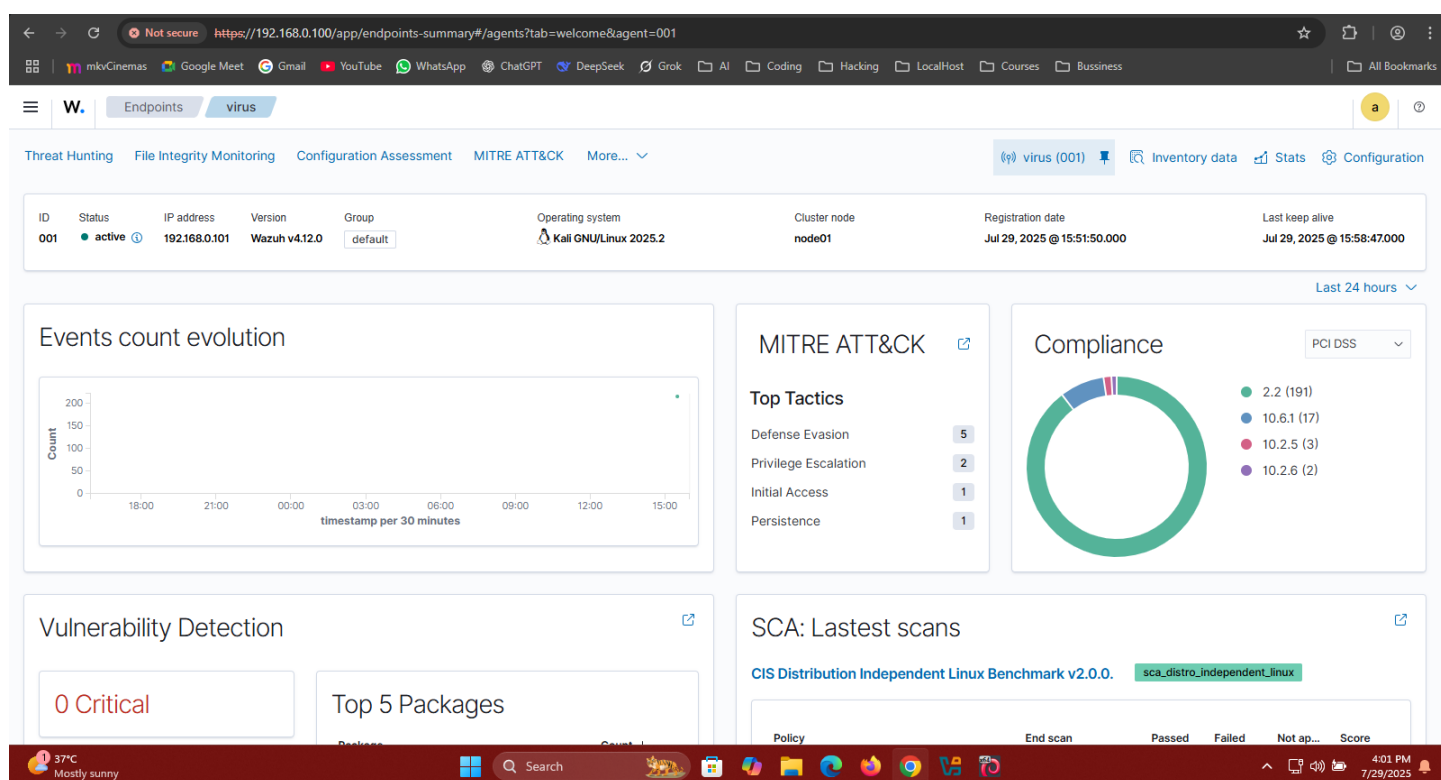
```
disable updates ,
```

```
sudo sed -i "s/^deb/#deb/" /etc/apt/sources.list.d/wazuh.list
```

```
echo "wazuh-agent hold" | sudo dpkg --set-selections
```

```
sudo apt-get update
```

ALL DONE !

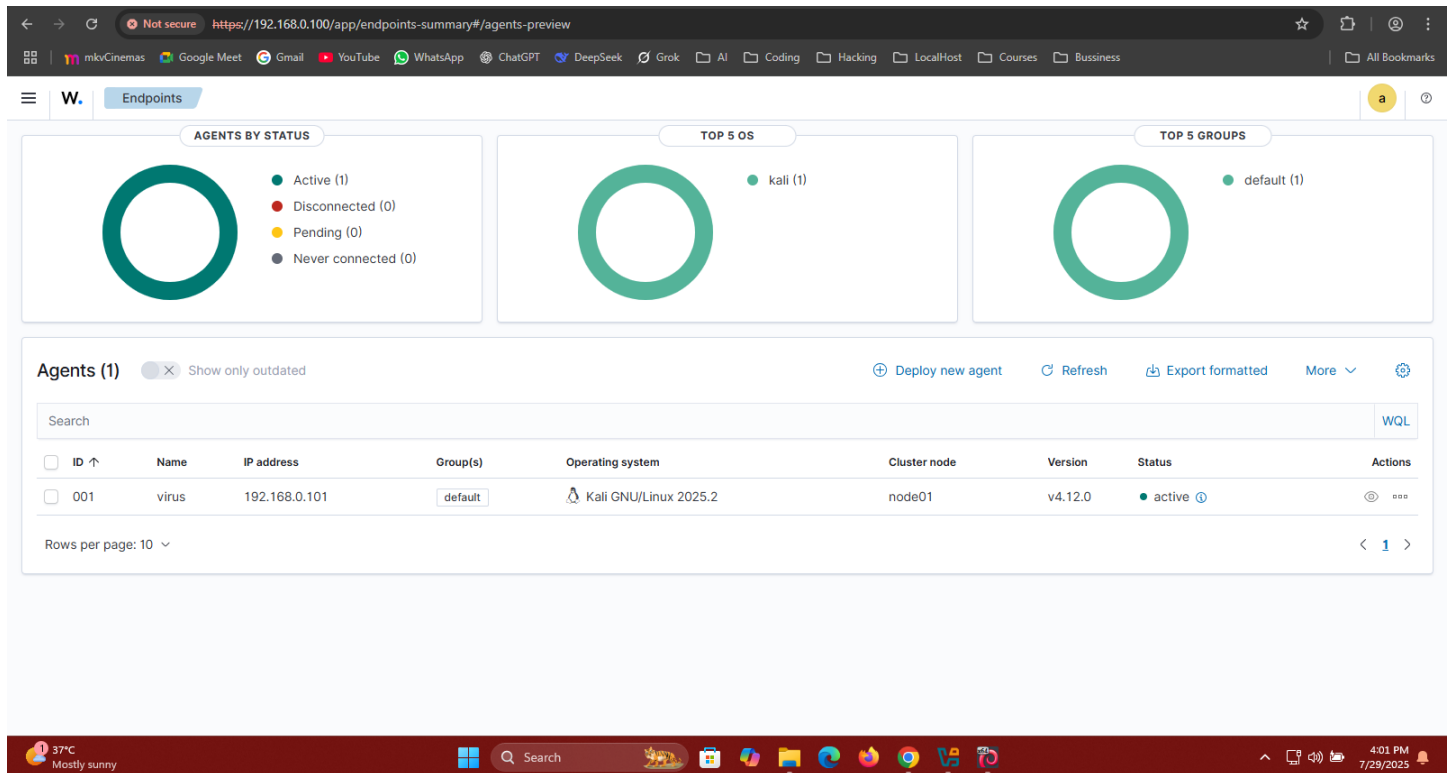


NOTE > after full setup , I note that my wifi router and default all routers run on DHCP server . ip assignment to nodes is automatic . so if our ip changes on another start (agent or server) . the configuration will be miss match and It will make issue . to fix this I have 2 options ,

- 1) Changes in internal configs of machine and assign static ip but in case of VMs we can stuck .
- 2) Access admin panel of my router and reserved the 3 ips for my agents and server in the DHCP range using mac .

So I chose to go for option 2 and it works perfectly !

Dashboard overview



Collecting logs & inventory .

The screenshot shows the 'File Integrity Monitoring' (FIM) inventory page for the 'virus' agent. It displays a table of files with columns for File, Last modified, User, User ID, Group, Group ID, and Size. The table lists various system files, including /bin, /boot/System.map, /boot/config, /boot/grub/fonts, /boot/grub/grub.cfg, /boot/grub/grubenv, /boot/grub/i386-pc/915resolution.mod, /boot/grub/i386-pc/acpi.mod, /boot/grub/i386-pc/adler32.mod, and /boot/grub/i386-pc/affs.mod. The bottom of the screenshot shows a Windows taskbar with a weather widget indicating 37°C and the date 7/29/2025.

File Integrity M... virus

Dashboard Inventory Events

Files (7,808) Refresh Export formatted

Search WQL

File	Last modified	User	User ID	Group	Group ID	Size
/bin	Mar 9, 2025 @ 02:13:31.000	root	0	root	0	7
/boot/System.map-6.12.25-amd64	Apr 30, 2025 @ 15:25:43.000	root	0	root	0	83
/boot/System.map-6.12.33+kali-amd64	Jun 25, 2025 @ 15:20:30.000	root	0	root	0	83
/boot/config-6.12.25-amd64	Apr 30, 2025 @ 15:25:43.000	root	0	root	0	283324
/boot/config-6.12.33+kali-amd64	Jun 25, 2025 @ 15:20:30.000	root	0	root	0	283418
/boot/grub/fonts/unicode.pf2	Jul 4, 2025 @ 14:50:23.000	root	0	root	0	2411806
/boot/grub/grub.cfg	Jul 29, 2025 @ 15:23:05.000	root	0	root	0	8882
/boot/grub/grubenv	Mar 9, 2025 @ 02:29:07.000	root	0	root	0	1024
/boot/grub/i386-pc/915resolution.mod	Jul 4, 2025 @ 14:50:23.000	root	0	root	0	7820
/boot/grub/i386-pc/acpi.mod	Jul 4, 2025 @ 14:50:23.000	root	0	root	0	10576
/boot/grub/i386-pc/adler32.mod	Jul 4, 2025 @ 14:50:23.000	root	0	root	0	1200
/boot/grub/i386-pc/affs.mod	Jul 4, 2025 @ 14:50:23.000	root	0	root	0	5644

3) COMMANDS USED .

Some mostly commands used after setup .

```
sudo gedit /var/ossec/etc/ossec.conf
```

```
sudo systemctl enable wazuh-agent
```

```
sudo systemctl start wazuh-agent
```

```
sudo systemctl status wazuh-agent
```

```
sudo systemctl restart wazuh-agent
```

Check the agent log: `sudo tail -n 50 /var/ossec/logs/ossec.log`

Wazuh Manager (OVA) Logs : `sudo tail -n 100 /var/ossec/logs/alerts/alerts.json | grep test_fim`

4) File Integrity Monitoring (FIM) .

Adding directories and setting agent time to 3600(1hr)

```
sudo gedit /var/ossec/etc/ossec.conf
```

```
<directories check_all="yes" report_changes="yes" realtime="yes">/root</directories>
```

```
<directories check_all="yes" report_changes="yes" realtime="yes">/etc</directories>
```

```
<directories check_all="yes" report_changes="yes" realtime="yes">/home</directories>
```

```
<directories check_all="yes" report_changes="yes" realtime="yes">/usr/bin</directories>
```

```
<directories check_all="yes" report_changes="yes" realtime="yes">/home/virus</directories>
```

,

Restart the agent ,

```
sudo systemctl restart wazuh-agent
```

after changing in directories and files , let's confirm if server received .

```
sudo tail -n 100 /var/ossec/logs/alerts/alerts.json | grep test_fim
```

ALL SET !

Real time FIM reports .

0 High

1 Medium

0 Low

Package	Count ↓
cryptography	1

Policy	End scan	Passed	Failed	Not ap...	Score
CIS Distribution Independent Linux Benchmark v2.0.0.	Jul 29, 2025 @ 19:45:48.000	83	99	8	45%

FIM: Recent events

Time ↓	Path	Action	Rule description	Rule Lev...	Rule Id
Jul 29, 2025 @ 19:51:57.912	/home/virus/.zsh_history	modified	Integrity checksum changed.	7	550
Jul 29, 2025 @ 19:51:57.912	/home/virus/.xsession-errors	modified	Integrity checksum changed.	7	550
Jul 29, 2025 @ 19:51:57.671	/home/virus/.config/qterminal.org/qterminal.ini	modified	Integrity checksum changed.	7	550
Jul 29, 2025 @ 19:51:57.661	/home/virus/.config/Thunar/accels.scm	modified	Integrity checksum changed.	7	550

FIM dashboard .

Wazuh

File Integrity M...virus

DashboardInventoryEvents

SearchDQLLast 24 hoursShow datesRefresh

manager.name: wazuh-serverrule.groups: syscheckagent.id: 001Add filter

Most active users

virus (100%)

Actions

modified (100%)

Events

modified

Files added

No results found

Files modified

/home/virus/.config/TI
/home/virus/.config/qt
/home/virus/.xsession
/home/virus/.zsh_hist

Files deleted

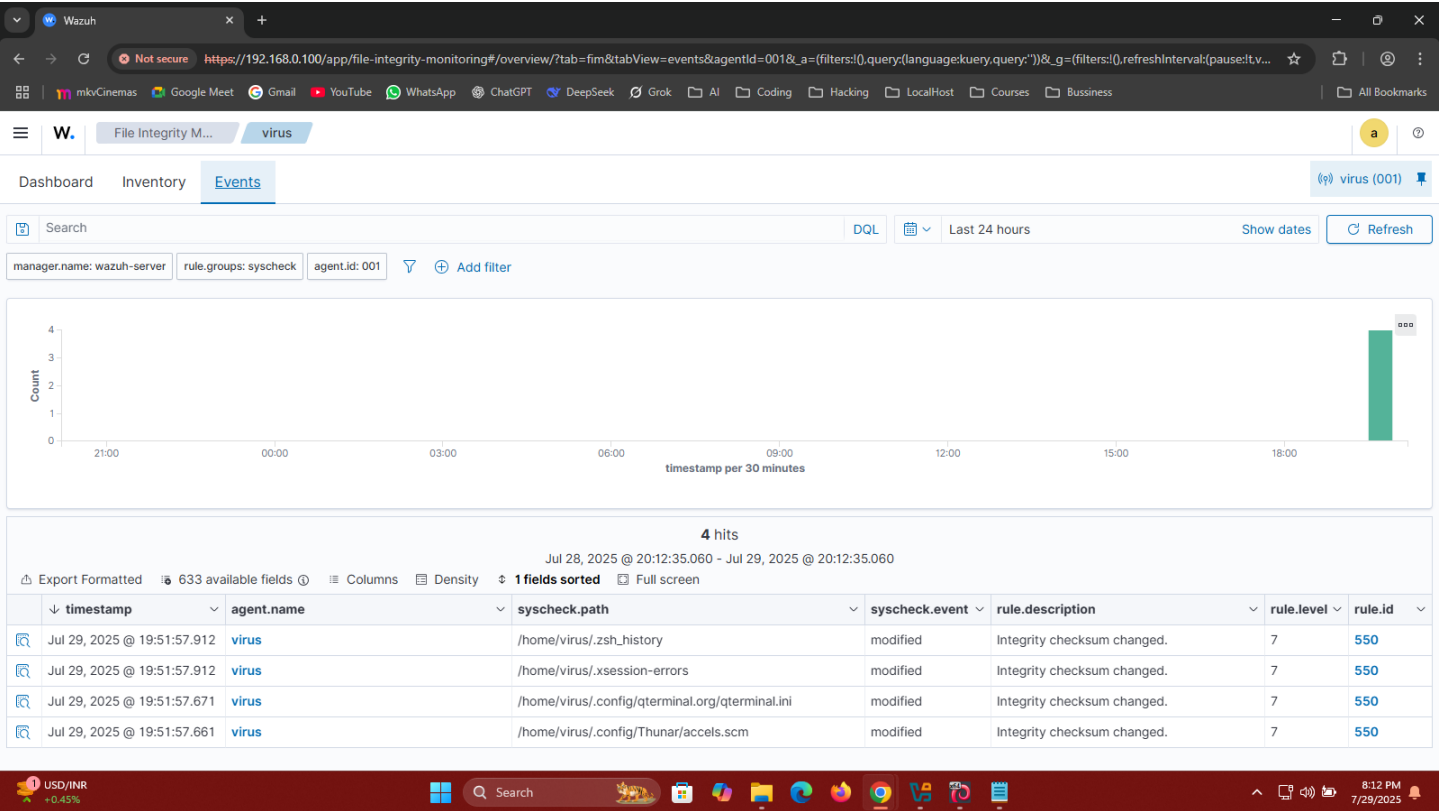
No results found

USD/INR
+0.45%

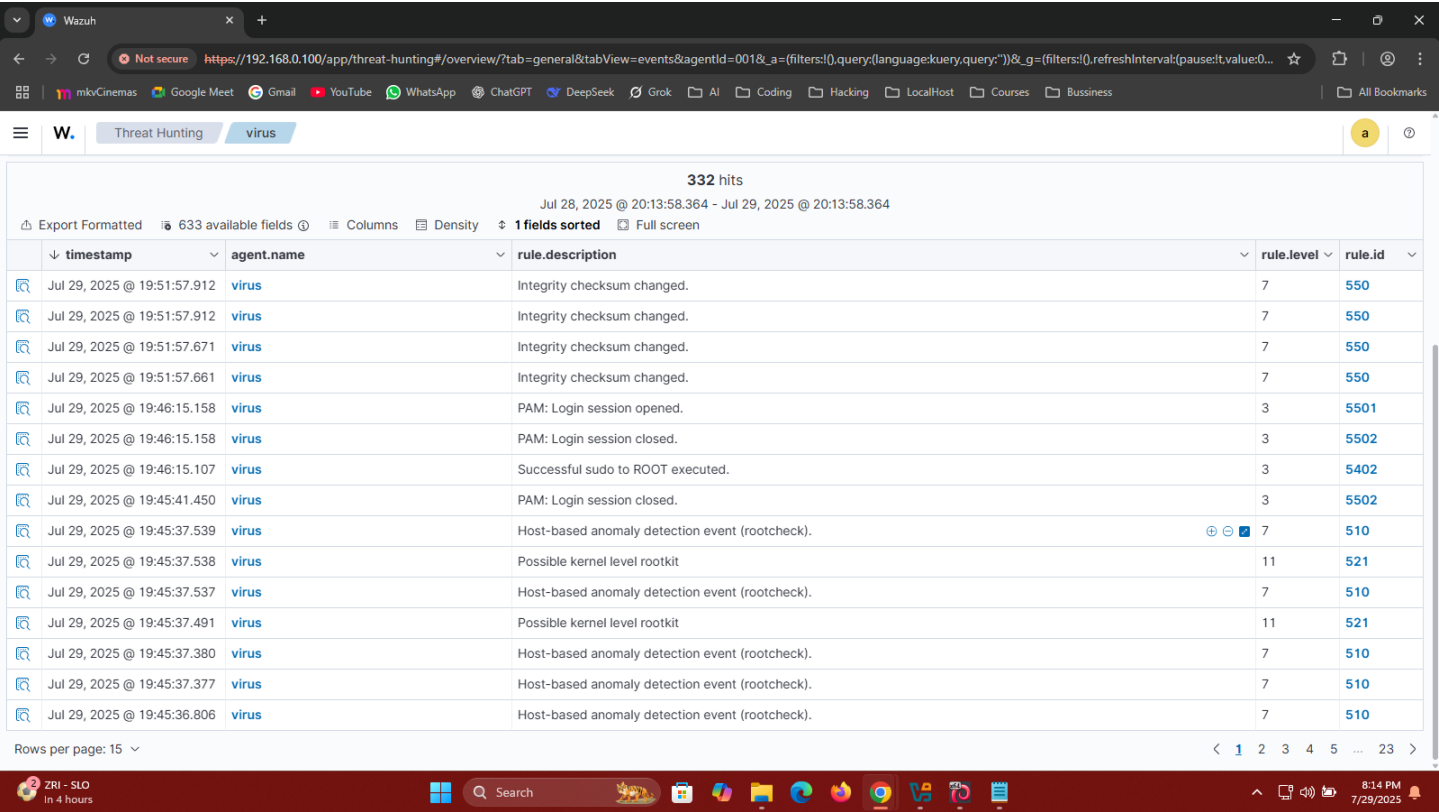
Search

8:12 PM
7/29/2025

Recent events FIM .



Threat Hunting Logs . Real Time Catch .



The End

SYED MUHAMMAD SHAH