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

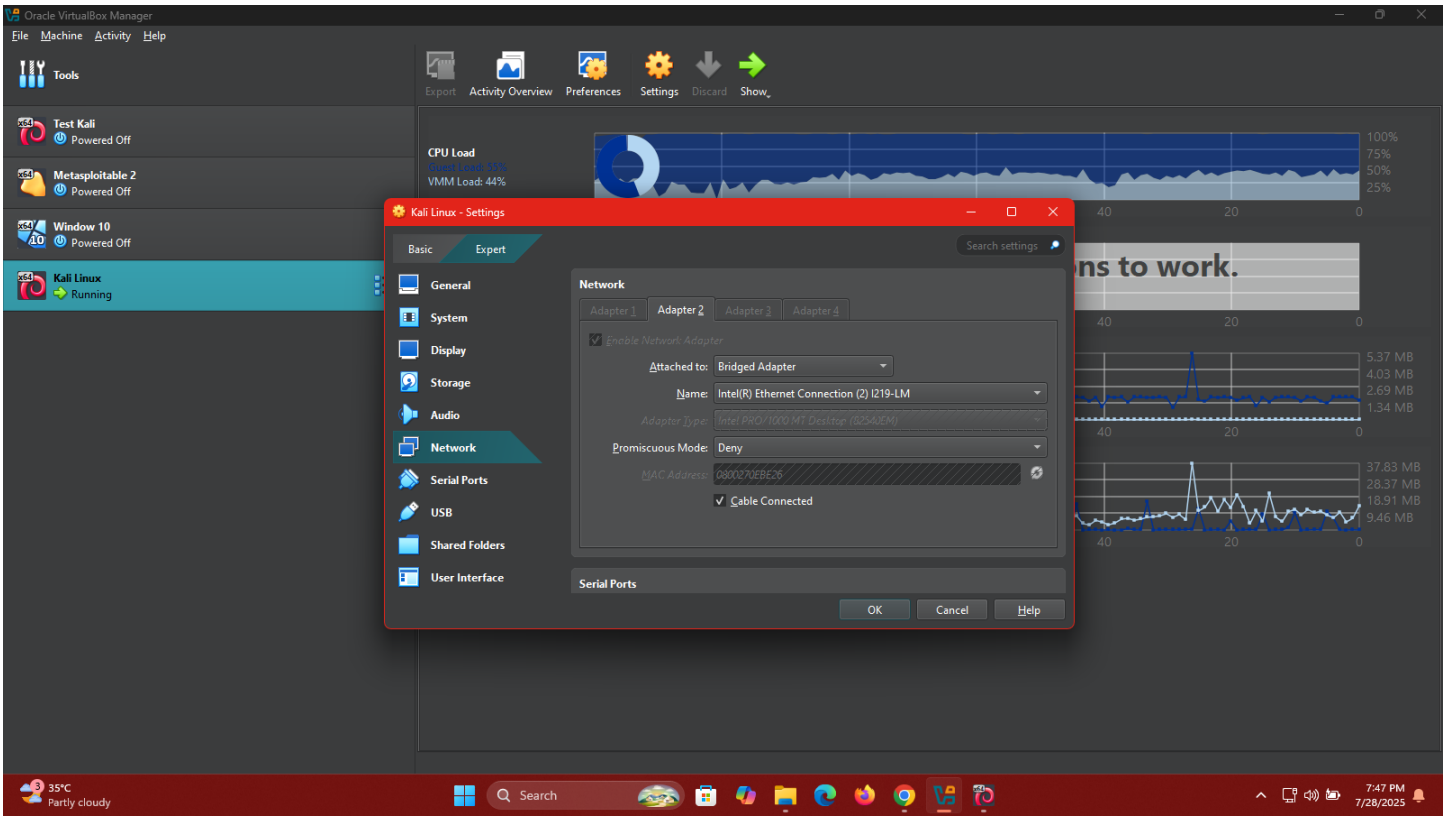
sudo ufw allow 1515/tcp

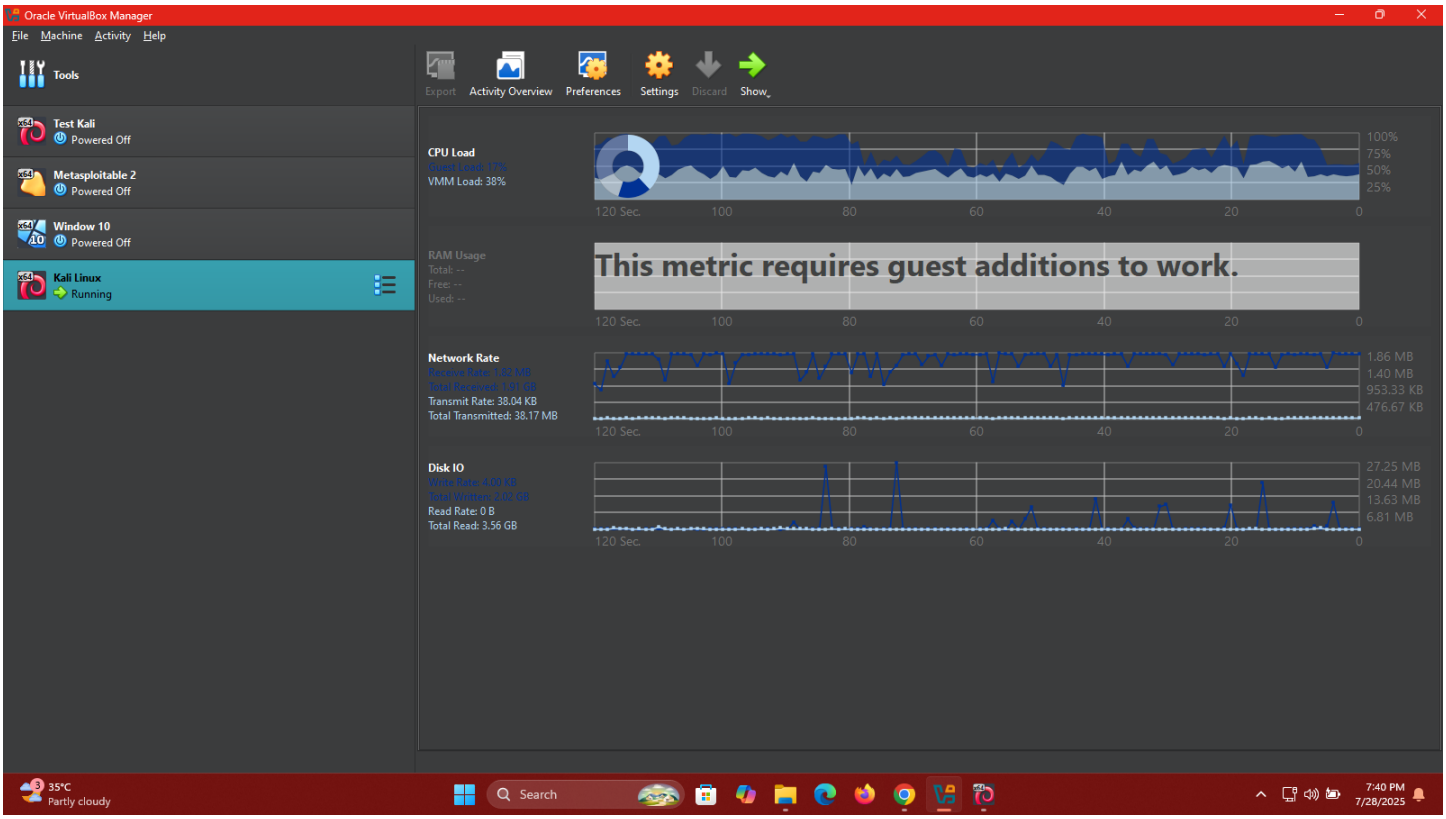
sudo ufw allow 1514/tcp

sudo ufw allow 443/tcp

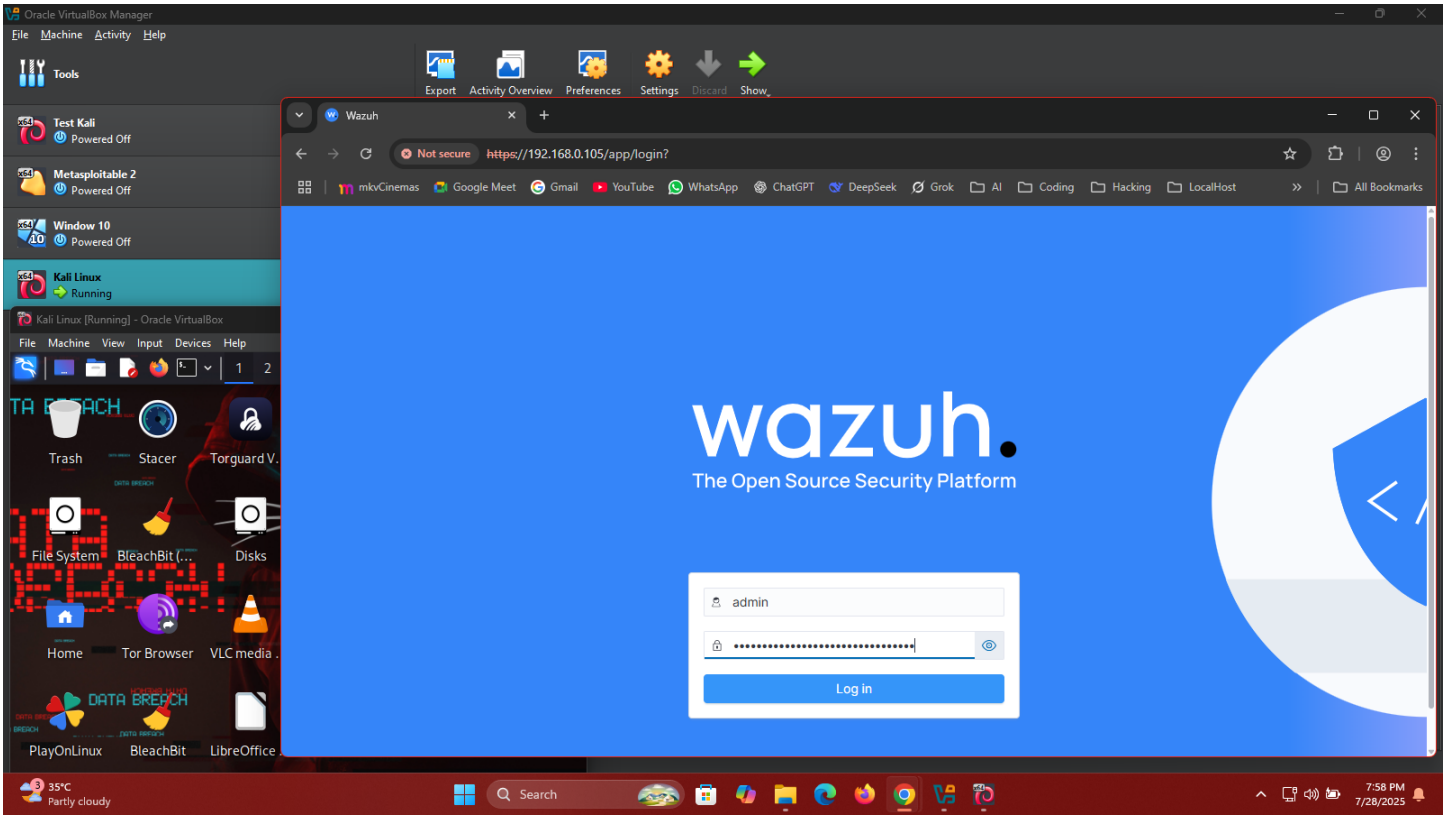
sudo ufw reload

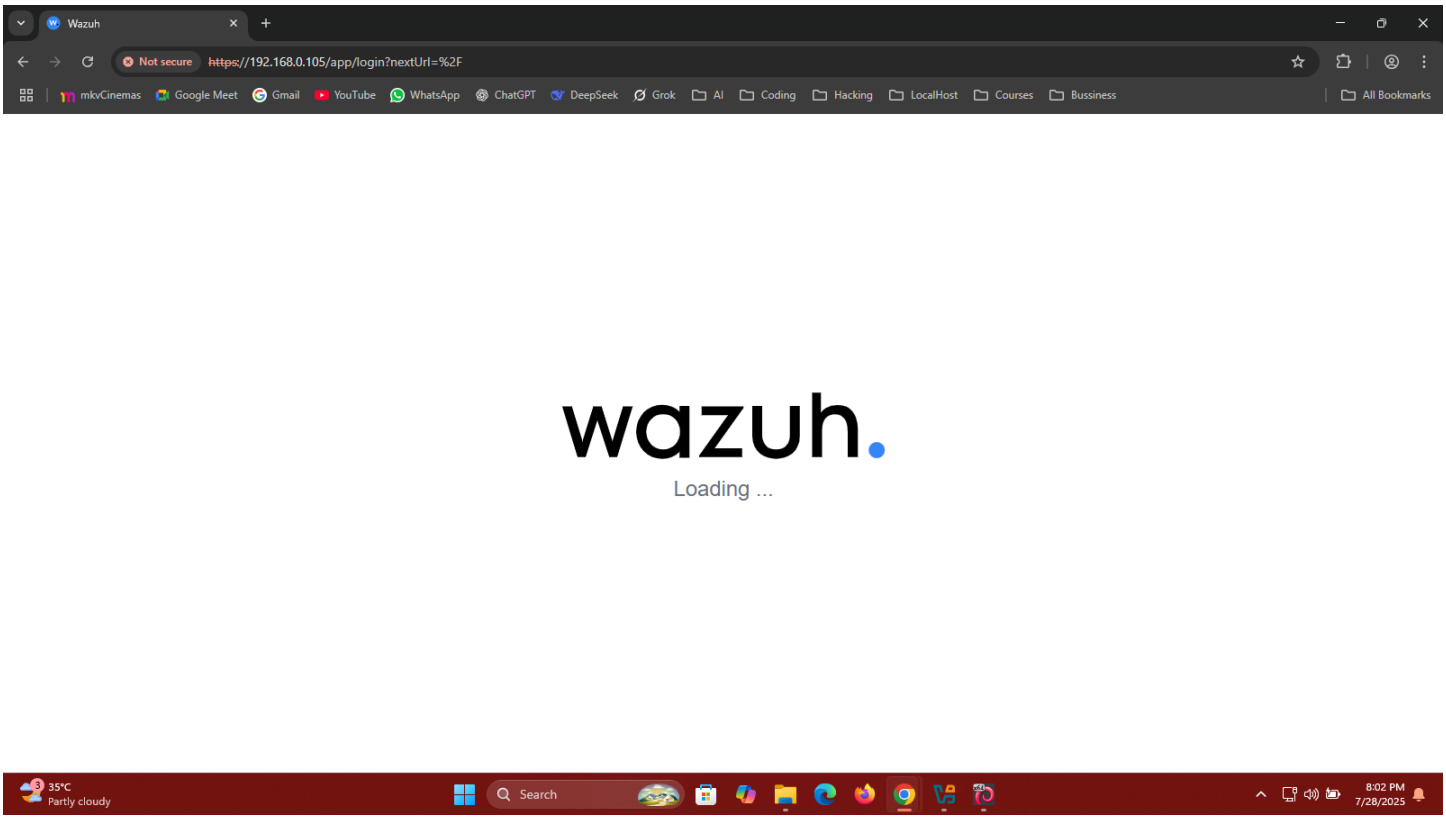
sudo ufw status



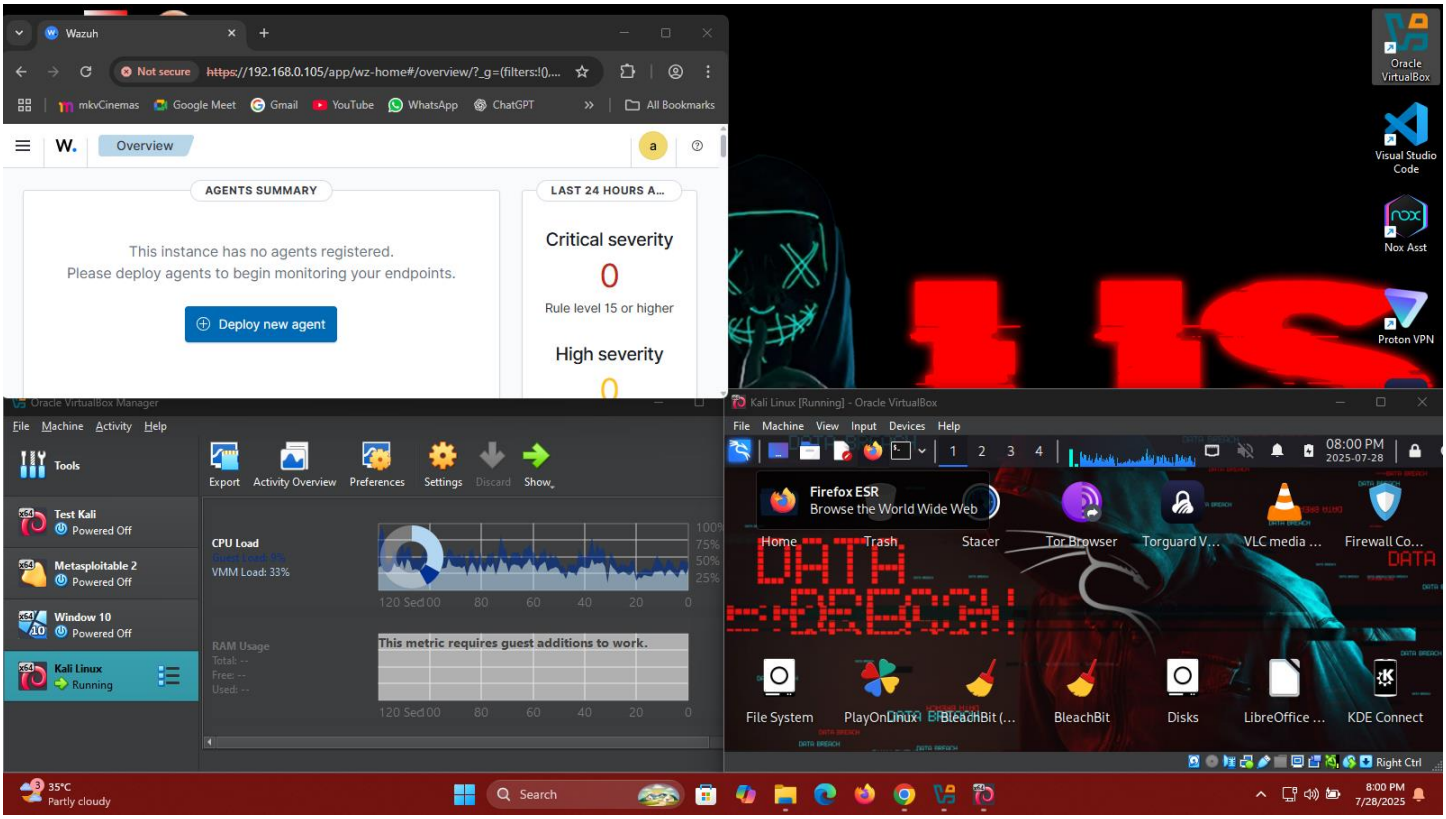


Accessing From Host !

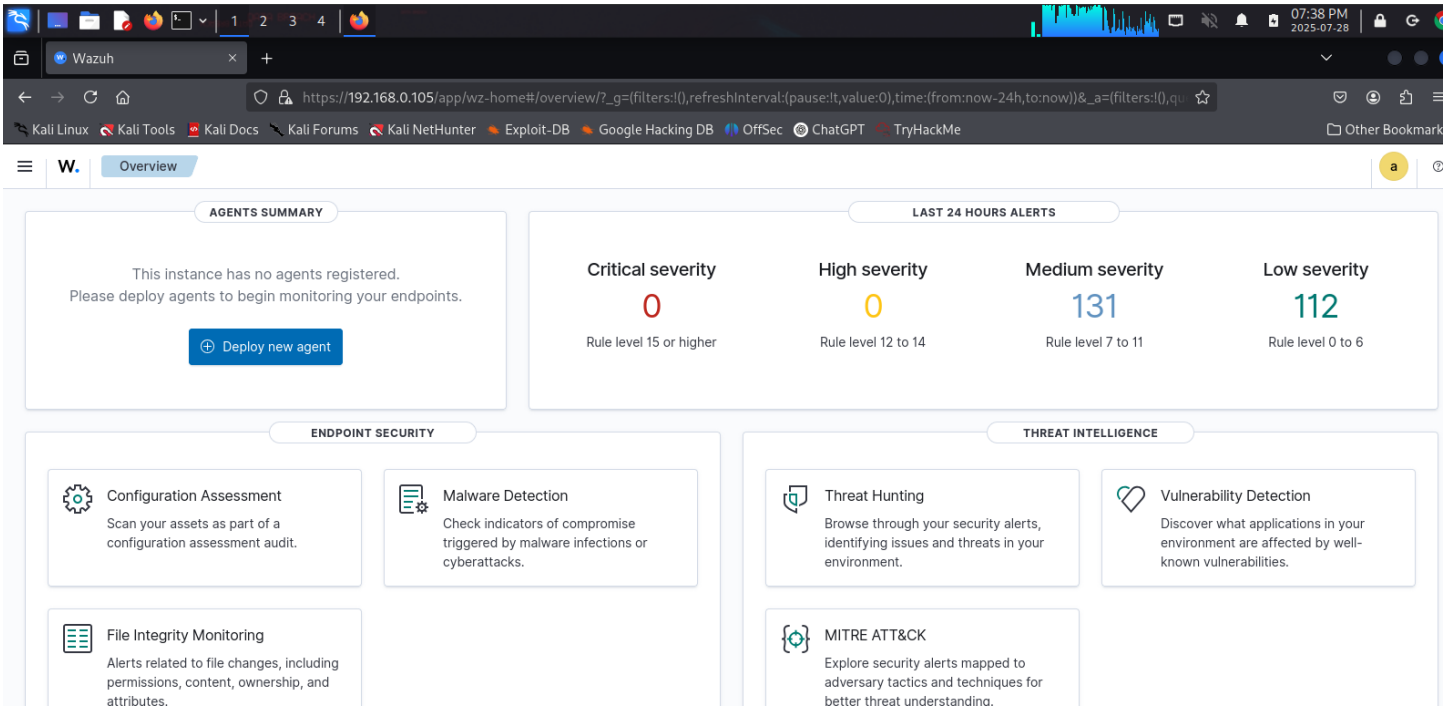


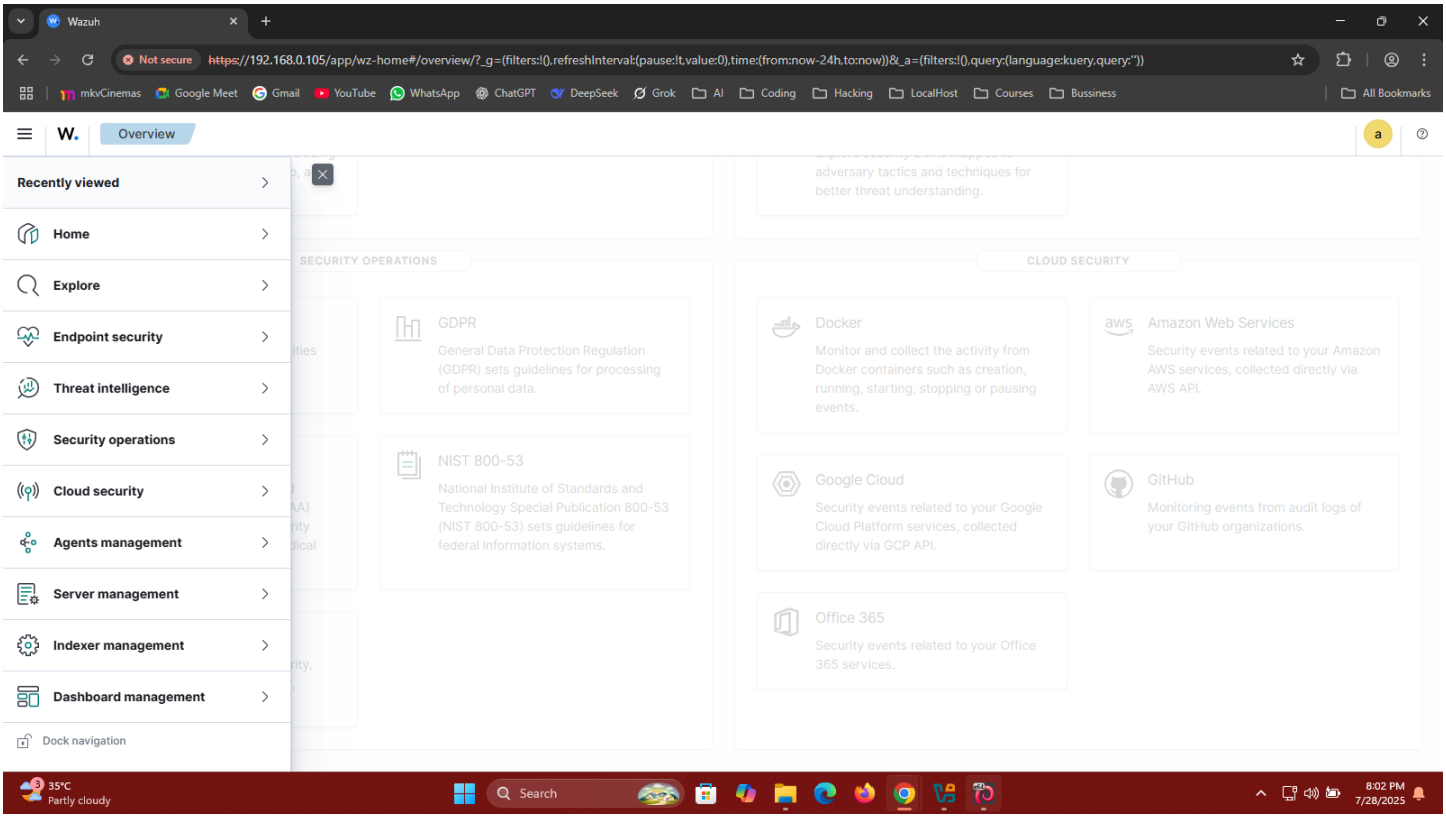


Wazuh server on linux & Access Dashboard From Host Window .

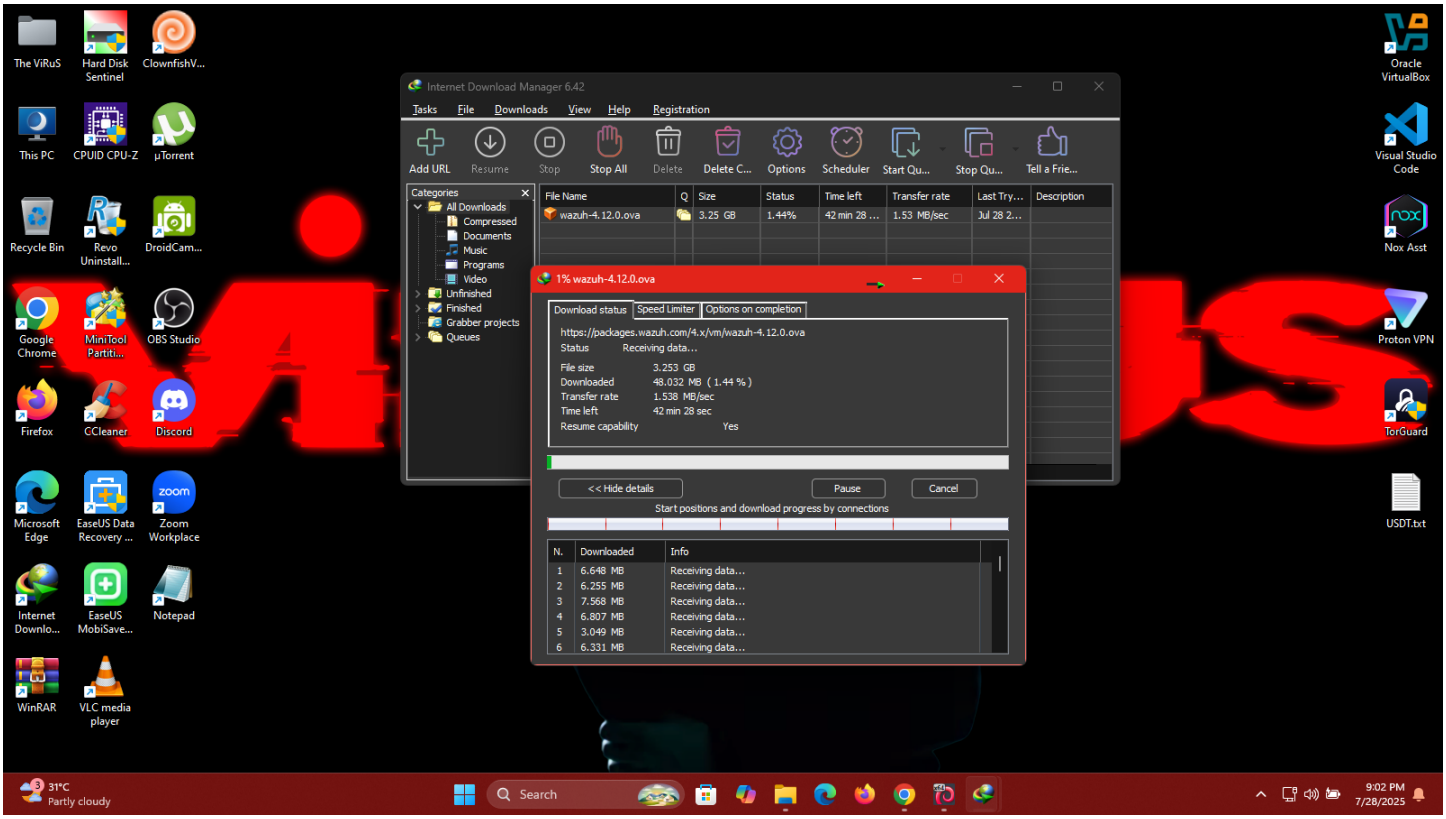


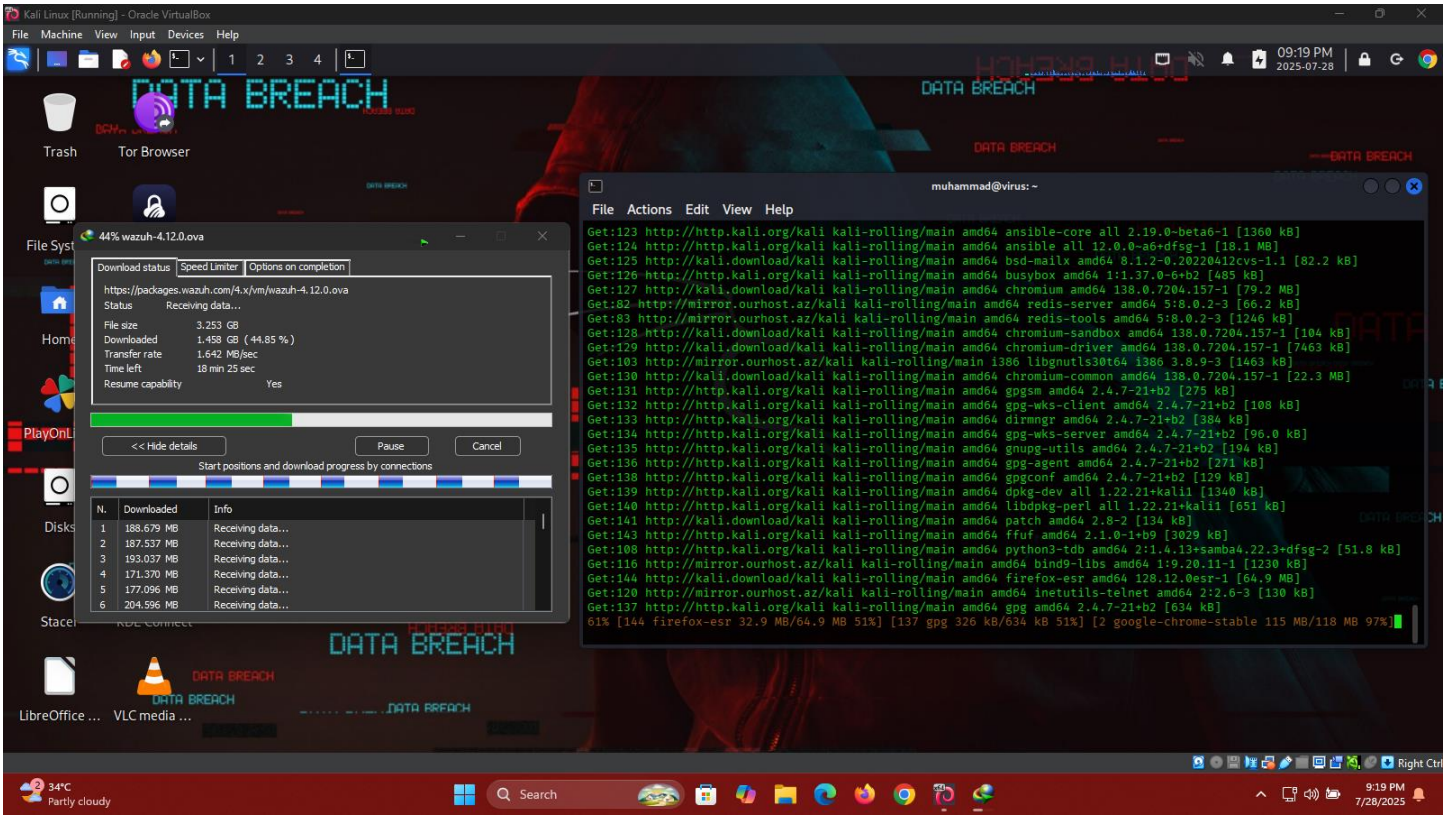
Access With in linux as a whole system .



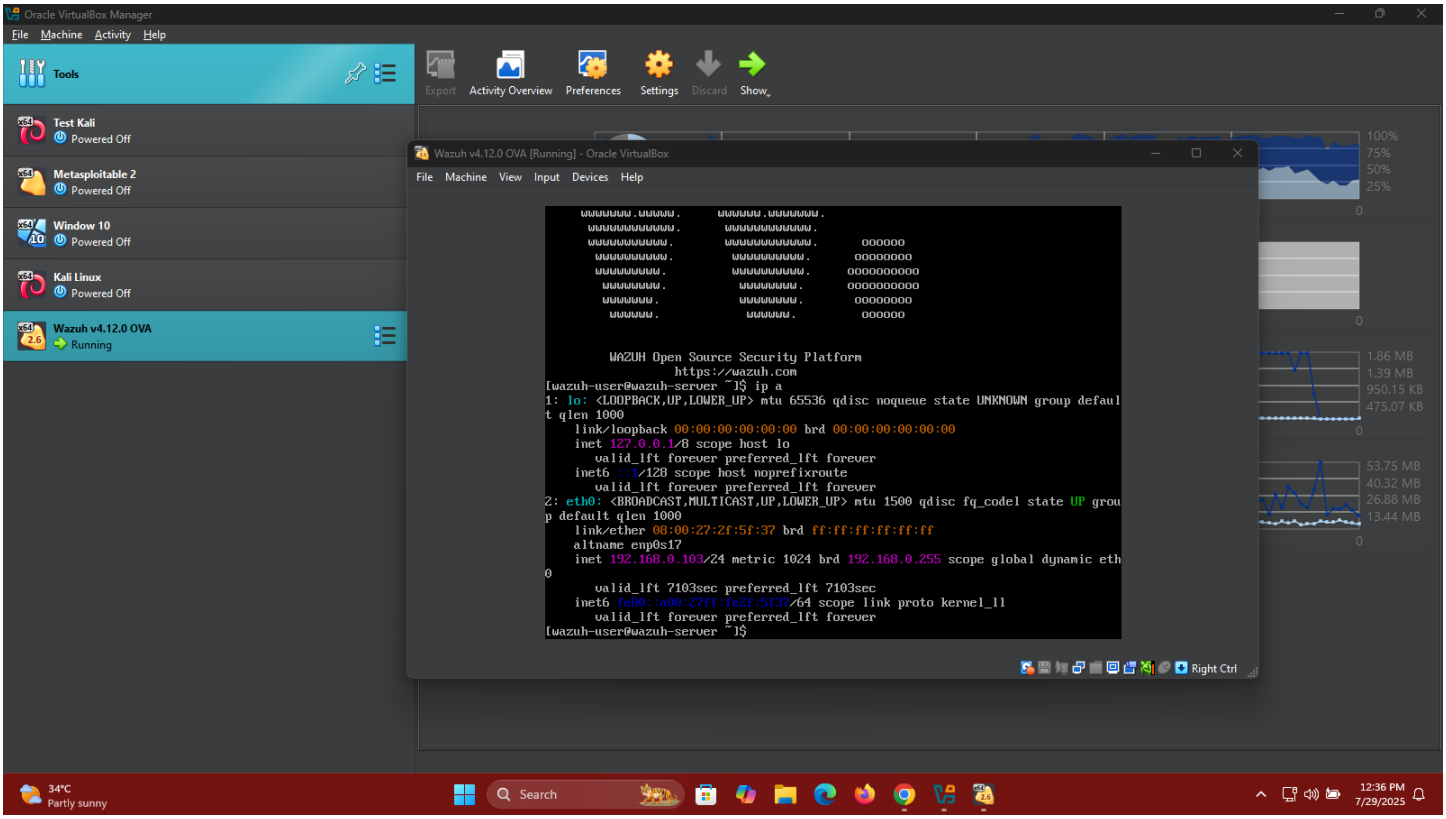


Installing wazuh as a separate server machine due to slow down of kali .

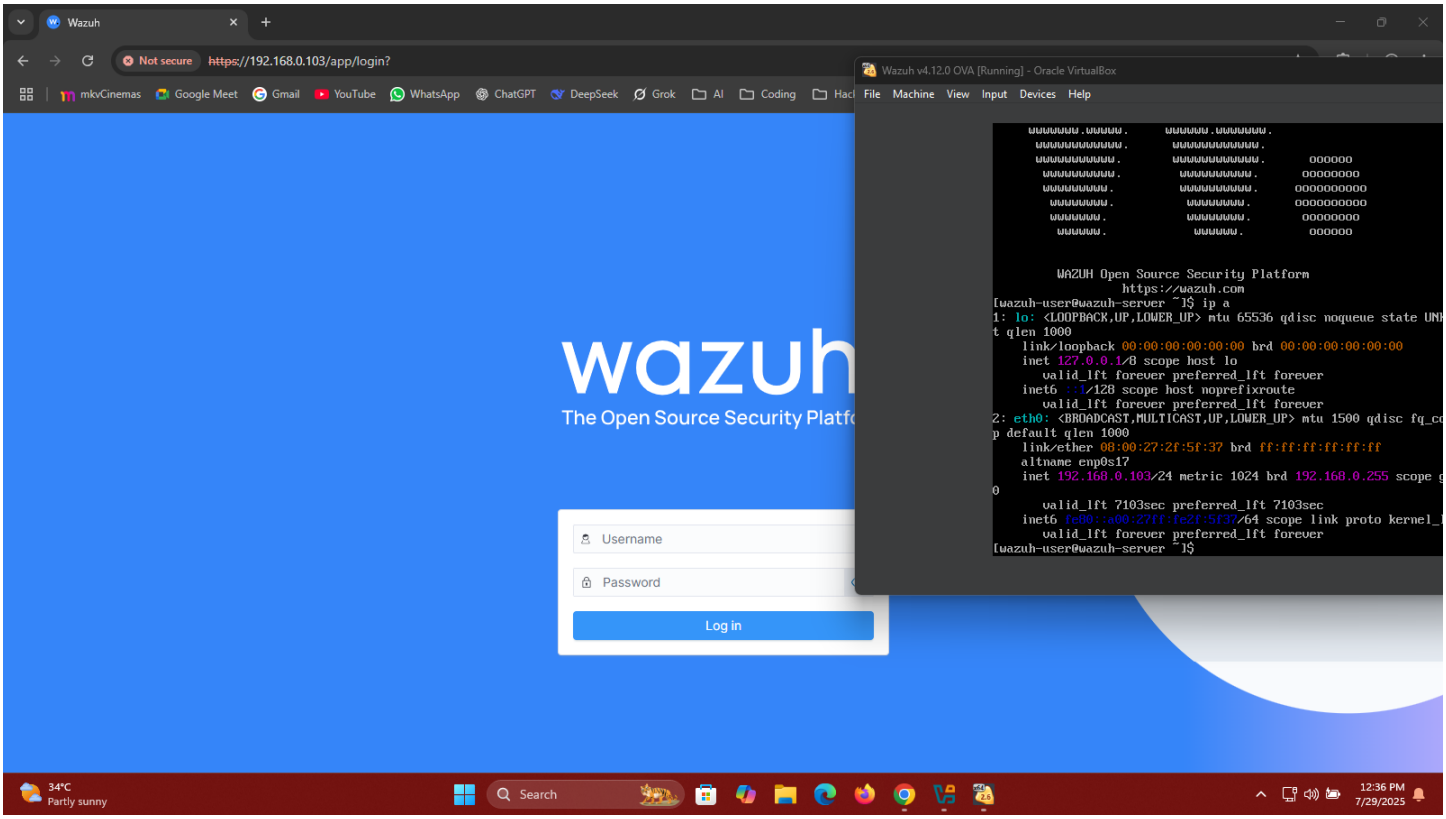


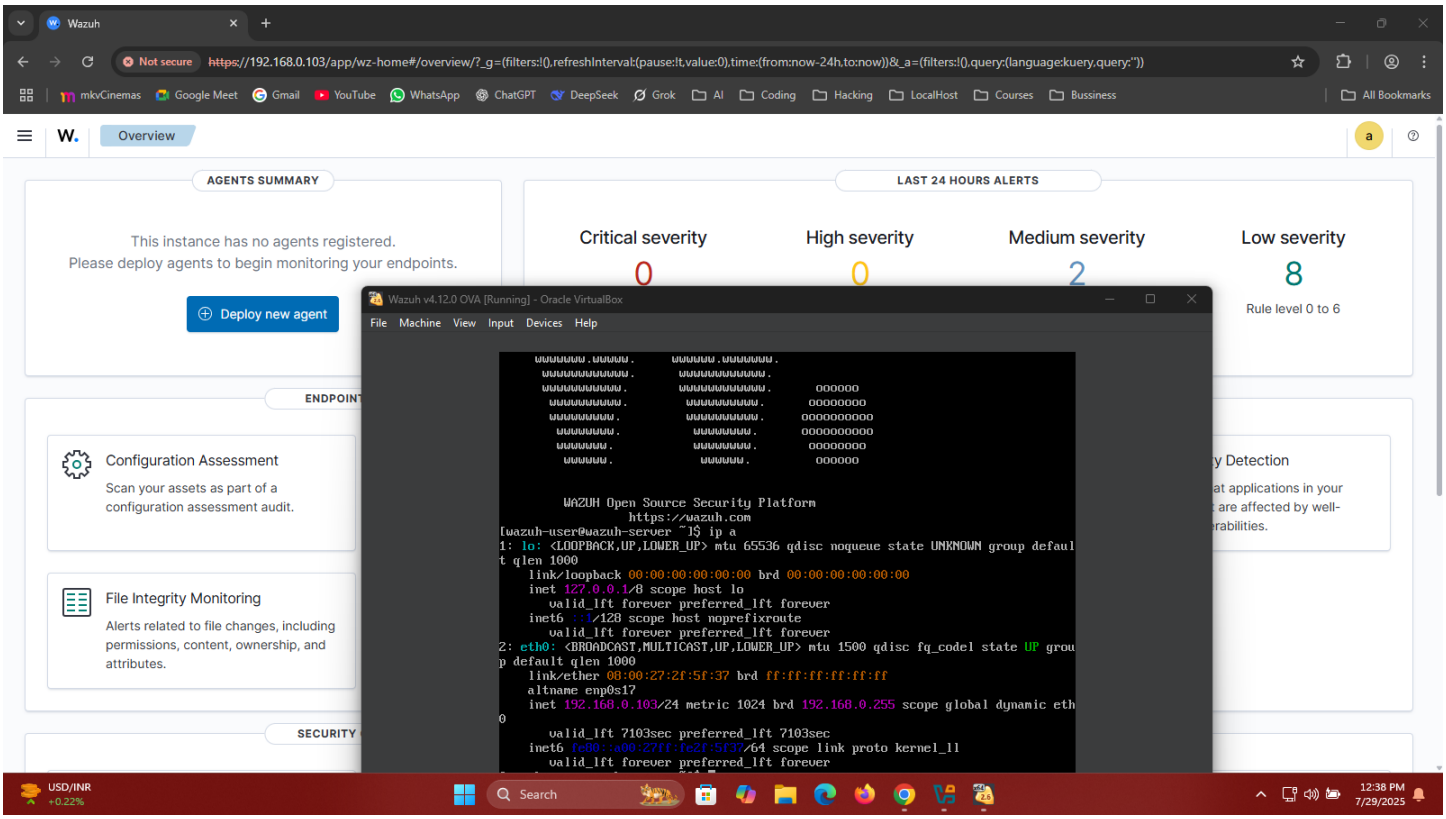


Running the OVA machine , separate full system . works perfect for me !



Accessing with Host , better & smoother then Kali .





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

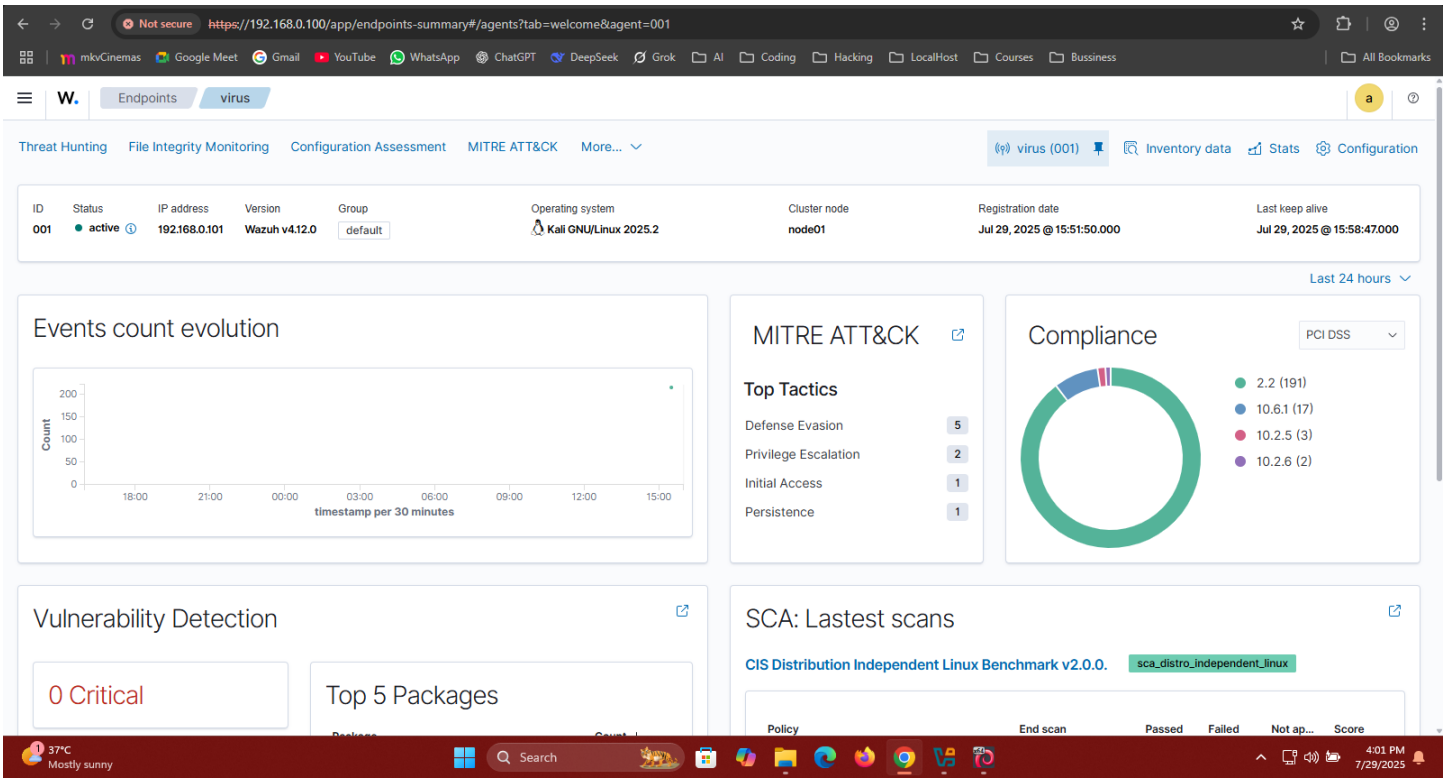
disable updates ,

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 !

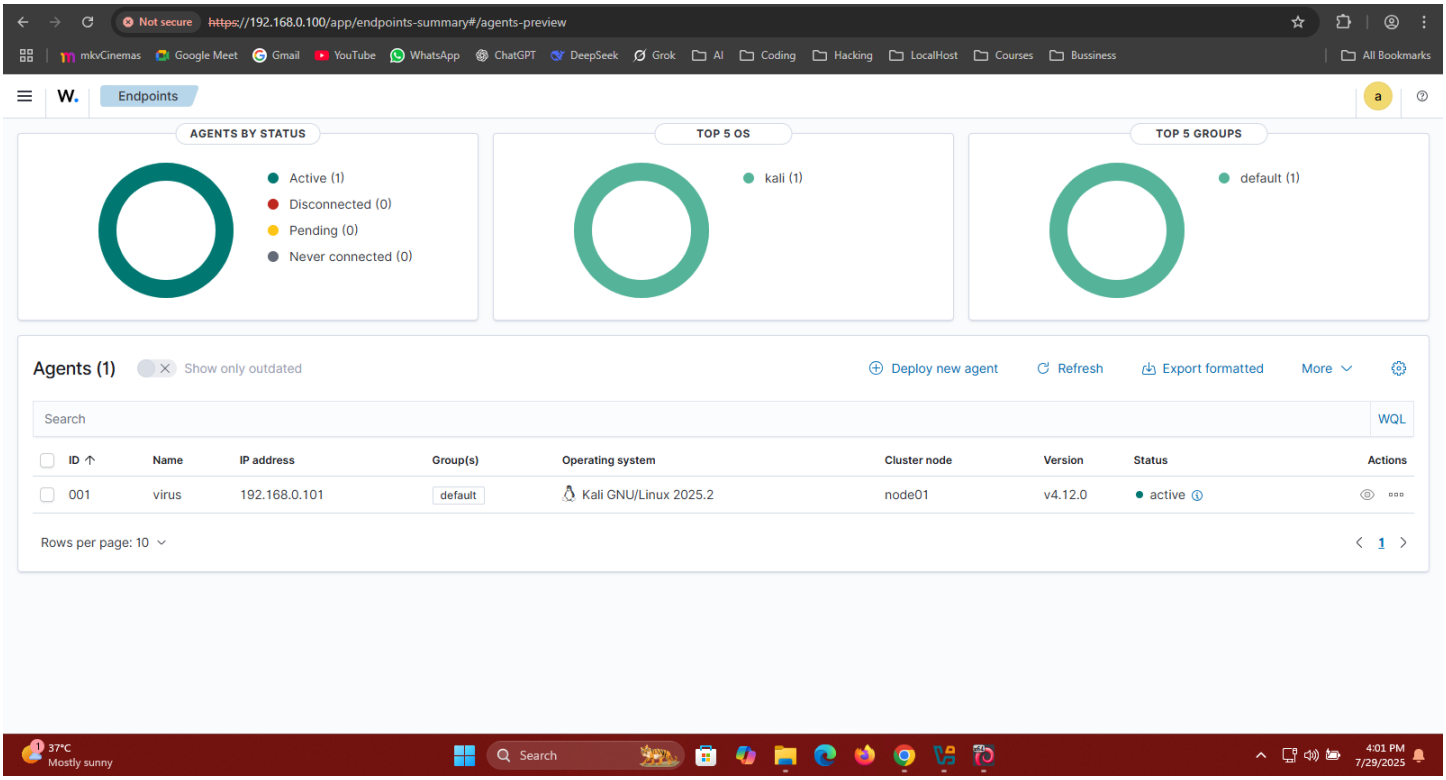


NOTE > after full setup , I note that my wifi router and default all routers run on DHCP server . ip assignment to nodes is automatic . so if our ip changes on another start (agent or server) . the configuration will be miss match and It will make issue . to fix this I have 2 options ,

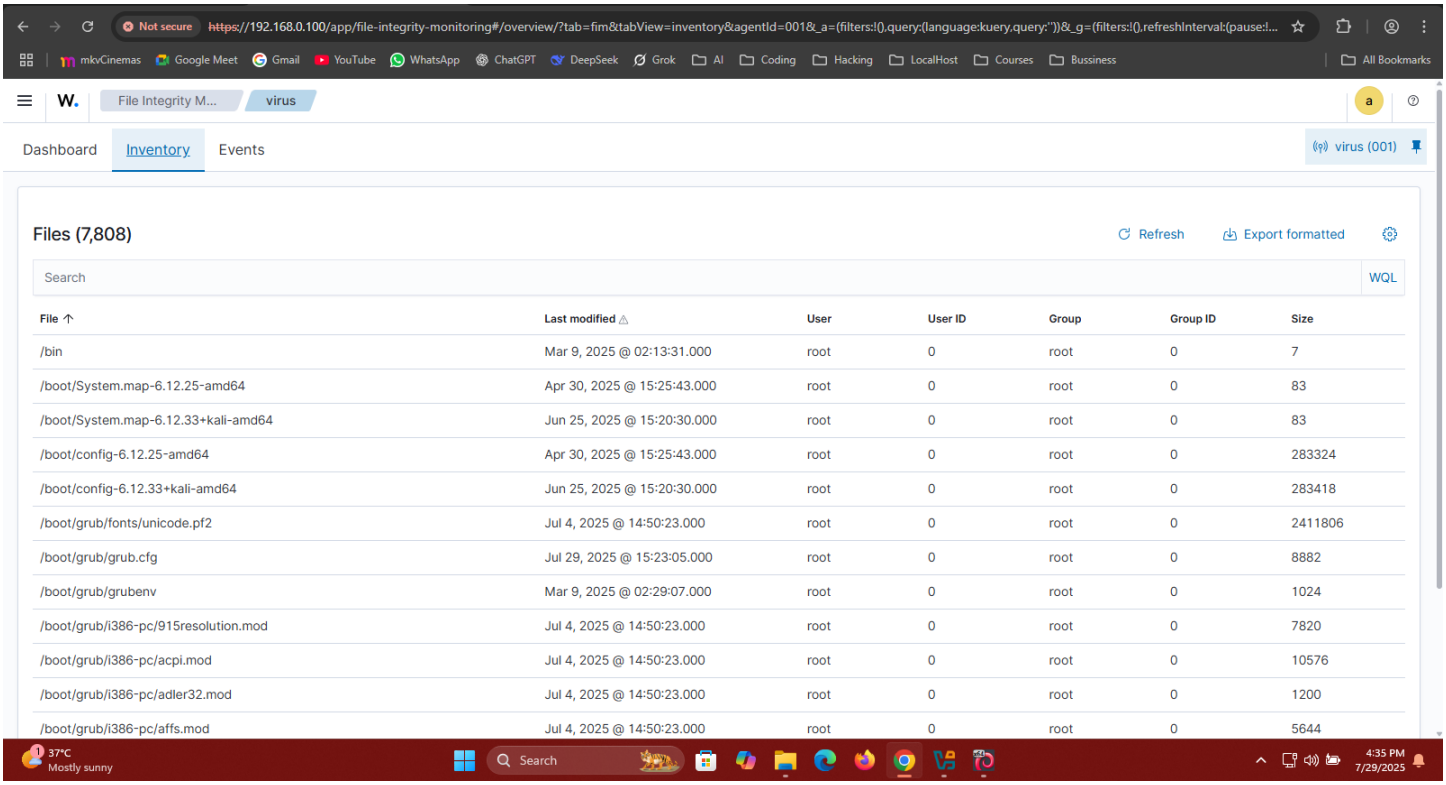
1) **Changes in internal configs of machine and assign static ip but in case of VMs we can stuck .**
2) **Access admin panel of my router and reserved the 3 ips for my agents and server in the DHCP range using mac .**

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

Dashboard overview



Collecting logs & inventory .



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 Monitering (FIM) .

Adding directories and seting 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 ,

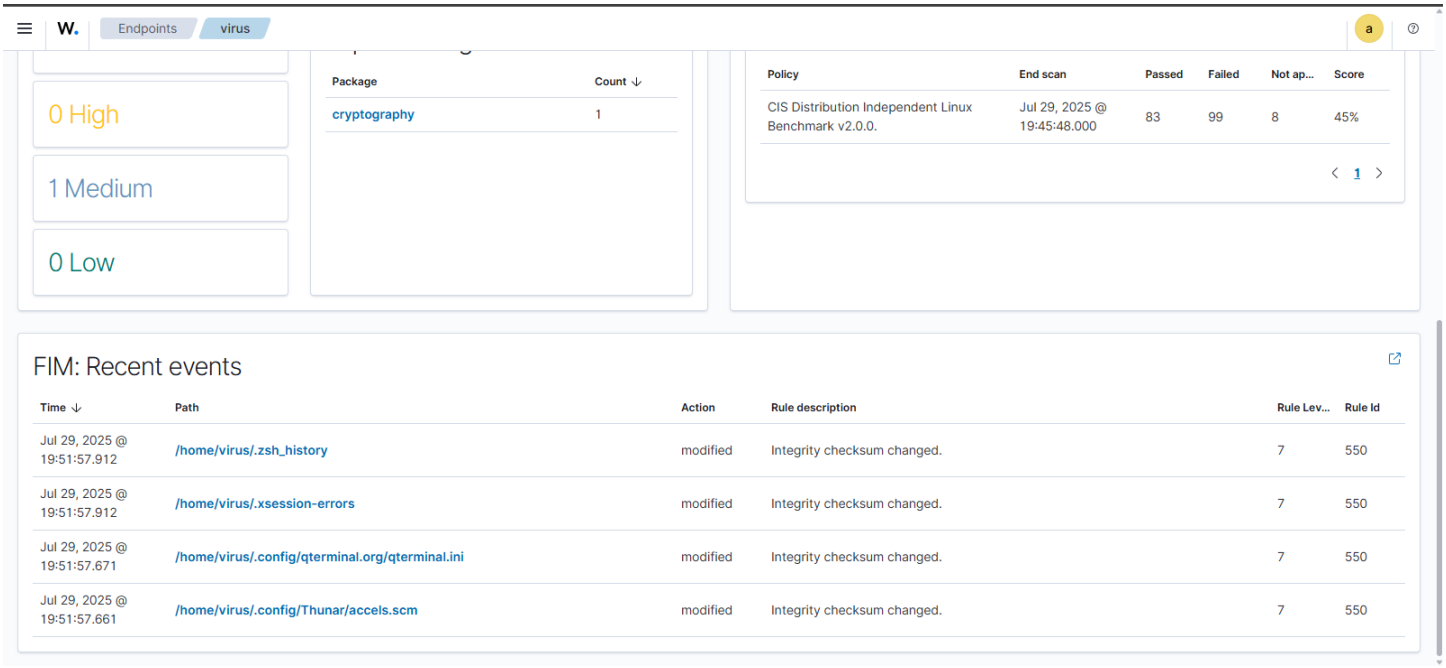
sudo systemctl restart wazuh-agent

after changing in directoires and files , lets confirm if server received .

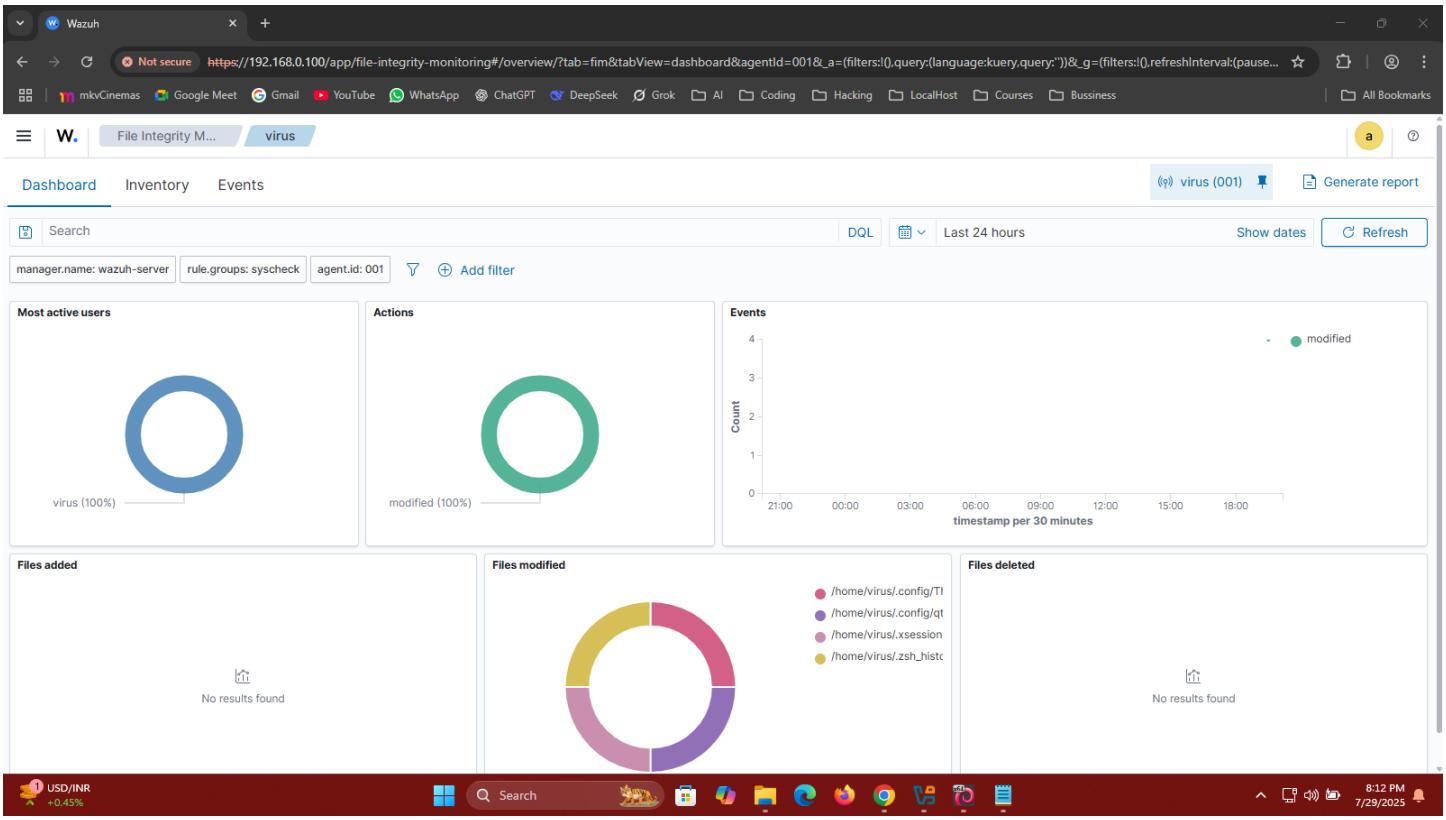
sudo tail -n 100 /var/ossec/logs/alerts/alerts.json | grep test_fim

ALL SET !

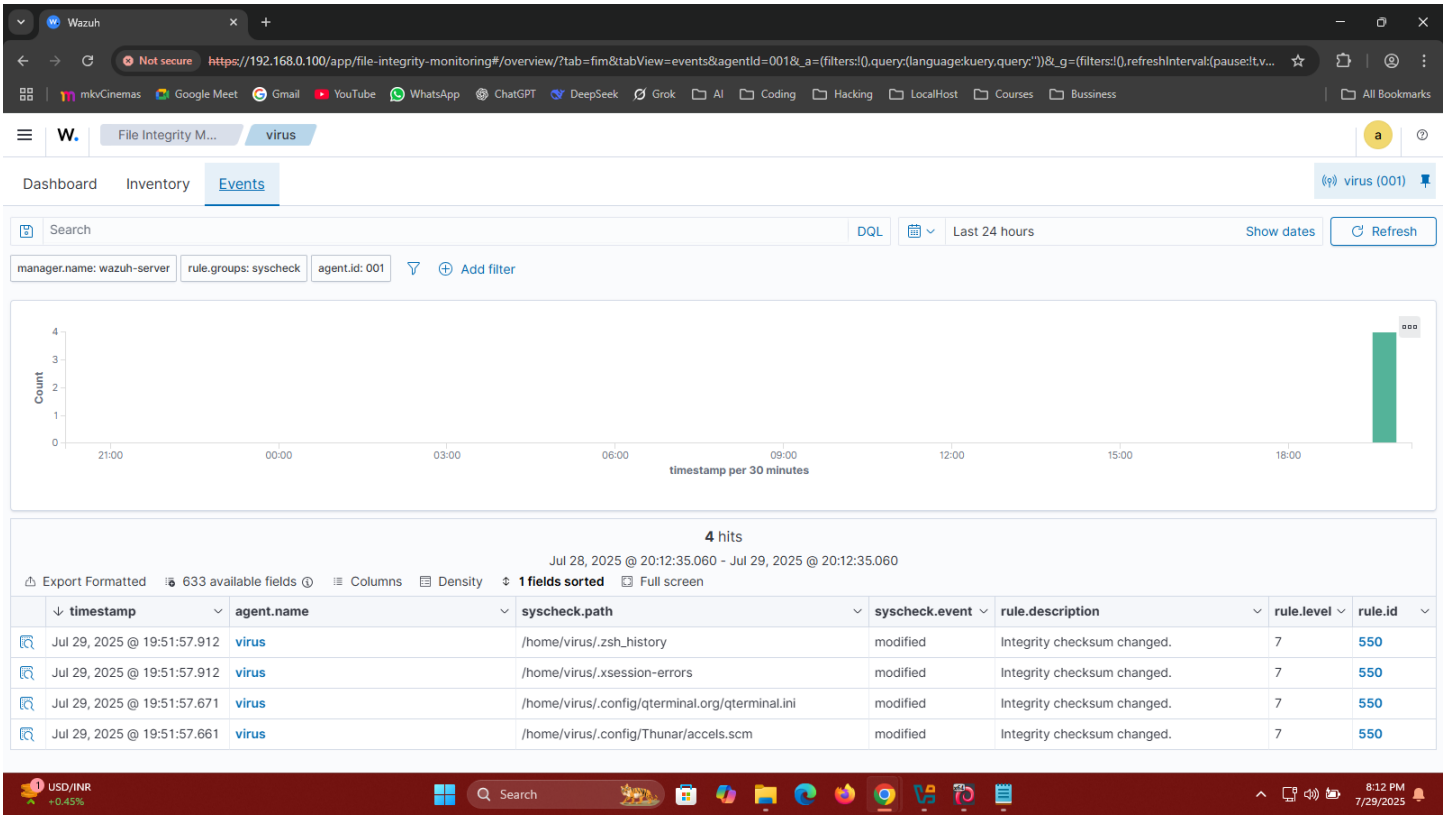
Real time FIM reports .



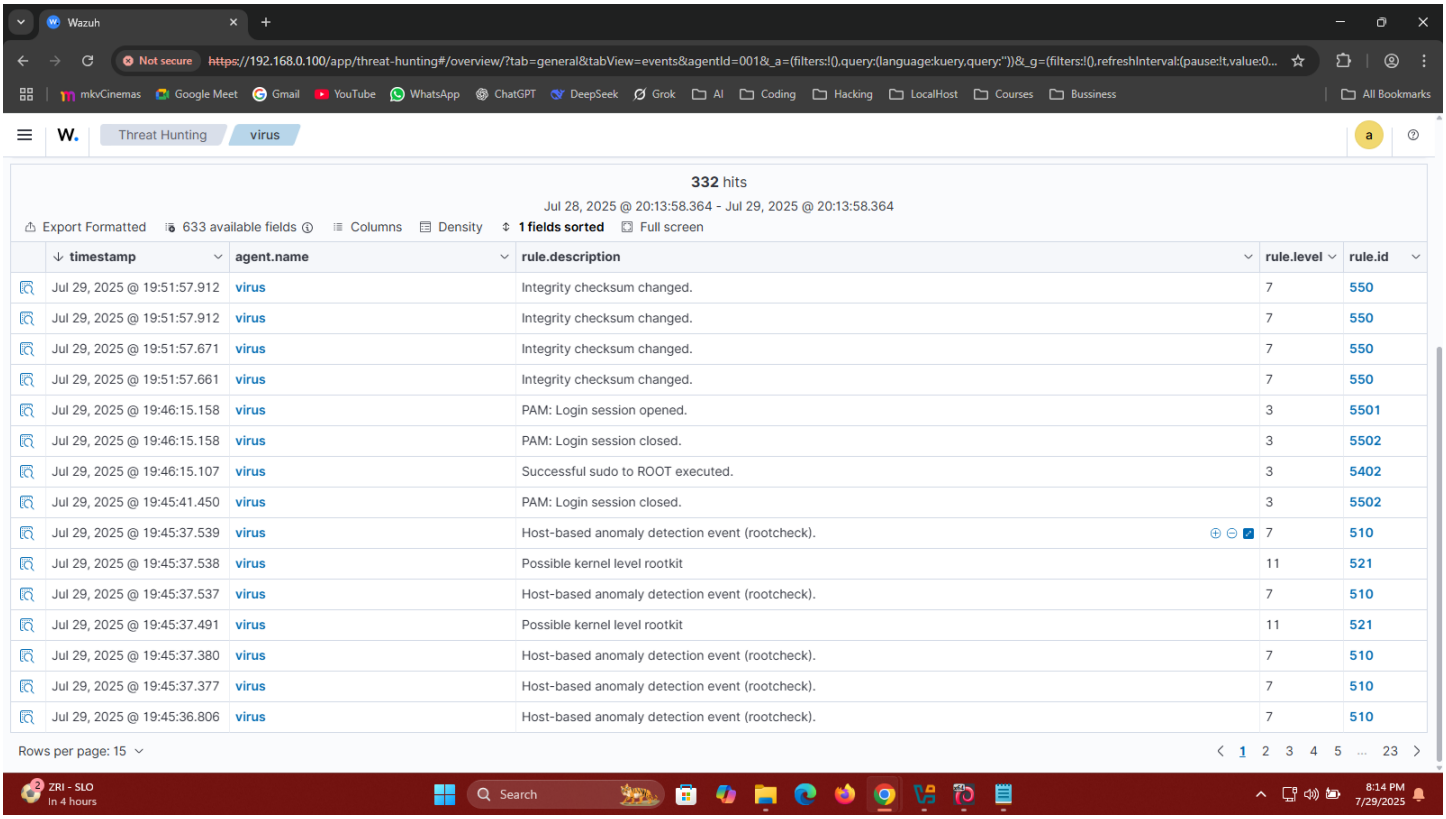
FIM dashboard .



Recent events FIM .



Threat Hunting Logs . Real Time Catch .



The End

SYED MUHAMMAD SHAH