wazuh.

Wazuh – SNORT IDS

Network Intrusion Detection

Lab Created By: MUHAMMAD MOIZ UD DIN RAFAY

Follow Me: linkedin.com/in/moizuddinrafay

Integrating Wazuh and Snort IDS for Enhanced Security Monitoring

Snort is a widely-used open-source Intrusion Detection System (IDS) that analyzes network traffic in real-time and detects suspicious activities. Wazuh, on the other hand, is an open-source security monitoring platform that includes capabilities for intrusion detection, log analysis, vulnerability detection, and more.

Integration of Snort IDS with Wazuh:

Snort Overview:

- Snort operates by inspecting packets as they pass through a network interface.
- It uses rulesets to detect known threats, anomalies, and policy violations.
- Alerts are generated when Snort detects suspicious activity based on these rules.

Wazuh Overview:

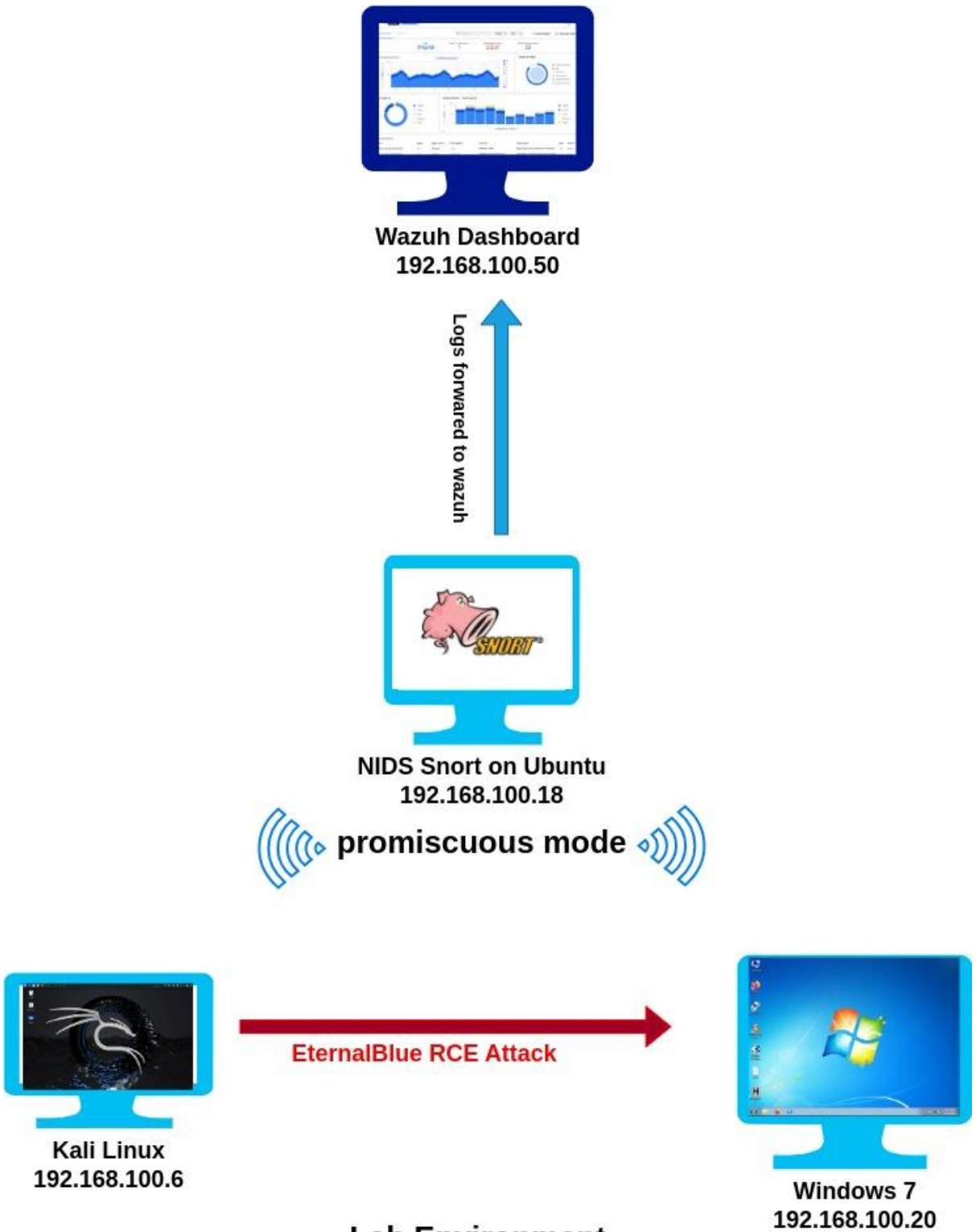
- Wazuh provides a comprehensive security monitoring solution.
- It integrates log analysis, intrusion detection, vulnerability detection, and more into a single platform.
- Wazuh uses agents deployed on monitored systems to collect and analyze data.

Integration Benefits:

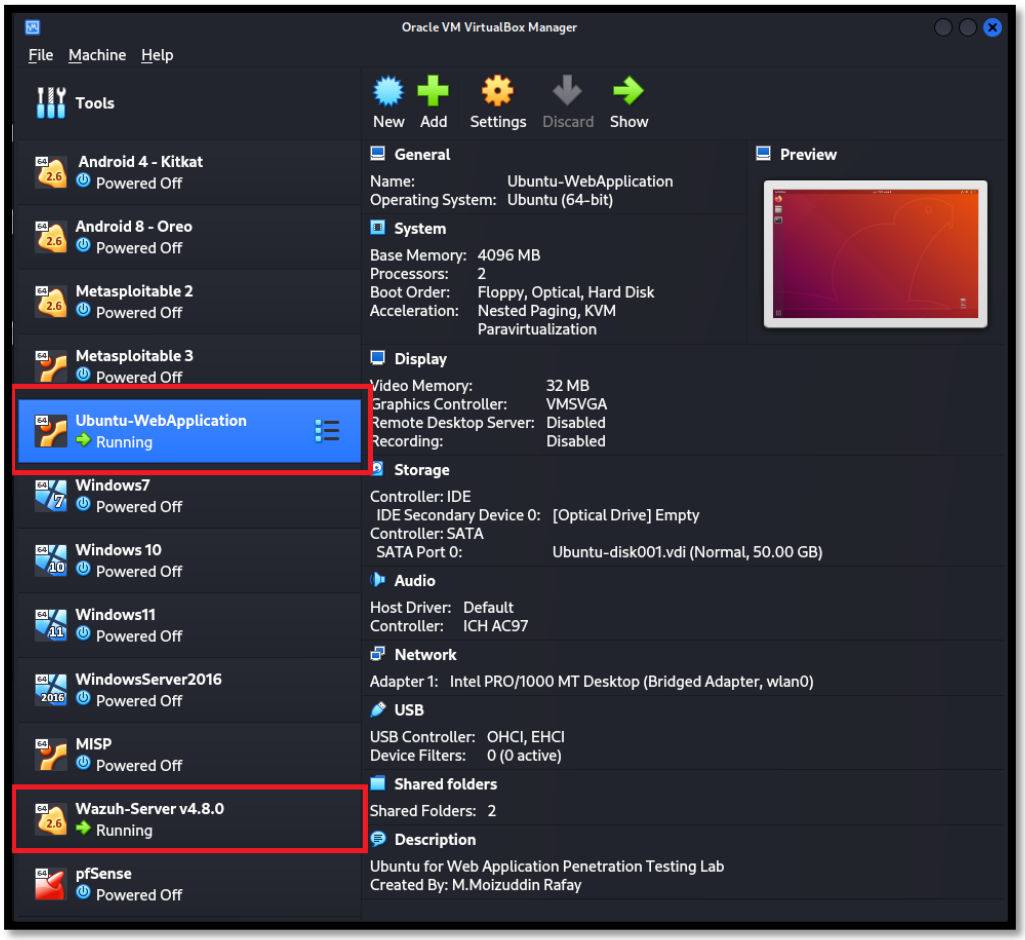
- Centralized Monitoring: Wazuh can centralize and correlate alerts generated by Snort across multiple network segments or hosts.
- Enhanced Visibility: By integrating Snort alerts into Wazuh, security teams gain a unified view of network and host-based security events.
- Scalability: Wazuh's scalability allows it to handle large volumes of data generated by Snort, ensuring that no alerts are missed.

Use Cases:

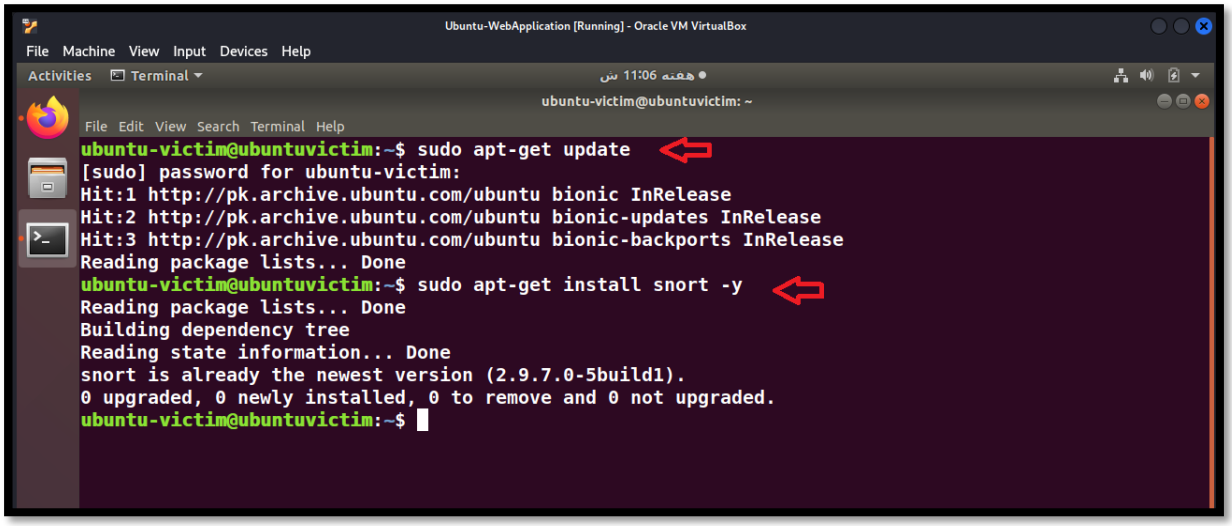
- Incident Response: Quickly identify and respond to potential threats detected by Snort through Wazuh's centralized alerting.
- Compliance Monitoring: Meet regulatory requirements by monitoring network traffic and generating comprehensive reports.
- Threat Hunting: Leverage combined data from Snort and Wazuh for proactive threat hunting and anomaly detection.


Wazuh Dashboard
192.168.100.50
Logs forwared to wazuh
NIDS Snort on Ubuntu
192.168.100.18
promiscuous mode
Kali Linux
192.168.100.6
EternalBlue RCE Attack
Windows 7
192.168.100.20
Lab Environment
Local Network
MUHAMMAD MOIZ UD DIN RAFAY
Follow me: https://www.linkedin.com/in/moizuddinrafay

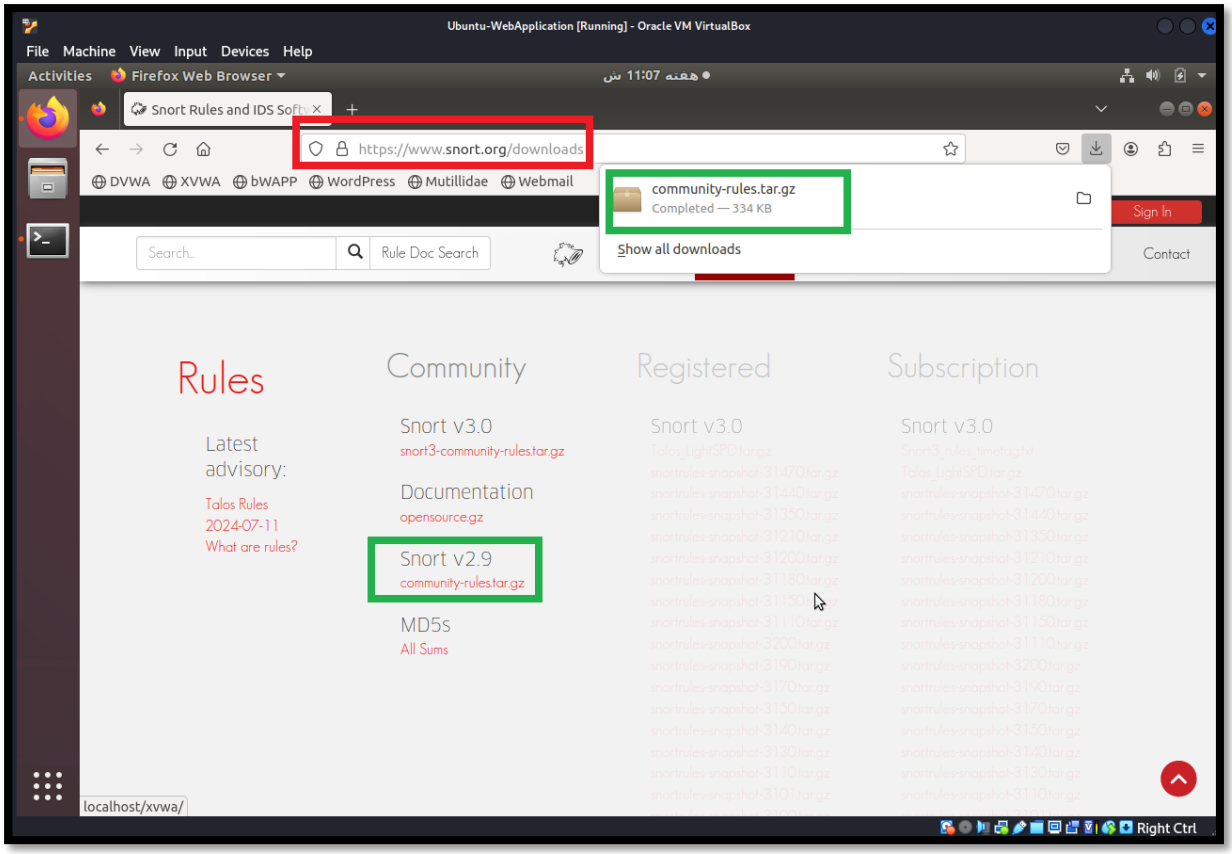
Here in my virtualbox Wazuh-server and Ubuntu machine is up and running.



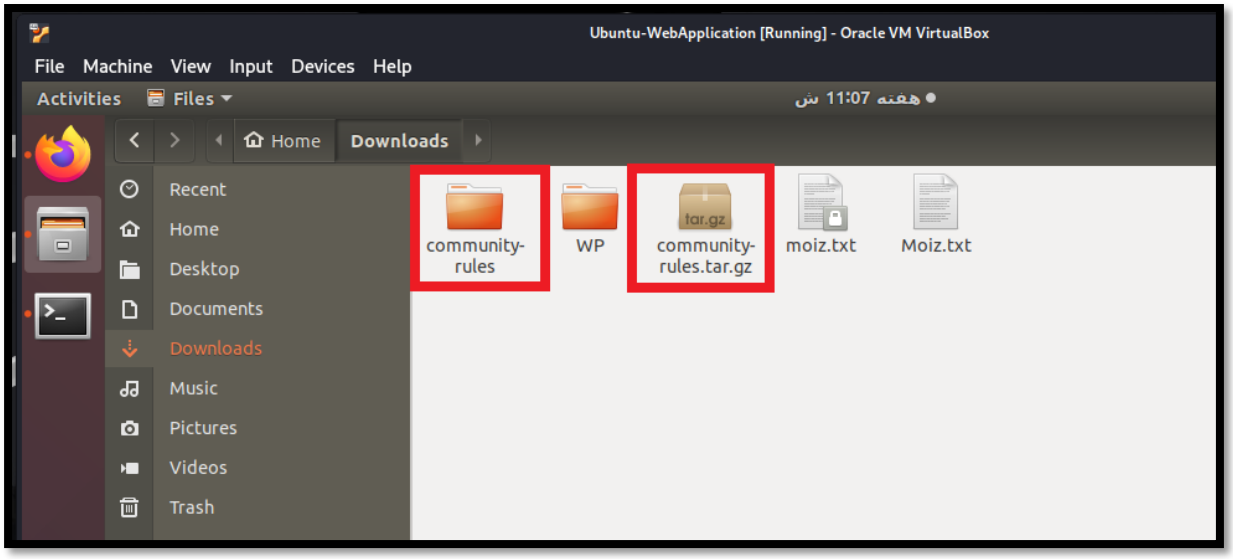
Step 01: First we have to install snort in Ubuntu machine.
Command: sudo apt-get update
Command: sudo apt-get install snort -y



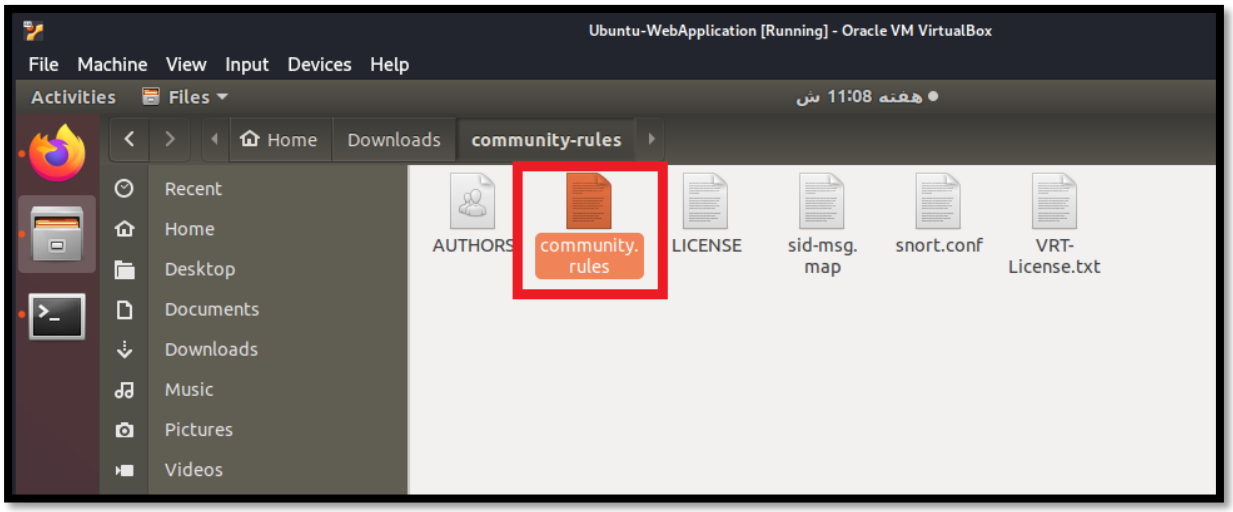
After installing the snort, we need to download "Community-rules" of snort.



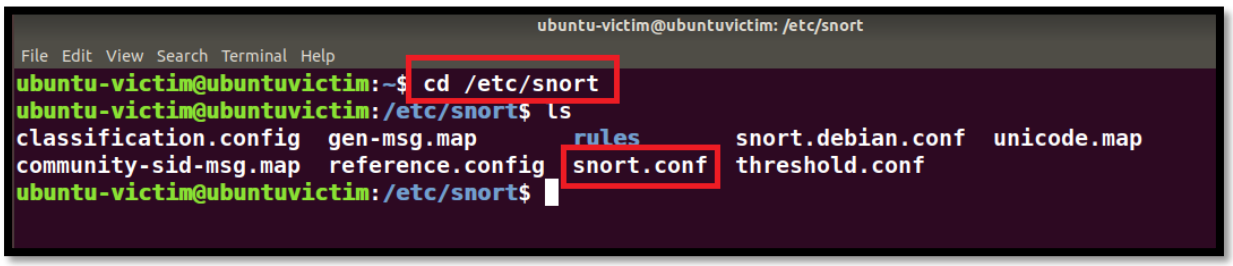
After download the snort “community-rules.tar.gz” we have to extract this file.



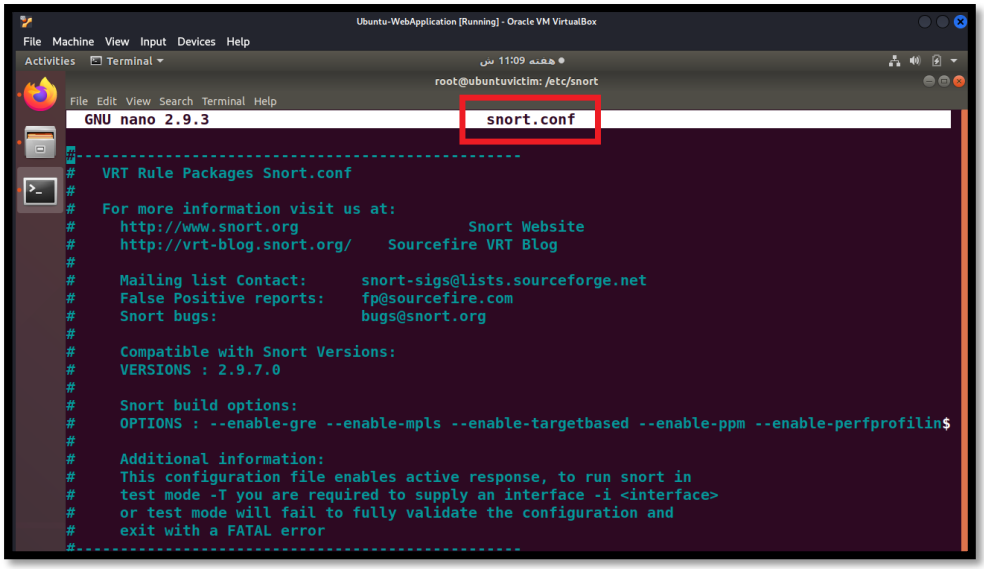
Here is the “community.rules” file, we will use this file later.



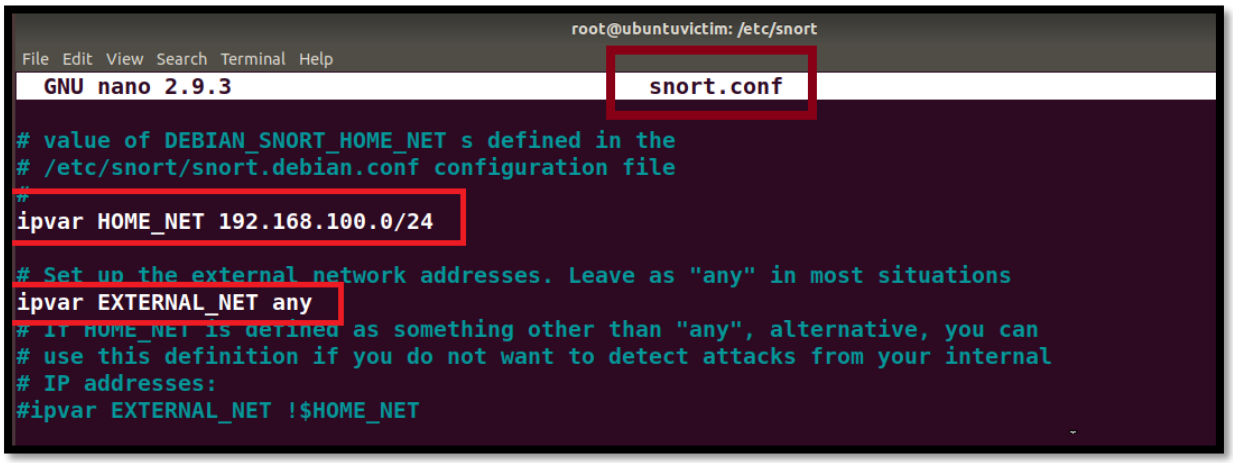
Now we have to edit snort configuration to setup according to our network.
Command: cd /etc/snort
Edit the snort.conf file follow the figures.



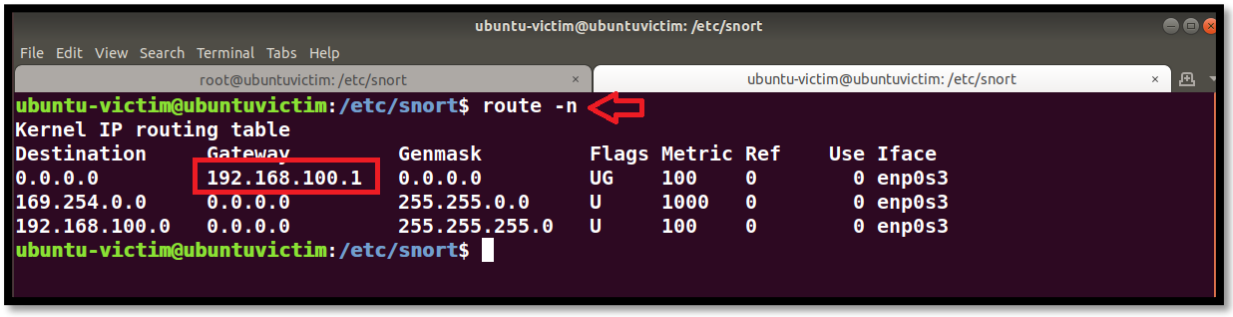
Here is “snort.conf” file is open in “nano” editor.



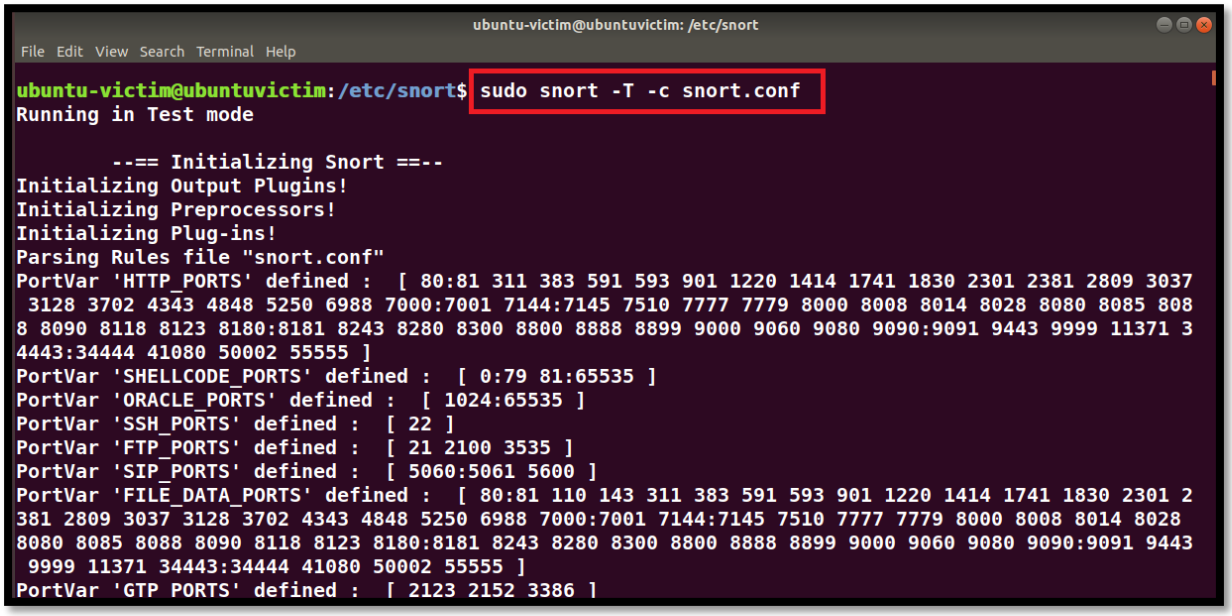
We have to change network setting here. Follow the figure and do same but according to your network.
Note: you have to configure your interface as well. Do little scroll down and edit you interface; I am not mentioning here to edit interface.

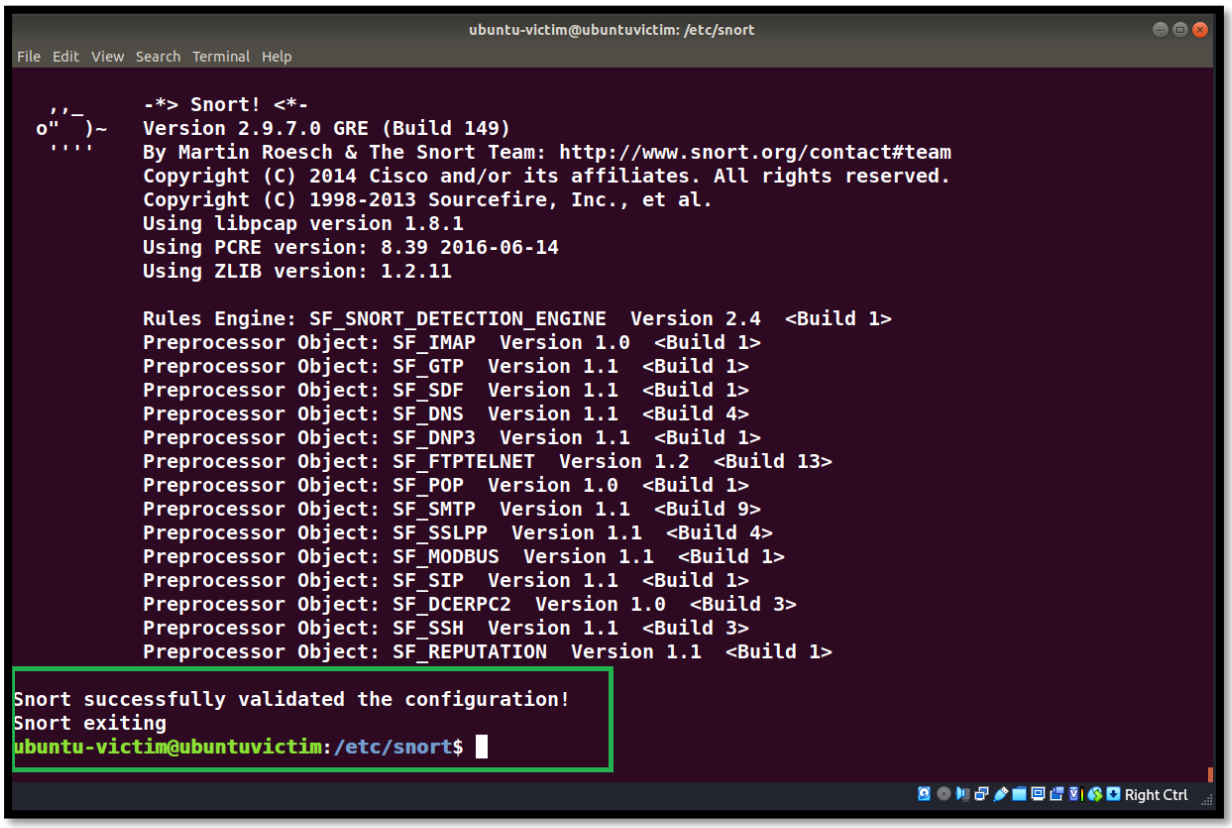


Find you network routing information with “route –n” command.



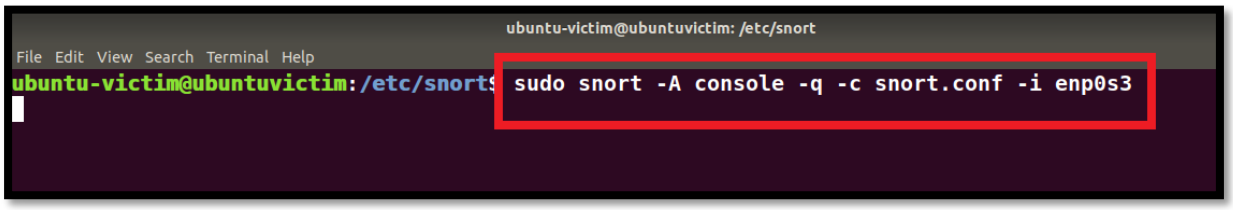
Save the “snort.conf” file and check the configuration is successful or not.
Command: sudo snort -T –c snort.conf
Note: It’s a case sensitive make sure you are in “/etc/snort” directory.



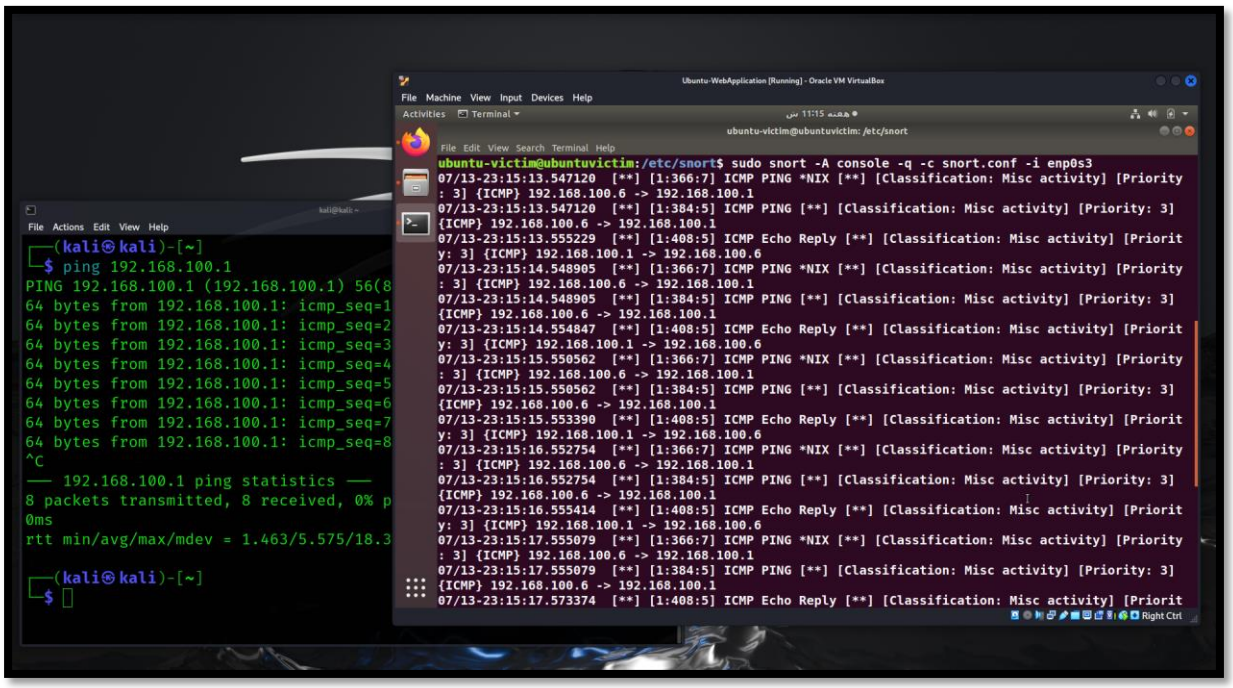


Now snort configure successfully.

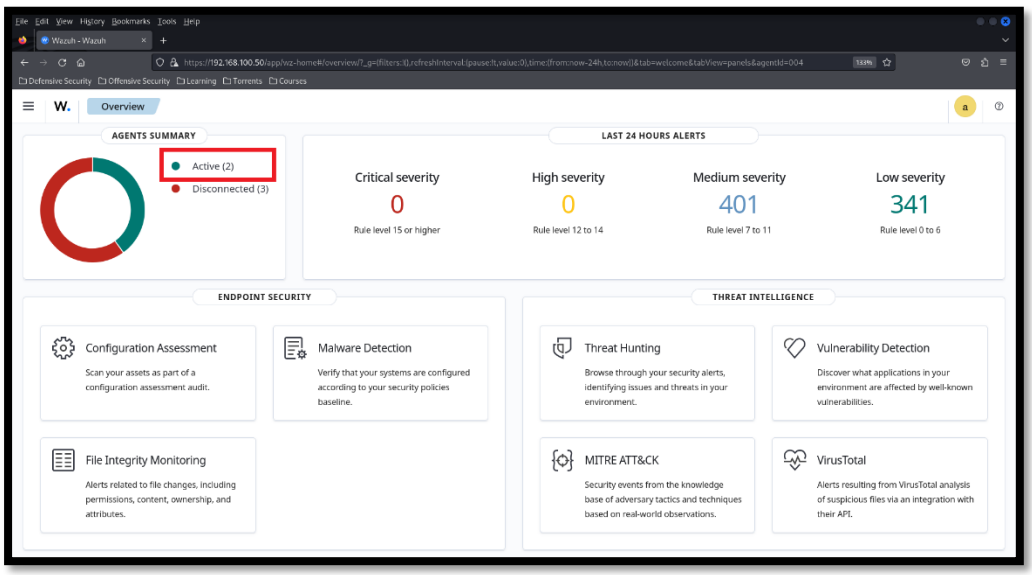
Now start snort and monitor network traffic.
Command: sudo snort -A console –q –c snort.conf –I enp0s3



Now open the “Kali Linux” and do ping to any IP address and monitor the snort. Follow same as shown in figure.

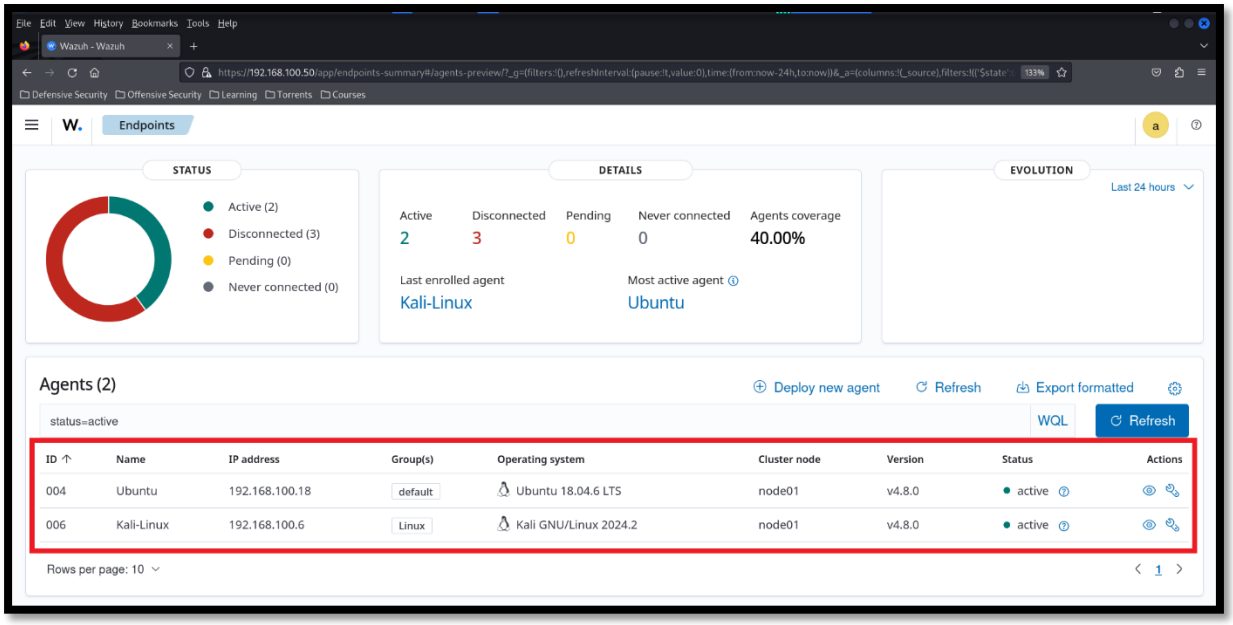


Now browse Wazuh-dashboard. And go to active agents.

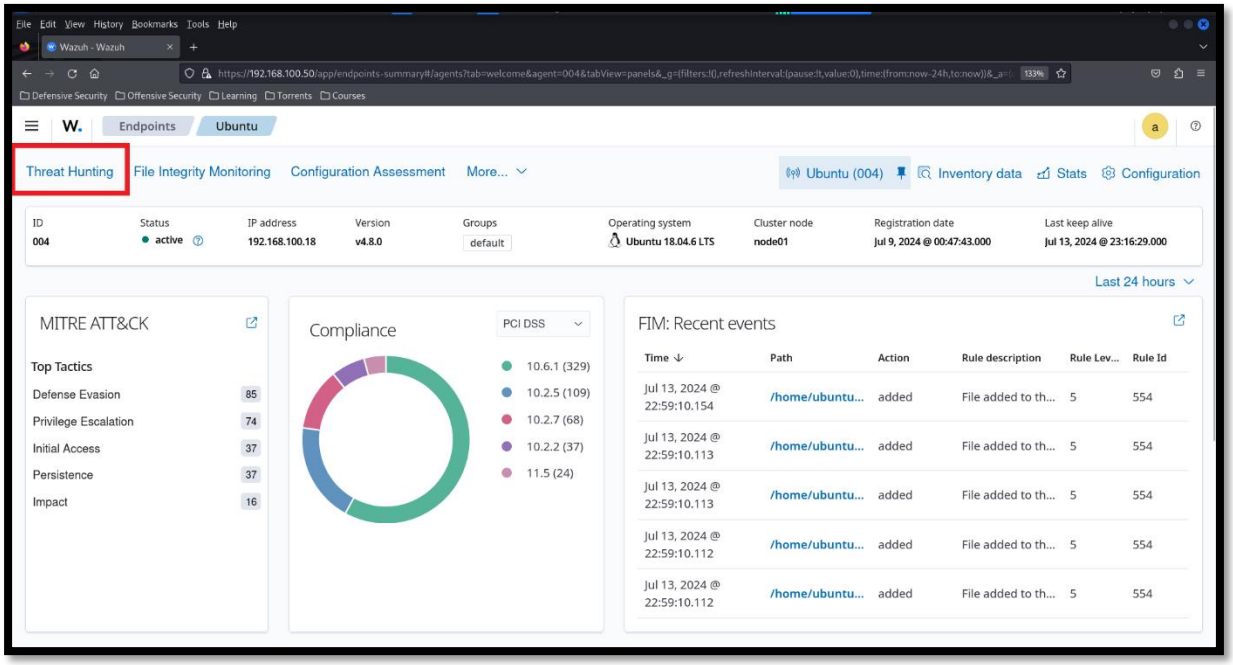


Wazuh – SNORT IDS – Network Intrusion Detection
Lab Created by: MUHAMMAD MOIZ UD DIN RAFAY

Here is I have two agents active “Kali-Linux” and “Ubunut”.

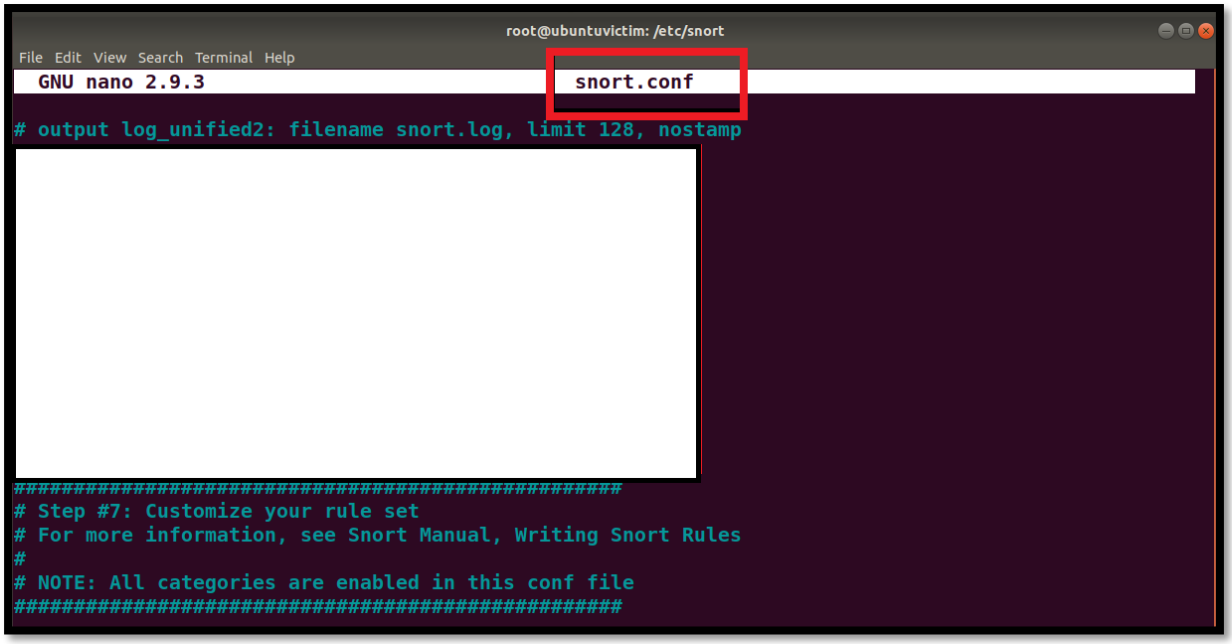


Select your “Ubuntu” agent.

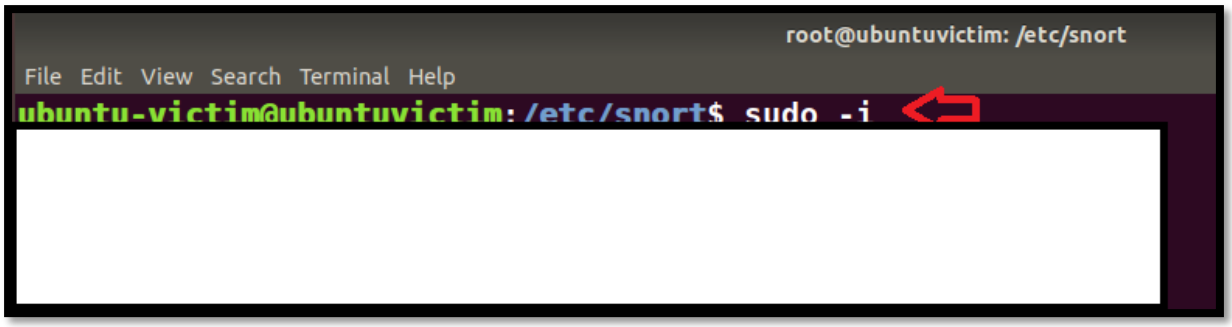


Go to “Threat Hunting” Tab.

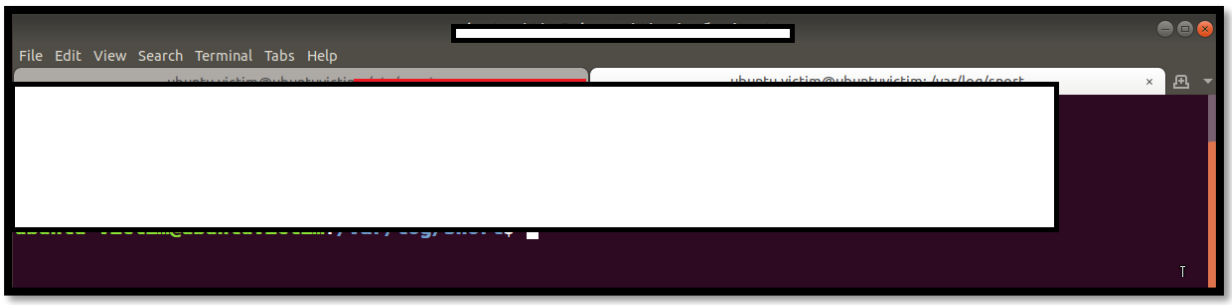
[redacted]



[redacted]



[redacted]



[redacted]

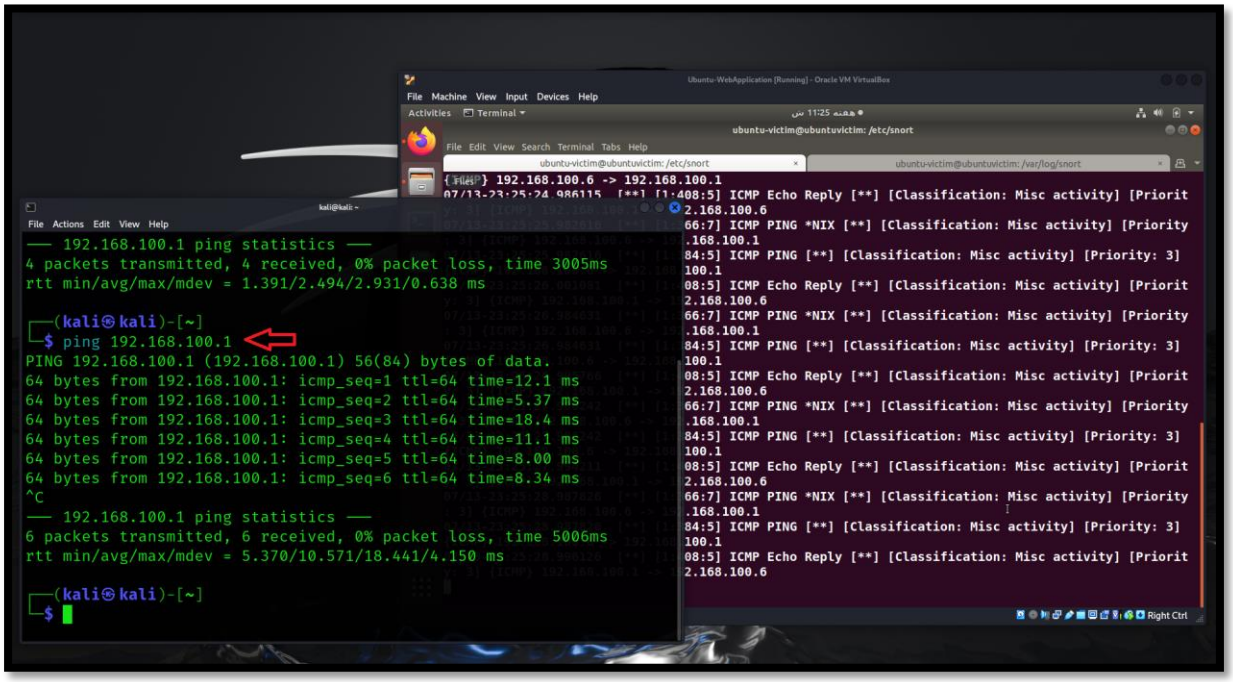
[redacted]

[redacted]

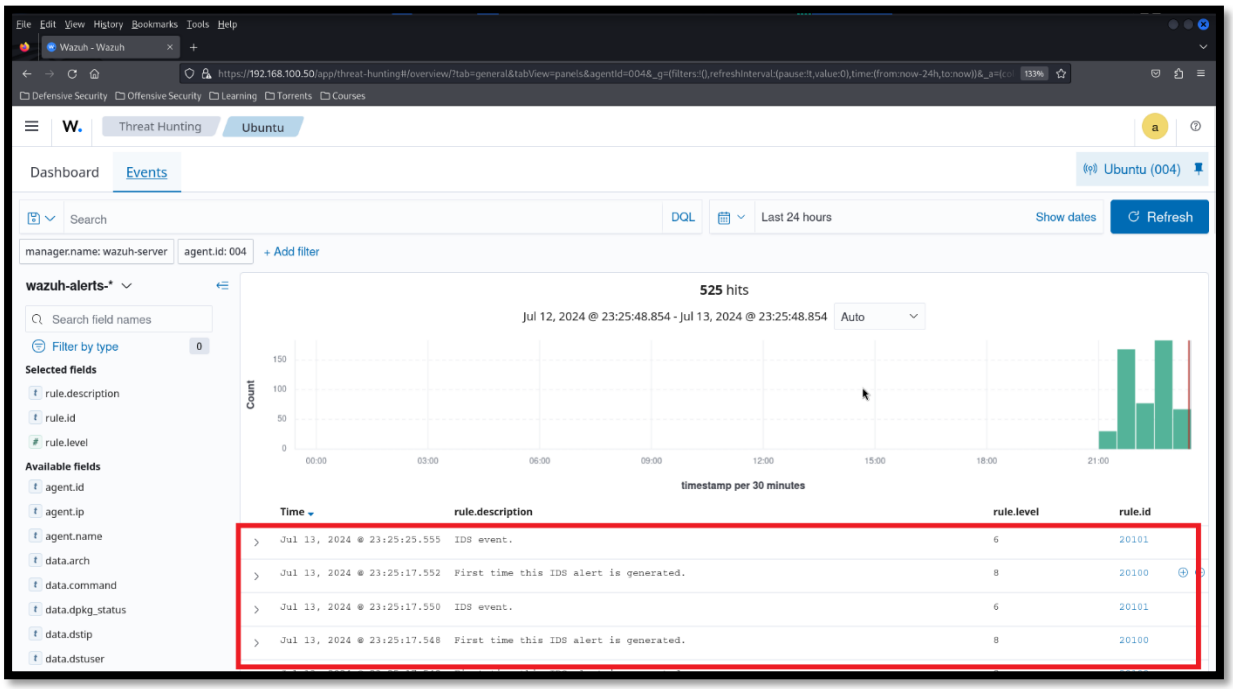
[redacted]

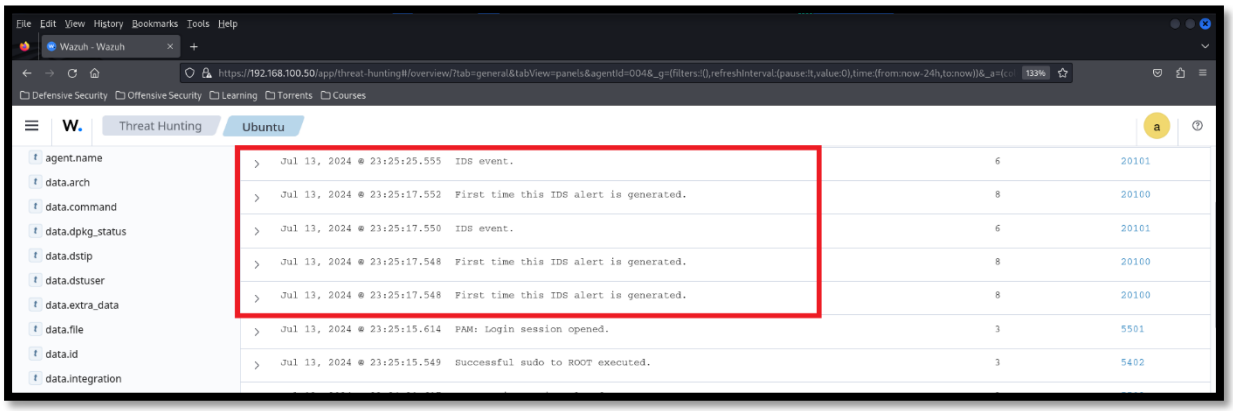
[redacted]

Now again do ping form “Kali Linux” and monitor snort traffic.

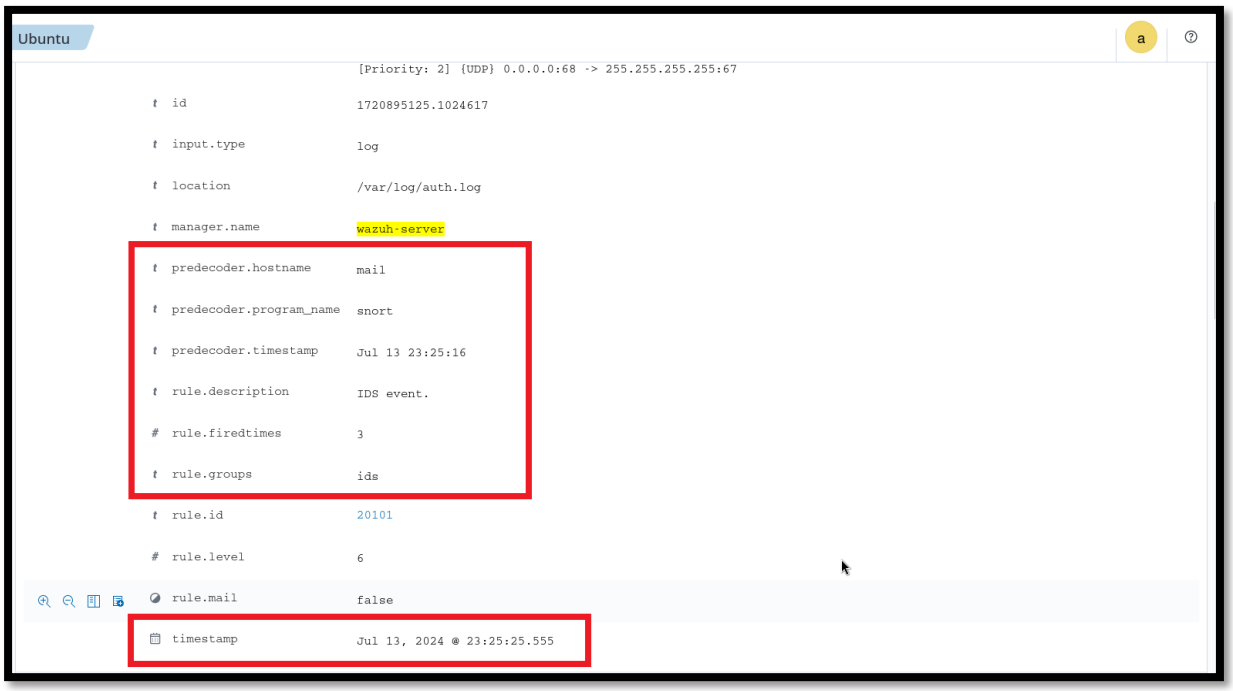


Now look at into “Ubuntu” machine “Events” tab. Here is IDS events. These events form snort IDS.

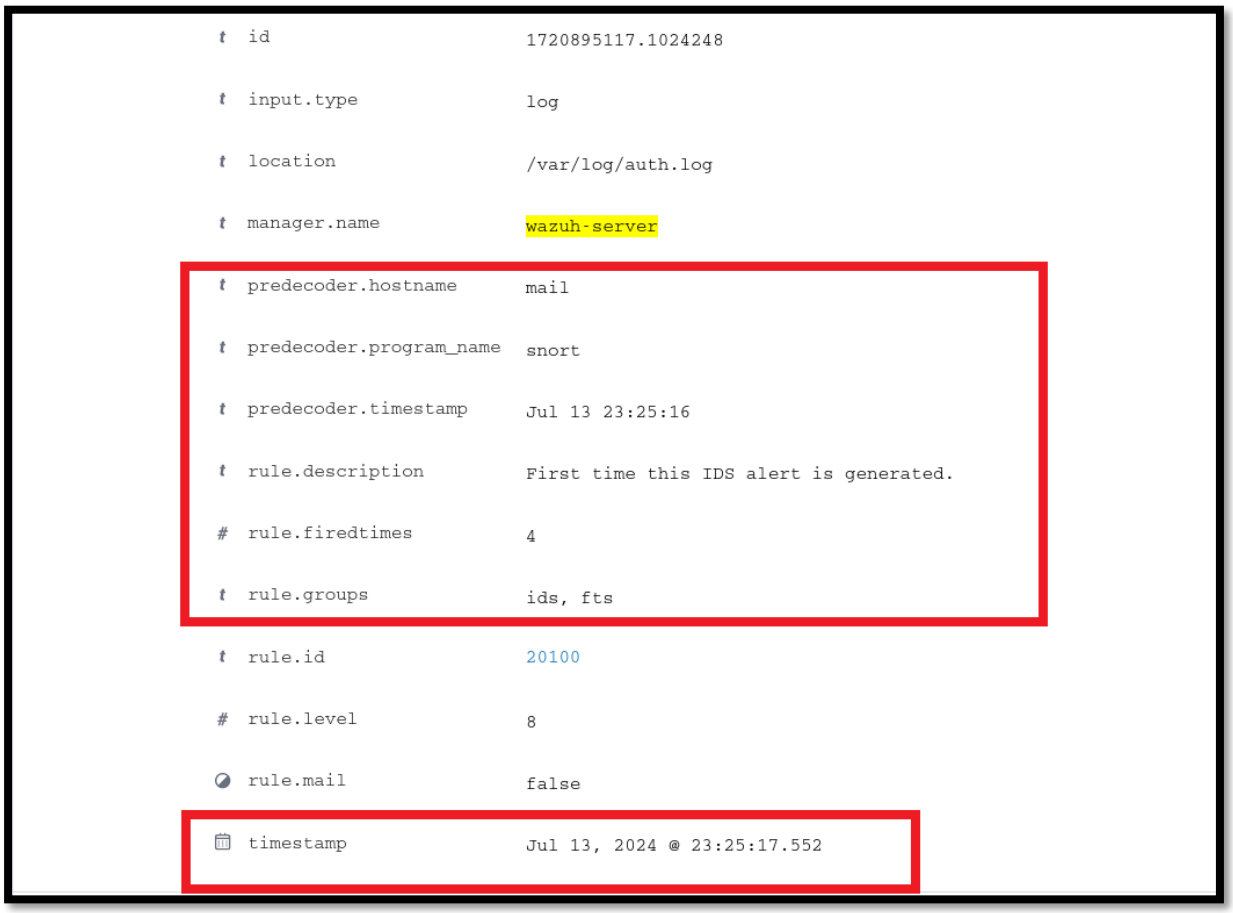





Ubuntu
a
Jul 13, 2024 @ 23:25:25.555 IDS event. 6 20101
Expanded document
View surrounding documents
View single document
Table
JSON
t _index wazuh-alerts-4.x-2024.07.13
t agent.id 004
t agent.ip 192.168.100.18
t agent.name Ubuntu
t data.dstip 255.255.255.255:67
t data.id 1:527:8
t data.srcip 0.0.0.0
t decoder.name snort
t decoder.parent snort
t full_log Jul 13 23:25:16 mail snort[11176]: [1:527:8] BAD-TRAFFIC same SRC/DST [Classification: Potentially Bad Traffic] [Priority: 2] {UDP} 0.0.0.0:68 -> 255.255.255.255:67
t id 1720895125.1024617
t input.type log

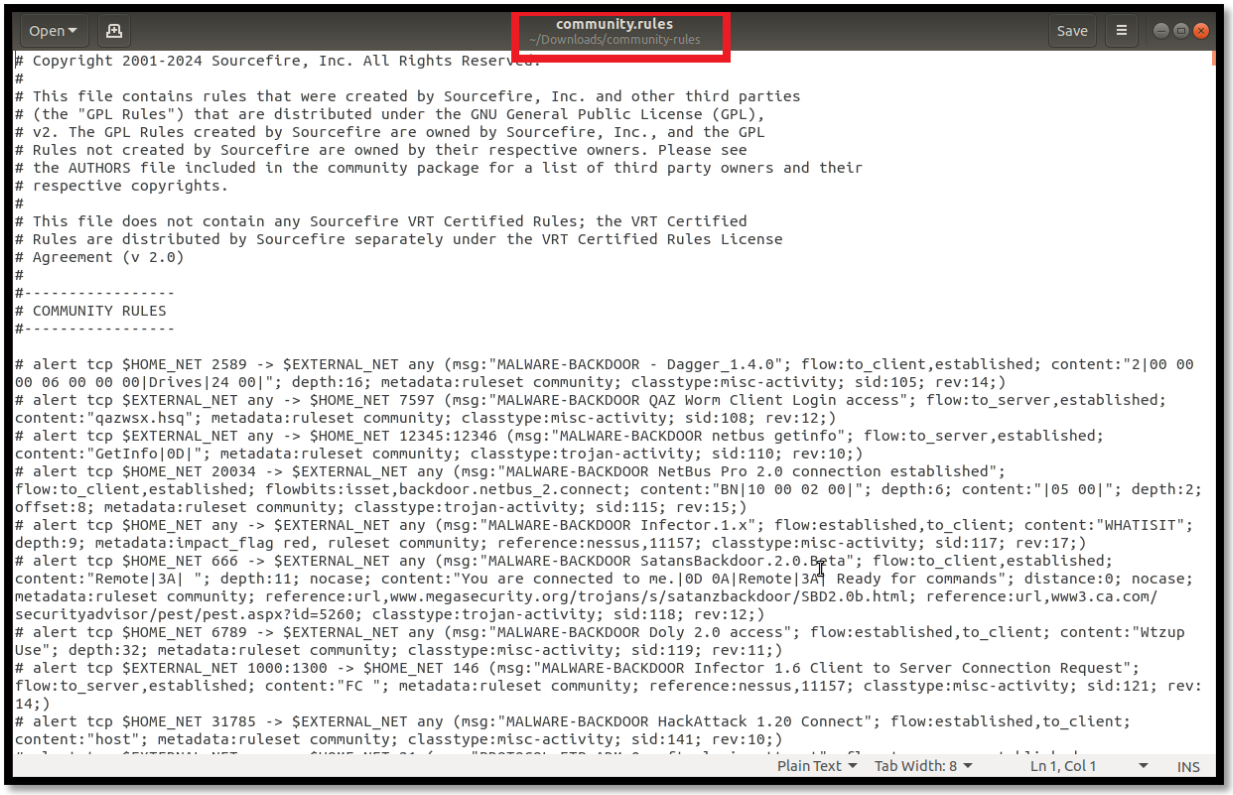

Ubuntu
a
[Priority: 2] {UDP} 0.0.0.0:68 -> 255.255.255.255:67
t id 1720895125.1024617
t input.type log
t location /var/log/auth.log
t manager.name wazuh-server
t predecoder.hostname mail
t predecoder.program_name snort
t predecoder.timestamp Jul 13 23:25:16
t rule.description IDS event.
rule.firedtimes 3
t rule.groups ids
t rule.id 20101
rule.level 6
rule.mail false
timestamp Jul 13, 2024 @ 23:25:25.555


Ubuntu
a
Jul 13, 2024 @ 23:25:17.552 First time this IDS alert is generated.
8
20100
Expanded document
View surrounding documents
View single document
Table
JSON
t _index wazuh-alerts-4.x-2024.07.13
t agent.id 004
t agent.ip 192.168.100.18
t agent.name Ubuntu
t data.dstip 255.255.255.255:67
t data.id 1:527:8
t data.srcip 0.0.0.0
t decoder.name snort
t decoder.parent snort
t full_log Jul 13 23:25:16 mail snort[11176]: [1:527:8] BAD-TRAFFIC same SRC/DST [Classification: Potentially Bad Traffic] [Priority: 2] {UDP} 0.0.0.0:68 -> 255.255.255.255:67
t id 1720895117.1024248
t input.type log

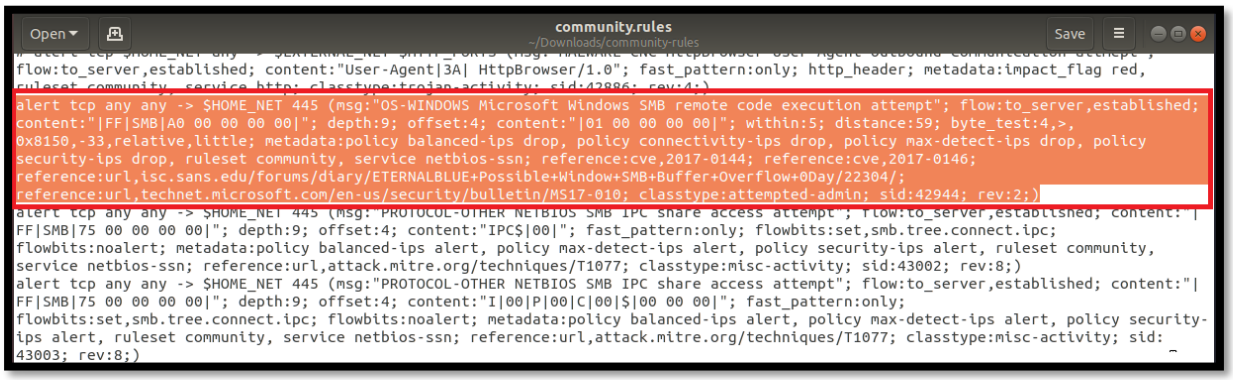

t id 1720895117.1024248
t input.type log
t location /var/log/auth.log
t manager.name wazuh-server
t predecoder.hostname mail
t predecoder.program_name snort
t predecoder.timestamp Jul 13 23:25:16
t rule.description First time this IDS alert is generated.
rule.firedtimes 4
t rule.groups ids, fts
t rule.id 20100
rule.level 8
rule.mail false
timestamp Jul 13, 2024 @ 23:25:17.552

Now we have to perform EternalBlue RCE Attack on Windows 7 and monitor SNORT IDS logs in to Wazuh.

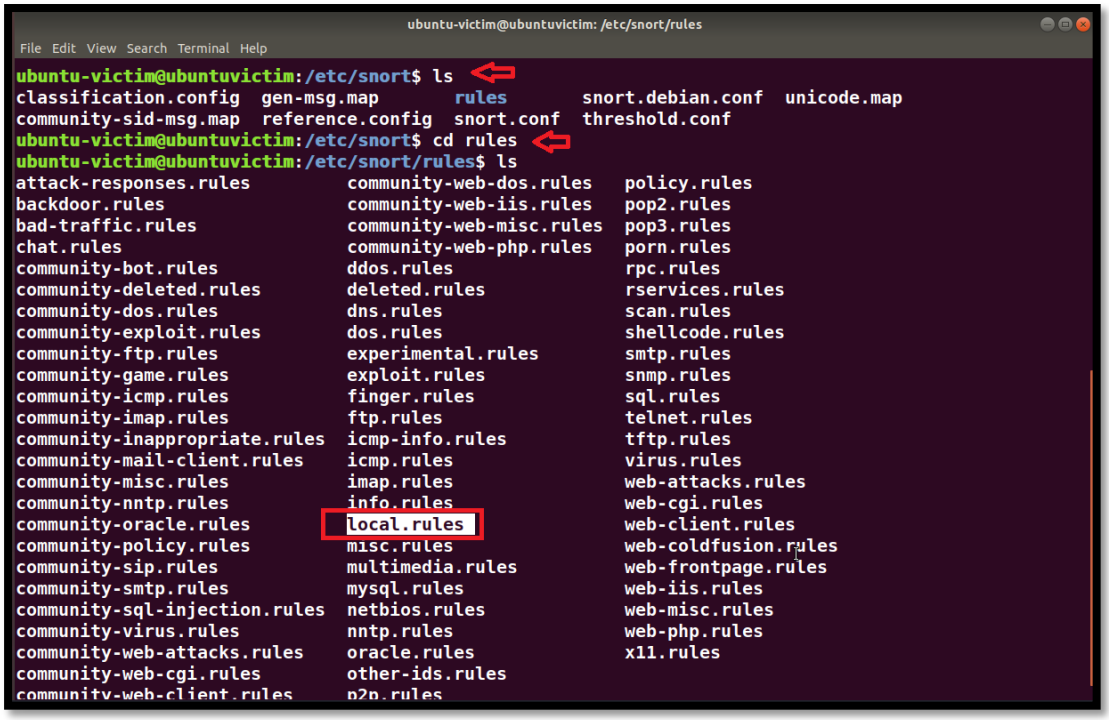
Step 04: Now open the “community.rules” file.



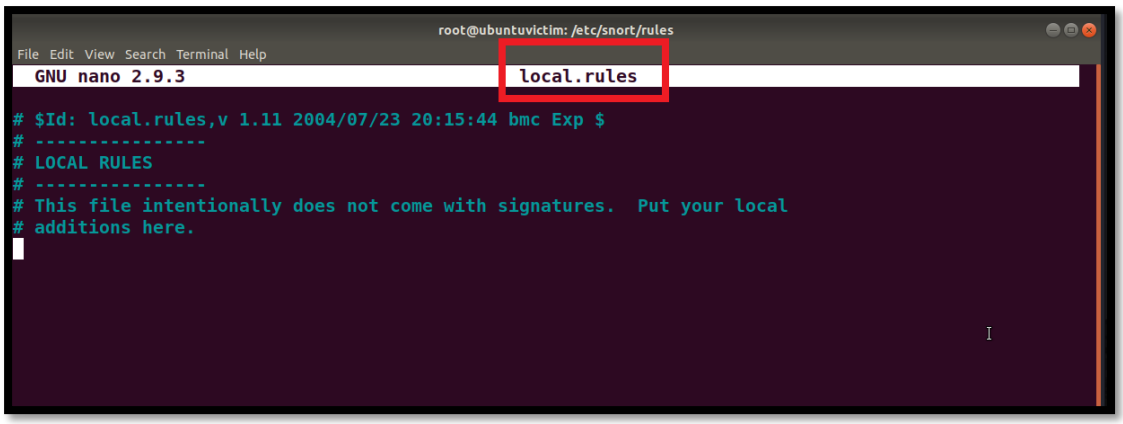
Select the rule which we use to monitor EternalBlue RCE attack.



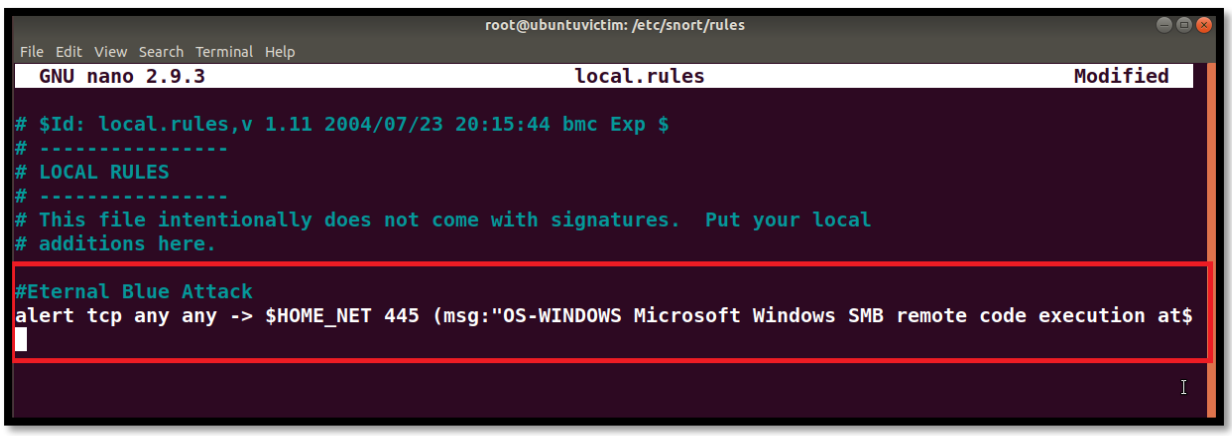
Go to snort rules directory and edit “local.rules”. Follow same as shown in the figure.



Use “nano” text editor for edit “local.rules” file.

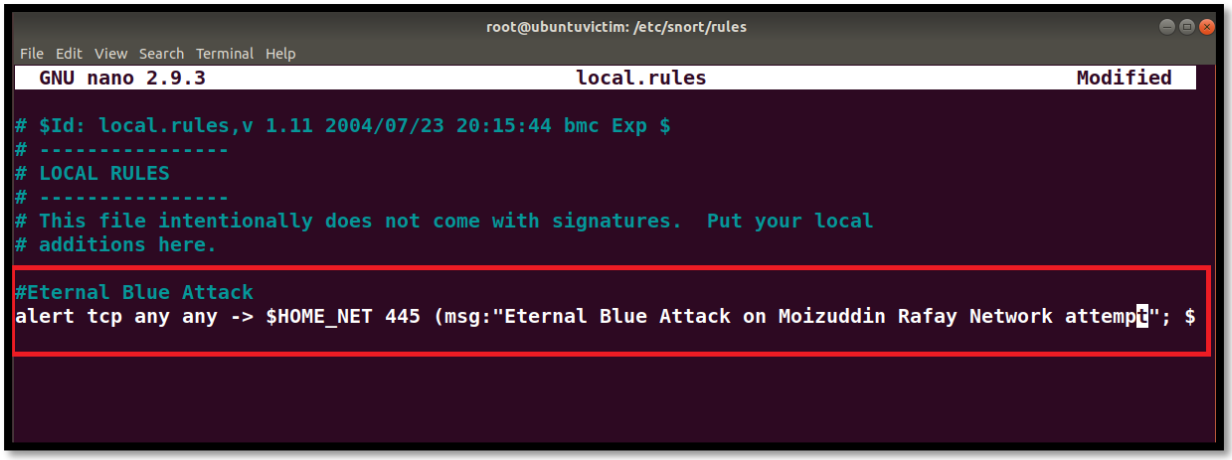


Paste the EternalBlue rule here.

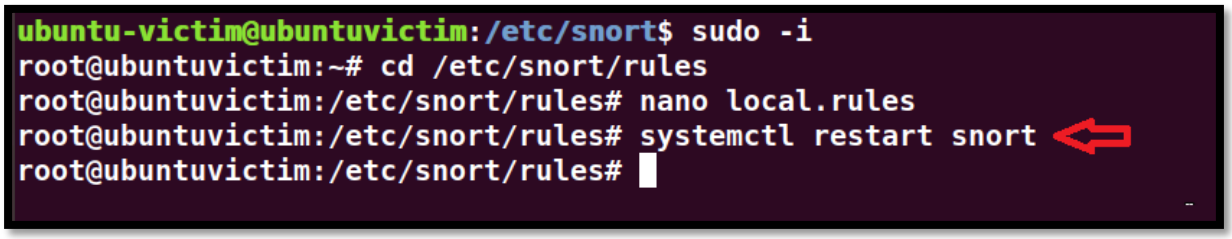


I am edit msg of the rule with my name for FUN.

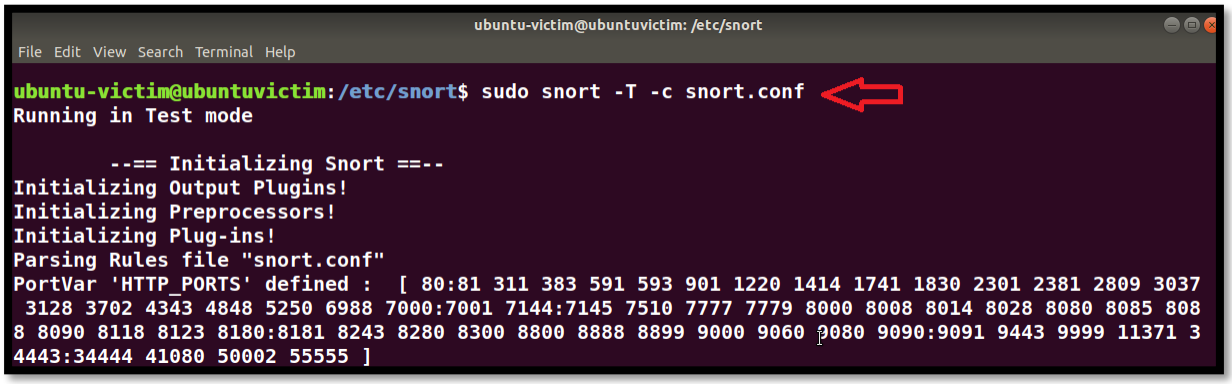
“Eternal Blue Attack on Moizuddin Rafay Network”



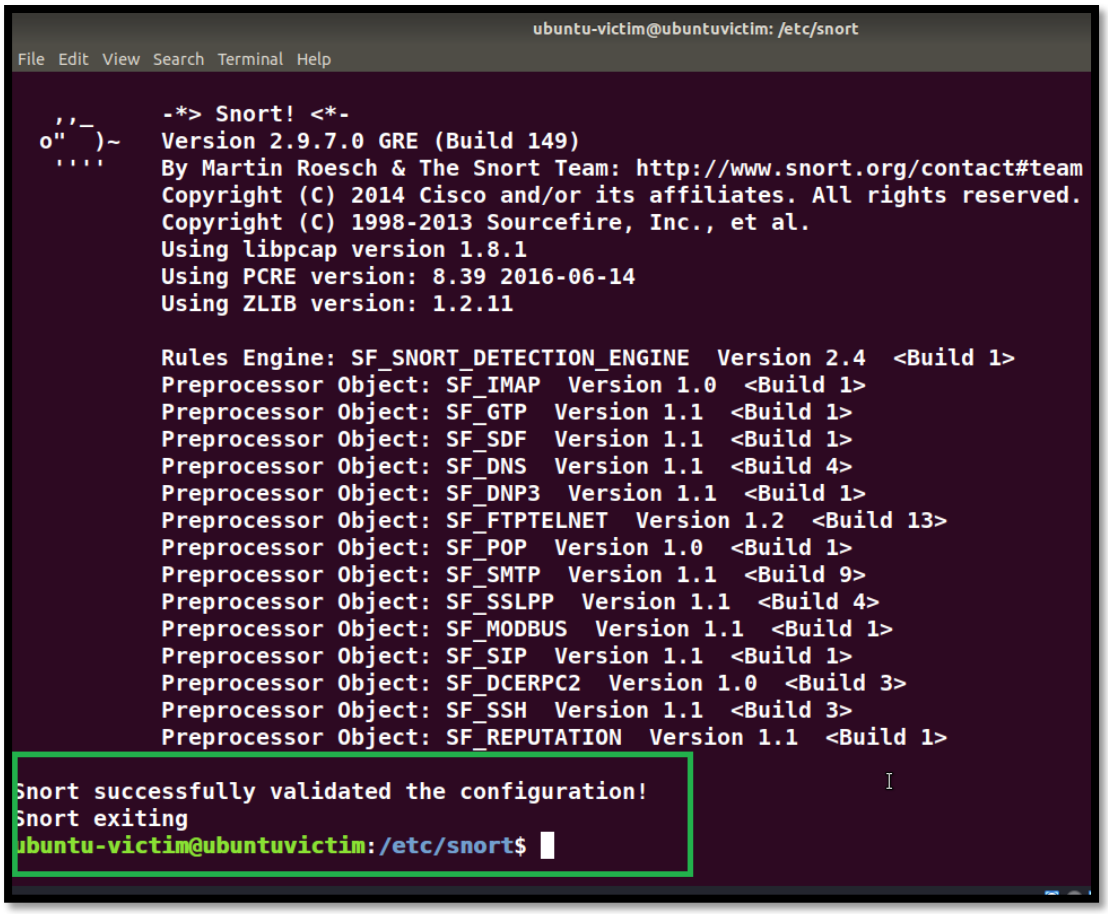
Now save the “local.rules” file and restart snort.



Check the snort configuration to verify it’s successfully done.



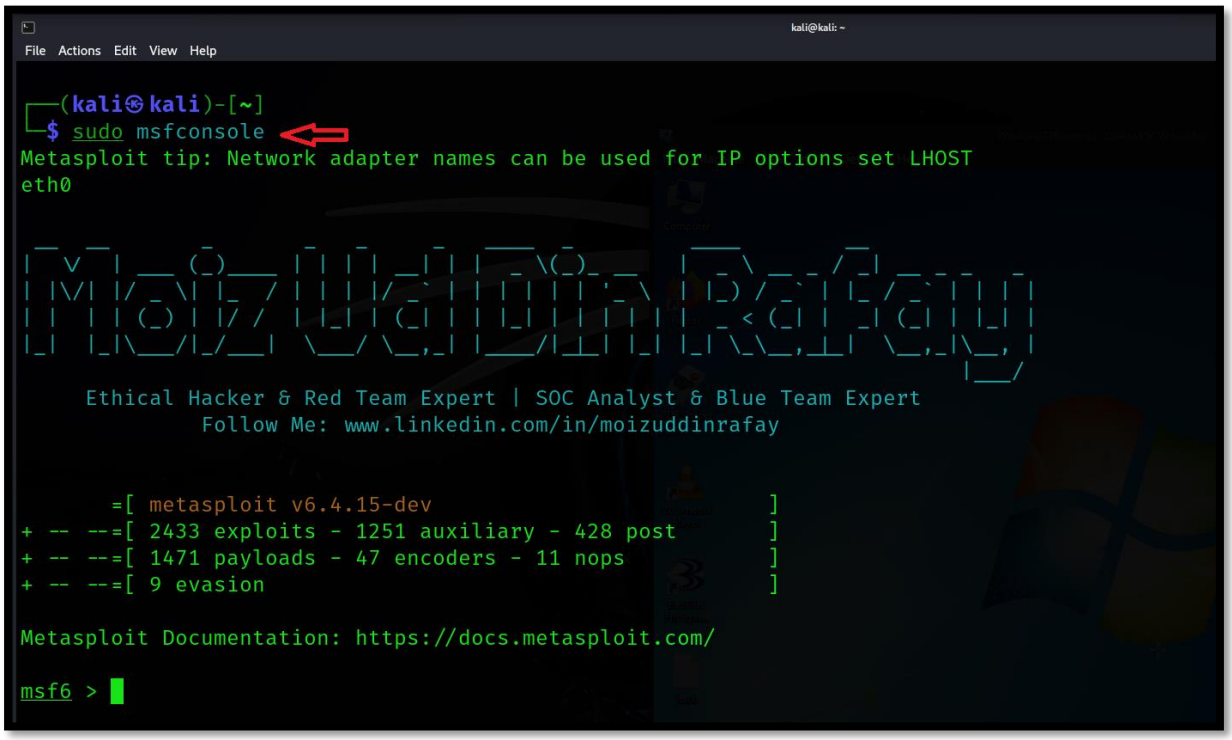
A



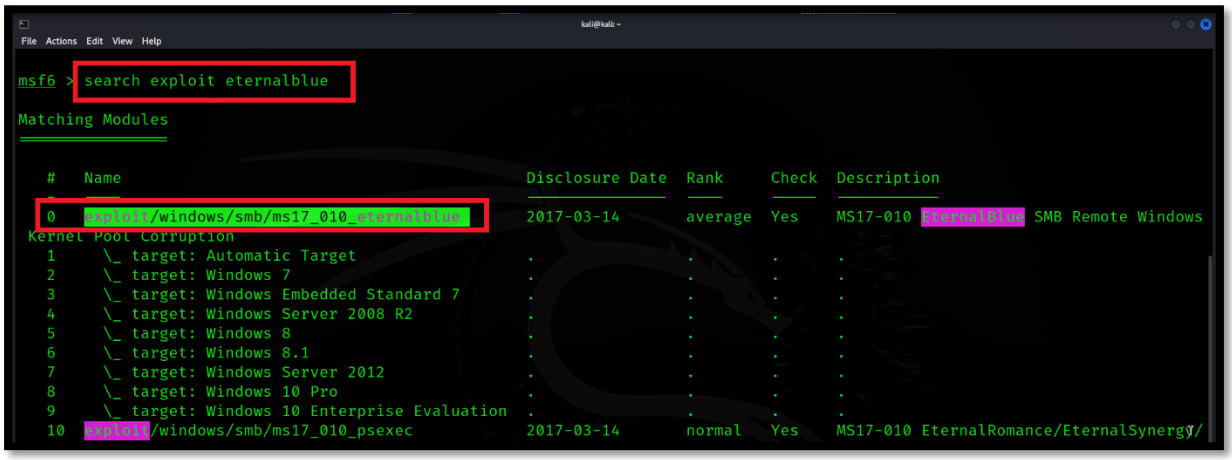
Step 05: Now open vulnerable windows 7

Note: I make my all machine highly vulnerable for my lab environment. If you want to learn how to make cybersecurity and penetration testing vulnerable labs. Book a meeting with me.

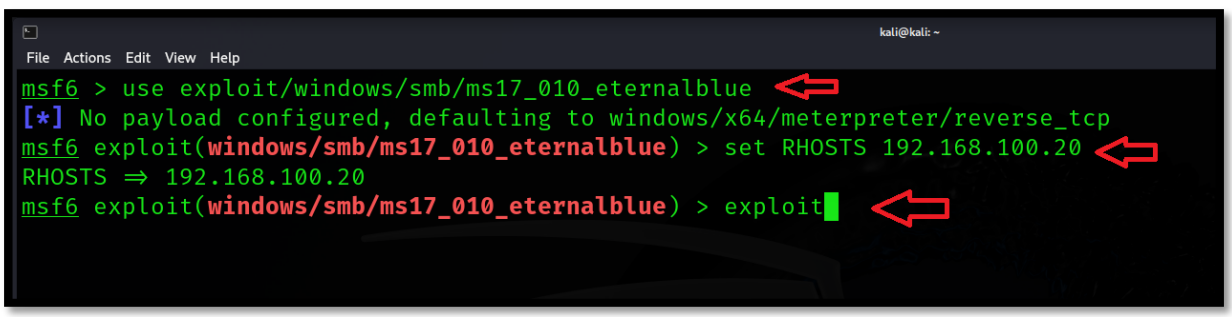
Launch Metasploit-Framework.
Command: sudo msfconsole



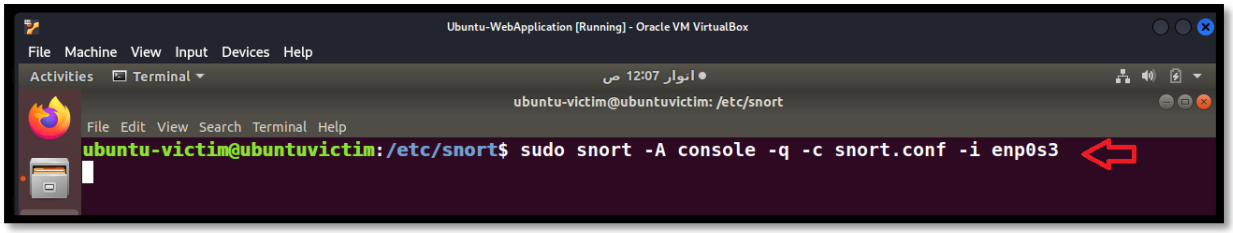
Search the EternalBlue exploit.

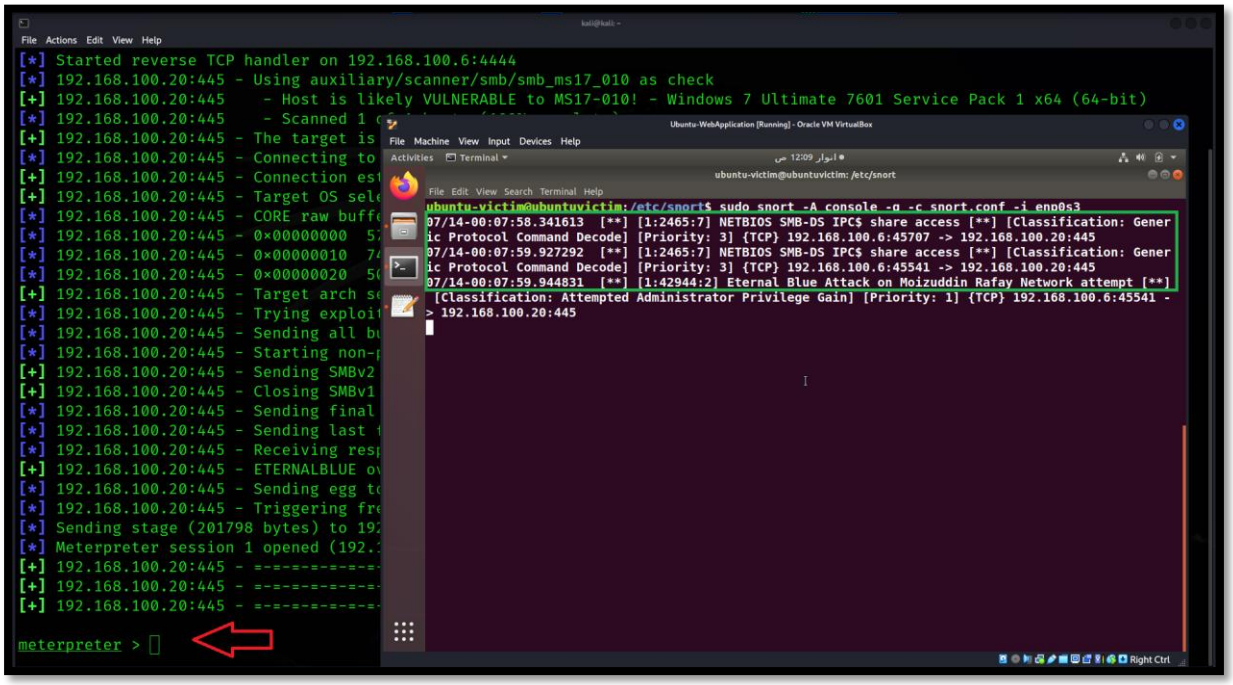


Configure the EternalBlue exploit. Follow the same show in figure.

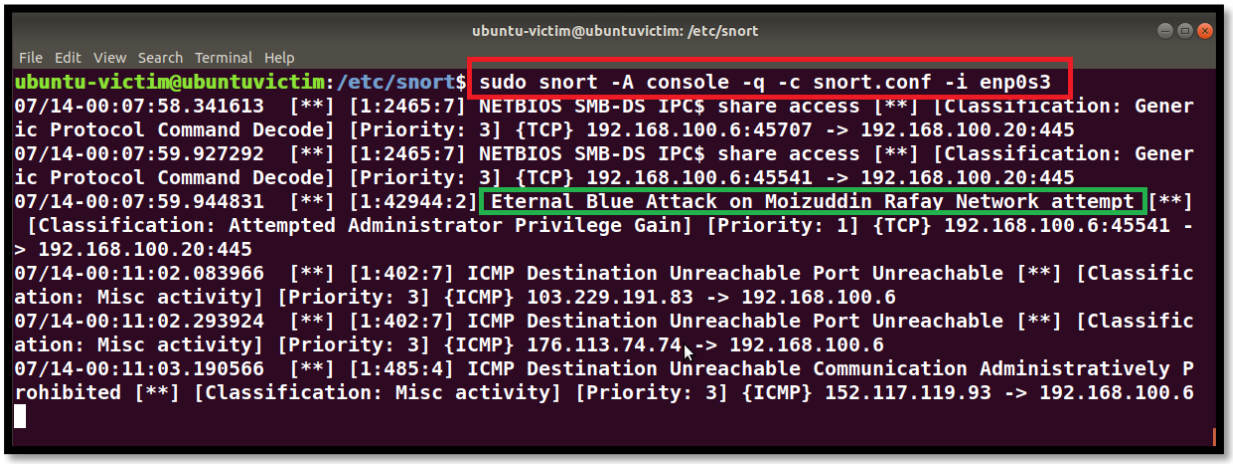


Step 06: Run snort again and monitor the EternalBlue Attack.

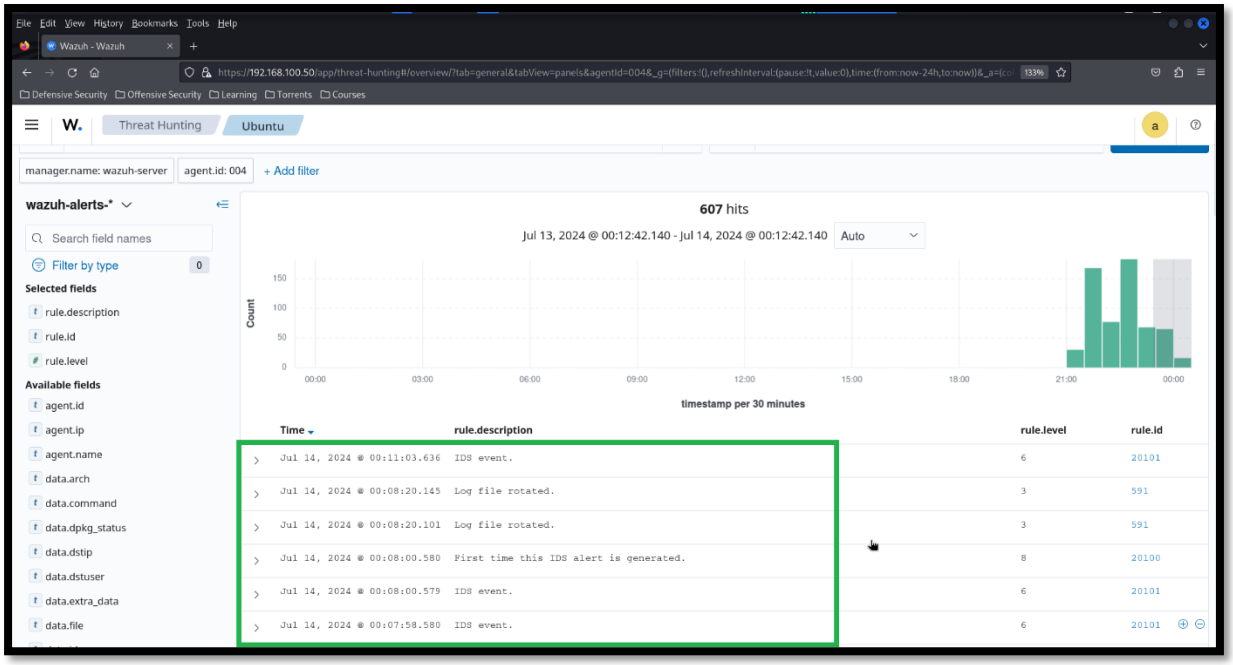


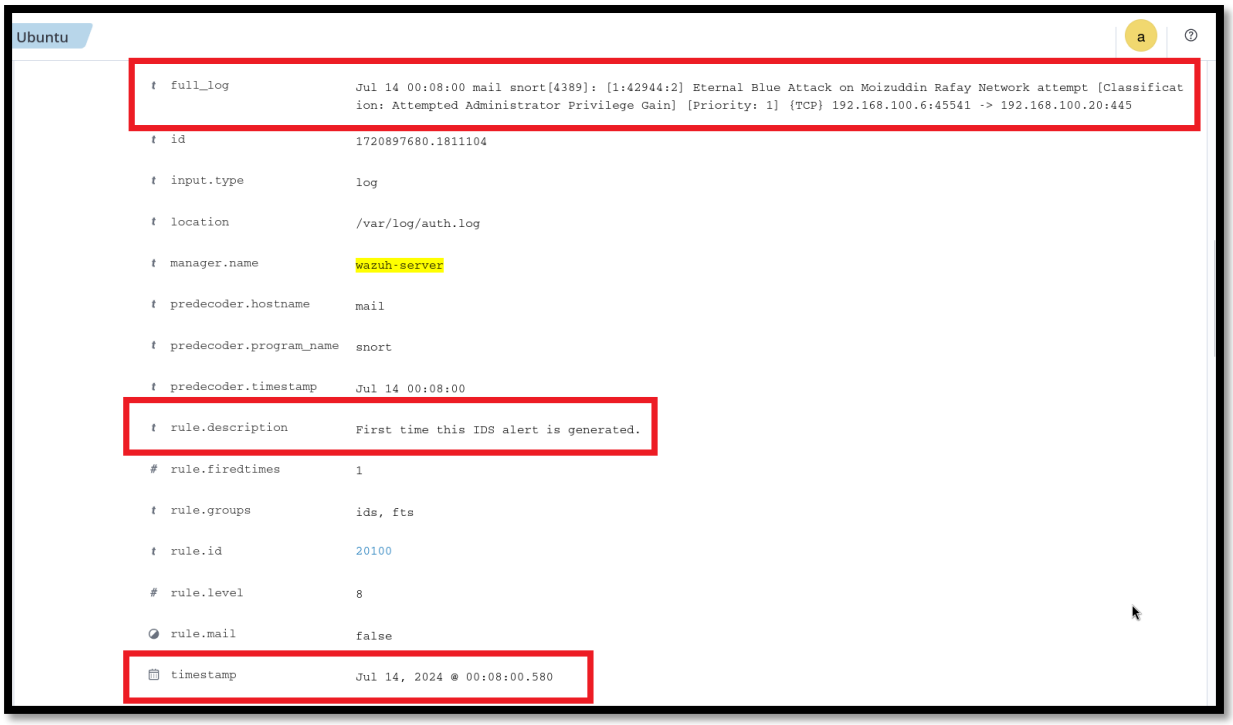


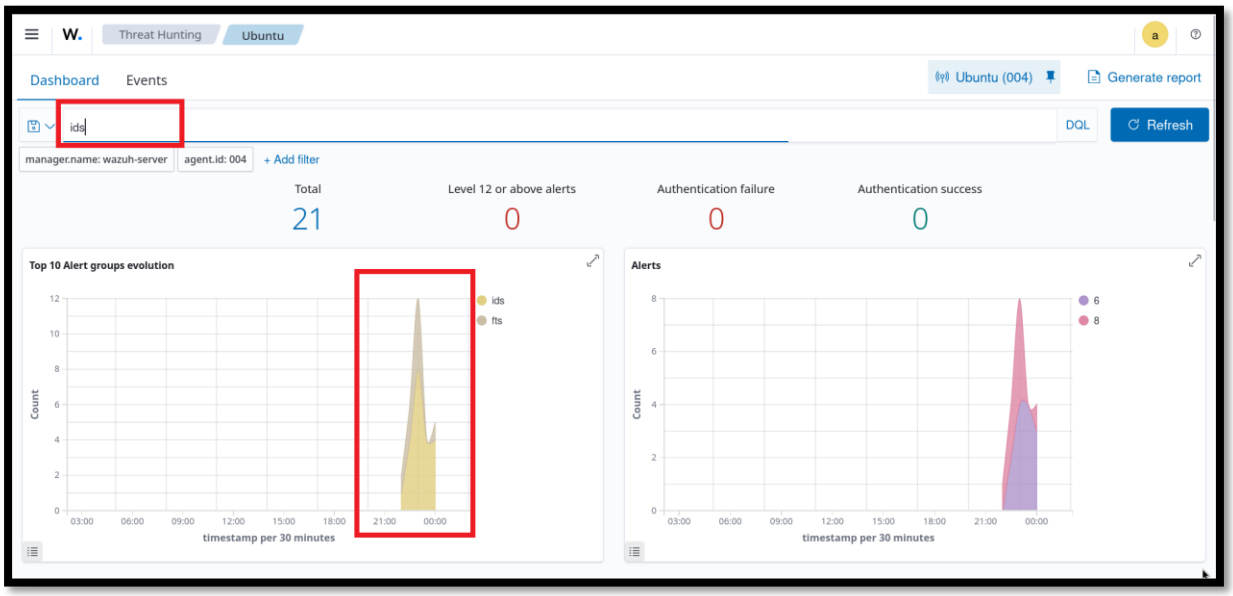
Here is EternalBlue RCE attack is detected by SNORT IDS.

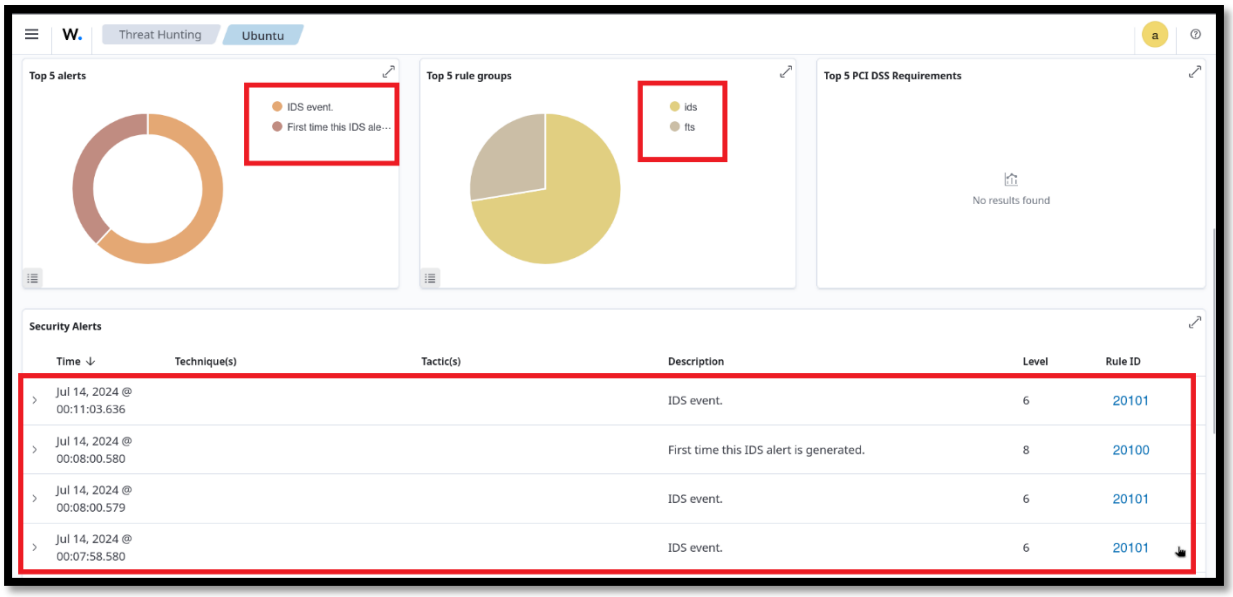


Now go to Wazuh-Dashboard and monitor the new IDS logs.




Ubuntu
a
t full_log Jul 14 00:08:00 mail snort[4389]: [1:42944:2] Eternal Blue Attack on Moizuddin Rafay Network attempt [Classification: Attempted Administrator Privilege Gain] [Priority: 1] {TCP} 192.168.100.6:45541 -> 192.168.100.20:445
t id 1720897680.1811104
t input.type log
t location /var/log/auth.log
t manager.name wazuh-server
t predecoder.hostname mail
t predecoder.program_name snort
t predecoder.timestamp Jul 14 00:08:00
t rule.description First time this IDS alert is generated.
rule.firedtimes 1
t rule.groups ids, fts
t rule.id 20100
rule.level 8
rule.mail false
timestamp Jul 14, 2024 @ 00:08:00.580


W.
Threat Hunting
Ubuntu
a
Dashboard
Events
Ubuntu (004)
Generate report
ids
DQL
Refresh
manager.name: wazuh-server
agent.id: 004
+ Add filter
Total
21
Level 12 or above alerts
0
Authentication failure
0
Authentication success
0
Top 10 Alert groups evolution
ids
fts
Count
timestamp per 30 minutes
Alerts
6
8
Count
timestamp per 30 minutes



SUMMARY:

Integrating Snort IDS with Wazuh enhances the overall security posture of an organization by providing real-time threat detection, centralized monitoring, and actionable insights into network activity. This integration enables security teams to effectively detect, respond to, and mitigate potential security incidents across their infrastructure.

Regards

MUHAMMAD MOIZ UD DIN RAFAY
Ethical Hacker | Cyber Security Analyst

Need Training on Wazuh..?

Contact: +92-3004962168
Email: muhammadmoizuddinrafay@gmail.com
LinkedIn: www.linkedin.com/in/moizuddinrafay