Snort

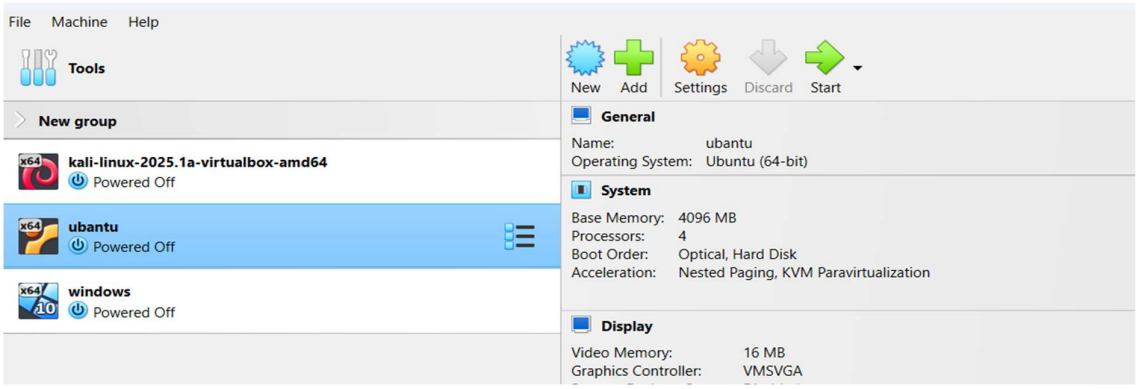
What is snort ?

Snort is an open-source intrusion detection and prevention system (IDS/IPS) developed by Cisco that monitors network traffic in real-time to detect and prevent cyber threats. It operates in three modes: sniffer mode (captures live traffic), packet logger mode (stores packets for analysis), and network intrusion detection mode (analyzes traffic using predefined rules). Snort uses signature-based detection, protocol analysis, and content matching to identify attacks such as malware, port scans, and DoS attempts. It is widely used due to its flexibility, custom rule support, and integration with security tools, making it a popular choice for network defense.

How to install snort? /snort setup

first I clear we need 2 virtual machines 1st for snort setup(ubantu) and 2nd for checking snort is working or not.

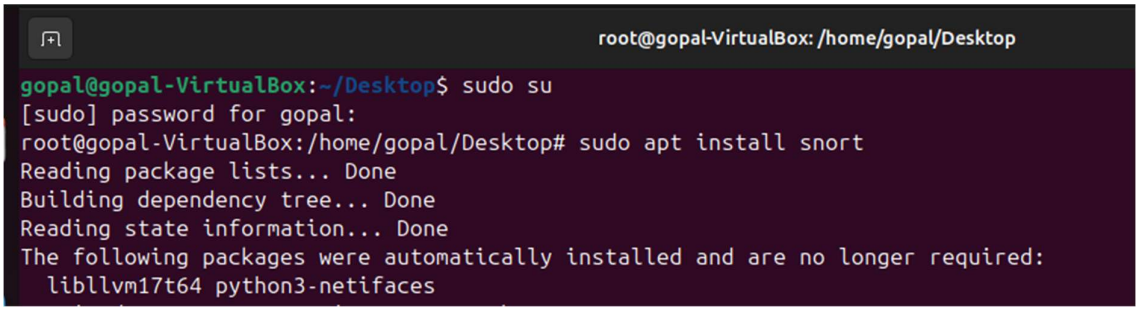
Start ubantu for snort setup



Open terminal

For snort installation we need root privillages so I am going into root user

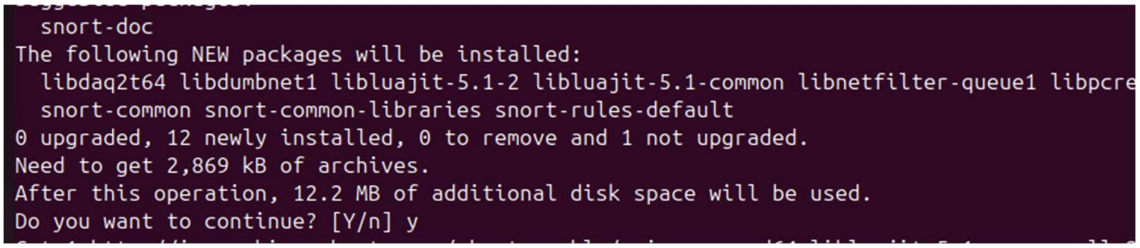
Enter this command for snort installation: **apt install snort**



When we installing snort a question is asked like this:

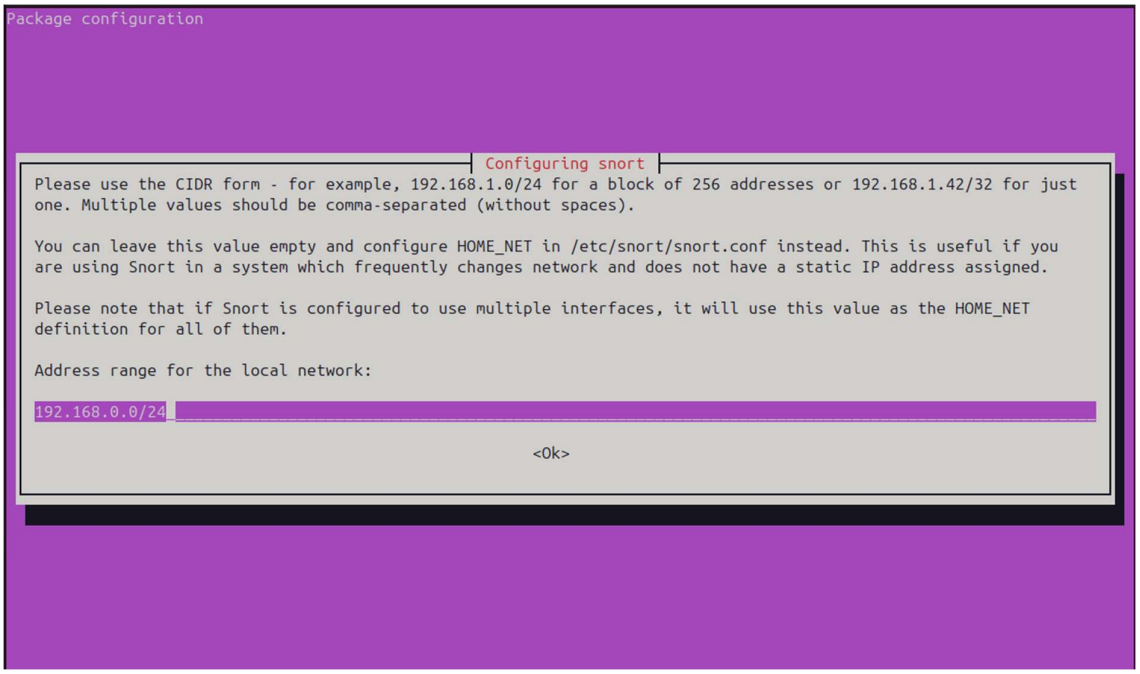
Do you want to cuntinue? **Y**

Click on **y** and press enter button

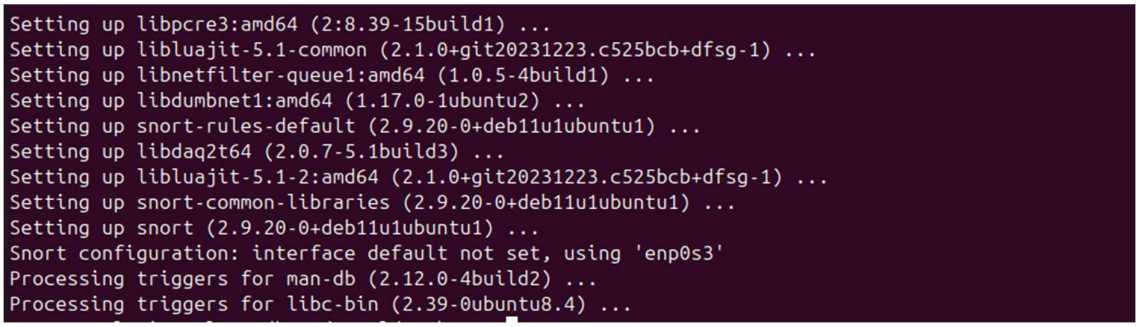


After that we have to add our network address in my case it is **192.168.155.0/24**

Then click ok



After installation it looks like this



Then we have to edit /etc/snort/snort.conf file

For this I am using this command: **nano /etc/snort/snort.conf**

```
root@gopal-VirtualBox:/home/gopal/Desktop# nano /etc/snort/snort.conf
```

We have to add our network ip address in front of **ipvar HOME_NET**

ipvar HOME_NET 192.168.155.0/24

then **ctrl + x** to save **y** and **Enter** botton

```
# Setup the network addresses you are protecting
#
# Note to Debian users: this value is overriden when starting
# up the Snort daemon through the init.d script by the
# value of DEBIAN_SNORT_HOME_NET s defined in the
# /etc/snort/snort.debian.conf configuration file
#
ipvar HOME_NET 192.168.155.0/24

# 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

# List of DNS servers on your network
ipvar DNS_SERVERS $HOME_NET
```

After this we have to add some snort rules in snort file

Nano /etc/snort/rules/local.rules

```
root@gopal-VirtualBox:/home/gopal/Desktop# nano /etc/snort/rules/local.rules
```

I am adding some snort rules on this file

- alert tcp any any -> $HOME_NET any (msg:"TCP Connect Scan"; sid:100001; rev:1;)
- alert icmp any any -> $HOME_NET any (msg:”ping scan detected"; sid:100002; rev:1;)
- alert tcp any any -> $HOME_NET any (msg:"TCP SYN Scan"; flags:S; sid:100003; rev:1;)
- alert tcp any any -> $HOME_NET any (msg:"TCP FIN Scan"; flags:F; sid:100004; rev:1;)
- alert tcp any any -> $HOME_NET any (msg:"TCP Xmas Scan"; flags:FUP; sid:100005; rev:1;)
- alert tcp any any -> $HOME_NET any (msg:"TCP Null Scan"; flags:0; sid:100006; rev:1;)
- alert tcp any any -> $HOME_NET any (msg:"Possible Nmap Scan"; flags:S; sid:100007; rev:1;)
- alert tcp any any -> $HOME_NET any (msg:"Nmap ACK Scan"; flags:A; sid:100008; rev:1;)
- alert tcp any any -> $HOME_NET any (msg:"Nmap Window Scan”; sid:100009; rev:1;)
- alert tcp any any -> $HOME_NET any (msg:"Nmap Zombie Scan"; flags:S; sid:100010; rev:1;)
- alert tcp any any -> $HOME_NET any (msg:"Nmap SYN-ACK Scan"; flags:SA; sid:100011; rev:1;)
- alert tcp any any -> $HOME_NET any (msg:"Nmap OS Fingerprint"; sid:100012; rev:1;)
- alert udp any any -> $HOME_NET any (msg:"UDP Traffic Detected"; sid:100013; rev:1;)
- alert udp any any -> $HOME_NET any (msg:"UDP Port Scan Detected"; sid:100014; rev:1;)
- alert udp any any -> $HOME_NET 53 (msg:"Suspicious DNS Query"; sid:100015; rev:1;)
- alert udp any any -> $HOME_NET any (msg:"UDP Flood Detected"; sid:100016; rev:1;)
- alert udp any any -> $HOME_NET any (msg:"Large UDP Packet Detected"; dsize:>1500; sid:100017; rev:1;)
- alert udp any any -> $HOME_NET any (msg:"Zero-Length UDP Packet Detected"; dsize:0; sid:100018; rev:1;)
- alert udp any any -> $HOME_NET 123 (msg:"NTP Reflection Attack Detected"; sid:100020; rev:1;)
- alert udp any any -> $HOME_NET 69 (msg:"TFTP Activity Detected"; sid:100021; rev:1;)
- alert udp any any -> 255.255.255.255 any (msg:"Smurf Attack Detected"; sid:100022; rev:1;)

After adding rule s **ctrl + x** to save **y** and click **Enter** button

```
# $Id: local.rules,v 1.11 2004/07/23 20:15:44 bmc Exp $
# ----------------
# LOCAL RULES
# ----------------
alert tcp any any -> $HOME_NET any (msg:"TCP Connect Scan"; sid:100001; rev:1;)
alert icmp any any -> $HOME_NET any (msg:ping scan detected"; sid:100002; rev:1;)
alert tcp any any -> $HOME_NET any (msg:"TCP SYN Scan"; flags:S; sid:100003; rev:1;)
alert tcp any any -> $HOME_NET any (msg:"TCP FIN Scan"; flags:F; sid:100004; rev:1;)
alert tcp any any -> $HOME_NET any (msg:"TCP Xmas Scan"; flags:FUP; sid:100005; rev:1;)
alert tcp any any -> $HOME_NET any (msg:"TCP Null Scan"; flags:0; sid:100006; rev:1;)
alert tcp any any -> $HOME_NET any (msg:"Possible Nmap Scan"; flags:S; sid:100007; rev:1;)
alert tcp any any -> $HOME_NET any (msg:"Nmap ACK Scan"; flags:A;  sid:100008; rev:1;)
alert tcp any any -> $HOME_NET any (msg:"Nmap Window Scan"; sid:100009; rev:1;)
alert tcp any any -> $HOME_NET any (msg:"Nmap Zombie Scan"; flags:S; sid:100010; rev:1;)
alert tcp any any -> $HOME_NET any (msg:"Nmap SYN-ACK Scan"; flags:SA; sid:100011; rev:1;)
alert tcp any any -> $HOME_NET any (msg:"Nmap OS Fingerprint"; sid:100012; rev:1;)
alert udp any any -> $HOME_NET any (msg:"UDP Traffic Detected"; sid:100013; rev:1;)
alert udp any any -> $HOME_NET any (msg:"UDP Port Scan Detected"; sid:100014; rev:1;)
alert udp any any -> $HOME_NET 53 (msg:"Suspicious DNS Query"; sid:100015; rev:1;)
alert udp any any -> $HOME_NET any (msg:"UDP Flood Detected";  sid:100016; rev:1;)
alert udp any any -> $HOME_NET any (msg:"Large UDP Packet Detected"; dsize:>1500; sid:100017; rev:1;)
alert udp any any -> $HOME_NET any (msg:"Zero-Length UDP Packet Detected"; dsize:0; sid:100018; rev:1;)
alert udp any any -> $HOME_NET 123 (msg:"NTP Reflection Attack Detected"; sid:100020; rev:1;)
alert udp any any -> $HOME_NET 69 (msg:"TFTP Activity Detected"; sid:100021; rev:1;)
alert udp any any -> 255.255.255.255 any (msg:"Smurf Attack Detected"; sid:100022; rev:1;)
# This file intentionally does not come with signatures.  Put your local
# additions here.
```

After that we need network interface id so we can use **ip a** command

In my case my network interface card is **enp0s3**

```
gopal@gopal-VirtualBox: ~
gopal@gopal-VirtualBox:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group defaul
t qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP gr
oup default qlen 1000
    link/ether 08:00:27:6e:a0:cf brd ff:ff:ff:ff:ff:ff
    inet 192.168.155.12/24 brd 192.168.155.255 scope global dynamic noprefixrout
e enp0s3
       valid_lft 3400sec preferred_lft 3400sec
    inet6 2401:4900:5628:c169:39f7:3680:5d70:1c36/64 scope global temporary dyna
mic
       valid_lft 7077sec preferred_lft 7077sec
    inet6 2401:4900:5628:c169:a00:27ff:fe6e:a0cf/64 scope global dynamic mngtmpa
ddr
       valid_lft 7077sec preferred_lft 7077sec
    inet6 fe80::a00:27ff:fe6e:a0cf/64 scope link
       valid_lft forever preferred_lft forever
gopal@gopal-VirtualBox:~$
```

Now we have configure our rules so we use this command

Snort -T -c /etc/snort/snort.conf -I enp0s3

```
root@gopal-VirtualBox:/home/gopal/Desktop# snort -T -c /etc/snort/snort.conf -i enp0s3
```

After configuration this type of interface is show

```
           Using libpcap version 1.10.4 (with TPACKET_V3)
           Using PCRE version: 8.39 2016-06-14
           Using ZLIB version: 1.3

           Rules Engine: SF_SNORT_DETECTION_ENGINE  Version 3.2  <Build 1>
           Preprocessor Object: SF_IMAP  Version 1.0  <Build 1>
           Preprocessor Object: SF_DCERPC2  Version 1.0  <Build 3>
           Preprocessor Object: SF_FTPTELNET  Version 1.2  <Build 13>
           Preprocessor Object: SF_MODBUS  Version 1.1  <Build 1>
           Preprocessor Object: SF_POP  Version 1.0  <Build 1>
           Preprocessor Object: SF_SMTP  Version 1.1  <Build 9>
           Preprocessor Object: SF_GTP  Version 1.1  <Build 1>
           Preprocessor Object: SF_SSLPP  Version 1.1  <Build 4>
           Preprocessor Object: SF_DNS  Version 1.1  <Build 4>
           Preprocessor Object: SF_REPUTATION  Version 1.1  <Build 1>
           Preprocessor Object: SF_SIP  Version 1.1  <Build 1>
           Preprocessor Object: SF_DNP3  Version 1.1  <Build 1>
           Preprocessor Object: SF_S7COMMPLUS  Version 1.0  <Build 1>
           Preprocessor Object: appid  Version 1.1  <Build 5>
           Preprocessor Object: SF_SDF  Version 1.1  <Build 1>
           Preprocessor Object: SF_SSH  Version 1.1  <Build 3>

Total snort Fixed Memory Cost - MaxRss:103764
Snort successfully validated the configuration!
Snort exiting
```

After this we can check our set up is done or not from this command

snort -A CONSOLE -q -c /etc/snort/snort.conf -i enp0s3

```
root@gopal-VirtualBox:/home/gopal/Desktop# snort -A CONSOLE -q -c /etc/snort/snort.conf -i enp0s3
```

From kali I am pinging this machine

```
┌──(root㉿gopal)-[/home/gopal]
└─# ping 192.168.155.12
PING 192.168.155.12 (192.168.155.12) 56(84) bytes of data.
64 bytes from 192.168.155.12: icmp_seq=1 ttl=64 time=1.28 ms
64 bytes from 192.168.155.12: icmp_seq=2 ttl=64 time=2.00 ms
64 bytes from 192.168.155.12: icmp_seq=3 ttl=64 time=0.920 ms
64 bytes from 192.168.155.12: icmp_seq=4 ttl=64 time=1.59 ms
64 bytes from 192.168.155.12: icmp_seq=5 ttl=64 time=1.30 ms
64 bytes from 192.168.155.12: icmp_seq=6 ttl=64 time=1.73 ms
64 bytes from 192.168.155.12: icmp_seq=7 ttl=64 time=4.86 ms
64 bytes from 192.168.155.12: icmp_seq=8 ttl=64 time=4.81 ms
64 bytes from 192.168.155.12: icmp_seq=9 ttl=64 time=2.97 ms
64 bytes from 192.168.155.12: icmp_seq=10 ttl=64 time=1.38 ms
^C
── 192.168.155.12 ping statistics ──
10 packets transmitted, 10 received, 0% packet loss, time 9820ms
rtt min/avg/max/mdev = 0.920/2.284/4.864/1.379 ms
```

Then the snort shows ping detected message

```
root@gopal-VirtualBox:/home/gopal/Desktop# snort -A CONSOLE -q -c /etc/snort/snort.conf -i enp0s3
03/31-11:16:02.381457  [**] [1:100016:1] UDP Flood Detected [**] [Priority: 0] {UDP} 192.168.155.6:57621 -> 192.168.155.255:57621
03/31-11:16:02.381457  [**] [1:100014:1] UDP Port Scan Detected [**] [Priority: 0] {UDP} 192.168.155.6:57621 -> 192.168.155.255:57621
03/31-11:16:02.381457  [**] [1:100013:1] UDP Traffic Detected [**] [Priority: 0] {UDP} 192.168.155.6:57621 -> 192.168.155.255:57621
03/31-11:16:12.907601  [**] [1:100002:1] ping scan detected" [**] [Priority: 0] {ICMP} 192.168.155.118 -> 192.168.155.12
03/31-11:16:12.907666  [**] [1:100002:1] ping scan detected" [**] [Priority: 0] {ICMP} 192.168.155.12 -> 192.168.155.118
03/31-11:16:14.235072  [**] [1:100002:1] ping scan detected" [**] [Priority: 0] {ICMP} 192.168.155.118 -> 192.168.155.12
03/31-11:16:14.235104  [**] [1:100002:1] ping scan detected" [**] [Priority: 0] {ICMP} 192.168.155.12 -> 192.168.155.118
03/31-11:16:15.237843  [**] [1:100002:1] ping scan detected" [**] [Priority: 0] {ICMP} 192.168.155.118 -> 192.168.155.12
03/31-11:16:15.237876  [**] [1:100002:1] ping scan detected" [**] [Priority: 0] {ICMP} 192.168.155.12 -> 192.168.155.118
03/31-11:16:16.247138  [**] [1:100002:1] ping scan detected" [**] [Priority: 0] {ICMP} 192.168.155.118 -> 192.168.155.12
03/31-11:16:16.247201  [**] [1:100002:1] ping scan detected" [**] [Priority: 0] {ICMP} 192.168.155.12 -> 192.168.155.118
03/31-11:16:17.270995  [**] [1:100002:1] ping scan detected" [**] [Priority: 0] {ICMP} 192.168.155.118 -> 192.168.155.12
03/31-11:16:17.271027  [**] [1:100002:1] ping scan detected" [**] [Priority: 0] {ICMP} 192.168.155.12 -> 192.168.155.118
03/31-11:16:18.309681  [**] [1:100002:1] ping scan detected" [**] [Priority: 0] {ICMP} 192.168.155.118 -> 192.168.155.12
03/31-11:16:18.309737  [**] [1:100002:1] ping scan detected" [**] [Priority: 0] {ICMP} 192.168.155.12 -> 192.168.155.118
03/31-11:16:19.469626  [**] [1:100002:1] ping scan detected" [**] [Priority: 0] {ICMP} 192.168.155.118 -> 192.168.155.12
03/31-11:16:19.469671  [**] [1:100002:1] ping scan detected" [**] [Priority: 0] {ICMP} 192.168.155.12 -> 192.168.155.118
03/31-11:16:20.722418  [**] [1:100002:1] ping scan detected" [**] [Priority: 0] {ICMP} 192.168.155.118 -> 192.168.155.12
03/31-11:16:20.722449  [**] [1:100002:1] ping scan detected" [**] [Priority: 0] {ICMP} 192.168.155.12 -> 192.168.155.118
03/31-11:16:21.722824  [**] [1:100002:1] ping scan detected" [**] [Priority: 0] {ICMP} 192.168.155.118 -> 192.168.155.12
03/31-11:16:21.722851  [**] [1:100002:1] ping scan detected" [**] [Priority: 0] {ICMP} 192.168.155.12 -> 192.168.155.118
```

Also we can test **nmap -A** command

```
┌──(root㉿gopal)-[/home/gopal]
└─# nmap -A 192.168.155.12
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-31 01:46 EDT
Nmap scan report for 192.168.155.12
Host is up (0.0019s latency).
All 1000 scanned ports on 192.168.155.12 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: 08:00:27:6E:A0:CF (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT     ADDRESS
1   1.90 ms 192.168.155.12

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 2.92 seconds
```

After that it shows nmap scan alert

```
03/31-11:16:32.366924  [**] [1:100013:1] UDP Traffic Detected [**] [Priority: 0] {UDP} 192.168.155.6:57621 -> 192.168.155.255:57621
03/31-11:16:45.935821  [**] [1:100010:1] Nmap Zombie Scan [**] [Priority: 0] {TCP} 192.168.155.118:37429 -> 192.168.155.12:993
03/31-11:16:45.935821  [**] [1:100009:1] Nmap Window Scan [**] [Priority: 0] {TCP} 192.168.155.118:37429 -> 192.168.155.12:993
03/31-11:16:45.935821  [**] [1:100007:1] Possible Nmap Scan [**] [Priority: 0] {TCP} 192.168.155.118:37429 -> 192.168.155.12:993
03/31-11:16:45.935821  [**] [1:100003:1] TCP SYN Scan [**] [Priority: 0] {TCP} 192.168.155.118:37429 -> 192.168.155.12:993
03/31-11:16:45.935821  [**] [1:100001:1] TCP Connect Scan [**] [Priority: 0] {TCP} 192.168.155.118:37429 -> 192.168.155.12:993
03/31-11:16:45.935823  [**] [1:100010:1] Nmap Zombie Scan [**] [Priority: 0] {TCP} 192.168.155.118:37429 -> 192.168.155.12:3306
03/31-11:16:45.935823  [**] [1:100009:1] Nmap Window Scan [**] [Priority: 0] {TCP} 192.168.155.118:37429 -> 192.168.155.12:3306
03/31-11:16:45.935823  [**] [1:100007:1] Possible Nmap Scan [**] [Priority: 0] {TCP} 192.168.155.118:37429 -> 192.168.155.12:3306
03/31-11:16:45.935823  [**] [1:100003:1] TCP SYN Scan [**] [Priority: 0] {TCP} 192.168.155.118:37429 -> 192.168.155.12:3306
03/31-11:16:45.935823  [**] [1:100001:1] TCP Connect Scan [**] [Priority: 0] {TCP} 192.168.155.118:37429 -> 192.168.155.12:3306
03/31-11:16:45.935824  [**] [1:100010:1] Nmap Zombie Scan [**] [Priority: 0] {TCP} 192.168.155.118:37429 -> 192.168.155.12:25
03/31-11:16:45.935824  [**] [1:100009:1] Nmap Window Scan [**] [Priority: 0] {TCP} 192.168.155.118:37429 -> 192.168.155.12:25
03/31-11:16:45.935824  [**] [1:100007:1] Possible Nmap Scan [**] [Priority: 0] {TCP} 192.168.155.118:37429 -> 192.168.155.12:25
03/31-11:16:45.935824  [**] [1:100003:1] TCP SYN Scan [**] [Priority: 0] {TCP} 192.168.155.118:37429 -> 192.168.155.12:25
03/31-11:16:45.935824  [**] [1:100001:1] TCP Connect Scan [**] [Priority: 0] {TCP} 192.168.155.118:37429 -> 192.168.155.12:25
03/31-11:16:45.935824  [**] [1:100010:1] Nmap Zombie Scan [**] [Priority: 0] {TCP} 192.168.155.118:37429 -> 192.168.155.12:139
03/31-11:16:45.935824  [**] [1:100009:1] Nmap Window Scan [**] [Priority: 0] {TCP} 192.168.155.118:37429 -> 192.168.155.12:139
03/31-11:16:45.935824  [**] [1:100007:1] Possible Nmap Scan [**] [Priority: 0] {TCP} 192.168.155.118:37429 -> 192.168.155.12:139
03/31-11:16:45.935824  [**] [1:100003:1] TCP SYN Scan [**] [Priority: 0] {TCP} 192.168.155.118:37429 -> 192.168.155.12:139
03/31-11:16:45.935824  [**] [1:100001:1] TCP Connect Scan [**] [Priority: 0] {TCP} 192.168.155.118:37429 -> 192.168.155.12:139
03/31-11:16:45.936405  [**] [1:100009:1] Nmap Window Scan [**] [Priority: 0] {TCP} 192.168.155.12:993 -> 192.168.155.118:37429
03/31-11:16:45.936405  [**] [1:100001:1] TCP Connect Scan [**] [Priority: 0] {TCP} 192.168.155.12:993 -> 192.168.155.118:37429
03/31-11:16:45.936665  [**] [1:100009:1] Nmap Window Scan [**] [Priority: 0] {TCP} 192.168.155.12:3306 -> 192.168.155.118:37429
```