Practical No 8

Aim : -Demonstrate intrusion detection system (ids) using any tool (snort or any other s/w).

Theory:

Network security is one of the biggest challenges that companies are facing from time to time. There are lots of attempts by the black hat hackers to break and compromise with the security of Company's network and some of them are even successful. As the use of internetincreasing, these malicious activities are gaining popularity among the black hats.

Intrusion detection system (ID) is a type of security system for computers and computer networks. Intrusion Detection basically helps in detecting outer and inner attacks performed by either user or hackers. An ID system collects information from various sources and analyses information from various areas within a computer or a network to identify possible security breaches, which include both intrusions (attacks from outside the organization) and misuse (attacks from within the organization). ID uses vulnerability assessment (sometimes referred to as scanning), which is a technology developed to assess the security of a computersystem or network.

Advantages of IDS:

- Track any changes in the behavior of network.
- Inspects system activity
- Can differentiate between normal and abnormal activities in the network
  Automated

Disadvantages of IDS:

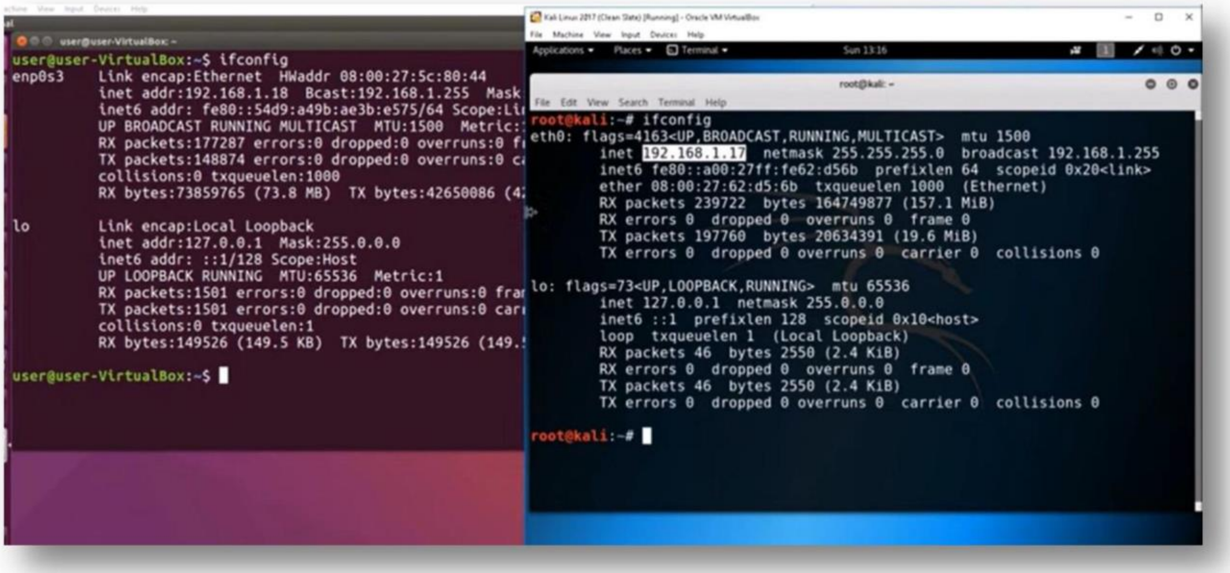
- Sometimes gives false alarms i.e. the packet wasn't malicious but IDS might still generate an alert.
- Time consuming
- Is not 100% safe from attacks

Snort tool:

Snort is a light-weight intrusion detection tool which logs the packets coming through the network and analyses the packets. Snort checks the packets coming against the rules written by the user and generate alerts if there are any matches found. The rules are written by the user in a text file which is linked with snort.conf file where all the snort configurations are mentioned. There are few commands which is used to get snort running so that it can analyze network behavior.

OUTPUT:

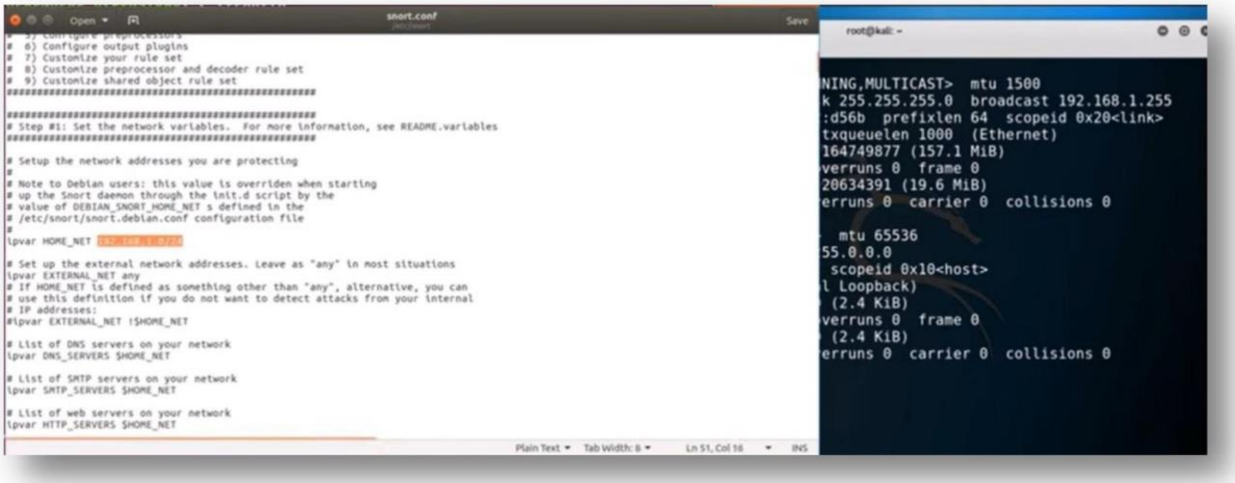
1.Checking IP Address using ifconfig.



```
user@user-VirtualBox:~$ ifconfig
enp0s3    Link encap:Ethernet  HWaddr 08:00:27:5c:80:44
          inet addr:192.168.1.18  Bcast:192.168.1.255  Mask
          inet6 addr: fe80::54d9:a49b:ae3b:e575/64 Scope:Li
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:
          RX packets:177287 errors:0 dropped:0 overruns:0 f
          TX packets:148874 errors:0 dropped:0 overruns:0 c
          collisions:0 txqueuelen:1000
          RX bytes:73859765 (73.8 MB)  TX bytes:42650086 (4

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:1501 errors:0 dropped:0 overruns:0 fra
          TX packets:1501 errors:0 dropped:0 overruns:0 car
          collisions:0 txqueuelen:1
          RX bytes:149526 (149.5 KB)  TX bytes:149526 (149.

user@user-VirtualBox:~$
```

```
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.17  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::a00:27ff:fe62:d56b  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:62:d5:6b  txqueuelen 1000  (Ethernet)
        RX packets 239722  bytes 164749877 (157.1 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 197760  bytes 20634391 (19.6 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1  (Local Loopback)
        RX packets 46  bytes 2550 (2.4 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 46  bytes 2550 (2.4 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

root@kali:~#
```

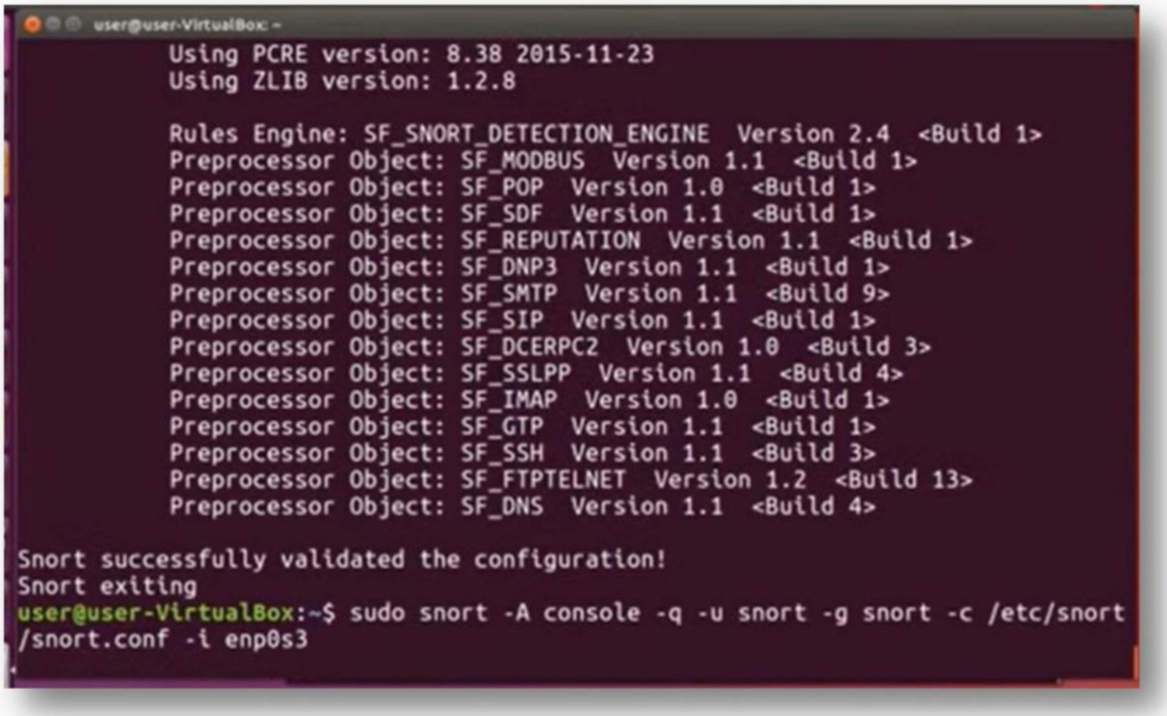
2. Checking Snort Configuration file.



```
#  6) Configure output plugins
#  7) Customize your rule set
#  8) Customize preprocessor and decoder rule set
#  9) Customize shared object rule set
###################################################

###################################################
# Step #1: Set the network variables.  For more information, see README.variables
###################################################

# 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 192.168.1.0/24

# 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

# List of SMTP servers on your network
ipvar SMTP_SERVERS $HOME_NET

# List of web servers on your network
ipvar HTTP_SERVERS $HOME_NET
```

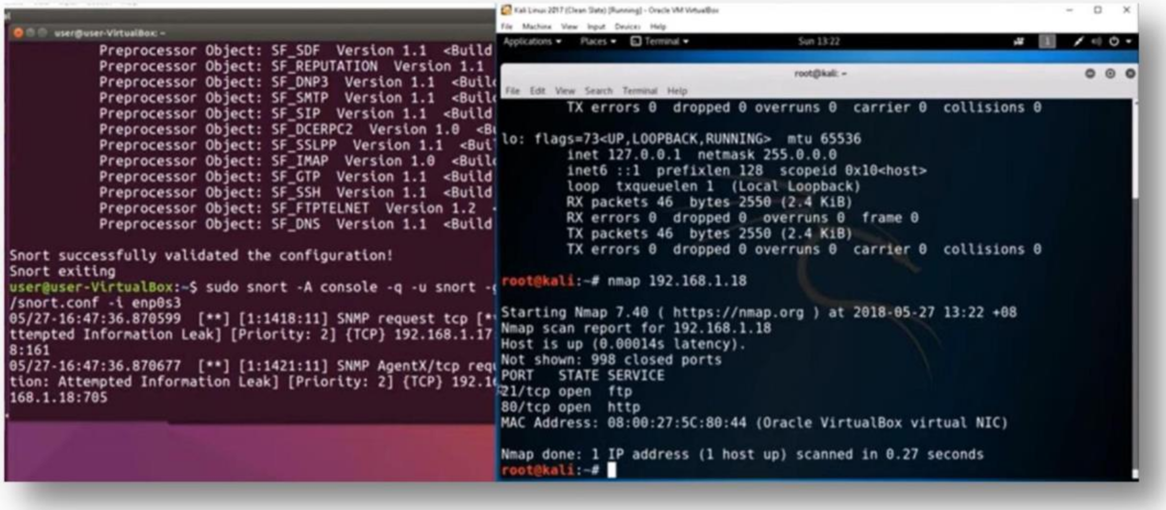
```
NING,MULTICAST>  mtu 1500
k 255.255.255.0  broadcast 192.168.1.255
:d56b  prefixlen 64  scopeid 0x20<link>
txqueuelen 1000  (Ethernet)
164749877 (157.1 MiB)
verruns 0  frame 0
20634391 (19.6 MiB)
erruns 0  carrier 0  collisions 0

  mtu 65536
55.0.0.0
 scopeid 0x10<host>
l Loopback)
 (2.4 KiB)
verruns 0  frame 0
 (2.4 KiB)
erruns 0  carrier 0  collisions 0
```

3. Validating configuration and enabling snort monitoring for UBUNTU.



```
          Using PCRE version: 8.38 2015-11-23
          Using ZLIB version: 1.2.8

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

Snort successfully validated the configuration!
Snort exiting
user@user-VirtualBox:~$ sudo snort -A console -q -u snort -g snort -c /etc/snort
/snort.conf -i enp0s3
```

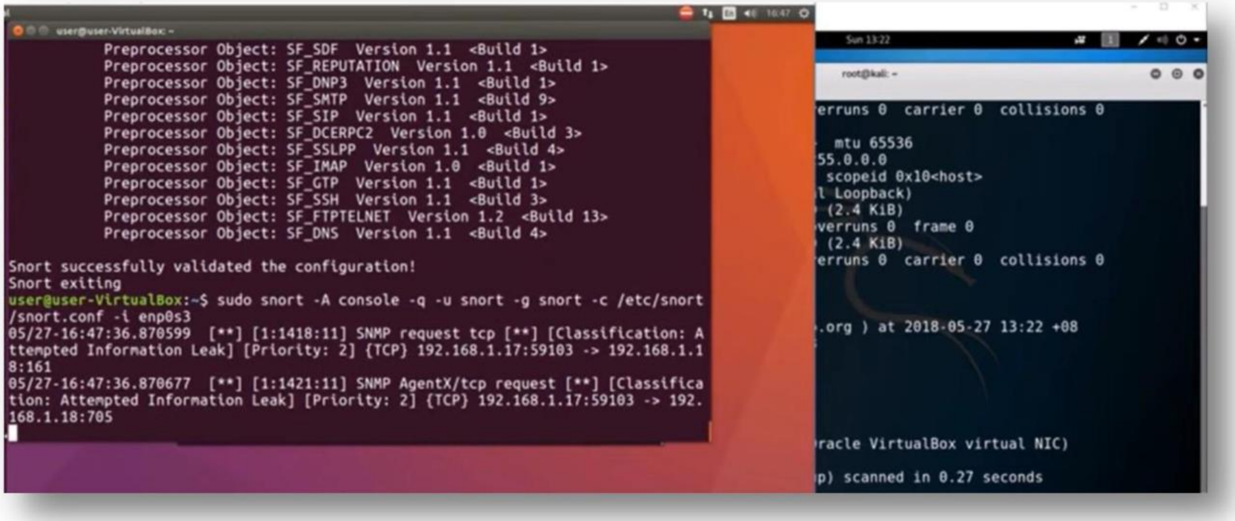
4. canning IP of UBUNTU using nmap.



```
          Preprocessor Object: SF_SDF  Version 1.1  <Build
          Preprocessor Object: SF_REPUTATION  Version 1.1
          Preprocessor Object: SF_DNP3  Version 1.1  <Buil
          Preprocessor Object: SF_SMTP  Version 1.1  <Buil
          Preprocessor Object: SF_SIP  Version 1.1  <Build
          Preprocessor Object: SF_DCERPC2  Version 1.0  <B
          Preprocessor Object: SF_SSLPP  Version 1.1  <Bui
          Preprocessor Object: SF_IMAP  Version 1.0  <Buil
          Preprocessor Object: SF_GTP  Version 1.1  <Build
          Preprocessor Object: SF_SSH  Version 1.1  <Build
          Preprocessor Object: SF_FTPTELNET  Version 1.2  
          Preprocessor Object: SF_DNS  Version 1.1  <Build

Snort successfully validated the configuration!
Snort exiting
user@user-VirtualBox:~$ sudo snort -A console -q -u snort -
/snort.conf -i enp0s3
05/27-16:47:36.870599  [**] [1:1418:11] SNMP request tcp [*
ttempted Information Leak] [Priority: 2] {TCP} 192.168.1.17
8:161
05/27-16:47:36.870677  [**] [1:1421:11] SNMP AgentX/tcp req
tion: Attempted Information Leak] [Priority: 2] {TCP} 192.1
168.1.18:705
```

```
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1  (Local Loopback)
        RX packets 46  bytes 2550 (2.4 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 46  bytes 2550 (2.4 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

root@kali:~# nmap 192.168.1.18

Starting Nmap 7.40 ( https://nmap.org ) at 2018-05-27 13:22 +08
Nmap scan report for 192.168.1.18
Host is up (0.00014s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE
21/tcp open  ftp
80/tcp open  http
MAC Address: 08:00:27:5C:80:44 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.27 seconds
root@kali:~# 
```

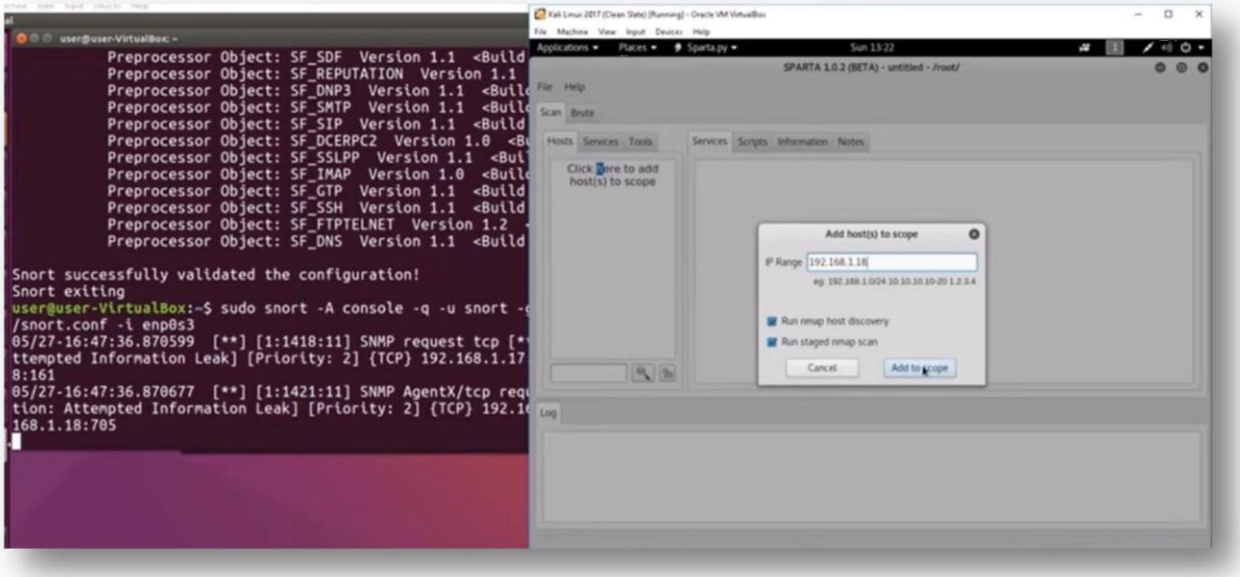
5. Snort detected the attack on open IP.



```
         Preprocessor Object: SF_SDF  Version 1.1  <Build 1>
         Preprocessor Object: SF_REPUTATION  Version 1.1  <Build 1>
         Preprocessor Object: SF_DNP3  Version 1.1  <Build 1>
         Preprocessor Object: SF_SMTP  Version 1.1  <Build 9>
         Preprocessor Object: SF_SIP  Version 1.1  <Build 1>
         Preprocessor Object: SF_DCERPC2  Version 1.0  <Build 3>
         Preprocessor Object: SF_SSLPP  Version 1.1  <Build 4>
         Preprocessor Object: SF_IMAP  Version 1.0  <Build 1>
         Preprocessor Object: SF_GTP  Version 1.1  <Build 1>
         Preprocessor Object: SF_SSH  Version 1.1  <Build 3>
         Preprocessor Object: SF_FTPTELNET  Version 1.2  <Build 13>
         Preprocessor Object: SF_DNS  Version 1.1  <Build 4>

Snort successfully validated the configuration!
Snort exiting
user@user-VirtualBox:~$ sudo snort -A console -q -u snort -g snort -c /etc/snort
/snort.conf -i enp0s3
05/27-16:47:36.870599  [**] [1:1418:11] SNMP request tcp [**] [Classification: A
ttempted Information Leak] [Priority: 2] {TCP} 192.168.1.17:59103 -> 192.168.1.1
8:161
05/27-16:47:36.870677  [**] [1:1421:11] SNMP AgentX/tcp request [**] [Classifica
tion: Attempted Information Leak] [Priority: 2] {TCP} 192.168.1.17:59103 -> 192.
168.1.18:705
```

```
errruns 0  carrier 0  collisions 0

  mtu 65536
55.0.0.0
 scopeid 0x10<host>
l Loopback)
 (2.4 KiB)
verruns 0  frame 0
 (2.4 KiB)
erruns 0  carrier 0  collisions 0


.org ) at 2018-05-27 13:22 +08



racle VirtualBox virtual NIC)

p) scanned in 0.27 seconds
```

6. Attacking IP address using SPARTA.



user@user-VirtualBox: ~
Kali Linux 2017 (Clean State) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications ▾ Places ▾ Sparta.py ▾
Sun 13:22
SPARTA 1.0.2 (BETA) - untitled - /root/
File Help
Scan Brute
Hosts Services Tools
Services Scripts Information Notes
Click here to add host(s) to scope
Add host(s) to scope
eg: 192.168.1.0/24 10.10.10.10-20 1.2.3.4
Cancel
Add to scope
Log

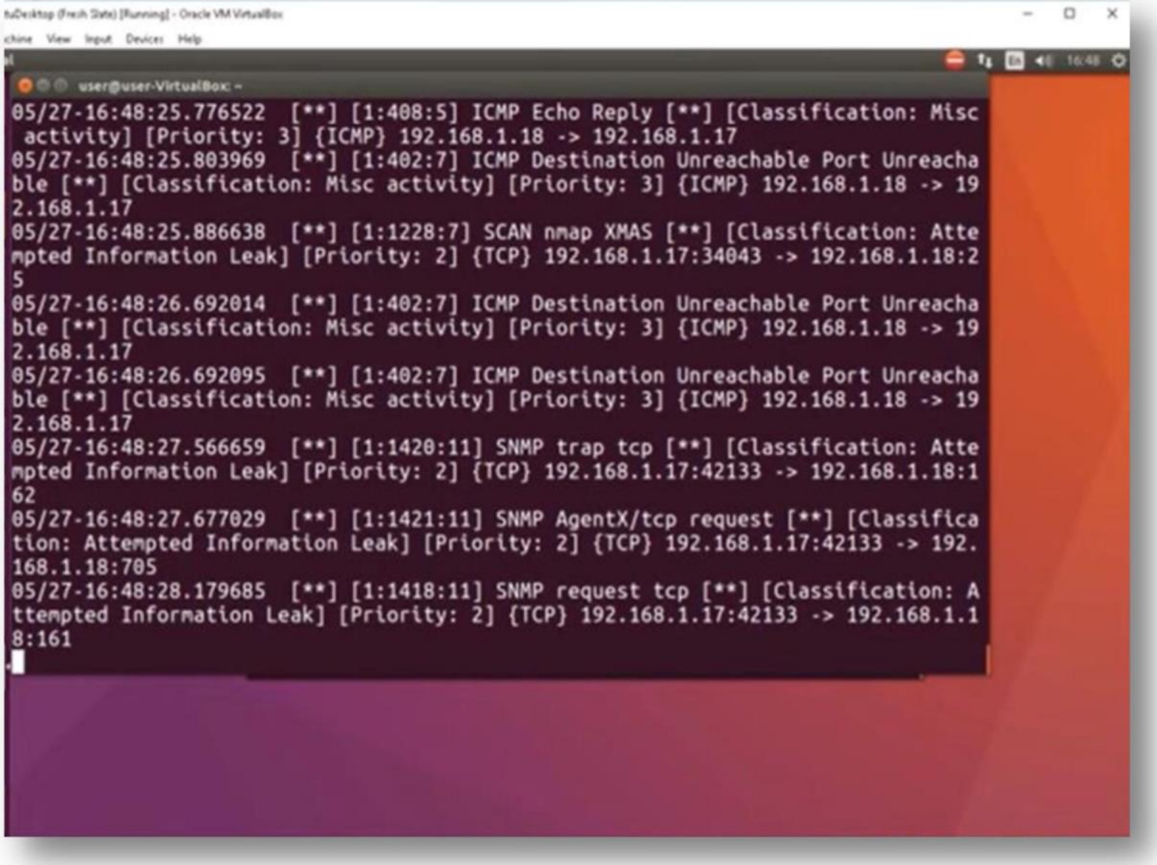
```
         Preprocessor Object: SF_SDF  Version 1.1  <Build
         Preprocessor Object: SF_REPUTATION  Version 1.1
         Preprocessor Object: SF_DNP3  Version 1.1  <Buil
         Preprocessor Object: SF_SMTP  Version 1.1  <Buil
         Preprocessor Object: SF_SIP  Version 1.1  <Build
         Preprocessor Object: SF_DCERPC2  Version 1.0  <B
         Preprocessor Object: SF_SSLPP  Version 1.1  <Bui
         Preprocessor Object: SF_IMAP  Version 1.0  <Buil
         Preprocessor Object: SF_GTP  Version 1.1  <Build
         Preprocessor Object: SF_SSH  Version 1.1  <Build
         Preprocessor Object: SF_FTPTELNET  Version 1.2  -
         Preprocessor Object: SF_DNS  Version 1.1  <Build

Snort successfully validated the configuration!
Snort exiting
user@user-VirtualBox:~$ sudo snort -A console -q -u snort -
/snort.conf -i enp0s3
05/27-16:47:36.870599  [**] [1:1418:11] SNMP request tcp [*
ttempted Information Leak] [Priority: 2] {TCP} 192.168.1.17
8:161
05/27-16:47:36.870677  [**] [1:1421:11] SNMP AgentX/tcp requ
tion: Attempted Information Leak] [Priority: 2] {TCP} 192.16
168.1.18:705
```

IP Range: 192.168.1.18

☑ Run nmap host discovery

☑ Run staged nmap scan

7. Snort detecting SPARTA attack.



tuDesktop (Fresh State) [Running] - Oracle VM VirtualBox
chine View Input Devices Help
16:48
user@user-VirtualBox: ~

```
05/27-16:48:25.776522  [**] [1:408:5] ICMP Echo Reply [**] [Classification: Misc
 activity] [Priority: 3] {ICMP} 192.168.1.18 -> 192.168.1.17
05/27-16:48:25.803969  [**] [1:402:7] ICMP Destination Unreachable Port Unreacha
ble [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.1.18 -> 19
2.168.1.17
05/27-16:48:25.886638  [**] [1:1228:7] SCAN nmap XMAS [**] [Classification: Atte
mpted Information Leak] [Priority: 2] {TCP} 192.168.1.17:34043 -> 192.168.1.18:2
5
05/27-16:48:26.692014  [**] [1:402:7] ICMP Destination Unreachable Port Unreacha
ble [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.1.18 -> 19
2.168.1.17
05/27-16:48:26.692095  [**] [1:402:7] ICMP Destination Unreachable Port Unreacha
ble [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.1.18 -> 19
2.168.1.17
05/27-16:48:27.566659  [**] [1:1420:11] SNMP trap tcp [**] [Classification: Atte
mpted Information Leak] [Priority: 2] {TCP} 192.168.1.17:42133 -> 192.168.1.18:1
62
05/27-16:48:27.677029  [**] [1:1421:11] SNMP AgentX/tcp request [**] [Classifica
tion: Attempted Information Leak] [Priority: 2] {TCP} 192.168.1.17:42133 -> 192.
168.1.18:705
05/27-16:48:28.179685  [**] [1:1418:11] SNMP request tcp [**] [Classification: A
ttempted Information Leak] [Priority: 2] {TCP} 192.168.1.17:42133 -> 192.168.1.1
8:161
```