ASSIGNMENT 11

AIM: Installing snort, configuring it in Intrusion Detection mode and writing rules for detecting pinging activity.

LO MAPPED: LO6

THEORY:

Steps to Install snort and configure it in Intrusion Detection Mode.

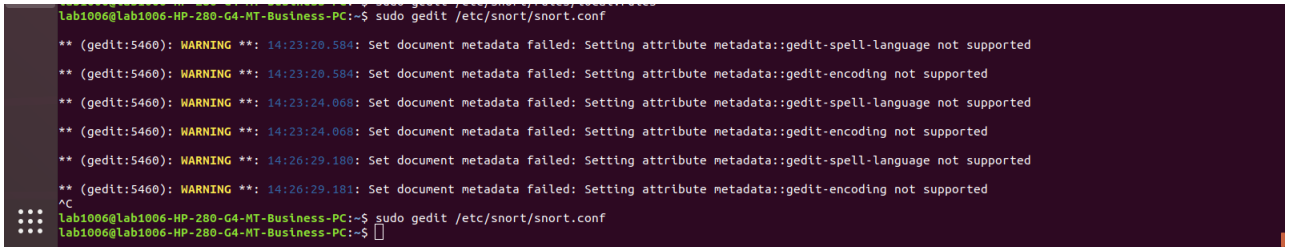
1. Check the name of the interface using command ifconfig.

```
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ ifconfig
enp3s0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.0.102  netmask 255.255.255.0  broadcast 192.168.0.255
        inet6 fe80::6099:62b5:a1f0:fb9  prefixlen 64  scopeid 0x20<link>
        ether 04:0e:3c:1a:64:38  txqueuelen 1000  (Ethernet)
        RX packets 117244  bytes 172441932 (172.4 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 22105  bytes 1752032 (1.7 MB)
        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 1000  (Local Loopback)
        RX packets 2965  bytes 250940 (250.9 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 2965  bytes 250940 (250.9 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

2. Install snort in ubuntu machine using command *sudo apt-get install snort*

```
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ sudo snort -T -c /etc/snort/snort.conf -i enp3s0
[sudo] password for lab1006:
Running in Test mode

        --== Initializing Snort ==--
Initializing Output Plugins!
Initializing Preprocessors!
Initializing Plug-ins!
Parsing Rules file "/etc/snort/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 800
0 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 '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 2381 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 555
55 ]
PortVar 'GTP_PORTS' defined :  [ 2123 2152 3386 ]
Detection:
   Search-Method = AC-Full-Q
    Split Any/Any group = enabled
    Search-Method-Optimizations = enabled
    Maximum pattern length = 20
Tagged Packet Limit: 256
```

3. While installing the snort, name of the interface will be asked on which snort is supposed to listen. Enter the interface name observed in step 1.
4. Run the command *sudo gedit /etc/snort/snort.conf* . This opens snort configuration file.



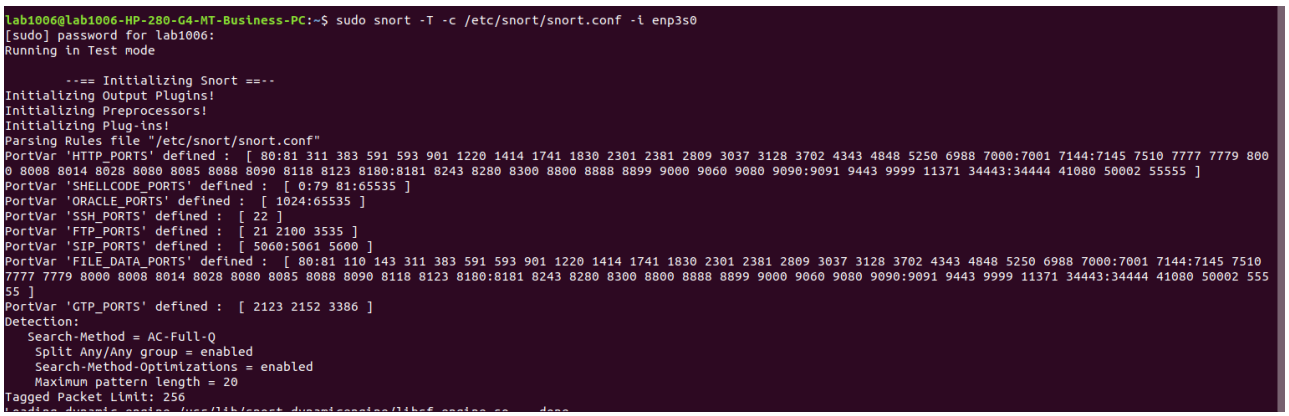
5. Make following changes to configuration file.
   a. ipvar HOME_NET **192.168.44.0/24 (in section 1)**
6. Open new terminal. Open ftp.rule file in it by typing the command *sudo gedit /etc/snort/rules/ftp.rules (optional)*
7. Open new terminal and type the command *sudo snort -T -c /etc/snort/snort.conf -i* ***ens33*** to validate that all rules are there.

   We use the

   -T flag to test the configuration file,

   -c flag to tell Snort which configuration file to use, and

   -i to specify the interface that Snort will listen on.



8. Type the command *sudo snort -A console -q -u snort -g snort -c /etc/snort/snort.conf -i ens33* (to start snort in NIDS mode)

   We use the

   -A console
   The ‘console’ option prints fast mode alerts to stdout

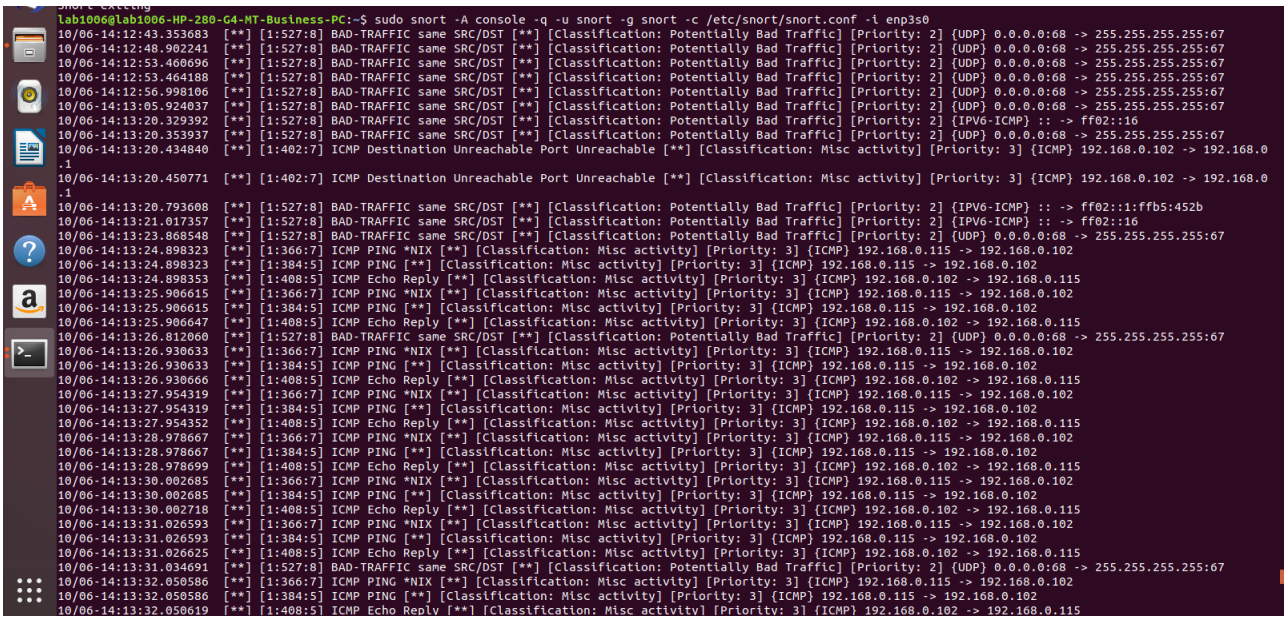
-q Quiet mode. Don't show banner and status report.

-u snort Run Snort as the following user after startup

-g snort Run Snort as the following group after startup

-c /etc/snort/snort.conf The path to our snort.conf file

-i ens33



he interface to listen on (change to your interface if different)

9. Now go to kali linux machine.
10. Type command *nmap 192.168.44.128* on it to start port scanning of ubuntu machine and observe the output in terminal where snort is started in detection environment.

    When you execute this command, you will not initially see any output. Snort is running, and is processing all packets that arrive on eth0 (or whichever interface you specified with the -i flag). Snort compares each packet to the rules it has loaded (in this case our single ICMP Ping rule), and will then print an alert to the console when a packet matches our rule.
11. Then try pinging ubuntu machine by typing the command *ping 192.168.44.128* and observe the output in terminal where snort is started in detection mode.

Conclusion: In this assignment we installed snort, configured it in Intrusion Detection mode and wrote rules for detecting pinging activity.