AMAN SINGH

128, T23

LAB ASSIGNMENT No. 11

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

Lab Outcome Attained: LO6

Theory:

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

1. Check the name of the interface using command ifconfig.
2. Install snort in ubuntu machine using command *sudo apt-get install snort*
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 **192.168.0.0/24 (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* ***enp3s0*** 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 enp3s0* (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 enp3s0 The interface to listen on (change to your interface if different)

9. Now go to kali linux machine.
10. Type command *nmap 192.168.0.107* 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*

192.168.0.107 and observe the output in terminal where snort is started in detection mode.

---

12. Adding rule for detecting ping activity performed by another machine:

---

a. In ubuntu machine, type the following command to create a file called local.rules : ***sudo gedit /etc/snort/rules/local.rules***
b. Write the following rule in it: ***alert icmp any any -> $HOME_NET any (msg:"ICMP test detected"; GID:1; sid:10000001; rev:001; classtype:icmp-event;)***
c. Save the local.rules file.
d. Comment the following lines in configuration file (snort.conf) of snort: icmp.rules and icmp-info.rules
e. Add the local.rules file in section 7 of configuration file of snort by writing: ***include $RULE_PATH local.rules***
f. Validate the changes made in snort.conf file by writing the command in terminal: ***sudo snort -T -c /etc/snort/snort.conf -i enp3s0***
g. Set the snort in Intrusion Detection Mode by typing the command: ***sudo snort -A console -q -u snort -g snort -c /etc/snort/snort.conf i enp3s0***
h. Now from kali machine ping the ubuntu machine and see the alert generated.

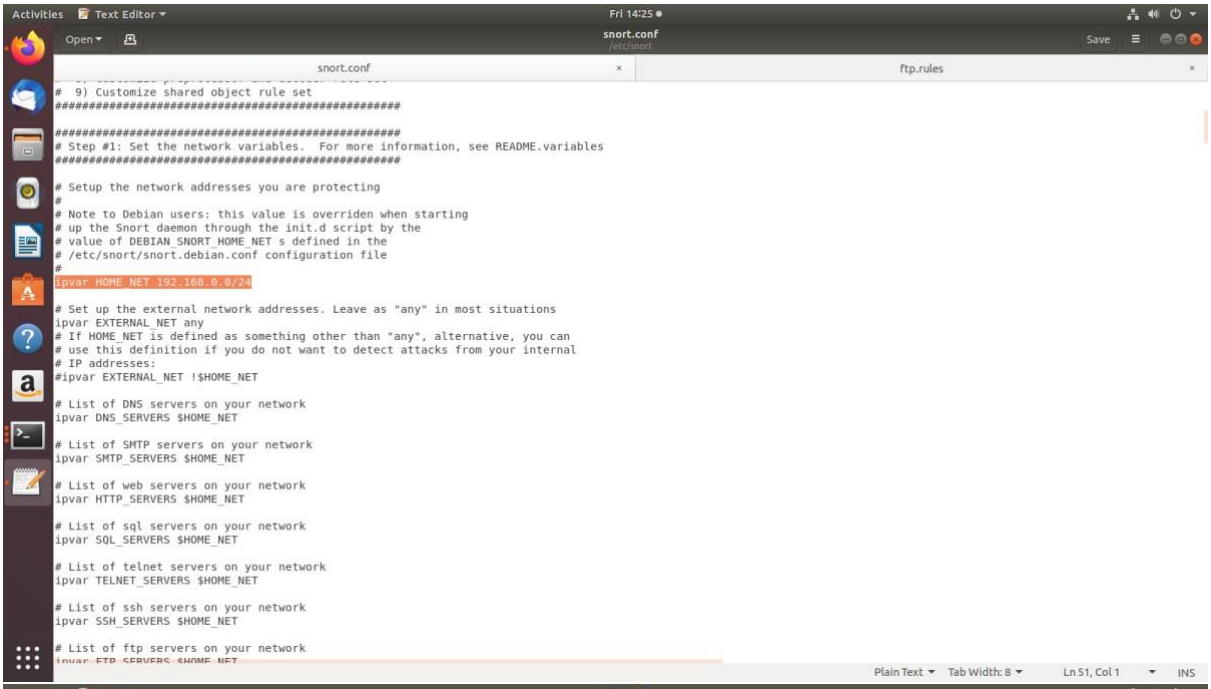
i. Observe the difference between the alerts generated when icmp.rules and icmp-info.rules are used and when local.rules is used to detect the ping activity.

Output:

AMAN SINGH

128,

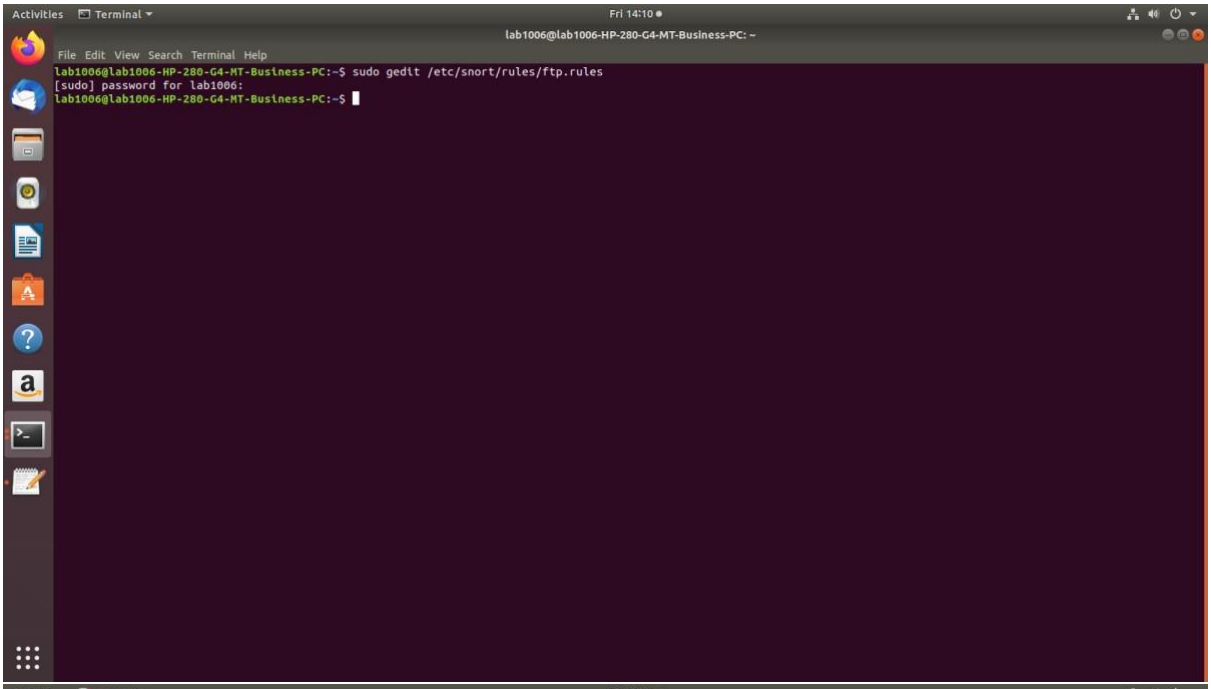
T23

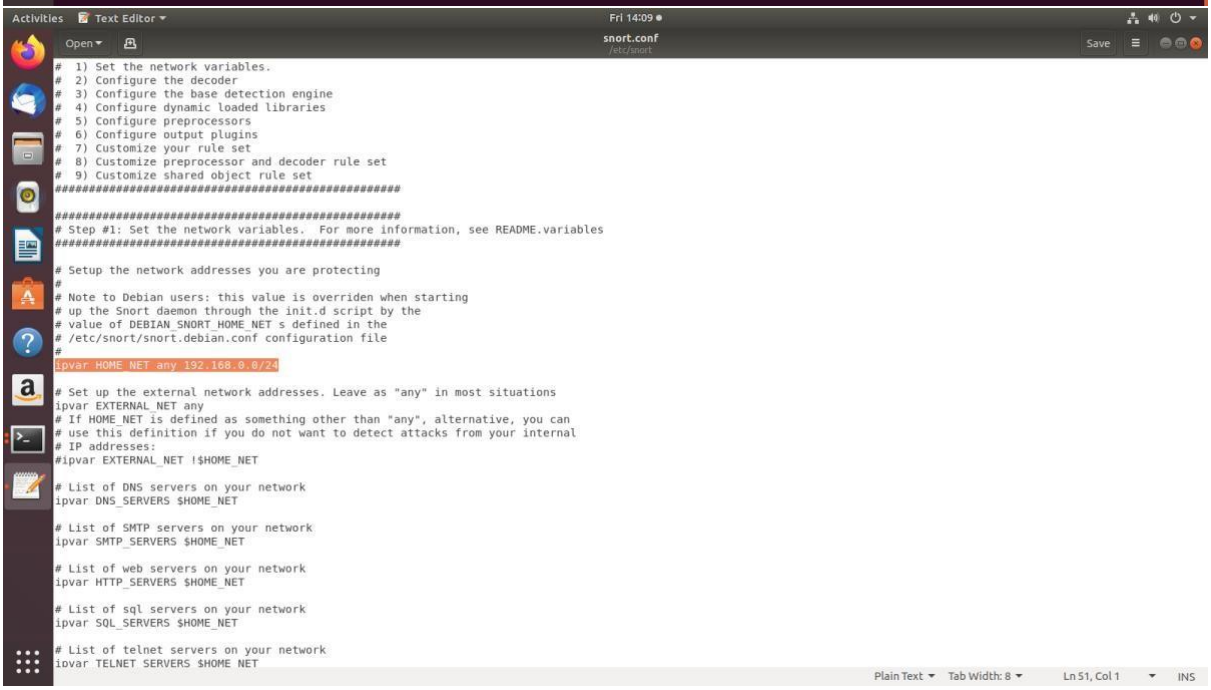


AMAN SINGH

128,

T23

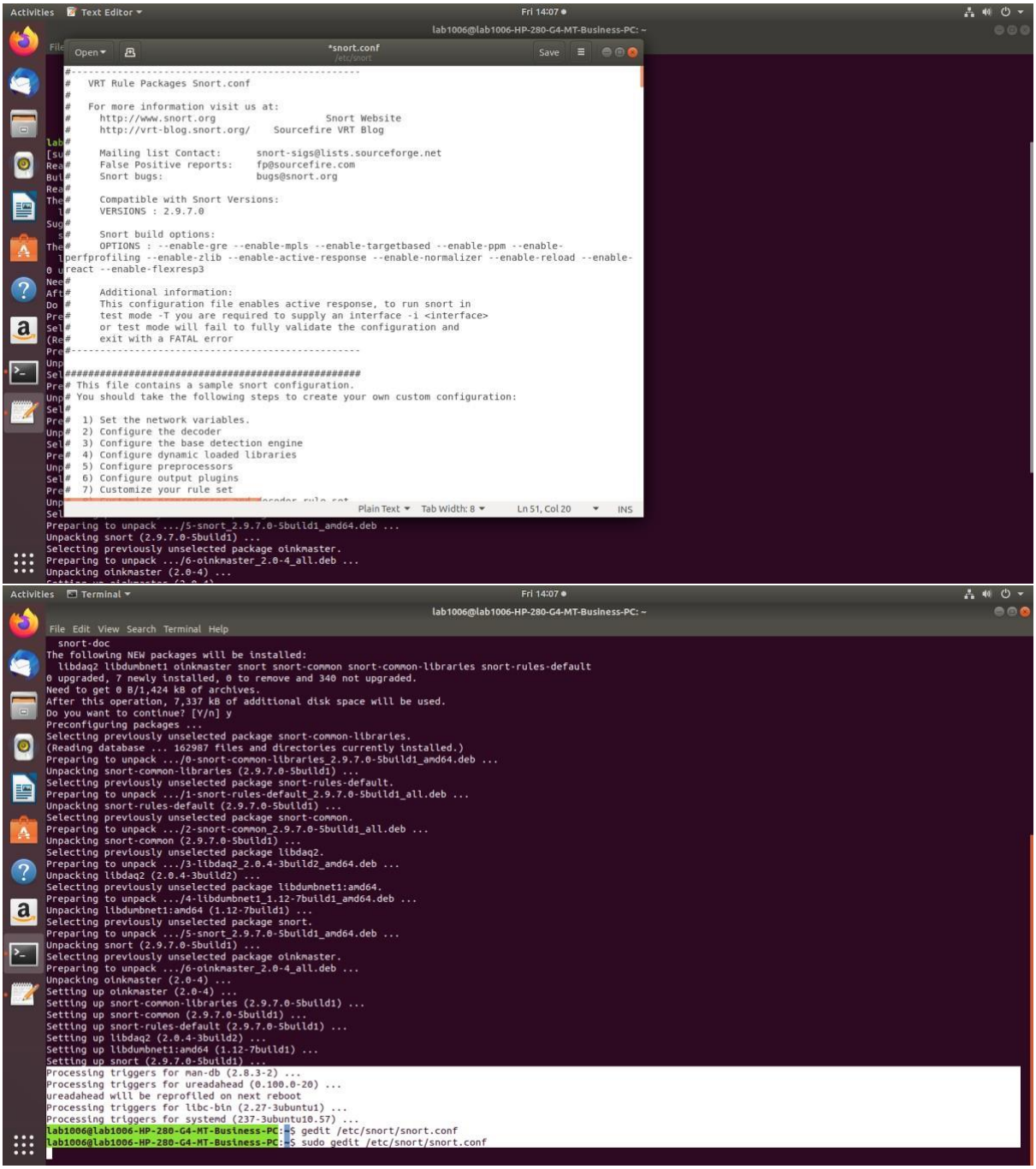




AMAN SINGH

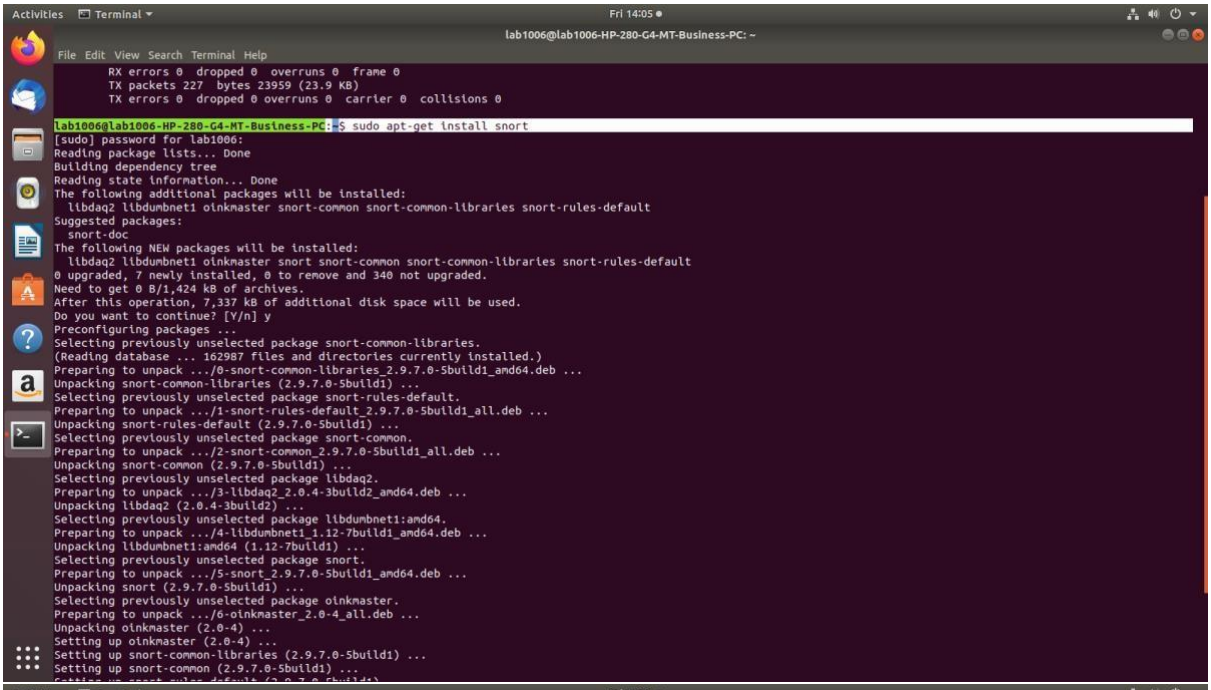
128,

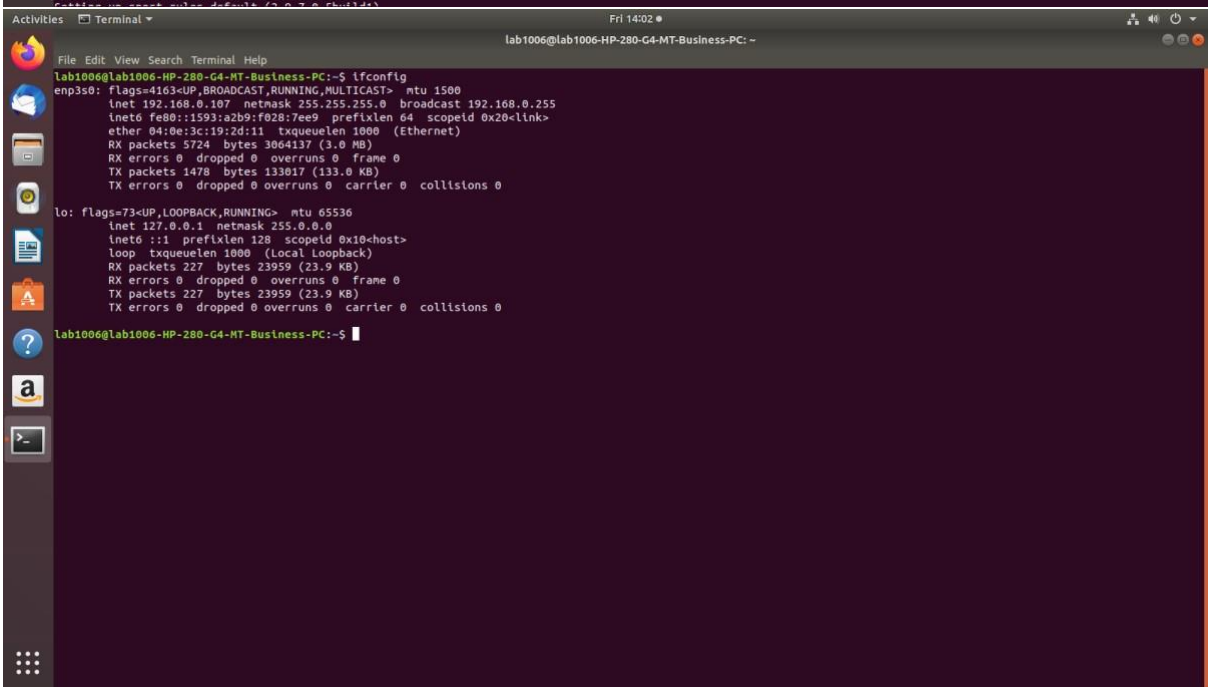
T23



AMAN SINGH

128, T23

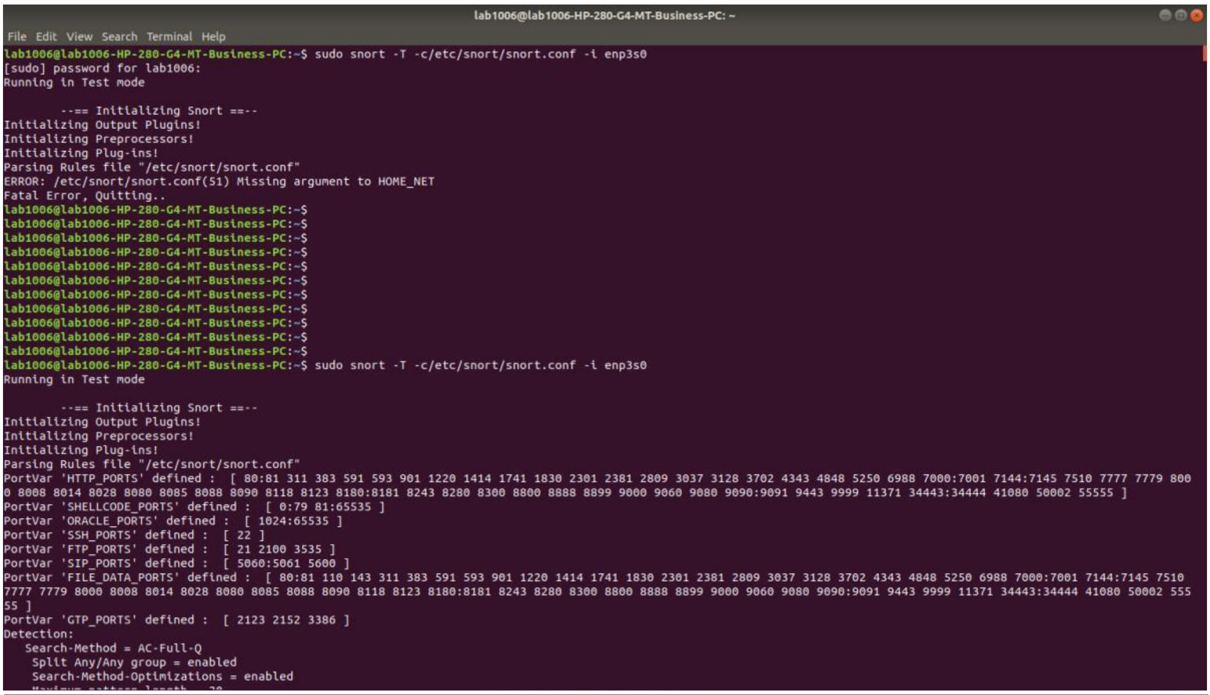




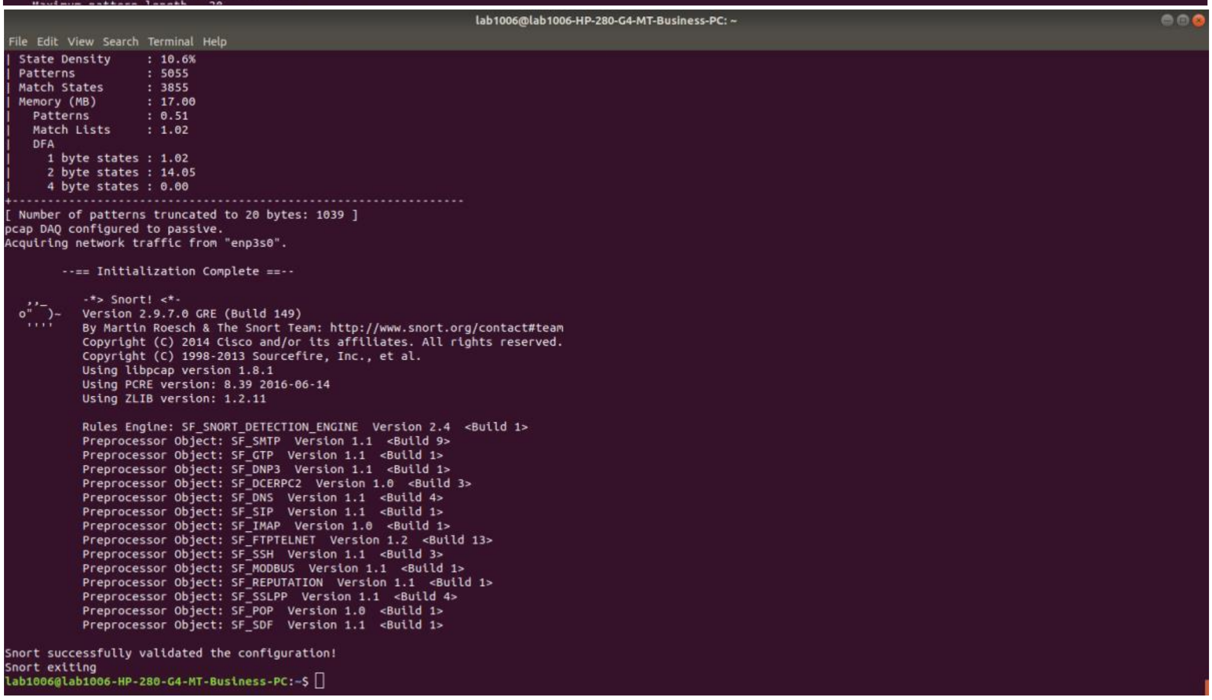
AMAN SINGH

128,

T23



```
lab1006@lab1006-HP-280-G4-MT-Business-PC: ~
File Edit View Search Terminal Help
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"
ERROR: /etc/snort/snort.conf(51) Missing argument to HOME_NET
Fatal Error, Quitting..
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ sudo snort -T -c/etc/snort/snort.conf -i enp3s0
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
```

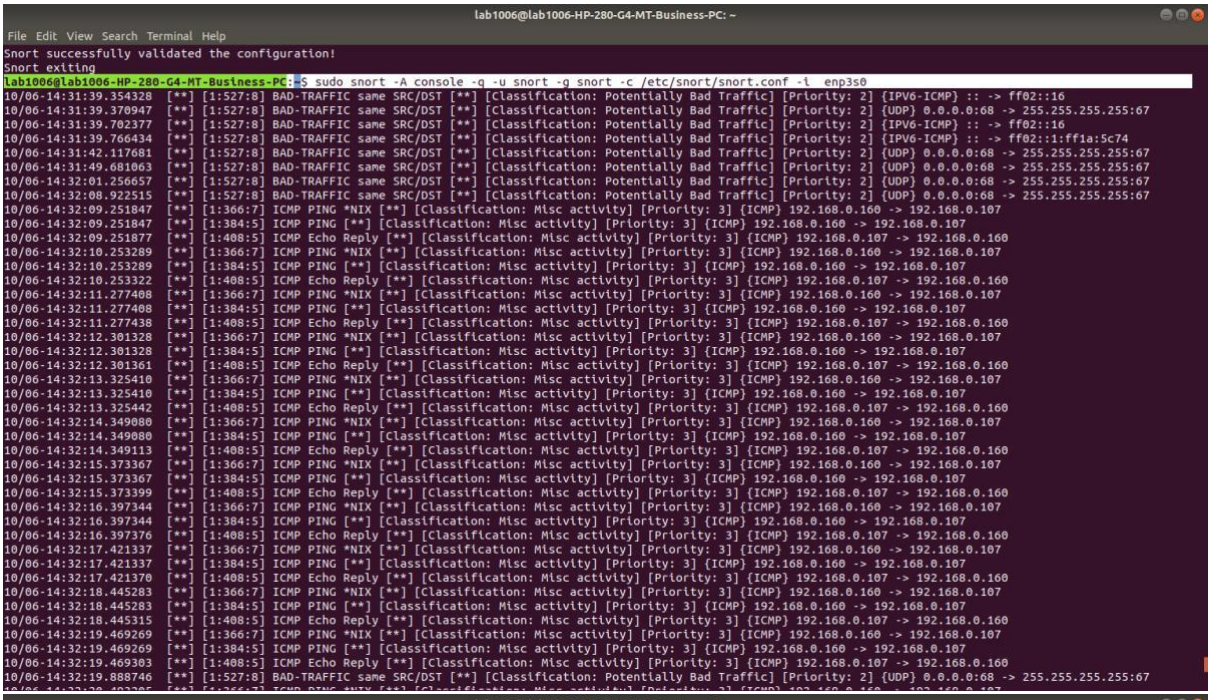


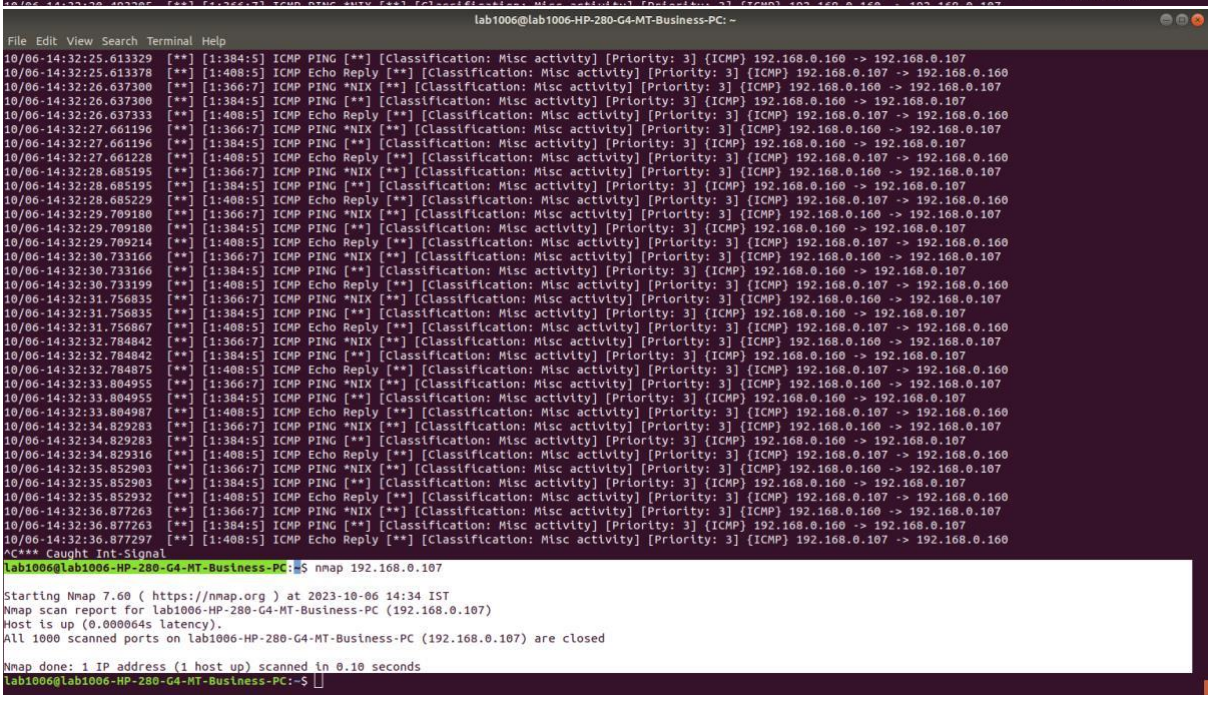
```
lab1006@lab1006-HP-280-G4-MT-Business-PC: ~
File Edit View Search Terminal Help
| State Density      : 10.6%
| Patterns           : 5055
| Match States       : 3855
| Memory (MB)        : 17.00
|   Patterns         : 0.51
|   Match Lists      : 1.02
|   DFA
|     1 byte states : 1.02
|     2 byte states : 14.05
|     4 byte states : 0.00
+----------------------------------------------------------------
[ Number of patterns truncated to 20 bytes: 1039 ]
pcap DAQ configured to passive.
Acquiring network traffic from "enp3s0".

        --== Initialization Complete ==--

   ,,_     -*> 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_SMTP  Version 1.1  <Build 9>
           Preprocessor Object: SF_GTP  Version 1.1  <Build 1>
           Preprocessor Object: SF_DNP3  Version 1.1  <Build 1>
           Preprocessor Object: SF_DCERPC2  Version 1.0  <Build 3>
           Preprocessor Object: SF_DNS  Version 1.1  <Build 4>
           Preprocessor Object: SF_SIP  Version 1.1  <Build 1>
           Preprocessor Object: SF_IMAP  Version 1.0  <Build 1>
           Preprocessor Object: SF_FTPTELNET  Version 1.2  <Build 13>
           Preprocessor Object: SF_SSH  Version 1.1  <Build 3>
           Preprocessor Object: SF_MODBUS  Version 1.1  <Build 1>
           Preprocessor Object: SF_REPUTATION  Version 1.1  <Build 1>
           Preprocessor Object: SF_SSLPP  Version 1.1  <Build 4>
           Preprocessor Object: SF_POP  Version 1.0  <Build 1>
           Preprocessor Object: SF_SDF  Version 1.1  <Build 1>

Snort successfully validated the configuration!
Snort exiting
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$
```

AMAN SINGH

128,

T23

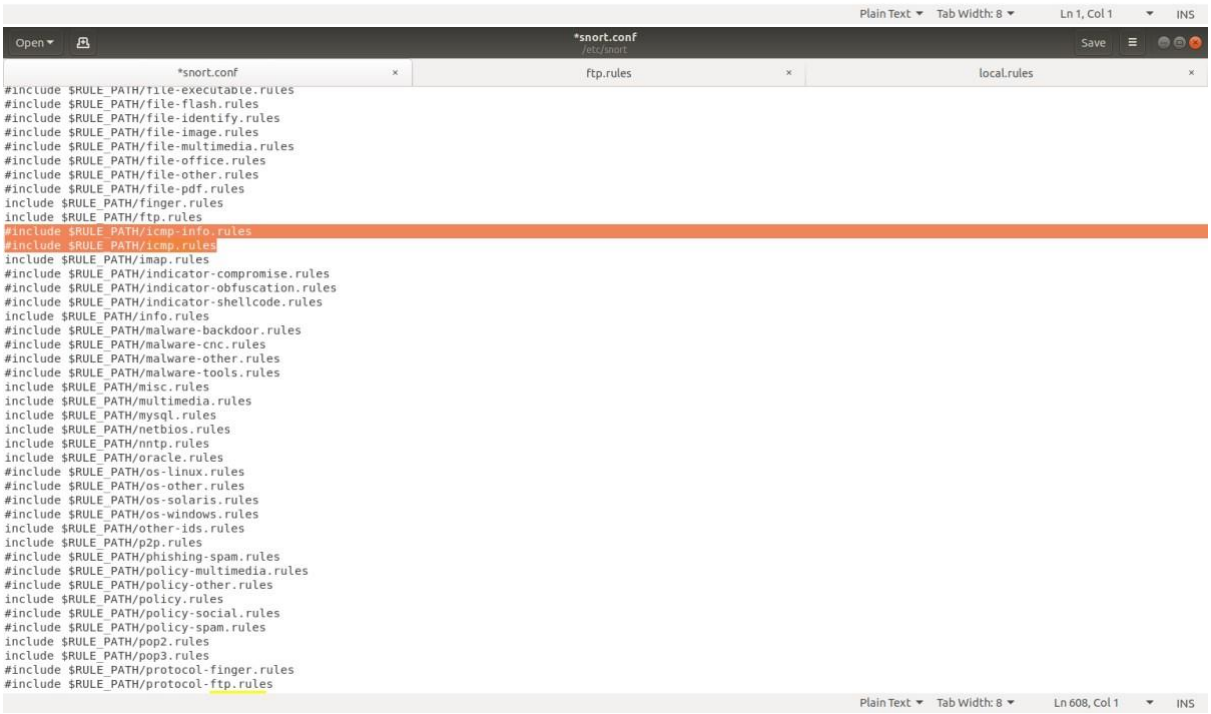




AMAN SINGH

128,

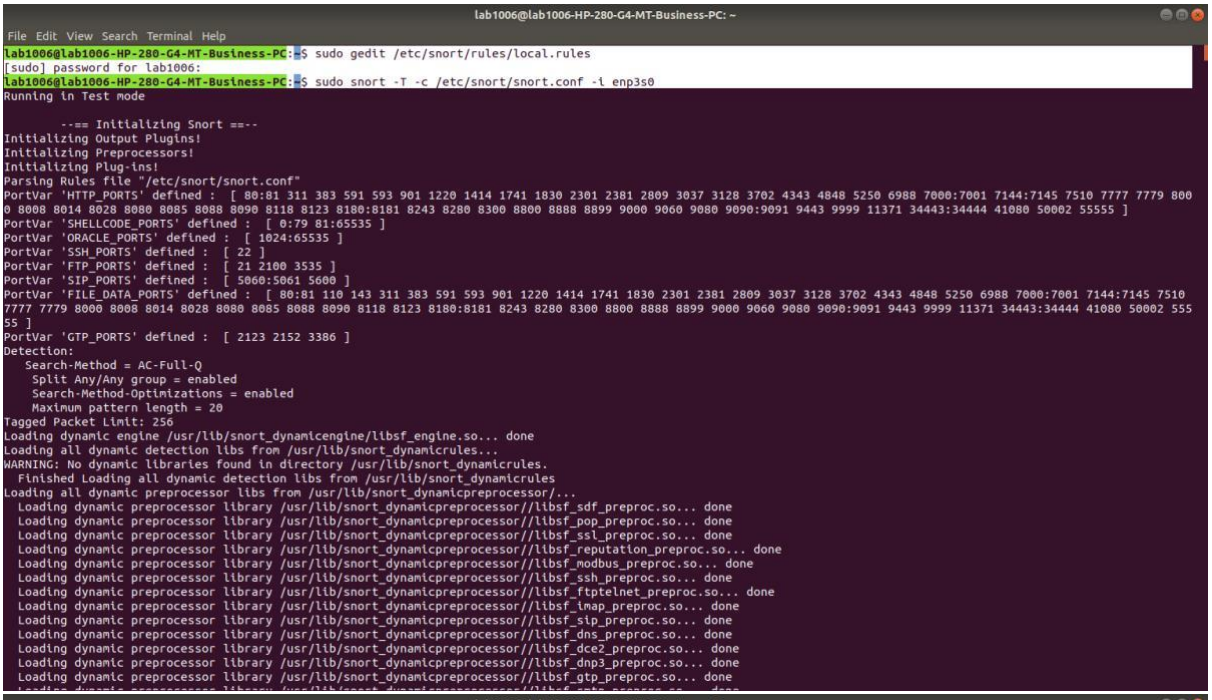
T23

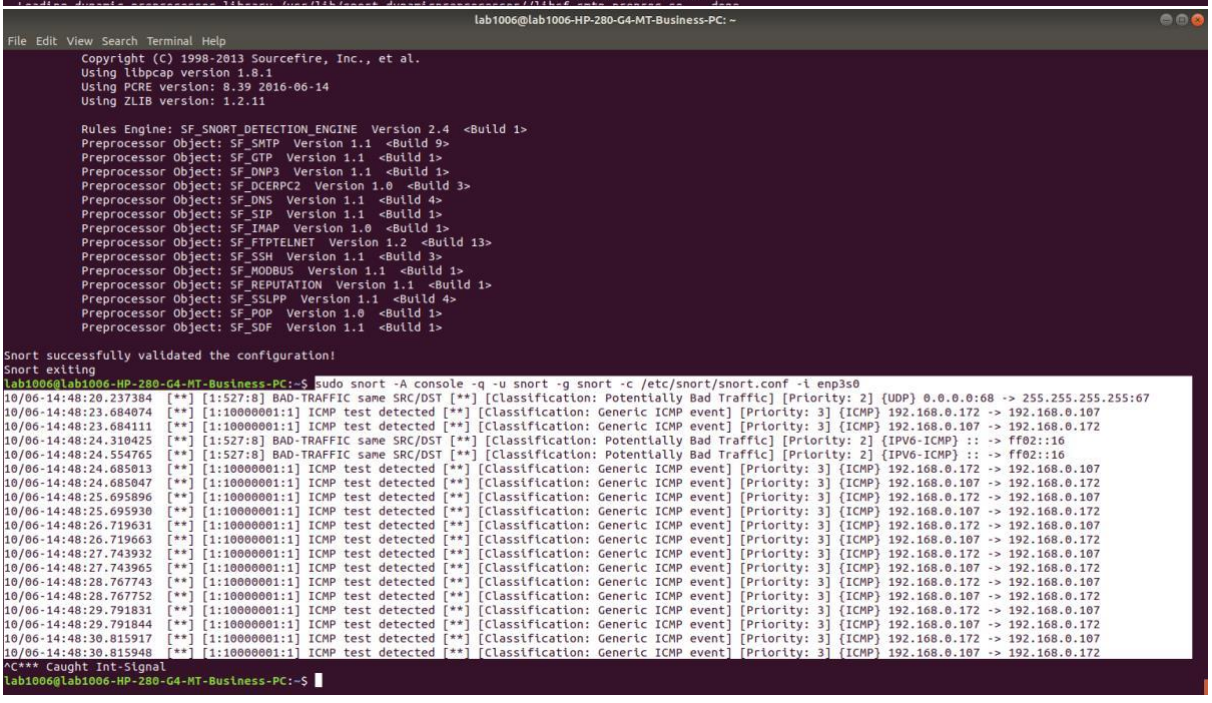


AMAN SINGH

128,

T23





Conclusion: In conclusion, this assignment involved the installation and configuration of Snort, a powerful Intrusion Detection System. By following the step-by-step instructions, we successfully installed Snort, edited its configuration

file, and executed rules to detect ICMP activities. This hands-on experience enhanced our understanding of network security and IDS functionality.