

Name: Rutikesh Sawant

Batch: B2

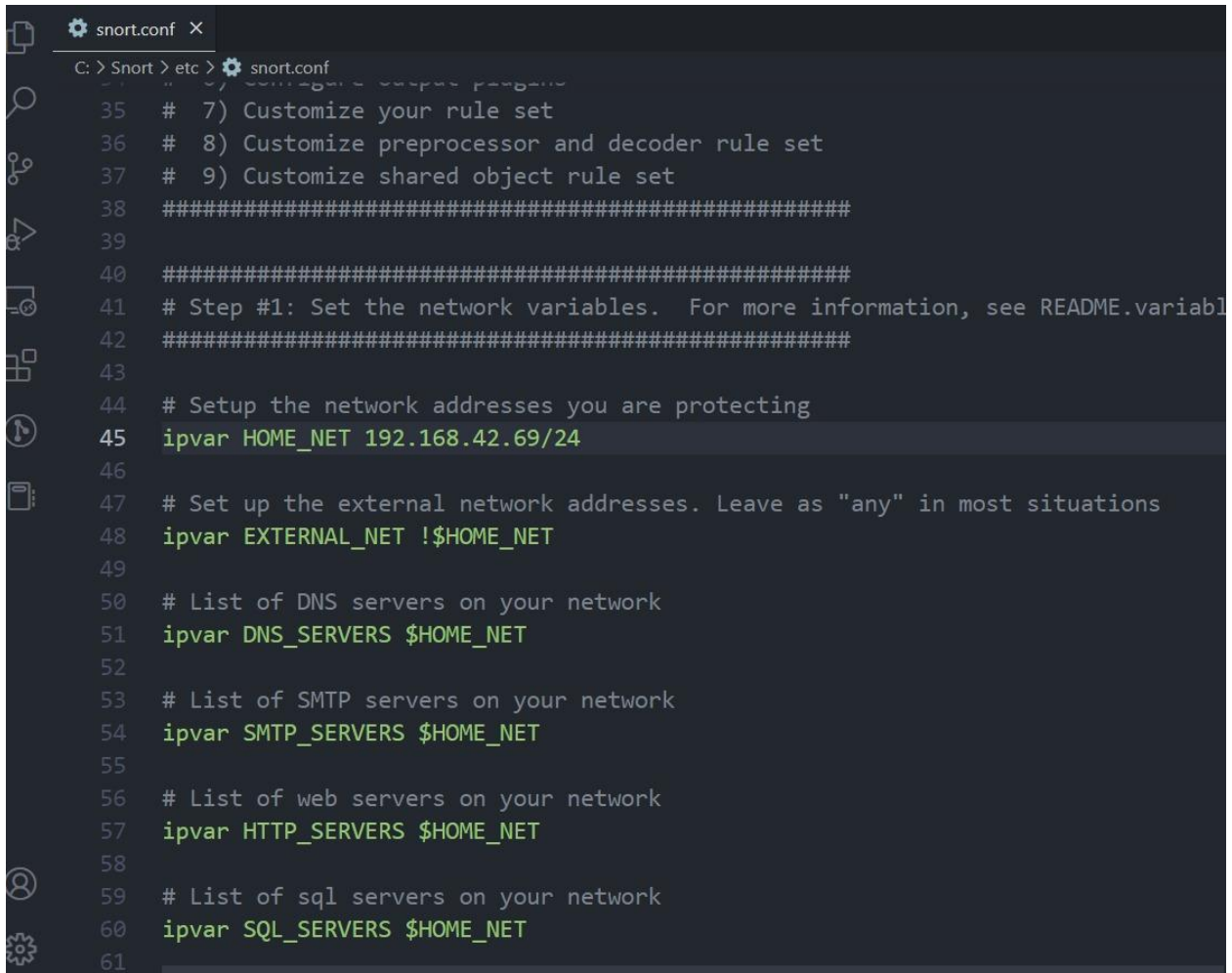
Subject: CNS Lab

PRN: 2019BTECS00034

## Assignment 16

Aim: Analysis of intrusions using snort software.

Output:



```
35 # 7) Customize your rule set
36 # 8) Customize preprocessor and decoder rule set
37 # 9) Customize shared object rule set
38 #####
39
40 #####
41 # Step #1: Set the network variables. For more information, see README.variab1
42 #####
43
44 # Setup the network addresses you are protecting
45 ipvar HOME_NET 192.168.42.69/24
46
47 # Set up the external network addresses. Leave as "any" in most situations
48 ipvar EXTERNAL_NET !$HOME_NET
49
50 # List of DNS servers on your network
51 ipvar DNS_SERVERS $HOME_NET
52
53 # List of SMTP servers on your network
54 ipvar SMTP_SERVERS $HOME_NET
55
56 # List of web servers on your network
57 ipvar HTTP_SERVERS $HOME_NET
58
59 # List of sql servers on your network
60 ipvar SQL_SERVERS $HOME_NET
61
```

[illegible]



```

| Patterns      : 10248
| Match States  : 10581
| Memory (MB)   : 122.72
|   Patterns    : 1.19
|   Match Lists : 2.70
|   DFA
|     1 byte states : 1.13
|     2 byte states : 49.26
|     4 byte states : 68.07
+-----+
[ Number of patterns truncated to 20 bytes: 575 ]

MaxRss at the end of detection rules:-57990272
pcap DAQ configured to passive.
The DAQ version does not support reload.
Acquiring network traffic from "-1".

--== Initialization Complete ==--

,,_  -*> Snort! <*-
o" )~ Version 2.9.20-WIN64 GRE (Build 82)
'''  By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
      Copyright (C) 2014-2022 Cisco and/or its affiliates. All rights reserved.
      Copyright (C) 1998-2013 Sourcefire, Inc., et al.
      Using PCRE version: 8.10 2010-06-25
      Using ZLIB version: 1.2.11

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

Total snort Fixed Memory Cost - MaxRss:-1029885280
Snort successfully validated the configuration!
Snort exiting

c:\Snort\bin>

```