Name: Rutikesh Sawant

Batch: B2

Subject: CNS Lab

PRN: 2019BTECS00034

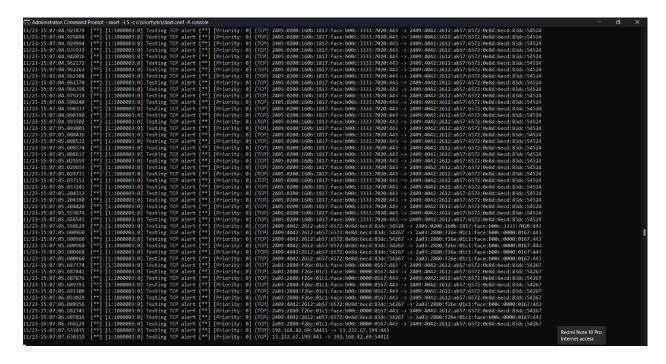
Assignment 16

Aim: Analysis of intrusions using snort software.

Output:

```
snort.conf X
   C: > Snort > etc > ✿ snort.conf
        # 9) Customize shared object rule set
         S
         # Step #1: Set the network variables. For more information, see README.variables
         # Setup the network addresses you are protecting
\bigcirc
        ipvar HOME_NET 192.168.42.69/24
         # Set up the external network addresses. Leave as "any" in most situations
         ipvar EXTERNAL_NET !$HOME_NET
        ipvar DNS SERVERS $HOME NET
        ipvar SMTP SERVERS $HOME NET
        ipvar HTTP_SERVERS $HOME_NET
     60 ipvar SQL_SERVERS $HOME_NET
```

Administrator: Command Prompt - snort -i 5 -c c\snort\etc\snort\conf. a console									
11/23-15:06:30.995190	[**]	[1:1000002:0]	Testing	UDP ale	rt [**]	[Priority:	01	{UDP}	2404:6800:4009:081b:0000:0000:0000:200e:443 -> 2409:4042:2612:ab57:6572:0e8d:6ecd:83dc:60807
11/23-15:06:32.004068		[1:1000003:0]							2404:6800:4009:0801:0000:0000:0000:200a:443 -> 2409:4042:2612:ab57:6572:0e8d:6ecd:83dc:54450
		[1:1000003:0]							2409:4042;2612;ab57:6572;0e8d:6ecd:83dc:54450 -> 2404:6800:4009:0801:0000:0000:0000:200a:443
		[1:1000003:0]							2404:6800:4009:0801:0000:0000:0000:200a:443 -> 2409:4042:2612:ab57:6572:0e8d:6ecd:83dc:54450
11/23-15:06:32.004286		[1:1000003:0]							2409:4042:2612:ab57:6572:0e8d:6ecd:83dc:54450 -> 2404:6800:4009:0801:0000:0000:0000:200a:443
11/23-15:06:32.082069		[1:1000003:0]						{TCP}	2494;6899;4909;0801;0000;0000;0000;200a;4443 -> 2409;4042;2612;ab57;6572;0e8d;6ecd;83dc;54449
		[1:1000003:0]							2409:4042:2612:ab57:6572:0e8d:6ecd:83dc:54449 -> 2404:6800:4009:0801:0000:0000:0000:200a:443
11/23-15:06:32.082229		[1:1000003:0]						{TCP}	2494;6890;4909;9801;9900;9900;9900;290a;4443 -> 2409;4942;2612;ab57;6577;9e8d;6ecd;83dc;54449
		[1:1000003:0]							2409:4042:2612;ab57;6572:0e8d:6ecd:83dc:54449 -> 2404:6800:4009:0801:0000:0000:0000:200a:443
11/23-15:06:32.732713		[1:1000002:0]							
		[1:1000002:0]							2404:6800:4009:0800:0000:0000:0000:200e:443 -> 2409:4042:2612:ab57:6572:0e8d:6ecd:83dc:65023
11/23-15:06:32.826292		[1:1000002:0]							2409:4042;2612;ab57:6572;0e8d:6ecd:83dc:65023 -> 2404:6800:4009:0800:0000:0000:0000:200e:443
11/23-15:06:33.063513		[1:1000002:0]							2404:6800:4009:0800:0000:0000:0000:200e:443 -> 2409:4042:2612:ab57:6572:0e8d:6ecd:83dc:65023
11/23-15:06:33.064133		[1:1000002:0]							2409:4042:2612:ab57:6572:0e8d:6ecd:83dc:65023 -> 2404:6800:4009:0800:0000:0000:0000:200e:443
		[1:1000002:0]							2404;6800;4009;0800;0000;0000;0000;200e;443 -> 2409;4042;2612;ab57;6572;0e8d;6ecd;83dc;65023
11/23-15:06:33.069636		[1:1000002:0]							2404:6800:4009:0800:0000:0000:0000:200e:443 -> 2409:4042:2612:ab57:6572:0e8d:6ecd:83dc:65023
11/23-15:06:33.090162									2409:4042:2612:ab57:6572:0e8d:6ecd:83dc:65023 -> 2404:6800:4009:0800:0000:0000:0000:200e:443
11/23-15:06:33.140995		[1:1000002:0]						{UDP}	2404:6800:4009:0800:0000:0000:0000:200e:443 -> 2409:4042:2612:ab57:6572:0e8d:6ecd:83dc:65023
11/23-15:06:33.166631		[1:1000002:0] [1:1000002:0]							
11/23-15:06:33.167093		[1:1000002:0]							2404:6800:4009:0800:0000:0000:0000:200e:443 -> 2409:4042:2612:ab57:6572:0e8d:6ecd:83dc:65023 2409:4042:2612:ab57:6572:0e8d:6ecd:83dc:65023 -> 2404:6800:4009:0800:0000:0000:0000:200e:443
11/23-15:06:35.086830		[1:1000003:0]							2409:4042:2612:ab57:6572:0e8d:6ecd:83dc:54345 -> 2606:2cc0:0002:0000:0000:0000:0000:0595:443
11/23-15:06:35.080830								{TCP}	2409:4042:2012:8057:0572:068d:06Cd:83dC:54345 -> 2409:4042:2612:8057:6572:068d:0000:0000:0595:443
11/23-15:06:35.338425		[1:1000003:0]							2409:4042:2612:ab57:6572:0e8d:6ecd:83dc:50517 -> 2404:6800:4009:0823:0000:0000:0000:200a:443
11/23-15:06:35.463908		[1:1000002:0]						{UDP}	2404:6800:4009:0823:0000:0000:0000:200a:443 -> 2404:6800:4009:0823:0000:0000:200a:443
		[1:1000002:0]							
11/23-15:06:37.313631 11/23-15:06:37.399554		[1:1000003:0] [1:1000003:0]							192.168.42.69:54502 -> 108.159.32.8:443
11/23-15:06:37.399554									108.159.32.8:443 -> 192.168.42.69:54502
11/23-15:06:40.553251		[1:1000002:0] [1:1000002:0]							2404:6800:4009:0823:0000:0000:0000:200a:443 -> 2409:4042:2612:ab57:6572:0e8d:6ecd:83dc:50517 2409:4042:2612:ab57:6572:0e8d:6ecd:83dc:50517 -> 2404:6800:4009:0823:0000:0000:0000:200a:443
11/23-15:06:40.533251		[1:1000002:0]							2409:4042:2612:ab57:6572:0e8d:0ecd:83dc:50517 -> 2404:6800:4009:0814:0000:0000:0000:2003:443
11/23-15:06:40.732839 11/23-15:06:40.733140		[1:1000002:0]							2409:4042:2612:ab57:6572:0e8d:6ecd:83dc:53771 -> 2404:6800:4009:0814:0000:0000:0000:2003:443 2409:4042:2612:ab57:6572:0e8d:6ecd:83dc:53771 -> 2404:6800:4009:0814:0000:0000:0000:2003:443
11/23-15:06:40.733140		[1:1000002:0]							2404:6800:4009:0814:0000:0000:0000:2003:443 -> 2409:4042:2612:ab57:6572:0e8d:6ecd:83dc:53771
11/23-15:06:40.873451		[1:1000002:0]							
		[1:1000002:0]							2404:6800:4009:0814:0000:0000:0000:2003:443 -> 2409:4042:2612:ab57:6572:0e8d:6ecd:83dc:53771
		[1:1000002:0]							2404:6800:4009:0814:0000:0000:0000:2003:443 -> 2409:4042:2612:ab57:6572:0e8d:6ecd:83dc:53771
		[1:1000002:0]							2404:6800:4009:0814:0000:0000:0000:2003:443 -> 2409:4042:2612:ab57:6572:0e8d:6ecd:83dc:53771
		[1:1000002:0]							2404:6800:4009:0814:0000:0000:0000:2003:443 -> 2409:4042:2612:ab57:6572:0e8d:6ecd:83dc:53771
		[1:1000002:0]							
		[1:1000002:0]							2404:6800:4009:0814:0000:0000:0000:2003:443 -> 2409:4042:2612:ab57:6572:0e8d:6ecd:83dc:53771
11/23-15:06:40.874365		[1:1000002:0]							2409:4042:2612:ab57:6572:0e8d:6ecd:83dc:53771 -> 2404:6800:4009:0814:0000:0000:0000:2003:443
		[1:1000002:0]							2409:4042:2612:ab57:6572:0e8d:6ecd:83dc:53771 -> 2404:6800:4009:0814:0000:0000:0000:0000:3443
11/23-15:06:40.936645		[1:1000002:0]							2404:6800:4009:0814:0000:0000:0000:2003:443 -> 2409:4042:2612:ab57:6572:0e8d:6ecd:83dc:53771
		[1:1000002:0]							2404:6800:4009:0814:0000:0000:0000:0000:2003:443 -> 2409:4042:2612:ab57:6572:0e8d:6ecd:83dc:53771
11/23-15:06:40.936813		[1:1000002:0]							2404:6800:4009:0814:0000:0000:0000:2003:443 -> 2409:4042:2612:ab57:6572:0e8d:6ecd:83dc:53771
11/23-15:06:40.937302		[1:1000002:0]							2409:4042:2612:ab57:6572:0e8d:6ecd:83dc:53771 -> 2404:6800:4009:0814:0000:0000:0000:2003:443
11/23-15:06:40.937458		[1:1000002:0]							2409:4042:2612:ab57:6572:0e8d:6ecd:83dc:53771 -> 2404:6800:4009:0814:0000:0000:0000:2003:443
11/23-15:06:40.999671		[1:1000002:0]							2404:6800:4009:0814:0000:0000:0000:2003:443 -> 2409:4042:2612:ab57:6572:0e8d:6ecd:83dc:53771
11/23-15:06:41.094934		[1:1000003:0]							2409:4042:2612:ab57:6572:0e8d:6ecd:83dc:54313 -> 2404:6800:4003:0c11:0000:0000:0000:000bc:5228
11/23-15:06:41.217788	[**]	[1:1000003:0]	lesting	TCP ale	rt [**]	[Priority:	0]	{TCP}	2404:6800:4003:0c11:0000:0000:0000:00bc:5228 -> 2409:4042:2612:ab57:6572:0e8d:6ecd:83dc:54313



```
Patterns
                   : 10248
 Match States
                   : 10581
                   : 122.72
 Memory (MB)
   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! <*-
          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
:\Snort\bin>
```