ST. FRANCIS INSTITUTE OF TECHNOLOGY
DEPARTMENT OF INFORMATION TECHNOLOGY
SECURITY LAB

Experiment – 10: Study of Intrusion detection system using SNORT

Aim: To study the Intrusion detection system using SNORT.

Objective: After performing the experiment, the students will be able to explore and use the Snort-IDS tool.

Lab objective mapped: L502.6: Students should be able to apply network security basics, analyze different attacks on networks and evaluate the performance of firewalls and security protocols, such as SSL, IPSEC, and PGP, and authentication mechanisms to design secure applications.

Prerequisite: Basic knowledge of network security.

Requirements: Windows OS, SNORT

Pre-Experiment Theory:

Snort is an open-source network intrusion prevention and detection system (IDS/IPS) developed by Sourcefire. Combining the benefits of signature, protocol, and anomaly-based inspection, Snort is the most widely deployed IDS/IPS technology worldwide. With millions of downloads and nearly 400,000 registered users, Snort has become the de facto standard for IPS.

Snort can be configured to run in three modes:

1. **Sniffer mode**: It simply reads the packets of the network and displays them for you in a continuous stream on the console (screen)
2. **Packet Logger mode**: logs the packets to disk.
3. **Network Intrusion Detection System (NIDS) mode**: it performs detection and analysis on network traffic. This is the most complex and configurable mode.

Implementation:

1. Install snort on your system. Refer/download the snort user manual from its official website [1].
2. Test snort IDS using following commands, observe the output of each command. Take screenshots (SS). Write your observations under each SS.

```
     a. Snort –V
C:\Snort\bin>snort -V

   ,,_     -*> 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
```

```
    b. Snort –v
    C:\Snort\bin>snort -v
    Running in packet dump mode

            --== Initializing Snort ==--
    Initializing Output Plugins!
    pcap DAQ configured to passive.
```

```
The DAQ version does not support reload.
Acquiring network traffic from "\Device\NPF_{8412B745-AC0D-40DC-B534-249DEA6A9DC7}".
Decoding Ethernet

        --== 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
```

c. Snort -vd

```
   C:\Snort\bin>snort -vd
   Running in packet dump mode

           --== Initializing Snort ==--
   Initializing Output Plugins!
   pcap DAQ configured to passive.
   The DAQ version does not support reload.
   Acquiring network traffic from "\Device\NPF_{8412B745-AC0D-40DC-B534-249DEA6A9DC7}".
   Decoding Ethernet

           --== 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

   Commencing packet processing (pid=1348)
   *** Caught Int-Signal
   WARNING: No preprocessors configured for policy 0.
   10/16-10:51:39.833978 192.168.5.28:5353 -> 224.0.0.251:5353
   UDP TTL:1 TOS:0x0 ID:62518 IpLen:20 DgmLen:57
   Len: 29
   00 00 00 00 00 01 00 00 00 00 00 00 05 68 74 74  .............htt
   70 73 05 6C 6F 63 61 6C 00 00 01 00 01           ps.local.....
```

d. Snort -W

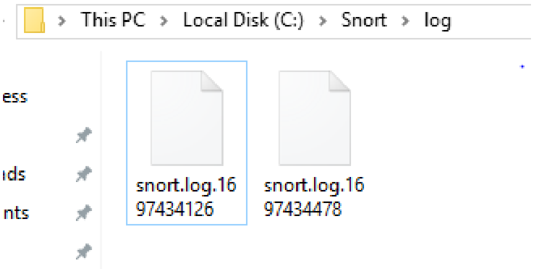
```
   C:\Users\Student>Snort -W
   Snort! <*-
   Version 2.9.20-WIN64 GRE (Build 82)
   By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
```

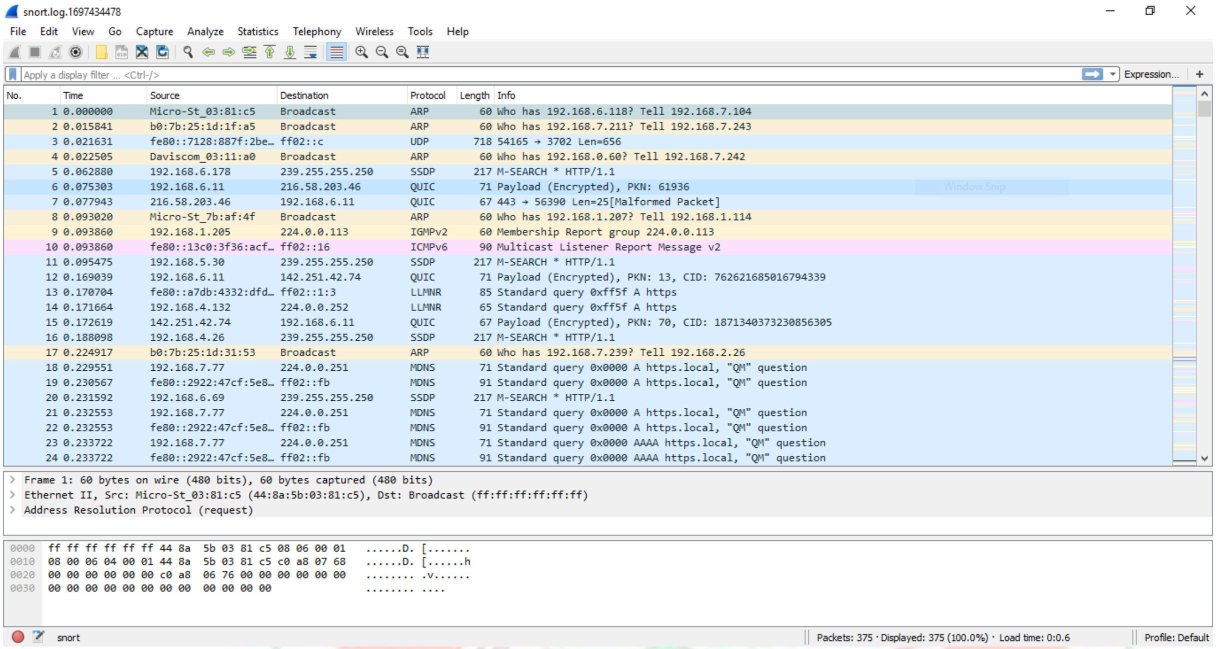
```
Copyright (C) 2014-2022 Cisco and/or its affiliates. All rights
reserved.
Copyright (C) 1998-2013 Sourcefire, Inc., et al.
Using PCRE version: 8.10 2010-06-25
Using ZLIB version: 1.2.11
Index
Physical Address
IP Address
Device Name
Description
1 D8:CB:8A:B3:76:EA
0000:0000: fd01:0000: 0000:0000:8553:5e8c \Device\NPF_{05E92A9A-
8694-49C4-A317-E449B514F0D1} Realtek PCIe GBE Family Controller
disabled \Device\NPF_Loopback Adapter for loopback traffic capture
2
C:\Users\Student>
```

3. Run following command to use snort in Packet logger mode. View the log file created. Observe the content of log file using any packet logger software (e.g. Wireshark). Take SS of command output, the log file creation and the content of the log file. Write your observations under each SS.

```
       Snort -dev -1 C:\Snort\log
```

```
:\Snort\bin>Snort -dev -l C:\Snort\log
Running in packet logging mode

        --== Initializing Snort ==--
Initializing Output Plugins!
Log directory = C:\Snort\log
pcap DAQ configured to passive.
The DAQ version does not support reload.
Acquiring network traffic from "\Device\NPF_{8412B745-AC0D-40DC-B534-
249DEA6A9DC7}".
Decoding Ethernet

        --== 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

C:\Snort\bin>   ''''    By Martin Roesch & The Snort Team:
http://www.snort.org/contact#team
'''''' is not recognized as an internal or external command,
operable program or batch file.
'The' is not recognized as an internal or external command,
operable program or batch file.
```




snort.log.1697434478
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
snort
Profile: Default

```
No.  Time      Source                Destination      Protocol Length Info
   1 0.000000  Micro-St_03:81:c5     Broadcast        ARP        60 Who has 192.168.6.118? Tell 192.168.7.104
   2 0.015841  b0:7b:25:1d:1f:a5     Broadcast        ARP        60 Who has 192.168.7.211? Tell 192.168.7.243
   3 0.021631  fe80::7128:887f:2be…  ff02::c          UDP       718 54165 → 3702 Len=656
   4 0.022505  Daviscom_03:11:a0     Broadcast        ARP        60 Who has 192.168.0.60? Tell 192.168.7.242
   5 0.062880  192.168.6.178         239.255.255.250  SSDP      217 M-SEARCH * HTTP/1.1
   6 0.075303  192.168.6.11          216.58.203.46    QUIC       71 Payload (Encrypted), PKN: 61936
   7 0.077943  216.58.203.46         192.168.6.11     QUIC       67 443 → 56390 Len=25[Malformed Packet]
   8 0.093020  Micro-St_7b:af:4f     Broadcast        ARP        60 Who has 192.168.1.207? Tell 192.168.1.114
   9 0.093860  192.168.1.205         224.0.0.113      IGMPv2     60 Membership Report group 224.0.0.113
  10 0.093860  fe80::13c0:3f36:acf…  ff02::16         ICMPv6     90 Multicast Listener Report Message v2
  11 0.095475  192.168.5.30          239.255.255.250  SSDP      217 M-SEARCH * HTTP/1.1
  12 0.169039  192.168.6.11          142.251.42.74    QUIC       71 Payload (Encrypted), PKN: 13, CID: 762621685016794339
  13 0.170704  fe80::a7db:4332:dfd…  ff02::1:3        LLMNR      85 Standard query 0xff5f A https
  14 0.171664  192.168.4.132         224.0.0.252      LLMNR      65 Standard query 0xff5f A https
  15 0.172619  142.251.42.74         192.168.6.11     QUIC       67 Payload (Encrypted), PKN: 70, CID: 1871340373230856305
  16 0.188098  192.168.4.26          239.255.255.250  SSDP      217 M-SEARCH * HTTP/1.1
  17 0.224917  b0:7b:25:1d:31:53     Broadcast        ARP        60 Who has 192.168.7.239? Tell 192.168.2.26
  18 0.229551  192.168.7.77          224.0.0.251      MDNS       71 Standard query 0x0000 A https.local, "QM" question
  19 0.230567  fe80::2922:47cf:5e8…  ff02::fb         MDNS       91 Standard query 0x0000 A https.local, "QM" question
  20 0.231592  192.168.6.69          239.255.255.250  SSDP      217 M-SEARCH * HTTP/1.1
  21 0.232553  192.168.7.77          224.0.0.251      MDNS       71 Standard query 0x0000 A https.local, "QM" question
  22 0.232553  fe80::2922:47cf:5e8…  ff02::fb         MDNS       91 Standard query 0x0000 A https.local, "QM" question
  23 0.233722  192.168.7.77          224.0.0.251      MDNS       71 Standard query 0x0000 AAAA https.local, "QM" question
  24 0.233722  fe80::2922:47cf:5e8…  ff02::fb         MDNS       91 Standard query 0x0000 AAAA https.local, "QM" question

> Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
> Ethernet II, Src: Micro-St_03:81:c5 (44:8a:5b:03:81:c5), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Address Resolution Protocol (request)

0000  ff ff ff ff ff ff 44 8a  5b 03 81 c5 08 06 00 01   ......D. [.......
0010  08 00 06 04 00 01 44 8a  5b 03 81 c5 c0 a8 07 68   ......D. [......h
0020  00 00 00 00 00 00 c0 a8  06 76 00 00 00 00 00 00   ........ .v......
0030  00 00 00 00 00 00 00 00  00 00 00 00               ........ ....

Packets: 375 · Displayed: 375 (100.0%) · Load time: 0:0.6
```

4. Learn commands to use snort as IDS. Observe the snort rule file *(i.e., snort.conf file)*. Analyze the rule file to configure it for your network environment.

```
      Snort -dev -l C:\Snort\log -h 192.168.1.0/24 -c snort.conf
#--------------------------------------------------
#   VRT Rule Packages Snort.conf
#
#   For more information visit us at:
#     http://www.snort.org                   Snort Website
#     http://vrt-blog.snort.org/    Sourcefire VRT Blog
#
#     Mailing list Contact:      snort-users@lists.snort.org
#     False Positive reports:    fp@sourcefire.com
#     Snort bugs:                bugs@snort.org
#
#     Compatible with Snort Versions:
#     VERSIONS : 2.9.20
#
#     Snort build options:
#     OPTIONS : --enable-gre --enable-mpls --enable-targetbased --enable-ppm --
enable-perfprofiling --enable-zlib --enable-active-response --enable-normalizer --
enable-reload --enable-react --enable-flexresp3
#
#     Additional information:
#     This configuration file enables active response, to run snort in
#     test mode -T you are required to supply an interface -i <interface>
#     or test mode will fail to fully validate the configuration and
#     exit with a FATAL error
#--------------------------------------------------

###################################################
# This file contains a sample snort configuration.
# You should take the following steps to create your own custom configuration:
```

```
#
#  1) Set the network variables.
#  2) Configure the decoder
#  3) Configure the base detection engine
#  4) Configure dynamic loaded libraries
#  5) Configure preprocessors
#  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
ipvar HOME_NET any
# Set up the external network addresses. Leave as "any" in most situations
ipvar EXTERNAL_NET any
# 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
# List of sql servers on your network
ipvar SQL_SERVERS $HOME_NET
# List of telnet servers on your network
ipvar TELNET_SERVERS $HOME_NET
# List of ssh servers on your network
ipvar SSH_SERVERS $HOME_NET
# List of ftp servers on your network
ipvar FTP_SERVERS $HOME_NET
# List of sip servers on your network
ipvar SIP_SERVERS $HOME_NET
# List of ports you run web servers on
portvar HTTP_PORTS
[80,81,311,383,591,593,901,1220,1414,1741,1830,2301,2381,2809,3037,3128,3702,4343,4
848,5250,6988,7000,7001,7144,7145,7510,7777,7779,8000,8008,8014,8028,8080,8085,8088
,8090,8118,8123,8180,8181,8243,8280,8300,8800,8888,8899,9000,9060,9080,9090,9091,94
43,9999,11371,34443,34444,41080,50002,55555]
# List of ports you want to look for SHELLCODE on.
portvar SHELLCODE_PORTS !80
# List of ports you might see oracle attacks on
portvar ORACLE_PORTS 1024:
# List of ports you want to look for SSH connections on:
portvar SSH_PORTS 22
# List of ports you run ftp servers on
portvar FTP_PORTS [21,2100,3535]
# List of ports you run SIP servers on
portvar SIP_PORTS [5060,5061,5600]
# List of file data ports for file inspection
portvar FILE_DATA_PORTS [$HTTP_PORTS,110,143]
# List of GTP ports for GTP preprocessor
portvar GTP_PORTS [2123,2152,3386]

# other variables, these should not be modified
ipvar AIM_SERVERS
[64.12.24.0/23,64.12.28.0/23,64.12.161.0/24,64.12.163.0/24,64.12.200.0/24,205.188.3
.0/24,205.188.5.0/24,205.188.7.0/24,205.188.9.0/24,205.188.153.0/24,205.188.179.0/2
4,205.188.248.0/24]
```

```
# Path to your rules files (this can be a relative path)
# Note for Windows users:  You are advised to make this an absolute path,
# such as:  c:\snort\rules
var RULE_PATH ../rules
var SO_RULE_PATH ../so_rules
var PREPROC_RULE_PATH ../preproc_rules

# If you are using reputation preprocessor set these
# Currently there is a bug with relative paths, they are relative to where snort is
# not relative to snort.conf like the above variables
# This is completely inconsistent with how other vars work, BUG 89986
# Set the absolute path appropriately
var WHITE_LIST_PATH ../rules
var BLACK_LIST_PATH ../rules
```

```
C:\Snort\bin>Snort -dev -l C:\Snort\log -h 192.168.1.0/24 -c snort.conf
Running in IDS mode

        --== Initializing Snort ==--
Initializing Output Plugins!
Initializing Preprocessors!
Initializing Plug-ins!
Parsing Rules file "snort.conf"
ERROR: snort.conf(0) Unable to open rules file "snort.conf": No such file or
directory.

Fatal Error, Quitting..
Could not create the registry key.
C:\Snort\bin>
```

Post Experimental Exercise- *(to be handwritten on journal sheets. Refer snort user manual for answers)*

1. ________ snort command display packet header, packet data as well as the data link layer headers.
2. Explain the snort command that will be used for logging the packets on a high-speed network.
3. Explain the use of '-h' option/switch while writing the snort rule.
4. Explain in detail Snort's NIDS mode output options.
5. Explain the following snort command `'snort -c snort.conf -A fast -h 192.168.1.0/24'`

Conclusion:

In this experiment we were introduced to most used IPS/IDS software 'Snort'. Snort acts as a security guard for any network, providing a proactive detection and prevention of any type of intrusion. Snort can perform packet sniffing, logging, and intrusion detection. We studied various options/switches that can be used for writing intrusion detection rules, for sniffing the network and for logging the network traffic.

References:

[1] "Snort User's Manual 2.9.16", https://snort.org/

[2] Bart Lenaerts-Bergmans , "SNORT AND SNORT RULES EXPLAINED", https://www.crowdstrike.com/cybersecurity-101/threat-intelligence/snort-rules/

[3] "Basic snort rules syntax and usage", https://resources.infosecinstitute.com/topics/penetration-testing/snort-rules-workshop-part-one/

[4] "Writing Snort Rules with Examples and Cheat Sheet", https://cyvatar.ai/write-configure-snort-rules/