Name: Miftahul Huq

Course: Network Security

Course Prefix: CSEC 744

Section: 01

Chapter 13: Intrusion Detection Systems and Network Security

Date: 03/28/2024

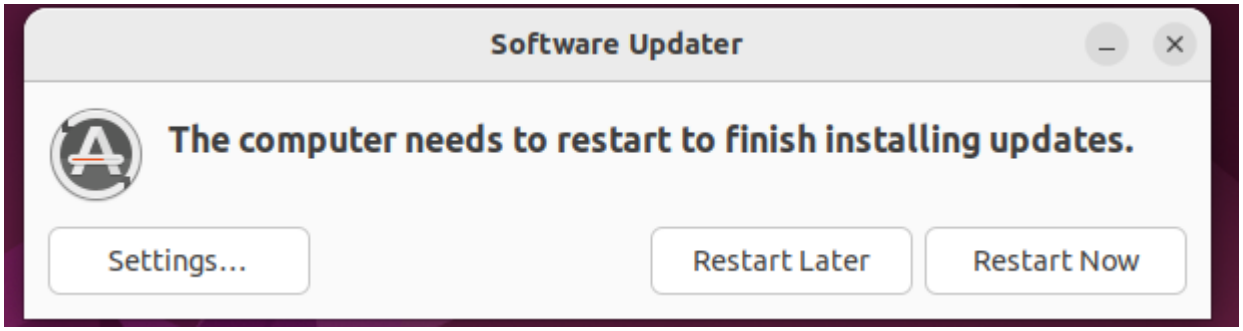
Lab Exercise 13.01: Installing Ubuntu and Snort

Note: I am using NAT because setting the network setting of the VM is not working. The screenshot below shows the ip address of the VMnet8. Through VMnet8 network traffic from the host reaches the VM.

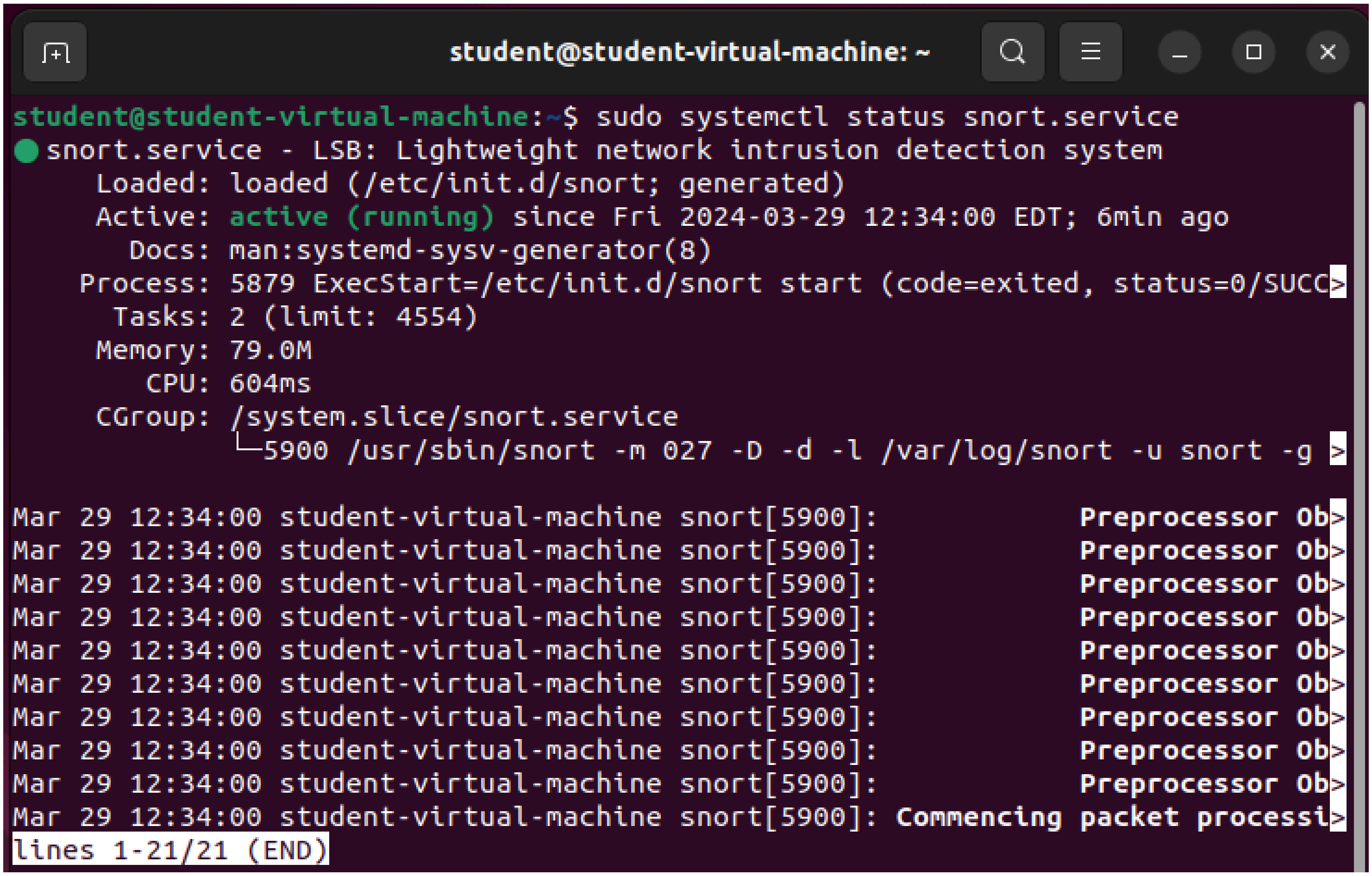
Command Prompt

```
C:\Users\Student>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . : rit.edu
   Link-local IPv6 Address . . . . . : fe80::dc6f:466e:72f9:6b89%3
   IPv4 Address. . . . . . . . . . . : 192.168.205.31
   Subnet Mask . . . . . . . . . . . : 255.255.240.0
   Default Gateway . . . . . . . . . : 192.168.207.254

Ethernet adapter VMware Network Adapter VMnet1:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::4dfb:c9d1:7eae:75a%7
   IPv4 Address. . . . . . . . . . . : 192.168.116.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Ethernet adapter VMware Network Adapter VMnet8:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::7d09:dfb3:539e:ea1e%5
   IPv4 Address. . . . . . . . . . . : 192.168.153.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

C:\Users\Student>
```

Step 1v: I restarted after the update was done.



Step 2e:



```
student@student-virtual-machine:~$ sudo systemctl status snort.service
● snort.service - LSB: Lightweight network intrusion detection system
     Loaded: loaded (/etc/init.d/snort; generated)
     Active: active (running) since Fri 2024-03-29 12:34:00 EDT; 6min ago
       Docs: man:systemd-sysv-generator(8)
    Process: 5879 ExecStart=/etc/init.d/snort start (code=exited, status=0/SUCC>
      Tasks: 2 (limit: 4554)
     Memory: 79.0M
        CPU: 604ms
     CGroup: /system.slice/snort.service
             └─5900 /usr/sbin/snort -m 027 -D -d -l /var/log/snort -u snort -g >

Mar 29 12:34:00 student-virtual-machine snort[5900]:           Preprocessor Ob>
Mar 29 12:34:00 student-virtual-machine snort[5900]:           Preprocessor Ob>
Mar 29 12:34:00 student-virtual-machine snort[5900]:           Preprocessor Ob>
Mar 29 12:34:00 student-virtual-machine snort[5900]:           Preprocessor Ob>
Mar 29 12:34:00 student-virtual-machine snort[5900]:           Preprocessor Ob>
Mar 29 12:34:00 student-virtual-machine snort[5900]:           Preprocessor Ob>
Mar 29 12:34:00 student-virtual-machine snort[5900]:           Preprocessor Ob>
Mar 29 12:34:00 student-virtual-machine snort[5900]:           Preprocessor Ob>
Mar 29 12:34:00 student-virtual-machine snort[5900]:           Preprocessor Ob>
Mar 29 12:34:00 student-virtual-machine snort[5900]: Commencing packet processi>
lines 1-21/21 (END)
```

Lab Exercise 13.02: Snort Sniffer Mode

Step 1a:

```
student@student-virtual-machine: ~
student@student-virtual-machine: ~    student@student-virtual-machine: ~

USAGE: snort [-options] <filter options>
Options:
        -A          Set alert mode: fast, full, console, test or none  (alert fil
e alerts only)
                    "unsock" enables UNIX socket logging (experimental).
        -b          Log packets in tcpdump format (much faster!)
        -B <mask>   Obfuscated IP addresses in alerts and packet dumps using CIDR
 mask
        -c <rules>  Use Rules File <rules>
        -C          Print out payloads with character data only (no hex)
        -d          Dump the Application Layer
        -D          Run Snort in background (daemon) mode
        -e          Display the second layer header info
        -f          Turn off fflush() calls after binary log writes
        -F <bpf>    Read BPF filters from file <bpf>
        -g <gname>  Run snort gid as <gname> group (or gid) after initialization
        -G <0xid>   Log Identifier (to uniquely id events for multiple snorts)
        -h <hn>     Set home network = <hn>
                    (for use with -l or -B, does NOT change $HOME_NET in IDS mode
)
        -H          Make hash tables deterministic.
        -i <if>     Listen on interface <if>
        -I          Add Interface name to alert output
:
```

Step 1b:

```
student@student-virtual-machine: ~
student@student-virtual-machine: ~    student@student-virtual-machine: ~

SNORT(8)                System Manager's Manual                SNORT(8)

NAME
       Snort - open source network intrusion detection system

SYNOPSIS
       snort  [-bCdDeEfHIMNOpqQsTUvVwWxXy?]  [-A alert-mode ] [-B address-con-
       version-mask ] [-c rules-file ] [-F bpf-file ] [-g group-name ] [-G  id
       ] [-h home-net ] [-i interface ] [-k checksum-mode ] [-K logging-mode ]
       [-l log-dir ] [-L bin-log-file ] [-m umask ]  [-n  packet-count  ]  [-P
       snap-length  ]  [-r  tcpdump-file ] [-R name ] [-S variable=value ] [-t
       chroot_directory ] [-u  user-name  ]  [-Z  pathname  ]  [--logid  id  ]
       [--perfmon-file  pathname  ]  [--pid-path  pathname  ] [--snaplen snap-
       length ] [--help ] [--version ]  [--dynamic-engine-lib  file  ]  [--dy-
       namic-engine-lib-dir directory ] [--dynamic-detection-lib file ] [--dy-
       namic-detection-lib-dir directory ] [--dump-dynamic-rules  directory  ]
       [--dynamic-preprocessor-lib  file ] [--dynamic-preprocessor-lib-dir di-
       rectory ] [--dynamic-output-lib file ] [--dynamic-output-lib-dir direc-
       tory  ]  [--alert-before-pass ] [--treat-drop-as-alert ] [--treat-drop-
       as-ignore ] [--process-all-events ] [--enable-inline-test ]  [--create-
       pidfile  ] [--nolock-pidfile ] [--no-interface-pidfile ] [--disable-at-
       tribute-reload-thread ] [--pcap-single= tcpdump-file ]  [--pcap-filter=
       filter  ]  [--pcap-list= list ] [--pcap-dir= directory ] [--pcap-file=
```

Step 1c:

```
student@student-virtual-machine: ~
student@student-virtual-machine: ~    student@student-virtual-machine: ~
student@student-virtual-machine:~$ snort -V

   ,,_     -*> Snort! <*-
  o"  )~   Version 2.9.15.1 GRE (Build 15125)
   ''''    By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
           Copyright (C) 2014-2019 Cisco and/or its affiliates. All rights reser
ved.
           Copyright (C) 1998-2013 Sourcefire, Inc., et al.
           Using libpcap version 1.10.1 (with TPACKET_V3)
           Using PCRE version: 8.39 2016-06-14
           Using ZLIB version: 1.2.11

student@student-virtual-machine:~$
```

Step 2a:

```
student@student-virtual-machine: ~
student@student-virtual-machine:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group defaul
t qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP gro
up default qlen 1000
    link/ether 00:0c:29:57:79:d4 brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    inet 192.168.153.128/24 brd 192.168.153.255 scope global dynamic noprefixrou
te ens33
       valid_lft 1379sec preferred_lft 1379sec
    inet6 fe80::8b33:fa04:88b:3f41/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
student@student-virtual-machine:~$
```

Step 2b:

```
student@student-virtual-machine: ~

student@student-virtual-machine:~$ sudo snort -v
Running in packet dump mode

        --== Initializing Snort ==--
Initializing Output Plugins!
pcap DAQ configured to passive.
Acquiring network traffic from "ens33".
Decoding Ethernet

        --== Initialization Complete ==--

   ,,_     -*> Snort! <*-
  o"  )~   Version 2.9.15.1 GRE (Build 15125)
   ''''    By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
           Copyright (C) 2014-2019 Cisco and/or its affiliates. All rights reser
ved.
           Copyright (C) 1998-2013 Sourcefire, Inc., et al.
           Using libpcap version 1.10.1 (with TPACKET_V3)
           Using PCRE version: 8.39 2016-06-14
           Using ZLIB version: 1.2.11

Commencing packet processing (pid=6534)
```

Step 2c (you can see that the traffic is coming from 192.168.153.1, which is the VMnet8 as states in above note)

```
student@student-virtual-machine

student@student-virtual-machine: ~

Commencing packet processing (pid=7580)
WARNING: No preprocessors configured for policy 0.
03/29-14:25:51.331569 192.168.153.1 -> 192.168.153.129
ICMP TTL:128 TOS:0x0 ID:383 IpLen:20 DgmLen:60
Type:8  Code:0  ID:1   Seq:17  ECHO
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

WARNING: No preprocessors configured for policy 0.
03/29-14:25:51.331608 192.168.153.129 -> 192.168.153.1
ICMP TTL:64 TOS:0x0 ID:42626 IpLen:20 DgmLen:60
Type:0  Code:0  ID:1  Seq:17  ECHO REPLY
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

WARNING: No preprocessors configured for policy 0.
03/29-14:25:52.336449 192.168.153.1 -> 192.168.153.129
ICMP TTL:128 TOS:0x0 ID:384 IpLen:20 DgmLen:60
Type:8  Code:0  ID:1   Seq:18  ECHO
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

WARNING: No preprocessors configured for policy 0.
03/29-14:25:52.336488 192.168.153.129 -> 192.168.153.1
ICMP TTL:64 TOS:0x0 ID:42872 IpLen:20 DgmLen:60
Type:0  Code:0  ID:1  Seq:18  ECHO REPLY
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

WARNING: No preprocessors configured for policy 0.
03/29-14:25:53.352232 192.168.153.1 -> 192.168.153.129
ICMP TTL:128 TOS:0x0 ID:385 IpLen:20 DgmLen:60
Type:8  Code:0  ID:1   Seq:19  ECHO
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
```

Step 2d:

```
Commencing packet processing (pid=7596)
WARNING: No preprocessors configured for policy 0.
03/29-14:30:08.214399 127.0.0.1 -> 127.0.0.1
ICMP TTL:64 TOS:0x0 ID:25830 IpLen:20 DgmLen:84 DF
Type:8  Code:0  ID:1   Seq:1  ECHO
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

WARNING: No preprocessors configured for policy 0.
03/29-14:30:08.214408 127.0.0.1 -> 127.0.0.1
ICMP TTL:64 TOS:0x0 ID:25831 IpLen:20 DgmLen:84
Type:0  Code:0  ID:1  Seq:1  ECHO REPLY
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

WARNING: No preprocessors configured for policy 0.
03/29-14:30:09.219831 127.0.0.1 -> 127.0.0.1
ICMP TTL:64 TOS:0x0 ID:25847 IpLen:20 DgmLen:84 DF
Type:8  Code:0  ID:1   Seq:2  ECHO
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

WARNING: No preprocessors configured for policy 0.
03/29-14:30:09.219841 127.0.0.1 -> 127.0.0.1
ICMP TTL:64 TOS:0x0 ID:25848 IpLen:20 DgmLen:84
Type:0  Code:0  ID:1  Seq:2  ECHO REPLY
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

WARNING: No preprocessors configured for policy 0.
03/29-14:30:10.243683 127.0.0.1 -> 127.0.0.1
ICMP TTL:64 TOS:0x0 ID:26090 IpLen:20 DgmLen:84 DF
Type:8  Code:0  ID:1   Seq:3  ECHO
```

Step 3a:

```
WARNING: No preprocessors configured for policy 0.
03/29-15:00:49.091083 192.168.153.1 -> 192.168.153.129
ICMP TTL:128 TOS:0x0 ID:387 IpLen:20 DgmLen:60
Type:8  Code:0  ID:1   Seq:21  ECHO
61 62 63 64 65 66 67 68 69 6A 6B 6C 6D 6E 6F 70  abcdefghijklmnop
71 72 73 74 75 76 77 61 62 63 64 65 66 67 68 69  qrstuvwabcdefghi

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

WARNING: No preprocessors configured for policy 0.
03/29-15:00:49.091116 192.168.153.129 -> 192.168.153.1
ICMP TTL:64 TOS:0x0 ID:52322 IpLen:20 DgmLen:60
Type:0  Code:0  ID:1  Seq:21  ECHO REPLY
61 62 63 64 65 66 67 68 69 6A 6B 6C 6D 6E 6F 70  abcdefghijklmnop
71 72 73 74 75 76 77 61 62 63 64 65 66 67 68 69  qrstuvwabcdefghi

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

WARNING: No preprocessors configured for policy 0.
03/29-15:00:50.102219 192.168.153.1 -> 192.168.153.129
ICMP TTL:128 TOS:0x0 ID:388 IpLen:20 DgmLen:60
Type:8  Code:0  ID:1   Seq:22  ECHO
61 62 63 64 65 66 67 68 69 6A 6B 6C 6D 6E 6F 70  abcdefghijklmnop
71 72 73 74 75 76 77 61 62 63 64 65 66 67 68 69  qrstuvwabcdefghi

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

WARNING: No preprocessors configured for policy 0.
03/29-15:00:50.102309 192.168.153.129 -> 192.168.153.1
ICMP TTL:64 TOS:0x0 ID:52433 IpLen:20 DgmLen:60
Type:0  Code:0  ID:1  Seq:22  ECHO REPLY
61 62 63 64 65 66 67 68 69 6A 6B 6C 6D 6E 6F 70  abcdefghijklmnop
71 72 73 74 75 76 77 61 62 63 64 65 66 67 68 69  qrstuvwabcdefghi
```

Step 3b:

```
Commencing packet processing (pid=8348)
WARNING: No preprocessors configured for policy 0.
03/29-15:02:07.583016 00:50:56:C0:00:08 -> 00:0C:29:57:79:D4 type:0x800 len:0x4A
192.168.153.1 -> 192.168.153.129 ICMP TTL:128 TOS:0x0 ID:391 IpLen:20 DgmLen:60
Type:8  Code:0  ID:1   Seq:25  ECHO
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

WARNING: No preprocessors configured for policy 0.
03/29-15:02:07.583052 00:0C:29:57:79:D4 -> 00:50:56:C0:00:08 type:0x800 len:0x4A
192.168.153.129 -> 192.168.153.1 ICMP TTL:64 TOS:0x0 ID:3796 IpLen:20 DgmLen:60
Type:0  Code:0  ID:1  Seq:25  ECHO REPLY
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

WARNING: No preprocessors configured for policy 0.
03/29-15:02:08.597090 00:50:56:C0:00:08 -> 00:0C:29:57:79:D4 type:0x800 len:0x4A
192.168.153.1 -> 192.168.153.129 ICMP TTL:128 TOS:0x0 ID:392 IpLen:20 DgmLen:60
Type:8  Code:0  ID:1   Seq:26  ECHO
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

WARNING: No preprocessors configured for policy 0.
03/29-15:02:08.597126 00:0C:29:57:79:D4 -> 00:50:56:C0:00:08 type:0x800 len:0x4A
192.168.153.129 -> 192.168.153.1 ICMP TTL:64 TOS:0x0 ID:3811 IpLen:20 DgmLen:60
Type:0  Code:0  ID:1  Seq:26  ECHO REPLY
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

WARNING: No preprocessors configured for policy 0.
03/29-15:02:09.610929 00:50:56:C0:00:08 -> 00:0C:29:57:79:D4 type:0x800 len:0x4A
192.168.153.1 -> 192.168.153.129 ICMP TTL:128 TOS:0x0 ID:393 IpLen:20 DgmLen:60
Type:8  Code:0  ID:1   Seq:27  ECHO
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

WARNING: No preprocessors configured for policy 0.
03/29-15:02:09.610961 00:0C:29:57:79:D4 -> 00:50:56:C0:00:08 type:0x800 len:0x4A
192.168.153.129 -> 192.168.153.1 ICMP TTL:64 TOS:0x0 ID:4055 IpLen:20 DgmLen:60
Type:0  Code:0  ID:1  Seq:27  ECHO REPLY
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
```

Step 3c:

```
Commencing packet processing (pid=8378)
WARNING: No preprocessors configured for policy 0.
03/29-15:03:13.309960 00:50:56:C0:00:08 -> 00:0C:29:57:79:D4 type:0x800 len:0x4A
192.168.153.1 -> 192.168.153.129 ICMP TTL:128 TOS:0x0 ID:395 IpLen:20 DgmLen:60
Type:8  Code:0  ID:1   Seq:29  ECHO
61 62 63 64 65 66 67 68 69 6A 6B 6C 6D 6E 6F 70  abcdefghijklmnop
71 72 73 74 75 76 77 61 62 63 64 65 66 67 68 69  qrstuvwabcdefghi

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

WARNING: No preprocessors configured for policy 0.
03/29-15:03:13.309995 00:0C:29:57:79:D4 -> 00:50:56:C0:00:08 type:0x800 len:0x4A
192.168.153.129 -> 192.168.153.1 ICMP TTL:64 TOS:0x0 ID:11393 IpLen:20 DgmLen:60
Type:0  Code:0  ID:1  Seq:29  ECHO REPLY
61 62 63 64 65 66 67 68 69 6A 6B 6C 6D 6E 6F 70  abcdefghijklmnop
71 72 73 74 75 76 77 61 62 63 64 65 66 67 68 69  qrstuvwabcdefghi

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

WARNING: No preprocessors configured for policy 0.
03/29-15:03:14.328448 00:50:56:C0:00:08 -> 00:0C:29:57:79:D4 type:0x800 len:0x4A
192.168.153.1 -> 192.168.153.129 ICMP TTL:128 TOS:0x0 ID:396 IpLen:20 DgmLen:60
Type:8  Code:0  ID:1   Seq:30  ECHO
61 62 63 64 65 66 67 68 69 6A 6B 6C 6D 6E 6F 70  abcdefghijklmnop
71 72 73 74 75 76 77 61 62 63 64 65 66 67 68 69  qrstuvwabcdefghi

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

WARNING: No preprocessors configured for policy 0.
03/29-15:03:14.328480 00:0C:29:57:79:D4 -> 00:50:56:C0:00:08 type:0x800 len:0x4A
192.168.153.129 -> 192.168.153.1 ICMP TTL:64 TOS:0x0 ID:11563 IpLen:20 DgmLen:60
```

Lab Exercise 13.03: Snort Packet Logger Mode

Step 1a:

```
student@student-virtual-machine:~$ sudo snort -l .
Running in packet logging mode

        --== Initializing Snort ==--
Initializing Output Plugins!
Log directory = .
pcap DAQ configured to passive.
Acquiring network traffic from "ens33".
Decoding Ethernet

        --== Initialization Complete ==--

   ,,_     -*> Snort! <*-
  o"  )~   Version 2.9.15.1 GRE (Build 15125)
   ''''    By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
           Copyright (C) 2014-2019 Cisco and/or its affiliates. All rights reserved.
           Copyright (C) 1998-2013 Sourcefire, Inc., et al.
           Using libpcap version 1.10.1 (with TPACKET_V3)
           Using PCRE version: 8.39 2016-06-14
           Using ZLIB version: 1.2.11

Commencing packet processing (pid=8715)
```

Step 1b:

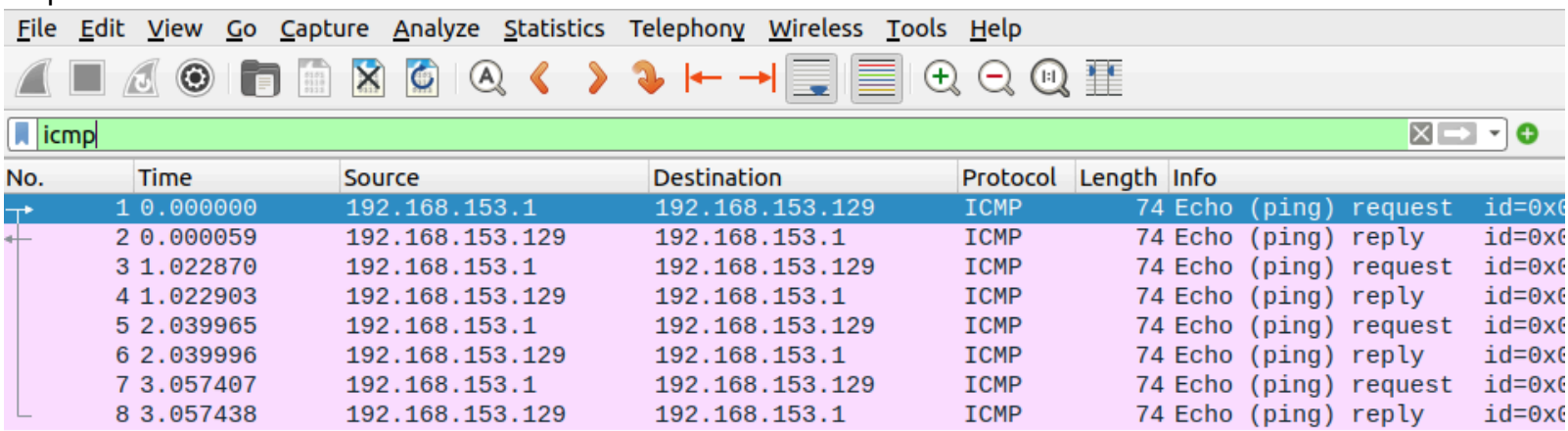
Command Prompt

```
C:\Users\Student>ping 192.168.153.129

Pinging 192.168.153.129 with 32 bytes of data:
Reply from 192.168.153.129: bytes=32 time<1ms TTL=64
Reply from 192.168.153.129: bytes=32 time<1ms TTL=64
Reply from 192.168.153.129: bytes=32 time<1ms TTL=64
Reply from 192.168.153.129: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.153.129:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\Student>
```

Step 2a:

```
student@student-virtual-machine: ~
student@student-virtual-machine:~$ ls
Desktop  Documents  Downloads  Music  Pictures  Public  snap  snort.log.1711740530
student@student-virtual-machine:~$
```

Step 2b:



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.153.1	192.168.153.129	ICMP	74	Echo (ping) request id=0x0
2	0.000059	192.168.153.129	192.168.153.1	ICMP	74	Echo (ping) reply id=0x0
3	1.022870	192.168.153.1	192.168.153.129	ICMP	74	Echo (ping) request id=0x0
4	1.022903	192.168.153.129	192.168.153.1	ICMP	74	Echo (ping) reply id=0x0
5	2.039965	192.168.153.1	192.168.153.129	ICMP	74	Echo (ping) request id=0x0
6	2.039996	192.168.153.129	192.168.153.1	ICMP	74	Echo (ping) reply id=0x0
7	3.057407	192.168.153.1	192.168.153.129	ICMP	74	Echo (ping) request id=0x0
8	3.057438	192.168.153.129	192.168.153.1	ICMP	74	Echo (ping) reply id=0x0

Lab Exercise 13.04: Snort Network Intrusion Detection System Mode

Step 1a:

```
student@student-virtual-machine:~$ sudo cat /etc/snort/snort.conf
#--------------------------------------------------
#   VRT Rule Packages Snort.conf
#

preprocessor frag3_global: max_frags 65536
include classification.config
ipvar HOME_NET 192.168.153.0/24
var RULE_PATH /etc/snort/rules
include $RULE_PATH/local.rules

#   For more information visit us at:
#     http://www.snort.org                                Snort Website
#     http://vrt-blog.snort.org/    Sourcefire VRT Blog
```

```
ipvar HOME_NET 192.168.153.0/24
```

Step 1b:

Open | local.rules /etc/snort/rules | Save

```
# $Id: local.rules,v 1.11 2004/07/23 20:15:44 bmc Exp $
# ----------------
# LOCAL RULES
# ----------------
# This file intentionally does not come with signatures.  Put your local
# additions here.
alert icmp any any -> $HOME_NET any (msg:"ICMP detected!";sid: 1000052; rev:1; classtype:icmp-event;)
```

Step 1c:

```
student@student-virtual-machine:~$ sudo snort -A console -A fast -c /etc/snort/snort.conf -i ens33
Running in IDS mode

        --== Initializing Snort ==--
Initializing Output Plugins!
Initializing Preprocessors!
Initializing Plug-ins!
Parsing Rules file "/etc/snort/snort.conf"
/etc/snort/snort.conf(72) Var 'HOME_NET' redefined.
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 70
00:7001 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 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 8
899 9000 9060 9080 9090:9091 9443 9999 11371 34443:34444 41080 50002 55555 ]
PortVar 'GTP_PORTS' defined :  [ 2123 2152 3386 ]
WARNING: /etc/snort/snort.conf(135) Var 'RULE_PATH' redefined

Detection:
   Search-Method = AC-Full-Q
    Split Any/Any group = enabled
    Search-Method-Optimizations = enabled
    Maximum pattern length = 20
WARNING: /etc/snort/classification.config(30) Duplicate classification "not-suspicious"found, ignoring this line
```

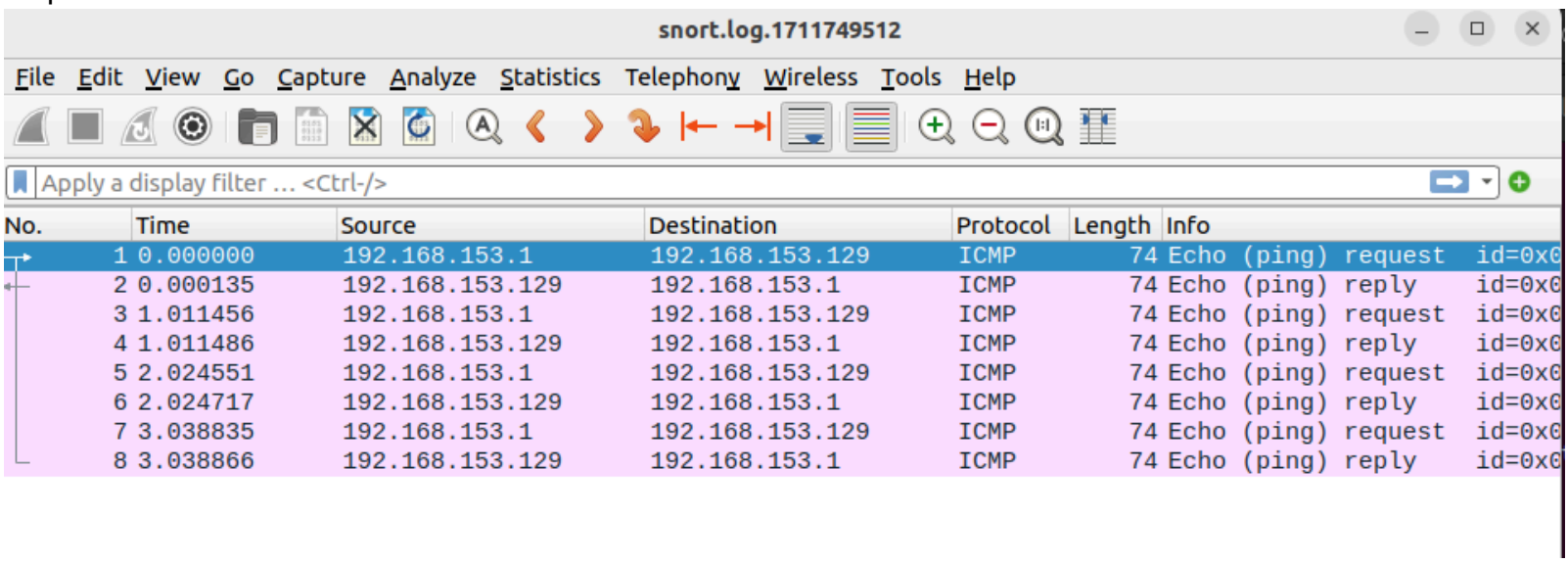
Step 1d:

```
           Preprocessor Object: SF_SDF  Version 1.1  <Build 1>
           Preprocessor Object: SF_SMTP  Version 1.1  <Build 9>
           Preprocessor Object: SF_REPUTATION  Version 1.1  <Build 1>
           Preprocessor Object: appid  Version 1.1  <Build 5>
Commencing packet processing (pid=9845)
03/29-18:00:34.583848  [**] [1:1000052:1] ICMP detected! [**] [Classification: Generic ICMP event] [Priority: 3] {ICMP} 192.168.153.
1 -> 192.168.153.129
03/29-18:00:34.583983  [**] [1:1000052:1] ICMP detected! [**] [Classification: Generic ICMP event] [Priority: 3] {ICMP} 192.168.153.
129 -> 192.168.153.1
03/29-18:00:35.595304  [**] [1:1000052:1] ICMP detected! [**] [Classification: Generic ICMP event] [Priority: 3] {ICMP} 192.168.153.
1 -> 192.168.153.129
03/29-18:00:35.595334  [**] [1:1000052:1] ICMP detected! [**] [Classification: Generic ICMP event] [Priority: 3] {ICMP} 192.168.153.
129 -> 192.168.153.1
03/29-18:00:36.608399  [**] [1:1000052:1] ICMP detected! [**] [Classification: Generic ICMP event] [Priority: 3] {ICMP} 192.168.153.
1 -> 192.168.153.129
03/29-18:00:36.608565  [**] [1:1000052:1] ICMP detected! [**] [Classification: Generic ICMP event] [Priority: 3] {ICMP} 192.168.153.
129 -> 192.168.153.1
03/29-18:00:37.622683  [**] [1:1000052:1] ICMP detected! [**] [Classification: Generic ICMP event] [Priority: 3] {ICMP} 192.168.153.
1 -> 192.168.153.129
03/29-18:00:37.622714  [**] [1:1000052:1] ICMP detected! [**] [Classification: Generic ICMP event] [Priority: 3] {ICMP} 192.168.153.
129 -> 192.168.153.1
```

Step 1e:

```
student@student-virtual-machine:~$ sudo ls -l /var/log/snort
[sudo] password for student:
total 544
-rw-r--r-- 1 root  adm   1224 Mar 29 18:00 alert
-rw-r----- 1 snort adm  51624 Mar 29 18:02 snort.alert
-rw-r--r-- 1 root  adm 154183 Mar 29 18:02 snort.alert.fast
-rw-r----- 1 snort adm 324768 Mar 29 18:02 snort.log
-rw------- 1 root  adm    744 Mar 29 18:00 snort.log.1711749512
student@student-virtual-machine:~$
```

Step 1f:



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.153.1	192.168.153.129	ICMP	74	Echo (ping) request id=0x0
2	0.000135	192.168.153.129	192.168.153.1	ICMP	74	Echo (ping) reply id=0x0
3	1.011456	192.168.153.1	192.168.153.129	ICMP	74	Echo (ping) request id=0x0
4	1.011486	192.168.153.129	192.168.153.1	ICMP	74	Echo (ping) reply id=0x0
5	2.024551	192.168.153.1	192.168.153.129	ICMP	74	Echo (ping) request id=0x0
6	2.024717	192.168.153.129	192.168.153.1	ICMP	74	Echo (ping) reply id=0x0
7	3.038835	192.168.153.1	192.168.153.129	ICMP	74	Echo (ping) request id=0x0
8	3.038866	192.168.153.129	192.168.153.1	ICMP	74	Echo (ping) reply id=0x0

Step 1g:

Open | alert /var/log/snort | Save

```
1 03/29-18:00:34.583848  [**] [1:1000052:1] ICMP detected! [**] [Classification: Generic ICMP
  event] [Priority: 3] {ICMP} 192.168.153.1 -> 192.168.153.129
2 03/29-18:00:34.583983  [**] [1:1000052:1] ICMP detected! [**] [Classification: Generic ICMP
  event] [Priority: 3] {ICMP} 192.168.153.129 -> 192.168.153.1
3 03/29-18:00:35.595304  [**] [1:1000052:1] ICMP detected! [**] [Classification: Generic ICMP
  event] [Priority: 3] {ICMP} 192.168.153.1 -> 192.168.153.129
4 03/29-18:00:35.595334  [**] [1:1000052:1] ICMP detected! [**] [Classification: Generic ICMP
  event] [Priority: 3] {ICMP} 192.168.153.129 -> 192.168.153.1
5 03/29-18:00:36.608399  [**] [1:1000052:1] ICMP detected! [**] [Classification: Generic ICMP
  event] [Priority: 3] {ICMP} 192.168.153.1 -> 192.168.153.129
6 03/29-18:00:36.608565  [**] [1:1000052:1] ICMP detected! [**] [Classification: Generic ICMP
  event] [Priority: 3] {ICMP} 192.168.153.129 -> 192.168.153.1
7 03/29-18:00:37.622683  [**] [1:1000052:1] ICMP detected! [**] [Classification: Generic ICMP
  event] [Priority: 3] {ICMP} 192.168.153.1 -> 192.168.153.129
8 03/29-18:00:37.622714  [**] [1:1000052:1] ICMP detected! [**] [Classification: Generic ICMP
  event] [Priority: 3] {ICMP} 192.168.153.129 -> 192.168.153.1
```

Step 1h:

```
student@student-virtual-machine:~$ sudo snort -A console -A full -c /etc/snort/snort.conf -i ens33
Running in IDS mode

        --== Initializing Snort ==--
Initializing Output Plugins!
Initializing Preprocessors!
Initializing Plug-ins!
Parsing Rules file "/etc/snort/snort.conf"
/etc/snort/snort.conf(72) Var 'HOME_NET' redefined.
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 70
00:7001 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 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 8
899 9000 9060 9080 9090:9091 9443 9999 11371 34443:34444 41080 50002 55555 ]
```

Step 1i:

Open

alert
/var/log/snort

```
[**] [1:1000052:1] ICMP detected! [**]
[Classification: Generic ICMP event] [Priority: 3]
03/29-18:12:32.232407 192.168.153.1 -> 192.168.153.129
ICMP TTL:128 TOS:0x0 ID:423 IpLen:20 DgmLen:60
Type:8  Code:0  ID:1   Seq:57  ECHO

[**] [1:1000052:1] ICMP detected! [**]
[Classification: Generic ICMP event] [Priority: 3]
03/29-18:12:32.232442 192.168.153.129 -> 192.168.153.1
ICMP TTL:64 TOS:0x0 ID:6040 IpLen:20 DgmLen:60
Type:0  Code:0  ID:1  Seq:57  ECHO REPLY

[**] [1:1000052:1] ICMP detected! [**]
[Classification: Generic ICMP event] [Priority: 3]
03/29-18:12:33.242661 192.168.153.1 -> 192.168.153.129
ICMP TTL:128 TOS:0x0 ID:424 IpLen:20 DgmLen:60
Type:8  Code:0  ID:1   Seq:58  ECHO

[**] [1:1000052:1] ICMP detected! [**]
[Classification: Generic ICMP event] [Priority: 3]
03/29-18:12:33.242692 192.168.153.129 -> 192.168.153.1
ICMP TTL:64 TOS:0x0 ID:6241 IpLen:20 DgmLen:60
Type:0  Code:0  ID:1  Seq:58  ECHO REPLY

[**] [1:1000052:1] ICMP detected! [**]
[Classification: Generic ICMP event] [Priority: 3]
03/29-18:12:34.255836 192.168.153.1 -> 192.168.153.129
ICMP TTL:128 TOS:0x0 ID:425 IpLen:20 DgmLen:60
Type:8  Code:0  ID:1   Seq:59  ECHO

[**] [1:1000052:1] ICMP detected! [**]
[Classification: Generic ICMP event] [Priority: 3]
03/29-18:12:34.255890 192.168.153.129 -> 192.168.153.1
```

Step 1j:

```
student@student-virtual-machine:~$ sudo snort -A console -A fast -A full -c /etc/snort/snort.conf -i ens33
Running in IDS mode

        --== Initializing Snort ==--
Initializing Output Plugins!
Initializing Preprocessors!
Initializing Plug-ins!
Parsing Rules file "/etc/snort/snort.conf"
/etc/snort/snort.conf(72) Var 'HOME_NET' redefined.
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 70
00:7001 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 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 ]
```

Step 1k:

Open | alert /var/log/snort | Save

```
[**] [1:1000052:1] ICMP detected! [**]
[Classification: Generic ICMP event] [Priority: 3]
03/29-18:21:35.505672 192.168.153.1 -> 192.168.153.129
ICMP TTL:128 TOS:0x0 ID:435 IpLen:20 DgmLen:60
Type:8  Code:0  ID:1   Seq:69  ECHO

03/29-18:21:35.505672  [**] [1:1000052:1] ICMP detected! [**] [Classification: Generic ICMP event] [Priority: 3] {ICMP} 192.168.153.1 -> 192.168.153.129
[**] [1:1000052:1] ICMP detected! [**]
[Classification: Generic ICMP event] [Priority: 3]
03/29-18:21:35.505705 192.168.153.129 -> 192.168.153.1
ICMP TTL:64 TOS:0x0 ID:15741 IpLen:20 DgmLen:60
Type:0  Code:0  ID:1  Seq:69  ECHO REPLY

03/29-18:21:35.505705  [**] [1:1000052:1] ICMP detected! [**] [Classification: Generic ICMP event] [Priority: 3] {ICMP} 192.168.153.129 -> 192.168.153.1
[**] [1:1000052:1] ICMP detected! [**]
[Classification: Generic ICMP event] [Priority: 3]
03/29-18:21:36.517831 192.168.153.1 -> 192.168.153.129
ICMP TTL:128 TOS:0x0 ID:436 IpLen:20 DgmLen:60
Type:8  Code:0  ID:1   Seq:70  ECHO

03/29-18:21:36.517831  [**] [1:1000052:1] ICMP detected! [**] [Classification: Generic ICMP event] [Priority: 3] {ICMP} 192.168.153.1 -> 192.168.153.129
[**] [1:1000052:1] ICMP detected! [**]
[Classification: Generic ICMP event] [Priority: 3]
03/29-18:21:36.517862 192.168.153.129 -> 192.168.153.1
ICMP TTL:64 TOS:0x0 ID:15777 IpLen:20 DgmLen:60
Type:0  Code:0  ID:1  Seq:70  ECHO REPLY

03/29-18:21:36.517862  [**] [1:1000052:1] ICMP detected! [**] [Classification: Generic ICMP event] [Priority: 3] {ICMP} 192.168.153.129 -> 192.168.153.1
```

Step 2a:

student@student-virtual-machine: /var/log/snort

student@student-virtu... | student@student-virtu... | student@student-virtu...

```
student@student-virtual-machine:/var/log/snort$ ls -l /etc/snort/rules
total 1600
-rw-r--r-- 1 root root   5520 Dec  3  2021 attack-responses.rules
-rw-r--r-- 1 root root  17898 Dec  3  2021 backdoor.rules
-rw-r--r-- 1 root root   3862 Dec  3  2021 bad-traffic.rules
-rw-r--r-- 1 root root   7994 Dec  3  2021 chat.rules
-rw-r--r-- 1 root root  12759 Dec  3  2021 community-bot.rules
-rw-r--r-- 1 root root   1223 Dec  3  2021 community-deleted.rules
-rw-r--r-- 1 root root   2042 Dec  3  2021 community-dos.rules
-rw-r--r-- 1 root root   2176 Dec  3  2021 community-exploit.rules
-rw-r--r-- 1 root root    249 Dec  3  2021 community-ftp.rules
-rw-r--r-- 1 root root   1376 Dec  3  2021 community-game.rules
-rw-r--r-- 1 root root    689 Dec  3  2021 community-icmp.rules
-rw-r--r-- 1 root root   2777 Dec  3  2021 community-imap.rules
-rw-r--r-- 1 root root    948 Dec  3  2021 community-inappropriate.rules
-rw-r--r-- 1 root root    257 Dec  3  2021 community-mail-client.rules
-rw-r--r-- 1 root root   7837 Dec  3  2021 community-misc.rules
-rw-r--r-- 1 root root    621 Dec  3  2021 community-nntp.rules
-rw-r--r-- 1 root root    775 Dec  3  2021 community-oracle.rules
-rw-r--r-- 1 root root   1621 Dec  3  2021 community-policy.rules
-rw-r--r-- 1 root root   3551 Dec  3  2021 community-sip.rules
-rw-r--r-- 1 root root   2722 Dec  3  2021 community-smtp.rules
```

Step 2c:

- The five categories of rules that are most interesting are dns.rules, ftp.rules, smtp.rules, web-attacks.rules, sql.rules. These categories are interesting because these are some of the common services in an infrastructure.

Step 2d:

- The individual rule with the message “WEB Attacks bin/python access attempts” in web-attack.rules
- individual rule with the message “DNS zone transfer TCP” in dns.rules.
- The Individual rule with the message “ftp cwd root directory traversal traversal” in the ftp.rules
- The individual rule with the message “SMTP verify root” in the smtp.rules
- The individual rule with the message “MY-SQL/SMB sp_password password change” in the sql.rules
- These are some of interesting rules because I have seen attacks that can be related to theses attacks.

Step a:

```
student@student-virtual-machine:/etc/snort$ ls
attribute_table.dtd    community-sid-msg.map  gen-msg.map       rules       snort.debian.conf  unicode.map
classification.config  file_magic.conf        reference.config  snort.conf  threshold.conf
student@student-virtual-machine:/etc/snort$ sudo cp ./snort.conf ./snort3.conf
student@student-virtual-machine:/etc/snort$
```

Step 3b:

```
# that you can run multiple instances.

###################################################
# Step #1: Set the network variables.  For more information, see README.variables
###################################################

# Setup the network addresses you are protecting
#
# Note to Debian users: this value is overriden when starting
# up the Snort daemon through the init.d script by the
# value of DEBIAN_SNORT_HOME_NET s defined in the
# /etc/snort/snort.debian.conf configuration file
#
ipvar HOME_NET 192.168.153.0/24

# Set up the external network addresses. Leave as "any" in most situations
ipvar EXTERNAL_NET any
```

Step 3c:

```
           Using ZLIB Version: 1.2.11

           Rules Engine: SF_SNORT_DETECTION_ENGINE  Version 3.1  <Build 1>
           Preprocessor Object: SF_POP  Version 1.0  <Build 1>
           Preprocessor Object: SF_DCERPC2  Version 1.0  <Build 3>
           Preprocessor Object: SF_GTP  Version 1.1  <Build 1>
           Preprocessor Object: SF_SSH  Version 1.1  <Build 3>
           Preprocessor Object: SF_DNS  Version 1.1  <Build 4>
           Preprocessor Object: SF_MODBUS  Version 1.1  <Build 1>
           Preprocessor Object: SF_SSLPP  Version 1.1  <Build 4>
           Preprocessor Object: SF_IMAP  Version 1.0  <Build 1>
           Preprocessor Object: SF_FTPTELNET  Version 1.2  <Build 13>
           Preprocessor Object: SF_DNP3  Version 1.1  <Build 1>
           Preprocessor Object: SF_SIP  Version 1.1  <Build 1>
           Preprocessor Object: SF_SDF  Version 1.1  <Build 1>
           Preprocessor Object: SF_SMTP  Version 1.1  <Build 9>
           Preprocessor Object: SF_REPUTATION  Version 1.1  <Build 1>
           Preprocessor Object: appid  Version 1.1  <Build 5>
Commencing packet processing (pid=12564)
03/30-01:42:48.087901  [**] [1:1000052:1] ICMP detected! [**] [Classification: Generic ICMP event] [Priority: 3] {ICMP} 192.168.153.
1 -> 192.168.153.129
03/30-01:42:48.088161  [**] [1:1000052:1] ICMP detected! [**] [Classification: Generic ICMP event] [Priority: 3] {ICMP} 192.168.153.
129 -> 192.168.153.1
03/30-01:42:49.099224  [**] [1:1000052:1] ICMP detected! [**] [Classification: Generic ICMP event] [Priority: 3] {ICMP} 192.168.153.
1 -> 192.168.153.129
03/30-01:42:49.099255  [**] [1:1000052:1] ICMP detected! [**] [Classification: Generic ICMP event] [Priority: 3] {ICMP} 192.168.153.
129 -> 192.168.153.1
03/30-01:42:50.118163  [**] [1:1000052:1] ICMP detected! [**] [Classification: Generic ICMP event] [Priority: 3] {ICMP} 192.168.153.
1 -> 192.168.153.129
03/30-01:42:50.118193  [**] [1:1000052:1] ICMP detected! [**] [Classification: Generic ICMP event] [Priority: 3] {ICMP} 192.168.153.
129 -> 192.168.153.1
03/30-01:42:51.136152  [**] [1:1000052:1] ICMP detected! [**] [Classification: Generic ICMP event] [Priority: 3] {ICMP} 192.168.153.
1 -> 192.168.153.129
03/30-01:42:51.136193  [**] [1:1000052:1] ICMP detected! [**] [Classification: Generic ICMP event] [Priority: 3] {ICMP} 192.168.153.
129 -> 192.168.153.1
```

Step 3d:

Open | alert /var/log/snort | Save

```
[**] [1:1000052:1] ICMP detected! [**]
[Classification: Generic ICMP event] [Priority: 3]
03/29-18:21:35.505672 192.168.153.1 -> 192.168.153.129
ICMP TTL:128 TOS:0x0 ID:435 IpLen:20 DgmLen:60
Type:8  Code:0  ID:1   Seq:69  ECHO

03/29-18:21:35.505672  [**] [1:1000052:1] ICMP detected! [**] [Classification: Generic ICMP event] [Priority: 3] {ICMP} 192.168.153.1 -> 192.168.153.129
[**] [1:1000052:1] ICMP detected! [**]
[Classification: Generic ICMP event] [Priority: 3]
03/29-18:21:35.505705 192.168.153.129 -> 192.168.153.1
ICMP TTL:64 TOS:0x0 ID:15741 IpLen:20 DgmLen:60
Type:0  Code:0  ID:1  Seq:69  ECHO REPLY

03/29-18:21:35.505705  [**] [1:1000052:1] ICMP detected! [**] [Classification: Generic ICMP event] [Priority: 3] {ICMP} 192.168.153.129 -> 192.168.153.1
[**] [1:1000052:1] ICMP detected! [**]
[Classification: Generic ICMP event] [Priority: 3]
03/29-18:21:36.517831 192.168.153.1 -> 192.168.153.129
ICMP TTL:128 TOS:0x0 ID:436 IpLen:20 DgmLen:60
Type:8  Code:0  ID:1   Seq:70  ECHO

03/29-18:21:36.517831  [**] [1:1000052:1] ICMP detected! [**] [Classification: Generic ICMP event] [Priority: 3] {ICMP} 192.168.153.1 -> 192.168.153.129
[**] [1:1000052:1] ICMP detected! [**]
[Classification: Generic ICMP event] [Priority: 3]
03/29-18:21:36.517862 192.168.153.129 -> 192.168.153.1
ICMP TTL:64 TOS:0x0 ID:15777 IpLen:20 DgmLen:60
Type:0  Code:0  ID:1  Seq:70  ECHO REPLY

03/29-18:21:36.517862  [**] [1:1000052:1] ICMP detected! [**] [Classification: Generic ICMP event] [Priority: 3] {ICMP} 192.168.153.129 -> 192.168.153.1
[**] [1:1000052:1] ICMP detected! [**]
```

Step 3e:

snort.log.1711777353

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.153.1	192.168.153.129	ICMP	74	Echo (ping) request id=0x0
2	0.000260	192.168.153.129	192.168.153.1	ICMP	74	Echo (ping) reply id=0x0
3	1.011323	192.168.153.1	192.168.153.129	ICMP	74	Echo (ping) request id=0x0
4	1.011354	192.168.153.129	192.168.153.1	ICMP	74	Echo (ping) reply id=0x0
5	2.030262	192.168.153.1	192.168.153.129	ICMP	74	Echo (ping) request id=0x0
6	2.030292	192.168.153.129	192.168.153.1	ICMP	74	Echo (ping) reply id=0x0
7	3.048251	192.168.153.1	192.168.153.129	ICMP	74	Echo (ping) request id=0x0
8	3.048292	192.168.153.129	192.168.153.1	ICMP	74	Echo (ping) reply id=0x0

Lab Analysis:

1. The three modes are packet sniffer mode, packet logger mode, network intrusion detection system mode
2. The mostly used mode is network intrusion detection system mode
3. Some categories of rules are dns, web attacks, ftp rules and etc.

Key term quiz:

1. Rules
2. Configuration
3. log