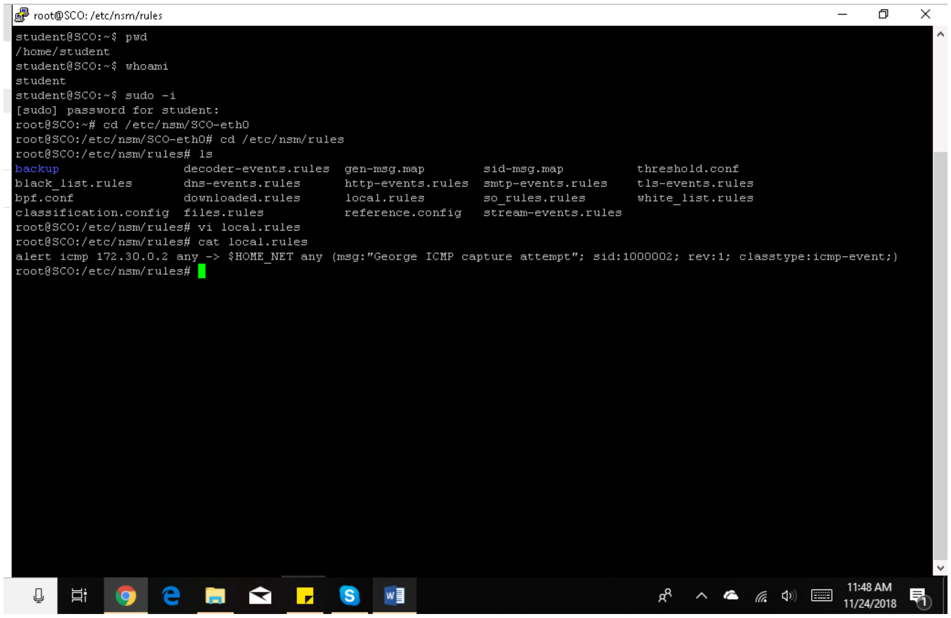
MARYMOUNT UNIVERSITY

Assignment: IT557; Monitoring, Auditing, and Penetration Testing
Assigned: Nov. 26, 2018
Instructor: Professor Ali Bicak
Student Name: George Boakye

LAB REPORT FILE (LAB10)

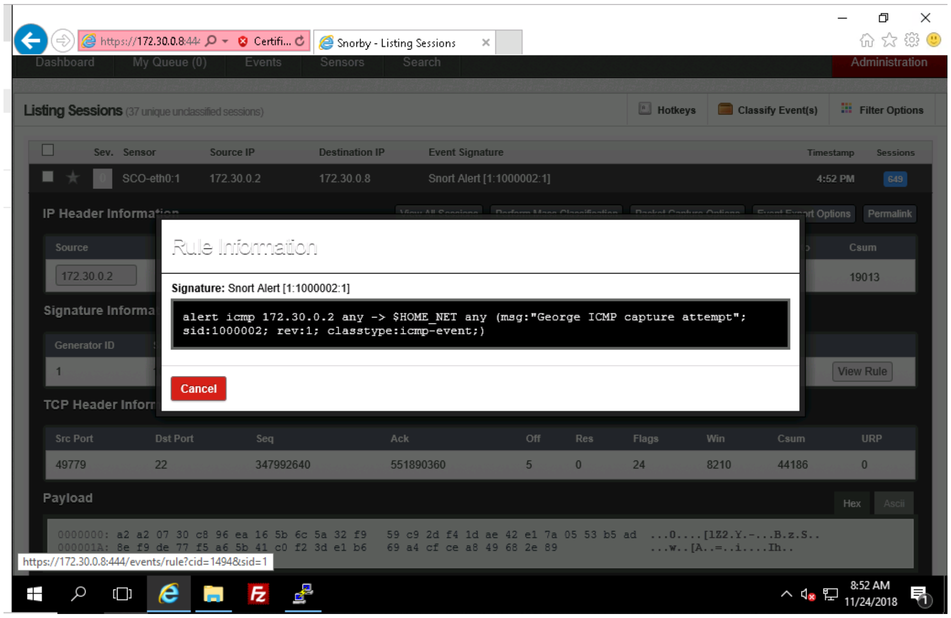
SECTION 3

Part 1A: Contents of local.rules showing ICMP



```
student@SCO:~$ pwd
/home/student
student@SCO:~$ whoami
student
student@SCO:~$ sudo -i
[sudo] password for student:
root@SCO:~# cd /etc/nsm/SCO-eth0
root@SCO:/etc/nsm/SCO-eth0# cd /etc/nsm/rules
root@SCO:/etc/nsm/rules# ls
backup                 decoder-events.rules  gen-msg.map        sid-msg.map          threshold.conf
black_list.rules       dns-events.rules      http-events.rules  smtp-events.rules    tls-events.rules
bpf.conf               downloaded.rules      local.rules        so_rules.rules       white_list.rules
classification.config  files.rules           reference.config   stream-events.rules
root@SCO:/etc/nsm/rules# vi local.rules
root@SCO:/etc/nsm/rules# cat local.rules
alert icmp 172.30.0.2 any -> $HOME_NET any (msg:"George ICMP capture attempt"; sid:1000002; rev:1; classtype:icmp-event;)
root@SCO:/etc/nsm/rules# 
```

Part 1B: Created ICMP Alert Rule Information



Listing Sessions (37 unique unclassified sessions)

	Sev.	Sensor	Source IP	Destination IP	Event Signature	Timestamp	Sessions
□ ★	0	SCO-eth0:1	172.30.0.2	172.30.0.8	Snort Alert [1:1000002:1]	4:52 PM	649

Source: 172.30.0.2 — Csum: 19013

Generator ID: 1

Rule Information

Signature: Snort Alert [1:1000002:1]

```
alert icmp 172.30.0.2 any -> $HOME_NET any (msg:"George ICMP capture attempt";
sid:1000002; rev:1; classtype:icmp-event;)
```

Src Port	Dst Port	Seq	Ack	Off	Res	Flags	Win	Csum	URP
49779	22	347992640	551890360	5	0	24	8210	44186	0

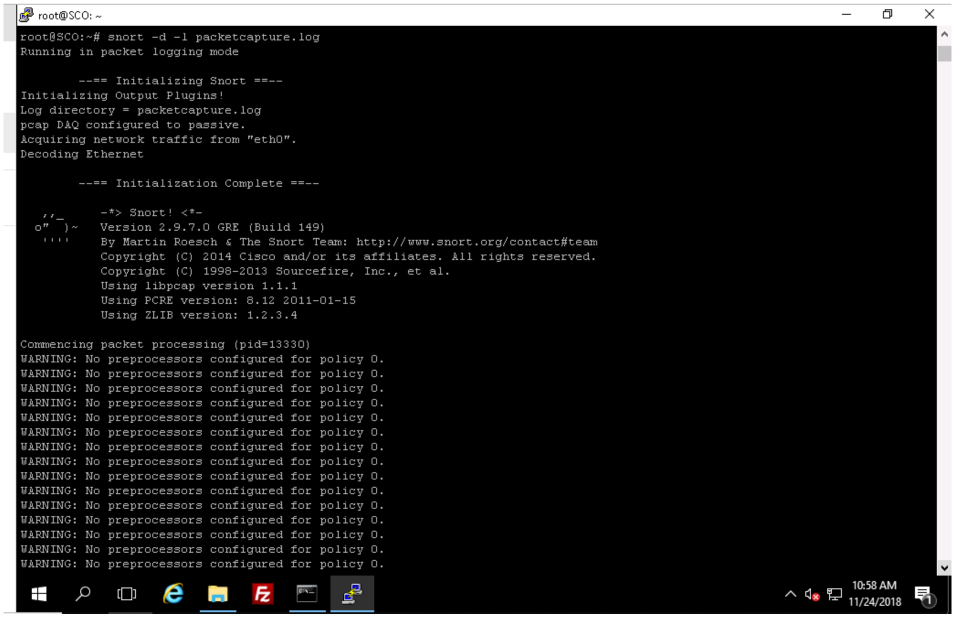
Payload

```
0000000: a2 a2 07 30 c8 96 ea 16 5b 6c 5a 32 f9   59 c9 2d f4 1d ae 42 e1 7a 05 53 b5 ad  ...0....[lZ2.Y.-...B.z.S..
000001A: 8e f9 de 77 f5 a6 5b 41 c0 f2 3d e1 b6   69 a4 cf ce a8 49 68 2e 89              ...w..[A..=..i....Ih..
```

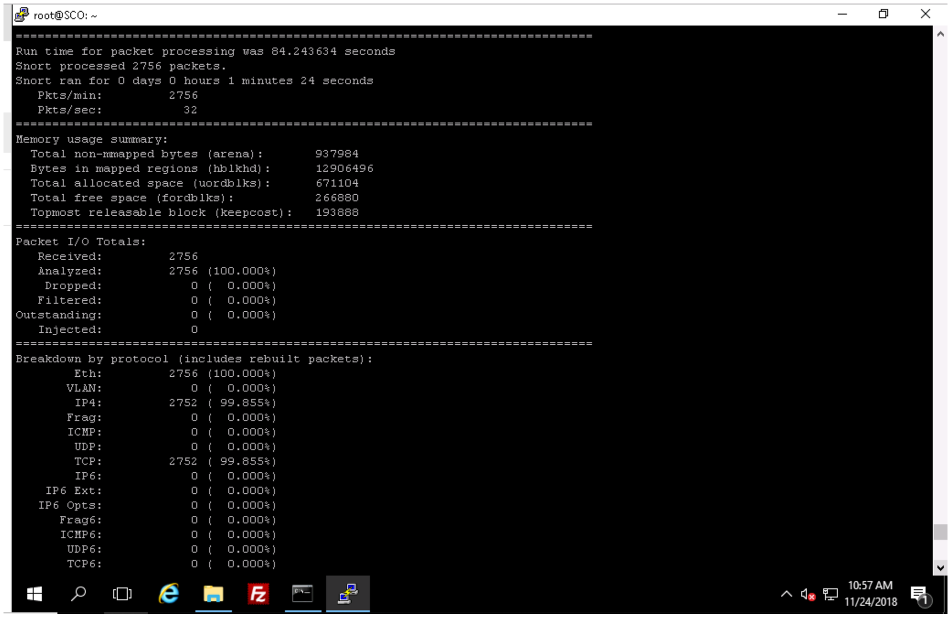
https://172.30.0.8:444/events/rule?cid=1494&sid=1

Part 2

Command ‘snort -d -l packetcapture.log’ logging active packets in ‘packetcapture.log’

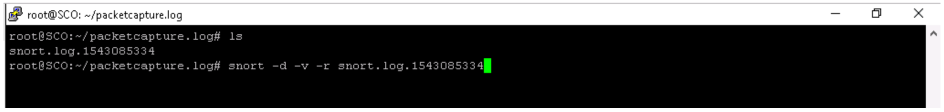


```
root@SCO:~# snort -d -l packetcapture.log
Running in packet logging mode

        --== Initializing Snort ==--
Initializing Output Plugins!
Log directory = packetcapture.log
pcap DAQ configured to passive.
Acquiring network traffic from "eth0".
Decoding Ethernet

        --== 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 1.1.1
           Using PCRE version: 8.12 2011-01-15
           Using ZLIB version: 1.2.3.4

Commencing packet processing (pid=13330)
WARNING: No preprocessors configured for policy 0.
WARNING: No preprocessors configured for policy 0.
WARNING: No preprocessors configured for policy 0.
WARNING: No preprocessors configured for policy 0.
WARNING: No preprocessors configured for policy 0.
WARNING: No preprocessors configured for policy 0.
WARNING: No preprocessors configured for policy 0.
WARNING: No preprocessors configured for policy 0.
WARNING: No preprocessors configured for policy 0.
WARNING: No preprocessors configured for policy 0.
WARNING: No preprocessors configured for policy 0.
WARNING: No preprocessors configured for policy 0.
WARNING: No preprocessors configured for policy 0.
WARNING: No preprocessors configured for policy 0.
WARNING: No preprocessors configured for policy 0.
```

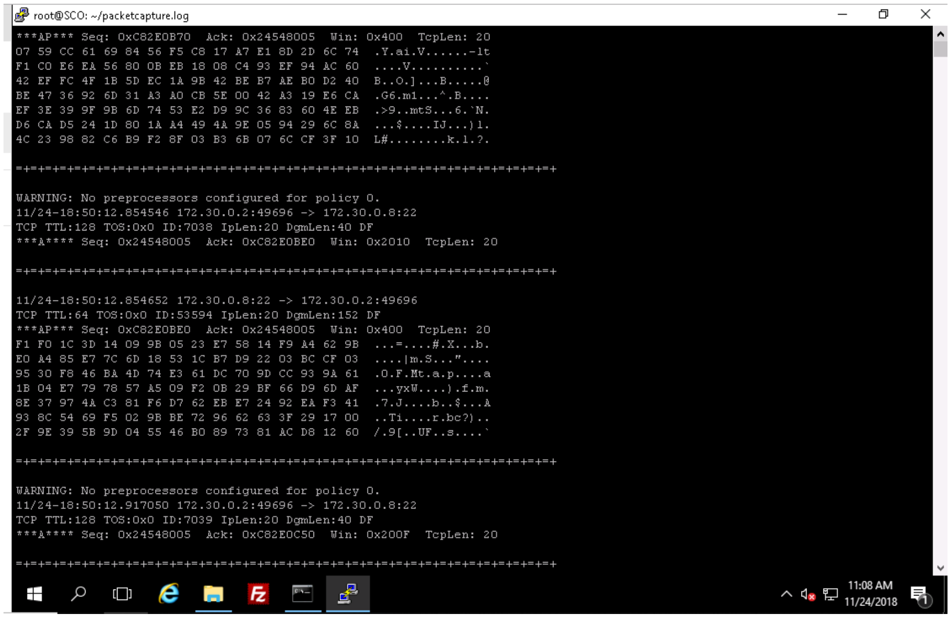


```
===============================================================================
Run time for packet processing was 84.243634 seconds
Snort processed 2756 packets.
Snort ran for 0 days 0 hours 1 minutes 24 seconds
   Pkts/min:         2756
   Pkts/sec:           32
===============================================================================
Memory usage summary:
  Total non-mmapped bytes (arena):       937984
  Bytes in mapped regions (hblkhd):      12906496
  Total allocated space (uordblks):      671104
  Total free space (fordblks):           266880
  Topmost releasable block (keepcost):   193888
===============================================================================
Packet I/O Totals:
   Received:         2756
   Analyzed:         2756 (100.000%)
    Dropped:            0 (  0.000%)
   Filtered:            0 (  0.000%)
Outstanding:            0 (  0.000%)
   Injected:            0
===============================================================================
Breakdown by protocol (includes rebuilt packets):
        Eth:         2756 (100.000%)
       VLAN:            0 (  0.000%)
        IP4:         2752 ( 99.855%)
       Frag:            0 (  0.000%)
       ICMP:            0 (  0.000%)
        UDP:            0 (  0.000%)
        TCP:         2752 ( 99.855%)
        IP6:            0 (  0.000%)
    IP6 Ext:            0 (  0.000%)
   IP6 Opts:            0 (  0.000%)
      Frag6:            0 (  0.000%)
      ICMP6:            0 (  0.000%)
       UDP6:            0 (  0.000%)
       TCP6:            0 (  0.000%)
```

The command 'snort -d -v -r snort.log.1543085334' printed the captured data below from 'packetcapture.log'



```
root@SCO:~/packetcapture.log# ls
snort.log.1543085334
root@SCO:~/packetcapture.log# snort -d -v -r snort.log.1543085334
```



```
***AP*** Seq: 0xC82E0B70  Ack: 0x24548005  Win: 0x400  TcpLen: 20
07 59 CC 61 69 84 56 F5 C8 17 A7 E1 8D 2D 6C 74  .Y.ai.V......-lt
F1 C0 E6 EA 56 80 0B EB 18 08 C4 93 EF 94 AC 60  ....V..........`
42 EF FC 4F 1B 5D EC 1A 9B 42 BE B7 AE B0 D2 40  B..O.]...B.....@
BE 47 36 92 6D 31 A3 A0 CB 5E 00 42 A3 19 E6 CA  .G6.m1...^.B....
EF 3E 39 9F 9B 6D 74 53 E2 D9 9C 36 83 60 4E EB  .>9..mtS...6.`N.
D6 CA D5 24 1D 80 1A A4 49 4A 9E 05 94 29 6C 8A  ...$....IJ...)l.
4C 23 98 82 C6 B9 F2 8F 03 B3 6B 07 6C CF 3F 10  L#........k.l.?.

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

WARNING: No preprocessors configured for policy 0.
11/24-18:50:12.854546 172.30.0.2:49696 -> 172.30.0.8:22
TCP TTL:128 TOS:0x0 ID:7038 IpLen:20 DgmLen:40 DF
***A**** Seq: 0x24548005  Ack: 0xC82E0BE0  Win: 0x2010  TcpLen: 20

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

11/24-18:50:12.854652 172.30.0.8:22 -> 172.30.0.2:49696
TCP TTL:64 TOS:0x0 ID:53594 IpLen:20 DgmLen:152 DF
***AP*** Seq: 0xC82E0BE0  Ack: 0x24548005  Win: 0x400  TcpLen: 20
F1 F0 1C 3D 14 09 9B 05 23 E7 58 14 F9 A4 62 9B  ...=....#.X...b.
E0 A4 85 E7 7C 6D 18 53 1C B7 D9 22 03 BC CF 03  ....|m.S..."....
95 30 F8 46 BA 4D 74 E3 61 DC 70 9D CC 93 9A 61  .0.F.Mt.a.p....a
1B 04 E7 79 78 57 A5 09 F2 0B 29 BF 66 D9 6D AF  ...yxW....).f.m.
8E 37 97 4A C3 81 F6 D7 62 EB E7 24 92 EA F3 41  .7.J....b..$...A
93 8C 54 69 F5 02 9B BE 72 96 62 63 3F 29 17 00  ..Ti....r.bc?)..
2F 9E 39 5B 9D 04 55 46 B0 89 73 81 AC D8 12 60  /.9[..UF..s....`

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

WARNING: No preprocessors configured for policy 0.
11/24-18:50:12.917050 172.30.0.2:49696 -> 172.30.0.8:22
TCP TTL:128 TOS:0x0 ID:7039 IpLen:20 DgmLen:40 DF
***A**** Seq: 0x24548005  Ack: 0xC82E0C50  Win: 0x200F  TcpLen: 20

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
```

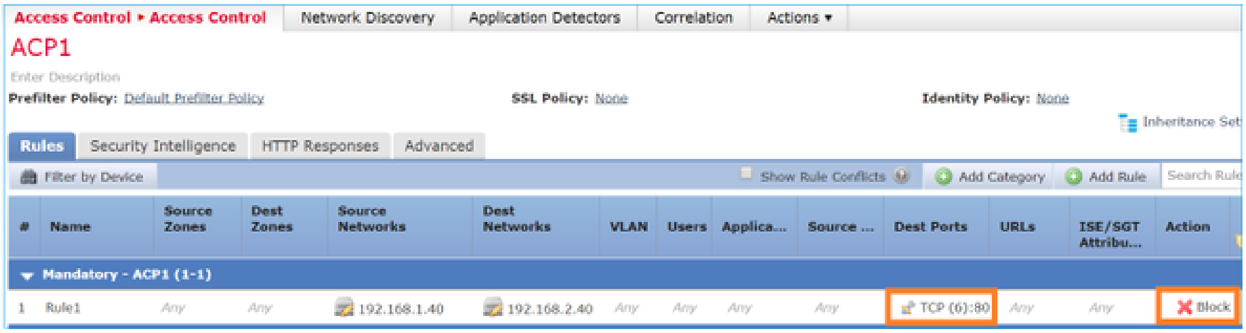
Part 3

Deployed policy in Snort:

268435461 deny any 192.168.1.40 32 any any 192.168.2.40 32 80 any 6

The Access Control Policy contains a Block rule (Destination Port TCP 80) as shown in the below figure. ***268435461*** is a rule-id

Fig. 1: Snort script for ACL policy in Cisco



ACP1

Prefilter Policy: Default Prefilter Policy **SSL Policy:** None **Identity Policy:** None

#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN	Users	Applica...	Source ...	Dest Ports	URLs	ISE/SGT Attribu...	Action
▾ Mandatory - ACP1 (1-1)													
1	Rule1	Any	Any	192.168.1.40	192.168.2.40	Any	Any	Any	Any	TCP (6):80	Any	Any	✕ Block

Source: Adapted from Cisco

When host-A (192.168.1.40) tries to open an HTTP session to host-B (192.168.2.40) the TCP synchronize (SYN) packets are dropped without reaching the Snort Engine or the destination (Zafeiroudis & Klauzova, 2018).

Having such a script in writing ACL policy does not overwhelm the snort engine with excessive data. By dropping packets that are to be denied before reaching the destination frees the systems from possible successful attacks.

Reference

Zafeiroudis, M., & Klauzova, V. (2018, September 28). *Clarify Firepower Threat Defense Access Control Policy Rule Actions.* Retrieved from Cisco: https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/212321-clarify-the-firepower-threat-defense-acc.html