SEC290 Fundamentals of Infrastructure Security

Developed by James Garlie

DeVry University

February 2023

Introduction

This project covers fundamentals of infrastructure security. It includes activities such as configuring firewall rules, deploying Snort sensors for network intrusion detection, exploring SSL encryption, analyzing traffic to detect attacks, exploiting Microsoft vulnerabilities, and conducting live memory analysis.

The presentation concludes with Challenges, Career Skills obtained, a Conclusion, and References.

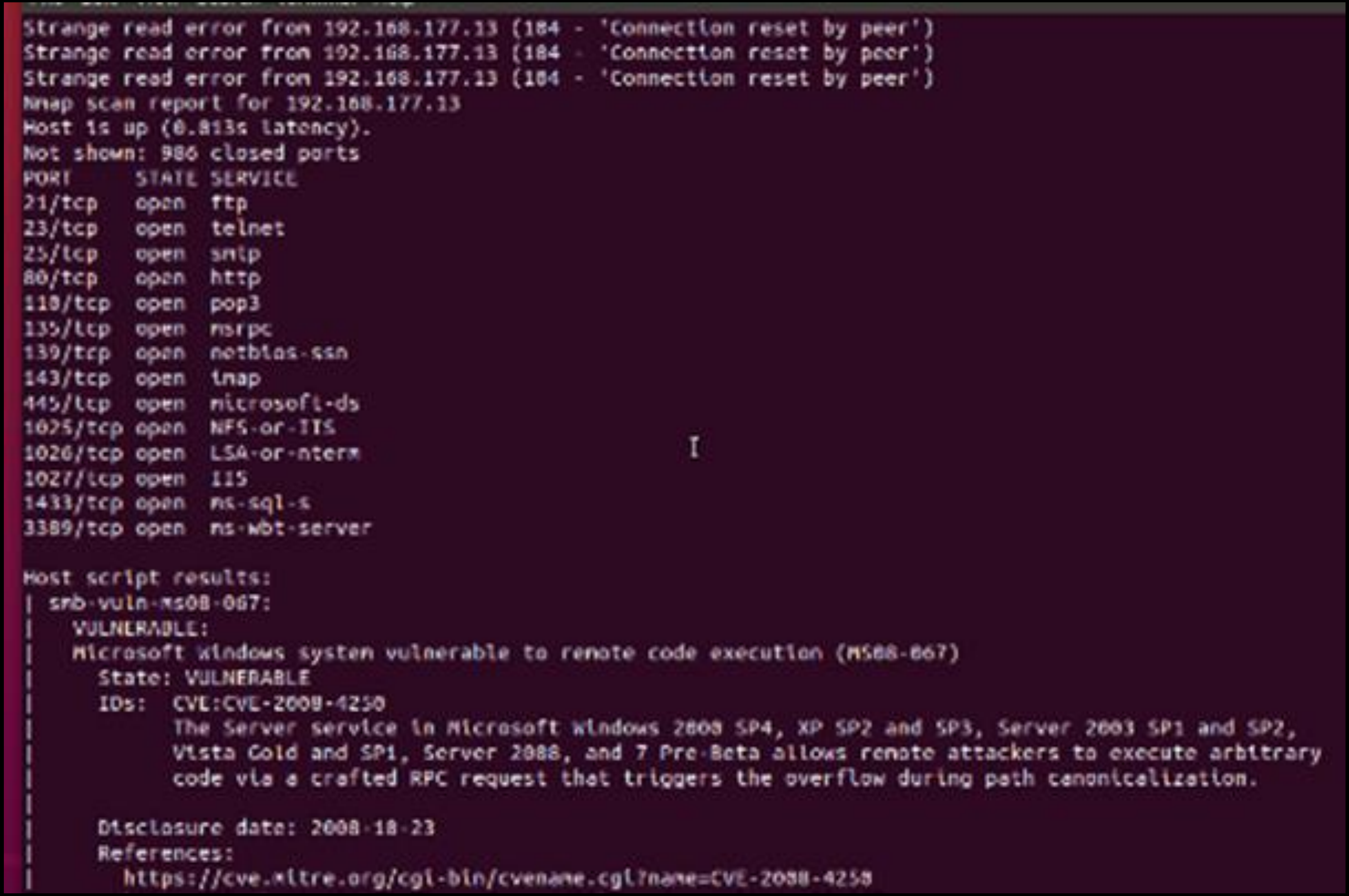
SEC290
Module 1

Manual Vulnerability Analysis (on a test VM network)

The next three slides show:
1) Microsoft Windows Bulletin MS08-067 vulnerability,
2) Microsoft Windows Bulletin MS17-010 vulnerability; and,
3) Meterpreter Session Command Output.

Microsoft Windows Bulletin MS08-067 vulnerability

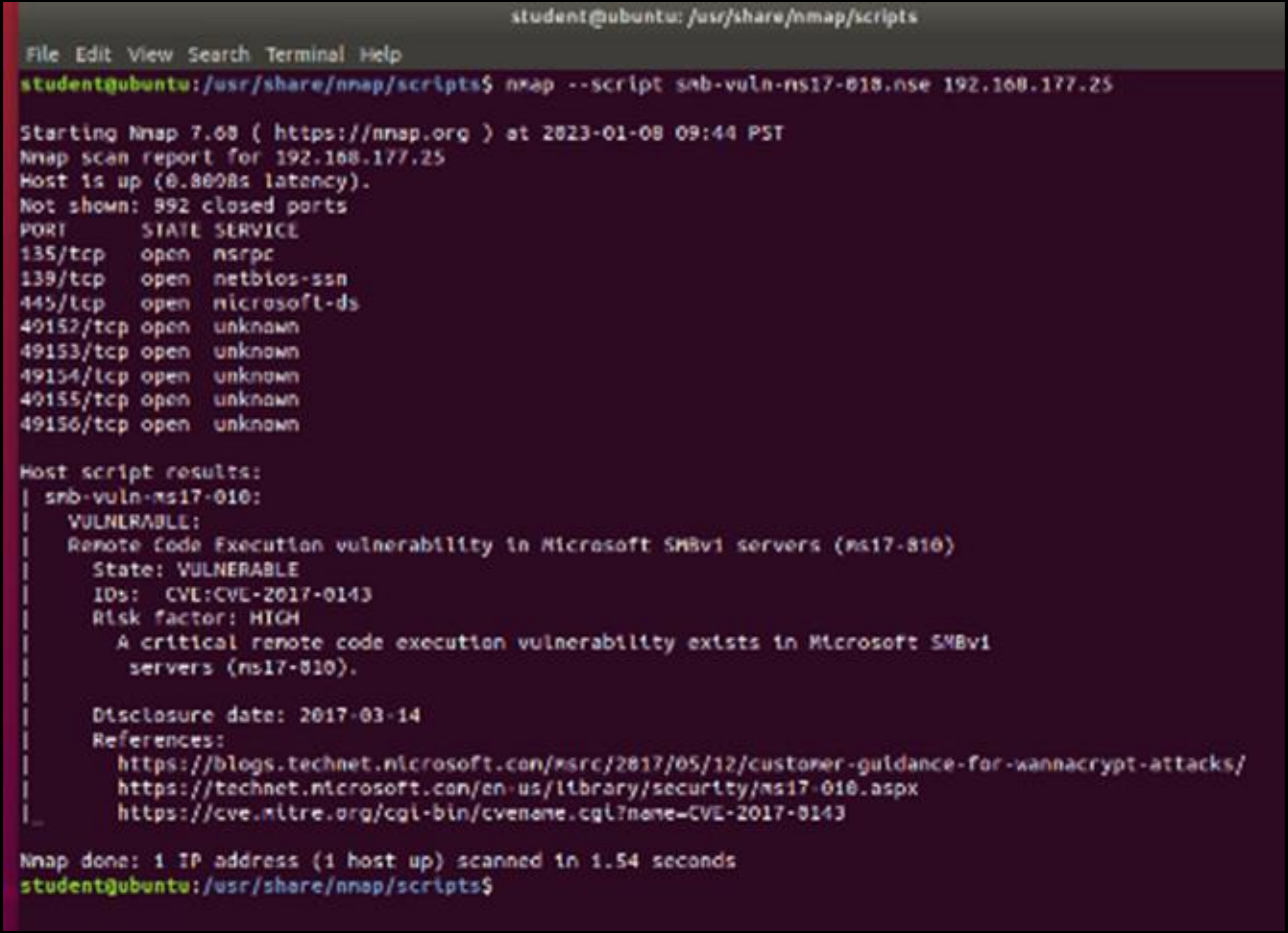
This screenshot shows that a vulnerability exists on the test VM.



```
Strange read error from 192.168.177.13 (104 - 'Connection reset by peer')
Strange read error from 192.168.177.13 (104 - 'Connection reset by peer')
Strange read error from 192.168.177.13 (104 - 'Connection reset by peer')
Nmap scan report for 192.168.177.13
Host is up (0.013s latency).
Not shown: 986 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
23/tcp   open  telnet
25/tcp   open  smtp
80/tcp   open  http
110/tcp  open  pop3
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
143/tcp  open  imap
445/tcp  open  microsoft-ds
1025/tcp open  NFS-or-IIS
1026/tcp open  LSA-or-nterm
1027/tcp open  IIS
1433/tcp open  ms-sql-s
3389/tcp open  ms-wbt-server

Host script results:
| smb-vuln-ms08-067:
|   VULNERABLE:
|   Microsoft Windows system vulnerable to remote code execution (MS08-067)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2008-4250
|           The Server service in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP1 and SP2,
|           Vista Gold and SP1, Server 2008, and 7 Pre-Beta allows remote attackers to execute arbitrary
|           code via a crafted RPC request that triggers the overflow during path canonicalization.
|
|     Disclosure date: 2008-10-23
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4250
```

Microsoft Windows Bulletin MS17-010 vulnerability

This screenshot shows that a vulnerability exists on the test VM.

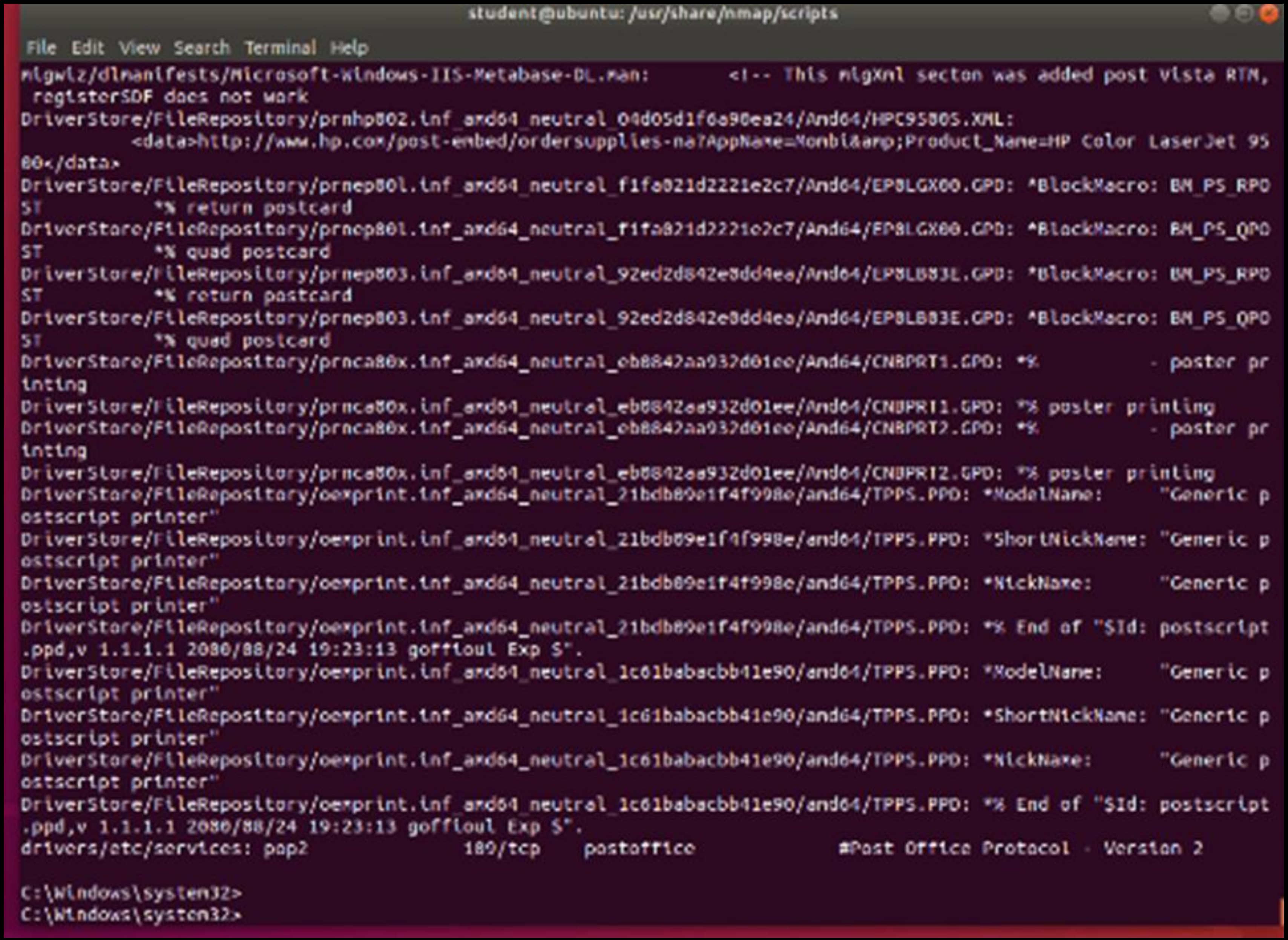


student@ubuntu: /usr/share/nmap/scripts
File Edit View Search Terminal Help

```
student@ubuntu:/usr/share/nmap/scripts$ nmap --script smb-vuln-ms17-010.nse 192.168.177.25

Starting Nmap 7.60 ( https://nmap.org ) at 2023-01-08 09:44 PST
Nmap scan report for 192.168.177.25
Host is up (0.0098s latency).
Not shown: 992 closed ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown

Host script results:
| smb-vuln-ms17-010:
|   VULNERABLE:
|   Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2017-0143
|     Risk factor: HIGH
|       A critical remote code execution vulnerability exists in Microsoft SMBv1
|        servers (ms17-010).
|
|     Disclosure date: 2017-03-14
|     References:
|       https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
|       https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143

Nmap done: 1 IP address (1 host up) scanned in 1.54 seconds
student@ubuntu:/usr/share/nmap/scripts$
```

Meterpreter session command output

This screenshot shows the output of the meterpreter session commands.



student@ubuntu: /usr/share/nmap/scripts
File Edit View Search Terminal Help

```
migwiz/dlmanifests/Microsoft-Windows-IIS-Metabase-DL.man:       <!-- This migXml secton was added post Vista RTM,
 registerSDF does not work
DriverStore/FileRepository/prnhp002.inf_amd64_neutral_04d05d1f6a98ea24/Amd64/HPC9500S.XML:
          <data>http://www.hp.com/post-embed/ordersupplies-na?AppName=Nonbi&amp;Product_Name=HP Color LaserJet 95
00</data>
DriverStore/FileRepository/prnep00l.inf_amd64_neutral_f1fa021d2221e2c7/Amd64/EP8LGX00.GPD: *BlockMacro: BM_PS_RPO
ST          *% return postcard
DriverStore/FileRepository/prnep00l.inf_amd64_neutral_f1fa021d2221e2c7/Amd64/EP8LGX00.GPD: *BlockMacro: BM_PS_QPO
ST          *% quad postcard
DriverStore/FileRepository/prnep003.inf_amd64_neutral_92ed2d842e0dd4ea/Amd64/EP8LB03L.GPD: *BlockMacro: BM_PS_RPO
ST          *% return postcard
DriverStore/FileRepository/prnep003.inf_amd64_neutral_92ed2d842e0dd4ea/Amd64/EP8LB03E.GPD: *BlockMacro: BM_PS_QPO
ST          *% quad postcard
DriverStore/FileRepository/prnca00x.inf_amd64_neutral_eb8842aa932d01ee/Amd64/CNBPRT1.GPD: *%              - poster pr
inting
DriverStore/FileRepository/prnca00x.inf_amd64_neutral_eb8842aa932d01ee/Amd64/CNBPRT1.GPD: *% poster printing
DriverStore/FileRepository/prnca00x.inf_amd64_neutral_eb8842aa932d01ee/Amd64/CNBPRT2.GPD: *%              - poster pr
inting
DriverStore/FileRepository/prnca00x.inf_amd64_neutral_eb8842aa932d01ee/Amd64/CNBPRT2.GPD: *% poster printing
DriverStore/FileRepository/oemprint.inf_amd64_neutral_21bdb89e1f4f998e/amd64/TPPS.PPD: *ModelName:     "Generic p
ostscript printer"
DriverStore/FileRepository/oemprint.inf_amd64_neutral_21bdb89e1f4f998e/amd64/TPPS.PPD: *ShortNickName: "Generic p
ostscript printer"
DriverStore/FileRepository/oemprint.inf_amd64_neutral_21bdb89e1f4f998e/amd64/TPPS.PPD: *NickName:      "Generic p
ostscript printer"
DriverStore/FileRepository/oemprint.inf_amd64_neutral_21bdb89e1f4f998e/amd64/TPPS.PPD: *% End of "$Id: postscript
.ppd,v 1.1.1.1 2000/08/24 19:23:13 goffioul Exp $".
DriverStore/FileRepository/oemprint.inf_amd64_neutral_1c61babacbb41e90/amd64/TPPS.PPD: *ModelName:     "Generic p
ostscript printer"
DriverStore/FileRepository/oemprint.inf_amd64_neutral_1c61babacbb41e90/amd64/TPPS.PPD: *ShortNickName: "Generic p
ostscript printer"
DriverStore/FileRepository/oemprint.inf_amd64_neutral_1c61babacbb41e90/amd64/TPPS.PPD: *NickName:      "Generic p
ostscript printer"
DriverStore/FileRepository/oemprint.inf_amd64_neutral_1c61babacbb41e90/amd64/TPPS.PPD: *% End of "$Id: postscript
.ppd,v 1.1.1.1 2000/08/24 19:23:13 goffioul Exp $".
drivers/etc/services: pop2              109/tcp    postoffice             #Post Office Protocol - Version 2

C:\Windows\system32>
C:\Windows\system32>
```

SEC290
Module 2

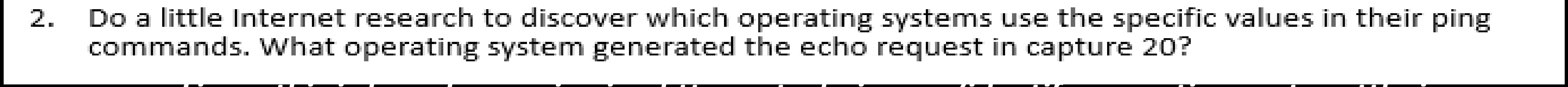
Intrusion Analysis using Wireshark

The next two slides show a Basic Attack Analysis.

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?

   64 for 20 and 128 for 22

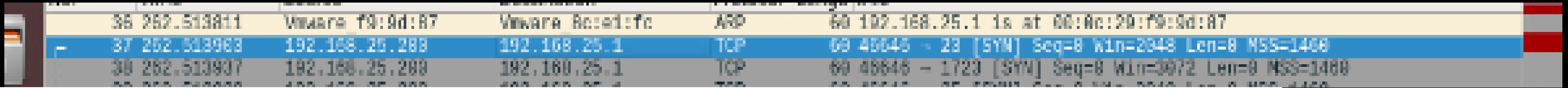


2. Do a little Internet research to discover which operating systems use the specific values in their ping commands. What operating system generated the echo request in capture 20?

   Linux, this is based on reviewing https:ostechnix.com/identify-operating-system-ttl-ping

3. Review packet no. 37 and beyond, what do you think is taking place here? ____________________

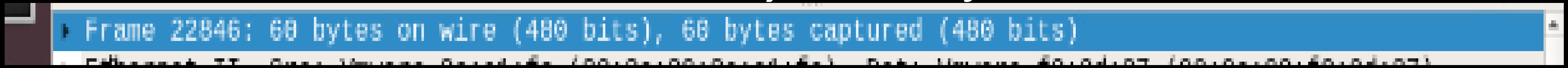
   a DDoS attack because there are multiple SYN packets being sent without waiting for an ACK. You can see the request is repeated in lines 38, 39 and probably the lines below as well.



```
36 252.513811  Vmware_f9:9d:87  Vmware_8c:e1:fc  ARP  60 192.168.25.1 is at 00:0c:29:f9:9d:87
37 252.513963  192.168.25.200   192.168.25.1     TCP  60 46646 → 23 [SYN] Seq=0 Win=2048 Len=0 MSS=1460
38 252.513937  192.168.25.200   192.168.25.1     TCP  60 46646 → 1723 [SYN] Seq=0 Win=3072 Len=0 MSS=1460
```

4. Look at capture 22846. What is suspicious about the flag settings in this packet?

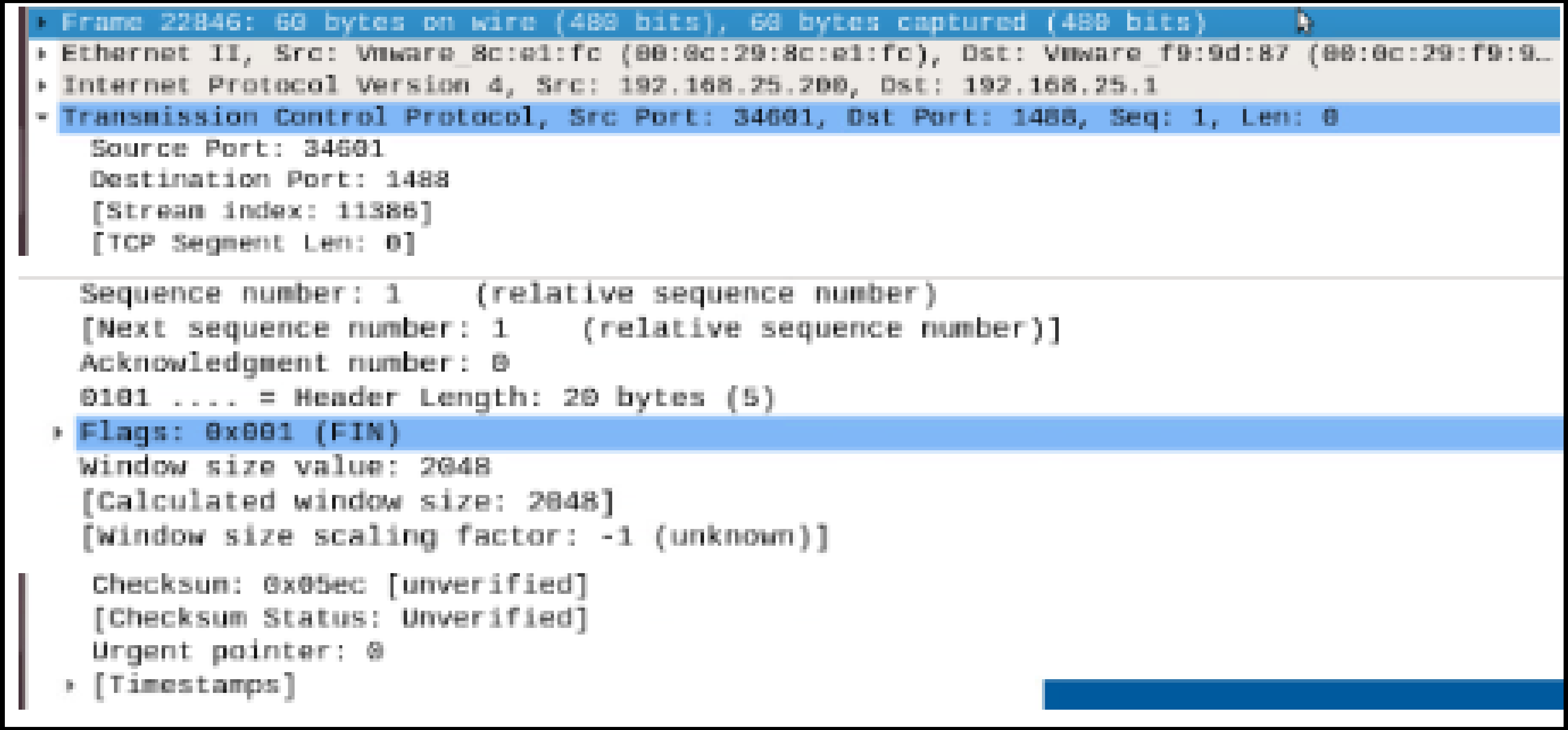
   The flag represents an Urgent Pointer and what is suspicious is that the checksum doesn’t match which is why it is unverified



```
▸ Frame 22846: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
```

(4 and 5 with capture 22846 continued on next slide)

This is the capture from 22846



```
▸ Frame 22846: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
▸ Ethernet II, Src: Vmware_8c:e1:fc (00:0c:29:8c:e1:fc), Dst: Vmware_f9:9d:87 (00:0c:29:f9:9…
▸ Internet Protocol Version 4, Src: 192.168.25.200, Dst: 192.168.25.1
▾ Transmission Control Protocol, Src Port: 34601, Dst Port: 1488, Seq: 1, Len: 0
    Source Port: 34601
    Destination Port: 1488
    [Stream index: 11386]
    [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: 0x001 (FIN)
   Window size value: 2048
   [Calculated window size: 2048]
   [Window size scaling factor: -1 (unknown)]
    Checksum: 0x05ec [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
  ▸ [Timestamps]
```

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

192.188.25.200 or 192.168.25.1

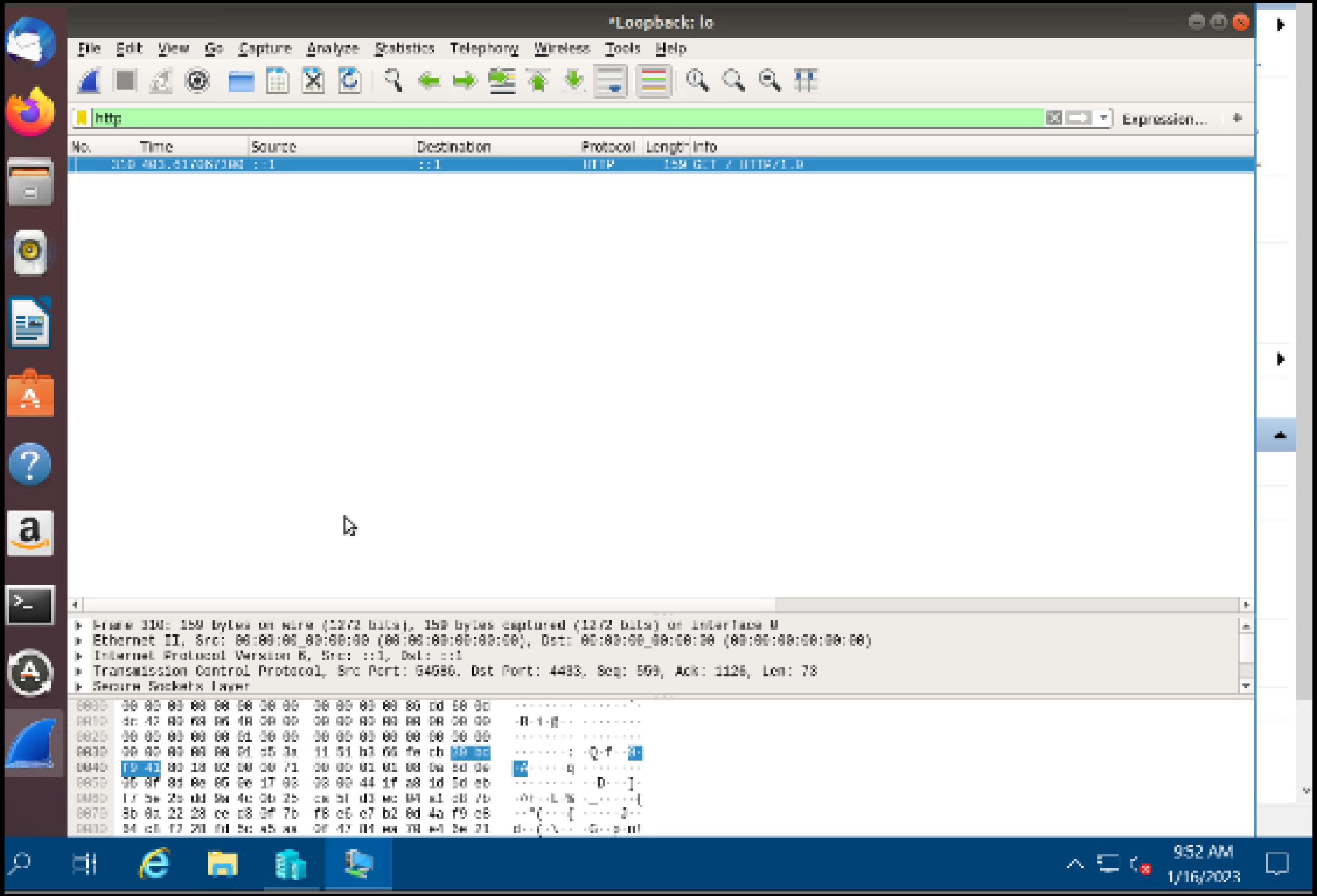
SEC290
Module 3

Open SSL

The next two slides show:
1) Creating and testing an SSL/TLS file; and,
2) The GET request and the decrypted SSL stream.

Creating and testing an SSL/TLS file

This screenshot shows the output of the GET request in the Info column.



*Loopback: lo
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression…
9:52 AM
1/16/2023

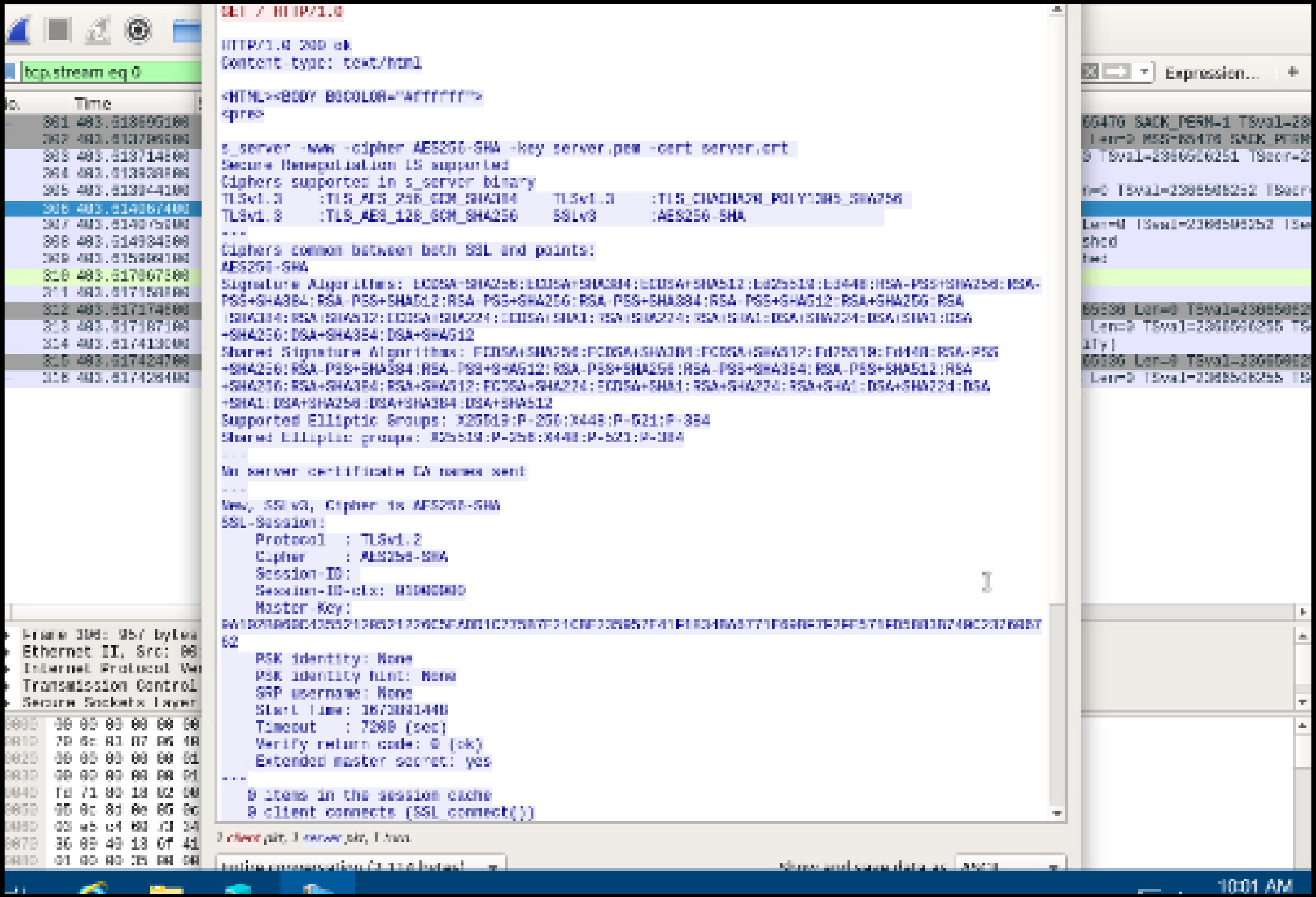
Display filter: http

```
No.   Time               Source   Destination   Protocol   Length   Info
  310 403.817087300      ::1      ::1           HTTP       159      GET / HTTP/1.0
```

```
▸ Frame 310: 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: 54586, Dst Port: 4433, Seq: 559, Ack: 1126, Len: 73
▸ Secure Sockets Layer
```

Creating and testing an SSL/TLS file cont'd

This screenshot sows the output of the decrypted SSL stream.



```
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:
[illegible]
62
    PSK identity: None
    PSK identity hint: None
    SRP username: None
    Start Time: 1673881448
    Timeout   : 7200 (sec)
    Verify return code: 0 (ok)
    Extended master secret: yes
---
   0 items in the session cache
   0 client connects (SSL_connect())
```

1 client pkt, 1 server pkt, 1 turn.

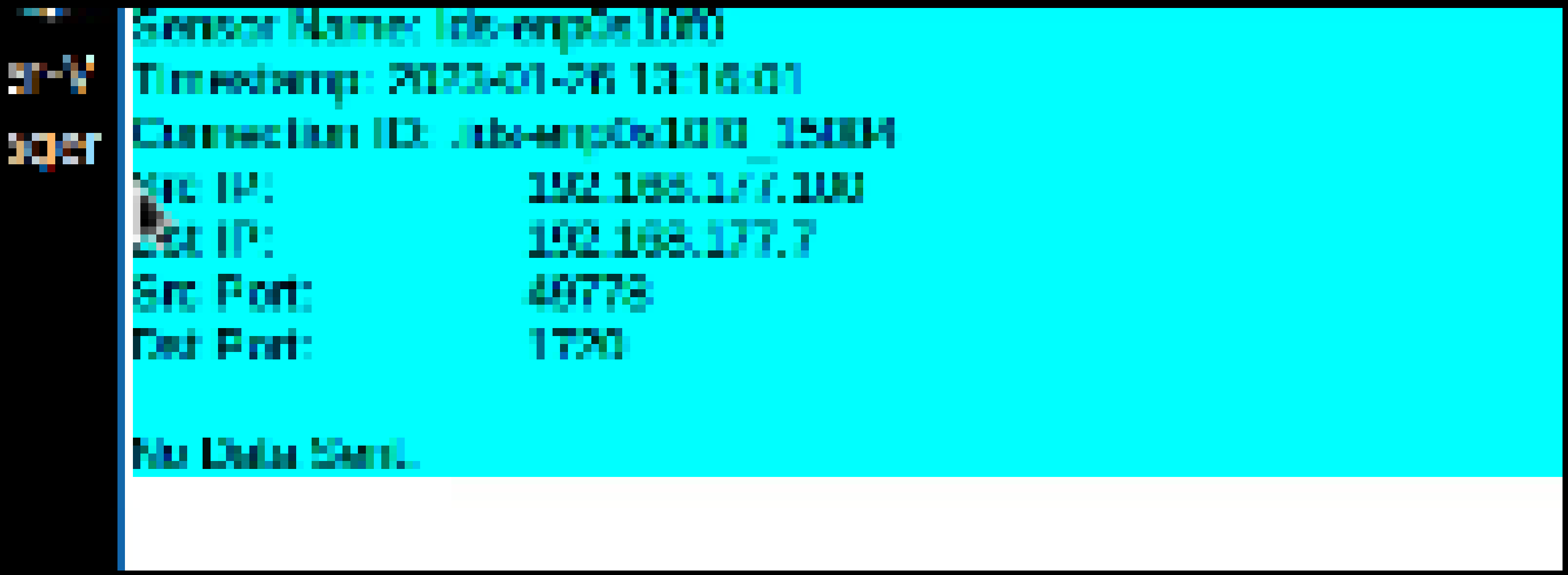
SEC290
Module 4

Snort (open-source network intrusion detection system)

The next four slides show:
1) Testing Snort rules showing the transcript of a XMAS scan alert,
2) the TCP packets generated by the XMAS scan,
3) the ping activity alert; and,
4) the ICMP packets generated by the ping activity.

Testing Snort rules

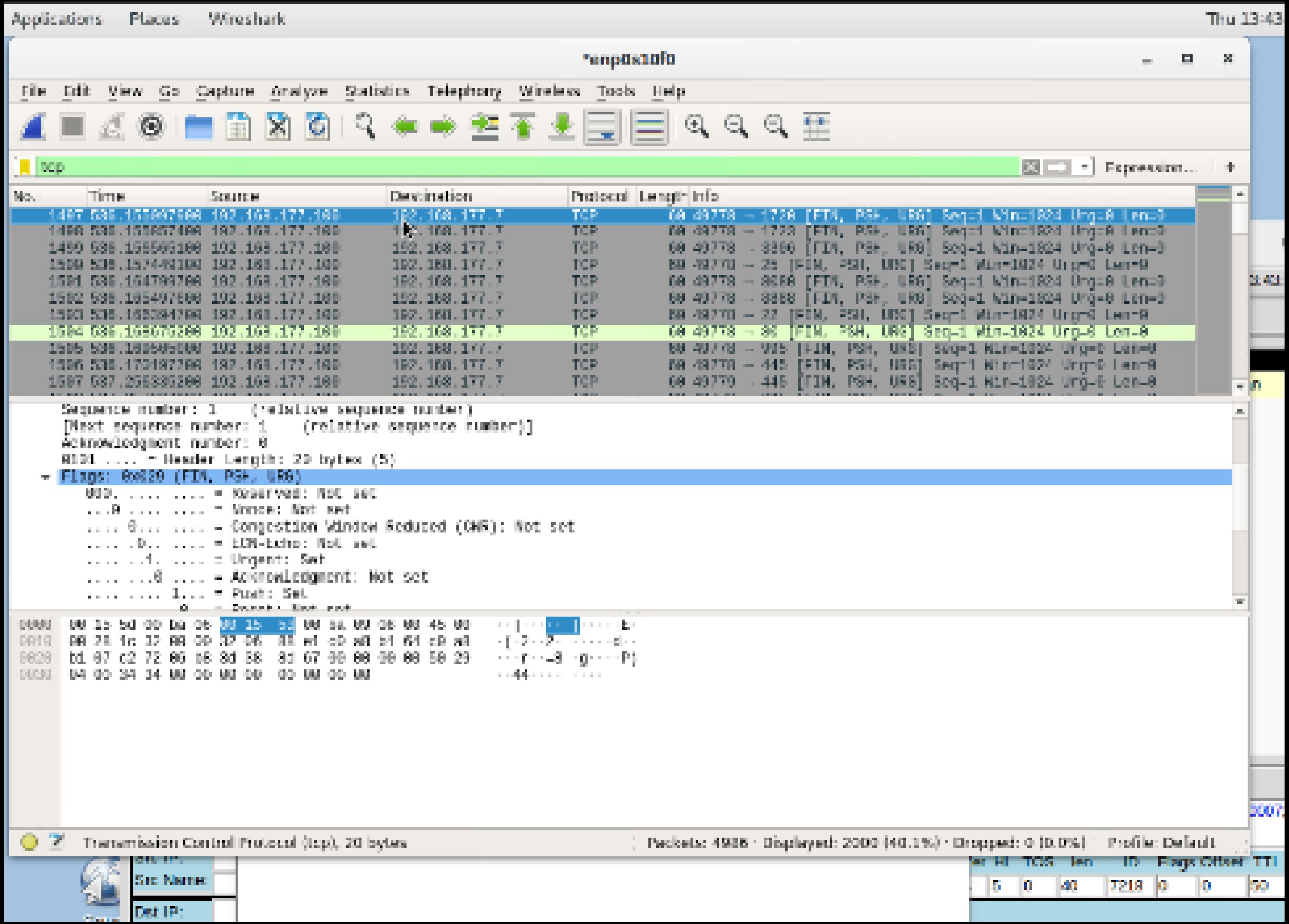
This is a screenshot of the output showing the transcript of a XMAS scan alert.



```
Sensor Name: ids-enp0s1000
Timestamp: 2023-01-26 13:16:01
Connection ID: ids-enp0s1000_15004
Src IP:                 192.168.177.100
Dst IP:                 192.168.177.7
Src Port:               40778
Dst Port:               1720


No Data Sent.
```

Testing Snort rules cont’d

This screenshot shows the TCP packets generated by the XMAS scan.



```
No.   Time           Source           Destination     Protocol Length Info
 1497 536.155997600 192.168.177.180 192.168.177.7   TCP      60 49778 → 1720 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
 1498 536.155857400 192.168.177.180 192.168.177.7   TCP      60 49778 → 1723 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
 1499 536.155506100 192.168.177.180 192.168.177.7   TCP      60 49778 → 3306 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
 1500 536.157449100 192.168.177.180 192.168.177.7   TCP      60 49778 → 25 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
 1501 536.164799700 192.168.177.180 192.168.177.7   TCP      60 49778 → 8080 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
 1502 536.165497600 192.168.177.180 192.168.177.7   TCP      60 49778 → 8888 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
 1503 536.165394700 192.168.177.180 192.168.177.7   TCP      60 49778 → 22 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
 1504 536.165676200 192.168.177.180 192.168.177.7   TCP      60 49778 → 80 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
 1505 536.165505000 192.168.177.180 192.168.177.7   TCP      60 49778 → 995 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
 1506 536.172197700 192.168.177.180 192.168.177.7   TCP      60 49778 → 445 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
 1507 537.256335200 192.168.177.180 192.168.177.7   TCP      60 49779 → 445 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 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
```

```
0000  00 15 5d 00 ba 06 00 15  5d 00 5a 09 06 00 45 00   ..]......].Z..E.
0010  00 28 1c 37 00 00 37 06  88 e1 c0 a8 b1 64 c0 a8   .(.7..7......d..
0020  b1 07 c2 72 06 b6 8d 58  83 67 00 00 00 00 50 29   ...r...X.g....P)
0030  04 00 34 34 00 00 00 00  00 00 00 00               ..44........
```

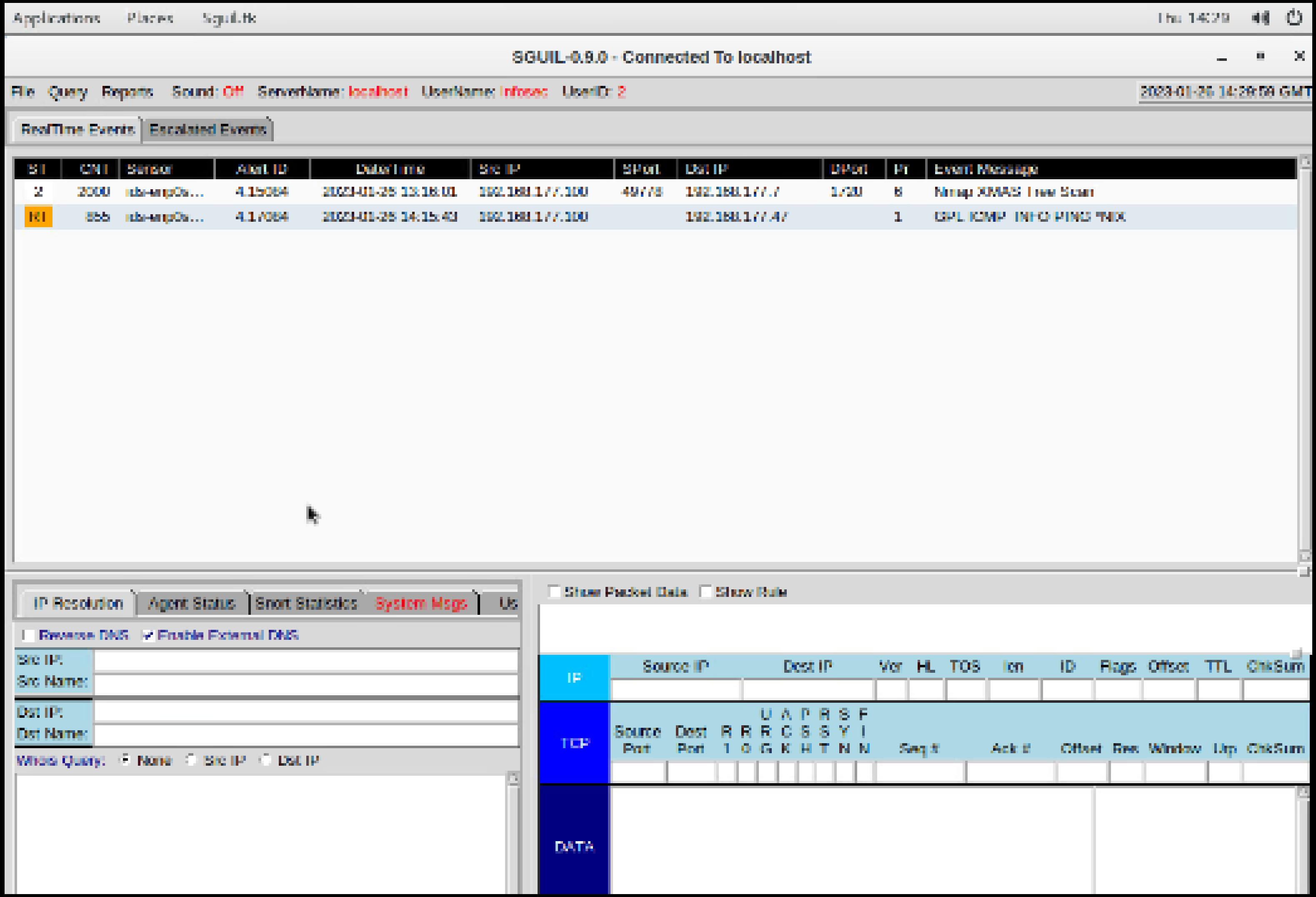
Transmission Control Protocol (tcp), 20 bytes

Packets: 4986 · Displayed: 2000 (40.1%) · Dropped: 0 (0.0%)

Profile: Default

Creating Snort rules

This screenshot shows the ping activity alert.



SGUIL-0.9.0 - Connected To localhost

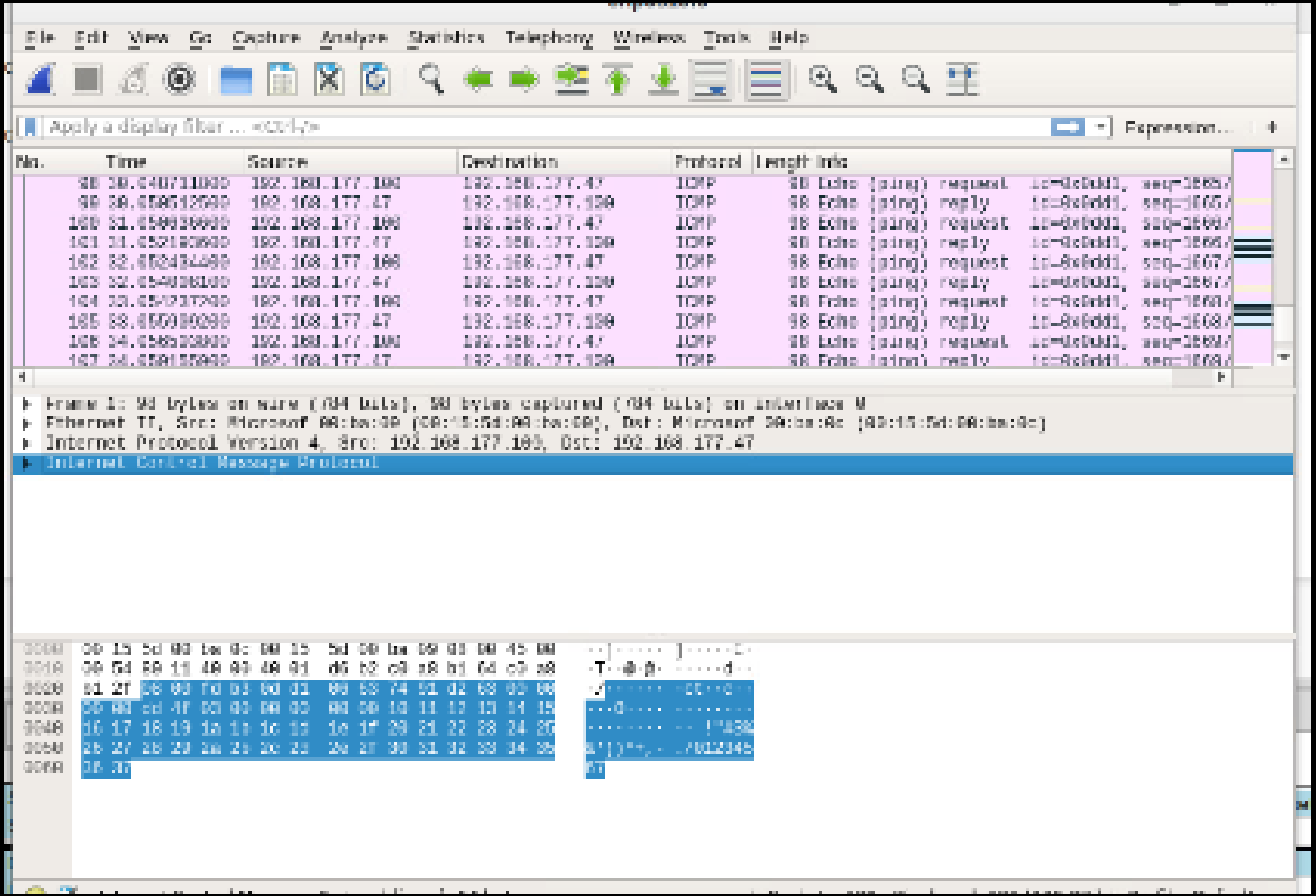
File Query Reports Sound: Off ServerName: localhost UserName: infosec UserID: 2 2023-01-26 14:29:59 GMT

RealTime Events | Escalated Events

ST	CNT	Sensor	Alert ID	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
2	2000	sb-enp0s...	4.15084	2023-01-26 13:18:01	192.168.177.100	49778	192.168.177.7	1720	6	Nmap XMAS Tree Scan
RT	855	sb-enp0s...	4.17084	2023-01-26 14:15:43	192.168.177.100		192.168.177.47		1	GPL ICMP_INFO PING *NIX

Creating Snort rules cont’d

This screenshot shows the ICMP packets generated by the ping activity.



No.	Time	Source	Destination	Protocol	Length	Info
98	30.040711000	192.168.177.100	192.168.177.47	ICMP	98	Echo (ping) request id=0x0dd1, seq=1665/
99	30.050512500	192.168.177.47	192.168.177.100	ICMP	98	Echo (ping) reply id=0x0dd1, seq=1665/
100	31.050030000	192.168.177.100	192.168.177.47	ICMP	98	Echo (ping) request id=0x0dd1, seq=1666/
101	31.052100000	192.168.177.47	192.168.177.100	ICMP	98	Echo (ping) reply id=0x0dd1, seq=1666/
102	32.052434400	192.168.177.100	192.168.177.47	ICMP	98	Echo (ping) request id=0x0dd1, seq=1667/
103	32.054030100	192.168.177.47	192.168.177.100	ICMP	98	Echo (ping) reply id=0x0dd1, seq=1667/
104	33.054737700	192.168.177.100	192.168.177.47	ICMP	98	Echo (ping) request id=0x0dd1, seq=1668/
105	33.055900200	192.168.177.47	192.168.177.100	ICMP	98	Echo (ping) reply id=0x0dd1, seq=1668/
106	34.056530800	192.168.177.100	192.168.177.47	ICMP	98	Echo (ping) request id=0x0dd1, seq=1669/
107	34.058155900	192.168.177.47	192.168.177.100	ICMP	98	Echo (ping) reply id=0x0dd1, seq=1669/

```
▸ Frame 1: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0
▸ Ethernet II, Src: Microsof 00:ba:09 (00:15:5d:00:ba:09), Dst: Microsof 00:ba:0c (00:15:5d:00:ba:0c)
▸ Internet Protocol Version 4, Src: 192.168.177.100, Dst: 192.168.177.47
▸ Internet Control Message Protocol
```

```
0000  00 15 5d 00 ba 0c 00 15  5d 00 ba 09 08 00 45 00   ··]·····]·····E·
0010  00 54 00 11 40 00 40 01  d6 b2 c0 a8 b1 64 c0 a8   ·T··@·@······d··
0020  b1 2f 08 00 fd 03 0d d1  00 63 74 51 d2 68 00 00   ·/······ ·ctQ·h··
0030  00 00 cd 4f 00 00 00 00  00 00 10 11 12 13 14 15   ···O···· ········
0040  16 17 18 19 1a 1b 1c 1d  1e 1f 20 21 22 23 24 25   ········ ·· !"#$%
0050  26 27 28 29 2a 2b 2c 2d  2e 2f 30 31 32 33 34 35   &'()*+,- ./012345
0060  36 37                                              67
```

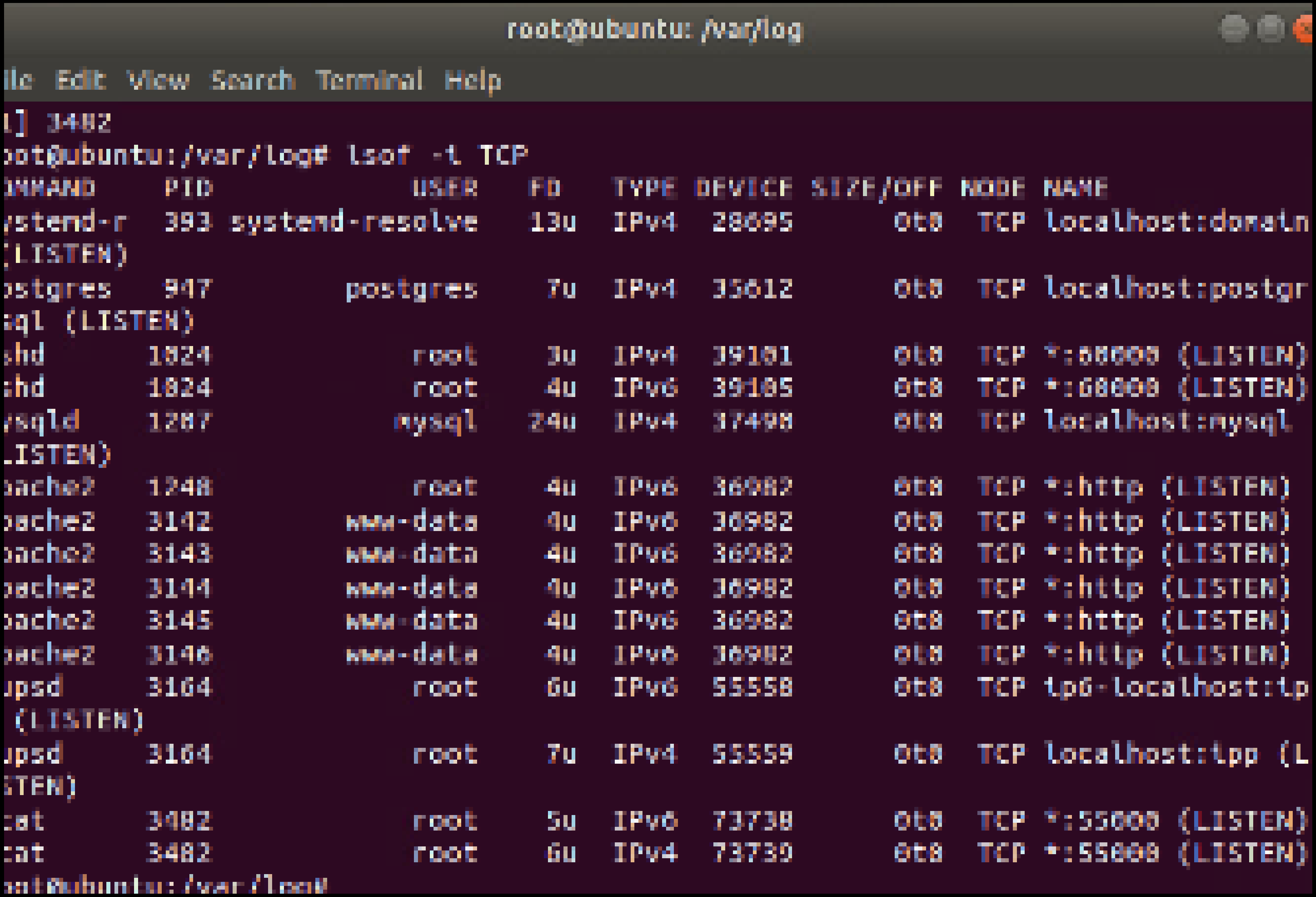
SEC290
Module 5

Live Memory Analysis

The next three slides show:
1) Linux Processes with port 55000 open for both IPv4 and IPv6,
2) A Process Hacker with properties of the chosen process; and,
3) The Process Monitor with ifFaceName in the Path column and data(Roman in the Detail column).

Linux Processes

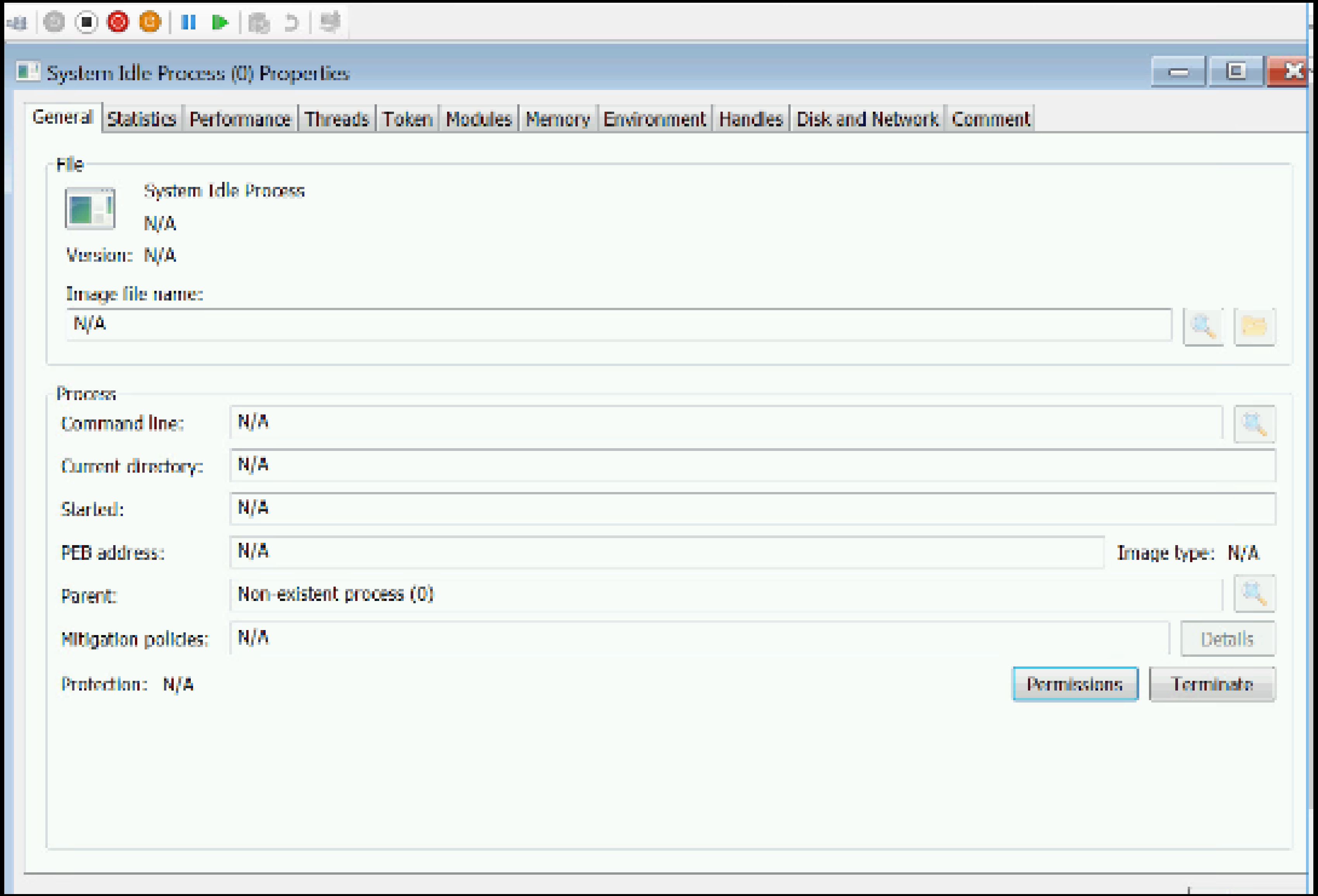
This screenshot shows port 55000 open for both IPv4 and IPv6.



```
1] 3482
oot@ubuntu:/var/log# lsof -i TCP
OMMAND     PID          USER   FD   TYPE DEVICE SIZE/OFF NODE NAME
ystemd-r   393 systemd-resolve   13u  IPv4  28695      0t0  TCP localhost:domain
(LISTEN)
ostgres    947        postgres    7u  IPv4  35612      0t0  TCP localhost:postgr
sql (LISTEN)
shd       1024            root    3u  IPv4  39101      0t0  TCP *:60000 (LISTEN)
shd       1024            root    4u  IPv6  39105      0t0  TCP *:60000 (LISTEN)
ysqld     1287           mysql   24u  IPv4  37490      0t0  TCP localhost:mysql
LISTEN)
pache2    1248            root    4u  IPv6  36982      0t0  TCP *:http (LISTEN)
pache2    3142        www-data    4u  IPv6  36982      0t0  TCP *:http (LISTEN)
pache2    3143        www-data    4u  IPv6  36982      0t0  TCP *:http (LISTEN)
pache2    3144        www-data    4u  IPv6  36982      0t0  TCP *:http (LISTEN)
pache2    3145        www-data    4u  IPv6  36982      0t0  TCP *:http (LISTEN)
pache2    3146        www-data    4u  IPv6  36982      0t0  TCP *:http (LISTEN)
upsd      3164            root    6u  IPv6  55558      0t0  TCP ip6-localhost:ip
 (LISTEN)
upsd      3164            root    7u  IPv4  55559      0t0  TCP localhost:ipp (L
STEN)
cat       3482            root    5u  IPv6  73738      0t0  TCP *:55000 (LISTEN)
cat       3482            root    6u  IPv4  73739      0t0  TCP *:55000 (LISTEN)
oot@ubuntu:/var/log#
```

Process Hacker

This screenshot shows properties of a chosen process.



System Idle Process

N/A

Version: N/A

Image file name: N/A

Command line: N/A

Current directory: N/A

Started: N/A

PEB address: N/A

Image type: N/A

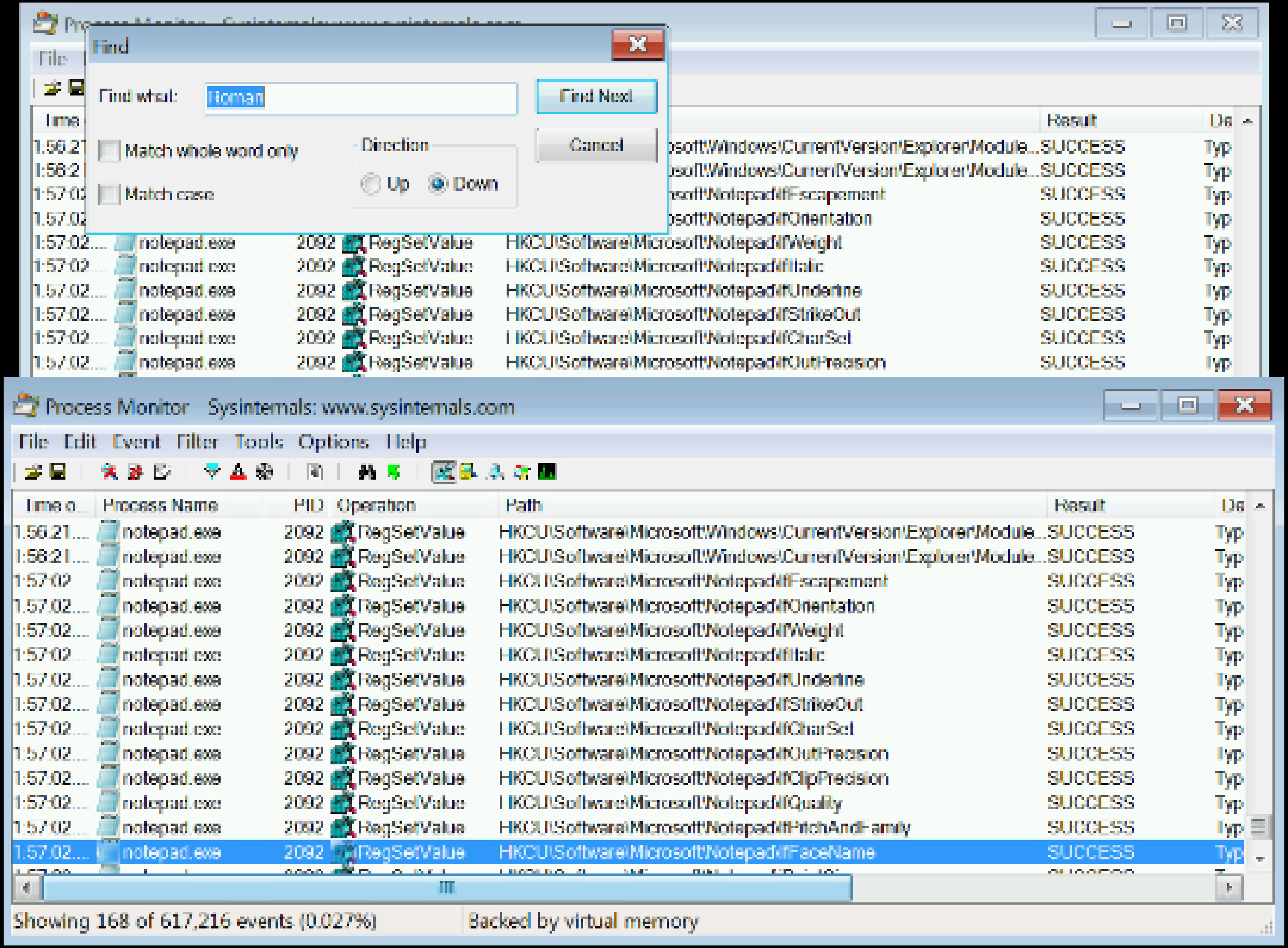
Parent: Non-existent process (0)

Mitigation policies: N/A

Protection: N/A

Process Monitor

This screenshot shows ifFaceName in the Path column and Data: Roman in the Detail column.



Find

Find what: Roman

□ Match whole word only

□ Match case

Direction ○ Up ● Down

Time	Process Name	PID	Operation	Path	Result	De
1:56:21				...soft\Windows\CurrentVersion\Explorer\Module...	SUCCESS	Typ
1:56:21				...soft\Windows\CurrentVersion\Explorer\Module...	SUCCESS	Typ
1:57:02				...soft\Notepad\lfEscapement	SUCCESS	Typ
1:57:02				...soft\Notepad\lfOrientation	SUCCESS	Typ
1:57:02....	notepad.exe	2092	RegSetValue	HKCU\Software\Microsoft\Notepad\lfWeight	SUCCESS	Typ
1:57:02....	notepad.exe	2092	RegSetValue	HKCU\Software\Microsoft\Notepad\lfItalic	SUCCESS	Typ
1:57:02....	notepad.exe	2092	RegSetValue	HKCU\Software\Microsoft\Notepad\lfUnderline	SUCCESS	Typ
1:57:02....	notepad.exe	2092	RegSetValue	HKCU\Software\Microsoft\Notepad\lfStrikeOut	SUCCESS	Typ
1:57:02....	notepad.exe	2092	RegSetValue	HKCU\Software\Microsoft\Notepad\lfCharSet	SUCCESS	Typ
1:57:02....	notepad.exe	2092	RegSetValue	HKCU\Software\Microsoft\Notepad\lfOutPrecision	SUCCESS	Typ

Process Monitor - Sysinternals: www.sysinternals.com

Time o...	Process Name	PID	Operation	Path	Result	De
1:56:21....	notepad.exe	2092	RegSetValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Module...	SUCCESS	Typ
1:56:21....	notepad.exe	2092	RegSetValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Module...	SUCCESS	Typ
1:57:02....	notepad.exe	2092	RegSetValue	HKCU\Software\Microsoft\Notepad\lfEscapement	SUCCESS	Typ
1:57:02....	notepad.exe	2092	RegSetValue	HKCU\Software\Microsoft\Notepad\lfOrientation	SUCCESS	Typ
1:57:02....	notepad.exe	2092	RegSetValue	HKCU\Software\Microsoft\Notepad\lfWeight	SUCCESS	Typ
1:57:02....	notepad.exe	2092	RegSetValue	HKCU\Software\Microsoft\Notepad\lfItalic	SUCCESS	Typ
1:57:02....	notepad.exe	2092	RegSetValue	HKCU\Software\Microsoft\Notepad\lfUnderline	SUCCESS	Typ
1:57:02....	notepad.exe	2092	RegSetValue	HKCU\Software\Microsoft\Notepad\lfStrikeOut	SUCCESS	Typ
1:57:02....	notepad.exe	2092	RegSetValue	HKCU\Software\Microsoft\Notepad\lfCharSet	SUCCESS	Typ
1:57:02....	notepad.exe	2092	RegSetValue	HKCU\Software\Microsoft\Notepad\lfOutPrecision	SUCCESS	Typ
1:57:02....	notepad.exe	2092	RegSetValue	HKCU\Software\Microsoft\Notepad\lfClipPrecision	SUCCESS	Typ
1:57:02....	notepad.exe	2092	RegSetValue	HKCU\Software\Microsoft\Notepad\lfQuality	SUCCESS	Typ
1:57:02....	notepad.exe	2092	RegSetValue	HKCU\Software\Microsoft\Notepad\lfPitchAndFamily	SUCCESS	Typ
1:57:02....	notepad.exe	2092	RegSetValue	HKCU\Software\Microsoft\Notepad\lfFaceName	SUCCESS	Typ

Showing 168 of 617,216 events (0.027%)   Backed by virtual memory

SEC290

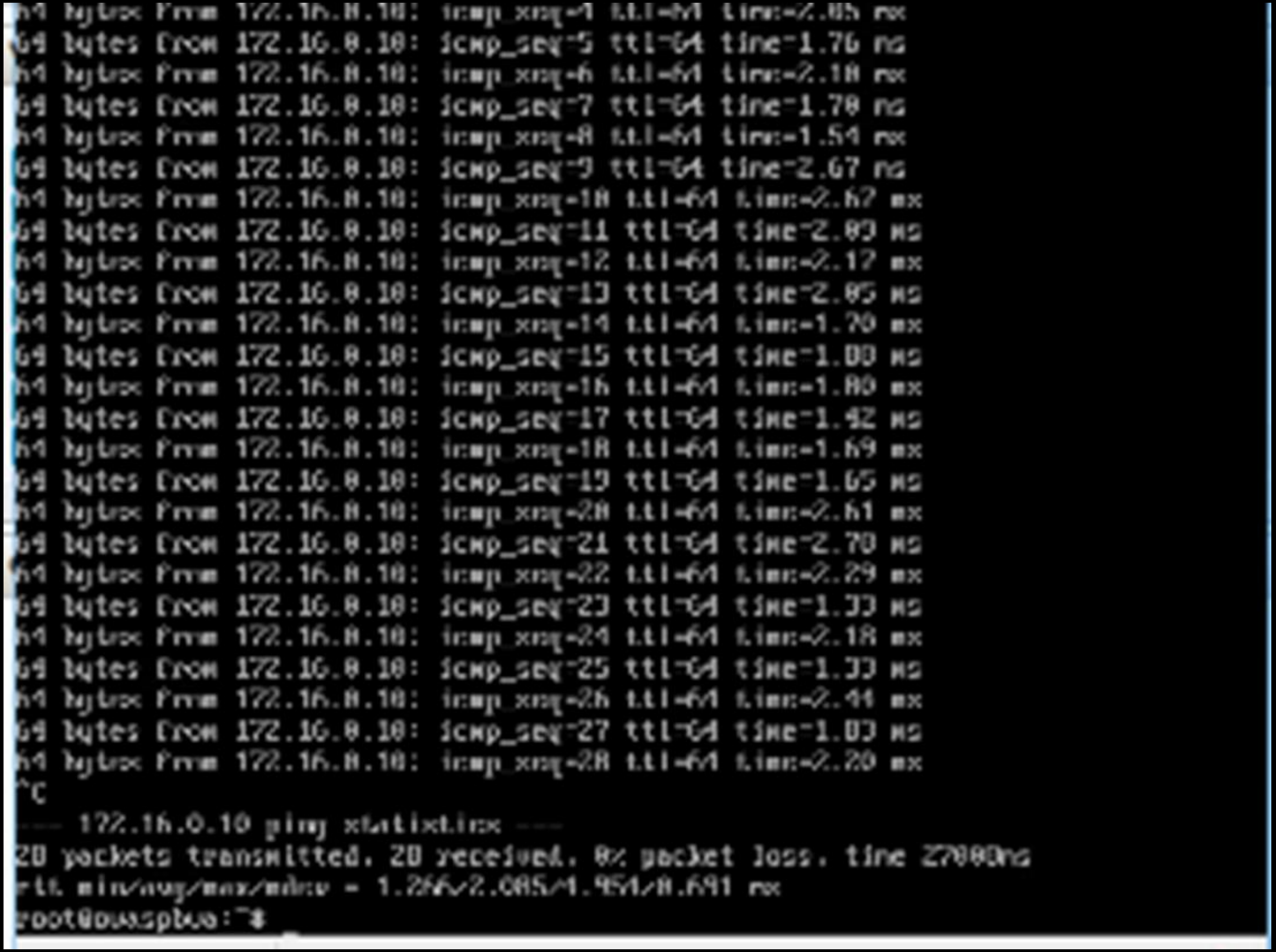
Module 6

Firewall and Time-based Access

The next three slides show:
1) The output of the DMZ Route Table,
2) A successful ping from the Ubuntu Web VM and the DMZ VM; and,
3) Two time-based access rules in the FORWARD chain.

Time-based Access

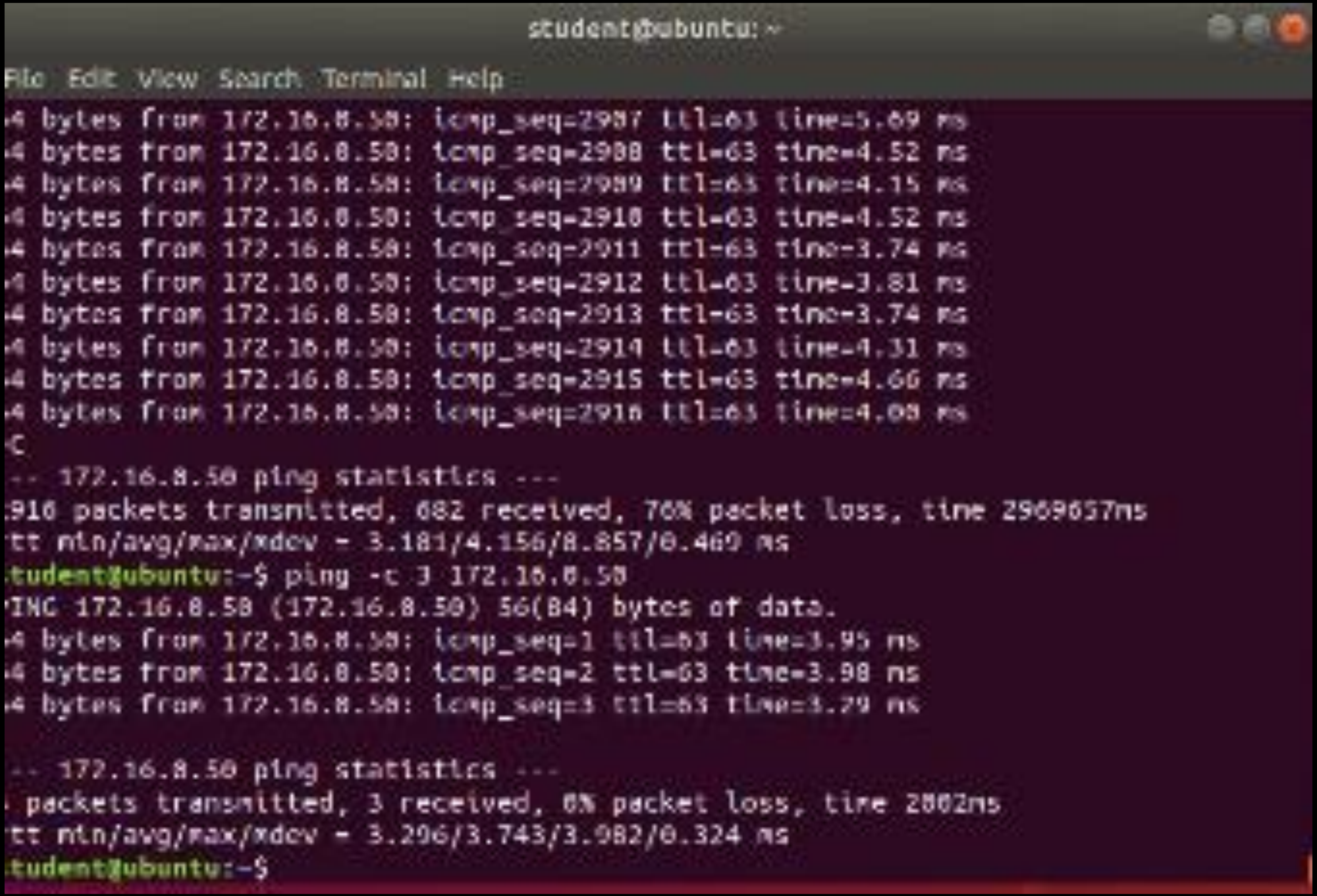
This slide shows the output of the DMZ Route Table.



```
64 bytes from 172.16.0.10: icmp_seq=4 ttl=64 time=2.05 ms
64 bytes from 172.16.0.10: icmp_seq=5 ttl=64 time=1.76 ms
64 bytes from 172.16.0.10: icmp_seq=6 ttl=64 time=2.10 ms
64 bytes from 172.16.0.10: icmp_seq=7 ttl=64 time=1.78 ms
64 bytes from 172.16.0.10: icmp_seq=8 ttl=64 time=1.54 ms
64 bytes from 172.16.0.10: icmp_seq=9 ttl=64 time=2.67 ms
64 bytes from 172.16.0.10: icmp_seq=10 ttl=64 time=2.67 ms
64 bytes from 172.16.0.10: icmp_seq=11 ttl=64 time=2.09 ms
64 bytes from 172.16.0.10: icmp_seq=12 ttl=64 time=2.17 ms
64 bytes from 172.16.0.10: icmp_seq=13 ttl=64 time=2.05 ms
64 bytes from 172.16.0.10: icmp_seq=14 ttl=64 time=1.70 ms
64 bytes from 172.16.0.10: icmp_seq=15 ttl=64 time=1.80 ms
64 bytes from 172.16.0.10: icmp_seq=16 ttl=64 time=1.80 ms
64 bytes from 172.16.0.10: icmp_seq=17 ttl=64 time=1.42 ms
64 bytes from 172.16.0.10: icmp_seq=18 ttl=64 time=1.69 ms
64 bytes from 172.16.0.10: icmp_seq=19 ttl=64 time=1.65 ms
64 bytes from 172.16.0.10: icmp_seq=20 ttl=64 time=2.61 ms
64 bytes from 172.16.0.10: icmp_seq=21 ttl=64 time=2.70 ms
64 bytes from 172.16.0.10: icmp_seq=22 ttl=64 time=2.29 ms
64 bytes from 172.16.0.10: icmp_seq=23 ttl=64 time=1.33 ms
64 bytes from 172.16.0.10: icmp_seq=24 ttl=64 time=2.18 ms
64 bytes from 172.16.0.10: icmp_seq=25 ttl=64 time=1.33 ms
64 bytes from 172.16.0.10: icmp_seq=26 ttl=64 time=2.44 ms
64 bytes from 172.16.0.10: icmp_seq=27 ttl=64 time=1.03 ms
64 bytes from 172.16.0.10: icmp_seq=28 ttl=64 time=2.20 ms
^C
--- 172.16.0.10 ping statistics ---
28 packets transmitted, 28 received, 0% packet loss, time 27080ms
rtt min/avg/max/mdev = 1.266/2.085/4.954/0.691 ms
root@owaspbwa:~$
```

Time-based Access

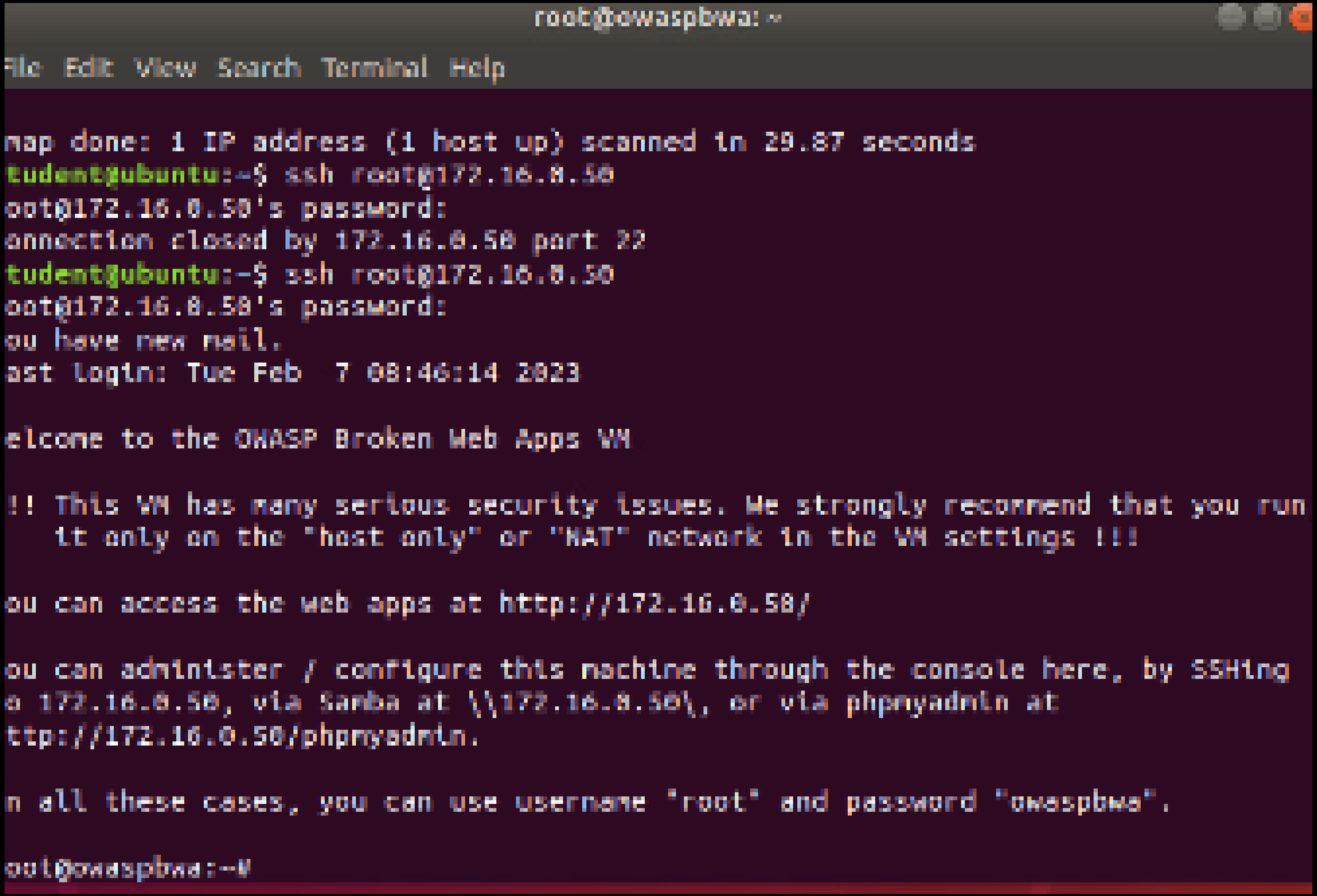
This screenshot shows a successful ping from the Ubuntu Web VM and the DMZ VM.



```
4 bytes from 172.16.8.50: icmp_seq=2907 ttl=63 time=5.69 ms
4 bytes from 172.16.8.50: icmp_seq=2908 ttl=63 time=4.52 ms
4 bytes from 172.16.8.50: icmp_seq=2909 ttl=63 time=4.15 ms
4 bytes from 172.16.8.50: icmp_seq=2910 ttl=63 time=4.52 ms
4 bytes from 172.16.8.50: icmp_seq=2911 ttl=63 time=3.74 ms
4 bytes from 172.16.8.50: icmp_seq=2912 ttl=63 time=3.81 ms
4 bytes from 172.16.8.50: icmp_seq=2913 ttl=63 time=3.74 ms
4 bytes from 172.16.8.50: icmp_seq=2914 ttl=63 time=4.31 ms
4 bytes from 172.16.8.50: icmp_seq=2915 ttl=63 time=4.66 ms
4 bytes from 172.16.8.50: icmp_seq=2916 ttl=63 time=4.08 ms
C
-- 172.16.8.50 ping statistics ---
916 packets transmitted, 682 received, 76% packet loss, time 2969657ms
tt min/avg/max/mdev = 3.181/4.156/8.857/0.469 ms
tudent@ubuntu:~$ ping -c 3 172.16.8.50
ING 172.16.8.50 (172.16.8.50) 56(84) bytes of data.
4 bytes from 172.16.8.50: icmp_seq=1 ttl=63 time=3.95 ms
4 bytes from 172.16.8.50: icmp_seq=2 ttl=63 time=3.98 ms
4 bytes from 172.16.8.50: icmp_seq=3 ttl=63 time=3.29 ms

-- 172.16.8.50 ping statistics ---
 packets transmitted, 3 received, 0% packet loss, time 2002ms
tt min/avg/max/mdev = 3.296/3.743/3.982/0.324 ms
tudent@ubuntu:~$
```

Time-based Access

This screenshot shows two time-based access rules in the FORWARD chain.



```
map done: 1 IP address (1 host up) scanned in 29.87 seconds
tudent@ubuntu:~$ ssh root@172.16.0.50
oot@172.16.0.50's password:
onnection closed by 172.16.0.58 port 22
tudent@ubuntu:~$ ssh root@172.16.0.50
oot@172.16.0.58's password:
ou have new mail.
ast login: Tue Feb  7 08:46:14 2023

elcome 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 !!!

ou can access the web apps at http://172.16.0.58/

ou can administer / configure this machine through the console here, by SSHing
o 172.16.0.50, via Samba at \\172.16.0.50\, or via phpmyadmin at
ttp://172.16.0.50/phpmyadmin.

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

oot@owaspbwa:~#
```

Challenges

Identifying the proper login procedures.

Learning how to work with new programs.

Testing the additions at each stage.

Learning how to discover and analyze new data.

Career Skills

Manual Vulnerability Analysis on a test VM network.

Intrusion Analysis using Wireshark.

Open SSL by Creating and testing an SSL/TLS file.

Using Snort and Live Memory Analysis.

Firewall and Time-based Access.

Further developed basic and advanced computer skills.

Conclusion

I found learning how to configure firewall rules, deploying Snort sensors for network intrusion detection, exploring SSL encryption, analyzing traffic to detect attacks, exploiting Microsoft vulnerabilities, and conducting live memory analysis to be very educational. Cybersecurity is truly an excited field.

I feel this project will help me in the future.

References

Professor Larry D. Burnette at DeVry University

DeVry SEC290 Course Project Videos

Chapple, M., & Seidl, D. (2020). *CompTIA CySA+ study guide exam CS0-002* (2nd ed.). Wiley Sybex

https://devry.webex.com/recordingservice/sites/devry/recording/29209165744b103bbf1f00505681e571/playback