

Lab 1

Intro to Wireshark

Question 1: Resolved ports should display names of well-known service, but this version of Wireshark did not, the list from [internet assigned numbers authority](#) provided the service name for resolved ports, such as dest port 53 from packet no. 1

The screenshot shows a Wireshark window titled "wireshark_setup.pcapng". The main pane displays a list of network packets. The first few packets are as follows:

- Frame 1: 71 bytes on wire (568 bits), 71 bytes captured (568 bits) on interface \Device\NPF_{05A55875-2B8B-45E5-94FA-964FA-9601
- Ethernet II, Src: VMware_5d:24:2c (00:0c:29:5d:24:2c), Dst: Broadcom_f6:5f:33 (00:10:18:f6:5f:33)
- Internet Protocol Version 4, Src: 172.21.2.217, Dst: 172.21.2.1
- User Datagram Protocol, Src Port: 56199, Dst Port: 53
- Domain Name System (query)

The bytes pane shows the raw data of the DNS query, which includes the domain name "www.msn.c".

On the right side of the screen, there are two question boxes:

- Question 1 of 5:** What is the difference between resolved and unresolved ports on the Wireshark display setup?
 - Resolved ports display all information about the port (including destination and header data), whereas unresolved sources only show the raw data.
 - Resolved ports display the name of the well-known service that runs on that port, whereas unresolved ports just display the number.
- Question 2 of 5:** What is the correct syntax to use on Wireshark for showing only SMTP and ICMP traffic?
 - None of the options listed are correct.

53 Search 1 2 3 4

Service Name	Port Number	Transport Protocol	Description	Assignee	Contact	Registration Date	Modification Date	Reference	Service Code	Unauthorized Use	Assignment Notes
smtp	25	tcp	Simple Mail Transfer	[IESG]	[IETF Chair]	2017-06-05		[RFC5321]			
smtp	25	udp	Simple Mail Transfer	[IESG]	[IETF Chair]	2017-06-05		[RFC5321]			
domain	53	tcp	Domain Name Server	[Paul Mockapetris]	[Paul Mockapetris]						
domain	53	udp	Domain Name Server	[Paul Mockapetris]	[Paul Mockapetris]						
sgmp	153	tcp	SGMP	[Marty Schoffstahl]	[Marty Schoffstahl]						
sgmp	153	udp	SGMP	[Marty Schoffstahl]	[Marty Schoffstahl]						
ndsauth	353	tcp	NDSAUTH	[Jayakumar Ramalingam]	[Jayakumar Ramalingam]						
ndsauth	353	udp	NDSAUTH	[Jayakumar Ramalingam]	[Jayakumar Ramalingam]						
creativeserver	453	tcp	CreativeServer								
creativeserver	453	udp	CreativeServer								
courier	530	tcp	rpc								
courier	530	udp	rpc								
conference	531	tcp	chat								
conference	531	udp	chat								
netnews	532	tcp	readnews								
netnews	532	udp	readnews								
netwall	533	tcp	for emergency broadcasts	[Andreas Heidemann]	[Andreas Heidemann]						
netwall	533	udp	for emergency broadcasts	[Andreas Heidemann]	[Andreas Heidemann]						
windream	534	tcp	windream Admin	[Uwe Honermann]	[Uwe Honermann]						
windream	534	udp	windream Admin	[Uwe Honermann]	[Uwe Honermann]						
iop	535	tcp	iop	[Jeff M Michaud]	[Jeff M Michaud]						
iop	535	udp	iop	[Jeff M Michaud]	[Jeff M Michaud]						
opalis-rdv	536	tcp	opalis-rdv	[Laurent Domenech]	[Laurent Domenech]						
opalis-rdv	536	udp	opalis-rdv	[Laurent Domenech]	[Laurent Domenech]						
nmsp	537	tcp	Networked Media Streaming Protocol	[Paul Santinelli Jr]	[Paul Santinelli Jr]						

Question 2: There is no SMTP or ICMP traffic

Question 2 of 5

What is the correct syntax to use on Wireshark for showing only SMTP and ICMP traffic?

tcp.port eq 25 or icmp
 tcp.show smtp & icmp
 tcpdump.list 25 7
 show 25 & icmp

Question 3, 4, 5: The source, time, and destination are listed under their respective column titles for the last packet.

Question 3 of 5

Using wireshark_setup.pcapng, filter the packets to view only HTTP requests. What is the source IP address shown on the last packet?

172.21.2.217

Question 4 of 5

Within that same packet, what is the time shown? Your answer must be in YYYY-MM-DD HH:MM:SS format adjusted for UTC.

2017-12-12 13:04:10

Question 5 of 5

What is the destination IP address of the last packet?

34.232.98.203

Results:

The screenshot shows a completion screen for a lab. At the top left is a blue square icon with a white 'IL' logo and the text 'Packet Analysis'. The top center says 'Intro to Wireshark'. The top right has an 'Exit' button with a red 'X'. In the center, it says 'Congratulations Amanda' and 'You have completed "Intro to Wireshark"'. Below this are two achievement icons: a hand holding a star labeled '+100' and a person climbing a mountain labeled '1/3'. It also says 'Total Points 100' and 'You've completed 1 of your 3 labs for this week!'. At the bottom right, there's a 'Next Lab' button with 'Packet Capture Basics >'. The background is dark blue with abstract geometric shapes.

Packet Analysis

Intro to Wireshark

Exit X

Congratulations Amanda

You have completed "Intro to Wireshark"

+100

Total Points
100

1/3

You've completed 1 of your 3
labs for this week!

Next Lab
Packet Capture Basics >

Packet Capture Basics

Question 1 & 2: The packet info (No. 1) displays the server name www.bing.com. The IP address returned is shown in the response packet in answers, which is 204.79.197.200.

The screenshot shows a Wireshark capture window titled "capture-basics.pcap". The packet list pane shows several DNS requests and responses. The first DNS request (No. 1) is from 192.168.0.49 to 204.79.197.200. The DNS response (No. 164) contains the answer "www.bing.com. 204.79.197.200". The details pane shows the DNS message structure, and the bytes pane shows the raw hex and ASCII data. To the right of the Wireshark window, there are three questions:

- Question 1 of 7:** What is the server name sought in the first DNS request that is issued by the client?
Answer: www.bing.com
- Question 2 of 7:** What is the first IP address returned in the DNS response for the domain in Q1?
Answer: 204.79.197.200
- Question 3 of 7:** What is the browser user agent string that issued the search request?
Answer: Mozilla/5.0 (X11; Linux x86_64; rv:38.0) Gecko/20100101 Firefox/38.0 Iceweasel/38.7.1

Question 3: The browser user agent string was Mozilla/5.0 (X11; Linux x86_64; rv:38.0) Gecko/20100101 Firefox/38.0 Iceweasel/38.7.1, found by filtering with http.user_agent.

The screenshot shows a Wireshark capture window titled "capture-basics.pcap" with a filter applied to "http.user_agent". The packet list pane shows several HTTP requests, with the first one being a GET to "/". The details pane shows the HTTP message headers, including the User-Agent: "Mozilla/5.0 (X11; Linux x86_64; rv:38.0) Gecko/20100101 Firefox/38.0 Iceweasel/38.7.1" header. The bytes pane shows the raw hex and ASCII data. To the right of the Wireshark window, there are two questions:

- for the domain in Q1?**
Answer: Mozilla/5.0 (X11; Linux x86_64; rv:38.0) Gecko/20100101 Firefox/38.0 Iceweasel/38.7.1
- What is the browser user agent string that issued the search request?**
Answer: Mozilla/5.0 (X11; Linux x86_64; rv:38.0) Gecko/20100101 Firefox/38.0 Iceweasel/38.7.1

Question 4: The web server engine was Microsoft-IIS/8.5 found by filtering with http.server.

capture-basics.pcap

No. Time Source Destination Protocol Length Info

No.	Time	Source	Destination	Protocol	Length	Info
33	0.125885	204.79.197.200	192.168.0.49	HTTP	619	HTTP/1.1 200 OK (text/html)
49	0.192988	204.79.197.200	192.168.0.49	HTTP	486	HTTP/1.1 200 OK (application/x-javascript)
64	0.209622	204.79.197.200	192.168.0.49	HTTP	1144	HTTP/1.1 200 OK (image/png)
65	0.211314	204.79.197.200	192.168.0.49	HTTP	738	HTTP/1.1 200 OK (image/png)
73	0.214070	204.79.197.200	192.168.0.49	HTTP/X...	1197	HTTP/1.1 200 OK
88	0.259399	204.79.197.200	192.168.0.49	HTTP	293	HTTP/1.1 204 OK
90	0.264840	204.79.197.200	192.168.0.49	HTTP	293	HTTP/1.1 204 OK
105	0.307196	204.79.197.200	192.168.0.49	HTTP	636	HTTP/1.1 200 OK (application/x-javascript)
122	0.344339	204.79.197.200	192.168.0.49	HTTP	1377	HTTP/1.1 200 OK (application/x-javascript)
123	0.344364	204.79.197.200	192.168.0.49	HTTP	549	HTTP/1.1 200 OK (application/x-javascript)
125	0.344401	204.79.197.200	192.168.0.49	HTTP	1271	HTTP/1.1 200 OK (application/x-javascript)
151	0.358046	204.79.197.200	192.168.0.49	HTTP	78	HTTP/1.1 200 OK (application/x-javascript)
199	0.469616	204.79.197.200	192.168.0.49	HTTP	463	HTTP/1.1 200 OK (application/x-javascript)

Frame 33: 619 bytes on wire (4952 bits), 619 bytes captured (4952 bits)
Ethernet II, Src: RealtekU_12:35:00 (52:54:00:12:35:00), Dst: PcsCompu_c3:2a:09 (08:00:27:c3:2a:09)
Internet Protocol Version 4, Src: 204.79.197.200, Dst: 192.168.0.49
Transmission Control Protocol, Src Port: 80, Dst Port: 53044, Seq: 43582, Ack: 300, Len: 565
[13] Reassembled TCP Segments (4414 bytes): #9(1448), #11(1448), #13(5840), #17(1460), #19(424)
HyperText Transfer Protocol
HTTP/1.1 200 OK\r\n
Cache-Control: private, max-age=0\r\n
Content-Length: 42923\r\n
Content-Type: text/html; charset=utf-8\r\n
Content-Encoding: gzip\r\n
Vary: Accept-Encoding\r\n

What is the browser user agent string that issued the search request?
Mozilla/5.0 (X11; Linux x86_64; rv:38.0) Gecko/2011

Correct

Question 4 of 7
What web server engine is running the website?
Microsoft-IIS/8.5

Correct

Question 5: The image was found by going to the HTTP object list and finding the filename we were looking for. To view the image, the file had to be downloaded and opened. The text states "Password Hacking".

Wireshark · Export · HTTP object list

Packet	Hostname	Content Type	Size	Filename
64	www.bing.com	image/png	6660 bytes	hpc18.png
335	www.bing.com	image/png	260 bytes	409a194b.png
999	www.bing.com	image/png	6798 bytes	sw_nh_smallid_hamleft_acstar.png
1544	a1.fdlstatic.com	image/png	2159 bytes	favicon-96.png
1546	a1.fdlstatic.com	image/png	5896 bytes	favicon-160.png
1561	a4.fdlstatic.com	image/png	886 bytes	favicon-32.png
1563	a4.fdlstatic.com	image/png	598 bytes	favicon-16.png
1571	a4.fdlstatic.com	image/png	6894 bytes	favicon-192.png
1579	a1.fdlstatic.com	image/png	1627 bytes	favicon-64.png
1659	a2.fdlstatic.com	image/png	3423 bytes	dl-download-com.png
1722	dl1.cbsistatic.com	image/png	2358 bytes	imgingest-2812493432922163076.png
1724	a3.fdlstatic.com	image/png	2344 bytes	dl-shuttle-flat.png
1726	a3.fdlstatic.com	image/png	1531 bytes	icon-clear-x.png
1728	a3.fdlstatic.com	image/png	1988 bytes	icon_windows_64.png
1742	dl1.cbsistatic.com	image/png	9377 bytes	imgingest-5015644562731850884.png
1744	dl1.cbsistatic.com	image/png	8888 bytes	imgingest-8323129358086705188.png
1756	i.i.cbsi.com	image/png	8473 bytes	iconimg_108366.png
1796	i.i.cbsi.com	image/png	2663 bytes	104013e4793aa0ae791416f6b6935782c810_
1847	a1.fdlstatic.com	image/png	1737 bytes	dl-serach-magnify.png
1859	a1.fdlstatic.com	image/png	8402 bytes	platform-links-s61b17ef8f4.png
1901	a3.fdlstatic.com	image/png	1146 bytes	serp-rating-0.png
1903	a1.fdlstatic.com	image/png	1145 bytes	serp-rating-red.png
1904	a2.fdlstatic.com	image/png	185 bytes	green_bullet.png
1906	a3.fdlstatic.com	image/png	1146 bytes	serp-rating-blue.png
1923	a3.fdlstatic.com	image/png	1406 bytes	icon-serp-windows-on.png
1936	a1.fdlstatic.com	image/png	11 kB	bg_dark.png
2185	a3.fdlstatic.com	image/png	1648 bytes	icon-serp-iOS-on.png
2187	a3.fdlstatic.com	image/png	1568 bytes	icon-serp-android-on.png
2206	a1.fdlstatic.com	image/png	174 kB	icons-se2c2dbe553.png
3278	pixel.everesttech.net	image/png	128 bytes	v?ev_loc=http%3A%2F%2Fdownload.cnet.c
3373	pixel.everesttech.net	image/png	128 bytes	s?=&s=12969
3667	pixel.everesttech.net	image/png	128 bytes	1x1
4231	dl1.cbsistatic.com	image/png	2105 bytes	imgingest-2806645026275045084.png

Text Filter: image/png

Save Save All Close Help

Question 4 of 7
What web server engine is running the website?
www.bing.com

Question 5 of 7
When exporting HTTP content from the capture and looking at 'imgingest-5015644562731850884.png', what is the text that appears on that image?
Password Hacking

Question 6 of 7
How many different IPv4 conversations are there in this capture file?
89

Firefox automatically sends some data to Mozilla so that we can improve your experience.

Question 6: There are 89 IPv4 Conversations, as found by going to Statistics > Conversations > IPv4.

Question 6 of 7
How many different IPv4 conversations are there in this capture file?
89

Question 7 of 7
What was the user searching for on the download.cnet.com website? (Enter your answer as two separate words, e.g., catching fish.)
download cnet

Address A	Address B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Star
2.18.213.98	192.168.0.49	20	4933	8	1912	12	2921	16.252
8.6.8.8	192.168.0.49	584	74 k	292	51 k	292	22 k	0.0001
13.107.42.10	192.168.0.49	34	22 k	16	20 k	18	2007	12.953
23.1.243.24	192.168.0.49	240	146 k	112	131 k	128	14 k	15.785
23.1.243.42	192.168.0.49	18	3709	7	941	11	2764	24.615
23.1.243.58	192.168.0.49	409	490 k	190	471 k	219	19 k	15.481
23.1.243.98	192.168.0.49	91	82 k	42	63 k	49	18 k	14.152
23.21.165.110	192.168.0.49	31	11 k	12	6944	19	4844	15.777
23.43.75.27	192.168.0.49	42	9376	19	6765	23	291	2.331
23.21.165.111	192.168.0.49	41	35 k	19	31 k	22	2217	1.00
23.21.115.200	192.168.0.49	14	1821	6	10208	8	793	19.215
40.112.149.111	192.168.0.49	18	4615	8	1248	10	3367	16.649
40.115.48.15	192.168.0.49	33	21 k	15	19 k	18	1987	12.280
40.116.232.104	192.168.0.49	171	55 k	79	44 k	92	10 k	0.984
46.137.74.233	192.168.0.49	18	1751	6	616	12	113	20.536
52.3.10.179	192.168.0.49	18	2187	7	791	11	1394	20.496
52.17.109.27	192.168.0.49	21	2025	9	1015	12	1016	18.679
52.18.40.195	192.168.0.49	12	1482	5	624	7	856	30.113
52.18.10.238	192.168.0.49	20	2065	9	821	11	1244	0.04
52.18.223.82	192.168.0.49	49	34 k	22	28 k	27	5948	18.532
52.30.233.197	192.168.0.49	30	7679	12	3414	18	4265	17.326
52.71.248.123	192.168.0.49	36	6464	16	3481	20	2983	18.866
52.73.61.242	192.168.0.49	18	2957	7	1398	11	1559	21.706
52.73.231.146	192.168.0.49	50	1k	76	6013	37	10 k	18.592

Name resolution Limit to display filter Absolute start time Conversation Types Copy Follow Stream... Graph... Close Help

Question 7: Found by going to Statistics > HTTP > Requests, under the host download.cnet.com, we can see the query for “password cracking”.

When exporting HTTP content from the capture and looking at 'imgingest-5015644562731850884.png', what is the text that appears on that image?
Password Hacking

Question 6 of 7
How many different IPv4 conversations are there in this capture file?
89

Question 7 of 7
What was the user searching for on the download.cnet.com website?
(Enter your answer as two separate words, e.g., catching fish.)
password cracking

Result:

Packet Analysis

Packet Capture Basics

Congratulations Amanda
You have completed "Packet Capture Basics"

+100 Total Points 200

2/3 You've completed 2 of your 3 labs for this week!

Next Lab Wireshark Display Filters: An Introduction >

TCP Dump

Question 1: The options show that -w will allow you to write to a file, you can do so with a command like tcpdump -r tcpdump.pcap -w output.txt

```
linux@tcpdump:~$ tcpdump --help
tcpdump version 4.9.3
libpcap version 1.9.1 (with TPACKET_V3)
OpenSSL 1.1.1f  31 Mar 2020
Usage: tcpdump [-aAbdDefhHIJKLMNOPStUvxX#] [ -B size ] [ -c count ]
              [ -C file_size ] [ -E algo:secret ] [ -F file ] [ -G seconds ]
              [ -i interface ] [ -j tstamptype ] [ -M secret ] [ -n number ]
              [ -O in|out|inout ]
              [ -r file ] [ -s snaplen ] [ --time-stamp-precision precision ]
              [ --immediate-mode ] [ -T type ] [ --version ] [ -V file ]
              [ -w file ] [ -W filecount ] [ -y datalinktype ] [ -z postrotate-command ]
              [ -Z user ] [ expression ]
linux@tcpdump:~$
```

Question 1 of 5

Which option can you pass to tcpdump to write captured packets out to a file?

-w

Correct

Question 2: Using the -D option, such as in the command tcpdump -D, we can see a list of all interfaces, and nflog is at number 5.

```
linux@tcpdump:~$ tcpdump -D
1.eth0 [Up, Running]
2.lo [Up, Running, Loopback]
3.any (Pseudo-device that captures on all interfaces) [Up, Running]
4.bluetooth-monitor (Bluetooth Linux Monitor) [none]
5.nflog (Linux netfilter log (NFLOG) interface) [none]
6.nfqueue (Linux netfilter queue (NFQUEUE) interface) [none]
linux@tcpdump:~$
```

Question 2 of 5

Using tcpdump, list all the available interfaces. What number is nflog listed as?

5

Correct

Question 3: By reading from tcpdump.pcap and filtering the IP address with the command, tcpdump -r tcpdump.pcap host 88.221.88.59, we can see the time on the last packet at the bottom to be 07:32:57.

```
linux@tcpdump:~$ tcpdump -r tcpdump.pcap host 88.221.88.59
reading from file tcpdump.pcap, link-type EN10MB (Ethernet)
07:31:56.197987 IP ip-192-168-21-133.eu-west-1.compute.internal.40646 > a88-221-88-59.deploy.static.akamaitechnologies.com.80: Flags [R], seq 0, ack 1, win 1, options [nop,nop,TS val 1000000 ecr 0], length 0
07:31:56.198136 IP a88-221-88-59.deploy.static.akamaitechnologies.com.80 > ip-192-168-21-133.eu-west-1.compute.internal.40646: Flags [R], seq 1, ack 0, win 1, options [nop,nop,TS val 1000000 ecr 0], length 0
07:32:06.438054 IP ip-192-168-21-133.eu-west-1.compute.internal.40646 > a88-221-88-59.deploy.static.akamaitechnologies.com.80: Flags [R], seq 0, ack 1, win 1, options [nop,nop,TS val 1000000 ecr 0], length 0
07:32:06.438365 IP a88-221-88-59.deploy.static.akamaitechnologies.com.80 > ip-192-168-21-133.eu-west-1.compute.internal.40646: Flags [R], seq 1, ack 0, win 1, options [nop,nop,TS val 1000000 ecr 0], length 0
07:32:16.677955 IP ip-192-168-21-133.eu-west-1.compute.internal.40646 > a88-221-88-59.deploy.static.akamaitechnologies.com.80: Flags [R], seq 0, ack 1, win 1, options [nop,nop,TS val 1000000 ecr 0], length 0
07:32:16.678082 IP a88-221-88-59.deploy.static.akamaitechnologies.com.80 > ip-192-168-21-133.eu-west-1.compute.internal.40646: Flags [R], seq 1, ack 0, win 1, options [nop,nop,TS val 1000000 ecr 0], length 0
07:32:26.921868 IP ip-192-168-21-133.eu-west-1.compute.internal.40646 > a88-221-88-59.deploy.static.akamaitechnologies.com.80: Flags [R], seq 0, ack 1, win 1, options [nop,nop,TS val 1000000 ecr 0], length 0
07:32:26.921990 IP a88-221-88-59.deploy.static.akamaitechnologies.com.80 > ip-192-168-21-133.eu-west-1.compute.internal.40646: Flags [R], seq 1, ack 0, win 1, options [nop,nop,TS val 1000000 ecr 0], length 0
07:32:37.158275 IP ip-192-168-21-133.eu-west-1.compute.internal.40646 > a88-221-88-59.deploy.static.akamaitechnologies.com.80: Flags [R], seq 0, ack 1, win 1, options [nop,nop,TS val 1000000 ecr 0], length 0
07:32:37.158725 IP a88-221-88-59.deploy.static.akamaitechnologies.com.80 > ip-192-168-21-133.eu-west-1.compute.internal.40646: Flags [R], seq 1, ack 0, win 1, options [nop,nop,TS val 1000000 ecr 0], length 0
07:32:47.397977 IP ip-192-168-21-133.eu-west-1.compute.internal.40646 > a88-221-88-59.deploy.static.akamaitechnologies.com.80: Flags [R], seq 0, ack 1, win 1, options [nop,nop,TS val 1000000 ecr 0], length 0
07:32:47.398547 IP a88-221-88-59.deploy.static.akamaitechnologies.com.80 > ip-192-168-21-133.eu-west-1.compute.internal.40646: Flags [R], seq 1, ack 0, win 1, options [nop,nop,TS val 1000000 ecr 0], length 0
07:32:57.638112 IP ip-192-168-21-133.eu-west-1.compute.internal.40646 > a88-221-88-59.deploy.static.akamaitechnologies.com.80: Flags [R], seq 0, ack 1, win 1, options [nop,nop,TS val 1000000 ecr 0], length 0
07:32:57.638538 IP a88-221-88-59.deploy.static.akamaitechnologies.com.80 > ip-192-168-21-133.eu-west-1.compute.internal.40646: Flags [R], seq 1, ack 0, win 1, options [nop,nop,TS val 1000000 ecr 0], length 0
```

Correct

Question 3 of 5

Using tcpdump, read the packets from tcpdump.pcap and filter packets to include IP address 88.221.88.59 only. What is the time shown on the final packet? (HH:MM:SS)

07:32:57

Correct

Question 4 of 5

Using tcpdump, read the packets from tcpdump.pcap and filter packets to include IP address 184.107.41.72 and port 80 only. Write these packets to a new file and md5sum that file. What is the md5sum shown?

Question 4: To first read packets from the pcap file and filter for IP and port 80, I typed in ‘tcpdump -nn -r tcpdump.pcap -w output.txt host 184.107.41.71 and port 80’. Where the first part is reading from the pcap file, -w signifies writing to the file output.txt and host and port are filters. After writing to output.txt, I got the md5Sum of the file with ‘md5sum output.txt’, which is the hash of that file.

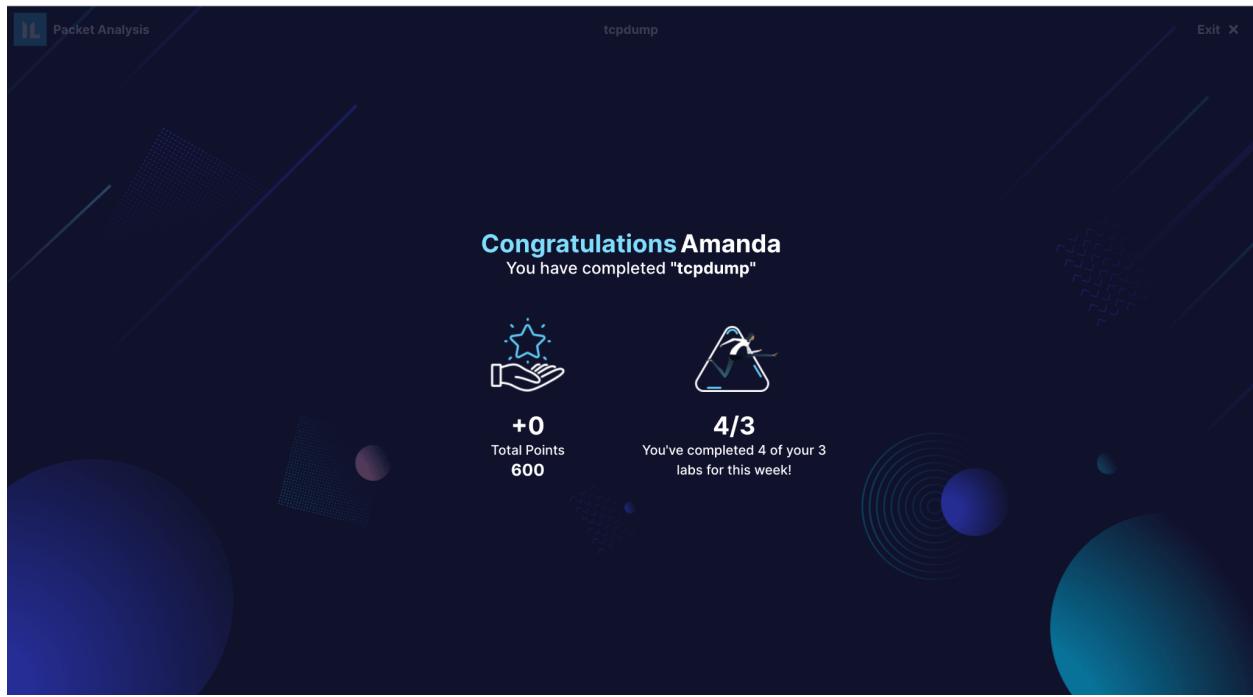
linux@tcpdump:~\$ tcpdump -nn -r tcpdump.pcap -w output.txt host 184.107.41.71 and port 80
reading from file tcpdump.pcap, link-type EN10MB (Ethernet)
linux@tcpdump:~\$ md5sum output.txt
8e4b92724d9034a49cf10f6b147ac482 output.txt
linux@tcpdump:~\$

Question 4 of 5
Using tcpdump, read the packets from tcpdump.pcap and filter packets to include IP address 184.107.41.71 and port 80 only. Write these packets to a new file and md5sum that file. What is the md5sum shown?
8e4b92724d9034a49cf10f6b147ac482
Correct

Question 5: To get ASCII and hex content from a packet, use the option -XX. I did this with tcpdump -r tcpdump.pcap -XX

● TCPDump
0x0c50: 6f7b 5dd7 79af 127e d223 7951 67cb 6e91 o{.y..~.#\0g.n.
0x0c60: e8a7 43fe ea25 aac0 e69d 3d41 27d1 3adc ..C..%...-N.:.
0x0c70: 7fec 37c5 03eb ac1b a970 809d 777e 2ce3 ..7.....p...-..
0x0c80: f416 6a40 74aa d8c5 18a5 4bb4 88bc a0c1 ..jKt...K...
0x0c90: aebd ace2 962b 593e c2b7 043b ee53 0d9d+Y>...;S..
0x0ca0: 9a99 035c b0d4 eb5a 985e bbbf 71f3 fd3b ...5...Z.^..q.;
0x0cb0: 396f 8562 f75b 0c48 dfde e897 afaf 6dd5 90.b.[H...
0x0cc0: 21dc f654 3dd6 f404 b82a c322 bd4e e0f4 !...=...*`..N.
0x0cd0: bf06 92d0 5dcb ab53 8361 12a7 e4ff 3f82]..S.a....
0x0ce0: 508c a3a6 d7cd 913f 3c93 0b52 bcbe 06fe P.....?<.R...
0x0cf0: 5566 f12a 2442 1e54 b684 04c4 ble7 879b Uf.*SB.T.....
0x0d00: fc7f 5f75 b76d 946f 9387 adaf 6928 a635 .._u.m.o...i(.5
0x0d10: 166d f68f 3a8a 6b76 d809 f141 9741 36f4 ..m...:kv...F.A6.
0x0d20: b232 7610 b69b a632 e459 7ada d94e 1557 +2v...2.Yz..N.W
0x0d30: 983e cfba dabc e404 e652 f955 aa37 f468 .>...R.U.6.j
0x0d40: 7c41 3d9d 7ef9 6a64 3a6c 5415 885c c7e4 |A=-.jd;lT.\..
0x0d50: 7c8f 917a 261c cd89 6a76 4e87 f62a 7a4b |...t...jvN.*zK
0x0d60: 7298 db30 8a81 97ac 5525 ba1b 10a8 4226 r....0.%..B6
0x0d70: 5b15 c3a6 daed b13d 21e0 1e61 3c08 d694 [.....=!.k<...
0x0d80: ff66 501f 67d4 326d 2c8d 2654 f827 5ca0 .fp.g.2m.,.G.'\..
0x0d90: 0b66 4b81 b292 3f6b 91bf a0a7 bb3c dd04 ..K...7k.....<..
0x0da0: 198a 1cd1 2317 f08d a726 9881 3e46 b746 ...#.&..>F
0x0db0: 2136 5bb4 765a e897 059e f2cc 66fe 98f0 !6[.VZ....f...
0x0dc0: 074c 24a5 881f f6c8 41d2 4054 c7ec b789 .L\$.....A.@T...
0x0dd0: 01de 2b5f 837d 6769 6d44 2e81 ec30 6be5 ..+.jgimD...0K.
0x0de0: 42cb a191 34d0 49e4 7373 0296 195e b6f6 B...4.I.ss...)..
0x0df0: 483b 581b d53d 61fa 5e69 c7f0 1b67 f838 H:X..=a.^..g.8
0x0e00: fdea c773 7772 35ed b65f a55b 6bc3 d862 ...swr5...[k.b
0x0e10: 0826 fec1 0c2a f59a 803f 269c e178 a5bf &..*..?&..
0x0e20: 7ef5 d548 2dc8 42a9 8e13 e82a 4bc5 568c ~..H..B....*K.V.
0x0e30: 65e0 5fac 5863 e1c0 71f9 e5b4 e1ae 8d66 e...Xc.,q....f
0x0e40: 068f e69d 3e75 3246 2ce6 9448 25bc 50e3>2F,.H%.P.
0x0e50: f2ff 8680 811f 641c a9be be11 e654 9fb7d....T..
0x0e60: b13e b781 d983 3fc8 269b d792 e40b 6e27 >....7.&....n'
0x0e70: ffd4 4db5 89ab 53a4 26fa 1459 3b00 80d2 ..M...S.&..Y;...
0x0e80: d064 0bae bb2a 7b22 1e62 cec7 7a6c 29a7 ..l...*".b..zL).
0x0e90: c528 6909 e24c 1a7a 6c23 348d 5b59 6367 .(i..L.zl#4.[Ycg
0x0ea0: c19a 7e09 f810 e055 3e93 f859 0c0a 8c56 ..~....U>..Y..V
Correct
Question 5 of 5
Which option can be passed to tcpdump to display the ASCII and hex representation of the packet contents?
-XX
Correct
Submit

Result:



Nmap

Question 1: Scanning the top 1000 ports with the option –top-ports 1000, we can see that 5 ports are open.

The terminal window shows the command \$ nmap -T4 -top-ports 1000 and the resulting scan report for IP 10.102.11.237. It lists five open ports: 21/tcp (FTP), 25/tcp (SMTP), 80/tcp (HTTP), 110/tcp (POP3), and 443/tcp (HTTPS). The question card asks "Using Nmap, scan the top 1000 TCP ports. How many are open?" with the answer "5".

Question 2: To scan UDP ports only, I used the option -sU, and again –top-ports for the top 100 ports. This showed two open ports.

The terminal window shows the command \$ sudo nmap -sU -T4 -top-ports 100 and the resulting scan report for IP 10.102.11.237. It lists two open ports: 7/udp (Echo) and 69/udp (TFTP). The question card asks "Scan the top 100 UDP ports. How many ports are open?" with the answer "2".

Question 3: I ran the banner scan with the command nmap -sV -v -p- 10.120.11.237. Reading through the text of the fingerprint, it states \x20Come\x20find\x20your\x20token!, followed by the token d363.

The terminal window shows the command \$ nmap -sV -v -p- 10.120.11.237 and the resulting banner grab output. It includes the text "\x20Come\x20find\x20your\x20token!" followed by "d363". The question card asks "Run a banner grab scan. What is the token shown under the FTP service?" with the answer "d363".

Question 4: The -oG option gives grepable output that lists the ports scanned.

```
(kali㉿iml-kali)-[~]
$ nmap -T4 -A -v -oG - 10.102.11.237
# Nmap 7.92 scan initiated Thu Sep 22 01:10:26 2022 as: nmap -T4 -A -v -oG -
10.102.11.237
# Ports scanned: TCP(1000;1,3-4,6-7,9,13,17,19-26,30,32-33,37,42-63,49,53,70,
79,85,88-90,99-100,106,109-111,113,119,125,135,139,143-144,146,161,163,179,19
9,211-212,222,254-256,259,264,280,301,306,311,340,366,389,406-407,416-417,425
,427,443-445,458,464-465,481,497,500,512-515,524,541,543-545,548,554-555,563,
587,593,616-617,625,631,636,646,649,666-668,683,687,691,700,705,711,714,720,7
22,726,749,765,777,783,787,800-801,808,843,873,880,888,898,900-903,911-912,98
1,987,990,992-993,995,999-1002,1007,1009-1011,1021-1100,1102,1104-1108,1110-1
114,1117,1119,1121-1124,1126,1130-1132,1137-1138,1141,1145,1147-1149,1151-115
2,1154,1163-1166,1169,1174-1175,1183,1185-1187,1192,1198-1199,1201,1213,1216-
1218,1233-1234,1236,1244,1247-1248,1259,1271-1272,1277,1287,1296,1300-1301,13
09-1311,1322,1328,1334,1352,1417,1433-1434,1443,1455,1461,1494,1500-1501,1503
,1521,1524,1533,1556,1580,1583,1594,1600,1641,1658,1666,1687-1688,1700,1717-1
721,1723,1755,1761,1782-1783,1801,1805,1812,1839-1840,1862-1864,1875,1900,191
4,1935,1947,1971-1972,1974,1984,1998-2010,2013,2020-2022,2030,2033-2035,2038,
2040-2043,2045-2049,2065,2068,2099-2107,2111,2119,2121,2126,21
25,2314,3150-3161,3170-3180,3191,3198,3200,3222,3251,3260,3288,3291,3292
```

Question 5: The option -sS is called a half-open TCP scan because a full TCP connection is not opened.

```
(kali㉿iml-kali)-[~]
$ sudo nmap -sS 10.102.11.237
Starting Nmap 7.92 ( https://nmap.org ) at 2022-09-22 01:13 UTC
Nmap scan report for ip-10-102-11-237.eu-west-1.compute.internal (10.102.11.2
37)
Host is up (0.00043s latency).
Not shown: 995 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
25/tcp    open  smtp
80/tcp    open  http
110/tcp   open  pop3
443/tcp   open  https

Nmap done: 1 IP address (1 host up) scanned in 0.26 seconds
```

Question 6: Doing a banner grab on just port 110, for the pop3 service shows that the host is named snailmailreadyforaction.

```
(kali㉿iml-kali)-[~]
$ nmap -sV -v -p 110 10.102.11.237
Starting Nmap 7.92 ( https://nmap.org ) at 2022-09-22 01:31 UTC
NSE: loaded 45 scripts for scanning.
Initiating Ping Scan at 01:31
Scanning 10.102.11.237 [2 ports]
Completed Ping Scan at 01:31, 0.00s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 01:31
Completed Parallel DNS resolution of 1 host. at 01:31, 0.00s elapsed
Initiating Connect Scan at 01:31
Scanning ip-10-102-11-237.eu-west-1.compute.internal (10.102.11.237) [1 port]
Discovered open port 110/tcp on 10.102.11.237
Completed Connect Scan at 01:31, 0.00s elapsed (1 total ports)
Initiating Service scan at 01:31
Scanning 1 service on ip-10-102-11-237.eu-west-1.compute.internal (10.102.11.
237)
Completed Service scan at 01:31, 0.01s elapsed (1 service on 1 host)
NSE: Script scanning 10.102.11.237.
Initiating NSE at 01:31
Completed NSE at 01:31, 0.00s elapsed
Initiating NSE at 01:31
Completed NSE at 01:31, 0.00s elapsed
Nmap scan report for ip-10-102-11-237.eu-west-1.compute.internal (10.102.11.2
37)
Host is up (0.00058s latency).

PORT      STATE SERVICE VERSION
110/tcp   open  pop3  Dovecot pop3d
Service Info: Host: snailmailreadyforaction

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.35 seconds
```

Question 7: From the prior banner grab, one of the open ports was on 35469, with a service called unknown.

```
Completed NSE at 00:40, 7.02s elapsed
Initiating NSE at 00:40
Completed NSE at 00:40, 1.06s elapsed
Nmap scan report for ip-10-102-11-237.eu-west-1.compute.internal (10.102.11.2
37)
Host is up (0.00045s latency).
Not shown: 65529 closed tcp ports (conn-refused)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp?
25/tcp    open  smtp
80/tcp    open  http    nginx 1.14.0
110/tcp   open  pop3   Dovecot pop3d
443/tcp   open  ssl/http nginx 1.14.0
35469/tcp open  unknown
3 services unrecognized despite returning data. If you know the service/version,
please submit the following fingerprints at https://nmap.org/cgi-bin/submit
.cgi?new-service :
=====NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)=====
SF-Port21-TCP:V=7,92%I=7%D=9/22%Time=632BAE5BXP=x86_64-pc-linux-gnu%R(NULL
SF:,20,"220\x20Come\x20find\x20your\x20token!\x20d363\r\n")%r(GenericLines
```

Question 7 of 8

There is an unknown service running that is not on the list of top 1000 ports. Which port is it running on?

35469

Correct

Question 8: The banner grab ran on the aforementioned port, using the command, nmap -sV -v -p 35469 10.120.11.237 returned its fingerprint and the token as 2137.

```
File Actions Edit View Help
Completed Parallel DNS resolution of 1 host. at 01:35, 0.00s elapsed
Initiating Connect Scan at 01:35
Scanning ip-10-102-11-237.eu-west-1.compute.internal (10.102.11.237) [1 port]
Discovered open port 35469/tcp on 10.102.11.237
Completed Connect Scan at 01:35, 0.00s elapsed (1 total ports)
Initiating Service scan at 01:35
Scanning 1 service on ip-10-102-11-237.eu-west-1.compute.internal (10.102.11.
237)
Completed Service scan at 01:37, 156.15s elapsed (1 service on 1 host)
NSE: Script scanning 10.102.11.237.
Initiating NSE at 01:37
Completed NSE at 01:37, 7.00s elapsed
Initiating NSE at 01:37
Completed NSE at 01:37, 1.00s elapsed
Nmap scan report for ip-10-102-11-237.eu-west-1.compute.internal (10.102.11.2
37)
Host is up (0.00061s latency).

PORT      STATE SERVICE VERSION
35469/tcp open  unknown
1 service unrecognized despite returning data. If you know the service/version,
please submit the following fingerprint at https://nmap.org/cgi-bin/submit
.cgi?new-service :
SF-Port35469-TCP:V=7,92%I=7%D=9/22%Time=632BBCA5P=x86_64-pc-linux-gnu%R(N
SF:UL,F,"token\x20is\x202137\r\n")%r(GenericLines,F,"token\x20is\x202137\
SF:\r\n")%r(RPCCheck,F,"token\x20is\x202137\r\n")%r(DNSVersionBindReqTCP,F,
SF:"token\x20is\x202137\r\n")%r(TerminalServer,F,"token\x20is\x202137\r\n"
SF:)%r(WMSRequest,F,"token\x20is\x202137\r\n")%r(oracle-tns,F,"token\x20is
SF:\x202137\r\n")%r(ms-sql-s,F,"token\x20is\x202137\r\n")%r(afp,F,"token\x
SF:20is\x202137\r\n");

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 164.51 seconds
```

Correct

Question 7 of 8

There is an unknown service running that is not on the list of top 1000 ports. Which port is it running on?

35469

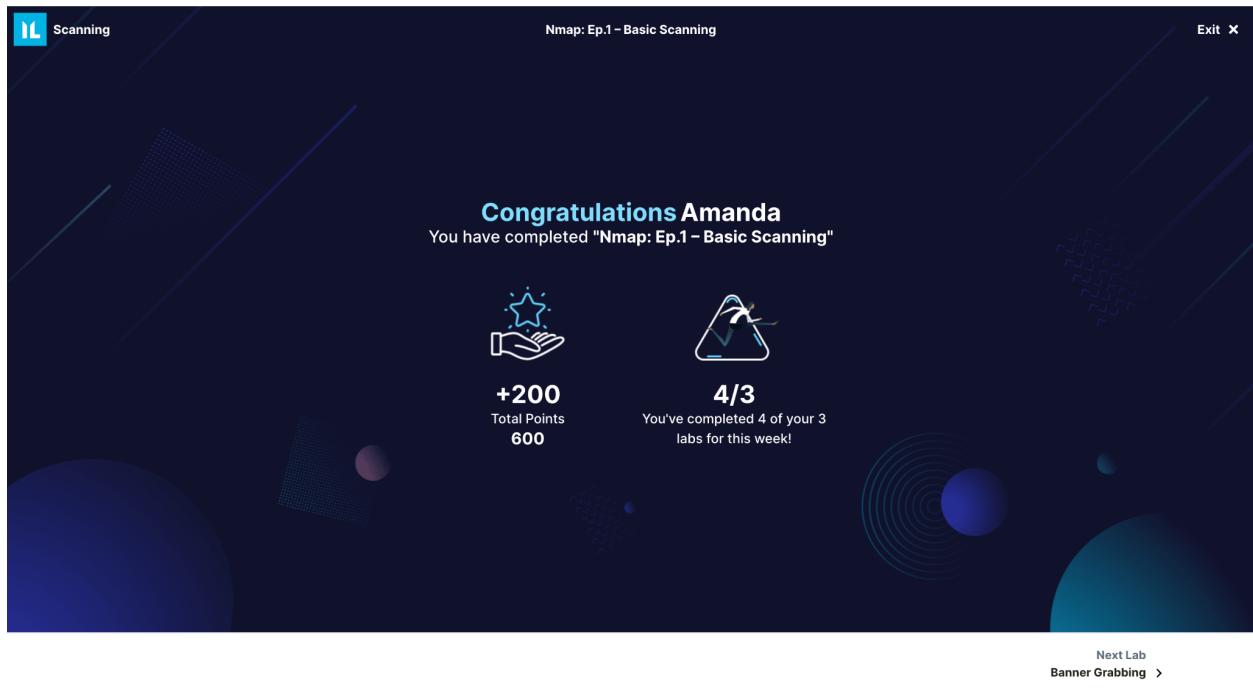
Correct

Question 8 of 8

Run a banner grab scan on the port found from the previous question. What is the token shown?

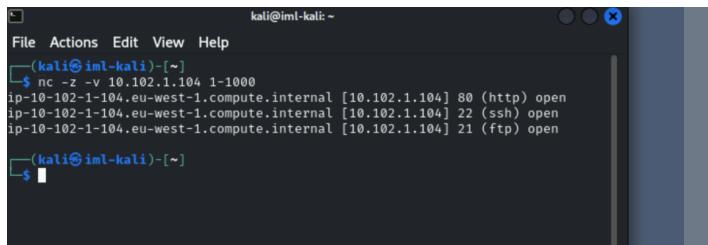
2137

Result:



Network Scanning

Question 1: I performed a port scan by specifying the option -z, and giving the target IP along with the range of 1-1000 ports in the command to find that 3 open ports were returned.

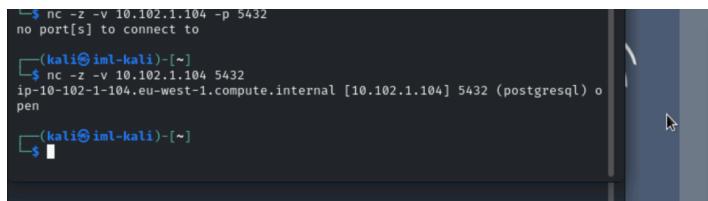


A terminal window titled "kali@iml-kali: ~". The user runs the command "nc -z -v 10.102.1.104 1-1000". The output shows three open ports: 80 (http), 22 (ssh), and 21 (ftp). The terminal prompt is "(kali㉿iml-kali) [~] \$".

Question 1 of 5
Use Netcat to perform a port scan of the first 1000 ports. How many open ports are returned?

Correct

Question 2: To do a port scan on just one port, instead of providing a range I provided the specific port. The service running on the port was returned as postgresql.



A terminal window titled "kali@iml-kali: ~". The user runs the command "nc -z -v 10.102.1.104 5432". The output shows port 5432 is open and running the postgresql service. The terminal prompt is "(kali㉿iml-kali) [~] \$".

Scan port 5432 using Netcat. What is the service running on this port?

Correct

Question 3: Doing the same process as from question 2, instead of seeing a service, a connection refused message was returned.

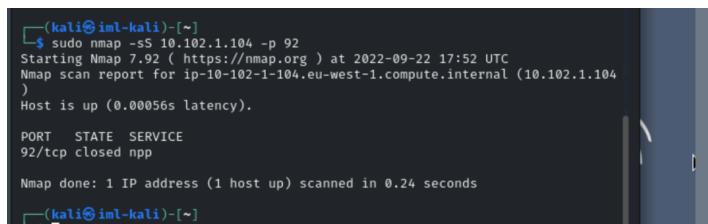


A terminal window titled "kali@iml-kali: ~". The user runs the command "nc -z -v 10.102.1.104 92". The output shows a connection refused message. The terminal prompt is "(kali㉿iml-kali) [~] \$".

Question 3 of 5
Scan port 92 using Netcat. What is the message shown?

Correct

Question 4: To do a port scan with Nmap, I used the option -sS which provides a half TCP SYN scan, and I specified the port 92. The state of the port was closed.



A terminal window titled "kali@iml-kali: ~". The user runs the command "sudo nmap -sS 10.102.1.104 -p 92". The output shows a basic SYN scan for port 92, which is closed. The terminal prompt is "(kali㉿iml-kali) [~] \$".

Question 4 of 5
Now, using Nmap, scan port 92 with a basic SYN scan. What is the status of the port?

Correct

Question 5: The same SYN scan was done for question 5, but instead of specifying one specific port, I used the option –top-ports to scan the top 1000 ports.

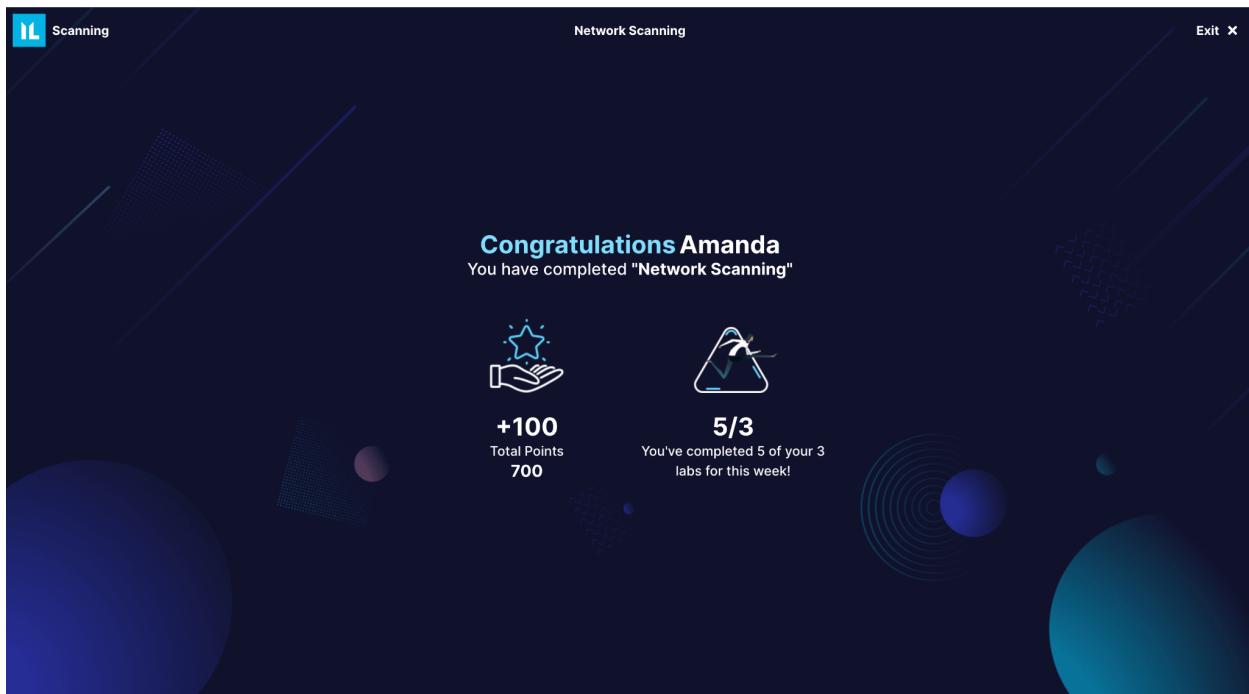
(kali㉿iml-kali) [~]\$ sudo nmap -sS 10.102.1.104 --top-ports 1000
Starting Nmap 7.92 (https://nmap.org) at 2022-09-22 17:53 UTC
Nmap scan report for ip-10-102-1-104.eu-west-1.compute.internal (10.102.1.104)
Host is up (0.00040s latency).
Not shown: 994 closed tcp ports (reset)
PORT STATE SERVICE
21/tcp open ftp
22/tcp open ssh
80/tcp open http
3306/tcp open mysql
5432/tcp open postgresql
31337/tcp open Elite
Nmap done: 1 IP address (1 host up) scanned in 0.30 seconds

(kali㉿iml-kali) [~]\$

The challenge interface shows the following:

- A box containing "closed" with a "Correct" button below it.
- A box labeled "Question 5 of 5" with the question: "Using Nmap, perform a basic SYN scan of the most common 1000 ports. How many open ports are returned?"
- An input field for the answer.

Result:



Writeup

There are a multitude of tools that can be used to analyze the traffic on a network. To get details on packets, we used Wireshark which provided a user-friendly GUI and filter system to narrow down on exchanges between source and destination. Specifically, I learned how to export a packet as a png file to view its content, which could be used to exploit weaknesses. Similarly, we used tcpdump to analyze packets via the command line, because there was no GUI, I had to filter my scans more technically, following the options in the guide for tcpdump. Further, Nmap

was used to single in on ports and their state. I was able to determine which ports were open in UDP or TCP, and ran a banner scan where I learned about a service print for unrecognized services. Finally, NetCat was used to port scan to identify services and connection messages.