

OLD DOMINION UNIVERSITY
CYSE 301 CYBERSECURITY TECHNIQUES AND OPERATIONS

ASSIGNMENT #2 – TRAFFIC TRACING AND SNIFFING

Name: Anna Mae Boubacar

UIN: 01242988

Course #: CYSE301_14735

Q1. How many packets are captured in total? How many packets are displayed?

96

Measurement	Captured	Displayed
Packets	96	96 (100.0%)
Time span, s	75.213	75.213
Average pps	1.3	1.3
Average packet size	70	70

Q2. Apply "ICMP" as a display filter in Wireshark. Then repeat the previous question (Q1).

The screenshot shows the Wireshark interface with the display filter 'icmp' applied. The packet list pane shows 40 ICMP packets. The packet details pane shows the details of the selected packet (No. 3), which is an ICMPv6 Router Solicitation message.

No.	Time	Source	Destination	Protocol	Length	Info
23	22.863932500	192.168.217.3	192.168.10.18	ICMP	98	Echo (ping) request id=0xca80, seq=...
24	22.866113700	192.168.10.18	192.168.217.3	ICMP	98	Echo (ping) reply id=0xca80, seq=...
25	23.865703800	192.168.217.3	192.168.10.18	ICMP	98	Echo (ping) request id=0xca80, seq=...
26	23.877140000	192.168.10.18	192.168.217.3	ICMP	98	Echo (ping) reply id=0xca80, seq=...
27	24.867118400	192.168.217.3	192.168.10.18	ICMP	98	Echo (ping) request id=0xca80, seq=...
28	24.884040300	192.168.10.18	192.168.217.3	ICMP	98	Echo (ping) reply id=0xca80, seq=...
33	25.868474600	192.168.217.3	192.168.10.18	ICMP	98	Echo (ping) request id=0xca80, seq=...
34	25.885356300	192.168.10.18	192.168.217.3	ICMP	98	Echo (ping) reply id=0xca80, seq=...
35	26.869974100	192.168.217.3	192.168.10.18	ICMP	98	Echo (ping) request id=0xca80, seq=...
36	26.871740900	192.168.10.18	192.168.217.3	ICMP	98	Echo (ping) reply id=0xca80, seq=...
37	27.871394700	192.168.217.3	192.168.10.18	ICMP	98	Echo (ping) request id=0xca80, seq=...
38	27.876164400	192.168.10.18	192.168.217.3	ICMP	98	Echo (ping) reply id=0xca80, seq=...
39	28.872176800	192.168.217.3	192.168.10.18	ICMP	98	Echo (ping) request id=0xca80, seq=...
40	28.874815200	192.168.10.18	192.168.217.3	ICMP	98	Echo (ping) reply id=0xca80, seq=...

No.	Time	Source	Destination	Protocol	Length	Info
3	31.269631200	fe80::cb74:1461:858...	ff02::2	ICMPv6	62	Router Solicit...

Q3. Select an Echo (reply) message from the list. What are the source and destination IPs of this packet? What are the sequence number and the size of the data? What is the response time?

Source: 192.168.10.18

Destination: 192.168.217.3

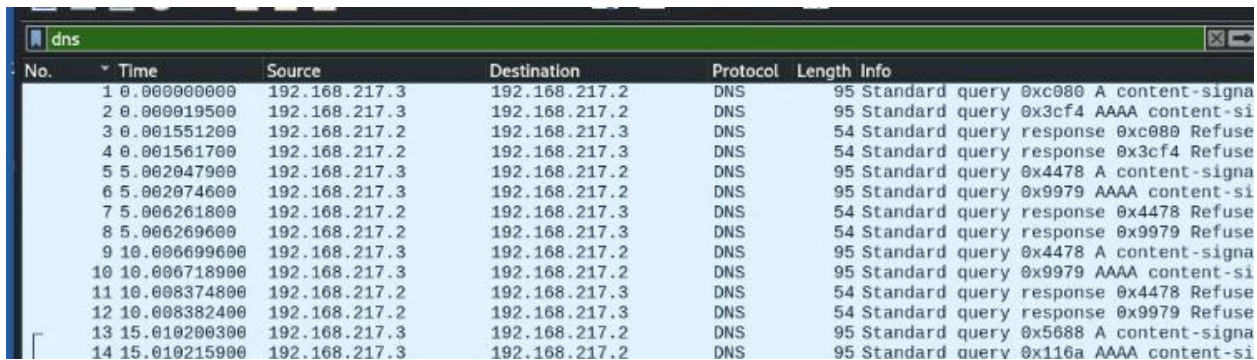
Sequence number: 1

Response time: 2.181 ms

```
Source Address: 192.168.10.18
Destination Address: 192.168.217.3
Internet Control Message Protocol
Type: 0 (Echo (ping) reply)
Code: 0
Checksum: 0x9c4d [correct]
[Checksum Status: Good]
Identifier (BE): 51840 (0xca80)
Identifier (LE): 32970 (0x80ca)
Sequence Number (BE): 1 (0x0001)
Sequence Number (LE): 256 (0x0100)
```

Q4. Apply “DNS” as a display filter in Wireshark. How many packets are displayed?

295



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.217.3	192.168.217.2	DNS	95	Standard query 0xc080 A content-signa
2	0.000019500	192.168.217.3	192.168.217.2	DNS	95	Standard query 0x3cf4 AAAA content-si
3	0.001551200	192.168.217.2	192.168.217.3	DNS	54	Standard query response 0xc080 Refuse
4	0.001561700	192.168.217.2	192.168.217.3	DNS	54	Standard query response 0x3cf4 Refuse
5	5.002047900	192.168.217.3	192.168.217.2	DNS	95	Standard query 0x4478 A content-signa
6	5.002074600	192.168.217.3	192.168.217.2	DNS	95	Standard query 0x9979 AAAA content-si
7	5.006261800	192.168.217.2	192.168.217.3	DNS	54	Standard query response 0x4478 Refuse
8	5.006269600	192.168.217.2	192.168.217.3	DNS	54	Standard query response 0x9979 Refuse
9	10.006699600	192.168.217.3	192.168.217.2	DNS	95	Standard query 0x4478 A content-signa
10	10.006718900	192.168.217.3	192.168.217.2	DNS	95	Standard query 0x9979 AAAA content-si
11	10.008374800	192.168.217.2	192.168.217.3	DNS	54	Standard query response 0x4478 Refuse
12	10.008382400	192.168.217.2	192.168.217.3	DNS	54	Standard query response 0x9979 Refuse
13	15.010200300	192.168.217.3	192.168.217.2	DNS	95	Standard query 0x5688 A content-signa
14	15.010215900	192.168.217.3	192.168.217.2	DNS	95	Standard query 0x116a AAAA content-si

Q5. Find a DNS query packet. What is the domain name this host is trying to resolve? What is the source IP and port number, destination IP and port number? Please express in the format: IP:port.

Source IP: 192.168.217.3/port: 40122

Destination: 192.168.217.2/port: 53

```
[Header: checksum status: overflight]
Source Address: 192.168.217.3
Destination Address: 192.168.217.2
User Datagram Protocol, Src Port: 40122, Dst Port: 53
Domain Name System (query)
Transaction ID: 0x3cf4
Flags: 0x0100 Standard query
Questions: 1
```

Q6. Find the corresponding DNS response to the query you selected at the previous step, and what is the source IP and port number, destination IP and port number? What is the message replied from the DNS server?

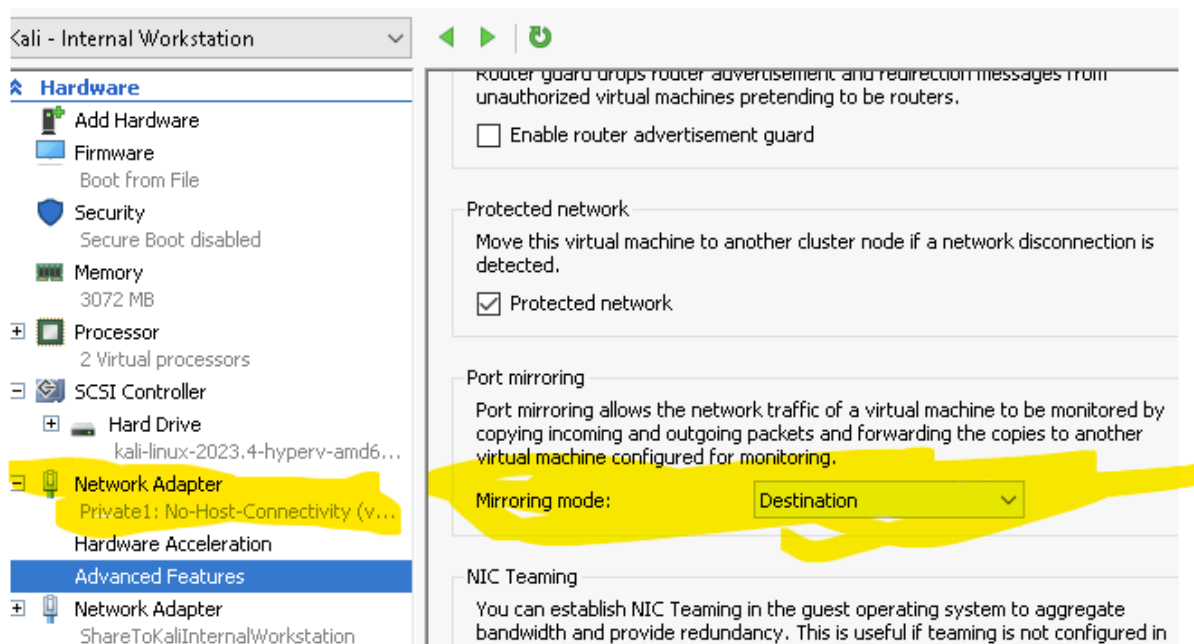
Source IP: 192.168.217.2/port: 53

Destination: 192.168.217.3/port: 40122

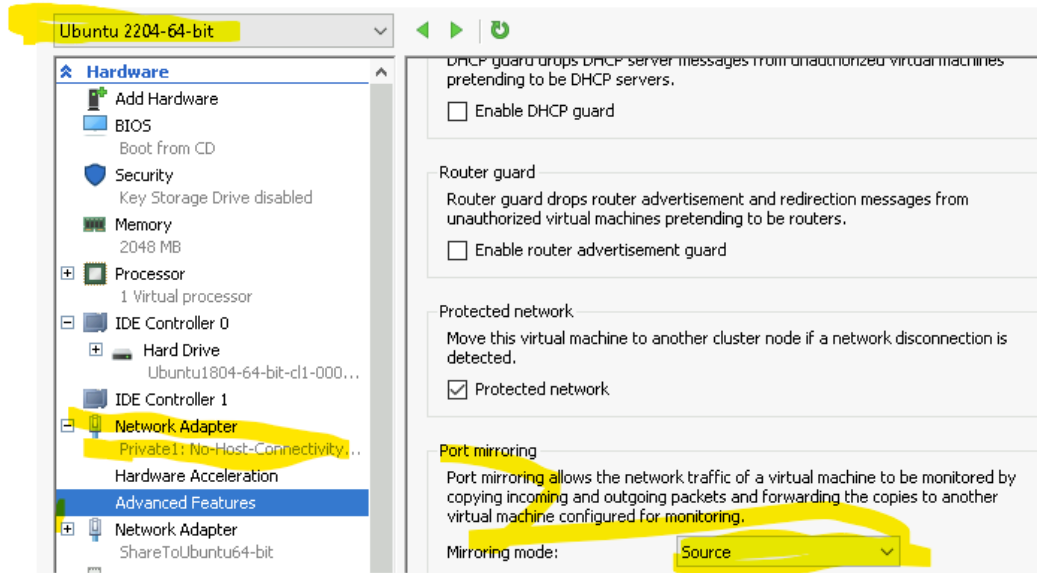
```
Source Address: 192.168.217.2
Destination Address: 192.168.217.3
User Datagram Protocol, Src Port: 53, Dst Port: 40122
Domain Name System (response)
Transaction ID: 0xc080
Flags: 0x8105 Standard query response, Refused
Questions: 0
Answer RRs: 0
```

Task B: Sniff LAN traffic

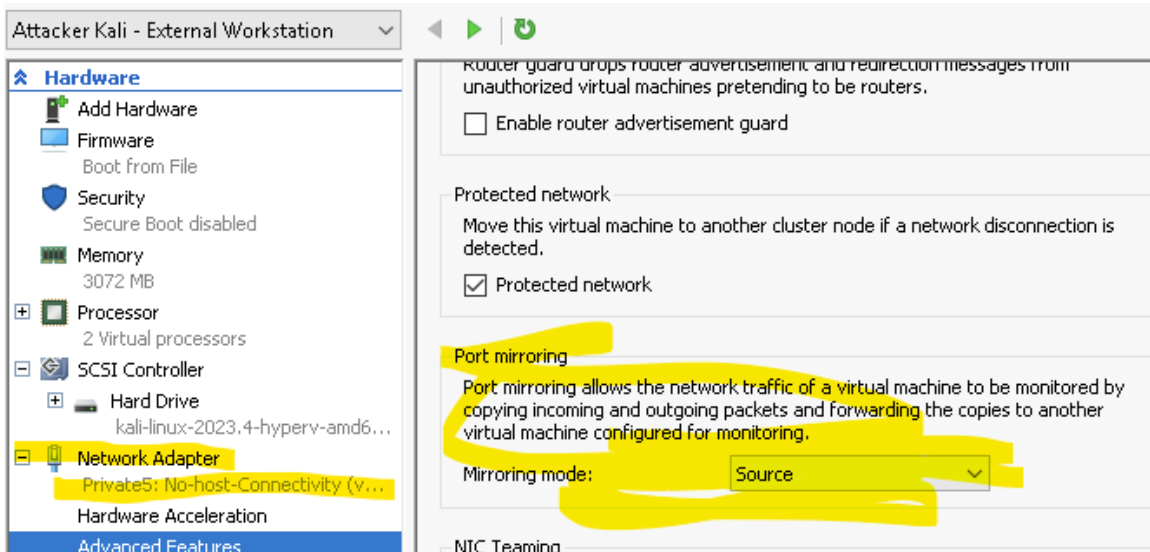
- Internal Kali: Set Mirroring mode to “Destination” in the “Port Mirroring”



- Ubuntu Kali: Set Mirroring mode to “Source” in the “Port Mirroring”



- External Kali: Set Mirroring mode to “Source” in the “Port Mirroring”



1. Sniff ICMP traffic (10 + 10 = 20 points)

a. Apply proper display or capture filter in Wireshark on Internal Kali VM to show active ICMP traffic.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.217.3	192.168.10.13	ICMP	98	Echo (ping) request id=0xd1e2, seq=119/30464, ttl=63 (reply in 2)
2	0.000039400	192.168.10.13	192.168.217.3	ICMP	98	Echo (ping) reply id=0xd1e2, seq=119/30464, ttl=64 (request in 1)
3	0.998370100	192.168.217.3	192.168.10.13	ICMP	98	Echo (ping) request id=0xd1e2, seq=120/30720, ttl=63 (reply in 4)
4	0.998403900	192.168.10.13	192.168.217.3	ICMP	98	Echo (ping) reply id=0xd1e2, seq=120/30720, ttl=64 (request in 3)
5	2.002751000	192.168.217.3	192.168.10.13	ICMP	98	Echo (ping) request id=0xd1e2, seq=121/30976, ttl=63 (reply in 6)
6	2.002790100	192.168.10.13	192.168.217.3	ICMP	98	Echo (ping) reply id=0xd1e2, seq=121/30976, ttl=64 (request in 5)
7	2.999967900	192.168.217.3	192.168.10.13	ICMP	98	Echo (ping) request id=0xd1e2, seq=122/31232, ttl=63 (reply in 8)
8	2.999999400	192.168.10.13	192.168.217.3	ICMP	98	Echo (ping) reply id=0xd1e2, seq=122/31232, ttl=64 (request in 7)
9	4.002106800	192.168.217.3	192.168.10.13	ICMP	98	Echo (ping) request id=0xd1e2, seq=123/31488, ttl=63 (reply in 10)
10	4.002151700	192.168.10.13	192.168.217.3	ICMP	98	Echo (ping) reply id=0xd1e2, seq=123/31488, ttl=64 (request in 9)
11	5.003740900	192.168.217.3	192.168.10.13	ICMP	98	Echo (ping) request id=0xd1e2, seq=124/31744, ttl=63 (reply in 12)
12	5.003777600	192.168.10.13	192.168.217.3	ICMP	98	Echo (ping) reply id=0xd1e2, seq=124/31744, ttl=64 (request in 11)
13	6.010238700	192.168.217.3	192.168.10.13	ICMP	98	Echo (ping) request id=0xd1e2, seq=125/32000, ttl=63 (reply in 14)
14	6.010274300	192.168.10.13	192.168.217.3	ICMP	98	Echo (ping) reply id=0xd1e2, seq=125/32000, ttl=64 (request in 13)
15	7.019716500	192.168.217.3	192.168.10.13	ICMP	98	Echo (ping) request id=0xd1e2, seq=126/32256, ttl=63 (reply in 16)
16	7.019751300	192.168.10.13	192.168.217.3	ICMP	98	Echo (ping) reply id=0xd1e2, seq=126/32256, ttl=64 (request in 15)

b. Apply a proper display or capture filter on the internal Kali VM that ONLY displays the ICMP request that originated from the external Kali VM and goes to the Ubuntu 64-bit VM.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.217.3	192.168.10.18	ICMP	98	Echo (ping) request id=0x3347, seq=33/8448, ttl=63 (reply in 2)
7	1.003138500	192.168.217.3	192.168.10.18	ICMP	98	Echo (ping) request id=0x3347, seq=34/8704, ttl=63 (reply in 8)
11	2.008360400	192.168.217.3	192.168.10.18	ICMP	98	Echo (ping) request id=0x3347, seq=35/8960, ttl=63 (reply in 12)
15	3.009557400	192.168.217.3	192.168.10.18	ICMP	98	Echo (ping) request id=0x3347, seq=36/9216, ttl=63 (reply in 16)
19	4.009084600	192.168.217.3	192.168.10.18	ICMP	98	Echo (ping) request id=0x3347, seq=37/9472, ttl=63 (reply in 20)
23	5.014022800	192.168.217.3	192.168.10.18	ICMP	98	Echo (ping) request id=0x3347, seq=38/9728, ttl=63 (reply in 24)
27	6.014398600	192.168.217.3	192.168.10.18	ICMP	98	Echo (ping) request id=0x3347, seq=39/9984, ttl=63 (reply in 28)
31	7.014824700	192.168.217.3	192.168.10.18	ICMP	98	Echo (ping) request id=0x3347, seq=40/10240, ttl=63 (reply in 32)
35	8.018518800	192.168.217.3	192.168.10.18	ICMP	98	Echo (ping) request id=0x3347, seq=41/10496, ttl=63 (reply in 36)
39	9.021681000	192.168.217.3	192.168.10.18	ICMP	98	Echo (ping) request id=0x3347, seq=42/10752, ttl=63 (reply in 40)
43	10.022861800	192.168.217.3	192.168.10.18	ICMP	98	Echo (ping) request id=0x3347, seq=43/11008, ttl=63 (reply in 44)
47	11.027620600	192.168.217.3	192.168.10.18	ICMP	98	Echo (ping) request id=0x3347, seq=44/11264, ttl=63 (reply in 48)
51	12.038960900	192.168.217.3	192.168.10.18	ICMP	98	Echo (ping) request id=0x3347, seq=45/11520, ttl=63 (reply in 52)
55	13.028875600	192.168.217.3	192.168.10.18	ICMP	98	Echo (ping) request id=0x3347, seq=46/11776, ttl=63 (reply in 56)
59	14.046652000	192.168.217.3	192.168.10.18	ICMP	98	Echo (ping) request id=0x3347, seq=47/12032, ttl=63 (reply in 60)
63	15.045118000	192.168.217.3	192.168.10.18	ICMP	98	Echo (ping) request id=0x3347, seq=48/12288, ttl=63 (reply in 64)

2. Sniff FTP traffic (10 + 15 + 15 = 40 pts points)

a. Ubuntu VM is also serving as an FTP server inside the LAN network. Now, you need to use External Kali to access this FTP server by using the command: ftp [ip_addr of ubuntu VM]. The

username for the FTP server is student, and the password is password. You can follow the steps below to access the FTP server.

b. Unfortunately, Internal Kali, the attacker, is also sniffing into the communication. Therefore, all of your communication is exposed to the attacker. Now, you need to find out the password used by External Kali to access the FTP server from the intercepted traffic on Internal Kali. You need to take a screenshot and explain how you found the password

No.	Time	Source	Destination	Protocol	Length	Info
311	75.142107500	192.168.10.18	192.168.217.3	FTP	86	Response: 220 (vsFTPd 3.0.5)
361	86.626014200	192.168.217.3	192.168.10.18	FTP	80	Request: USER student
363	86.626619400	192.168.10.18	192.168.217.3	FTP	100	Response: 331 Please specify the password.
383	90.823949200	192.168.217.3	192.168.10.18	FTP	81	Request: PASS password
384	90.835316200	192.168.10.18	192.168.217.3	FTP	89	Response: 230 Login successful.
386	90.838296300	192.168.217.3	192.168.10.18	FTP	72	Request: SYST
387	90.839263200	192.168.10.18	192.168.217.3	FTP	85	Response: 215 UNIX Type: L8
388	90.841124100	192.168.217.3	192.168.10.18	FTP	72	Request: FEAT
389	90.843040400	192.168.10.18	192.168.217.3	FTP	81	Response: 211-Features:
390	90.843048000	192.168.10.18	192.168.217.3	FTP	87	Response: EPRT
391	90.843234600	192.168.10.18	192.168.217.3	FTP	110	Response: PASV

c. After you successfully find the username & password from the FTP traffic, repeat the previous step (2.a), and use your MIDAS ID as the username and UIN as the password to re-access the FTP server from External Kali. Although External Kali may not access the FTP server, you need to intercept the packets containing these “secrets” from the attacker VM, which is Internal Kali.

1127	261.496928500	192.168.10.18	192.168.217.3	FTP	80	Response: 221 Goodbye.
1179	271.769158900	192.168.10.18	192.168.217.3	FTP	86	Response: 220 (vsFTPd 3.0.5)
1265	292.555357100	192.168.217.3	192.168.10.18	FTP	81	Request: USER atabo003
1267	292.556482900	192.168.10.18	192.168.217.3	FTP	100	Response: 331 Please specify the password.
1367	316.943934100	192.168.217.3	192.168.10.18	FTP	81	Request: PASS 01242988
1381	320.154735300	192.168.10.18	192.168.217.3	FTP	88	Response: 530 Login incorrect.