

OLD DOMINION UNIVERSITY  
CYSE 301 CYBERSECURITY TECHNIQUES AND OPERATIONS

---

ASSIGNMENT 2: Traffic Tracing and Sniffing

---

Mary Lelina-Ford

Task A:

## Q1. Packets: 218 Displayed 218

Attacker Kali - External Workstation on CY301-MLEL001 - Virtual Machine Connection

File Action Media View Help

\*eth0

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
204	56.113721400	192.168.10.18	192.168.217.3	ICMP	98	Echo (ping) reply id=0x3180, seq=65/16640, ttl=
205	57.109149400	192.168.217.3	192.168.10.18	ICMP	98	Echo (ping) request id=0x3180, seq=66/16896, ttl=
206	57.111764400	192.168.10.18	192.168.217.3	ICMP	98	Echo (ping) reply id=0x3180, seq=66/16896, ttl=
207	58.111323500	192.168.217.3	192.168.10.18	ICMP	98	Echo (ping) request id=0x3180, seq=67/17152, ttl=
208	58.115368300	192.168.10.18	192.168.217.3	ICMP	98	Echo (ping) reply id=0x3180, seq=67/17152, ttl=
209	58.378937100	192.168.217.3	192.168.217.2	DNS	85	Standard query 0x94da A push.services.mozilla.com
210	58.378956100	192.168.217.3	192.168.217.2	DNS	85	Standard query 0xc9a AAAA push.services.mozilla.c
211	58.381725900	192.168.217.2	192.168.217.3	DNS	54	Standard query response 0x94da Refused
212	58.381733600	192.168.217.2	192.168.217.3	DNS	54	Standard query response 0xc9a Refused
213	58.663061300	192.168.217.3	192.168.217.2	DNS	95	Standard query 0x1329 A content-signature-2.cdn.mo
214	58.663083100	192.168.217.3	192.168.217.2	DNS	95	Standard query 0xc9c AAAA content-signature-2.cdn
215	58.670712500	192.168.217.2	192.168.217.3	DNS	54	Standard query response 0x1329 Refused
216	58.670719900	192.168.217.2	192.168.217.3	DNS	54	Standard query response 0xc9c Refused
217	59.112787600	192.168.217.3	192.168.10.18	ICMP	98	Echo (ping) request id=0x3180, seq=68/17408, ttl=
218	59.114839100	192.168.10.18	192.168.217.3	ICMP	98	Echo (ping) reply id=0x3180, seq=68/17408, ttl=

Frame 1: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on in  
Ethernet II, Src: Microsoft\_40:57:27 (00:15:5d:40:57:27), Dst: Microsoft\_00:15:5d:40:57:27  
Internet Protocol Version 4, Src: 192.168.217.3, Dst: 192.168.10.18  
Internet Control Message Protocol

0000 00 15 5d 40 57 38 00 15 5d 40 57 27 08 00 45 00  
0010 00 54 d0 44 40 00 01 05 fe c0 a8 d9 03 c0 a8  
0020 0a 12 08 00 29 b5 31 80 00 09 70 71 a6 67 00 00  
0030 00 00 c0 15 07 00 00 00 00 00 10 11 12 13 14 15  
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  
0060 36 37

Activate Window  
Go to Settings to activate window

wireshark\_eth0402V12.pcapng | Packets: 218 - Displayed: 218 (100.0%) - Dropped:

## Q2. Packets: 218 Displayed: 120

Attacker Kali - External Workstation on CY301-MLEL001 - Virtual Machine Connection

File Action Media View Help

\*eth0

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

icmp

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.217.3	192.168.10.18	ICMP	98	Echo (ping) request id=0x3180, seq=9/2304, ttl=64
2	0.002704800	192.168.10.18	192.168.217.3	ICMP	98	Echo (ping) reply id=0x3180, seq=9/2304, ttl=63
3	1.001563800	192.168.217.3	192.168.10.18	ICMP	98	Echo (ping) request id=0x3180, seq=10/2560, ttl=64
4	1.029669400	192.168.10.18	192.168.217.3	ICMP	98	Echo (ping) reply id=0x3180, seq=10/2560, ttl=63
7	2.003409400	192.168.217.3	192.168.10.18	ICMP	98	Echo (ping) request id=0x3180, seq=11/2816, ttl=64
8	2.028894200	192.168.10.18	192.168.217.3	ICMP	98	Echo (ping) reply id=0x3180, seq=11/2816, ttl=63
9	3.004876800	192.168.217.3	192.168.10.18	ICMP	98	Echo (ping) request id=0x3180, seq=12/3072, ttl=64
10	3.021186000	192.168.10.18	192.168.217.3	ICMP	98	Echo (ping) reply id=0x3180, seq=12/3072, ttl=63
23	4.006905900	192.168.217.3	192.168.10.18	ICMP	98	Echo (ping) request id=0x3180, seq=13/3328, ttl=64
24	4.008841700	192.168.10.18	192.168.217.3	ICMP	98	Echo (ping) reply id=0x3180, seq=13/3328, ttl=63
25	5.0008515200	192.168.217.3	192.168.10.18	ICMP	98	Echo (ping) request id=0x3180, seq=14/3584, ttl=64
26	5.022890300	192.168.10.18	192.168.217.3	ICMP	98	Echo (ping) reply id=0x3180, seq=14/3584, ttl=63
27	6.010482300	192.168.217.3	192.168.10.18	ICMP	98	Echo (ping) request id=0x3180, seq=15/3840, ttl=64
28	6.012856700	192.168.10.18	192.168.217.3	ICMP	98	Echo (ping) reply id=0x3180, seq=15/3840, ttl=63
29	7.012645800	192.168.217.3	192.168.10.18	ICMP	98	Echo (ping) request id=0x3180, seq=16/4096, ttl=64
30	7.016820500	192.168.10.18	192.168.217.3	ICMP	98	Echo (ping) reply id=0x3180, seq=16/4096, ttl=63

Frame 1: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on in  
Ethernet II, Src: Microsoft\_40:57:27 (00:15:5d:40:57:27), Dst: Microsoft\_00:15:5d:40:57:27  
Internet Protocol Version 4, Src: 192.168.217.3, Dst: 192.168.10.18  
Internet Control Message Protocol

0000 00 15 5d 40 57 38 00 15 5d 40 57 27 08 00 45 00  
0010 00 54 d0 44 40 00 01 05 fe c0 a8 d9 03 c0 a8  
0020 0a 12 08 00 29 b5 31 80 00 09 70 71 a6 67 00 00  
0030 00 00 c0 15 07 00 00 00 00 00 10 11 12 13 14 15  
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  
0060 36 37

Activate Window  
Go to Settings to activate window

Internet Control Message Protocol: Protocol | Packets: 218 - Displayed: 120 (55.0%) - Dropped:

## Q3. Source: 192.168.217.3 Destination IP: 192.168.10.18

Sequence Number: 29 Size of Data: 98 bytes Response Time: 7.012

Attacker Kali - External Workstation on CY301-MLEI001 - Virtual Machine Connection

File Action Media View Help

1 2 3 4

\*eth0

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

icmp.type==8

No.	Time	Source	Destination	Protocol	Length	Info
10.000000000	192.168.217.3	192.168.10.18	ICMP	98	Echo (ping) request	id=0x3180, seq=9/2384, ttl=64 (reply in 2)
31.001563000	192.168.217.3	192.168.10.18	ICMP	98	Echo (ping) request	id=0x3180, seq=10/2560, ttl=64 (reply in 4)
72.003499400	192.168.217.3	192.168.10.18	ICMP	98	Echo (ping) request	id=0x3180, seq=11/2816, ttl=64 (reply in 8)
93.004876800	192.168.217.3	192.168.10.18	ICMP	98	Echo (ping) request	id=0x3180, seq=12/3072, ttl=64 (reply in 10)
234.006905000	192.168.217.3	192.168.10.18	ICMP	98	Echo (ping) request	id=0x3180, seq=13/3328, ttl=64 (reply in 24)
255.008515200	192.168.217.3	192.168.10.18	ICMP	98	Echo (ping) request	id=0x3180, seq=14/3584, ttl=64 (reply in 26)
276.010482300	192.168.217.3	192.168.10.18	ICMP	98	Echo (ping) request	id=0x3180, seq=15/3840, ttl=64 (reply in 30)
297.012645800	192.168.217.3	192.168.10.18	ICMP	98	Echo (ping) request	id=0x3180, seq=16/4096, ttl=64 (reply in 38)
318.014411400	192.168.217.3	192.168.10.18	ICMP	98	Echo (ping) request	id=0x3180, seq=17/4352, ttl=64 (reply in 32)
459.018615600	192.168.217.3	192.168.10.18	ICMP	98	Echo (ping) request	id=0x3180, seq=18/4608, ttl=64 (reply in 46)
4710.019985700	192.168.217.3	192.168.10.18	ICMP	98	Echo (ping) request	id=0x3180, seq=19/4864, ttl=64 (reply in 48)
4911.021634200	192.168.217.3	192.168.10.18	ICMP	98	Echo (ping) request	id=0x3180, seq=20/5120, ttl=64 (reply in 50)
5112.023255500	192.168.217.3	192.168.10.18	ICMP	98	Echo (ping) request	id=0x3180, seq=21/5376, ttl=64 (reply in 52)
5313.026207700	192.168.217.3	192.168.10.18	ICMP	98	Echo (ping) request	id=0x3180, seq=22/5632, ttl=64 (reply in 54)
6714.027983800	192.168.217.3	192.168.10.18	ICMP	98	Echo (ping) request	id=0x3180, seq=23/5888, ttl=64 (reply in 68)
6915.029663000	192.168.217.3	192.168.10.18	ICMP	98	Echo (ping) request	id=0x3180, seq=24/6144, ttl=64 (reply in 70)

Frame 29: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface eth0  
Ethernet II, Src: Microsoft\_40:57:27 (08:15:5d:40:57:27), Dst: Microsoft\_08:00:00:00:00:00  
Internet Protocol Version 4, Src: 192.168.217.3, Dst: 192.168.10.18  
Internet Control Message Protocol

0000 00 15 5d 40 57 38 00 15 5d 40 57 27 08 00 45 00 ... @w8 ...  
0010 00 54 d4 21 40 00 40 01 02 21 c0 a8 d9 03 c0 a8 ... T!@ @ ...  
0020 0a 12 08 00 b9 7c 31 80 00 10 77 71 a6 67 00 00 ... :G ...  
0030 00 00 29 47 07 00 00 00 00 00 10 11 12 13 14 15 ... )G ...  
0040 10 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 ... &(){}~ ...  
0060 36 37

Activate Windows  
Go to Settings to activate Windows.

wireshark\_eth0402V12.pcapng

Packets: 218 · Displayed: 60 (27.5%) · Dropped: 0 (0.0%) · Profile: Default

Q4. Packets: 218 Display: 92

Attacker Kali - External Workstation on CY301-MLEI001 - Virtual Machine Connection

File Action Media View Help

1 2 3 4

\*eth0

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

dns

No.	Time	Source	Destination	Protocol	Length	Info
153.590880700	192.168.217.3	192.168.217.2	DNS	84	Standard query	0x5640 A ciscobinary.openh2
163.590910200	192.168.217.3	192.168.217.2	DNS	84	Standard query	0x4761 AAAA ciscobinary.openh2
173.593275200	192.168.217.2	192.168.217.3	DNS	54	Standard query response	0x5640 Refused
183.593282500	192.168.217.2	192.168.217.3	DNS	54	Standard query response	0x4761 Refused
193.612029300	192.168.217.3	192.168.217.2	DNS	95	Standard query	0x11e4 A content-signature-
203.612048500	192.168.217.3	192.168.217.2	DNS	95	Standard query	0xed15 AAAA content-signature-
213.614434000	192.168.217.2	192.168.217.3	DNS	54	Standard query response	0x11e4 Refused
223.614441500	192.168.217.2	192.168.217.3	DNS	54	Standard query response	0xed15 Refused
338.362839900	192.168.217.3	192.168.217.2	DNS	85	Standard query	0xb95c A push.services.mozilla
348.362860500	192.168.217.3	192.168.217.2	DNS	85	Standard query	0x937a AAAA push.services.mozilla
358.364225600	192.168.217.2	192.168.217.3	DNS	54	Standard query response	0xb95c Refused
368.364233000	192.168.217.2	192.168.217.3	DNS	54	Standard query response	0x937a Refused
378.592358700	192.168.217.3	192.168.217.2	DNS	84	Standard query	0x553a A ciscobinary.openh2
388.592380800	192.168.217.3	192.168.217.2	DNS	84	Standard query	0x5e65 AAAA ciscobinary.openh2
398.596499600	192.168.217.2	192.168.217.3	DNS	54	Standard query response	0x553a Refused

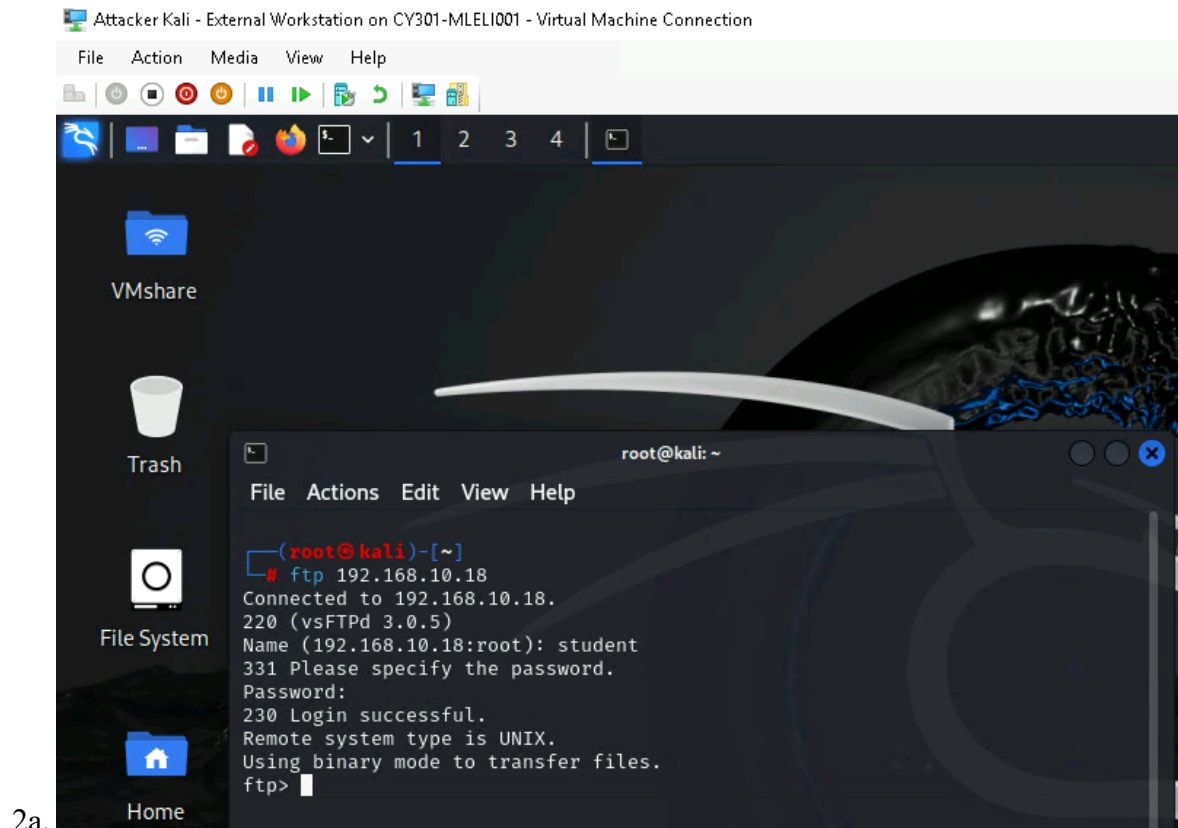
Frame 22: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface eth0  
Ethernet II, Src: Microsoft\_40:57:38 (08:15:5d:40:57:38), Dst: Microsoft\_08:00:00:00:00:00  
Internet Protocol Version 4, Src: 192.168.217.2, Dst: 192.168.217.3  
User Datagram Protocol, Src Port: 53, Dst Port: 38656  
Domain Name System (response)

0000 00 15 5d 40 57 27 00 15 5d 40 57 38 00 00 00 ... @w8 ...  
0010 00 28 ea 92 00 00 40 11 5c db c0 a8 d9 ... T!@ @ ...  
0020 d0 03 00 35 07 00 00 14 c7 1d ed 15 81 ... :G ...  
0030 00 00 00 00 00 00

Activate Windows  
Go to Settings to activate Windows.

Domain Name System: Protocol

Packets: 218 · Displayed: 92 (42.2%)



2b. To find out the password used by external Kali. I used the Wireshark in Internal Kali and filtered it to ftp. It says on the information the requests and responses which gave me the password/username for Ubuntu.

