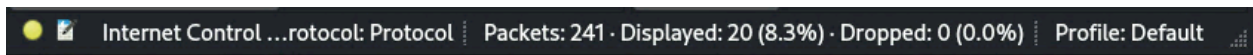
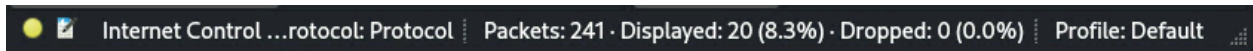


TASK A

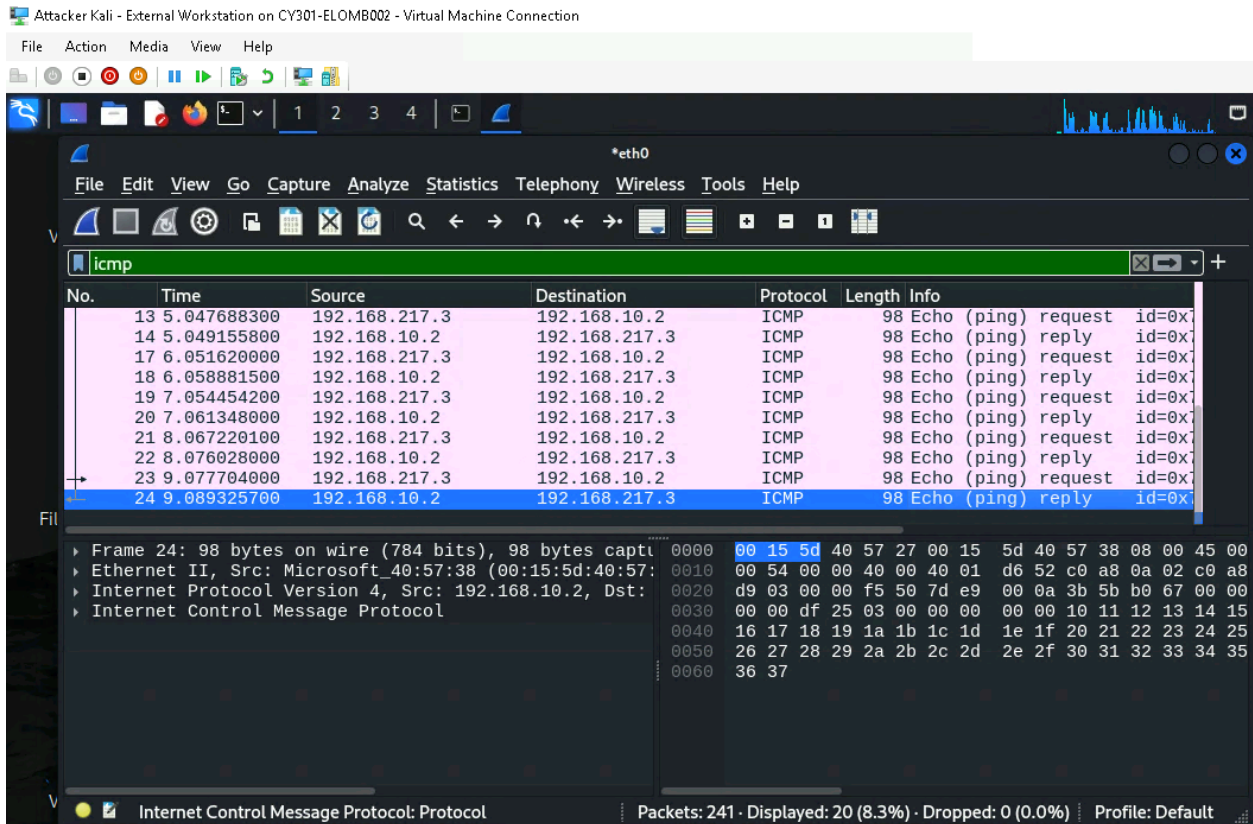
q1



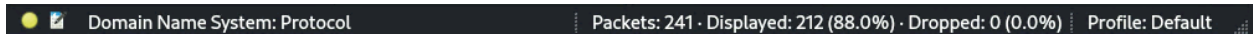
Q2



q3



q4



q5

Attacker Kali - External Workstation on CY301-ELOMB002 - Virtual Machine Connection

File Action Media View Help

1 2 3 4

(genmon)XXX

*eth0

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

dns

Time	Source	Destination	Protocol	Length	Info
232	108.379380000	192.168.217.2	DNS	54	Standard query response 0x6fa0 Refused
233	108.379392700	192.168.217.2	DNS	54	Standard query response 0x5a68 Refused
234	108.613580600	192.168.217.3	DNS	87	Standard query 0x16ec A services.addons.mozill
235	108.613611700	192.168.217.3	DNS	87	Standard query 0xbcbec AAAA services.addons.moz
236	108.630917900	192.168.217.2	DNS	54	Standard query response 0x16ec Refused
237	108.630930900	192.168.217.2	DNS	54	Standard query response 0xbcbec Refused
238	111.401766300	192.168.217.2	DNS	79	Standard query 0xf00b A spocs.getpocket.com
239	111.401802800	192.168.217.3	DNS	79	Standard query 0xe047 AAAA spocs.getpocket.com
240	111.415330700	192.168.217.2	DNS	54	Standard query response 0xf00b Refused
241	111.415343400	192.168.217.2	DNS	54	Standard query response 0xe047 Refused

File

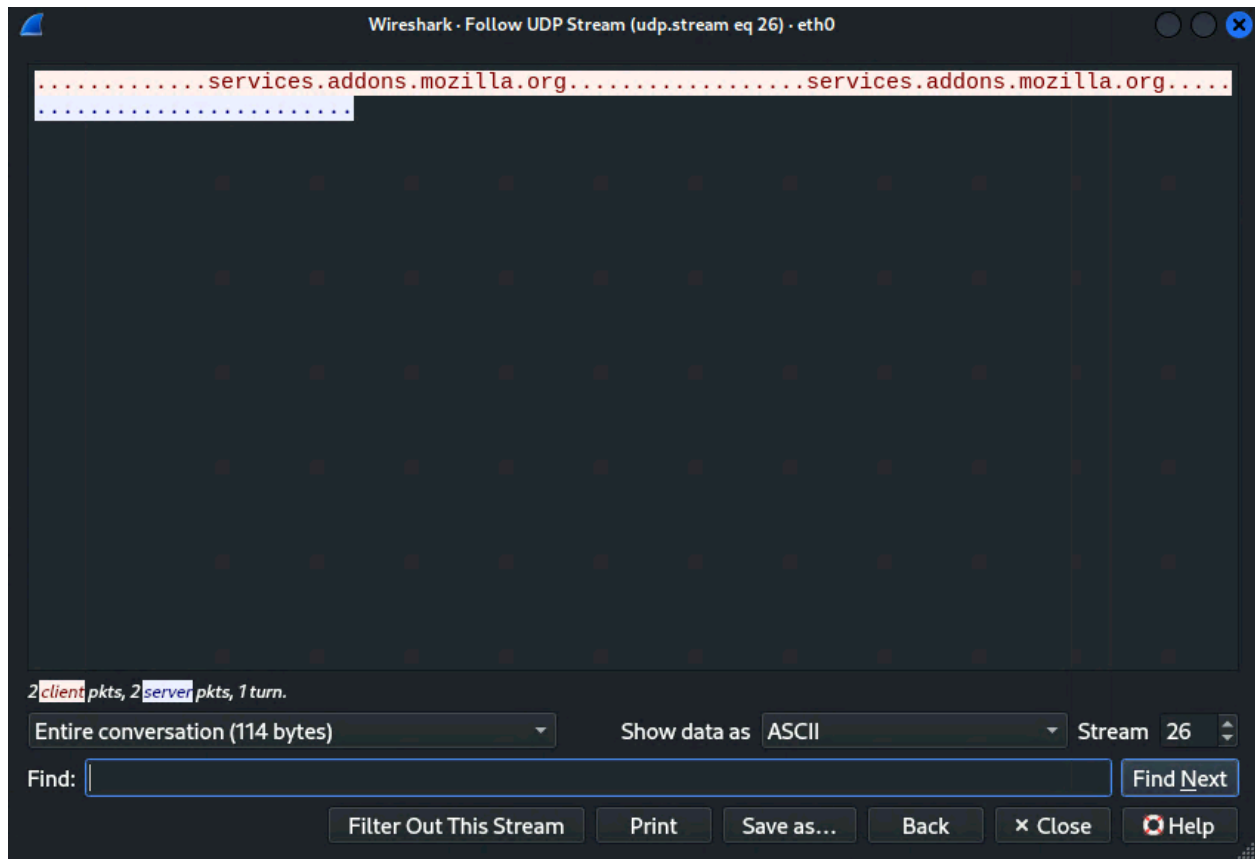
Frame 235: 87 bytes on wire (696 bits), 87 bytes captured (696 bits) on interface eth0, id 0

- Ethernet II, Src: Microsoft_40:57:27 (00:15:5d:40:57:27), Dst: Microsoft_40:57:38 (00:15:5d:40:57:38)
- Internet Protocol Version 4, Src: 192.168.217.3, Dst: 192.168.217.2
- User Datagram Protocol, Src Port: 44960, Dst Port: 53
- Domain Name System (query)

Domain Name System: Protocol

Packets: 241 · Displayed: 212 (88.0%) · Dropped: 0 (0.0%) · Profile: Default

Q6



TASK B

Q1

The screenshot shows a Wireshark capture of ICMP traffic on interface eth0. The packet list displays 23 packets, all of which are Echo (ping) requests and replies between 192.168.10.13 and 192.168.217.3. The packet details pane shows the structure of a selected packet: Ethernet II, Internet Protocol Version 4, and Internet Control Message Protocol.

No.	Time	Source	Destination	Protocol	Length	Info
12	128.909116800	192.168.217.3	192.168.10.13	ICMP	98	Echo (ping) request id=0x5705, seq=6/1536, ttl=63 (reply in ...)
13	128.909168700	192.168.10.13	192.168.217.3	ICMP	98	Echo (ping) reply id=0x5705, seq=6/1536, ttl=64 (request in ...)
16	129.913174000	192.168.217.3	192.168.10.13	ICMP	98	Echo (ping) request id=0x5705, seq=7/1792, ttl=63 (reply in ...)
17	129.913227300	192.168.10.13	192.168.217.3	ICMP	98	Echo (ping) reply id=0x5705, seq=7/1792, ttl=64 (request in ...)
18	130.913545700	192.168.217.3	192.168.10.13	ICMP	98	Echo (ping) request id=0x5705, seq=8/2048, ttl=63 (reply in ...)
19	130.913598700	192.168.10.13	192.168.217.3	ICMP	98	Echo (ping) reply id=0x5705, seq=8/2048, ttl=64 (request in ...)
20	131.921201600	192.168.217.3	192.168.10.13	ICMP	98	Echo (ping) request id=0x5705, seq=9/2304, ttl=63 (reply in ...)
21	131.921255100	192.168.10.13	192.168.217.3	ICMP	98	Echo (ping) reply id=0x5705, seq=9/2304, ttl=64 (request in ...)
22	132.917751300	192.168.217.3	192.168.10.13	ICMP	98	Echo (ping) request id=0x5705, seq=10/2560, ttl=63 (reply in ...)
23	132.917806000	192.168.10.13	192.168.217.3	ICMP	98	Echo (ping) reply id=0x5705, seq=10/2560, ttl=64 (request in ...)

Q2

The screenshot shows a Wireshark capture of FTP traffic on interface eth0. The packet list displays 17 packets, including requests for user login and password specification, and responses from the server.

No.	Time	Source	Destination	Protocol	Length	Info
10	9.619557100	192.168.10.18	192.168.217.3	FTP	86	Response: 220 (vsFTPD 3.0.5)
12	14.354218200	192.168.217.3	192.168.10.18	FTP	80	Request: USER student
14	14.354244000	192.168.10.18	192.168.217.3	FTP	100	Response: 331 Please specify the password.
16	18.078148800	192.168.217.3	192.168.10.18	FTP	81	Request: PASS password
17	18.122264300	192.168.10.18	192.168.217.3	FTP	89	Response: 230 Login successful.

Q3

The screenshot shows a Wireshark capture of FTP traffic on interface eth0. The packet list displays 17 packets, including requests for user login and password specification, and responses from the server.

No.	Time	Source	Destination	Protocol	Length	Info
22	18.146807200	192.168.10.18	192.168.217.3	FTP	81	Response: 211-Features:
23	18.146819500	192.168.10.18	192.168.217.3	FTP	87	Response: EPRT
24	18.146831800	192.168.10.18	192.168.217.3	FTP	110	Response: PASV
27	54.570826500	192.168.217.3	192.168.10.18	FTP	72	Request: EPSV
28	54.570841100	192.168.10.18	192.168.217.3	FTP	114	Response: 229 Entering Extended Passive Mode (39258)
57	197.698230700	192.168.10.18	192.168.217.3	FTP	86	Response: 220 (vsFTPD 3.0.5)
61	202.728992200	192.168.217.3	192.168.10.18	FTP	81	Request: USER elomb002
63	202.730021600	192.168.10.18	192.168.217.3	FTP	100	Response: 331 Please specify the password.
65	220.588978400	192.168.217.3	192.168.10.18	FTP	81	Request: PASS 01206946
67	223.377698600	192.168.10.18	192.168.217.3	FTP	88	Response: 530 Login incorrect.