

# CYSE301: Cybersecurity Technique and Operations

## Assignment 2: Traffic Tracing and Sniffing

By George Trey Smith

No.	Time	Source	Destination	Protocol	Length	Info
60	0.000000	192.168.1.10	192.168.1.1	ICMP	60	Standard query request 0x...
61	0.000000	192.168.1.1	192.168.1.10	ICMP	60	Standard query response 0x...
62	0.000000	192.168.1.10	192.168.1.1	ICMP	60	Standard query request 0x...
63	0.000000	192.168.1.1	192.168.1.10	ICMP	60	Standard query response 0x...
64	0.000000	192.168.1.10	192.168.1.1	ICMP	60	Standard query request 0x...
65	0.000000	192.168.1.1	192.168.1.10	ICMP	60	Standard query response 0x...

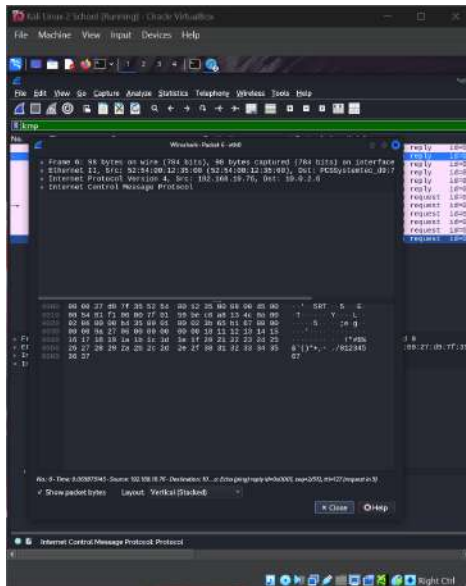
Q1.

How many packets are captured in total? How many packets are displayed?  
6 packets

No.	Time	Source	Destination	Protocol	Length	Info
60	0.000000	192.168.1.10	192.168.1.1	ICMP	60	Standard query request 0x...
61	0.000000	192.168.1.1	192.168.1.10	ICMP	60	Standard query response 0x...
62	0.000000	192.168.1.10	192.168.1.1	ICMP	60	Standard query request 0x...
63	0.000000	192.168.1.1	192.168.1.10	ICMP	60	Standard query response 0x...
64	0.000000	192.168.1.10	192.168.1.1	ICMP	60	Standard query request 0x...
65	0.000000	192.168.1.1	192.168.1.10	ICMP	60	Standard query response 0x...

Q2.

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

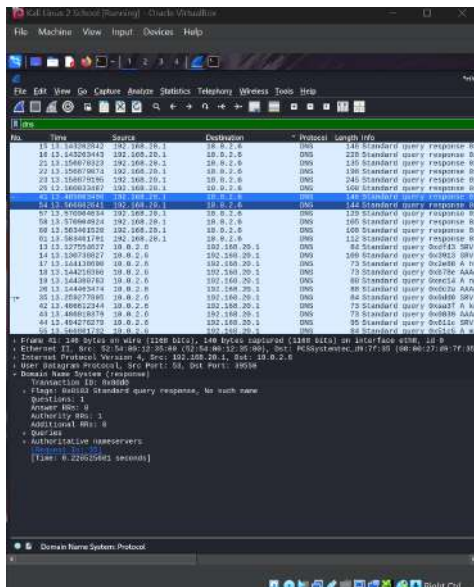


Q3.

Select an Echo (replay) 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?

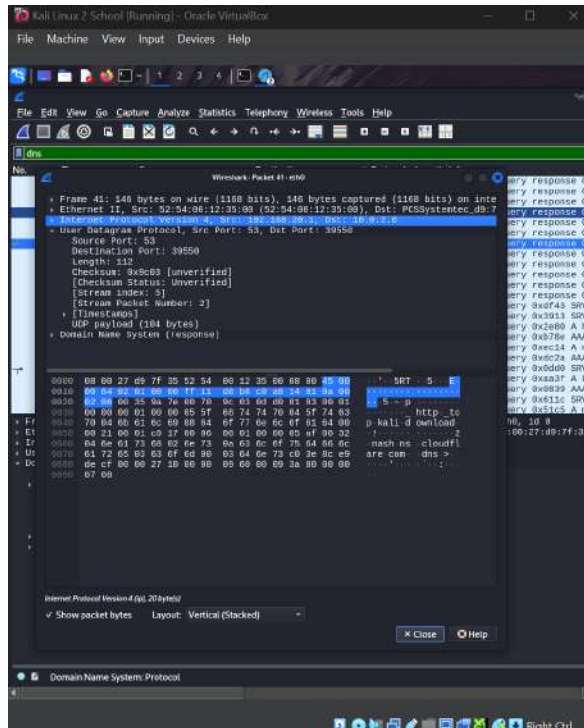
Src: 192.168.19.76 | Dest: 10.0.2.6 | Sequence number: 1 (0x0001) 256 (0x0100) | RT: 0.788 ms



Q4.

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

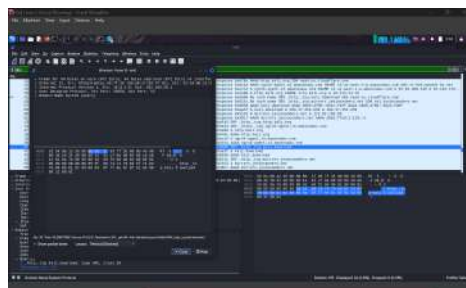
The total number of DNS packets displayed within the capture.



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.

Http.tcp.kali.download | Src: 192.168.20.1 : PortNum: 53 | Dest: 10.0.2.6 : PortNum: 39550 |



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?

Src: 10.0.2.6 : PortNum: 39550 | Dest: 192.168.20.1 : PortNum: 53 | Answer RRs: 0

## Task B. Sniffing

Attacker Kali - Internal Workstation on C:\301-GSM-T036 - Virtual Machine Connection

Kali - Internal Workstation on C:\301-GSM-T036 - Virtual Machine Connection

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

\*eth0

icmp and ip.src == 192.168.217.3 && ip.dst == 192.168.10.18

No.	Time	Source	Destination	Protocol	Length	Info
1901	476.534709496	192.168.217.3	192.168.10.18	ICMP	98	Echo (ping)
1907	476.632246396	192.168.217.3	192.168.10.18	ICMP	98	Echo (ping)
1971	480.034296796	192.168.217.3	192.168.10.18	ICMP	98	Echo (ping)
1975	481.837255396	192.168.217.3	192.168.10.18	ICMP	98	Echo (ping)
1979	482.5309054796	192.168.217.3	192.168.10.18	ICMP	98	Echo (ping)
1983	483.940198996	192.168.217.3	192.168.10.18	ICMP	98	Echo (ping)
1987	484.842793396	192.168.217.3	192.168.10.18	ICMP	98	Echo (ping)
1991	486.044072496	192.168.217.3	192.168.10.18	ICMP	98	Echo (ping)
1995	486.049368096	192.168.217.3	192.168.10.18	ICMP	98	Echo (ping)
1999	487.654956496	192.168.217.3	192.168.10.18	ICMP	98	Echo (ping)

Frame 705: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface eth0  
Ethernet II, Src: Microsoft\_08:00:54:00:15:00 (08:00:54:00:15:00), Dst: 192.168.10.18 (08:00:00:00:00:00)  
Internet Protocol Version 4, Src: 192.168.217.3, Dst: 192.168.10.18  
Internet Control Message Protocol

root@kali:~#  
CAST, RUNNING, MULTICAST> mtu 1500  
3 netmask 255.255.255.0 broadcast 0  
0444:5b9f:6e54 prefixlen 64 scope 0  
:57:24 txqueuelen 1000 (Ethernet)  
tes 7720 (7.5 KiB)  
ped 0 overruns 0 frame 0  
tes 4572 (4.4 KiB)  
ped 0 overruns 0 carrier 0 collisions 0  
CAST, RUNNING, MULTICAST> mtu 1500  
23 netmask 255.255.255.0 broadcast 0  
1461:8589:5a88 prefixlen 64 scope 0  
:57:25 txqueuelen 1000 (Ethernet)  
tes 21803 (21.2 KiB)  
ped 0 overruns 0 frame 0  
ytes 22877 (22.3 KiB)  
ped 0 overruns 0 carrier 0 collisions 0  
Activate Windows  
Go to Settings to activate Windows.

Q1.

Attacker Kali - Internal Workstation on C:\301-GSM-T036 - Virtual Machine Connection

Kali - Internal Workstation on C:\301-GSM-T036 - Virtual Machine Connection

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

\*eth0

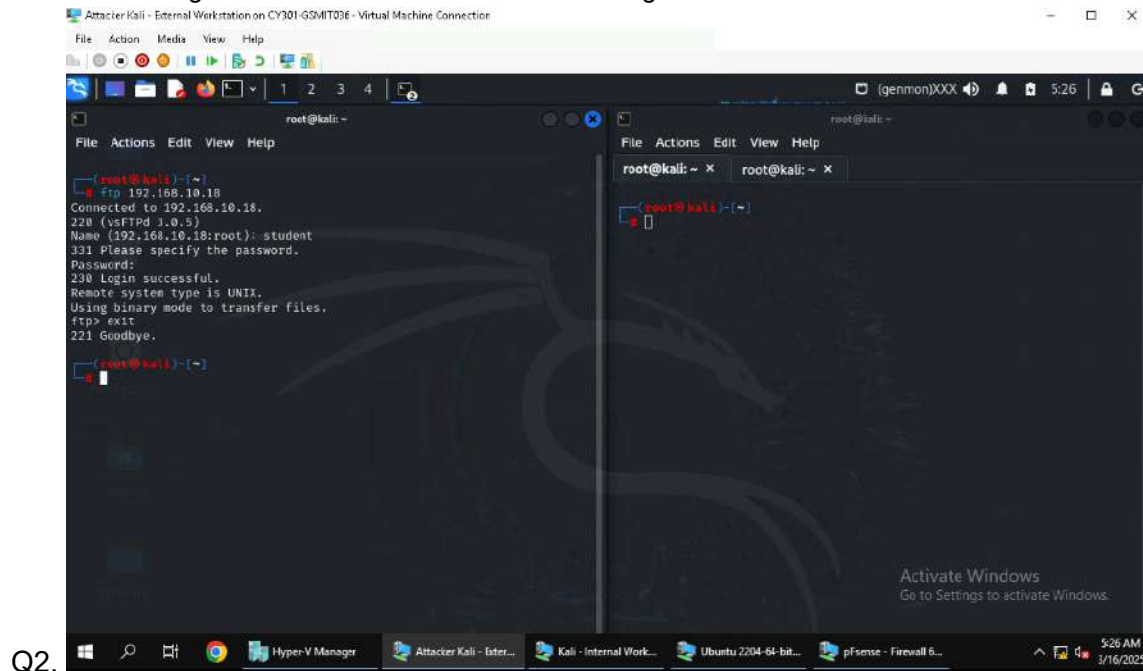
icmp

No.	Time	Source	Destination	Protocol	Length	Info
235	56.533929800	192.168.217.3	192.168.10.18	ICMP	98	Echo (ping)
236	56.534745300	192.168.10.18	192.168.217.3	ICMP	98	Echo (ping)
237	57.163542300	192.168.217.3	192.168.10.13	ICMP	98	Echo (ping)
238	57.163580200	192.168.10.13	192.168.217.3	ICMP	98	Echo (ping)
239	57.535571700	192.168.217.3	192.168.10.18	ICMP	98	Echo (ping)
240	57.536132100	192.168.10.18	192.168.217.3	ICMP	98	Echo (ping)
241	58.167234200	192.168.217.3	192.168.10.13	ICMP	98	Echo (ping)
242	58.167294100	192.168.10.13	192.168.217.3	ICMP	98	Echo (ping)
243	58.537453200	192.168.217.3	192.168.10.18	ICMP	98	Echo (ping)
244	58.539401300	192.168.10.18	192.168.217.3	ICMP	98	Echo (ping)

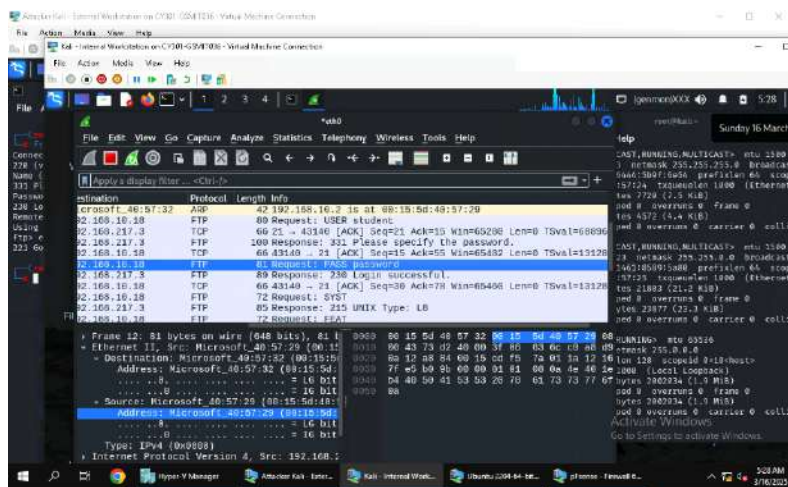
Frame 1: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface eth0  
Ethernet II, Src: Microsoft\_08:00:54:00:15:00 (08:00:54:00:15:00), Dst: 192.168.10.18 (08:00:00:00:00:00)  
Internet Protocol Version 4, Src: 192.168.217.3, Dst: 192.168.10.18  
Internet Control Message Protocol

root@kali:~#  
CAST, RUNNING, MULTICAST> mtu 1500  
3 netmask 255.255.255.0 broadcast 0  
0444:5b9f:6e54 prefixlen 64 scope 0  
:57:24 txqueuelen 1000 (Ethernet)  
tes 7720 (7.5 KiB)  
ped 0 overruns 0 frame 0  
tes 4572 (4.4 KiB)  
ped 0 overruns 0 carrier 0 collisions 0  
CAST, RUNNING, MULTICAST> mtu 1500  
23 netmask 255.255.255.0 broadcast 0  
1461:8589:5a88 prefixlen 64 scope 0  
:57:25 txqueuelen 1000 (Ethernet)  
tes 21803 (21.2 KiB)  
ped 0 overruns 0 frame 0  
ytes 22877 (22.3 KiB)  
ped 0 overruns 0 carrier 0 collisions 0  
Activate Windows  
Go to Settings to activate Windows.

- Apply the proper display or capture filter in Wireshark on the internal Kali VM to show active ICMP traffic.
- 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

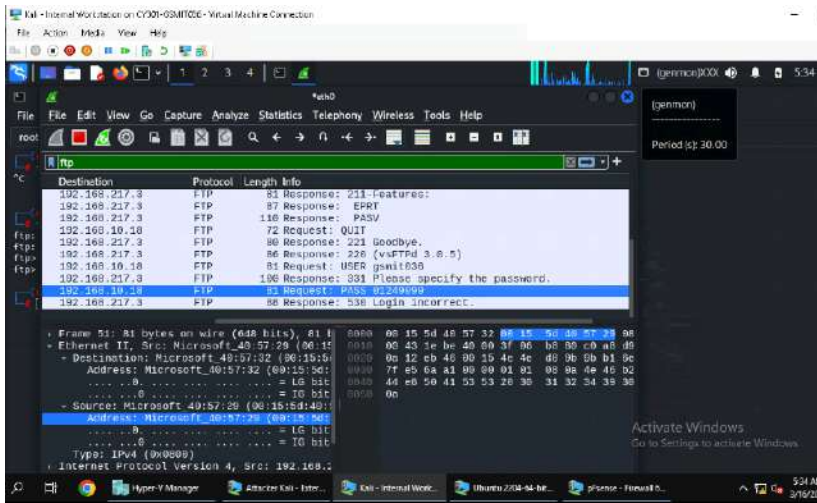


- ^^



- Looked at the password field in the packet request through wireshark





C.