

Experiment - 10

Student Name: Ekansh Sharma

Branch: CSE-IS

Semester: 5th Semester

Name: Network Defence Essentials Lab

UID: 20BCS3630

Section/Group: 20BIS1-B

Date of Performance: 10-11-2022 Subject

1. Aim/Overview of the practical:

Perform the practical of sniffing tool -Wireshark on Windows.

2. Task to be performed

1. Packet tracing through Wireshark between 2 systems

3. Output and screenshots:

I. Packet tracing through Wireshark

Step1:- configure the IP addresses of the systems

Step2:- ping the one system from another. Here the source IP is 192.168.22.128 and the destination IP is 192.168.22.129. as the connection is established correctly, we can see packets information from

Wireshark

```

Metasploitable2-Linux - VMware Workstation
Metasploitable2-Linux
Kali-Linux-2022.2-vmware-amd64

Metasploitable2-Linux:~$ ifconfig
Link encap:Ethernet HWaddr 00:0c:29:0b:39:e4
inet addr:192.168.22.128 Bcast:192.168.22.255 Mask:255.255.255.0
inet6 addr: fe80::20c:29ff:fe0b:39e4/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:18 errors:0 dropped:0 overruns:0 frame:0
TX packets:54 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:2096 (2.0 KB) TX bytes:5576 (5.4 KB)
Interrupt:17 Base address:0x2000

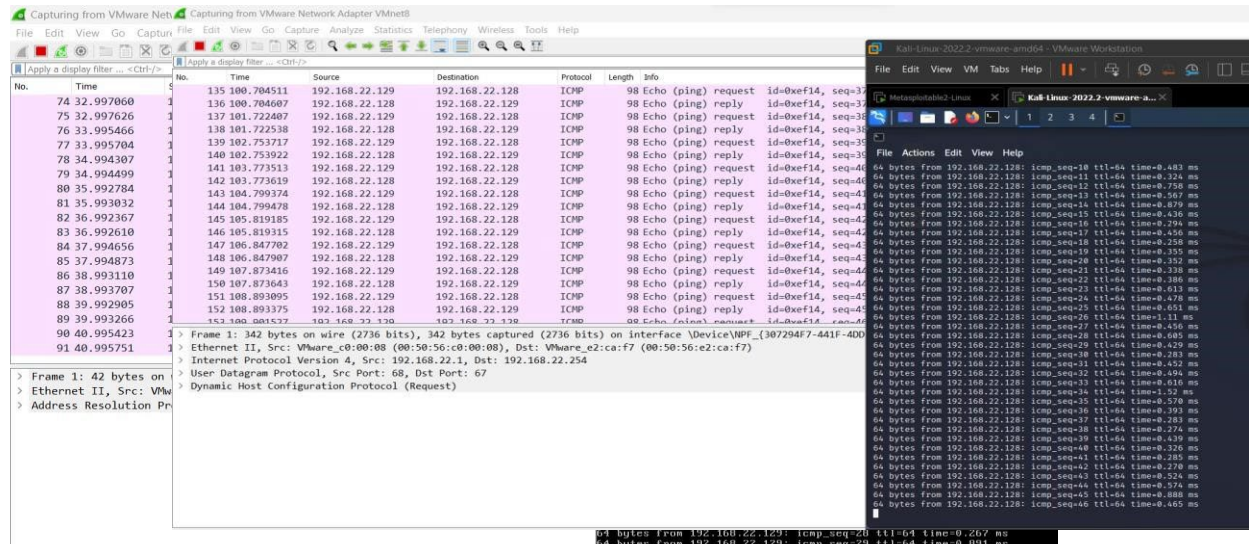
Link encap:Local Loopback
inet addr:127.0.0.1 Mask:255.0.0.0
inet6 addr: ::1/128 Scope:Host
UP LOOPBACK RUNNING MTU:16436 Metric:1
RX packets:92 errors:0 dropped:0 overruns:0 frame:0
TX packets:92 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:19393 (18.9 KB) TX bytes:19393 (18.9 KB)

Metasploitable2-Linux:~$ _

Kali-Linux-2022.2-vmware-amd64 - VMware Workstation
Kali-Linux-2022.2-vmware-amd64
Kali-Linux-2022.2-vmware-amd64:~$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 192.168.22.129 netmask 255.255.255.0 broadcast 192.168.22.255
inet6 fe80::20c:29ff:feea:f557 prefixlen 64 scopeid 0x20<link>
ether 00:0c:29:ea:f5:57 txqueuelen 1000 (Ethernet)
RX packets 33 bytes 3121 (3.0 KiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 59 bytes 6120 (5.9 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

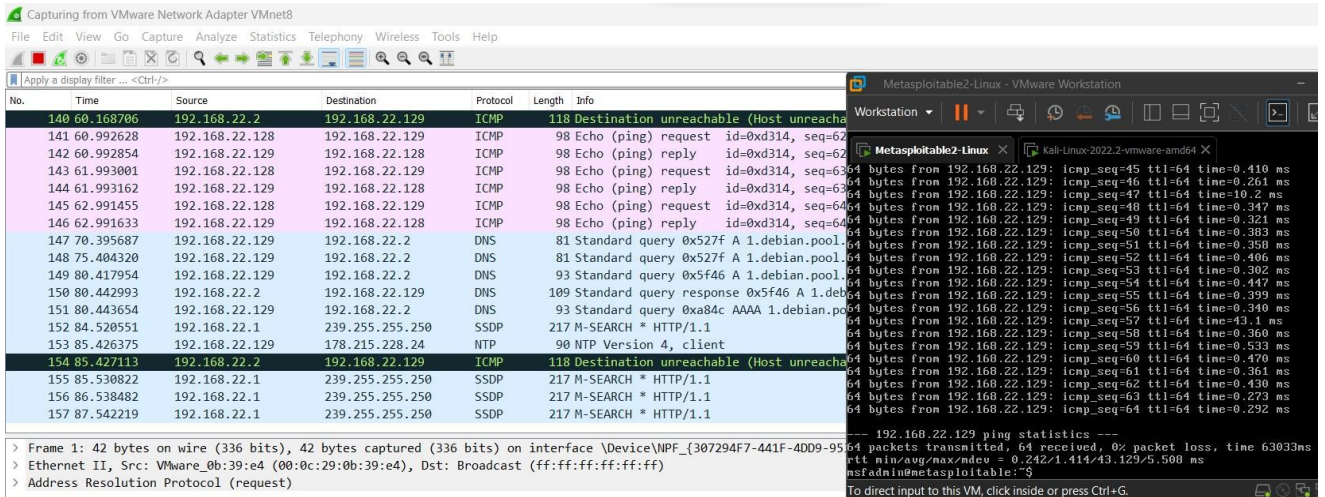
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
inet 127.0.0.1 netmask 255.0.0.0
inet6 ::1 prefixlen 128 scopeid 0x10<host>
loop txqueuelen 1000 (Local Loopback)
RX packets 0 bytes 0 (0.0 B)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 0 bytes 0 (0.0 B)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

```



No.	Time	Source	Destination	Protocol	Length	Info
74	32.997860	135.100.784511	192.168.22.129	ICMP	98	Echo (ping) request id=0xef14, seq=31
75	32.997626	137.101.722407	192.168.22.129	ICMP	98	Echo (ping) request id=0xef14, seq=31
76	33.995466	138.101.722538	192.168.22.129	ICMP	98	Echo (ping) request id=0xef14, seq=31
77	33.995704	139.102.753717	192.168.22.129	ICMP	98	Echo (ping) request id=0xef14, seq=31
78	34.994307	140.102.753922	192.168.22.129	ICMP	98	Echo (ping) request id=0xef14, seq=31
79	34.994499	141.103.773513	192.168.22.129	ICMP	98	Echo (ping) request id=0xef14, seq=31
80	35.992784	142.103.773619	192.168.22.129	ICMP	98	Echo (ping) request id=0xef14, seq=31
81	35.993032	143.104.799374	192.168.22.129	ICMP	98	Echo (ping) request id=0xef14, seq=31
82	36.992367	144.104.799478	192.168.22.129	ICMP	98	Echo (ping) request id=0xef14, seq=31
83	36.992610	145.105.819185	192.168.22.129	ICMP	98	Echo (ping) request id=0xef14, seq=31
84	37.994656	146.105.819315	192.168.22.129	ICMP	98	Echo (ping) request id=0xef14, seq=31
85	37.994873	147.106.847702	192.168.22.129	ICMP	98	Echo (ping) request id=0xef14, seq=31
86	38.993110	148.106.847907	192.168.22.129	ICMP	98	Echo (ping) request id=0xef14, seq=31
87	38.993707	149.107.873416	192.168.22.129	ICMP	98	Echo (ping) request id=0xef14, seq=31
88	39.992905	150.107.873643	192.168.22.129	ICMP	98	Echo (ping) request id=0xef14, seq=31
89	39.993266	151.108.893905	192.168.22.129	ICMP	98	Echo (ping) request id=0xef14, seq=31
90	40.995423	152.108.893375	192.168.22.129	ICMP	98	Echo (ping) request id=0xef14, seq=31
91	40.995751	153.100.001537	192.168.22.129	ICMP	98	Echo (ping) request id=0xef14, seq=31

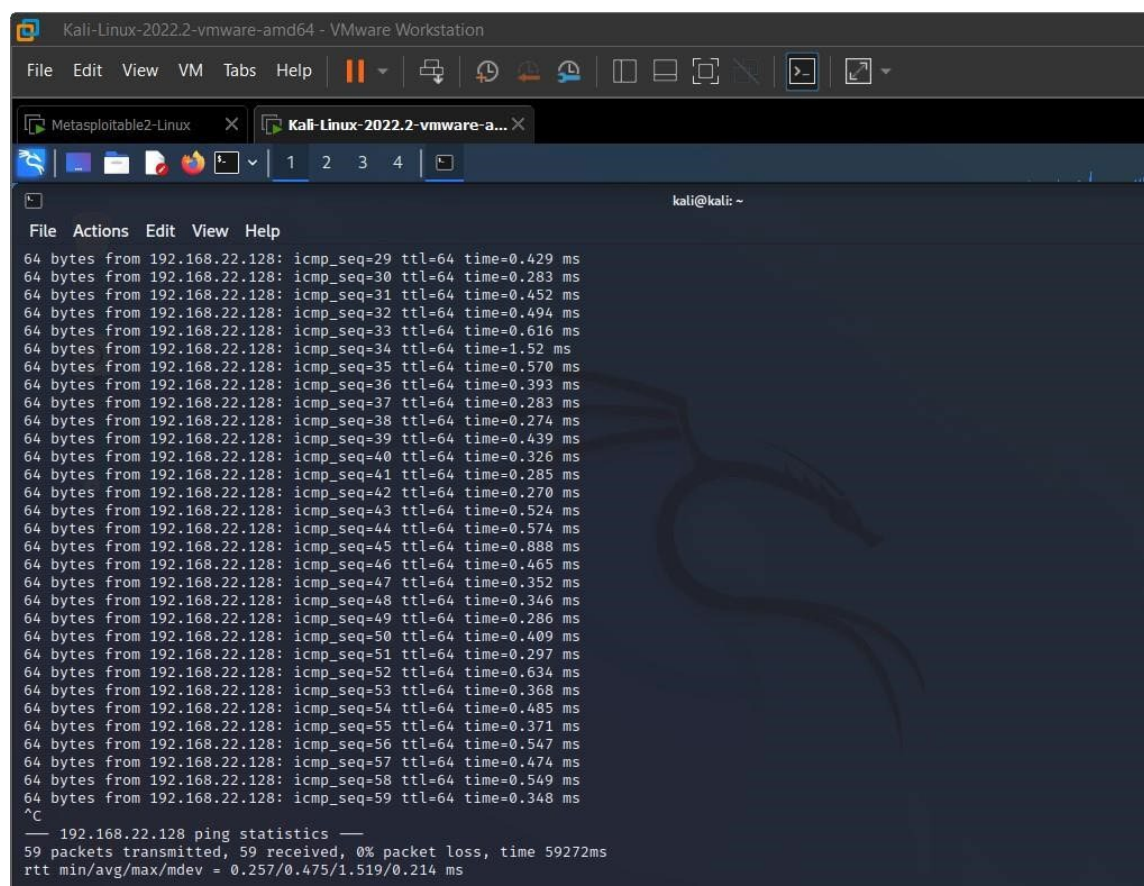
Step3:- to stop the ping command press ctrl+C. we can see in the Wireshark the packets transfer will be stopped.



No.	Time	Source	Destination	Protocol	Length	Info
140	60.168706	192.168.22.2	192.168.22.129	ICMP	118	Destination unreachable (Host unreachable)
141	60.992628	192.168.22.128	192.168.22.129	ICMP	98	Echo (ping) request id=0xd314, seq=62
142	60.992854	192.168.22.129	192.168.22.128	ICMP	98	Echo (ping) reply id=0xd314, seq=62
143	61.993001	192.168.22.128	192.168.22.129	ICMP	98	Echo (ping) request id=0xd314, seq=63
144	61.993161	192.168.22.129	192.168.22.128	ICMP	98	Echo (ping) reply id=0xd314, seq=63
145	62.991455	192.168.22.128	192.168.22.129	ICMP	98	Echo (ping) request id=0xd314, seq=64
146	62.991633	192.168.22.129	192.168.22.128	ICMP	98	Echo (ping) reply id=0xd314, seq=64
147	70.395687	192.168.22.129	192.168.22.2	DNS	81	Standard query 0x527f A 1.debian.pool
148	75.404320	192.168.22.129	192.168.22.2	DNS	81	Standard query 0x527f A 1.debian.pool
149	80.417954	192.168.22.129	192.168.22.2	DNS	93	Standard query 0x5f46 A 1.debian.pool
150	80.442993	192.168.22.2	192.168.22.129	DNS	109	Standard query response 0x5f46 A 1.debian.pool
151	80.443654	192.168.22.129	192.168.22.2	DNS	93	Standard query 0xa84c AAAA 1.debian.pool
152	84.520551	192.168.22.1	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
153	85.426375	192.168.22.129	178.215.228.24	NTP	90	NTP Version 4, client
154	85.427113	192.168.22.2	192.168.22.129	ICMP	118	Destination unreachable (Host unreachable)
155	85.530822	192.168.22.1	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
156	86.538482	192.168.22.1	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
157	87.542219	192.168.22.1	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1

Step4:- repeat step 2 but this time source will be 192.168.22.129 and destination IP is 192.168.22.128 This again confirms the transfer of packets between the network and Wireshark can be used to sniff the packets between the system network.

Step5:- press 'ctrl+c' to stop the ping command



```

Kali-Linux-2022.2-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Metasploitable2-Linux x Kali-Linux-2022.2-vmware-a... x
kali@kali: ~
File Actions Edit View Help
64 bytes from 192.168.22.128: icmp_seq=29 ttl=64 time=0.429 ms
64 bytes from 192.168.22.128: icmp_seq=30 ttl=64 time=0.283 ms
64 bytes from 192.168.22.128: icmp_seq=31 ttl=64 time=0.452 ms
64 bytes from 192.168.22.128: icmp_seq=32 ttl=64 time=0.494 ms
64 bytes from 192.168.22.128: icmp_seq=33 ttl=64 time=0.616 ms
64 bytes from 192.168.22.128: icmp_seq=34 ttl=64 time=1.52 ms
64 bytes from 192.168.22.128: icmp_seq=35 ttl=64 time=0.570 ms
64 bytes from 192.168.22.128: icmp_seq=36 ttl=64 time=0.393 ms
64 bytes from 192.168.22.128: icmp_seq=37 ttl=64 time=0.283 ms
64 bytes from 192.168.22.128: icmp_seq=38 ttl=64 time=0.274 ms
64 bytes from 192.168.22.128: icmp_seq=39 ttl=64 time=0.439 ms
64 bytes from 192.168.22.128: icmp_seq=40 ttl=64 time=0.326 ms
64 bytes from 192.168.22.128: icmp_seq=41 ttl=64 time=0.285 ms
64 bytes from 192.168.22.128: icmp_seq=42 ttl=64 time=0.270 ms
64 bytes from 192.168.22.128: icmp_seq=43 ttl=64 time=0.524 ms
64 bytes from 192.168.22.128: icmp_seq=44 ttl=64 time=0.574 ms
64 bytes from 192.168.22.128: icmp_seq=45 ttl=64 time=0.888 ms
64 bytes from 192.168.22.128: icmp_seq=46 ttl=64 time=0.465 ms
64 bytes from 192.168.22.128: icmp_seq=47 ttl=64 time=0.352 ms
64 bytes from 192.168.22.128: icmp_seq=48 ttl=64 time=0.346 ms
64 bytes from 192.168.22.128: icmp_seq=49 ttl=64 time=0.286 ms
64 bytes from 192.168.22.128: icmp_seq=50 ttl=64 time=0.409 ms
64 bytes from 192.168.22.128: icmp_seq=51 ttl=64 time=0.297 ms
64 bytes from 192.168.22.128: icmp_seq=52 ttl=64 time=0.634 ms
64 bytes from 192.168.22.128: icmp_seq=53 ttl=64 time=0.368 ms
64 bytes from 192.168.22.128: icmp_seq=54 ttl=64 time=0.485 ms
64 bytes from 192.168.22.128: icmp_seq=55 ttl=64 time=0.371 ms
64 bytes from 192.168.22.128: icmp_seq=56 ttl=64 time=0.547 ms
64 bytes from 192.168.22.128: icmp_seq=57 ttl=64 time=0.474 ms
64 bytes from 192.168.22.128: icmp_seq=58 ttl=64 time=0.549 ms
64 bytes from 192.168.22.128: icmp_seq=59 ttl=64 time=0.348 ms
^C
  192.168.22.128 ping statistics
  59 packets transmitted, 59 received, 0% packet loss, time 59272ms
  rtt min/avg/max/mdev = 0.257/0.475/1.519/0.214 ms
  
```

Learning Outcomes:

1. DNS security and working of Quad9
2. Work with 9.9.9.9
3. Packet sniffing through Wireshark

Evaluation Grid (To be created as per the SOP and Assessment guidelines by the faculty):

Sr. No.	Parameters	Marks Obtained	Maximum Marks
1.	Conduct		12
2.	Viva		10
3.	Worksheet		8
4.	Total		30