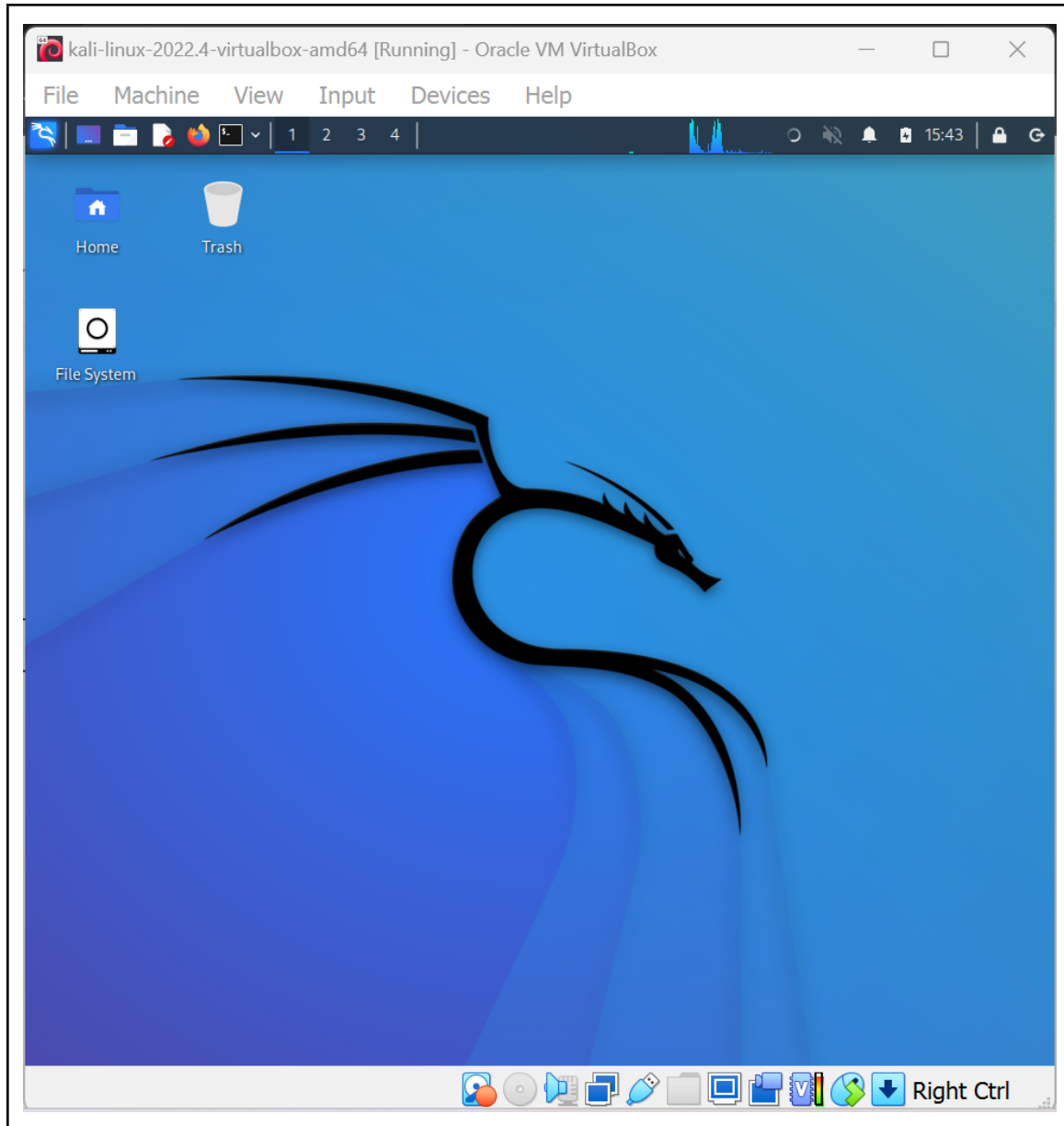


Table of Contents

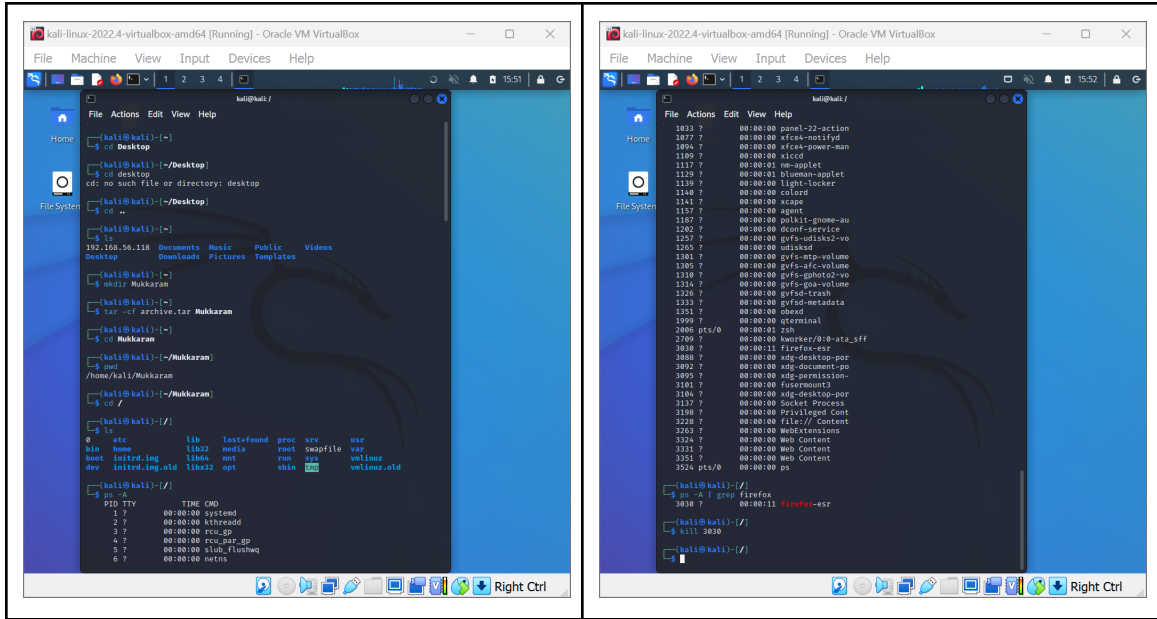
Lab 1	2
Lab 2	4
Lab 3	7

Lab 1

- Installed Kali Linux

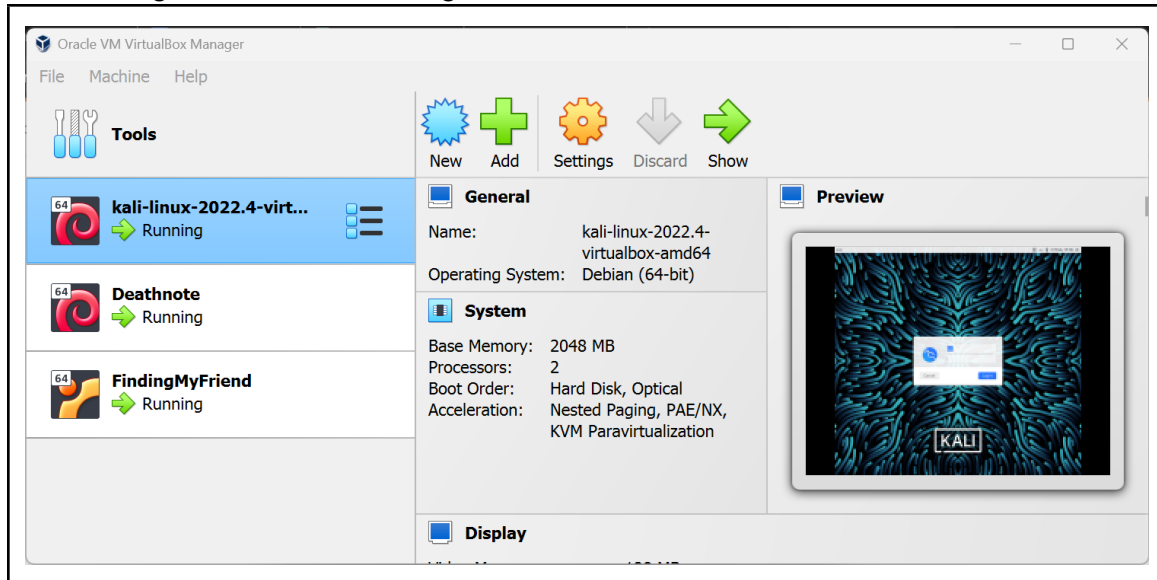


- Getting familiar with basic commands

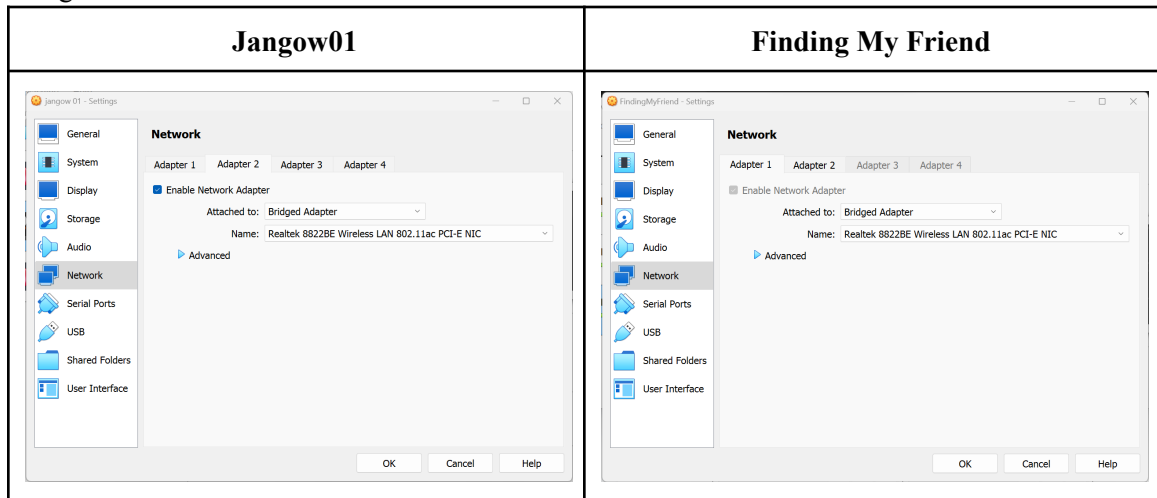


Lab 2

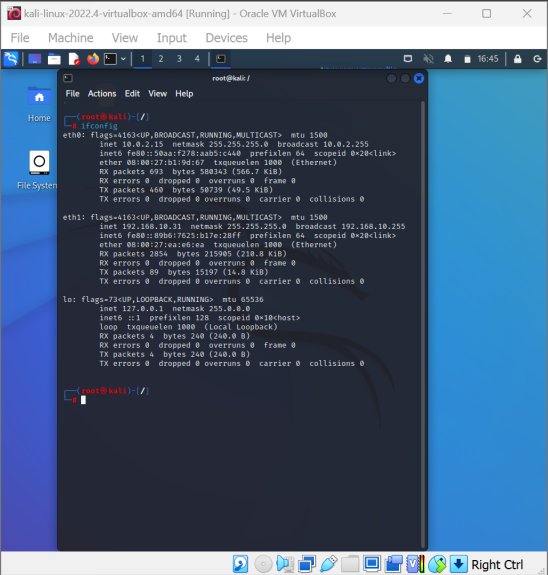
- Installed Target Machines named Jangow01 & Deathnote



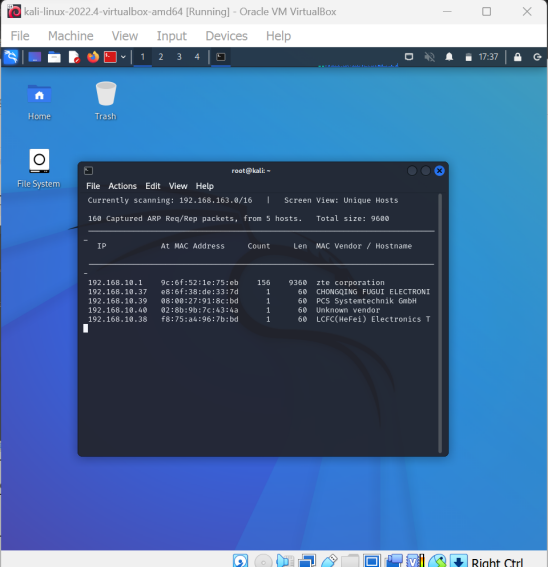
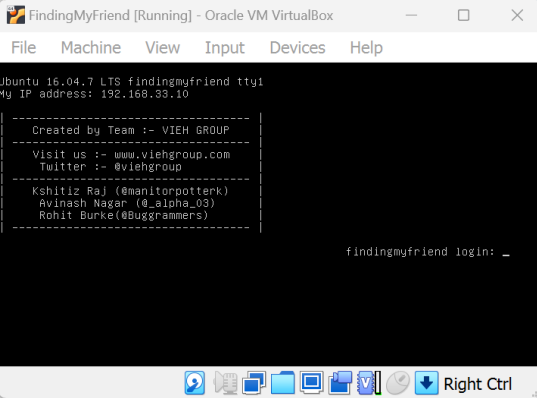
- Bridged Network



- Finding Ip Address of my kali

 <pre> root@kali: / root@kali:~# ifconfig eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500 inet 10.0.2.15 netmask 255.255.255.0 broadcast 10.0.2.255 inet6 fe80::2aa:f73:3a05:c44a prefixlen 64 scopeid 0x20<link> ether 08:00:27:1d:19:d7 txqueuelen 1000 (Ethernet) RX packets 693 bytes 58824 (56.9 KiB) RX errors 0 dropped 0 overruns 0 frame 0 TX packets 460 bytes 90739 (49.5 KiB) TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0 eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500 inet 192.168.10.11 netmask 255.255.255.0 broadcast 192.168.10.255 inet6 fe80::c9a:72d:2b7c:28ff prefixlen 64 scopeid 0x20<link> ether 08:00:27:ea:e6:ea txqueuelen 1000 (Ethernet) RX packets 2804 bytes 21980 (21.8 KiB) RX errors 0 dropped 0 overruns 0 frame 0 TX packets 89 bytes 15197 (11.8 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 4 bytes 240 (240.0 B) RX errors 0 dropped 0 overruns 0 frame 0 TX packets 4 bytes 240 (240.0 B) TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0 </pre>	<p>Command: ifconfig Ip address: 192.168.10.31</p>
--	--

- Discovering Ip Address of target machines

<p style="text-align: center;">Jangow01</p> <p>IP Address: 192.168.10.38 Command: netdiscover -i eth1</p>  <pre> root@kali:~# netdiscover -i eth1 Currently scanning: 192.168.10.0/16 Screen View: Unique Hosts 160 Captured ARP Req/Rep packets, from 5 hosts. Total size: 9680 - IP At MAC Address Count Len MAC Vendor / Hostname - 192.168.10.1 9c:6f:52:1e:75:eb 156 9360 zte corporation 192.168.10.37 e8:6f:38:0e:13:7d 1 60 CHONGQING TUDUI ELECTRONI 192.168.10.39 08:00:27:01:16:bd 1 60 PCS Systemtechnik GmbH 192.168.10.40 02:8b:9b:7c:43:4a 1 60 unknown vendor 192.168.10.38 f8:73:a4:96:7b:bd 1 60 LCFE(Merel) Electronics T </pre>	<p style="text-align: center;">Finding My Friend</p> <p>IP Address: 192.168.33.10 Given in the target machine</p>  <pre> FindingMyFriend [Running] - Oracle VM VirtualBox File Machine View Input Devices Help Ubuntu 16.04.7 LTS findingmyfriend tty1 My IP address: 192.168.33.10 Created by Team :- VIEH GROUP Visit us :- www.viehgroup.com Twitter :- @viehgroup Kshitiz Raj (@manitorpottenk) Avinash Nagar (@alpha_03) Rohit Burke (@Buggrammers) findingmyfriend login: _ </pre>
--	---

- Executing Ping Command

<p style="text-align: center;">Jangow01</p>	<p style="text-align: center;">Finding My Friend</p>
--	---



The image contains two side-by-side terminal window screenshots. The left terminal window shows a ping command to 192.168.10.38, which successfully receives data from the target. The right terminal window shows a ping command to 192.168.33.10, which results in 100% packet loss.

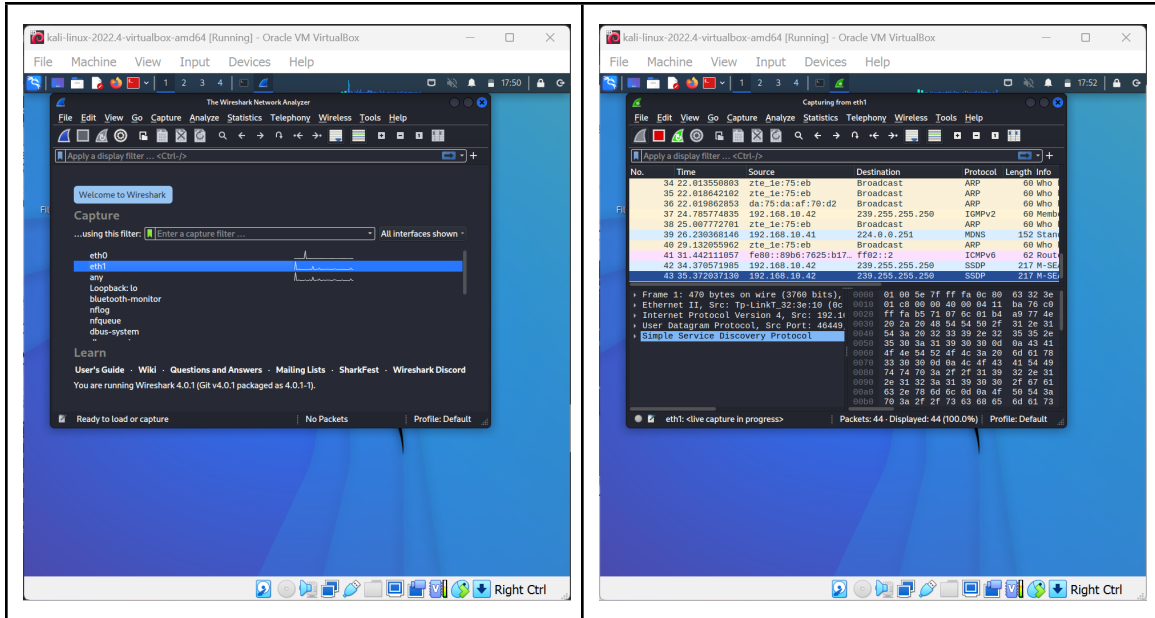
```
root@kali: ~  
File Actions Edit View Help  
root@kali: ~  
$ ping 192.168.10.38  
PING 192.168.10.38 (192.168.10.38) 56(84) bytes of data.  
^C  
— 192.168.10.38 ping statistics —  
36 packets transmitted, 0 received, 100% packet loss, time 36774ms
```

```
root@kali: ~  
$ ping 192.168.33.10  
PING 192.168.33.10 (192.168.33.10) 56(84) bytes of data.  
^C  
— 192.168.33.10 ping statistics —  
7 packets transmitted, 0 received, 100% packet loss, time 6224ms
```

Comments: Both machine are working properly as no packet is lost while executing the ping command.

Lab 3

- Starting Wireshark and selection of the network



- Statistics

File	Packets Captured	No. ICMP packets	No. of HTTP packets
ping.pcapng	188	40	0
web.pcapng	1202	0	28

- For the last task creating my own file of youtube using firefox as done in the previous task

How many packets are there in total?	4377
How many different protocols are there, and what are they?	Internet Control Message Protocol v6 1 QUIC IFTF 2925 Domain Name System 62 Transport Layer Security 240 Online Certificate Status Protocol 8 Address Resolution Protocol 4
Easy Way	Go to Statistics -> Protocol Hierarchy Statistics
Packet 1 Src IP Address	192.168.10.31
Packet 1 Dest IP Address	192.168.10.1
Which Layer hold ip address info	Network Layer
Packet 1 Src port	44468

Packet 1 Dest port	53
Information from above points	<p>The source port 44468 and destination port 53 suggest that a network communication session is likely taking place between a client and a DNS server. Port 53 is the well-known port used by the DNS protocol for name resolution and the fact that the destination port is set to 53 indicates that the traffic is targeting the DNS server.</p> <p>Meanwhile, the source port 44468 is likely a dynamically assigned port number used by the client to send the DNS request. When a client initiates a communication session, it typically selects a random source port to use, in this case, 44468</p>
Which layer holds port info	Transport Layer
TCP flag in packet 1	DNS service thus no TCP Flags
TCP flag in packet 2	DNS service thus no TCP Flags
TCP flag in packet 3	DNS service thus no TCP Flags
Info about Packt 1, 2, 3	<p>The source port 44468 and destination port 53 suggest that a network communication session is likely taking place between a client and a DNS server. Port 53 is the well-known port used by the DNS protocol for name resolution and the fact that the destination port is set to 53 indicates that the traffic is targeting the DNS server.</p> <p>Meanwhile, the source port 44468 is likely a dynamically assigned port number used by the client to send the DNS request. When a client initiates a communication session, it typically selects a random source port to use, in this case, 44468</p>
Protocol in Packet 4	DNS
IP address and other info of Packet 4	192.168.10.31 & 192.168.10.1 Standard Query for 0x6fff and 0x4cfa
Packet 13 info	13 6.454391993 142.250.185.46 192.168.10.31 TCP 74 443 → 35836 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1412 SACK_PERM TSval=2664872550 TSecr=2121977103 WS=256

TCP Flags	SYN and ACK
-----------	-------------

- Commands to check permission

ls -l <file_name>	<pre>(kali㉿kali)-[~/Desktop] \$ ls -l exampleFile.txt -rw-r--r-- 1 kali kali 0 Feb 17 18:58 exampleFile.txt</pre>
chmod +x <file_name> *** grants execution permission	<pre>(kali㉿kali)-[~/Desktop] \$ ls -l exampleFile.txt -rw-r--r-- 1 kali kali 0 Feb 17 18:58 exampleFile.txt</pre>
chmod +r <file_name> *** grants read permission	<pre>(kali㉿kali)-[~/Desktop] \$ chmod +r exampleFile.txt</pre>
chmod +w <file_name> *** grants writing permission	<pre>(kali㉿kali)-[~/Desktop] \$ chmod +w exampleFile.txt</pre>
chmod +xwr <file_name> *** grants execution, write and read permission	<pre>(kali㉿kali)-[~/Desktop] \$ chmod +xwr exampleFile.txt</pre>