Project name: **Gray Box Examples**

Date Completed: **August 27, 2023**

Created: **Jason Patrick Salerno**

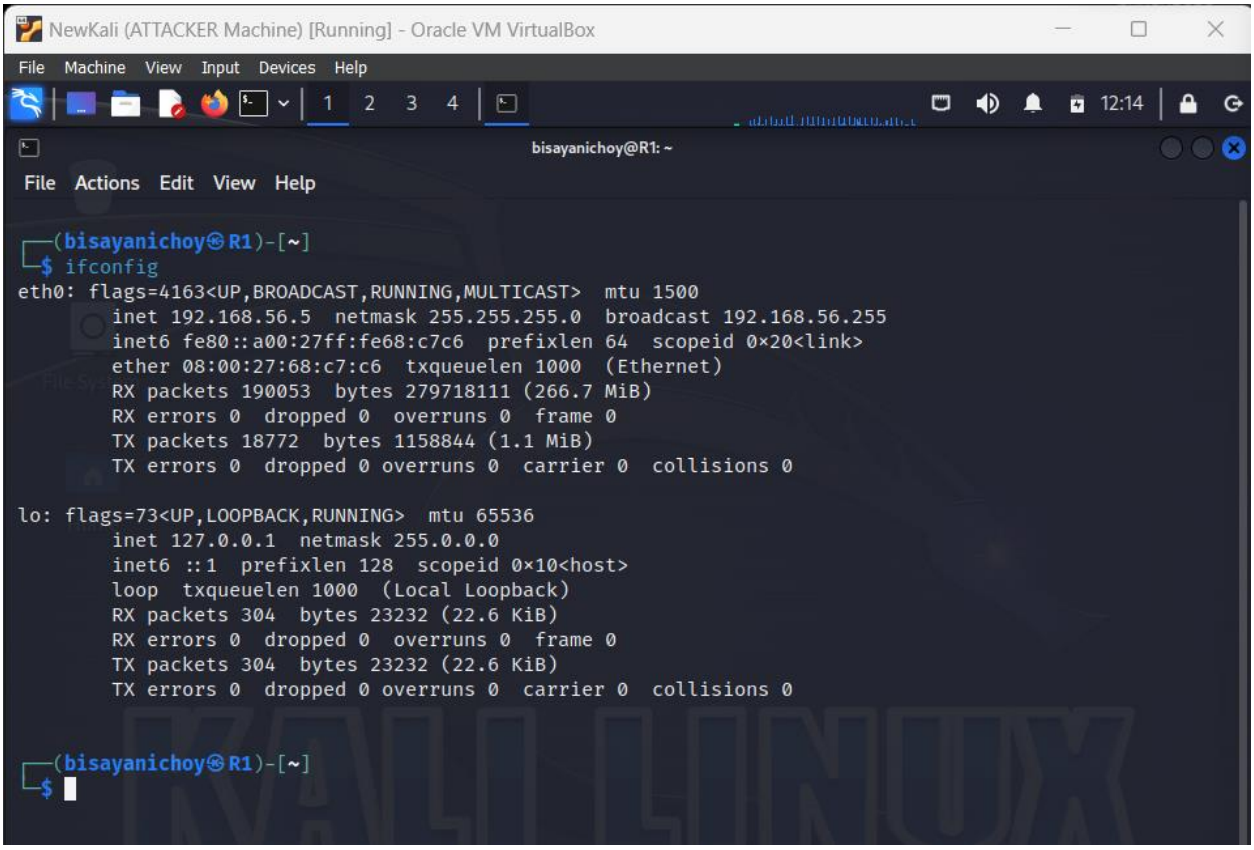
Purpose: **Creating my own example of a gray box**

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:

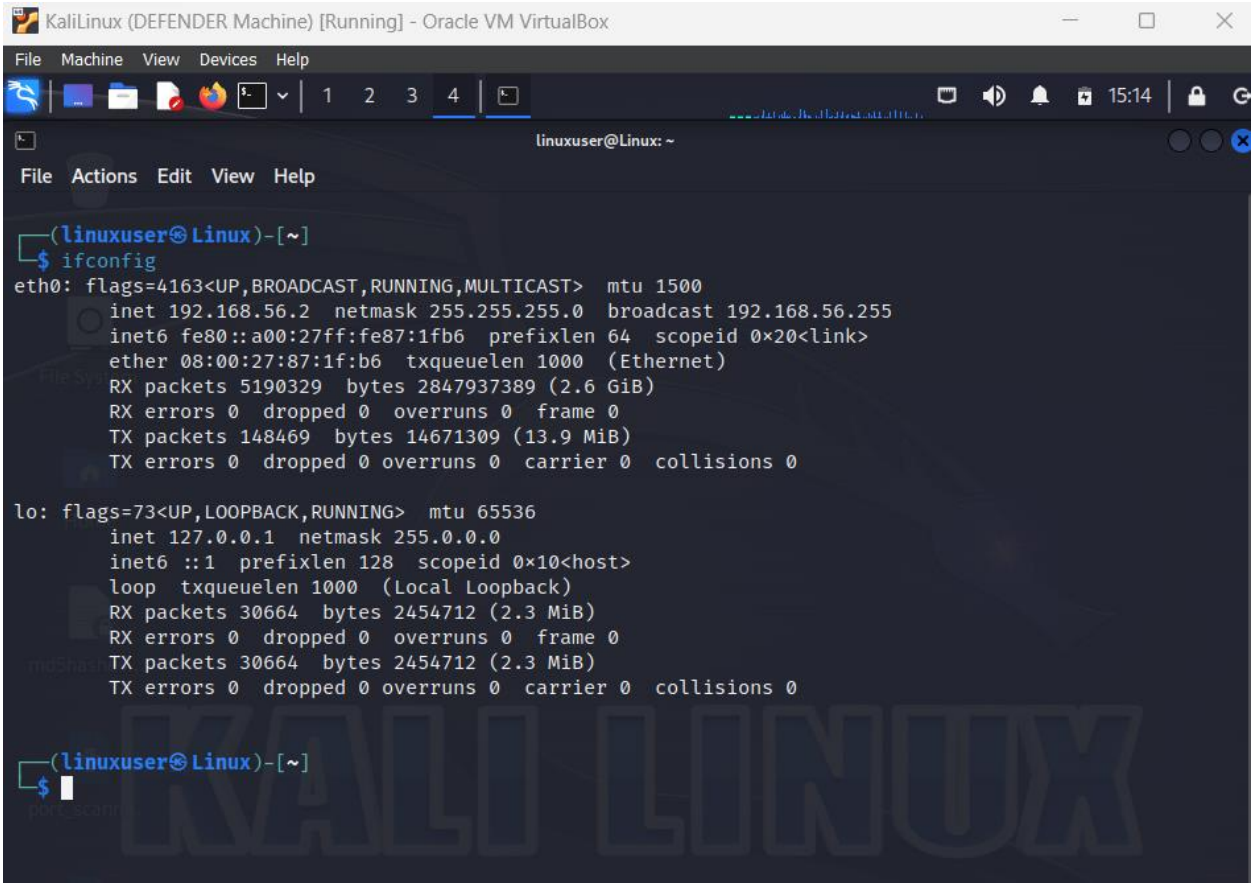
1. I run the command **ifconfig** to check and see our ip address, so the ip address of our **Attacker Machine** is **192.168.56.5**.

Attacker Machine:



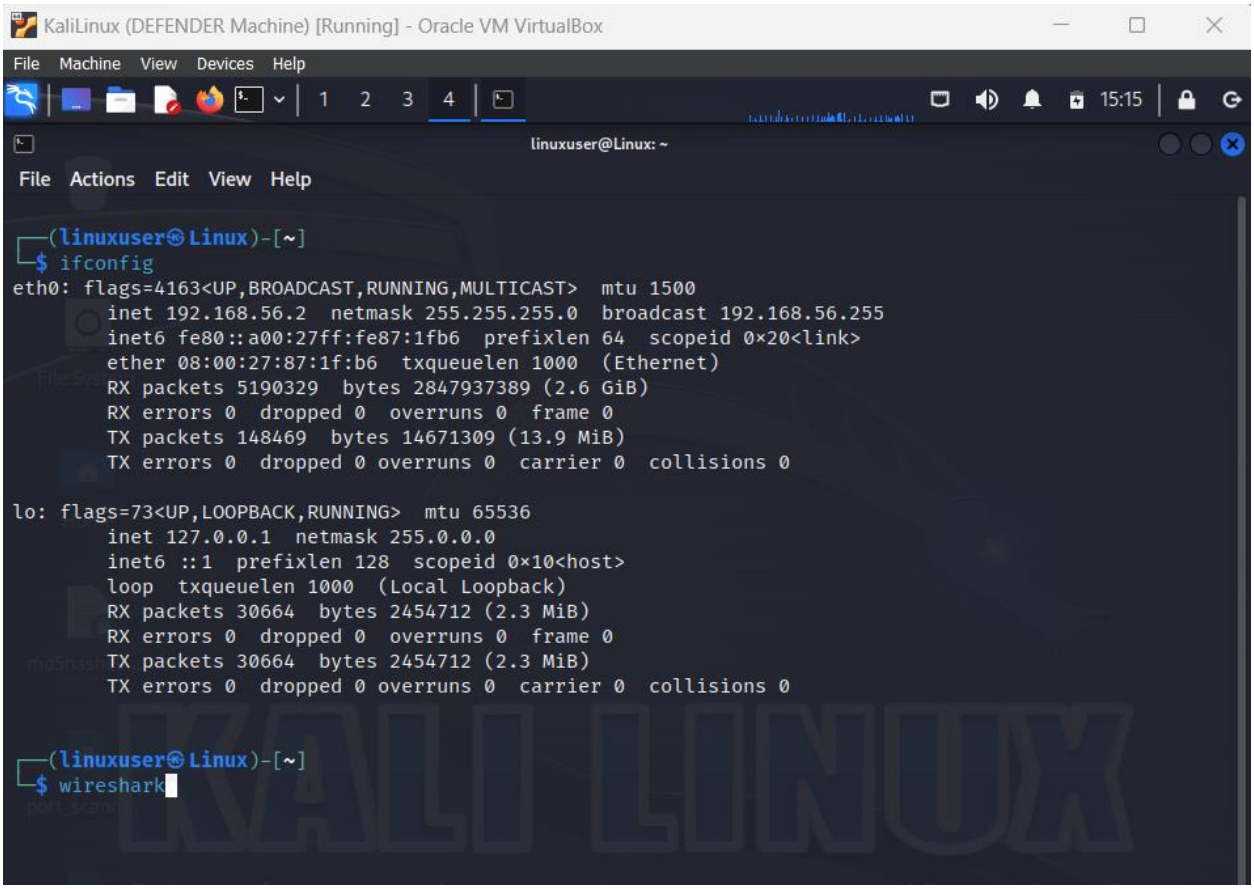
2. So, I do the same thing for our **Defender Machine**, I run the command **ifconfig** to see our ip address, and our ip address is **192.168.56.2**.

Defender Machine:



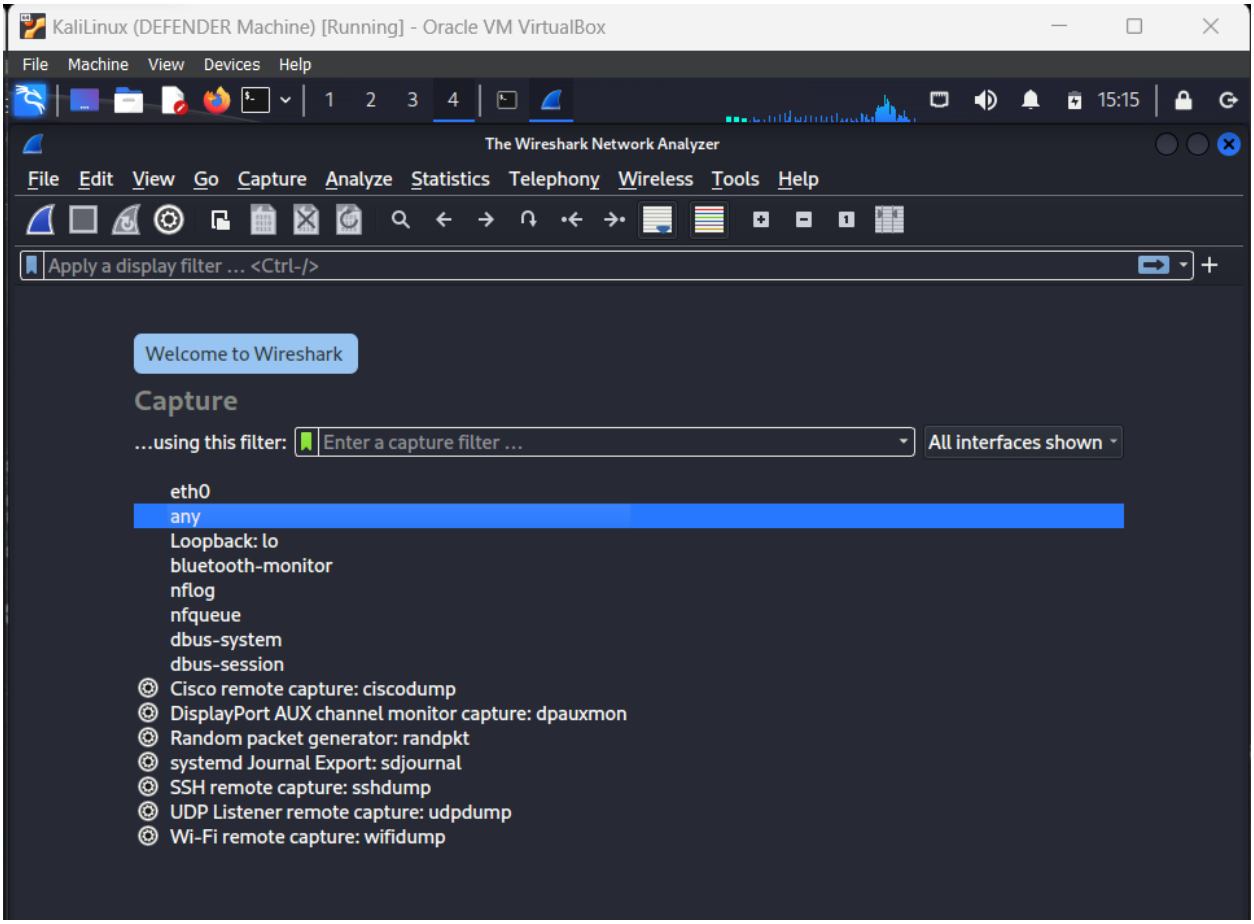
3. For my next step I opened **Wireshark** to capture network traffic on the internal network.

Defender Machine:



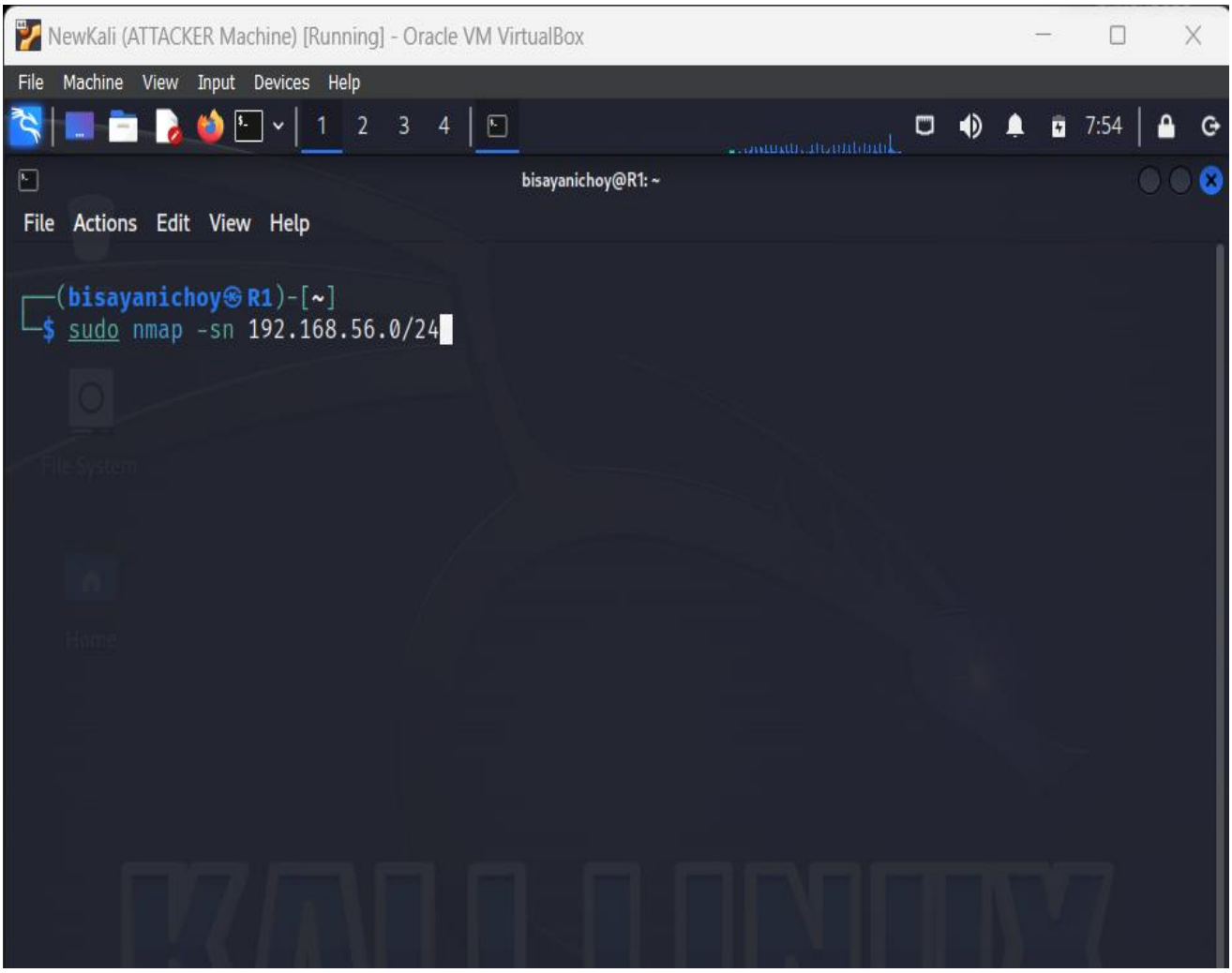
4. Next, I click on **any** so we can capture packets from **any** interface, then it will start capturing packets in our internal network.

Defender Machine:



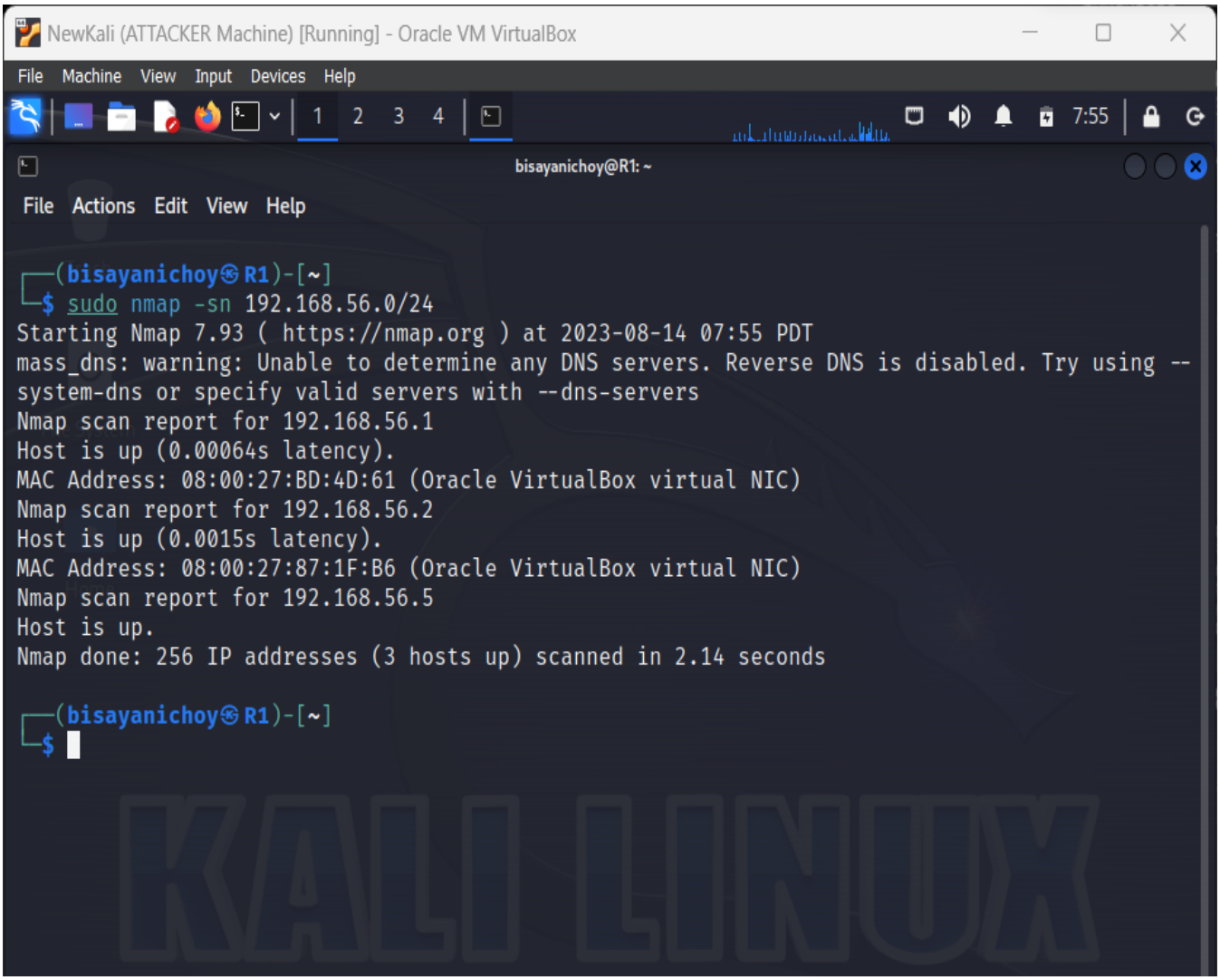
5. So, we are gonna scan our network using the tool called: **nmap**, nmap is a network mapper that can discover endpoints on a network, services and check for open ports. Since we know on what network we are on, by running the **ifconfig** command it gave us a bit of information such as what network 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:



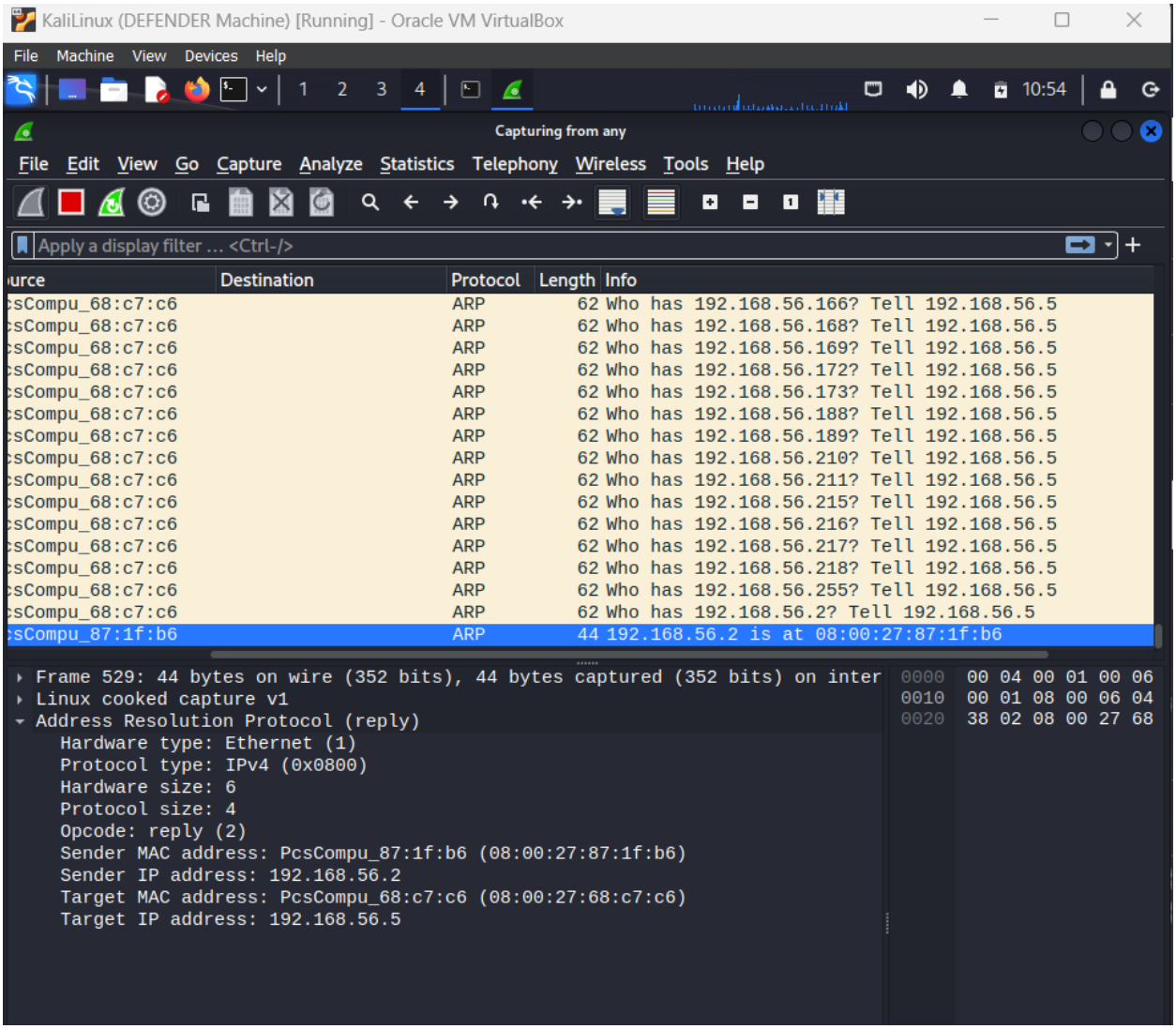
6. After the command has been executed, we can now see the results, it seems there are 3 endpoints that are up, the ip address: **192.168.56.5** is my own ip address (**Attacker Machine**). So, there are 2 other machines on the internal network, I will only want more information on the ip address: **192.168.56.2**.

Attacker Machine:



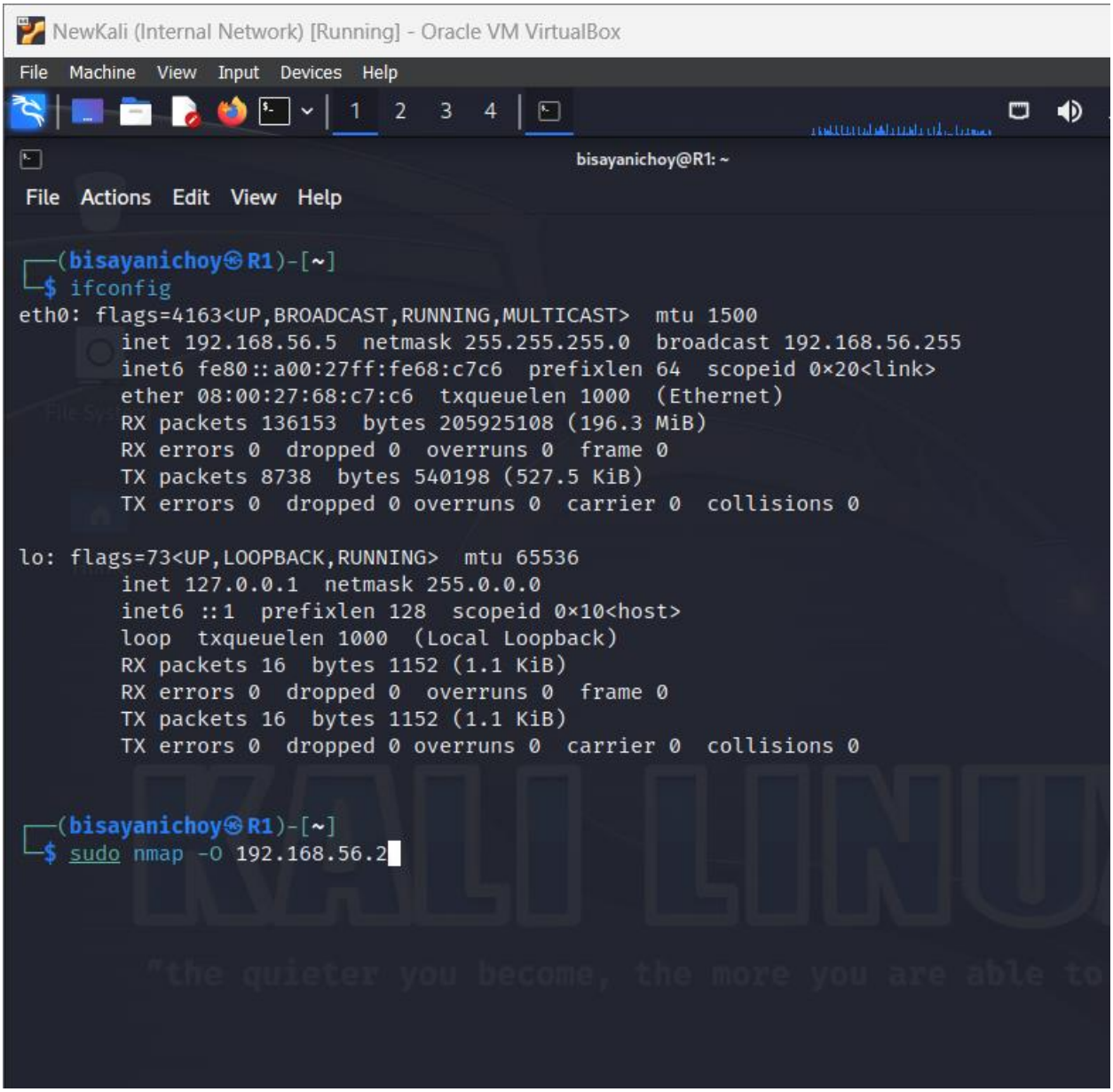
7. Back to our defender machine we can see that our attacker machine generates a lot of ARP Traffic, and in the highlighted section below we can also see that **192.168.56.2 is at 08:00:27:87:1f:b6** which is its MAC address.

Defender Machine:



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:



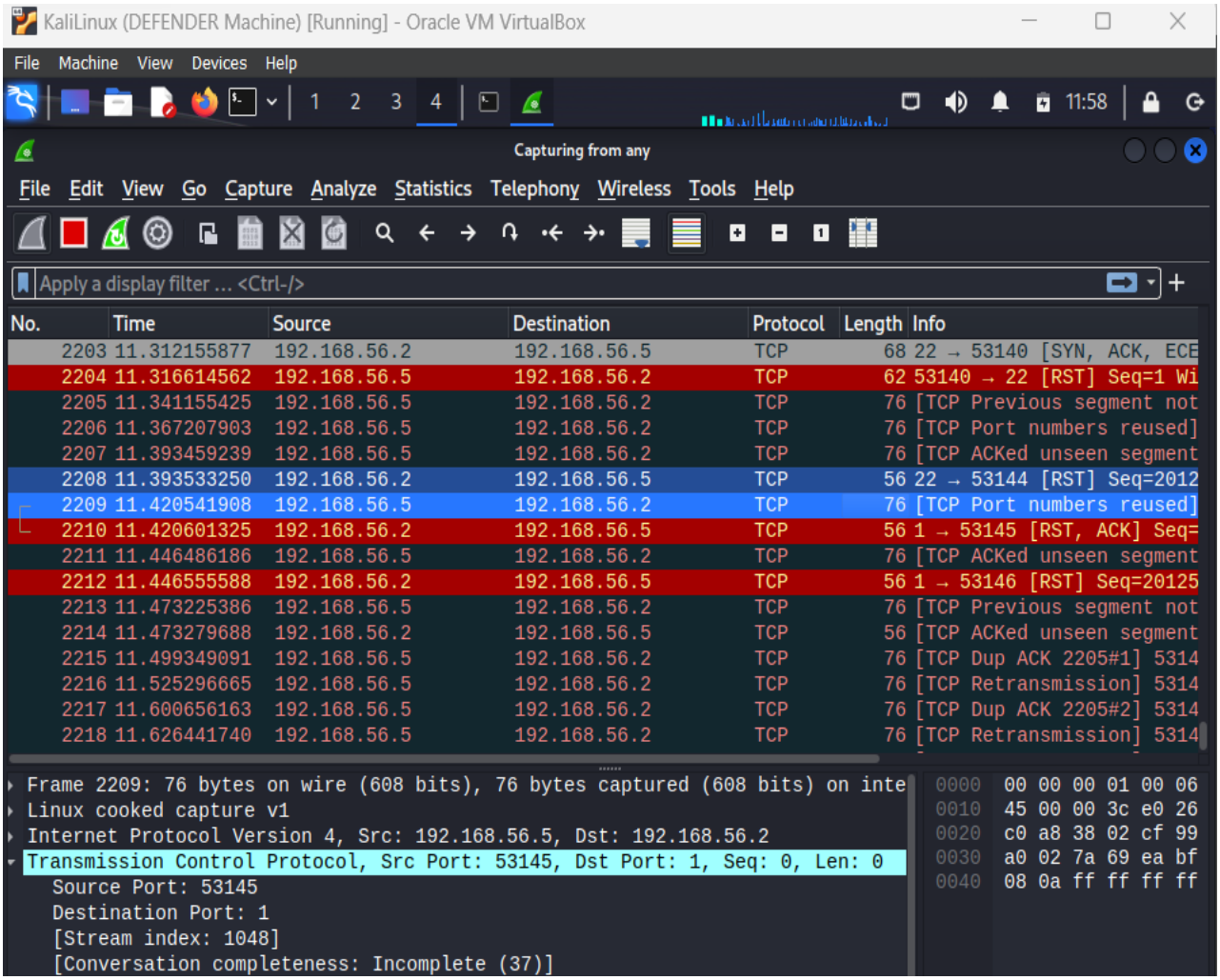
9. So, after executing the command, we can now see what OS it's running, which is **Linux 4.15 - 5.6** and we can also see its MAC address, purpose, and lastly open ports, which we can see its **SSH port 22** is currently open on that machine.

Attacker Machine:

```
NewKali (Internal Network) [Running] - Oracle VM VirtualBox
File  Machine  View  Input  Devices  Help
1  2  3  4                                                    10:14
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 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
[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)-[~]
└─$
```

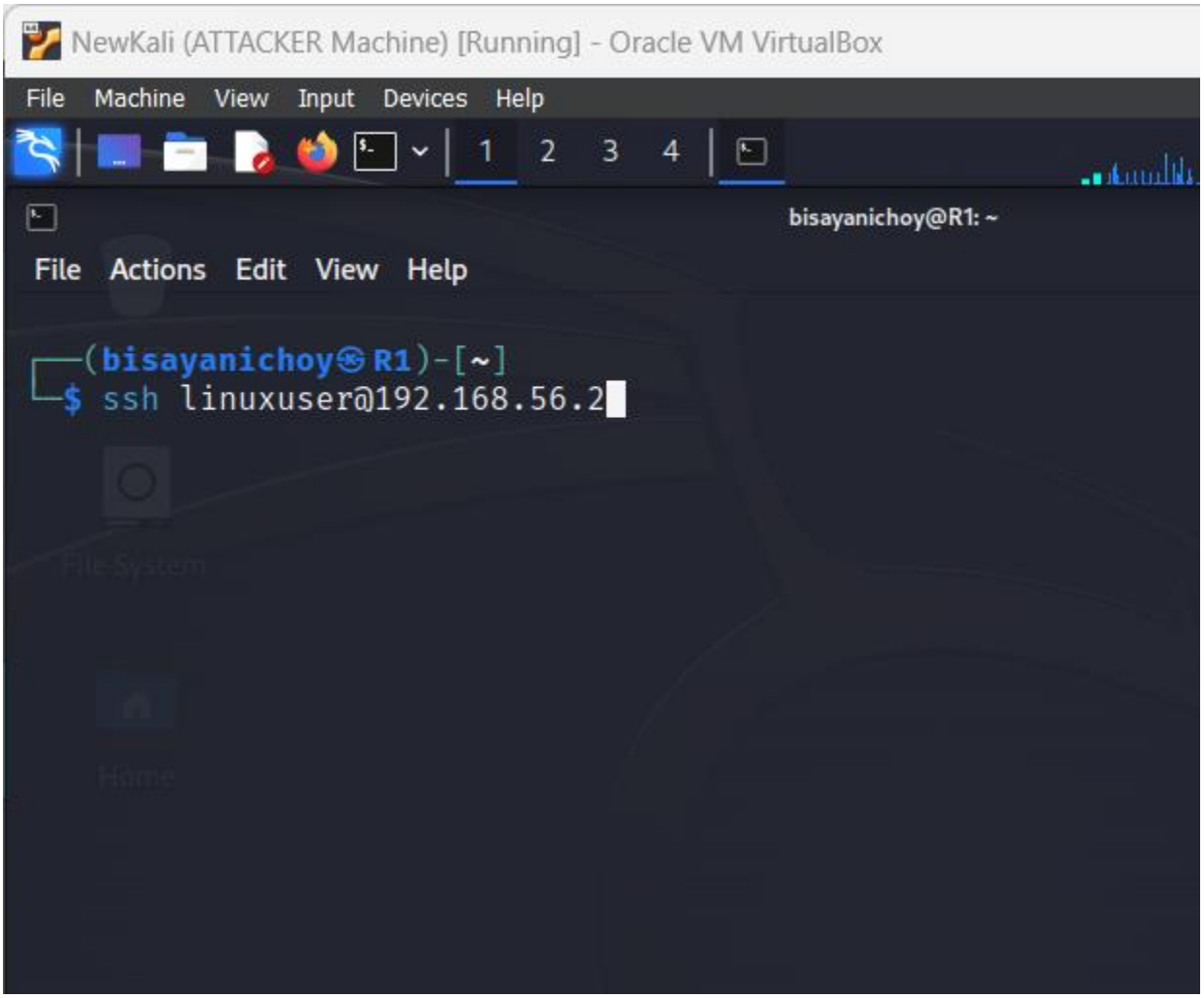
10. Here is the traffic captured, after running the command: **sudo nmap -O 192.168.56.2** on our Attacker Machine we can see where this traffic originates from.

Defender Machine:



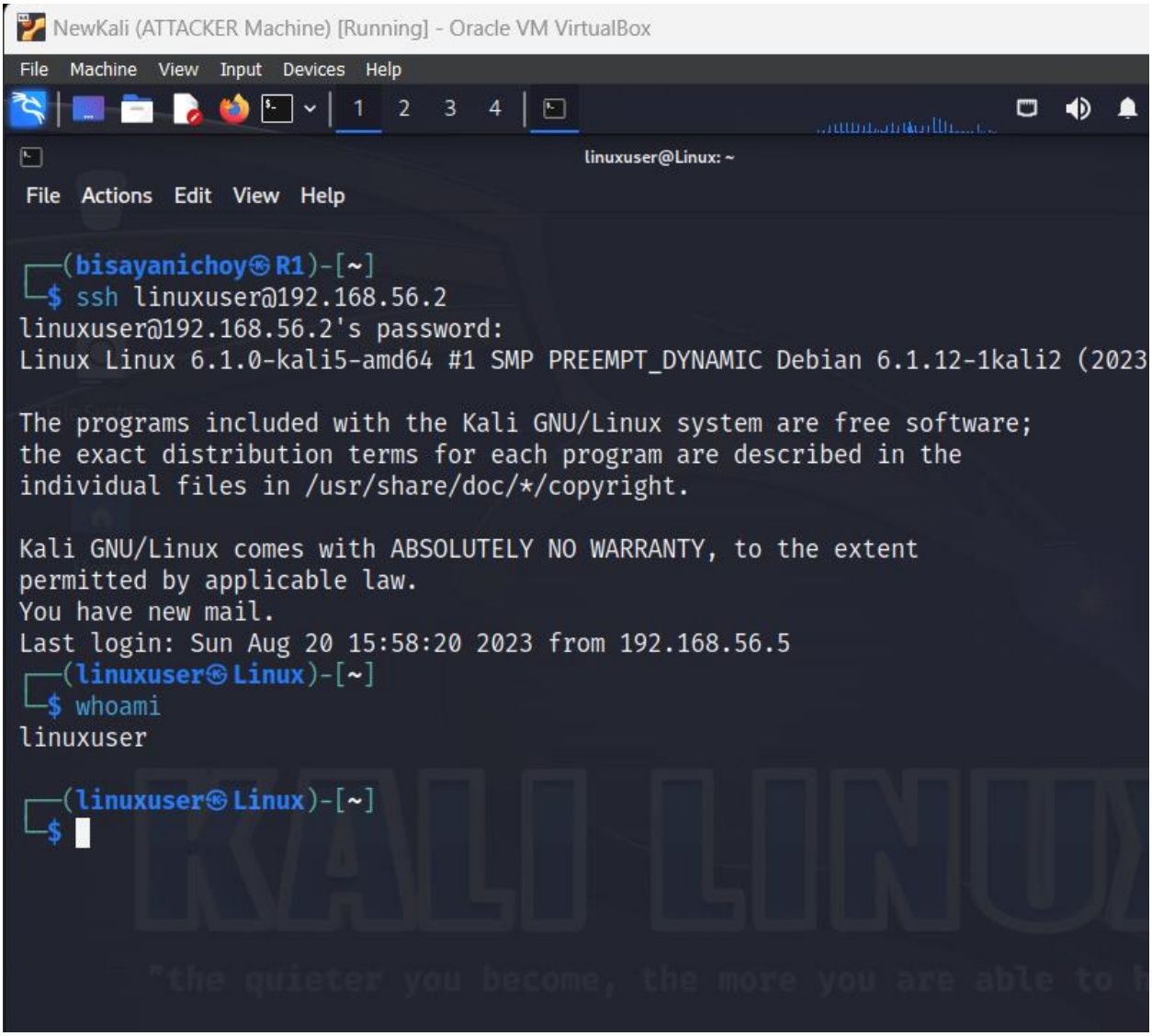
11. The previous Nmap outputs have given us information on what ports are open, since port 22 is open we are gonna establish a connection with the **Defender Machine**. I will run the command: **ssh linuxuser@192.168.56.2**.

    Attacker Machine:



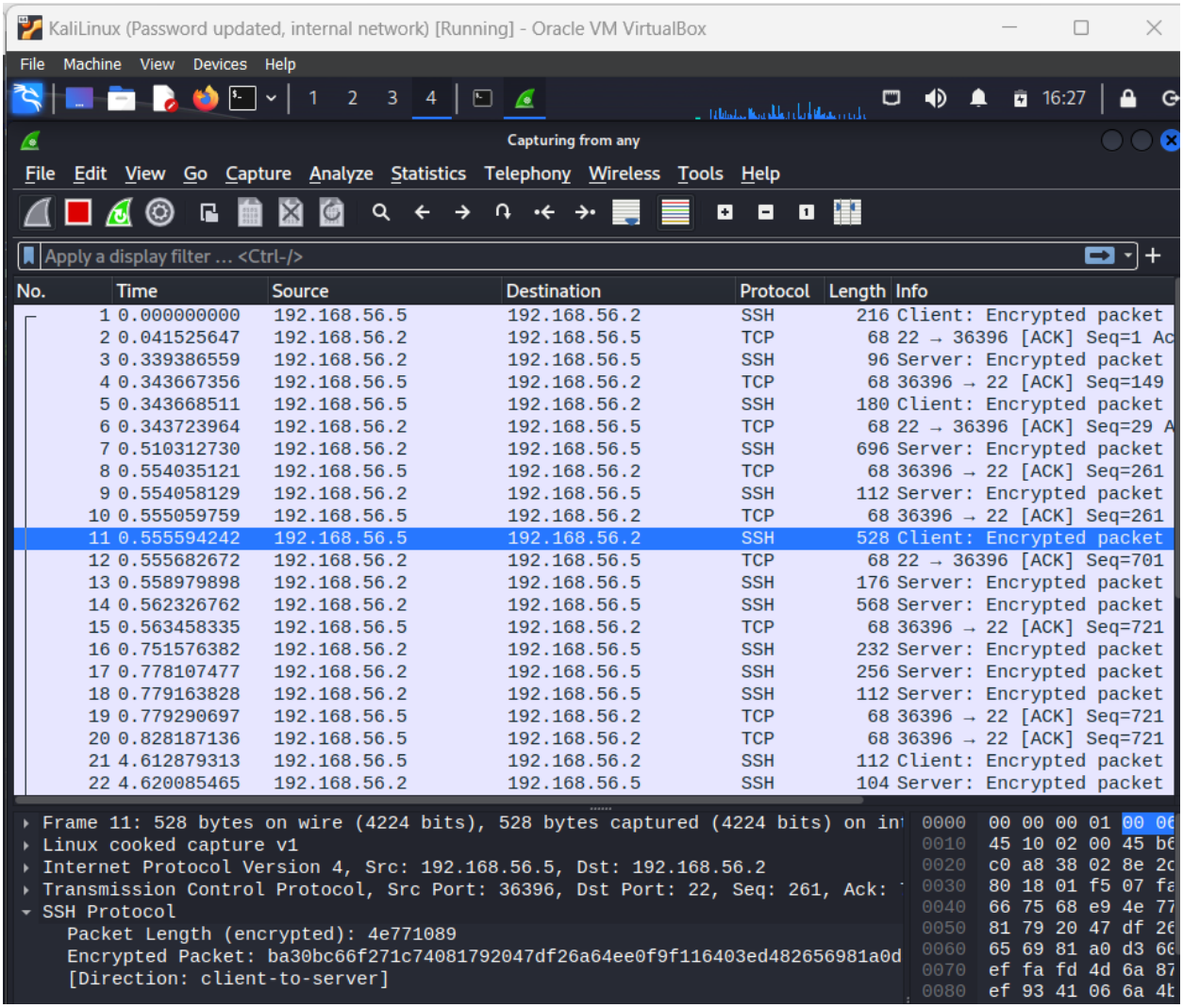
12. We have now successfully established a SSH connection with our Attacker Machine, I also execute the **whoami** command to verify we are in **linuxuser** account, so from the account named: **bisayanichoy** to **linuxuser** we can now verify that we are in the defender machines CLI.

Attacker Machine:



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.

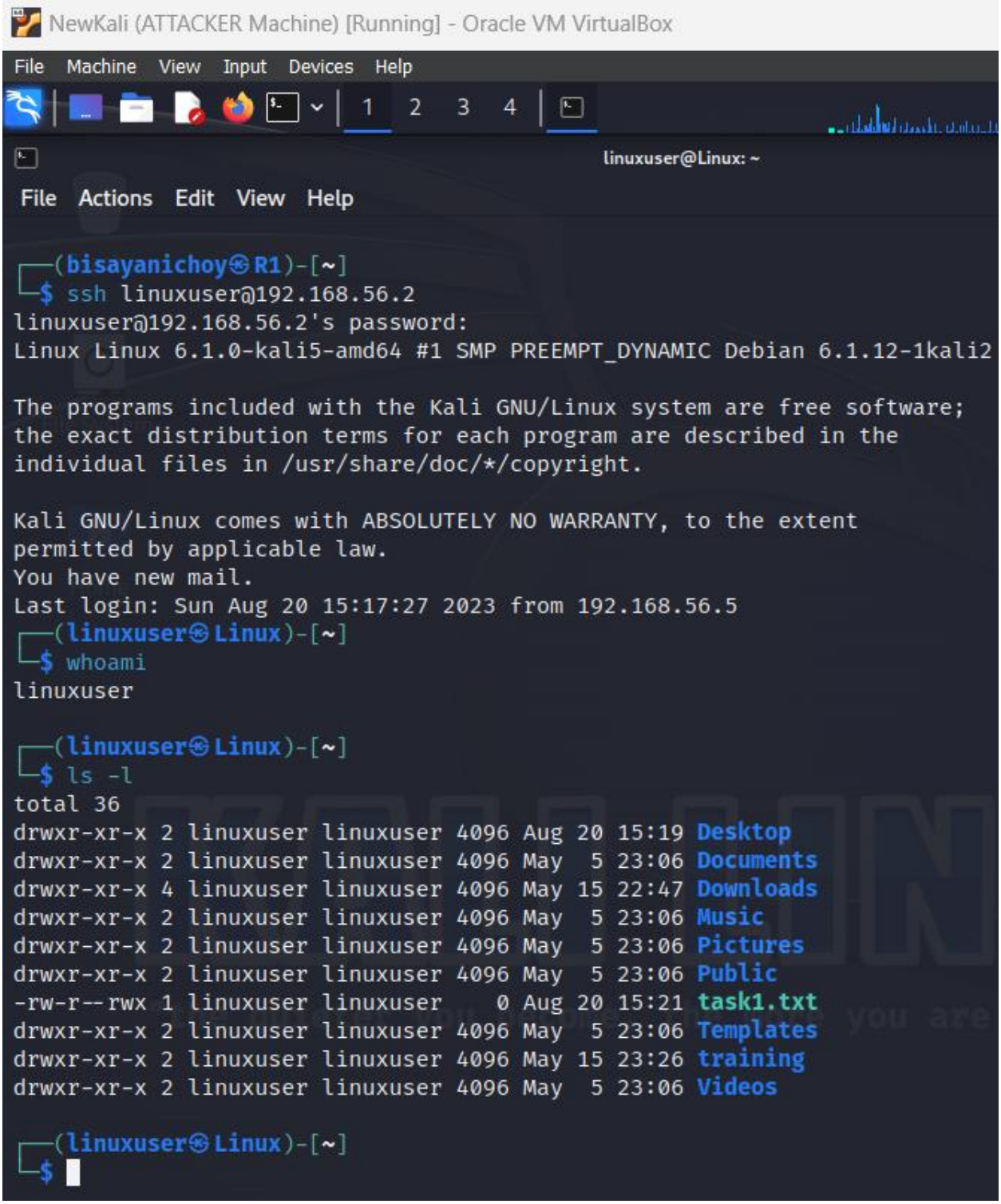
Defender Machine:



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

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.

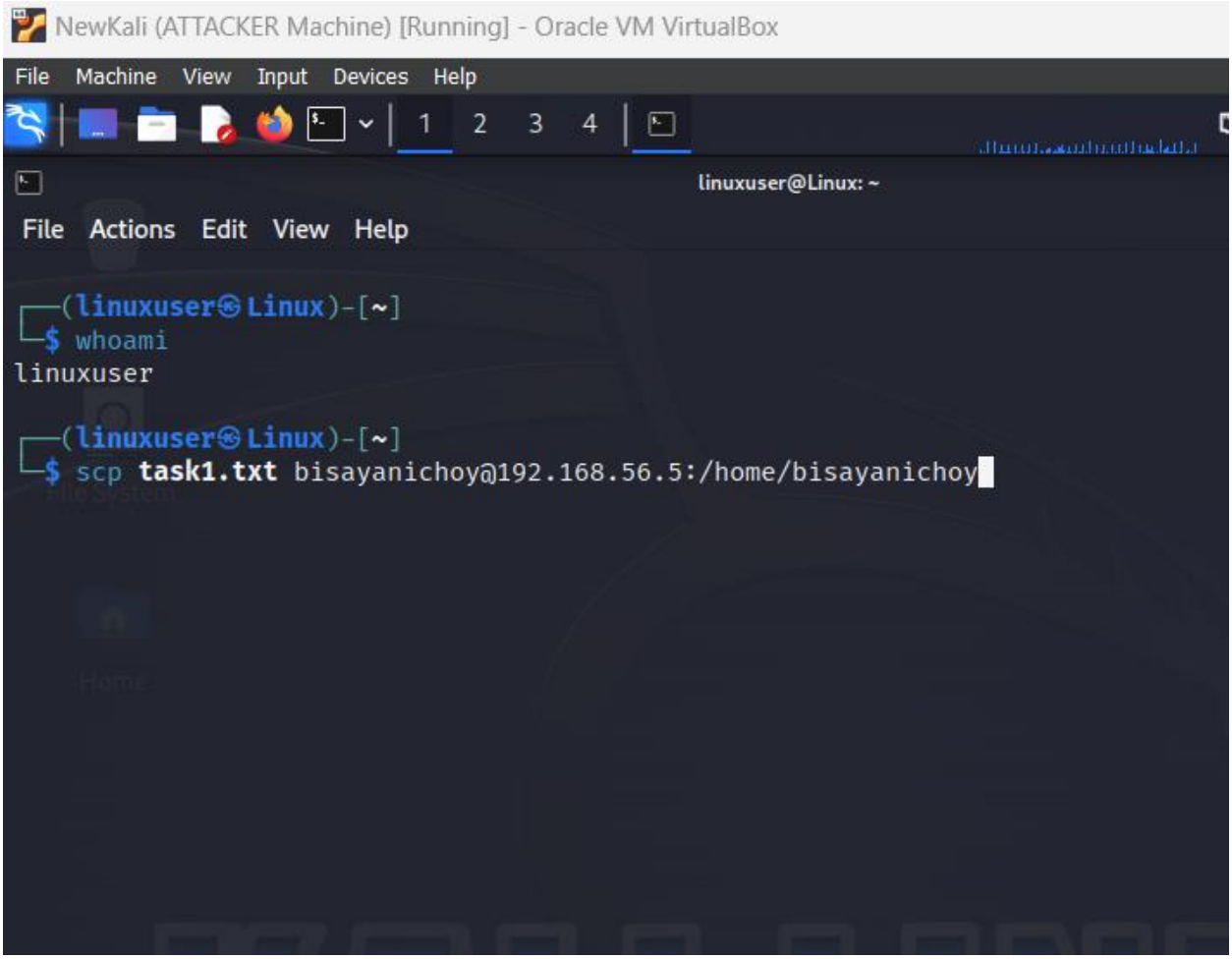
    Attacker Machine:



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

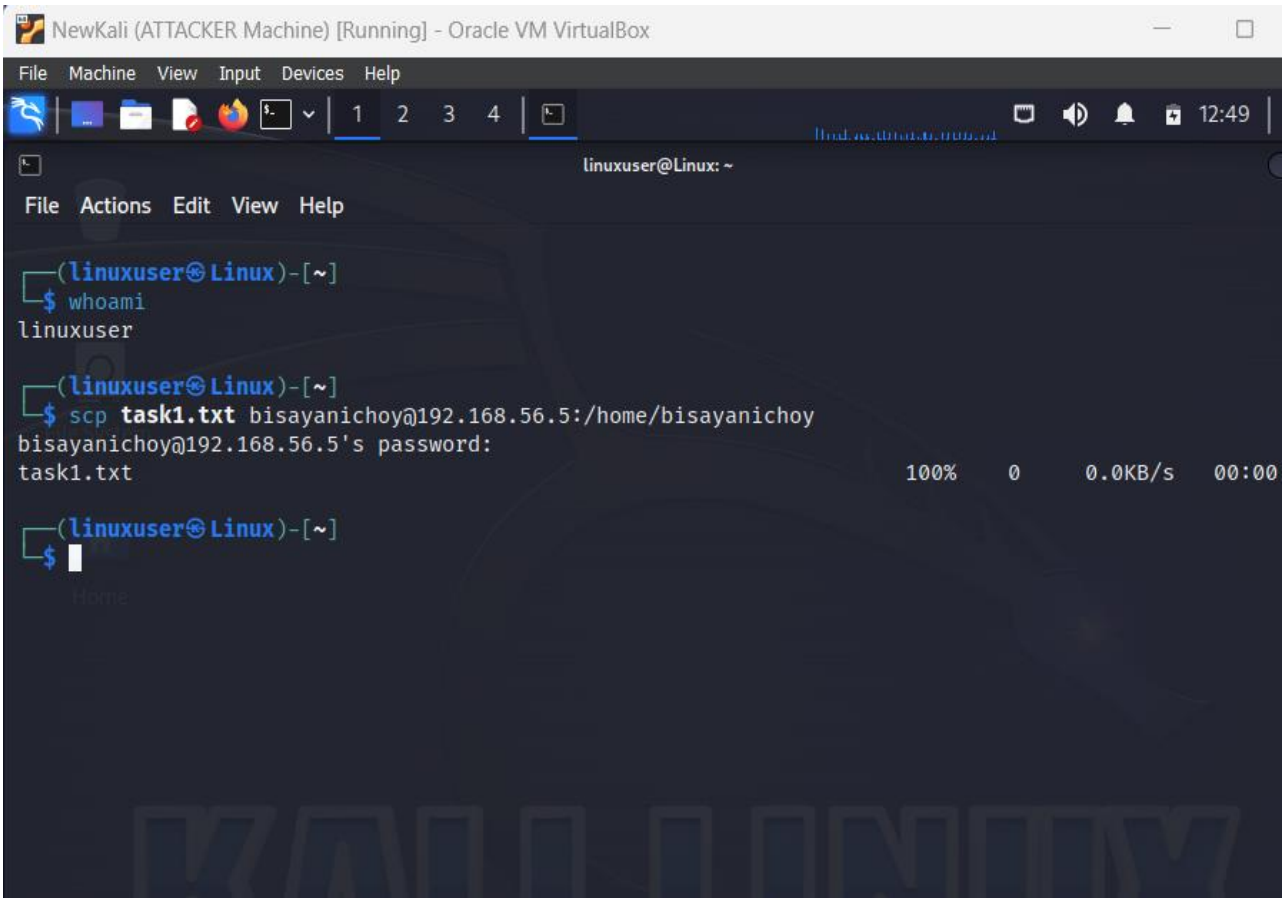
secure copy and it will copy the specified file we want to our **Attacker Machine** by specifying its account name and ip address.

Attacker Machine:



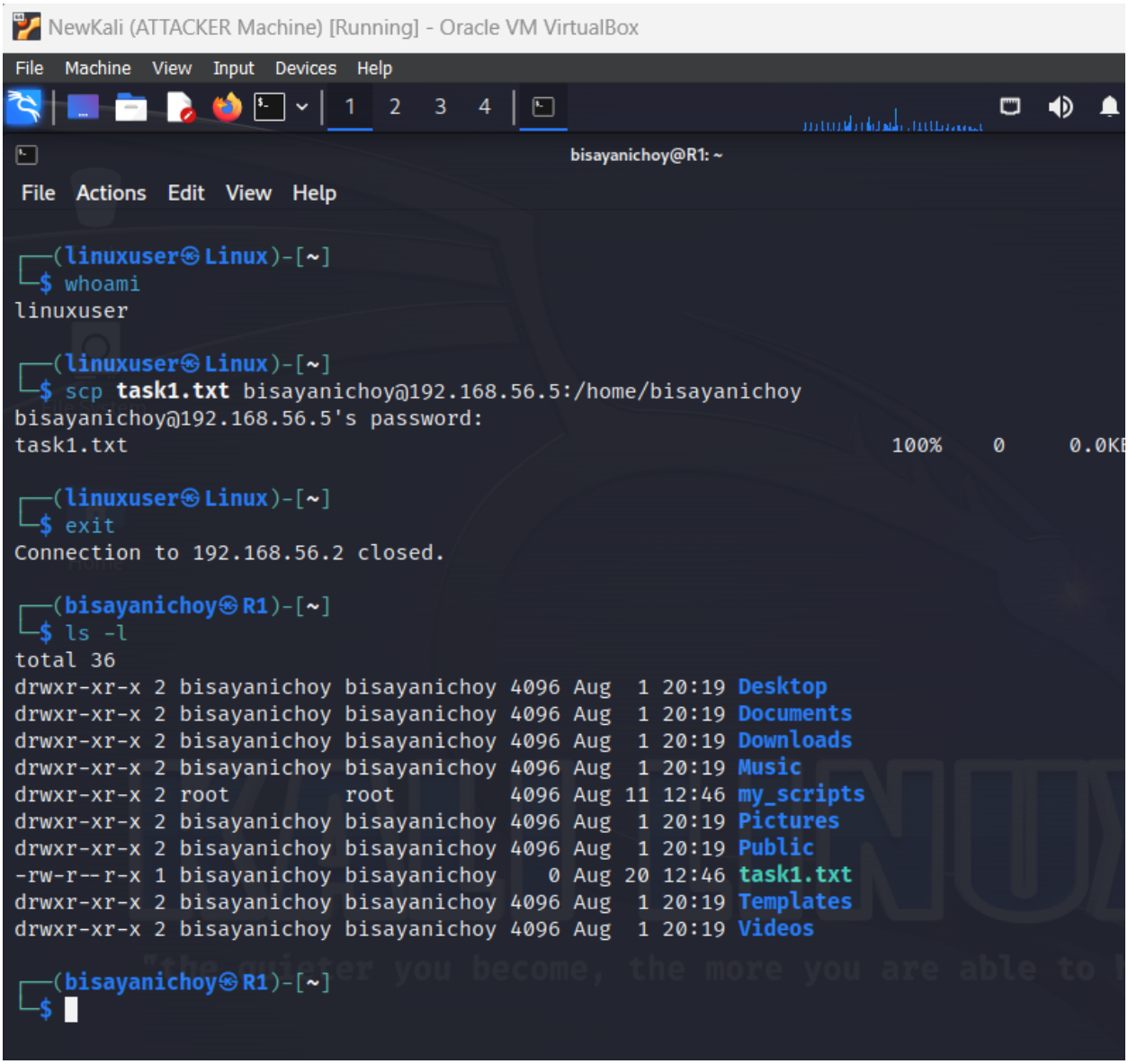
16. After running the command: **scp task1.txt bisayanichoy@192.168.56.5:/home/bisayanichoy**. It prompts me to enter bisayanichoy's password in order to continue with the scp process, as we can see in the screenshot below it displays **100%** indicating that our secure copy is now complete.

Attacker Machine:



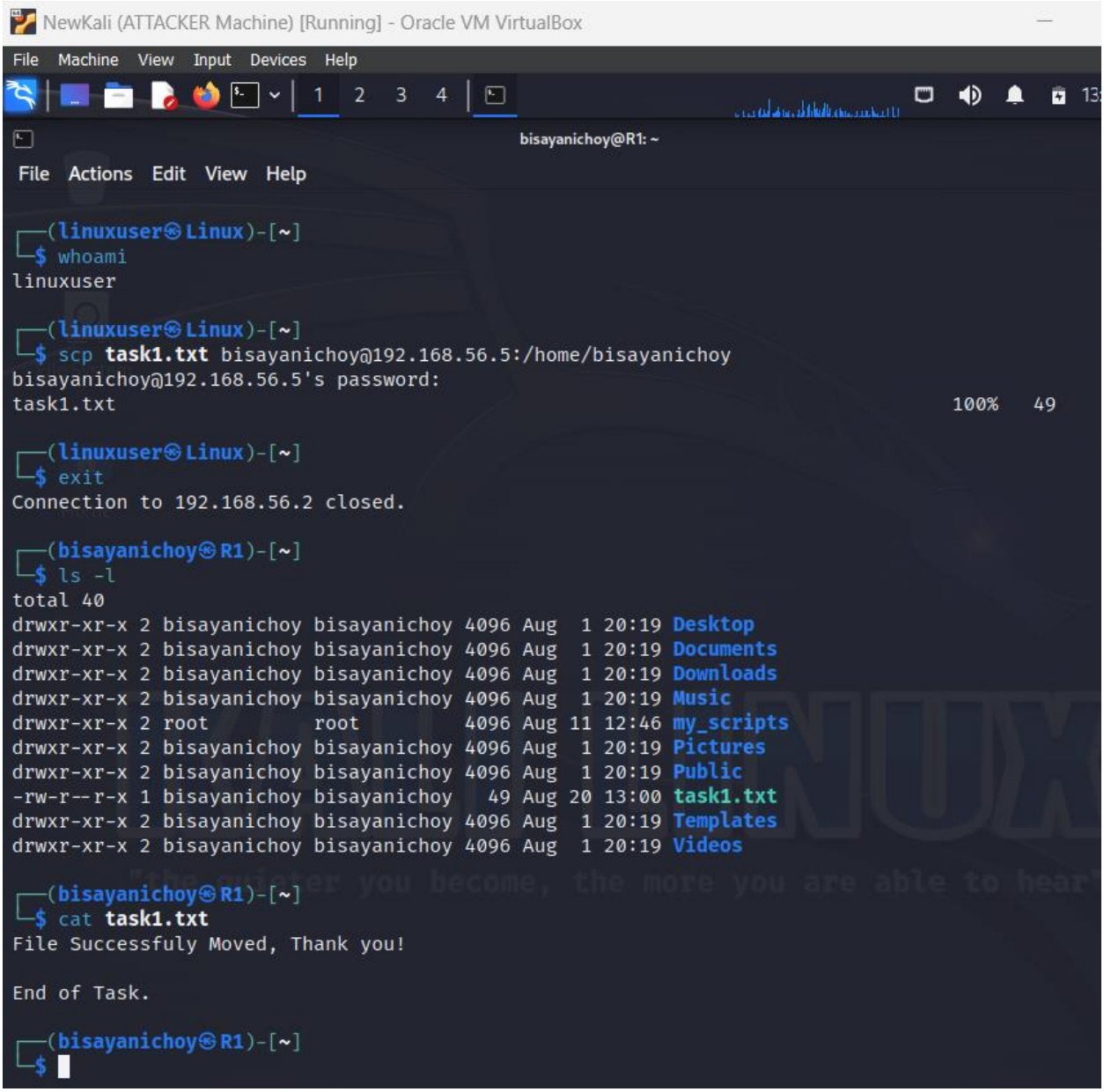
17. I now exit the ssh connection by running the command: **exit**. I type in **ls -l** to verify that we have successfully securely copy the text file from Defender Machine.

Attacker Machine:



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:



Secure Copy Completed

By: **Jason**