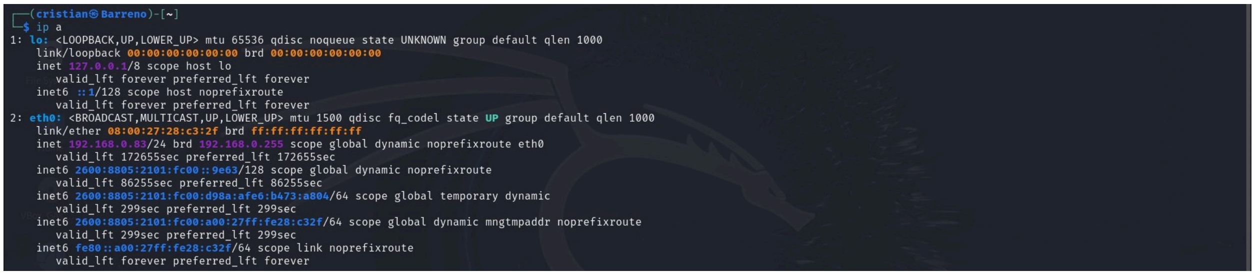
Name: Cristian Barreno

Mission Lab ALPHA Recon1: Network Identification and Reconnaissance

Mission Tasks:

Task 1: Orientation in the Unknown Virtual Environment

- Use the ‘ip a’ command to check the network interfaces on your current system.
- Execute the ip route command to view the routing table and identify the default gateway

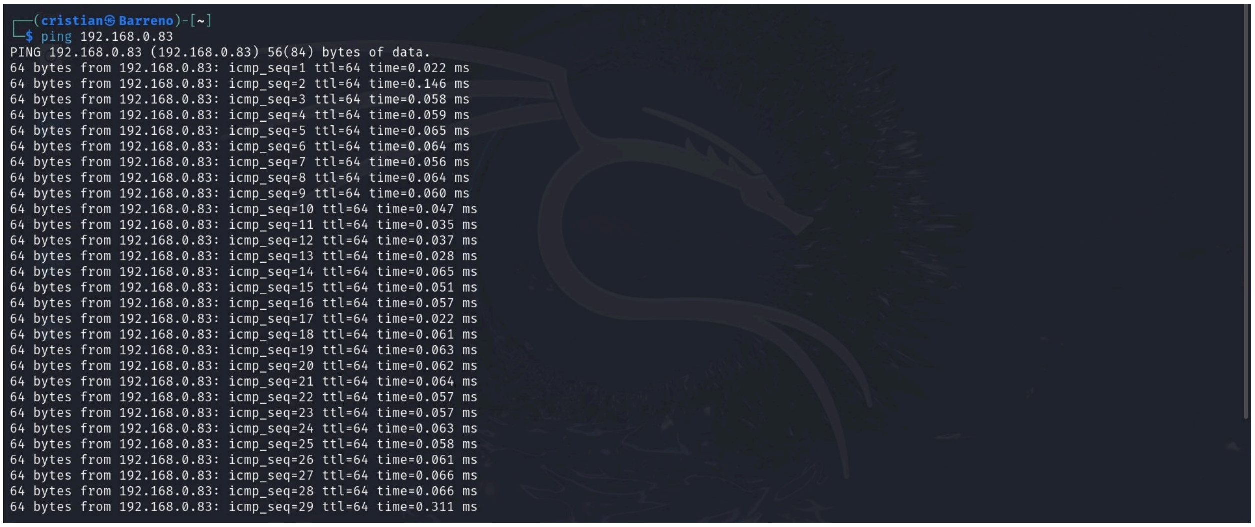


```
┌──(cristian㉿Barreno)-[~]
└─$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:28:c3:2f brd ff:ff:ff:ff:ff:ff
    inet 192.168.0.83/24 brd 192.168.0.255 scope global dynamic noprefixroute eth0
       valid_lft 172655sec preferred_lft 172655sec
    inet6 2600:8805:2101:fc00::9e63/128 scope global dynamic noprefixroute
       valid_lft 86255sec preferred_lft 86255sec
    inet6 2600:8805:2101:fc00:d98a:afe6:b473:a804/64 scope global temporary dynamic
       valid_lft 299sec preferred_lft 299sec
    inet6 2600:8805:2101:fc00:a00:27ff:fe28:c32f/64 scope global dynamic mngtmpaddr noprefixroute
       valid_lft 299sec preferred_lft 299sec
    inet6 fe80::a00:27ff:fe28:c32f/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

In the screenshot above i can see my loopback address, and also my IP address: 192.168.0.83

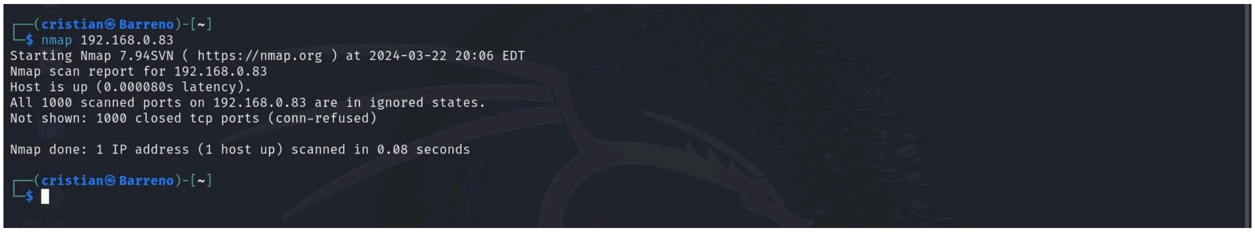
Task 2: Identifying Live Systems

- Scan the network to identify live hosts using the ‘ping’ command.
- Use ‘nmap’ to perform a port scan and identify open ports on the live hosts. (optional)



```
┌──(cristian㉿Barreno)-[~]
└─$ ping 192.168.0.83
PING 192.168.0.83 (192.168.0.83) 56(84) bytes of data.
64 bytes from 192.168.0.83: icmp_seq=1 ttl=64 time=0.022 ms
64 bytes from 192.168.0.83: icmp_seq=2 ttl=64 time=0.146 ms
64 bytes from 192.168.0.83: icmp_seq=3 ttl=64 time=0.058 ms
64 bytes from 192.168.0.83: icmp_seq=4 ttl=64 time=0.059 ms
64 bytes from 192.168.0.83: icmp_seq=5 ttl=64 time=0.065 ms
64 bytes from 192.168.0.83: icmp_seq=6 ttl=64 time=0.064 ms
64 bytes from 192.168.0.83: icmp_seq=7 ttl=64 time=0.056 ms
64 bytes from 192.168.0.83: icmp_seq=8 ttl=64 time=0.064 ms
64 bytes from 192.168.0.83: icmp_seq=9 ttl=64 time=0.060 ms
64 bytes from 192.168.0.83: icmp_seq=10 ttl=64 time=0.047 ms
64 bytes from 192.168.0.83: icmp_seq=11 ttl=64 time=0.035 ms
64 bytes from 192.168.0.83: icmp_seq=12 ttl=64 time=0.037 ms
64 bytes from 192.168.0.83: icmp_seq=13 ttl=64 time=0.028 ms
64 bytes from 192.168.0.83: icmp_seq=14 ttl=64 time=0.065 ms
64 bytes from 192.168.0.83: icmp_seq=15 ttl=64 time=0.051 ms
64 bytes from 192.168.0.83: icmp_seq=16 ttl=64 time=0.057 ms
64 bytes from 192.168.0.83: icmp_seq=17 ttl=64 time=0.022 ms
64 bytes from 192.168.0.83: icmp_seq=18 ttl=64 time=0.061 ms
64 bytes from 192.168.0.83: icmp_seq=19 ttl=64 time=0.063 ms
64 bytes from 192.168.0.83: icmp_seq=20 ttl=64 time=0.062 ms
64 bytes from 192.168.0.83: icmp_seq=21 ttl=64 time=0.064 ms
64 bytes from 192.168.0.83: icmp_seq=22 ttl=64 time=0.057 ms
64 bytes from 192.168.0.83: icmp_seq=23 ttl=64 time=0.057 ms
64 bytes from 192.168.0.83: icmp_seq=24 ttl=64 time=0.063 ms
64 bytes from 192.168.0.83: icmp_seq=25 ttl=64 time=0.058 ms
64 bytes from 192.168.0.83: icmp_seq=26 ttl=64 time=0.061 ms
64 bytes from 192.168.0.83: icmp_seq=27 ttl=64 time=0.066 ms
64 bytes from 192.168.0.83: icmp_seq=28 ttl=64 time=0.066 ms
64 bytes from 192.168.0.83: icmp_seq=29 ttl=64 time=0.311 ms
```

I used ping to test connectivity.

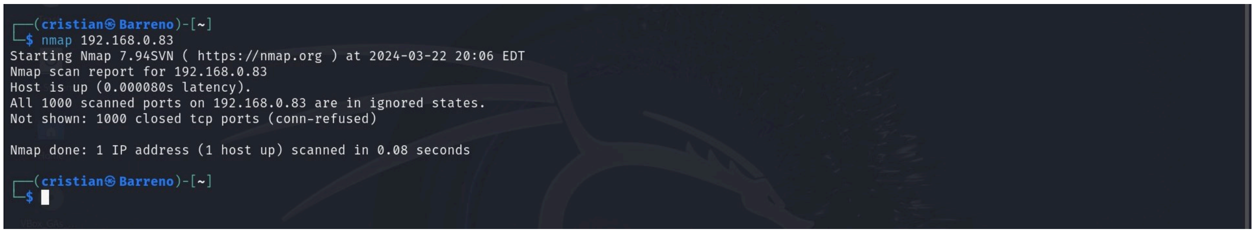


```
┌──(cristian㉿Barreno)-[~]
└─$ nmap 192.168.0.83
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-22 20:06 EDT
Nmap scan report for 192.168.0.83
Host is up (0.000080s latency).
All 1000 scanned ports on 192.168.0.83 are in ignored states.
Not shown: 1000 closed tcp ports (conn-refused)

Nmap done: 1 IP address (1 host up) scanned in 0.08 seconds

┌──(cristian㉿Barreno)-[~]
└─$ 
```

Nmap is short for network mapper, and is a tool used to scan IP addresses and ports in a network.

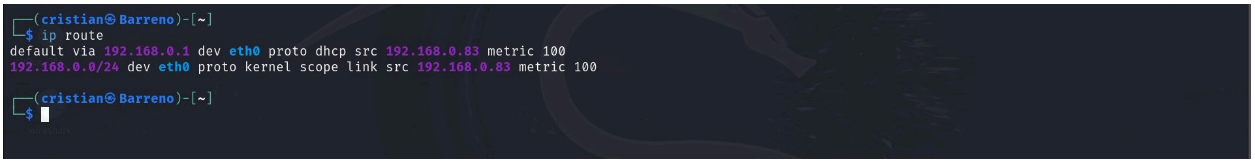
Task 3: Network Mapping and System Discovery

Perform a detailed network scan using nmap to identify all active systems and their open ports. Use nmap to discover the operating system and service versions on the identified systems.



```
┌──(cristian㉿Barreno)-[~]
└─$ nmap 192.168.0.83
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-22 20:06 EDT
Nmap scan report for 192.168.0.83
Host is up (0.000080s latency).
All 1000 scanned ports on 192.168.0.83 are in ignored states.
Not shown: 1000 closed tcp ports (conn-refused)

Nmap done: 1 IP address (1 host up) scanned in 0.08 seconds

┌──(cristian㉿Barreno)-[~]
└─$ 
```

ip route command

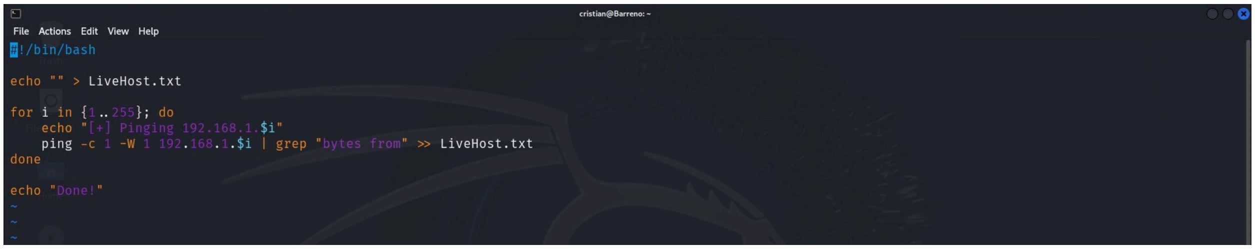


```
┌──(cristian㉿Barreno)-[~]
└─$ ip route
default via 192.168.0.1 dev eth0 proto dhcp src 192.168.0.83 metric 100
192.168.0.0/24 dev eth0 proto kernel scope link src 192.168.0.83 metric 100

┌──(cristian㉿Barreno)-[~]
└─$ 
```

With ip route i can check the routing table and find the default waterway.

Task 4: ASSIGNMENT

Create a bash script called “recon1.sh” that will contain the for loop provided above that will run and create an output file on the results. Please write down a short list of the commands and tools we used during the mission. Store your output in a file called “TargetList.txt” and upload this file with your assignment submission.

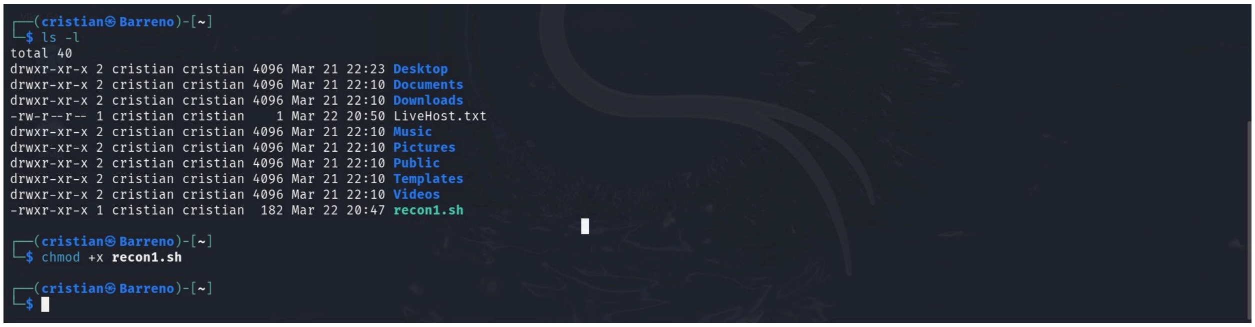


```
#!/bin/bash

echo "" > LiveHost.txt

for i in {1..255}; do
    echo "[+] Pinging 192.168.1.$i"
    ping -c 1 -W 1 192.168.1.$i | grep "bytes from" >> LiveHost.txt
done

echo "Done!"
~
~
~
```

In the screenshot above i used the text editor vim to create a bash script inside the recon1.sh file

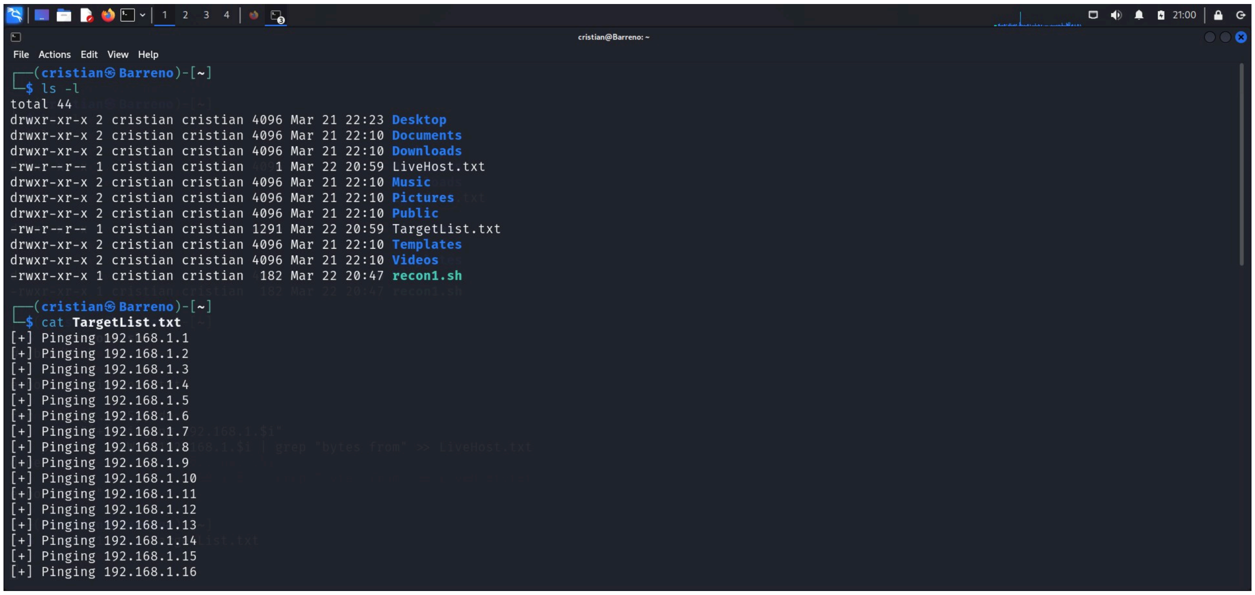
The tools and commands and tools that we used during this mission are:

- ip a
- ping
- nmap
- ip route
- chmod
- cat
- Vim
- Pwd



```
┌──(cristian㉿Barreno)-[~]
└─$ ls -l
total 40
drwxr-xr-x 2 cristian cristian 4096 Mar 21 22:23 Desktop
drwxr-xr-x 2 cristian cristian 4096 Mar 21 22:10 Documents
drwxr-xr-x 2 cristian cristian 4096 Mar 21 22:10 Downloads
-rw-r--r-- 1 cristian cristian    1 Mar 22 20:50 LiveHost.txt
drwxr-xr-x 2 cristian cristian 4096 Mar 21 22:10 Music
drwxr-xr-x 2 cristian cristian 4096 Mar 21 22:10 Pictures
drwxr-xr-x 2 cristian cristian 4096 Mar 21 22:10 Public
drwxr-xr-x 2 cristian cristian 4096 Mar 21 22:10 Templates
drwxr-xr-x 2 cristian cristian 4096 Mar 21 22:10 Videos
-rwxr-xr-x 1 cristian cristian  182 Mar 22 20:47 recon1.sh

┌──(cristian㉿Barreno)-[~]
└─$ chmod +x recon1.sh

┌──(cristian㉿Barreno)-[~]
└─$ 
```

In the screenshot above I used chmod, or change mode to modify the file’s permissions.



```
┌──(cristian㉿Barreno)-[~]
└─$ ls -l
total 44
drwxr-xr-x 2 cristian cristian 4096 Mar 21 22:23 Desktop
drwxr-xr-x 2 cristian cristian 4096 Mar 21 22:10 Documents
drwxr-xr-x 2 cristian cristian 4096 Mar 21 22:10 Downloads
-rw-r--r-- 1 cristian cristian    1 Mar 22 20:59 LiveHost.txt
drwxr-xr-x 2 cristian cristian 4096 Mar 21 22:10 Music
drwxr-xr-x 2 cristian cristian 4096 Mar 21 22:10 Pictures
drwxr-xr-x 2 cristian cristian 4096 Mar 21 22:10 Public
-rw-r--r-- 1 cristian cristian 1291 Mar 22 20:59 TargetList.txt
drwxr-xr-x 2 cristian cristian 4096 Mar 21 22:10 Templates
drwxr-xr-x 2 cristian cristian 4096 Mar 21 22:10 Videos
-rwxr-xr-x 1 cristian cristian  182 Mar 22 20:47 recon1.sh

┌──(cristian㉿Barreno)-[~]
└─$ cat TargetList.txt
[+] Pinging 192.168.1.1
[+] Pinging 192.168.1.2
[+] Pinging 192.168.1.3
[+] Pinging 192.168.1.4
[+] Pinging 192.168.1.5
[+] Pinging 192.168.1.6
[+] Pinging 192.168.1.7
[+] Pinging 192.168.1.8
[+] Pinging 192.168.1.9
[+] Pinging 192.168.1.10
[+] Pinging 192.168.1.11
[+] Pinging 192.168.1.12
[+] Pinging 192.168.1.13
[+] Pinging 192.168.1.14
[+] Pinging 192.168.1.15
[+] Pinging 192.168.1.16
```

In the screenshot above i stored the output of the script onto a file called TargetList.txt