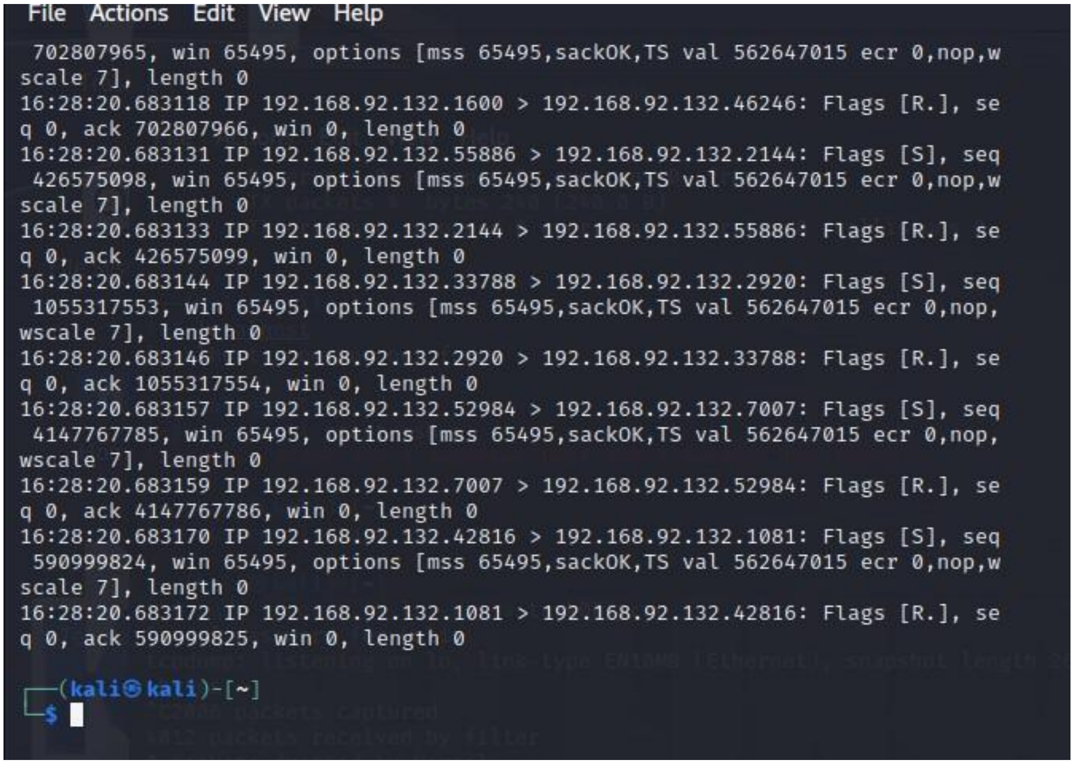
OVERVIEW:

The objective of this lab was to perform different types of network scans and analyze the results using network scanning tools. The lab was completed using my own devices within my personal network.

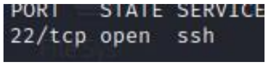
ANALYSIS:

Task00:



```
 702807965, win 65495, options [mss 65495,sackOK,TS val 562647015 ecr 0,nop,w
scale 7], length 0
16:28:20.683118 IP 192.168.92.132.1600 > 192.168.92.132.46246: Flags [R.], se
q 0, ack 702807966, win 0, length 0
16:28:20.683131 IP 192.168.92.132.55886 > 192.168.92.132.2144: Flags [S], seq
 426575098, win 65495, options [mss 65495,sackOK,TS val 562647015 ecr 0,nop,w
scale 7], length 0
16:28:20.683133 IP 192.168.92.132.2144 > 192.168.92.132.55886: Flags [R.], se
q 0, ack 426575099, win 0, length 0
16:28:20.683144 IP 192.168.92.132.33788 > 192.168.92.132.2920: Flags [S], seq
 1055317553, win 65495, options [mss 65495,sackOK,TS val 562647015 ecr 0,nop,
wscale 7], length 0
16:28:20.683146 IP 192.168.92.132.2920 > 192.168.92.132.33788: Flags [R.], se
q 0, ack 1055317554, win 0, length 0
16:28:20.683157 IP 192.168.92.132.52984 > 192.168.92.132.7007: Flags [S], seq
 4147767785, win 65495, options [mss 65495,sackOK,TS val 562647015 ecr 0,nop,
wscale 7], length 0
16:28:20.683159 IP 192.168.92.132.7007 > 192.168.92.132.52984: Flags [R.], se
q 0, ack 4147767786, win 0, length 0
16:28:20.683170 IP 192.168.92.132.42816 > 192.168.92.132.1081: Flags [S], seq
 590999824, win 65495, options [mss 65495,sackOK,TS val 562647015 ecr 0,nop,w
scale 7], length 0
16:28:20.683172 IP 192.168.92.132.1081 > 192.168.92.132.42816: Flags [R.], se
q 0, ack 590999825, win 0, length 0

┌──(kali㉿kali)-[~]
└─$ 
```

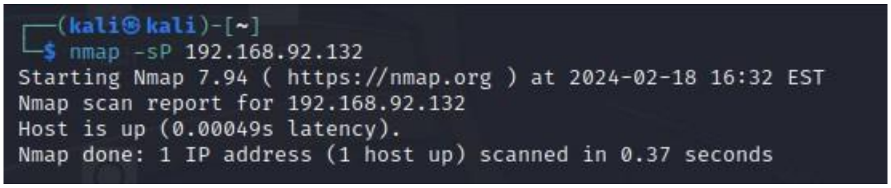


```
PORT   STATE SERVICE
22/tcp open  ssh
```

Task01:

Active System:

192.168.92.132



```
┌──(kali㉿kali)-[~]
└─$ nmap -sP 192.168.92.132
Starting Nmap 7.94 ( https://nmap.org ) at 2024-02-18 16:32 EST
Nmap scan report for 192.168.92.132
Host is up (0.00049s latency).
Nmap done: 1 IP address (1 host up) scanned in 0.37 seconds
```

Task02:

You could use a command like:

nmap -iL discovered_hosts.txt -sV -n -Pn -p- --open -oA port_scan_results

-iL would read the hosts from the file listed

-sV would detect the versions

-n would tell nmap to not perfrom DNS resolution

-Pn would skip host discovery

-p- would scan all ports

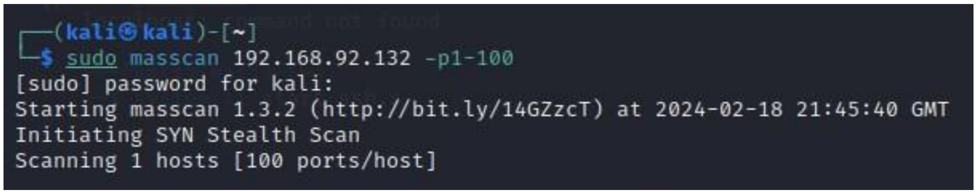
--open would only show open ports in the results -

oA would output the results to the listed file.

Now for my lab I only had SSH open on my machine. So

the result would be – ***22/tcp open ssh OpenSSH 8.8***

Task03:



```
┌──(kali㉿kali)-[~]
└─$ sudo masscan 192.168.92.132 -p1-100
[sudo] password for kali:
Starting masscan 1.3.2 (http://bit.ly/14GZzcT) at 2024-02-18 21:45:40 GMT
Initiating SYN Stealth Scan
Scanning 1 hosts [100 ports/host]
```

On the machine that I targeted only SSH is open port 22. Typically, on other networks or computers this isn't the case.

For example, what ports are commonly open?

HTTPS – 443

HTTP – 80

DNS – 53

FTP - 21

TCP- 8080 & 1433

SMTP – 25

etc.

Task04:

My scan didn’t show any results. But I also have most ports disabled on the test machine that I was targeting. It is good though to be aware of the vulnerabilities, however. Even with commonly open ports like 443 or 21. Vulnerabilities still exist. For example, some newer vulnerabilities that could be used to exploit these open ports are CVE-2021-34527. This is a vulnerability in the Windows Print Spooler service that allows for remote code execution. This could be exploited over 443. Additionally, a vulnerability like CVE-2022-0538 could be used over port 21 to exploit FTP. The vulnerability specifically is a vulnerability in Cisco IOS software that allows authenticated attackers to execute commands via crafted requests.

Throughout this lab you can see how easy it is to find open ports. These ports serve as a way into a network, and they will be prime targets of attackers. Using NMAP to discover these vulnerabilities is good because you can then take measures to mitigate the problem.

Task06:

The ARP scan revealed the MAC addresses associated with each IP address on the target network. I’m seeing this because ARP or the Address Resolution protocol is what connects IP addresses to a fixed physical machines address, known as a MAC address. This type of scan is useful for discovering devices within the same area as it provides information about the devices' MAC addresses, aiding in network mapping and device identification.