Students: Paulo Henrique Gonçalves e Arthur Henrique Cavalcanti

PA2Q4
a) How does nmap work? (organizations, scripts, techniques....)

nmap is a port and network scanning tool focused on protection, it uses protocols such as tcp, UDP, ftp and can perform all these protocols completely or incompletely, according to the user's needs to reduce network noise. For example: the -sS flag that only sends a Syn connection and waits for a response, without completing the TCP connection, being a silent way of scanning another flag is -sU which uses the UDP protocol Furthermore, it has flags such as s0 which uses IP protocol and -b for FTP protocol.

For the organization, nmap expects an IP address, or a set of IP addresses to scan, that is, nmap can also scan networks and discover all the addresses there, for this it supports CIDR notation with the number of bits at the end.

To improve scanning, nmap is also able to continue a conversation with the port to detect the software running there and often the current version of it. Through this bit analysis it is sometimes possible to also detect the operating system that is running on the target. But obviously, when these scans are carried out, the exchange of information on your part is also large, generating logs and noise on the network

Nmap Features:
Fast scan Host discovery, Port scanning, Version detection, Ping Scan, TCP/IP stack fingerprinting, Scriptable interaction with the target,

Some nmap scripts:

brute:
These scripts use brute force attacks to guess authentication credentials of a remote server

exploit:
These scripts aim to actively exploit some vunerability.

fuzzer:
This category contains scripts which are designed to send server software randomized fields in each packet.

safe:
Scripts which weren't designed to crash services.

b) Explain how to perform portscan through firewalls (simple state filter).

Nmap has standard support for some techniques for some search techniques to cross the firewalls, ome of which are: -f flag: fragments the packets sent from scan to confuse the firewall. -D flag: uses the scan between serveral decoys, meaning that the firewall does not know which one is doing the scan and may let the scan be carried out. However, with deeper analysis, the target is able to discover the origin of the attack.

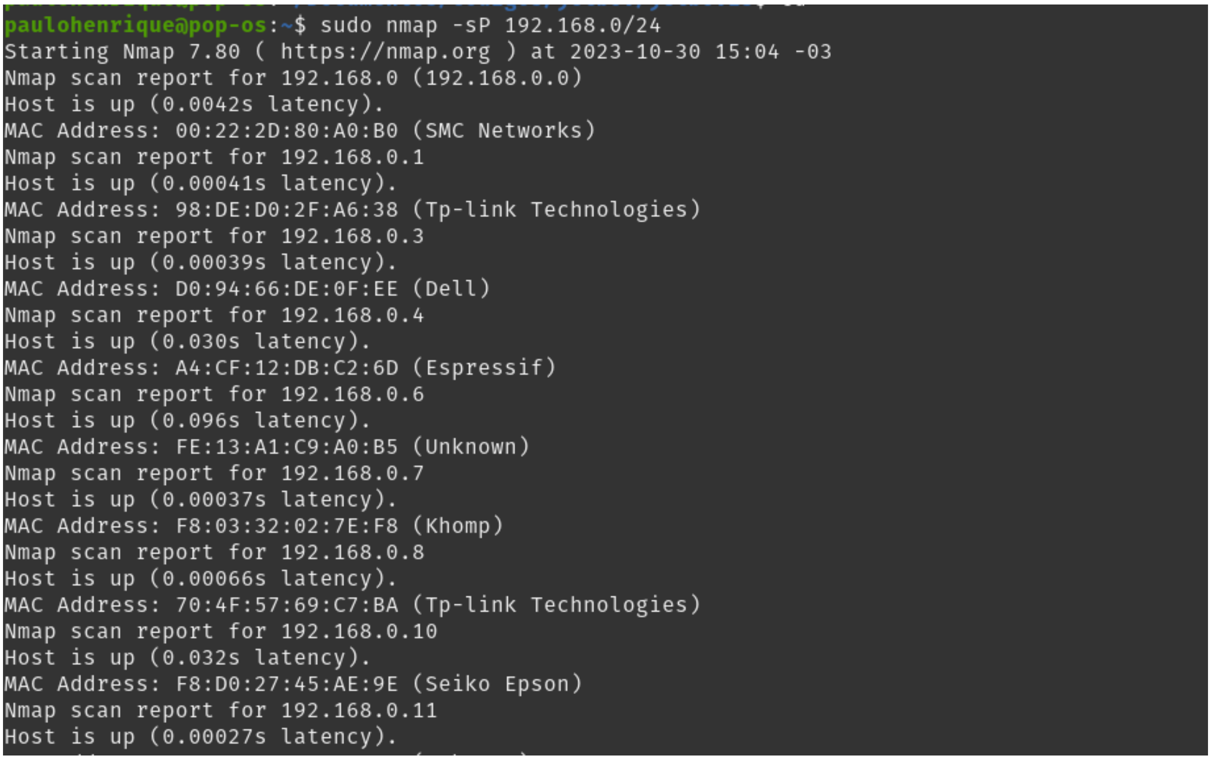
Furthermore, Nmap provides serveral ways to change the packets sent in the desired way, including source IP, port, and TTL, allowing the user to disguise the packet as they wish. In addition to being able to create proxies to tunnel the connection. In short, it is possible to change the way the scan is performed to perform more specific scans such as IDLE or FTP bounce

c) Systematize how to map a network using nmap. What limitations? What can be obtained?

you can start using the flag that "skip port scan" to quickly outline each subnet. As the name suggests, this nmap scan doesn't scan ports. Instead, it is just a "ping scan".

ex:# nmap -sP (ip of device or subnet of scan)

with this you can see the subnet ipadress and MAC



```
paulohenrique@pop-os:~$ sudo nmap -sP 192.168.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2023-10-30 15:04 -03
Nmap scan report for 192.168.0 (192.168.0.0)
Host is up (0.0042s latency).
MAC Address: 00:22:2D:80:A0:B0 (SMC Networks)
Nmap scan report for 192.168.0.1
Host is up (0.00041s latency).
MAC Address: 98:DE:D0:2F:A6:38 (Tp-link Technologies)
Nmap scan report for 192.168.0.3
Host is up (0.00039s latency).
MAC Address: D0:94:66:DE:0F:EE (Dell)
Nmap scan report for 192.168.0.4
Host is up (0.030s latency).
MAC Address: A4:CF:12:DB:C2:6D (Espressif)
Nmap scan report for 192.168.0.6
Host is up (0.096s latency).
MAC Address: FE:13:A1:C9:A0:B5 (Unknown)
Nmap scan report for 192.168.0.7
Host is up (0.00037s latency).
MAC Address: F8:03:32:02:7E:F8 (Khomp)
Nmap scan report for 192.168.0.8
Host is up (0.00066s latency).
MAC Address: 70:4F:57:69:C7:BA (Tp-link Technologies)
Nmap scan report for 192.168.0.10
Host is up (0.032s latency).
MAC Address: F8:D0:27:45:AE:9E (Seiko Epson)
Nmap scan report for 192.168.0.11
Host is up (0.00027s latency).
```

As can see, sometimes you can have more information about the subnet.

Souce:https://www.youtube.com/watch?v=RxoQTV74s1c
https://nmap.org/docs.html
https://pt.wikipedia.org/wiki/Nmap
https://en.wikipedia.org/wiki/Nmap
https://www.networkworld.com/article/2761930/unix-how-to--using-nmap-to-map-your-network.html