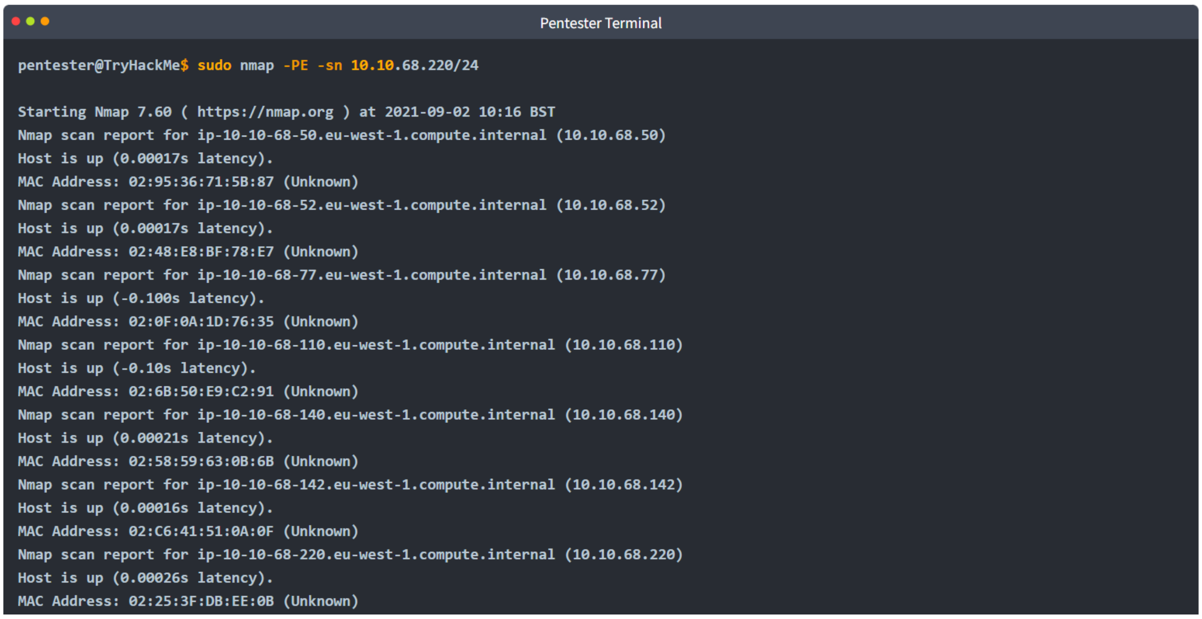
3.1 Interrogate a network to identify the network assets and their configuration.

Scan the network – Discover devices connected to the network by using network scanning tools such as Nmap, Advanced IP Scanner and list all active devices.

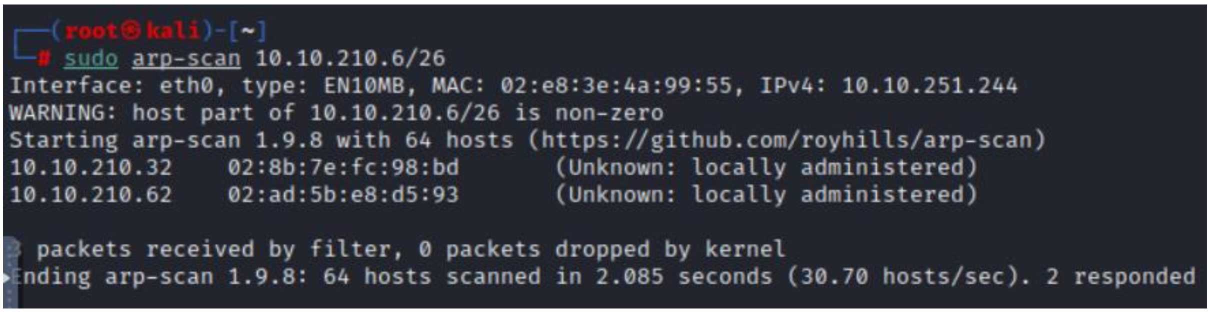


```
pentester@TryHackMe$ sudo nmap -PE -sn 10.10.68.220/24

Starting Nmap 7.60 ( https://nmap.org ) at 2021-09-02 10:16 BST
Nmap scan report for ip-10-10-68-50.eu-west-1.compute.internal (10.10.68.50)
Host is up (0.00017s latency).
MAC Address: 02:95:36:71:5B:87 (Unknown)
Nmap scan report for ip-10-10-68-52.eu-west-1.compute.internal (10.10.68.52)
Host is up (0.00017s latency).
MAC Address: 02:48:E8:BF:78:E7 (Unknown)
Nmap scan report for ip-10-10-68-77.eu-west-1.compute.internal (10.10.68.77)
Host is up (-0.100s latency).
MAC Address: 02:0F:0A:1D:76:35 (Unknown)
Nmap scan report for ip-10-10-68-110.eu-west-1.compute.internal (10.10.68.110)
Host is up (-0.10s latency).
MAC Address: 02:6B:50:E9:C2:91 (Unknown)
Nmap scan report for ip-10-10-68-140.eu-west-1.compute.internal (10.10.68.140)
Host is up (0.00021s latency).
MAC Address: 02:58:59:63:0B:6B (Unknown)
Nmap scan report for ip-10-10-68-142.eu-west-1.compute.internal (10.10.68.142)
Host is up (0.00016s latency).
MAC Address: 02:C6:41:51:0A:0F (Unknown)
Nmap scan report for ip-10-10-68-220.eu-west-1.compute.internal (10.10.68.220)
Host is up (0.00026s latency).
MAC Address: 02:25:3F:DB:EE:0B (Unknown)
```

Fig (3.1/1) – Using Nmap in Try Hack Me by sending ICMP echo packets to every IP address on the subnet. We can see live hosts reply together with their MAC addresses.

Identify network devices – identify assets and collect data. Discover network devices such as router, switch, server, printer etc. Keep detailed records of these devices including IP addresses, hostnames and MAC addresses of the devices in the network, interface details, port configurations, etc.



```
┌──(root㉿kali)-[~]
└─# sudo arp-scan 10.10.210.6/26
Interface: eth0, type: EN10MB, MAC: 02:e8:3e:4a:99:55, IPv4: 10.10.251.244
WARNING: host part of 10.10.210.6/26 is non-zero
Starting arp-scan 1.9.8 with 64 hosts (https://github.com/royhills/arp-scan)
10.10.210.32    02:8b:7e:fc:98:bd       (Unknown: locally administered)
10.10.210.62    02:ad:5b:e8:d5:93       (Unknown: locally administered)

 packets received by filter, 0 packets dropped by kernel
nding arp-scan 1.9.8: 64 hosts scanned in 2.085 seconds (30.70 hosts/sec). 2 responded
```

Fig (3.1/2) – Using ARP scan to find MAC addresses of the specific IP addresses.

Get device information – Gather detailed information of each identified device in the network. Understand its role and configuration within the network. Identify devices using protocols such as SNMP for information such as system description, system name, and other operational statistics, SSH for configuration details and system information.

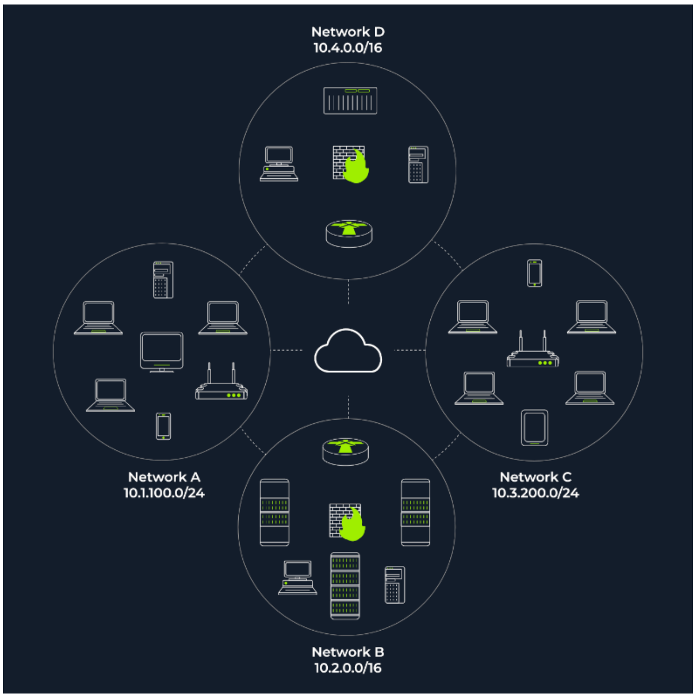


Fig (3.1/3) a network diagram with four network segments

Look at the configuration setting – Utilize protocols to access and retrieve configurations files (for backup). This includes running configuration, startup configuration, ACLs, and other policy settings. Analyze configuration data (for configuration management) of the current setup including device roles, network topology, and operational settings. Identify misconfigurations and inconsistencies which could impact network performance or security.

Documentation – Document details of network assests and their configurations and maintain the records up-to-date. This documentation should include:

- Device, names, types, and roles.
- IP addresses and MAC addresses.
- Detailed configuration settings.
- Firmware/software versions.
- Network topology diagrams.
- Specific configuration and policies applied to the devices.

Monitor and Updates – Continuously monitor the devices and configurations and keep them up-to-date. Detect any changes in the network and alert administrators to any inconsistencies.