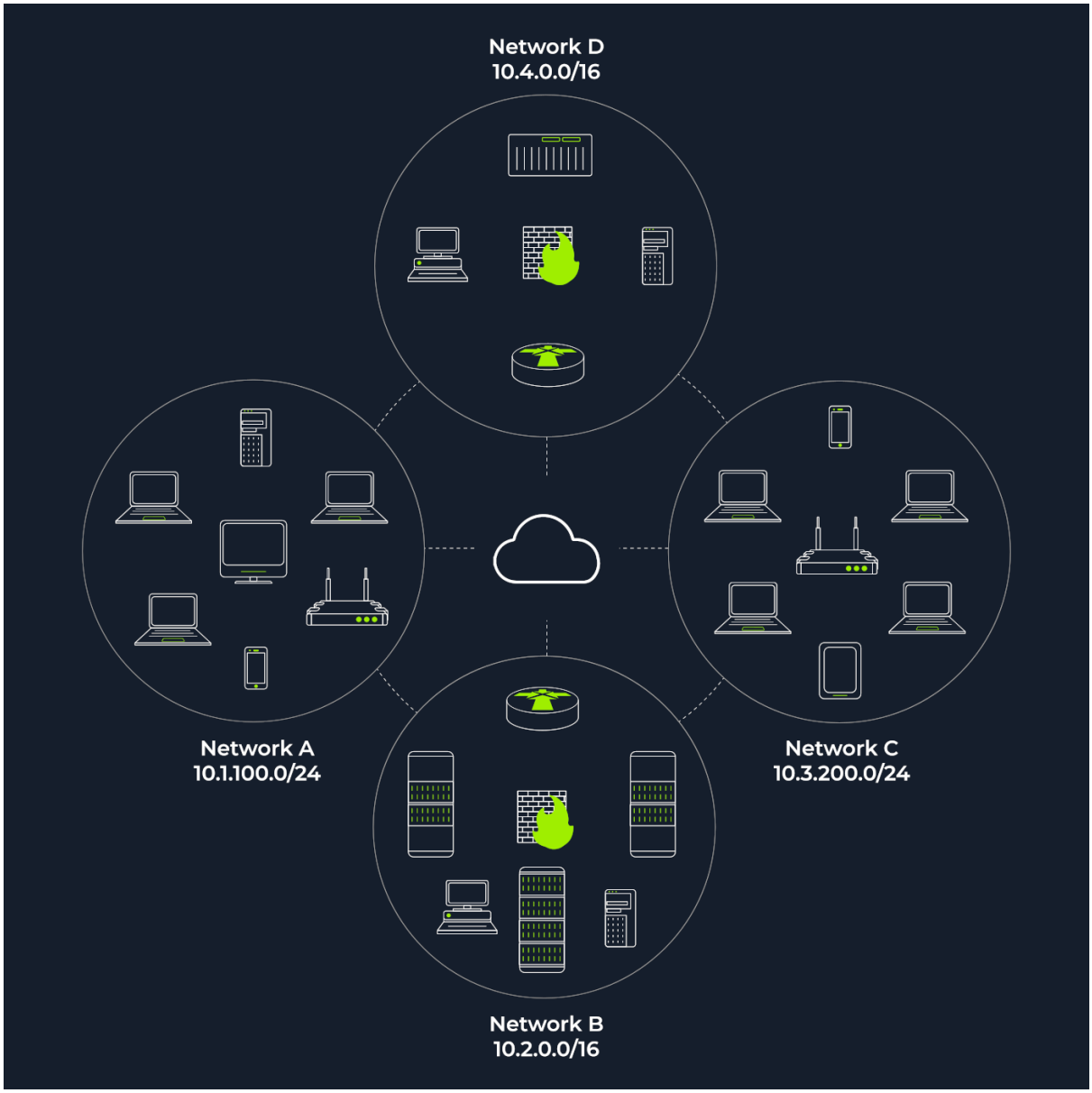
Nmap01 - Tryhackme

Introduction

- Nmap uses different approaches to discover live hosts. In particular they are-
  - **ARP Scan :** This scan uses ARP requests to discover live hosts
  - **ICMP Scan :** This scan uses ICMP requests to identify live hosts
  - **TCP/UDP ping Scan:** This scan sends packets to TCP ports and UDP ports to determine live hosts.

Subnetwork

- **Network Segment:** It is a group of computers connected using a shared medium. The medium can be the Ethernet switch or WiFi access point.
- **Subnetwork:** It is usually the equivalent of one or more network segments connected together and configured to use the same router. The network segment refers to a physical connection, while a subnetwork refers to a logical connection.



- The above figure has two types of subnets (subnets with /16 which means that the subnet mask can be written as 255.255.0.0 and subnets with /24 which means that the subnet mask can be written as 255.255.255.0)

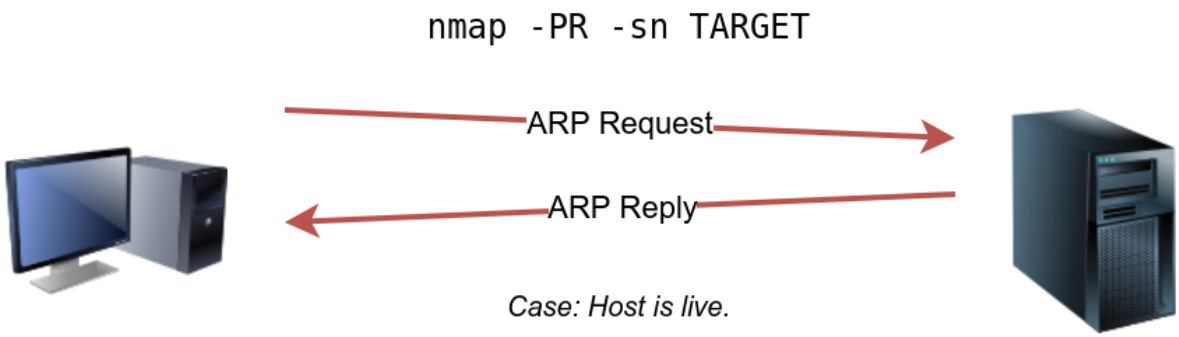
Enumerating Targets

- We can provide a file as a input for our list of targets to nmap, using the command - `nmap -iL list_of_hosts.txt`
- If we want to check the list of hosts that Nmap will scan, we can use - `nmap -sL TARGETS`

- Nmap attempts a reverse-DNS resolution on all the targets to obtain their names.
- For no reverse DNS resolution, we can add the flag `-n`

Nmap Host Discovery using ARP

- If a privileged user tries to scan targets on a local network (Ethernet) , Nmap uses ARP requests.
- If a privileged user tries to scan targets outside the local network, Nmap uses ICMP echo requests, TCP ACK (Acknowledge) to port 80, TCP SYN (Synchronize) to port 443, and ICMP timestamp request.
- If an unprivileged user tries to scan targets outside the local network, Nmap uses 3-way handshake method sending SYN packets to ports 80 and 443.
- Nmap by default uses a ping scan to find live hosts and then proceed with scanning live hosts only.
- If we want Nmap to discover only live hosts without port scanning then we can use - `nmap -sn targets`
- ARP scan is possible if the attacker and the target system, both are on the same subnet.
- To make Nmap perform only ARP scan without port-scanning, use - `nmap -PR -sn targets`
- Nmap sends ARP requests to all the target computers, and those online should send an ARP reply back.

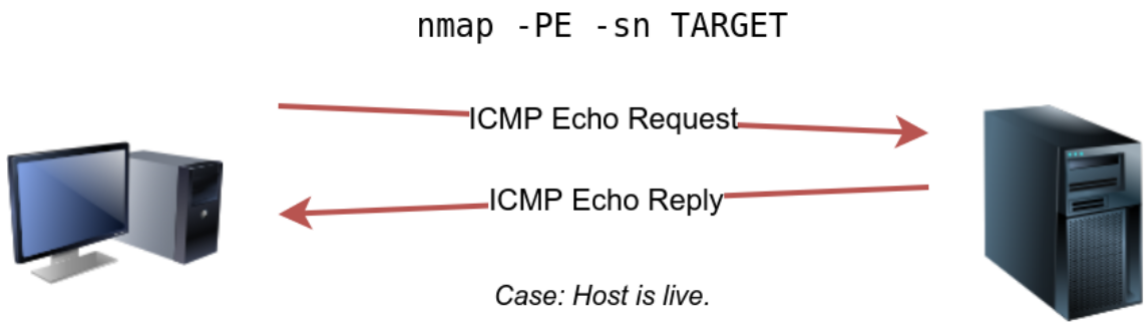


- `arp-scan` is a tool/scanner built around ARP queries. For more details - http://www.royhills.co.uk/wiki/index.php/Main_Page

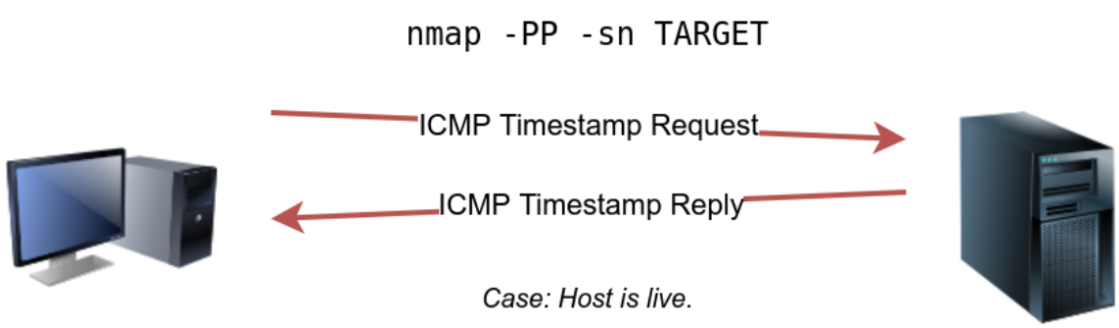
- `arp-scan --localnet` OR `arp-scan -l` commands send ARP queries to all valid IP addresses on our local network.
- We can specify the interface if we have more than one interface, using- `arp-scan -I eth0 -l`
- It can be installed using - `apt-get install arp-scan`

Nmap Host Discovery using ICMP

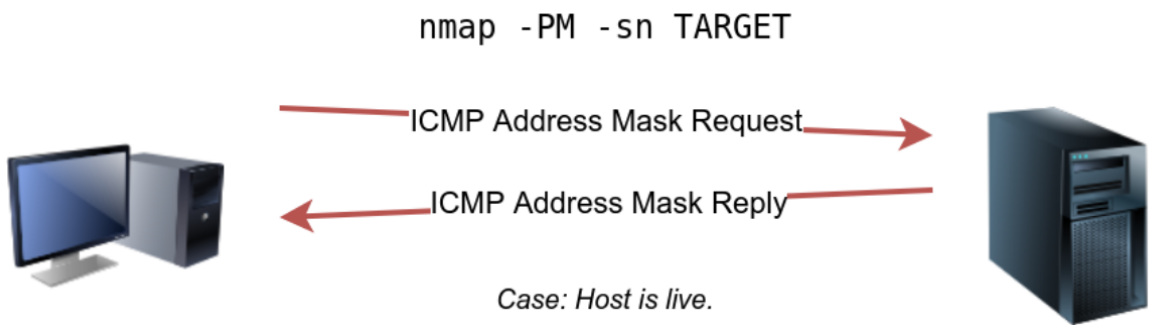
- ICMP has many types.
- ICMP ping uses Type 8 (Echo) and Type 0 (Echo Reply).
- An ARP query always precedes the ICMP request if our target is on the same subnet.
- To use ICMP echo request to discover live hosts - `nmap -PE targets`. We can add `-sn` to avoid port-scanning the live targets.



- Many firewalls block ICMP.
- If ICMP echo requests tend to be blocked, we can use ICMP timestamp request (ICMP type 13) and expect for a ICMP timestamp reply (ICMP type 14).
- It can be done using - `nmap -PP -sn target`



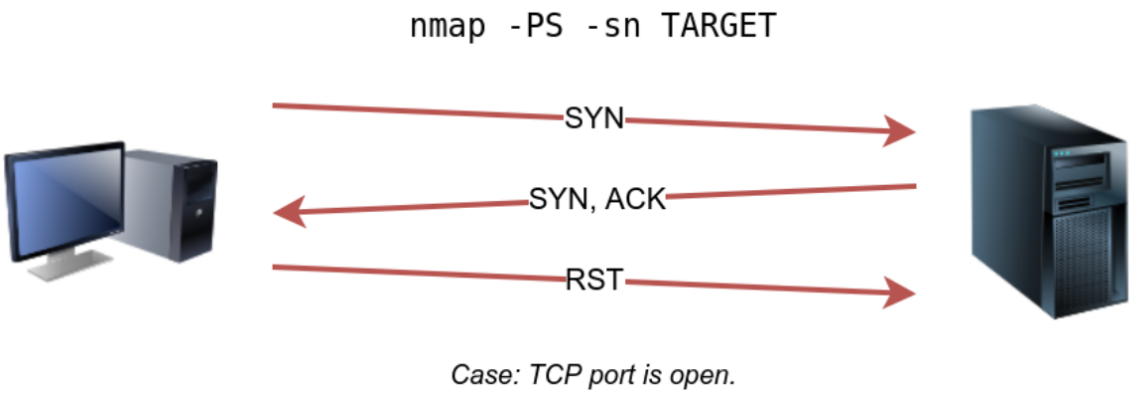
- Similarly we can use ICMP address mask requests (ICMP Type 17) and expect for ICMP address mask reply (ICMP Type 18). It can be done using the `-PM` flag.



Nmap Host Discovery using TCP and UDP

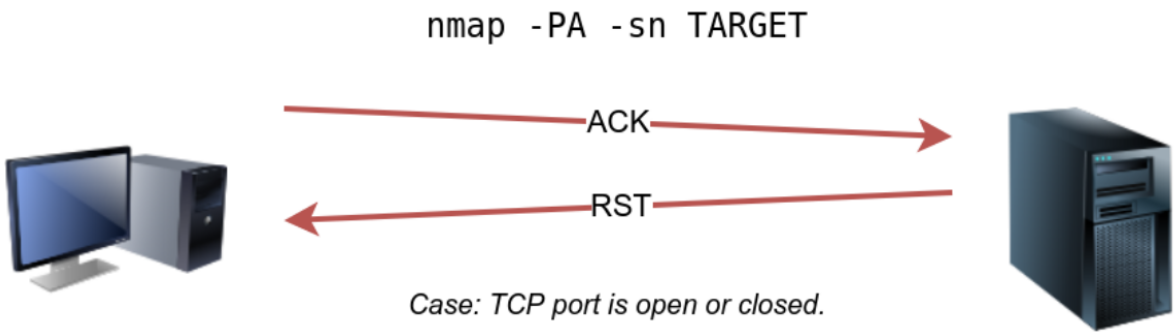
TCP SYN Ping

- We can send a packet with the SYN flag set to a TCP port (default 80).
- An open port should reply with a SYN/ACK.
- A closed port should reply with RST (reset).
- We only check whether we get any response to infer whether the host is up.
- To use Nmap TCP SYN ping - we can use the flag - `-PS` followed by port number, or range of port numbers
- Privileged users can send TCP SYN packets and don't need to complete the TCP 3-way handshake even if the port is open.
- Unprivileged users have to complete the 3-way handshake if the port is open.



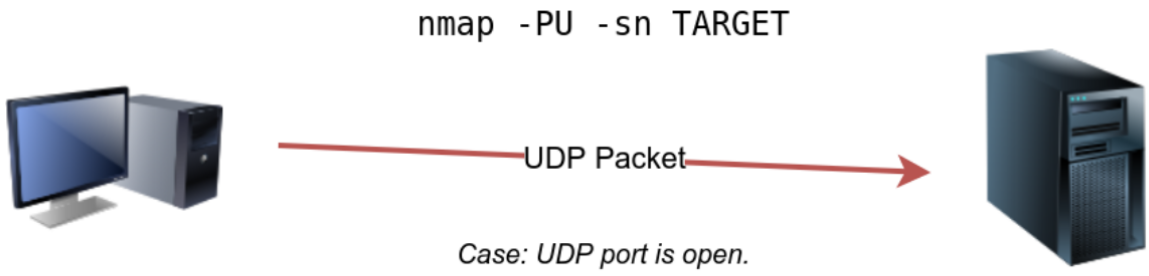
TCP ACK Ping

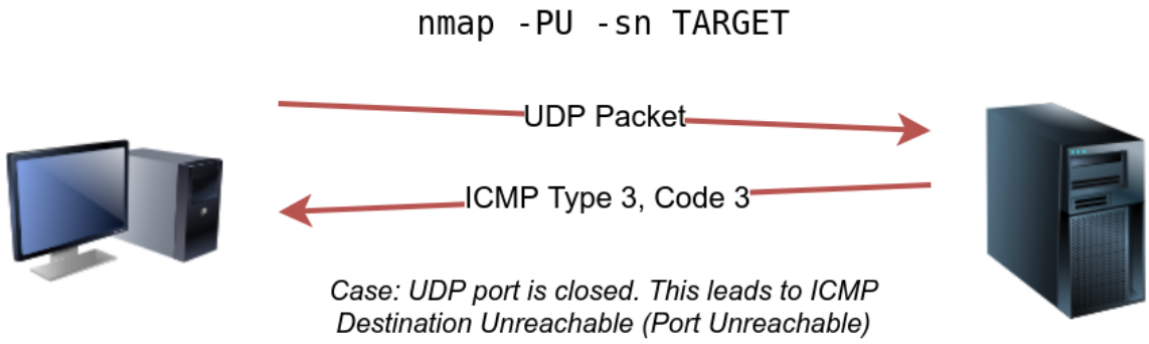
- This sends a packet with an ACK flag set.
- We need to run Nmap as a privileged user to be able to perform this.
- In case of unprivileged user, Nmap will attempt a 3-way handshake.
- By default, port 80 is used.
- To perform TCP ACK ping, we can use the flag - `-PA` followed by a port number, range, list, or a combination of them.
- If no port is specified, port 80 will be used.
- The expected response is used to detect if the target host is up.



UDP Ping

- We can use UDP to discover if the host is online.
- Sending a UDP packet to an open port is not expected to lead to any reply.
- If we send a UDP packet to a closed UDP port, we expect to get an ICMP port unreachable packet.
- That indicates that the target system is up.





- We use the flag- `-PU` for UDP ping.

Using Reverse-DNS Lookup

- Nmap by default looks for online hosts.
- We can use the flag - `-R` to query the DNS server even for offline hosts.
- If we want to use a specific DNS server, we can add `--dns-servers DNS_SERVER`.

Summary

Scan Type	Example Command
ARP Scan	`sudo nmap -PR -sn MACHINE_IP/24`
ICMP Echo Scan	`sudo nmap -PE -sn MACHINE_IP/24`
ICMP Timestamp Scan	`sudo nmap -PP -sn MACHINE_IP/24`
ICMP Address Mask Scan	`sudo nmap -PM -sn MACHINE_IP/24`
TCP SYN Ping Scan	`sudo nmap -PS22,80,443 -sn MACHINE_IP/30`
TCP ACK Ping Scan	`sudo nmap -PA22,80,443 -sn MACHINE_IP/30`
UDP Ping Scan	`sudo nmap -PU53,161,162 -sn MACHINE_IP/30`

Option	Purpose
`-n`	no DNS lookup
`-R`	reverse-DNS lookup for all hosts
`-sn`	host discovery only