# NMAP LIVE HOST DISCOVERY

## CHEAT SHEET



**Sources:**

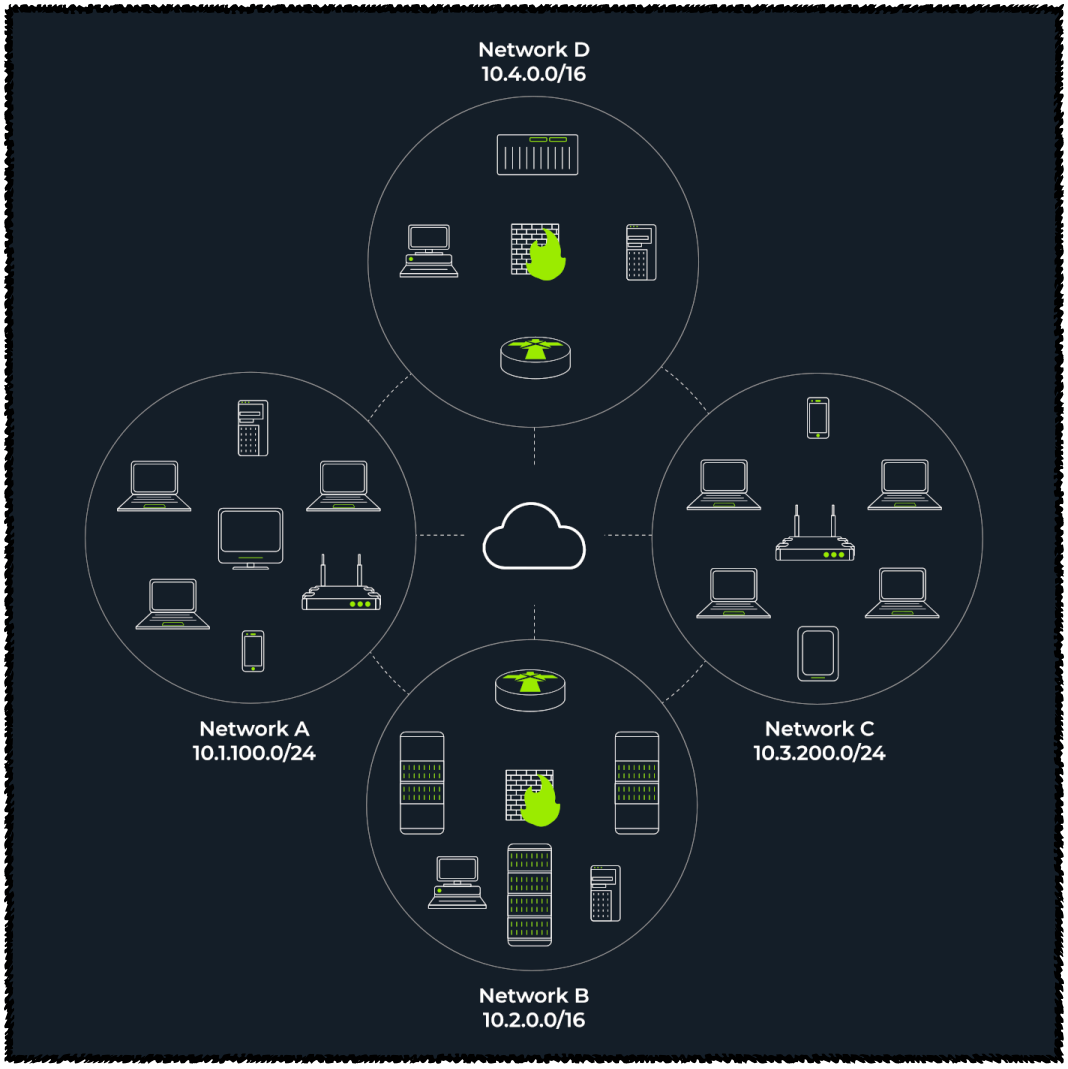
- *TryHackMe.com*
- *NMap.org*


**Author:**

***CyberxyzGator***

# SUBNETWORKS

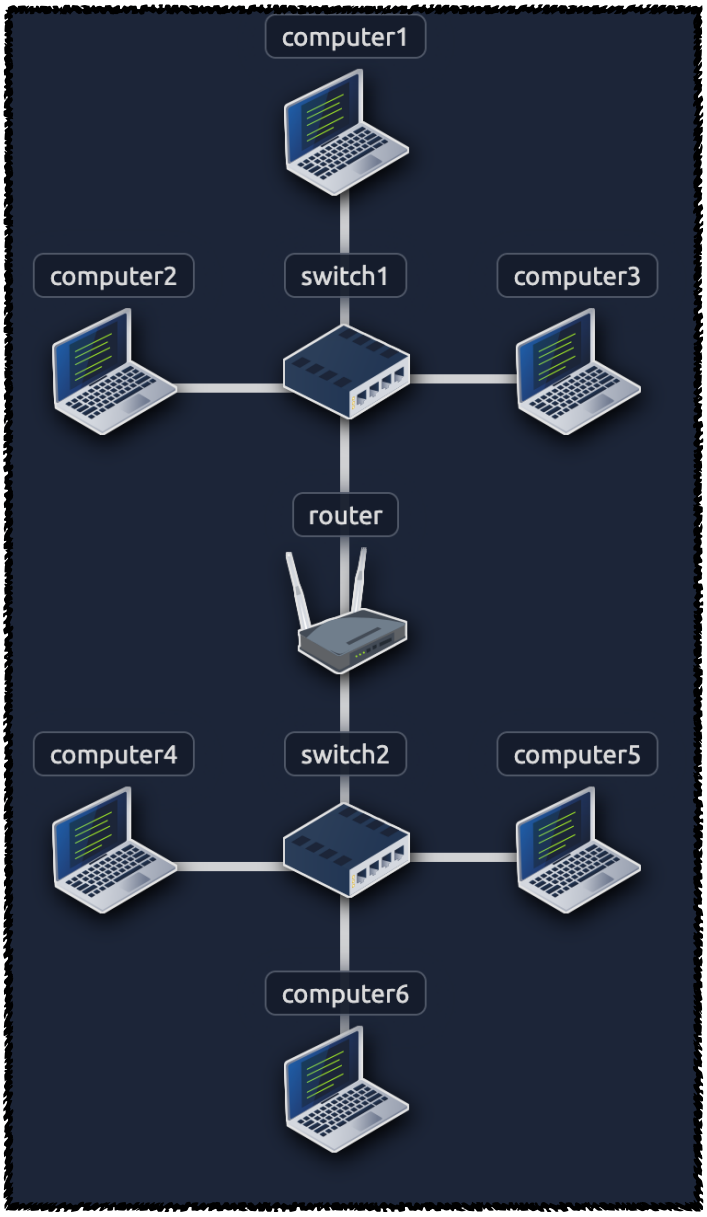
A. Subnetworks have segments. These segments are devices on the subnet.
B. Subnets have their own IP Range. Each device receives an IP from the DHCP.
C. Subnets with /16 means they can be written as 255.255.0.0
D. Subnets with /24 means they can be written as 255.255.255.0




Souce: https://tryhackme.com/room/nmap01

# SUBNETWORKS- CONTINUED

Example Network with Subnets.




Souce: https://tryhackme.com/room/nmap01

## Scan Types

| | |
|---|---|
| **A.** | **ARP (Address Resolution Protocol)** |
| | *Use ARP to discover the devices within a subnet.* |
| **B.** | **ICMP(Internet Control Message Protocol)** |
| | *Uses ICMP requests to identify live hosts.* |
| **C.** | **TCP / UDP (Transmission Control Protocol / User Datagram Protocol)** |
| | *This scan sends packets to TCP and UDP Ports to determine live hosts.* |

# ENUMERATING TARGETS

## NMAP Discovery Scans

| | |
|---|---|
| **A.** | **nmap -sT MACHINE_IP scanme.nmap.org example.com** |
| | *This will TCP  scan 3 IP addresses. Replace these with your targets.* |
| **B.** | **nmap -sn -PR MACHINE_IP** |
| | *This will do an ARP scan on the MACHIN_IP.* |
| **C.** | **nmap -sL MACHINE_IP/30** |
| | *This will list IP's up to .30 Octet that nmap will scan.* |
| **D.** | **nmap -sL -n 10.10.0-255.0-255** |
| | *This will list IP's to be scanned using aa range from 0-255 on the third octet and 0-255 on the fourth octet.* |
| **E.** | **sudo nmap -PR -sn MACHINE_IP** |
| | *This will enumerate the live hosts using an ARP scan.* |
| **F.** | **sudo nmap -PE -sn MACHINE_IP/24** |
| | *This scan will send ICMP echo packets to every IP address on the subnet. The response identifies live hosts.* |
| **G.** | **sudo nmap -PP -sn MACHINE_IP/24** |
| | *This scan will send ICMP timestamps requests to find live hosts.* |
| **H.** | **sudo nmap -PM -sn MACHINE_IP/24** |
| | *This scan uses address mask queries (ICMP Type 17) to check wether it gets an address mask reply (ICMP Type 18. Live Hosts are expected to reply to ICMP AMR's.* |

# TCP AND UDP SCANS

## NMAP TCP Scans

| | |
|---|---|
| **A.** | **sudo nmap -PS(Port# 80 Default) -sn MACHINE_IP/24** |
| | *This scan uses the TCP SYN (Synchronize) flag to set a TCP port, 80 by default and wait for a response. Open ports will reply with SYN/ACK (Acknowledge). while closed ports will reply with RST (Reset). Does NOT require SUDO to work.* |
| **B.** | **sudo nmap -PA(Port# 80 Default) -sn MACHINE_IP/24** |
| | *This scan sends a TCP ACK (Acknowledge) packet to the target, then wait for a RST (Reset) reply from the target indicating live hosts.* |

## NMAP UDP Scans

| | |
|---|---|
| **A.** | **sudo nmap -PU -sn MACHINE_IP/24** |
| | *This scan sends a UDP packet to an open UDP port on the target. If the port is open, we get no response, now if the port is closed the target sends an ICMP Type 3 response, indicating the port is closed, unreachable.* |

# ARP-SCAN DISCOVERY SCANS

## Running Arp-scan

| | |
|---|---|
| **A.** | **sudo arp-scan —localnet (-l)** |
| | *This will scan the local network for live hosts* |
| **B.** | **sudo arp-scan -I eth0** |
| | *This will scan all valid IP addresses on the eth0 interface.* |

# MASSCAN DISCOVERY SCANS

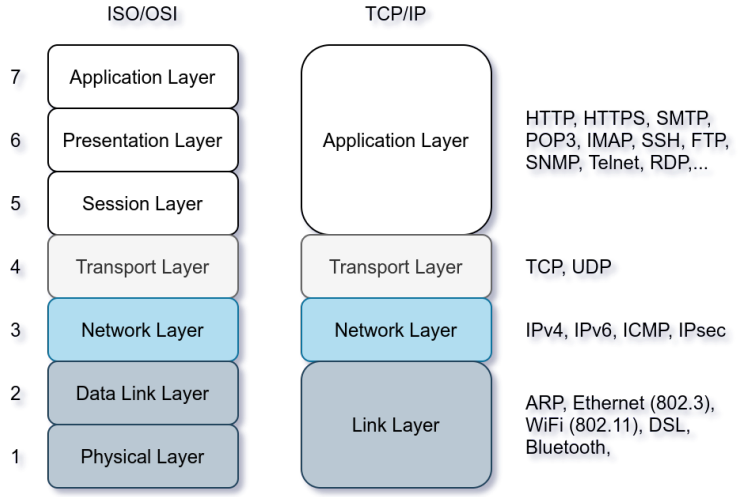
## Running Masscan

| | |
|---|---|
| **A.** | **masscan MACHINE_IP/24 -p(PORT #)** |
| | *This scan an aggressive rate of packets to discover live hosts.* |
| **B.** | **masscan MACHINE_IP/24 —top-ports (# of Ports)** |
| | *This scan will only scan the top # of Ports to identify live hosts.l* |

# SCAN LAYERS

## Layers

| | |
|---|---|
| **A.** | ARP (Link Layer) |
| **B.** | ICMP (Network Layer) |
| **C.** | TCP (Transport Layer) |
| **D.** | UDP (Transport Layer) |




Souce: https://tryhackme.com/room/nmap01

# REVERSE-DNS LOOKUP

## DNS-Lookup

| | |
|---|---|
| **A.** | **sudo nmap -PS -n MACHINE_IP/24** |
| | *This scan uses TCP SYN scan without querying the DNS Lookup.* |
| **B.** | **sudo nmap -PS -R MACHINE_IP/24** |
| | *This scan uses -R to use Reverse-DNS Lookup to identify hosts.* |
| **C.** | **sudo nmap -PS -R —dns-servers DNS_SERVER MACHINE_IP/24** |
| | *This scan uses —dns-servers to use a specific DNS Server to query.* |

# TOP 20 MOST COMMONLY OPEN TCP PORTS

| Port Number | Service Name | Description |
|---|---|---|
| 80 | HTTP | If you don't even know this service, you're reading the wrong book. This accounted for more than 14% of the open ports we discovered. |
| 23 | Telnet | Telnet lives on (particularly as an administration port on devices such as routers and smart switches) even though it is insecure (unencrypted). |
| 443 | HTTPS | SSL-encrypted web servers use this port by default. |
| 21 | FTP | FTP, like Telnet, is another insecure protocol which should die. |
| 22 | SSH | Secure Shell, an encrypted replacement for Telnet (and, in some cases, FTP). |
| 25 | SMTP | Simple Mail Transfer Protocol (also insecure). |
| 3389 | ms-term-server | Microsoft Terminal Services administration port. |
| 110 | POP3 | Post Office Protocol version 3 for email retrieval (insecure). |
| 445 | Microsoft-DS | For SMB communication over IP with MS Windows services (such as file/printer sharing). |
| 139 | NetBIOS-SSN | NetBIOS Session Service for communication with MS Windows services (such as file/printer sharing). |
| 143 | IMAP | Internet Message Access Protocol version 2. An insecure email retrieval protocol. |
| 53 | Domain | Domain Name System (DNS), an insecure system for conversion between host/domain names and IP addresses. |
| 135 | MSRPC | Another common port for MS Windows services. |
| 3306 | MySQL | For communication with MySQL databases. |
| 8080 | HTTP-Proxy | Commonly used for HTTP proxies or as an alternate port for normal web servers. |
| 1723 | PPTP | Point-to-point tunneling protocol (a method of implementing VPNs). |
| 111 | RPCBind | Maps SunRPC program numbers to their current TCP or UDP port numbers. |
| 995 | POP3S | POP3 with SSL added for security. |
| 993 | IMAPS | IMAPv2 with SSL added for security. |
| 5900 | VNC | A graphical desktop sharing system (insecure). |

# TOP 20 MOST COMMONLY OPEN UDP PORTS

| Port Number | Service Name | Description |
|---|---|---|
| **631** | **IPP** | Internet Printing Protocol. |
| **161** | **SNMP** | Simple Network Management Protocol. |
| **137** | **NETBIOS-NS** | One of many UDP ports for Windows services such as file and printer sharing. |
| **123** | **NTP** | Network Time Protocol. |
| **138** | **NETBIOS-DGM** | Another Windows service. |
| **1434** | **MS-SQL-DS** | Microsoft SQL Server. |
| **445** | **Microsoft-DS** | Another Windows Services port. |
| **135** | **MSRPC** | Yet Another Windows Services port. |
| **67** | **DHCPS** | Dynamic Host Configuration Protocol Server (gives out IP addresses to clients). |
| **53** | **Domain** | Domain Name System (DNS) server. |
| **139** | **NETBIOS-SSN** | Another Windows Services port. |
| **500** | **ISAKMP** | The Internet Security Association and Key Management Protocol for IPsec VPNs. |
| **68** | **DHCPC** | DHCP client port. |
| **520** | **Route** | Routing Information Protocol (RIP). |
| **1900** | **UPNP** | Microsoft Simple Service Discovery Protocol. |
| **4500** | **nat-t-ike** | For negotiating Network Address Translation traversal while initiating IPsec connections. |
| **514** | **Syslog** | The standard UNIX log daemon. |
| **49152** | **Varies** | The first of the IANA-specified dynamic/private ports. |
| **162** | **SNMPTrap** | Simple Network Management Protocol trap port. |
| **69** | **TFTP** | Trivial File Transfer Protocol. |