Task 1

What is Network Scanning?

- Technique for identifying "devices"
- These devices have IPs & MAC addresses
- IP addresses have TCP/UDP ports (1-65,535)
- Ports are open, closed, filtered or unfiltered
- Ports run OS & Services

-Common Ports

Port	Protocol/Service	Full Form
21	FTP	File Transfer Protocol
22	SSH	Secure Shell
23	Telnet	Telecommunication Network
25	SMTP	Simple Mail Transfer Protocol
53	DNS	Domain Name System
80	HTTP	HyperText Transfer Protocol
88	Kerberos	Kerberos Authentication Protocol
110	POP3	Post Office Protocol version 3
135	RPC	Remote Procedure Call
139	SMB (old)	Server Message Block (legacy)
143	IMAP4	Internet Message Access Protocol v4
161	SNMP	Simple Network Management Protocol
162	SNMP traps	SNMP Trap Protocol
389	LDAP	Lightweight Directory Access Protocol
443	HTTPS	HyperText Transfer Protocol Secure
445	SMB	Server Message Block
111	NIX	UNIX RPC Portmapper
3389	RDP	Remote Desktop Protocol

What is Nmap?

- Free, Powerful Network Discovery tool
- IP/Host/Port scanning
- Services discovery
- OS detection
- Version detection
- Scriptable interaction with targets (NSE)
- Info on targets, including reverse DNS names, device types, and MAC addresses
- Nmap.org

Who Uses Nmap?

- Pen-testers / Ethical Hackers
- Reconnaissance & Info Gathering
- IT Personnel
- Inventory, network topology
- Adversary entities

Syntax

nmap [Scan Types] [Options] <target>

Example:

nmap -sS -p 22 172.16.148.203

Option	Description
-h	Show Nmap help
-sP / -sn	Ping scan (discover live hosts only, no port scan)
-sS	TCP SYN scan (half-open scan)
-sT	TCP connect scan (full open scan)
-Pn	Treat all hosts as online (skip ping)
-sV	Detect service version information
-sU	UDP scan
-sL	List targets only (no scanning)
-sA	TCP ACK scan (used to test firewall rules)
-r	Don't randomize port order
--top-ports <n>	Scan top <n> most common ports
-6	Enable IPv6 scanning
-iL <file>	Input targets from a file
-oA <basename>	Output in all formats (normal, XML, grepable)
-oX <file>	Output in XML format
-oN <file>	Output in normal format
--exclude <hosts>	Exclude given hosts from the scan
-n	Don't resolve DNS names
-F	Fast scan (scans fewer ports for speed)
-v, -vv, -vvv	Increase verbosity level
--version-intensity <0-9>	Set intensity of version detection (0 = light, 9 = aggressive)
-A	Aggressive scan: OS detection, version, script scan, traceroute
-O	OS detection
-sC	Run default scripts
-PR	ARP ping (for local networks)
-PS <port list>	TCP SYN ping to specified ports