**1. Basic Command Structure**

* **sudo**: Ensures root privileges for advanced scanning techniques (required for some scan types like SYN scans).
* **nmap**: The base command for the Nmap tool.
* **-v**: Verbose mode. Provides detailed output of the scanning process.

**2. Command Options Explained**

**Scan Types**

* **-sS**: SYN scan (default). A stealthy scan that sends TCP SYN packets to identify open ports without completing the three-way handshake.
* **-sT**: TCP Connect scan. A full three-way handshake is established. Used when SYN scan isn’t possible.
* **-sU**: UDP scan. Probes open UDP ports by sending UDP packets.
* **-sA**: ACK scan. Used to map firewall rules, not to detect open ports.
* **-sW**: Window scan. Similar to ACK scan but checks TCP window size to detect open ports.
* **-sM**: Maimon scan. Exploits a TCP flaw to identify open ports.

**Host Discovery**

* **-sL**: List scan. Lists targets without sending any packets.
* **-sn**: No port scan. Performs host discovery only.
* **-Pn**: No host discovery. Assumes all hosts are online and directly scans their ports.
* **-PS**: TCP SYN ping on specified ports (default port is 80).
* **-PA**: TCP ACK ping on specified ports (default port is 80).
* **-PU**: UDP ping on specified ports (default port is 40125).
* **-PR**: ARP ping for local networks.
* **-n**: Disables DNS resolution for faster scans.

**Service and Version Detection**

* **-O**: Enables OS detection to identify the operating system of the target.
* **-sV**: Version detection. Identifies software versions running on open ports.
* **-A**: Aggressive mode. Combines OS detection, version detection, script scanning, and traceroute.

**Scan Speed**

* **-T0**: Paranoid mode. Very slow; designed to avoid Intrusion Detection Systems (IDS).
* **-T1**: Sneaky mode. Slower scan to reduce the chance of detection.
* **-T2**: Polite mode. Limits bandwidth usage and minimizes impact on target.
* **-T3**: Normal mode. Default speed for scans.
* **-T4**: Aggressive mode. Faster scan for reliable networks.
* **-T5**: Insane mode. Extremely fast; suitable only for very reliable networks.

**Nmap Scripting Engine (NSE) Scripts**

* **-sC**: Runs default scripts. Useful for general discovery and safe scanning.
* **--script=vuln**: Runs vulnerability scripts to identify known vulnerabilities.
* **--script=safe**: Runs only non-intrusive and safe scripts.
* **--script=intrusive**: Runs intrusive scripts that may affect the target.

**3. Putting It Together**

The script dynamically builds the Nmap command based on user inputs. Here’s how the process works:

1. The user selects scan options step by step (e.g., type of scan, host discovery method).
2. The script appends the appropriate flags to the base command (nmap).
3. The user provides the target IP address or range (e.g., 192.168.1.1).
4. The final Nmap command is constructed and executed in verbose mode (-v).
5. The output is saved to a file (nmap\_report.txt).

**4. Example Commands Generated by the Script**

Here are examples of Nmap commands that might be generated:

1. **Basic TCP SYN Scan**:

bash

Copy code

sudo nmap -sS -Pn -T3 -sC -v 192.168.1.1

* + Performs a SYN scan without host discovery, using normal speed, default scripts, and verbose mode.

1. **Aggressive Scan with OS and Version Detection**:

bash

Copy code

sudo nmap -sS -A -T4 -v 192.168.1.1

* + Performs a SYN scan with aggressive mode, enabling OS and version detection, and script scanning.

1. **UDP Vulnerability Scan**:

bash

Copy code

sudo nmap -sU --script=vuln -v 192.168.1.1

* + Scans for open UDP ports and runs vulnerability scripts.

**Tips for Your Exam**

1. **Memorize Key Flags**:
   * Scan types: -sS, -sT, -sU, -sA.
   * Host discovery: -sL, -sn, -Pn.
   * Service/version detection: -sV, -O, -A.
   * NSE scripts: -sC, --script=vuln.
   * Scan speed: -T0 to -T5.
2. **Understand Use Cases**:
   * Use SYN scans (-sS) for stealth.
   * Use version detection (-sV) to identify running services.
   * Use -A for comprehensive scans.
3. **Write Complete Commands**:
   * Practice writing full commands combining multiple options, like:

sudo nmap -sS -Pn -sV -T4 -v 192.168.1.1