1. Scanning & Enumeration

1.1 Definition

- **Scanning**: The process of actively probing target systems to identify live hosts, open ports, services, versions, and potential vulnerabilities.
- **Enumeration:** The process of extracting more detailed and specific information about discovered services such as usernames, shares, banners, SNMP data, and system details.

1.2 Difference between Scanning and Enumeration

• Scanning = 'What is available?' (Discovery phase) • Enumeration = 'What can we extract?' (Information gathering phase)

1.3 Why Important?

- Helps build a clear attack surface map.
- Identifies possible entry points and weaknesses.
- Supports vulnerability prioritization.
- Provides foundation for penetration testing and exploitation.

1.4 Types of Scans (Nmap Examples)

- TCP Connect (-sT) → Performs a full 3-way handshake, reliable but very noisy, easily detected.
  Example: nmap -sT 192.168.1.10
- SYN Scan (-sS) → Performs a half-open scan, stealthier and faster.
  Example: nmap -sS 192.168.1.10

- UDP Scan (-sU) → Checks for UDP-based services like DNS, SNMP, DHCP. Slower due to no handshake.
  Example: nmap -sU 192.168.1.10

- Service Version (-sV) → Determines version of running services for vulnerability matching.
  Example: nmap -sV 192.168.1.10

- OS Detection (-O) → Detects target operating system via TCP/IP stack fingerprinting.
  Example: nmap -O 192.168.1.10

- Aggressive Scan (-A) → Combines OS detection, version detection, script scanning, and traceroute.
  Example: nmap -A 192.168.1.10 •

Full Port Scan (-p-) → Scans all 65535 ports instead of default 1000.
Example: nmap -p- 192.168.1.10

1.5 Enumeration Techniques

- NetBIOS Enumeration (nbtscan, nmap --script nbstat) → Reveals shares, sessions, logged-in users.
- SNMP Enumeration (snmpwalk, snmpenum) → Reveals system details, routing tables, software versions.
- LDAP Enumeration (ldapsearch, Nmap NSE) → Extracts users, groups, policies.

• SMTP Enumeration (VRFY, EXPN commands, smtp-user-enum tool) → Identifies valid users.
• DNS Enumeration (dig, nslookup, dnsenum) → Zone transfers, subdomain discovery.
• SMB Enumeration (enum4linux, rpcclient) → Extracts users, groups, shares, policies.

1.6 Vulnerability Scanning Tools

(a) Nmap

• Powerful port scanner with scripting engine (NSE).
• Useful for OS detection, version detection, and script-based vulnerability checks.

(b) OpenVAS

• Open-source vulnerability scanner.
• Uses a database of CVEs and CVSS for risk scoring.
• Workflow: Start OpenVAS → Configure target → Launch scan → Review/export results.

(c) Nikto

• Web server vulnerability scanner.
• Detects outdated software, insecure HTTP headers, misconfigured files, and dangerous scripts.
• Example: nikto -h http://192.168.1.10

(d) Nessus

• Widely used vulnerability scanner (commercial + free version).
• Provides detailed remediation guidance.
• Example: Checks for missing patches, weak SSL/TLS, misconfigurations.

1.7 Outputs & Reporting

• Always document scan results properly.
• Nmap output options: -oN → Normal text
-oX → XML
-oG → Greppable
-oA → All formats

Example: nmap -sV -oA results 192.168.1.10 1.8 Example Case Study Target: Metasploitable 2 (IP: 192.168.1.100)
• Step 1: Nmap Scan → Found open ports (21/FTP, 80/HTTP, 3306/MySQL).
• Step 2: Enumeration → - FTP: Anonymous login allowed.
- HTTP: Apache outdated, potential CVE found. - MySQL: Weak credentials (root:root).
• Step 3: Vulnerability Scanning → Verified issues with OpenVAS and Nikto.
• Step 4: Reporting → Documented CVEs, risk levels, and mitigation.

1.9 Key Notes

• Scanning = Broad discovery; Enumeration = Deep details.
• Always validate scan results to reduce false positives.
• IDS/IPS may detect scans → Use stealth techniques where applicable