VULNERABILITY SCANNING ON NETWORK

MODULE 4 — VULNERABILITY SCANNING (FULL ADVANCED MODULE)

Vulnerability scanning is the process of **identifying security weaknesses in networks, systems, and applications** using automated tools and manual validation techniques.

This phase comes **after Enumeration** and **before Exploitation**.

---

1. What is Vulnerability Scanning? (Professional Explanation)

Vulnerability scanning is an **automated process** where specialized tools analyze a target's:

- Services
- Configurations
- Software versions
- Patch levels
- Misconfigurations
- Known CVEs
- Weak protocols
- Open ports

The goal is to identify potential weaknesses **before exploiting them**.

It's a mix of **automated scanning + manual verification**.

---

2. Why is Vulnerability Scanning Important?

Reason	Explanation
Attack surface mapping	Identifies exploitable entry points
CVE mapping	Matches detected versions with vulnerabilities
Prioritization	Helps classify risks: Critical/High/Medium/Low
Compliance	PCI-DSS, HIPAA, ISO 27001 require vulnerability assessments
Mitigation planning	Helps sysadmins patch and secure systems

3. Types of Vulnerability Scanning

✔️ 1. Network Vulnerability Scanning

Find weaknesses in:

- Open ports
- Services
- OS versions
- Weak protocols

Tools: **Nessus, OpenVAS, Nmap NSE, Qualys**

✔️ 2. Web Application Vulnerability Scanning

Detect issues in:

- Input validation
- SQLi
- XSS
- Auth bypass
- Insecure cookies

Tools: **Nikto, BurpSuite Scanner, OWASP ZAP**

✔️ 3. Host-Based Vulnerability Scanning

Detect issues inside systems:

- Missing patches
- Weak passwords
- Misconfigured services

Tools: **Lynis, Nessus Agents**

✔ 4. Credentialed vs Non-Credentialed Scanning

Type	Meaning	Accuracy
Credentialed	Scanner logs in with username/password	High accuracy
Non-credentialed	Scanner scans from outside only	Medium accuracy

Professional pentesters use **both**.

---

4. Vulnerability Scanning Tools (FULL ADVANCED + COMMANDS + INTERNAL WORKING)

---

1. NESSUS (Professional Grade Vulnerability Scanner)

Nessus is the industry-standard scanner used by:

- Cybersecurity companies
- SOC teams
- Government agencies
- Professional pentesters

Uses **plugin-based architecture**, where each plugin maps to a **CVE**, **CWE**, or **vulnerability check**.

✔ How Nessus Works (Internal Breakdown)

1. Performs port scan

2. Identifies service versions
3. Matches versions with Nessus plugins
4. Performs exploit-style tests (safe checks)
5. Generates severity score using **CVSS**
6. Provides remediation steps

✔️ Installing Nessus (Linux)

```
sudo dpkg -i Nessus-10.6.0-Ubuntu-amd64.deb
sudo systemctl start nessusd.service
```

Access at:

```
https://localhost:8834
```

✔️ Running a Basic Scan (GUI)

1. New Scan → Basic Network Scan
2. Enter Target IP
3. Save → Launch

✔️ Running Advanced Scan

Choose:

➡️ **Advanced Scan → Discovery → Port Scanning → Service Detection → OS Detection → Vulnerability Checks**

---

2. OPENVAS (Greenbone) — Open Source Enterprise Vulnerability Scanner

OpenVAS is a free alternative to Nessus.

✔️ How OpenVAS Works

- Uses the **Greenbone Vulnerability Feed (GVF)**
- Performs full port scan
- Identifies vulnerabilities using NVTs (Network Vulnerability Tests)
- Generates risk factor scores

✔️ Install on Kali Linux

```
sudo apt update
sudo apt install openvas
sudo gvm-setup
sudo gvm-start
```

Access:

```
https://127.0.0.1:9392
```

---

3. NMAP NSE (Nmap Scripting Engine)

Nmap's scripting engine can detect:

- CVEs
- Weak passwords
- Misconfigurations
- Known vulnerabilities

✔️ Run All Vulnerability Scripts

```
nmap --script vuln <target>
```

✔️ Run Specific Scripts

CVE detection:

```
nmap --script=cve <target>
```

HTTP vulnerabilities:

```
nmap --script http-vuln* <target>
```

SMB vulnerabilities:

```
nmap --script smb-vuln* <target>
```

---

4. NIKTO — Web Server Vulnerability Scanner

Nikto checks for:

- Outdated server software
- Dangerous files
- Misconfigurations
- Open directories
- Insecure default files

✔️ Basic Scan:

```
nikto -h http://target.com
```

✔️ SSL Scan:

```
nikto -ssl -h https://target.com
```

✔️ Scan with plugins:

```
nikto -Plugins apache -h http://target.com
```

---

5. BURP SUITE SCANNER (Web Vulnerability Scanner)

Burp Suite Professional offers:

- Active scanning
- Passive scanning
- Automatic SQLi/XSS detection
- CSP evaluation

✔️ Steps

1. Intercept traffic
2. Send to Scanner
3. Analyze results
4. Validate vulnerabilities

---

5. Vulnerability Scanning Workflow (Real Professional Flow)

STEP 1 — Discover Hosts

```
nmap -sn 10.10.0.0/24
```

STEP 2 — Identify Open Ports

```
nmap -sS -p- 10.10.0.5
```

STEP 3 — Service Version Detection

```
nmap -sV 10.10.0.5
```

STEP 4 — Run NSE Vulnerability Scripts

```
nmap --script vuln 10.10.0.5
```

STEP 5 — Run Nessus / OpenVAS Scan

(Through GUI)

STEP 6 — Manual Validation

Using:

- Netcat
- Curl
- Telnet
- Browser
- Exploit-DB
- Searchsploit

STEP 7 — Prioritization (CVSS Scoring)

Critical 9.0–10

High 7.0–8.9

Medium 4.0–6.9

Low <4

STEP 8 — Document Findings

6. Manual Validation Commands (Very Important for Students)

✔️ Check HTTP headers

```
curl -I http://target.com
```

✔️ Check SSL vulnerabilities

```
openssl s_client -connect target.com:443
```

✔️ Check SMB vulnerability manually

```
smbclient -L //10.10.0.5 -N
```

✔️ Banner grabbing with Netcat

```
nc -nv 10.10.0.5 80
```

7. What Goes in a Professional Report

✔️ 1. Summary

- Target
- Scope
- Date
- Tools used

✔️ 2. Detailed Vulnerability Findings

Field	Explanation
Vulnerability Name	e.g., SMBv1 Enabled
Severity	Critical/High/Medium/Low
CVE/CWE	CVE-2017-0144
Description	What the issue means
Affected Hosts	10.10.0.5
Proof of Concept	Screenshot, command output
Impact	Data leak, RCE, etc.
Recommendation	Patch, firewall rule, disable SMBv1

✔️ 3. Attach Logs

- Nmap output
- Nessus report
- Screenshots

---

8. Real Example Finding (Professional)

Title:

SMBv1 Protocol Enabled (Critical)

Vulnerability ID:

- CVE-2017-0144 (EternalBlue)

Affected Host:

10.10.0.5

Proof of Concept:

```
nmap --script smb-vuln-ms17-010 10.10.0.5
```

Impact:

Full remote code execution possible.

Recommendation:

- Disable SMBv1
- Apply MS17-010 patches
