AIM 1: NMAP (Network Mapper)

AIM

To perform network scanning using Nmap for host discovery, port scanning, service detection, OS detection, and vulnerability assessment.

TOOL USED

Tool: Nmap (Network Mapper)
Operating System: Kali Linux
Target: scanme.nmap.org

COMMANDS USED

Step	Command	Purpose
1	nmap -sn scanme.nmap.org	Host discovery
2	nmap -p 1-1000 scanme.nmap.org	Port scanning
3	nmap -sV scanme.nmap.org	Service & version detection
4	nmap -O scanme.nmap.org	OS detection
5	nmap -sC scanme.nmap.org	Default script scan
6	nmap -sU --top-ports 20 scanme.nmap.org	UDP scan
7	nmap -sS -T2 -f scanme.nmap.org	Stealth scan
8	nmap -sA scanme.nmap.org	Firewall detection
9	nmap -A -T4 -oN nmap_report.txt scanme.nmap.org	Full scan with report

PROOF OF CONCEPT (POC)

Scan Type	Finding
Host Discovery	Host is UP
Open Ports	22, 80, 443
Services	Apache, SSH
OS	Linux

Scan Type	**Finding**
UDP Ports	DNS (53)
Firewall	Filtered ports detected

(Fill actual results from your screenshots.)

IMPACT

1. Open ports expose services to attackers.
2. Outdated services may contain vulnerabilities.
3. OS detection helps attackers plan targeted attacks.
4. Lack of firewall increases exposure.

PREVENTION

1. Close unnecessary ports.
2. Keep services updated.
3. Enable firewall and IDS/IPS.
4. Disable unnecessary ICMP responses.

CONCLUSION

Nmap successfully identified open ports, services, and OS information. Proper hardening is required to reduce attack surface.

AIM 2: WIRESHARK (Packet Analysis)

AIM

To capture and analyze network packets using Wireshark and identify cleartext credentials.

TOOL USED

Tool: Wireshark
Operating System: Kali Linux

TASKS PERFORMED

1. Captured ICMP packets (ping traffic)

2. Captured HTTPS traffic (TLS encrypted)
3. Captured DNS queries
4. Observed TCP 3-way handshake
5. Captured HTTP credentials
6. Saved capture file (.pcapng)

COMMANDS USED

Task	Command
Ping	ping google.com -c 5
DNS	nslookup google.com
TCP Handshake	curl http://testphp.vulnweb.com

PROOF OF CONCEPT (POC)

Filter Used	Observation
icmp	Echo Request & Reply
tcp.port == 443	TLS encrypted packets
dns	DNS query & response
tcp.flags.syn == 1	SYN, SYN-ACK, ACK
http.request.method == "POST"	Credentials captured

IMPACT

1. HTTP transmits passwords in plaintext.
2. Attackers on the same network can steal credentials.
3. Session hijacking is possible.

PREVENTION

1. Enforce HTTPS.
2. Enable HSTS.
3. Use VPN.

4. Enable WPA3 on WiFi.
5. Implement MFA.

CONCLUSION

Wireshark demonstrated that HTTP is insecure. HTTPS must be enforced.

AIM 3: JOHN THE RIPPER (Password Cracking)

AIM

To crack password hashes using John the Ripper and identify hash algorithms.

TOOL USED

Tool: John the Ripper
Wordlist: rockyou.txt
OS: Kali Linux

HASH IDENTIFICATION

Hash Length	Algorithm
40 characters	SHA-1
96 characters	SHA-384

COMMANDS USED

```
echo "" > hash.txt
john --format=raw-sha1 --wordlist=/usr/share/wordlists/rockyou.txt hash.txt
john --show hash.txt
```

PROOF OF CONCEPT

Hash	Algorithm	Cracked Password
Hash1	SHA-1	(from output)
Hash2	SHA-1	(from output)
Hash3	SHA-384	(from output)

IMPACT

1. Weak passwords can be cracked quickly.

2. Password reuse leads to multiple account compromise.

PREVENTION

1. Use bcrypt or Argon2.
2. Add salt to hashes.
3. Enforce strong passwords.
4. Enable MFA.

CONCLUSION

Weak passwords were cracked successfully. Strong hashing and MFA are required.

AIM 4: WHOIS (Domain Lookup)

AIM

To retrieve domain registration details using WHOIS.

TOOL USED

Tool: WHOIS
Target: google.com

COMMANDS USED

```
whois google.com
whois google.com | grep -i registrar
whois google.com | grep -i date
```

PROOF OF CONCEPT

Category	Value
Registrar	MarkMonitor Inc.
Created	1997-09-15
Organization	Google LLC
Nameservers	ns1.google.com

IMPACT

WHOIS reveals domain ownership and infrastructure details.

PREVENTION

1. Enable WHOIS privacy.
2. Enable domain lock.
3. Use 2FA at registrar.

CONCLUSION

WHOIS exposes domain information which attackers can use.

AIM 5: DIG (DNS Query Tool)

AIM

To retrieve DNS records using DIG.

COMMANDS USED

```
dig google.com A
dig google.com MX
dig google.com NS
dig google.com TXT
dig google.com +trace
```

POC

Record	**Result**
A	IP Address
MX	Mail server
NS	Name servers
TXT	SPF record

IMPACT

DNS records reveal infrastructure details.

PREVENTION

1. Block zone transfers.
2. Implement DNSSEC.

3. Configure SPF/DKIM/DMARC.

CONCLUSION

DNS information must be secured to prevent reconnaissance.

AIM 6: THEHARVESTER (OSINT Gathering)

AIM

To gather emails and subdomains using TheHarvester.

COMMAND

```
theHarvester -d example.com -l 500 -b all
```

POC

Data Type	Result
Emails	12
Subdomains	15

IMPACT

Exposed emails and subdomains increase attack surface.

PREVENTION

1. Remove unnecessary public emails.
2. Delete unused subdomains.
3. Monitor OSINT exposure.

CONCLUSION

Public information can be used for reconnaissance.

AIM 7: SUBLIST3R (Subdomain Enumeration)

AIM

To enumerate subdomains using Sublist3r.

COMMAND

```
sublist3r -d nmap.org -e google,bing -p 80,443 -t 50 -v
```

POC

Subdomain	Open Ports
www.nmap.org	80, 443

IMPACT

Hidden subdomains increase attack vectors.

PREVENTION

Audit and remove unused subdomains.

CONCLUSION

Subdomain enumeration increases attack surface.

AIM 8: SHODAN (Internet Device Search)

AIM

To identify exposed devices using Shodan.

TOOL USED

Website: https://www.shodan.io

SEARCHES PERFORMED

```
hostname:nmap.org
webcam country:IN
port:22
vuln:CVE-2021-44228
```

IMPACT

1. Exposed services visible globally.
2. Vulnerable servers easily found.

PREVENTION

1. Close unused ports.
2. Patch systems.

3. Change default credentials.

CONCLUSION

Shodan enables passive reconnaissance of internet-connected devices.

AIM 9: DNSENUM (DNS Enumeration)

AIM

To gather complete DNS information using Dnsenum.

COMMAND

```
dnsenum --enum nmap.org
```

POC

Record	**Value**
A	45.33.32.156
NS	ns1.linode.com
MX	mail.nmap.org

IMPACT

Zone transfer leaks full DNS database.

PREVENTION

1. Block zone transfers.
2. Implement DNSSEC.

CONCLUSION

Dnsenum reveals DNS infrastructure which must be secured.