NATIONAL UNIVERSITY OF SCIENCE AND TECHNOLOGY

DEPARTMENT OF COMPUTER SCIENCE

INFORMATION SECURITY LAB

NAME	Ayesha Imran
Class	CS-A
Lab	09
Course	Information Security
Date	24-November-25
Submitted To	Lec. Attiya Ashraf

LAB TASKS

Getting Started with NMAP:

Open the Terminal and type: nmap

```
ayesha-imran@ayesha-imran:~/Desktop$ nmap
Nmap 7.94SVN ( https://nmap.org )
Usage: nmap [Scan Type(s)] [Options] {target specification}
TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
  -iL <inputfilename>: Input from list of hosts/networks
  -iR <num hosts>: Choose random targets
  --exclude <host1[,host2][,host3],...>: Exclude hosts/networks
  --excludefile <exclude_file>: Exclude list from file
HOST DISCOVERY:
  -sL: List Scan - simply list targets to scan
  -sn: Ping Scan - disable port scan
  -Pn: Treat all hosts as online -- skip host discovery
  -PS/PA/PU/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given ports
  -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
  -PO[protocol list]: IP Protocol Ping
  -n/-R: Never do DNS resolution/Always resolve [default: sometimes]
  --dns-servers <serv1[,serv2],...>: Specify custom DNS servers
  --system-dns: Use OS's DNS resolver
  --traceroute: Trace hop path to each host
```

Find Live Machines:

Command: nmap –sP <target>

```
ayesha-imran@ayesha-imran:~/Desktop$ nmap -sP 142.250.201.142
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-11-24 14:18 PKT
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.01 seconds
ayesha-imran@ayesha-imran:~/Desktop$
```

Discover Open Ports:

Command: nmap –p <port> -v <target>

```
ayesha-imran@ayesha-imran:~/Desktop$ nmap -p 1-65535 -v 104.21.82.247
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-11-24 15:21 PKT
Initiating Ping Scan at 15:21
Scanning 104.21.82.247 [2 ports]
Completed Ping Scan at 15:21, 0.11s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 15:21
Completed Parallel DNS resolution of 1 host. at 15:21, 0.01s elapsed
Initiating Connect Scan at 15:21
Scanning 104.21.82.247 [65535 ports]
Discovered open port 8080/tcp on 104.21.82.247
Discovered open port 2096/tcp on 104.21.82.247
Connect Scan Timing: About 0.71% done
Discovered open port 80/tcp on 104.21.82.247
Discovered open port 443/tcp on 104.21.82.247
```

a) TCP Connect Scan [-sT]:

Command: nmap -sT <target>

```
ayesha-imran@ayesha-imran:~/Desktop$ nmap -sT 192.168.17.133
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-11-24 14:28 PKT
Nmap scan report for ayesha-imran (192.168.17.133)
Host is up (0.00030s latency).
All 1000 scanned ports on ayesha-imran (192.168.17.133) are in ignored states.
Not shown: 1000 closed tcp ports (conn-refused)

Nmap done: 1 IP address (1 host up) scanned in 0.25 seconds
ayesha-imran@ayesha-imran:~/Desktop$
```

```
ayesha-imran@ayesha-imran:~/Desktop$ nmap -sT -Pn 192.168.17.1
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-11-24 14:31 PKT
Nmap scan report for 192.168.17.1
Host is up.
All 1000 scanned ports on 192.168.17.1 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 203.06 seconds
```

b) SYN Stealth Scan [-sS]:

Command: nmap –sS –A –O <target> –p <port>

```
ayesha-imran@ayesha-imran:~/Desktop$ sudo nmap -sS -A -O -p- 192.168.17.1
[sudo] password for ayesha-imran:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-11-24 14:36 PKT
sendto in send_ip_packet_sd: sendto(6, packet, 44, 0, 192.168.17.1, 16) => Network is u
nreachable
Offending packet: TCP 192.168.17.133:41261 > 192.168.17.1:8008 S ttl=57 id=42402 iplen=
44  seq=1974993598 win=1024 <mss 1460>
sendto in send_ip_packet_sd: sendto(6, packet, 44, 0, 192.168.17.1, 16) => Network is u
nreachable
Offending packet: TCP 192.168.17.133:41261 > 192.168.17.1:14918 S ttl=42 id=29341 iplen
=44  seq=1974993598 win=1024 <mss 1460>
sendto in send_ip_packet_sd: sendto(6, packet, 44, 0, 192.168.17.1, 16) => Network is u
nreachable
Offending packet: TCP 192.168.17.133:41261 > 192.168.17.1:14778 S ttl=38 id=4377 iplen=
```

c) UDP Scan [-sU]:

Command: nmap –sU <target>

```
ayesha-imran@ayesha-imran:~/Desktop$ sudo nmap -sU 192.168.17.1
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-11-24 15:04 PKT
Nmap scan report for 192.168.17.1
Host is up (0.00049s latency).
All 1000 scanned ports on 192.168.17.1 are in ignored states.
Not shown: 1000 open|filtered udp ports (no-response)
MAC Address: 00:50:56:C0:00:08 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 22.09 seconds
```

Post-Lab Tasks

Question 1:

Write a brief summary of each scan type you performed. Include the benefits and drawbacks of each method. Why might one use SYN Stealth Scan over a TCP Connect Scan, or vice versa?

Answer:

- **TCP Connect Scan**
  - **Summary:** Performs a full TCP three-way handshake (SYN → SYN/ACK → ACK).
  - **Benefits:**
    - Works without special privileges.
    - Reliable results since connections are fully established.
  - **Drawbacks:**
    - Easily logged by the target system.
    - Slower due to full connection establishment.
  - **Use Case:** Suitable when stealth is not required or when running scans without elevated privileges.
- **SYN Stealth Scan (Half-Open Scan)**

- **Summary:** Sends SYN, receives SYN/ACK, then immediately sends RST instead of completing the handshake.
- **Benefits:**
  - Faster and less detectable.
  - Commonly used in penetration testing for stealth.
- **Drawbacks:**
  - Requires root/admin privileges.
  - Can still be detected by advanced IDS.
- **Use Case:** Preferred when stealth and speed are important, such as penetration testing.

Comparison:

- Use **SYN Stealth Scan** when avoiding detection is critical.
- Use **TCP Connect Scan** when reliability is more important than stealth.

Question 2:

Describe how a network administrator might use these scan techniques to secure a network. How could an attacker use Nmap scanning to identify vulnerable services, and what defenses could mitigate these scans?

Answer:

- **Network Administrator Use:**
  - Identify open and unnecessary services.
  - Audit firewall rules and confirm only intended ports are accessible.
  - Establish a baseline of network services for monitoring changes.
- **Attacker Use:**
  - Reconnaissance: Map hosts, services, and OS versions.
  - Exploit targeting: Identify outdated or misconfigured services.
  - Stealth probing: Use stealth scans to avoid detection before launching attacks.
- **Defenses Against Scans:**
  - **Firewalls:** Restrict responses to suspicious probes.
  - **IDS/IPS:** Detect abnormal scanning patterns.
  - **Rate Limiting:** Slow down repeated connection attempts.
  - **Honeypots:** Trap attackers and mislead reconnaissance attempts.

Question 3:

Explore the concept of "stealth scanning" further. Research additional techniques (e.g., Idle Scans) that can make Nmap scanning less detectable.

Answer:

- **Idle Scan (Zombie Scan):**
  - Uses a third-party "zombie" host to send probes, hiding the attacker's IP.

    - **Benefit:** Extremely stealthy; attacker remains hidden.
    - **Drawback:** Requires a predictable idle host; complex setup.
- **FIN/NULL/Xmas Scans:**
    - Send unusual TCP flags (FIN, NULL, or Xmas packets).
    - **Benefit:** Can bypass some firewalls and filters.
    - **Drawback:** Less reliable; some OSes respond inconsistently.
- **Fragmentation Scans:**
    - Break packets into fragments to evade detection.
    - **Benefit:** Can bypass simple IDS signatures.
    - **Drawback:** Modern IDS can reassemble packets, reducing effectiveness.
- **Decoy Scans:**
    - Mix attacker's IP with decoys to confuse defenders.
    - **Benefit:** Makes attribution difficult.
    - **Drawback:** Can raise suspicion if too many decoys are used.

Conclusion

- **SYN Stealth Scans** balance speed and stealth, making them ideal for penetration testing.
- **TCP Connect Scans** are reliable but noisy, useful for administrators without elevated privileges.
- **Advanced stealth techniques** (Idle, FIN, Xmas, Decoy) enhance concealment but require more complexity.
- **Defenders** must combine firewalls, IDS, and monitoring to counter these scans effectively.