Task 01 — Networking Fundamentals, Nmap Scanning, and Automation Scripting

Intern: Aliya Ansari
Date: 30-09-2025

1. Target description

- **Target name / label:** Personal Laptop (Windows) — *Host A*
- **Target IP:** `192.168.0.206`
- **Scanner:** Kali Linux VM — `192.168.253.130`
- **Network / Notes:** Home LAN. Scans were run from the Kali VM; ICMP ping replies confirmed reachability prior to scans.

2. Exact Nmap commands used

All scans were executed from the Kali VM with the commands and output files shown below :

1. SYN scan (stealth scan)

```
sudo nmap -sS 192.168.0.206 -oN syn_scan.txt
```

2. TCP connect scan (fallback)

```
nmap -sT 192.168.0.206 -oN tcp_connect_scan.txt
```

3. UDP quick scan (top 100 UDP ports)

```
sudo nmap -sU 192.168.0.206 -oN udp_scan.txt
```

> Note: During initial attempts Nmap displayed retransmission warnings; I reran conservative scans as needed. Full-port scans (`-p-`) were considered but not required for this deliverable after the open ports were identified.

3. Scan outputs (excerpts)

Below are the important excerpts from the scans

SYN scan (`syn_scan.txt`) excerpt:

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-29 12:44 EDT
Nmap scan report for 192.168.0.206
Host is up (0.0018s latency).
Not shown: 995 filtered tcp ports (no-response)
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
903/tcp  open  iss-console-mgr
1521/tcp open  oracle
Nmap done: 1 IP address (1 host up) scanned in 4.87 seconds
```

TCP connect scan (`tcp_connect_scan.txt`) excerpt:

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-29 12:48 EDT
Nmap scan report for 192.168.0.206
Host is up (0.010s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
1521/tcp open  oracle
Nmap done: 1 IP address (1 host up) scanned in 10.19 seconds
```

UDP quick scan (`udp_scan.txt`) excerpt:

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-29 12:50 EDT
Nmap scan report for 192.168.0.206
Host is up (0.0012s latency).
All 1000 scanned ports on 192.168.0.206 are in ignored states.
Not shown: 1000 open|filtered udp ports (no-response)
Nmap done: 1 IP address (1 host up) scanned in 22.08 seconds
```

4. Findings — open ports, services, (versions if detected)

The table below summarizes the open TCP ports discovered during the SYN and TCP connect scans. Nmap did not return explicit product/version strings for all services in these runs — if required, re-run with `-sV --version-all` for more aggressive version detection.

Port	Proto	Service	Notes (detection/source)
135	tcp	msrpc	RPC endpoint mapper (SYN & connect)
139	tcp	netbios-ssn	NetBIOS/SMB legacy (SYN & connect)
445	tcp	microsoft-ds	SMB / Microsoft-DS (SYN & connect)

Port	Proto	Service	Notes (detection/source)
903	tcp	iss-console-mgr	Observed open in SYN scan only
1521	tcp	oracle	Oracle TNS listener (SYN & connect)

UDP results: UDP quick scan returned `open|filtered` for the scanned ports — typical when UDP responses are blocked/filtered by a firewall.

5. Potential security risks (per service)

- **135/tcp (MSRPC)**
  Risk: Exposes Windows RPC interfaces. Vulnerabilities in RPC implementations have historically allowed remote code execution and privilege escalation. RPC exposure increases attack surface.
  Mitigation: Restrict RPC access to trusted networks, apply Windows updates, and minimize exposed RPC services.

- **139/tcp (NetBIOS session)**
  Risk: NetBIOS reveals shares and machine names and can be used for reconnaissance and lateral movement. Legacy protocol — unnecessary on modern, segmented networks.
  Mitigation: Disable NetBIOS over TCP/IP if unused, restrict to internal networks, and harden shares with least privilege.

- **445/tcp (SMB / microsoft-ds)**
  Risk: SMB has been exploited for high-impact worms and ransomware (e.g., EternalBlue leveraged SMBv1). Exposed SMB increases risk of remote code execution and data theft.
  Mitigation: Block SMB at the edge, disable SMBv1, keep OS patched, enforce strong authentication and segment file servers.

- **903/tcp (iss-console-mgr)**
  Risk: Management/console services can expose administrative interfaces; appears only in SYN scan — may be transient or filtered. Unauthenticated or default-credential consoles are high risk.
  Mitigation: Identify application, restrict access to management interfaces, use VPN/firewall rules, require strong authentication.

- **1521/tcp (Oracle TNS listener)**
  Risk: Database listeners exposed to the network can leak database metadata or be subject to exploitation if listeners or databases are unpatched/misconfigured. Databases are high-value targets.
  Mitigation: Bind listeners to internal addresses, restrict connect access to trusted hosts, enforce authentication, apply vendor patches and database hardening guides.

6. Notes on two researched services

A — SMB (port 445) — brief research notes

- **Purpose:** Server Message Block (SMB) is used for file and printer sharing, and for inter-process communication on Windows networks.

- **Common weaknesses:** Outdated SMB implementations (notably SMBv1) have been exploited in high-impact incidents (ransomware/worms). Misconfiguration and exposure to untrusted networks are common root causes.

- **Example CVE (historic, for reporting context):** CVE-2017-0144 (EternalBlue) — remote code execution via SMBv1

- **Mitigations / best practice:** Disable SMBv1, apply OS patches, use firewall rules to limit SMB access to internal subnets only, enable logging/monitoring for SMB access.

B — Oracle TNS Listener (port 1521) — brief research notes

- **Purpose:** Oracle TNS listener accepts incoming client connections for Oracle Database instances (default port 1521).

- **Common weaknesses:** Misconfigured or publicly exposed listeners can enable information leakage, unauthenticated connection attempts, and in some cases remote exploits depending on Oracle version.

- **Example CVE (historic example):** CVE-2012-1675 — check NVD for current TNS-related vulnerabilities.

- **Mitigations / best practice:** Restrict listener access by IP, configure secure authentication and service registration, patch Oracle components promptly, and follow Oracle hardening guidelines.

7. Key learnings from the task

- Nmap scan types produce different results: SYN (`-sS`) is stealthier but can be rate-limited/blocked; TCP connect (`-sT`) completes handshakes and may succeed where `-sS` does not. UDP scans are slow and often return `open|filtered`.

- Always verify reachability (ICMP/ping) and ensure scanner/target are on the same network/subnet (or use bridged/host-only VM networking).

- Many services on modern OSes (RPC/SMB/DB listeners) are high-risk when exposed; reducing attack surface and applying vendor patches are first steps for mitigation.

- Automation (python-nmap or XML parsing) makes reproducible reporting straightforward—include XML outputs for parsing and archival.

8. Recommended next actions

1. **Immediate:** Restrict SMB/RPC (block 135/139/445 from untrusted networks); investigate port 903 service.

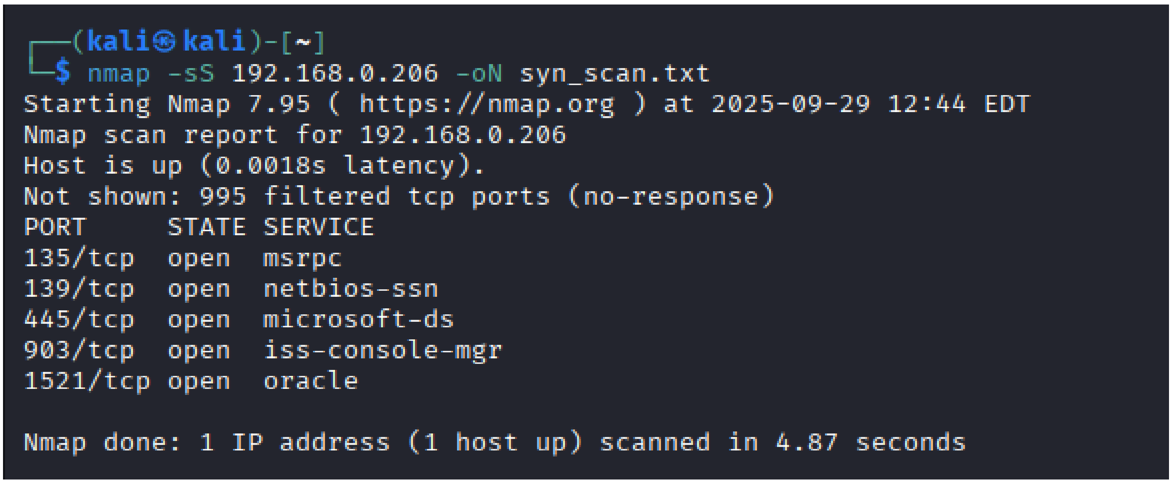
2. **Patch & Hardening:** Apply OS and Oracle updates, disable legacy protocols (SMBv1), harden database listener configuration.

3. **Monitoring:** Enable logging and review recent connections to the exposed ports; look for anomalous patterns.

4. **Automation:** Run `nmap_automation.py` to create repeatable scan reports and store outputs in version control for auditability.

9. Files & evidence (attached)

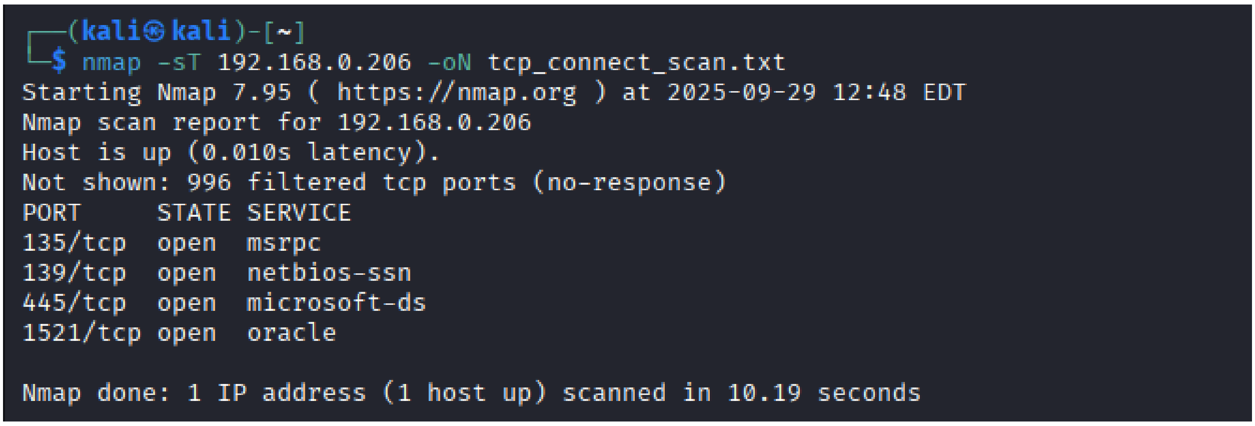
Figure 1: SYN Scan.



```
┌──(kali㉿kali)-[~]
└─$ nmap -sS 192.168.0.206 -oN syn_scan.txt
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-29 12:44 EDT
Nmap scan report for 192.168.0.206
Host is up (0.0018s latency).
Not shown: 995 filtered tcp ports (no-response)
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
903/tcp  open  iss-console-mgr
1521/tcp open  oracle

Nmap done: 1 IP address (1 host up) scanned in 4.87 seconds
```

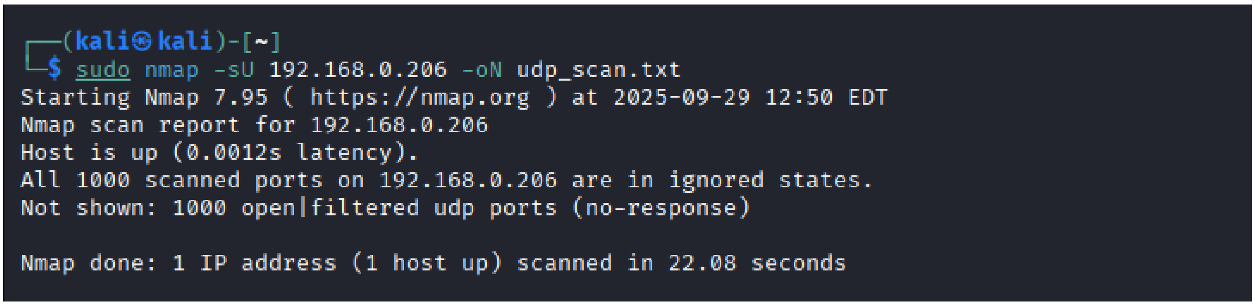
Figure 2: TCP Connect Scan.



```
┌──(kali㉿kali)-[~]
└─$ nmap -sT 192.168.0.206 -oN tcp_connect_scan.txt
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-29 12:48 EDT
Nmap scan report for 192.168.0.206
Host is up (0.010s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
1521/tcp open  oracle

Nmap done: 1 IP address (1 host up) scanned in 10.19 seconds
```

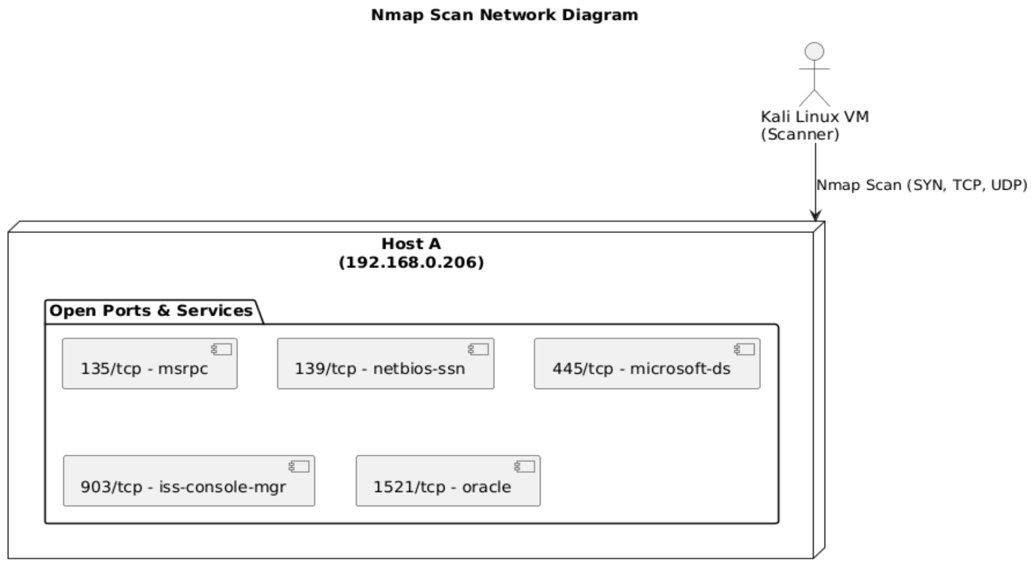
Figure 3: UDP Scan.



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sU 192.168.0.206 -oN udp_scan.txt
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-29 12:50 EDT
Nmap scan report for 192.168.0.206
Host is up (0.0012s latency).
All 1000 scanned ports on 192.168.0.206 are in ignored states.
Not shown: 1000 open|filtered udp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 22.08 seconds
```

Figure 4: Network Diagram of Host A and Open Ports.



End of report — Prepared by: ~Aliya