Offensive Security Assessment — Task 1

Title: Local Network Port & Service Discovery — Task 1
Prepared for: Course Instructor / Assessment Panel
Prepared by: Aman Rajak (Tester)
Date: 22 September 2025
Version: 1.0
Confidentiality: Confidential — For internal use only. Unauthorized disclosure or distribution is prohibited.

Table of Contents

---

1. Introduction

This report documents Task 1 of the offensive security practical: discovering open ports and identifying exposed services on hosts within a controlled lab local network. The assessment focuses on reconnaissance and service identification to evaluate potential attack surface and recommend mitigations.

---

2. Scope & Notes on Test Environment

In-scope: IP range 192.168.xxx.xxx/24 (scan invoked using 192.168.xxx.xxx/24).
Targets scanned: 192.168.xxx.xxx, 192.168.xxx.xxx, 192.168.xxx.xxx, 192.168.xxx.xxx (**four hosts observed up during the first scan**).
Important note (tester-supplied): The IP addresses used in this exercise were **manually assigned by the tester** to virtual machines (VMs) in a controlled lab environment. These addresses are static assignments for the VM instances and do not reflect DHCP allocations from a production DHCP server. All testing was performed in that isolated lab environment under authorized conditions.

Out-of-scope: Any hosts or networks outside the lab environment; any exploitation beyond safe/non-destructive checks without explicit authorization.

---

3. Objective

Learn and demonstrate basic network reconnaissance skills by discovering open ports and services on local-network hosts and providing an initial risk assessment and remediation recommendations.

---

4. Tools & Methodology

Tools used

- nmap (versions: 7.95 used on Kali VM) — TCP SYN scan and service/version detection.
- (Wireshark optional — not used for captured evidence in this submission.)

Methodology

1. Identify scan base and run a TCP SYN scan across the /24 network.
2. Note responsive hosts and the open ports discovered.
3. Perform targeted service/version detection (-sV) on ports of interest.
4. Classify severity and provide remediation recommendations.
5. Save and include raw outputs as evidence.

Commands used

- Initial SYN scan: *nmap -sS 192.168.1.7/24*
- Targeted service/version detection: *nmap -sV -p 53,135,445,3306 192.168.1.1 192.168.1.2*

---

5. Findings (Per Host)

5.1 Host: 192.168.xxx.xxx

- **Status:** Up
- **Open services discovered (after -sV):**
  - 53/tcp — dnsmasq 2.51 (DNS) — **open**
- **Other scanned ports:** 135, 445, 3306 — **closed**
- **MAC:** *5X:5X:00:1X:XX:0X*
- **Impact & analysis:**
  dnsmasq running on TCP 53 can be acceptable in a lab if configured correctly. However, older dnsmasq versions may have known CVEs. If misconfigured (e.g., unrestricted recursion, zone transfers), it could lead to information disclosure or misuse. DNS amplification attacks typically use UDP 53 — check UDP exposure separately if needed.
- **Preliminary severity: Medium** (depends on patch level & configuration).

5.2 Host: 192.168.xxx.xxx

- **Status:** Up
- **Open services discovered (after -sV):**
  - 135/tcp — msrpc — **open**
  - 445/tcp — microsoft-ds (SMB) — **open**
  - 3306/tcp — MySQL 8.0.35 — **open**
  - 53/tcp — **filtered**

- **MAC:** *5X:5X:00:1X:XX:0X*
- **Service Info (nmap):** OS: Windows
- **Impact & analysis:**
  This host is the primary risk. SMB and MSRPC are common vectors for lateral movement, credential theft, and RCE in Windows environments if unpatched or misconfigured. Remote MySQL access increases data exposure risk (unauthorized queries, default/weak credentials). Immediate controls and patching are recommended.
- **Preliminary severity: High**

5.3 Host: 192.168.xxx.xxx

- **Status:** Up
- **Ports:** All 1000 scanned TCP ports filtered (no open TCP services found).
- **MAC:** *5X:5X:00:1X:XX:0X*
- **Preliminary severity: Low** (no TCP services exposed in default scan).

5.4 Host: 192.168.xxx.xxx

- **Status:** Up (scanner host or another VM)
- **Ports:** All 1000 scanned TCP ports closed.
- **Preliminary severity: Low**

6. Risk Summary & Prioritization

Host	Open Services	Initial Severity
192.168.XXX.XXX	135 (MSRPC), 445 (SMB), 3306 (MySQL 8.0.35)	High
192.168.XXX.XXX	53 (dnsmasq 2.51)	Medium
192.168.XXX.XXX	No open TCP ports (filtered)	Low
192.168.XXX.XXX	No open TCP ports (closed)	Low

Rationale: Windows host 192.168. . exposes multiple high-risk services (**SMB/MSRPC and remote DB**). 192.168. . runs dnsmasq — medium risk until patch/configuration verified. Other hosts show no TCP exposure on the scanned ports.

7. Remediation & Action Plan (Actionable tickets)

Ticket 1 — Immediate (Critical) — Host 192.168.XXX.XXX

Title: Restrict & Harden SMB, RPC & MySQL on 192.168.**XXX.XXX**
Description / Steps:

1. Apply pending Windows updates and security patches immediately.
2. Disable SMBv1 if present.
3. Implement firewall rules to restrict ports 135 and 445 to management hosts only.
4. Block or restrict MySQL (3306) to authorized hosts only; if not required remotely, bind MySQL to localhost.
5. Review MySQL user accounts, rotate credentials, and enforce least privilege.

6. Enable logging and monitoring for suspicious login/SMB activity.
   Priority: Critical / Immediate
   Owner: Host Admin / Network Admin

Ticket 2 — Short-term (High) — Host 192.168.XXX.XXX

Title: Verify dnsmasq version & secure DNS configuration on 192.168.**XXX.XXX**
Description / Steps:

1. Check installed dnsmasq version; if possible, upgrade to latest stable release.
2. Verify dnsmasq configuration: disable zone transfers (if any), restrict recursion and recursive queries to trusted hosts only.
3. Confirm UDP 53 exposure and adjust firewall rules if necessary.
4. Review DNS logs for anomalies.
   Priority: High
   Owner: DNS/Host Admin

Ticket 3 — Medium — Network hardening

Title: Network segmentation & monitoring
Description / Steps:

1. Apply network segmentation to isolate services (DBs, management VMs) from general user networks.
2. Deploy IDS/host monitoring signatures for SMB and DNS anomalies.
3. Implement a scheduled patching process for server VMs.
   Priority: Medium
   Owner: Network Security Team

---

8. Steps to Reproduce / Commands Run

Initial SYN scan

```
nmap -sS 192.168.XXX.XXX/24
```

Targeted service/version detection

```
nmap -sV -p 53,135,445,3306 192.168.XXX.XXX   192.168.XXX.XXX
```

Suggested follow-up (authorized only)

- Full aggressive scan for more detail:

```
nmap -A -p 1-65535 192.168.XXX.XXX -oN 192.168.XXX.XXX_full_scan.txt
```

- Non-invasive vulnerability script scan (review scripts first):

```
nmap --script vuln -p 53,135,445,3306 192.168.XXX.XXX  192.168.XXX.XXX  -oN task1_vuln_scan.txt
```

- Save outputs:

```
nmap -sV -p 53,135,445,3306 192.168.XXX.XXX  192.168.XXX.XXX  -oN task1_sv_2025-09-22.txt
```

Authorization reminder: Run intrusive or authenticated checks only in an environment you own or are explicitly authorized to test.

---

9. Evidence (Raw Output)

(Raw nmap outputs captured during the assessment — included verbatim)

Initial SYN scan

```
┌──(kali㉿kali)-[~]
└─$ nmap -sS 192.168.XXX.XXX/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-23 17:39 IST
Nmap scan report for 192.168.XXX.XXX
Host is up (0.00070s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE
53/tcp open  domain
MAC Address: 5X:5X:00:1X:XX:0X

Nmap scan report for 192.168.XXX.XXX
Host is up (0.0019s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT     STATE SERVICE
135/tcp  open  msrpc
445/tcp  open  microsoft-ds
3306/tcp open  mysql
MAC Address: 5X:5X:00:1X:XX:0X

Nmap scan report for 192.168.XXX.XXX
Host is up (0.00036s latency).
All 1000 scanned ports on 192.168.XXX.XXX are in ignored states.
Not shown: 1000 filtered tcp ports (proto-unreach)
MAC Address: 5X:5X:00:1X:XX:0X

Nmap scan report for 192.168.XXX.XXX
Host is up (0.0000060s latency).
All 1000 scanned ports on 192.168.XXX.XXX are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap done: 256 IP addresses (4 hosts up) scanned in 14.54 seconds
```

Service/version detection (-sV)

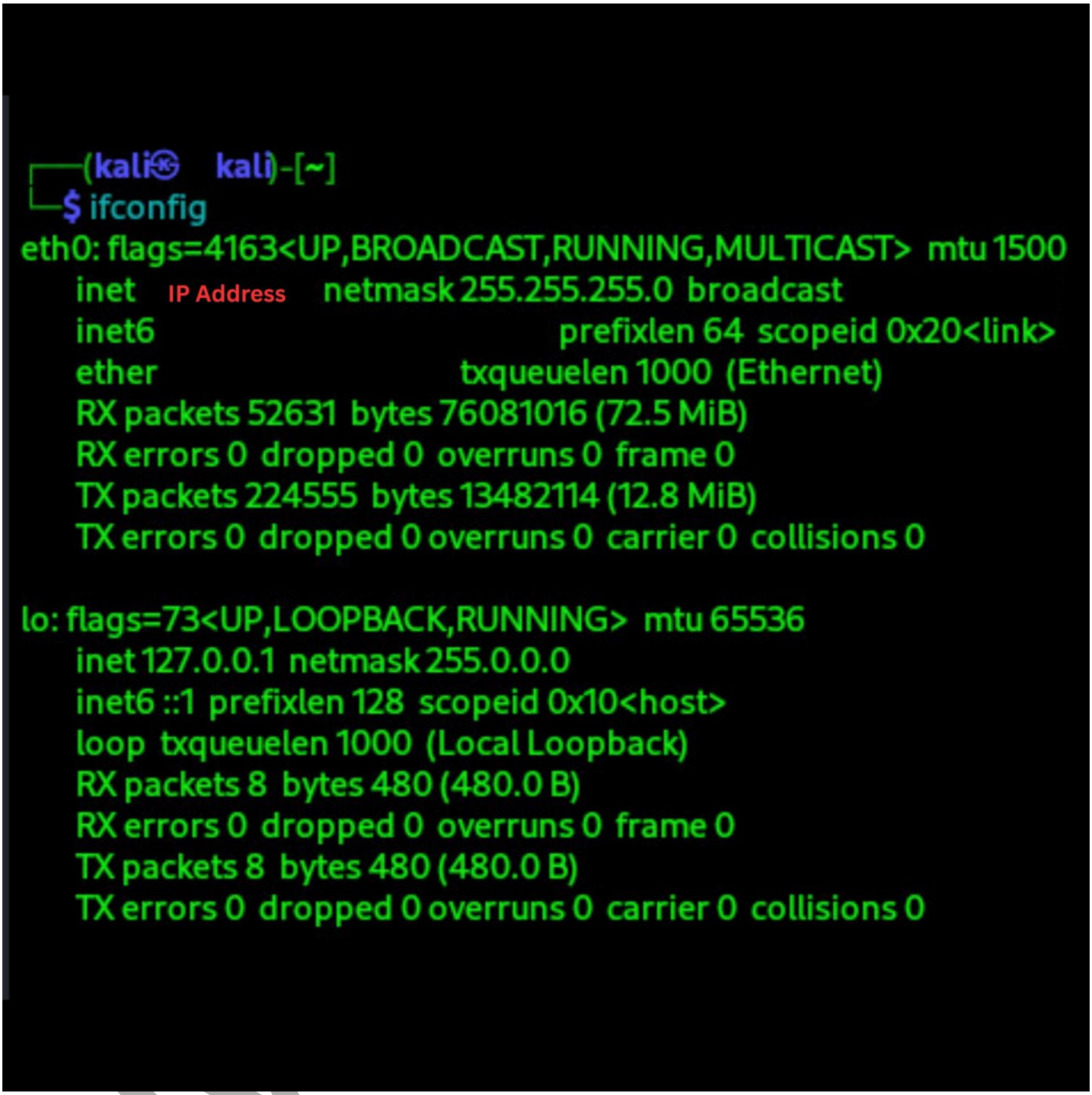
```
┌──(kali㉿kali)-[~]
└─$ nmap -sV -p 53,135,445,3306 192.168.1.1 192.168.xxx.xxx

Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-23 17:43 IST
Nmap scan report for 192.168.xxx.xxx
Host is up (0.00091s latency).

PORT     STATE  SERVICE     VERSION
```

```
53/tcp   open   domain      dnsmasq 2.51
135/tcp  closed msrpc
445/tcp  closed microsoft-ds
3306/tcp closed mysql
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)

Nmap scan report for 192.168.xxx.xxx
Host is up (0.00086s latency).

PORT     STATE    SERVICE      VERSION
53/tcp   filtered domain
135/tcp  open     msrpc        Microsoft Windows RPC
445/tcp  open     microsoft-ds?
3306/tcp open     mysql        MySQL 8.0.35
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 2 IP addresses (2 hosts up) scanned in 7.91 seconds
```

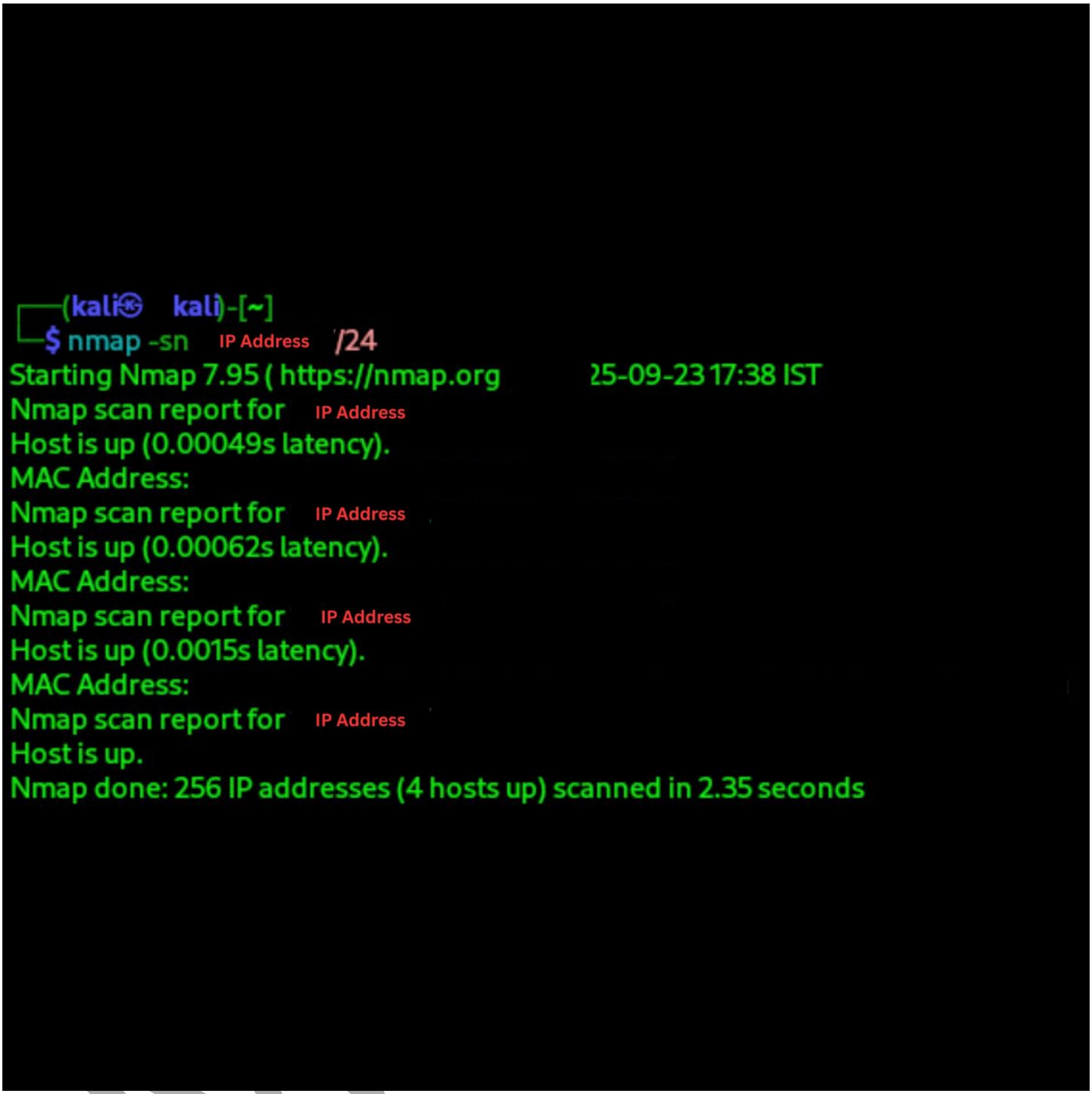
10. Conclusion

Task 1 objectives were met: the local network was scanned, open ports and services were identified, and an initial risk assessment was produced. The main risk is 192.168.xxx.xxx (Windows host) exposing SMB/MSRPC and MySQL; this requires immediate mitigation (patching, restricting access, credential review). 192.168.xxx.xxx runs dnsmasq 2.51 and should be checked for known vulnerabilities and configuration issues. Other hosts in the scan presented minimal TCP exposure.

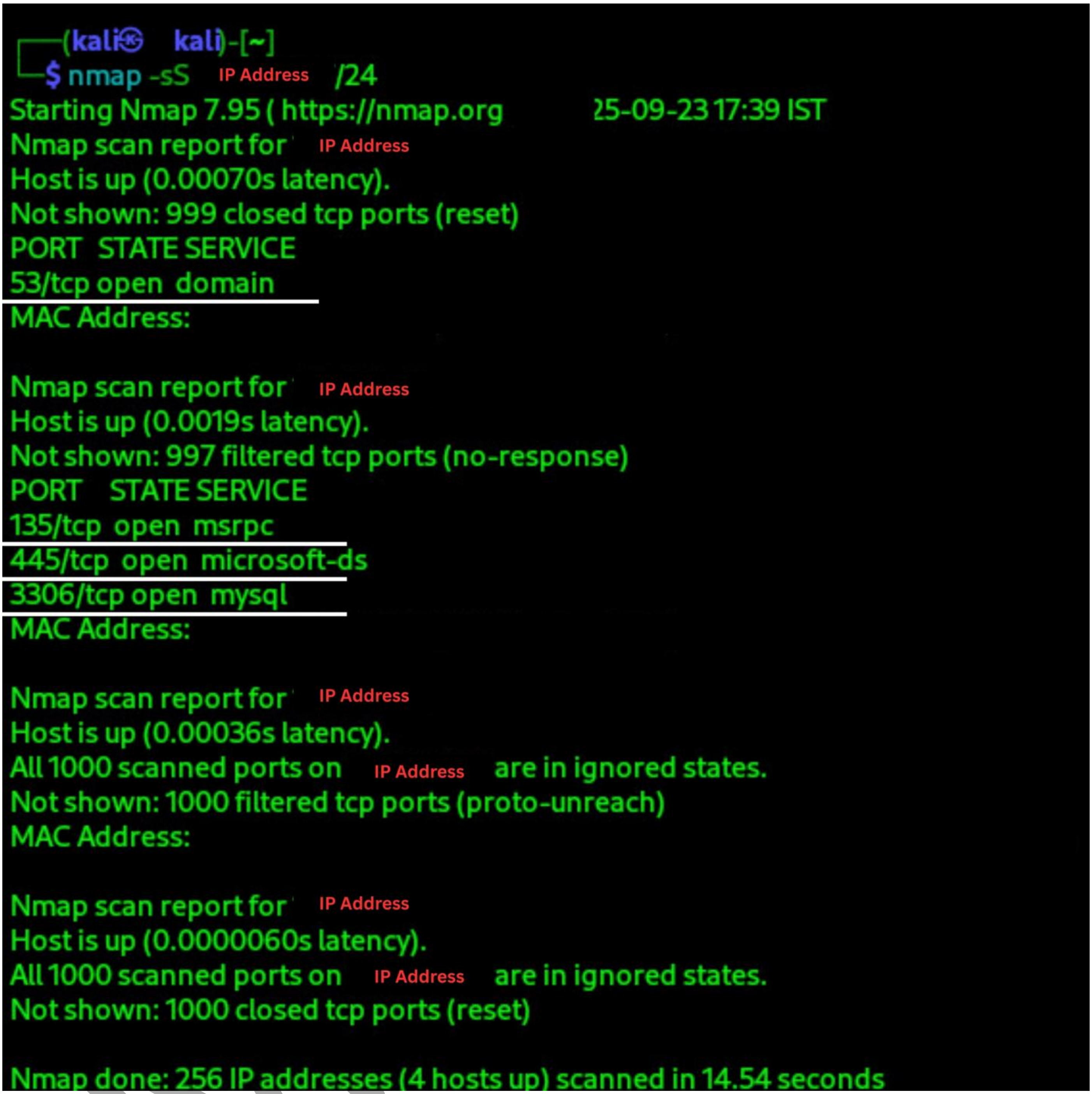
This report is prepared for submission as evidence of Task 1 completion and includes actionable remediation tickets and suggested next steps for deeper authorized testing.



```
┌──(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
      inet  IP Address   netmask 255.255.255.0  broadcast
      inet6                                  prefixlen 64  scopeid 0x20<link>
      ether                             txqueuelen 1000  (Ethernet)
      RX packets 52631  bytes 76081016 (72.5 MiB)
      RX errors 0  dropped 0  overruns 0  frame 0
      TX packets 224555  bytes 13482114 (12.8 MiB)
      TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
      inet 127.0.0.1  netmask 255.0.0.0
      inet6 ::1  prefixlen 128  scopeid 0x10<host>
      loop  txqueuelen 1000  (Local Loopback)
      RX packets 8  bytes 480 (480.0 B)
      RX errors 0  dropped 0  overruns 0  frame 0
      TX packets 8  bytes 480 (480.0 B)
      TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```



```
┌──(kali㉿ kali)-[~]
└─$ nmap -sn IP Address /24
Starting Nmap 7.95 ( https://nmap.org [redacted] 25-09-23 17:38 IST
Nmap scan report for IP Address
Host is up (0.00049s latency).
MAC Address: [redacted]
Nmap scan report for IP Address
Host is up (0.00062s latency).
MAC Address: [redacted]
Nmap scan report for IP Address
Host is up (0.0015s latency).
MAC Address: [redacted]
Nmap scan report for IP Address
Host is up.
Nmap done: 256 IP addresses (4 hosts up) scanned in 2.35 seconds
```



```
┌──(kali㉿ kali)-[~]
└─$ nmap -sS IP Address /24
Starting Nmap 7.95 ( https://nmap.org          25-09-23 17:39 IST
Nmap scan report for  IP Address
Host is up (0.00070s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE
53/tcp open  domain
MAC Address:

Nmap scan report for  IP Address
Host is up (0.0019s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT     STATE SERVICE
135/tcp  open  msrpc
445/tcp  open  microsoft-ds
3306/tcp open  mysql
MAC Address:

Nmap scan report for  IP Address
Host is up (0.00036s latency).
All 1000 scanned ports on  IP Address  are in ignored states.
Not shown: 1000 filtered tcp ports (proto-unreach)
MAC Address:

Nmap scan report for  IP Address
Host is up (0.0000060s latency).
All 1000 scanned ports on  IP Address  are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap done: 256 IP addresses (4 hosts up) scanned in 14.54 seconds
```