Network Scan Package

Included: commands, sample scan results, and screenshots from the task.

Generated for: User's network scanning task

Safety note: Only scan networks you own or are permitted to scan.

README.md

Network Scan Package
====================
What this contains

- README.md (this file)
- commands.txt (the exact commands I used to find IPs and scan)
- scan_results.txt (sample scan output saved as a text file)
- Network_Scan_Package.pdf (this PDF with screenshots, commands, and notes)
- Screenshots included in the PDF were taken from your console (ipconfig and nmap outputs).

What I did
----
1. Checked the machine IP and subnet using `ipconfig` on Windows to determine the local network (e.g., 10.87.32.0/24).
2. Performed a ping sweep to find live hosts:
   `nmap -sn 10.87.32.0/24`
3. Ran a TCP SYN scan to find open TCP ports:
   `nmap -sS 10.87.32.0/24`
4. Saved results to a text/XM file when needed (examples provided).
5. Optionally analyzed packet capture with Wireshark (not included).

Safety & Legal

Only scan devices you own or have explicit permission to scan. Scanning other people's or external networks can be illegal.

Notes

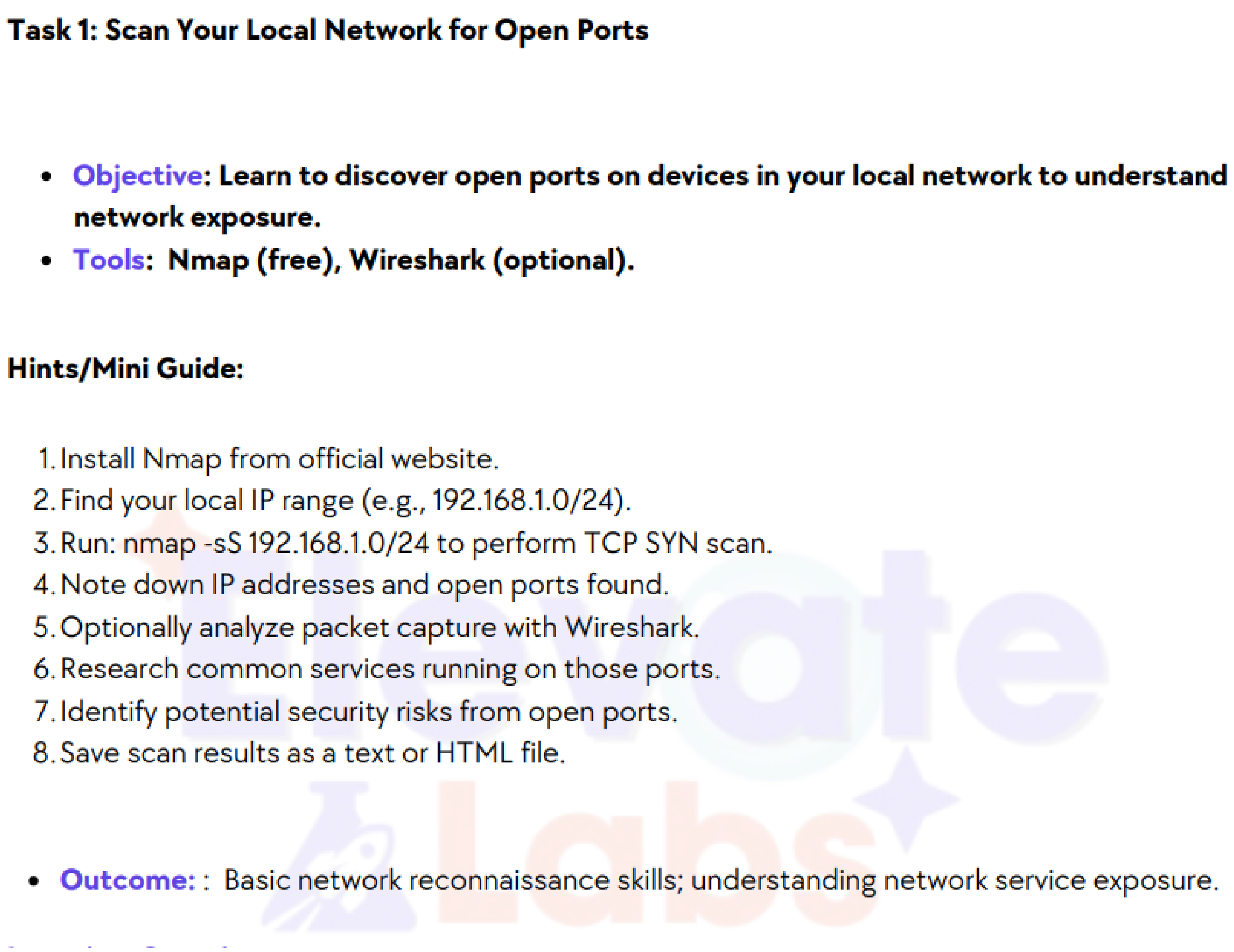
- IPs and MAC addresses shown in screenshots are from your local environment.
- I included sanitized example outputs in scan_results.txt and the full commands used in commands.txt.

commands.txt

```
# Commands I ran (Windows Command Prompt)
:: 1) Check IP and subnet
ipconfig
:: 2) Ping-sweep to list live hosts in network (replace with your network)
nmap -sn 10.87.32.0/24
:: 3) TCP SYN scan for open ports (run as Administrator)
nmap -sS 10.87.32.0/24
:: 4) Save human-readable results
nmap -sS 10.87.32.0/24 -oN scan_results.txt
:: 5) Save XML results
nmap -sS 10.87.32.0/24 -oX scan_results.xml
:: 6) Service/version detection (slower)
nmap -sS -sV -O 10.87.32.0/24
:: 7) Scan a single host (when you know the IP)
nmap -sS -sV 10.87.32.14
:: 8) UDP scan (much slower)
nmap -sU 10.87.32.0/24
:: 9) Save grepable output (old format)
nmap -sS 10.87.32.0/24 -oG scan_results.gnmap
```

scan_results.txt (example)

```
# Example scan results (sanitized)
# Ping sweep
Nmap scan report for 10.87.32.1
Host is up (0.035s latency).
MAC Address: 90:65:84:93:D0:32 (Intel Corporate)
Nmap scan report for 10.87.32.168
Host is up (0.014s latency).
MAC Address: C2:7B:D4:54:F7:B4 (Unknown)
Nmap done: 256 IP addresses (3 hosts up) scanned in 3.49 seconds
# TCP SYN scan sample for one host (10.87.32.168)
Nmap scan report for 10.87.32.168
Host is up (0.024s latency).
PORT   STATE SERVICE
53/tcp open  domain
# (other ports closed)
```



Task 1: Scan Your Local Network for Open Ports

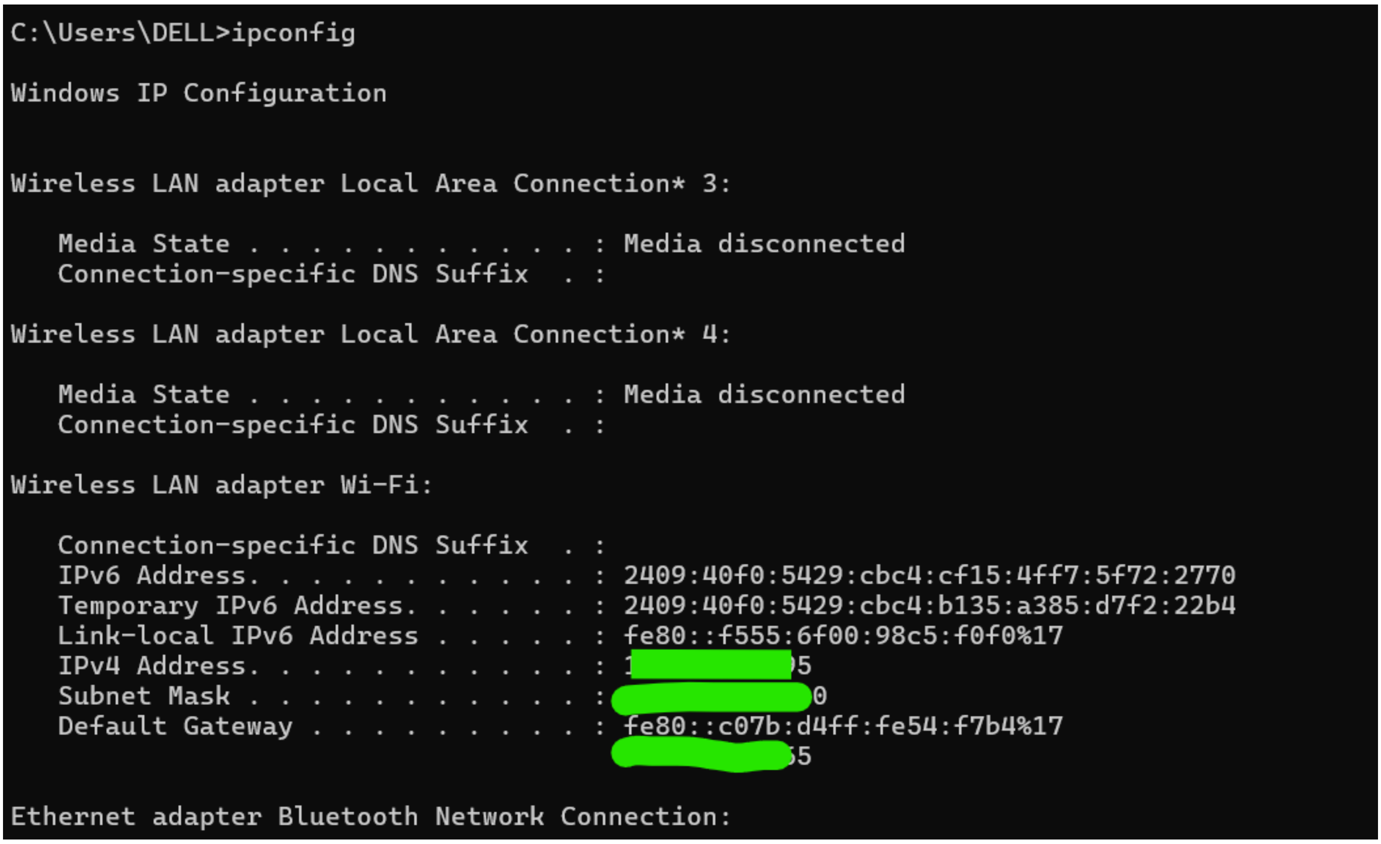
- **Objective: Learn to discover open ports on devices in your local network to understand network exposure.**
- **Tools: Nmap (free), Wireshark (optional).**

Hints/Mini Guide:

1. Install Nmap from official website.
2. Find your local IP range (e.g., 192.168.1.0/24).
3. Run: nmap -sS 192.168.1.0/24 to perform TCP SYN scan.
4. Note down IP addresses and open ports found.
5. Optionally analyze packet capture with Wireshark.
6. Research common services running on those ports.
7. Identify potential security risks from open ports.
8. Save scan results as a text or HTML file.

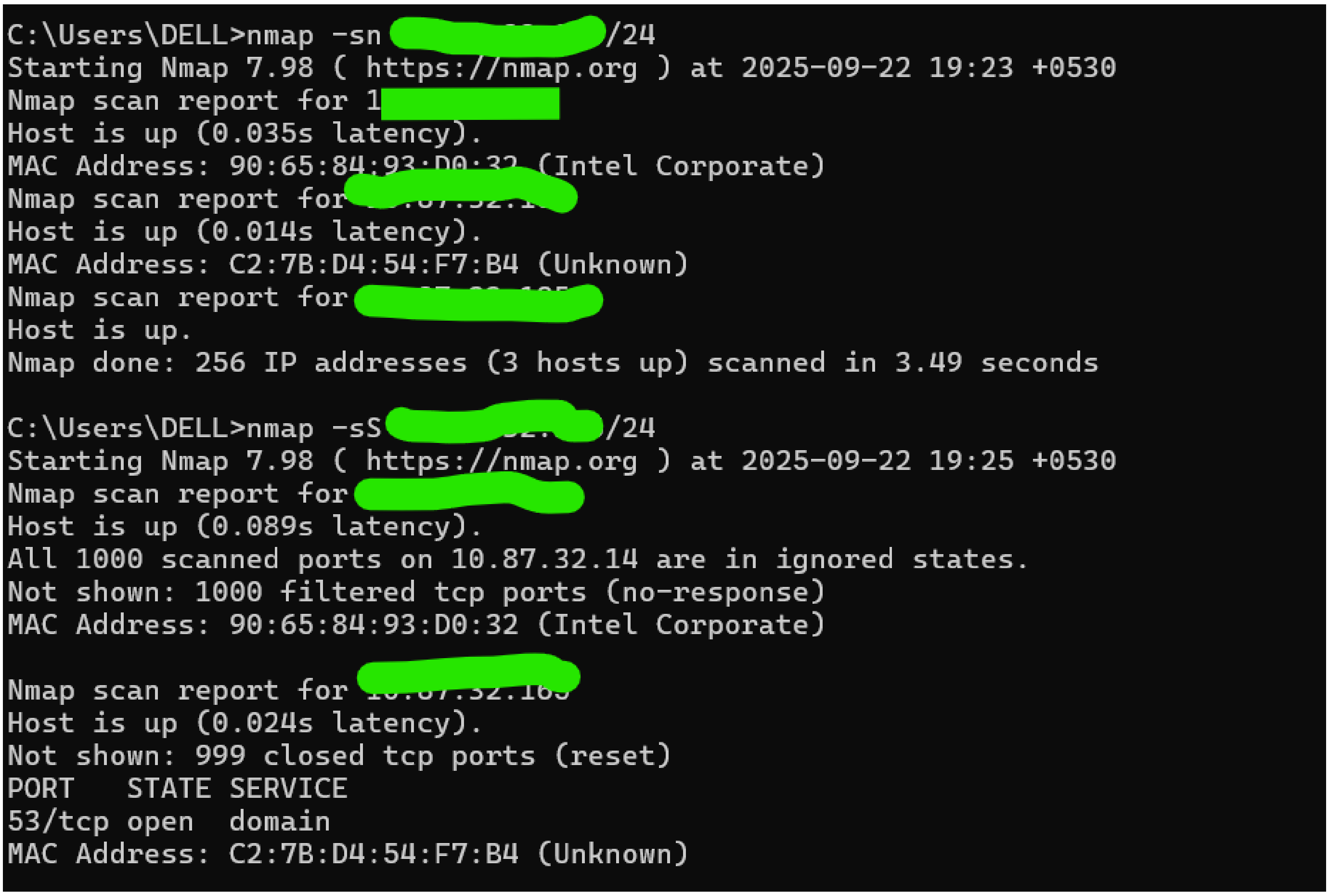
- **Outcome:** : Basic network reconnaissance skills; understanding network service exposure.

Screenshot 1: Screenshot 2025-09-22 190607.png



```
C:\Users\DELL>ipconfig

Windows IP Configuration


Wireless LAN adapter Local Area Connection* 3:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 4:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 2409:40f0:5429:cbc4:cf15:4ff7:5f72:2770
   Temporary IPv6 Address. . . . . . : 2409:40f0:5429:cbc4:b135:a385:d7f2:22b4
   Link-local IPv6 Address . . . . . : fe80::f555:6f00:98c5:f0f0%17
   IPv4 Address. . . . . . . . . . . : [redacted]
   Subnet Mask . . . . . . . . . . . : [redacted]
   Default Gateway . . . . . . . . . : fe80::c07b:d4ff:fe54:f7b4%17
                                       [redacted]

Ethernet adapter Bluetooth Network Connection:
```

Screenshot 2: Screenshot 2025-09-22 194157.png



```
C:\Users\DELL>nmap -sn [redacted]/24
Starting Nmap 7.98 ( https://nmap.org ) at 2025-09-22 19:23 +0530
Nmap scan report for 1[redacted]
Host is up (0.035s latency).
MAC Address: 90:65:84:93:D0:32 (Intel Corporate)
Nmap scan report for [redacted]
Host is up (0.014s latency).
MAC Address: C2:7B:D4:54:F7:B4 (Unknown)
Nmap scan report for [redacted]
Host is up.
Nmap done: 256 IP addresses (3 hosts up) scanned in 3.49 seconds

C:\Users\DELL>nmap -sS [redacted]/24
Starting Nmap 7.98 ( https://nmap.org ) at 2025-09-22 19:25 +0530
Nmap scan report for [redacted]
Host is up (0.089s latency).
All 1000 scanned ports on 10.87.32.14 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 90:65:84:93:D0:32 (Intel Corporate)

Nmap scan report for [redacted]
Host is up (0.024s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE
53/tcp open  domain
MAC Address: C2:7B:D4:54:F7:B4 (Unknown)
```

Screenshot 3: Screenshot 2025-09-22 194438.png