

FUTURE_CS_03

SECURE YOUR OWN WI-FI NETWORK

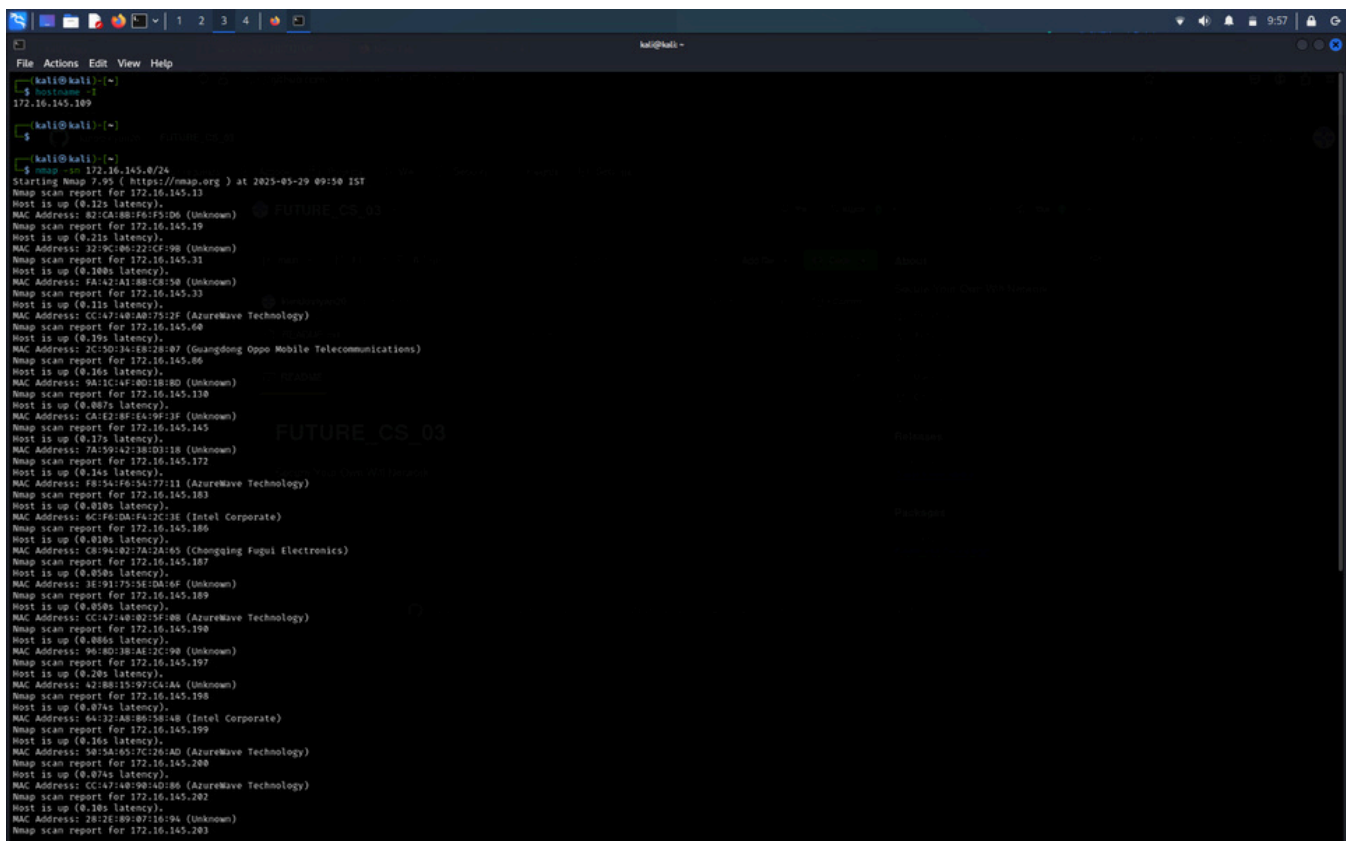
TASK:

*Task: Conduct a Wi-Fi security assessment on your home network, checking for weak passwords, open ports, and unauthorized devices.

*Skills Gained: Network security basics, Wi-Fi encryption, penetration testing.

*Tools: Wireshark, Aircrack-ng, Nmap.

*Deliverable: A report outlining vulnerabilities and recommendations to improve security



```
File Actions Edit View Help
kali@kali:~$ sudo nmap -sn 172.16.145.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-29 09:58 IST
Nmap scan report for 172.16.145.13
Host is up (0.32s latency).
MAC Address: 82:CA:8B:F6:F5:D6 (Unknown)
Nmap scan report for 172.16.145.19
Host is up (0.21s latency).
MAC Address: 32:9C:06:22:CF:98 (Unknown)
Nmap scan report for 172.16.145.31
Host is up (0.108s latency).
MAC Address: FA:42:A1:8B:CA:58 (Unknown)
Nmap scan report for 172.16.145.33
Host is up (0.11s latency).
MAC Address: CC:47:40:80:75:2F (AzureWave Technology)
Nmap scan report for 172.16.145.60
Host is up (0.19s latency).
MAC Address: 2C:5D:3A:18:28:87 (Guangdong Oppo Mobile Telecommunications)
Nmap scan report for 172.16.145.86
Host is up (0.16s latency).
MAC Address: 9A:1C:4F:8D:18:8D (Unknown)
Nmap scan report for 172.16.145.110
Host is up (0.087s latency).
MAC Address: CA:E2:8F:1E:49:2F (Unknown)
Nmap scan report for 172.16.145.145
Host is up (0.17s latency).
MAC Address: 7A:59:42:38:D3:18 (Unknown)
Nmap scan report for 172.16.145.172
Host is up (0.14s latency).
MAC Address: F8:5A:F6:5A:77:11 (AzureWave Technology)
Nmap scan report for 172.16.145.183
Host is up (0.018s latency).
MAC Address: 6C:F6:DA:FA:2C:3E (Intel Corporate)
Nmap scan report for 172.16.145.186
Host is up (0.018s latency).
MAC Address: C8:94:02:7A:2A:65 (Chongqing Fugui Electronics)
Nmap scan report for 172.16.145.187
Host is up (0.058s latency).
MAC Address: 3E:91:75:5E:DA:6F (Unknown)
Nmap scan report for 172.16.145.189
Host is up (0.058s latency).
MAC Address: CC:47:40:80:75:2F (AzureWave Technology)
Nmap scan report for 172.16.145.190
Host is up (0.086s latency).
MAC Address: 96:8D:38:AE:2C:98 (Unknown)
Nmap scan report for 172.16.145.197
Host is up (0.28s latency).
MAC Address: 42:18:15:97:CC:A6 (Unknown)
Nmap scan report for 172.16.145.198
Host is up (0.074s latency).
MAC Address: 64:22:4B:8B:34:48 (Intel Corporate)
Nmap scan report for 172.16.145.199
Host is up (0.16s latency).
MAC Address: 9A:1C:4F:8D:18:8D (AzureWave Technology)
Nmap scan report for 172.16.145.200
Host is up (0.074s latency).
MAC Address: CC:47:40:80:75:2F (AzureWave Technology)
Nmap scan report for 172.16.145.202
Host is up (0.18s latency).
MAC Address: 28:2E:89:D7:16:9A (Unknown)
Nmap scan report for 172.16.145.203
```

"I performed a scan on our Wi-Fi network and found 24 active devices, including several with unknown MAC addresses. This indicates potential unauthorized access, and I recommend reviewing connected devices and enhancing network security."

Device: 172.16.145.200

- **Open Ports:**
 - 3306/tcp → MySQL
- **Risk Level: High**
- **Reason:** Exposed MySQL port allows access to database if weak password or remote access allowed.
- **Action:** Bind MySQL to localhost only, or firewall the port.

Device: 172.16.145.199

- **Open Ports:**
 - 135/tcp → MS RPC
 - 139/tcp → NetBIOS-ssn
 - 445/tcp → Microsoft-ds (SMB)
- **Risk Level: Moderate to High**
- **Reason:** SMB and NetBIOS are common vectors for attacks.
- **Action:** Disable SMB if unused, apply access control or firewall rules.

```
File Actions Edit View Help
Nmap done: 256 IP addresses (24 hosts up) scanned in 36.21 seconds

kali@kali:~$ nmap -v 172.16.145.189

Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-29 09:58 IST
Nmap scan report for 172.16.145.189
Host is up (0.868s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
3500/tcp  open  http    National Instruments LabVIEW service locator httpd 1.0.0
5800/tcp  open  vnc-http TightVNC (user: vasanth; VNC TCP port: 5900)
5900/tcp  open  vnc     VNC (protocol 3.8)
MAC Address: CC:47:48:02:5F:80 (AzureWave Technology)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 27.36 seconds

kali@kali:~$ nmap -v 172.16.145.186

Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-29 10:00 IST
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 1.54 seconds

kali@kali:~$ nmap -v 172.16.145.200

Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-29 10:00 IST
Nmap scan report for 172.16.145.200
Host is up (0.856s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
2386/tcp  open  mysql   MySQL (unauthorized)
MAC Address: CC:47:48:90:4D:86 (AzureWave Technology)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 19.43 seconds

kali@kali:~$ nmap -v 172.16.145.199

Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-29 10:02 IST
Nmap scan report for 172.16.145.199
Host is up (0.856s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
135/tcp  open  msrpc   Microsoft Windows RPC
139/tcp  open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds?
MAC Address: 50:5A:65:7C:28:AD (AzureWave Technology)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 22.71 seconds

kali@kali:~$ nmap -v 172.16.145.198

Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-29 10:04 IST
Nmap scan report for 172.16.145.198
Host is up (0.844s latency).
All 1000 scanned ports on 172.16.145.198 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: 64:12:AB:85:58:4B (Intel Corporate)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 3.29 seconds

kali@kali:~$
```

Security Recommendations

1. **Disable Unused Services:** Like SMB, VNC, MySQL if not in active use.
2. **Filter Unknown Devices:** Use MAC filtering in router settings.
3. **Use WPA3/WPA2 Encryption:** Ensure strong password.
4. **Update Router Firmware:** Patch known security bugs.
5. **Disable WPS:** Prevent brute-force attacks.
6. **Use Firewall:** Block unnecessary inbound ports.
7. **Change Router Login:** Avoid default admin credentials.
8. **Periodic Monitoring:** Run nmap weekly to detect changes.