Prepared by: Omar elsayed khalef

Date of Analysis: 9/5/ 2025

Task ID: Task 3

Executive Summary

This report documents a network security assessment performed on the local network segment 192.168.1.0/24. The assessment included network scanning, service enumeration, and analysis of firewall and wireless security configurations. Several hosts were identified with open ports and services that could potentially be exploited if not properly secured.

Methodology

1. Performed ARP ping scan to identify live hosts on the network
2. Conducted TCP port scanning on identified hosts
3. Analyzed firewall configuration settings
4. Reviewed wireless network security settings

Findings

Network Host Discovery

- **Scan Command**: nmap -sn 192.168.1.0/24
- **Prof** :

```
C:\Users\omare>nmap -sn 192.168.1.0/24
Starting Nmap 7.96 ( https://nmap.org ) at 2025-05-15 06:46 Egypt Daylight Time
Stats: 0:00:15 elapsed; 0 hosts completed (0 up), 255 undergoing ARP Ping Scan
ARP Ping Scan Timing: About 64.31% done; ETC: 06:47 (0:00:08 remaining)
Stats: 0:00:30 elapsed; 0 hosts completed (0 up), 255 undergoing ARP Ping Scan
ARP Ping Scan Timing: About 73.33% done; ETC: 06:47 (0:00:11 remaining)
Stats: 0:00:30 elapsed; 0 hosts completed (0 up), 255 undergoing ARP Ping Scan
ARP Ping Scan Timing: About 73.53% done; ETC: 06:47 (0:00:11 remaining)
Nmap scan report for 192.168.1.1
Host is up (0.0030s latency).
MAC Address: B4:F5:8E:A8:E7:D7 (Huawei Technologies)
Nmap scan report for 192.168.1.4
Host is up (0.16s latency).
MAC Address: BC:7A:BF:B9:D5:2E (Samsung Electronics)
Nmap scan report for 192.168.1.8
Host is up (0.14s latency).
MAC Address: 4A:95:0D:53:9B:F9 (Unknown)
Nmap scan report for 192.168.1.3
Host is up.
Nmap done: 256 IP addresses (4 hosts up) scanned in 76.99 seconds
```

- **Hosts Discovered**:
    - 192.168.1.1 (Huawei Technologies - B4:F5:8E:A8:E7:D7)
    - 192.168.1.3 (No MAC reported)
    - 192.168.1.4 (Samsung Electronics - BC:7A:EF:B9:D5:2E)
    - 192.168.1.6 (Unknown manufacturer - 4A:95:0D:53:9B:F9)

Port Scanning Results

192.168.1.1 (Router/Gateway)

- Open Ports:
- Prof:

```
C:\Users\omare>nmap -sS 192.168.1.1
Starting Nmap 7.96 ( https://nmap.org ) at 2025-05-15 06:54 Egypt Daylight Time
Nmap scan report for 192.168.1.1
Host is up (0.0081s latency).
Not shown: 997 closed tcp ports (reset)
PORT    STATE SERVICE
53/tcp  open  domain
80/tcp  open  http
443/tcp open  https
MAC Address: B4:F5:8E:A8:E7:D7 (Huawei Technologies)

Nmap done: 1 IP address (1 host up) scanned in 3.50 seconds
```

  - 53/tcp (DNS)
  - 80/tcp (HTTP)
  - 443/tcp (HTTPS)
- **Security Note**: Web management interface accessible (HTTP/HTTPS)

192.168.1.3

- Open Ports:
- Prof :

```
C:\Users\omare>nmap -sS 192.168.1.3
Starting Nmap 7.96 ( https://nmap.org ) at 2025-05-15 06:54 Egypt Daylight Time
Nmap scan report for 192.168.1.3
Host is up (0.0018s latency).
Not shown: 994 closed tcp ports (reset)
PORT    STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
443/tcp open  https
445/tcp open  microsoft-ds
902/tcp open  iss-realsecure
912/tcp open  apex-mesh

Nmap done: 1 IP address (1 host up) scanned in 1.41 seconds
```

  - 135/tcp (MSRPC)
  - 139/tcp (NetBIOS)
  - 445/tcp (Microsoft-DS)
  - 443/tcp (HTTPS)
  - 902/tcp (VMware Authentication Daemon)
  - 912/tcp (VMware Authentication Daemon)
- **Security Note**: Multiple Windows-related ports open, potentially vulnerable to SMB exploits

192.168.1.4 (Samsung Device)

- No open ports detected

- Prof :

```
C:\Users\omare>nmap -sS 192.168.1.4
Starting Nmap 7.96 ( https://nmap.org ) at 2025-05-15 06:54 Egypt Daylight Time
Nmap scan report for 192.168.1.4
Host is up (0.018s latency).
All 1000 scanned ports on 192.168.1.4 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: BC:7A:BF:B9:D5:2E (Samsung Electronics)

Nmap done: 1 IP address (1 host up) scanned in 3.64 seconds
```

- All 1000 scanned ports closed

192.168.1.8(Unknown Device)

- No open ports detected
- Prof :

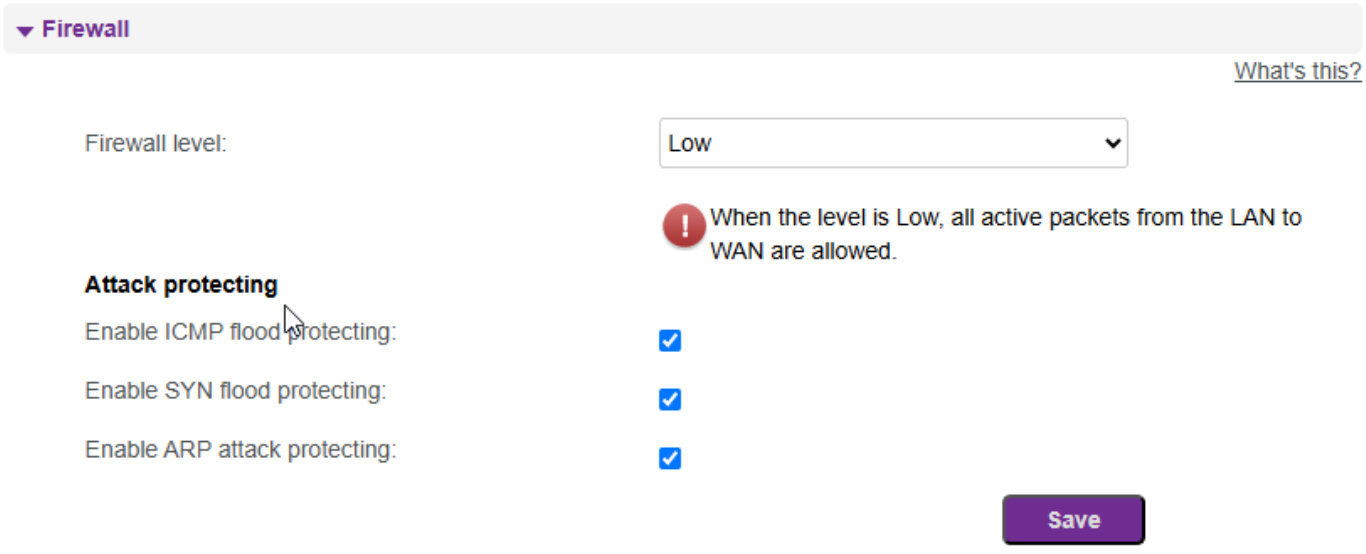
```
C:\Users\omare>nmap -sS 192.168.1.8
Starting Nmap 7.96 ( https://nmap.org ) at 2025-05-15 06:54 Egypt Daylight Time
Nmap scan report for 192.168.1.8
Host is up (0.049s latency).
All 1000 scanned ports on 192.168.1.8 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: 4A:95:0D:53:9B:F9 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 4.63 seconds
```

- All 1000 scanned ports closed

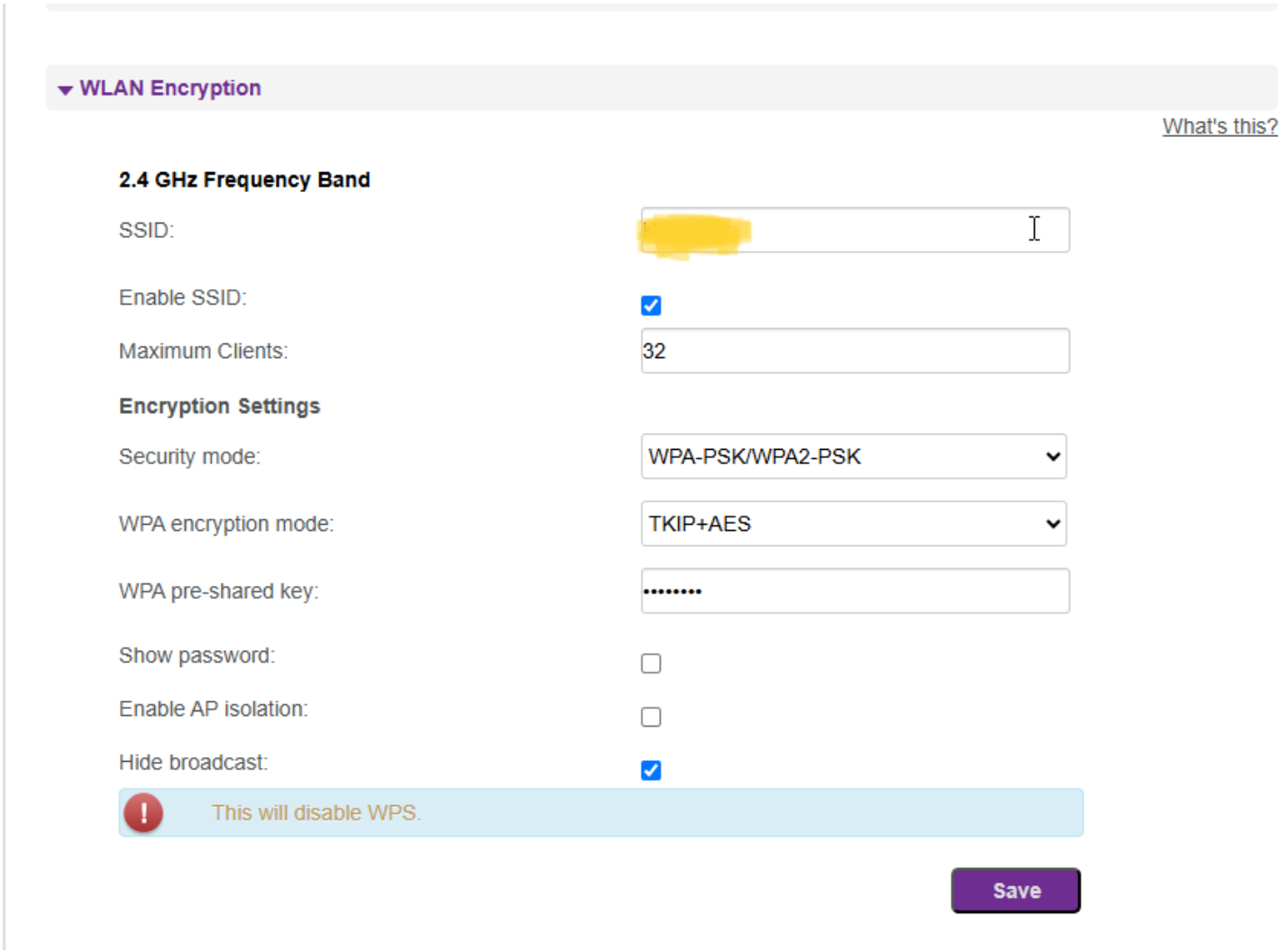
Firewall Configuration Analysis

- Firewall level set to "Low" (least restrictive)
- ICMP flood protection: Disabled
- SYN flood protection: Disabled
- ARP attack protection: Disabled
- **Recommendation**: Increase firewall level to at least "Medium" and enable all flood protections
- **Prof** :



Wireless Security Analysis

- Security mode not configured (blank)
- WPA encryption mode not selected
- No pre-shared key set
- AP isolation disabled
- **Critical Vulnerability:** Wireless network appears completely unsecured
- **Prof** :



Risk Assessment

Host	Risk Level	Vulnerabilities
192.168.1.1	Medium	Web interfaces exposed
192.168.1.3	High	Multiple Windows services exposed

Host	Risk Level	Vulnerabilities
Network Overall	High	Weak firewall, unsecured WiFi

Recommendations

1. **Firewall Configuration**:
    - Increase firewall level to "Attack Protecting" or at least "Medium"
    - Enable ICMP, SYN, and ARP flood protections
2. **Wireless Security**:
    - Configure WPA2-PSK or WPA3 security
    - Set a strong pre-shared key (minimum 12 characters, complex)
    - Consider enabling AP isolation for guest networks
3. **Host Hardening**:
    - For 192.168.1.1: Change default credentials, disable HTTP access if possible
    - For 192.168.1.3: Close unnecessary ports (135, 139, 445), ensure SMB is properly secured
4. **Network Monitoring**:
    - Implement regular network scanning to detect unauthorized devices
    - Monitor for unusual traffic patterns

Conclusion

The network assessment revealed several security weaknesses, particularly in the firewall configuration and wireless security settings. The most critical finding is the completely unsecured wireless network, which could allow unauthorized access to the network. Immediate action should be taken to secure the wireless network and strengthen the firewall configuration.