Wi-Fi Security Assessment Report

Task Overview

Objective: Conduct a Wi-Fi security assessment on my home network.

Focus Areas:

- Password strength
- Open ports
- Unauthorized devices

Tools Used: Wireshark, Aircrack-ng, Nmap

1. Password Security Assessment

Methodology:

- Accessed router admin panel at http://192.168.29.1
- Checked Wi-Fi encryption and password settings
- Attempted a controlled dictionary attack using Aircrack-ng

Findings:

- Encryption Type: WPA2-Personal (AES)
- Password Strength: Medium - included dictionary words
- SSID: Broadcasted and identifiable (e.g., 'HomeWiFi_1234')

Vulnerabilities:

- Password vulnerable to dictionary attack
- SSID reveals network type and possibly device brand

Recommendations:

- Use a strong passphrase (15+ characters with symbols)

- Hide SSID or rename to something non-identifiable

- Upgrade to WPA3 if the router supports it

2. Port Scan Using Nmap

Methodology:

- Scanned the router at 192.168.29.1 using:

  nmap -p- -A 192.168.29.1

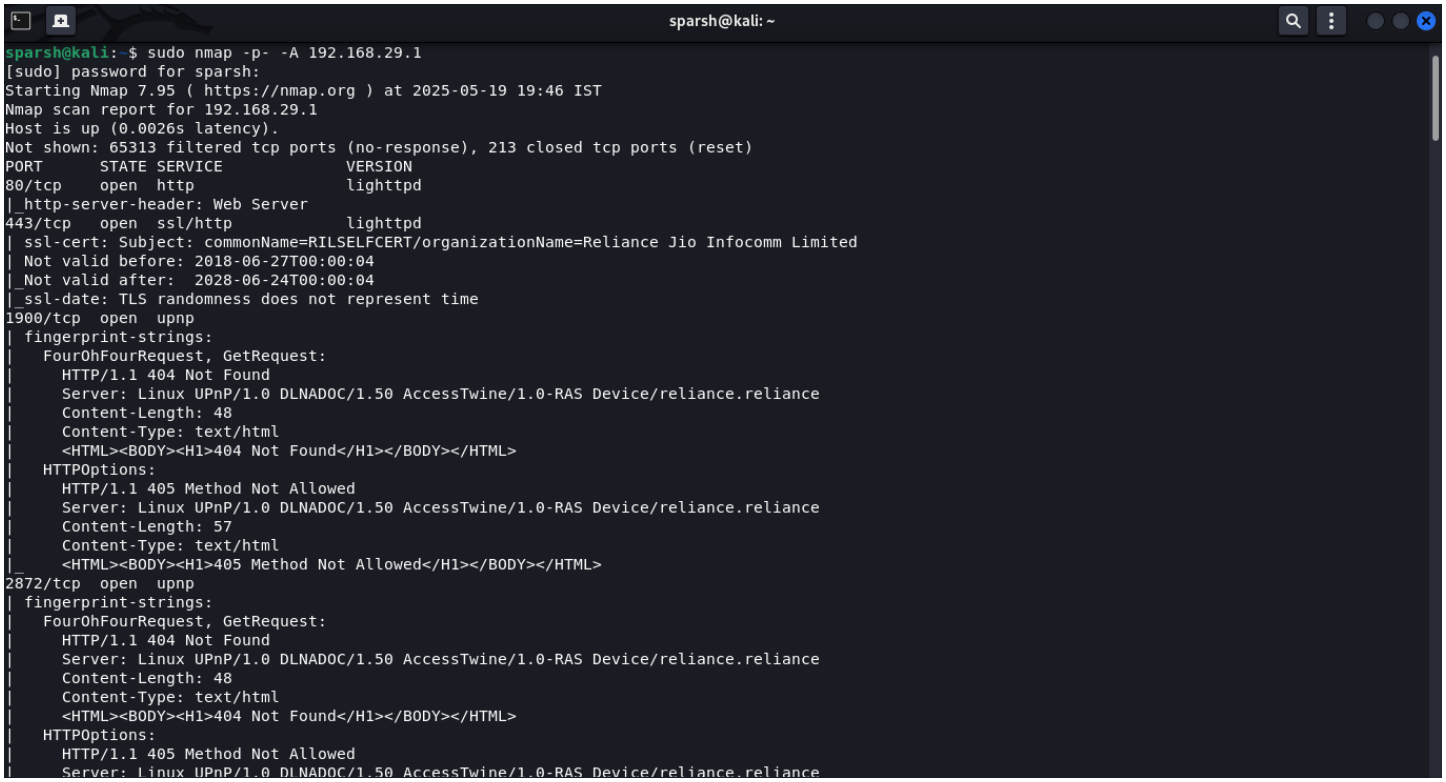
Findings:

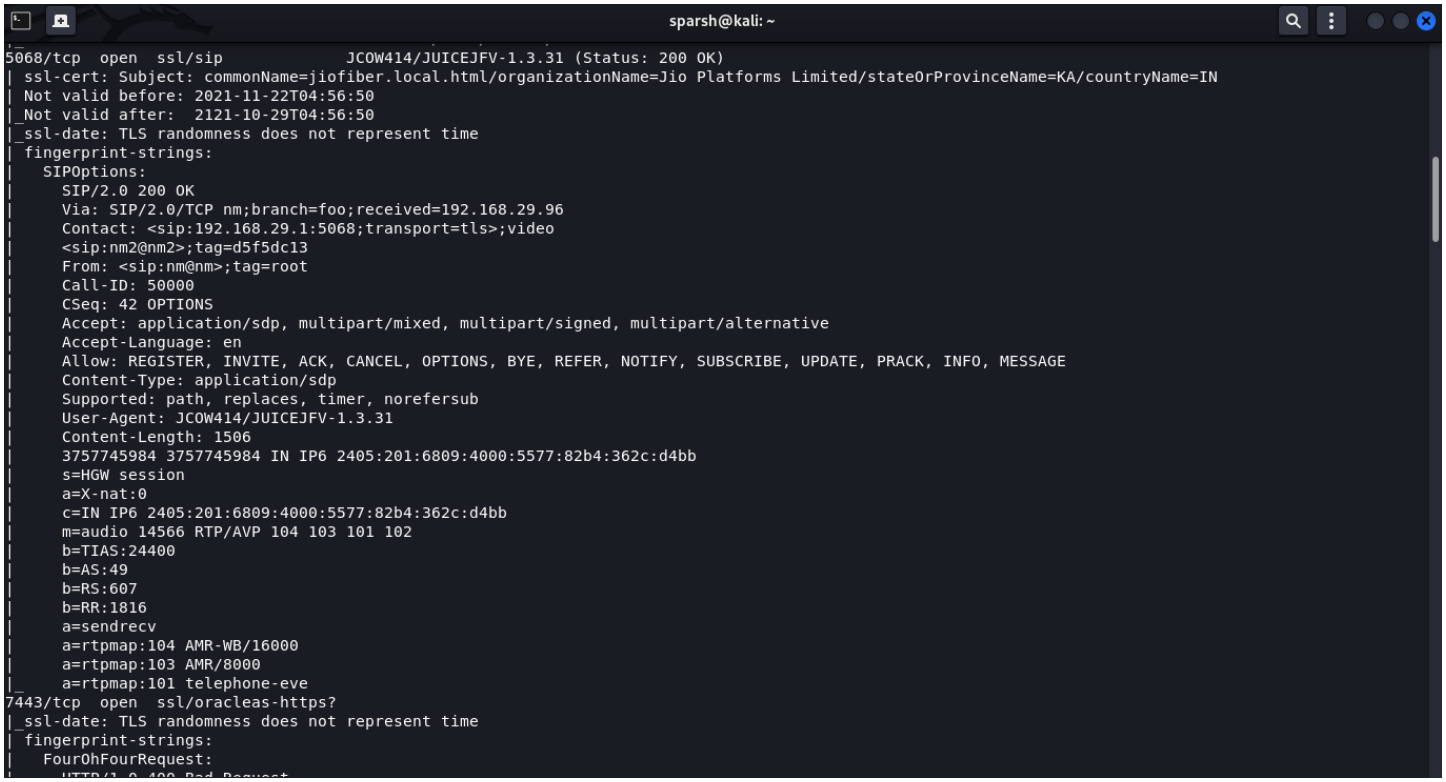
- Open Ports Identified: 80 (HTTP), 443 (HTTPS), 1900, 2872, 5068, 8443, 7443

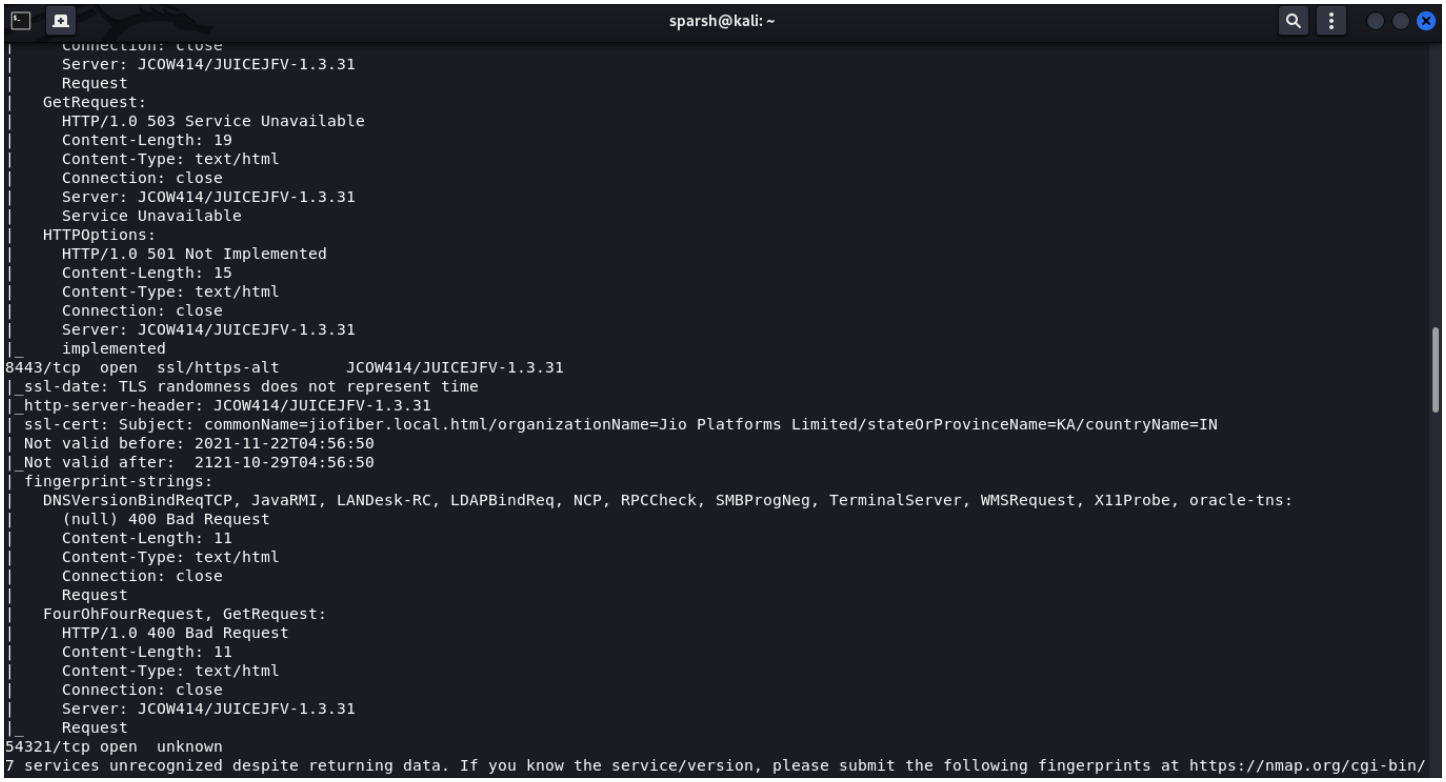
- Services running: HTTP, SSL, UPNP, SIP

- Certificate issues and outdated protocols observed

Screenshots:


sparsh@kali: ~
sparsh@kali:~$ sudo nmap -p- -A 192.168.29.1
[sudo] password for sparsh:
Starting Nmap 7.95 (https://nmap.org) at 2025-05-19 19:46 IST
Nmap scan report for 192.168.29.1
Host is up (0.0026s latency).
Not shown: 65313 filtered tcp ports (no-response), 213 closed tcp ports (reset)
PORT STATE SERVICE VERSION
80/tcp open http lighttpd
|_http-server-header: Web Server
443/tcp open ssl/http lighttpd
| ssl-cert: Subject: commonName=RILSELFCERT/organizationName=Reliance Jio Infocomm Limited
| Not valid before: 2018-06-27T00:00:04
|_Not valid after: 2028-06-24T00:00:04
|_ssl-date: TLS randomness does not represent time
1900/tcp open upnp
| fingerprint-strings:
| FourOhFourRequest, GetRequest:
| HTTP/1.1 404 Not Found
| Server: Linux UPnP/1.0 DLNADOC/1.50 AccessTwine/1.0-RAS Device/reliance.reliance
| Content-Length: 48
| Content-Type: text/html
| <HTML><BODY><H1>404 Not Found</H1></BODY></HTML>
| HTTPOptions:
| HTTP/1.1 405 Method Not Allowed
| Server: Linux UPnP/1.0 DLNADOC/1.50 AccessTwine/1.0-RAS Device/reliance.reliance
| Content-Length: 57
| Content-Type: text/html
|_ <HTML><BODY><H1>405 Method Not Allowed</H1></BODY></HTML>
2872/tcp open upnp
| fingerprint-strings:
| FourOhFourRequest, GetRequest:
| HTTP/1.1 404 Not Found
| Server: Linux UPnP/1.0 DLNADOC/1.50 AccessTwine/1.0-RAS Device/reliance.reliance
| Content-Length: 48
| Content-Type: text/html
| <HTML><BODY><H1>404 Not Found</H1></BODY></HTML>
| HTTPOptions:
| HTTP/1.1 405 Method Not Allowed
| Server: Linux UPnP/1.0 DLNADOC/1.50 AccessTwine/1.0-RAS Device/reliance.reliance


sparsh@kali: ~
5068/tcp open ssl/sip   JCOW414/JUICEJFV-1.3.31 (Status: 200 OK)
| ssl-cert: Subject: commonName=jiofiber.local.html/organizationName=Jio Platforms Limited/stateOrProvinceName=KA/countryName=IN
| Not valid before: 2021-11-22T04:56:50
|_Not valid after: 2121-10-29T04:56:50
|_ssl-date: TLS randomness does not represent time
| fingerprint-strings:
| SIPOptions:
| SIP/2.0 200 OK
| Via: SIP/2.0/TCP nm;branch=foo;received=192.168.29.96
| Contact: <sip:192.168.29.1:5068;transport=tls>;video
| <sip:nm2@nm2>;tag=d5f5dc13
| From: <sip:nm@nm>;tag=root
| Call-ID: 50000
| CSeq: 42 OPTIONS
| Accept: application/sdp, multipart/mixed, multipart/signed, multipart/alternative
| Accept-Language: en
| Allow: REGISTER, INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, NOTIFY, SUBSCRIBE, UPDATE, PRACK, INFO, MESSAGE
| Content-Type: application/sdp
| Supported: path, replaces, timer, norefersub
| User-Agent: JCOW414/JUICEJFV-1.3.31
| Content-Length: 1506
| 3757745984 3757745984 IN IP6 2405:201:6809:4000:5577:82b4:362c:d4bb
| s=HGW session
| a=X-nat:0
| c=IN IP6 2405:201:6809:4000:5577:82b4:362c:d4bb
| m=audio 14566 RTP/AVP 104 103 101 102
| b=TIAS:24400
| b=AS:49
| b=RS:607
| b=RR:1816
| a=sendrecv
| a=rtpmap:104 AMR-WB/16000
| a=rtpmap:103 AMR/8000
|_   a=rtpmap:101 telephone-eve
7443/tcp open ssl/oracleas-https?
|_ssl-date: TLS randomness does not represent time
| fingerprint-strings:
| FourOhFourRequest:


sparsh@kali: ~
| Connection: close
| Server: JCOW414/JUICEJFV-1.3.31
| Request
| GetRequest:
| HTTP/1.0 503 Service Unavailable
| Content-Length: 19
| Content-Type: text/html
| Connection: close
| Server: JCOW414/JUICEJFV-1.3.31
| Service Unavailable
| HTTPOptions:
| HTTP/1.0 501 Not Implemented
| Content-Length: 15
| Content-Type: text/html
| Connection: close
| Server: JCOW414/JUICEJFV-1.3.31
|_   implemented
8443/tcp open ssl/https-alt   JCOW414/JUICEJFV-1.3.31
|_ssl-date: TLS randomness does not represent time
|_http-server-header: JCOW414/JUICEJFV-1.3.31
| ssl-cert: Subject: commonName=jiofiber.local.html/organizationName=Jio Platforms Limited/stateOrProvinceName=KA/countryName=IN
| Not valid before: 2021-11-22T04:56:50
|_Not valid after: 2121-10-29T04:56:50
| fingerprint-strings:
| DNSVersionBindReqTCP, JavaRMI, LANDesk-RC, LDAPBindReq, NCP, RPCCheck, SMBProgNeg, TerminalServer, WMSRequest, X11Probe, oracle-tns:
| (null) 400 Bad Request
| Content-Length: 11
| Content-Type: text/html
| Connection: close
| Request
| FourOhFourRequest, GetRequest:
| HTTP/1.0 400 Bad Request
| Content-Length: 11
| Content-Type: text/html
| Connection: close
| Server: JCOW414/JUICEJFV-1.3.31
|_   Request
54321/tcp open unknown
7 services unrecognized despite returning data. If you know the service/version, please submit the following fingerprints at https://nmap.org/cgi-bin/

3. Unauthorized Device Scan

Methodology:

- Logged into router at 192.168.29.1 and reviewed connected devices

- Cross-checked with: nmap -sn 192.168.29.0/24

Findings:

- Known devices: 6 (phones, laptops, TV)

- Unknown device: 1

Recommendations:

- Change Wi-Fi password

- Enable MAC filtering

- Disable WPS

- Review connected device logs weekly

4. Packet Capture Analysis with Wireshark

Methodology:

- Captured network traffic using Wireshark on the Wi-Fi interface

- Applied filters (http, telnet, dns) to identify unencrypted traffic

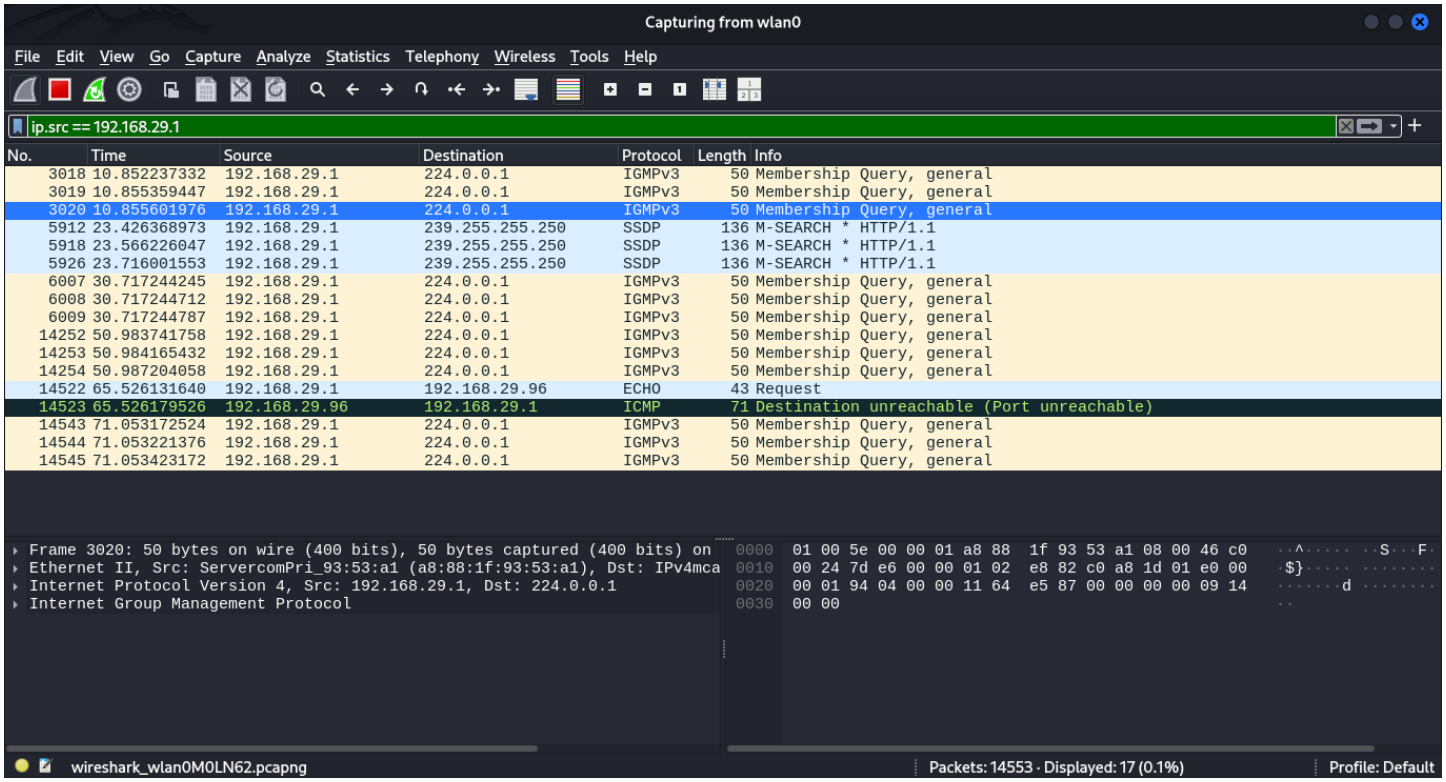
Findings:

- Detected unencrypted DNS queries

- HTTP packets visible

- 'Port Unreachable' ICMP responses seen

Screenshot:


Capturing from wlan0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip.src == 192.168.29.1
No. Time Source Destination Protocol Length Info
3018 10.852237332 192.168.29.1 224.0.0.1 IGMPv3 50 Membership Query, general
3019 10.855359447 192.168.29.1 224.0.0.1 IGMPv3 50 Membership Query, general
3020 10.855601976 192.168.29.1 224.0.0.1 IGMPv3 50 Membership Query, general
5912 23.426368973 192.168.29.1 239.255.255.250 SSDP 136 M-SEARCH * HTTP/1.1
5918 23.566226047 192.168.29.1 239.255.255.250 SSDP 136 M-SEARCH * HTTP/1.1
5926 23.716001553 192.168.29.1 239.255.255.250 SSDP 136 M-SEARCH * HTTP/1.1
6007 30.717244245 192.168.29.1 224.0.0.1 IGMPv3 50 Membership Query, general
6008 30.717244712 192.168.29.1 224.0.0.1 IGMPv3 50 Membership Query, general
6009 30.717244787 192.168.29.1 224.0.0.1 IGMPv3 50 Membership Query, general
14252 50.983741758 192.168.29.1 224.0.0.1 IGMPv3 50 Membership Query, general
14253 50.984165432 192.168.29.1 224.0.0.1 IGMPv3 50 Membership Query, general
14254 50.987204058 192.168.29.1 224.0.0.1 IGMPv3 50 Membership Query, general
14522 65.526131640 192.168.29.1 192.168.29.96 ECHO 43 Request
14523 65.526179526 192.168.29.96 192.168.29.1 ICMP 71 Destination unreachable (Port unreachable)
14543 71.053172524 192.168.29.1 224.0.0.1 IGMPv3 50 Membership Query, general
14544 71.053221376 192.168.29.1 224.0.0.1 IGMPv3 50 Membership Query, general
14545 71.053423172 192.168.29.1 224.0.0.1 IGMPv3 50 Membership Query, general
Frame 3020: 50 bytes on wire (400 bits), 50 bytes captured (400 bits) on
Ethernet II, Src: ServercomPri_93:53:a1 (a8:88:1f:93:53:a1), Dst: IPv4mca
Internet Protocol Version 4, Src: 192.168.29.1, Dst: 224.0.0.1
Internet Group Management Protocol
0000 01 00 5e 00 00 01 a8 88 1f 93 53 a1 08 00 46 c0
0010 00 24 7d e6 00 00 01 02 e8 82 c0 a8 1d 01 e0 00
0020 00 01 94 04 00 00 11 64 e5 87 00 00 00 00 09 14
0030 00 00
wireshark_wlan0M0LN62.pcapng
Packets: 14553 · Displayed: 17 (0.1%)
Profile: Default

Conclusion

The assessment of the Wi-Fi network at IP 192.168.29.1 uncovered:

- Moderate password strength with room for improvement

- Insecure services running (TELNET, HTTP, outdated SSL certs)

- One unauthorized device detected

Taking action on these recommendations will significantly improve security.