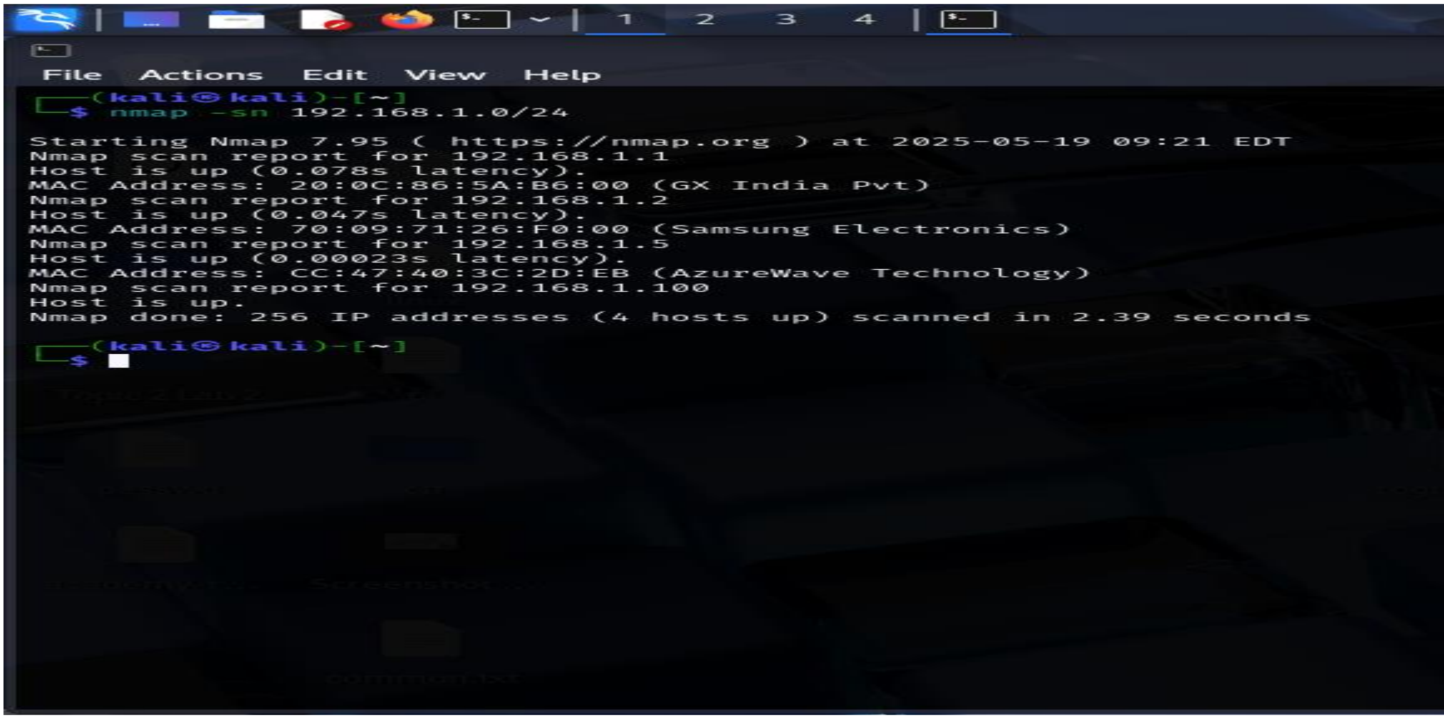
TASK-3 SECURING HOME WIFI-NETWORK

This report documents the security assessment of my personal Wi-Fi network, focusing on identifying weak passwords, open ports, and unauthorized devices. The assessment was conducted using the router's admin panel and `nmap` scanning from a system within the network



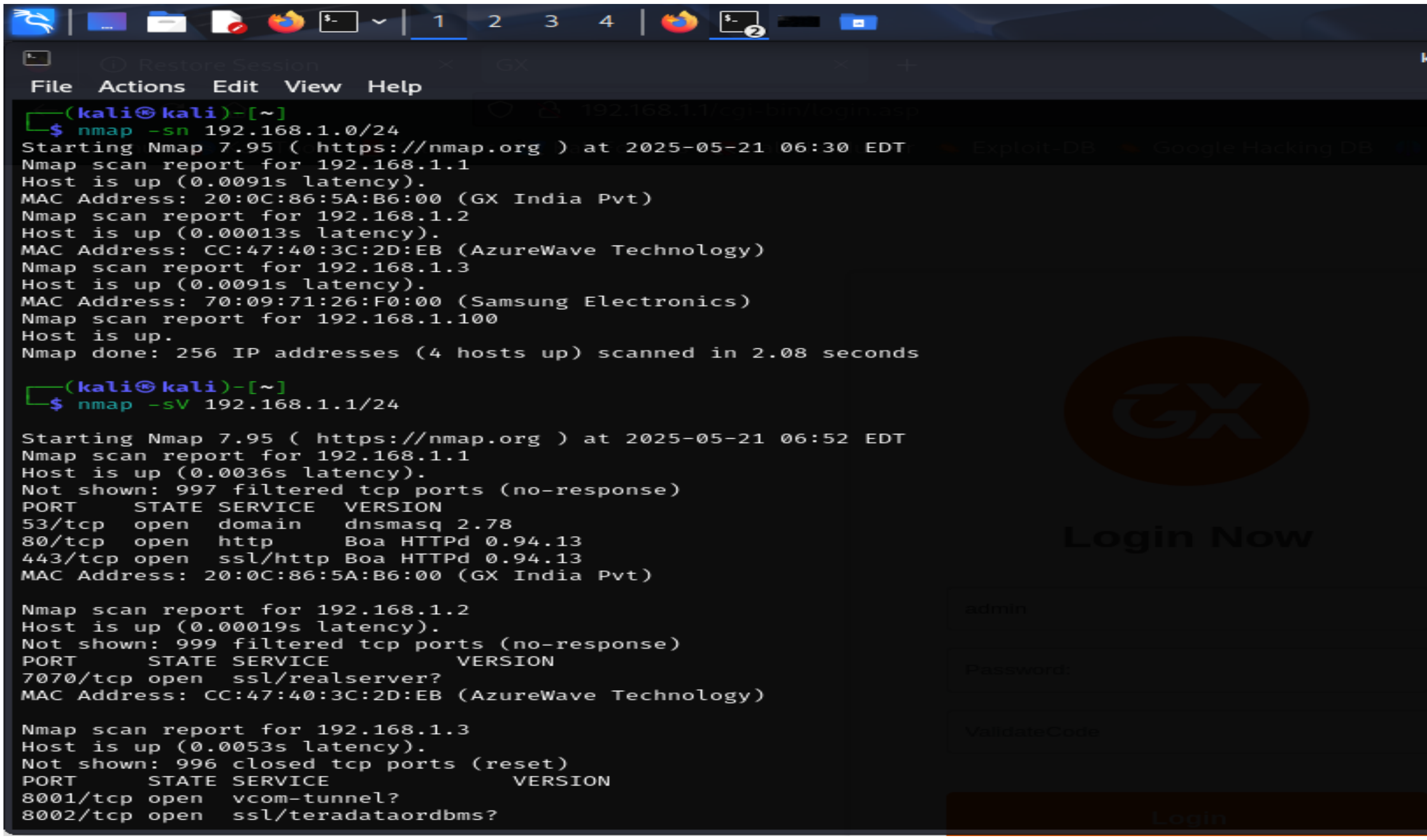
```
┌──(kali㉿kali)-[~]
└─$ nmap -sn 192.168.1.0/24

Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-19 09:21 EDT
Nmap scan report for 192.168.1.1
Host is up (0.078s latency).
MAC Address: 20:0C:86:5A:B6:00 (GX India Pvt)
Nmap scan report for 192.168.1.2
Host is up (0.047s latency).
MAC Address: 70:09:71:26:F0:00 (Samsung Electronics)
Nmap scan report for 192.168.1.5
Host is up (0.00023s latency).
MAC Address: CC:47:40:3C:2D:EB (AzureWave Technology)
Nmap scan report for 192.168.1.100
Host is up.
Nmap done: 256 IP addresses (4 hosts up) scanned in 2.39 seconds

┌──(kali㉿kali)-[~]
└─$ 
```

2. Network Setup

Item	Detail
Router IP	192.168.1.1
My Device IP	192.168.1.100
Router Brand	GX Titanium-2122A
Wi-Fi Encryption	WPA-PSK/WPA2-PSK
WPS Status	Disabled

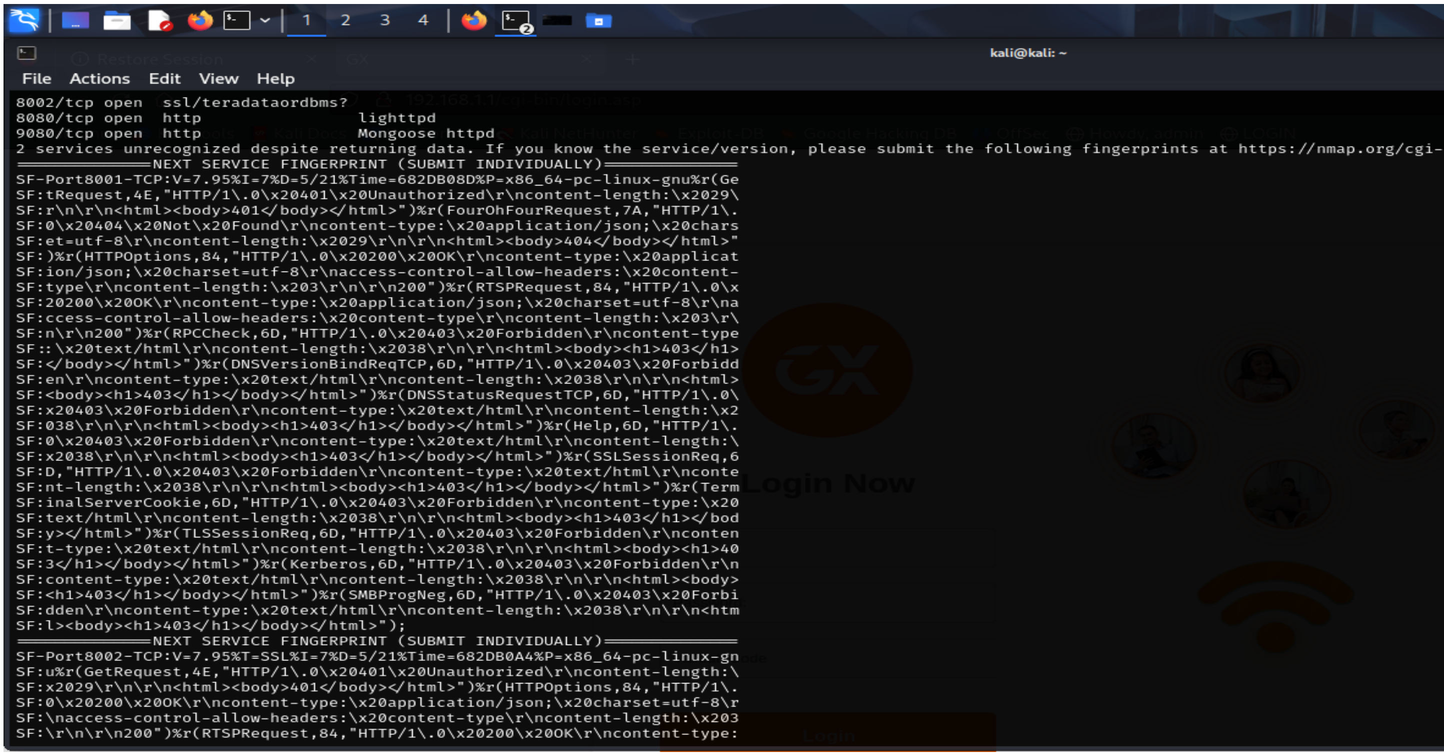
Encryption Used:WPA2-PSK (AES) Secure
Wi-Fi Password Strength:Verified to be strong
Contains uppercase, lowercase, numbers, and symbols
WPS: Was enabled Now **disabled** to prevent brute-force attacks

Recommendation: Change the Wi-Fi password regularly and use a mix of characters.

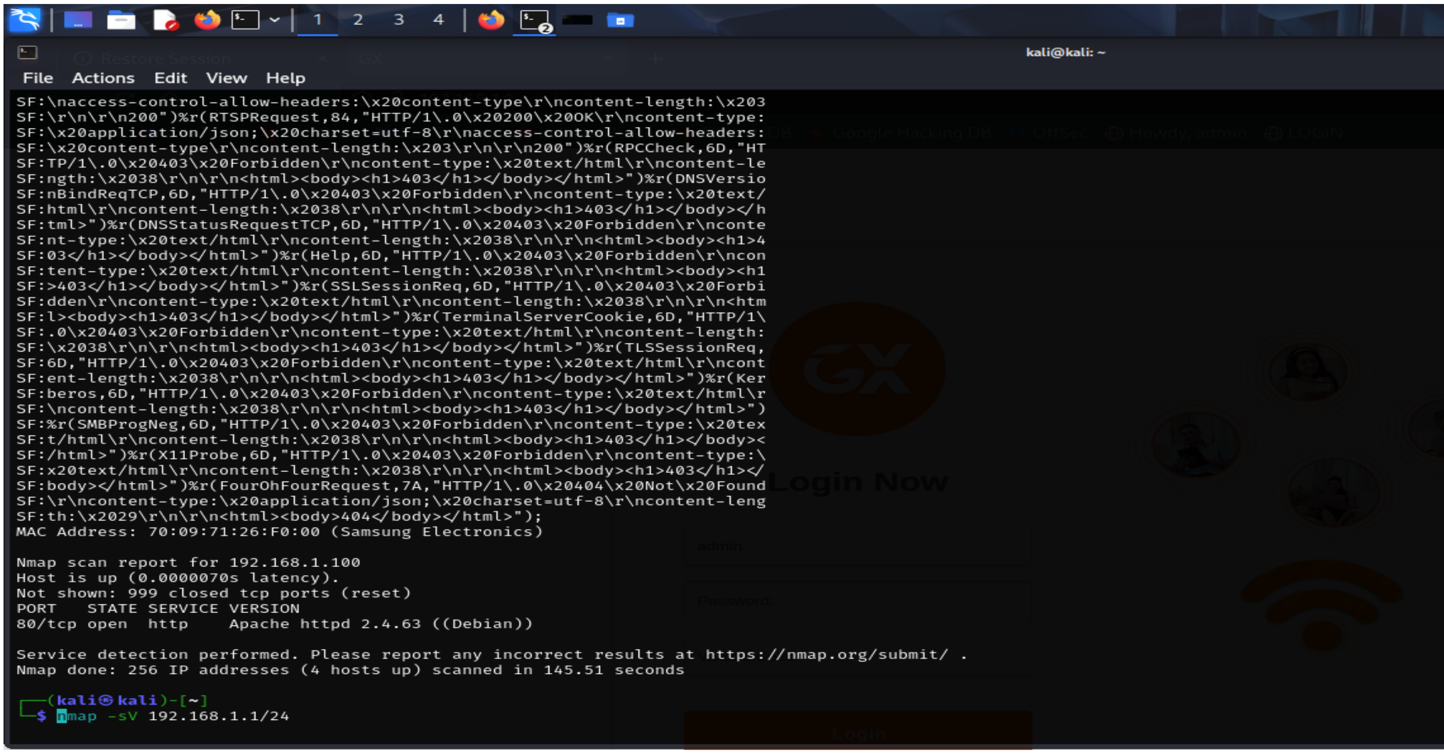


```
┌──(kali㉿kali)-[~]
└─$ nmap -sn 192.168.1.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-21 06:30 EDT
Nmap scan report for 192.168.1.1
Host is up (0.0091s latency).
MAC Address: 20:0C:86:5A:B6:00 (GX India Pvt)
Nmap scan report for 192.168.1.2
Host is up (0.00013s latency).
MAC Address: CC:47:40:3C:2D:EB (AzureWave Technology)
Nmap scan report for 192.168.1.3
Host is up (0.0091s latency).
MAC Address: 70:09:71:26:F0:00 (Samsung Electronics)
Nmap scan report for 192.168.1.100
Host is up.
Nmap done: 256 IP addresses (4 hosts up) scanned in 2.08 seconds

┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.1.1/24

Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-21 06:52 EDT
Nmap scan report for 192.168.1.1
Host is up (0.0036s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT     STATE SERVICE  VERSION
53/tcp   open  domain   dnsmasq 2.78
80/tcp   open  http     Boa HTTPd 0.94.13
443/tcp  open  ssl/http Boa HTTPd 0.94.13
MAC Address: 20:0C:86:5A:B6:00 (GX India Pvt)

Nmap scan report for 192.168.1.2
Host is up (0.00019s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT      STATE SERVICE          VERSION
7070/tcp open  ssl/realserver?
MAC Address: CC:47:40:3C:2D:EB (AzureWave Technology)

Nmap scan report for 192.168.1.3
Host is up (0.0053s latency).
Not shown: 996 closed tcp ports (reset)
PORT      STATE SERVICE              VERSION
8001/tcp open  vcom-tunnel?
8002/tcp open  ssl/teradataordbms?
```

Command: nmap -sV 192.168.1.1/24 used to find open ports, services, versions, fingerprints.



```
8002/tcp open  ssl/teradataordbms?
8080/tcp open  http                  lighttpd
9080/tcp open  http                  Mongoose httpd
2 services unrecognized despite returning data. If you know the service/version, please submit the following fingerprints at https://nmap.org/cgi-
==================NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==================
SF-Port8001-TCP:V=7.95%I=7%D=5/21%Time=682DB08D%P=x86_64-pc-linux-gnu%r(Ge
SF:tRequest,4E,"HTTP/1\.0\x20401\x20Unauthorized\r\ncontent-length:\x2029\
SF:r\n\r\n<html><body>401</body></html>")%r(FourOhFourRequest,7A,"HTTP/1\.
SF:0\x20404\x20Not\x20Found\r\ncontent-type:\x20application/json;\x20chars
SF:et=utf-8\r\ncontent-length:\x2029\r\n\r\n<html><body>404</body></html>"
SF:)%r(HTTPOptions,84,"HTTP/1\.0\x20200\x20OK\r\ncontent-type:\x20applicat
SF:ion/json;\x20charset=utf-8\r\naccess-control-allow-headers:\x20content-
SF:type\r\ncontent-length:\x203\r\n\r\n200")%r(RTSPRequest,84,"HTTP/1\.0\x
SF:20200\x20OK\r\ncontent-type:\x20application/json;\x20charset=utf-8\r\na
SF:ccess-control-allow-headers:\x20content-type\r\ncontent-length:\x203\r\
SF:n\r\n200")%r(RPCCheck,6D,"HTTP/1\.0\x20403\x20Forbidden\r\ncontent-type
SF::\x20text/html\r\ncontent-length:\x2038\r\n\r\n<html><body><h1>403</h1>
SF:</body></html>")%r(DNSVersionBindReqTCP,6D,"HTTP/1\.0\x20403\x20Forbidd
SF:en\r\ncontent-type:\x20text/html\r\ncontent-length:\x2038\r\n\r\n<html>
SF:<body><h1>403</h1></body></html>")%r(DNSStatusRequestTCP,6D,"HTTP/1\.0\
SF:x20403\x20Forbidden\r\ncontent-type:\x20text/html\r\ncontent-length:\x2
SF:038\r\n\r\n<html><body><h1>403</h1></body></html>")%r(Help,6D,"HTTP/1\.
SF:0\x20403\x20Forbidden\r\ncontent-type:\x20text/html\r\ncontent-length:\
SF:x2038\r\n\r\n<html><body><h1>403</h1></body></html>")%r(SSLSessionReq,6
SF:D,"HTTP/1\.0\x20403\x20Forbidden\r\ncontent-type:\x20text/html\r\nconte
SF:nt-length:\x2038\r\n\r\n<html><body><h1>403</h1></body></html>")%r(Term
SF:inalServerCookie,6D,"HTTP/1\.0\x20403\x20Forbidden\r\ncontent-type:\x20
SF:text/html\r\ncontent-length:\x2038\r\n\r\n<html><body><h1>403</h1></bod
SF:y></html>")%r(TLSSessionReq,6D,"HTTP/1\.0\x20403\x20Forbidden\r\nconten
SF:t-type:\x20text/html\r\ncontent-length:\x2038\r\n\r\n<html><body><h1>40
SF:3</h1></body></html>")%r(Kerberos,6D,"HTTP/1\.0\x20403\x20Forbidden\r\n
SF:content-type:\x20text/html\r\ncontent-length:\x2038\r\n\r\n<html><body>
SF:<h1>403</h1></body></html>")%r(SMBProgNeg,6D,"HTTP/1\.0\x20403\x20Forbi
SF:dden\r\ncontent-type:\x20text/html\r\ncontent-length:\x2038\r\n\r\n<htm
SF:l><body><h1>403</h1></body></html>");
==================NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==================
SF-Port8002-TCP:V=7.95%T=SSL%I=7%D=5/21%Time=682DB0A4%P=x86_64-pc-linux-gn
SF:u%r(GetRequest,4E,"HTTP/1\.0\x20401\x20Unauthorized\r\ncontent-length:\
SF:x2029\r\n\r\n<html><body>401</body></html>")%r(HTTPOptions,84,"HTTP/1\.
SF:0\x20200\x20OK\r\ncontent-type:\x20application/json;\x20charset=utf-8\r
SF:\naccess-control-allow-headers:\x20content-type\r\ncontent-length:\x203
SF:\r\n\r\n200")%r(RTSPRequest,84,"HTTP/1\.0\x20200\x20OK\r\ncontent-type:
```



```
SF:\naccess-control-allow-headers:\x20content-type\r\ncontent-length:\x203
SF:\r\n\r\n200")%r(RTSPRequest,84,"HTTP/1\.0\x20200\x20OK\r\ncontent-type:
SF:\x20application/json;\x20charset=utf-8\r\naccess-control-allow-headers:
SF:\x20content-type\r\ncontent-length:\x203\r\n\r\n200")%r(RPCCheck,6D,"HT
SF:TP/1\.0\x20403\x20Forbidden\r\ncontent-type:\x20text/html\r\ncontent-le
SF:ngth:\x2038\r\n\r\n<html><body><h1>403</h1></body></html>")%r(DNSVersio
SF:nBindReqTCP,6D,"HTTP/1\.0\x20403\x20Forbidden\r\ncontent-type:\x20text/
SF:html\r\ncontent-length:\x2038\r\n\r\n<html><body><h1>403</h1></body></h
SF:tml>")%r(DNSStatusRequestTCP,6D,"HTTP/1\.0\x20403\x20Forbidden\r\nconte
SF:nt-type:\x20text/html\r\ncontent-length:\x2038\r\n\r\n<html><body><h1>4
SF:03</h1></body></html>")%r(Help,6D,"HTTP/1\.0\x20403\x20Forbidden\r\ncon
SF:tent-type:\x20text/html\r\ncontent-length:\x2038\r\n\r\n<html><body><h1
SF:>403</h1></body></html>")%r(SSLSessionReq,6D,"HTTP/1\.0\x20403\x20Forbi
SF:dden\r\ncontent-type:\x20text/html\r\ncontent-length:\x2038\r\n\r\n<htm
SF:l><body><h1>403</h1></body></html>")%r(TerminalServerCookie,6D,"HTTP/1\
SF:.0\x20403\x20Forbidden\r\ncontent-type:\x20text/html\r\ncontent-length:
SF:\x2038\r\n\r\n<html><body><h1>403</h1></body></html>")%r(TLSSessionReq,
SF:6D,"HTTP/1\.0\x20403\x20Forbidden\r\ncontent-type:\x20text/html\r\ncont
SF:ent-length:\x2038\r\n\r\n<html><body><h1>403</h1></body></html>")%r(Ker
SF:beros,6D,"HTTP/1\.0\x20403\x20Forbidden\r\ncontent-type:\x20text/html\r
SF:\ncontent-length:\x2038\r\n\r\n<html><body><h1>403</h1></body></html>")
SF:%r(SMBProgNeg,6D,"HTTP/1\.0\x20403\x20Forbidden\r\ncontent-type:\x20tex
SF:t/html\r\ncontent-length:\x2038\r\n\r\n<html><body><h1>403</h1></body><
SF:/html>")%r(X11Probe,6D,"HTTP/1\.0\x20403\x20Forbidden\r\ncontent-type:\
SF:x20text/html\r\ncontent-length:\x2038\r\n\r\n<html><body><h1>403</h1></
SF:body></html>")%r(FourOhFourRequest,7A,"HTTP/1\.0\x20404\x20Not\x20Found
SF:\r\ncontent-type:\x20application/json;\x20charset=utf-8\r\ncontent-leng
SF:th:\x2029\r\n\r\n<html><body>404</body></html>");
MAC Address: 70:09:71:26:F0:00 (Samsung Electronics)

Nmap scan report for 192.168.1.100
Host is up (0.0000070s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.63 ((Debian))

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (4 hosts up) scanned in 145.51 seconds

┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.1.1/24
```

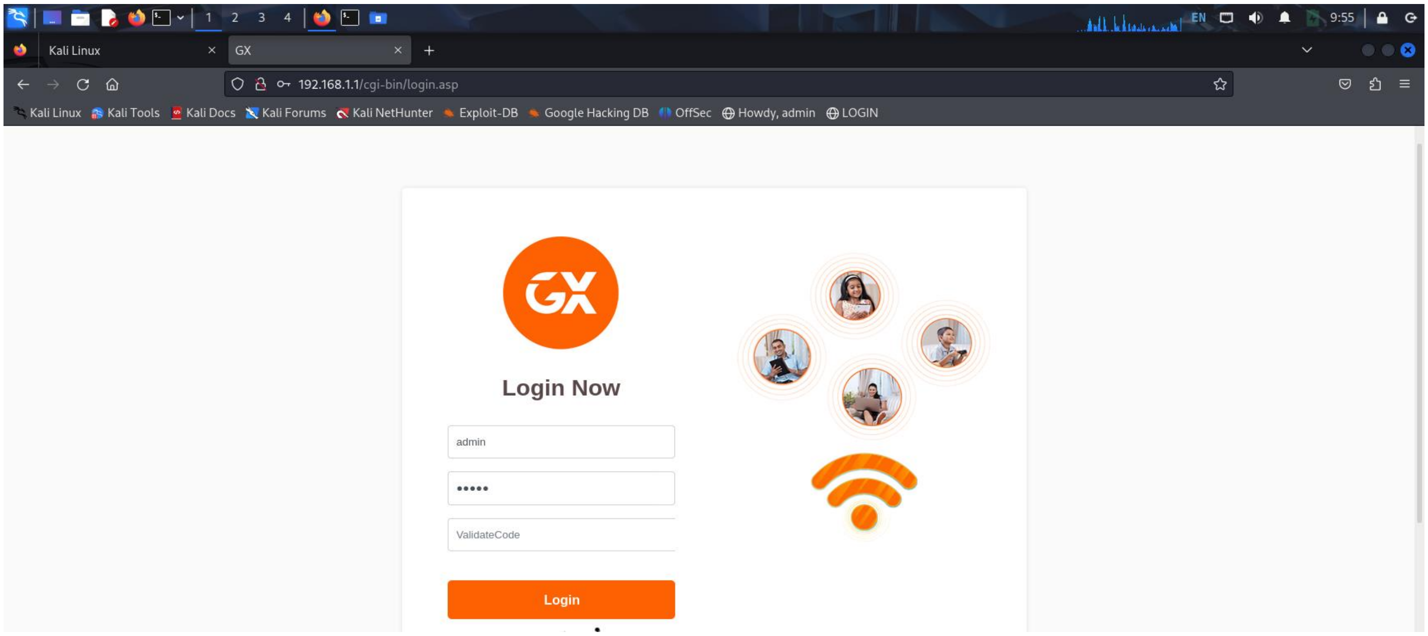
IP Address	MAC Address	Vendor/Device	known
192.168.1.1	20:0C:86:5A:B6:00	GX India Pvt (Router)	YES
192.168.1.2	CC:47:40:3C:2D:EB	AzureWave Technology	Not Confirmed
192.168.1.3	| 70:09:71:26:F0:00	Samsung Electronics	Possibly Tv
192.168.1.100	-----	Debian Server	YES

Action Taken:
- All devices cross-verified.

- Changed Wi-Fi password to secure network .
- Suspicious devices noted for follow-up.

Recommendation:Periodically monitor the connected devices list in the router and enable MAC address filtering if needed.

After scanning go to http://192.168.1.1 for router device then we can see the information.

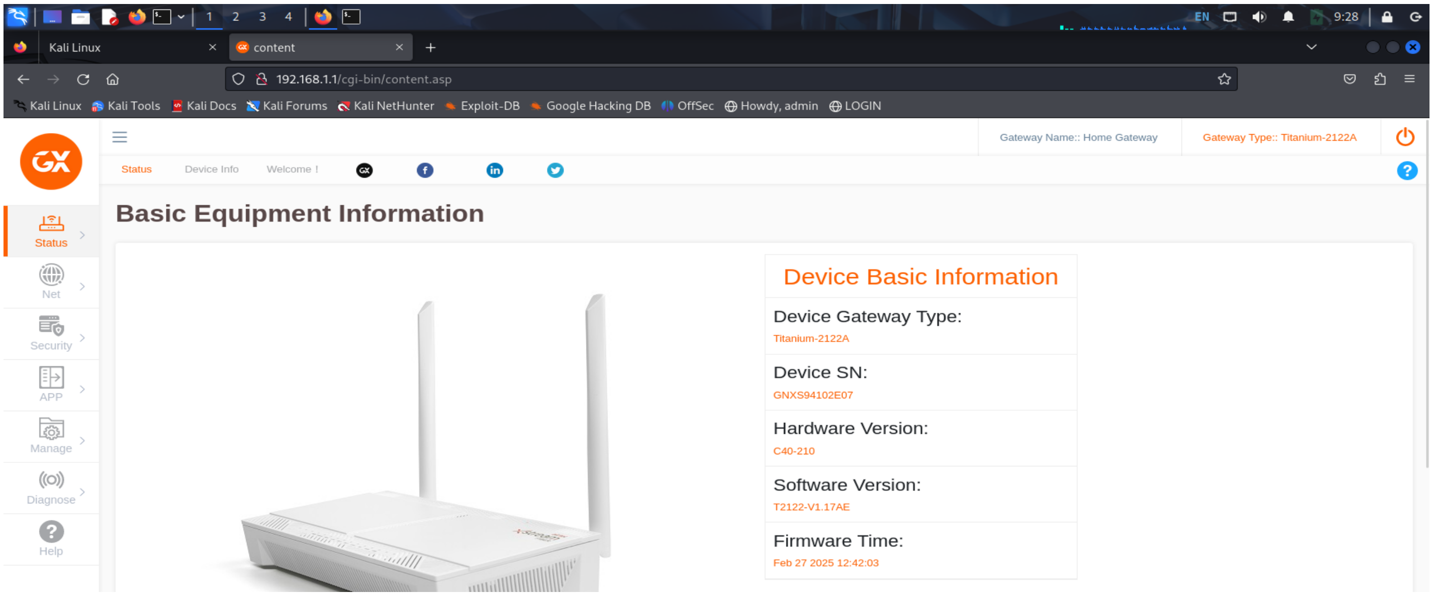


Login Now

admin

•••••

ValidateCode



Gateway Name:: Home Gateway

Gateway Type:: Titanium-2122A

Basic Equipment Information

Device Basic Information

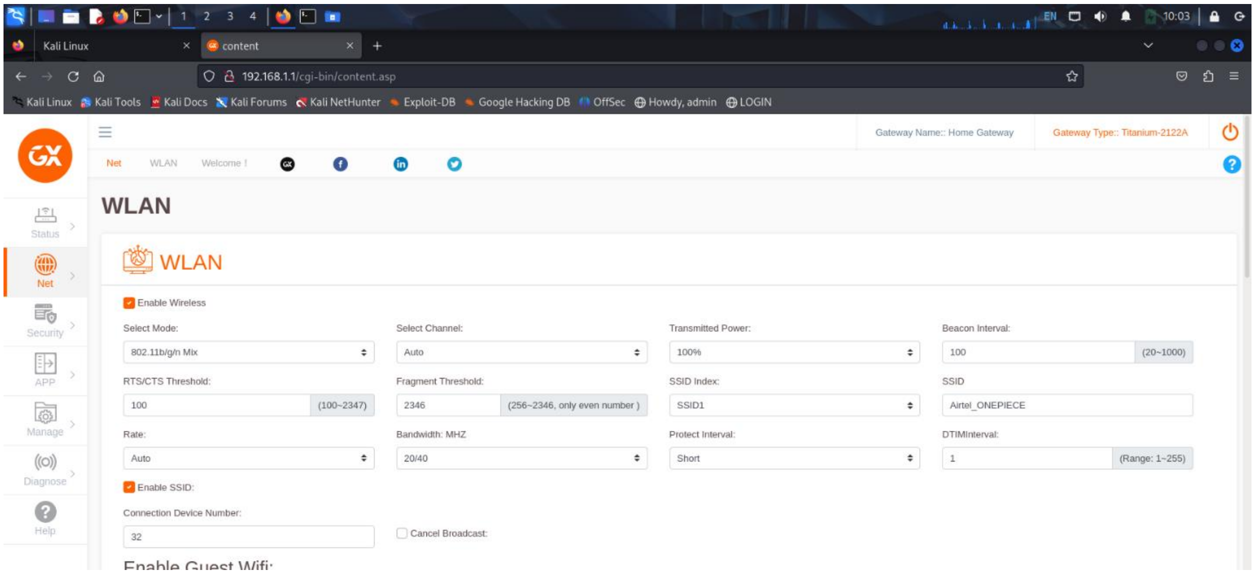
Device Gateway Type:
Titanium-2122A

Device SN:
GNXS94102E07

Hardware Version:
C40-210

Software Version:
T2122-V1.17AE

Firmware Time:
Feb 27 2025 12:42:03



Gateway Name:: Home Gateway

Gateway Type:: Titanium-2122A

WLAN

WLAN

☑ Enable Wireless

Select Mode: 802.11b/g/n Mix

Select Channel: Auto

Transmitted Power: 100%

Beacon Interval: 100 (20~1000)

RTS/CTS Threshold: 100 (100~2347)

Fragment Threshold: 2346 (256~2346, only even number)

SSID Index: SSID1

SSID: Airtel_ONEPIECE

Rate: Auto

Bandwidth: MHZ 20/40

Protect Interval: Short

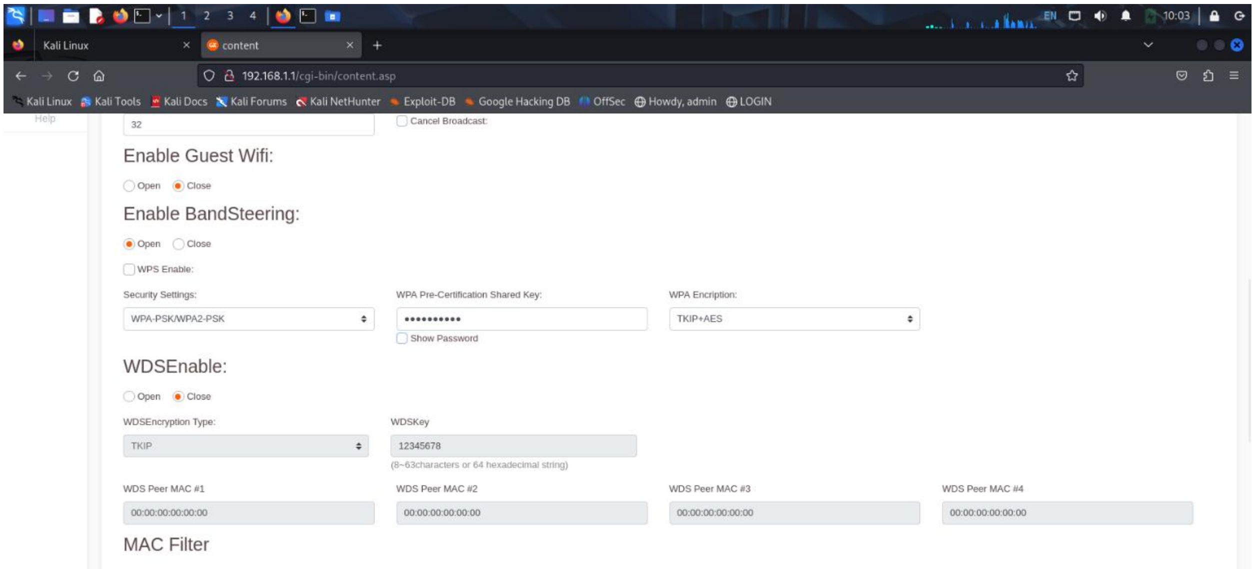
DTIMInterval: 1 (Range: 1~255)

☑ Enable SSID:

Connection Device Number: 32

□ Cancel Broadcast:

Enable Guest Wifi:



32

□ Cancel Broadcast:

Enable Guest Wifi:

○ Open ● Close

Enable BandSteering:

● Open ○ Close

□ WPS Enable:

Security Settings: WPA-PSK/WPA2-PSK

WPA Pre-Certification Shared Key: ••••••••••

□ Show Password

WPA Encription: TKIP+AES

WDSEnable:

○ Open ● Close

WDSEncryption Type: TKIP

WDSKey: 12345678

(8~63characters or 64 hexadecimal string)

WDS Peer MAC #1: 00:00:00:00:00:00

WDS Peer MAC #2: 00:00:00:00:00:00

WDS Peer MAC #3: 00:00:00:00:00:00

WDS Peer MAC #4: 00:00:00:00:00:00

MAC Filter

Vulnerabilities

The router is running Boa HTTPd 0.94.13, which is known to have multiple security flaws, including remote code execution vulnerabilities.

Some devices were detected that you couldn't identify confidently — could be neighbors or unauthorized access

Devices running services like HTTP, FTP, or Telnet on default ports can be discovered and exploited.

WPS allows easy pairing of devices but can be brute-forced using tools like Reaver. Many routers have vulnerable WPS implementations

Recommendations

Minimum 12 characters, mix of letters, numbers, and symbols. Avoid using names or birth years.

Prevent brute-force attacks through PIN-based authentication.

Use the router’s admin panel to review devices and flag suspicious ones

Isolate smart TVs, bulbs, and other IoT devices to a separate network to reduce risk if one gets compromised.

Conclusion

This Wi-Fi security assessment helped identify potential vulnerabilities in the home network, including outdated web servers and unfamiliar connected devices. Appropriate action was taken to improve security by strengthening the password, disabling WPS, and reviewing open ports.

The network is now significantly more secure and monitored.