GRL
Connecting the World

graniteriverlabs.com

Wi-Fi Network Analysis Tools

Sanjay K Sharma

Associate Director, Cyber Security Services. GRL

Wi-Fi Security Concerns

- Wireless networks are easy to set up and inexpensive.
- You can access the network from anywhere within the coverage area.

- But other side of the advantages, there are some security concerns as well.

Sensitive Data Confidentiality

Unauthorized Access

Cyberattacks

Illegal Activities

IoT Device Vulnerabilities

Personal Privacy Disclosure

Disrupt Business Continuity

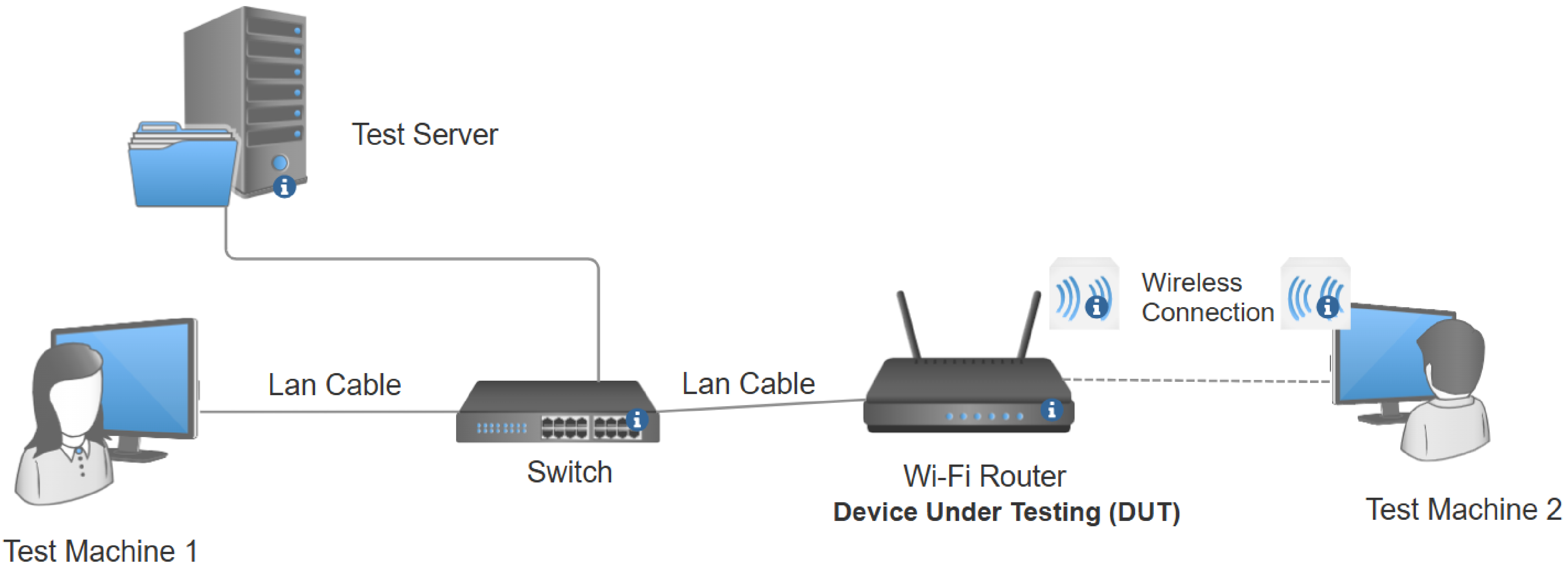
Wi-Fi Network security is important? Yes………Yes…………Yes

Addressing threats like unauthorized access, data theft, and cyberattacks **DoT** envisages to implement the mandatory testing and certification in respect of Security Requirements through a Scheme titled ‘**Communication Security Certification Scheme’ (ComSec)** that every telecom equipment must undergo mandatory testing and certification prior to sale, import or use in India. The Testing and Certification framework requires that the telecom equipment meets the essential requirements called **Indian Telecom Security Assurance Requirements (ITSAR)** for every Telecom equipment.

The types of devices for which Wi-Fi ITSAR is applicable:

- Wi-Fi Routers,
- Wi-Fi Modems,
- Broadband Modems with Wi-Fi facility,
- Cable Modems with Wi-Fi facility,
- FTTH ONTs with Wi-Fi facility, and
- Wi-Fi Data cards which provide Wi-Fi facility with backend 2G / 3G / 4G connectivity.
- Cloud hosted, external controller-based APs

Wi-Fi Network Analysis Tools



Wi-Fi Network Test Bed

Pre-Conditions :

- High Privilege Credentials
- Software Hash Verification
- CLI Mode Access to DUT (Recommended SSH)
- Test Machine with Wi-Fi feature or Wi-Fi Adapter
- Configuration Documents
- Necessary Undertakings / Declarations

For Traffic Analysis & Secure Communication Validation

Wireshark -Wireshark is a powerful tool for capturing and analyzing network packets. It can be used for testing the integrity and encryption of management traffic (e.g., HTTPS, SSHv2) as well as ensuring cryptographic-based secure communication.

Installation: Available for Windows, macOS, and Linux. Download from Wireshark.org.

Usage:

1. Open Wireshark and select the network interface (Wi-Fi or Ethernet) to capture traffic.
2. Set filters to capture specific traffic:
   - -For HTTPS traffic: tcp.port == 443
   - -For SSH traffic: tcp.port == 22
   - -For IPsec traffic: esp
3. Start capturing and interact with your CPE's web interface or other management interfaces.
4. Analyze packets to ensure encryption:
   - -Look for encryption indicators (e.g., TLS handshake, IPsec ESP encryption).
   - -Ensure that sensitive data (passwords, keys) are not transmitted in plaintext.

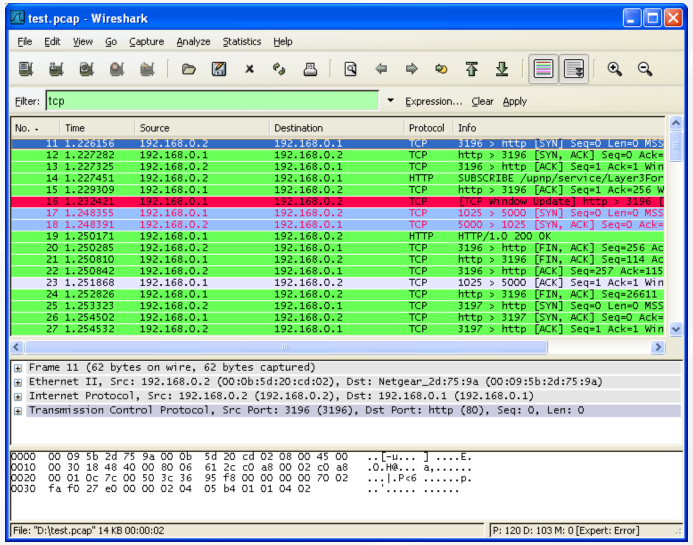
ITSAR Sections:

1.1.2: Management Traffic Protection.

1.6.1: Cryptographic-based Secure Communication.

1.7.1: Traffic Filtering – Network Level.

Wireshark User's Guide: https://www.wireshark.org/docs/wsug_html/


test.pcap - Wireshark
File Edit View Go Capture Analyze Statistics Help
Expression... Clear Apply

Filter: tcp

No.	Time	Source	Destination	Protocol	Info
11	1.226156	192.168.0.2	192.168.0.1	TCP	3196 > http [SYN] Seq=0 Len=0 MSS
12	1.227282	192.168.0.1	192.168.0.2	TCP	http > 3196 [SYN, ACK] Seq=0 Ack=
13	1.227325	192.168.0.2	192.168.0.1	TCP	3196 > http [ACK] Seq=1 Ack=1 Win
14	1.227451	192.168.0.2	192.168.0.1	HTTP	SUBSCRIBE /upnp/service/Layer3For
15	1.229309	192.168.0.1	192.168.0.2	TCP	http > 3196 [ACK] Seq=1 Ack=256 W
16	1.232421	192.168.0.1	192.168.0.2	TCP	[TCP Window Update] http > 3196 [
17	1.248355	192.168.0.1	192.168.0.2	TCP	1025 > 5000 [SYN] Seq=0 Len=0 MSS
18	1.248391	192.168.0.2	192.168.0.1	TCP	5000 > 1025 [SYN, ACK] Seq=0 Ack=
19	1.250171	192.168.0.1	192.168.0.2	HTTP	HTTP/1.0 200 OK
20	1.250285	192.168.0.2	192.168.0.1	TCP	3196 > http [FIN, ACK] Seq=256 Ac
21	1.250810	192.168.0.1	192.168.0.2	TCP	http > 3196 [FIN, ACK] Seq=114 Ac
22	1.250842	192.168.0.2	192.168.0.1	TCP	3196 > http [ACK] Seq=257 Ack=115
23	1.251868	192.168.0.1	192.168.0.2	TCP	1025 > 5000 [ACK] Seq=1 Ack=1 Win
24	1.252826	192.168.0.1	192.168.0.2	TCP	http > 3196 [FIN, ACK] Seq=26611
25	1.253323	192.168.0.2	192.168.0.1	TCP	3197 > http [SYN] Seq=0 Len=0 MSS
26	1.254502	192.168.0.1	192.168.0.2	TCP	http > 3197 [SYN, ACK] Seq=0 Ack=
27	1.254532	192.168.0.2	192.168.0.1	TCP	3197 > http [ACK] Seq=1 Ack=1 Win

```
⊞ Frame 11 (62 bytes on wire, 62 bytes captured)
⊞ Ethernet II, Src: 192.168.0.2 (00:0b:5d:20:cd:02), Dst: Netgear_2d:75:9a (00:09:5b:2d:75:9a)
⊞ Internet Protocol, Src: 192.168.0.2 (192.168.0.2), Dst: 192.168.0.1 (192.168.0.1)
⊞ Transmission Control Protocol, Src Port: 3196 (3196), Dst Port: http (80), Seq: 0, Len: 0
```

```
0000  00 09 5b 2d 75 9a 00 0b  5d 20 cd 02 08 00 45 00   ..[-u... ] ....E.
0010  00 30 18 48 40 00 80 06  61 2c c0 a8 00 02 c0 a8   .0.H@... a,......
0020  00 01 0c 7c 00 50 3c 36  95 f8 00 00 00 00 70 02   ...|.P<6 ......p.
0030  fa f0 27 e0 00 00 02 04  05 b4 01 01 04 02         ..'..... ......
```

File: "D:\test.pcap" 14 KB 00:00:02

P: 120 D: 103 M: 0 [Expert: Error]

For Traffic Analysis & Secure Communication Validation

Acrylic Wi-Fi Analyzer - helps monitor the Wi-Fi network to ensure that the default encryption standards (e.g., WPA2-PSK with AES) are being used. It also allows the user to verify whether the network is vulnerable to common Wi-Fi attacks, such as capture-decrypting, key reinstallation, and PIN detection.

Installation: Available for Windows. Download from Acrylicwifi

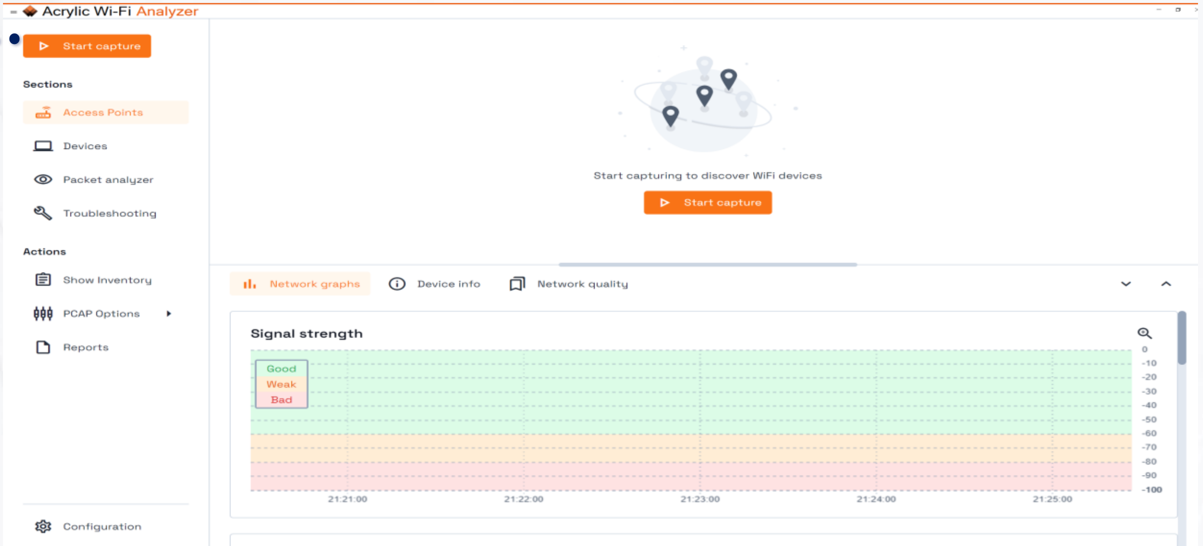
Use Cases:

1. **Wi-Fi Security Assessment (Section 1.6.2: Cryptographic Based Secure Communication on Wi-Fi Access) -** Acrylic Wi-Fi Analyzer helps monitor the Wi-Fi network to ensure that the default encryption standards (e.g., WPA2-PSK with AES) are being used.
2. **SSID Scanning and Hiding (Section 1.9.3: SSID Scanning) -** Acrylic Wi-Fi Analyzer can scan the network for available SSIDs and display associated details such as signal strength, encryption type, and more. This is important for verifying the CPE's ability to hide SSIDs as per ITSAR recommendations. The tool helps ensure that sensitive information is not disclosed and that the SSID can be hidden on user selection
3. **Traffic Analysis (Section 1.6.1: Cryptographic Based Secure Communication) -** Acrylic Wi-Fi Analyzer allows monitoring of Wi-Fi channel utilization and traffic analysis. This helps verify that secure communication protocols such as IPsec or TLS are implemented properly, and that unauthorized traffic is minimized.
4. **Traffic Filtering and Network Security (Section 1.7.1: Traffic Filtering – Network Level) -**Acrylic Wi-Fi Analyzer assists in assessing whether the CPE has implemented adequate traffic filtering. By monitoring incoming and outgoing traffic on the network, the tool helps verify if the access control list (ACL) is properly filtering packets as per the ITSAR specifications.

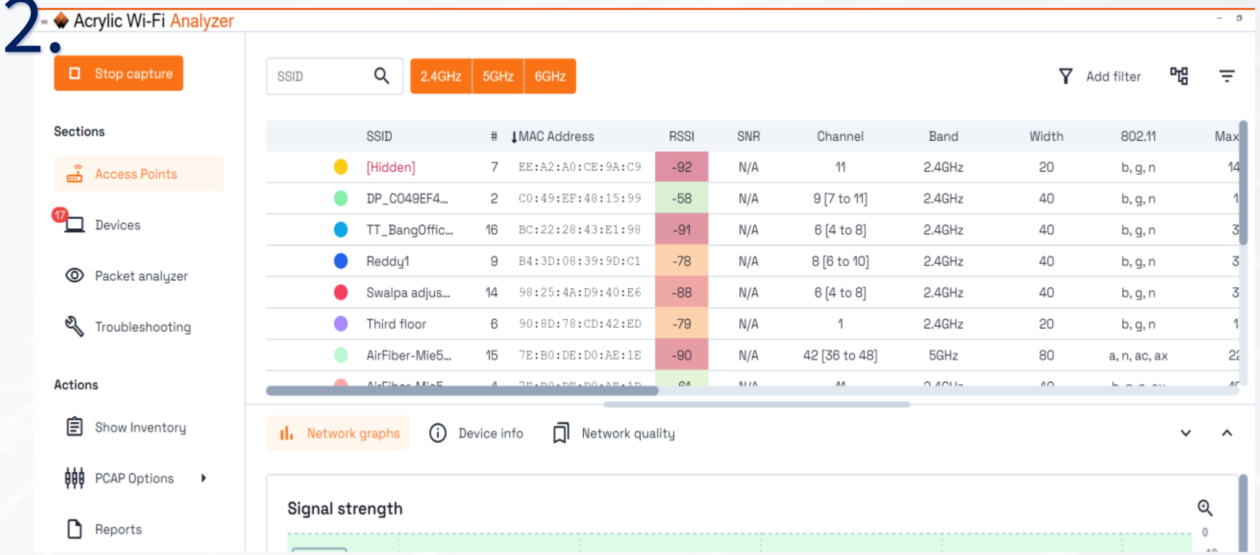
Acrylic Source site : https://www.acrylicwifi.com/en/wifi-analyzer/

Acrylic Wi-Fi Analyzer

1.

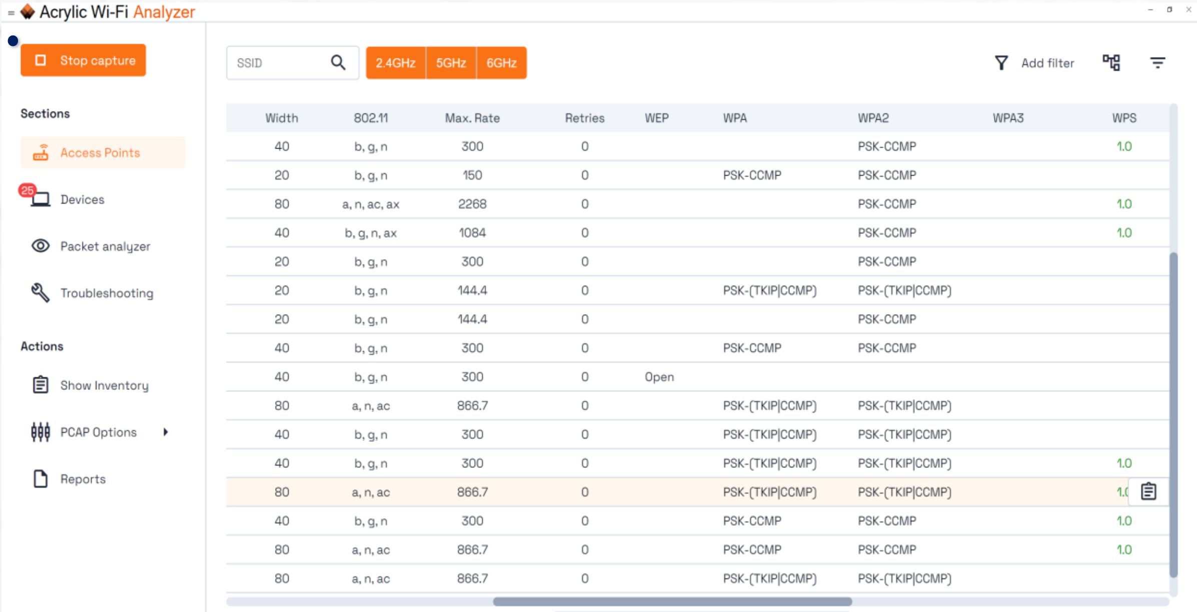


2.



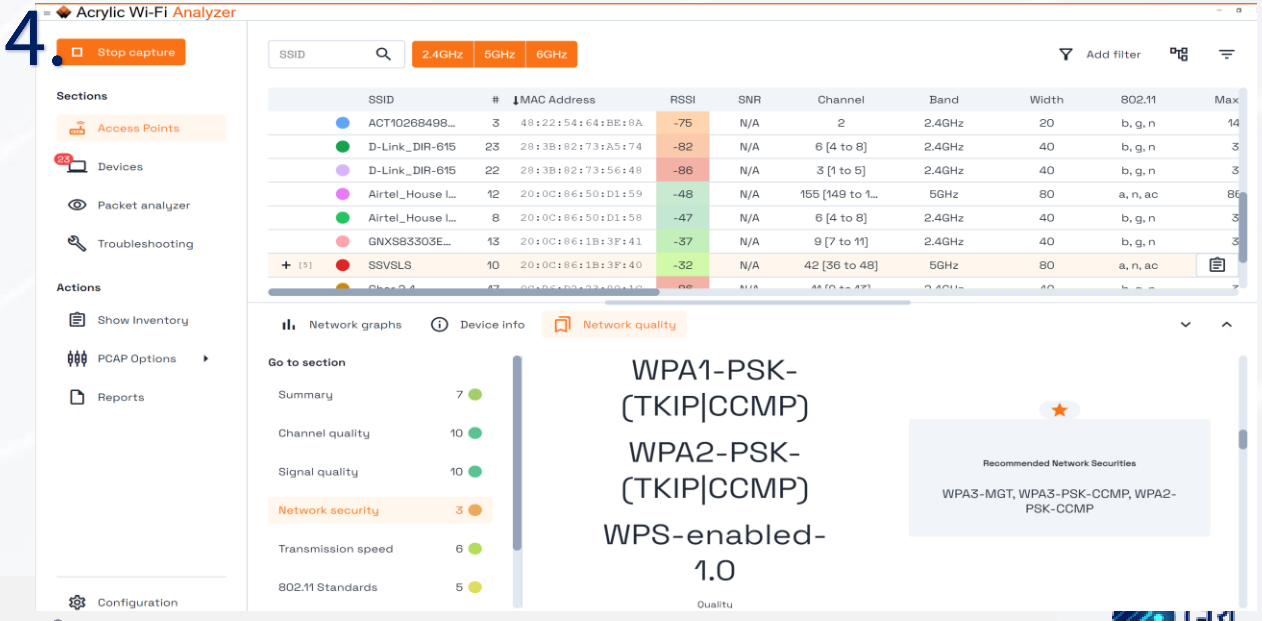
SSID	#	MAC Address	RSSI	SNR	Channel	Band	Width	802.11	Max
[Hidden]	7	EE:A2:A0:CE:9A:C9	-92	N/A	11	2.4GHz	20	b, g, n	14
DP_C049EF4...	2	C0:49:EF:48:15:99	-58	N/A	9 [7 to 11]	2.4GHz	40	b, g, n	1
TT_BangOffic...	16	BC:22:28:43:E1:98	-91	N/A	6 [4 to 8]	2.4GHz	40	b, g, n	3
Reddy1	9	B4:3D:08:39:9D:C1	-78	N/A	8 [6 to 10]	2.4GHz	40	b, g, n	3
Swalpa adjus...	14	98:25:4A:D9:40:E6	-88	N/A	6 [4 to 8]	2.4GHz	40	b, g, n	3
Third floor	6	90:8D:78:CD:42:ED	-79	N/A	1	2.4GHz	20	b, g, n	1
AirFiber-Mie5...	15	7E:B0:DE:D0:AE:1E	-90	N/A	42 [36 to 48]	5GHz	80	a, n, ac, ax	22

3.



Width	802.11	Max. Rate	Retries	WEP	WPA	WPA2	WPA3	WPS
40	b, g, n	300	0			PSK-CCMP		1.0
20	b, g, n	150	0		PSK-CCMP	PSK-CCMP		
80	a, n, ac, ax	2268	0			PSK-CCMP		1.0
40	b, g, n, ax	1084	0			PSK-CCMP		1.0
20	b, g, n	300	0			PSK-CCMP		
20	b, g, n	144.4	0		PSK-(TKIP|CCMP)	PSK-(TKIP|CCMP)		
20	b, g, n	144.4	0			PSK-CCMP		
40	b, g, n	300	0		PSK-CCMP	PSK-CCMP		
40	b, g, n	300	0	Open				
80	a, n, ac	866.7	0		PSK-(TKIP|CCMP)	PSK-(TKIP|CCMP)		
40	b, g, n	300	0		PSK-(TKIP|CCMP)	PSK-(TKIP|CCMP)		
40	b, g, n	300	0		PSK-(TKIP|CCMP)	PSK-(TKIP|CCMP)		1.0
80	a, n, ac	866.7	0		PSK-(TKIP|CCMP)	PSK-(TKIP|CCMP)		1.(
40	b, g, n	300	0		PSK-CCMP	PSK-CCMP		1.0
80	a, n, ac	866.7	0		PSK-CCMP	PSK-CCMP		1.0
80	a, n, ac	866.7	0		PSK-(TKIP|CCMP)	PSK-(TKIP|CCMP)		

4.



	SSID	#	MAC Address	RSSI	SNR	Channel	Band	Width	802.11	Max
	ACT10268498...	3	48:22:54:64:BE:8A	-75	N/A	2	2.4GHz	20	b, g, n	14
	D-Link_DIR-615	23	28:3B:82:73:A5:74	-82	N/A	6 [4 to 8]	2.4GHz	40	b, g, n	3
	D-Link_DIR-615	22	28:3B:82:73:56:48	-86	N/A	3 [1 to 5]	2.4GHz	40	b, g, n	3
	Airtel_House I...	12	20:0C:86:50:D1:59	-48	N/A	155 [149 to 1...	5GHz	80	a, n, ac	86
	Airtel_House I...	8	20:0C:86:50:D1:58	-47	N/A	6 [4 to 8]	2.4GHz	40	b, g, n	3
	GNXS83303E...	13	20:0C:86:1B:3F:41	-37	N/A	9 [7 to 11]	2.4GHz	40	b, g, n	3
+ [5]	SSVSLS	10	20:0C:86:1B:3F:40	-32	N/A	42 [36 to 48]	5GHz	80	a, n, ac	

Go to section

Summary	7
Channel quality	10
Signal quality	10
Network security	3
Transmission speed	6
802.11 Standards	5

WPA1-PSK-(TKIP|CCMP)

WPA2-PSK-(TKIP|CCMP)

WPS-enabled-1.0

Quality

Recommended Network Securities

WPA3-MGT, WPA3-PSK-CCMP, WPA2-PSK-CCMP

For Password Cracking & Brute-force Protection Testing

Hydra - helps monitor used for testing the strength of authentication mechanisms by attempting brute-force attacks, as required for testing protection against brute-force and dictionary attacks.

Installation: Hydra: Hydra comes pre-installed with Kali Linux And available via package managers on Linux (apt install hydra) or from Hydra's GitHub.

Usage (Hydra):

Hydra can perform rapid dictionary attacks against more than 50 protocols. This includes telnet, FTP, HTTP, HTTPS, SMB, databases, and several other services.

Perform a brute-force attack on the CPE's login interface (ensure permission for testing!):

```
hydra -l admin -P /path/to/password_list.txt <CPE_IP> http-post-form "/login_page:username=^USER^&password=^PASS^:Invalid login"
```

This command will attempt to log into the CPE using the credentials from the password list.

Monitor how the CPE responds to multiple failed login attempts. The system should block the account after a number of failed attempts or introduce delays (as required in 1.2.3).

ITSAR Sections:

1.2.3: Protection against brute-force and dictionary attacks.

How to Perform a Dictionary Attack with Hydra

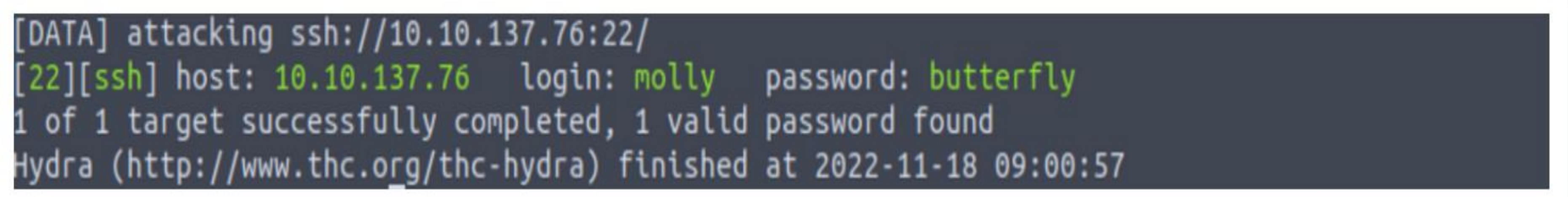
A dictionary attack is where we have single/multiple usernames, and we provide a password wordlist to Hydra. Hydra then tests all these passwords against every user in the list.

1. I am going to use the Rockyou wordlist for this example along with the users.txt file we created in the previous attack. If you are using Kali Linux, you can find the RockYou wordlist under /usr/share/wordlists/rockyou.txt.

2. Here is the command for a dictionary attack:

$ hydra -L users.txt -P /usr/share/wordlists/rockyou.txt 1010.137.76 ssh

3. We will get a similar result to the following output if any of the users match with the given password. You should also notice that we have used the flag -L instead of -l. -l is for a single username and -L is for a list of usernames.



```
[DATA] attacking ssh://10.10.137.76:22/
[22][ssh] host: 10.10.137.76   login: molly   password: butterfly
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2022-11-18 09:00:57
```

users.txt

root
admin
user
molly
steve
richard

For Vulnerability Scanning

Nessus- Nessus is a comprehensive vulnerability scanning tool used to identify security vulnerabilities, misconfigurations, and compliance issues in Wi-Fi Customer Premises Equipment (CPE). It can scan for weak configurations, outdated software, and other security flaws, ensuring that the CPE adheres to required security standards.

Installation: Available for Windows, macOS, and Linux. Download from Tenable Nessus.

Usage:

1. Install Nessus on a compatible system and configure it to scan the network where the CPE is connected.
2. Start a scan by adding the IP address of the CPE. Nessus will automatically analyze the device for vulnerabilities such as outdated software, insecure configurations, open ports, weak encryption protocols, and more.
3. Review the scan results to identify any vulnerabilities, default credentials, missing security patches, or unnecessary services running on the device.
4. Ensure that all identified vulnerabilities are resolved by updating software, disabling unnecessary services, and implementing proper security controls.

ITSAR Sections:

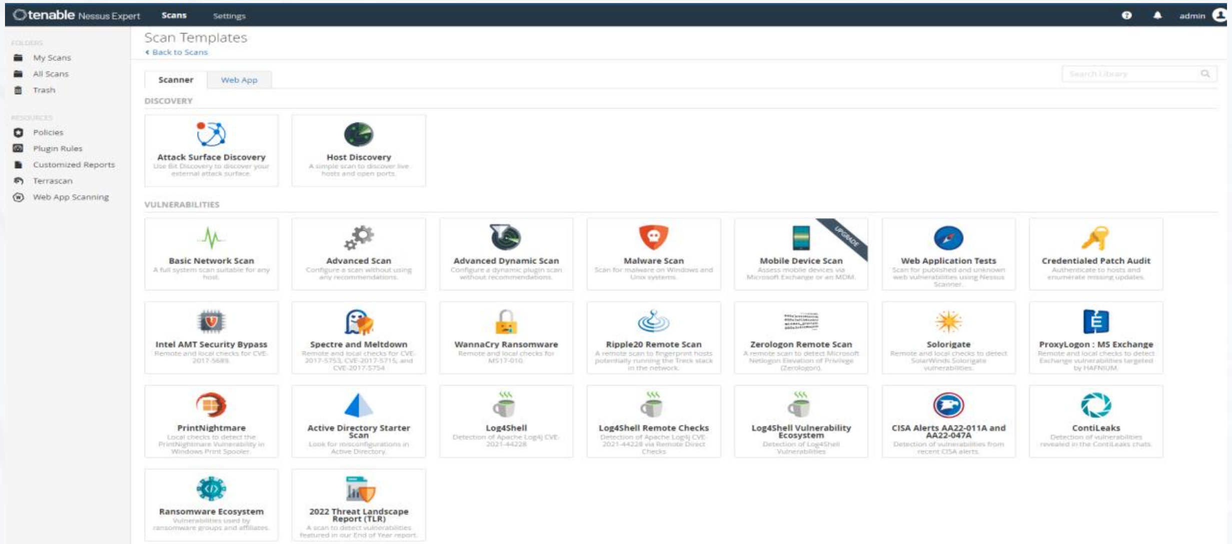
1.9.4: Vulnerability Scanning: Nessus helps identify known security vulnerabilities in CPE software and configurations.

1.3.4: Known Malware Check: It ensures that the CPE is free from malware and other security threats by scanning for malicious software and vulnerable components.

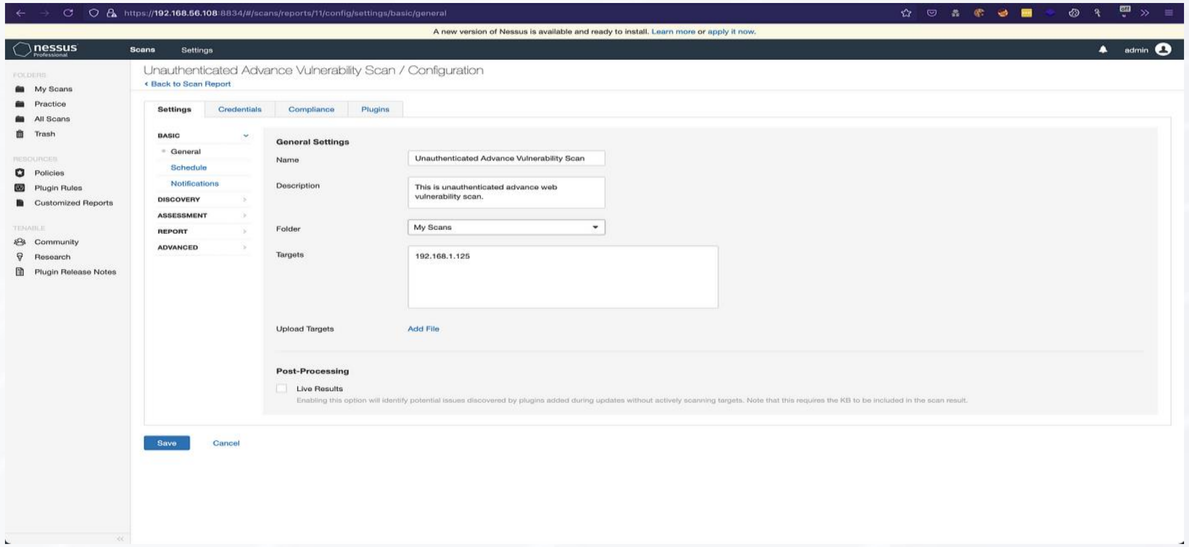
1.3.6: Unnecessary Service Removal: Nessus flags any unnecessary services running on the device that could be potential attack vectors.

VA Scanning using Nessus

1. Choose the right template


tenable Nessus Expert
Scans
Settings
admin
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Customized Reports
Terrascan
Web App Scanning
Scan Templates
‹ Back to Scans
Scanner
Web App
Search Library
DISCOVERY
Attack Surface Discovery
Use Bit Discovery to discover your external attack surface.
Host Discovery
A simple scan to discover live hosts and open ports.
VULNERABILITIES
Basic Network Scan
A full system scan suitable for any host.
Advanced Scan
Configure a scan without using any recommendations.
Advanced Dynamic Scan
Configure a dynamic plugin scan without recommendations.
Malware Scan
Scan for malware on Windows and Unix systems.
Mobile Device Scan
Assess mobile devices via Microsoft Exchange or an MDM.
UPGRADE
Web Application Tests
Scan for published and unknown web vulnerabilities using Nessus Scanner.
Credentialed Patch Audit
Authenticate to hosts and enumerate missing updates.
Intel AMT Security Bypass
Remote and local checks for CVE-2017-5689.
Spectre and Meltdown
Remote and local checks for CVE-2017-5753, CVE-2017-5715, and CVE-2017-5754
WannaCry Ransomware
Remote and local checks for MS17-010.
Ripple20 Remote Scan
A remote scan to fingerprint hosts potentially running the Treck stack in the network.
Zerologon Remote Scan
A remote scan to detect Microsoft Netlogon Elevation of Privilege (Zerologon).
Solorigate
Remote and local checks to detect SolarWinds Solorigate vulnerabilities.
ProxyLogon : MS Exchange
Remote and local checks to detect Exchange vulnerabilities targeted by HAFNIUM.
PrintNightmare
Local checks to detect the PrintNightmare Vulnerability in Windows Print Spooler.
Active Directory Starter Scan
Look for misconfigurations in Active Directory.
Log4Shell
Detection of Apache Log4j CVE-2021-44228
Log4Shell Remote Checks
Detection of Apache Log4j CVE-2021-44228 via Remote Direct Checks
Log4Shell Vulnerability Ecosystem
Detection of Log4Shell Vulnerabilities
CISA Alerts AA22-011A and AA22-047A
Detection of vulnerabilities from recent CISA alerts.
ContiLeaks
Detection of vulnerabilities revealed in the ContiLeaks chats.
Ransomware Ecosystem
Vulnerabilities used by ransomware groups and affiliates.
2022 Threat Landscape Report (TLR)
A scan to detect vulnerabilities featured in our End of Year report.

2. Fill the Target Details



A new version of Nessus is available and ready to install. Learn more or apply it now.

Unauthenticated Advance Vulnerability Scan / Configuration

General Settings

Name: Unauthenticated Advance Vulnerability Scan

Description: This is unauthenticated advance web vulnerability scan.

Folder: My Scans

Targets: 192.168.1.125

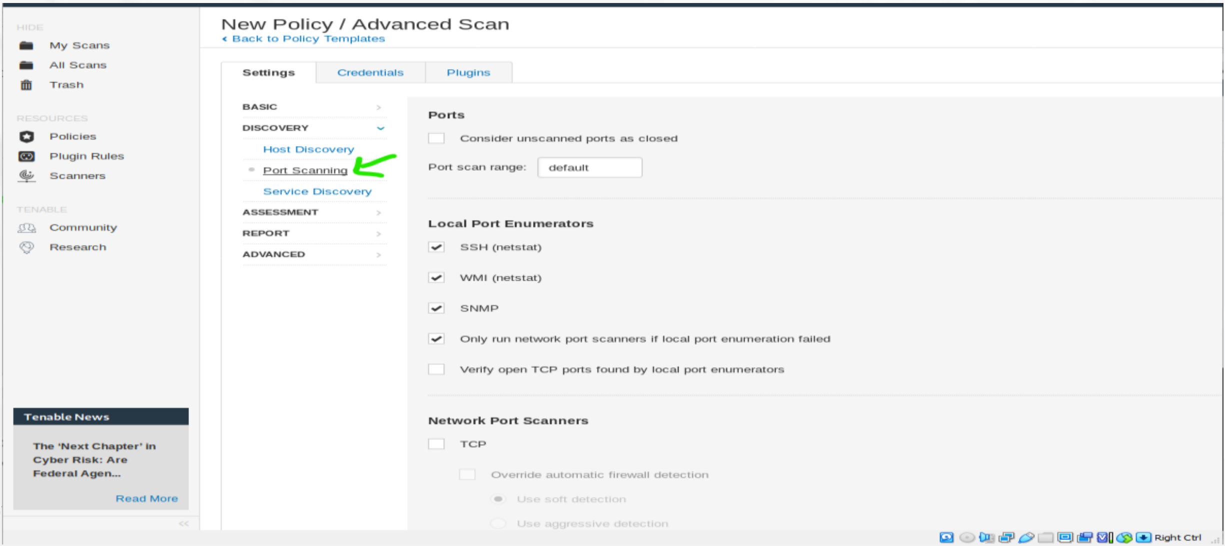
Upload Targets: Add File

Post-Processing

□ Live Results

Enabling this option will identify potential issues discovered by plugins added during updates without actively scanning targets. Note that this requires the KB to be included in the scan result.

3. Do Port Scanning to identify the Open Ports



New Policy / Advanced Scan

Ports

□ Consider unscanned ports as closed

Port scan range: default

Local Port Enumerators

☑ SSH (netstat)

☑ WMI (netstat)

☑ SNMP

☑ Only run network port scanners if local port enumeration failed

□ Verify open TCP ports found by local port enumerators

Network Port Scanners

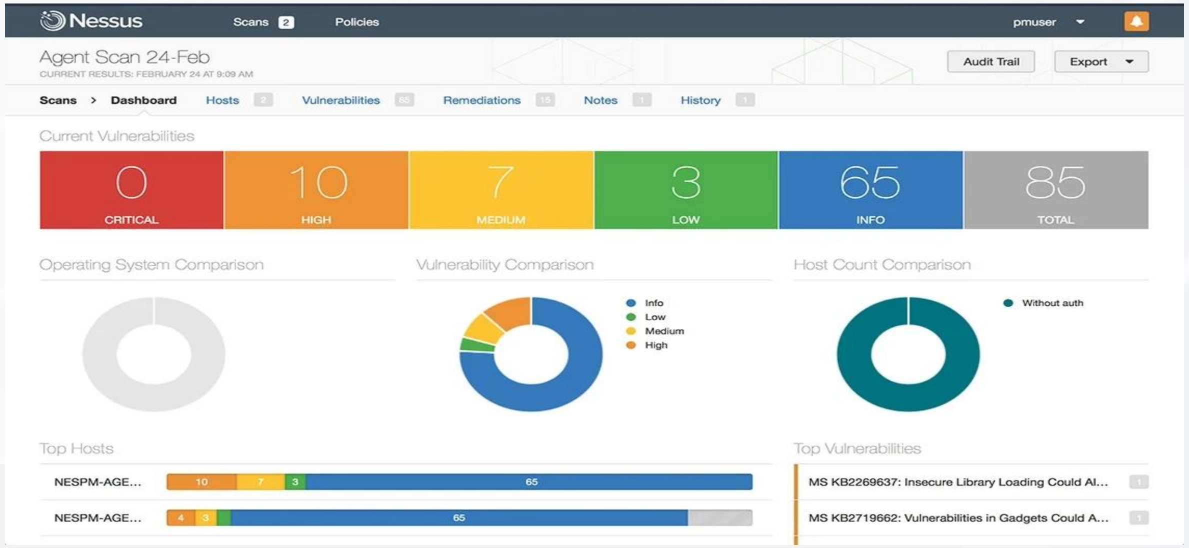
□ TCP

□ Override automatic firewall detection

○ Use soft detection

○ Use aggressive detection

4. Run Scan, and find the Results



Agent Scan 24-Feb

CURRENT RESULTS: FEBRUARY 24 AT 9:09 AM

Current Vulnerabilities

0	10	7	3	65	85
CRITICAL	HIGH	MEDIUM	LOW	INFO	TOTAL

Top Hosts

NESPM-AGE...	10	7	3	65
NESPM-AGE...	4	3		65

Top Vulnerabilities

MS KB2269637: Insecure Library Loading Could Al...	1
MS KB2719662: Vulnerabilities in Gadgets Could A...	1

For Wi-Fi network security

Aircrack-ng- Aircrack-ng is a suite of tools for auditing Wi-Fi network security. It can be used to test the encryption standards used for Wi-Fi access (WPA2-PSK, AES, etc.).

Installation: Available for Linux, macOS, and Windows. Download from Aircrack-ng.

Usage:

1. Enable monitor mode on your Wi-Fi adapter.

2. Capture WPA2-PSK handshakes using.

3. Once you capture the handshake, use Aircrack-ng to test the strength of the encryption.

4. Ensure that WPA2-PSK with AES-128 is being used as required by ITSAR and verify that weaker encryption (like WEP or TKIP) is not available for selection.

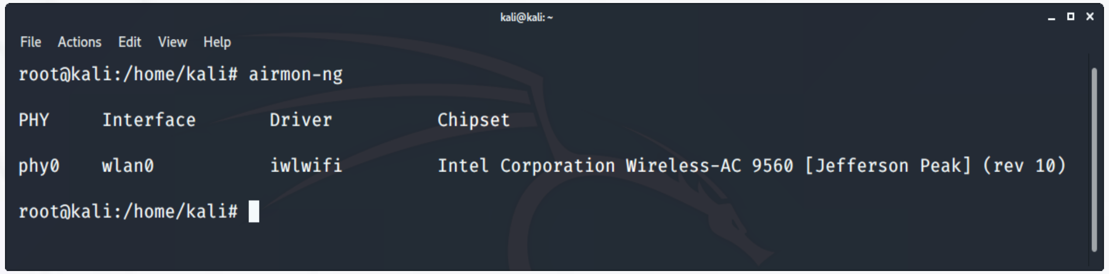
ITSAR Sections:

1.6.2: Cryptographic-Based Secure Communication on Wi-Fi Access.

1.6.3: Cryptographic Algorithm Selection for Wi-Fi Access.

Working with aircrack-ng

1. To list all network interfaces.



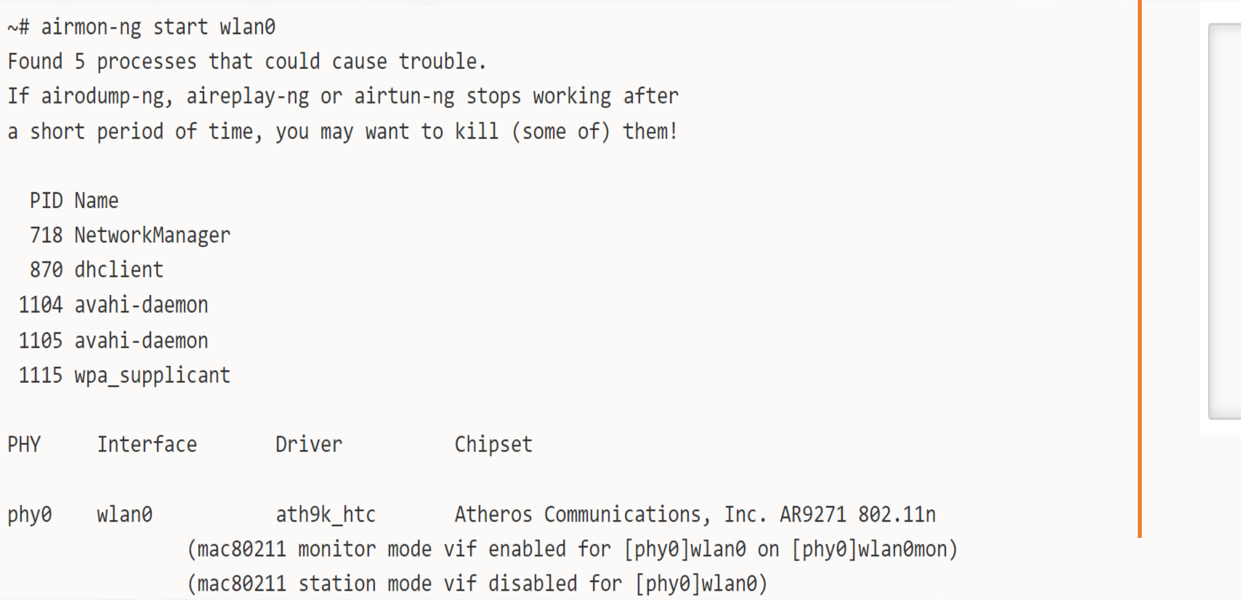
```
root@kali:/home/kali# airmon-ng

PHY     Interface       Driver          Chipset

phy0    wlan0           iwlwifi         Intel Corporation Wireless-AC 9560 [Jefferson Peak] (rev 10)

root@kali:/home/kali#
```

2. Enable monitor mode on your Wi-Fi adapter



```
~# airmon-ng start wlan0
Found 5 processes that could cause trouble.
If airodump-ng, aireplay-ng or airtun-ng stops working after
a short period of time, you may want to kill (some of) them!

  PID Name
  718 NetworkManager
  870 dhclient
 1104 avahi-daemon
 1105 avahi-daemon
 1115 wpa_supplicant

PHY     Interface       Driver          Chipset

phy0    wlan0           ath9k_htc       Atheros Communications, Inc. AR9271 802.11n
                (mac80211 monitor mode vif enabled for [phy0]wlan0 on [phy0]wlan0mon)
                (mac80211 station mode vif disabled for [phy0]wlan0)
```

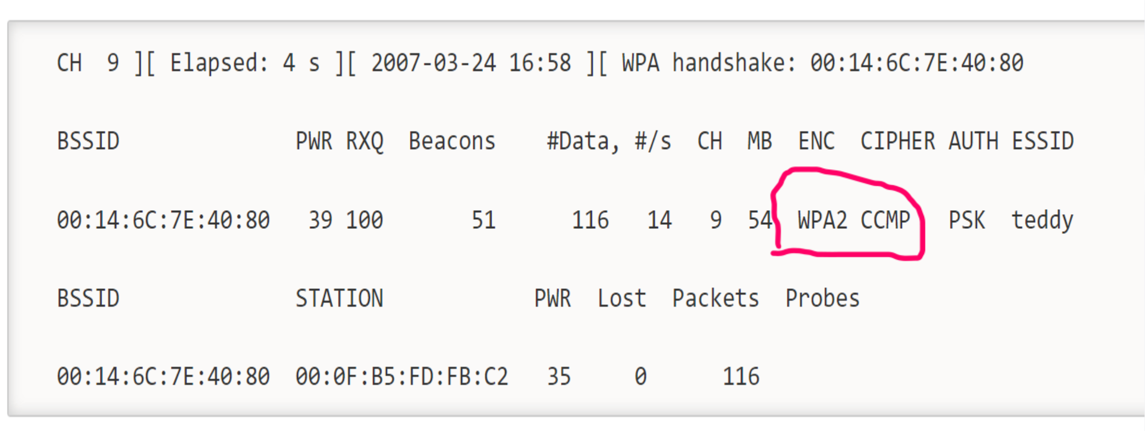
3. Start airodump-ng to collect authentication handshake

airodump-ng -c 9 --bssid 00:14:6C:7E:40:80 -w psk ath0

Where:

-c 9 is the channel for the wireless network
--bssid 00:14:6C:7E:40:80 is the access point MAC address. This eliminates extraneous traffic.
-w psk is the file name prefix for the file which will contain the IVs.

ath0 is the interface name.



```
 CH  9 ][ Elapsed: 4 s ][ 2007-03-24 16:58 ][ WPA handshake: 00:14:6C:7E:40:80

 BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB  ENC  CIPHER AUTH ESSID

 00:14:6C:7E:40:80   39 100       51      116   14   9  54  WPA2 CCMP   PSK  teddy

 BSSID              STATION            PWR  Lost  Packets  Probes

 00:14:6C:7E:40:80  00:0F:B5:FD:FB:C2   35     0      116
```

For Web Interface Testing

Burp Suite- Burp Suite is a powerful web application security testing tool used for identifying vulnerabilities such as authentication weaknesses, session management issues, and encryption problems in the web interfaces of Wi-Fi CPEs.

Installation: Available for Windows, macOS, and Linux. Download from PortSwigger.

Usage:

1: Install Burp Suite and launch it.

2: Configure Burp Suite as a proxy in your browser to intercept traffic between the browser and the CPE's web interface.

3: Visit the web interface of the Wi-Fi CPE through your browser.

4: Use Burp's automated scanning feature to identify vulnerabilities such as:

- Missing or weak HTTPS implementation.
- Insecure session management (e.g., session IDs not being regenerated).
- Issues with authentication mechanisms like password strength, authentication feedback, or lack of multi-factor authentication.

5: Analyze the results and review the identified vulnerabilities. Burp Suite will highlight potential security issues and offer suggestions for remediating those vulnerabilities.

ITSAR Sections:

1.11.1: HTTPS Support – Ensures that the CPE's web interface supports HTTPS and encrypts sensitive data.
1.2.9: Storage of Passwords in Encrypted Form – Verifies that the CPE securely stores passwords and protects them from exposure.
1.11.4: HTTP Input Validation – Tests whether user inputs are properly validated to prevent cross-site scripting (XSS), SQL injection, and other attacks.

Many more tools can help for Wi-Fi Network Analysis

NetSpot (For SSID Scanning and Wi-Fi Network Analysis)

NetSpot is a versatile Wi-Fi analysis tool that allows you to scan for SSIDs and analyze Wi-Fi network coverage. It helps assess signal strength, network channels, and security settings to ensure compliance with Wi-Fi security standards for CPEs.

Installation: Available for Windows and macOS. Download from **NetSpot.**

ITSAR Sections:

•1.9.3: SSID Scanning – Verifies that the CPE prevents the disclosure of sensitive information and offers the option to hide SSIDs.
•1.6.2: Cryptographic Based Secure Communication on Wi-Fi Access – Ensures the scanned SSIDs are using secure encryption standards (e.g., WPA2-PSK).

Hping3 (For DDoS Testing)

Hping3 is a powerful packet crafting tool that can be used for Distributed Denial of Service (DDoS) testing. It allows users to create custom network packets and simulate various types of DDoS attacks, including SYN floods, UDP floods, and ICMP floods, making it highly useful in assessing the resilience of a Wi-Fi CPE or network under simulated attack conditions.

Installation: Available on Linux and can be installed using the following command: *sudo apt-get install hping3*

Usages: Hping3 can overwhelm a device by sending a flood of packets, exhausting the target's resources. Can simulate SYN Flood Attack, UDP Flood Attack, CMP Flood (Ping Flood) Attack, TCP ACK Flood and many more.

ITSAR Sections:

•1.8.1: Excessive Overload Protection

Many more tools can help for Wi-Fi Network Analysis

Nmap 7.95 (For Port Scanning & Service Discovery)

Nmap is a network scanning tool that can be used to identify open ports and services on the CPE, ensuring that only documented and necessary services are active.

Installation: Available for Windows, macOS, and Linux. Download from **Nmap.org**.

Synopsis:
nmap [<Scan Type> ...] [<Options>] { <target specification> }

Use different switches as per requirement -sS (TCP SYN scan), -sU (UDP scans), -sY (SCTP INIT scan), -sA (TCP ACK scan)

ITSAR Sections:

- 1.9.2: Port Scanning.
- 1.3.6: Unnecessary Service Removal.

Ensuring Secure Wi-Fi

1

Comprehensive Testing

Using a suite of tools to thoroughly get it test the device from accredited TSTL.

2

Compliance

Meeting ITSAR requirements for Wi-Fi CPE security.

3

Secure by Design

Implementing robust security measures from the ground up.

Thank You!

https://graniteriverlabs.com/