

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

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 interface

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: <a href="https://www.wireshark.org/docs/wsug\_html/">https://www.wireshark.org/docs/wsug\_html/</a>

									_	-					_
Filter	: tcp									• Exp	ression	⊆le-	ar <u>A</u> ppl;	/	
No.	Time	•	Source			Des	tination	1		Pro	tocol	Info			
	11 1.2	26156	192.1	168.0.2		19.	2.168.	0.1		TC	,	3196	> http	D LSYN	Seq
	12 1.2	27282	192.1	168.0.1		192	2.168.	0.2		TC		110C	> 3196	D LSYN,	ACK.
	14 1 3	27 3 2 3	192.1	68 0 2		192	2 168	0.1		HT	гр	SUBSO	PTRC	/unnn/e	i seqi
	15 1.2	29309	192.1	68.0.1		192	2.168	0.2		TC		http	> 3196	5 FACK	Sea
	16 1.2	32421	192.1	68.0.1		192	2.168.	0.2		TC		ETCP	Window	v Updat	e] h
	17 1.2	48355	192.1	168.0.1		192	2.168.	0.2		TCI	2	1025	> 5000	) [SYN]	Seq
	18 1.2	48391	192.1	168.0.2		197	2.168.	0.1		TCI	•	5000	> 1025	5 [SYN,	ACK)
	19 1.2	250171	192.1	168.0.1		192	2.168.	0.2		HT	TP	HTTP/	1.0 20	юок	
	20 1.2	50285	192.1	168.0.Z		192	2.168.	.0.1		TC		3196	> http	D LFIN,	ACK
	21 1.2	50810	192.1	68.0.1		192	2.168.	0.2		TCI		2106	> 3196	D LEIN,	ALK
	22 1.2	51868	192.1	68 0 1		103	2 168	0.2		TC		1025	> 5000	D FACK	l Seg
	24 1.2	52826	192.1	68.0.1		192	2.168	0.2		TC		http	> 3196	FETN.	ACK
	25 1.2	53323	192.1	68.0.2		192	2.168.	0.1		TC		3197	> http	<b>FSYN</b>	Sea
	26 1.2	54502	192.1	168.0.1		192	2.168.	.0.2		TCI		http	> 3197	² [SYN,	ACK
	27 1.2	254532	192.1	168.0.2		192	2.168.	.0.1		TCI	•	3197	> http	) [ACK]	Seq
<															
I E	came 11	(62 by	tes on i	wire, 6	2 hvte	s cantu	redì								
E F	thernet	TT. Sr	r: 192.	168.0.2	(00:0)	h:5d:20	ord of	2). De	st · Ne	trear	2d:7	5 · 9a	(00:09	·Sh·2d	.75.9
	nternet	Protoc	ol Sec	. 107 1	50 D 2	(192 1	68 0	2) De	nt • 10	169	0.1	(102 -	168 0	1)	
	nanemie	rion Co	etrol R	rotocol	Sec	Pont · 2	106 /	2106)	Det	Post.	httn	(200)	Sear	0 10	
	ansin's:	sion ce	neror P	000001	, sici	FOIC. J	190 (	,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,	DSC	POLC.	neep	(00)	, seq.	v,	1. V
0000	00 09	5b 2d	75 9a 0	0 06 5	d 20 c	d 02 08	8 00 4	15 00	- <u>, </u> [-	-u	J	.E.			
0020	00 50	16 46 Oc 7c	40 00 8	0066 c369	1 20 0 5 f8 0	0 00 00		0 ao	.0.6	Pr6	d,	 n			
0020		20,00	00 50 5					0 01				· p ·			



## 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 Wi-Fi Analyzer

crylic Wi-Fi Analyzer										•••••••••••••••••••••••••••••••••••••••									
Start capture						9				Stop capture	SSID Q	2.4GHz	5GHz 6GHz					Y	Add filter
ocess Points					•					Sections	com		# IMAC Address	DOOL	CNID	Chappel	Pand	Width	000.1/
evices											- [Hidden	1	7 EE:A2:A0:CE:9A:C	9 -92	N/A	11	2 4GHz	20	602.11
acket analyzer				Start	t capturing to dis	scover WiFi devices				Access Points			2 CO:49.FF:48:15:0	9 .59	N/A	9 [7 to 11]	2.4012	40	b, g, n
roubleshooting					▶ Start	capture				Devices		οΩffic	16 BC • 22 • 28 • 43 • E1 • 6	8 -91	N/A	6 [/ to 8]	2 /10Hz	40	b, g, r
											Beddul	gomo	9 B4:3D:08:39:9D:0	1 -78	N/A	8 [6 to 10]	2.4GHz	40	b, g, i
iow Inventory	I. Network	graphs (i)	Device info	Network quality	:y				~ ^	Packet analyzer	Swalna	adius	14 98-25-4A-D9-40-E	6 -88	N/A	6 [4 to 8]	2 /16Hz	40	b,g,
CAP Options			-							S Traublasheating		or	6 90:8D:78:CD:42:E	D -79	N/A	1	2.4GHz	20	b,g,
ports	Signal stre	ength							Q	Troubleshooting	AirFiber	Mie5	15 7E:B0:DE:D0:AE:1	E -90	N/A	42 [36 to 48]	5GHz	80	a n ac
	Good								-10 -20	Actions	AirFiber	Mie5	4 7E.DO.DE.DO.AE.1		N/A	42 [00 t0 40]	0.4011-	40	a, 11, au
	Bad									Actiona							_		
									-50	E Show Inventory	II. Network graphs	(i) Devia	ce info 🏾 🎵 Network	quality					
									-70 -80	PCAP Options									
		21:21:00	21:22:0	00	21:23:00	0	21:24:00	21:25:00	-100		Signal strength								
iguration										Reports	olghai strongth								
										= 🗢 Acrylic Wi-Fi Analyzer									
lic Wi-Fi <mark>Analyzer</mark>									- 0 ×	Acrylic Wi-Fi Analyzer									
lic Wi-Fi Analyzer	SSID	Q 2.4GHz	5GHz 6GHz					Y Add filter	- • ×	Acrylic Wi-Fi Analyzer	SSID Q	2.4GHz 5	5GHz 6GHz					Υ,	Add filter
lic Wi-Fi Analyzer	SSID	Q 2.4GHz	5GHz 6GHz					Y Add filter	- • ×	Acrylic Wi-Fi Analyzer	SSID Q SSID	2.4GHz 5	5GHz 6GHz # 1MAC Address	RSSI	SNR	Channel	Band	Y /	Add filter 802.1
c Wi-Fi Analyzer	SSID Width	Q 2.4GHz 802.11	5GHz 6GHz Max. Rate	Retries	WEP	WPA	WPA2	Y Add filter	ra ÷ ₩PS	Acrylic Wi-Fi Analyzer  A Consequence  A Consequenc	SSID Q SSID ACT102: D-Link	2.4GHz 5 68498 DIR-615 2	5GHz         6GHz           # IMAC Address         3           48:22:54:64:BE:62         28:3B:62:73:A5:7	<b>RSSI</b> A -75 4 -82	SNR N/A N/A	Channel 2 6 [4 to 8]	Band 2.4GHz 2.4GHz	Width 20 40	Add filter 802. b, g, b, g,
c Wi-Fi Analyzer	SSID Width 40	Q 2.4GHz 802.11 b, g, n	As a constraint of the constra	Retries 0	WEP	WPA	WPA2 PSK-CCMP	Add filter     WPA3     WPA3	- a × Pta = WPS 1.0	Acrylic Wi-Fi Analyzer  A Consequence  A Consequenc	SSID Q SSID ACT102: D-Link D-Link	2.4GHz 5 38498 DIR-615 2 DIR-615 2	6GHz         6GHz           # LMAC Address         3           3         481:221:541:641:8E16           22         281:381:021:731:651:4           22         201:381:021:731:561:4	RSSI           A        75           4        82           0        86	SNR N/A N/A N/A	Channel 2 6 (4 to 8) 3 (1 to 5)	Band 2.4GHz 2.4GHz 2.4GHz 2.4GHz	₩idth 20 40 40	Add filter 802.' b, g, b, g,
c Wi-Fi Analyzer	SSID Width 40 20 80	Q 2.4GHz 802.11 b, g, n b, g, n	5GHz 6GHz Max. Rate 300 150 2288	Retries 0 0	WEP	WPA PSK-CCMP	WPA2 PSK-CCMP PSK-CCMP PSK-CCMP	Y Add filter	- 0 ×	Acrylic Wi-Fi Analyzer  Acrylic Wi-Fi Analyzer  Sections  Cons  Co	SSID Q SSID ACT102/ D-Link_ D-Link_ Airtel_H	2.4GHz 5 38498 DIR-615 2 DIR-615 2 OUR-615 2	EGHz         EGHz           # IMAC Address         3           48:22:54:64:BE:6         28           28:3B:82:73:75:7         22           20:3B:82:73:56:4         12           20:00:86:50:101:5         12	RSSI           A        75           4        82           8        86           9        48	SNR N/A N/A N/A N/A	Channel 2 6 (4 to 8) 3 (1 to 5) 155 (149 to 1	Band           2.4GHz           2.4GHz           2.4GHz           5GHz	Width 20 40 40 80	Add filter 802. b, g, b, g, b, g, a, n, a
c Wi-Fi Analyzer	SSID Width 40 20 80 40	Q 2.4GHz 802.11 b, g, n b, g, n a, n, ac, ax b, g, n, ax	5GHz         6GHz           Max. Rate         300           150         2268           1084         304	Retries 0 0 0	WEP	WPA PSK-CCMP	WPA2 PSK-CCMP PSK-CCMP PSK-CCMP PSK-CCMP	Y Add filter	- 0 × PtB = WPS 1.0 1.0 1.0	Acrylic Wi-Fi Analyzer  Acrylic Wi-Fi Analyzer  Sections  Access Points  Access Points  Pevices  Packet analyzer  Access Points  Comparison  Compariso	SSID Q SSID ACT102 D-Link Airtel_H Airtel_H	2.4GHz 5 38498 DIR-615 2 DIR-615 2 DIR-615 2 ouse I 3035	EGHz         EGHz           # IMAC Address         3           40:22:54:64:BE:6         2           20:3B:02:73:56:4         2           12         20:00:06:50:01:5           8         20:00:06:50:01:5           3         20:00:06:01:01:5	RSSI           A         -75           4         -82           8         -86           9         -48           6         -47           1         -87	SNR N/A N/A N/A N/A	Channel 2 6 (4 to 8) 3 (1 to 5) 155 (149 to 1 6 (4 to 8) 9 (7 to 11)	Band           2.4GHz           2.4GHz           2.4GHz           2.4GHz           2.4GHz	♥ // Width 20 40 40 80 80 40	Add filter 802: b, g, b, g, b, g, a, n, i b, g,
c Wi-Fi Analyzer	SSID Wildth 40 20 80 40 20	Q 2.4GHz 802.11 b, g, n b, g, n a, n, ac, ax b, g, n, ax b, g, n, ax	5GHz         6GHz           Max. Rate         300           150         2268           1084         300	Retries 0 0 0 0 0	WEP	WPA PSK-CCMP	WPA2 PSK-CCMP PSK-CCMP PSK-CCMP PSK-CCMP PSK-CCMP	Y Add filter	- 0 × -	Acrylic Wi-Fi Analyzer  Acrylic Wi-Fi Analyzer  Sections  Access Points  Access Points  Pevices  Packet analyzer  Note Packet analyz	SSID         Q           SSID         ACT102           D-Link         D-Link           D-Link         AIrtel_P           Airtel_P         GINXS83           + (5)         SSVSLS	2.4GHz 5 38498 DIR-615 2 DIR-615 2 DIR-615 2 0use I 303E	GGHz         6GHz           # IMAC Address         3           40:22:54:64:BE:6         28           20:3B:02:73:76:4         20:00:16:50:11:5           20:00:16:50:11:5         3           20:00:16:50:11:5         3           20:00:16:1B:3F:4         20:00:16:1B:3F:4	RSSI A75 482 686 948 948 947 137 032	SNR N/A N/A N/A N/A N/A N/A N/A	Channel 2 6 [4 to 8] 3 [1 to 5] 155 [149 to 1 6 [4 to 8] 9 [7 to 11] 42 [36 to 48]	Band           2.4GHz           2.4GHz           2.4GHz           5GHz           2.4GHz	Width 20 40 80 40 80 80 80	Add filter 802, b, g, b, g, b, g, a, n, a b, g, b, g, b, g,
ic Wi-Fi Analyzer	SSID Width 40 20 80 40 20 20	2.4GHz 802.11 b, g, n b, g, n a, n, ac, ax b, g, n, ax b, g, n	5GHz         6GHz           Max. Rate         300           150         2268           1084         300           144.4         300	Retries           0           0           0           0           0           0           0           0           0           0           0           0           0           0	WEP	WPA PSK-CCMP PSK-(TKIPICCMP)	WPA2 PSK-CCMP PSK-CCMP PSK-CCMP PSK-CCMP PSK-CCMP PSK-CCMP PSK-CTKIP CCMP)	♥ Add filter WPA3	- 0 × -	Acrylic Wi-Fi Analyzer Acrylic Wi-Fi Analyzer Sections Consections Consections Consections Consections Consections Consections	SSID         Q           SSID         ACT102           ACT102         D-Link           D-Link         Airtel_H           Airtel_H         Airtel_H           GNXS83         SSVSLS           Chen 2         Chen 2	2.4GHz 5 38498 DIR-615 2 DIR-615 2 DIR-615 2 DIR-615 2 0use I 303E	5GHz         6GHz           #         IMAC Address           3         48:22:54:64:82:6           23         28:38:82:73:56:4           22         28:38:62:73:56:4           22         20:02:86:50:11:5           8         20:02:86:50:11:5           13         20:02:86:18:3F:4           10         20:02:86:18:3F:4	RSSI           4         -75           4         -82           6         -86           9         -48           6         -47           1         -37           1         -32           1         -32           1         -32           1         -32           1         -32	SNR N/A N/A N/A N/A N/A N/A N/A N/A	Channel 2 6 [4 to 8] 3 [1 to 5] 155 [149 to 1 6 [4 to 8] 9 [7 to 11] 42 [36 to 48]	Band           2.4GHz           2.4GHz           2.4GHz           5GHz           2.4GHz           5GHz           2.4GHz	Width 20 40 40 80 80 40 40 40 40 40 40 40 40 40 40 40 40 40	Add filter 802. b, g, b, g, b, g, a, n, a b, g, b, g, b, g, b, g, b, c
c Wi-Fi Analyzer	SSID Width 40 20 80 40 20 20 20	2.4GHz 802.11 b, g, n b, g, n a, n, ac, ax b, g, n, ax b, g, n b, g, n b, g, n	5GHz         6GHz           Max. Rate         300           150         2268           1084         300           144.4         144.4	Retries           0	WEP	WPA PSK-CCMP PSK-(TKIP[CCMP)	WPA2 PSK-CCMP PSK-CCMP PSK-CCMP PSK-CCMP PSK-CCMP PSK-CCMP PSK-CTKIP[CCMP] PSK-CCMP	♥ Add filter WPA3	- 0 × Pra = WPS 1.0 1.0 1.0	<ul> <li>Acrylic Wi-Fi Analyzer</li> <li>Stop capture</li> <li>Sections</li> <li>Access Points</li> <li>Consections</li> <li>Packet analyzer</li> <li>Troubleshooting</li> <li>Actions</li> <li>Show Inventory</li> </ul>	SSID Q SSID ACT102 D-Link, D-Link, Airtel_H GNX83 + (3) SSVSLS Chaol II, Network graphs	2.4GHz 2 38498 DIR-615 2 DIR-615 2 0use L 3035 3035	SCHz         6GHz           #         IMAC Address           3         48:22;54:64:BE:6           23         28:38:82:73:65:7           24         29:38:82:73:65:7           22         29:38:82:73:65:7           22         29:38:82:73:56:1           8         20:00:86:50:10:5           8         20:00:86:18:37:4           10         20:00:86:18:37:4           10         20:00:80:19:39:4           10         20:00:80:19:40:4           10         20:00:80:19:40:4           10         20:00:80:19:40:4           10         20:00:80:19:40:4	RSSI           A         -75           4         -82           0         -86           9         -448           0         -471           1         -371           0         -322           0         -324	SNR N/A N/A N/A N/A N/A N/A N/A	Channel 2 6 [4 to 8] 3 [1 to 5] 155 [149 to 1 6 [4 to 8] 9 [7 to 11] 42 [36 to 48] 41 [0 to 47]	Band           2.4GHz           2.4GHz           2.4GHz           5GHz           2.4GHz           5GHz           0.4GHz	Width 20 40 40 80 40 40 40 40 40 40 40 40	Add filter 802. <sup>4</sup> b, g, b, g, b, g, b, g, b, g, b, g, c, n, a
c Wi-Fi Analyzer	SSID Width 40 20 80 40 20 20 20 20 40	2.4GHz 802.11 b, g, n b, g, n a, n, ac, ax b, g, n b, g, n b, g, n b, g, n b, g, n	5GHz         6GHz           Max. Rate         300           150         2268           1084         300           144.4         300	Retries           0	WEP	WPA PSK-CCMP PSK-(TKIP[CCMP) PSK-CCMP	WPA2 PSK-CCMP PSK-CCMP PSK-CCMP PSK-CCMP PSK-CCMP PSK-CCMP PSK-CCMP PSK-CCMP	Y Add filter WPA3	- 0 × Pg ÷ WPS 1.0 1.0 1.0	Acrylic Wi-Fi Analyzer Acrylic Wi-Fi Analyzer Sections Consections Consections Consections Actions Consections Consections Consections Consections Consections Consections Consections Consections Consections Consections	SSID         Q           SSID         ACT102           D-Link         D-Link           D-Link         Airtel_H           Airtel_H         Airtel_H           SSVS         Standard           Ih. Network graphs         Standard	2.4GHz 2 38498 DIR-615 2 0IR-615 2 0IR-615 2 0USe L 303E 303E	5CHz         6CHz           #         IMAC Address           3         40:22:54:64:BE:6           23         28:38:62:73:56:4           12         20:00:166:50:D1:5           8         20:00:166:50:D1:5           13         20:00:166:18:3F:4           10         20:00:16:D2:32:00:1           142         00:D5:D2:32:00:1           15         00:D5:D2:32:00:1           16         D1:D2:32:00:1           17         00:D5:D2:32:00:1	RSSI           A         -75           4         -82           0         -86           9         -48           1         -37           1         -32           0         -32           1         -32	SNR N/A N/A N/A N/A N/A N/A	Channel 2 6 [4 to 8] 3 [1 to 5] 155 [149 to 1 6 [4 to 8] 9 [7 to 11] 42 [36 to 48] 41 [0 to 17]	Band           2.4GHz           2.4GHz           2.4GHz           2.4GHz           2.4GHz           5GHz           2.4GHz           5GHz           2.4GHz           5GHz           2.4GHz	Width 20 40 40 80 40 40 80 40 80 80	Add filter 802. b, g, b, g, b, g, a, n, a b, g, b, g, c, n, a
c Wi-Fi Analyzer	SSID Width 40 20 80 40 20 20 20 20 40 40	2.4GHz 802.11 b, g, n b, g, n a, n, ac, ax b, g, n b, g, n b, g, n b, g, n b, g, n b, g, n b, g, n	SGHz         6GHz           Max. Rate         300           150         2268           1084         300           144.4         144.4           300         300	Retries           0	WEP	WPA PSK-CCMP PSK-(TKIP[CCMP) PSK-CCMP	WPA2 PSK-CCMP PSK-CCMP PSK-CCMP PSK-CCMP PSK-CCMP PSK-CCMP PSK-CCMP	Y Add filter WPA3	- 0 × Prg = WPS 1.0 1.0 1.0	Acrylic Wi-Fi Analyzer Acrylic Wi-Fi Analyzer Sections Consections	SSID Q SSID Q ACTIO22 D-Link D-Link Airtel_H GNX833 + (3) SSVSLS Chara d I, Network graphs Go to section	2.4GHz 5 38498 DIR-615 2 DIR-615 2 0USe L 1 303E 1 303E 1 303E	6GHz         6GHz           #         IMAC Address           3         48:22:54:64:18E:6           22:54:64:18E:6         22:54:64:18E:73:25:173:56:14           22:20:38:02:73:56:14         22:20:38:02:173:56:14           22:20:38:02:73:56:14         22:20:02:86:15:01:15           8:20:00:186:50:101:5         32:20:00:186:18:37:4           10:20:00:06:18:37:4         20:00:06:18:37:4           10:20:00:06:10:19:43:00:13         00:05:10:10:30:00:13           10:00:06:10:07:07:07:00:13         00:05:10:07:07:00:13           10:00:06:10:07:07:07:07:07:07:07:07:07:07:07:07:07	RSSI           4         -75           4         -82           9         -48           9         -43           1         -37           0         -32           1         -37           1         -37           1         -32	SNR N/A N/A N/A N/A N/A N/A N/A	Channel 2 6 (4 to 8) 3 (1 to 5) 155 (149 to 1 6 (4 to 8) 9 (7 to 11) 42 (36 to 48) 61 (0 to 17)	Band           2.4GHz           2.4GHz           2.4GHz           5GHz           2.4GHz           5GHz           2.4GHz           5GHz           2.4GHz	Width 20 40 40 40 40 40 40 40 40 40 40 40	Add filter 802. b, g, b, g, b, g, a, n, a b, g, b, g, c, n, a
ess Points ces ket analyzer bleshooting w Inventory	SSID Width 40 20 80 40 20 20 20 20 20 40 40 40 80	2.4GHz 802.11 b, g, n b, g, n a, n, ac, ax b, g, n, ax b, g, n b, g, n b, g, n b, g, n b, g, n b, g, n a, n, ac	SGHz         GGHz           Max. Rate         300           150         2268           1084         300           144.4         300           300         300           300         300           300         300           300         300           300         300	Retries           0	WEP	WPA PSK-CCMP PSK-(TKIP[CCMP) PSK-CCMP PSK-(TKIP[CCMP)	WPA2 PSK-CCMP PSK-CCMP PSK-CCMP PSK-CCMP PSK-CCMP PSK-CCMP PSK-CCMP PSK-CCMP	Y Add filter WPA3	- 0 × Prg ÷ WPS 1.0 1.0 1.0	Acrylic Wi-Fi Analyzer Acrylic Wi-Fi Analyzer Sections Consections Consections Actions Show Inventory PCAP Options Reports	SSID Q SSID Q SSID ACT102: D-Link O D-Link Airtel_H Airtel_H GNX883 + (5) SSVSLS Cheeo II. Network graphs Go to section Summary	2.4GHz ( 38498 DIR-015 ( DIR-015 ( DI	GGHz         GGHz           #         IMAC Address           3         48:22:54:64:BE:E           23         28:38:82:73:35:7           22         20:38:82:73:35:14           22         20:38:82:73:35:14           22         20:38:62:73:35:14           20:00:86:50:101:5         8           20:00:86:50:101:5         13           20:00:86:18:3F:4         10           20:00:86:18:3F:4         20:00:86:18:3F:4           Ce info	RSSI 4 -75 4 -82 9 -48 9 -48 9 -48 9 -47 1 -37 0 -32 0 -32 0 -32 0 -32 1 -37 1 -37 1 -37 0 -32 0 -32 1 -37 1 -	SNR N/A N/A N/A N/A N/A N/A N/A	Channel 2 6 (4 to 8) 3 (1 to 5) 155 (149 to 1 6 (4 to 8) 9 (7 to 11) 42 (36 to 48) 44 (0 ± - 47)	Band           2.4GHz           2.4GHz           2.4GHz           5GHz           2.4GHz           5GHz           2.4GHz           5GHz           2.4GHz	▼ / Width 20 40 40 40 80 40 80 80 80 80 80 80 80 80	Add filter 802, <sup>4</sup> b, g, b, g, b, g, b, g, b, g, b, g, c, c, c, c, c
ess Points ces ket analyzer bleshooting w Inventory P Options	SSID Width 40 20 80 40 20 20 20 20 20 40 40 40 40	2.4GHz 802.11 b, g, n b, g, n a, n, ac, ax b, g, n, ax b, g, n b, g, n	SGHz         6GHz           Max. Rate         300           150         2268           1084         300           144.4         300           300         300           866.7         300	Retries           0	WEP	WPA PSK-CCMP PSK-CTKIP[CCMP] PSK-CTKIP[CCMP] PSK-(TKIP[CCMP] PSK-(TKIP[CCMP]	WPA2 PSK-CCMP PSK-CCMP PSK-CCMP PSK-CCMP PSK-CCMP PSK-CCMP PSK-CCMP PSK-CCMP PSK-CCMP PSK-CCMP PSK-CTKIP[CCMP] PSK-CTKIP[CCMP]	Y Add filter WPA3	- 0 ×	Acrylic Wi-Fi Analyzer Acrylic Wi-Fi Analyzer Sections Consections Consections Actions Consections Packet analyzer Consections Consections Packet analyzer Consections Consections Packet analyzer Consections Consections Packet analyzer Consections	SSID Q SSID Q SSID ACT102: D-Link O D-Link Airtel_H Airtel_H GNXS33 + (3) SSVSLS Chancel quality	2.4GHz ( 38498 DIR-615 ( DIR-615 ( OUSe L 303E 7 0 Devic 7 0 10 0	5GHz         6GHz           #         IMAC Address           3         48:22:54:64:BE:E           22:03:38:02:73:56:4         12           20:03:86:50:01:5         12           20:00:86:50:01:5         13           20:00:86:10:37:4         10           20:00:86:13:37:4         10           20:00:86:13:37:4         10           ce info         IN Network	RSSI       A     -75       4     -82       9     -88       9     -48       9     -43       1     -37       1     -32       quality	snr N/A N/A N/A N/A N/A N/A N/A N/A	Channel 2 6 [4 to 8] 3 [1 to 5] 155 [149 to 1 6 [4 to 8] 9 [7 to 11] 42 [36 to 48] 44 [0 ± 47]	Band           2.4GHz           2.4GHz           2.4GHz           5GHz           2.4GHz           5GHz           0.4GHz	▼ / Width 20 40 40 40 40 40 80 80 80 80 **	Add filter 802 b, g, b, g, d, t, d
c Wi-Fi Analyzer p capture eses Points icces ket analyzer ubleshooting wi Inventory P Options	SSID Width 40 20 80 40 20 20 20 20 20 40 40 40 40 40	Q 2.4GHz 802.11 b, g, n b, g, n a, n, ac, ax b, g, n, ax b, g, n, ax b, g, n b, g, n b	SGHz         6GHz           Max. Rate         300           1150         2268           1084         300           144.4         300           300         866.7           300         300	Retries           0	WEP	WPA PSK-CCMP PSK-CCMP PSK-(TKIP[CCMP] PSK-(TKIP[CCMP] PSK-(TKIP[CCMP] PSK-(TKIP[CCMP]	WPA2 PSK-CCMP PSK-CCMP PSK-CCMP PSK-CCMP PSK-CCMP PSK-CCMP PSK-CCMP PSK-CCMP PSK-CCMP PSK-CCMP PSK-CCMP PSK-CCMP PSK-(TKIP]CCMP) PSK-(TKIP]CCMP)	✓ Add filter WPA3	- 0 × Prg ÷ WPS 1.0 1.0 1.0 1.0 1.0	Acrylic Wi-Fi Analyzer Composition Sections Composition Compositio	SSID Q SSID ACTION ACTION D-Link O-Link Airtel_H Airtel_H GNXS33 + (3) SSVSLS Obsolution Summary Channel quality Signal quality	2.4GHz ( 38498 DIR-015 ( DIR-015 ( DI	5GHz         6GHz           #         IMAC Address           3         48:22:54:64:BE:6           23         28:38:62:73:35:7           22         20:38:62:73:35:7           22         20:38:62:73:35:61:4           12         20:00:86:50:01:5           8         20:00:86:50:01:5           13         20:00:86:18:3F:4           10         20:00:86:18:3F:4           12         20:00:86:18:3F:4           13         20:00:86:18:3F:4           14         20:00:86:18:3F:4           15         20:00:86:18:3F:4           16         Point Control (Point	RSSI 4 -75 4 -82 9 -48 9 -48 9 -48 9 -47 1 -37 0 -37 0 -37 0 -37 0 -37 1 -37 1 -37 1 -37 0 -37 1 -37 -37 -37 -37 -37 -37 -37 -37	SNR N/A N/A N/A N/A N/A N/A N/A N/A N/A SCCMI 2-PSK	Channel 2 6 (4 to 8) 3 (1 to 5) 155 (149 to 1 6 (4 to 8) 9 (7 to 11) 42 (36 to 48) 44 (0 to 47)	Band           2.4GHz           2.4GHz           2.4GHz           5GHz           2.4GHz           5GHz           2.4GHz	Viidth 20 40 40 40 40 40 40 40 40 40 40 40 40 40	Add filter 802. b, g, b, g, b, g, b, g, b, g, b, g, c, n, a b, g, b, g, c, n, a c, n,
cess Points	SSID Width 40 20 80 40 20 20 20 20 20 40 40 40 40 40 40 80 40	Q 2.4GHz 802.11 b, g, n b, g, n a, n, ac, ax b, g, n, ax b, g, n, ax b, g, n, ax b, g, n b, g, g, g, n b, g, g, g, g, g, g,	SCHz         6GHz           Max. Rate         300           300         2268           1084         300           1084         300           144.4         300           300         866.7           300         300           866.7         300           300         866.7	Retries           0	WEP	WPA PSK-CCMP PSK-CCMP PSK-(TKIP[CCMP] PSK-CTKIP[CCMP] PSK-(TKIP[CCMP] PSK-(TKIP[CCMP] PSK-(TKIP[CCMP]	WPA2 PSK-CCMP PSK-CCMP PSK-CCMP PSK-CCMP PSK-CCMP PSK-CCMP PSK-CCMP PSK-CCMP PSK-CCMP PSK-CCMP PSK-(TKIP[CCMP] PSK-(TKIP[CCMP] PSK-(TKIP[CCMP]	VPA3	- 0 × -	Acrylic Wi-Fi Analyzer Corporations Sections Corporatio	SSID Q SSID ACT1024 D-Link D-Link Airtel_H Airtel_H GNXS33 + (3) SSVSLS Channel quality Signal quality	2.4GHz ( 38498 DIR-615 ( DIR-615 ( 0008 L 303E 7 0 0 0 0 0 0 0 0 0 0 0 0 0	SGHz         6GHz           #         IMAC Address           3         48:22:54:64:BE:6           23         28:3B:82:73:56:4           12         20:00:86:50:D1:5           8         20:00:86:50:D1:5           13         20:00:86:50:D1:5           14         20:00:86:150:D1:5           15         20:00:86:150:D1:5           16         20:00:86:18:3F:4           17         20:00:86:18:3F:4           10         20:00:86:18:3F:4           10         20:00:86:18:3F:4           10         20:00:86:18:3F:4           10         20:00:86:18:3F:4           10         20:00:86:18:3F:4           10         20:00:86:18:3F:4           11         20:00:86:18:3F:4           12         20:00:86:18:3F:4           13         20:00:86:18:3F:4           14         20:00:86:18:3F:4           15         20:00:86:18:3F:4           16         20:00:86:18:3F:4           17         20:00:86:18:3F:4           18         20:00:86:18:3F:4           19         20:00:86:18:3F:4           10         20:00:86:18:3F:4           10         20:00:86:18:3F:4	RSSI       4     -75       4     -82       9     -86       9     -48       1     -37       0     -32       0     -32       0     TKIPI	SNR N/A N/A N/A N/A N/A N/A N/A N/A SCOMI 2-PSK CCMI	Channel 2 6 [4 to 8] 3 [1 to 5] 155 [149 to 1 6 [4 to 8] 9 [7 to 11] 42 [36 to 48] 47 [0 to 47]	Band           2.4GHz           2.4GHz           2.4GHz           5GHz           2.4GHz           5GHz           2.4GHz           5GHz           2.4GHz           80Hz	Viidth     20     40	Add filter 802. b, g, b, g, b, g, b, g, b, g, b, g, c, n, a b, g, b, g, c, n, a c, n,
c Wi-Fi Analyzer p capture cess Points vices cket analyzer ubleshooting ow Inventory AP Options	SSID Width 40 20 80 40 20 20 20 20 20 20 40 40 40 40 40 40 40 40	2.4GHz 802.11 b, g, n b, g, n a, n, ac, ax b, g, n, ax b, g, n, ax b, g, n, ax b, g, n, ax b, g, n b,	SCHz         6GHz           Max. Rate         300           150         2268           1084         300           144.4         300           300         866.7           300         300           866.7         300           300         300           300         300	Retries           0	WEP	WPA PSK-CCMP PSK-CCMP PSK-(TKIP[CCMP] PSK-(TKIP[CCMP] PSK-(TKIP[CCMP] PSK-(TKIP[CCMP] PSK-(TKIP[CCMP] PSK-(TKIP[CCMP] PSK-(TKIP[CCMP]	WPA2 PSK-CCMP PSK-CCMP PSK-CCMP PSK-CCMP PSK-CCMP PSK-CTKIP[CCMP] PSK-CTKIP[CCMP] PSK-(TKIP[CCMP] PSK-(TKIP[CCMP] PSK-(TKIP[CCMP] PSK-(TKIP[CCMP] PSK-CTKIP[CCMP]	Add filter  WPA3	- 0 × PG = WPS 1.0 1.0 1.0 1.0 1.0 1.0 1.0 1.0	Acrylic Wi-Fi Analyzer Corrections Correct	SSID Q SSID ACT1024 D-Link D-Link Airtel_H Airtel_H GNX583 + (3) SSV5LS Channel quality Channel quality Signal quality Network security	2.4GHz 5 38498 DIR-615 2 DIR-615 2 DI	SCHz         6GHz           #         IMAC Address           3         48:22:54:64:BE:6           23         28:3B:82:73:A5:7           22         20:3B:82:73:A5:7           22         20:3B:82:73:A5:7           22         20:3B:82:73:A5:7           22         20:0C:86:50:D1:5           8         20:0C:86:10:15           13         20:0C:86:1B:37:4           14         20:0C:86:1B:37:4           10         20:0C:86:1B:37:4 <t< td=""><td>RSSI 4 -75 4 -82 9 -48 9 -48 9 -48 9 -47 1 -32 0 -</td><td>SNR N/A N/A N/A N/A N/A N/A N/A N/A SCCMI 2-PSK CCMI 2-PSK</td><td>Channel 2 6 [4 to 8] 3 [1 to 5] 155 [149 to 1 6 [4 to 8] 9 [7 to 11] 42 [36 to 48] 47 [0 to 47]</td><td>Band 2.4GHz 2.4GHz 2.4GHz 2.4GHz 2.4GHz 5GHz 2.4GHz 5GHz 2.4GHz 8GHz 9.4GHZ 9.4</td><td>Viidth 20 40 40 80 40 80 40 80 60 80 60 80 80 80 80 80 80 80 80 80 80 80 80 80</td><td>Add filter 802.1 b, g, l b, g, l b, g, l b, g, l b, g, l b, g, l b, g, l c securities</td></t<>	RSSI 4 -75 4 -82 9 -48 9 -48 9 -48 9 -47 1 -32 0 -	SNR N/A N/A N/A N/A N/A N/A N/A N/A SCCMI 2-PSK CCMI 2-PSK	Channel 2 6 [4 to 8] 3 [1 to 5] 155 [149 to 1 6 [4 to 8] 9 [7 to 11] 42 [36 to 48] 47 [0 to 47]	Band 2.4GHz 2.4GHz 2.4GHz 2.4GHz 2.4GHz 5GHz 2.4GHz 5GHz 2.4GHz 8GHz 9.4GHZ 9.4	Viidth 20 40 40 80 40 80 40 80 60 80 60 80 80 80 80 80 80 80 80 80 80 80 80 80	Add filter 802.1 b, g, l b, g, l b, g, l b, g, l b, g, l b, g, l b, g, l c securities
ic Wi-Fi Analyzer	SSID Width 40 20 80 40 20 20 20 20 20 20 40 40 40 40 40 40 40 80 80 80	2.4GHz 802.11 b, g, n b, g, n d, n, ac, ax b, g, n, ax b, g, n, ax b, g, n, ax b, g, n, ax b, g, n b, g, n b, g, n b, g, n d, n, ac b, g, n b, g, n d, n, ac b, g, n d, n d, n, ac b, g, n d, n d, n d, n d, n d, n d, n d, n d	SCH2     6CH2       Max. Rate       300       150       2268       1084       300       144.4       300       300       300       300       300       300       300       300       866.7       300       866.7       300	Retries           0	WEP	WPA WPA PSK-CCMP PSK-CCMP PSK-(TKIP[CCMP] PSK-(TKIP[CCMP] PSK-(TKIP[CCMP] PSK-(TKIP[CCMP] PSK-(TKIP[CCMP] PSK-(TKIP[CCMP] PSK-(TKIP[CCMP] PSK-(TKIP[CCMP] PSK-(TKIP[CCMP] PSK-(TKIP[CCMP]) PSK-(TKIP[CCMP] PSK-(TKIP[CCMP])	WPA2 PSK-CCMP PSK-CCMP PSK-CCMP PSK-CCMP PSK-CCMP PSK-CCMP PSK-CCMP PSK-CCMP PSK-CCMP PSK-(TKIP[CCMP] PSK-(TKIP[CCMP] PSK-(TKIP[CCMP] PSK-CKMP	Add filter  WPA3	- 0 × PG = WPS 1.0 1.0 1.0 1.0 1.0 1.0 1.0 1.0	Acrylic Wi-Fi Analyzer Coordination of the sector of the	SSID Q SSID ACT1024 D-Link D-Link Airtel_H Airtel_H GNX583 + (3) SSV513 Channel quality Signal quality Signal quality Network security Transmission speed	2.4GHz 5 38498 DIR-615 2 DIR-615 2 DIR-615 2 JOUSE L 303E 7 0 0 0 0 0 0 0 0 0 0 0 0 0	SGHz         6GHz           #         IMAC Address           3         40:22:54:64:BE:6           23         20:3B:02:73:56:4           12         20:02:86:50:D1:5           8         20:02:86:50:D1:5           13         20:02:86:1B:37:4           14         20:00:86:1B:37:4           15         00:00:86:1B:37:4           16         00:00:86:1B:37:4           17         00:00:86:1B:37:4           18         00:00:86:1B:37:4           19         00:00:86:1B:37:4           10         20:00:86:1B:37:4           10         20:00:86:1B:37:4           10         20:00:86:1B:37:4           10         20:00:86:1B:37:4           10         20:00:86:1B:37:4           10         20:00:86:1B:37:4           11         20:00:86:1B:37:4           12         00:90:97:40:4         0           13         20:00:86:1B:37:4         0           14         00:90:97:40:4         0           15         00:97:40:4         0           16         00:97:40:4         0           17         00:97:40:4         0           18         00:97:40:4         0 <td>RSSI A -75 4 -82 9 -48 9 -48 9 -47 1 -37 0 -32 0 -32 0 -32 0 -32 0 -37 1 -37 1 -37 1 -37 1 -57 1 -</td> <td>SNF N/A N/A N/A N/A N/A N/A SMA SMA SMA SMA SMA SMA SMA SMA SMA SM</td> <td>Channel 2 6 [4 to 8] 3 [1 to 5] 155 [149 to 1 6 [4 to 8] 9 [7 to 11] 42 [36 to 48] 41 [0 to 42] P C P</td> <td>Band 2.4GHz 2.4GHz 2.4GHz 2.4GHz 2.4GHz 3.6GHz 2.4GHz 3.6GHz 3.4GHz 4.4GHZ 4.4G</td> <td>Viidth     20     40     40     40     40     40     40     80     40     40     80     40     80     40     80     60</td> <td>Add filter 802.<sup>4</sup> b, g, b, g, b, g, b, g, b, g, b, g, b, g, b, g, l, d, n, a c</td>	RSSI A -75 4 -82 9 -48 9 -48 9 -47 1 -37 0 -32 0 -32 0 -32 0 -32 0 -37 1 -37 1 -37 1 -37 1 -57 1 -	SNF N/A N/A N/A N/A N/A N/A SMA SMA SMA SMA SMA SMA SMA SMA SMA SM	Channel 2 6 [4 to 8] 3 [1 to 5] 155 [149 to 1 6 [4 to 8] 9 [7 to 11] 42 [36 to 48] 41 [0 to 42] P C P	Band 2.4GHz 2.4GHz 2.4GHz 2.4GHz 2.4GHz 3.6GHz 2.4GHz 3.6GHz 3.4GHz 4.4GHZ 4.4G	Viidth     20     40     40     40     40     40     40     80     40     40     80     40     80     40     80     60	Add filter 802. <sup>4</sup> b, g, b, g, b, g, b, g, b, g, b, g, b, g, b, g, l, d, n, a c

## 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.

- I am going to use the <u>Rockyou wordlist</u> 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.o<u>rg</u>/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



#### 3. Do Port Scanning to identify the Open Ports

HIDE	New Policy / Advar	nced Scan
My Scans     All Scans	Settings Credentials	Plugins
<ul> <li>Trash</li> <li>RESOURCES</li> <li>Policies</li> <li>Plugin Rules</li> <li>Scanners</li> <li>TEMABLE</li> <li>Community</li> <li>Research</li> </ul>	BASIC >> DISCOVERY > Host Discovery Port Scanning Service Discovery ASSESSMENT >> REPORT >> ADVANCED >>	Ports         Consider unscanned ports as closed         Port scan range:         default         Local Port Enumerators         SSH (netstat)         WMM (netstat)         SNMP         Only run network port scanners if local port enumeration failed         Verify open TCP ports found by local port enumerators
Tenable News The 'Next Chapter' in Cyber Risk: Are Federal Agen Read More		Network Port Scanners TCP Override automatic firewall detection Use soft detection
۷ «		Use aggressive detection

#### 2. Fill the Target Details

0

.

2

					A new version of Nessus is available and ready to install. Learn more or apply it now.					
essus fessional	Scans Setting	16				🔺 admin 🔔				
s y Scans	Unauthentie « Back to Scan B	cated Advi Report	ance Vulnerab	ility Scan /	Configuration					
actice	Settings	Credentials	Compliance	Plugins						
ish	BASIC	~	General Setting							
	= General		Name		Unwitherticated Advances Millinershills Scop					
dician	Schedule				Oneurientouried Advance Constanting Scient					
ucio Rulee	Notificatio	ons	Description		This is unauthenticated artvance web					
istomized Reports	DISCOVERY				vulnerability scan.					
	ASSESSMENT									
	REPORT	REPORT , Folder My Boans *								
ommunity	ADVANCED									
ugin Release Notes			Unlosd Targets		And Dis					
	Save	Cancel	Post-Processing Live Results Enabling this of	ption will identi	y potential linuaria discovered by plugina added during updates without actively solaring segats. Note that this requires the RB to be included in the scan result.					

#### 4. Run Scan, and find the Results

Nessus Scans 2 Polici	ies	pmuser 👻 🌅
Agent Scan 24-Feb current results: february 24 at 9:09 am		Audit Trail Export 💌
Scans > Dashboard Hosts 2 Vulnerabilit	ies 85 Remediations 15 Notes 1 History	
Current Vulnerabilities		
CRITICAL HIGH	7 З	65 85 INFO TOTAL
Operating System Comparison	Vulnerability Comparison	Host Count Comparison
	Info     Low     High	• Without auth
Top Hosts		Top Vulnerabilities
NESPM-AGE 10 7 3	65	MS KB2269637: Insecure Library Loading Could Al
NESPM-AGE 4 3	65	MS KB2719662; Vulnerabilities in Gadgets Could A

## 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.

			kali@kali: ~	- • ×
File Actio	ns Edit View Help			
root@ka	li:/home/kali# a	irmon-ng		1
РНҮ	Interface	Driver	Chipset	
phy0	wlan0	iwlwifi	Intel Corporation Wireless-AC 9560 [Jefferson Peak] (rev 1	0)
root@ka	li:/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

in incertace i

Chipset

phy0wlan0ath9k\_htcAtheros 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 atho

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.

atho is the interface name.

CH 9 ][ Elapsed:	4 s ][ 2007-03-24 1	L6:58 ][ 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 <u>NetSpot</u>.

#### **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**

#### Comprehensive Testing

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

Compliance

Meeting ITSAR requirements for Wi-Fi CPE security.

### Secure by Design

Implementing robust security measures from the ground up.





1

2

3

## Thank You!



https://graniteriverlabs.com/