

Articles sur le piratage

Le blog de Raj Chandel

Menu

🏠 Maison » Tests de pénétration sans fil » Tests de pénétration sans fil : découverte du SSID

[Tests de pénétration sans fil](#)

Tests de pénétration sans fil : découverte du SSID

25 Juillet 2021 Par Raj

Cet article décrira « Comment découvrir le SSID pour un réseau WiFi » à l'aide de plusieurs outils conçus pour les plates-formes Windows et Linux. La découverte du SSID est applicable au piratage Wi-Fi ou aux tests d'intrusion.

Table des matières

- dansSSIDer
- NetView sans fil
- Moniteur réseau Microsoft
- NetSurveyor
- Kismet
- Airodump-ng
- Laver
- Requin filaire

L'acronyme SSID est utilisé pour **Service Set Identifier**, également connu sous le nom d'identification du réseau, qui est le nom du réseau sans fil. Ceci peut être consulté par toute personne disposant d'un appareil sans fil à portée de votre réseau. Il peut contenir jusqu'à 32 caractères et est sensible à la casse de votre choix.





☒ Enable Wireless Radio

Network Name (SSID): ☐ Hide SSID

Security:

Type: ☒ Auto ☐ Open System ☐ Shared Key

WEP Key Format: ☐ ASCII ☒ Hexadecimal

Key Type: ☒ 64-bit ☐ 128-bit

Key Value:

Mode:

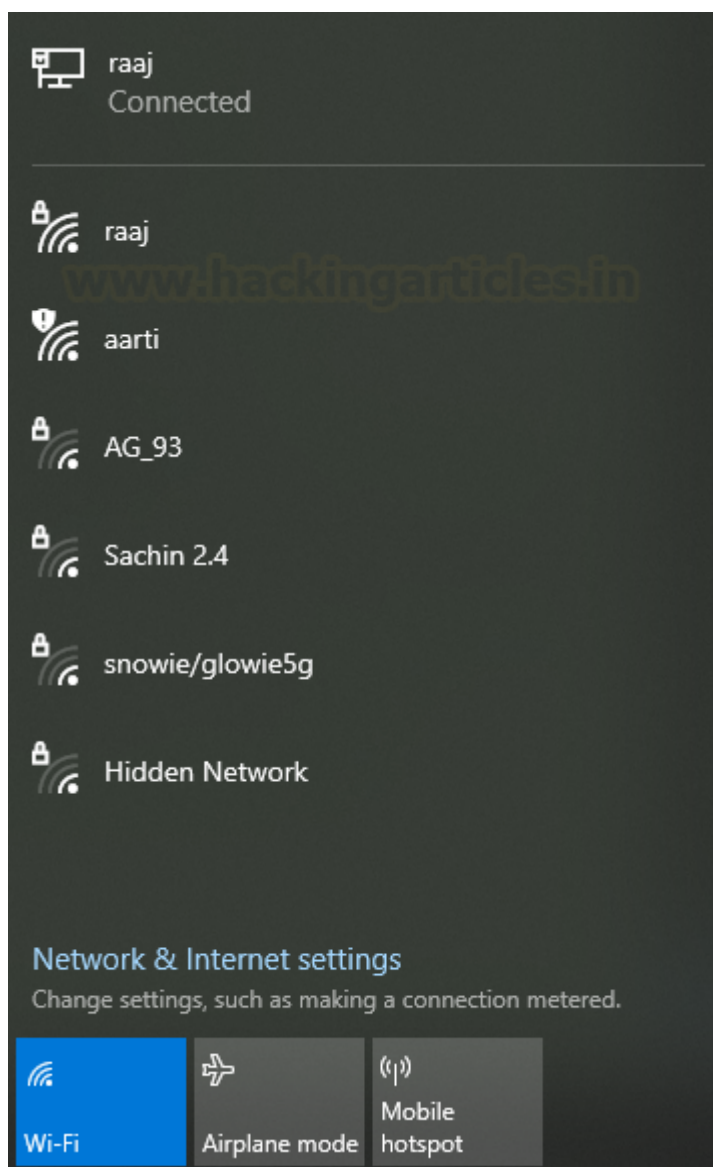
Channel Width:

Channel:

Transmit Power: ☐ Low ☐ Middle ☒ High

[Save](#)

Une fois que le gestionnaire de réseau a configuré le SSID, le routeur ou une autre station de base Wi-Fi le diffuse dans la région environnante. Ensuite, lorsqu'un appareil scanne les réseaux voisins, ses SSID sont affichés : l'utilisateur n'a qu'à en choisir un et à se connecter à l'appareil.



Dans le test Wi-Fi, nous devons découvrir le SSID, la sécurité, les canaux et le client connecté pour une exploitation ultérieure. A travers cet article, je divulgue quelques noms d'outils qui pourront vous aider à découvrir les éléments suivants :

- Nom du réseau Wi-Fi
- Adresse Mac
- Canal
- Mode Wi-Fi
- Client
- Sécurité

dansSSIDer

inSSIDer analyse la configuration de votre WiFi, y compris les paramètres des canaux, la sécurité, la force du signal et l'impact des réseaux WiFi voisins. Il est facile à installer et à utiliser pour énumérer les réseaux WiFi voisins.

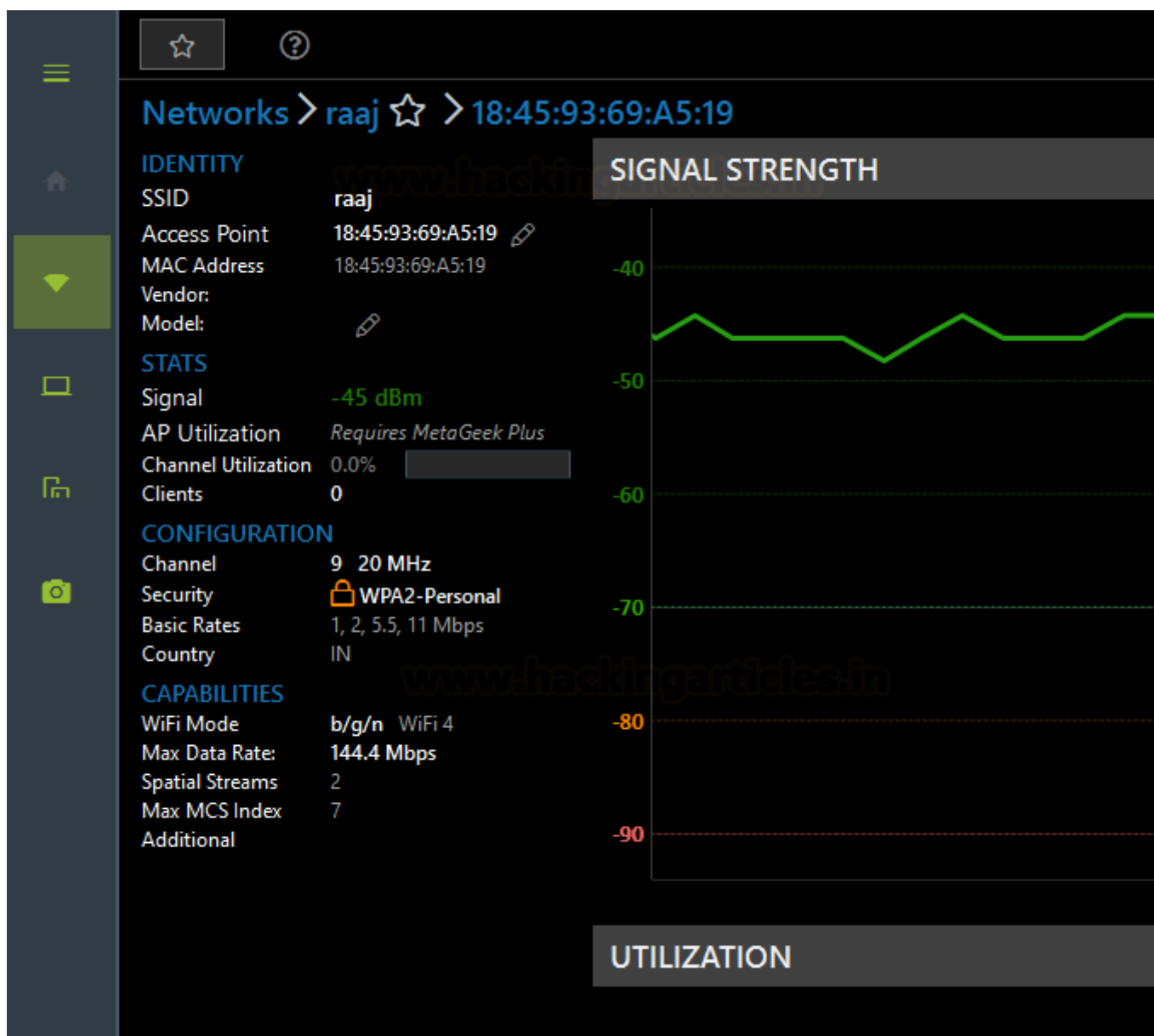
Téléchargez-le à partir d' [ici](#)



	☆		?	FILTERS:	ALL	{HIDDEN}				
	📄	SSID	Signal	Radios	Clients	Channels	Security	Mode	Max Rate	Last Seen
		aarti	-39 dBm	1	-	11	🔒	b/g	54.0	now
		raaj	-45 dBm	1	-	9	🔒	b/g/n	144.4	now
		Amit 2.4G	-81 dBm	1	-	1	🔒	b/g/n	216.7	now
		[HIDDEN] on AG_93	-83 dBm	1	-	11	🔒	n	144.4	< 30 sec ago
		Mehak jain_4G	-85 dBm	1	-	11	🔒	n	144.4	now
		AG_93	-85 dBm	1	-	11	🔒	n	144.4	now
		Sachin 2.4	-85 dBm	1	1	1	🔒	b/g/n	216.7	now
		703 jio_4G	-87 dBm	1	-	11	🔒	n	144.4	now
		[HIDDEN] on Mehak jain_4G	-87 dBm	1	-	11	🔒	n	144.4	now
		Vikas	-87 dBm	1	-	5	🔒	b/g/n	130.0	now
		[HIDDEN] on AA:DA:0C:58:3	-87 dBm	1	-	10	🔒	n	144.4	1 min ago
		[HIDDEN] on 703 jio_4G	-89 dBm	1	-	11	🔒	n	144.4	< 1 min ago
		601 2.4G	-89 dBm	1	1	1	🔒	b/g/n	216.7	1 min ago
		snowie/glowie5g	-91 dBm	1	1	5	🔒	b/g/n	144.4	< 30 sec ago
		Kavz	-91 dBm	1	-	7	🔒	b/g/n	144.4	< 30 sec ago

Après exécution, il listera tous les SSID et sélectionnera un SSID qui vous intéresse.





NetView sans fil

Wireless NetView est un petit utilitaire qui s'exécute en arrière-plan et surveille l'activité des réseaux sans fil autour de vous. Pour chaque réseau détecté, il affiche les informations suivantes : SSID, qualité du dernier signal, qualité moyenne du signal, compteur de détection, algorithme d'authentification, algorithme de chiffrement, adresse MAC, RSSI, fréquence du canal, numéro de canal, etc.

Téléchargez-le à partir d' [ici](#)

Cet outil est très simple à utiliser, décompressez le dossier et exécutez le fichier exécutable qui lancera l'analyse SSID et listera les réseaux Wi-Fi voisins.

WirelessNetView

File Edit View Options Help

SSID	Last Sig...	Average Si...	Detect...	% Detection	Security En...	Connect...	Authentication
aarti	30%	30%	1	20.0%	Yes	Yes	802.11 Open
Sachin 2.4	34%	33%	4	80.0%	Yes	Yes	RSNA-PSK
Vikas	22%	22%	1	20.0%	Yes	Yes	RSNA-PSK

3 Wireless Networks NirSoft Freeware. <http://www.nirsoft.net>

Moniteur réseau Microsoft

Microsoft Network Monitor est un outil permettant d'afficher le contenu des paquets réseau envoyés et reçus via une connexion réseau en direct ou à partir d'un fichier de données précédemment capturé. Il fournit des options de filtrage pour l'analyse complexe des données réseau.

Remarque : Pour utiliser cet outil, vous aurez peut-être besoin d'un adaptateur Wi-Fi externe.

Vous pouvez le télécharger à partir d' [ici](#) :

Microsoft Network Monitor 3.4

File Edit View Frames Capture Filter Experts Tools Help

New Capture Open Capture Save As Capture Settings Start Pause Stop

Capture1 Start Page Parsers

Frame Summary

Find Autoscroll

Fr...	Description	Time Offset	Source
1	NetmonFilter:Updated Capture Filter: None	0.0130384	
2	NetworkInfoEx:Network info for , Network Adapter Count = 1	0.0130384	
3	WiFi: [ManagementBeacon] RSSI = -77 dBm, Rate = 3.5 Mbps, SSID = aarti, Channel = 11	0.0130384	[D84732 E93F33]
4	WiFi: [ManagementBeacon] RSSI = -77 dBm, Rate = 3.5 Mbps, SSID = AG_93, Channel = 11	0.0160101	[94FBA7 6A06AF]
5	WiFi: [ManagementBeacon] RSSI = -77 dBm, Rate = 3.5 Mbps, SSID = BroadCast SSID, Channel = 11	0.0193294	[96FBA7 5A06AF]
6	WiFi: [ManagementBeacon] RSSI = -77 dBm, Rate = 3.5 Mbps, SSID = Mehak jain_4G, Channel = 11	0.0737218	[A8DA0C 36DD82]
7	WiFi: [ManagementBeacon] RSSI = -77 dBm, Rate = 3.5 Mbps, SSID = aarti, Channel = 11	0.1154529	[D84732 E93F33]
8	WiFi: [ManagementBeacon] RSSI = -77 dBm, Rate = 3.5 Mbps, SSID = AG_93, Channel = 11	0.1184536	[94FBA7 6A06AF]
9	WiFi: [ManagementBeacon] RSSI = -77 dBm, Rate = 3.5 Mbps, SSID = BroadCast SSID, Channel = 11	0.1217658	[96FBA7 5A06AF]
10	WiFi: [ManagementBeacon] RSSI = -77 dBm, Rate = 3.5 Mbps, SSID = Mehak jain_4G, Channel = 11	0.1761015	[A8DA0C 36DD82]
11	WiFi: [ManagementBeacon] RSSI = -77 dBm, Rate = 3.5 Mbps, SSID = BroadCast SSID, Channel = 11	0.1820669	[AADA0C 16DD82]
12	WiFi: [ManagementBeacon] RSSI = -77 dBm, Rate = 3.5 Mbps, SSID = BroadCast SSID, Channel = 11	0.2145176	[C28F20 19C5B2]
13	WiFi: [ManagementBeacon] RSSI = -77 dBm, Rate = 3.5 Mbps, SSID = aarti, Channel = 11	0.2178508	[D84732 E93F33]
14	WiFi: [ManagementBeacon] RSSI = -77 dBm, Rate = 3.5 Mbps, SSID = AG_93, Channel = 11	0.2208729	[94FBA7 6A06AF]
15	WiFi: [ManagementBeacon] RSSI = -77 dBm, Rate = 3.5 Mbps, SSID = BroadCast SSID, Channel = 11	0.2246620	[96FBA7 5A06AF]
16	WiFi: [ManagementBeacon] RSSI = -77 dBm, Rate = 3.5 Mbps, SSID = Mehak jain_4G, Channel = 11	0.2786083	[A8DA0C 36DD82]
17	WiFi: [ManagementBeacon] RSSI = -77 dBm, Rate = 3.5 Mbps, SSID = AG_93, Channel = 11	0.3232530	[94FBA7 6A06AF]
18	WiFi: [ManagementBeacon] RSSI = -77 dBm, Rate = 3.5 Mbps, SSID = BroadCast SSID, Channel = 11	0.3265792	[96FBA7 5A06AF]
19	WiFi: [ManagementBeacon] RSSI = -77 dBm, Rate = 3.5 Mbps, SSID = Mehak jain_4G, Channel = 11	0.3808941	[A8DA0C 36DD82]
20	WiFi: [ManagementBeacon] RSSI = -77 dBm, Rate = 3.5 Mbps, SSID = BroadCast SSID, Channel = 11	0.4175165	[C28F20 19C5B2]
21	WiFi: [ManagementBeacon] RSSI = -77 dBm, Rate = 3.5 Mbps, SSID = aarti, Channel = 11	0.4226624	[D84732 E93F33]
22	WiFi: [ManagementBeacon] RSSI = -77 dBm, Rate = 3.5 Mbps, SSID = BroadCast SSID, Channel = 11	0.4289757	[96FBA7 5A06AF]
23	WiFi: [ManagementBeacon] RSSI = -77 dBm, Rate = 3.5 Mbps, SSID = Mehak jain_4G, Channel = 11	0.4833103	[A8DA0C 36DD82]
24	WiFi: [ManagementBeacon] RSSI = -77 dBm, Rate = 3.5 Mbps, SSID = BroadCast SSID, Channel = 11	0.4870996	[AADA0C 16DD82]
25	WiFi: [ManagementBeacon] RSSI = -77 dBm, Rate = 3.5 Mbps, SSID = aarti, Channel = 11	0.5251336	[D84732 E93F33]
26	WiFi: [ManagementBeacon] RSSI = -77 dBm, Rate = 3.5 Mbps, SSID = BroadCast SSID, Channel = 11	0.5313752	[96FBA7 5A06AF]
27	WiFi: [ManagementBeacon] RSSI = -77 dBm, Rate = 3.5 Mbps, SSID = Mehak jain_4G, Channel = 11	0.5857259	[A8DA0C 36DD82]
28	WiFi: [ManagementBeacon] RSSI = -77 dBm, Rate = 3.5 Mbps, SSID = BroadCast SSID, Channel = 11	0.5913118	[AADA0C 16DD82]
29	WiFi: [ManagementBeacon] RSSI = -77 dBm, Rate = 3.5 Mbps, SSID = aarti, Channel = 11	0.6274706	[D84732 E93F33]
30	WiFi: [ManagementBeacon] RSSI = -77 dBm, Rate = 3.5 Mbps, SSID = BroadCast SSID, Channel = 11	0.6339520	[96FBA7 5A06AF]
31	WiFi: [ManagementBeacon] RSSI = -77 dBm, Rate = 3.5 Mbps, SSID = Mehak jain_4G, Channel = 11	0.6880990	[A8DA0C 36DD82]
32	WiFi: [ManagementBeacon] RSSI = -77 dBm, Rate = 3.5 Mbps, SSID = 703 jio_4G, Channel = 11	0.7206670	[C08F20 39C5B2]
33	WiFi: [ManagementBeacon] RSSI = -77 dBm, Rate = 3.5 Mbps, SSID = BroadCast SSID, Channel = 11	0.7247053	[C28F20 19C5B2]
34	WiFi: [ManagementBeacon] RSSI = -77 dBm, Rate = 3.5 Mbps, SSID = BroadCast SSID, Channel = 11	0.7362070	[96FBA7 5A06AF]
35	WiFi: [ManagementBeacon] RSSI = -77 dBm, Rate = 3.5 Mbps, SSID = Mehak jain_4G, Channel = 11	0.7906865	[A8DA0C 36DD82]
36	WiFi: [ManagementBeacon] RSSI = -77 dBm, Rate = 3.5 Mbps, SSID = BroadCast SSID, Channel = 11	0.7967137	[AADA0C 16DD82]
37	WiFi: [ManagementBeacon] RSSI = -77 dBm, Rate = 3.5 Mbps, SSID = aarti, Channel = 11	0.8327627	[D84732 E93F33]

NetSurveyor

NetSurveyor is a diagnostic tool that falls under the category of WiFi Scanners or 802.11 Network Discovery Tools. The best known in this category is NetStumbler. A discovery tool reports the Service Set Identifier (SSID) for each wireless network it detects, along with the channel used by the access point (AP) servicing that network.

You can download it from [here](#):

	SSID	BSSID (MAC)	Cha...	Bea...	Beaco...	Signal Quality	Radio Type	Encryption	Active
▶	UNKNOWN_SSID_...	96:fb:a7:5a:06:af	11	-100	2	No Signal	Unknown	YES	NO
	aarti	d8:47:32:e9:3f:33	11	-39	77	Excellent	OFDM24	YES	YES
	raaj	18:45:93:69:a5:19	9	-45	70	Excellent	Unknown	YES	YES
	UNKNOWN_SSID_...	aa:da:0c:16:dd:82	11	-100	2	No Signal	Unknown	YES	NO
	Amit 2.4G	68:14:01:5a:0e:9c	1	-100	2	No Signal	Unknown	YES	NO
	UNKNOWN_SSID_...	c2:8f:20:19:c5:b2	11	-100	2	No Signal	Unknown	YES	NO
	Sachin 2.4	40:49:0f:3c:49:88	1	-77	30	Low	Unknown	YES	YES
	AG_93	94:fb:a7:6a:06:af	11	-100	2	No Signal	Unknown	YES	NO
	A602_4G	a8:da:0c:78:34:fe	10	-100	2	No Signal	Unknown	YES	NO
	ajoy	70:c7:f2:ed:6a:44	4	-100	2	No Signal	Unknown	YES	NO
	Vikas	30:cc:21:e3:47:88	8	-85	20	Very Low	Unknown	YES	YES
	Mehak jain_4G	a8:da:0c:36:dd:82	11	-100	2	No Signal	Unknown	YES	NO
	703 jio_4G	c0:8f:20:39:c5:b2	11	-100	2	No Signal	Unknown	YES	NO
	snowie/glowie5g	6c:eb:b6:2f:83:34	5	-100	2	No Signal	Unknown	YES	NO
	UNKNOWN_SSID_...	aa:da:0c:1c:fc:a3	1	-89	16	Very Low	Unknown	YES	YES
	Kavz	74:5a:aa:76:66:44	7	-100	2	No Signal	Unknown	YES	NO
	Tan_4	a8:da:0c:1c:fc:a3	1	-100	2	No Signal	Unknown	YES	NO
	UNKNOWN_SSID_...	aa:da:0c:58:34:fe	10	-100	2	No Signal	Unknown	YES	NO

Kismet

Kismet is an 802.11 layer-2 wireless network and device detector, sniffer, wardriving tool, and WIDS (wireless intrusion detection) framework. Kismet works with Wi-Fi interfaces, Bluetooth interfaces, some SDR (software-defined radio) hardware like the RTLSDR, and other specialized capture hardware. Kismet works on Linux, OSX, and, to a degree, Windows 10 under the WSL framework.

Start the Kismet server, using the wireless interface as the capture source (-c wlan0mon)

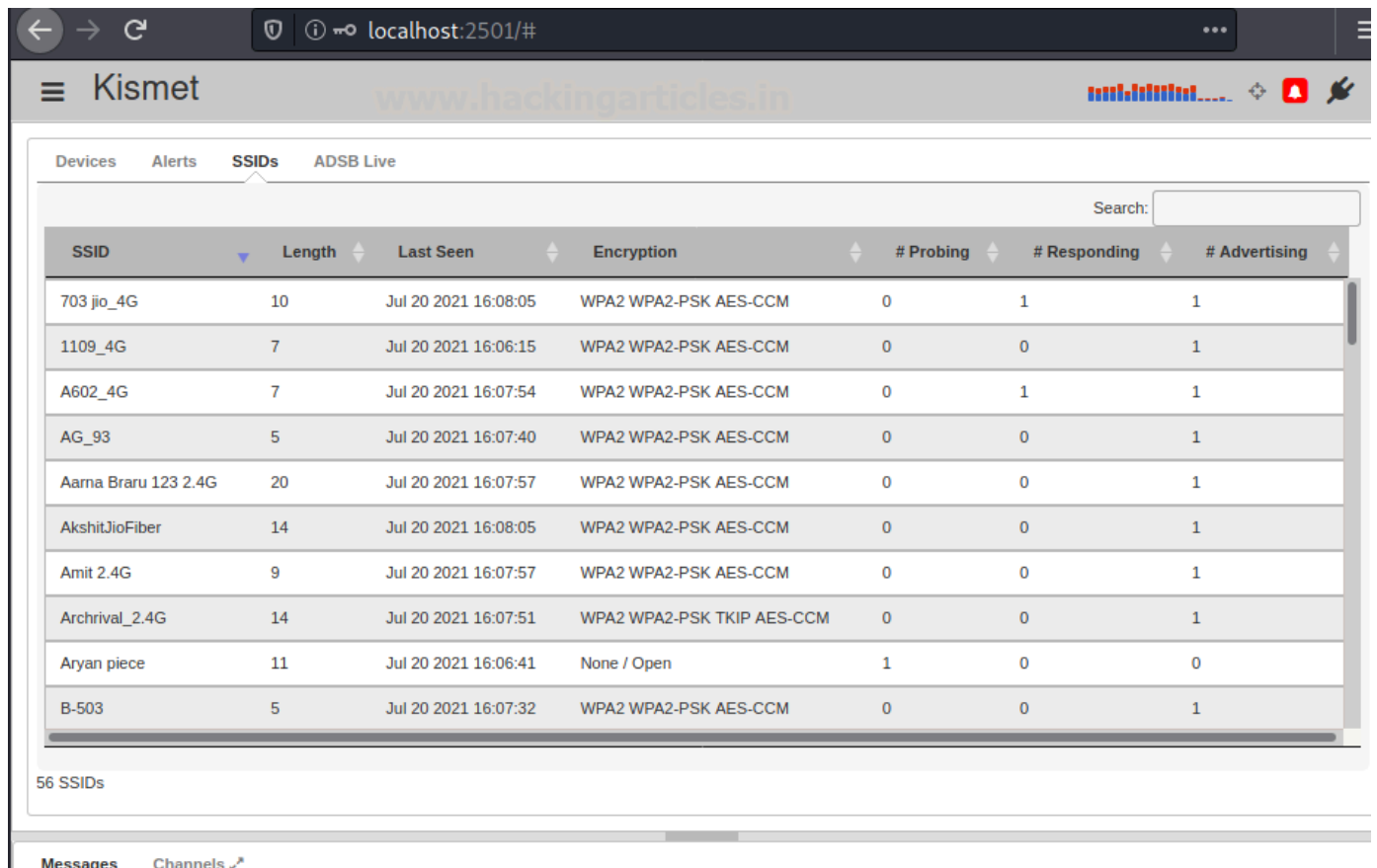
Note: To use this tool you may need an external wi-fi adapter.

```
(root@kali)-[~]
# kismet -c wlan0mon
```

The service will be running at localhost on port 2501 which is accessible through web browser <http://localhost:2501>

```
KISMET - Point your browser to http://localhost:2501 (or the address of this system) for
INFO: Registered PHY handler 'BTLE' as ID 6
INFO: Registered PHY handler 'RTLAMR' as ID 7
INFO: Indexing ADSB ICAO db
INFO: Completed indexing ADSB ICAO db, 322495 lines 6450 indexes
INFO: Registered PHY handler 'RTLADSB' as ID 8
INFO: Registered PHY handler '802.15.4' as ID 9
INFO: Could not open system plugin directory (/usr/lib/x86_64-linux-gnu/kis
met/), skipping: No such file or directory
INFO: Did not find a user plugin directory (/root/.kismet/plugins/).
```


Kismet will enumerate neighboring WiFi networks along with their MAC address and Encryption type.



The screenshot shows the Kismet web interface in a browser window. The address bar displays 'localhost:2501/#'. The page title is 'Kismet' and the URL is 'www.hackingarticles.in'. The interface has a navigation bar with 'Devices', 'Alerts', 'SSIDs', and 'ADSB Live'. The 'SSIDs' tab is active, showing a table of detected networks. The table has columns for SSID, Length, Last Seen, Encryption, # Probing, # Responding, and # Advertising. There are 11 rows of data visible, with a scrollbar on the right indicating more results. Below the table, it says '56 SSIDs'. At the bottom, there are tabs for 'Messages' and 'Channels'.

SSID	Length	Last Seen	Encryption	# Probing	# Responding	# Advertising
703 jio_4G	10	Jul 20 2021 16:08:05	WPA2 WPA2-PSK AES-CCM	0	1	1
1109_4G	7	Jul 20 2021 16:06:15	WPA2 WPA2-PSK AES-CCM	0	0	1
A602_4G	7	Jul 20 2021 16:07:54	WPA2 WPA2-PSK AES-CCM	0	1	1
AG_93	5	Jul 20 2021 16:07:40	WPA2 WPA2-PSK AES-CCM	0	0	1
Aarna Braru 123 2.4G	20	Jul 20 2021 16:07:57	WPA2 WPA2-PSK AES-CCM	0	0	1
AkshitJioFiber	14	Jul 20 2021 16:08:05	WPA2 WPA2-PSK AES-CCM	0	0	1
Amit 2.4G	9	Jul 20 2021 16:07:57	WPA2 WPA2-PSK AES-CCM	0	0	1
Archival_2.4G	14	Jul 20 2021 16:07:51	WPA2 WPA2-PSK TKIP AES-CCM	0	0	1
Aryan piece	11	Jul 20 2021 16:06:41	None / Open	1	0	0
B-503	5	Jul 20 2021 16:07:32	WPA2 WPA2-PSK AES-CCM	0	0	1

If you choose any Network ID it will depict the Wi-Fi configuration details. As you can see, we are interested in “SSID: AARTI” that has WEP encryptions 🚩 (less secure and highly exploitable).

SSID: AARTI

Wi-Fi (802.11) SSIDs

SSID ?aarti (5 characters)

First SeenJul 20 2021 16:06:06

Last SeenJul 20 2021 16:09:59

Encryption ?WEP

Advertising APs ?

aarti - D8:47:32:E9:3F:33 - WEP

Advertising DeviceView Device Details

MACD8:47:32:E9:3F:33 (TP-Link Technologies Ltd)

Nameaarti

TypeWi-Fi AP

Advertised encryption ?WEP

First advertisedJul 20 2021 16:06:06

Last advertisedJul 20 2021 16:09:55

Last advertised SSIDAarti

Responding APs ?

aarti - D8:47:32:E9:3F:33 - WEP

Responding DeviceView Device Details

MACD8:47:32:E9:3F:33 (TP-Link Technologies Ltd)

Nameaarti

TypeWi-Fi AP

Advertised encryption ?WEP

First respondedJul 20 2021 16:08:09

Last respondedJul 20 2021 16:09:59

Last advertised SSIDAarti

Airodump-ng

Airodump-ng is included in the aircrack-ng package and is used for packet capturing of raw 802.11 frames. It is ideal for collecting WEP IVs for use with aircrack-ng. If you have a GPS receiver connected to the computer, airodump-ng can log the coordinates of the discovered access points.

Note: To use this tool you may need an external wi-fi adapter.

```
(root@kali)-[~]
# airodump-ng wlan0mon
```

The following command monitors all wireless networks, frequency hopping between all wireless channels.

1. airodump-ng wlan0mon

CH 11][Elapsed: 6 s][2021-07-20 16:13

BSSID	PWR	Beacons	#Data, #/s	CH	MB	ENC CIPHER	AUTH	ESSID
F4:79:60:3B:55:58	-66	2	0	5	270	WPA2 CCMP	PSK	K 307
30:CC:21:E8:8E:EA	-73	2	0	5	130	WPA2 CCMP	PSK	Abhiraj
AA:DA:0C:58:34:FE	-67	3	0	10	130	WPA2 CCMP	PSK	<length: 0>
98:35:ED:D9:A1:B8	-1	0	0	7	-1			<length: 0>
18:45:93:69:A5:19	-21	1	2	9	130	WPA2 CCMP	PSK	raaj
68:14:01:5A:0E:9C	-61	2	0	1	195	WPA2 CCMP	PSK	Amit 2.4G
70:C7:F2:ED:6A:44	-65	2	0	4	130	WPA2 CCMP	PSK	ajoy
1A:59:C0:33:EB:8A	-67	1	4	13	360	WPA2 CCMP	PSK	riddikenator@orbi
E8:D0:B9:A3:12:F9	-67	2	0	7	270	WPA2 CCMP	PSK	Jasmeen_2G
AC:37:28:64:D5:C9	-70	0	0	9	130	WPA2 CCMP	PSK	Abhiaka
04:95:E6:63:6F:D8	-71	2	0	8	130	WPA2 CCMP	PSK	B-503
B0:08:75:19:83:50	-73	2	0	4	130	WPA2 CCMP	PSK	Mayank-A

BSSID	STATION	PWR	Rate	Lost	Frames	Notes	Probes
98:35:ED:D9:A1:B8	52:83:23:F2:A8:94	-76	0 - 1	0	2		
(not associated)	38:A4:ED:CF:8E:8D	-48	0 - 1	0	2		
(not associated)	CA:7B:54:EE:02:1D	-70	0 - 1	10	4		Kavz_5G
(not associated)	96:D9:7A:8D:95:18	-74	0 - 1	0	1		
(not associated)	F8:E4:E3:9E:24:9C	-76	0 - 1	0	1		MetNet
18:45:93:69:A5:19	2A:84:98:9F:E5:5E	-20	1e- 1e	126	8		

Wash

Wash is a tool for discovering WPS-enabled access points. It may either survey from a live interface or scan a list of pcap files. Wash is included in the Reaver package. It comes preinstalled in Kali Linux and you can execute the following command for SSID discovery.

```
wash -l wlan0mon
```

Note: To use this tool you may need an external wi-fi adapter.

```
(root@kali)-[~]
# wash -i wlan0mon
```

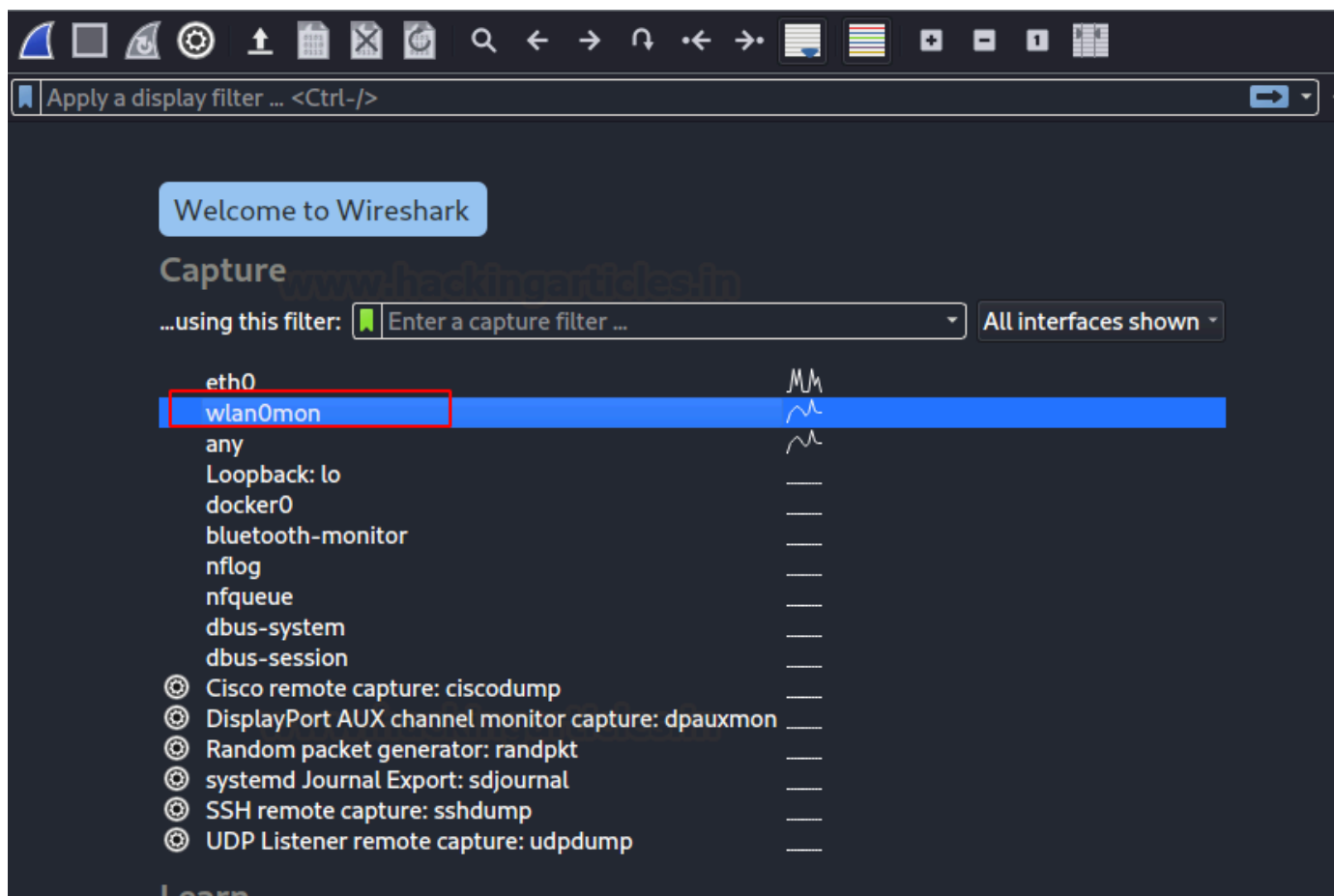
BSSID	Ch	dBm	WPS	Lck	Vendor	ESSID
68:14:01:5A:0E:9C	1	-65	2.0	No	Broadcom	Amit 2.4G
68:14:01:0B:BB:B5	1	-71	2.0	No	Broadcom	Aarna Braru 123 2.4G
96:FB:A7:54:C1:F4	1	-73	1.0	No	RalinkTe	(null)
68:14:01:34:B9:E3	1	-71	2.0	No	Broadcom	JioFiber-QwXYk
40:49:0F:3C:49:88	1	-57	2.0	No	Broadcom	Sachin 2.4
68:14:01:6A:F1:57	1	-69	2.0	No	Broadcom	Jas303 2.4G
18:82:8C:F2:5C:C8	1	-75	2.0	No	Broadcom	Vikash jio_4G
68:14:01:35:45:96	1	-79	2.0	No	Broadcom	Mohsinhind 2.4 G
40:49:0F:0A:AB:D6	1	-75	2.0	No	Broadcom	203 Jio 2.4 G
A8:DA:0C:B3:65:99	1	-75	2.0	No	Broadcom	1109_4G
18:82:8C:ED:86:CA	1	-79	2.0	No	Broadcom	Marvel
68:14:01:3A:AF:3A	1	-75	2.0	No	Broadcom	Durgesh 2.4G
96:FB:A7:54:F1:26	2	-75	1.0	No	RalinkTe	(null)
94:FB:A7:64:F1:26	2	-75	1.0	No	RalinkTe	Ankush 4G
30:CC:21:E3:47:88	3	-49	2.0	No		Vikas

Wireshark

Wireshark is the world's foremost and widely-used network protocol analyzer. It lets you see what's happening on your network at a microscopic level. It is also WAN/LAN Analyzer

Decryption support for many protocols, including IPsec, ISAKMP, Kerberos, SNMPv3, SSL/TLS, WEP, and WPA/WPA2

Note: To use this tool you may need an external wi-fi adapter for SSID discovery.



Start Wireshark and choose the interface for the Wi-Fi adapter and it will list all network ID available in the surroundings.

Apply a display filter ... <Ctrl-/>			
Info	Time	Source	
Clear-to-send, Flags=.....	3.767434390		
Beacon frame, SN=1164, FN=0, Flags=....., BI=100, SSID=Mohsinhind 2.4 G	3.773424556	HonHaiPr_35:45:96	
Data, SN=1985, FN=0, Flags=.p....F.	3.790863798	Arcadyan_ed:1a:1c	
Beacon frame, SN=3742, FN=0, Flags=....., BI=100, SSID=Aarna Braru 123 ...	3.793770268	HonHaiPr_0b:bb:b5	
Beacon frame, SN=2491, FN=0, Flags=....., BI=100, SSID=Rudra	3.810137029	TaicangT_83:9f:49	
Beacon frame, SN=4024, FN=0, Flags=....., BI=100, SSID=Aayush 2.4G	3.846794840	HonHaiPr_59:fd:69	
Acknowledgement, Flags=.....	3.893578812		
Beacon frame, SN=923, FN=0, Flags=....., BI=100, SSID=LIMITED_ACCESS_24	3.897012439	Sercomm_04:c1:f4	
Beacon frame, SN=35, FN=0, Flags=....., BI=100, SSID=Amit 2.4G	3.943441958	HonHaiPr_5a:0e:9c	
Beacon frame, SN=1958, FN=0, Flags=....., BI=100, SSID=Marvel	3.963847680	Arcadyan_ed:86:ca	
Beacon frame, SN=1220, FN=0, Flags=....., BI=100, SSID=jiofbr001 2.4G	4.007184331	HonHaiPr_59:2c:18	
Beacon frame, SN=2163, FN=0, Flags=....., BI=100, SSID=JioFiber-802	4.016672208	Fiberhom_f4:23:81	
802.11 Block Ack Req, Flags=.....	4.035385805	Sercomm_0e:be:83 (1	
Beacon frame, SN=36, FN=0, Flags=....., BI=100, SSID=Amit 2.4G	4.045727766	HonHaiPr_5a:0e:9c	
Beacon frame, SN=1995, FN=0, Flags=....., BI=100, SSID=ASHU-101	4.053066636	D-LinkIn_27:a0:a4	
Beacon frame, SN=1959, FN=0, Flags=....., BI=100, SSID=Marvel	4.066111586	Arcadyan_ed:86:ca	
802.11 Block Ack Req, Flags=.....	4.076830017	Serverco_b3:61:f6 (
Null function (No data), SN=1111, FN=0, Flags=...P...T	4.080635060	vivoMobi_0d:62:7e	
802.11 Block Ack Req, Flags=.....	4.082974624	Serverco_b3:61:f6 (
Beacon frame, SN=32, FN=0, Flags=....., BI=100, SSID=Jas303 2.4G	4.095925069	HonHaiPr_6a:f1:57	

Author: Aarti Singh is a Researcher and Technical Writer at Hacking Articles an Information Security Consultant Social Media Lover and Gadgets. Contact [here](#)



Leave a Reply

Votre adresse email ne sera pas publiée. Les champs requis sont indiqués *

Commentaire * *

Nom

E-mail

Site web

☐ Enregistrez mon nom, mon adresse e-mail et mon site Web dans ce navigateur pour la prochaine fois que je commenterai.

☐ Prévenez-moi des nouveaux articles par email.

Poster un commentaire

Recherche ...	Recherche
---------------	-----------

Abonnez-Vous Au Blog Par E-Mail

Entrez votre adresse e-mail pour vous abonner à ce blog et recevoir des notifications de nouveaux articles par e-mail.



S'abonner



IGITE
Technologies

JOIN OUR **CYBER SECURITY** TRAINING PROGRAMS

Enroll Today ➔

www.ignitetechnologies.in

This banner features a dark blue background with a blurred image of a computer monitor displaying a key icon inside a circle. The text is in white and blue, with a call to action button and a website URL.



FORENSIC ARTICLES

[click here to view](#)

This banner has a dark blue background with a glowing fingerprint graphic. The text is in a white, monospace-style font, and there is a button with a link to view the articles.



IGITE
Technologies

CYBER SECURITY

Mindmaps & Cheatsheet

www.ignitetechnologies.in

www.hackingarticles.in

This banner features a colorful, abstract graphic of a person standing next to a large, glowing sphere composed of various icons representing different aspects of cyber security. The background is a gradient of blue and yellow. The text is in white, and there are two website URLs at the bottom.





Support Us

Catégories

Choisir une catégorie

