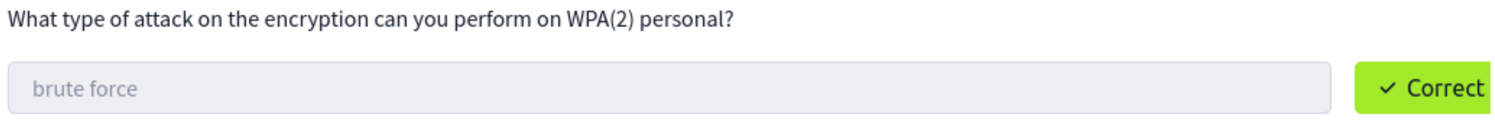
WIFI HACKING 101

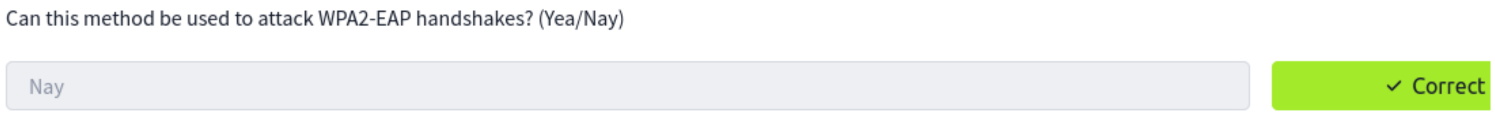
INTRODUCTION
Securing wireless networks is crucial in today's digital landscape, where Wi-Fi networks are pervasive and vulnerable to various attacks. Understanding how these attacks work is essential for both defending networks and testing their resilience. This report delves into the methodologies and tools used to attack WPA(2) networks, highlighting key techniques and considerations.
This report show my approach and findings on how I arrived to the answers to the questions. Let's get started.



What type of attack on the encryption can you perform on WPA(2) personal?

brute force

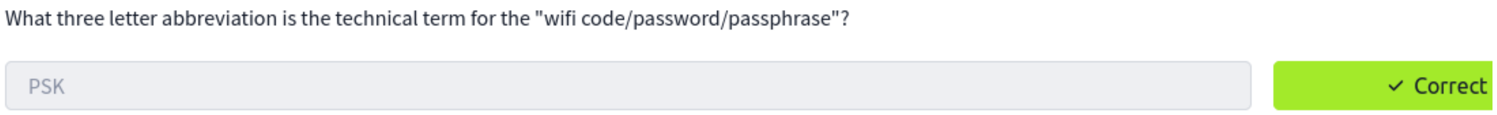
It is mention that the WPA(2) will require both ESSID and password to get in and thus make dictionary attack difficult to crack.
So the only possible could be *Brute force*



Can this method be used to attack WPA2-EAP handshakes? (Yea/Nay)

Nay

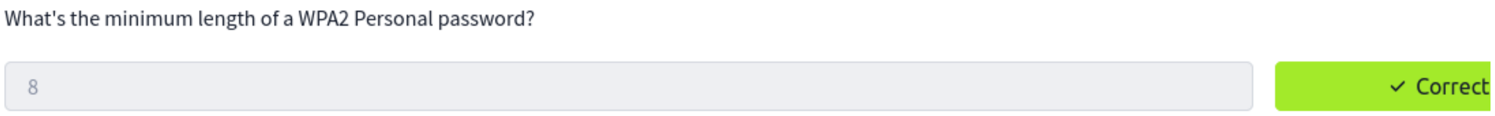
WPA2-EAP require to enter a username and password in order to connect.So it would be grinding to use Brute force attack So it is a *nay*



What three letter abbreviation is the technical term for the "wifi code/password/passphrase"?

PSK

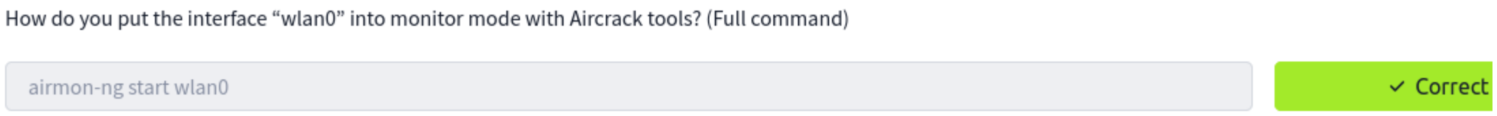
That is the Pre-Shared Key. This is used in WPA/WPA2-PSK and WPA3-PSK security protocols.



What's the minimum length of a WPA2 Personal password?

8

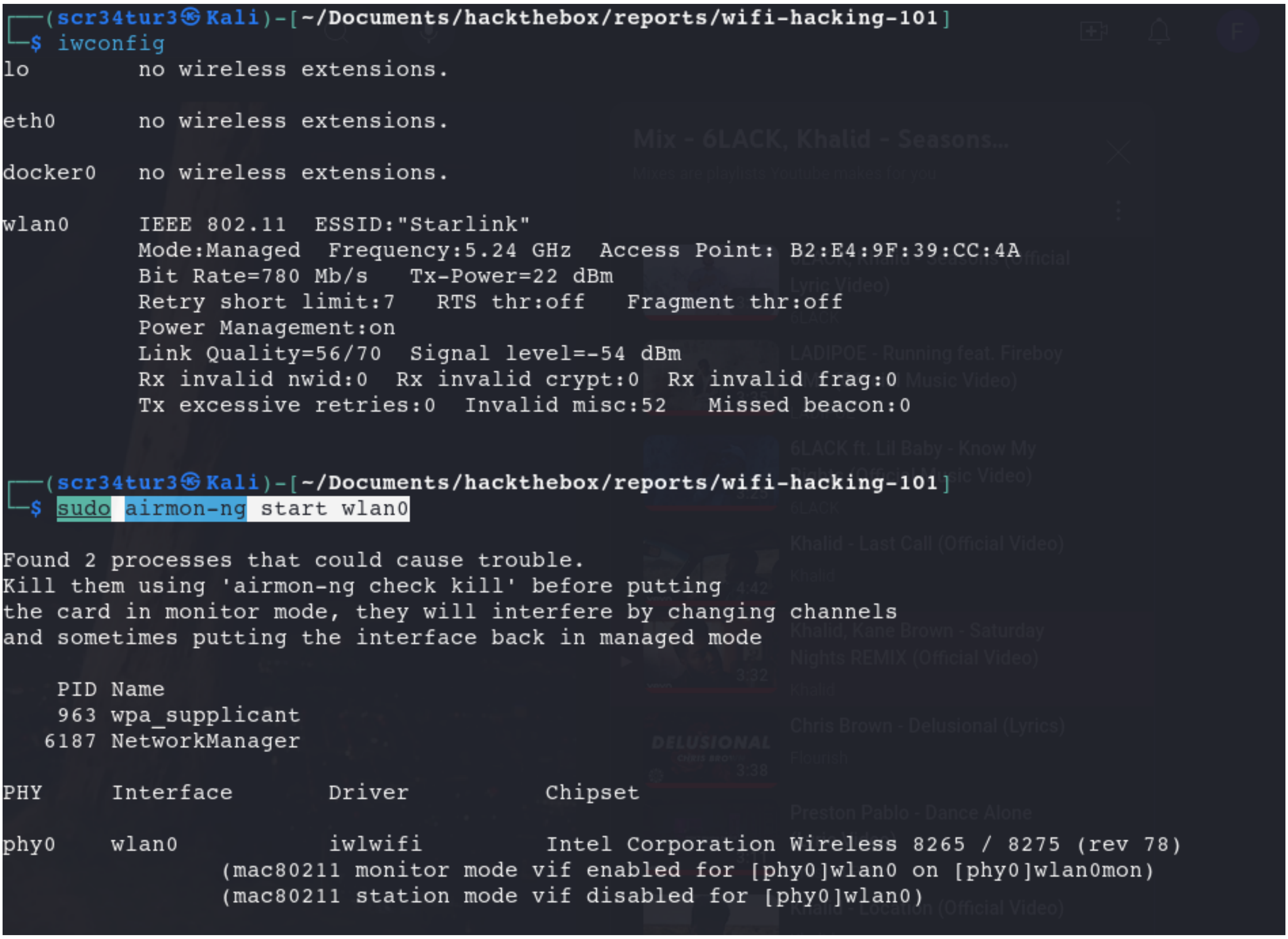
In a couple of circumstances, I have tried to connect to different networks be it institutional or home networks, and when I am promted for password, it requires me to input not less than 8 characters.



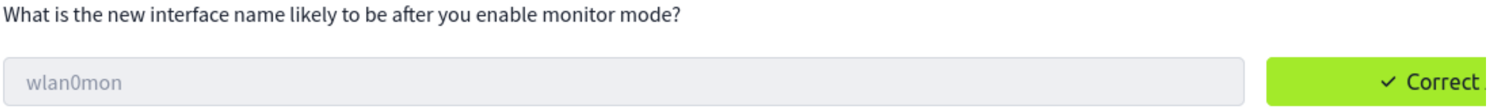
How do you put the interface “wlan0” into monitor mode with Aircrack tools? (Full command)

airmon-ng start wlan0

First I confirmed the name of my network interface I am using using the iwconfig cmd. Then using the airmon-ng start <net-interface name> with sudo previleges, I was able to put my net interface into monitor mode as shown below.



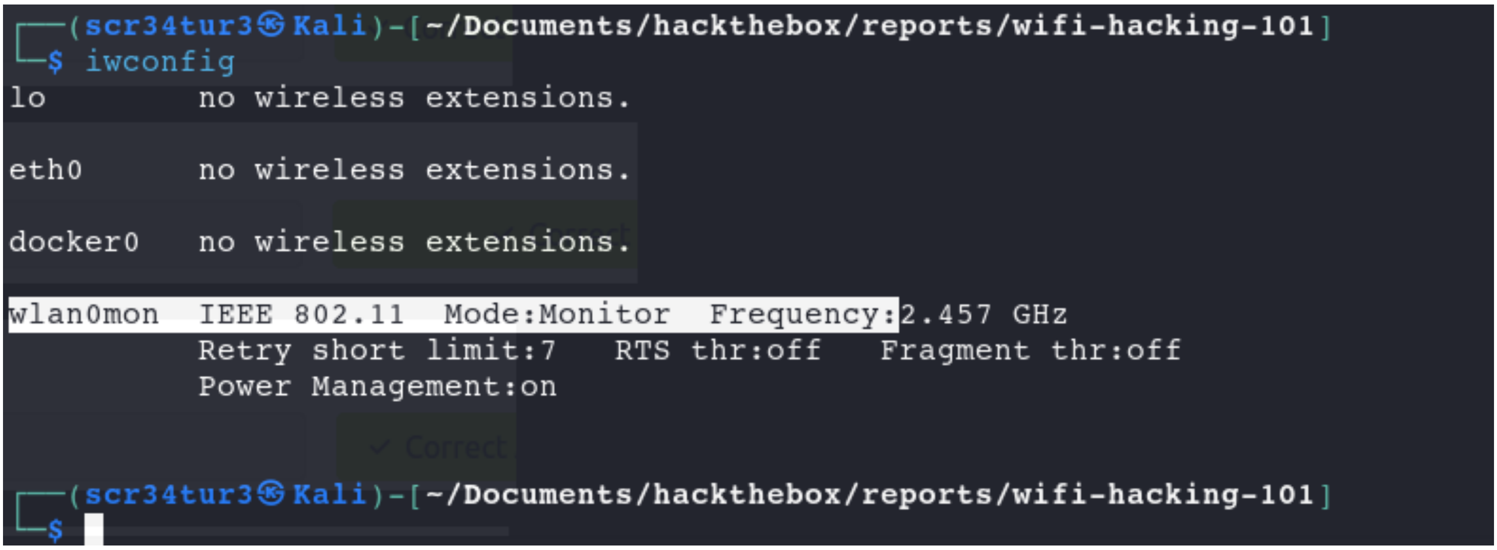
```
┌──(scr34tur3㉿Kali)-[~/Documents/hackthebox/reports/wifi-hacking-101]
└─$ iwconfig
lo        no wireless extensions.

eth0      no wireless extensions.

docker0   no wireless extensions.

wlan0     IEEE 802.11  ESSID:"Starlink"
          Mode:Managed  Frequency:5.24 GHz  Access Point: B2:E4:9F:39:CC:4A
          Bit Rate=780 Mb/s   Tx-Power=22 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Power Management:on
          Link Quality=56/70  Signal level=-54 dBm
          Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
          Tx excessive retries:0  Invalid misc:52   Missed beacon:0


┌──(scr34tur3㉿Kali)-[~/Documents/hackthebox/reports/wifi-hacking-101]
└─$ sudo airmon-ng start wlan0

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

    PID Name
    963 wpa_supplicant
   6187 NetworkManager

PHY     Interface       Driver          Chipset

phy0    wlan0           iwlwifi         Intel Corporation Wireless 8265 / 8275 (rev 78)
                (mac80211 monitor mode vif enabled for [phy0]wlan0 on [phy0]wlan0mon)
                (mac80211 station mode vif disabled for [phy0]wlan0)
```



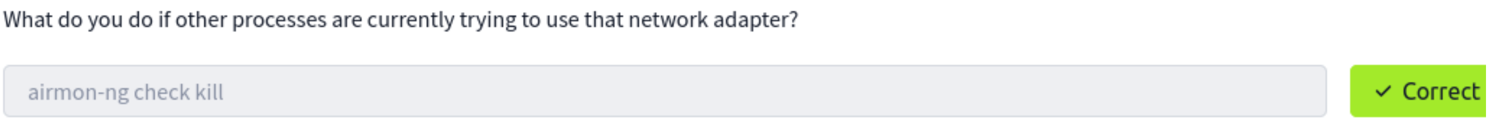
What is the new interface name likely to be after you enable monitor mode?

wlan0mon

I checked for this by running the iwconfig cmd as shown below.



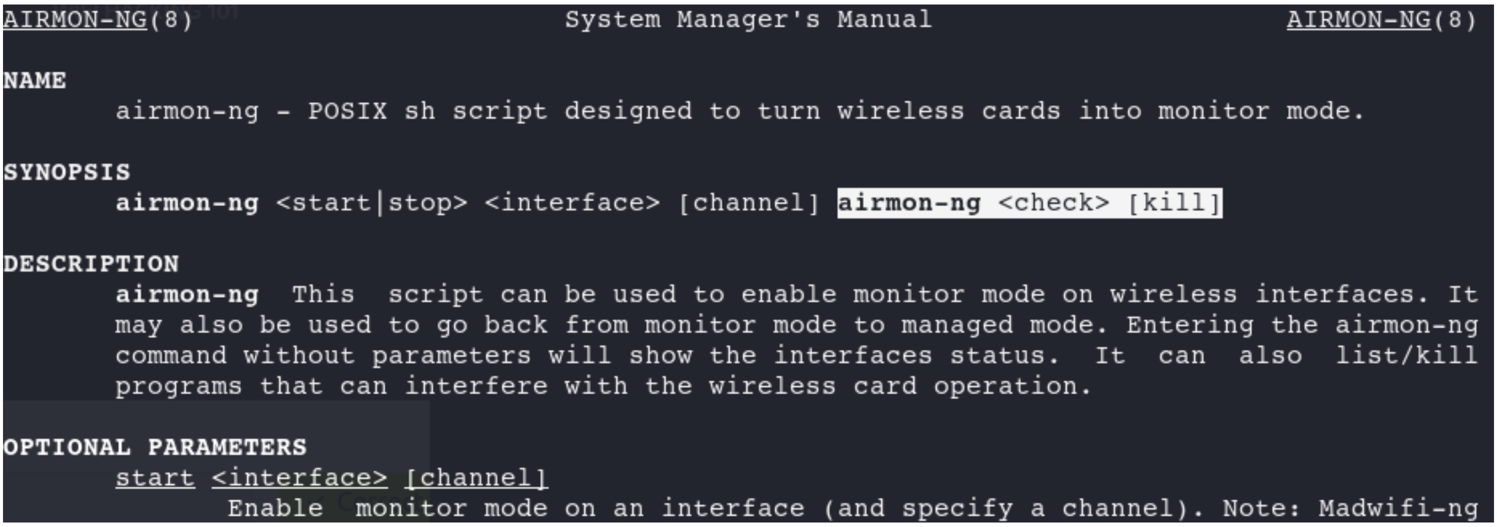
```
┌──(scr34tur3㉿Kali)-[~/Documents/hackthebox/reports/wifi-hacking-101]
└─$ iwconfig
lo        no wireless extensions.

eth0      no wireless extensions.

docker0   no wireless extensions.

wlan0mon  IEEE 802.11  Mode:Monitor  Frequency:2.457 GHz
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Power Management:on


┌──(scr34tur3㉿Kali)-[~/Documents/hackthebox/reports/wifi-hacking-101]
└─$ 
```



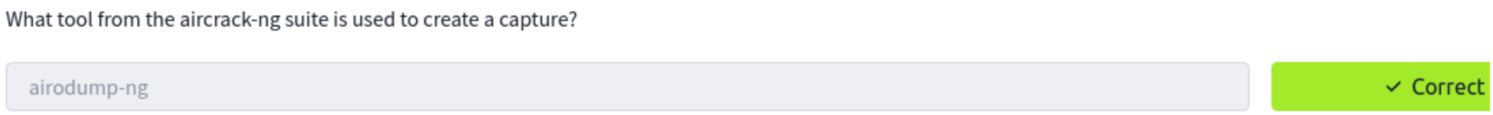
What do you do if other processes are currently trying to use that network adapter?

airmon-ng check kill

Accessing the man page using the man airmon-ng cmd, I was able to see what I can do to kill other processes trying to use my network adapter.



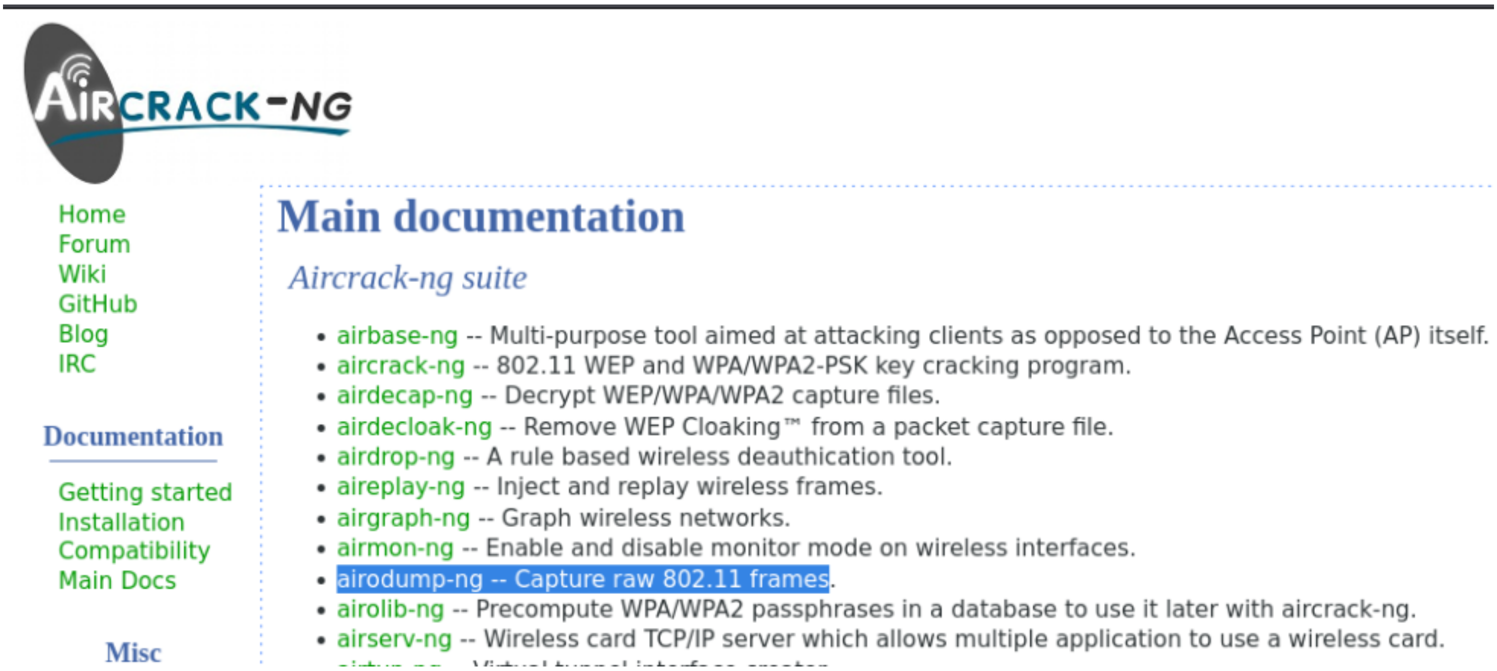
```
AIRMON-NG(8)                  System Manager's Manual                  AIRMON-NG(8)

NAME
       airmon-ng - POSIX sh script designed to turn wireless cards into monitor mode.

SYNOPSIS
       airmon-ng <start|stop> <interface> [channel] airmon-ng <check> [kill]

DESCRIPTION
       airmon-ng  This  script can be used to enable monitor mode on wireless interfaces. It
       may also be used to go back from monitor mode to managed mode. Entering the airmon-ng
       command without parameters will show the interfaces status.  It  can  also  list/kill
       programs that can interfere with the wireless card operation.

OPTIONAL PARAMETERS
       start <interface> [channel]
              Enable  monitor mode on an interface (and specify a channel). Note: Madwifi-ng
```



What tool from the aircrack-ng suite is used to create a capture?

airodump-ng

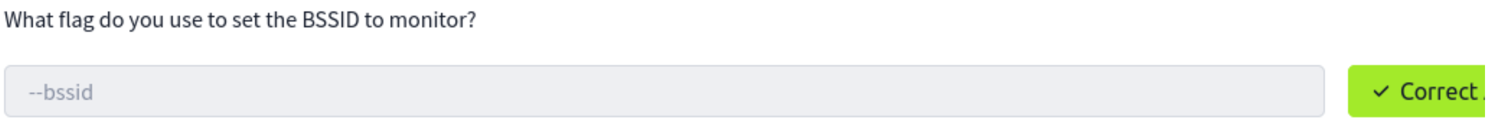
You can visit this website for the answer https://www.aircrack-ng.org/documentation.html



Main documentation

Aircrack-ng suite

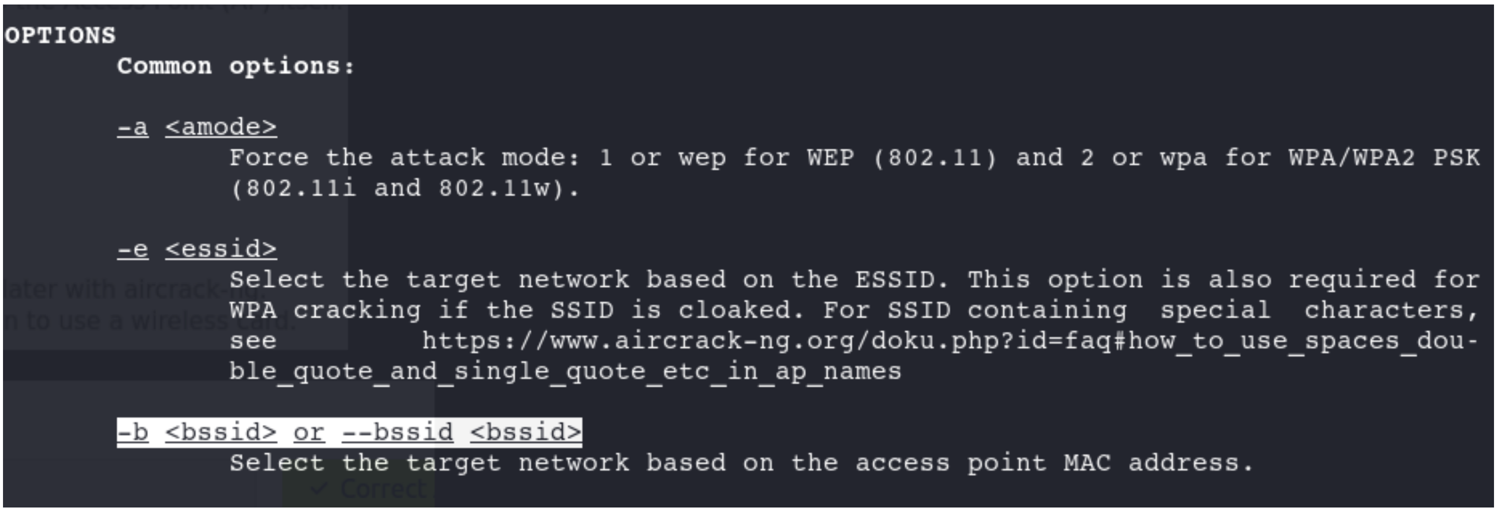
- airbase-ng -- Multi-purpose tool aimed at attacking clients as opposed to the Access Point (AP) itself.
- aircrack-ng -- 802.11 WEP and WPA/WPA2-PSK key cracking program.
- airdecap-ng -- Decrypt WEP/WPA/WPA2 capture files.
- airdecloak-ng -- Remove WEP Cloaking™ from a packet capture file.
- airdrop-ng -- A rule based wireless deauthication tool.
- aireplay-ng -- Inject and replay wireless frames.
- airgraph-ng -- Graph wireless networks.
- airmon-ng -- Enable and disable monitor mode on wireless interfaces.
- airodump-ng -- Capture raw 802.11 frames.
- airolib-ng -- Precompute WPA/WPA2 passphrases in a database to use it later with aircrack-ng.
- airserv-ng -- Wireless card TCP/IP server which allows multiple application to use a wireless card.
- airtun-ng -- Virtual tunnel interface creator



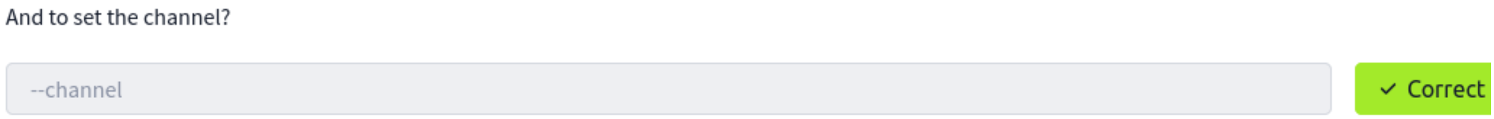
What flag do you use to set the BSSID to monitor?

--bssid

This can be seen by visiting the man page of aircrack-ng as shown below.



```
OPTIONS
       Common options:

       -a <amode>
              Force the attack mode: 1 or wep for WEP (802.11) and 2 or wpa for WPA/WPA2 PSK
              (802.11i and 802.11w).

       -e <essid>
              Select the target network based on the ESSID. This option is also required for
              WPA cracking if the SSID is cloaked. For SSID containing  special  characters,
              see        https://www.aircrack-ng.org/doku.php?id=faq#how_to_use_spaces_dou-
              ble_quote_and_single_quote_etc_in_ap_names

       -b <bssid> or --bssid <bssid>
              Select the target network based on the access point MAC address.
```

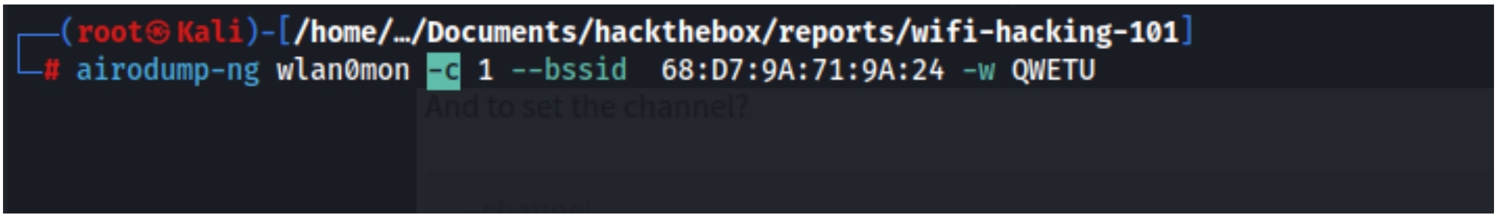


And to set the channel?

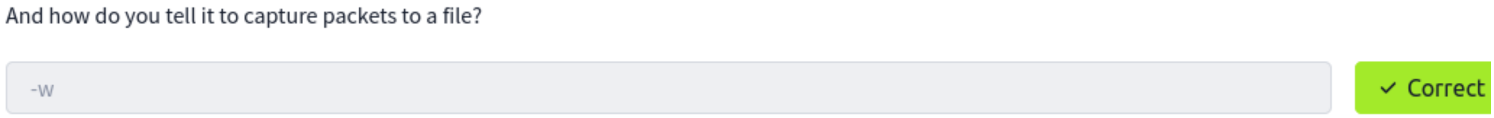
--channel

✓ Correct

For us to set the channel, we can use -c or --channel flag as seen in the image below.



```
┌──(root㉿Kali)-[/home/…/Documents/hackthebox/reports/wifi-hacking-101]
└─# airodump-ng wlan0mon -c 1 --bssid  68:D7:9A:71:9A:24 -w QWETU
```

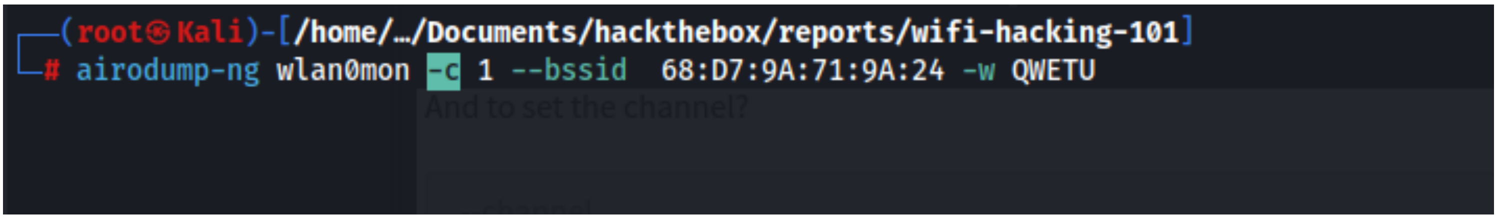


And how do you tell it to capture packets to a file?

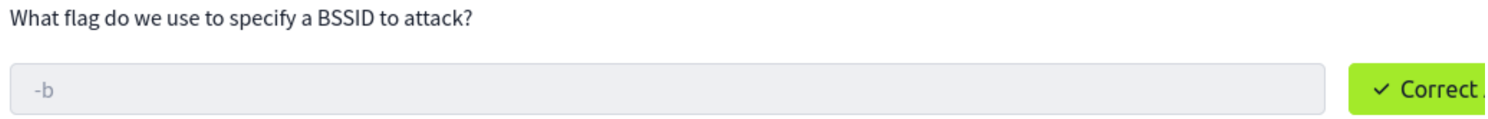
-w

✓ Correct

Using the -w flag, we can write the captured packets into a file



```
┌──(root㉿Kali)-[/home/…/Documents/hackthebox/reports/wifi-hacking-101]
└─# airodump-ng wlan0mon -c 1 --bssid  68:D7:9A:71:9A:24 -w QWETU
```

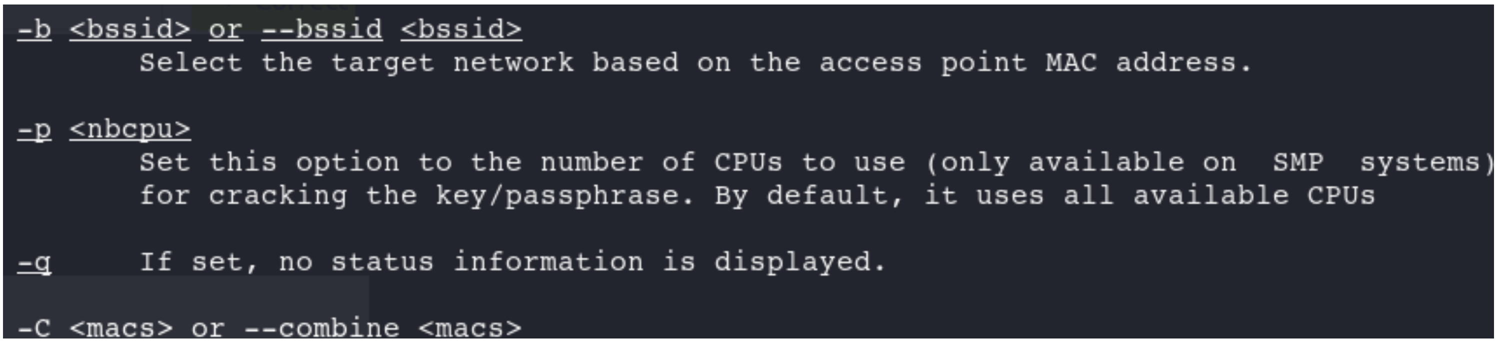


What flag do we use to specify a BSSID to attack?

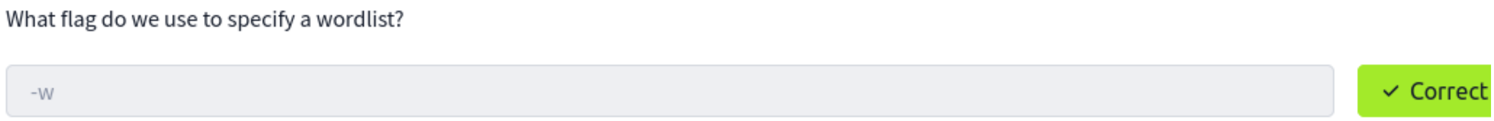
-b

✓ Correct

This can be found by checking the man page as seen below.



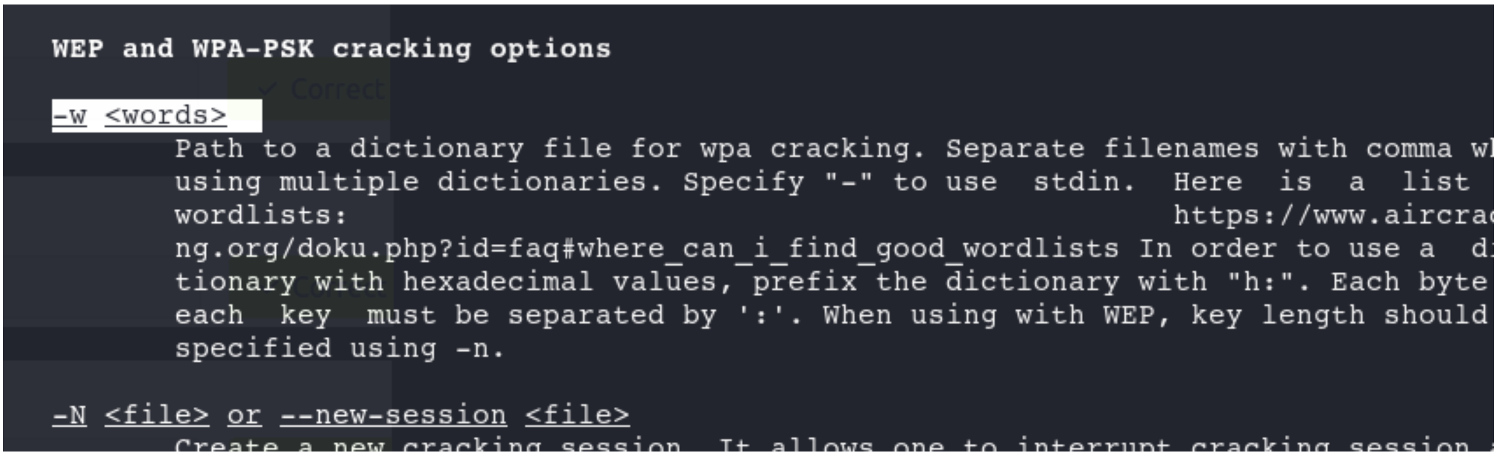
```
-b <bssid> or --bssid <bssid>
        Select the target network based on the access point MAC address.

-p <nbcpu>
        Set this option to the number of CPUs to use (only available on  SMP  systems)
        for cracking the key/passphrase. By default, it uses all available CPUs

-q      If set, no status information is displayed.

-C <macs> or --combine <macs>
```



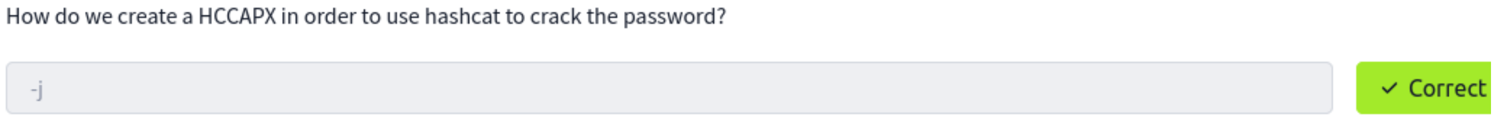
What flag do we use to specify a wordlist?

-w

This can be found by on the man page of aircrack-ng as seen below.



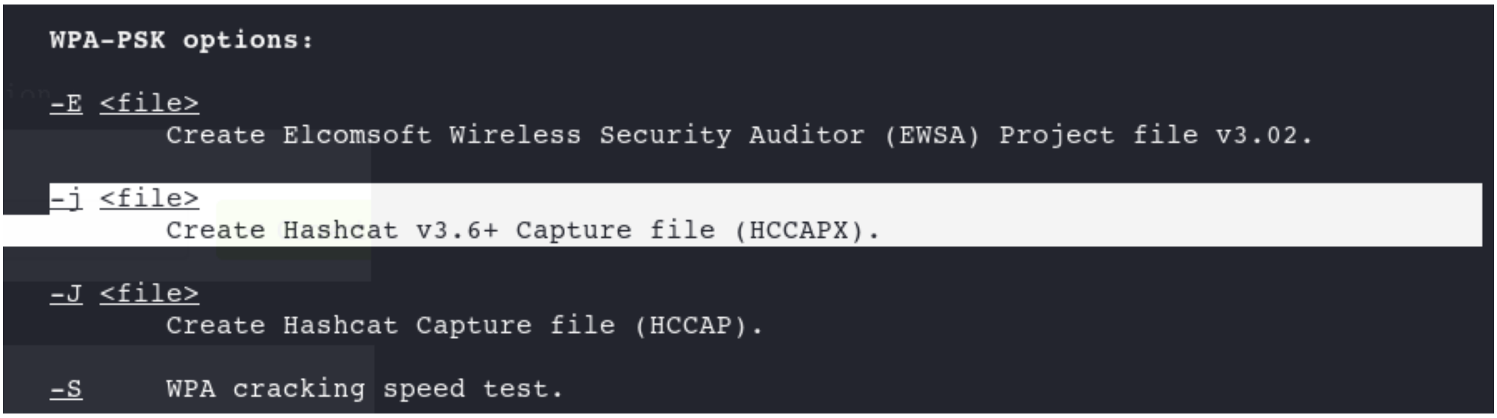
```
  WEP and WPA-PSK cracking options

  -w <words>
          Path to a dictionary file for wpa cracking. Separate filenames with comma wl
          using multiple dictionaries. Specify "-" to use  stdin.  Here  is  a  list
          wordlists:                                           https://www.aircrac
          ng.org/doku.php?id=faq#where_can_i_find_good_wordlists In order to use a  di
          tionary with hexadecimal values, prefix the dictionary with "h:". Each byte
          each  key  must be separated by ':'. When using with WEP, key length should
          specified using -n.

  -N <file> or --new-session <file>
          Create a new cracking session.  It allows one to interrupt cracking session
```



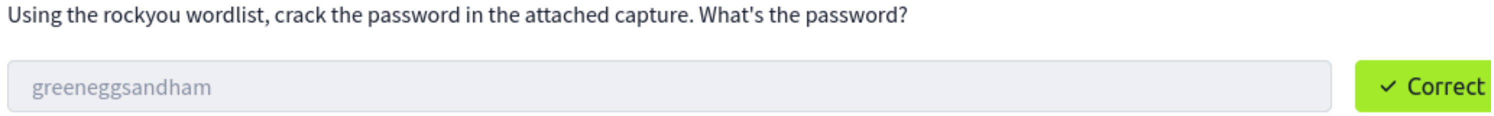
How do we create a HCCAPX in order to use hashcat to crack the password?

-j

This can be found by visiting the man page of aircrack-ng as shown below.



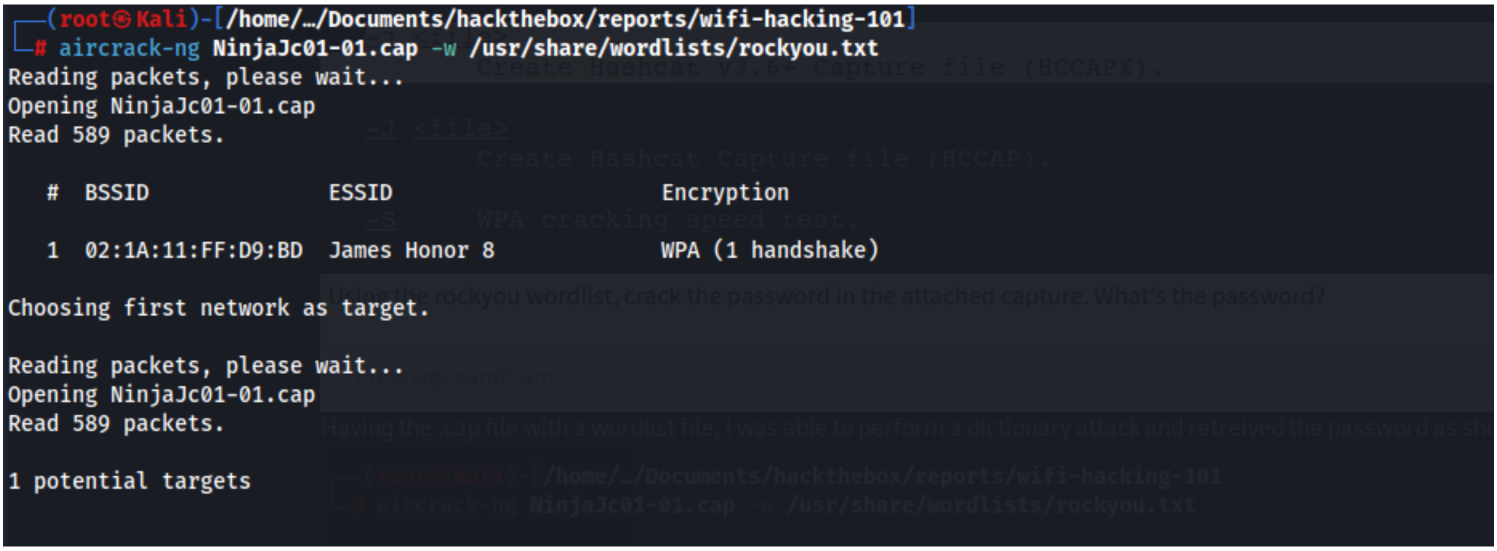
```
  WPA-PSK options:

  -E <file>
         Create Elcomsoft Wireless Security Auditor (EWSA) Project file v3.02.

  -j <file>
         Create Hashcat v3.6+ Capture file (HCCAPX).

  -J <file>
         Create Hashcat Capture file (HCCAP).

  -S     WPA cracking speed test.
```



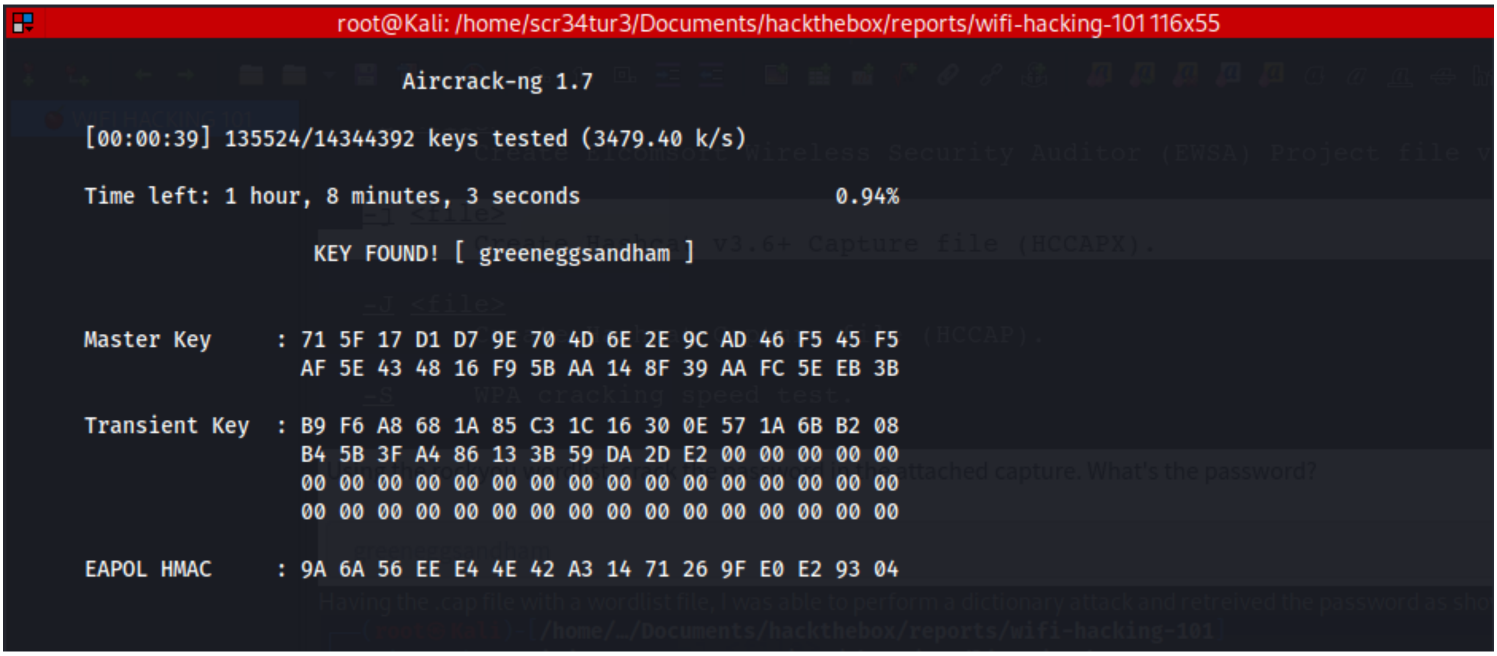
Using the rockyou wordlist, crack the password in the attached capture. What's the password?

greeneggsandham

Having the .cap file with a wordlist file, I was able to perform a dictionary attack and retreived the password as shown in the images below.

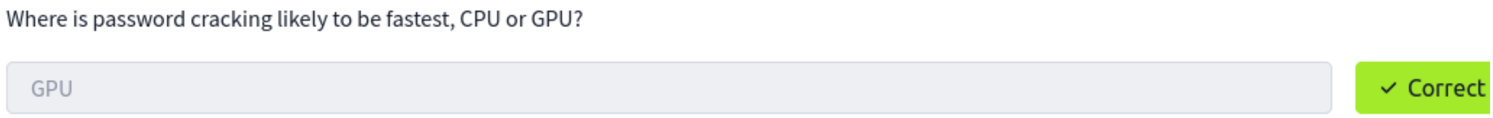


```
┌──(root㉿Kali)-[/home/…/Documents/hackthebox/reports/wifi-hacking-101]
└─# aircrack-ng NinjaJc01-01.cap -w /usr/share/wordlists/rockyou.txt
Reading packets, please wait...
Opening NinjaJc01-01.cap
Read 589 packets.

   #  BSSID              ESSID                     Encryption

   1  02:1A:11:FF:D9:BD  James Honor 8             WPA (1 handshake)

Choosing first network as target.

Reading packets, please wait...
Opening NinjaJc01-01.cap
Read 589 packets.

1 potential targets
```



root@Kali: /home/scr34tur3/Documents/hackthebox/reports/wifi-hacking-101 116x55

```
                               Aircrack-ng 1.7

      [00:00:39] 135524/14344392 keys tested (3479.40 k/s)

      Time left: 1 hour, 8 minutes, 3 seconds                    0.94%

                           KEY FOUND! [ greeneggsandham ]


      Master Key     : 71 5F 17 D1 D7 9E 70 4D 6E 2E 9C AD 46 F5 45 F5
                       AF 5E 43 48 16 F9 5B AA 14 8F 39 AA FC 5E EB 3B

      Transient Key  : B9 F6 A8 68 1A 85 C3 1C 16 30 0E 57 1A 6B B2 08
                       B4 5B 3F A4 86 13 3B 59 DA 2D E2 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     : 9A 6A 56 EE E4 4E 42 A3 14 71 26 9F E0 E2 93 04
```

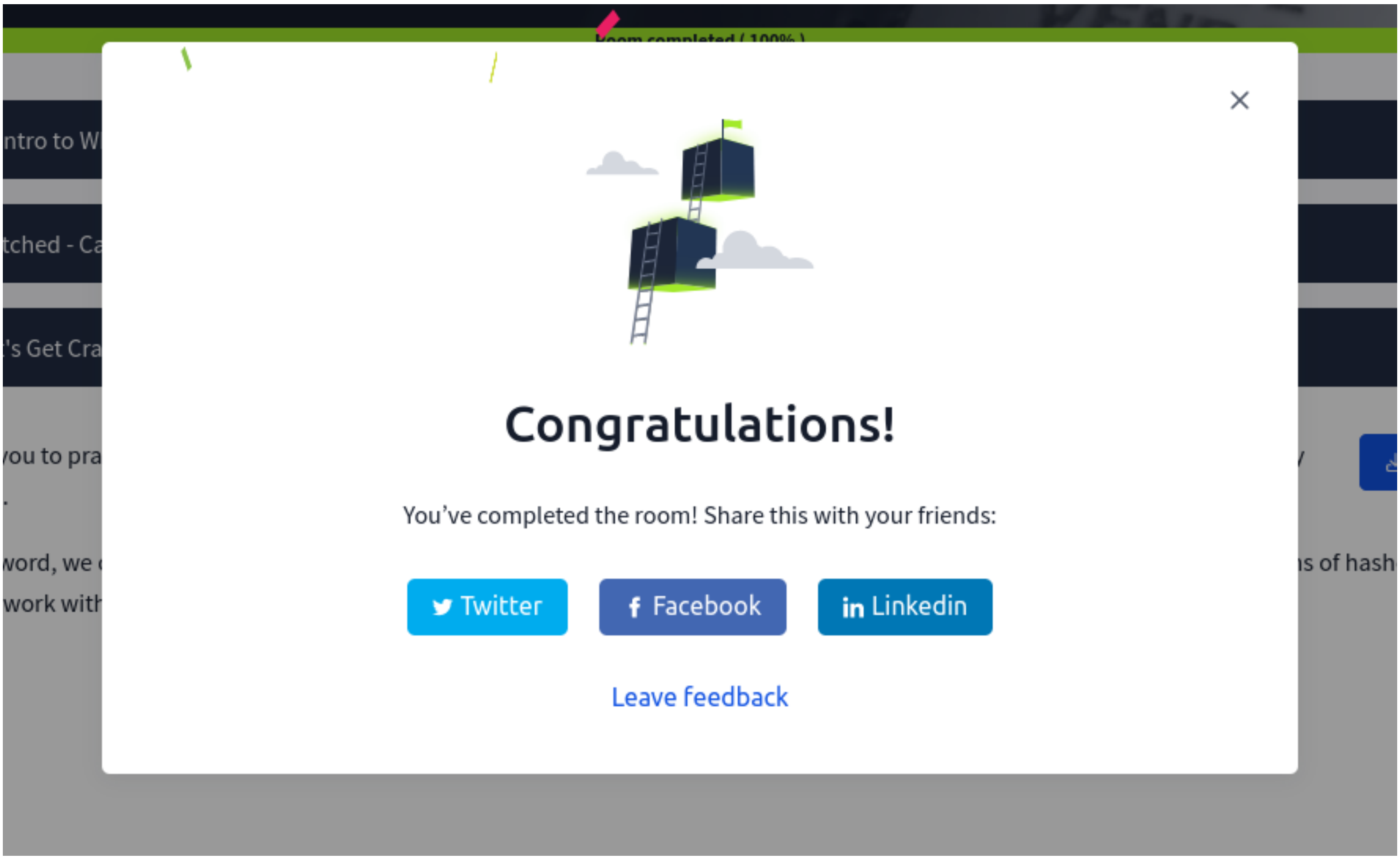


Where is password cracking likely to be fastest, CPU or GPU?

GPU

✓ Correct

GPUs and CPUs are complementary in their capabilities, with GPUs excelling in parallel processing and high throughput tasks, while CPUs are versatile for general-purpose computing and complex decision-making tasks. The choice between GPU and CPU depends on the specific requirements of the application and the nature of the workload being performed and in the case of password cracking, GPU standsout to be our cup of tea.



Congratulations!

You've completed the room! Share this with your friends:

https://tryhackme.com/r/room/wifihacking101

CONCLUSION
Learning to attack WPA(2) networks provides insights into their vulnerabilities and enhances cybersecurity awareness. By understanding how attackers exploit weaknesses, network administrators can better defend against such threats. Continual education and proactive security measures are essential in safeguarding wireless networks from evolving risks.
In my cup of knowlege with a prior knowlege of wifi attack, I have accumulated more skills, and also learned about other tools outside the scope of this room, i.e wifite, wifiphisher e.t.c

Common Attacks on WPA(2) Networks

- **Dictionary Attacks**: Exploiting weak passwords by guessing or using pre-compiled lists.
- **Brute Force Attacks**: Exhaustively trying every possible combination to crack the password.
- **WPS (Wi-Fi Protected Setup) Attacks**: Exploiting vulnerabilities in WPS implementations.
- **KRACK Attack (Key Reinstallation Attack)**: Exploiting weaknesses in the WPA(2) protocol itself.