

Wifi Hacking 101

Introduction

This sub task introduces the learner to the practical knowledge of attacking a wifi network by going through a series of what is called rooms for a special skill particularly.

The activities to be covered in details are: The basics – An Intro to WPA, – Capturing packets to attack, Aircrack-ng – Let's Get Cracking.

Activities

Task 1: The basics – An Intro to WPA

This section outlines objectives such as the social media site to be attacked using a virtual machine, the location of the site.

Previously, the WEP (Wired Equivalent Privacy) standard was used. This was shown to be insecure and can be broken by capturing a key via statistical methods.

The 4 way handshake allows the client and the AP to both prove that they know the key, without telling each other. WPA and WPA2 use practically the same authentication method, so the attacks on both are the same.

The keys for WPA are derived from both the ESSID and the password for the network. The ESSID acts as a salt, making dictionary attacks more difficult. It means that for a given password, the key will still vary for each access point. This means that unless you precompute the dictionary for just that access point/MAC address, you will need to try passwords until you find the correct one.

Room Banner by [Frank Wang](#) on [Unsplash](#)

Answer the questions below

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

Correct Answer Hint

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

Submit

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

Submit

Woop woopl! Your answer is correct.

1 You've started a streak. Keep it going for 6 days for a badge!

authentication method, so the attacks on both are the same.

The keys for WPA are derived from both the ESSID and the password for the network. The ESSID acts as a salt, making dictionary attacks less effective. That means that for a given password, the key will still vary for each access point. This means that unless you precompute the dictionary for just one access point, you will need to try passwords until you find the correct one.

Room Banner by [Frank Wang](#) on [Unsplash](#)

Answer the questions below

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

brute force Correct Answer Hint

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

Nay Correct Answer

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

Answer format: *** Submit

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

Answer format: * Submit

Woop woop! Your answer is correct.

Room Banner by [Frank Wang](#) on [Unsplash](#)

Answer the questions below

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

brute force Correct Answer Hint

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

Nay Correct Answer

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

psk Correct Answer

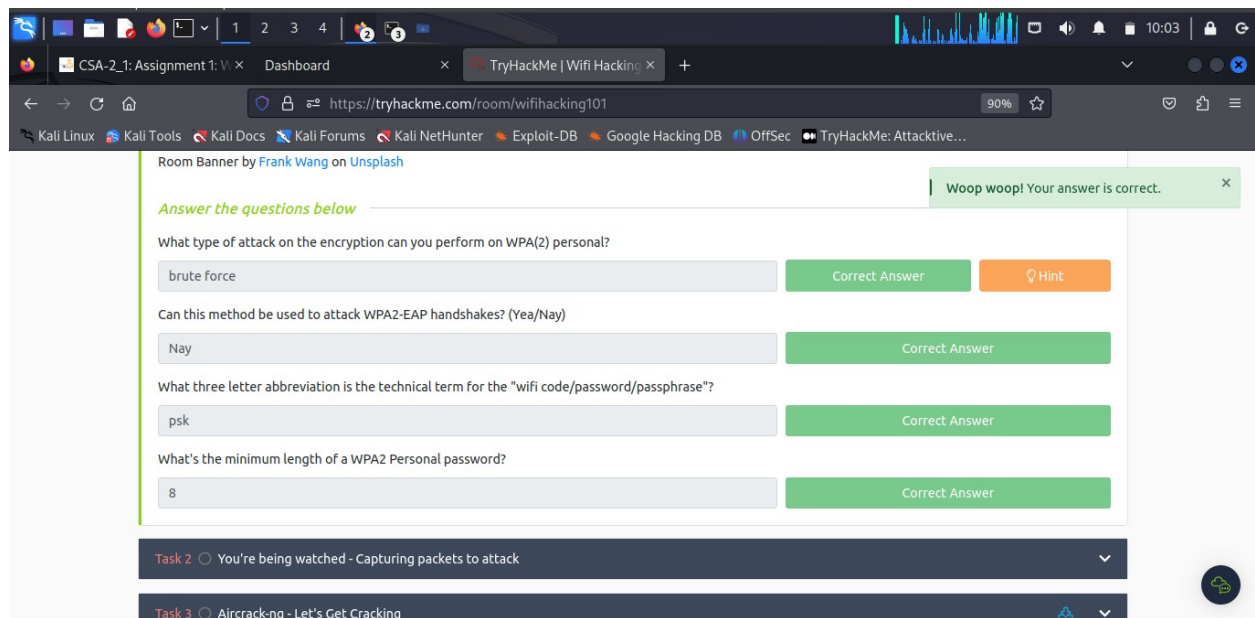
What's the minimum length of a WPA2 Personal password?

Answer format: * Submit

Task 2 ☐ You're being watched - Capturing packets to attack

Task 3 ☐ Aircrack-ng - Let's Get Cracking

Woop woop! Your answer is correct.



Task 2: You're being watched – Capturing packets to attack

The Aircrack-ng suite is used to attack a wifi network, and the learner will walk through attacking a network themselves, assuming they have a monitor mode enabled NIC.

To attack WPA networks, the learner will require **aircrack-ng**, **airodump-ng** and **airmon-ng**.

Task 3: Aircrack-ng – Let's Get Cracking

We'll want to use aircrack-ng, airodump-ng and airmong-ng to attack WPA networks.

The aircrack tools come by default with Kali, or can be installed with a package manager or from <https://www.aircrack-ng.org/>

I suggest creating a hotspot on a phone/tablet, picking a weak password (From rockyou.txt) and following along with every stage. passwords from rockyou, you can use this command on Kali: `head /usr/share/wordlists/rockyou.txt -n 10000 | shuf -n 5 -`

You will need a monitor mode NIC in order to capture the 4 way handshake. Many wireless cards support this, but it's important to note that not all of them do.

Injection mode helps, as you can use it to deauth a client in order to force a reconnect which forces the handshake to occur again. Otherwise, you have to wait for a client to connect normally.

Answer the questions below

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

Correct Answer

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

Submit

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

Submit Hint

To put the interface "wlan0" into monitor mode with Aircrack tools? (Full command): ***sudo airmon-ng start wlan0***

a client to connect normally.

Answer the questions below

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

Correct Answer

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

Correct Answer

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

Submit Hint

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

Submit

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

Submit Hint

And to set the channel?

The new interface name likely to be after you enable monitor mode is **wlan0mon**

a client to connect normally.

Answer the questions below

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

Correct Answer

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

Correct Answer

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

Correct Answer Hint

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

Submit

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

Submit Hint

And to set the channel?

Woop woop! Your answer is correct.

If other processes are currently trying to use that network adapter use **airmon-ng check kill**.

a client to connect normally.

Answer the questions below

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

Correct Answer

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

Correct Answer

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

Correct Answer Hint

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

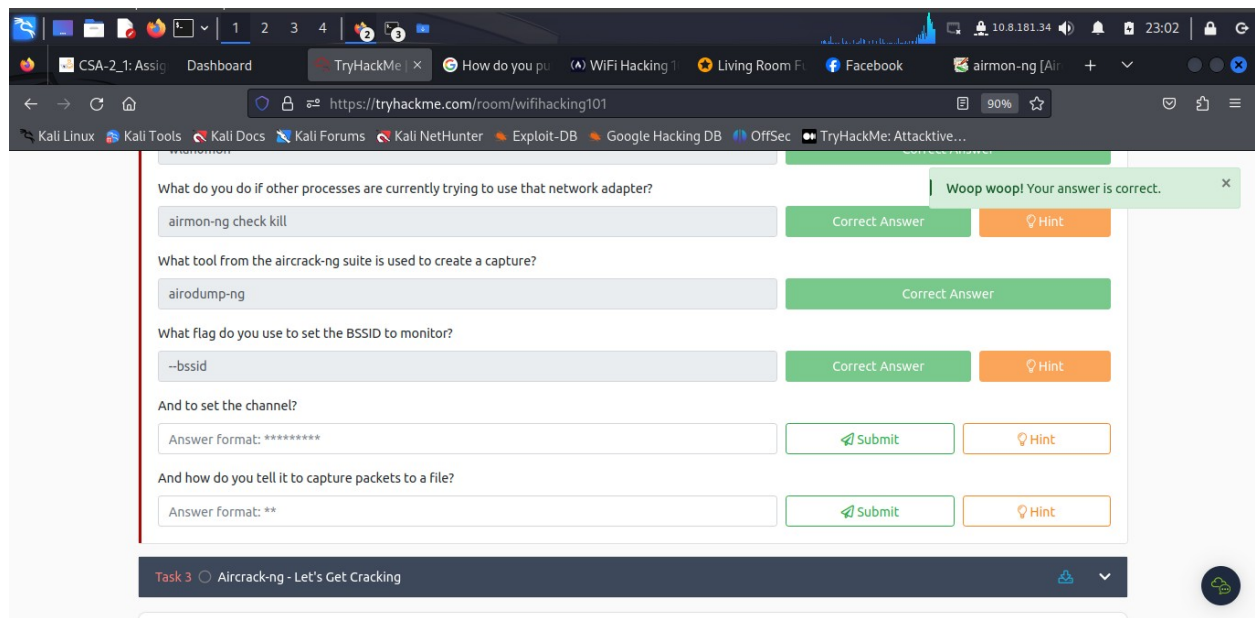
Correct Answer

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

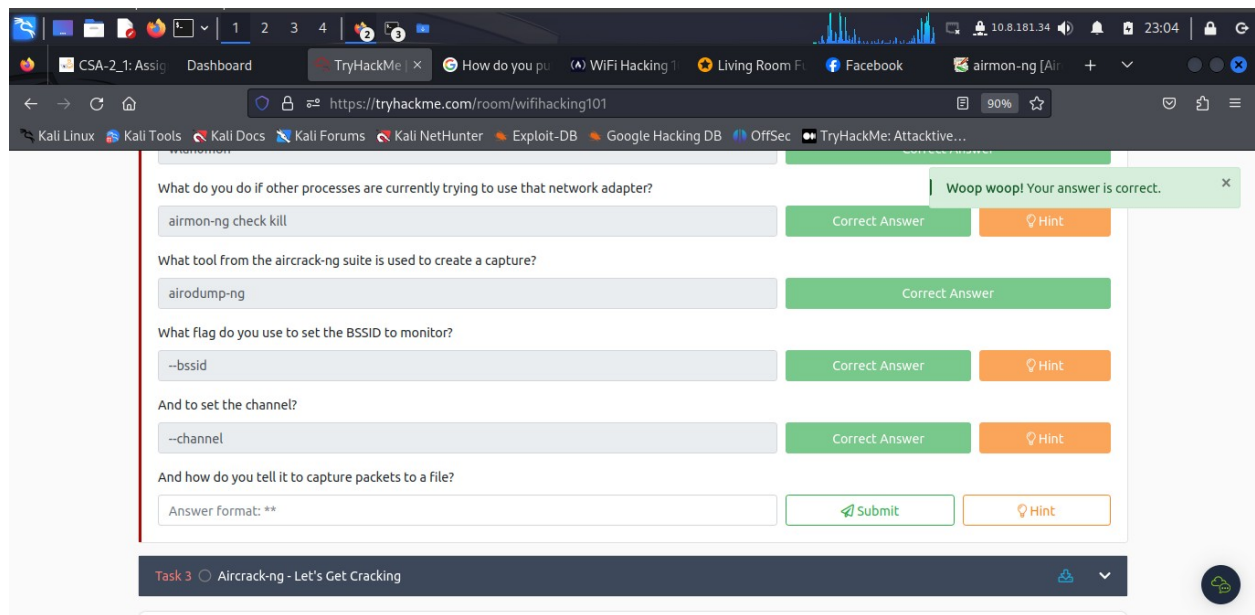
Submit Hint

And to set the channel?

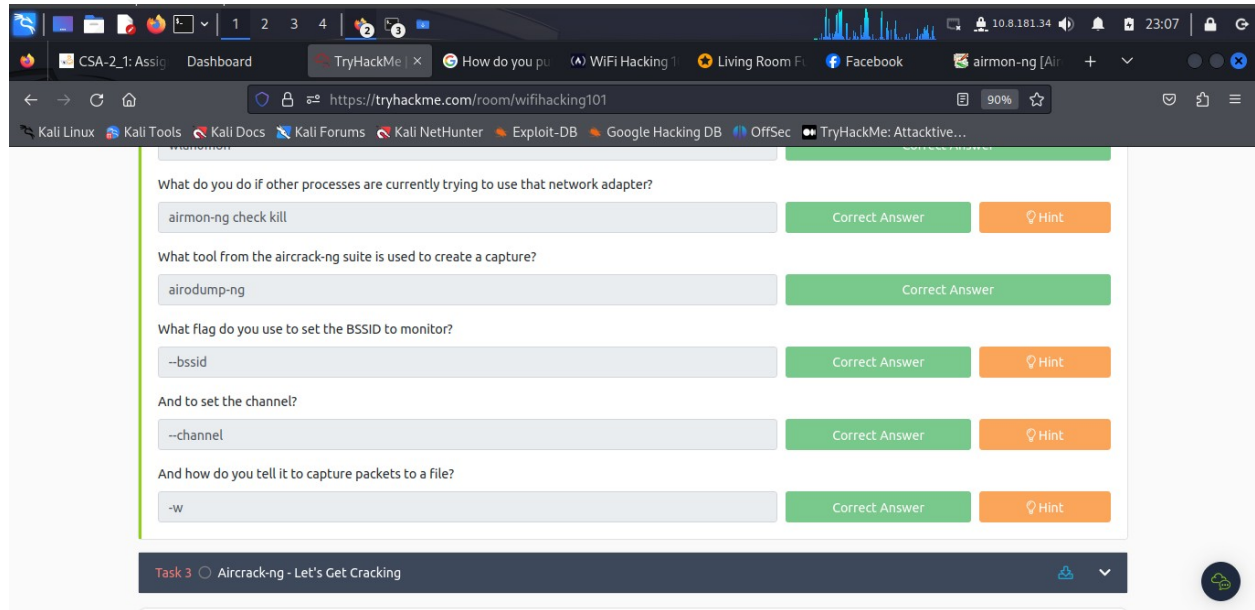
Woop woop! Your answer is correct.



The flag used to set the BSSID to monitor is **--bssid**

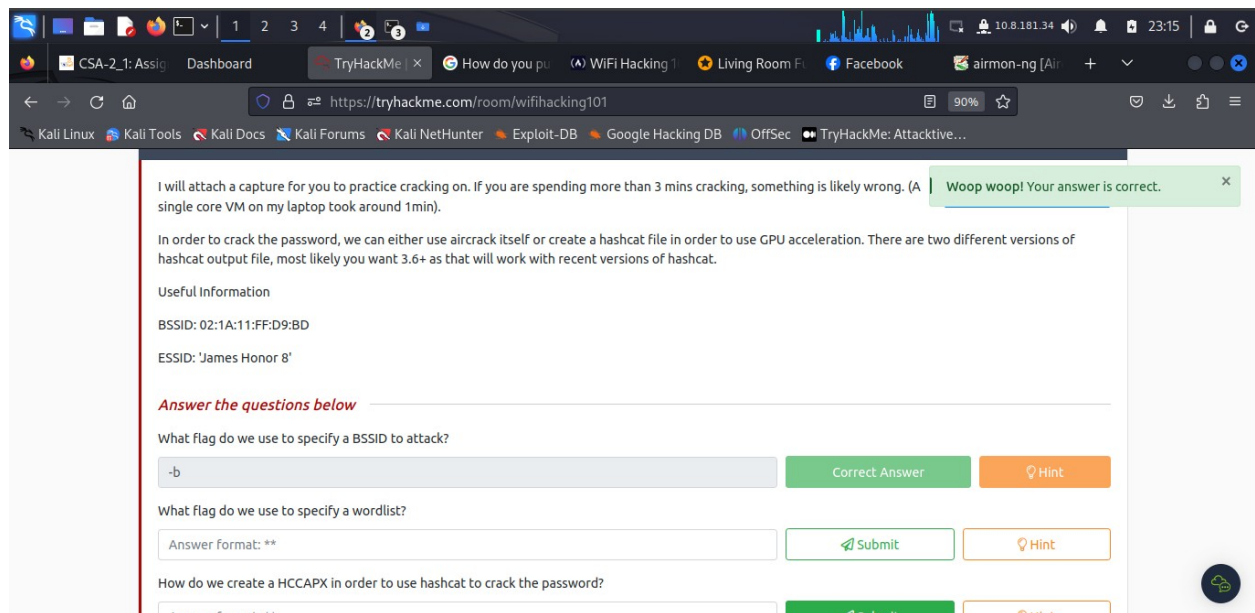


To set the channel run **--channel**



To tell it to capture packets to a file run **-w**.

Task 3: Aircrack-ng - Let's Get Cracking



The flag do we use to specify a BSSID to attack is **-b**.

I will attach a capture for you to practice cracking on. (single core VM on my laptop took around 1min).

In order to crack the password, we can either use aircrack-ng or create a hashcat file in order to use GPU acceleration. There are two different versions of hashcat output file, most likely you want 3.6+ as that will work with recent versions of hashcat.

Useful Information

BSSID: 02:1A:11:FF:D9:BD

ESSID: 'James Honor 8'

Answer the questions below

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

What flag do we use to specify a wordlist?

Answer format: **

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

Answer format: **

```
obed@kali: ~  
- (obed@kali)~  
$ sudo aircrack-ng check kill  
[sudo] password for obed:  
- (obed@kali)~  
$ aircrack-ng --help  
Aircrack-ng 1.7 - (C) 2006-2022 Thomas d'Otreppe  
https://www.aircrack-ng.org  
usage: aircrack-ng [options] <input file(s)>  
  
Common options:  
-a <amode> : force attack mode (1/WEP, 2/WPA-PSK)  
-e <essid> : target selection: network identifier  
-b <bssid> : target selection: access point's MAC  
-p <nbcpu> : # of CPU to use (default: all CPUs)  
-q : enable quiet mode (no status output)  
-C <macs> : merge the given APs to a virtual one  
-l <file> : write key to file. Overwrites file.  
  
Static WEP cracking options:  
-m <maddr> : MAC address to filter usable packets  
-n <nbits> : WEP key length : 64/128/152/256/512  
-i <index> : WEP key index (1 to 4), default: any  
-f <fudge> : bruteforce fudge factor, default: 2  
-k <korek> : disable one attack method (1 to 17)  
-x or -x0 : disable bruteforce for last keybytes  
-x1 : last keybyte bruteforcing (default)  
-x2 : enable last 2 keybytes bruteforcing  
-y : experimental single bruteforce mode  
-K : use only old Korek attacks (pre-PTW)  
-s : show the key in ASCII while cracking  
-M <num> : specify maximum number of IVs to use  
-D : WEP decloak, skips broken keystreams  
-P <num> : PTW debug: 1: disable Klein, 2: PTW  
-1 : run only 1 try to crack key with PTW  
-V : run in visual inspection mode  
  
WEP and WPA-PSK cracking options:  
-w <words> : path to wordlist(s) filename(s)  
-N <file> : path to new session filename  
-R <file> : path to existing session filename  
  
WPA-PSK options:
```

The flag we use to specify a wordlist is **-w**

ESSID: 'James Honor 8'

Answer the questions below

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

What flag do we use to specify a wordlist?

Answer format: **

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

Answer format: **

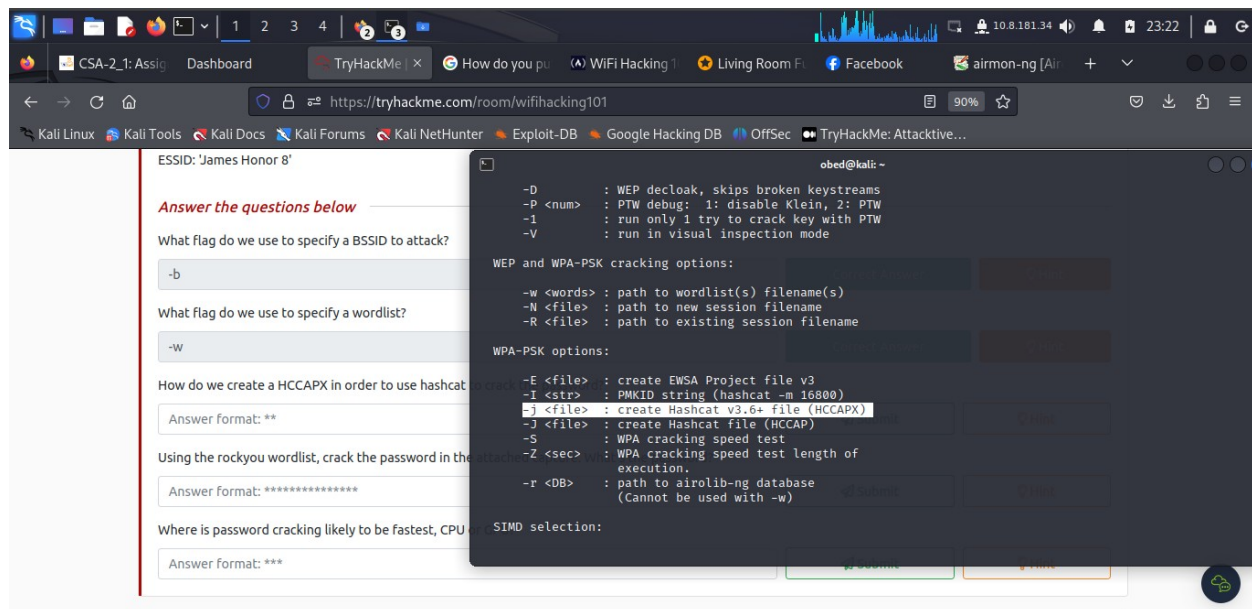
Using the rockyou wordlist, crack the password in the attached capture.

Answer format: *****

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

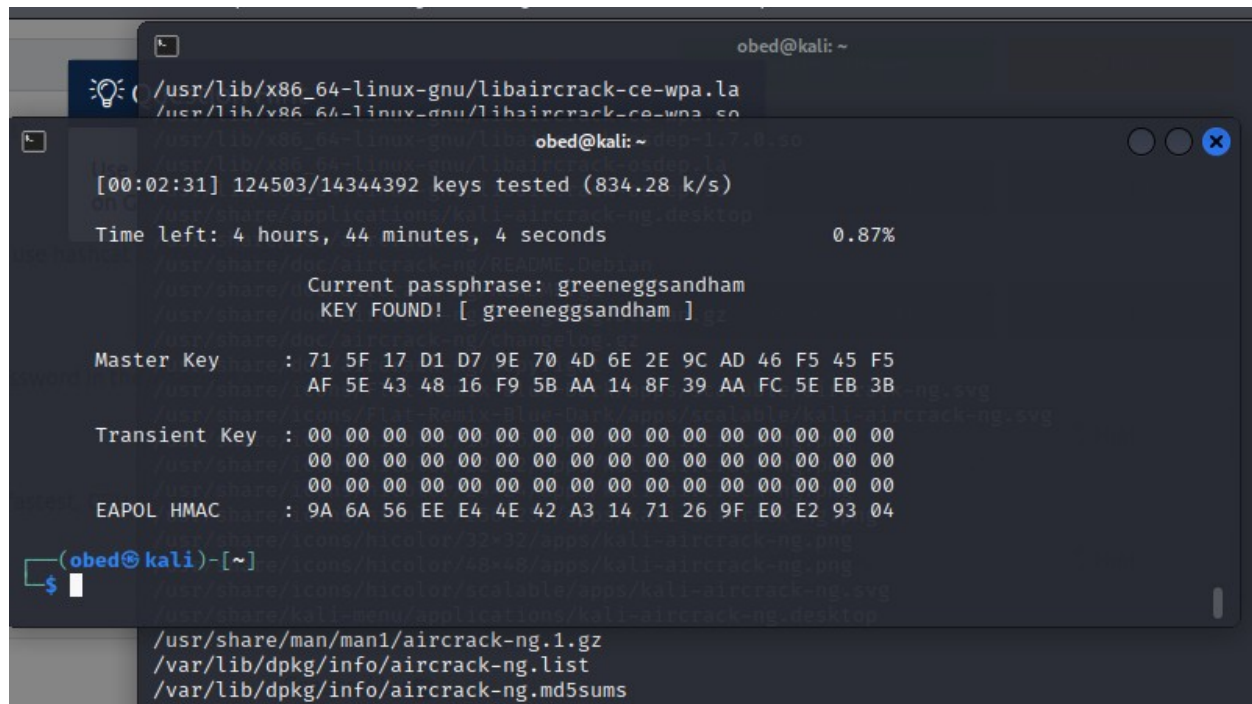
Answer format: ***

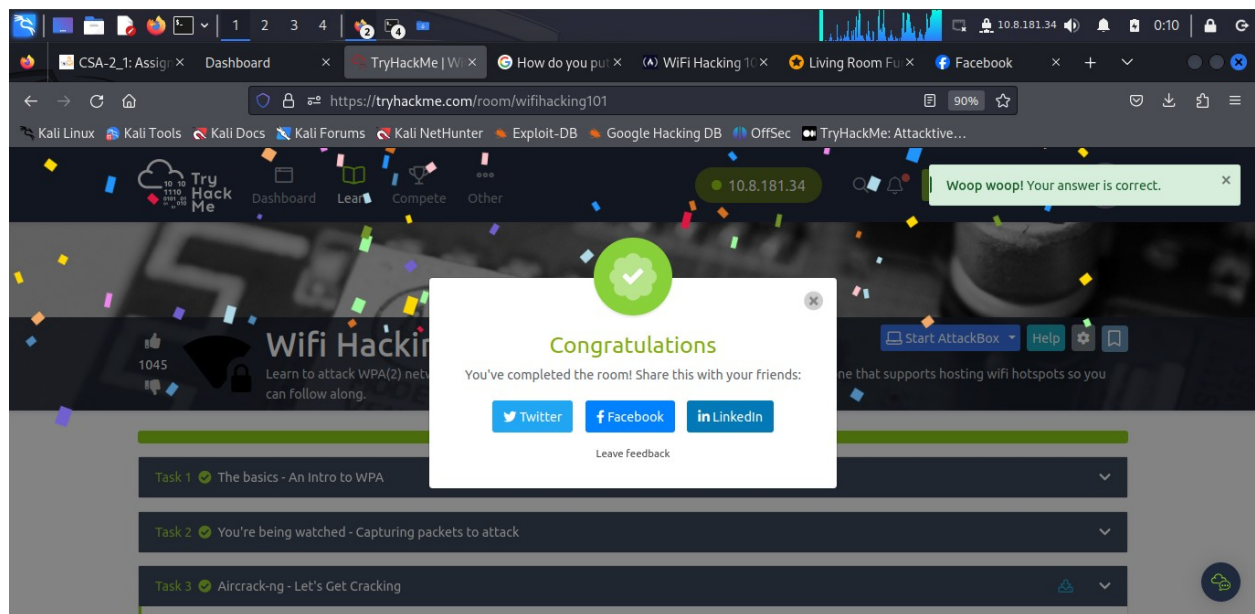
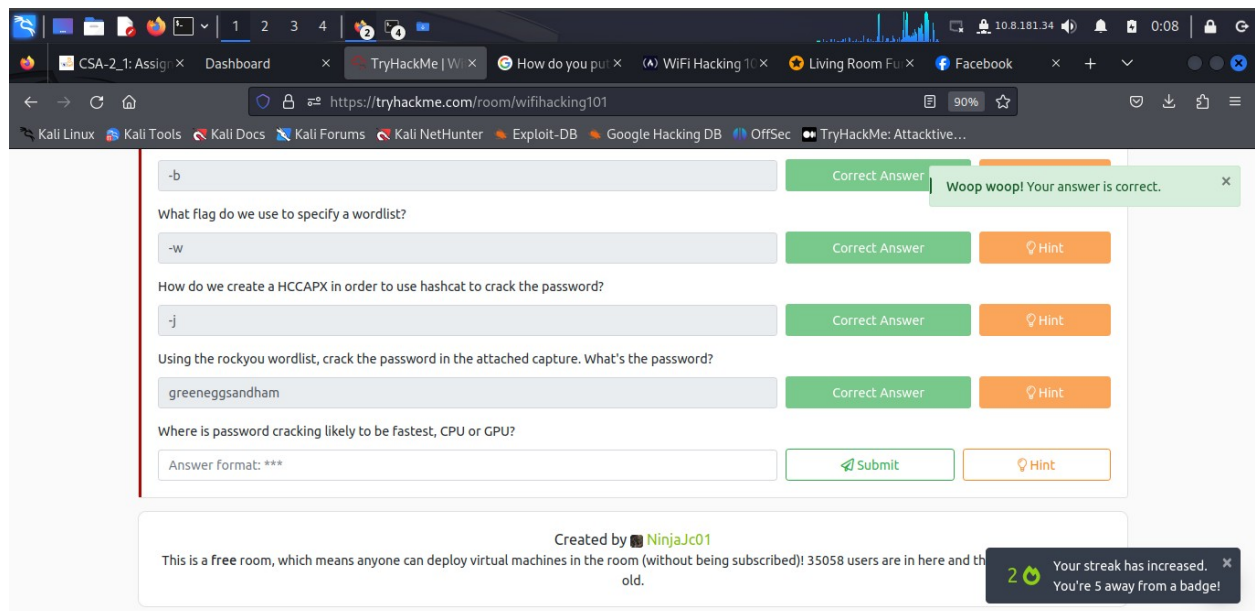
```
obed@kali: ~  
- (obed@kali)~  
$ sudo aircrack-ng check kill  
[sudo] password for obed:  
- (obed@kali)~  
$ aircrack-ng --help  
Aircrack-ng 1.7 - (C) 2006-2022 Thomas d'Otreppe  
https://www.aircrack-ng.org  
usage: aircrack-ng [options] <input file(s)>  
  
Common options:  
-a <amode> : force attack mode (1/WEP, 2/WPA-PSK)  
-e <essid> : target selection: network identifier  
-b <bssid> : target selection: access point's MAC  
-p <nbcpu> : # of CPU to use (default: all CPUs)  
-q : enable quiet mode (no status output)  
-C <macs> : merge the given APs to a virtual one  
-l <file> : write key to file. Overwrites file.  
  
Static WEP cracking options:  
-m <maddr> : MAC address to filter usable packets  
-n <nbits> : WEP key length : 64/128/152/256/512  
-i <index> : WEP key index (1 to 4), default: any  
-f <fudge> : bruteforce fudge factor, default: 2  
-k <korek> : disable one attack method (1 to 17)  
-x or -x0 : disable bruteforce for last keybytes  
-x1 : last keybyte bruteforcing (default)  
-x2 : enable last 2 keybytes bruteforcing  
-y : experimental single bruteforce mode  
-K : use only old Korek attacks (pre-PTW)  
-s : show the key in ASCII while cracking  
-M <num> : specify maximum number of IVs to use  
-D : WEP decloak, skips broken keystreams  
-P <num> : PTW debug: 1: disable Klein, 2: PTW  
-1 : run only 1 try to crack key with PTW  
-V : run in visual inspection mode  
  
WEP and WPA-PSK cracking options:  
-w <words> : path to wordlist(s) filename(s)  
-N <file> : path to new session filename  
-R <file> : path to existing session filename  
  
WPA-PSK options:
```

We create a HCCAPX in order to use hashcat to crack the password is `-j`

Using the rockyou wordlist, upon cracking the password in the attached capture, the password is **greeneggsandham**





Password cracking is likely to be fastest in **GPU**

Conclusion

The learner dived deeply to learning how to access a wireless network and navigating with **Aircrack-ng** tool and **rockyou**

Completion Link: <https://tryhackme.com/room/wifihacking101>