Wifi Hacking 101

Introduction

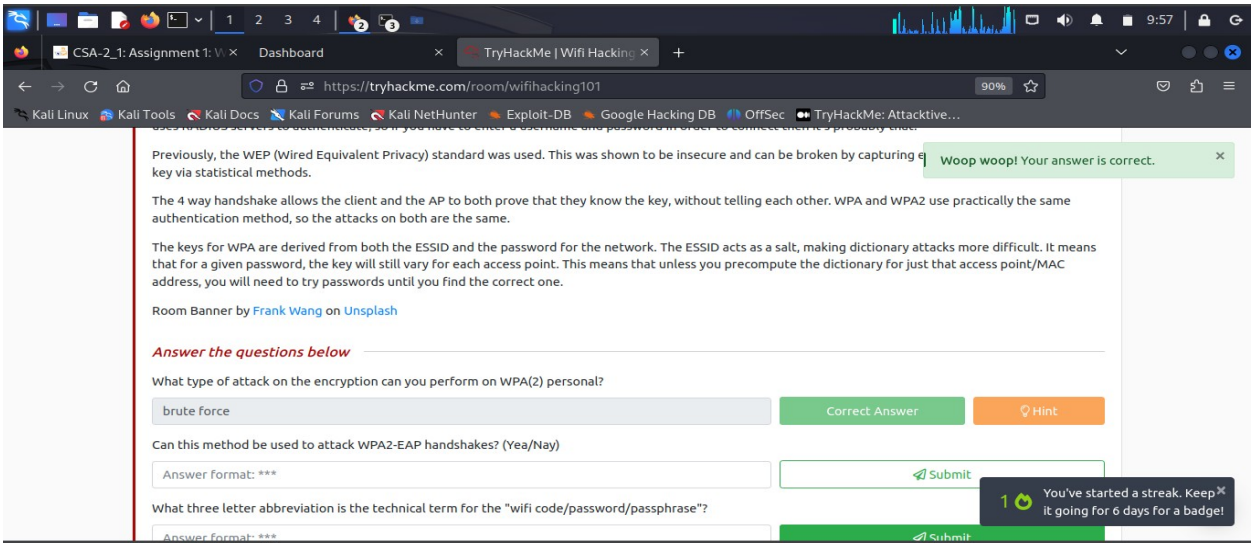
This sub task introduces the learner to the practical knowledge of attacking a wifi network by going through a series of what is called rooms for a special skill particularly.

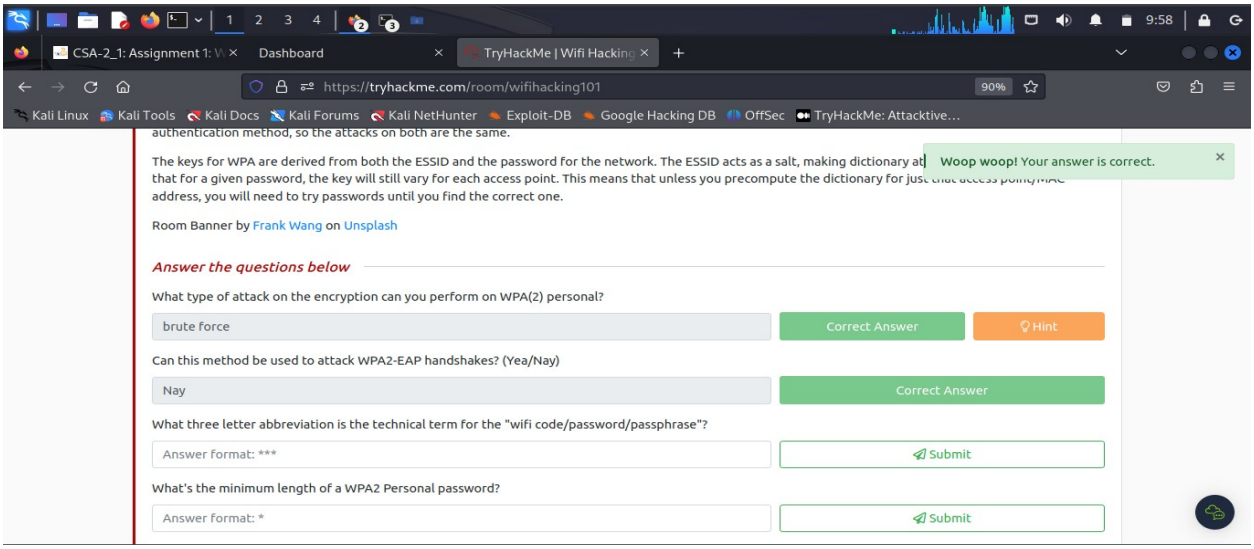
The activities to be covered in details are: The basics – An Intro to WPA, – Capturing packets to attack, Aircrack-ng – Let's Get Cracking.

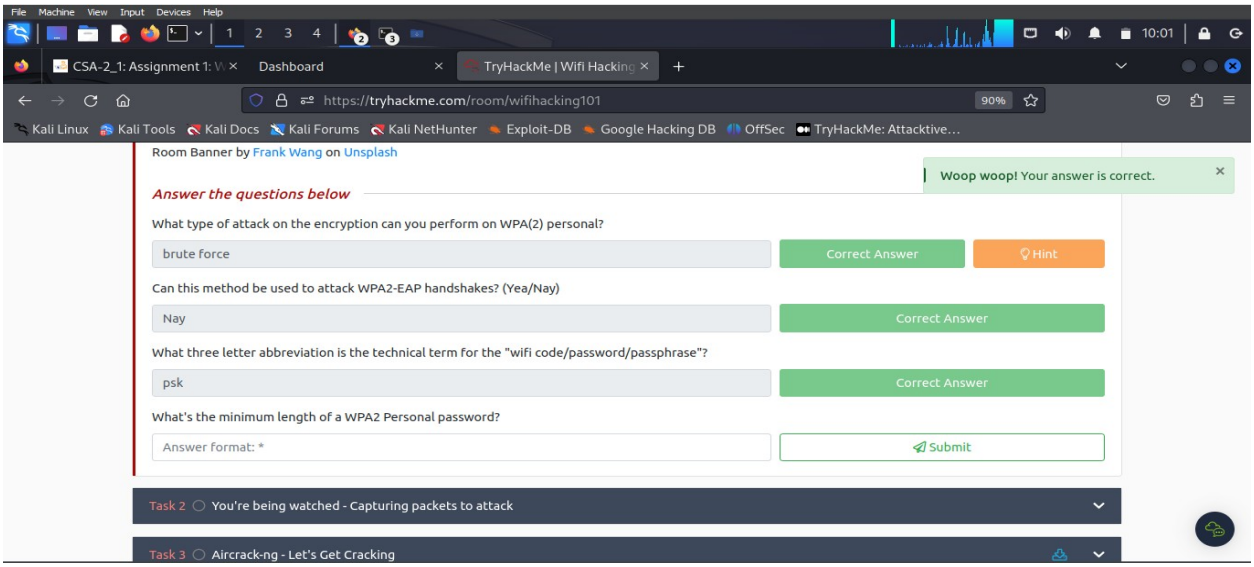
Activities

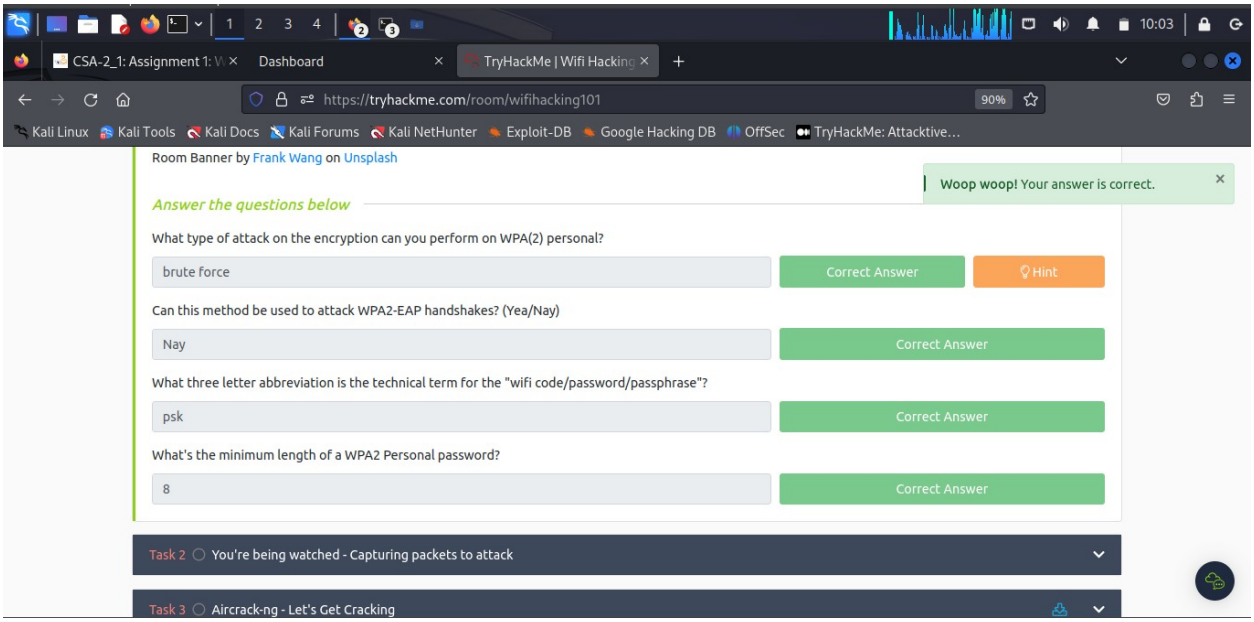
Task 1: The basics – An Intro to WPA

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




CSA-2_1: Assignment 1:
Dashboard
TryHackMe | Wifi Hacking
https://tryhackme.com/room/wifihacking101
90%
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
TryHackMe: Attacktive...
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 at
that for a given password, the key will still vary for each access point. This means that unless you precompute the dictionary for just
address, you will need to try passwords until you find the correct one.
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"?
Answer format: ***
Submit
What's the minimum length of a WPA2 Personal password?
Answer format: *
Submit


File Machine View Input Devices Help
CSA-2_1: Assignment 1:
Dashboard
TryHackMe | Wifi Hacking
https://tryhackme.com/room/wifihacking101
90%
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
TryHackMe: Attacktive...
Room Banner by Frank Wang on Unsplash
Woop woop! Your answer is correct.
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

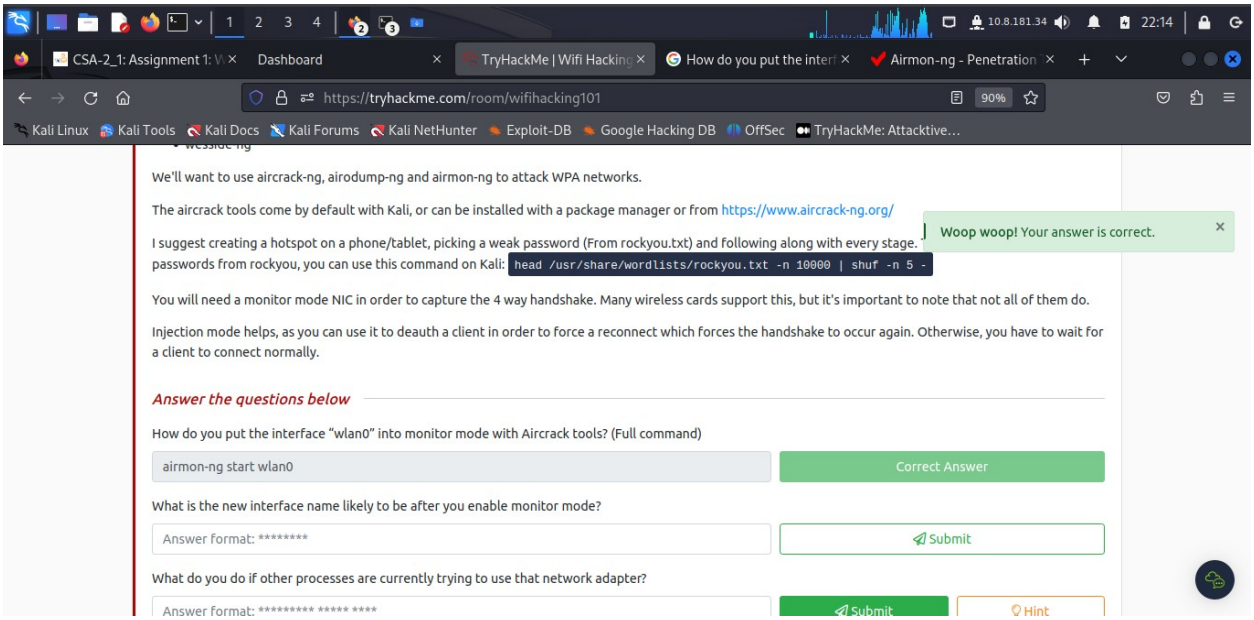


Task 2: You're being watched – Capturing packets to attack

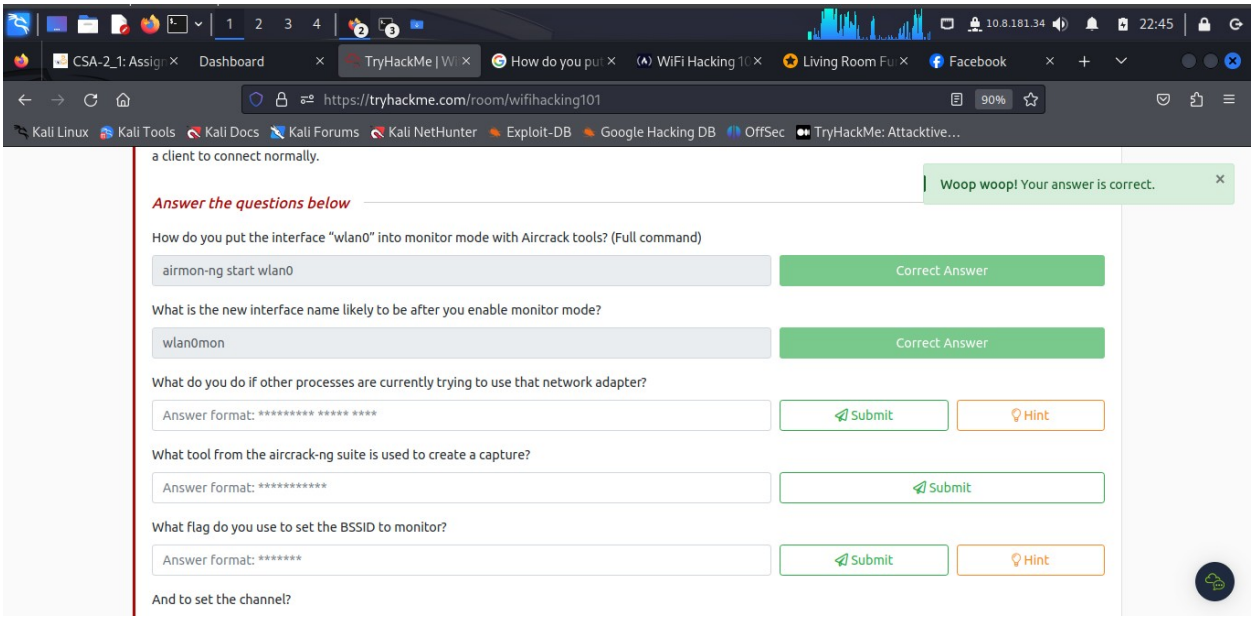
The Aircrack-ng suite is used attack a wifi network, and the learner will walk through attacking a network themselves, assuming they have a monitor mode enabled NIC.

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

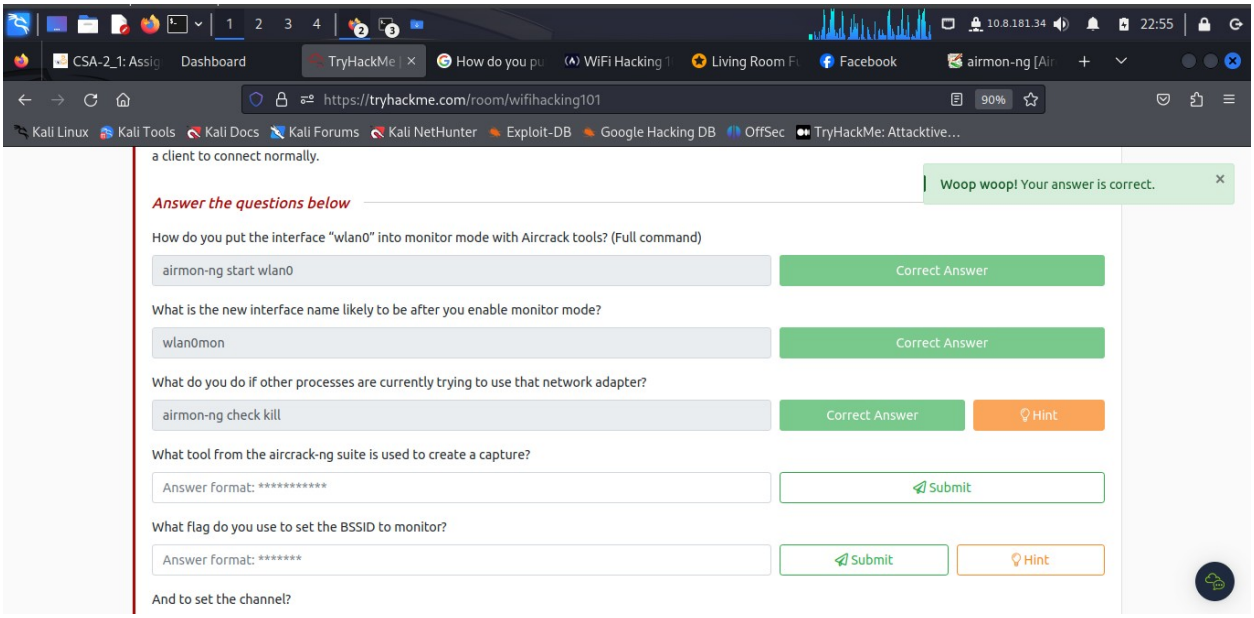
Task 3: Aircrack-ng – Let's Get Cracking



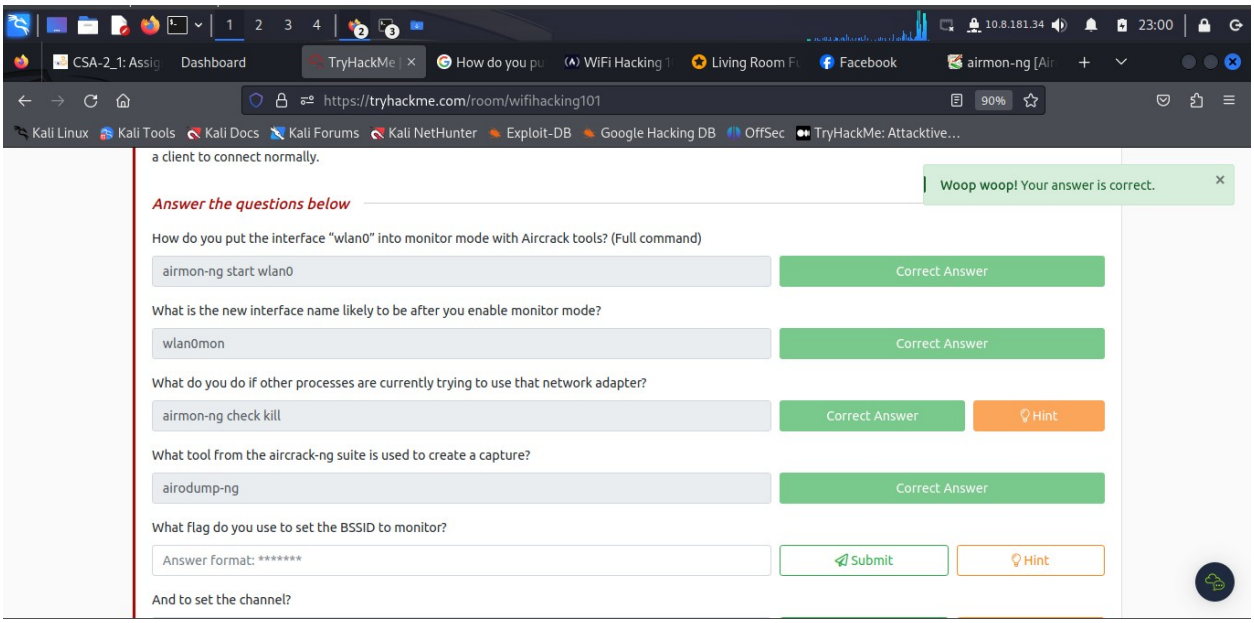
To put the interface "wlan0" into monitor mode with Aircrack tools? (Full command): ***sudo airmon-ng start wlan0***

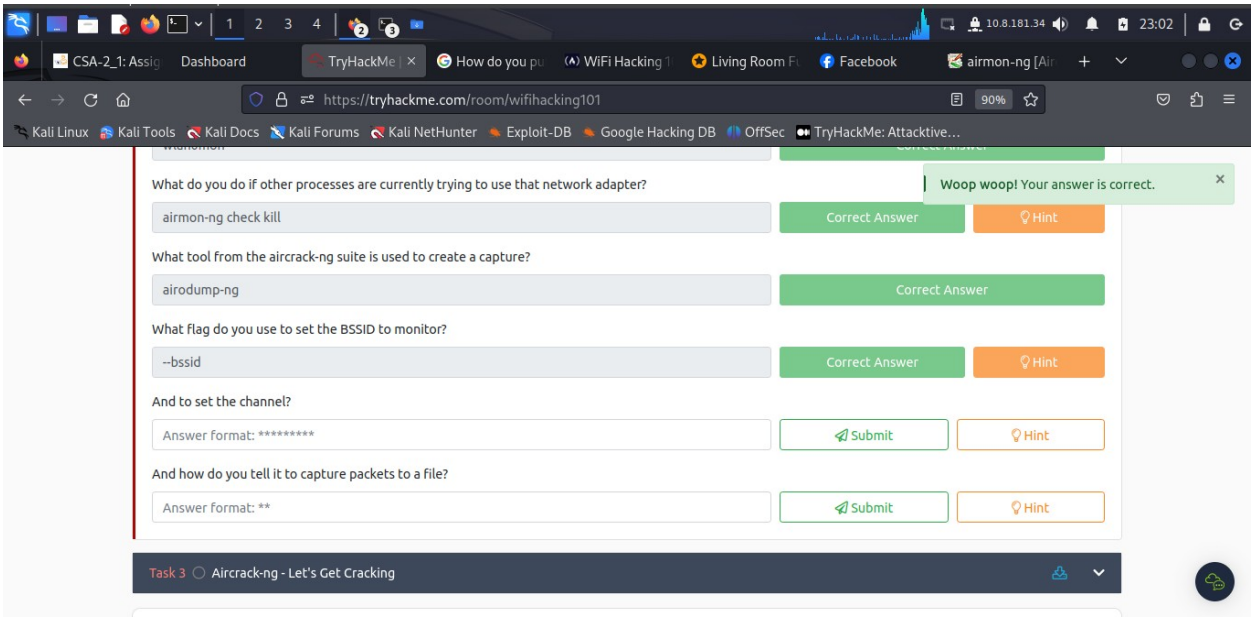


The new interface name likely to be after you enable monitor mode is **wlan0mon**

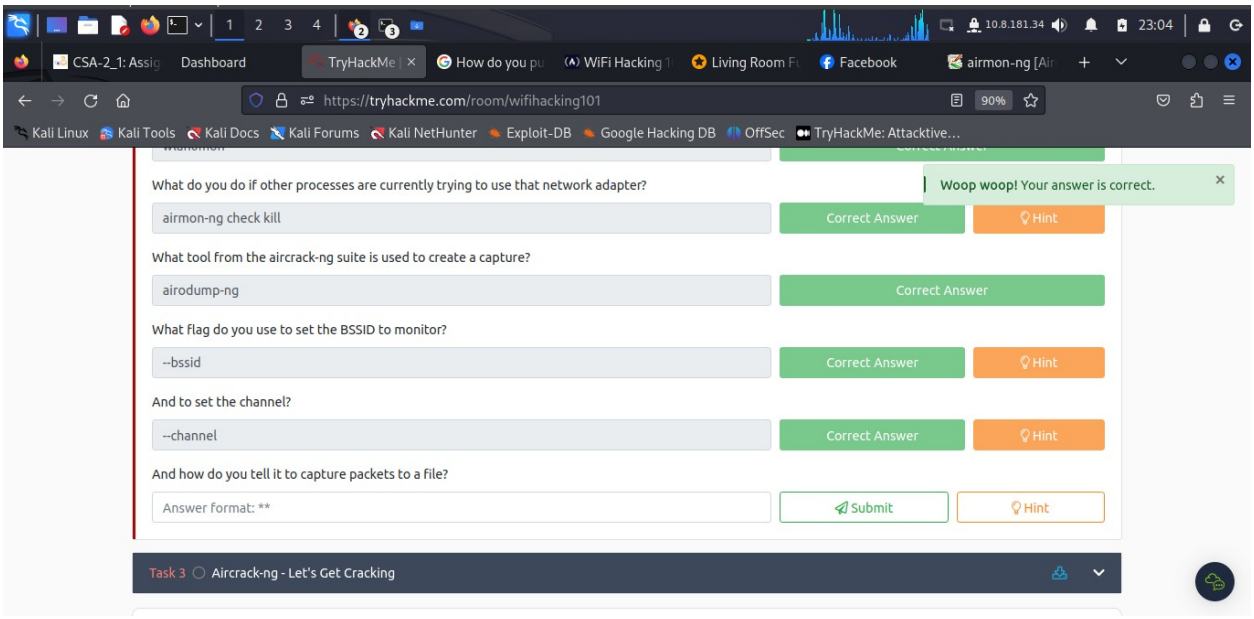


If other processes are currently trying to use that network adapter use **airmon-ng check kill.**

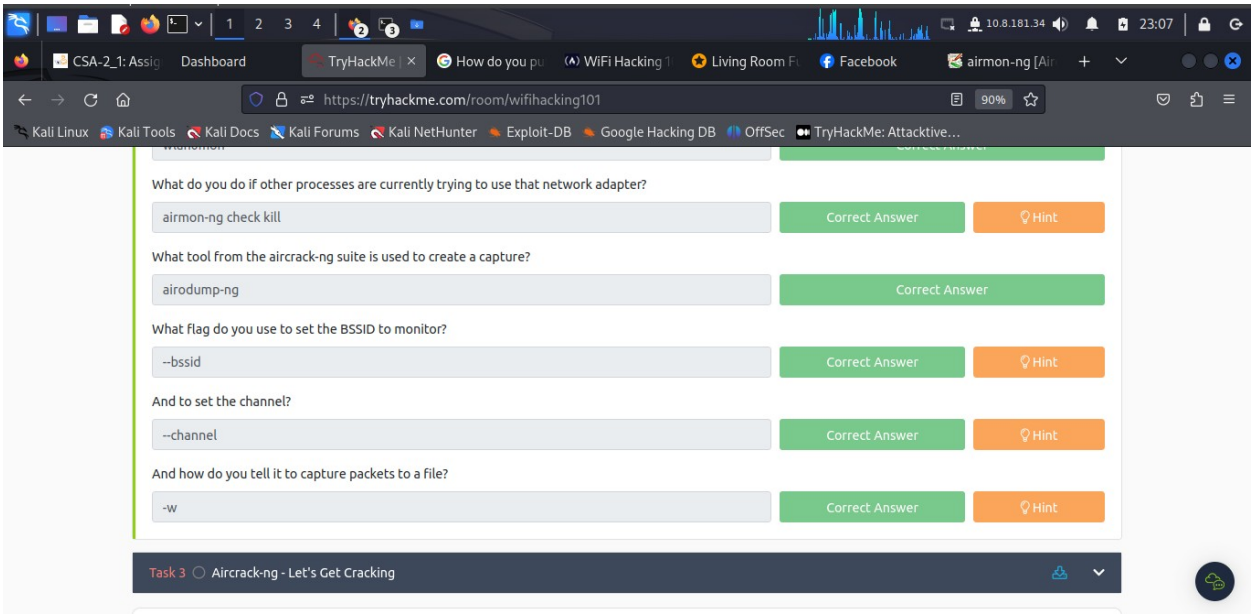




The flag used to set the BSSID to monitor is **–bssid**

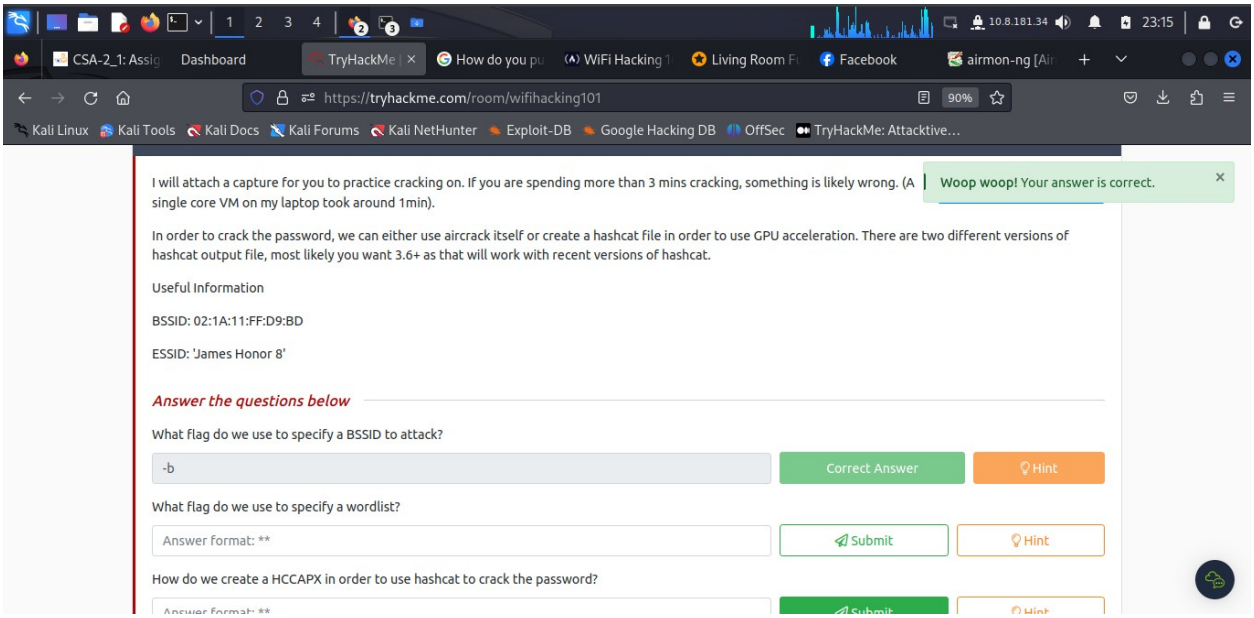


To set the channel run **--channel**

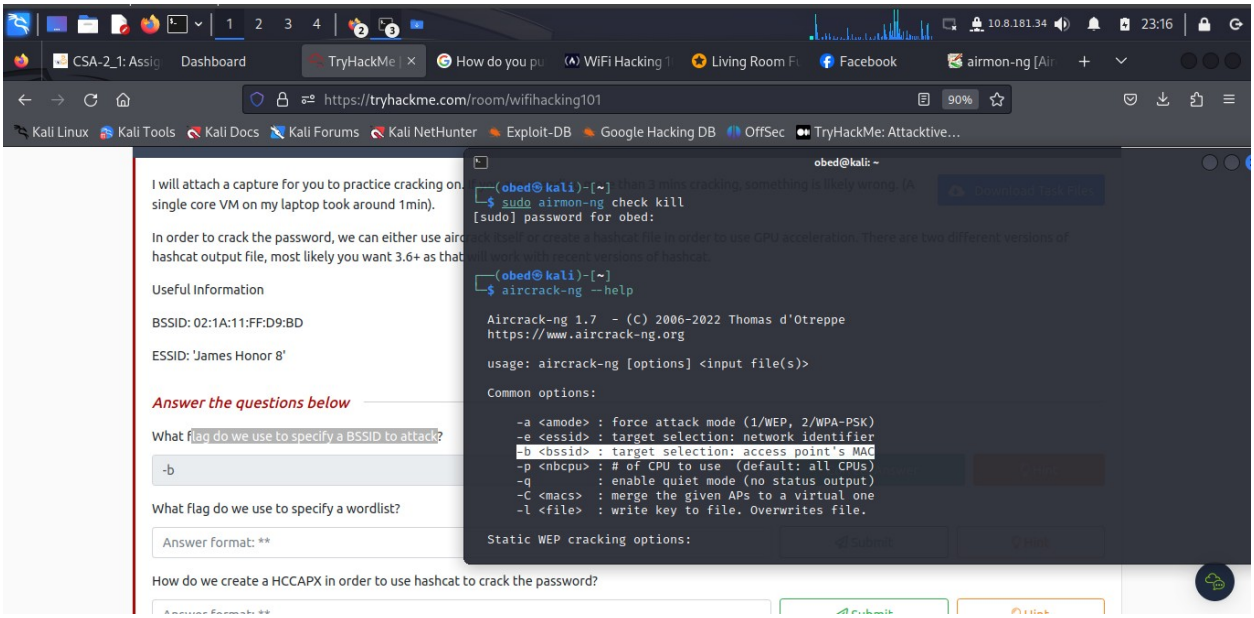


To tell it to capture packets to a file run **–w.**

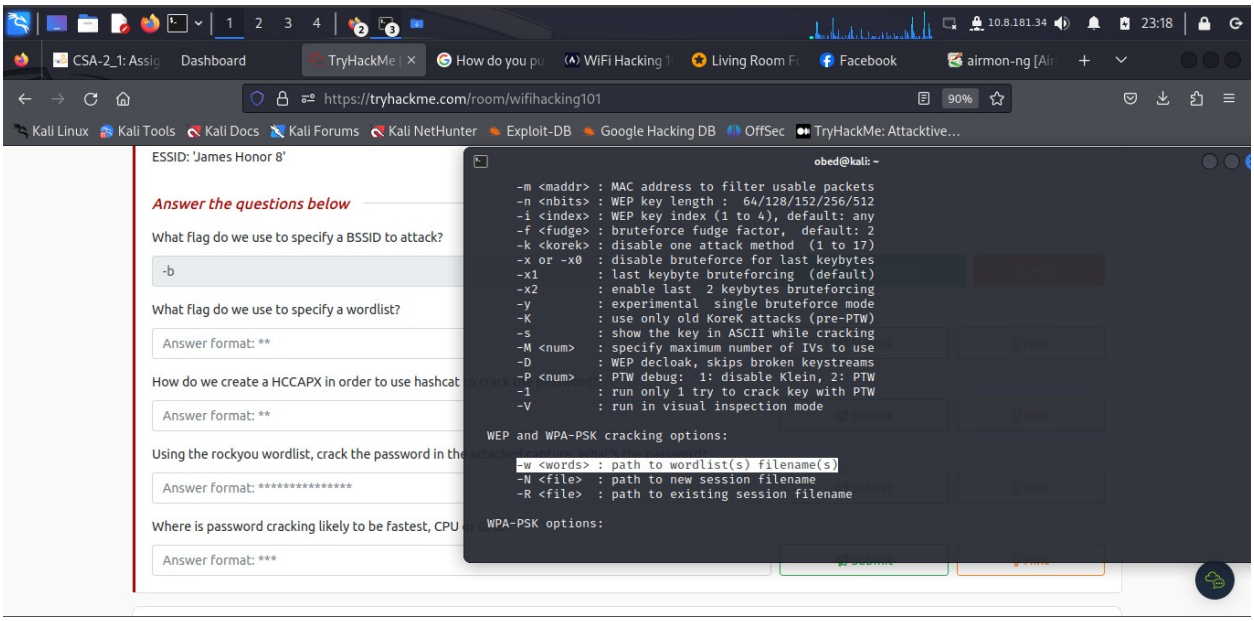
Task 3: Aircrack-ng - Let's Get Cracking

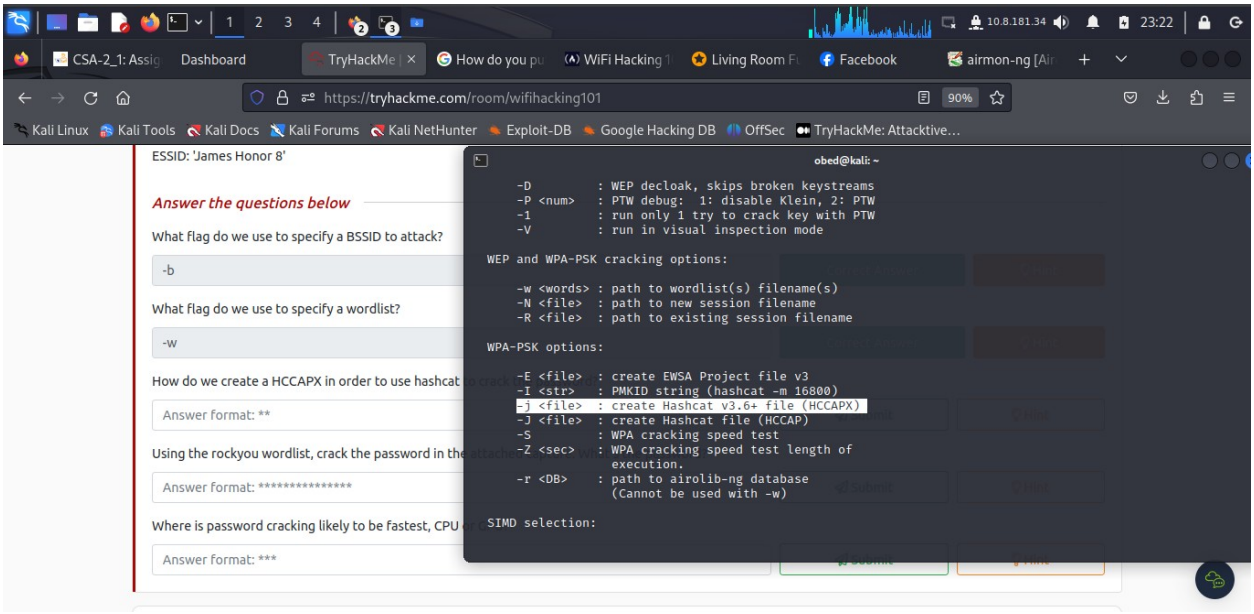


The flag do we use to specify a BSSID to attack is **–b.**



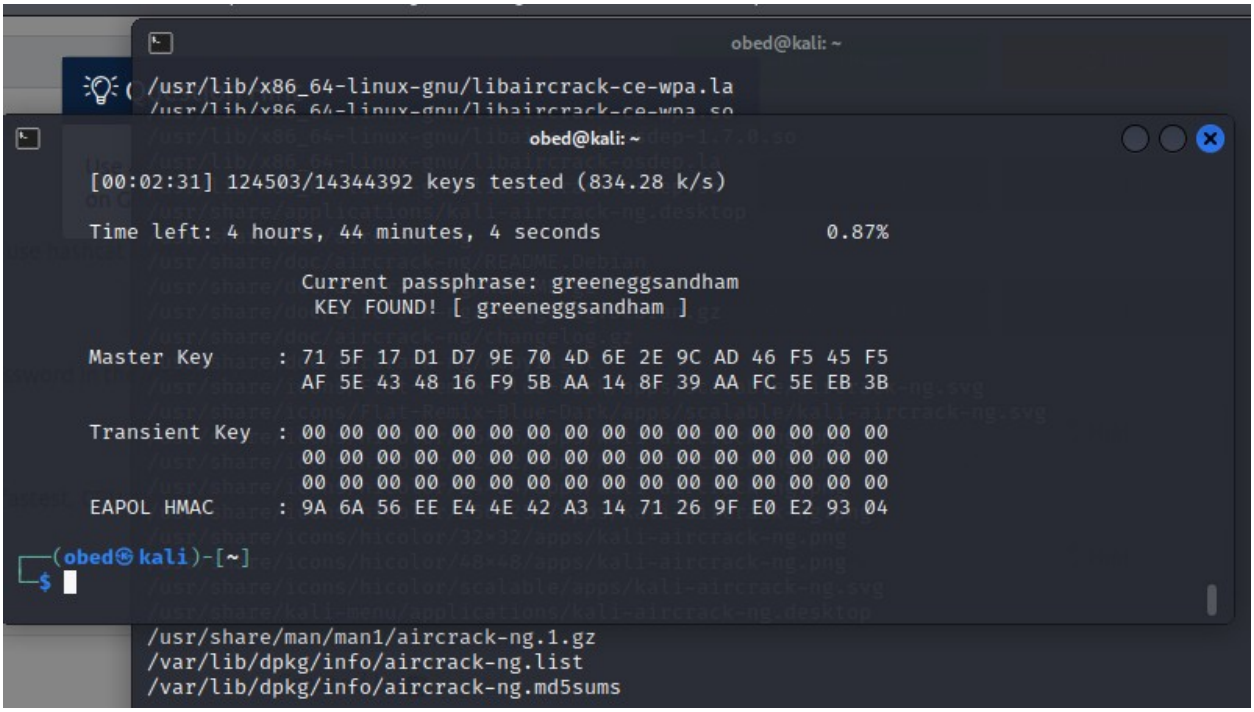
The flag we use to specify a wordlist is **-w**

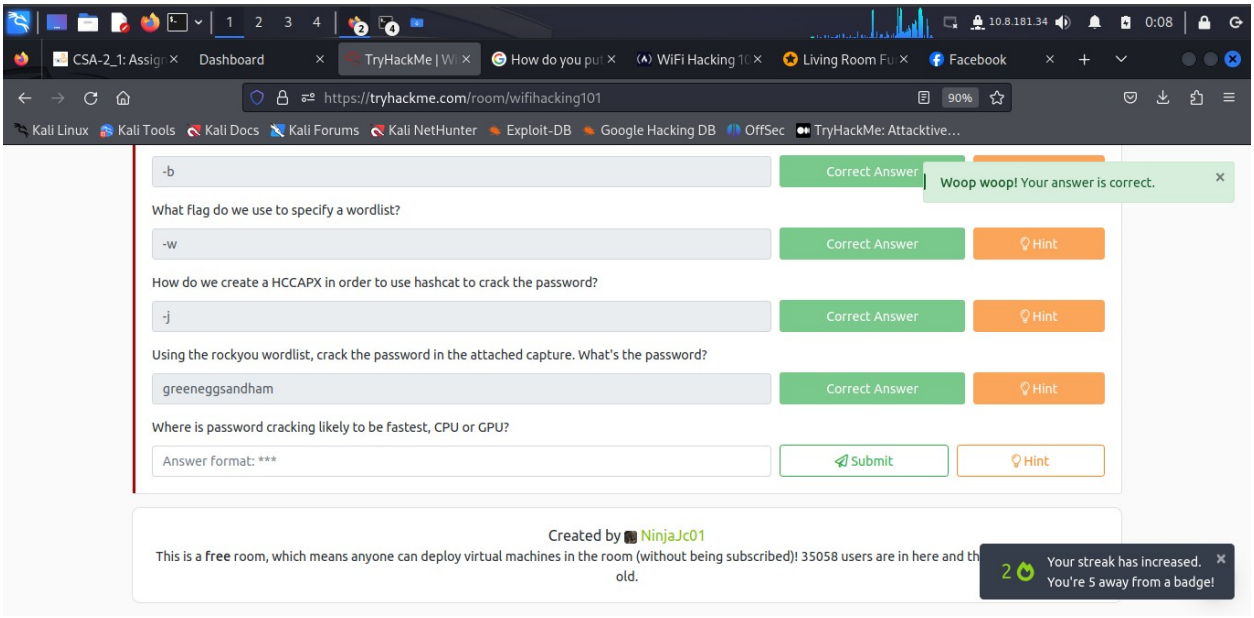


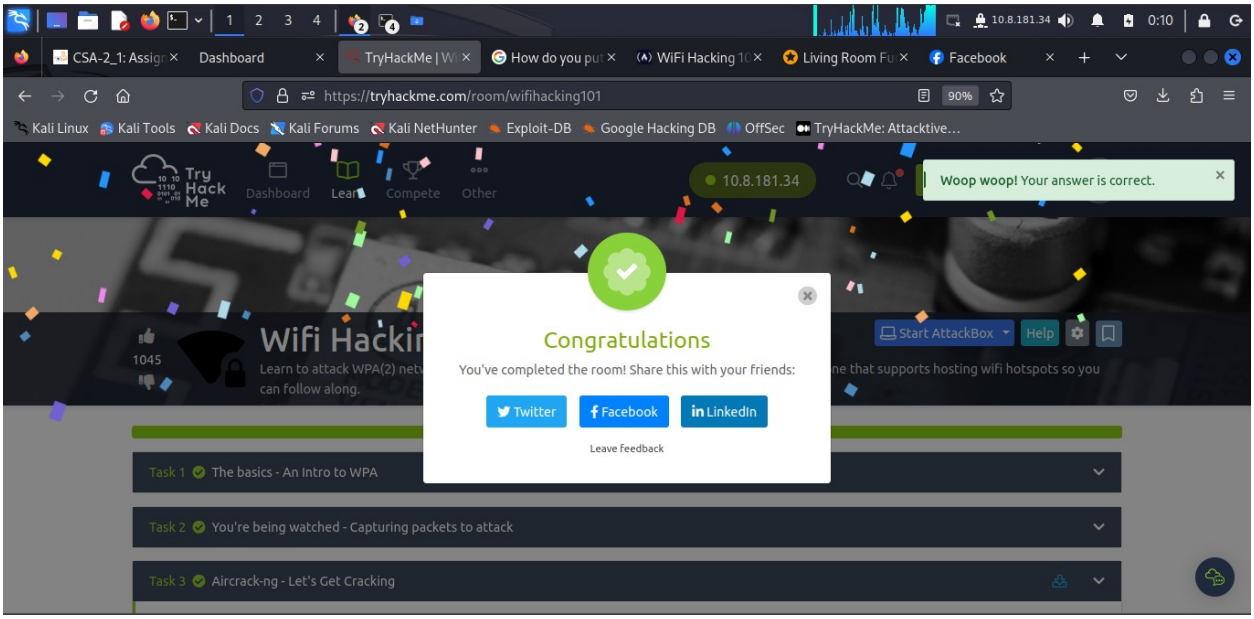


We create a HCCAPX in order to use hashcat to crack the password is **–j**

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