**Wifi Hacking 101**

**Introduction**

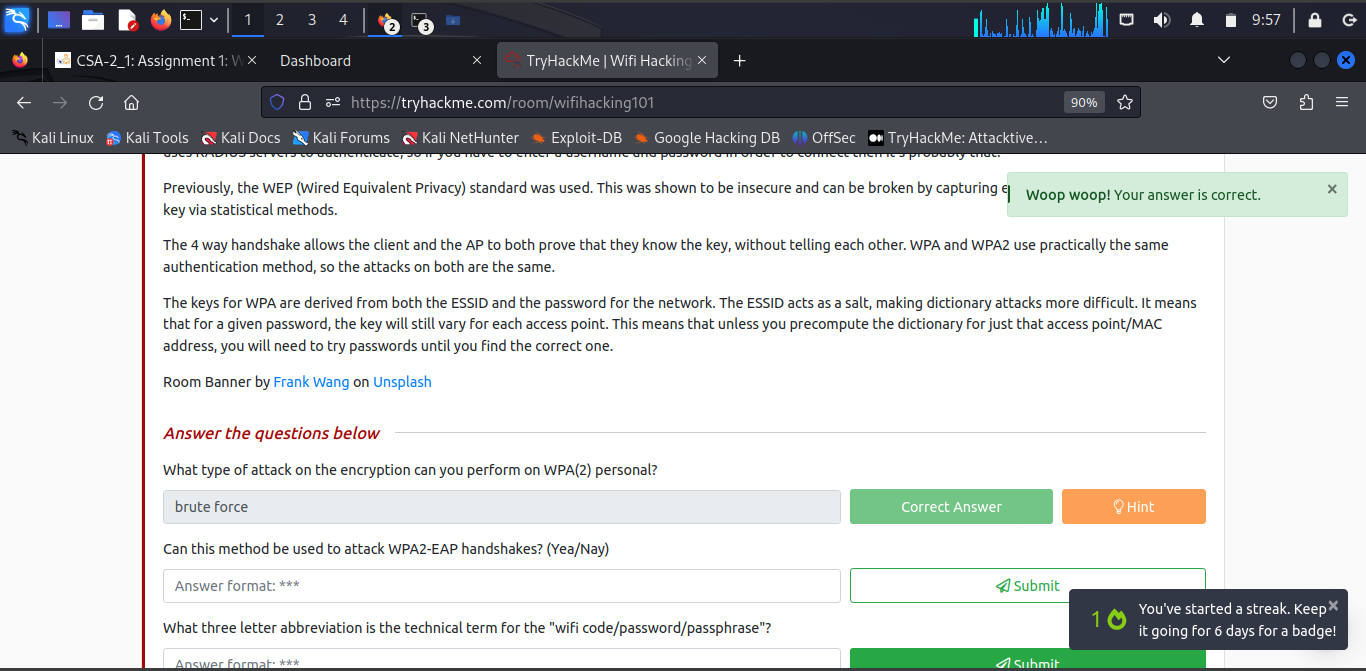
This sub task introduces the learner to the practical knowledge of attacking a wifi network by going through a series of what is called rooms for a special skill particularly.

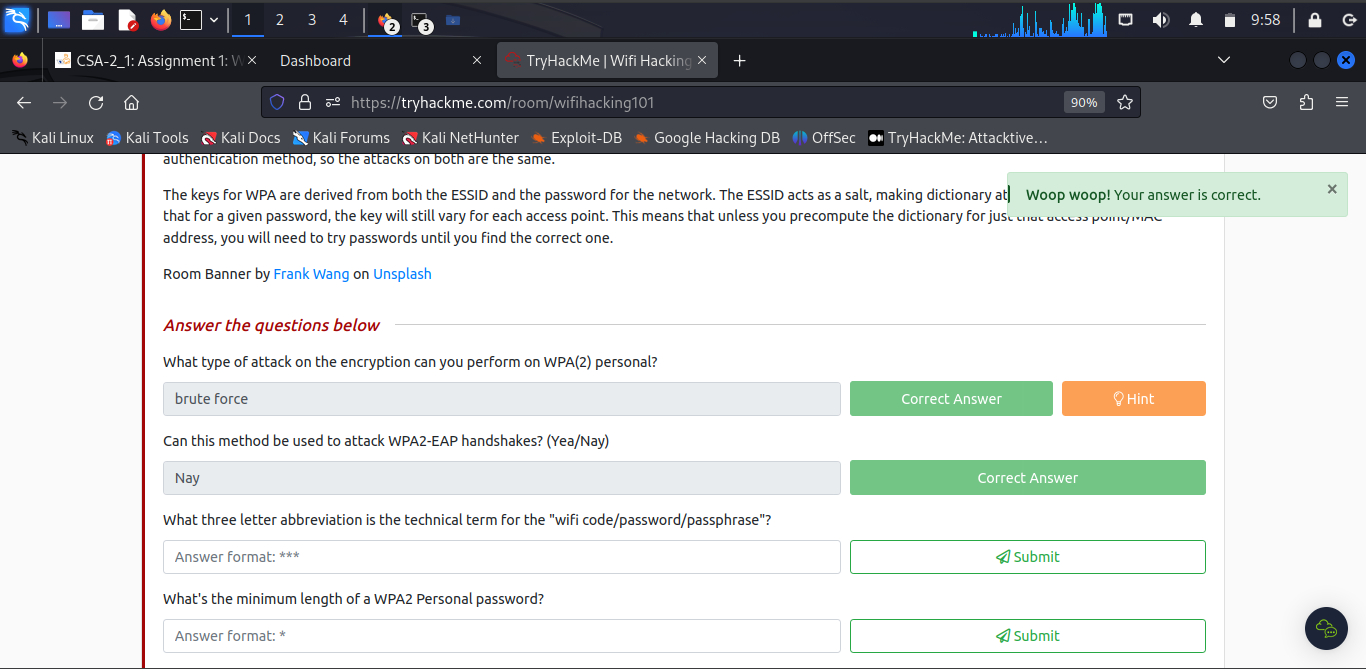
The activities to be covered in details are: The basics – An Intro to WPA, – Capturing packets to attack, Aircrack-ng – Let’s Get Cracking.

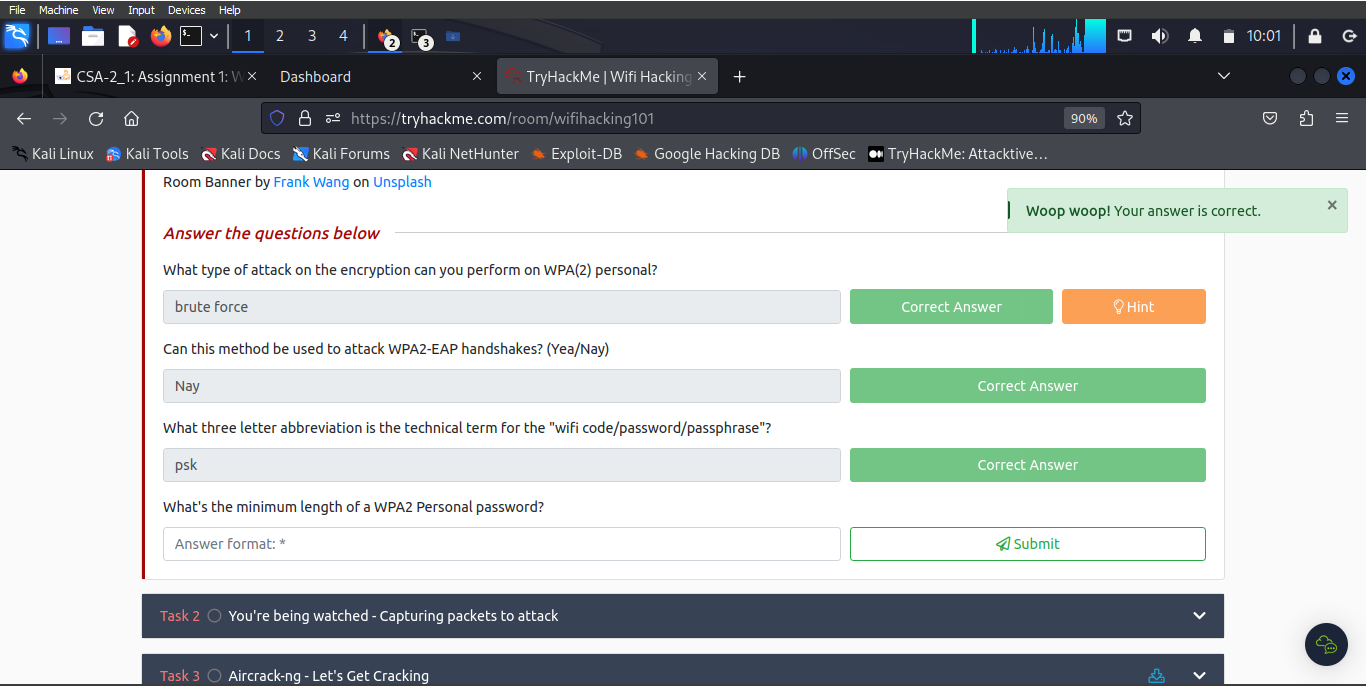
***Activities***

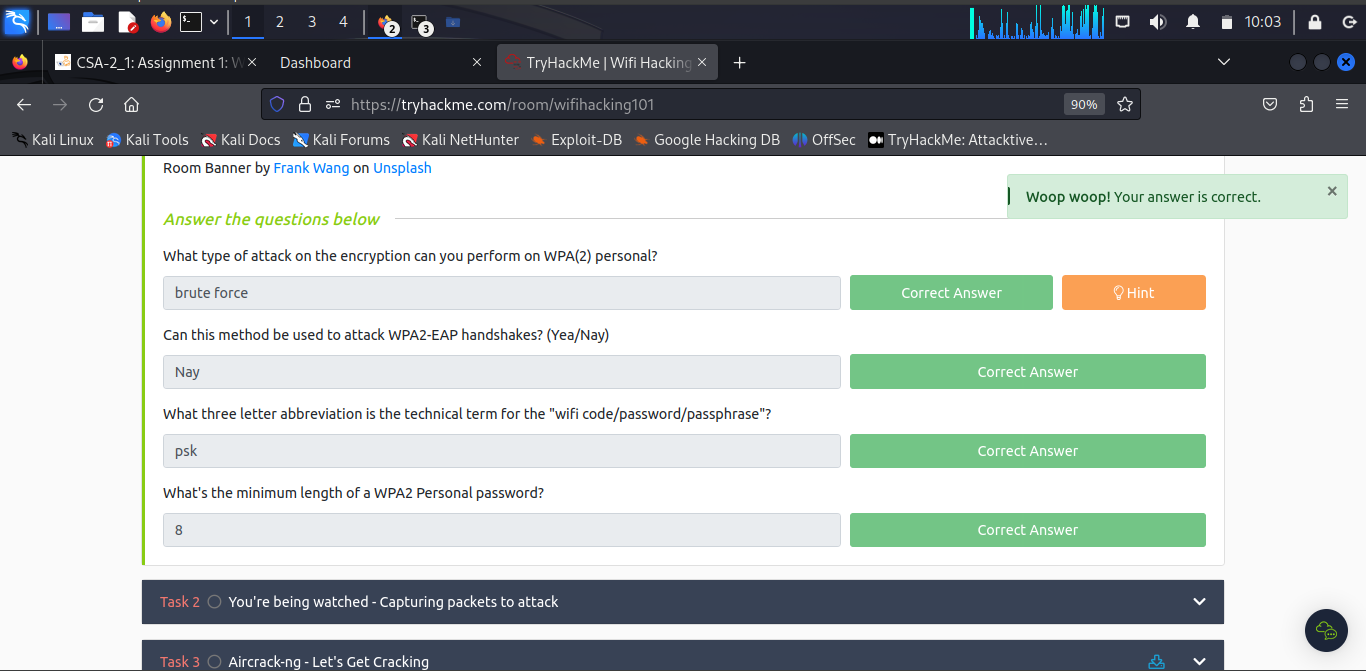
***Task 1: The basics – An Intro to WPA***

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







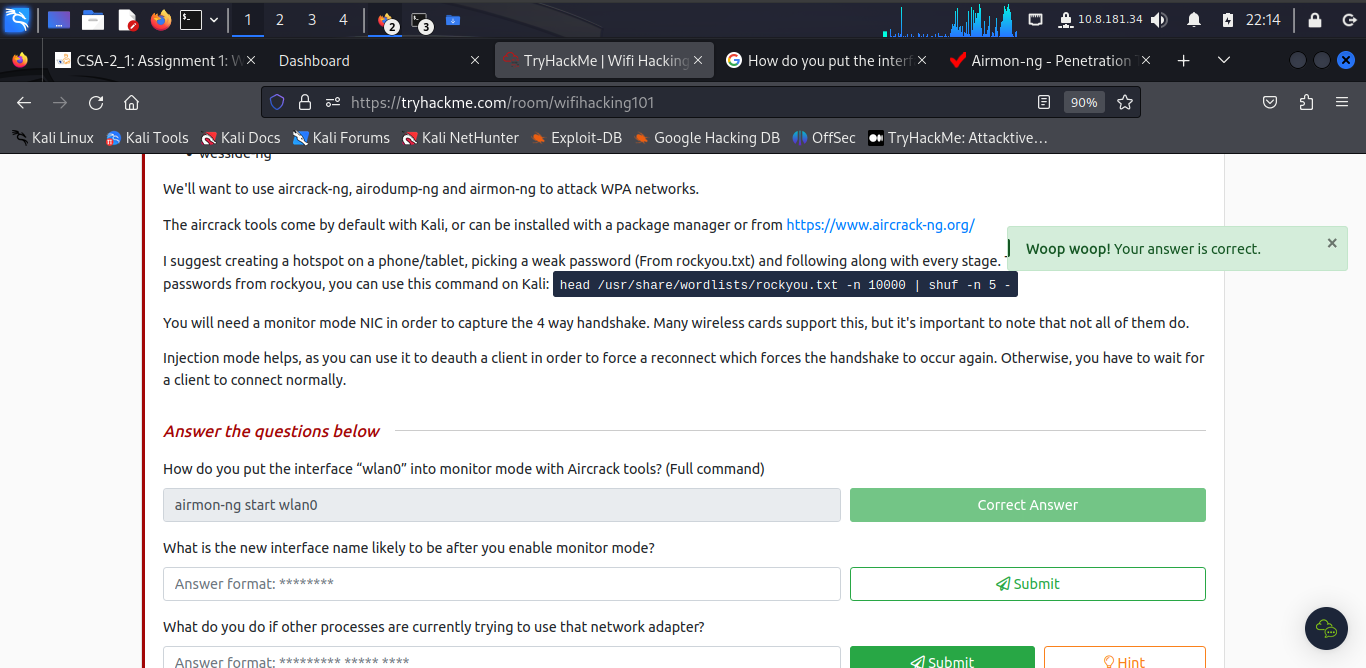


***Task 2: You’re being watched – Capturing packets to attack***

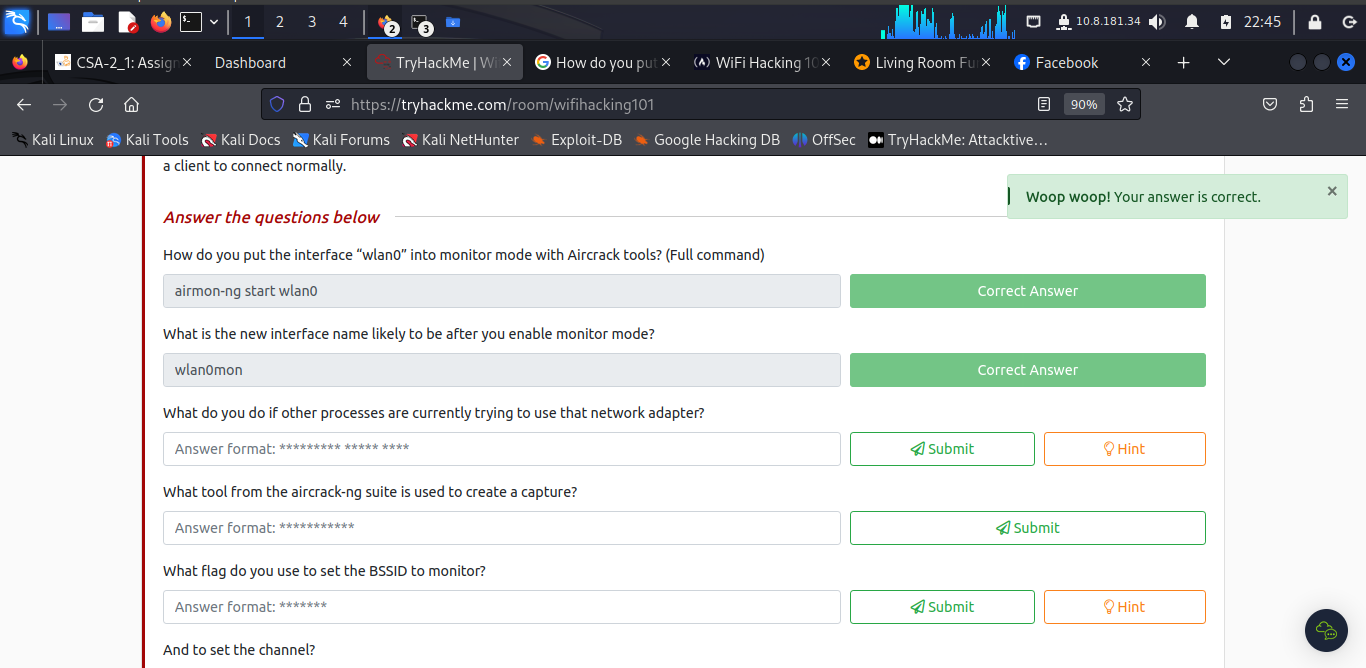
The Aircrack-ng suite is used attack a wifi network, and the learner will walk through attacking a network themselves, assuming they have a monitor mode enabled NIC.

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

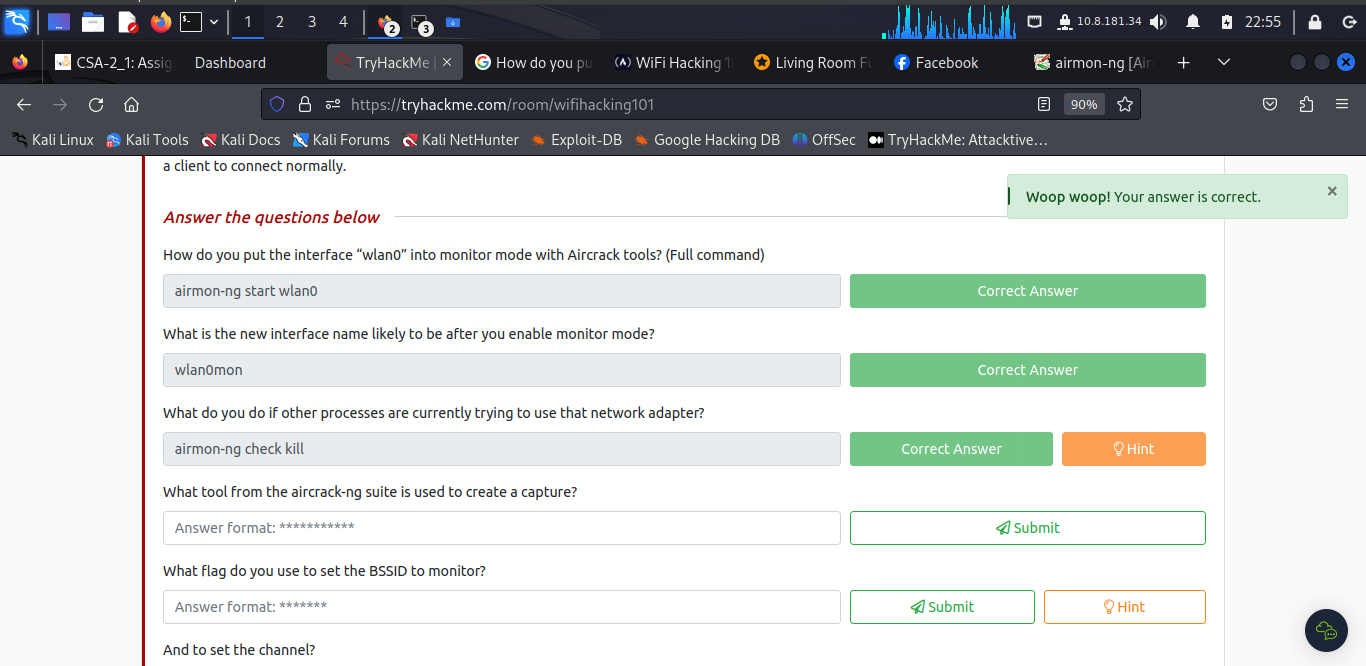
***Task 3: Aircrack-ng – Let’s Get Cracking***



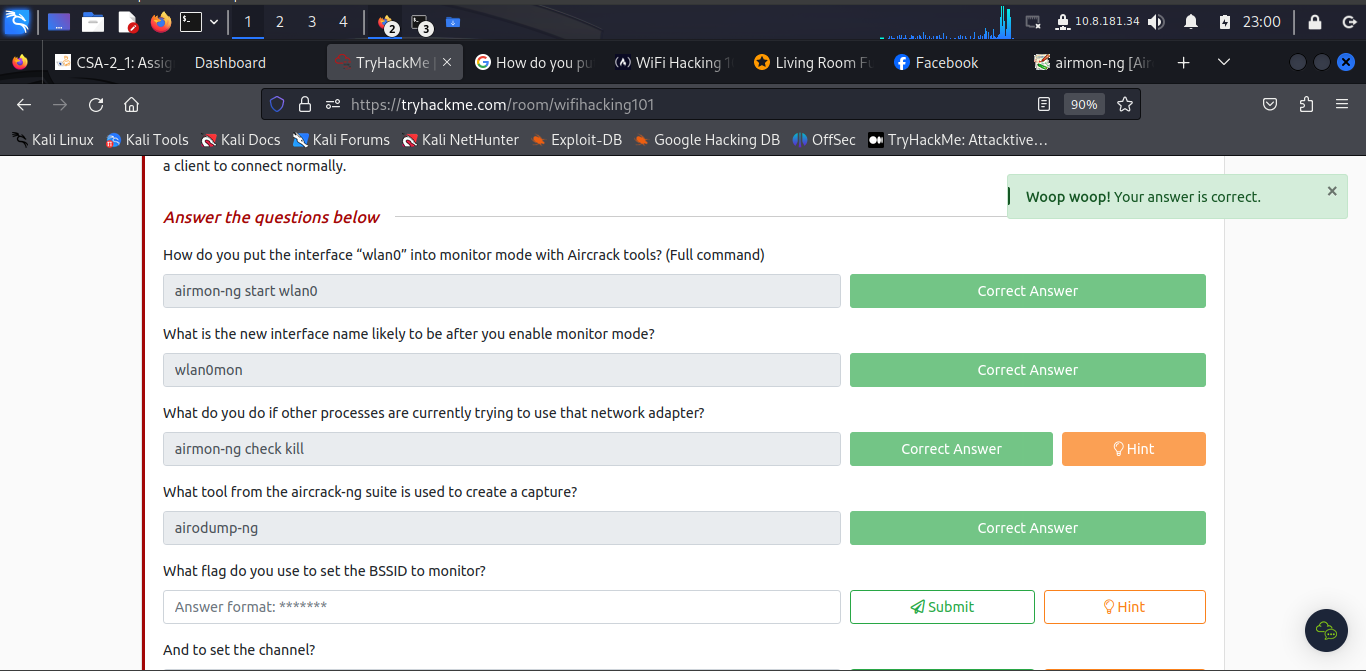
To put the interface “wlan0” into monitor mode with Aircrack tools? (Full command): ***sudo airmon-ng start wlan0***

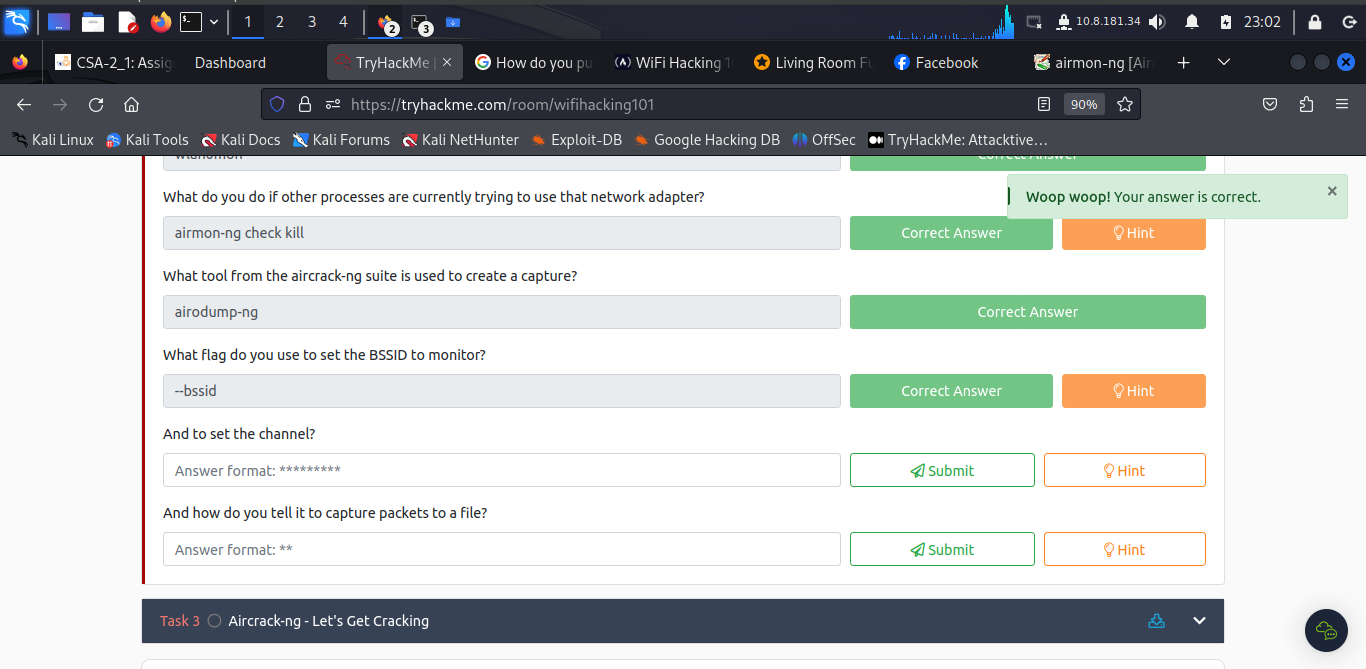


The new interface name likely to be after you enable monitor mode is **wlan0mon**

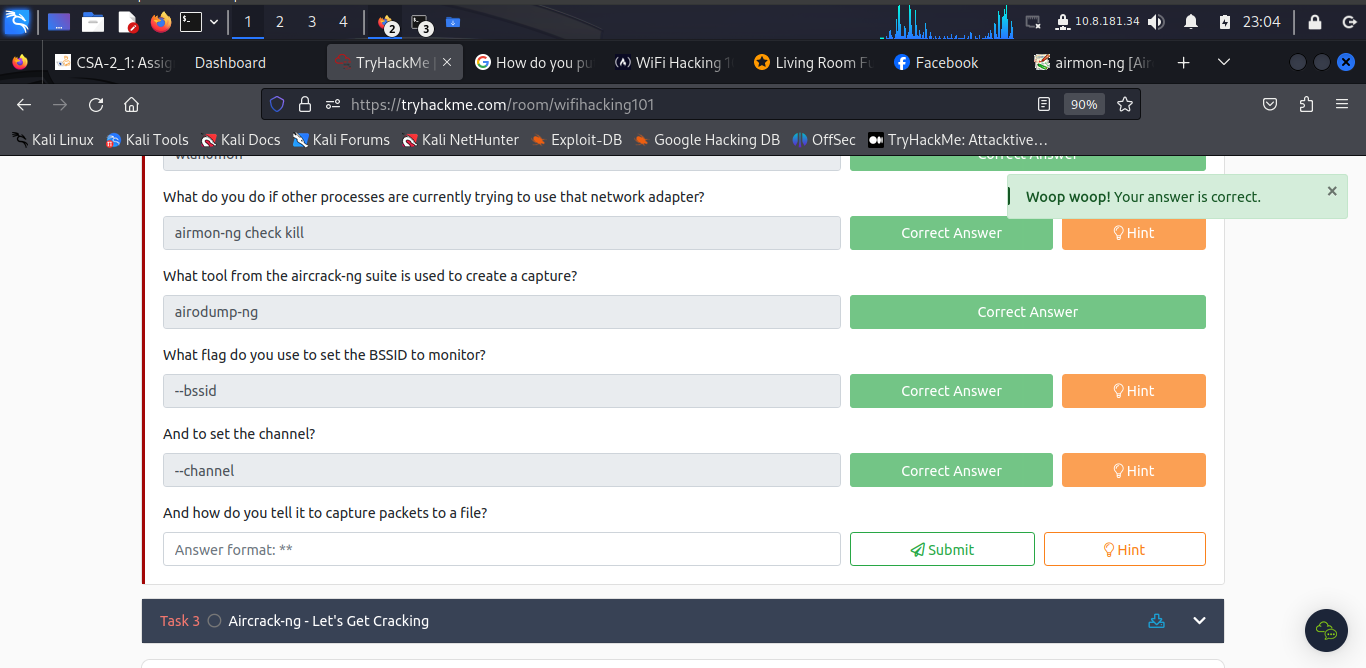
****

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

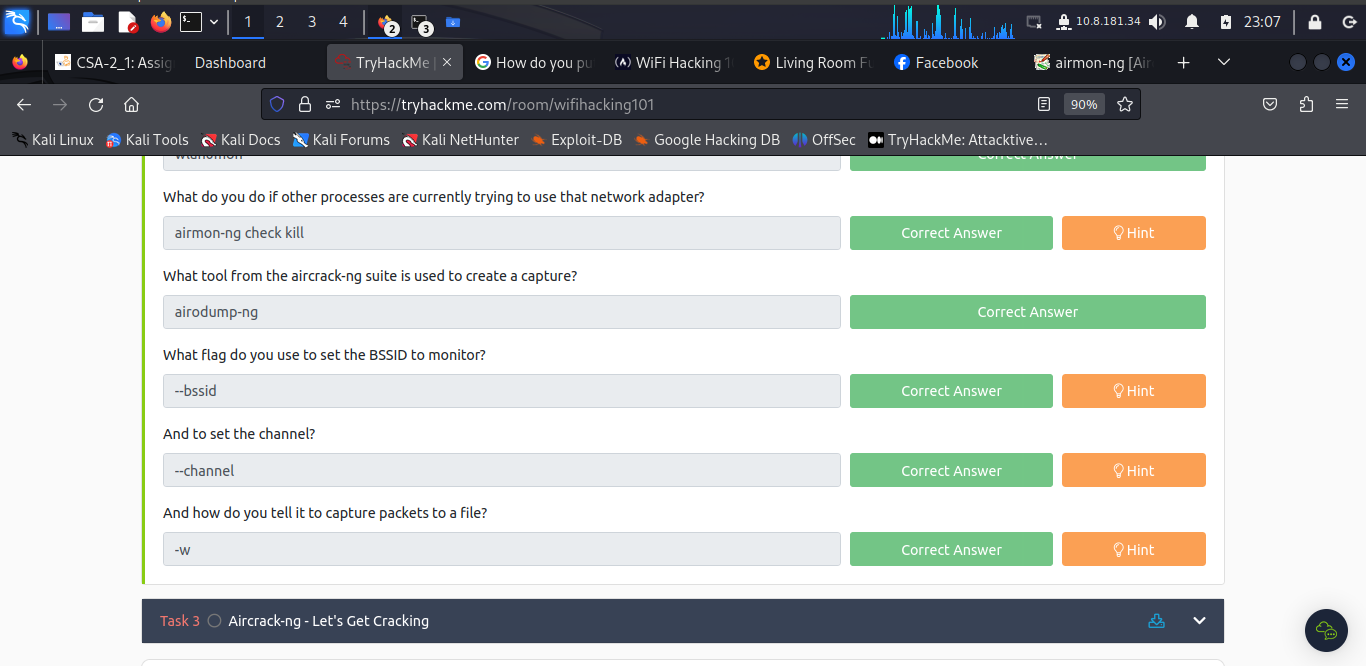
****

****

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

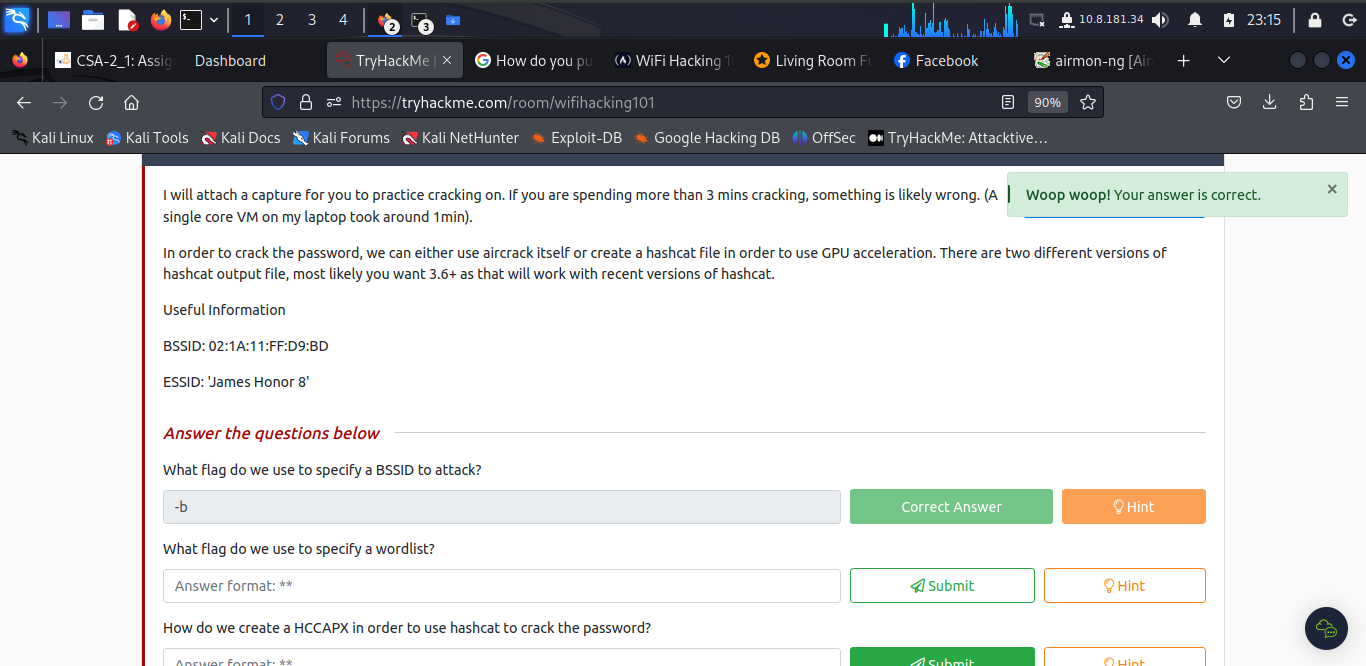
****

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

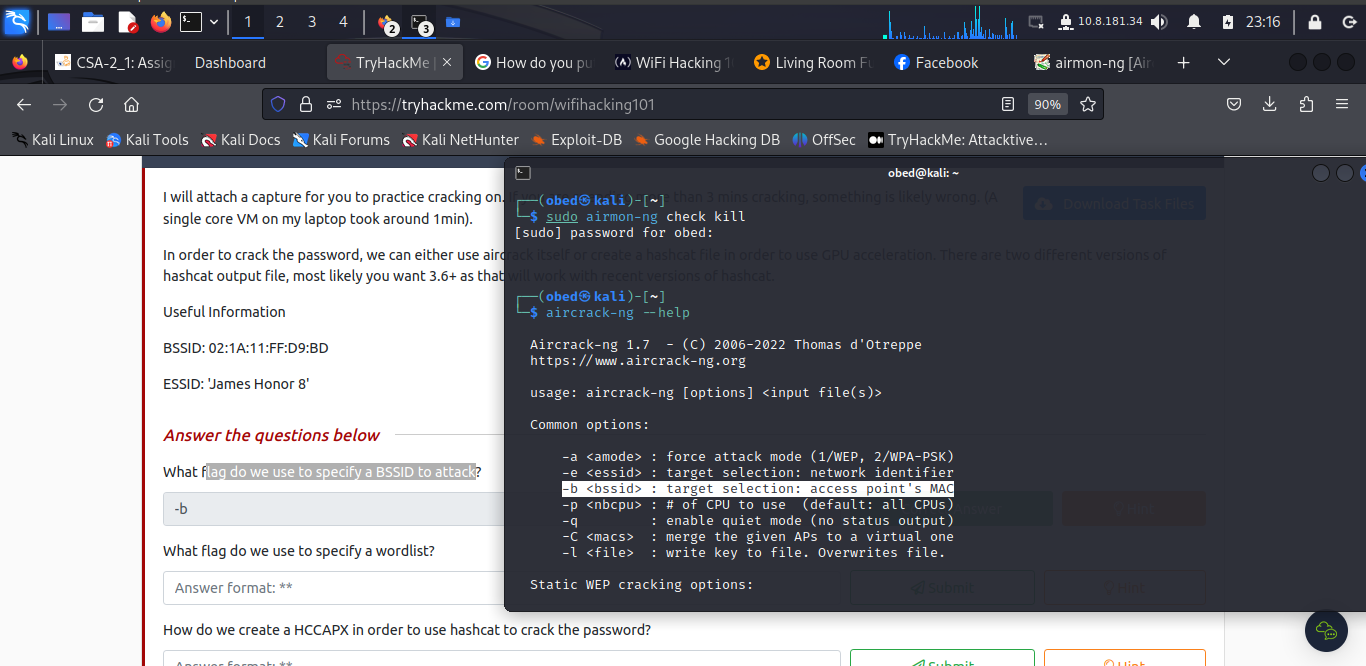
****

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

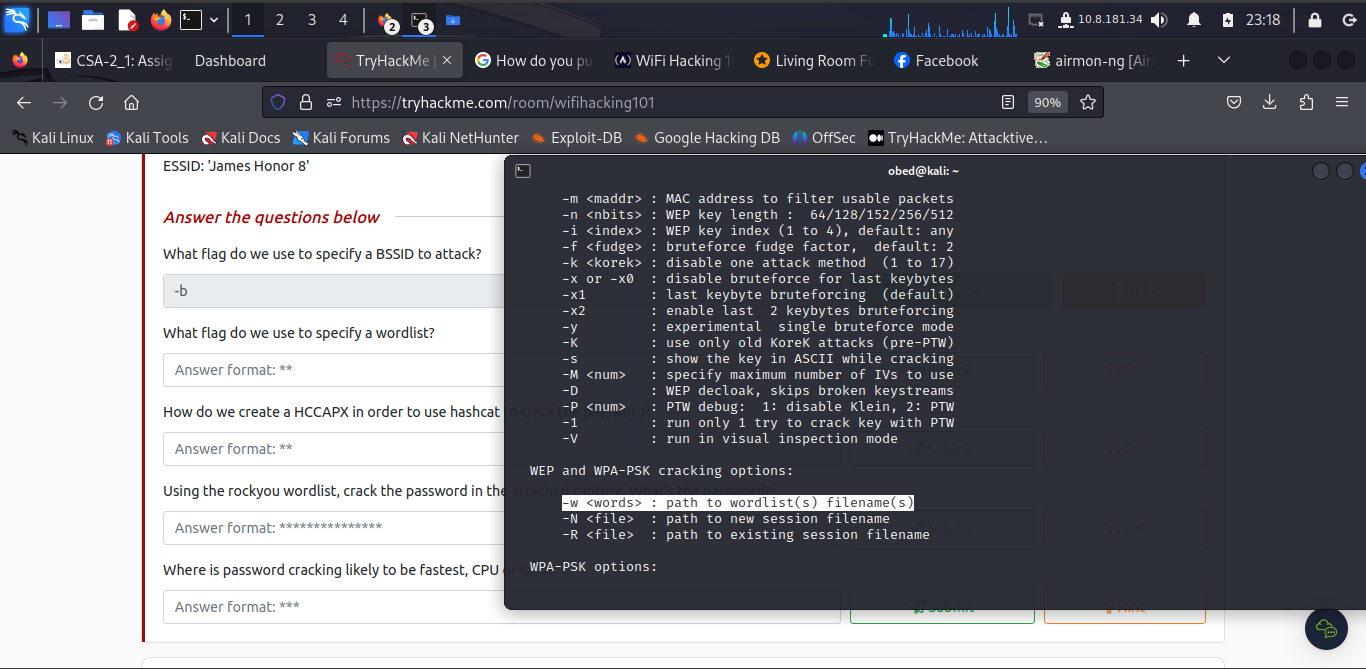
***Task 3: Aircrack-ng - Let's Get Cracking***

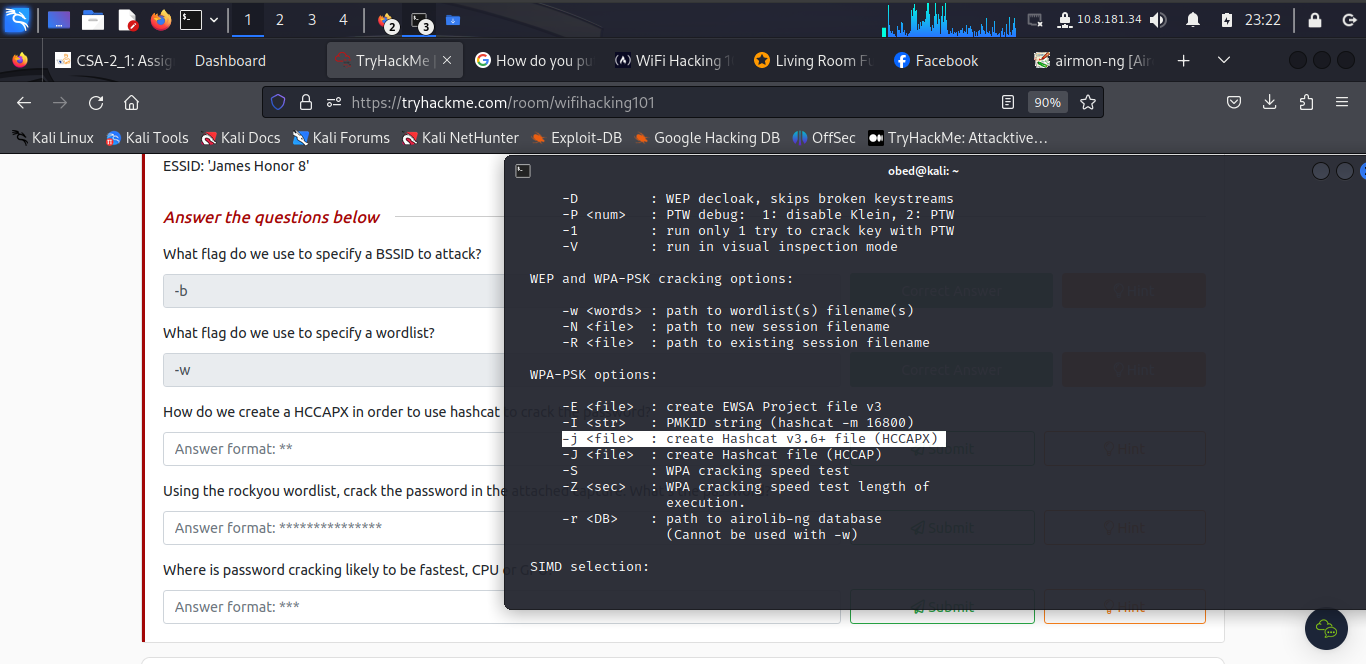


The flag do we use to specify a BSSID to attack is **–b.**

****

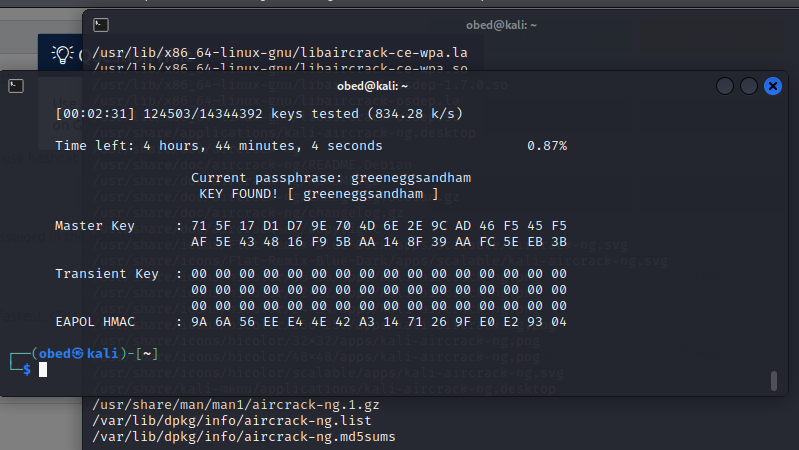
The flag we use to specify a wordlist is **-w**

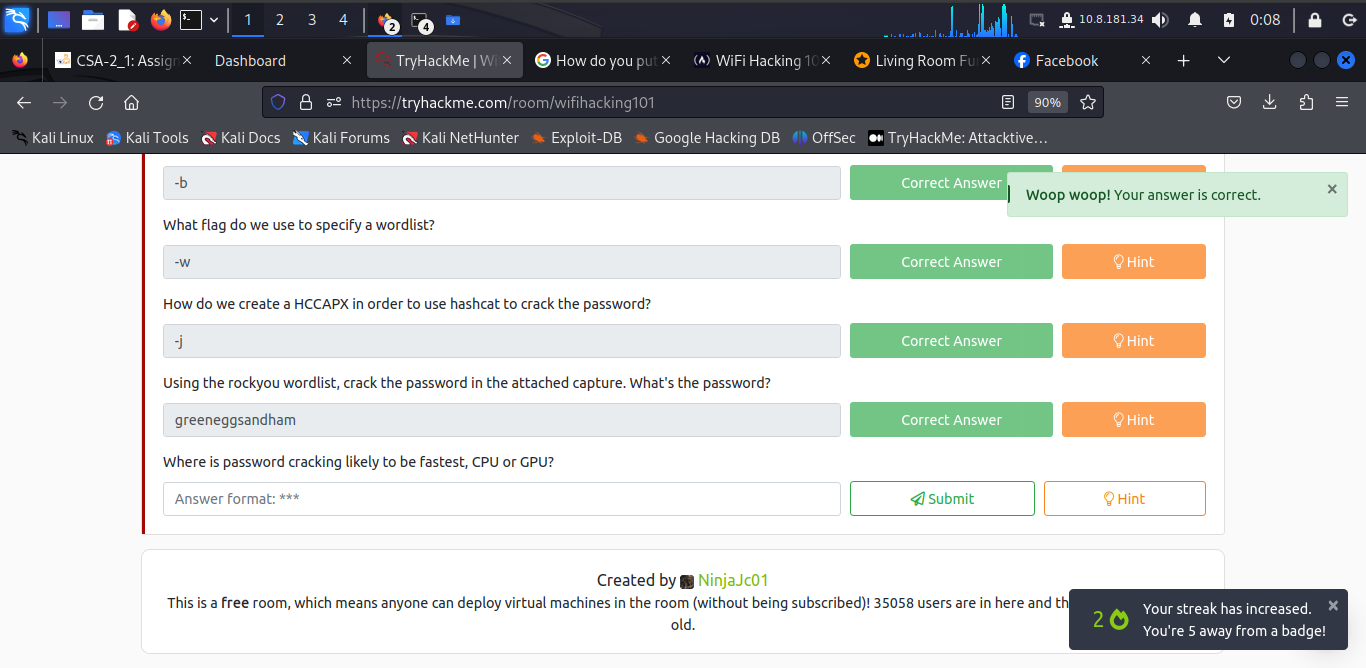


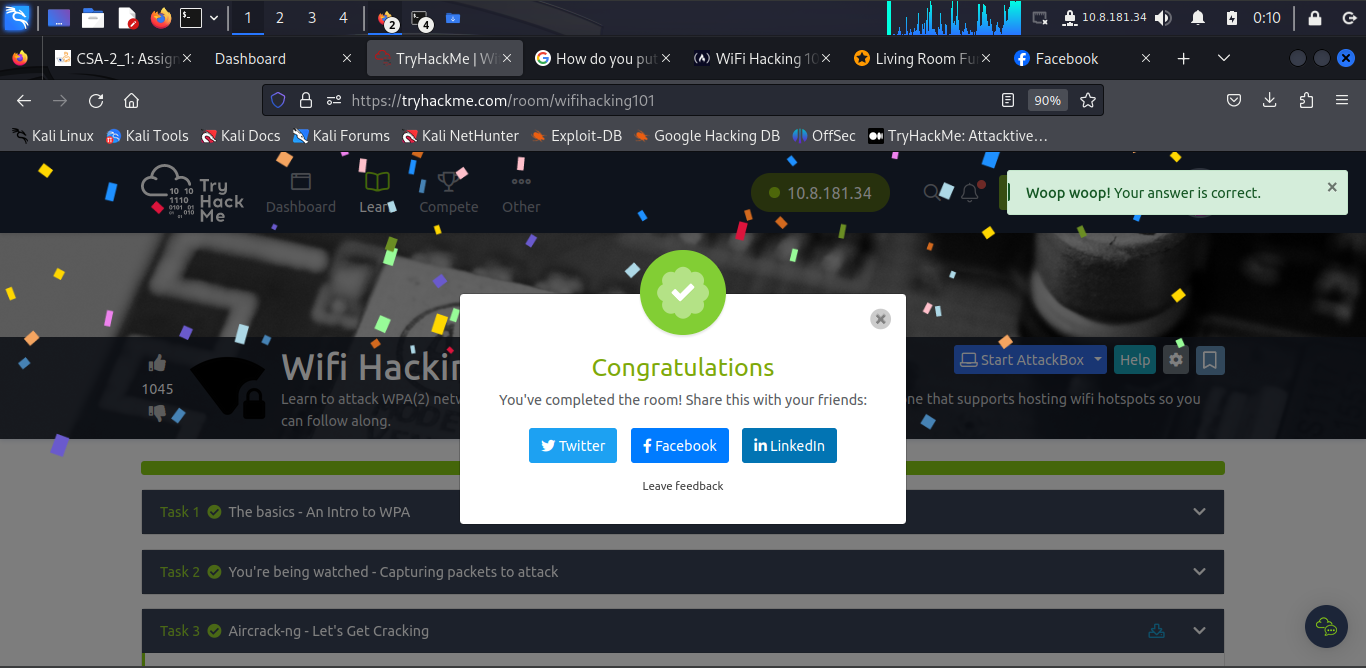


We create a HCCAPX in order to use hashcat to crack the password is **–j**

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>