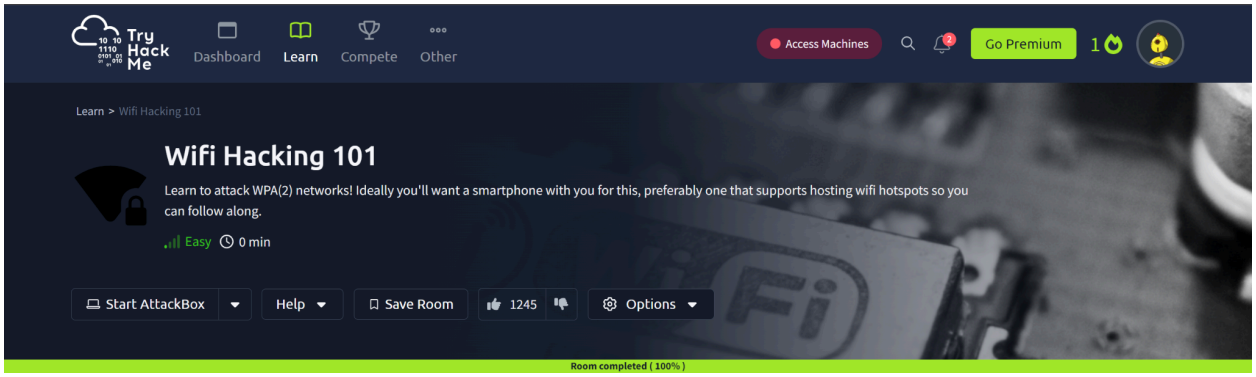
WIFI HACKING 101

ASSIGNMENT REPORT



Peter Kinyumu,
cs-sa07-24067,
July 2nd, 2024.

1. INTRODUCTION

This room teaches how to attack the Wireless Protected Access 2 network using the **Aircrack-ng** suite of tools, including **aircrack-ng airodump-ng** and **airmon-ng**.

2. ANSWERS TO QUESTIONS

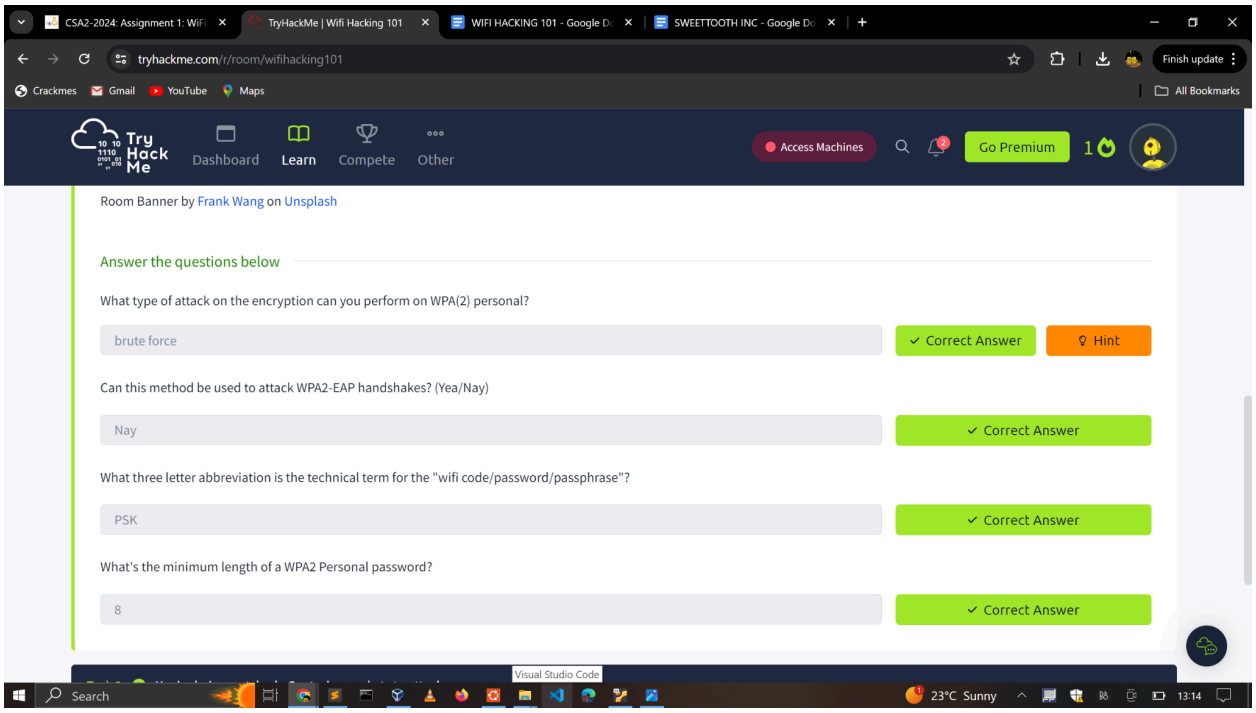
The Basics

a. **What type of attack on the encryption can you perform on WPA(2) personal?**
   - Bruteforce Attack -

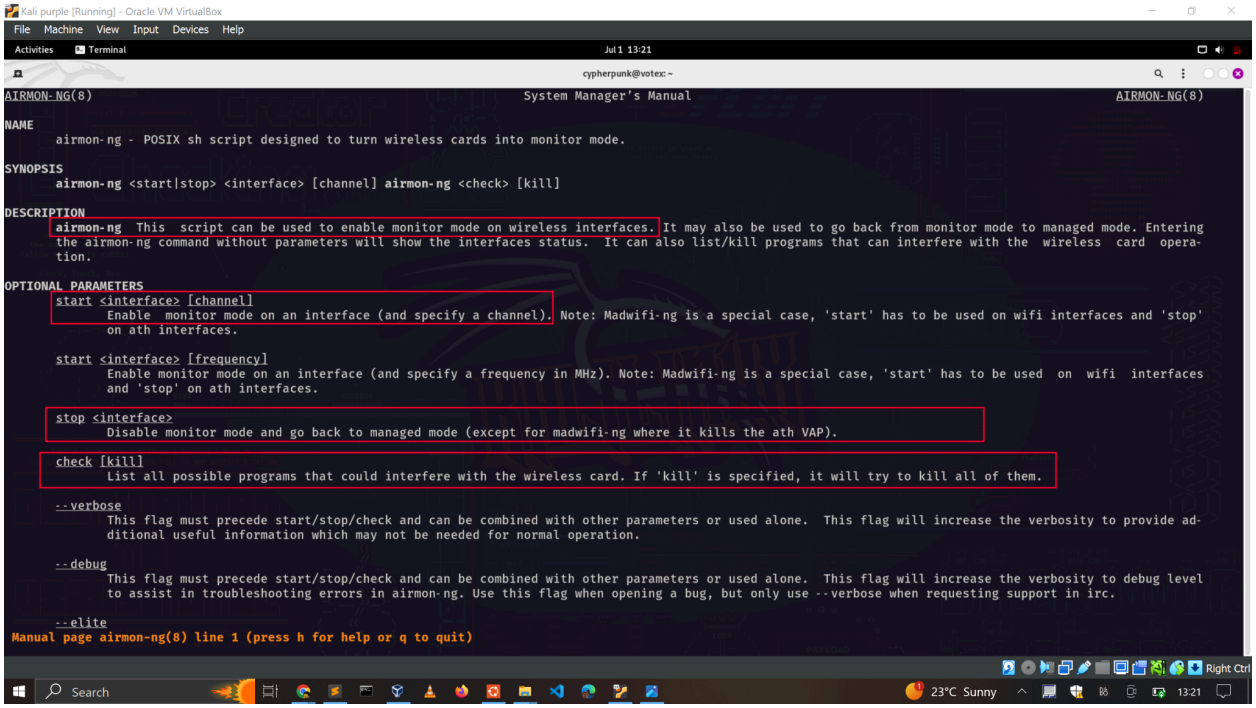
b. **Can this method be used to attack WPA2-EAP handshakes? (Yea/Nay)'**
   - Nay

c. **What three letter abbreviation is the technical term for the "wifi code/password/passphrase"?**
   - PSK - Pre Shared Key

d. **What's the minimum length of a WPA2 Personal password?**
   - 8 characters.



You're Being Watched

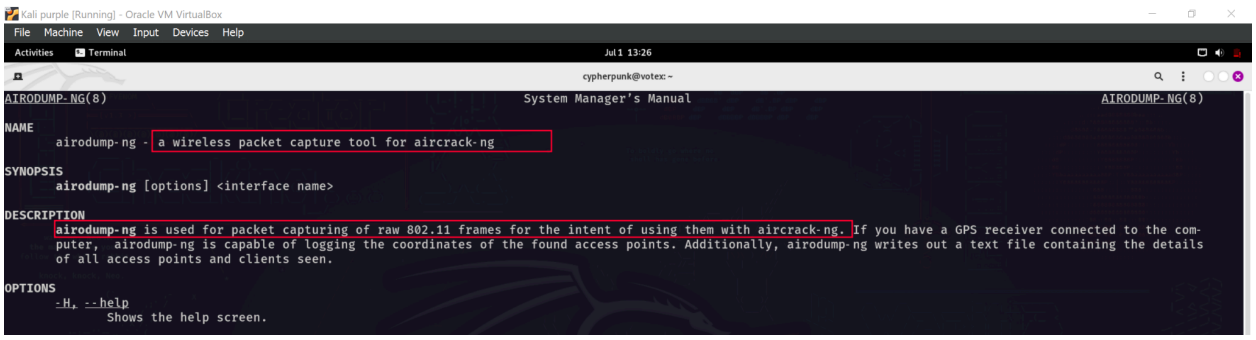


a. **How do you put the interface "wlan0" into monitor mode with Aircrack tools? (Full command)**
   - `airmon-ng start wlan0`

b. **What is the new interface name likely to be after you enable monitor mode?**
   - `wlan0mon` - The interface will be renamed to wlan0mon.

c. **What do you do if other processes are currently trying to use that network adapter?**
   - If there are existing conflicting processes using the network adapter, you kill them using `sudo airmon-ng check kill`

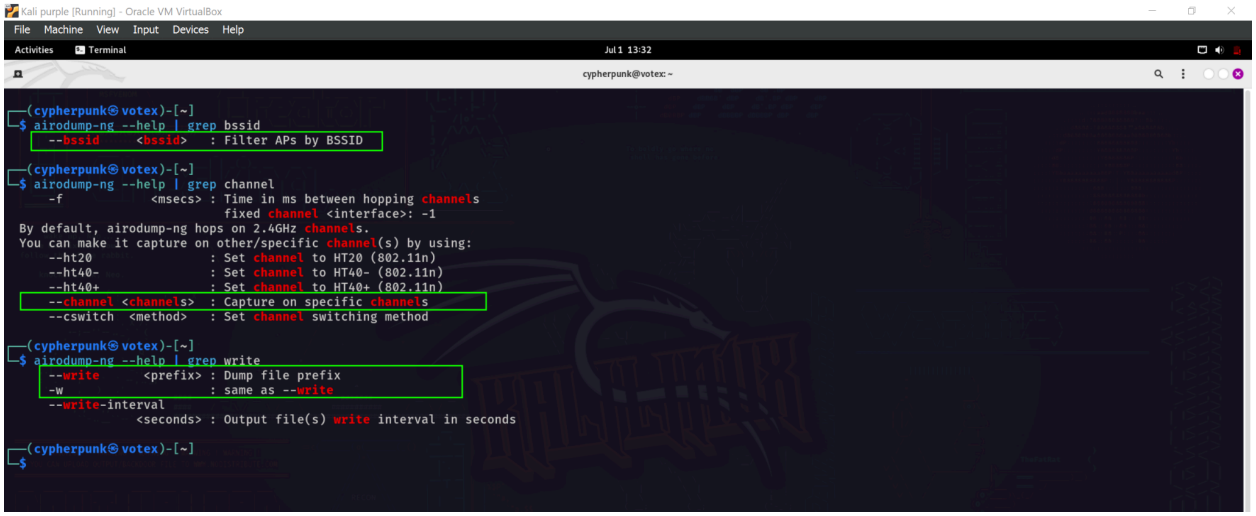
d. **What tool from the aircrack-ng suite is used to create a capture?**
   - `airodump-ng`



e. **What flag do you use to set the BSSID to monitor?**
   - `--bssid`

f. **And to set the channel?**
   - `--channel` captures on a specific channel

g. **And how do you tell it to capture packets to a file?**
   - `-w` writes to a file

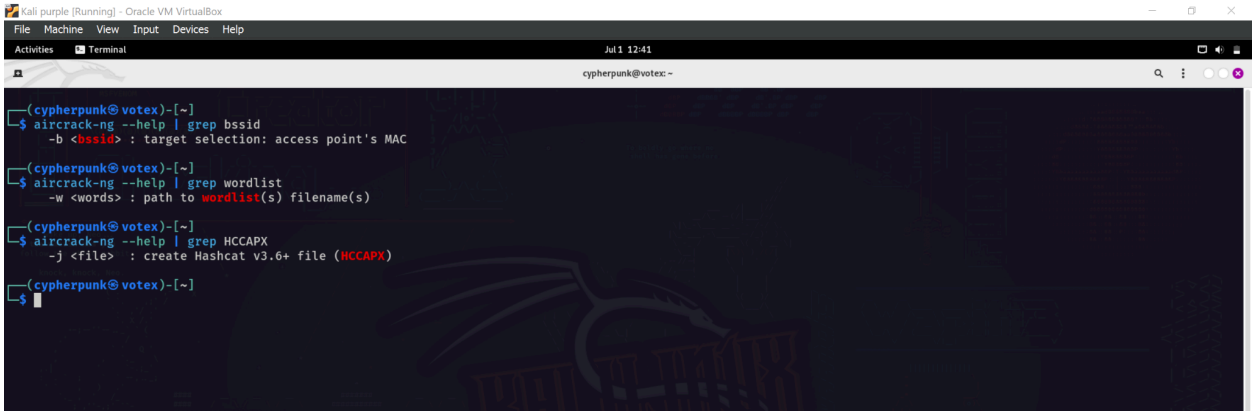


Aircrack-ng - Let's get cracking.

a. **What flag do we use to specify a BSSID to attack?**
   - `-b`

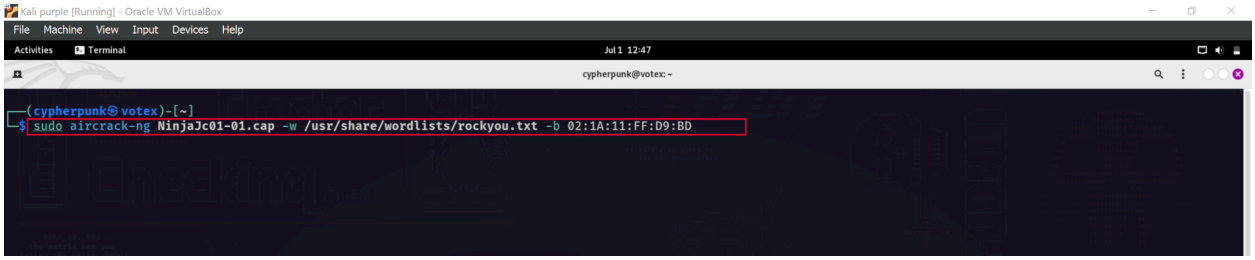
b. **What flag do we use to specify a wordlist?**
   - `-w`

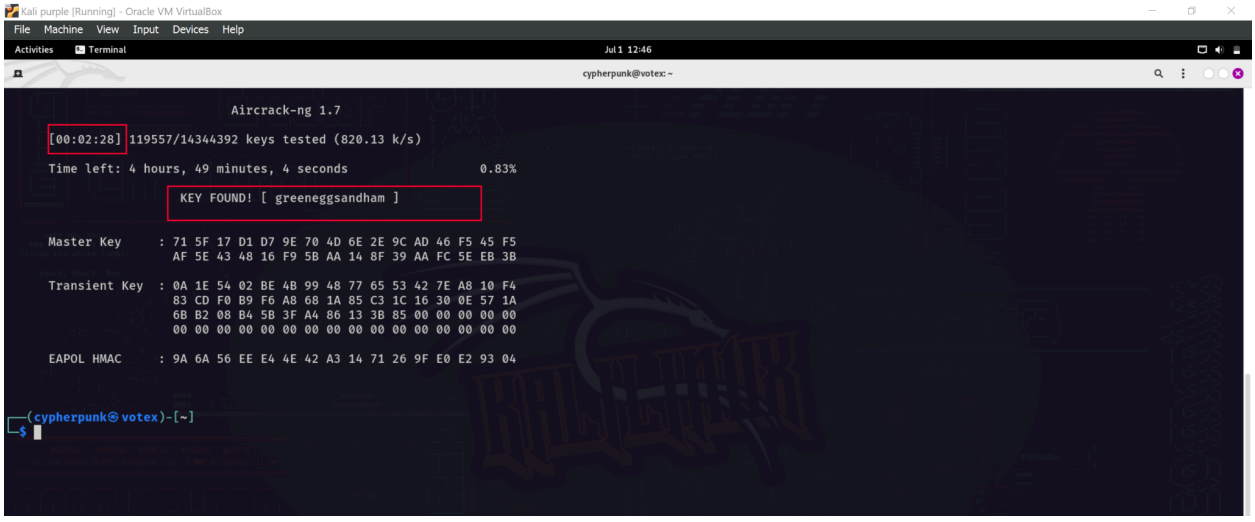
c. **How do we create a HCCAPX in order to use hashcat to crack the password?**
   - `-j`



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

- `greeneggsandham`



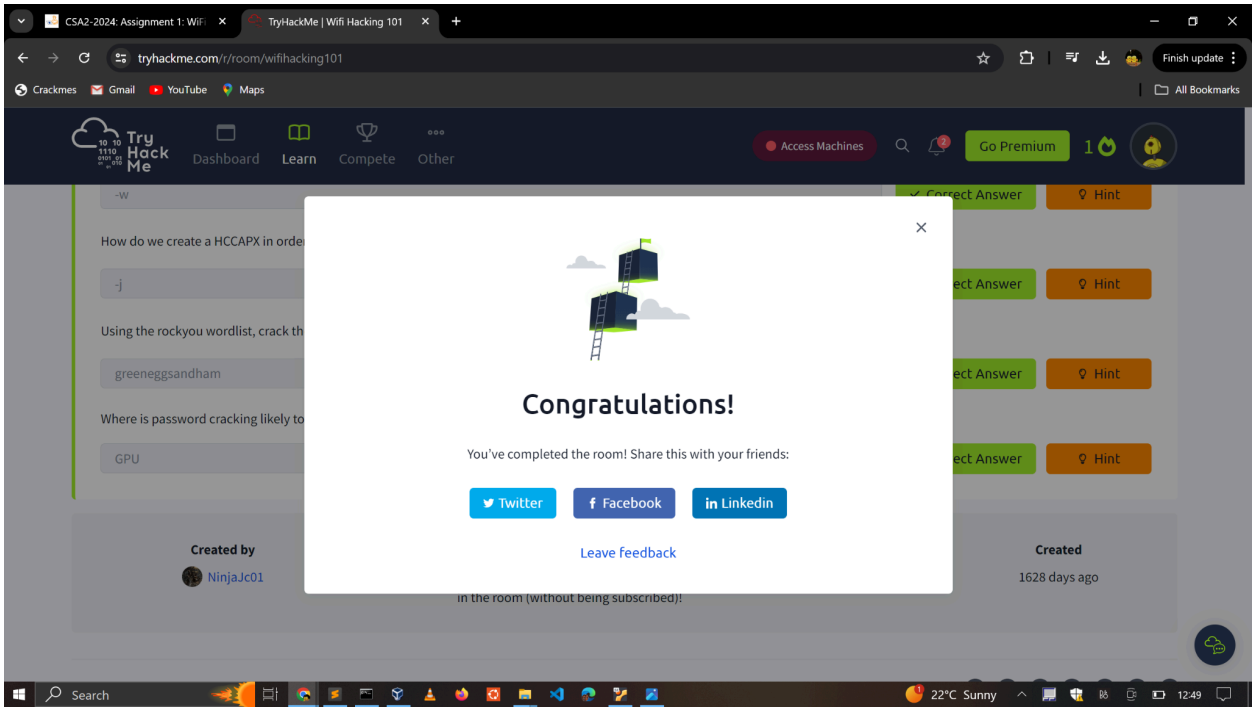


e. Where is password cracking likely to be fastest, CPU or GPU?

GPU

3. MODULE COMPLETION

https://tryhackme.com/p/c1ph3rbnuk



4. CONCLUSION

This assignment taught me how to monitor wireless network interfaces and identify access points using **airmon-ng**. Then, capture the authentication handshake packets with **airodump-ng** and finally how to crack the password with **aircrack-ng or hashcat**. It was so informative and the knowledge I have gained on wireless security will help me as a security analyst to perform wireless network assessment and protect wireless networks.