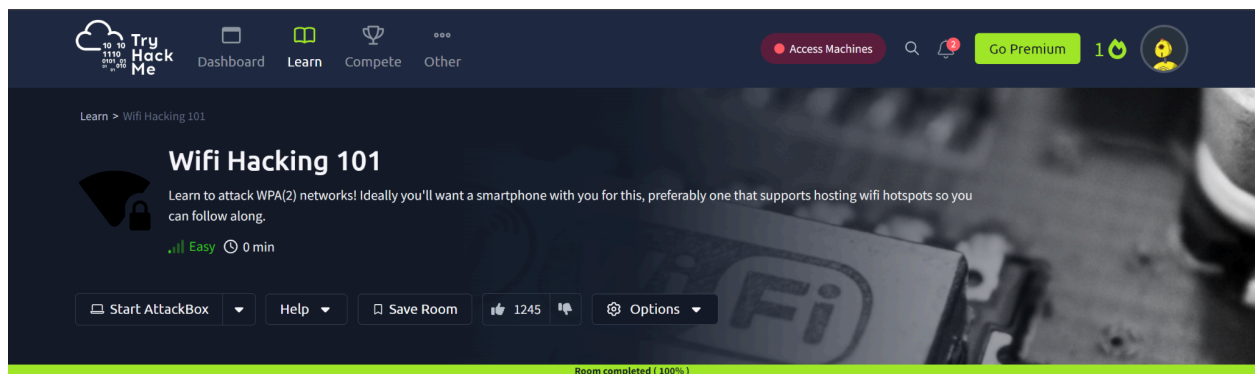


WIFI HACKING 101

ASSIGNMENT REPORT



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

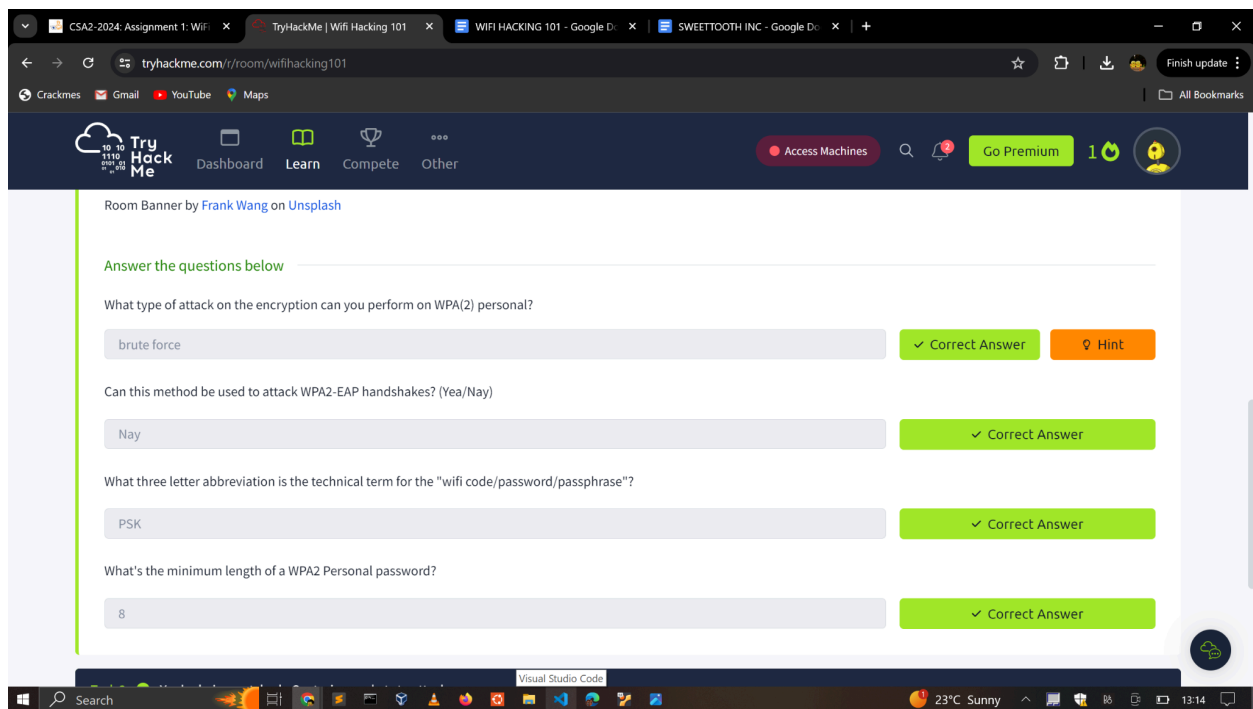
1. INTRODUCTION

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

- How do you put the interface “wlan0” into monitor mode with Aircrack tools? (Full command)
 - `airmon-ng start wlan0`
- What is the new interface name likely to be after you enable monitor mode?
 - `wlan0mon` - The interface will be renamed to wlan0mon.
- 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`
- 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

```
(cypherpunk@votex)-[~]
$ airodump-ng --help | grep bssid
--bssid <bssid> : Filter APs by BSSID

(cypherpunk@votex)-[~]
$ airodump-ng --help | grep channel
-f <msecs> : Time in ms between hopping channels
fixed channel <interface>: -i
By default, airodump-ng hops on 2.4GHz channels.
You can make it capture on other/specific channel(s) by using:
--ht20 : Set channel to HT20 (802.11n)
--ht40- : Set channel to HT40- (802.11n)
--ht40+ : Set channel to HT40+ (802.11n)
--channel <channels> : Capture on specific channels
--cswitch <method> : Set channel switching method

(cypherpunk@votex)-[~]
$ airodump-ng --help | grep write
--write <prefix> : Dump file prefix
-w : same as --write
--write-interval <seconds> : Output file(s) write interval in seconds

(cypherpunk@votex)-[~]
$
```

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**

```
Kali purple [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal
Jul 1 12:41
cypherpunk@votex: ~

(cypherpunk@votex)-[~]
$ aircrack-ng --help | grep bssid
-b <bssid> : target selection: access point's MAC

(cypherpunk@votex)-[~]
$ aircrack-ng --help | grep wordlist
-w <words> : path to wordlist(s) filename(s)

(cypherpunk@votex)-[~]
$ aircrack-ng --help | grep HCCAPX
-j <file> : create Hashcat v3.6+ file (HCCAPX)

(cypherpunk@votex)-[~]
$
```

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

- greeneggsandham

```
Kali purple [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal
Jul 1 12:47
cypherpunk@votex: ~

(cypherpunk@votex)-[~]
$ sudo aircrack-ng NinjaJc01-01.cap -w /usr/share/wordlists/rockyou.txt -b 02:1A:11:FF:D9:BD
```

```
Kali purple [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal
Jul 1 12:46
cypherpunk@votex: ~

Aircrack-ng 1.7
[00:02:28] 119557/14344392 keys tested (820.13 k/s)
Time left: 4 hours, 49 minutes, 4 seconds 0.83%
KEY FOUND! [ greeneggsandham ]

Master Key : 71 5F 17 D1 07 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 : 0A 1E 54 02 BE 4B 99 48 77 65 53 42 7E A8 10 F4
83 CD F0 B9 F6 A8 68 1A 85 C3 1C 16 30 0E 57 1A
6B B2 08 B4 5B 3F A4 86 13 3B 85 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

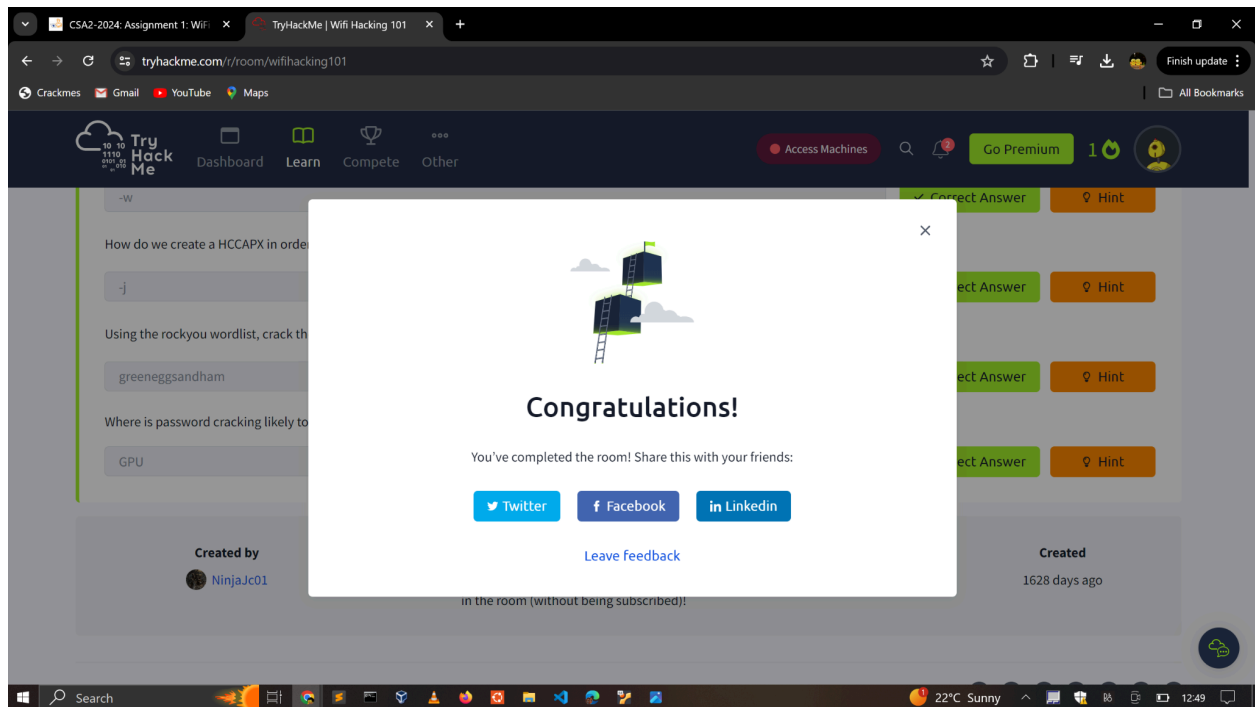
EAPOL HMAC : 9A 6A 56 EE E4 4E 42 A3 14 71 26 9F E0 E2 93 04

(cypherpunk@votex)-[~]
$
```

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.