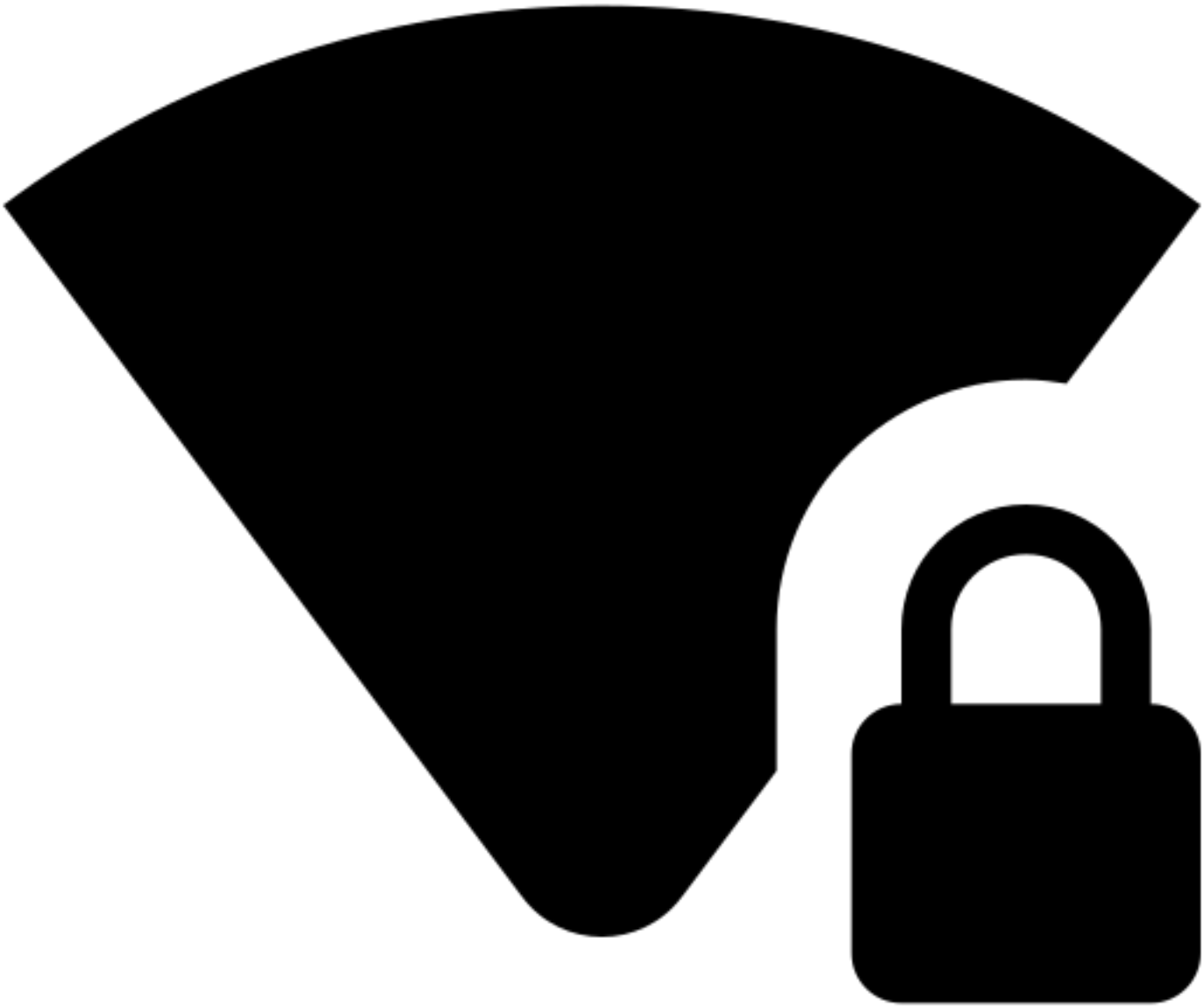
Wifi Hacking 101

Learn to attack WPA(2) networks! Ideally you'll want a smartphone with you for this, preferably one that supports hosting wifi hotspots so you can follow along.



[Task 1] The basics - An Intro to WPA

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.**

The core of WPA(2) authentication is the 4 way handshake.

Most home WiFi networks, and many others, use WPA(2) personal. If you have to log in with a password and it's not WEP, then it's WPA(2) personal. WPA2-EAP uses RADIUS servers to authenticate, so if you have to enter a username and password in order to connect then it's probably that.

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.

The 4 way handshake allows the client and the AP to both prove that they know they key, without telling each other. WPA and WPA2 use practically the same 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 somewhat similar to a salt in that it makes dictionary attacks more difficult. It means that for a given password, the key will still vary for each access point. This means that unless you precompute the dictionary for just that accesspoint, you will need to try passwords until you find the correct one.

Room Banner **by Frank Wang on Unsplash**

#1
What type of attack on the encryption can you perform on WPA(2) personal?

brute force

#2
Can this method be used to attack WPA2-EAP handshakes? (Yea/Nay)

nay

#3
What three letter abbreviation is the technical term for the "wifi code/password/-passphrase"?

psk

#4
What's the minimum length of a WPA2 Personal password?

8

[Task 2] You're being watched - Capturing packets to attack

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**
• **airserv-ng**

- **buddy-ng**
- **ivstools**
- **easside-ng**
- **tkiptun-ng**
- **wesside-ng**

We'll want to use aircrack-ng, airodump-ng and airmon-ng to attack WPA networks.
The aircrack tools come by default with Kali, or can be installed with a package manager or from https://www.aircrack-ng.org/

I suggest creating a hotspot on a phone/tablet, picking a weak password (From rockyou.txt) and following along with every stage. To generate 5 random passwords from rockyou, you can use this command on Kali: `head /usr/share/-wordlists/rockyou.txt -n 10000 | shuf -n 5 -`

You will need a monitor mode NIC in order to capture the 4 way handshake. Many wireless cards support this, but it's important to note that not all of them do.
Injection mode helps, as you can use it to deauth a client in order to force a reconnect which forces the handshake to occur again. Otherwise, you have to wait for a client to connect normally.

#1

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

airmon-ng start wlan0

#2

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

wlan0mon

#3

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

airmon-ng check kill

#4

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

airodump-ng

#5

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

--bssid

#6

And to set the channel?

--channel

#7

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

-w

[Task 3] Aircrack-ng - Let's Get Cracking

I will attach a capture for you to practice cracking on. If you are spending more than 3 mins cracking, something is likely wrong.
(A single core VM on my laptop took around 1min).
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'

#1
What flag do we use to specify a BSSID to attack?

-b

#2
What flag do we use to specify a wordlist?

-w

#3
How do we create a HCCAPX in order to use hashcat to crack the password?

-j

#4
Using the rockyou wordlist, crack the password in the attached capture. What's the password?

greeneggsandham

#5
Where is password cracking likely to be fastest, CPU or GPU?

gpu