Tests de pénétration sans fil

Tests de pénétration sans fil : Aircrack-ng

8 Juillet 2021 Par Raj

Dans notre série de tests d'intrusion sans fil, nous nous concentrons cette fois sur un outil qui existe depuis des lustres. C'est l'outil qui a donné naissance à de nombreuses attaques et outils sans fil. Aircrack-ng n'est pas un outil mais c'est une suite d'outils qui effectuent tous différents types d'attaques ou d'activités liées aux points d'accès sans fil. Dans cette démonstration, nous nous concentrerons sur quelques-uns des outils de l'arsenal Aircrack-ng.

Table des matières

Introduction

Aircrack-ng est un ensemble d'outils d'évaluation de la sécurité du réseau Wi-Fi. Il dispose d'un détecteur, d'un renifleur de paquets, de WPA/WPA2-PSK, ainsi que d'un cracker et analyseur WEP pour les réseaux locaux sans fil 802.11. Avec l'aide d'Aircrack-ng, un testeur d'intrusion peut se concentrer sur les aspects de surveillance, d'attaque, de test et de piratage de la sécurité Wi-Fi. La surveillance comprend la capture par Packer et l'exportation

des données vers des fichiers texte pour traitement par tout outil tiers. Les attaques incluent les attaques par rejeu, la désauthentification, les attaques de jumeaux maléfiques et les attaques par injection de paquets. Les tests incluent le test des cartes Wi-Fi et des capacités des pilotes en fonction de la capture et des injections. Enfin, Cracking inclut la possibilité de cracker les clés WEP et WPA PSK.

Aircrack-ng est pris en charge sur Linux, FreeBSD, macOS, OpenBSD, Android et Windows.

Il existe de nombreux outils dans la suite Aircrack-ng. Dans cette démonstration, nous nous concentrerons sur les éléments suivants :

airmon-ng : Il est utilisé pour activer le mode moniteur sur la carte Wi-Fi

airodump-ng : Il est utilisé pour détecter les paquets. Il place le trafic aérien dans un fichier pcap et affiche des informations sur le réseau

aireplay-ng : il est utilisé pour les attaques par injection de paquets

aircrack-ng : Il est utilisé pour déchiffrer les clés WEP à l'aide des attaques Fluhrer, Mantin et Shamir (FMS), des attaques PTW et des attaques par dictionnaire, et WPA/WPA2-PSK à l'aide d'attaques par dictionnaire.

Remarque : Pour effectuer des attaques à l'aide d'Aircrack-ng, vous avez besoin d'une carte Wi-Fi externe avec mode de surveillance.

Activation du mode moniteur

En termes généraux, le mode moniteur est un mode pris en charge par certains appareils Wi-Fi. Lorsqu'elle est activée, la carte Wi-Fi cessera d'envoyer des données et sera entièrement dédiée à la surveillance du trafic sans fil. Ce n'est pas le seul mode pris en charge sur les appareils Wi-Fi, il existe un total de 6 modes. Cependant, dans cette démonstration, nous nous concentrerons uniquement sur le mode Moniteur.

As discussed in the Introduction, airmon-ng is used for enabling the Monitor mode on Wi-Fi cards. After connecting the external card with our machine, we will use airmon-ng to start monitor mode by providing the interface. In our case the interface in question is wlan0. If you seem to have issues with enabling the monitor mode, kill the processes that are mentioned with their respective PIDs to ensure that no processes conflict. If not, this will put our Wi-Fi card in Monitor mode.

```
1.  airmon-ng start wlan0
```

```
┌──(root💀kali)-[~]
└─# airmon-ng start wlan0

Found 2 processes that could cause trouble.
Kill them using 'airmon-ng check kill' before putting
the card in monitor mode, they will interfere by changing channels
and sometimes putting the interface back in managed mode

    PID Name
    548 NetworkManager
   1537 wpa_supplicant

PHY     Interface       Driver          Chipset

phy3    wlan0           rt2800usb       Ralink Technology, Corp. RT5370
                (mac80211 monitor mode vif enabled for [phy3]wlan0 on [phy3]wlan0mon)
                (mac80211 station mode vif disabled for [phy3]wlan0)
```

After using the airmon-ng, we can check the enabling of monitor mode by using the iwconfig command. It is a Linux command that can be used to configure a wireless network interface. It is similar to ifconfig which is used for general interface configurations. After running iwconfig we can see that the interface that we used with airmon-ng has now changed from wlan0 to wlan0mon. Here mon indicates the monitor mode.

```
1. iwconfig
```

```
┌──(root💀kali)-[~]
└─# iwconfig
lo        no wireless extensions.

eth0      no wireless extensions.

docker0   no wireless extensions.

eth1      no wireless extensions.

wlan0mon  IEEE 802.11  Mode:Monitor  Frequency:2.457 GHz  Tx-Power=20 dBm
          Retry short  long limit:2   RTS thr:off   Fragment thr:off
          Power Management:off
```

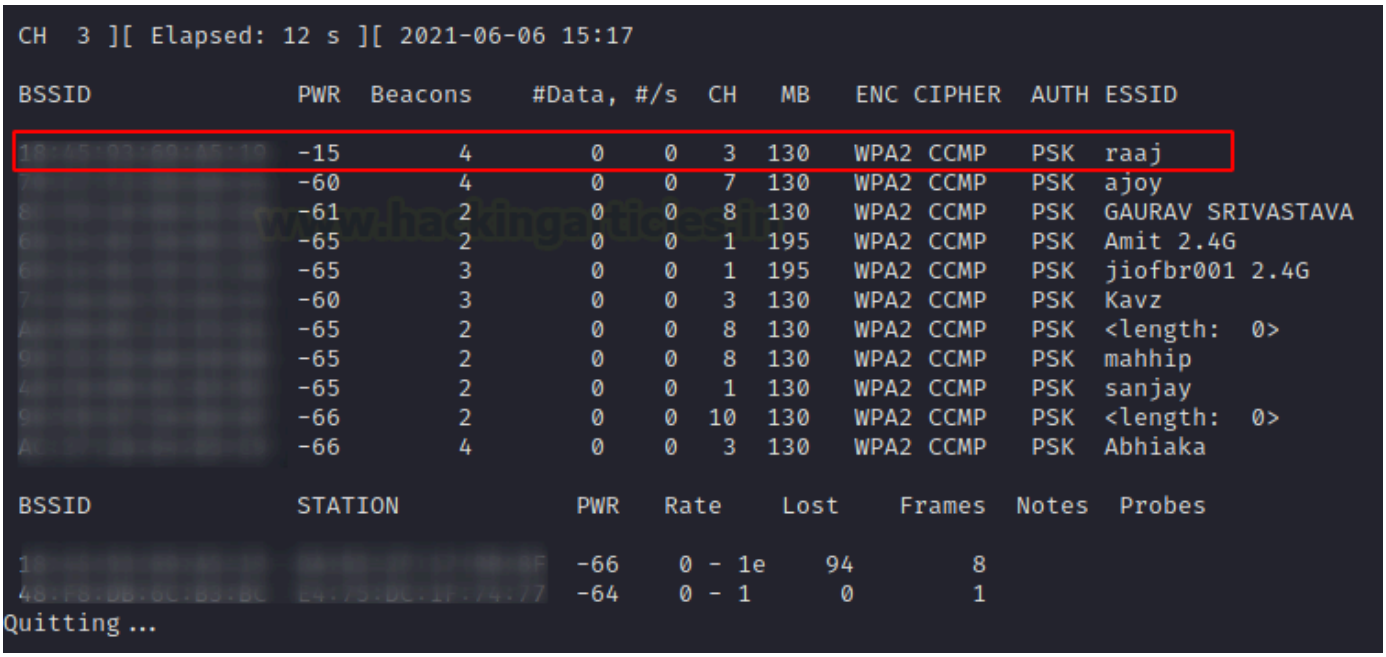
Sniffing Wireless Packets

After placing the Wi-Fi card in the Monitor mode, we can then move to sniff network packets. As discussed in the Introduction, airodump-ng can be used for this activity. To start sniffing, we need to provide the airodump-ng with the ESSID of the access point with other details. To get the information required run airodump-ng with the interface only as demonstrated below.

```
1. airodump-ng wlan0mon
```

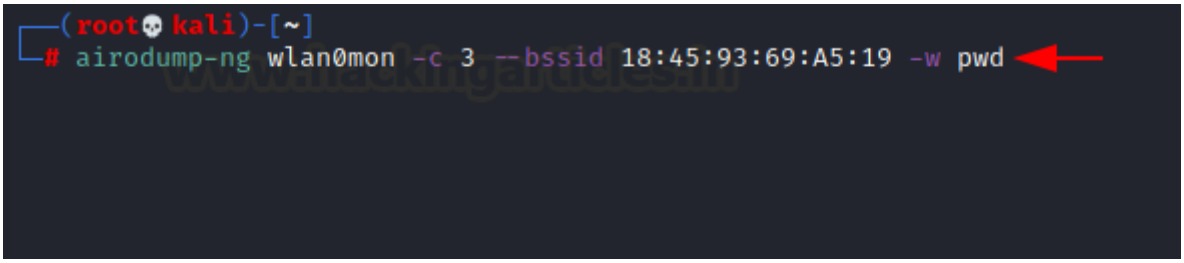
```
┌──(root💀kali)-[~]
└─# airodump-ng wlan0mon
```

As soon as we start the airodump-ng, we will see the list of Access Points with details such as their BSSID (MAC Address), Strength (PWR), Encryption (WPA/WPA2), Authentication Method, and ESSID (Name of Wireless Access Point) as demonstrated below. We will be targeting the wireless Access Point by the name of “raaj”. We can see that the access point is broadcasting on channel 3 and has WPA2-PSK.



Now that we have the ESSID of the access point that we want to target, we can initiate the sniffing on that particular device. We will need to provide the interface that we have monitor mode on and the details such as the channel of the device, BSSID as demonstrated below. This will begin the network capture.

```
1. airodump-ng wlan0mon -c 3 --bssid 18:X:X:X:X:X -w pwd
```

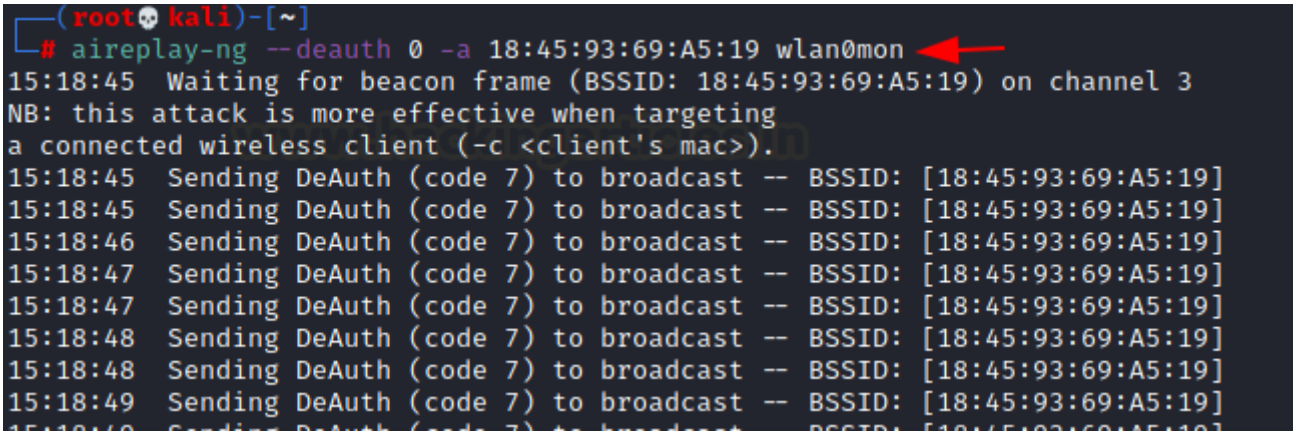


Deauthencating Users

Since we want to crack the password for the targeted access point, we need the handshake that can be attacked. We will be using the airodump-ng for capturing that handshake. But since all the devices are already connected to the access point hence, there won’t be any authentication performed or we can say that we won’t be able to capture the handshake. So, we will be sending a deauthentication signal to all the devices so that they will be disconnected from the access point. Then they will try to reconnect and at that moment we will capture the handshake. We will be using the aireplay-ng for sending the deauthentication signal. We need to provide the BSSID of the access point to deauthenticate

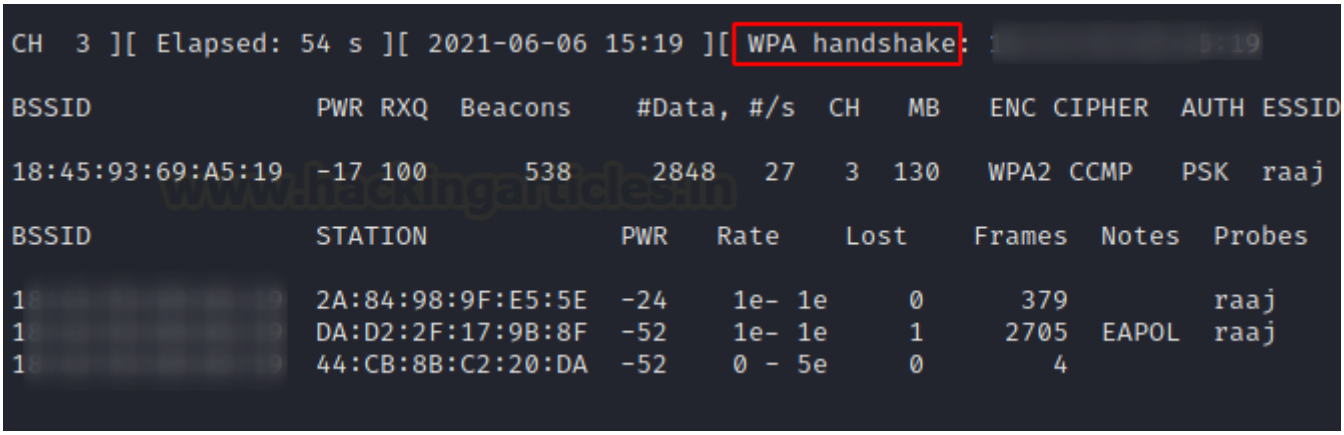
all devices as demonstrated below. Make sure to use a new terminal while running the aireplay and let the airodump-ng running. So that it can capture the handshake.

```
1.  aireplay-ng --deauth 0 -a 18:X:X:X:X:X wlan0mon
```



Capturing Handshake

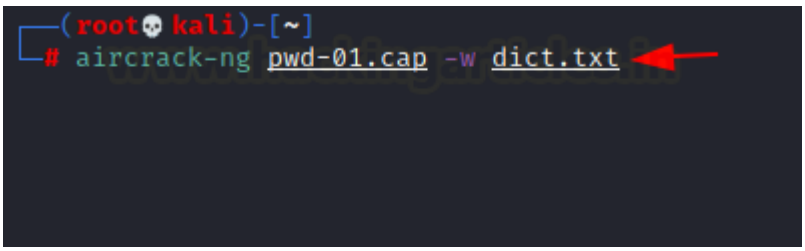
We go back to the terminal where we started the airodump-ng and we can see all the devices that attempted to reconnect to our targeted access point and on the top right-hand side, we can see that airodump-ng was able to capture the WPA handshake between the access point and one of its users.



Cracking Password

While running the airodump-ng we mentioned the pwd as the file in which the handshake should be saved. While checking we see that it has been captured into the file named pwd-01.cap. We can now perform a Bruteforce to crack the password using the aircrack-ng. We need to provide a dictionary for the attack that contains the probable passwords.

```
1.  aircrack-ng pwd-01.cap -w dict.txt
```



The time that aircrack-ng takes depends on your system configurations and the number of entries in the dictionary file that you provided. The dictionary that we provided had 7 keys. Hence, we were able to crack it in a matter of seconds. We can see the Master and Transient Key that would be used while forming the PSK-PTK combination. The password for the access point was cracked to be raj12345.

Conclusion

The collection of tools in the Aircrack-ng suite is useful in testing the Wireless Access Point Security. With the help of just 4 tools, we were able to crack the password required to connect the targeted Access Point. Aircrack-ng is one of the oldest tools that is used in the domain but we were still able to crack the authentication of a device today.

Author: Pavandeep Singh is a Technical Writer, Researcher, and Penetration Tester. Can be Contacted on **Twitter** and **LinkedIn**

PREVIOUS POST
Metasploit for Pentester: Sessions

NEXT POST
Wireless Penetration Testing: Bettercap

Leave a Reply

Your email address will not be published. Required fields are marked *

Comment * *

Name

Email

Website

Enregistrez mon nom, mon adresse e-mail et mon site Web dans ce navigateur pour la prochaine fois que je commenterai.

Prévenez-moi des nouveaux articles par email.

Poster un commentaire

Recherche ... Recherche

Abonnez-Vous Au Blog Par E-Mail

Entrez votre adresse e-mail pour vous abonner à ce blog et recevoir des notifications de nouveaux articles par e-mail.

Adresse e-mail

S'abonner

Catégories

Choisir une catégorie