Curso de Hacking ético Master. D

Ejercicio 12

REDES WIRELESS

Alumno: Julián Gordon

Índice

Introducción

En este trabajo, aprenderemos cómo funcionan las redes Wireless, como podemos configurar nuestra interfaz de red, y con eso, observar todo el tráfico que transita a través de dicha red. El objetivo será conseguir el HandShake, para luego intentar crackearlo de manera offline y poder así obtener la contraseña de la red Wireless. Identificar y documentar aspectos clave de estas redes, incluyendo el canal de operación, el ESSID (nombre de la red) y el BSSID (identificador único del punto de acceso) ,serán el foco de nuestro trabajo.

Para este trabajo utilizaremos la máquina de nuestro laboratorio llamada WifiChallenge, que cuenta con una interfaz de red que nos permite ponerla en modo monitor.

Localizar redes Wireless

En Linux, utilizamos 2 comandos que nos dirán las interfaces de redes en nuestro sistema. El comando ‘ifconfig’, mostrará información detallada sobre las interfaces de red , incluidas sus direcciones IP, máscaras de red, direcciónes MAC, estadísticas de tráfico, etc. Por otro lado, el comando ‘iwconfig’ , se utiliza para para configurar y mostrar información sobre interfaces de red inalámbricas. A continuación veremos 2 imágenes que nos muestran los resultados de estos 2 comandos, ejecutados en nuestra máquina llamada WifiChallenge de nuestro laboratorio.

```
root@WiFiChallengeLab:/home/vagrant# ifconfig
br-befd52fe3513: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.18.0.1  netmask 255.255.0.0  broadcast 172.18.255.255
        ether           5:9d  txqueuelen 0  (Ethernet)
        RX packets 251391  bytes 29803810 (29.8 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 290202  bytes 34505610 (34.5 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

docker0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        inet 172.17.0.1  netmask 255.255.0.0  broadcast 172.17.255.255
        ether                 f  txqueuelen 0  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.13  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::a00:27ff:fe8e:a077  prefixlen 64  scopeid 0x20<link>
        ether                 '  txqueuelen 1000  (Ethernet)
        RX packets 1400  bytes 1884961 (1.8 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 646  bytes 51851 (51.8 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 542682  bytes 60303642 (60.3 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 542682  bytes 60303642 (60.3 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

veth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.200.1.1  netmask 255.255.255.0  broadcast 0.0.0.0
        ether                 txqueuelen 1000  (Ethernet)
        RX packets 26  bytes 1924 (1.9 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 54  bytes 4976 (4.9 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

veth2: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.200.2.1  netmask 255.255.255.0  broadcast 0.0.0.0
        ether                 txqueuelen 1000  (Ethernet)
        RX packets 1625  bytes 109218 (109.2 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 94  bytes 6480 (6.4 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

veth2aef015: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        ether 0a:68:c9:a7:e7:75  txqueuelen 0  (Ethernet)
        RX packets 251391  bytes 33323284 (33.3 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 290198  bytes 34505191 (34.5 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

wlan60: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        unspec 02-00-00-00-3C-00-00-00-00-00-00-00-00-00-00-00  txqueuelen 1000  (UNSPEC)
        RX packets 50826  bytes 33029967 (33.0 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

wlan0mon: flags=867<UP,BROADCAST,NOTRAILERS,RUNNING,PROMISC,ALLMULTI>  mtu 1500
        unspec 02-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00  txqueuelen 1000  (UNSPEC)
        RX packets 396572  bytes 403837809 (403.8 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

```
root@WiFiChallengeLab:/home/vagrant# iwconfig
wlan3     IEEE 802.11  ESSID:off/any
          Mode:Managed  Access Point: Not-Associated   Tx-Power=20 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:on

veth2aef015  no wireless extensions.

wlan0mon  IEEE 802.11  Mode:Monitor  Frequency:2.422 GHz  Tx-Power=20 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Power Management:on

wlan6     IEEE 802.11  ESSID:off/any
          Mode:Managed  Access Point: Not-Associated   Tx-Power=20 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:on

wlan60    IEEE 802.11  Mode:Monitor  Frequency:5.785 GHz  Tx-Power=13 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Power Management:on

hwsim0    no wireless extensions.

wlan2     IEEE 802.11  ESSID:off/any
          Mode:Managed  Access Point: Not-Associated   Tx-Power=20 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:on

docker0   no wireless extensions.

wlan5     IEEE 802.11  ESSID:off/any
          Mode:Managed  Access Point: Not-Associated   Tx-Power=20 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:on

eth0      no wireless extensions.

lo        no wireless extensions.

veth2     no wireless extensions.

wlan1     IEEE 802.11  ESSID:off/any
          Mode:Managed  Access Point: Not-Associated   Tx-Power=20 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:on

br-befd52fe3513  no wireless extensions.

wlan4     IEEE 802.11  ESSID:off/any
          Mode:Managed  Access Point: Not-Associated   Tx-Power=20 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:on

veth1     no wireless extensions.
```

Uso de Suite Airoplay-ng

Una vez que ya tenemos listadas todas las interfaces de red disponibles, para poder analizar las redes wireless que estan activas a nuestro alcance, lo que debemos hacer primero, es poner una tarjeta de red en modo monitor. Lo haremos utilizando la suite de airoplay-ng, que tiene como función la de auditoría de redes wireless. El comando ‘airmon-ng start wlan0’ , hará que la interfaz de red wlan0 , se quede en modo monitor y nos permitirá comenzar a esnifar el tráfico de balizas que hay. Para ver el listado usamos el comando ‘airodump-ng wlan0mon’. Los más importantes, son los puntos que tengan clientes (Station), navegando, ya que son el modo por el que podremos robar el handshake. A continuación mostraremos una imagen de este proceso, con el listado de redes wireless disponibles, y luego lo explicaremos detalladamente.

```
BSSID              PWR  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH ESSID
CH  7 ][ Elapsed: 1 min ][ 2024-02-09 10:20

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

F0:                -28       42       28    0   6   54        CCMP   PSK  wifi-mobile
F0:                -28       42       38    0   6   54   OPN             wifi-guest
FA:                -28       41        0    0   6   54   WPA2 CCMP   PSK  MiFibra-5-D6G3
F6:                -28       41        0    0   6   54        CCMP   PSK  WIFI-JUAN
F0:                -28       45       17    0  11   54e       TKIP   SAE  wifi-IT
F0:                -28       44        0    0  11   54   OPN             <length:  9>
F0:                -28       45        0    0  11   54e       TKIP   SAE  wifi-management
9E:                -28       43        0    0   9   54        TKIP   PSK  vodafone7123
9E:                -28       90        0    0   3   54        CCMP   PSK  MOVISTAR_JYG2
F0:                -28      624    15043  209   1   54   WEP  WEP         wifi-old

BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

(not associated)   6                    2  -29    0 - 1       9         3
(not associated)   6                    0  -29    0 - 1       0         6         AP_router,wifi-corp
(not associated)   6                    1  -29    0 - 1       0         4         wifi-corp
(not associated)   6                    1  -29    0 - 1       0         8         open-wifi,home-WiFi,WiFi-Restaurant
(not associated)   6                    3  -49    0 - 1      46        32         wifi-corp-legacy
(not associated)   B                    5  -49    0 - 1      18        45         wifi-offices,Jason
(not associated)   7                    6  -49    0 - 1      51        39         wifi-offices,Jason
F0:                                       -29   54 -54       3        28
F0:                                       -29   36 -12       0        10
F0:                                       -29   11 -54       0        10
F0:                                       -29   54 -54       3        19
F0:                                       -29    5e- 9e      0        15
F0:                                       -29    1 - 2       0     14997
```

En la imagen anterior, podemos ver la información disponible de nuestro objetivo. **BSSID** significa "Basic Service Set Identifier", es una dirección única que identifica de manera exclusiva un punto de acceso (AP) en una red inalámbrica. Es la dirección MAC del enrutador inalámbrico o del punto de acceso WiFi. **ESSID** significa "Extended Service Set Identifier", es un identificador único que se utiliza para nombrar una red inalámbrica (el nombre de la red WiFi a la que nos conectamos). Cada red inalámbrica tiene su propio ESSID, que es transmitido por el enrutador inalámbrico y puede ser detectado por dispositivos cercanos, que estén buscando redes WiFi disponibles. Nuestro objetivo está en el canal 6 y tiene el ESSID ‘wifi-mobile’. Ahora filtraremos la búsqueda de redes a nuestro objetivo, para ello utilizamos este comando:

‘airodump-ng wlan0mon --channel 6 --bssid F0:9F:C2:71:22:12’

En la siguiente imagen observamos este proceso, en el cual solo vemos nuestro objetivo

```
CH  6 ][ Elapsed: 4 mins ][ 2024-02-09 11:04

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

F0                  28   0     2337     1014    1   6   54        CCMP   PSK  wifi-mobile

BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

F0                                    -29   54 - 1      0       29         wifi-mobile
F0                                    -29   54 -54      0      976         wifi-mobile
```

Conclusiones

Con la realización de este ejercicio, aprendimos a usar la suite airoplay-ng, que es un conjunto de herramientas para la auditoría de redes wireless. Llevamos a cabo un análisis de redes inalámbricas, utilizando la interfaz de red en modo monitor. Durante el proceso, se identificaron las redes cercanas, destacando aspectos clave como el canal, el ESSID y el BSSID de la red objetivo. A través de las capturas de pantallas proporcionadas, se mostraron las redes identificadas, asegurándonos de ocultar las direcciones MAC para preservar la privacidad y la seguridad de los dispositivos.