ANÁLISIS DE HERRAMIENTAS DE PENETRACIÓN DE REDES WIFI EN RASPBERRY PI

Gonzalo Figueroa del Val

Curso 2022-2023

Universidad Europea

17-11-2023

AGENDA

Introducción

Objetivos

Background teórico

Airgeddon y entorno

Ataques

Conclusiones

Universidad Europea

INTRODUCCIÓN

- Redes inalámbricas presentes en el día a día y en cualquier lugar
- Exposición continua de redes
- Herramientas de ataque de fácil acceso y sobre todo de fáciles de usar
- La información expuesta puede ser muy valiosa para los atacantes
- 1 de cada 4 redes públicas no son seguras (Kapersky)
- Caso DarkHotel: spyware en redes WiFi públicas en hoteles (2007-2014)

OBJETIVOS

- Obtención de una herramienta de penetración de redes inalámbricas completa

Objetivos secundarios:

- Despliegue de un entorno de pruebas adecuado
- Realización de ataques contra redes WiFi en un entorno controlado
- Análisis de los resultados obtenidos durante el caso práctico

BACKGROUND TEÓRICO

Protocolos de Seguridad y Herramientas

Universidad Europea

PROTOCOLOS DE SEGURIDAD

WEP (1999)

- Cifrado Rivest Cipher 4 (RC4)
- Clave compartida de 40 bits (104 en su última versión)
- Vector de Inicialización (IV) de 24 bits
- CRC-32 para garantizar integridad
- Handshake con número aleatorio

WPA (2003)

- Temporal Key Integrity Protocol (TKIP) que aporta confidencialidad e integridad
- WPA-PSK y WPA-Enterprise
- IV de 48 bits y cifrado RC4
- Handshake de 4 vías
- WiFi Protected Setup (WPS)

WPA2 (2004)

- Requerido a partir de 2006
- Cifrado de bloque CCMP basado en Advanced Encryption Standard (AES)
- Disponible TKIP para compatibilidad con WPA
- Handshake de 4 vías
- Mejoras en WPA2-Enterprise

WPA3 (2018)

- Requerido a partir de 2020
- Incompatibilidad de clientes
- WPA3-Transition Mode
- Handshake SAE (Simultaneous Authentication of Equals) - Management Frame Protection (MFP)

HERRAMIENTAS Y FRAMEWORKS

- Wireshark
- Suite Aircrack-ng (airmon-ng, aireplay-ng, airodump-ng…)
- Hashcat
- Bettercap
- Reaver
- Wifite2
- “The lazy script”
- Airgeddon

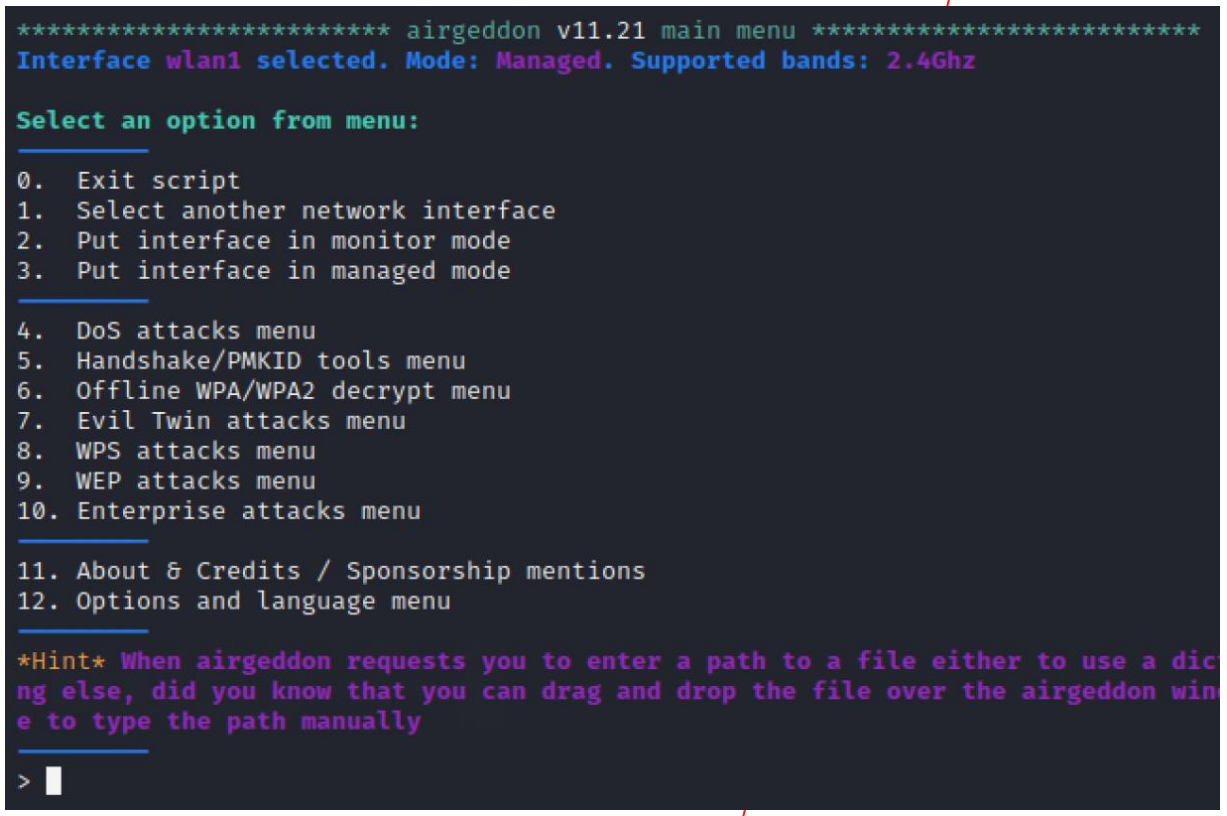
AIRGEDDON Y ENTORNO

Herramienta, Raspberry Pi, SO y Antena

Universidad Europea

AIRGEDDON

- Selección de interfaz de red y modo monitor
- Escaneo de redes
- Ataques DoS
- Captura PMKID y Handshake
- Descifrado de WPA/WPA2 offline
- Creación de diccionarios para fuerza bruta
- Evil Twin (solo AP, sniffer y portal cautivo)
- Ataques a WPS
- Ataque a WEP
- Evil Twin a WPA Enterprise



ENTORNO DE PRUEBAS

- Raspberry Pi 4 b
- Kali Linux 2023
- Atheros AR9271
- Router “Comtrend” AR5387un

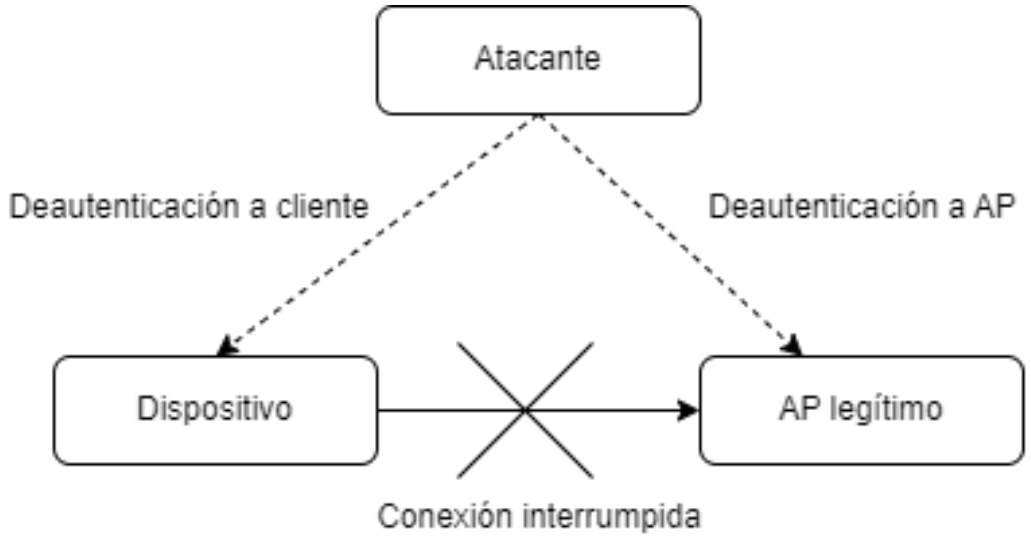
ATAQUES REALIZADOS

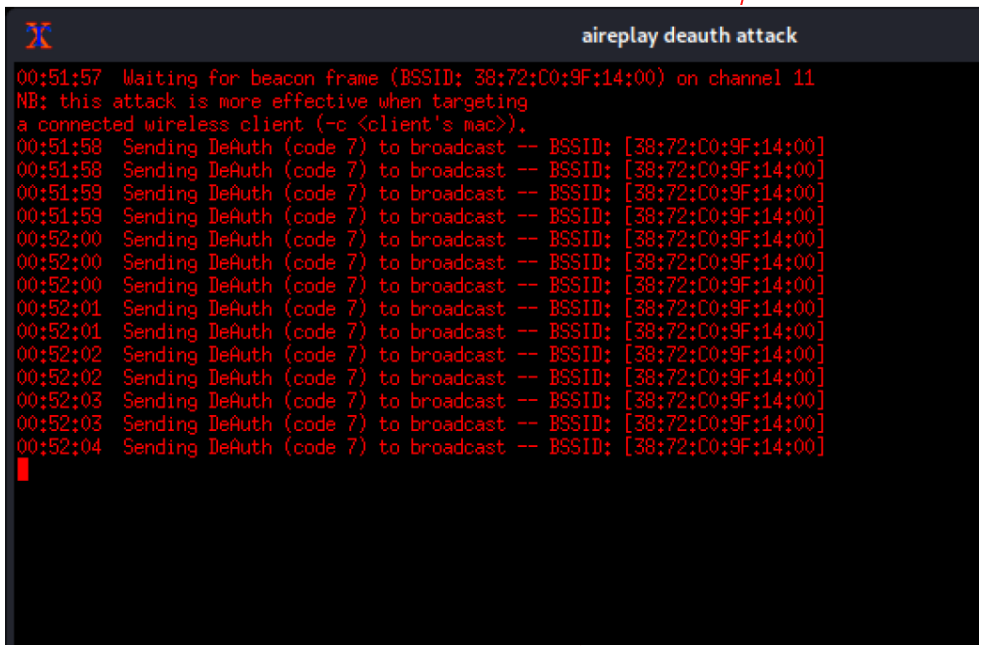
Deautenticación, WPA PSK Cracking, WPA PMKID, Evil Twin y WPS Attack

Universidad Europea

DEAUTENTICACIÓN

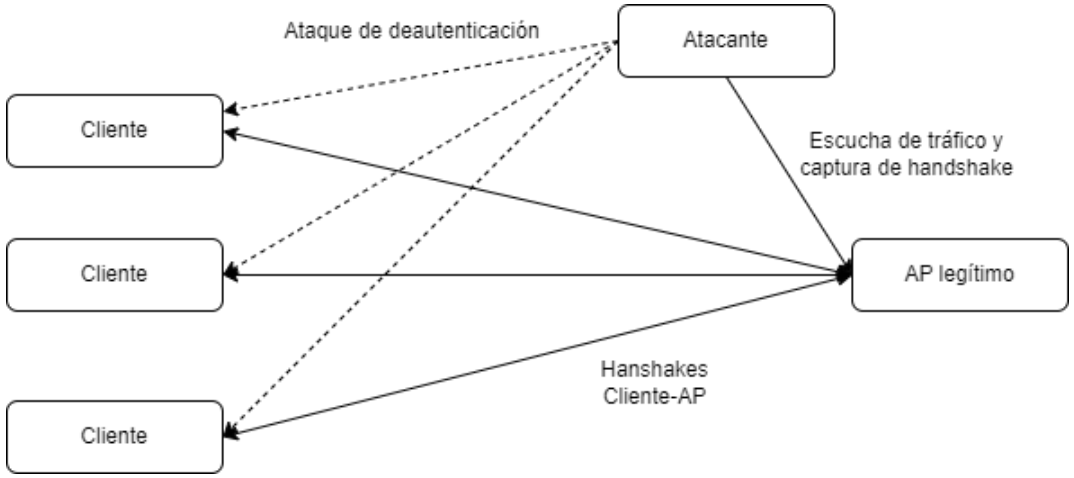
- Envío de paquetes de desconexión hacia clientes o hacia el punto de acceso
- Reconexión de clientes
- Denegación de servicio

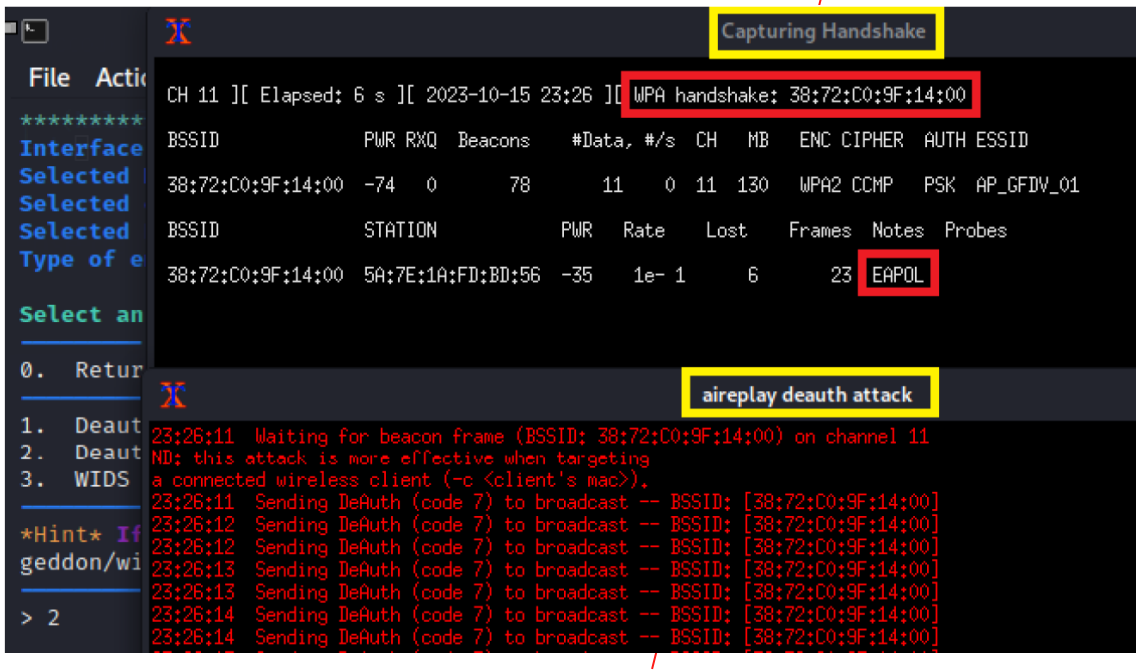




WPA PSK CRACKING

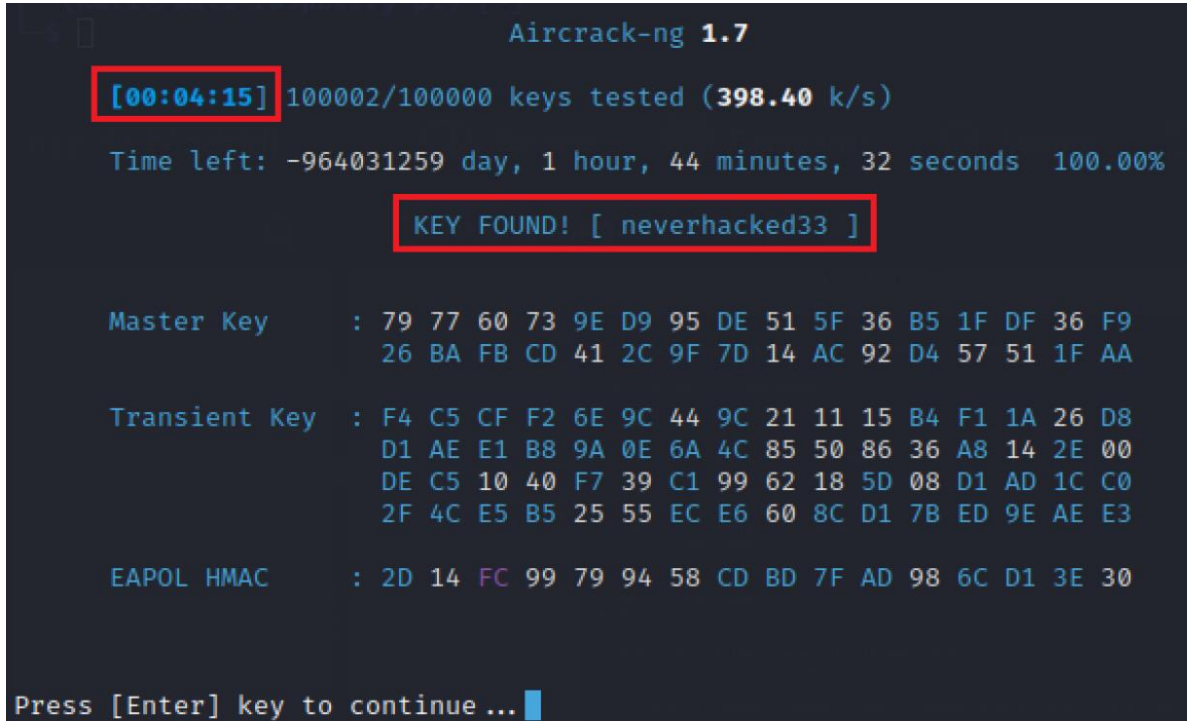
- Escaneo de redes
- Ataque de deautenticación
- Captura de handshake completo
- Fuerza bruta o diccionario (aircrack o hashcat)





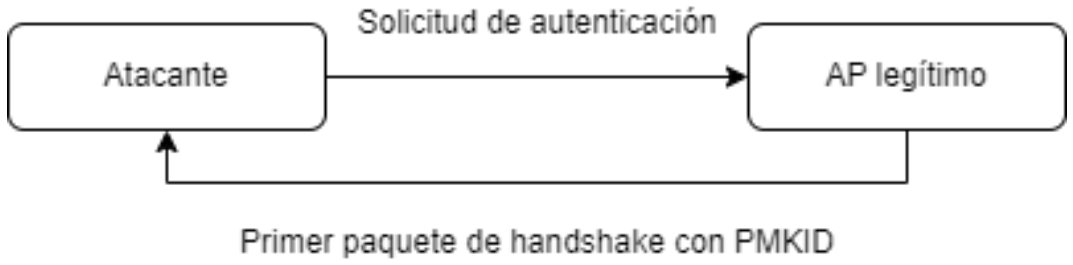
WPA PSK CRACKING

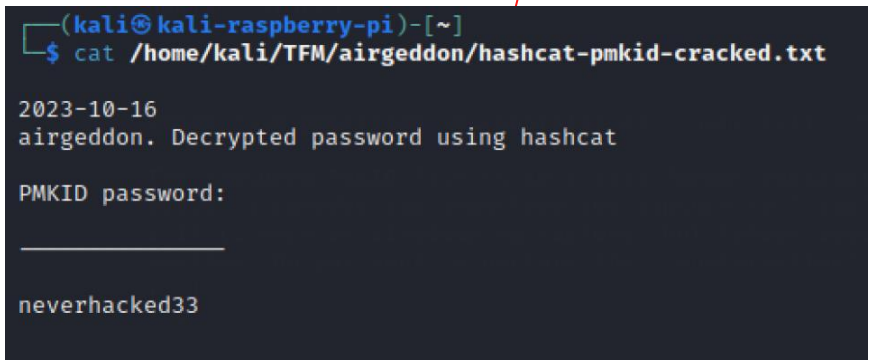
- Diccionario de 100.000 líneas construido a partir de rockyou.txt



WPA2 PMKID

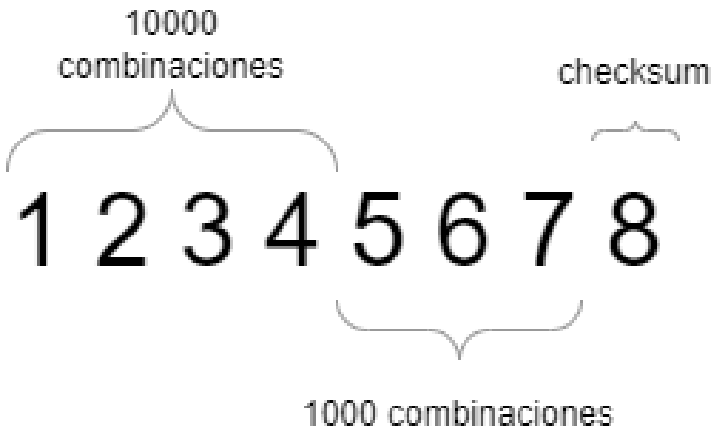
- Ataque más reciente contra WPA2 (2018)
- No es necesaria la interacción de un cliente ni de obtener un handshake completo
- Se captura únicamente el primer paquete del handshake
- Aircrack-ng o Hashcat para obtener la contraseña





WPS

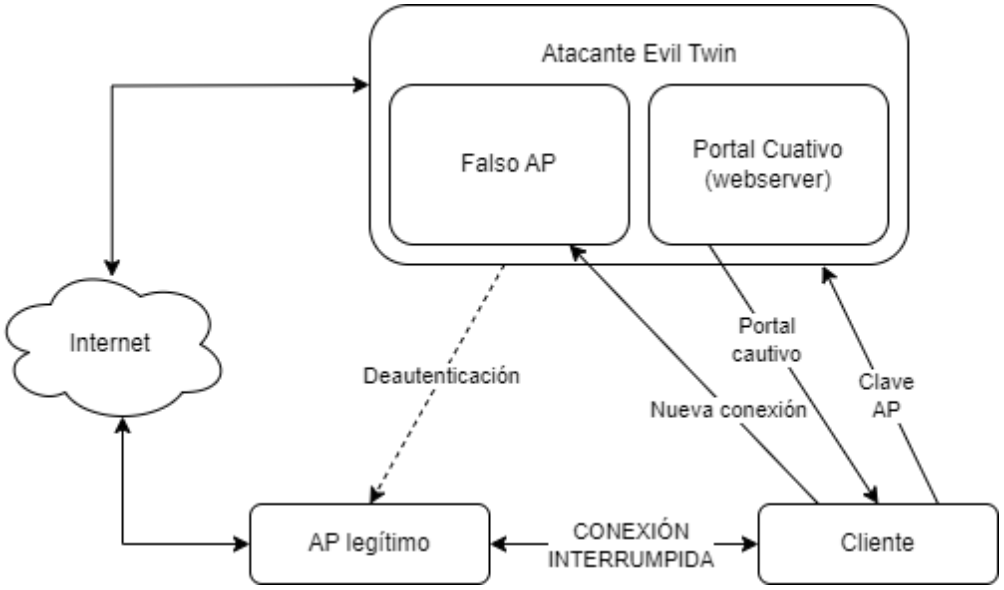
- PIN de 8 dígitos dividido en 2 partes y un checksum (dígito 8)
- Algoritmos de generación de PINs, bases de datos o fuerza bruta

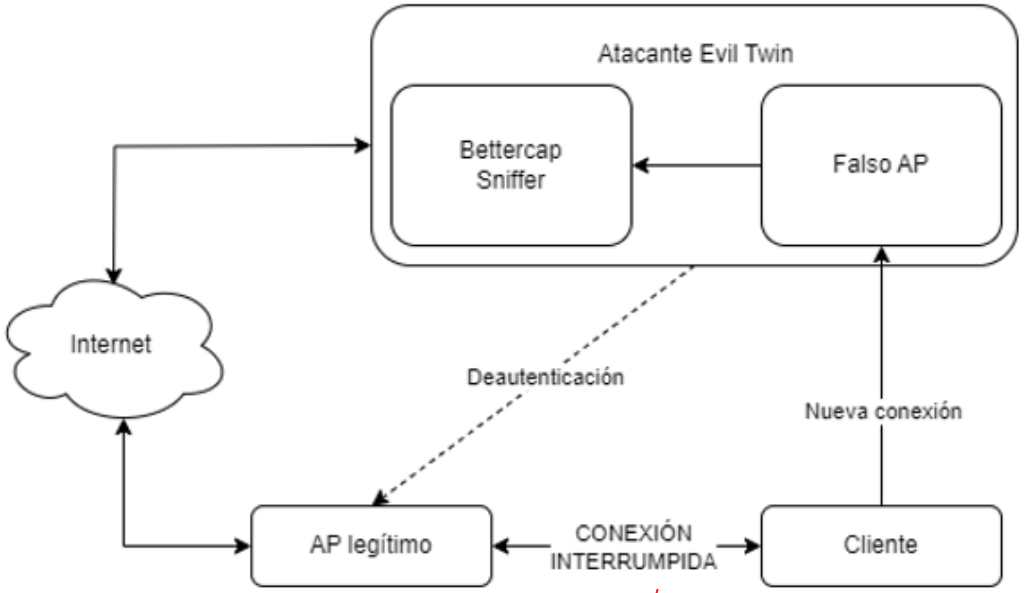



```
[-] Failed to recover WPA key

Testing PIN 18836486 (9/15)

Reaver v1.6.6 WiFi Protected Setup Attack Tool
Copyright (c) 2011, Tactical Network Solutions, Craig Heffner <cheffner@tacnetsol.com>

[+] Switching wlan1mon to channel 11
[+] Waiting for beacon from 38:72:C0:9F:14:00
[+] Received beacon from 38:72:C0:9F:14:00
[+] Vendor: Broadcom
WPS: A new PIN configured (timeout=0)
WPS: UUID - hexdump(len=16): [NULL]
WPS: PIN - hexdump_ascii(len=8):
     31 38 38 33 36 34 38 36                         18836486
WPS: Selected registrar information changed

[+] Pin cracked in 8 seconds
[+] WPS PIN: '18836486'
[+] WPA PSK: 'neverhacked33'
[+] AP SSID: 'AP_GFDV_01'

PIN cracked: 18836486
Password cracked: neverhacked33

The password was saved on file: /home/kali/TFM/airgeddon/wps_database_based.txt
```

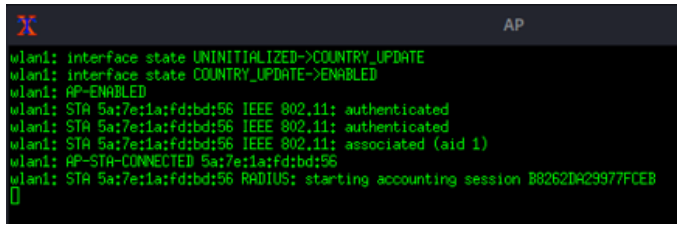
EVIL TWIN

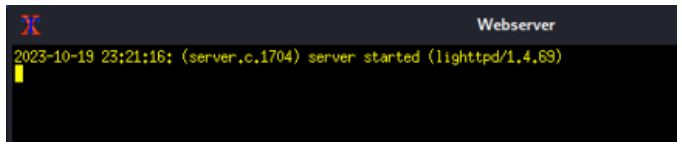
- Falsificación de un punto de acceso legítimo
- Simula tanto el BSSID como el ESSID
- Con portal cautivo o con sniffer de tráfico

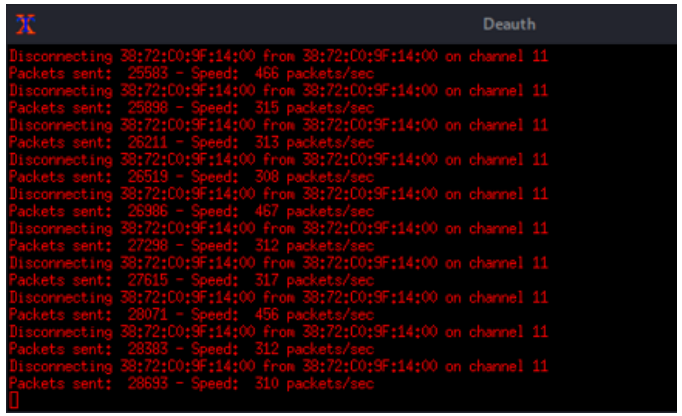


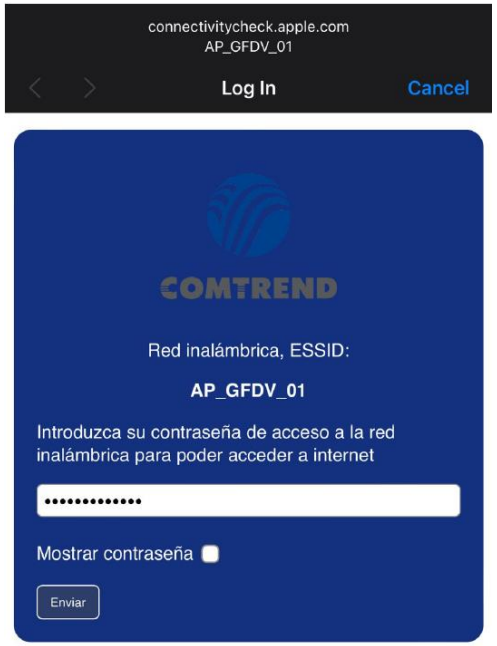


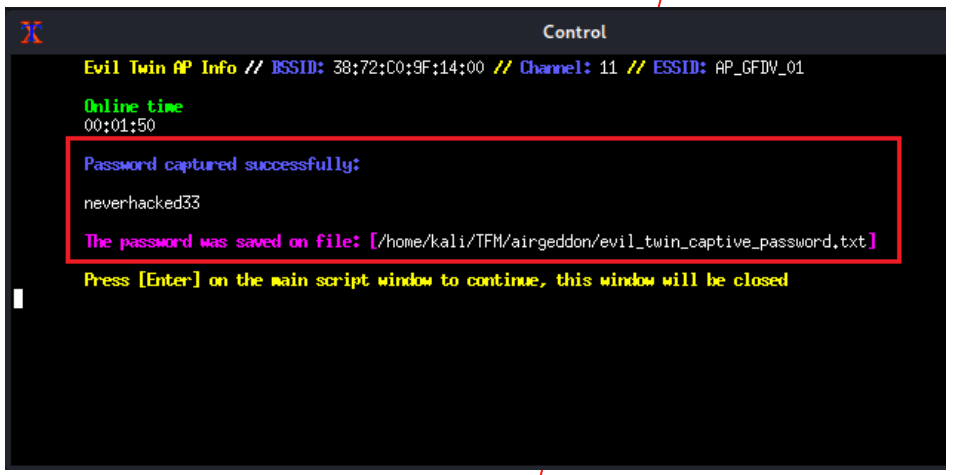
EVIL TWIN CON PORTAL CAUTIVO





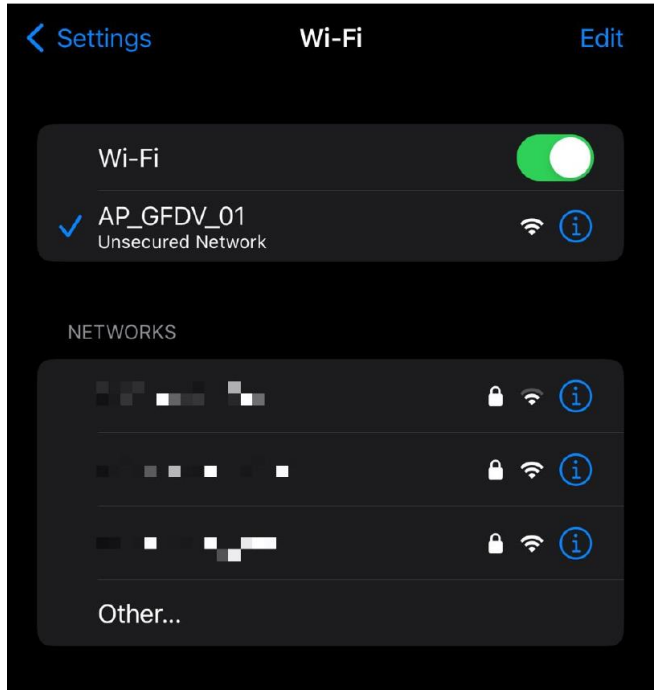


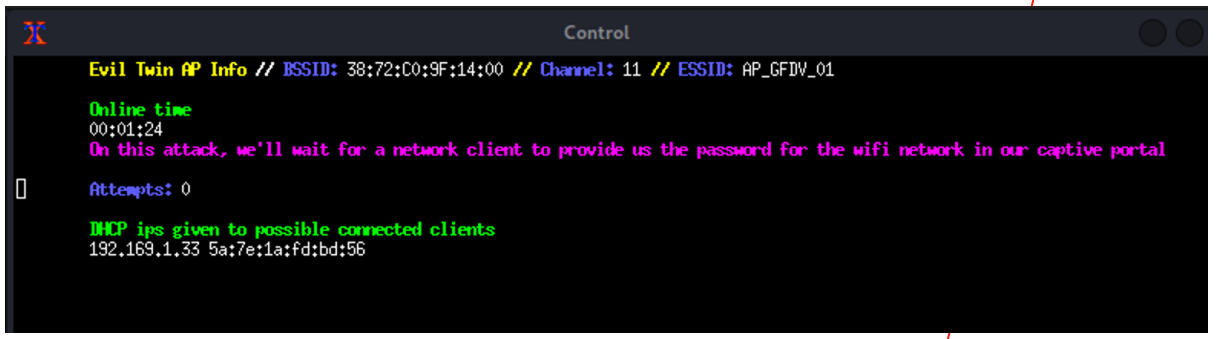




Universidad Europea

EVIL TWIN CON SNIFFER





CONCLUSIONES

Universidad Europea

CONCLUSIONES

- Realización de ataques más comunes con éxito
- Imposibilidad de realizar ataques a WEP y a WPA Enterprise
- Facilidad de acceso a herramientas que pueden ser utilizadas con fines maliciosos
- El humano es el eslabón más débil
- Importancia de aplicar buenas prácticas de seguridad:
  - Contraseñas robustas
  - Deshabilitar WPS
  - Evitar conexión a redes públicas
  - Uso de últimas actualizaciones de seguridad

Repositorio de GitHub: https://github.com/gonzalofdv/TFM_redesWifi