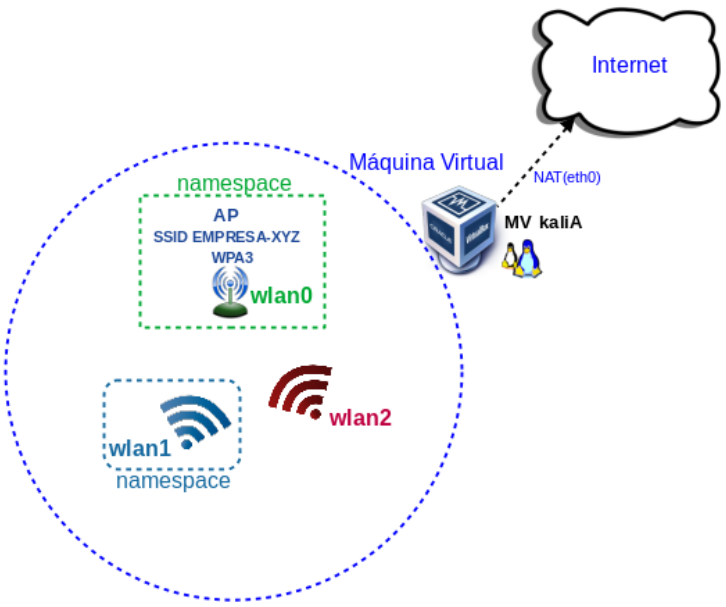
TALLER HE PRÁCTICA Auditar contrasinal Wi-Fi WPA3 (SAE)	
Apelidos	**Nome**

ESCENARIO: AP → SSID EMPRESA-XYZ → WPA3 (SAE)

MV kaliA
- RAM ≥ 2048MB
- CPU ≥ 2
- PAE/NX habilitado
- BIOS: Óptica
- ISO: Live Kali amd64
- Rede: NAT(eth0)
- Wordlist: rockyou
- **mac80211_hwsim**
  - radios=3 → wlan0, wlan1, wlan2
  - wlan0 → AP (hostapd, ip netns)
  - wlan1 → Cliente
  - wlan2 → unknown (tools suite: aircrack-ng →auditar handshake)
- **Namespaces**
  - phy0 → wlan0 → AP aillado
  - phy1 → wlan1 → cliente autenticado aillado



Material necesario	Práctica: Auditar contrasinal Wi-Fi WPA3 (SAE)
■ Host alumnado ■ Máquina virtual GNU/Linux Kali ■ [0] 3-Taller-HE-Practica-WIFI-1 ■ [1] Curvas elípticas e criptografía ■ [2] Matemáticas detrás das curvas elípticas e Bitcoin	(1) Prerrequisito: Realizar [0] (2) Host alumnado. Máquina virtual GNU/Linux Kali amd64: ■ Crear seguindo especificacións do escenario. ■ Arrancar ■ Configurar a rede según o escenario: NAT(eth0), AP(wlan0), cliente(wlan1), unknown(wlan2) ■ Montar AP simulado con WPA3-SAE e aillar ■ Conectar co cliente simulado e aillar ■ Investigar co cliente unknown(airodump-ng) →desconectar cliente simulado → capturar handshake SAE→comprobar fortaleza contrasinal → auditar handshake con aircrack-ng e ataque por diccionario (rockyou) → Método WPA3 non soportado →verificar protección contra KRACK

Protocolo	Método de autenticación	Seguridade	Ventaxes	Desvantaxes	Ataques típicos	Como protexerse contra os ataques	Nível seguridade
WPA2-PSK	Pre-Shared Key (clave común)	Cifrado AES, pero usa unha chave compartida	Fácil de configurar e usar	Menos seguro en redes grandes ou abertas, risco se a clave é débil	**Ataques de dicionario** (forza bruta usando claves débiles), **Ataques de captura de handshakes**	1. **Usa contrasinais longos e complexos** (máis de 16 caracteres, combinación de maiúsculas, minúsculas, números e caracteres especiais). 2. **Habilita o control de acceso á rede (filtrado MAC)**. 3. **Desactiva a reemitición do handshake** para dificultar a captura do handshake. 4. **Habilitar 802.11w (protección de tramas de xestión):** ieee80211w=2→tramas desautenticación/desasociación están cifradas e non poden ser manipuladas por un atacante. Require o uso de **WPA2** o **WPA3** con **AES** (non se admite **TKIP**).	↑
WPA2-EAP	Extensible Authentication Protocol (EAP)	Cifrado AES, require autenticación baseada en servidor (RADIUS)	Maior seguridade, pode usar certificados e outros métodos de autenticación	Require configuración de servidor (RADIUS), máis complexo	**Ataques Man-in-the-Middle** (se non hai cifrado TLS adecuado), **Ataques de diccionario contra credenciais**	1. **Usa TLS ou outros métodos EAP seguros** para a comunicación entre o cliente e o servidor. 2. **Implementa certificados para autenticación EAP** para evitar ataques de MITM. 3. **Utiliza contrasinais fortes e técnicas de autenticación multifactorial** para protexer as credenciais.	↑↑
WPA3-SAE	Simultaneous Authentication of Equals (SAE)	Cifrado AES, resistencia mellorada contra ataques de forza bruta	Máxima seguridade, mellora a protección contra ataques offline	Asegúrese de que todos os dispositivos son compatibles	**Ataques de dicionario offline** (reducidos significativamente, pero aínda posibles en certas condicións), **Ataques de downgrading** (forzar a conexión a WPA2)	1. **Activar protección contra downgrading** en routers (forzar WPA3 en vez de WPA2). 2. **Usa claves longas e únicas para cada dispositivo**. 3. **Reforza a seguridade da configuración de WPA3** nas túas redes e dispositivos para evitar vulnerabilidades de implementación.	↑↑↑

Conclusión:

- **WPA2-PSK**: Ten un nivel de seguridade básico, ideal para redes pequenas ou domésticas, pero pode mellorar se se seguen as boas prácticas.
- **WPA2-EAP**: Ten unha maior seguridade grazas á autenticación centralizada (RADIUS), pero require máis configuración.
- **WPA3-SAE**: O protocolo máis seguro, protexendo contra moitos tipos de ataques, pero require compatibilidade de dispositivos.

WPA3-SAE (Wi-Fi Protected Access 3 con Simultaneous Authentication of Equals)

É o estándar máis recente de seguridade para redes inalámbricas, que reemplaza a WPA2-PSK como método de autenticación baseado en contrasinal. A súa principal innovación é o protocolo **Simultaneous Authentication of Equals (SAE)**, tamén coñecido como **Dragonfly**, que resolve as vulnerabilidades dos handshakes WPA2 fronte a ataques de forza bruta offline.

WPA3-SAE está deseñado para entornos residenciais e de pequenas empresas onde se comparte un contrasinal común entre usuarios, pero cunha seguridade significativamente mellorada fronte a ataques de dicionario, replay e man-in-the-middle(MITM).

Diferenzas Clave respecto a WPA2-PSK

Característica	WPA2-PSK	WPA3-SAE
Derivación de Claves	PMK derivado de PSK (PBKDF2)	PMK derivado mediante SAE (Dragonfly)
Vulnerabilidade a Dicionario	✗ Handshake capturado é crackeable offline	✓ Handshake NON é crackeable (Forward Secrecy)
Protección contra Replay	✗ Vulnerable	✓ Protexido mediante commit/confirm
Forward Secrecy	✗ Non	✓ Si (claves únicas por sesión)
Cifrado Mínimo	CCMP (AES-128)	GCMP-256 (AES-256) recomendado
PMF (802.11w)	Opcional	**Obrigatorio**

Fluxo de Autenticación

O protocolo SAE utiliza un intercambio criptográfico baseado en **curvas elípticas (EC)** ou **grupos Diffie-Hellman** para establecer unha clave compartida sen revelar o contrasinal.

Fase 1: Commit (Intercambio de Compromisos)

1. **Cliente e AP xeneran valores aleatorios**:
    - Cada parte escolle un escalar aleatorio privado e calcula un elemento público da curva elíptica.
2. **Envío de Commit**:
    - Cliente → AP: Envía o seu elemento público + hash de confirmación.
    - AP → Cliente: Envía o seu elemento público + hash de confirmación.
3. **Propiedades de Seguridade**:
    - Os valores aleatorios **únicanse en cada sesión** (Forward Secrecy).
    - O contrasinal **nunca se transmite** nin se pode derivar dende o tráfico capturado.

Fase 2: Confirm (Verificación Mutua)

1. **Ambas partes calculan a PMK (Pairwise Master Key)**:
    - Usando o seu escalar privado e o elemento público recibido, calculan un **secreto compartido**.
    - Este secreto combínase co contrasinal (mediante HMAC) para derivar a **PMK**.
2. **Verificación mediante hashes**:
    - Cliente → AP: Envía un hash de confirmación (probando que coñece o contrasinal).
    - AP → Cliente: Envía o seu hash de confirmación.
3. **Resultado**:
    - Se ambos hashes coinciden, a autenticación ten éxito.
    - A PMK **xérase de forma única** para esta sesión.

Fase 3: 4-Way Handshake (Derivación de Claves de Sesión)

1. **Calcular PTK (Pairwise Transient Key)**:
    - A partir da PMK, o cliente e o AP calculan a PTK usando:
        - Nonces únicos (ANonce do AP, SNonce do cliente).
        - Direccións MAC de ambas partes.
2. **Establecer Cifrado**:
    - Cliente e AP usan AES-GCMP para cifrar o tráfico de datos.
    - **PMF (Protected Management Frames)** actívase automaticamente.

Resumo do Fluxo con Participantes

1. Cliente ↔ AP → Intercambio de Commit (elementos públicos da curva)
2. Cliente ↔ AP → Cálculo do secreto compartido (sen transmitir contrasinal)
3. Cliente ↔ AP → Verificación Confirm (hashes mutuos)
4. Cliente ↔ AP → Derivación da PMK (única para esta sesión)
5. Cliente ↔ AP → 4-Way Handshake (cálculo da PTK)
6. Cliente ↔ AP → Cifrado AES-GCMP activado + PMF obrigatorio

Vantaxes de Seguridade

1. **Forward Secrecy**: Cada sesión xera claves únicas. Capturar tráfico pasado non permite descifrado.
2. **Resistencia a Ataques de Dicionario Offline**: O handshake SAE **non contén información crackeable** sen interacción activa.
3. **Protección contra Man-in-the-Middle**: A verificación mutua mediante hashes impide suplantación.
4. **PMF Obrigatorio**: As tramas de xestión van cifradas, evitando desautenticacións maliciosas.
5. **Modo de Transición**: WPA3-SAE permite modo mixto WPA2/WPA3 para compatibilidade.

Limitacións e Consideracións

1. **Compatibilidade**: Require hardware e drivers actualizados (soporte EC ou Diffie-Hellman).
2. **Vulnerabilidades de Implementación**: Ataques como **Dragonblood** (CVE-2019-9494) demostraron debilidades en implementacións iniciais (xa parcheadas).
3. **Configuración Incorrecta**: O modo de transición WPA2/WPA3 pode permitir ataques de downgrade se non se desactiva WPA2.
4. **Rendimiento**: O cálculo de curvas elípticas pode ser lixeiramente máis lento que PBKDF2.

Conclusión

WPA3-SAE representa un avance fundamental na seguridade de redes inalámbricas baseadas en contrasinal, resolvendo as vulnerabilidades críticas de WPA2-PSK:

- **Elimina a posibilidade de crackear handshakes capturados**.
- **Garante Forward Secrecy** para protexer sesións pasadas.
- **Obriga a usar PMF** para evitar ataques de desautenticación.

É o **estándar recomendado** para redes domésticas e pequenas empresas a partir de 2020, aínda que a súa adopción completa require actualización de hardware e firmware en todos os dispositivos.

Nota para o Laboratorio: A implementación de WPA3-SAE en hostapd require versións ≥ 2.10 e soporte do kernel para curvas elípticas. Non todos os dispositivos mac80211_hwsim poden soportar SAE, polo que se recomenda verificar compatibilidade antes de despregar escenarios WPA3.

Procedemento:

(1) Host alumnado. Máquina virtual GNU/Linux Kali:

(a) Crear e arrancar unha máquina virtual no equipo do alumnado coas seguintes características (ver escenario):

i. RAM ≥ 2048MB
ii. CPU ≥ 2
iii. PAE/NX habilitado
iv. ISO: Kali Live amd64 [3]
v. Rede: 1 tarxeta en modo NAT *(as wlanX serán simuladas por mac80211_hwsim)*
vi. Nome: Practica-Kali-Auditar-WPA3

(b) Executar nunha consola (consola1):

```
$ setxkbmap es #Configurar teclado en español

$ ip addr show eth0 #Amosar información sobre a NIC eth0. Verificar que a configuración de rede para a NIC eth0 é a seguinte: IP=10.0.2.15, MS=255.255.255.0

$ ip route #Ver a táboa de rutas do sistema.Verificar que GW=10.0.2.2

$ cat /etc/resolv.conf #Ver o contido do ficheiro /etc/resolv.conf, o cal contén a configuración os servidores DNS a empregar para a resolución de nomes. Comprobar que as directivas nameserver coinciden cos DNS1 e DNS2 da aula taller.

$ sudo modprobe mac80211_hwsim radios=3 #Este comando permite crear radios simuladas para probas e desenvolvemento, o que pode ser útil nun ambiente de test ou investigación. Non require hardware físico e simula varias interfaces de rede Wi-Fi que funcionan dentro do sistema: wlan0, wlan1 e wlan2

$ ip addr show #Amosar información sobre as NIC existentes no sistema, é dicir, verificar a configuración de rede  para as NIC: lo, eth0, wlan0, wlan1, wlan2 e hwsim0
```

(c) Rol interfaces Wi-Fi:

Imos empregar:

i. wlan0 para AP WPA2 (PSK) (shell bash consola1)
ii. wlan1 para o cliente que se conecta a AP (shell bash consola2)
iii. wlan2 como un cliente que non sabe o contrasinal para conectarse ao AP (shell bash consola3).

(d) Configura wlan0 como AP e aillala do resto de interfaces: na consola1

`$ sudo su -` #Acceder á consola de root(administrador) a través dos permisos configurados co comando sudo (/etc/sudoers, visudo)

`# apt update && apt -y install hostapd` #Actualizar o listado de paquetes dos repositorios (/etc/apt/sources.list, /etc/apt/sources.list.d/) e se este comando ten éxisto ($?=0) faise o segundo comando, o cal instálase o paquete hostapd. Co parámetro -y automaticamente asumimos yes a calquera pregunta que ocorra na instalación do paquete.

`# ip netns add wifi_ap_wlan0` #Crear un novo **namespace de rede** chamado wifi_ap_wlan0 no sistema. Un **namespace de rede** é unha funcionalidade de Linux que permite crear espazos de rede illados, onde cada espazo pode ter as súas propias interfaces de rede, routers e configuracións independentes. Neste caso, o nome wifi_ap_wlan0 identifica o namespace que se está a crear, e permitirá que as interfaces de rede, como **wlan0**, operen de forma illada dentro dese namespace, sen interferir co resto das interfaces ou redes do sistema. Isto é útil para crear ambientes de proba ou para a xestión de múltiples redes illadas na mesma máquina sen que compartan recursos.

`# iw phy phy0 set netns name wifi_ap_wlan0` #Asignar a interface de radio phy0 (que representa a primeira interfaz de hardware de rede Wi-Fi) ao namespace de rede identificado por **wifi_ap_wlan0**. Isto significa que a interface phy0 pasará a formar parte do espazo de rede illado **wifi_ap_wlan0**, o que permite que a súa configuración e operación (como a asignación de IPs ou a conexión a redes Wi-Fi) se realicen de maneira independente das outras interfaces ou do namespace principal do sistema. Este comando é útil cando se traballa con múltiples namespaces de rede para crear entornos de rede separados e illados, por exemplo, en simulacións ou probas de redes.

`# ip netns exec wifi_ap_wlan0 bash` #Executar unha instancia do **shell bash** dentro do namespace de rede chamado wifi_ap_wlan0. Isto significa que, ao executar o comando, ábrese un terminal onde as interfaces de rede e as rutas de rede serán específicas para o namespace wifi_ap_wlan0, permitindo interactuar con redes ou dispositivos dentro dese espazo illado. A principal utilidade é traballar cunha rede virtual illada sen afectar a rede principal do sistema, o que é útil para tarefas como probar configuracións de rede ou simular entornos de rede controlados.

(e) Executar na consola1:

```
# echo 'interface=wlan0
driver=nl80211
country_code=ES
ssid=EMPRESA-XYZ
channel=6
hw_mode=g
ieee80211w=2
wpa=2
wpa_key_mgmt=SAE
rsn_pairwise=CCMP
sae_password=spongebob19
sae_require_mfp=1' > wpa3-sae.conf
```

#Este comando crea un ficheiro de configuración chamado wpa3-sae.conf para configurar un punto de acceso Wi-Fi, tal que:

interface=wlan0: Especifica que a interface de rede a configurar é wlan0 (tarxeta Wi-Fi).
driver=nl80211: Usa o driver nl80211, que é común para dispositivos Wi-Fi modernos.
country_code=ES: Establece o código do país como ES (España), para aplicar as regulacións de canal e potencia locais.
ssid=EMPRESA-XYZ: Define o nome da rede Wi-Fi como EMPRESA-XYZ.
channel=6: Define o canal a usar, neste caso o canal 6 na banda de 2.4GHz(2437MHz).
hw_mode=g: Establece o modo de hardware como **g** (Wi-Fi 802.11g)
ieee80211w=2: **PMF (Protected Management Frames) obrigatorio**. Isto protexe tramas de xestión (por exemplo, deauth/disassoc) e é requisito típico en WPA3.
wpa=2: Habilita RSN (o "WPA2/WPA3" moderno en `hostapd`). *O valor 2 aquí indica "usar RSN"; non significa que sexa WPA2-PSK, iso ven dado por* ***wpa_key_mgmt.***
wpa_key_mgmt=SAE: escolle **SAE (Simultaneous Authentication of Equals)** como método de autenticación → isto é **WPA3-Personal**, non PSK.
rsn_pairwise=CCMP: Establece o algoritmo de cifrado con **AES-CCMP**.
sae_password=spongebob19: Define a clave de acceso (**spongebob19**) para a rede Wi-Fi.
sae_require_mfp=1: Require **PMF** para conexións SAE (vai na mesma liña de `ieee80211w=2`).

`# hostapd wpa3-sae.conf` #Iniciar o **hostapd**, que é un daemon que permite que un dispositivo actúe como punto de acceso Wi-Fi. Ao executar este comando, **hostapd** carga o ficheiro de configuración `wpa3-sae.conf` para configurar o punto de acceso, utilizando os parámetros especificados neste ficheiro, como a interface de rede, o nome da rede (SSID), a clave WPA3-SAE, os algoritmos de cifrado, e outros axustes de seguridade e rede. Isto fai que o dispositivo se converta nun punto de acceso Wi-Fi, permitindo que os clientes se conecten á rede de forma segura.

```
wlan0: interface state UNINITIALIZED->COUNTRY_UPDATE
wlan0: interface state COUNTRY_UPDATE->ENABLED
wlan0: AP-ENABLED
```

(f) Configura wlan1 como cliente autentificado e aillala do resto de interfaces. Executar na consola2:

`$ sudo su -` #Acceder á consola de root(administrador) a través dos permisos configurados co comando sudo (/etc/sudoers, visudo)

`# ip netns add wifi_cliente_wlan1` #Crear un novo **namespace de rede** chamado wifi_cliente_wlan1 no sistema. Un **namespace de rede** é unha funcionalidade de Linux que permite crear espazos de rede illados, onde cada espazo pode ter as súas propias interfaces de rede, routers e configuracións independentes. Neste caso, o nome wifi_cliente_wlan1 identifica o namespace que se está a crear, e permitirá que as interfaces de rede, como **wlan1**, operen de forma illada dentro dese namespace, sen interferir co resto das interfaces ou redes do sistema. Isto é útil para crear ambientes de proba ou para a xestión de múltiples redes illadas na mesma máquina sen que compartan recursos.

`# iw phy phy1 set netns name wifi_cliente_wlan1` #Asignar a interface de radio phy1 (que representa a segunda interfaz de hardware de rede Wi-Fi) ao namespace de rede identificado por **wifi_cliente_wlan1**. Isto significa que a interface phy1 pasará a formar parte do espazo de rede illado co id **wifi_cliente_wlan1**, o que permite que a súa configuración e operación (como a asignación de IPs ou a conexión a redes Wi-Fi) se realicen de maneira independente das outras interfaces ou do namespace principal do sistema. Este comando é útil cando se traballa con múltiples namespaces de rede para crear entornos de rede separados e illados, por exemplo, en simulacións ou probas de redes.

`# ip netns exec wifi_cliente_wlan1 bash` #Executar unha instancia do **shell bash** dentro do *network namespace* chamado **wifi_cliente_wlan1**. A partir deste momento, todos os comandos executados nesta consola afectarán unicamente ás interfaces, rutas e configuracións de rede dese namespace. Isto permite simular un **cliente Wi-Fi illado**, sen interferir coa rede principal nin co namespace do punto de acceso.

`# ip link set lo up` #Activar a interface **loopback (lo)** dentro do namespace **wifi_cliente_wlan1**. A interface loopback é necesaria para o correcto funcionamento de múltiples aplicacións de rede, incluído wpa_supplicant, e garante que os servizos locais poidan comunicarse correctamente dentro do namespace.

```
# echo 'network={
ssid="EMPRESA-XYZ"
key_mgmt=SAE
ieee80211w=2
sae_password="spongebob19"
}' >> wpa_supplicant_wpa3.conf
```

#Este comando engade unha configuración a un ficheiro chamado wpa_supplicant_wpa3.conf para configurar a conexión Wi-Fi dun cliente. Así:

network={: Inicia a sección de configuración dunha rede Wi-Fi.

ssid="EMPRESA-XYZ": Define nome da rede Wi-Fi á que o cliente se quere conectar(SSID): EMPRESA-XYZ

key_mgmt=SAE: Indica que o método de autenticación é **SAE** → é dicir, **WPA3-Personal** (non WPA2-PSK). SAE substitúe ao PSK tradicional e usa un intercambio máis robusto (Dragonfly/SAE).

ieee80211w=2: **PMF (Protected Management Frames) obrigatorio** no lado cliente(0: desactivado, 1: opcional, 2: obrigatorio). Isto ten que encaixar co AP: se o AP require PMF, o cliente debe levar 2 (ou non conectará).

sae_passord="spongebob19": Define a clave de acceso á rede Wi-Fi (spongebob19). A *passphrase* para SAE (o contrasinal "humano" da rede WPA3). En WPA3 non se usa como "PSK directo", senón como entrada do protocolo SAE para derivar claves de sesión.

}: Pecha a sección de configuración da rede.

`# wpa_supplicant -B -i wlan1 -c wpa_supplicant_wpa3.conf` #Iniciar o **wpa_supplicant**, que é un programa utilizado para conectar un dispositivo a unha rede Wi-Fi de forma segura. A explicación de cada opción é a seguinte:

-B: Executa **wpa_supplicant** en segundo plano (background).
-i wlan1: Especifica a interface de rede a usar para a conexión Wi-Fi, neste caso wlan1.
-c wpa_supplicant_wpa3.conf: Indica o ficheiro de configuración que contén os parámetros da rede Wi-Fi (como SSID, clave, etc.), neste caso wpa_supplicant_wpa3.conf.

(g) Consola1: Comprobar que ten lugar a conexión do cliente(neste caso MAC Cliente= 8e:b3:b5:62:2d:b9):

```
wlan0: STA 8e:b3:b5:62:2d:b9 IEEE 802.11: associated (aid 1)
wlan0: AP-STA-CONNECTED 8e:b3:b5:62:2d:b9
wlan0: STA 8e:b3:b5:62:2d:b9 RADIUS: starting accounting session 3544351FB857A3D9
wlan0: STA 8e:b3:b5:62:2d:b9 WPA: pairwise key handshake completed (RSN)
wlan0: EAPOL-4WAY-HS-COMPLETED 8e:b3:b5:62:2d:b9
```

(h) Executar na consola3:

`$ sudo su -` #Acceder á consola de root(administrador) a través dos permisos configurados co comando sudo (/etc/sudoers, visudo)

`# ~~airmon-ng check kill~~` #Deter calquera proceso que poida interferir co funcionamento das ferramentas de auditoría Wi-Fi, como **airodump-ng** ou **aireplay-ng**, cando unha interface está en modo monitor. Estes procesos inclúen xestores de rede (como **NetworkManager** ou **wpa_supplicant**) que automaticamente configuran as interfaces de rede, podendo interferir co modo monitor. Deténdoos, **airmon-ng** garante que a interface poida funcionar correctamente en modo monitor sen interrupcións.

```
# airmon-ng start wlan2 #Habilitar o modo monitor na interface de rede sen fíos chamada wlan2,
```
permitindo que esta capture todos os paquetes Wi-Fi que estean no aire, sen estar asociada a unha rede específica. O **modo monitor** é esencial para tarefas de auditoría ou análise de redes Wi-Fi, xa que permite escoitar o tráfico de calquera dispositivo na mesma canle sen necesidade de estar conectado. Ademais, este comando crea unha nova interface virtual (xeralmente chamada `wlan2mon`) asociada á interface orixinal para usar en operacións de monitoraxe.

```
# airodump-ng wlan2mon #Iniciar a ferramenta airodump-ng para capturar paquetes de redes Wi-Fi,
```
utilizando a interface `wlan2mon`, que debe estar en modo monitor. Este comando permite escanear e listar todas as redes Wi-Fi dispoñibles no rango da interface, mostrando información como o nome das redes (**SSID**), os enderezos MAC dos puntos de acceso (**BSSID**), os canais que están a usar, o tipo de cifrado (WPA, WPA2, etc.), e unha lista de clientes conectados a esas redes. É unha ferramenta comumente utilizada para auditorías de seguridade en redes sen fíos.

```
# Ctrl^C #Envíar unha sinal SIGINT (Interrupt) ao proceso en execución no terminal actual,
```
indicándolle que debe deter a súa execución. Esta combinación de teclas úsase para interromper ou finalizar procesos que están en curso, como scripts, programas ou comandos que se están executando.

```
# mkdir capturas && airodump-ng wlan2mon -c 6 -w capturas/cap #Crear un directorio
```
chamado `capturas` e logo executa `airodump-ng` na interface `wlan2mon` (configurada en modo monitor) para capturar paquetes Wi-Fi no canal **6***, gardando os datos capturados no directorio `capturas` co prefixo de ficheiro `cap`. Como resultado, os ficheiros xerados (por exemplo, `cap-01.cap`) conterán os paquetes capturados, útiles para análises ou auditorías de redes sen fíos.

***(sustituír polo canal que está a usar o AP)**

(i) Voltar a conectar o cliente1. Executar na consola2:

```
# pkill -f wpa_supplicant || true #Eliminar os procesos wpa_supplicant existentes.
  #Ver na consola1 a desconexión do cliente
   wlan0: AP-STA-DISCONNECTED 8e:b3:b5:62:2d:b9
```

```
# wpa_supplicant -B -i wlan1 -c wpa_supplicant_wpa3.conf #Iniciar o proceso
```
`wpa_supplicant`, que é usado para xestionar a conexión dunha interface Wi-Fi a unha rede inalámbrica. A opción `-B` executa o proceso en segundo plano (background), `-i wlan1` especifica que a interface Wi-Fi a utilizar é `wlan1`, e `-c wpa_supplicant_wpa3.conf` indica que o ficheiro de configuración a usar é `wpa_supplicant_wpa3.conf`, que contén os detalles de autenticación e parámetros da rede, como o SSID, método de cifrado e contrasinal. Este comando configura e conecta a interface Wi-Fi a unha rede segundo a configuración proporcionada.

```
  #Ver na consola1 a reconexión do cliente
   wlan0: AP-STA-CONNECTED 8e:b3:b5:62:2d:b9
   wlan0: STA 8e:b3:b5:62:2d:b9 RADIUS: starting accounting session 30793625FB0FE410
   wlan0: STA 8e:b3:b5:62:2d:b9 WPA: pairwise key handshake completed (RSN)
   wlan0: EAPOL-4WAY-HS-COMPLETED 8e:b3:b5:62:2d:b9
```

(j) Consola3. Unha vez capturado o handshake:

```
CH  6 ][ Elapsed: 48 s ][ 2026-01-13 17:24 ][ WPA handshake: AA:BB:CC:DD:EE:FF ← BSSID
```

Executar na consola3:

```
# Ctrl^C #Envíar unha sinal SIGINT (Interrupt) ao proceso en execución no terminal actual
```

Auditar contrasinal

```
# gunzip -c /usr/share/wordlists/rockyou.txt.gz > /tmp/rockyou.txt #Descomprimir o
```
ficheiro rockyou.txt.gz, que contén un popular dicionario de contrasinais, sen eliminar o ficheiro comprimido orixinal. A opción -c fai que o contido descomprimido sexa enviado ao estándar de saída, e co redirixidor > ese contido gárdase como un novo ficheiro chamado rockyou.txt no directorio /tmp. Deste xeito, o ficheiro descomprimido queda dispoñible en /tmp sen modificar o ficheiro comprimido orixinal en /usr/share/wordlists.

```
# aircrack-ng capturas/cap-01.cap -w /tmp/rockyou.txt #Usar a ferramenta Aircrack-ng
```
para realizar un ataque de forza bruta contra un ficheiro de captura de paquetes (`cap-o1.cap`) almacenado no directorio `capturas`. Este ficheiro contén un **handshake** de WPA/WPA2, e o comando tenta descifrar a clave de acceso utilizando un dicionario de contrasinais. O dicionario de contrasinais está especificado no ficheiro `rockyou.txt`, que está no directorio `/tmp`. O proceso consistirá en probar cada palabra no dicionario para ver se coincide co contrasinal usado na rede Wi-Fi, permitindo obter a clave se está no dicionario.

```
                                    Unsupported key version 0 encountered.
        May be WPA3 - not yet supported.
        Aborted
```

Método non soportado (non funciona SAE como PSK):

En **WPA3-SAE** o que captura `airodump-ng` non é un **handshake reutilizable** como en WPA2-PSK, senón o **intercambio de autenticación SAE (EAPOL/SAE commit-confirm)** e o **4-way handshake asociado**, que non permite derivar unha clave para un ataque por dicionario offline.

(k) Consola4. Verificación de Protección KRACK(Key Reinstallation Attack):

KRACK (CVE-2017-13077 e relacionadas) é unha vulnerabilidade crítica descuberta en 2017 que afecta ao **4-Way Handshake de WPA2**, independentemente de se usa PSK ou Enterprise. O ataque explota unha debilidade no **protocolo 802.11i** que permite reinstalar claves de cifrado xa usadas, rompendo a protección do tráfico.

Como Funciona o Ataque: Vulnerabilidade no 4-Way Handshake

No handshake normal WPA2:

1. AP → Cliente: ANonce (Message 1)
2. Cliente → AP: SNonce + MIC (Message 2)
3. AP → Cliente: GTK + MIC (Message 3) **← VULNERABILIDADE AQUÍ**
4. Cliente → AP: ACK (Message 4)

O problema: Se o **Mensaxe 3** se perde ou non chega ao AP, o AP **reenvíao**. O cliente, ao recibir o Mensaxe 3 duplicado, **reinstala a PTK** (Pairwise Transient Key) que xa estaba usando.

Consecuencias da Reinstalación de Claves

Cando se reinstala unha clave de cifrado:

1) **O nonce de cifrado reséntase a 0** (ou a un valor predicible)
2) **Reutilízanse os mesmos valores de cifrado** para distintos paquetes
3) **Permite ao atacante:**
    1. **Descifrar tráfico** capturado previamente
    2. **Inxectar paquetes maliciosos** na conexión
    3. **Realizar ataques de replay**

Protección en WPA3-SAE

WPA3-SAE **NON é vulnerable a KRACK** porque:

1. **PMF Obrigatorio (802.11w=2):**
    - As tramas do 4-Way Handshake van **protexidas**
    - Un atacante **non pode inxectar Mensaxes 3 falsos** para forzar reinstalacións
2. **Forward Secrecy:**
    - Cada sesión usa claves **únicas e non reutilizables**
    - Capturar tráfico pasado **non permite descifrado futuro**
3. **Implementacións Modernas:**
    - hostapd >= 2.6 e wpa_supplicant >= 2.6 **inclúen parcheados KRACK**
    - O kernel Linux >= 4.13 **protexe contra reinstalacións**

WPA3-SAE está deseñado para ser inmune ao ataque KRACK. Verificamos nunha Consola4:

```
$ hostapd -v # Comprobar versións (deben ser >= 2.6)
$ wpa_supplicant -v # Comprobar versións (deben ser >= 2.6)
$ sudo grep "ieee80211w=2" /root/wpa3-sae.conf # Verificar PMF activo nos logs do AP (Consola 1)
$ #Analizar Tramas de Xestión: Ver se as tramas de deauth van cifradas
$ sudo tshark -r /root/capturas/cap-01.cap \
  -Y "wlan.fc.type_subtype == 0x000c" \
  -T fields -e frame.number -e wlan.fc.protected -e wlan.sa -e wlan.da
  #Resultado Esperado (WPA3-SAE con PMF)
    4       True    8e:b3:b5:62:2d:b9       be:47:31:18:d3:d8
```

Campo	Valor	Significado
frame.number	4	Número de trama na captura
wlan.fc.protected	True	TRAMA CIFRADA (PMF activo)
wlan.sa	8e:b3:b5:62:2d:b9	MAC orixe (quen envía deauth)= MAC cliente
wlan.da	**be:47:31:18:d3:d8**	**MAC destino (quen recibe deauth) = MAC AP**

Conclusión: Ao contrario de WPA2-PSK, WPA3-SAE con PMF obrigatorio **impide completamente** ataques de reinstalación de claves (KRACK).