TALLER HE

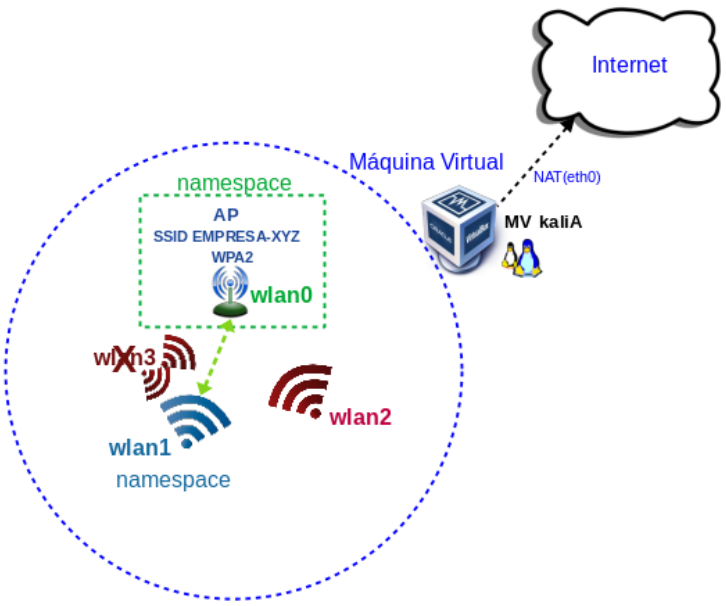
PRÁCTICA Auditar contrasinal Wi-Fi WPA2 (PSK)

(ieee80211w → ~~deautenticación cliente~~)

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=4 → wlan0, wlan1, wlan2, wlan3
  - wlan0 → AP (hostapd(ieee80211w), ip netns)
  - wlan1 → Cliente(wpa_supplicant(ieee80211w))
  - wlan2 → unknown (tools suite: aircrack-ng →auditar handshake)
  - wlan3 → unknown (tools suite: aircrack-ng →~~deautenticacion~~)
- **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 (PSK) (ieee80211w → ~~deautenticación cliente~~)
■ Host alumnado ■ Máquina virtual GNU/Linux Kali ■ [0] 1-Taller-HE-Practica-WiFi-2 ■ [1] ieee80211w	(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, wlan3) ■ Montar AP simulado e aillar ■ Conectar co cliente simulado ■ Investigar co cliente unknown(airodump-ng) →intentar desconectar cliente simulado → ieee82011w activo → non desconecta cliente simulado

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.

IEEE 802.11w: Fortalecendo a Seguridade nas Redes Wi-Fi

Que é o IEEE 802.11w?

O IEEE 802.11w é un estándar de seguridade que se basea no protocolo 802.11i (WPA2). O seu obxectivo principal é reforzar a protección das redes inalámbricas (WLAN) contra unha serie de ataques sofisticados que poderían comprometer a integridade das tramas de xestión.

Por que é importante?

- **Máis alá dos datos:** Mentres que o 802.11i se centra en protexer a transmisión de datos, o 802.11w estende esa protección ás tramas de xestión, que son responsables das principais operacións dunha rede Wi-Fi, como a autenticación, asociación e configuración.
- **Ataques ás tramas de xestión:** Estes ataques poden ser utilizados para interromper o servizo, roubar información confidencial ou incluso tomar o control da rede. O 802.11w fai que estes ataques sexan moito máis difíciles de levar a cabo.

Como funciona o 802.11w?

- **Protección de integridade:** Introduce un mecanismo de protección de integridade de mensaxe (MIP) que utiliza un código de autenticación de mensaxe (MAC) para verificar a autenticidade das tramas de xestión.
- **Detección de intrusións:** Ao verificar a integridade de cada trama, o 802.11w pode detectar rapidamente calquera intento de manipulación ou intrusión na rede.
- **Prevención de falsificación:** O MIP fai que sexa extremadamente difícil para un atacante falsificar unha trama de xestión e enganar aos dispositivos da rede.
- **Resistencia a Ataques de Replay:** Este estándar tamén evita que os atacantes reutilicen tramas capturadas anteriormente para enganar á rede.

Beneficios clave do 802.11w

- **Maior seguridade:** Ofrece unha capa adicional de protección contra unha ampla gama de ataques, facendo que as redes Wi-Fi sexan máis resistentes ás ameazas.
- **Maior fiabilidade:** Ao previr a falsificación de tramas de xestión, o 802.11w contribúe a unha operación máis estable e fiable da rede.
- **Compatibilidade co 802.11i:** Intégrase sen problemas co estándar 802.11i, o que facilita a súa implementación en redes existentes.

Por que son tan importantes as tramas de xestión?

Imaxina a túa rede Wi-Fi como unha cidade: as tramas de xestión son as sinais de tráfico que indican aos dispositivos como moverse e comunicarse. Se un atacante pode manipular estas sinais, pode causar caos na rede, desconectando dispositivos, interceptando datos ou incluso tomando o control da mesma.

Ferramentas como AirCrack-ng e 802.11w

Ferramentas como AirCrack-ng úsanse para realizar probas de seguridade en redes Wi-Fi e, en mans equivocadas, poden explotar vulnerabilidades. Non obstante, o 802.11w dificulta significativamente o traballo destas ferramentas ao facer que as tramas de xestión sexan moito máis difíciles de falsificar.

Que debes facer?

- **Verifica a Compatibilidade:** Asegúrate de que os teus dispositivos Wi-Fi (puntos de acceso e clientes) sexan compatibles co estándar 802.11w.
- **Configura Correctamente:** Segue as instrucións do fabricante para configurar correctamente a protección de tramas de xestión na túa rede.
- **Combínao con Outras Medidas:** O 802.11w é unha peza clave, pero non a única. Utiliza contrasinais fortes, mantén o teu firmware actualizado e considera outras medidas de seguridade para unha protección integral.

Configuración hostapd:

Para activar `ieee80211w`, é necesario configurar as seguintes opcións relacionadas co cifrado:

wpa=2 #Activa WPA2
wpa_key_mgmt=WPA-PSK-SHA256 #Usa SHA-256 para a xestión de claves, necesario para PMF
wpa_pairwise=CCMP #Configura AES como cifrado para WPA
rsn_pairwise=CCMP #Configura AES para RSN (Robust Security Network), que é unha extensión de WPA2 para PMF
ieee80211w=2 #PMF obrigatorio

Configuración wpa_supplicant:

Para activar `ieee80211w`, é necesario configurar a seguinte opción:

key_mgmt=WPA-PSK-SHA256 #Usa SHA-256 para a xestión de claves, necesario para PMF
pairwise=CCMP #Configura AES como cifrado para WPA (comunicacións unicast)
group=CCMP #Configura AES como cifrado para WPA (comunicacións multicast)
ieee80211w=2 #PMF obrigatorio

Conclusión

O IEEE 802.11w é un estándar esencial para calquera persoa que valore a seguridade da súa rede Wi-Fi. Ao fortalecer a protección das tramas de xestión, este protocolo fai que sexa moito máis difícil para os atacantes comprometer a túa rede e os teus datos.

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-PSK-ieee80211w-Deautenticacion

(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 e wlan3 como un cliente que non sabe o contrasinal para conectarse ao AP (shell bash consola3 → mode monitor)(shell bash consola4 → deautenticar cliente conectado wlan1).

Consola1

```
$ setxkbmap es
$ ip addr show
$ ip route
$ cat /etc/resolv.conf
$ sudo modprobe mac80211_hwsim radios=4
$ ip addr show
$ sudo su -
 # apt update && apt -y install hostapd
 # ip netns add wifi_ap_wlan0
 # ip netns exec wifi_ap_wlan0 bash
 # echo $$ > /tmp/consola1-pid.txt
 # 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.conf
```

Consola2:

```
$ PID=$(cat /tmp/consola1-pid.txt)
$ sudo iw phy phy0 set netns ${PID}
```

Consola1:

```
 # hostapd -d wpa-psk.conf | tee -a hostapd.log #Comprobar en consola1 o estado habiliatado do AP → wlan0: AP-ENABLED
```

Consola2:

```
$ sudo su -
  # echo -e 'network={\nssid="EMPRESA-XYZ"\nkey_mgmt=WPA-PSK-SHA256\npairwise=CCMP\ngroup=CCMP\npsk="spongebob19"\nieee80211w=2\n}' >
    wpa_supplicant.conf
  # wpa_supplicant -B -i wlan1 -c wpa_supplicant.conf -D nl80211 #Comprobar en consola1 a conexión realizada wlan0: AP-STA-CONNECTED xx:xx:xx:xx:xx:xx
```

Consola3:

```
$ 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 && airodump-ng wlan2mon -c 6 -w capturas/cap
```

Consola4:

```
$ sudo su -
  # ifconfig wlan3 down || ip link set wlan3 down
  # iwconfig wlan3 channel 6 || (iw wlan3 set type monitor && iw wlan3 set channel 6 && iw wlan3 set type managed)
  # ifconfig wlan3 up || ip link set wlan3 up
  # aireplay-ng -0 1 -a yy:yy:yy:yy:yy::yy -c xx:xx:xx:xx:xx:xx wlan3 #Opcións: -a BSSID -c MAC-Cliente-Autenticado
```

Consola1:

```
Comprobar que non se produce a deautenticación (ver saída por terminal ou log no ficheiro hostapd.log)
      ...
      nl80211: BSS Event 59 (NL80211_CMD_FRAME) received for wlan0
      nl80211: RX frame da=yy:yy:yy:yy:yy:yy sa=xx:xx:xx:xx:xx:xx bssid=yy:yy:yy:yy:yy:yy freq=2437 ssi_signal=-50 fc=0xc0 seq_ctrl=0x57f0
      stype=12 (WLAN_FC_STYPE_DEAUTH) len=26
      wlan0: Event RX_MGMT (18) received
      wlan0: mgmt::deauth
      wlan0: deauthentication: STA=xx:xx:xx:xx:xx:xx reason_code=7
      wlan0: Station xx:xx:xx:xx:xx:xx trying to deauthenticate, but it is not authenticated
      ...
```