ZABALA GAILETAK

S.L. - Segurtasun Dokumentazioa

WiFi Pentesting Gida

2026(e)ko otsailaren 23(a)

WiFi Penetration Testing - Zabala Gailetak

📋 Laburpena / Resumen

Dokumentazio honek Zabala Gailetak-en WiFi sareen segurtasun-ebaluazioa deskribatzen du, **wifi-CTF** entorno simulatua erabiliz. Sare erradioaren frogak egiteko diseinatuta dago, seinale fisikoak erabili gabe.

Este documento describe la evaluación de seguridad de redes WiFi de Zabala Gailetak, utilizando el entorno simulado **wifi-CTF**. Está diseñado para realizar pruebas de redes inalámbricas sin utilizar señales físicas.

🎯 Helburua / Objetivo

WiFi sareen segurtasuna ebaluatzea entorno kontrolatu batean:

- Sare irekien arriskuak identifikatzea
- WPA2/WPA3 protokoloen ahultasunak aztertzea
- SSID ezkutuak "decloak" egiteko gaitasuna frogatzea
- Segurtasun neurri egokiak proposatzea

Evaluar la seguridad de redes WiFi en un entorno controlado:

- Identificar riesgos de redes abiertas
- Analizar vulnerabilidades en protocolos WPA2/WPA3
- Demostrar capacidad de "decloaking" de SSID ocultos
- Proponer medidas de seguridad adecuadas

🏗️ Egitura / Estructura

```
wifi/
├── README.md                                    # Dokumentazio hau
├── WiFi_Pentest_Report_ZabalaGailetak.docx      # Informe completo
├── generar_informe_wifi_pentest.js              # Generador del informe
├── scripts/
│   └── wifi_pentest_automation.sh              # Script de automatización
└── evidencias/                                  # Directorio para evidencia
```

🚀 Nola erabili / Cómo usar

1. Instalación / Instalazioa

```
cd scripts/
sudo ./wifi_pentest_automation.sh setup
```

2. Entorno abiarazi / Iniciar entorno

```
sudo ./wifi_pentest_automation.sh start
```

3. Test osoa exekutatu / Ejecutar test completo

```
sudo ./wifi_pentest_automation.sh full
```

4. Beste komandoak / Otros comandos

```
# Eskaneatzea
./wifi_pentest_automation.sh scan

# AP zehatzak testeatu
./wifi_pentest_automation.sh guest   # AP-Guest
./wifi_pentest_automation.sh wpa2    # AP-Bridged
./wifi_pentest_automation.sh wpa3    # AP-WPA3
./wifi_pentest_automation.sh hidden  # AP-Hidden

# Garbitu
sudo ./wifi_pentest_automation.sh stop
./wifi_pentest_automation.sh clean
```

📊 4 Eszenario Probaktuak / 4 Escenarios Probados

1. AP-Guest (Open WiFi)

- **Konfigurazioa**: AP irekia, gabe autentikaziorik
- **Helburua**: MAC helbideak eta trafikoa bildu
- **Tresnak**: airodump-ng, tshark
- **Arriskua**: Information disclosure (CVSS 5.3)

2. AP-Bridged (WPA2-PSK)

- **Konfigurazioa**: WPA2-PSK pasahitzarekin
- **Helburua**: Handshake-a harrapatu eta crack egin
- **Tresnak**: airodump-ng, aireplay-ng, aircrack-ng
- **Arriskua**: Sareko sarbide osoa (CVSS 7.5)

3. AP-WPA3 (SAE)

- **Konfigurazioa**: WPA3-SAE (Simultaneous Authentication of Equals)
- **Helburua**: Online brute-force erasoa

- **Tresnak**: wacker (Dragonfly handshake exploit)
- **Arriskua**: WPA3 "u Breaking" (CVSS 8.1)

4. AP-Hidden (SSID Ezkutua)

- **Konfigurazioa**: SSID ezkutua 5GHz-n
- **Helburua**: SSID-a "decloak" egitea
- **Tresnak**: airodump-ng (5GHz banda)
- **Arriskua**: AP identifikazioa (CVSS 5.3)

🛡️ Segurtasun Gomendioak / Recomendaciones de Seguridad

Kritikoak (Lehentasun I)

1. **WPA3-Enterprise ezarri**
   - 802.1X autentikazioa
   - RADIUS zerbitzaria
   - Ziurtagirietan oinarritutako autentikazioa
2. **Pasahitz politikak indartu**
   - 12+ karaktere minimo
   - Konplexutasuna (maiuskulak, minuskulak, zenbakiak, sinboloak)
   - Rotazio periodikoa
3. **WiFi irekiak debekatu**
   - Gonbidatuen sarea ere WPA2/WPA3-rekin babestu
   - Captive portal seguruak erabili

Osagarriak (Lehentasun II)

- **WIDS/WIPS**: WiFi Intrusion Detection/Prevention System
- **Rogue AP Detection**: AP baimendu gabeen detekzioa
- **Network Segmentation**: VLAN isolamendua
- **Regular Audits**: WiFi pentest periodikoak

📚 Iturriak / Fuentes

- wifi-CTF GitHub - Sealing Tech
- wacker - WPA3 Brute Force - Blunderbuss WCTF
- Aircrack-ng Suite
- OWASP Wireless Testing Guide
- WPA3 Dragonblood Vulnerabilities

⚠️ Ohar Legala / Nota Legal

ABISUA / ADVERTENCIA

Tresna hauek **baimendutako hacking etiko** jardueretarako soilik dira. Ez erabili baimenik gabe!

Estas herramientas son **solo para actividades de hacking ético autorizado**. ¡No usar sin permiso!

📧 Kontaktua / Contacto

Zabala Gailetak, S.L.
Segurtasun Taldea / Equipo de Seguridad
security@zabala-gailetak.eus

Azken eguneraketa: 2026-02-23
Versión: 1.0