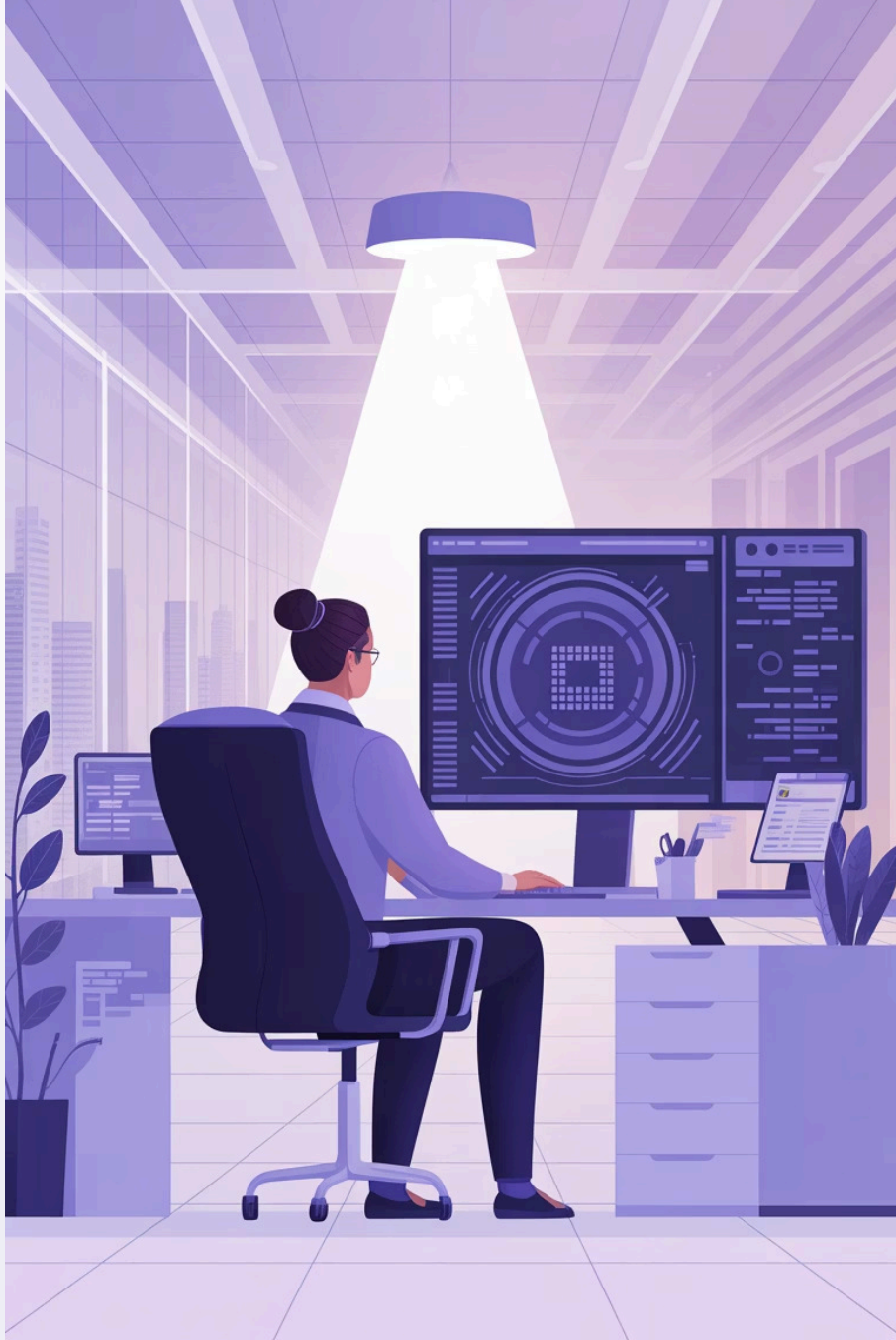
Servicios de Auditoría Ofensiva

Evaluación profesional de seguridad desde la perspectiva de un atacante real



Nuestra Misión

Este dossier presenta los servicios de auditoría ofensiva ofrecidos por nuestra empresa, describiendo en detalle su alcance, metodología aplicada y las herramientas utilizadas en cada caso. El objetivo es proporcionar a las organizaciones una visión clara y profesional de cómo evaluamos su seguridad ante amenazas reales.

Utilizamos metodologías internacionales reconocidas y herramientas especializadas para garantizar un análisis exhaustivo y profesional, orientado a identificar vulnerabilidades críticas y fortalecer la postura de seguridad del cliente.

Nuestros Servicios Principales

Auditoría de Aplicaciones Web

Evaluación exhaustiva de aplicaciones web para identificar vulnerabilidades que puedan comprometer datos, funcionalidades o infraestructura

Auditoría de Red Interna

Simulación de un atacante con acceso a la red interna de la organización para evaluar robustez del entorno

Auditoría de Dispositivos IoT

Evaluación de seguridad en dispositivos conectados, incluyendo dispositivos industriales, cámaras IP y sensores

Auditoría de Seguridad de Aplicaciones Web

Alcance del Servicio

- Validación de autenticación y gestión de sesiones
- Revisión de inyecciones (SQLi, XSS, LDAP)
- Validación de controles de acceso
- Pruebas de subida de archivos
- Fuzzing de entradas

Resultados Esperados

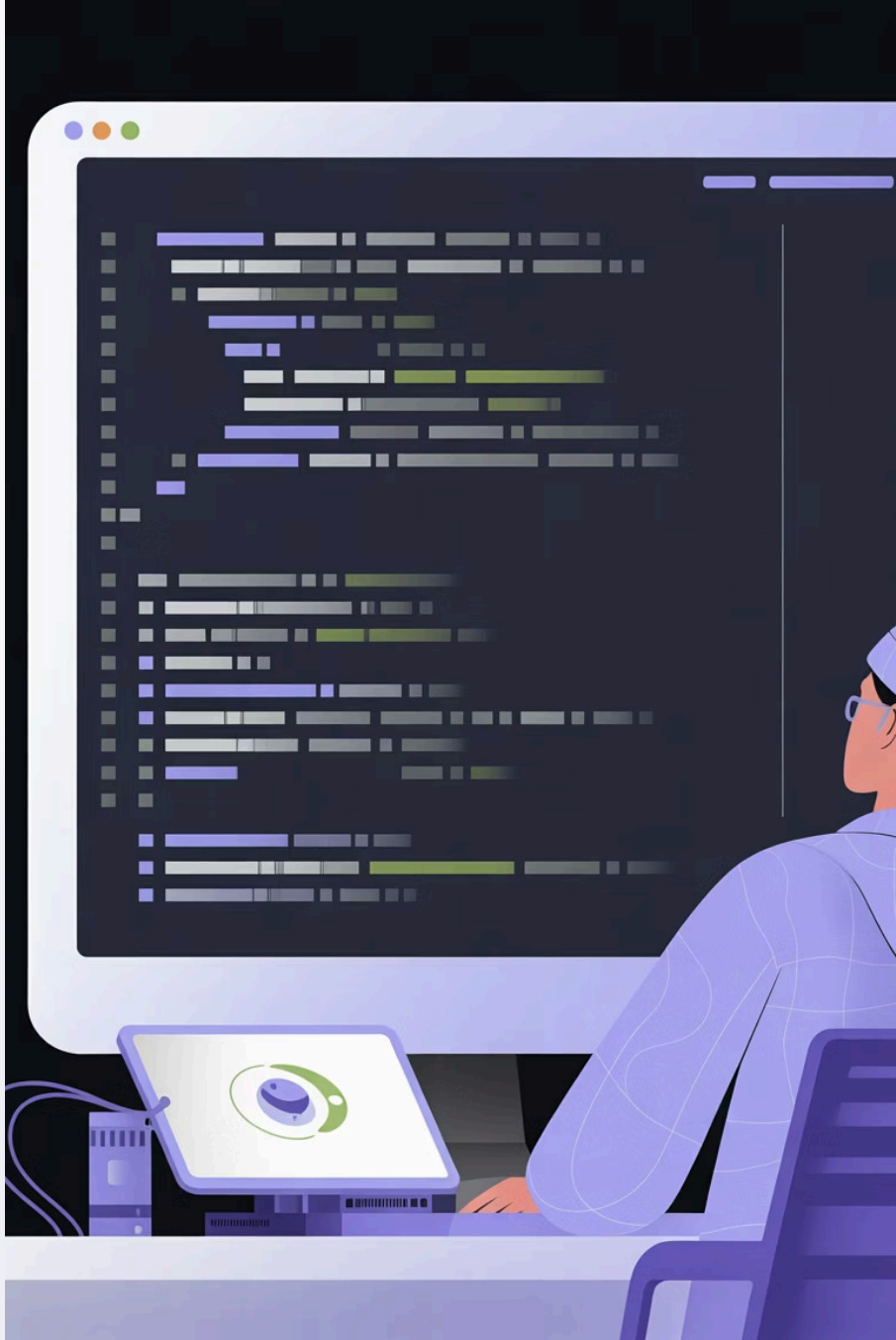
Informe técnico con vulnerabilidades clasificadas por criticidad, recomendaciones precisas de mitigación y evidencias técnicas del impacto.

Metodología

Basada en **OWASP Web Security Testing Guide (WSTG)**, enmarcada dentro de PTES para fases previas y posteriores.

Herramientas

- Burp Suite Pro
- OWASP ZAP
- Gobuster/Dirbuster
- SQLMap
- Nmap



Auditoría de Red Interna

Simulación de un atacante con acceso a la red interna de la organización. Se evalúa la robustez del entorno, configuraciones, accesos y posibles rutas de movimiento lateral.

01

Descubrimiento

Identificación de equipos y servicios activos en la red

02

Enumeración

Análisis de puertos, protocolos y recursos compartidos

03

Explotación

Pruebas de explotación interna y escalada de privilegios

04

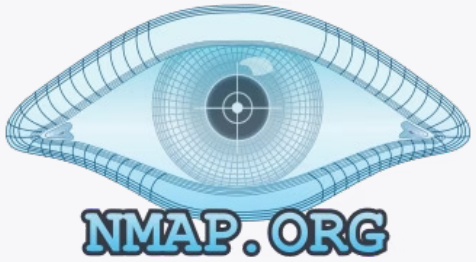
Movimiento Lateral

Validación de segmentación de red y rutas de compromiso

Herramientas de Red Interna

Nmap

Escaneo de puertos y descubrimiento de servicios



BloodHound

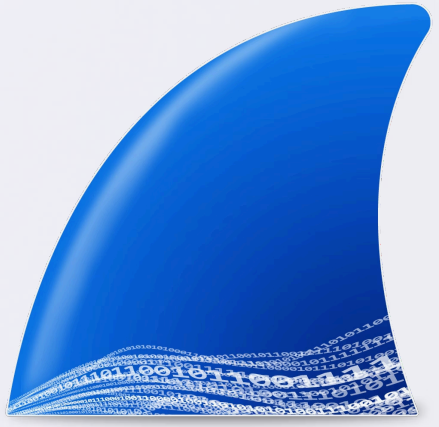
Análisis de rutas de ataque en Active Directory

Metasploit

Framework completo de explotación y post-explotación

Wireshark

Captura y análisis de tráfico de red

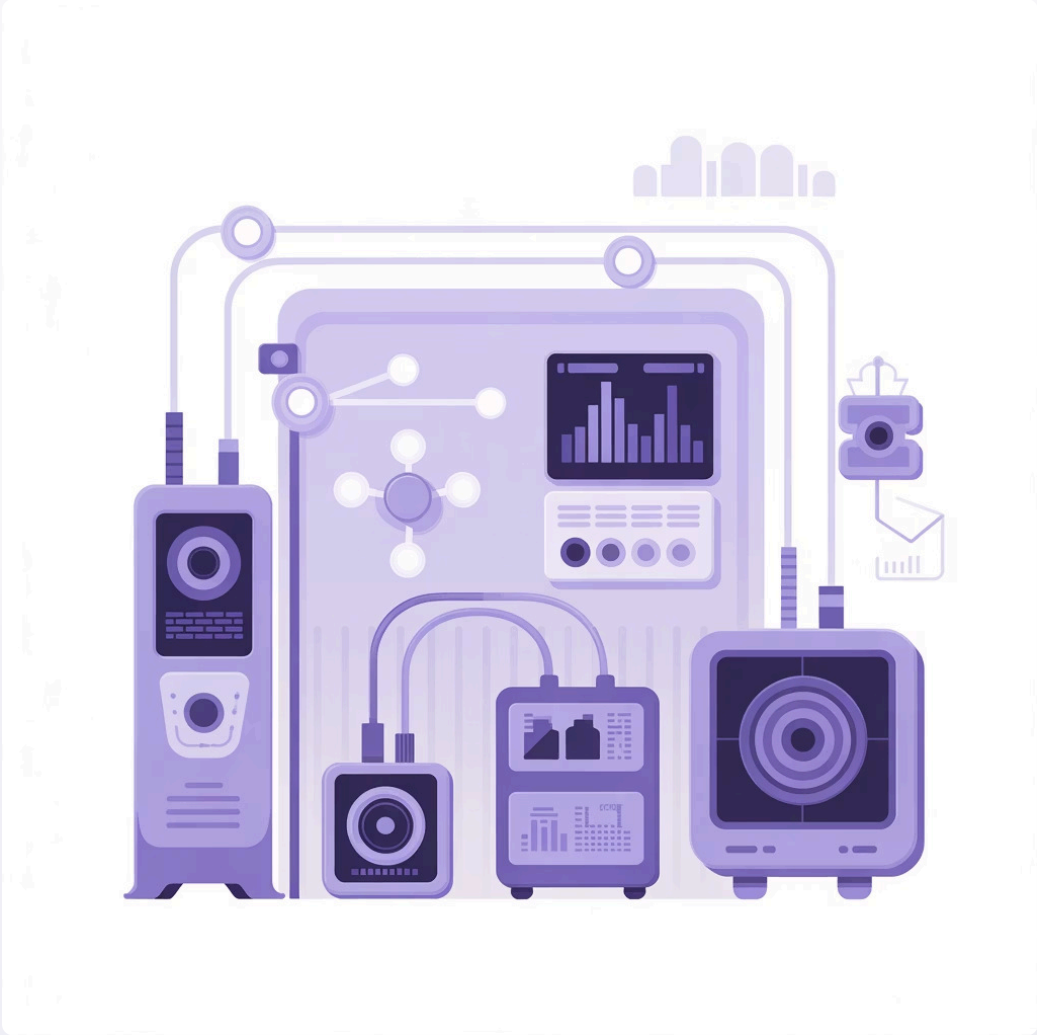


Auditoría de Seguridad en Dispositivos IoT

Evaluación de la seguridad en dispositivos conectados, incluyendo dispositivos industriales, cámaras IP, sensores y routers.

Alcance Completo

- Identificación de firmware vulnerable
- Pruebas de credenciales por defecto
- Análisis de servicios expuestos
- Validación de comunicaciones cifradas
- Explotación de vulnerabilidades conocidas



Metodología General: Enfoque Híbrido

Adoptamos un enfoque híbrido combinando tres referencias principales reconocidas internacionalmente para garantizar auditorías exhaustivas y profesionales.

PTES

Penetration Testing Execution Standard - Define el ciclo completo de auditoría ofensiva, desde la planificación hasta el reporte final

OWASP WSTG

Web Security Testing Guide - Aplicado en auditorías web para pruebas específicas y profundas de aplicaciones

MITRE ATT&CK

Utilizado para alinear ataques simulados con tácticas empleadas por adversarios reales en el mundo

Fases de Cada Auditoría

Reconocimiento

Recolección de información

Enumeración

Identificación detallada

Explotación

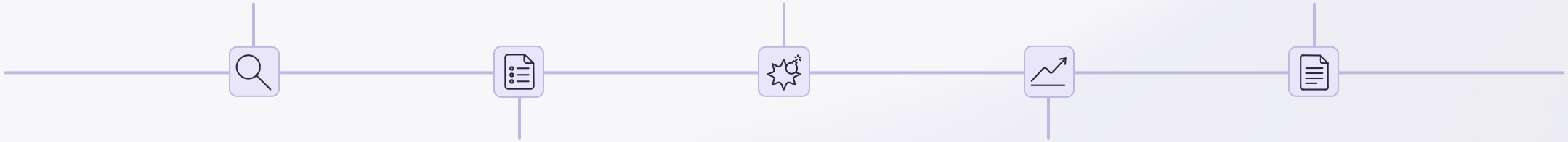
Vulneración de sistemas

Escalada

Obtención de privilegios

Reporte

Documentación final



Clasificación de Tipos de Ataque

La comprensión de los distintos tipos de ataques es fundamental para identificar, evaluar y mitigar vulnerabilidades dentro de una organización.

Ataques Basados en Credenciales

Fuerza bruta: intentos automatizados para adivinar contraseñas usando Hydra o Medusa

Credential Stuffing: reutilización de credenciales filtradas

Ataques a Aplicaciones Web

SQLi: manipulación de consultas SQL

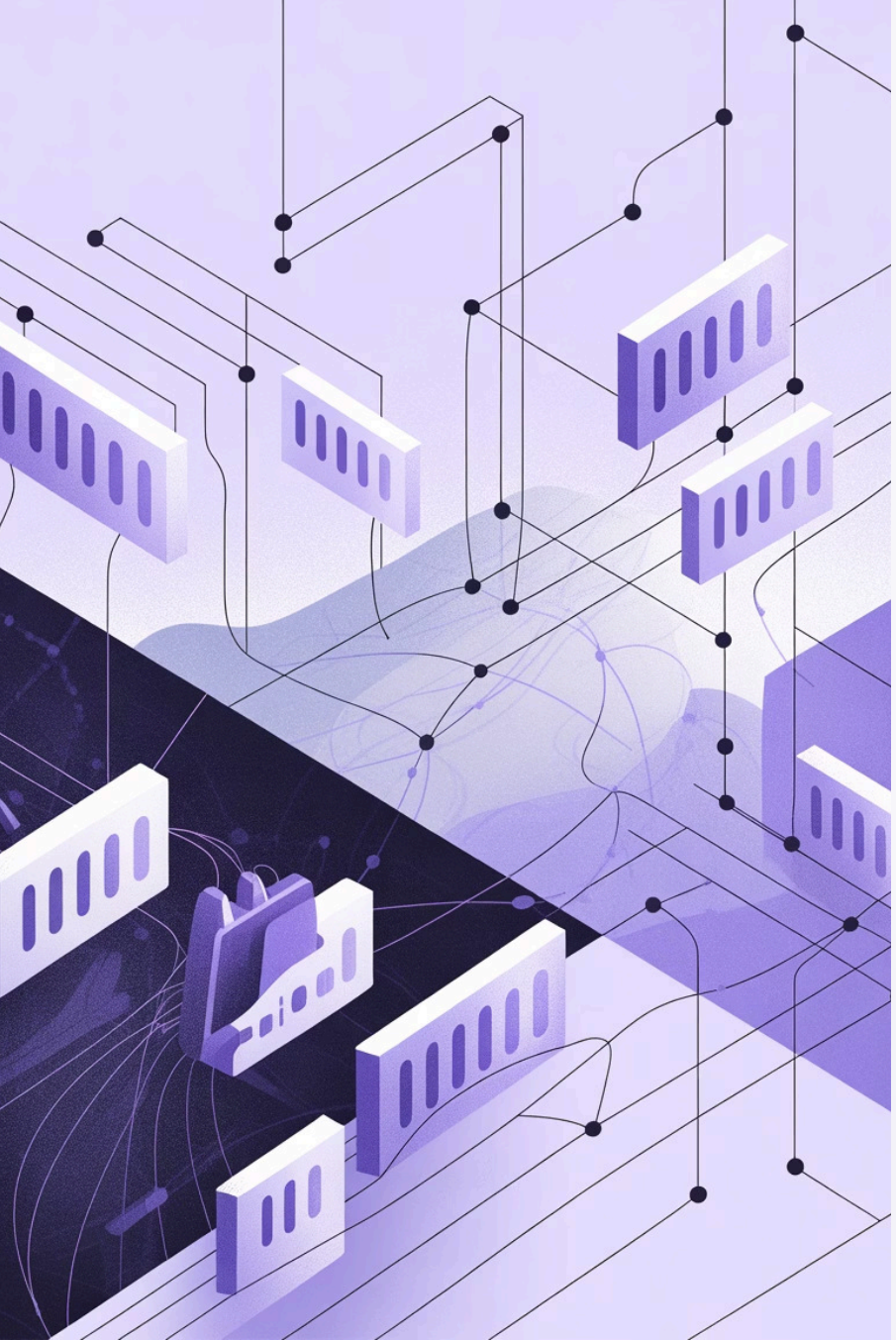
XSS: ejecución de scripts maliciosos

RCE: ejecución remota de código

Ingeniería Social

Phishing: suplantación de identidad

Vishing/Smishing: variantes mediante llamadas o SMS



Ataques a Redes y Dispositivos

Ataques a Redes Internas

- **Sniffing:** captura de tráfico para obtener contraseñas sin cifrar
- **ARP Spoofing:** redirección de tráfico para ataques Man in the Middle
- **Escalada de privilegios:** aprovechamiento de fallos en configuraciones

Ataques a Dispositivos IoT

Incluyen vulnerabilidades por contraseñas por defecto, firmware inseguro o puertos expuestos innecesariamente.

Ciclo Completo de un Ataque Ofensivo

1

Reconocimiento

Recolección pasiva y activa de información sobre el objetivo

2

Enumeración

Identificación detallada de usuarios, servicios activos y versiones

3

Explotación

Ejecución de técnicas para vulnerar sistemas

4

Escalada de Privilegios

Obtención de permisos más altos mediante fallos del sistema

5

Movimiento Lateral

Desplazamiento dentro de la red para comprometer sistemas adicionales

6

Persistencia

Creación de puertas traseras para mantener acceso

7

Exfiltración

Extracción de información sensible

8

Eliminación de Huellas

Borrado de trazas y registros para evitar detección

Comparativa de Metodologías

Metodología	Enfoque Principal	Mejor Uso
OWASP WSTG	Aplicaciones web con casos de prueba detallados	Auditorías web específicas y profundas
PTES	Ciclo completo de pentesting profesional	Auditorías completas de infraestructura
MITRE ATT&CK	Tácticas reales de adversarios	Simulaciones avanzadas de amenazas

Recomendación: Combinación de PTES como estructura general y OWASP WSTG para auditorías web, complementadas con MITRE ATT&CK en simulaciones de amenazas avanzadas.

Herramientas Principales por Servicio

Auditoría Web

Burp Suite, OWASP ZAP, Nmap, SQLMap, Gobuster

Auditoría de Red Interna

Nessus, OpenVAS, Nmap, BloodHound, Mimikatz, Metasploit, Wireshark

Auditoría IoT

Firmware Analysis Toolkit, Nmap, Wireshark, Metasploit, Shodan

Evaluación de Herramientas de Monitorización

Selección de herramientas según funciones, coste, escalabilidad y facilidad de uso para garantizar auditorías efectivas.

Nmap

Escaneo de puertos y servicios - Gratuito y de código abierto

Burp Suite Pro

Auditoría web profesional - Licencia anual 399€

Nessus Pro

Escaneo de vulnerabilidades - Alto nivel de automatización

Wireshark

Captura de tráfico - Gratuito y ampliamente utilizado

Metasploit

Marco completo para explotación y post-explotación

Gobuster

Descubrimiento de recursos web - Rápido y eficiente

Comparativa de Herramientas Clave

Burp Suite vs OWASP ZAP

Burp Suite: interfaz intuitiva, gran potencia en pruebas web, versión Pro con funcionalidades avanzadas

OWASP ZAP: alternativa gratuita y de código abierto, ideal para presupuestos limitados

Nessus vs OpenVAS

Nessus: fácil de usar, alto nivel de automatización, soporte comercial

OpenVAS: alternativa gratuita, con curva de aprendizaje mayor pero muy completa

Estimación de Inversión

La inversión depende del tamaño del equipo y servicios ofrecidos. A continuación se presentan los costes aproximados para establecer un servicio profesional de auditoría ofensiva.

399€

Burp Suite Pro

Licencia anual por usuario

3.000€

Nessus Pro

Licencia anual completa

1.500€

Hardware Específico

Equipos especializados

800€

Formación Anual

Actualización de conocimientos

Resultados y Entregables

Informe Técnico Detallado

Vulnerabilidades clasificadas por criticidad con evidencias técnicas completas del impacto

Recomendaciones de Mitigación

Propuestas precisas y accionables para resolver cada vulnerabilidad identificada

Inventario de Activos

Mapeo completo de la infraestructura evaluada y vectores de ataque identificados

Ventajas de Nuestro Enfoque

Metodologías Reconocidas Internacionalmente

Utilizamos estándares como PTES, OWASP WSTG y MITRE ATT&CK para garantizar evaluaciones exhaustivas y alineadas con las mejores prácticas del sector

Herramientas Profesionales de Última Generación

Combinamos herramientas comerciales y de código abierto para obtener resultados completos y precisos en cada auditoría

Perspectiva de Atacante Real

Simulamos amenazas reales para identificar vulnerabilidades críticas antes de que sean explotadas por adversarios maliciosos

Informes Accionables y Detallados

Proporcionamos documentación técnica completa con recomendaciones específicas para fortalecer la postura de seguridad

Fortalezca su Seguridad

Proteja su Organización

Los servicios de auditoría ofensiva aquí descritos permiten evaluar la seguridad de una organización desde la perspectiva de un atacante real. El uso de metodologías internacionales y herramientas reconocidas garantiza un análisis exhaustivo y profesional, orientado a identificar vulnerabilidades críticas y a fortalecer la postura de seguridad del cliente.

El conocimiento de los principales tipos de ataques, sus fases y las herramientas adecuadas contribuye a realizar evaluaciones exhaustivas y alineadas con estándares del sector.

Solicitar Auditoría | Más Información