Everyone should ***feel secure*** online.

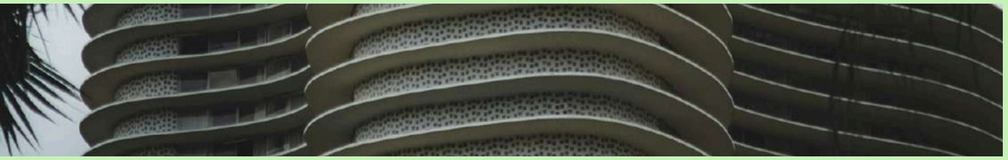
We emulate threat ***adversaries.***

Al llevar a cabo simulaciones de ataques reales, las organizaciones tienen la oportunidad de descubrir y abordar vulnerabilidades en sus sistemas antes de que los ciberdelincuentes actúen.

Esta estrategia preventiva no solo es crucial para resguardar la información confidencial y los activos intelectuales, sino que también constituye una defensa esencial contra los riesgos financieros y el deterioro de la imagen corporativa.

Las pruebas de penetración son cruciales para cumplir con los estándares regulatorios y de conformidad, ya que ofrecen una demostración concreta del compromiso de una organización con la seguridad.

Mediante la realización periódica de estas pruebas, las organizaciones pueden evaluar de manera continua su postura de seguridad, perfeccionar sus estrategias de defensa y mantener una posición resiliente frente a las amenazas cibernéticas en constante evolución.



Nuestro ***enfoque.***

HAWKTESTERS es una empresa especializada en ciberseguridad, redes empresariales, gestión de riesgos de TI. Con una expertiz extensa en penetration testing para negocios de todos los tamaños.

Nuestras pruebas pueden cubrir cada aspecto de su red y sistemas, incluidas las pruebas de seguridad y garantía para aplicaciones personalizadas. Identificamos y reportamos vulnerabilidades y riesgos en un formato claro y priorizado, con recomendaciones.

El enfoque de pruebas de penetración de HAWKTESTERS está estrechamente alineado con las directrices del Open Web Application Security Project OWASP . Para proporcionar un resultado consistente, repetible y de alta calidad, utilizamos una serie de metodologías dependiendo de la organización y los objetivos. Estas incluyen estándares bien definidos como:

OWASP Top 10 (Web, Mobile, y API)

OSSTMM

NIST

MITRE ATT&CK

Beneficios *claves.*

1.

Valide su ciberseguridad en toda su superficie de ataque y alinee la gestión de vulnerabilidades con los objetivos comerciales clave.

2.

Informes priorizados y accionables para guiar la remediación de vulnerabilidades y la gestión de riesgos.

3.

Obtenga un entendimiento de las fortalezas y debilidades en la gestión de sus sistemas para guiar la continua mejora del proceso de seguridad.

4.

La revalidación de las pruebas asegura que las remediaciones se apliquen y las brechas de seguridad se cierren.

5.

Cumpla con las regulaciones incluyendo la privacidad y seguridad de datos, para construir la confianza del cliente y proteger su organización de sanciones.

1 Evaluación de aplicaciones web.

Las pruebas web se basan en las metodologías de la industria del Open Web Application Security Project (OWASP) así como en el Common Weakness Enumeration (CWE) Top 25.

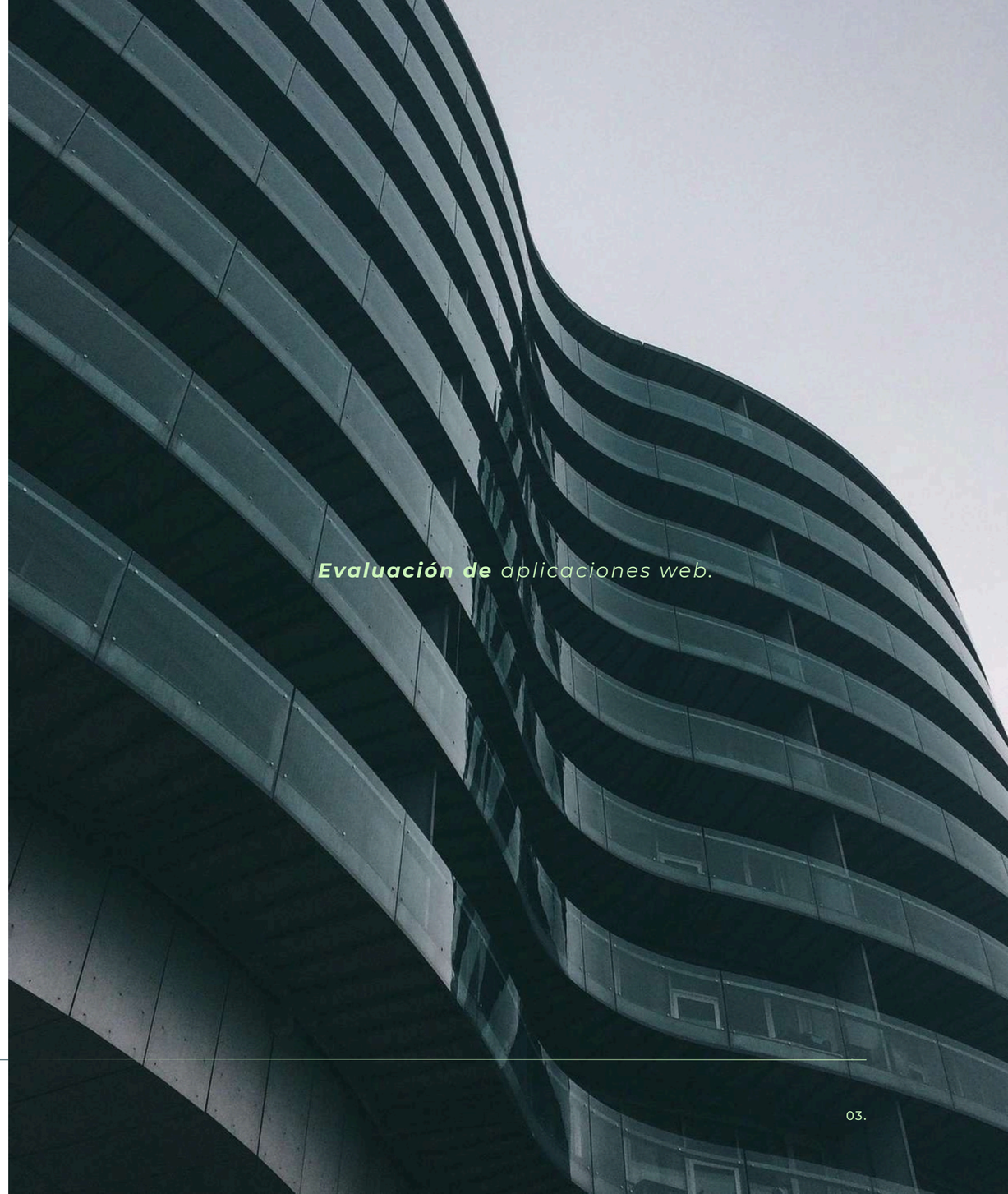
Los resultados de las pruebas de aplicaciones son indicadores valiosos de las habilidades y las lagunas en el desarrollo de aplicaciones internas, brindando oportunidades para la capacitación y la mejora de herramientas frente a problemas futuros.

Con cada prueba utilizando el mismo flujo de trabajo y prácticas, incluyendo un extenso proceso de control de calidad realizado por un probador senior, puede estar seguro de obtener resultados exhaustivos y consistentes.

Inclusiones

Hawktesters puede probar todas sus aplicaciones web, ya sean:

- Sitios pequeños de tipo folleto, Wordpress o similares.
- Aplicaciones web de tamaño mediano
- Aplicaciones web grandes y complejas



***Evaluación de** aplicaciones web.*

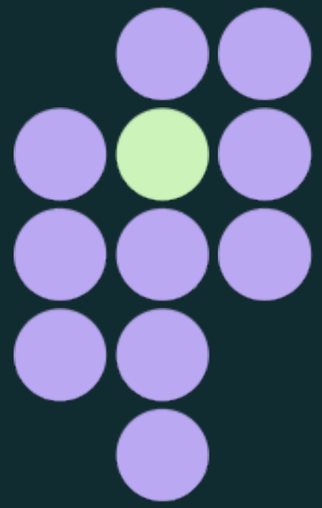
2 *Evaluación de seguridad* inalámbrica (Wireless)

Las redes inalámbricas pueden proporcionar una superficie de ataque que se extiende mucho más allá del límite físico de las instalaciones de una organización. Esto las convierte en un objetivo atractivo para un atacante determinado.

Inclusiones

Las auditorías de seguridad inalámbrica se enfocan en los siguientes componentes:

- ***Entorno inalámbrico:*** Escaneo y descubrimiento.
- ***Infraestructura inalámbrica:*** Revisión de la configuración de dispositivos
- ***Infraestructura inalámbrica:*** Evaluación de la implementación y operaciones
- Validación de la segregación de la red entre redes inalámbricas, como las redes de invitados y corporativas
- Después de completar la revisión inicial y abordar cualquier problema, esto formará una línea base de seguridad

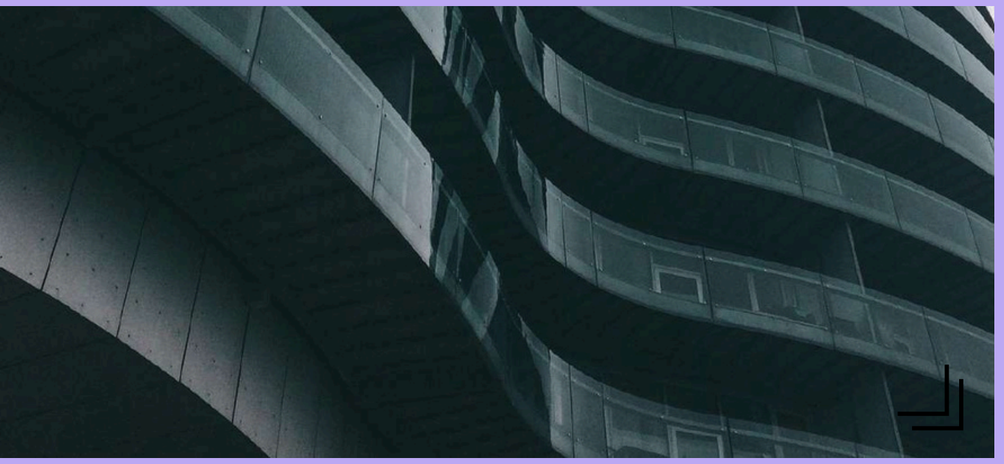


3.Evaluación de *seguridad de API*

Nuestro enfoque se basa en las directrices de la industria del Open Web Application Security Project OWASP para la pruebas de API.

Inclusiones

Las pruebas pueden realizarse de manera independiente (usando una especificación de Postman o Open API o como parte de una prueba más amplia que incluya la aplicación web u otro cliente de API.
Todas las pruebas se realizan conforme a las mejores prácticas de la industria, y los hallazgos se mapean con el último OWASP API Top 10.



4. Evaluación de *configuración de host*

La evaluación de configuración de host considera la configuración de dispositivos de servidores específicos (y aplicacio-nes de soporte) u otros dispositivos.

Inclusiones

Las áreas de enfoque y revisión durante esta actividad pueden incluir:

- **Actualizaciones y parches del sistema operativo (o equivalente)**
- **Configuraciones predeterminadas**
- **Permisos del sistema de archivos**
- **Configuración incorrecta y vulnerabilidades conocidas con servicios instalados**
- **Superficie de ataque minimizada (no se ejecutan servicios innecesarios)**
- **Comparación contra una línea base proporcionada / configuraciones documentadas**
- **Acceso a datos sensibles, como archivos de configuración que contienen credenciales**

5 *Evaluación de seguridad* móvil (Android & iOS)

Inclusiones

Dado que muchas aplicaciones se entregan actualmente a través de dispositivos móviles, cumplimos con sus requisitos de pruebas de seguridad, ya sean nativas, web o híbridas.

Todas las pruebas se realizan conforme a las mejores prácticas de la industria, y los hallazgos se mapean con el último OWASP Mobile Top 10.

6 *Prueba de penetración de red interna*

Inclusiones

Este se realiza típicamente bajo uno de los tres enfoques siguientes:

- Prueba basada en objetivos, donde se proporciona al probador una cuenta de usuario estándar dentro de la red, y tiene el objetivo de obtener acceso a un objetivo acordado (como Active Directory, DatosFinancieros o de Clientes).
- Vivir del terreno (Living off the Land - LoL) donde se le proporciona al probador acceso a la red interna, y luego utiliza herramientas y técnicas estándar para acceder a los sistemas, explorando vulnerabilidades identificadas y oportunidades de movimiento lateral.
- Evaluación de vulnerabilidad, donde todos los objetivos dentro del alcance son escaneados utilizando herramientas líderes en la industria, y todos los hallazgos son revisados manualmente y categorizados para ayudar a evaluar el riesgo general.

7 *Prueba de penetración* de red externa

La prueba de penetración de red externa evalúa la postura de seguridad de la infraestructura expuesta a Internet en general.

Inclusiones

Esto se realiza en dos categorías amplias:

- Escaneo automatizado: escanea todos los servicios expuestos en busca de configuraciones incorrectas o vulnerabilidades conocidas.
- Pruebas manuales: aplica técnicas de prueba manuales y experiencia para revisar los hosts y servicios expuestos. Los activos identificados son analizados usando una variedad de herramientas para identificar puertos abiertos, servicios y vulnerabilidades.

Las áreas de enfoque y revisión incluyen:

- Configuraciones incorrectas de infraestructura
- Vulnerabilidades conocidas relacionadas con servicios expuestos
- Configuraciones de certificados SSL
- Análisis de resultados de herramientas de evaluación de seguridad de red como Nessus y Nmap
- Análisis manual de las vulnerabilidades reportadas para evaluar la explotabilidad y la criticidad

8 *Simulación de* adversarios (Red Team)

Planificación, coordinación, ejecución, evaluación, análisis y reporte de ataques simulados del mundo real utilizando técnicas de equipo rojo, TTPs y la metodología TIBER-EU.
Empleamos herramientas de ataque y penetración para evaluar de manera encubierta los controles tecnológicos y procesos de la organización frente a amenazas como phishing, malware y ataques a aplicaciones o infraestructura, garantizando una evaluación integral y alineada con los estándares europeos de ciberseguridad.

Inclusiones

Al llevar a cabo un ejercicio de equipo rojo, simulamos un ataque real dirigido a objetivos críticos para sus operaciones actuales y futuras. Este proceso permite evaluar la preparación de su organización frente a amenazas avanzadas, mejorar su postura de seguridad y proporcionar recomendaciones y oportunidades de aprendizaje para optimizar la respuesta a incidentes de seguridad.

Se espera que este compromiso siga un enfoque por fases:

- **Planificación y preparación**
- **Obtención de un punto de apoyo inicial (actividades de ataque externo)**
- **Identificación de caminos internos hacia los objetivos específicos**
- **Obtención de objetivos (actividades de ataque interno)**
- **Incremento del 'ruido' para intentar validar la respuesta del equipo azul**
- **Reporte**
- **Equipo púrpura (opcional)**
- **Capacitación en conciencia de seguridad para empleados (opcional)**

9 *Revisión de código* de aplicaciones

Hawktesters puede realizar revisiones centradas en la seguridad de aplicaciones desarrolladas utilizando una amplia variedad de lenguajes y plataformas, aplicando las metodologías OWASP ASVS y NIST-SSIF.

Inclusiones

- Revisión manual de alto nivel donde se busca en el código problemas y debilidades de seguridad comunes.
- Evaluaciones de escaneo de código usando herramientas SAST o DAST.
- Identificación de debilidades y vulnerabilidades de seguridad a nivel de código fuente y demostración de cómo estas resultan en defectos de seguridad.
- Revisión de código adicional para aplicaciones que funcionan en bases de código y marcos antiguos para identificar nuevas y emergentes clases de vulnerabilidades de codificación.

10 *Revisión de seguridad* de servicios en la nube (Cloud)

Evaluación de seguridad de servicios basados en la nube (SaaS/PaaS/IaaS) como AWS, Azure y O365 basada en una revisión de configuración e implementación.

Inclusiones

- Revisar la configuración y opciones contra las mejores prácticas del proveedor y la industria.
- Examinar las prácticas y la efectividad de la administración de usuarios y grupos.
- Analizar las medidas de protección de datos.
- Evaluar las políticas de servicio
- Documentación y reporte de resultados con recomendaciones accionables.

11 *Campañas* de Phishing

Ofrecemos un servicio integral de campañas de phishing diseñado para evaluar y mejorar la conciencia de seguridad de los empleados en su organización.
El objetivo de estas campañas es proporcionar una medición realista del nivel de conciencia de seguridad entre los empleados, identificar áreas de mejora y fortalecer las defensas de la organización contra tácticas engañosas.

Inclusiones

Phishing: Realizamos campañas de correo electrónico simuladas para medir la respuesta de los empleados ante intentos de phishing, proporcionando una visión clara de la vulnerabilidad organizacional a este tipo de ataques.

Vishing: Implementamos pruebas de ingeniería social por teléfono para evaluar cómo los empleados responden a las solicitudes verbales de información sensible o acciones que podrían comprometer la seguridad.

Smishing: Enviamos mensajes de texto que imitan tácticas utilizadas por ciberdelincuentes para determinar la susceptibilidad de los empleados a ataques SMS phishing.

12 *Capacitaciones de* desarrollo seguro

Hawktesters puede realizar revisiones centradas en la seguridad de aplicaciones desarrolladas utilizando una amplia variedad de lenguajes y plataformas.

Inclusiones

Capacitación en Desarrollo Seguro según ASVS:

Adoptamos el estándar ASVS de OWASP para proporcionar una base sólida en prácticas de seguridad durante el desarrollo de aplicaciones, asegurando que los equipos comprendan y puedan implementar los requisitos de seguridad necesarios.

Sesiones interactivas y prácticas:

Las capacitaciones están diseñadas para ser dinámicas, con ejercicios prácticos y análisis de casos reales que permiten aplicar los conocimientos en escenarios concretos.

Contenido actualizado y relevante:

Aseguramos que el contenido de la capacitación refleje las últimas tendencias y amenazas en el ámbito de la ciberseguridad, preparando a los equipos para enfrentar desafíos actuales.

Evaluación del aprendizaje y mejora continua:

Medimos el progreso y la comprensión de los temas tratados, ofreciendo una retroalimentación detallada y sugerencias para el fortalecimiento de las habilidades y los conocimientos

13 Pruebas de Hardware Hacking

Los dispositivos físicos, como routers, dispositivos IoT, SCADAs y PLCs, suelen pasarse por alto, pero son tan vulnerables como cualquier otro activo.

Inclusiones

Esto se realiza en tres categorías amplias:

- **Evaluación Física**: Evaluamos la resistencia de tu hardware contra ataques físicos utilizando técnicas como ataques de canal lateral, ingeniería inversa y pruebas de manipulación.
- **Evaluación de interfaces de comunicación**: Analizamos canales de comunicación inalámbricos y cableados para detectar vulnerabilidades, evaluando protocolos, identificando vectores de ataque y proponiendo soluciones.
- **Evaluación de firmware y software**: Análisis estático y dinámico, buscando vulnerabilidades, realizando ingeniería inversa y evaluando la seguridad general de tu sistema.

Las áreas de enfoque y revisión incluyen:

- Detectamos fugas de información por variaciones de energía y emisiones electromagnéticas.
- Evaluamos la capacidad del hardware para resistir aperturas y alteraciones físicas.
- Inspeccionamos la seguridad de Bluetooth, Wi-Fi, Ethernet y otros protocolos.
- Descompilamos y analizamos firmware para identificar puertas traseras y evaluar su integridad.
- Detectamos y mitigamos riesgos de ejecución no autorizada y explotación de vulnerabilidades.

Informes y análisis ↘

Nuestro informe estándar incluye un resumen **ejecutivo y técnico** de los hallazgos, junto con:

↘ Una descripción detallada de cada resultado

↘ Las clasificaciones de riesgo asociadas

↘ Las recomendaciones para resolver la vulnerabilidad.

*Además, organizamos una **sesión** virtual para compartir y **discutir los hallazgos** con el equipo técnico de la empresa, así fomentando un enfoque colaborativo en la **mitigación de riesgos**.*

Nuestras credenciales en pruebas de penetración ↘

Hawktesters se distingue por su alta especialización y por sus ***25 años*** de experiencia acumulada en pruebas de penetración y Ethical Hacking.

Nuestro equipo posee una amplia gama de certificaciones reconocidas en la industria, incluyendo: **OSCE**, **OSWE**, **OSCP**, **OSEP**, **OSWA**, **eWPTXv2**, **PNPT**, etc...