NETPLOY
SECURITY

Servicios de seguridad

Netploy Security

Defendiendo tu mundo digital

https://www.netploysecurity.com

Pruebas de penetración

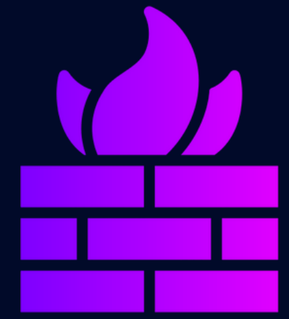
Nuestro servicio principal

Las pruebas de penetración, a menudo denominadas "pen testing", son una práctica de ciberseguridad que consiste en simular ciberataques contra un sistema informático, una red o una aplicación para identificar vulnerabilidades y puntos débiles. El objetivo principal de las pruebas de penetración es evaluar la seguridad del objetivo y proporcionar información procesable para mejorar sus defensas. Los profesionales cualificados en ciberseguridad, conocidos como penetration testers, utilizan diversas herramientas y técnicas para imitar las amenazas del mundo real e intentar explotar los fallos de seguridad. Los resultados de una prueba de penetración ayudan a las organizaciones a reforzar sus medidas de seguridad y a protegerse contra posibles ciberamenazas y violaciones de datos.

1 Pruebas de penetración internas

Durante un pentesting de infraestructura interna, los profesionales de seguridad utilizan diversas técnicas y herramientas para simular ataques reales que podrían ser realizados por un atacante interno o un empleado malintencionado. El objetivo principal es descubrir fallos de seguridad antes de que sean aprovechados por personas no autorizadas.

- Análisis de la configuración de redes internas y segmentación de red.
- Revisión de la seguridad de los sistemas de autenticación y autorización internos.
- Evaluación de las políticas de contraseñas y su cumplimiento.
- Pruebas de vulnerabilidades en sistemas operativos y aplicaciones de escritorio.
- Análisis de la seguridad de los sistemas de gestión de bases de datos internos.
- Evaluación de la seguridad de los servidores de aplicaciones internas.
- Revisión de la configuración de firewalls y sistemas de detección y prevención de intrusiones (IDS/IPS).
- Pruebas de seguridad en servicios internos, como correo electrónico, transferencia de archivos y comunicaciones internas.
- Análisis de la seguridad de las aplicaciones web internas y posibles vectores de ataque.
- Evaluación de la seguridad de los sistemas de almacenamiento y respaldo de datos.
- Revisión de los permisos y controles de acceso a archivos y carpetas internas.
- Pruebas de vulnerabilidades en sistemas de virtualización y contenedores.
- Revisión de las políticas de seguridad interna y su cumplimiento.



2 Pruebas de penetración externas

Nuestro equipo de seguridad puede auditar toda su infraestructura que esté expuesta ante internet simulando un hacker que desea ingresar a los sistemas de la empresa y que se encuentre en cualquier parte del mundo.

- Identificación de puertos abiertos y servicios expuestos.
- Evaluación de la seguridad de los servicios web y aplicaciones en línea.
- Búsqueda de vulnerabilidades en protocolos de red. Análisis de la robustez de las contraseñas y políticas de autenticación.
- Examen de la seguridad de los servidores de correo electrónico.
- Pruebas de seguridad en servicios de transferencia de archivos (FTP, SFTP, etc.).
- Evaluación de la seguridad de servicios en la nube y aplicaciones web alojadas.
- Análisis de la seguridad de sistemas de gestión de bases de datos.
- Análisis de la configuración de sistemas operativos y aplicaciones de servidor.
- Pruebas de vulnerabilidades conocidas y explotación de las mismas.
- Búsqueda de agujeros de seguridad en sistemas de autenticación y autorización.
- Revisión de la seguridad de la infraestructura de red y arquitectura de red.

Pruebas de penetración en Apps móviles

Sabemos que las aplicaciones móviles son una parte fundamental de muchas empresas, pero la seguridad de estas aplicaciones móviles a menudo se pasa por alto. Nuestro equipo de expertos en seguridad informática está aquí para ayudarte a proteger tu aplicación móvil de posibles amenazas de seguridad.

- Autenticación y autorización: Evaluación de la seguridad de los mecanismos de autenticación y autorización utilizados en la aplicación móvil, incluyendo la fortaleza de las contraseñas, la protección contra ataques de fuerza bruta y la adecuada gestión de tokens de acceso.
- Comunicaciones seguras: Evaluación de la seguridad de las comunicaciones entre la aplicación móvil y los servidores remotos, verificando el uso de protocolos seguros (como HTTPS) y la implementación adecuada de certificados SSL/TLS.
- Integridad y protección de la aplicación: Verificación de la integridad de la aplicación móvil, incluyendo la prevención de modificaciones no autorizadas, la detección de malware y la implementación de firmas digitales para verificar la autenticidad de las actualizaciones.
- Almacenamiento seguro de credenciales: Evaluación de cómo se almacenan y protegen las credenciales de acceso, como nombres de usuario y contraseñas, en el dispositivo móvil, evitando el acceso no autorizado.
- Análisis de código estático y dinámico: Revisión del código fuente de la aplicación móvil en busca de vulnerabilidades conocidas y potenciales, así como pruebas dinámicas para detectar posibles fallos de seguridad durante la ejecución.
- Prevención de ataques de seguridad en el dispositivo: Evaluación de la protección de la aplicación móvil contra ataques comunes dirigidos al dispositivo, como el rooting o jailbreaking, la extracción no autorizada de datos o la manipulación del comportamiento de la aplicación.

4 Pruebas de penetración en aplicativos webs

A través de pruebas rigurosas descubrimos posibles debilidades que podrían ser explotadas por actores maliciosos. Nuestro enfoque integral garantiza que sus aplicaciones web y API estén fortificadas contra amenazas comunes, protegiendo sus datos sensibles y asegurando la confianza de sus usuarios.

- Autenticación y autorización: Evaluación de la seguridad de los mecanismos de autenticación y autorización de la aplicación, incluyendo la robustez de las contraseñas, la gestión de sesiones y los controles de acceso.
- Inyección de código: Búsqueda de vulnerabilidades de inyección de código, como inyecciones SQL, inyecciones de comandos y XSS (Cross-Site Scripting), para garantizar que la aplicación esté protegida contra estas amenazas.
- Validación de entrada: Verificación de que la aplicación realiza una adecuada validación y filtrado de los datos de entrada, evitando así ataques como la inyección de código malicioso o la manipulación de parámetros.
- Manejo de sesiones: Evaluación de la seguridad de la gestión de sesiones, incluyendo la generación de tokens, la protección contra secuestro de sesiones (session hijacking) y la expiración adecuada de sesiones inactivas.
- Control de acceso: Análisis de los controles de acceso implementados en la aplicación para garantizar que los usuarios solo puedan acceder a los recursos y funcionalidades a los que están autorizados.
- Vulnerabilidades conocidas: Búsqueda de vulnerabilidades conocidas en la aplicación y sus componentes, como bibliotecas o frameworks utilizados, y aplicación de parches o soluciones apropiadas.

Nuevo servicio

Ciberinteligencia

Proteger la información sensible de tu empresa es fundamental para salvaguardar tu reputación y evitar pérdidas financieras. Nuestro servicio de investigación de datos confidenciales está diseñado para identificar cualquier información comprometida relacionada con tu empresa y empleados, incluyendo contraseñas, datos financieros y otros activos críticos.

- Búsqueda de foros de la **dark web** en busca de información relacionada con la empresa, como credenciales de empleados, contraseñas filtradas o datos de acceso comprometidos.
- Verificación de la existencia de ventas o intercambios de información confidencial de la empresa.
- Identificación de indicios de que las credenciales robadas corresponden a empleados de la empresa.
- Monitoreo de bases de datos públicas y privadas de contraseñas filtradas en busca de credenciales de correo electrónico y otros servicios asociados con la empresa.
- Verificación de la autenticidad de las credenciales filtradas y su posible relación con empleados de la empresa.
- Intentos de inicio de sesión no autorizados en servicios corporativos utilizando credenciales filtradas.

Otros servicios

Análisis de vulnerabilidades en código fuente

Nuestro equipo de expertos en seguridad realiza una exhaustiva revisión del código fuente, utilizando herramientas avanzadas y técnicas de revisión manual para detectar vulnerabilidades como errores de programación, posibles puertas traseras, problemas de seguridad de datos y más.

Capacitación en desarrollo de código seguro

Nuestro programa de formación en desarrollo seguro ofrece a sus desarrolladores las habilidades y conocimientos necesarios para integrar prácticas de seguridad desde el principio del ciclo de desarrollo de software.

Capacitación en ataques a infraestructura

Aprende a evaluar la seguridad de servidores, software y redes, adquiriendo habilidades avanzadas para identificar y mitigar vulnerabilidades, garantizando la protección de tus sistemas mientras fortaleces tus habilidades en seguridad informática.

Charla de concientización sobre ciberseguridad

Nuestra charla de concientización sobre ciberseguridad está diseñada para empoderar a su personal o audiencia con el conocimiento necesario para tomar decisiones seguras en línea y proteger los activos digitales de su organización.

Lo que nos diferencia del resto

Disponemos de las certificaciones más exigentes relacionadas con las pruebas de penetración: OSWE (Offensive Security Web Expert), OSCP (OffSec Certified Professional), eCPPTv2 (eLearnSecurity Certified Professional Penetration Tester), eMAPT (Mobile Application Penetration Tester), eWPTX (Web application Penetration Tester eXtreme), Burp Certified Practitioner, CPTE (Certified Penetration Testing Engineer), 7asecurity Mobile Certification and CEH (Certified Ethical Hacker).

OFFENSIVE security

INE

PortSwigger

NETPLOY
SECURITY

Conecta con nosotros.

Email
info@netploysecurity.com

X
@NetploySecurity