ESET CYBERSOC

ETHICAL HACKING

Servicios de EH confiables para mantener los sistemas corporativos seguros

Wifi Penetration Test

Wifi Penetration Test

Un WIFI Penetration Test es una técnica utilizada para evaluar la seguridad de los recursos y activos de la organización desde el punto de vista de la materia de seguridad en redes inalámbricas (2,4GHZ y 5GHZ)

Esta técnica no solo identifica las vulnerabilidades existentes en la infraestructura WIFI, sino que ejecuta un análisis con profundidad. Específicamente, se busca además de la identificación, la explotación de las vulnerabilidades y de esa manera se observa el impacto real sobre la organización por medio de esta.

Este tipo de servicio se realiza de manera interna, en donde se busca identificar y explotar las vulnerabilidades que sean visibles desde un escenario con acceso a los recursos y activos de la organización mientras.

Objetivos principales

- ✓ Obtener una fotografía del estado de la seguridad que la organización, sistema u objetivo WIFI en un momento determinado.
- ✓ Visualizar su compañía desde el punto de vista del atacante, localizando debilidades, vulnerabilidades y puntos de acceso no autorizados, antes que lo hagan los atacantes.
- ✓ Comprobar el verdadero impacto de las vulnerabilidades en su entorno particular.
- ✓ Comprobar si el nivel de protección existente se condice con la política de seguridad establecida por la organización.
- ✓ Comprobar la efectividad de sus medidas de protección, políticas y procesos de detección de intrusos y respuesta a incidentes.

¿Por qué realizar un Wifi Penetration Test?

- ✓ Para conocer el estado de la seguridad de una organización (especialmente si nunca se realizó una auditoría de estas características), referido a redes inalámbricas.
- ✓ Para saber el estado actual de los dispositivos implementados en la organización.
- ✓ Para establecer un punto de partida y comenzar a gestionar la seguridad de la organización.
- ✓ Para constituir un ciclo de revisión y mejora para la seguridad inalámbrica de manera continua.

Las etapas asociadas a este servicio son:

- ✓ Reconocimiento de Routers y Access Point
- ✓ Análisis y detección de Vulnerabilidades asociadas a los Routers y Access Point
- ✓ Explotación de vulnerabilidades
- ✓ Armado y presentación de reportes

Reportes

En este servicio se generan 2 entregables o reportes que ayudan y guían al cliente en el proceso de remediación de vulnerabilidades.

El primero de ellos, el **Informe Ejecutivo**, describe el nivel de riesgo de la compañía sin entrar en detalles técnicos, evidenciando las problemáticas por medio de conceptos claros y gráficas.

El segundo reporte, el **Informe Técnico**, apunta al área técnica de la empresa, ayudando al personal de TI a solucionar los problemas detectados.

En este reporte se muestran todas las evidencias de los tests ejecutados de manera tal que todas las tareas sean repetibles y transparentes para el cliente.


ESET CYBERSOC