PENTESTING INTERNO

Pentesting Interno

Descripción

Nuestro servicio de Pentesting Interno permite evaluar la seguridad de tu organización frente a atacantes internos en tu organización. El foco principal de nuestro servicio de pentesting interno es evaluar que tan probable es para un atacante tener acceso a activos internos de tu organización o empresa mediante movimiento lateral desde un sistema organizacional. Todas las pruebas realizadas en el presente servicio son coordinadas y programadas con el cliente para no levantar falsos positivos.

Las pruebas realizadas en nuestro servicio de Pentesting Interno se realizan de forma manual y con herramientas automatizadas.

- ✓ Esta evaluación simula un ataque interno a la organización, ejecutando vectores de ataques reales.
- ✓ Los ejercicios de Pentesting tienen como objetivo identificar potenciales vulnerabilidades en la red y plataforma del cliente.
- ✓ Las vulnerabilidades detectadas son explotadas, con el fin de evidenciar el impacto real y nivel de riesgo.
- ✓ Formular medidas de mitigación e iniciativas de ciberseguridad.

Objetivos

- ✓ Obtener posibles riesgos en la organización o empresa frente a ataques internos mediante movimiento lateral en la organización.
- ✓ Analizar posibles vectores de ataques y servicios expuestos internamente.
- ✓ Entregar un panorama acerca de las vulnerabilidades encontradas para tomar medidas a corto, mediano y largo plazo.
- ✓ Disminuir el tiempo y esfuerzo para afrontar posibles situaciones de riesgo.

Método

- ✓ Todas las pruebas realizadas se basan en la guía técnica NIST SP 800-115, OWASP, MITRE y marcos de pruebas personalizados.
- ✓ Descubrimiento mediante escaneo y enumeración (utilizando técnicas de OSINT y descubrimiento activo) para identificar posibles vulnerabilidades, áreas débiles y exploits.
- ✓ Obtención de accesos a plataformas y movimiento lateral con el fin de lograr el objetivo definido.
- ✓ Comunicación continua con contraparte técnica.

Entregables

- ✓ Informe de Pentesting Interno que incluye lo siguiente:
  - identificación de amenazas por nivel de riesgo.
  - Si es necesario, una presentación ejecutiva de resultados.
  - Recomendación de mitigaciones por amenaza detectada.
  - PoC de vulnerabilidades explotadas.
  - Evidencia de componentes afectados.

Alcance

- ✓ Un objetivo de éxito a definir en conjunto con cliente (como, por ejemplo, tomar el control del Active Directory).
- ✓ El plazo de ejecución de los servicios será de cuatro semanas.
- ✓ Se ejecutará de forma remota vía conexión VPN.
- ✓ Se provee un informe de resultados, acciones de mitigación y los detalles de los hallazgos.
- ✓ El servicio se realiza en modalidad de caja gris.

Metodología del servicio

Fase I. Modo Pasivo

- ✓ El objetivo de esta fase consiste en comprender los servicios expuestos internamente e identificar los posibles vectores de ataque que componen la organización evaluada

Fase II. Modo Activo

- ✓ Recolección de Información, Pruebas de: Gestión de configuración, Gestión de Identidad, Autenticación y Autorización, Gestión de Sesión, Validación de Entradas, Pruebas de Lógica de Negocio, Explotaciones de vulnerabilidades previa autorización del cliente, etc.

Fase III. Reporte

- ✓ Se genera un reporte con la siguiente información. Nombre de los dispositivos evaluados, descripción de servicios expuestos, Vectores de ataque, Vulnerabilidades descubiertas, Resultados de la explotación con evidencia de éxito, Impacto de las vulnerabilidades, Medidas de mitigación de vulnerabilidades.