TEST DE INTRUSIÓN

El **Test de Intrusión Interno** tiene como objetivo evaluar la seguridad de los sistemas frente a un posible ataque interno, es decir, analizar los riesgos procedentes de empleados que podrían violar la seguridad interna de los sistemas de información de la propia organización.

El **Test de Intrusión Externo** tiene como objetivo la evaluación de los niveles de seguridad asociados a los servicios y aplicativos publicados en Internet sobre un rango de direcciones acotadas en el alcance y definidas por el cliente, con el fin de identificar posibles vulnerabilidades que pudieran afectar a su operativa normal o que pudieran revelar información sensible o provocar accesos no autorizados.

NUESTRO SERVICIO

La consultoría para la realización de **Test de Intrusión Interno** es un servicio orientado a organizaciones que basan parte de su actividad en datos confidenciales que no deben ser accesibles por todo el personal interno y que si fueran filtrados podrían causar problemas a la misma. Se ejecutan desde las instalaciones del cliente pruebas en modo "Caja Blanca" o "Caja Negra".

La consultoría para la realización de un **Test de Intrusión Externo** trata de dilucidar hasta qué punto puede un atacante externo tener acceso a los sistemas de información de la organización desde Internet. Se podría considerar una auditoría de "Caja Negra".

Un proyecto completo contempla los siguientes aspectos:

- ✔ Planificación del proyecto:
  - › Definición y establecimiento de los requerimientos de información necesarios para la ejecución del proyecto
  - › Desarrollo de un plan de trabajo
- ✔ Test de intrusión interno: sondeos de red y obtención de información de sistemas y puertos:
- ✔ Test de intrusión Externo: identificación y detección de recursos alcanzables desde Internet
- ✔ Escaneo automático de vulnerabilidades en los servicios activos
- ✔ Test de intrusión interno: análisis de estructura de red, segmentación y políticas de filtrado
- ✔ Comprobación manual de falsos positivos
- ✔ Análisis y detección manual de vulnerabilidades a través de los resultados obtenidos de las pruebas anteriores
- ✔ Test de intrusión externo: test no privilegiado de aplicaciones externas:
  - › Auditoría de aplicaciones sin analizar el código fuente de las mismas
  - › Se explotan las posibles entradas en el sistema para acceder al back-end, ya sea directamente o mediante errores en el front-end
  - › Búsqueda de los errores más comunes que se producen y posibles bugs
- ✔ Elaboración de entregables de revisión:
  - › Informe con las pruebas realizadas, los hallazgos, sus implicaciones y recomendaciones para su solución en relación con las debilidades identificadas durante la auditoría

FUNCIONALIDADES

- ✔ Evaluación de los niveles de seguridad de la organización
- ✔ Identificación de posibles vulnerabilidades que pudieran revelar información sensible o provocar accesos no autorizados
- ✔ Descubre fallas de seguridad tras cambios de configuración, determina sistemas en peligro e identifica configuraciones erróneas que pudieran desembocar en fallos de seguridad en dispositivos de red (switches, routers, firewalls, etc.)

BENEFICIOS APORTADOS

- ✔ Proporciona un conocimiento del grado de vulnerabilidad de los sistemas de información.
- ✔ Descubre fallas de seguridad tras cambios de configuración, determina sistemas en peligro e identifica configuraciones erróneas que pudieran desembocar en fallos de seguridad en dispositivos de red (switches, routers, firewalls, etc.).
- ✔ Optimización de recursos económicos y de tiempo por acciones preventivas