

Panorama General

El servicio de pruebas de intrusión está diseñado para realizar ejercicios de hackeo ético, con la finalidad de identificar y explotar vulnerabilidades en la infraestructura o aplicaciones de la organización, el propósito es encontrar potenciales vectores de ataque que podrían ser utilizadas por una amenaza para así lograr comprometer la confidencialidad, integridad o disponibilidad de la información.

Estas pruebas permitirán a "CLIENTE" visualizar el potencial impacto en el que puede derivar la materialización de un ataque a su infraestructura.

HIXSA ha desarrollado un conjunto de metodologías basadas en las mejores prácticas de la industria y metodologías mundialmente reconocidas como NIST, 560 del SANS Institute, OSCP de Offensive Security, OWASP "The Web Security Testing Guide v4" y pruebas de Draft v5, OSSTMM principalmente.

Se ofrece la ejecución de pruebas de intrusión desde 3 perspectivas distintas, mismas que se describen a continuación.

Perspectiva Caja negra modalidad externa

Las pruebas de intrusión bajo esta perspectiva serán ejecutadas desde una red externa, sin tener un previo conocimiento de la organización, la finalidad de ejecutar las pruebas bajo esta perspectiva consiste en simular las vulnerabilidades que un atacante, crimen organizado, hackers o cualquier agente externo pudiera identificar y explotar para comprometer la seguridad de la información.

Los consultores asignados por parte de HIXSA realizará el descubrimiento y enumeración de los activos tecnológicos para lograr la identificación de:

- Servicios publicado a Internet (sin credenciales)
- Servicios web
- Dispositivos de Seguridad Perimetral
- Switches y Routers
- Servicio de Correo
- Servicios Corporativos
- Información sensible publicada en fuentes de información

Es importante mencionar que, las pruebas a los activos en AWS (de ser identificados) se realizarán de acuerdo con las políticas publicadas por el **proveedor**.

Durante el ejercicio se tienen consideradas pruebas de DDoS (de tener pleno consentimiento de personal autorizado de "CLIENTE"), dichas pruebas tendrán particularidades de acuerdo con los controles implementados, tecnología, versiones y configuraciones identificadas por el equipo de HIXSA sin embargo, se consideran las siguientes pruebas:

HTTP GET/Post Attack: El ataque HTTP Get/Post consiste en enviar múltiples peticiones utilizando los métodos Get/POST, dichas peticiones son del tamaño máximo permitido (Content length) y se envían byte a byte hacia el servidor.

SSL Half Connect: El ataque se aprovecha de la renegociación de llaves del protocolo SSL, debido a que el consumo de recursos para generar las mismas es alto. Adicionalmente se crean múltiples conexiones a través del protocolo SSL y se mantienen activas el máximo tiempo permitido

Slowloris: Se inician múltiples conexiones en el servidor y se mantienen abiertas el máximo tiempo permitido por el mismo

HTTP Flood: El ataque tiene impacto cuando se fuerza al servidor asignar el máximo de recursos disponibles en cada respuesta derivado de cada petición.

Alcance: Activos tecnológicos publicados a Internet considerando dentro de los mismos los siguientes activos:

No. de Activos	Infraestructura / Aplicación
Los activos que sean identificados publicados a Internet	Infraestructura & Aplicación
C/S Credenciales	Duración aproximada
SIN CRED	20 días hábiles



Perspectiva Caja gris modalidad interna

Las pruebas de intrusión bajo esta perspectiva serán ejecutadas desde una red interna, este escenario simula ataques de personas con conocimientos sobre la arquitectura tecnológica, funcionamiento de aplicativos, procesos internos entre otros, como pudieran ser colaboradores internos descontentos, clientes, proveedores, socios de negocio o competencia dentro de la industria.

La finalidad del ejercicio es poder comprometer los activos críticos que soporten los procesos core de negocio.

Los consultores asignados por parte de HIXSA complementarán el descubrimiento y enumeración de los activos tecnológicos con la información proporcionada por personal autorizado de "CLIENTE", se pueden considerar dentro del análisis los siguientes tipos de activos:

- Aplicativos transaccionales y de consulta
- Servidores Principales
- Bases de datos Anexo F – Metodología de Pruebas de Penetración a Bases de Datos
- Dispositivos de Seguridad Perimetral
- Active Directory.
- Sistemas operativos en servidores de aplicaciones (Windows, Linux, etc.)
- Sistemas operativos en máquinas y equipos conectados a la red.
- Revisión de VoIP (Se buscará la identificación de los siguientes riesgos):
- Enumeración del directorio telefónico de "CLIENTE"
- Obtención de archivos de configuración de VoIP
- Captura y reconstrucción de llamada telefónica
- Alterar una conversación
- Redirección de llamadas
- Suplantación de usuarios

Se considera como alcance el siguiente escenario:

No. de Activos	Infraestructura / Aplicación
Los activos vulnerables que permitan, trazar un vector de ataque y comprometer la gestión o activos críticos.	Infraestructura & Aplicación
C/S Credenciales	Duración aproximada
SIN CRED	20 días hábiles

Revisión ATM

Derivado de la criticidad que los ATM (cajeros automáticos) representan para la operación de nuestros clientes de la Banca, HIXSA tiene la capacidad de realizar la evaluación integral de un cajero automático en la Ciudad de México, dichas pruebas consideran estándares y metodologías mundialmente reconocidas como Payment Card Industry Data Security Standard (PCI DSS), NIST, 560 del SANS Institute, OSCP de Offensive Security, ATMIA/GASA Best Practices for ATM Cyber Security y OWASP. Se considera por mencionar la revisión y validación de:

- Componentes de Hardware
- Componentes de Software
- Revisión de operación
- Revisión de aplicativos y servicios instalados

Para la ejecución de la revisión, se requiere la autorización y acompañamiento de personal

El set de pruebas a desarrollar por el equipo de HIXSA se encuentra alineado a las buenas prácticas y estándares líderes de la industria.

Se considera como alcance el siguiente escenario:

No. de ATM	Ubicación	Infraestructura / Aplicación
1	CDMX	Revisión lógica, física y de red
C/S Credenciales		Duración aproximada
Con Credenciales		5 días hábiles