Servicios de Penetration Testing

Los tipos de Penetration Testing que ofrecemos son:

- Pruebas de Infraestructura.
- Pruebas de Aplicaciones Web.
- Pruebas de Aplicaciones Móviles.
- Pruebas de Redes Inalámbricas.
- Pruebas de Servicios en la Nube.
- Pruebas de Dispositivos Embebidos / IoT.
- Pruebas de Sistemas de Control Industrial (ICS).
- Pruebas de Desarrollo Agil.

M3 6D SECURITY

Índice del Brochure

Metodologias de un Penetration Testing

Caja Negra Penetration Testing

Ejecución de un Penetration test en el sitio "On-Site" del cliente, con nivel 0 de información pre-consentida para:

- Presentar un esquema de las vulnerabilidades encontradas en relación con su dificultad de remediación y su impacto en los activos de información de la organización.
- Recomendar las soluciones más eficaces para su estructura organizativa y/o activos de información en particular, definidas en el alcance; que maximicen la eficiencia de la inversión para mantener niveles óptimos de seguridad a corto y mediano plazo.
- Que el esquema de soluciones recomendadas en base a las vulnerabilidades encontradas, permita tomar decisiones estratégicas y tácticas en relación a los activos de información del segmento analizado.
- Recomendar estrategias óptimas para la seguridad de los activos de información, teniendo en cuenta las características del negocio propio de la organización.

Caja Gris Penetration Testing

Ejecución de pruebas de intrusión en el sitio ONSITE del cliente, con al menos 1 (una) información previa sobre el sistema objetivo, esta información se obtendría en primera instancia a través de algún intento satisfactorio de la etapa de Back Box o de otra manera, por consenso con el equipo de trabajo.

El objetivo es detectar las vulnerabilidades, identificarlas y asignarles un nivel de criticidad aproximado para conocer los riesgos asociados y elaborar un plan de remediación.

En función de lo que se detecte en las etapas de descubrimiento y evaluación, se acordarán con el responsable del contrato los servicios y direcciones IP que se analizarán y el nivel de profundidad que se alcanzará en cada caso. En algunos casos, las vulnerabilidades pueden ser explotadas.

Metodologias de un Penetration Testing

Caja Blanca Penetration Testing

Este tipo de evaluación corresponde a la perspectiva interna, en la que el cliente proporciona una estructura detallada de su infraestructura de red y mediante técnicas de ethical hacking se obtiene la información necesaria para continuar con la evaluación. Esto previene los ataques internos de los empleados, proveedores, etc.

Se realiza una evaluación con credenciales válidas y autorizadas, para analizar toda la información sensible y los privilegios que tiene la estructura interna de la organización. El objetivo es detectar las vulnerabilidades, identificarlas y asignarles un nivel de criticidad aproximado para conocer los riesgos asociados y elaborar un plan de remediación.

Etapa de Reconocimiento Pasivo

Aunque el cliente proporcionará información sobre los objetivos, para dar un valor añadido trataremos de obtener información relacionada con ellos a través de la interacción con los motores de búsqueda publicos, grupos de consulta, información de registros dns, información en bases a whois y todo aquel contenedor de información que tenga relación directa con los objetivos.

En esta etapa de reconocimiento, se informa al cliente del nivel de visibilidad que tienen los objetivos desde el exterior a los ojos de un potencial atacante. Cabe señalar que un alto nivel de visibilidad no implica necesariamente una vulnerabilidad, pero el objetivo de esta etapa es proporcionar toda la información disponible sobre ellos para que el cliente pueda determinar y exponer posteriormente sólo la información estrictamente necesaria de su organización.

Etapas de Reconocimiento

Etapa de Reconocimiento Activo en Superficie

En esta etapa y a diferencia de la anterior, se comenzará a identificar los puntos directamente relacionados con los objetivos e interactuando con ellos, de esta manera esta etapa busca identificar en principio los objetivos activos y luego practicar en el mismo análisis más profundo que los descritos en las etapas siguientes a esta.

Etapa de Reconocimiento Profundo

El objetivo de esta etapa crítica es practicar un análisis mucho más profundo de los objetivos detectados en la etapa anterior.
Las pruebas realizadas en esta etapa tienen por objeto identificar todos los puertos abiertos tanto TCP como UDP, enumerar e identificar con la mayor precisión posible todos los servicios que se ejecutan en los puertos abiertos, identificar las versiones de los sistemas operativos en los que se ejecutan las aplicaciones.
Identificar la topología de red en la que viven los objetivos, para analizar la correcta implementación de los dispositivos de filtrado y detección que puedan existir.

Etapa de Análisis de Vulnerabilidad

Con la información obtenida en la etapa anterior, el objetivo de esta etapa es detectar las posibles vulnerabilidades que los objetivos puedan tener tanto a nivel de infraestructura como de aplicación.

Esta etapa puede considerarse sensible, ya que se debe trabajar adecuadamente para erradicar los falsos positivos que puedan ser mal reportados.

Fases de un Penetration Test

Las diferentes fases del análisis se describen a continuación

Recon:

Se definen los objetivos y se recoge la mayor cantidad de información posible para luego utilizarla en las siguientes fases. La información que se busca va desde los nombres y direcciones de correo electrónico de los empleados de la organización, hasta la topología de la red, las direcciones IP, entre otros. Incluye, entre otras, las siguientes actividades (siempre dependiendo del alcance definido):

- Identificar la topología de la red.
- Identificar el dominio de red lógico utilizado y su configuración.
- Identificar los dispositivos de red (Firewalls, UTMs, Routers, etc.) y los puertos filtrados.
- Análisis de todos los puertos (1 a 65535) abiertos a nivel TCP, en los diferentes sistemas de la Compañía que se detectan en el escaneo de las direcciones IP en Internet.
- Análisis de todos los puertos (1 a 65535) abiertos a nivel UDP, en los diferentes sistemas de la Compañía que se detectan en el escaneo de las direcciones IP en Internet.
- Análisis de la seguridad de los enlaces que la organización posee en la nube.

Fases de un Penetration Test

Las diferentes fases del análisis se describen a continuación

- Análisis de las conexiones con terceros.
- Detección de servicios activos.
- Detección de protocolos en uso.
- Identificar versiones y modelos de Routers, Switches, Firewalls y/o UTMs.
- Análisis de respuestas a diferentes protocolos y paquetes.
- Detección de servidores utilizados y su versionado.
- Detección remota de Sistemas Operativos de base de servidores.

Estudio de la lógica de la plataforma, tratando de detectar:

- Switches.
- Routers.
- Firewalls/UTMs.
- Balanceadores de carga.
- Servidores de correo electrónico.
- Servidores de DNS.
- Servidores proxy.
- Servidores FTP.
- Servidores WEB.
- Terminales VPN y sistemas de acceso remoto.
- Sistemas de bases de datos (SQL Server, Oracle, MySQL, PostgreSQL, etc.).

QUIENES SOMOS

Un equipo de profesionales altamente calificados con:

Habilidades Avanzadas de Ethical hacking.
Certificaciones Profesionales Reconocidas Internacionalmente.
Mas de 10 Años de Experiencia Comprobados en Ciberseguridad.
Habilidades de ataque avanzadas sobre diferentes aspectos de la ciberseguridad.

Lo que nos diferencia de las consultoras tradicionales es que pensamos como los cibercriminales.

World Class Penetration Testing

M360 SECURITY