Instituto Tecnológico Superior de Uruapan.

Ingeniería en Sistemas Computacionales.

Grupo:

9-A

Materia:

Seguridad Informática

Docente:

Jonathan Zacek Alcazar Jurado

Título:

Pentesting

Integrantes:

Piedra Calderón Jacqueline.

Torres Ángeles Mariana.

Villalobos Rodríguez Maria Guadalupe

Uruapan Michoacán

Jueves 19 de octubre del 2023

INTRODUCCIÓN

Ataque, debilidad, simulación de ataques para encontrar los puntos débiles del sistema.

Los sistemas de cualquier tipo son vulnerables a distintos ataques que día con día se actualizan y mejoran a la par o incluso más allá de los métodos de protección orientados a seguridad.

Encontrar una debilidad en un sistema que estás desarrollando por tu propia cuenta o con ayuda de un equipo de desarrollo puede llegar a ser todo un reto puesto que, al conocer todo el proceso puedes no localizar a simple vista aquello que no se está considerando pero que sigue siendo de suma importancia. Suele ser muy fácil suponer que se estableció una buena base de seguridad para la protección, sin embargo, esto llega a estar muy lejos de la realidad.

Proteger la información que se está manejando dentro de un sistema es la principal tarea y preocupación dentro de la seguridad. El tipo de información que viaja, muy a pesar de ser variante, supone un detonante para aquellas personas que se encargan de el robo de la misma.

El Pentesting se encarga de simular un conjunto de ataques dirigidos al sistema. La persona que se encarga de este trabajo es preferentemente alguien ajeno al proyecto, pero especialista en el campo. Esto se hace con el propósito de no omitir todas las posibles vulnerabilidades.

Todo sistema en desarrollo tiene puntos débiles qué a la larga salen y ocasionan inconvenientes. El pentesting se encarga de encontrarlos y alertar para corregirlos.

El propósito general se centra en la seguridad y optimización para un bien desarrollo.

¿Qué es pentesting?

Un pentesting es un conjunto de ataques simulados dirigidos a un sistema informático con una única finalidad: detectar posibles debilidades o vulnerabilidades para que sean corregidas y no puedan ser explotadas. (INCIBE, 2019)

¿Quién hace el pentesting?

El mejor candidato sería un miembro del equipo de seguridad de la organización, que conoce el sistema al dedillo, sus puntos débiles y sus puntos fuertes, pero no está tan claro. Si la prueba de pentesting es realizada por un especialista con un conocimiento mínimo del sistema de protección construido, es más probable que encuentre los llamados «puntos ciegos», pasados por alto por los desarrolladores al construir y organizar los niveles de protección. Por este motivo, los servicios de pentesting se suelen subcontratar a proveedores especializados en este ámbito.

Los hackers éticos (también conocidos como hackers de sombrero blanco) también son adecuados para este papel. Porque tienen mucha experiencia, que aplican de buena fe, con el objetivo, de mejorar la seguridad. (Lucena, 2023)

¿Qué incluye un pentesting?

Prueba de pentesting en la red:

- Identificación de las vulnerabilidades en cuanto a la red y de sistema
- Identificar los errores de configuración y los ajustes
- Identificación de las vulnerabilidades de las redes inalámbricas
- Servicios fraudulentos
- Ausencia de contraseñas fuertes y presencia de protocolos débiles.

Prueba de pentesting de aplicaciones:

- Identificación de fallos en la capa de aplicación
- Suplantación de solicitudes
- Uso de scripts maliciosos
- La interrupción de la gestión de la sesión.

Prueba de pentesting física:

- Romper las barreras físicas
- Pruebas y manipulación de cerraduras
- La interrupción y la derivación de los sensores
- Desactivar las cámaras de vigilancia.

Pruebas de intrusión en dispositivos (IoT):

- Identificar los fallos de hardware y software de los dispositivos
- Forzar contraseñas débiles
- Identificación de protocolos, APIs y canales de comunicación inseguros
- Infracciones de la configuración y mucho más.

(Lucena, 2023)

¿Cuáles son las etapas de un pentesting?

1. **Recopilación de información:** Búsqueda de información sobre la organización y los empleados en fuentes públicas, redes sociales, foros y blogs.

2. **Encontrar los antecedentes técnicos:** identificar los recursos, aplicaciones e instalaciones técnicas existentes en la empresa.

3. **Análisis de vulnerabilidades y amenazas:** identificación de vulnerabilidades en sistemas y aplicaciones de seguridad mediante un conjunto de herramientas y utilidades, tanto comerciales como desarrolladas internamente por pentestores.

4. **Explotar y procesar los datos:** simula un ciberataque real para obtener información sobre cualquier vulnerabilidad con un análisis posterior.

5. **Generación de informes:** formalización y presentación de los resultados del pentesting con sugerencias para mejorar el sistema de seguridad existente.

(Lusena, 2023).

Tipos de pentesting (pruebas de penetración)

Pentest de "caja blanca" (o white box):

En esta prueba de penetración, se proporcionará al Pentester información sobre la estructura de seguridad implementada de la organización. Además, este método se puede implementar junto con el equipo de TI de la organización y el equipo de pruebas de penetración.

Pentest de "caja negra" (o "black box"):

En este caso, las acciones de un atacante real son simuladas, ya que no proporcionan ninguna información relevante a un especialista o equipo, excepto el nombre y los datos básicos para una idea general del trabajo de la empresa.

Pentest de “caja gris” (o " gray box "):

En esta situación, solo una pequeña parte de los empleados de la organización (1 - 2 personas), incluidos los profesionales de TI y seguridad que responderán a los ataques no tienen información sobre el escaneo existente. Para este tipo de prueba, es muy importante que el pentester o el equipo tengan el documento apropiado para evitar problemas con las agencias de aplicación de la ley, si el servicio de seguridad responde adecuadamente.

Pentest externo:

Un ataque de un hacker "ético" que se lleva a cabo contra servidores o dispositivos externos de la organización, como su sitio web y servidores de red. El objetivo es determinar si un atacante puede penetrar el sistema de forma remota y hasta dónde puede hacerlo.

Pentest interno:

Un usuario autorizado con derechos de acceso estándar realiza una imitación de un ataque, lo que le permite determinar qué daño puede causar un empleado que tiene algunas cuentas personales con respecto a la administración.

(Rodríguez, 2021)

CONCLUSIÓN

Contar con un sistema que simule ataques a las vulnerabilidades encontradas en un sistema, más que una desventaja para el desarrollo, se considera una ventaja que a largo plazo evita inconvenientes. Estos ataques simulados muestran la realidad previa a la que se enfrenta y compromete toda la información que cayendo en manos equivocadas puede ocasionar pérdidas.

El proceso de Pentesting ayuda a identificar recursos de distintos aspectos, se adentra en la estructura completa ya que todo representa una posible debilidad. Considerar los recursos técnicos y de infraestructura previenen problemas de este aspecto, sin embargo, esto no es todo, el sistema puede ser débil en cuanto al aspecto físico y humano.

Mantener pentesting periódico ayuda en el constante análisis en el que siempre hay probabilidad de crear vulnerabilidades.

Llevar un mantenimiento significa hacer chequeos de corrección. Estas consultas las lleva a cabo un profesional en el campo pues es un trabajo que una persona debe de conocer muy bien, así se evita fallos en este proceso y hace que sea confiable.

Al final, el propósito de todo esto es evitar que personas externas puedan corroer o hacer mal uso de información o directamente del manejo de un sistema, todo esto es parte de la seguridad de una organización.

REFERENCIAS BIBLIOGRÁFICAS

- INCIBE. (2019, 4 julio). *¿Qué es el pentesting? Auditando la seguridad de tus sistemas INCIBE* https://www.incibe.es/empresas/blog/el-pentesting-auditando-seguridad-tus-sistemas
- Lucena, P. (2023, 24 mayo). *¿Qué es el pentesting? CESUMA* https://www.cesuma.mx/blog/que-es-el-pentesting.html#abh_about
- Rodríguez, F. (2021, 14 octubre). *Todo lo que debes saber del pentesting. iDric.* https://www.idric.com.mx/blog/post/todo-lo-que-debes-saber-del-pentesting