Ethical Hacking – Actividad 3 Metodología.

Andrés Mena Salazar

Giovanni Quintal Llanes

Alexis Rosaldo Pacheco

Diferencias entre una prueba de penetración y un análisis de vulnerabilidades

	Prueba de penetración	Análisis de vulnerabilidades
Propósito	Simular un ataque real para identificar y explotar vulnerabilidades en un sistema.	Identificar y cuantificar vulnerabilidades conocidas en un sistema a través de herramientas automatizadas.
¿Cuándo se hace?	De forma periódica como parte de auditorías de seguridad o despues de cambios significativos en una infraesctructura.	A través de un programa continuo de gestión de vulnerabilidades. Se suelen hacer antes de un pentest.
¿Cómo se hace?	Con herramientas automatizadas junto con técnicas manuales para intentar explotar vulnerabilidades.	A travpes de herramientas automatizadas se escanea el sistema para buscar vulnerabilidades conocidas, basandose de datos.
¿Qué se reporta?	Descripción de las vulnerabilidades explotadas y el impacto potencial.	Listado de vulnerabilidades con niveles de riesgo asociados.
Duración	Depende del alcance y complejidad del sistema.	Horas o días dado que se usa una herramienta automatizada.

Pruebas de caja negra

El atacante no tiene conocimiento previo de la infraestructura del sistema que se intenta acceder. Es decir, se simula un ataque externo.

Se evalua la resistencia del sistema frente a atacantes externos que no tienen acceso privilegiado, el pentester usa técnicas de reconocimiento para recolectar información antes de intentar explotar vulnerabilidades. Sin embargo, no siempre se hallán vulnerabilidades por falta de conocimiento previo.

Se realiza escaneo de puertos, mapeo de red, para luego intentar explotar las vulnerabilidades descubiertas.

Pruebas de caja blanca

El atacante (pentester) tiene acceso completo a la información interna del sistema o red, como diagramas, código fuente, configuraciones y detalles de la infraestructura. Con ello se prueba la seguridad como si fuera alguien que tiene acceso legitimo y se realiza un análisis exhaustivo para detectar vulnerabilidades que no serían evidentes para un atacante externo.

Se reportan vulnerabilidades encontradas tanto en los componentes internos como en la configuración del sistema, junto con las pruebas de explotación realizadas y las recomendaciones de mitigación.

Pruebas de caja gris

Para este enfoque, se trae un conocimiento parcial sobre el sistema a probar, un evaluador no tiene acceso completo al código fuente de la aplicación, pero tiene suficiente conocimiento y documentación para comprender las funciones principales de la aplicación. Esto permite diseñar casos de prueba que se centren en posibles problemas de funcionalidad y seguridad en lugar de realizar pruebas a ciegas.

Representa el ataque de alguien con acceso restringido o alguien que ha comprometido parcialmente el sistema.

Categorización de una prueba de penetración

Intrusión interna

Consisten en pruebas controladas de ataques informáticos, dentro de entornos seguros desde la red interna de la empresa, con el objetivo de descubrir posibles vulnerabilidades que no pueden ser detectadas por otros medios.

Estas pruebas se realizan por un hacker ético, en aplicaciones web, redes, servidores, computadoras, dispositivos móviles, equipos industriales, Cloud (Azure, AWS, etc.) y otros sistemas informáticos especificados por el cliente.

Categorización de una prueba de penetración

Intrusión externa

En este tipo de pruebas el hacker ético se enfrenta a la tecnología expuesta al exterior de la empresa, como su sitio web y servidores de red externos.

Permite simular las tácticas y técnicas de atacantes reales para identificar y explotar vulnerabilidades en los sistemas y redes externas de una organización.

Fases del Método

Rastreo y Reconocimiento

Durante esta fase, se identifican los activos (páginas web, roles de usuario, APIs, redes, etc.) que serán sometidos a la prueba de penetración.

También se comparten los detalles y accesos necesarios para las pruebas de penetración.

Y finalmente los investigadores de seguridad y la organización deciden el tipo de prueba de penetración que se realizará.

Fases del Método

Escaneo de la red (identificación de vulnerabilidades)

Implica tomar la información descubierta durante el reconocimiento y usarla para examinar la red.

Incluye actividades como el escaneo inteligente de puertos del sistema, que se utiliza para determinar puertos abiertos y servicios vulnerables.

Finalmente el atacante puede usar diferentes herramientas automatizadas para descubrir vulnerabilidades del sistema.

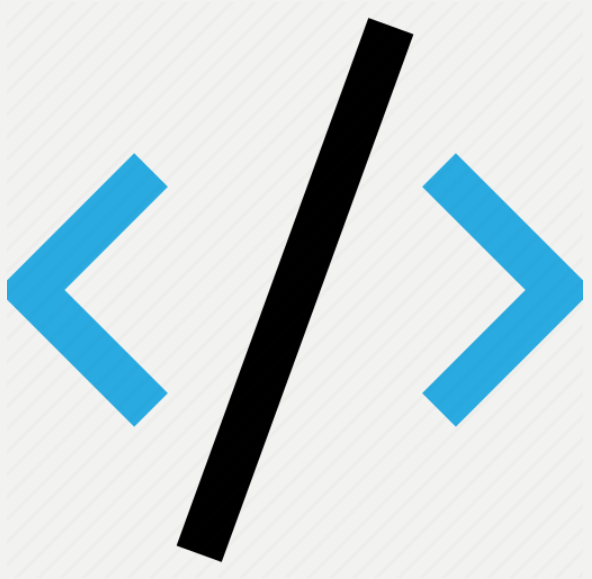
Fases del Método

Enumeración del sistema

Proceso de recopilar información detallada y específica sobre los sistemas, redes y aplicaciones de un objetivo. Durante la enumeración, un atacante o un probador de seguridad busca identificar componentes activos y características de los sistemas que pueden ser explotados. Por ejemplo:

- Identificación de cuentas de usuario, grupos de usuarios, roles y permisos asociados en el sistema.
- Identificar los servicios que se están ejecutando y las versiones específicas de esos servicios.
- Utilización de herramientas automatizadas para escanear el sistema en busca de vulnerabilidades conocidas.

Fases del Método



Ataque al objetivo

En esta fase, el hacker ético toma las vulnerabilidades identificadas en las etapas anteriores (escaneo de red y enumeración del sistema) y busca explotarlas para ganar acceso no autorizado al sistema. El objetivo principal es comprobar hasta qué punto un atacante real podría comprometer el sistema o la red.

Esto puede implicar el uso de exploits, scripts personalizados o técnicas de ingeniería social. El objetivo es comprobar hasta qué punto un atacante real podría comprometer el sistema.

Fases del Método

Acciones posteriores al ataque

Después de realizar el ataque con éxito, el hacker ético analiza el impacto total del ataque. Esto implica evaluar el nivel de acceso obtenido (como administrador o usuario), los datos que pudieron haber sido comprometidos, y qué tan lejos se podría haber extendido un atacante dentro del sistema o la red.

Una vez que se comprende el impacto, se implementan medidas para contener el daño.

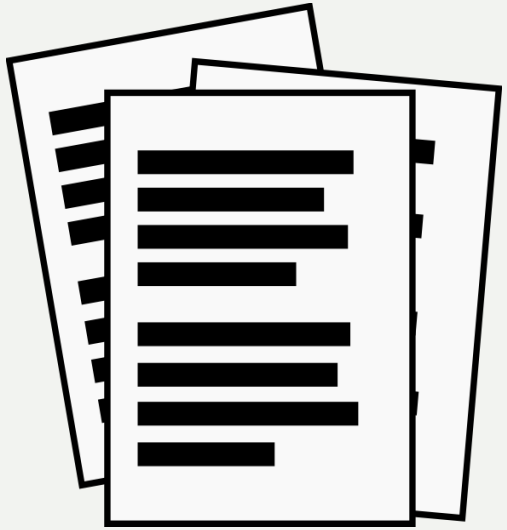
Al final el hacker ético trabaja en colaboración con el equipo de seguridad para implementar mejoras que refuercen el sistema contra ataques futuros. Esto puede incluir aplicar parches de seguridad, cambiar contraseñas, reforzar las políticas de acceso, o agregar capas adicionales de seguridad.

Fases del Método

Documentación de evidencias

1. Durante el proceso de hacking ético, es fundamental registrar y almacenar todas las evidencias relacionadas con los ataques realizados, los resultados obtenidos, y cualquier dato comprometido.
2. El hacker ético documenta cada paso del proceso, desde el rastreo inicial hasta las acciones posteriores al ataque. Se deben incluir todas las herramientas, exploits y técnicas que se emplearon para comprometer el sistema.
3. El informe debe incluir una evaluación clara del riesgo que cada vulnerabilidad presenta para la organización.
4. Da recomendaciones prácticas y claras, de modo que el equipo de seguridad de la organización pueda implementarlas fácilmente.

Fases del Método



Reporte Final

El reporte final es un documento completo que se entrega a la organización.

- **Resumen Ejecutivo:** Una visión general del ataque, los riesgos y recomendaciones.
- **Metodología:** Explicación detallada de cómo se realizó el hacking ético (herramientas y técnicas utilizadas).
- **Vulnerabilidades Descubiertas:** Listado y descripción de las vulnerabilidades con su nivel de severidad.
- **Impacto Potencial:** Detalle de lo que un atacante real podría hacer si explotara esas vulnerabilidades.
- **Recomendaciones:** Propuestas de soluciones para mitigar los riesgos.

Referencias

- Cloudflare. (n.d.). *What is penetration testing?* Recuperado de https://www.cloudflare.com/learning/security/glossary/what-is-penetration-testing/
- Coursera. (n.d.). *Types of penetration testing*. Recuperado de https://www.coursera.org/articles/types-of-penetration-testing
- Astra Security. (n.d.). *External penetration testing*. Recuperado de https://www.getastra.com/blog/security-audit/external-penetration-testing/
- ladiferencia.net. (n.d.). *Análisis vs Prueba de Penetración: Claves de Ciberseguridad*. Recuperado de https://ladiferencia.net/analisis-vs-prueba-de-penetracion-claves-de-ciberseguridad/
- LogMeOnce. (n.d.). *Vulnerability Scan Vs Penetration Test*. Recuperado de https://www.logmeonce.com/recursos/vulnerability-scan-vs-penetration-test/
- TI Rescue. (n.d.). *Qué son las pruebas de caja negra, blanca y gris*. Recuperado de https://tirescue.com/que-son-las-pruebas-de-caja-negra-blanca-y-gris/
- IBM. (n.d.). *Penetration testing*. Recuperado de https://www.ibm.com/mx-es/topics/penetration-testing