Universidad Autónoma De Chiapas.

Act- 4.2 Investigar en artículos métodos, tipos y componentes de pruebas de penetración web.

Estudiante: José Gilberto Guzmán Gutiérrez.

LIDTS. 7ºM.

A200119.

Catedrático: DR. Luis Gutiérrez Alfaro.

Tuxtla Gutiérrez Chiapas. 21 de octubre del 2023.

Índice.

1. Introducción.

El en presente trabajo a entregar se pretende ver mas a fondo el tema de pruebas de penetración, conoceremos su definición e importancia, sus métodos, tipos y componentes. Todo ello desde un enfoque ético y educativo.

2. Desarrollo.

Pruebas de penetración.

Definición.

También conocidas como pruebas de seguridad, **son un enfoque esencial para evaluar la robustez de un sistema o red informática al exponer sus posibles vulnerabilidades.** Estas evaluaciones son llevadas a cabo por expertos en seguridad informática éticos, quienes emplean técnicas similares a las utilizadas por ciberdelincuentes, pero con el objetivo de identificar debilidades sin causar daño al sistema ni a la organización en cuestión.

Importancia.

Se destacan al adoptar la perspectiva de un hacker para detectar y mitigar proactivamente los riesgos de seguridad cibernética antes de que puedan ser explotados. A diferencia de otros métodos de evaluación de seguridad, estas pruebas no solo identifican vulnerabilidades, sino que también cuantifican su impacto en el negocio. Esto permite a los equipos de TI y seguridad mejorar sus medidas de protección de manera anticipada, reduciendo significativamente las posibilidades de un ataque exitoso.

Métodos.

- **Prueba de Caja Negra:** **Este se inicia sin ningún conocimiento previo o permisos de acceso al entorno de destino.** Simula las acciones que un actor malicioso podría llevar a cabo para comprometer el sistema. Incluye actividades como la recopilación de información y la exploración del objetivo. Se considera la evaluación más realista de las amenazas externas, ya que el probador opera en un estado de total desconocimiento del sistema.
- **Prueba de Cuadro Gris:** **Este tiene un nivel de conocimiento inicial limitado y acceso autorizado al entorno de destino.** El probador puede comenzar con una cuenta de usuario legítima y tener cierto conocimiento de la red a nivel de empleado. Esta categoría simula un ataque de amenaza interna o las acciones de un actor malicioso después de haber obtenido acceso inicial a través de credenciales comprometidas, phishing u otros medios. La prueba de Cuadro Gris se sitúa entre la Caja Negra y la Caja Blanca en términos de acceso y conocimiento.
- **Prueba de Caja Blanca:** **Este cuenta con acceso completo y autorizado al objetivo, incluyendo toda la información y documentación relacionada.** Siendo que, el probador tiene un profundo conocimiento del sistema y puede explorar sus vulnerabilidades sin necesidad de realizar un proceso de reconocimiento. Sin embargo, es importante tener en cuenta que las ideas preconcebidas de los administradores sobre el funcionamiento del sistema pueden influir en la evaluación, lo que hace que esta prueba sea más rápida pero potencialmente menos objetiva.
- **Prueba Externa:** **Este se lleva a cabo una evaluación atacando activos de información que son visibles para personas externas, tales como aplicaciones, sitios**

web, servidores DNS y correo electrónico. El objetivo puede ser la extracción de datos, la realización de transacciones o la ejecución de otras actividades maliciosas. Esta prueba tiene como finalidad identificar vulnerabilidades que podrían ser explotadas por atacantes externos.

- **Prueba Interna:** **Este lleva a cabo un ataque simulado desde dentro del sistema con el propósito de exponer el alcance de los posibles daños causados por amenazas internas.** El escenario incluye a personas internas y empleados malintencionados que podrían responder a ataques de phishing o ingeniería social. Su objetivo es evaluar la capacidad del sistema para resistir amenazas desde el interior.

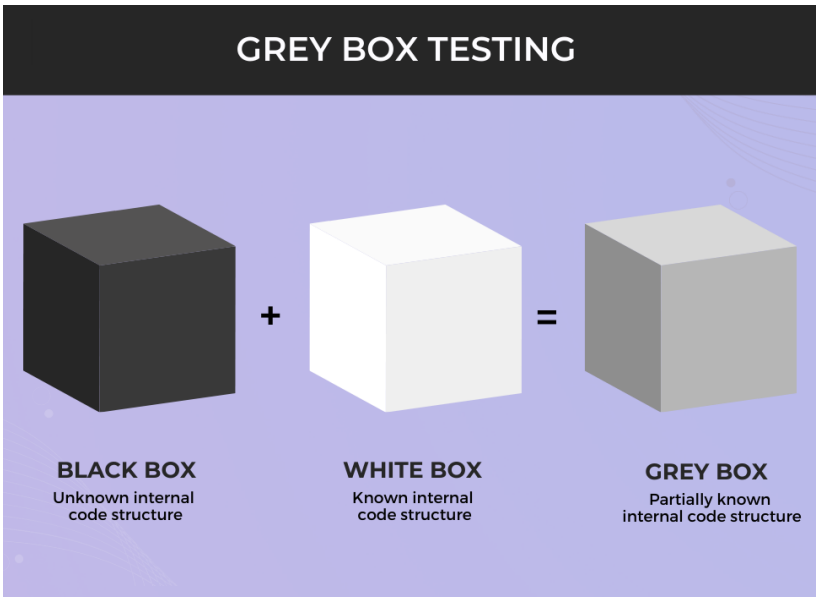


Imagen 1. Prueba de caja negra, caja blanca y caja gris.

- **Prueba Ciega:** **Este se basa en información disponible públicamente acerca del objetivo. El evaluador no dispone de ningún conocimiento privilegiado sobre la postura de seguridad del objetivo.** La empresa objetivo es informada sobre cuándo y dónde ocurrirá el ataque, lo que le permite prepararse previamente para la evaluación.

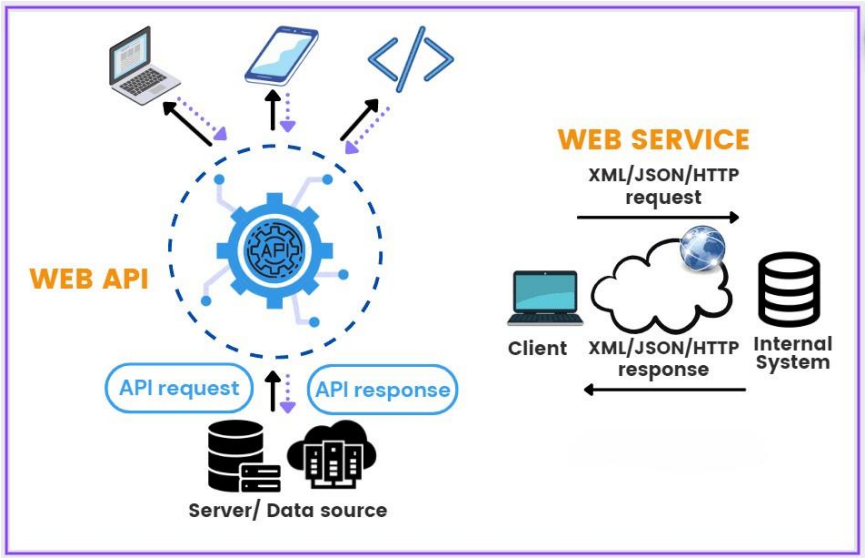
- **Prueba Doble Ciego:** **Este es la realización de un ataque cuando ni el evaluador ni el objetivo tienen información previa sobre la prueba.** En este contexto, se requiere que los evaluadores confíen en las herramientas y habilidades disponibles para sortear las defensas del objetivo. Por su parte, la empresa objetivo debe confiar en sus propios recursos para evitar que el evaluador comprometa sus defensas. Este escenario pone a prueba tanto la capacidad de ataque como de defensa sin conocimiento previo.

Tipos

- **Prueba de Penetración de Aplicaciones Web:** **Este se centra en la búsqueda de vulnerabilidades relacionadas con la integridad y validación de datos, problemas de autenticación, y la gestión de sesiones de usuario, entre otros aspectos.** Identifica fallos de seguridad tanto en el código fuente de las aplicaciones web como en las bases de datos y las redes subyacentes. Suele dividirse en tres etapas: reconocimiento, descubrimiento de vulnerabilidades e intento de explotarlas con el fin de obtener acceso no autorizado a aplicaciones o sistemas backend.
- **Prueba de Penetración de Red:** **Este se enfoca en la identificación de vulnerabilidades de seguridad en la infraestructura de red, incluyendo firewalls, conmutadores y enrutadores, así como vulnerabilidades relacionadas con los puntos finales de la red.** Su objetivo es prevenir ataques que puedan aprovechar configuraciones incorrectas de firewalls, ataques a conmutadores o enrutadores, y problemas relacionados con DNS, proxy e intermediarios (ataques de intermediario del tipo "man-in-the-middle" o MiTM). Emplean técnicas como el escaneo de puertos, la toma de huellas digitales del sistema, la evaluación de configuraciones vulnerables, el análisis de virus y malware, así como la manipulación de tráfico de red.

- **Prueba de Penetración de API:** **Este consiste en aprender la estructura y los comandos de las API** (algunas herramientas utilizan estándares como OpenAPI) **y pueden identificar diversos problemas de seguridad**, incluyendo autenticación débil, vulnerabilidades de inyección de código, restricciones de recursos y fugas de datos.
- Prueba de Penetración de Aplicaciones Móviles: **Este se enfoca en identificar nuevos vectores de ataque**, como la distribución de malware a través de **aplicaciones móviles**, ataques de phishing dirigidos a dispositivos BYOD, explotación de vulnerabilidades en redes WiFi y violaciones del protocolo de administración de dispositivos móviles (MDM).

  Imagen 2. Pruebas de penetración Web, Red y API.



Componentes.

- **Planificación:** **En este se establecen los objetivos de la prueba y se lleva a cabo una exploración inicial del sistema.** Se recopila información, a menudo empleando técnicas de ingeniería social para obtener los datos necesarios para llevar a cabo el análisis.

- **Escaneo:** **Este implica el análisis del sistema para evaluar su respuesta frente a un posible ataque.** Los evaluadores de penetración emplean herramientas técnicas en este proceso, realizando un análisis de vulnerabilidades y buscando posibles puntos de acceso no autorizado.
- **Infiltración:** **Este involucra la utilización de diversas estrategias, como la inyección SQL y la exploración de puertas traseras, con el fin de eludir el firewall y violar el sistema.** Posteriormente, el probador de penetración puede tomar control del sistema, dispositivos o redes y extraer datos.
- **Persistencia: Este se centra en determinar cuánto tiempo puede mantenerse el probador en el sistema, identificar información potencialmente comprometedora y hasta qué profundidad puede adentrarse en el sistema.** El pentester se esfuerza por mantener el acceso el mayor tiempo posible, a menudo estableciendo puertas traseras y colocando rootkits.
- **Análisis:** **Este implica la creación de una revisión detallada de la configuración y la presentación de los resultados de la prueba.** Además, los evaluadores de penetración pueden simular cómo un atacante malicioso intentaría encubrir sus rastros. Al concluir la prueba, el pentester recopila toda la información obtenida y presenta informes sobre las vulnerabilidades que pueden ser explotadas.

3. Conclusión.

Posterior a la realización de esta investigación, pude comprender que las pruebas de penetración no son mas que una forma de evaluación la cual busca identificar vulnerabilidades

de un sistema, y estas se pueden llevar a cabo de muchas formas según el contexto y problemática a resolver.

4. Referencias.

Enlaces.

Fernandez, R. (2023, junio 28). 7 types of penetration testing: Guide to pentest methods & types. ESecurity Planet. https://www.esecurityplanet.com/networks/types-of-penetration-testing/

Penetration testing: Complete guide to process, types, and tools. (2022, septiembre 20). BlueVoyant. https://www.bluevoyant.com/knowledge-center/penetration-testing-complete-guide-to-process-types-and-tools

What is penetration testing or pentest? (2022, diciembre 19). EC-Council. https://www.eccouncil.org/cybersecurity/what-is-penetration-testing/

Imágenes.

Imagen 1. Prueba de caja negra, caja blanca y caja gris.

Simic, P. (2023, marzo 22). Black box vs white box vs grey box testing. Shake | Bug and Crash Reports That Tell You Everything. https://www.shakebugs.com/blog/black-vs-white-vs-grey-box-testing/

Imagen 2. Pruebas de penetración Web, Red y API.

Ali, S. (2023, julio 23). What is Web API? Everything you need to learn. Shekh Ali's Blog. https://www.shekhali.com/what-is-web-api/