

Seguridad: PenTesting e IDS

Por:

- Valentina Galvis Bergsneider
- Yaire Catalina López Santana
- Daniel David Delgado Cervantes

Avance del proyecto: Documento

¿Qué es?

PenTest

Un PenTest, o prueba de penetración, es un tipo de ciberataque simulado y autorizado el cual es utilizado contra diferentes tipos de redes y servidores con el fin de identificar las posibles vulnerabilidades del sistema que podrían ser explotadas en el caso de un ataque real. ¹

En este sentido, el PenTesting, es una herramienta invaluable en cuanto a medir la seguridad de una red se refiere puesto que este permite conocer las falencias de seguridad sin tener que exponer la red, y más importante, información sensible; y corregir los problemas antes que se presenten.

El PenTest, se realiza, normalmente, en cuatro partes. Recolección de información, análisis de vulnerabilidades, *olfateo* y suplantación de tráfico, y pruebas de estrés.

IDS

IDS, o *Intruder Detection System* por sus siglas en inglés, es definido como una herramienta de seguridad informática la cual está encargada de realizar monitoreo de los eventos que ocurren dentro de la red con el fin de detectar cualquier tipo de acceso no autorizado al sistema. ²

Monitoreo de la red

¿Para qué sirve?

PenTesting

Como se había establecido antes, el PenTesting tiene la principal función de ser una herramienta para la detección de vulnerabilidades dentro de un sistema o red dada. En este sentido, está pensado como una herramienta que permite la evaluación de la seguridad de una red respecto a los posibles ataques reales. ¹

IDS

Los IDS, tienen como función principal la detección de accesos no autorizados a una red o servidor. Estos, tras la detección, y dependiendo del tipo de IDS, realiza una serie de acciones con el fin de alertar la intrusión, en el caso de los IDS pasivos; o expulsar de la red al atacante, en el caso de los IDS activos. ²

Estos funcionan como medida de protección contra ataques o meramente como sistemas de alarma dentro de los servidores.

Estado del arte

PenTest, PenTesting y pruebas de penetración

Estructura:

- Cienciometría de PenTest
 - Interés de los últimos 20 años
 - Incremento del interés del PenTest como materia de estudio
- Principales herramientas de PenTest
 - ¿Cuales son?
 - ¿Qué tienen de especial?
- Técnicas de PenTest
 - ¿Cuales son?
 - ¿Qué hacen diferente?
 - ¿Qué ventajas posee?

IDS

- Cienciometría de los IDS
 - Interés de los últimos 20 años
 - Incremento del interés de los IDS como materia de estudio
- Principales herramientas de IDS
 - ¿Cuales son?
 - ¿Qué tienen de especial?
- Técnicas de PenTest
 - ¿Cuales son?
 - ¿Qué hacen diferente?
 - ¿Qué ventajas posee?

¿Cómo se implementa?

PenTest

IDS

Referencias

1. José, G. (2017). Introducción al pentesting. [Trabajo de Grado, Universidad de Barcelona]. Dipòsit Digital de la Universitat de Barcelona. Recuperado de <http://diposit.ub.edu/dspace/bitstream/2445/124085/2/memoria.pdf>.
2. Emilio, M. (2002). Implantación de un Sistema de Detección de Intrusos en la Universidad de Valencia. [Trabajo de Grado, Universidad de Valencia]. Red Iris. Recuperado de <https://www.rediris.es/cert/doc/pdf/ids-uv.pdf>