Universidad Corporativa | Programas Académicos

Ingeniería en Desarrollo de Software

Actividad | # 2 | Prevención de Fuentes de Ataques e Intrusión

Seguridad Informática I

Ingeniería en Desarrollo de Software

academia global

TUTOR: Jessica Hernández Romero

ALUMNO: Casandra Montserrat Ortiz Cortes

FECHA:08/09/2025

Índice

INTRODUCCION

La Evaluación de Seguridad en Aplicaciones Web es clave para organizaciones que desarrollan o utilizan plataformas digitales, portales de clientes, e-commerce.
ejerce el control de acceso en una red informática para proteger a los sistemas computacionales de ataques y abusos. La tecnología de prevención de intrusos es considerada por algunos como una extensión de los sistemas de detección de intrusos (IDS), pero en realidad es otro tipo de control de acceso, más cercano a las tecnologías cortafuegos. Los IPS fueron inventados de forma independiente por Jed Haile y Vern Paxon para resolver ambigüedades en la monitorización pasiva de redes de computadoras, al situar sistemas de detecciones en la vía del tráfico. Los IPS presentan una mejora importante sobre las tecnologías de cortafuegos tradicionales, al tomar decisiones de control de acceso basados en los contenidos del tráfico, en lugar de direcciones IP o puertos de los sistemas IDS, continúan en relación.

DESCRIPCION

La infraestructura de la institución de Veracruz, con sus salones y departamentos y edificios, así como el centro de cómputo y la biblioteca, requiere sus factores de riesgo y recomendaciones incluyendo sus fuentes de riesgo e intrusos , lo que se debe checar cuales son esa partes de fallas de cada amenaza y vulnerabilidad diferencia de las vulnerabilidades identificadas, como la falta de control de accesos y la deficiencia en instalaciones eléctricas, representan riesgos significativos que podrían ser explotados, poniendo en peligro la seguridad de equipos y datos críticos, estas pueden encontrarse en diferentes niveles: físico, como instalaciones sin control de acceso o equipos, lógico, como sistemas desactualizados, contraseñas débiles o ausencia de copias de seguridad; y humano, derivado de la falta de capacitación o el descuido de los usuarios. son los eventos, intencionales o accidentales, que pueden aprovechar dichas vulnerabilidades para causar algún daño o ataque Wifi o Web.

JUSTIFICACION

Un Sistema de Prevención de Intrusos o Intrusion Prevention System ("IPS" en sus siglas en inglés), es un dispositivo de seguridad de red que monitoriza el tráfico de red y/o las actividades de un sistema, en busca de actividad maliciosa. Entre sus principales funciones, se encuentran no sólo la de identificar la actividad maliciosa, sino la de intentar detener esta actividad. Siendo esta última una característica que distingue a este tipo de dispositivos de los llamados Sistemas de Detección de Intrusos o Intrusion Detection Systems ("IDS" en sus siglas en inglés).

Detección estadística de anormalidades: El IPS analiza el tráfico de red por un determinado periodo de tiempo y crea una línea base de comparación. Cuando el tráfico varía demasiado con respecto a la línea base de comportamiento, se genera una alarma.
Detección no estadística de anormalidades: En este tipo de detección, es el administrador quien define el patrón «normal».

DESARROLLO

TABLAS DE RECOMENDACIONES

	Amenazas humanas	**Amenazas Lógicas**	**Amenazas Físicas**	**Vulnerabilidades de almacenamiento**	**Vulnerabilidades De comunicación**
Factor de riesgo	Filtración de datos, al acceder a las redes sociales en correos electrónicos. Archivos e imágenes infectadas de enlaces por fraudes enviados por números desconocidos.	Posibles amenazas en los datos personales expuestos, accesos no autorizados.	Los fenómenos naturales como huracanes , inundaciones , sismos, también los daños en los edificios que no es muy seguro para los alumnos.	Fallas de seguridad, error en la configuración del servidor, manipulación incorrecta.	Acceso directo a la red, vulnerabilidad en la conexión de Wi-Fi
Recomendaciones	Se puede utilizar el monitoreo en los sitios que se visiten para detectar cualquier sospecha.	Habilitar el firewall para hacer escaneo de exploración, en los programas para detectar cualquier amenaza . Enseñar al personal para el manejo adecuado de la navegación segura.	Tener un protocolo preventivo de algún desastre natural y evitar riesgos , tener las copias de seguridad de los datos del instituto, y tener un seguro social para daños.	Actualizar el sistema operativo, tener el control de la temperatura,, copias de seguridad en la base de datos y tener en la nube con una contraseña que asegure que ningún intruso entre al sistema.	Seguridad del cableado, en la red de Wi-Fi, monitoreo no autorizado, equipos críticos.
Fuente de ataque e intrusos	Fuentes de ataques en sitios web no	El equipo puede ser expuesto por	Fenómenos naturales , fallas técnicas, Riesgo de	Servicios expuestos, vulnerabilidad en	Acceso a la red interna, ataques en la red inalámbrica por

	seguros como anuncios publicitarios descargas de sitios web.	hackers , la vulnerabilidad en la seguridad de los datos y programas.	sobrecalentamiento , hackers y robos externos.	el sistema operativo, daño en el hardware, fallas o mantenimiento del servidor en accesos no autorizados.	contraseñas, dispositivos personales.

CONCLUSION

Los Sistemas de Prevención de Intrusiones (IPS) son indispensables en el panorama cibernético actual, ya que ofrecen detección y bloqueos proactivos de amenazas para proteger su red. Al abordar las vulnerabilidades de las aplicaciones, prevenir el malware y contrarrestar los intentos de acceso no autorizado, los IPS mejoran la seguridad general. Al integrarse con otras soluciones de seguridad y utilizar métodos de detección avanzados, los IPS proporcionan una protección integral y aumentan la eficiencia operativa.

A medida que las ciberamenazas se vuelven cada vez más sofisticadas, la necesidad de contar con medidas de seguridad robustas es primordial. Aproveche el poder de IPS para fortalecer su infraestructura de seguridad y proteger sus activos digitales. Este enfoque proactivo no solo mejora la detección y la respuesta ante amenazas, sino que también agiliza las operaciones al minimizar las alertas innecesarias y optimizar el uso de recursos, una defensa más robusta contra las ciberamenazas.

REFERENCIA

Nason, A. (2024, 3 junio). What is an Intrusion Prevention System (IPS)? Coro Cybersecurity. https://www.coro.net/glossary/intrusion-prevention-system-ips

¿Qué es un IPS (Sistema de Prevención de Intrusiones)? | Fortinet. (s. f.). Fortinet. https://www.fortinet.com/lat/resources/cyberglossary/what-is-an-ips#:~:text=Definici%C3%B3n%20de%20Sistema%20de%20prevenci%C3%B3n,una%20posible%20filtraci%C3%B3n%20de%20seguridad.