UNEMI
UNIVERSIDAD ESTATAL DE MILAGRO

FACULTAD DE CIENCIAS E INGENIERÍA
CARRERA DE INGENIERÍA DE SOFTWARE

TEMA:

DETECCIÓN DE INTRUSOS Y PROTECCIÓN FRENTE A VIRUS

AUTORES:

ANGIE DAYANNA MENDOZA BARRETO

GABRIEL LEONARDO HASQUI ORTEGA

WILMER JOSUE ESPINOZA OLVERA

ASIGNATURA:

SISTEMAS OPERATIVOS

DOCENTE:

JAVIER RICARDO BERMEO PAUCAR

FECHA DE ENTREGA:

1 DE NOVIEMBRE DEL 2024

PERIODO:

abril 2024 a agosto 2025

MILAGRO-ECUADOR

Índice

1. Introducción

La detección de intrusos es un componente crucial en la seguridad informática que se enfoca en identificar y responder a actividades sospechosas o no autorizadas en un sistema o red. Este proceso puede ser llevado a cabo mediante sistemas de detección de intrusos (IDS), que monitorizan el tráfico de la red y los eventos del sistema para detectar patrones inusuales o conocidos que indiquen un posible ataque. La implementación efectiva de un IDS permite a las organizaciones identificar amenazas potenciales en tiempo real y tomar medidas correctivas antes de que causen daño significativo.

La protección frente a virus es otra pieza fundamental en la defensa cibernética, enfocándose en prevenir, detectar y eliminar programas maliciosos que pueden infectar un sistema. Los virus informáticos son softwares malintencionados que pueden replicarse y propagarse de un equipo a otro, causando desde pérdida de datos hasta el control total del sistema por parte de un atacante. Para combatir estos programas, se utilizan herramientas de antivirus que escanean archivos y comportamientos del sistema en busca de signos de infección. Estas herramientas emplean tanto bases de datos de firmas de virus conocidos como técnicas heurísticas para identificar nuevas amenazas. La actualización constante de los programas antivirus es esencial para mantener una defensa eficaz contra las amenazas emergentes.

Ambos aspectos, la detección de intrusos y la protección frente a virus, son componentes complementarios en una estrategia de ciberseguridad robusta. Mientras que los IDS ayudan a identificar y responder a intentos de intrusión y actividades anómalas, los antivirus se centran en prevenir y eliminar programas maliciosos. Juntos, estos sistemas contribuyen a crear una barrera multifacética que protege la integridad, confidencialidad y disponibilidad de los recursos informáticos en una organización. La integración y correcta administración de estas herramientas son esenciales para mitigar riesgos y asegurar un entorno digital seguro.

2. Desarrollo

2.1. Detección de intrusos, conceptualización

La detección de intrusos es un proceso en la ciberseguridad que implica la identificación y respuesta a actividades no autorizadas o sospechosas dentro de un sistema informático o red. Este proceso se realiza a través de sistemas de detección de intrusos (IDS), que monitorizan y analizan continuamente el tráfico de red, los registros del sistema y otros eventos relacionados con la seguridad para identificar posibles amenazas.

2.2. Ventajas

Entre las ventajas de un IDS tenemos:

- Permite identificar incidentes de seguridad gracias al registro que hace de ellos.
- Puede ayudar a identificar problemas o errores de seguridad en la red o en los dispositivos.
- Permite el monitoreo de la red y los dispositivos en tiempo real.
- Puede ayudar a automatizar nuevos patrones de búsqueda de amenazas en los paquetes de datos enviados a través de la red.
- Ayuda con el cumplimiento normativo en materia de ciberseguridad y seguridad de la información.

2.3. Desventajas

Las desventajas de los IDS:

- No previene los ataques por sí solo; su principal función es la detección.
- Puede generar falsos positivos que requieren tiempo y recursos para investigar.
- Requiere un monitoreo constante y personal dedicado para analizar y responder a las alertas.
- Requiere actualizaciones y ajustes frecuentes para mantener su

eficacia.

2.4. 3 ejemplos de detección de intrusos

Algunos ejemplos de sistemas de detección de intrusos (IDS) son Snort, Suricata, Ossec.

- **Snort:** Es uno de los IDS más conocidos y utilizados en el mundo. Snort es una herramienta de código abierto que realiza análisis de tráfico en tiempo real y detección de intrusos en redes IP.
- **Suricata:** Similar a Snort, Suricata es un motor de detección de intrusos de código abierto que puede realizar inspección profunda de paquetes, detección de intrusos, monitoreo de seguridad de la red y registro de eventos.
- **Ossec**: Es un sistema de detección de intrusos basado en host (HIDS) que es de código abierto y ofrece capacidades de monitoreo de archivos, análisis de registros, detección de rootkits y respuesta activa a incidentes.

2.5. Protección frente a virus, conceptualización

La protección frente a virus es una práctica esencial en la ciberseguridad que busca prevenir, detectar y eliminar programas maliciosos conocidos como virus, los cuales pueden infectar sistemas informáticos y causar diversos tipos de daño, desde la corrupción de datos hasta el control remoto del equipo afectado. Esta protección se realiza principalmente mediante el uso de software antivirus y otras herramientas de seguridad que trabajan de manera conjunta para mantener la integridad y seguridad del sistema.

2.6. Ventajas

Las ventajas de la protección frente a virus son:

- **Prevención de Infecciones:** El software antivirus ayuda a prevenir la infección de sistemas por virus y otros tipos de malware, manteniendo así la integridad y funcionalidad del sistema.
- **Detección Temprana:** Los antivirus pueden detectar y neutralizar amenazas rápidamente, minimizando el tiempo que un virus tiene para causar daño.
- **Protección en Tiempo Real:** La mayoría de los antivirus modernos ofrecen protección en tiempo real, escaneando archivos y actividades en el sistema de manera continua.
- **Actualizaciones Automáticas:** Las bases de datos de firmas de virus se actualizan automáticamente, lo que permite al software antivirus reconocer y combatir nuevas amenazas de manera eficaz.

2.7. Desventajas

Las desventajas de la protección frente a virus:

- **Falsos Positivos:** Los antivirus pueden generar falsos positivos, identificando archivos legítimos como amenazas, lo que puede interferir con el funcionamiento normal del sistema.
- **Impacto en el Rendimiento:** La ejecución de un antivirus, especialmente durante los escaneos completos del sistema, puede consumir una cantidad significativa de recursos, ralentizando el rendimiento del sistema.
- **Costos:** Los antivirus de calidad suelen tener costos asociados, ya sea en forma de suscripciones anuales o tarifas únicas, lo que puede representar un gasto adicional para los usuarios y organizaciones.
- **Dependencia de Firmas**: Los antivirus basados en firmas pueden ser menos eficaces contra amenazas nuevas o modificadas que no están incluidas en la base de datos de firmas.

- **Complejidad en la Configuración:** Algunos programas antivirus pueden ser complejos de configurar y mantener, especialmente en entornos empresariales con múltiples sistemas y usuarios.

2.8. 3 ejemplos de Protección frente a virus

- **Norton Antivirus:** es una solución de seguridad integral que protege los sistemas contra virus, malware, spyware y ransomware. Ofrece protección en tiempo real y cuenta con funciones adicionales como control parental, firewall, y protección de la identidad en línea.
- **Kaspersky Antivirus:** es reconocido por su alta tasa de detección de amenazas. Proporciona protección contra virus, malware y otras amenazas cibernéticas, además de ofrecer herramientas adicionales como protección de la webcam, VPN, y monitoreo de actividades en línea para prevenir ataques de phishing y fraude.
- **Bitdefender Antivirus:** combina un rendimiento eficiente con una interfaz fácil de usar. Ofrece protección en tiempo real, escaneo basado en la nube, y herramientas avanzadas como un gestor de contraseñas, protección contra ransomware y un navegador seguro para transacciones financieras.

3. Conclusión

Podemos decir que la ciberseguridad abarca una variedad de estrategias y herramientas diseñadas para proteger sistemas informáticos contra amenazas como intrusos y virus. La detección de intrusos se centra en la identificación y respuesta a actividades no autorizadas, mientras que la protección frente a virus se enfoca en prevenir, detectar y eliminar programas maliciosos que pueden comprometer la integridad de los sistemas.

Los sistemas de detección de intrusos (IDS) como Snort, Suricata y Ossec, junto con software antivirus como Norton, Kaspersky y Bitdefender, son ejemplos clave de herramientas utilizadas para fortalecer la seguridad cibernética. Estas soluciones no solo ayudan a prevenir y detectar amenazas, sino que también ofrecen protección en tiempo real, actualizaciones automáticas y funcionalidades adicionales para garantizar la seguridad integral de los sistemas.

Sin embargo, estas medidas de protección no están exentas de desafíos, como el riesgo de falsos positivos, el impacto en el rendimiento del sistema y los costos asociados con la implementación y mantenimiento de estas soluciones. A pesar de estas consideraciones, una implementación adecuada y una gestión eficaz de estas herramientas son fundamentales para mitigar riesgos y mantener un entorno digital seguro y protegido contra las amenazas emergentes en el panorama cibernético actual.

Bibliografía

Ramírez, H. (2021, septiembre 28). *El sistema de detección de intrusiones (IDS)*. Grupo Atico34; Ático34 Protección de datos para empresas y autónomos. https://protecciondatos-lopd.com/empresas/sistema-deteccion-intrusiones-ids/

Escalante, M. (2023, junio 27). *Qué es un Sistema de Detección de Intrusiones (IDS)*. abcXperts; ABC Xperts by Academy Xperts. https://abcxperts.com/que-es-un-sistema-de-deteccion-de-intrusiones-ids/

TREND. (2018). *Ventajas de la protección*. Trendmicro.com. https://docs.trendmicro.com/es-es/documentation/article/worry-free-business-security-services-66-security-agent-help-benefits-of-protecti

La importancia de tener un buen antivirus. (2022, junio 21). Punt. https://www.puntsistemes.es/blog/sistema-antivirus/

RomeroSeguir, E. J. (2010, diciembre 6). *Ventajas y desventajas de los antivirus*. SlideShare. https://es.slideshare.net/slideshow/ventajas-y-desventajas-de-los-antivirus/6056895