HACKING ÉTICO

Unidad 1. Actividad 13

5 DE DICIEMBRE DE 2023

CARLOS DÍAZ MONTES
ESPECIALIZACIÓN DE CIBERSEGURIDAD

Índice

Enunciado

Son herramientas destinadas a la protección de sistemas informáticos: servidores, ordenadores de sobremesa, portátiles, dispositivos móviles, etc., frente a todo tipo de software malicioso.-

¿Qué es?

"Antimalware" es un término que se utiliza para describir software diseñado para detectar, prevenir y eliminar software malicioso o malware en un sistema informático. El malware es un término general que abarca una variedad de software malicioso, incluyendo virus, troyanos, gusanos, spyware, adware y otros tipos de amenazas que pueden comprometer la seguridad y el rendimiento de un sistema.

Un programa antimalware, también conocido como programa antivirus, es una herramienta esencial para proteger los sistemas contra las amenazas en línea y fuera de línea. Estos programas utilizan una variedad de técnicas para identificar y eliminar el malware, como el análisis heurístico, las firmas de virus, el análisis de comportamiento y la protección en tiempo real.

Funciones

- Análisis de virus y malware: Escanea archivos y programas en busca de patrones de código malicioso o comportamientos sospechosos.

- Protección en tiempo real: Supervisa constantemente la actividad en el sistema para detectar y bloquear amenazas en el momento en que ocurren.

- Actualizaciones de definiciones: Actualiza regularmente su base de datos de definiciones de malware para reconocer nuevas amenazas.

- Protección contra amenazas en línea: Proporciona protección contra amenazas mientras navegas por Internet, descargas archivos y utilizas aplicaciones en línea.

- Cuarentena y eliminación: Aísla o elimina archivos infectados para evitar la propagación del malware.

Tipos

- Antivirus: Este es el tipo más básico de software antimalware. Los programas antivirus están diseñados para detectar, bloquear y eliminar virus y otros tipos de malware. Utilizan firmas de virus y heurísticas para identificar amenazas conocidas y comportamientos sospechosos.

- Antispyware: Este tipo de software está especializado en detectar y eliminar spyware, que es un tipo de malware diseñado para recopilar información sobre actividades en línea y enviarla a terceros sin el conocimiento del usuario.

- Antiadware: Enfocado en bloquear y eliminar programas de adware, que muestran anuncios no deseados en el sistema. El adware a menudo se instala junto con software gratuito y puede afectar la experiencia del usuario con anuncios invasivos.

- Antimalware de comportamiento: Este tipo de software analiza el comportamiento de los programas y procesos en tiempo real. Si detecta actividad sospechosa o comportamientos maliciosos, puede bloquear o tomar medidas para prevenir posibles amenazas.

- Antiransomware: Especializado en prevenir y combatir ransomware, que cifra archivos en el sistema y exige un rescate para su liberación. Algunos programas antiransomware pueden detectar patrones de cifrado y bloquear estos ataques.

- Firewalls personales: Aunque no son exclusivamente antimalware, los firewalls personales pueden ayudar a prevenir intrusiones y bloquear conexiones no autorizadas. Pueden ser parte integral de un conjunto de herramientas de seguridad.

- Antiphishing: Diseñado para detectar y bloquear sitios web y correos electrónicos de phishing que intentan engañar a los usuarios para que revelen información confidencial, como contraseñas y detalles de cuentas.

- Antispam: Aunque más comúnmente asociado con el correo electrónico, los programas antispam pueden ayudar a filtrar mensajes no deseados y posiblemente maliciosos.

Recomendaciones

- Mantener los sistemas actualizados y libres de virus y vulnerabilidades es crucial para protegernos contra ataques cibernéticos y malware.

- Concienciar a nuestros empleados sobre el uso adecuado de los sistemas corporativos es esencial. Esto incluye evitar la instalación no autorizada de software, no navegar por páginas web de contenido dudoso y cumplir con todas las directrices establecidas en la política de seguridad de la empresa.

- Mantener actualizados los sistemas operativos y aplicaciones reduce los riesgos potenciales de seguridad.

- Evitar la descarga e instalación de programas desde sitios web que no ofrezcan garantías es una medida preventiva importante.

- Utilizar redes seguras para todas las comunicaciones con clientes y emplear cifrado cuando se intercambie información especialmente sensible son prácticas recomendadas.

- Realizar copias periódicas de seguridad, que incluyan los datos del cliente que debemos proteger, es fundamental para la prevención de pérdida de información.

- Contar con procedimientos de restauración para estas copias garantiza que estemos preparados para recuperar la información en caso de cualquier eventualidad.