INCIDENTES DE CIBERSEGURIDAD

Unidad 1. Actividad 21

30 DE ENERO DE 2024

CARLOS DÍAZ MONTES
ESPECIALIZACIÓN DE CIBERSEGURIDAD

Índice

Enunciado

Realiza un informe que explique las características básicas de esta herramienta :

1º.- Perfil comercial.-

2º.- Utilidad básica.-

3º.- Aplicación en nuestra organización de recursos.-

4º.- Necesidad de recursos para su puesta en funcionamiento.-

Snort

¿Qué es?

Snort es un sistema de detección de intrusos en red (IDS, por sus siglas en inglés) de código abierto y ampliamente utilizado. Fue creado por Martin Roesch en 1998 y desde entonces ha sido una herramienta popular en el ámbito de la seguridad informática.

El propósito principal de Snort es monitorear y analizar el tráfico de red en busca de actividades sospechosas o maliciosas. Funciona mediante la captura de paquetes de red y la aplicación de reglas predefinidas para detectar patrones que puedan indicar actividades maliciosas, como intentos de intrusión, escaneo de puertos, tráfico de malware, entre otros.

Snort puede ser utilizado tanto como un sistema de detección de intrusos (IDS), que alerta sobre posibles amenazas, como también en modo de prevención de intrusiones (IPS), donde puede bloquear automáticamente el tráfico considerado malicioso.

Además de ser una herramienta de seguridad altamente eficaz, Snort es conocido por su flexibilidad y extensibilidad. Los usuarios pueden crear y personalizar sus propias reglas para adaptarse a las necesidades específicas de su red, lo que lo convierte en una opción popular tanto para pequeñas empresas como para grandes organizaciones.

Perfil comercial

Para un perfil comercial, Snort puede significar varias cosas dependiendo de las necesidades y el enfoque de la organización en cuestión:

- **Seguridad de la red:** Snort proporciona una capa adicional de seguridad para la infraestructura de red de una empresa. Esto puede ser crucial para proteger los activos digitales y la información confidencial contra intrusiones maliciosas, ataques de malware y otras amenazas cibernéticas.

- Cumplimiento normativo: Para muchas empresas, el cumplimiento de regulaciones y estándares de seguridad es un requisito importante. Snort puede ayudar a cumplir con ciertos requisitos de cumplimiento, ya que proporciona capacidades de monitoreo y detección de intrusiones que pueden ser necesarias según las regulaciones aplicables.

- Reducción de riesgos: Al detectar y responder rápidamente a actividades sospechosas en la red, Snort puede ayudar a reducir los riesgos de brechas de seguridad y pérdida de datos. Esto puede ser especialmente valioso para empresas que manejan información sensible o que son blanco frecuente de ataques cibernéticos.

- Mejora de la visibilidad de la red: Snort no solo detecta intrusiones, sino que también proporciona visibilidad sobre el tráfico de red y los posibles puntos débiles en la infraestructura. Esto permite a las empresas identificar y abordar proactivamente problemas de seguridad, así como optimizar el rendimiento de la red.

- Ahorro de costos a largo plazo: Aunque implementar y mantener Snort puede requerir una inversión inicial, a largo plazo puede ayudar a ahorrar costos asociados con incidentes de seguridad, pérdida de datos, interrupciones del negocio y daños a la reputación de la empresa.

Utilidades básicas

- Detección de intrusiones en tiempo real: Snort es principalmente conocido por su capacidad para detectar intrusiones en tiempo real. Analiza el tráfico de red en busca de patrones y firmas conocidas de ataques, alertando a los administradores sobre posibles amenazas.

- Registro de eventos: Snort puede registrar eventos de red significativos, como intentos de intrusión, escaneo de puertos, tráfico sospechoso y otros eventos relevantes. Estos registros pueden ser utilizados para investigaciones forenses, análisis de incidentes y auditorías de seguridad.

- Análisis de tráfico: Snort proporciona herramientas para analizar el tráfico de red capturado, lo que ayuda a identificar patrones de comportamiento anómalos y posibles vulnerabilidades en la infraestructura de red.

- Generación de alertas: Cuando Snort detecta una actividad sospechosa o maliciosa, puede generar alertas para notificar a los administradores de seguridad. Estas alertas pueden ser

enviadas por correo electrónico, mensajes de texto u otros métodos de notificación configurados.

- Bloqueo de tráfico: En modo de prevención de intrusiones (IPS), Snort puede bloquear automáticamente el tráfico identificado como malicioso, ayudando a prevenir ataques antes de que comprometan la seguridad de la red.

- Personalización de reglas: Snort permite a los administradores de seguridad crear y personalizar reglas de detección para adaptarse a las necesidades específicas de su red y para abordar las amenazas emergentes.

- Integración con otras herramientas de seguridad: Snort puede integrarse con otras herramientas de seguridad, como firewalls, sistemas de gestión de eventos e información de seguridad (SIEM), y soluciones de análisis de vulnerabilidades, para proporcionar una defensa en capas más completa contra las amenazas cibernéticas.

Aplicación en nuestra organización de recursos.

- Detección de amenazas en la red: Snort puede monitorear el tráfico de red dentro del centro educativo en busca de posibles amenazas, como intentos de intrusión, malware o tráfico malicioso. Esto ayuda a proteger la red contra posibles ataques y a mantener la integridad de los sistemas informáticos.

- Control de acceso a Internet: Snort puede utilizarse para controlar y filtrar el tráfico de Internet, bloqueando el acceso a sitios web maliciosos o inapropiados. Esto es especialmente importante en un entorno educativo para proteger a los estudiantes de contenidos inapropiados y mantener un entorno de aprendizaje seguro.

- Detección de actividades no autorizadas: Snort puede alertar sobre actividades no autorizadas en la red, como intentos de acceso no autorizado a sistemas o recursos, escaneo de puertos o tráfico sospechoso. Esto ayuda a detectar y prevenir posibles infracciones de seguridad dentro del centro educativo.

- Monitoreo de uso de la red: Snort puede proporcionar información detallada sobre el uso de la red dentro del centro educativo, incluyendo qué aplicaciones y servicios están siendo utilizados, qué dispositivos están conectados a la red y cómo se está utilizando el ancho de banda. Esto puede ayudar a los administradores de red a optimizar el rendimiento de la red y a identificar posibles problemas de congestión.

- Cumplimiento de políticas de seguridad: Snort puede ayudar a hacer cumplir las políticas de seguridad de la red dentro del centro educativo, asegurando que se cumplan los estándares de seguridad establecidos y que se tomen medidas proactivas para proteger la red y los datos sensibles.

Necesidad de recursos para su puesta en funcionamiento

- Hardware: Se necesita hardware adecuado para ejecutar Snort de manera eficiente, especialmente si se está monitoreando una red grande o con un alto volumen de tráfico. Esto puede incluir servidores dedicados o máquinas virtuales con suficiente capacidad de procesamiento, memoria y almacenamiento para manejar el tráfico de red y ejecutar Snort junto con otros servicios necesarios.

- Sistema operativo: Snort es compatible con una variedad de sistemas operativos, incluidos Linux, BSD y Windows. Seleccionar el sistema operativo adecuado y configurarlo correctamente es importante para garantizar un rendimiento óptimo y una seguridad adecuada.

- Software adicional: Además de Snort, es posible que se necesiten otros programas o herramientas para complementar su funcionalidad. Esto puede incluir software de gestión de eventos e información de seguridad (SIEM) para el análisis y la correlación de eventos, así como herramientas de visualización para presentar los datos de forma clara y comprensible.

- Reglas y actualizaciones: Es importante mantener actualizadas las reglas de detección de Snort para proteger contra las últimas amenazas y vulnerabilidades. Esto puede requerir una suscripción a servicios de actualización de reglas o la configuración de un sistema automatizado para descargar y aplicar las actualizaciones regularmente.

- Personal capacitado: Se necesita personal capacitado para configurar, mantener y monitorear Snort de manera efectiva. Esto puede incluir administradores de red, analistas de seguridad y otros profesionales con experiencia en seguridad de la información y gestión de redes.