Universidad Corporativa | Programas Académicos

Ingeniería en Desarrollo de Software

Actividad 1 – Detección y prevención de ataques de acceso

Seguridad informática II

Ingeniería en Desarrollo de Software

Tutor:

Jessica Hernández Romero

Alumno:

Alejandro Abarca Gerónimo

Fecha:

19 de septiembre de 2024

Indice

Introducción

La seguridad de la tecnología de la información incluye una amplia gama de medidas de seguridad interdisciplinaria diseñada para proteger las redes informáticas y sus datos de cualquier forma de daño, fuga, filtración de información privada o ataques.

La ciberseguridad es fundamental para prevenir ataques e intentos de robo de información, violaciones de seguridad y daños a la propiedad. Los dispositivos de todo tipo, incluidas tabletas y teléfonos, corren cada vez más riesgos porque ahora almacenan más datos públicos y privados que la mayoría de las computadoras.

Dado que los ataques cibernéticos han aumentado exponencialmente durante años anteriores, la mayoría de las empresas y las personas enfrentan interrupciones comerciales y robo de datos.

Durante el desarrollo de esta actividad analizaremos el contexto presentado, ya que el objetivo es utilizar algunas técnicas de protección ante ataques de explotación y obtención de acceso a sistemas realizando auditorías a la red mediante herramientas tecnológicas ya sea especializadas o que presenten esta funcionalidad de auditoría, asi como también implementaremos los mecanismos de seguridad informática para detectar posibles vulnerabilidades y amenazas para prevenir posibles irregularidades y robo de información.

Descripción

Como objetivo principal durante esta actividad realizaremos el análisis de nuestro equipo con una herramienta de escaneo para detectar posibles amenazas y detección de intrusos, para ello se pretende utilizar técnicas de protección ante ataques de explotación y obtención de acceso a sistemas realizando auditorías a la red mediante herramientas tecnológicas ya sea especializadas o que presenten esta funcionalidad de auditoría.

Para lograrlo se requiere analizar los factores que enfatizan la importancia de la seguridad y que se describen a continuación:

- Prevenir los ataques de acceso.
- Prevenir accesos a las redes.
- Monitoreo completo de la red.

Se realizará la instalación de Nessus, este es un software que nos permitirá detectar y prevenir ataques de acceso del sistema y la red. La actividad a realizar será la siguiente: auditoría de vulnerabilidades en la red y para ello realizaremos los pasos siguientes:

- Instalar y analizar el equipo.
- Analizar un equipo en búsqueda de posibles ataques como son virus, accesos o percances en red.
- Adjuntar el reporte generado desde la herramienta o capturar el resultado del análisis.

Justificación

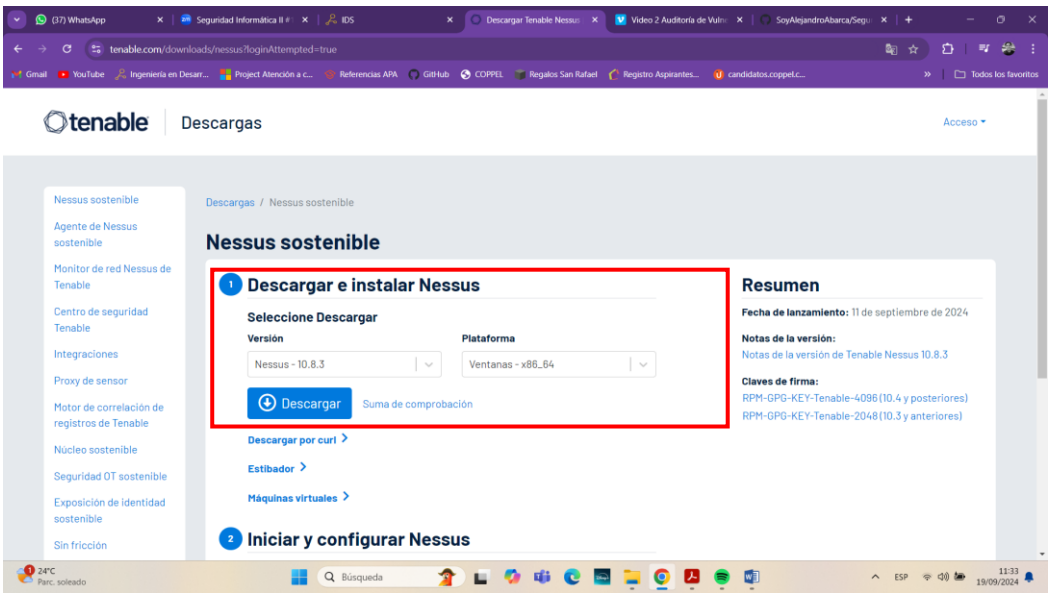
La ciberseguridad proporciona a los clientes y empresas protección contra los ciberataques. Si su información no está protegida, puede causar pérdidas financieras importantes y afectar su reputación como organización.

Los ciberataques representan una amenaza cada vez mayor para las empresas de todo el mundo. En los últimos años, con el aumento de los ataques a la información, los cortafuegos, el software antivirus y el software antispyware son esenciales para la seguridad operativa. Todos ellos incluyen un conjunto de procesos y herramientas, cuyo objetivo principal es proteger los recursos informáticos de la organización del uso no autorizado de los sistemas informáticos y sus recursos.

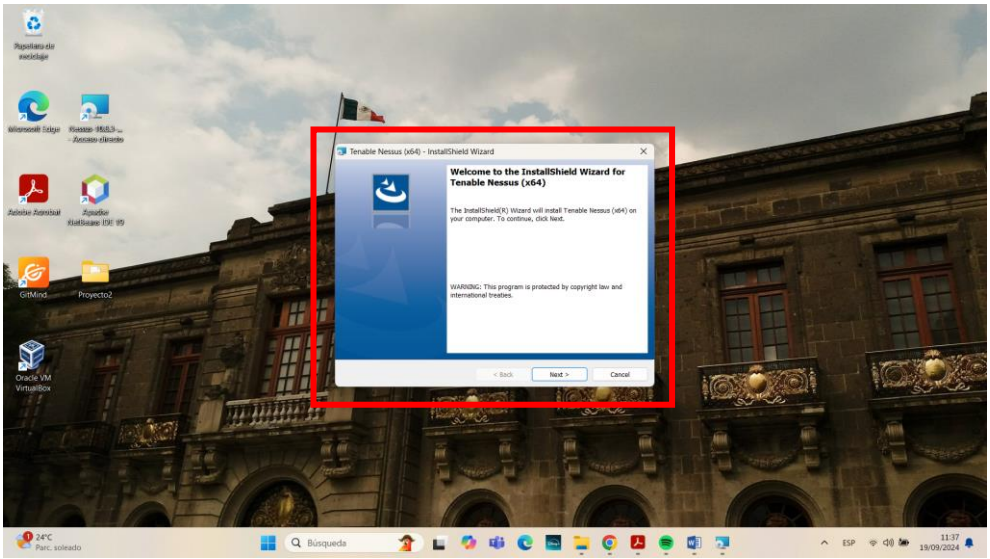
La protección incluye servidores e infraestructura de comunicaciones, sistemas informáticos, bases de datos, archivos y equipos terminales o puntos finales. En definitiva, todos los componentes informáticos que ayudan al funcionamiento de una empresa. Cuando se trata de ciberseguridad, la prevención es siempre la mejor opción, porque una vez que eres víctima de un ataque, la recuperación puede ser difícil. Por ello, es importante identificar los elementos que hacen de la ciberseguridad un aspecto importante.

Desarrollo:

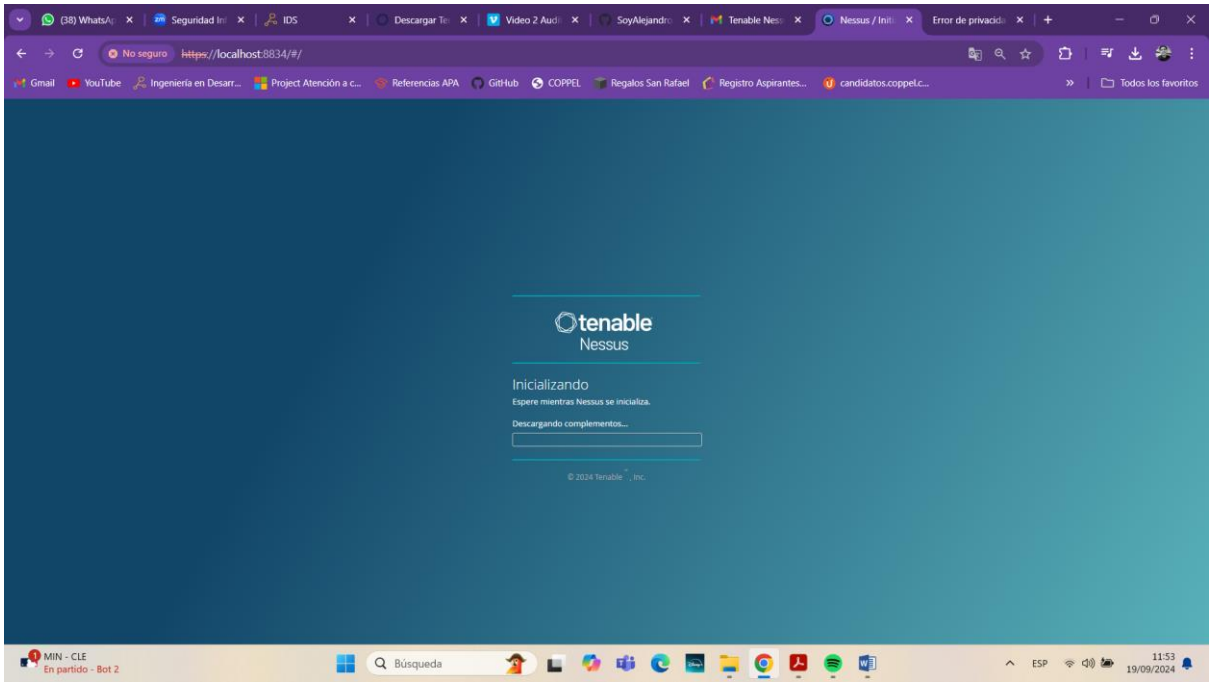
Proceso de búsqueda y descarga desde el sitio web oficial.



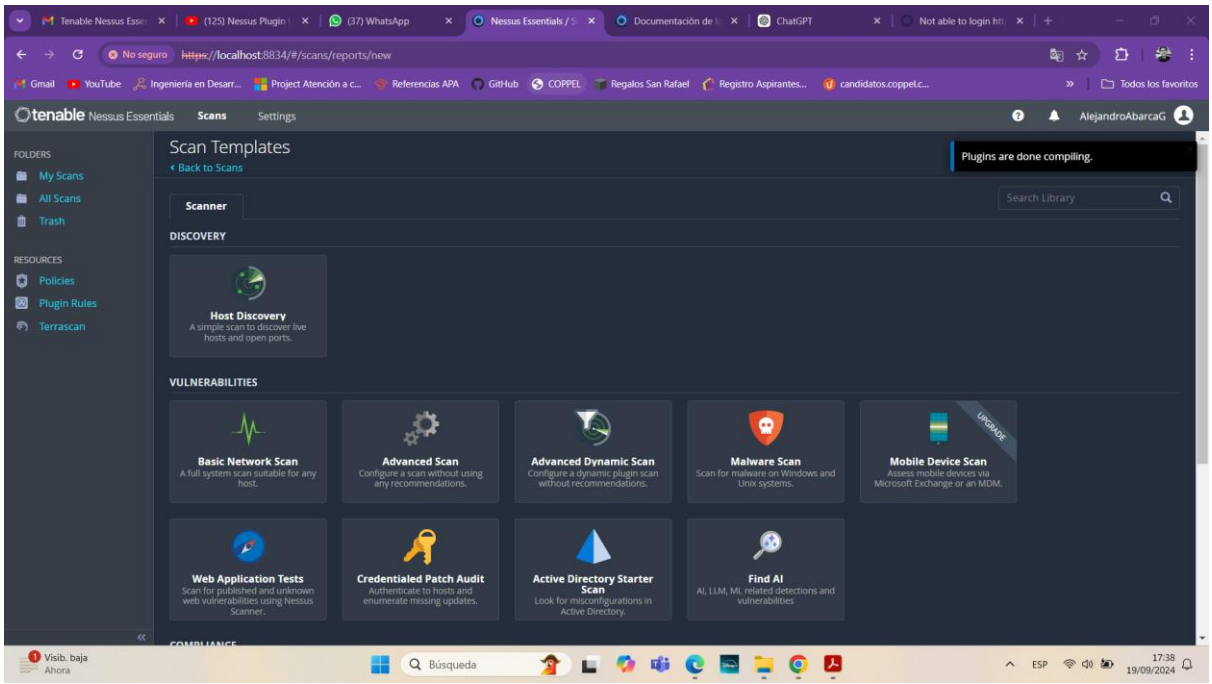
Instalación del Software en el equipo de cómputo para realizar la auditoria.



Termino de la instalación del Software una vez ingresados todos y cada uno de los datos para el registro y descarga de complementos.

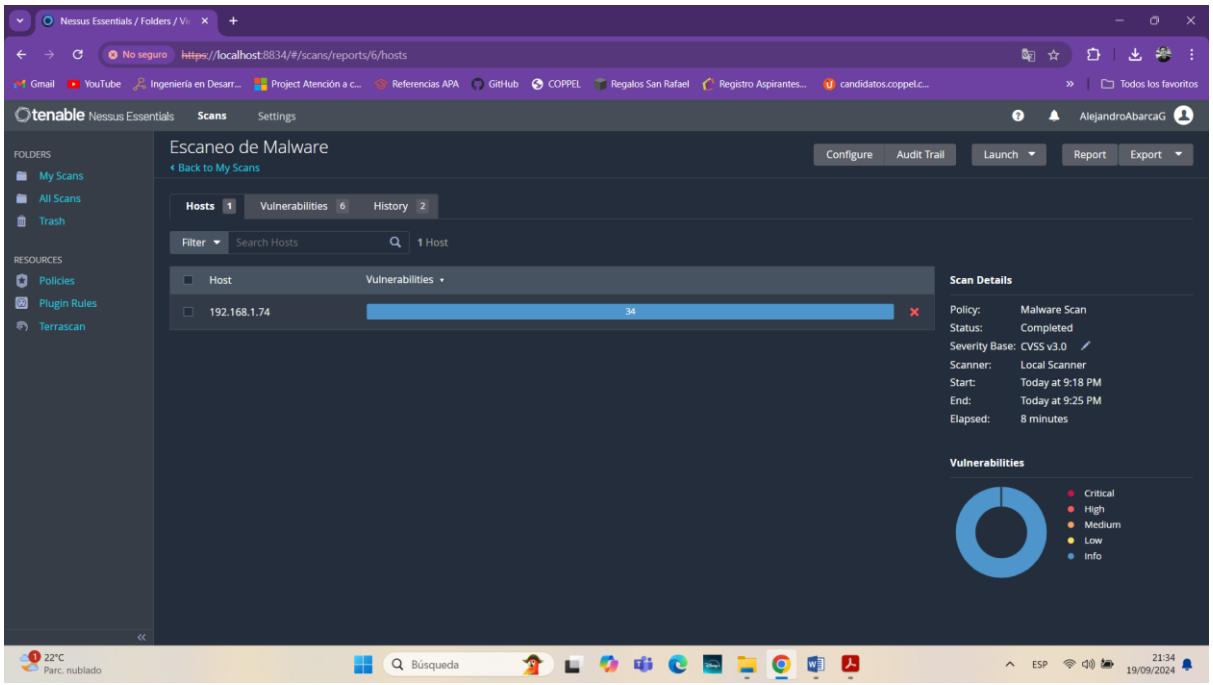


Acceso de la plataforma para realizar los escaneos de red y detectar las vulnerabilidades que se lleguen a tener en el equipo.

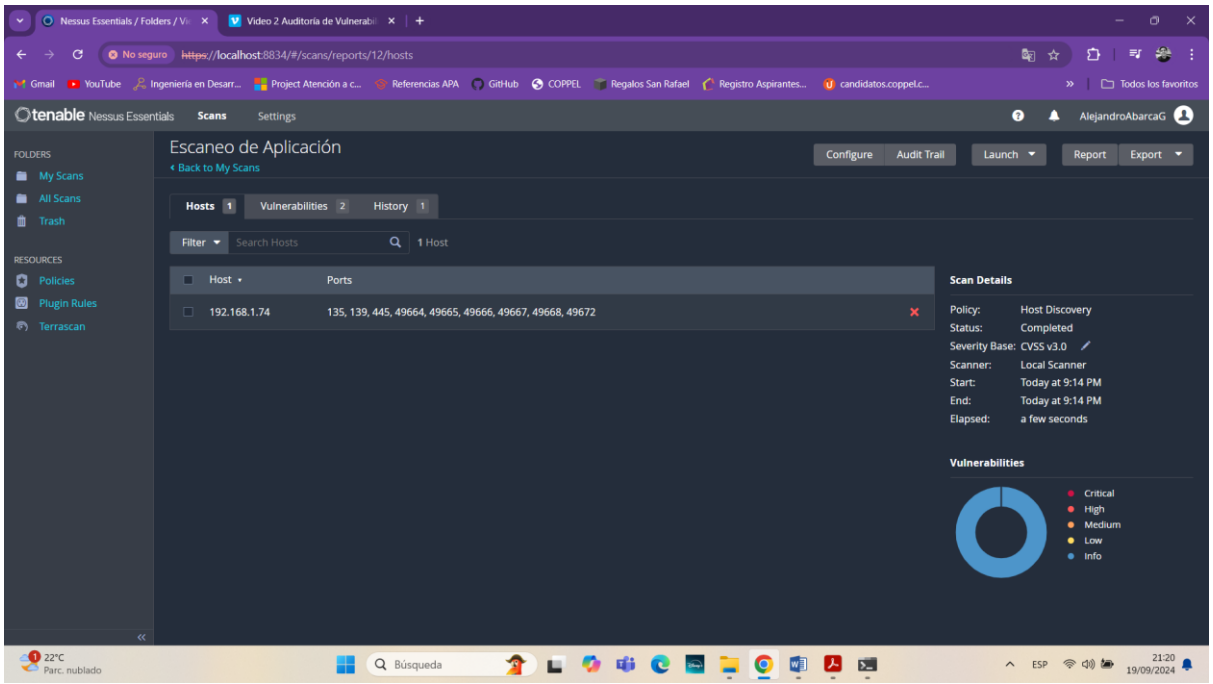


Incidencias encontradas

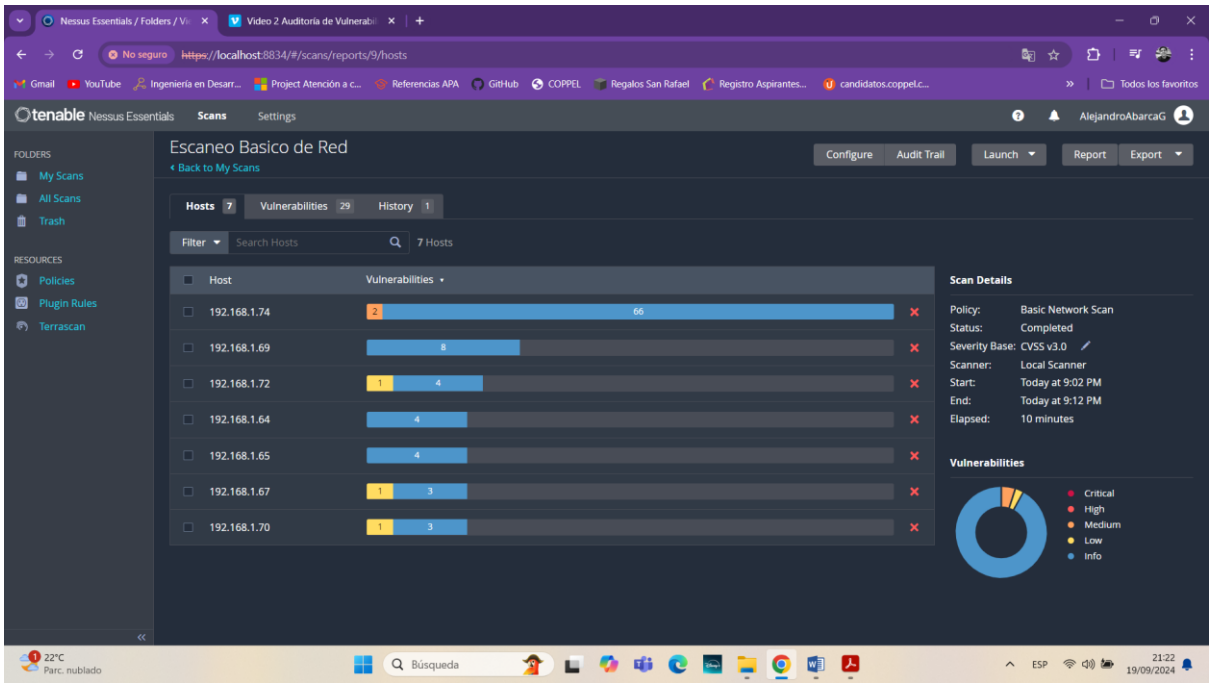
1. **Malware** detectados mediante el escaneo en la red local, link del reporte en el apartado reportes.



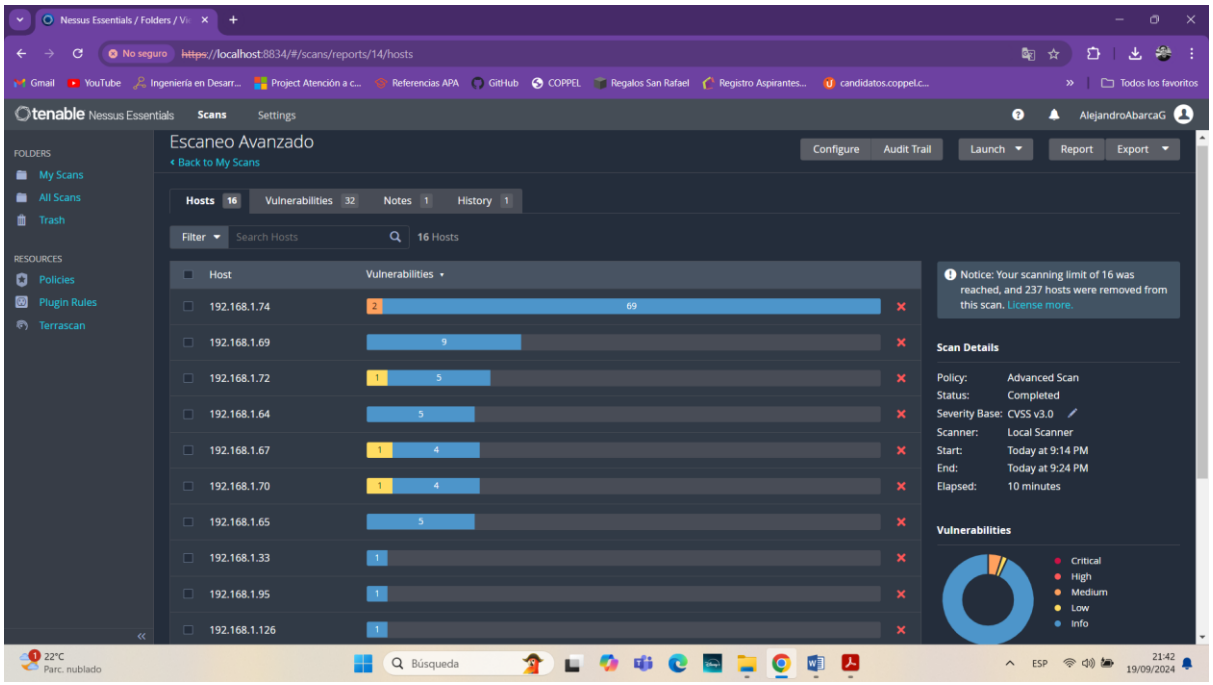
2. Detección de vulnerabilidades durante el **escaneo por aplicación**, link de reporte en el apartado reportes.



3. Durante el **escaneo básico de red** se muestran algunas de las IP utilizadas en el rango de red local las cuales presentan vulnerabilidades y se muestran detalladamente en el siguiente link en el apartado reporte.



4. Evidencia del escaneo avanzado realizado al equipo de cómputo donde se muestran las vulnerabilidades, link del resultado en el apartado reportes.



Reportes

1. https://drive.google.com/file/d/1iuqhYw8z8shnm74rZ5HiY9fLRcPfeRHL/view?usp=drive_link

2. https://drive.google.com/file/d/1lvHebN_zGFS1fag-UrPV7o5F8X3c3srW/view?usp=drive_link

3. https://drive.google.com/file/d/1anhzia69-f_xTkfiU9NKCF4buP5ldn0r/view?usp=drive_link

4. https://drive.google.com/file/d/1gJnsNJkm9wYHBGYGJK5KvUJoDQhboWFz/view?usp=drive_link

Análisis e Identificación de mejoras.

Puntos a mejorar:

Revisión periódica: Implementar revisiones periódicas para garantizar que IP forwarding esté deshabilitado en los sistemas que no deben enrutar paquetes.

Configuraciones seguras: Mantener políticas de seguridad que deshabiliten IP forwarding en sistemas que no requieren esta funcionalidad.

Deshabilitar servicios inseguros: Eliminar o desactivar servicios que no utilizan cifrado y que pueden ser vulnerables a la interceptación.

Seguridad de la red: Asegurarse de que todos los servicios críticos utilicen protocolos seguros como SSH en lugar de Telnet.

Habilitar firma SMB: Protege contra ataques de intermediario y asegura la autenticidad de las comunicaciones SMB.

Configuración adecuada: Verificar y asegurar que todas las configuraciones SMB están correctamente implementadas para prevenir ataques.

Políticas de firma de mensajes: Aplicar y mantener políticas que requieran la firma de mensajes en las comunicaciones SMB para proteger la integridad de los datos.

Conclusión

Durante el desarrollo de la actividad se realizaron algunos análisis a la red que se encuentra conectado el equipo de cómputo. Se realizó el análisis completo para detectar vulnerabilidades y amenazas que pudiera presentarse en la red local, la seguridad informática busca la preservación de la confidencialidad, integridad y disponibilidad de la información. Debido a que la información corporativa es uno de los activos más importantes que manejan las empresas, es importante invertir en un sistema de gestión que busque garantizar su protección. Existen diferentes maneras de recibir un ataque cibernético por lo cual las empresas deben estar preparadas y tener un plan de contingencia en caso de ser víctimas de un ataque cibernético.

Los computadores y toda la información contenida en ellos pueden ser blanco de delincuentes cibernéticos por medio de virus informáticos con los que buscan alterar el funcionamiento del dispositivo y así extraer, dañar o borrar datos.

Es importante estar preparados ante cualquier ataque teniendo en cuenta los principios básicos de la seguridad informática que son: integridad, confidencialidad, disponibilidad y autenticidad.

Referencias

1. *SEGURIDAD INFORMATICA.* (2024). HEWLETT PACKARD ENTERPRISE. Recuperado 1 de abril de 2024, de https://www.hpe.com/mx/es/what-is/it-security.html#:~:text=La%20seguridad%20de%20la%20tecnolog%C3%ADa,de%20informaci%C3%B3n%20privada%20o%20ataque