2.- Entregar los resultados de la Guía 2 de la materia de Sniffer, indicando

las vulnerabilidades que se presentan, su impacto y recomendaciones para

mitigarlas.

Guía 2 Sniffer

Una importante organización sospecha de ciertas negligencias en el equipo de Ingeniería de Sistemas y Redes que tiene a cargo la administración de la infraestructura productiva TIC.

Usando las herramientas de auditorías vistas en clases, verifique los servicios que poseen

los servidores 10.150.45.201 y la 10.150.45.202, mediante una escucha pasiva analice los

problemas de seguridad que posee este activo.

ip.addr == 10.150.45.201 or ip.addr == 10.150.45.202

**Introducción**

Este informe detalla los servicios activos y los posibles problemas de seguridad identificados en los servidores 10.150.45.201 y 10.150.45.202 a los cuales se le creo tráfico que se detallara en el transcurso del informe para un correcto análisis de este el cual se realizó mediante una escucha pasiva utilizando la herramienta Wireshark.

**Metodología**

* Se utilizó Wireshark para capturar y analizar el tráfico de red de forma pasiva y con el permiso adecuado para la captura de paquetes.
* Los filtros de captura se configuraron para centrarse en las IPs:
* 10.150.45.201
* 10.150.45.202.
* Se creo y analizo los puertos y protocolos nombrados a continuación para identificar servicios activos y potenciales vulnerabilidades.

1. Ping (ICMP)

La comunicación ICMP se ha realizado con éxito entre la dirección IP 10.145.21.133 y los servidores 10.150.45.201 y 10.150.45.202. Este se realizó con el fin de Asegurar que existe una conexión a las IPs.

Posible Problema de Seguridad: Aunque el ICMP es útil para la administración de red, puede ser explotado en ataques de tipo "Ping Flood".

10.150.45.201

Captura de pantalla de computadora

Descripción generada automáticamente

10.150.45.202

Captura de pantalla de computadora

Descripción generada automáticamente

1. Telnet

Se creo tráfico Telnet en los servidores 10.150.45.201 y 10.150.45.202.

Posible Problema de Seguridad: Telnet transmite datos, incluidas las credenciales, en texto plano, lo que es un riesgo significativo de seguridad.

10.150.45.201

Captura de pantalla de computadora

Descripción generada automáticamente

10.150.45.202

Imagen que contiene Tabla

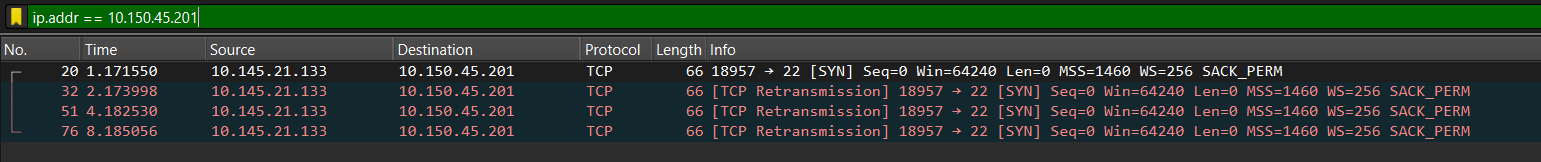
Descripción generada automáticamente

1. SSH

Se creado tráfico SSH en ambos servidores.

Posible Problema de Seguridad: El uso de SSH es una buena práctica. Asegurarse de que solo se permitan conexiones SSH desde direcciones IP de confianza y que se utilicen autenticaciones basadas en claves en lugar de contraseñas.

10.150.45.201



10.150.45.202

Texto

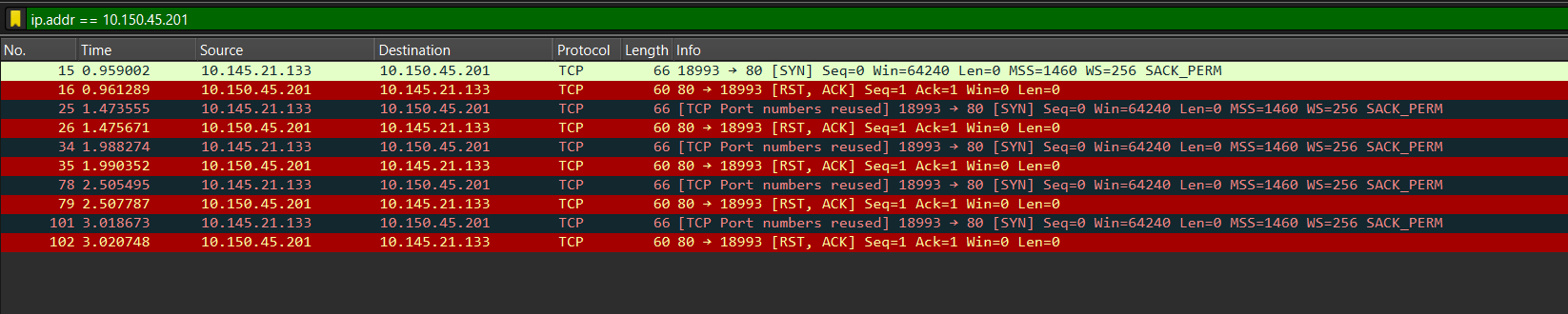
Descripción generada automáticamente

1. Curl (HTTP)

Se creado tráfico HTTP desde y hacia los servidores.

Posible Problema de Seguridad: HTTP no cifra los datos en tránsito, lo que puede exponer información sensible.

10.150.45.201



10.150.45.202

Pantalla de computadora

Descripción generada automáticamente

1. nmap-sV

Existen registros de que se han realizado escaneos de puertos con `nmap`.

Posible Problema de Seguridad: Si estos escaneos no fueron autorizados, podrían ser indicativos de un intento de reconocimiento por parte de un atacante.

10.150.45.201

Una captura de pantalla de una computadora

Descripción generada automáticamente

10.150.45.202

Captura de pantalla de computadora

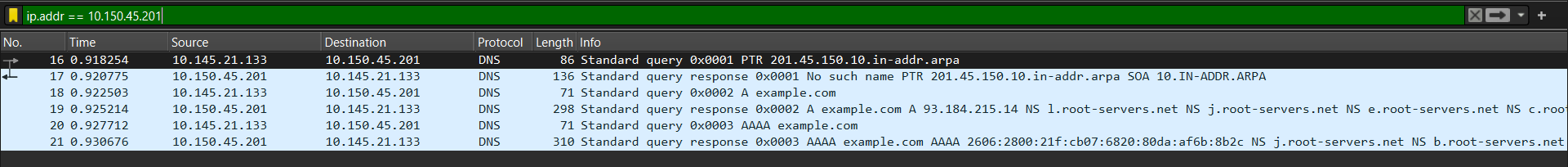
Descripción generada automáticamente

1. nslookup (DNS)

Se ha realizado una consulta DNS.

Posible Problema de Seguridad: Las consultas DNS en sí no son problemáticas, pero asegúrate de que el servidor DNS no esté configurado para permitir consultas recursivas desde cualquier IP externa, lo cual puede ser explotado en ataques de amplificación DNS.

10.150.45.201



10.150.45.202

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

**Problemas de Seguridad Encontrados**

1. Ping (ICMP): Posible explotación en ataques de tipo "Ping Flood".
2. Telnet: Transmisión de datos en texto plano, riesgo significativo de seguridad.
3. SSH: Uso de SSH es adecuado, pero asegurar configuraciones.
4. HTTP: Transmisión de datos en texto plano, riesgo de exposición de información sensible.
5. nmap-sV: Indicios de escaneos de puertos no autorizados.
6. DNS: Asegurar configuración para prevenir consultas recursivas no autorizadas.

**Recomendaciones**

1. Limitar Tráfico ICMP: Implementa reglas en el firewall para limitar el tráfico ICMP a solo lo necesario para la administración de red.
2. Deshabilitar Telnet: Telnet debe ser deshabilitado y reemplazado por SSH en todos los servidores.
3. Fortalecer Configuración de SSH: Asegúrate de que SSH esté configurado para aceptar solo autenticaciones basadas en claves y que las conexiones solo se permitan desde IPs de confianza.
4. Migrar HTTP a HTTPS: Actualiza todos los servicios HTTP a HTTPS para proteger los datos en tránsito.
5. Monitoreo y Alertas: Configura sistemas de monitoreo y alertas para detectar y responder rápidamente a actividades sospechosas, como escaneos de puertos no autorizados.
6. Seguridad DNS: Configura el servidor DNS para restringir las consultas recursivas y protegerlo contra ataques de amplificación.

**Anexos**

Dentro del siguiente repositorio se encuentran los archivos [.pcapng] en los cuales se realizaron los análisis de vulnerabilidades con el programa wireshark.

**B. Zarate, K. Diaz, I. Salinas "Seguridad de Sistemas," GitHub repository, 2024. [Online]. Available:** [**https://github.com/ZarateBenjamin/Seguridad-de-Sistemas.git**](https://github.com/ZarateBenjamin/Seguridad-de-Sistemas.git)