Prueba - Análisis de Seguridad en Redes de Datos

En esta prueba validaremos nuestros conocimientos de la aplicación de herramientas y metodologías de análisis de seguridad para la identificación y análisis de tráfico en redes de datos corporativas. Para lograrlo, necesitarás aplicar los requerimientos que serán solicitados utilizando las herramientas Kali Linux y Wireshark.

Lee todo el documento antes de comenzar el desarrollo individual para asegurarte de tener el máximo de puntaje y enfocar bien los esfuerzos.

Tiempo asociado: 3 horas cronológicas.

Descripción

La empresa Desafío Latam ha implementado una red corporativa en donde deberás realizar una serie de análisis de tráfico y pruebas de conectividad que permita evaluar el comportamiento de la red desde el punto de vista de seguridad, así como la identificación de patrones de tráfico y posibles anomalías.

Requerimientos de la Prueba:

1. Análisis de Tráfico con hping3 en Kali Linux

Utilizando Kali Linux, deberás realizar las siguientes actividades con la herramienta hping3:

- **a)** Crear un archivo de texto plano con información personal (nombre, curso, fecha)
- **b)** Utilizar hping3 para enviar diferentes tipos de paquetes a un host objetivo (puede ser google.com o la puerta de enlace local):
    - ICMP ping normal
    - TCP SYN a puerto 80
    - UDP a puerto 53
    - TCP con datos personalizados
- **c)** Documentar los comandos utilizados y explicar las diferencias en las respuestas
- **d)** Capturar el tráfico generado con Wireshark durante las pruebas

2. Captura y Análisis de Tráfico con Wireshark

Realizar una sesión de captura de tráfico de red durante 10-15 minutos mientras navegas por diferentes sitios web:

- **a)** Acceder a al menos 5 sitios web diferentes (incluir HTTP y HTTPS)
- **b)** Realizar una descarga de archivo pequeño
- **c)** Enviar un correo electrónico o usar una aplicación de mensajería
- **d)** Aplicar los siguientes filtros en Wireshark y documentar los resultados:
    - `http` - Tráfico HTTP
    - `dns` - Consultas DNS
    - `tcp.port == 443` - Tráfico HTTPS
    - `icmp` - Tráfico ICMP
    - `ip.addr == [tu_IP]` - Todo el tráfico de tu máquina
- **e)** Identificar y explicar:
    - Protocolos más utilizados
    - Direcciones IP de destino más frecuentes
    - Puertos más utilizados
    - Posibles vulnerabilidades observadas (tráfico no cifrado, etc.)

3. Análisis de Conectividad y Respuesta de Red

Utilizando tanto hping3 como Wireshark:

- **a)** Realizar un análisis de conectividad a diferentes puertos de un servidor remoto:
    - Puerto 22 (SSH)
    - Puerto 80 (HTTP)
    - Puerto 443 (HTTPS)
    - Puerto 21 (FTP)
- **b)** Documentar qué puertos están abiertos, cerrados o filtrados
- **c)** Analizar los tiempos de respuesta y patrones de conectividad

4. Informe Técnico

Realizar un informe profesional que contenga:

- **Portada** con datos del estudiante
- **Introducción** explicando los objetivos del análisis
- **Desarrollo** con cada punto de la evaluación documentado mediante:
    - Capturas de pantalla de comandos ejecutados
    - Capturas de Wireshark con filtros aplicados
    - Análisis de los resultados obtenidos
- **Recomendaciones** para mejorar la seguridad de la red analizada
- **Conclusiones** sobre los hallazgos más relevantes

Criterios de Evaluación

Requerimientos y Puntajes:

1. **Análisis con hping3** (2.5 puntos)
2. **Captura y filtrado en Wireshark** (2.5 puntos)
3. **Análisis de conectividad** (2.0 puntos)
4. **Informe técnico completo** (3.0 puntos)

Total: 10 puntos

Rúbrica de Evaluación

1. Análisis con hping3 (2.5 puntos)

Criterio	Excelente (2.5)	Bueno (2.0)	Suficiente (1.5)	Insuficiente (0-1.0)
Comandos hping3	Ejecuta todos los comandos solicitados correctamente con sintaxis perfecta	Ejecuta la mayoría de comandos con sintaxis correcta	Ejecuta algunos comandos con errores menores	Comandos incorrectos o incompletos
Documentación	Documenta todos los comandos y explica claramente las diferencias	Documenta la mayoría de comandos con explicaciones básicas	Documentación incompleta	Sin documentación adecuada
Capturas	Capturas claras y bien organizadas de todos los procesos	Capturas de la mayoría de procesos	Capturas incompletas pero legibles	Sin capturas o ilegibles

2. Análisis con Wireshark (2.5 puntos)

Criterio	Excelente (2.5)	Bueno (2.0)	Suficiente (1.5)	Insuficiente (0-1.0)
Filtros aplicados	Aplica todos los filtros solicitados correctamente	Aplica la mayoría de filtros correctamente	Aplica algunos filtros con errores menores	Filtros incorrectos o incompletos
Análisis de tráfico	Identifica y explica correctamente todos los elementos solicitados	Identifica la mayoría de elementos con explicaciones básicas	Identificación parcial de elementos	Análisis incorrecto o ausente
Interpretación	Interpreta correctamente los protocolos, IPs y puertos observados	Interpretación mayormente correcta	Interpretación básica pero funcional	Sin interpretación o incorrecta

3. Análisis de Conectividad (2.0 puntos)

Criterio	Excelente (2.0)	Bueno (1.5)	Suficiente (1.0)	Insuficiente (0-0.5)
Análisis de puertos	Analiza todos los puertos solicitados con interpretación correcta	Analiza la mayoría de puertos correctamente	Análisis básico pero funcional	Análisis incorrecto o incompleto
Identificación de seguridad	Identifica claramente medidas de seguridad y su funcionamiento	Identifica algunas medidas de seguridad	Identificación básica	Sin identificación de medidas

4. Informe Técnico (3.0 puntos)

Criterio	Excelente (1.0)	Bueno (0.8)	Suficiente (0.6)	Insuficiente (0-0.4)
Estructura y formato	Informe profesional, bien estructurado con todos los elementos solicitados	Estructura correcta con elementos completos	Estructura básica, algunos elementos faltantes	Estructura deficiente o incompleta
Capturas y evidencias	Todas las capturas son claras, relevantes y están bien explicadas	Mayoría de capturas claras y explicadas	Capturas presentes pero con explicaciones básicas	Capturas ausentes, poco claras o sin explicar
Recomendaciones	Recomendaciones técnicas específicas, viables y bien fundamentadas	Recomendaciones correctas pero genéricas	Recomendaciones básicas	Sin recomendaciones o irrelevantes

---

¡Mucho éxito en tu evaluación!