Desafío - Análisis de Tráfico en la Red

En este desafío validaremos nuestros conocimientos en utilizar herramientas de análisis de tráfico en la red para identificar y documentar patrones anómalos y amenazas de seguridad.

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: 1 hora cronológica.

Descripción

La empresa DesafioLatam se encuentra en un proceso de análisis del tráfico de red que ingresa y sale dentro de la red de su organización. Por lo cual su labor es la captura del tráfico y realizar el análisis necesario para esto.

Actividades a Realizar:

1. **Realizar un escaneo de puerto** a scanme.nmap.org utilizando diferentes técnicas, proporcionando la mayor cantidad de información posible.

2. **Capture tráfico por 3 minutos** usando Wireshark en su interfaz de red y responda las siguientes preguntas específicas:

Requerimientos

1. Escaneo de Puertos con Nmap (3 Puntos)

Ejecuta este comando y documenta los resultados:

```shell
nmap -sV scanme.nmap.org
```

Responde:

- Lista 3 puertos abiertos y sus servicios: _____
- ¿Qué servidor web detectaste? _____

2. Análisis de Tráfico ARP (2 Puntos)

Comando para generar tráfico ARP:

```shell
ping -c 3 [IP_de_tu_gateway]
```

Filtro de Wireshark:

```
arp
```

Responde:

- Selecciona un ARP Request y completa:
  - MAC origen: _____
  - IP que busca: _____
- ¿Qué indica cuando ves muchos ARP Request para la misma IP? _____

3. Análisis de Tráfico DHCP (3 Puntos)

Comando:

```shell
# Windows: ipconfig /release && ipconfig /renew

# Linux: sudo dhclient -r eth0 && sudo dhclient eth0
```

Filtro de Wireshark:

```
dhcp
```

Responde:

- ¿Qué 4 tipos de mensajes DHCP observaste? _____
- ¿Qué IP te asignó el servidor DHCP? _____

4. Análisis de Tráfico HTTPS (2 Puntos)

Comando:

```shell
curl -v https://github.com
```

Filtro de Wireshark:

```none
tcp.port == 443
```

Responde:

- ¿Qué versión de TLS se negoció? _____
- ¿Cuántos paquetes se intercambiaron en el handshake? _____

Entregables

1. **Documento con las respuestas** completadas
2. **Una captura de pantalla** de Wireshark mostrando el filtro aplicado para cada protocolo

Puntuación

- **Escaneo de puertos:** 3 puntos
- **Análisis ARP:** 2 puntos
- **Análisis DHCP:** 3 puntos
- **Análisis HTTPS:** 2 puntos
- **Total:** 10 puntos

¡Mucho éxito!