Informe de Seguridad de la Red: Evaluación y Mitigación de Amenazas

Elaborado por: Daniel Dávila
Curso: Seguridad en redes de datos G3
Fecha 28-08-2025

1. Introducción.

Este informe se presenta en respuesta a la solicitud de la empresa TechSecure para evaluar la seguridad de su infraestructura de red, con un enfoque particular en un servidor Linux clave. El objetivo es documentar la vulnerabilidad de la red a ataques de tipo Man-in-the-Middle (MitM) mediante ARP Spoofing y proponer contramedidas para mitigar dicho riesgo, cumpliendo con los requerimientos específicos de control de acceso al servidor.

2. Procedimiento del Ataque

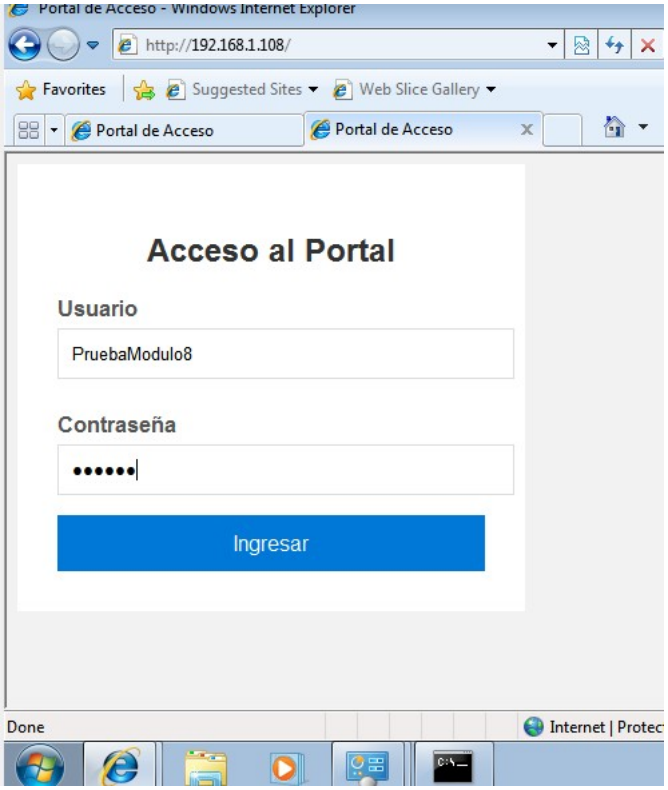
El ataque se llevó a cabo utilizando la herramienta Ettercap en la máquina Kali Linux. Los pasos seguidos fueron:

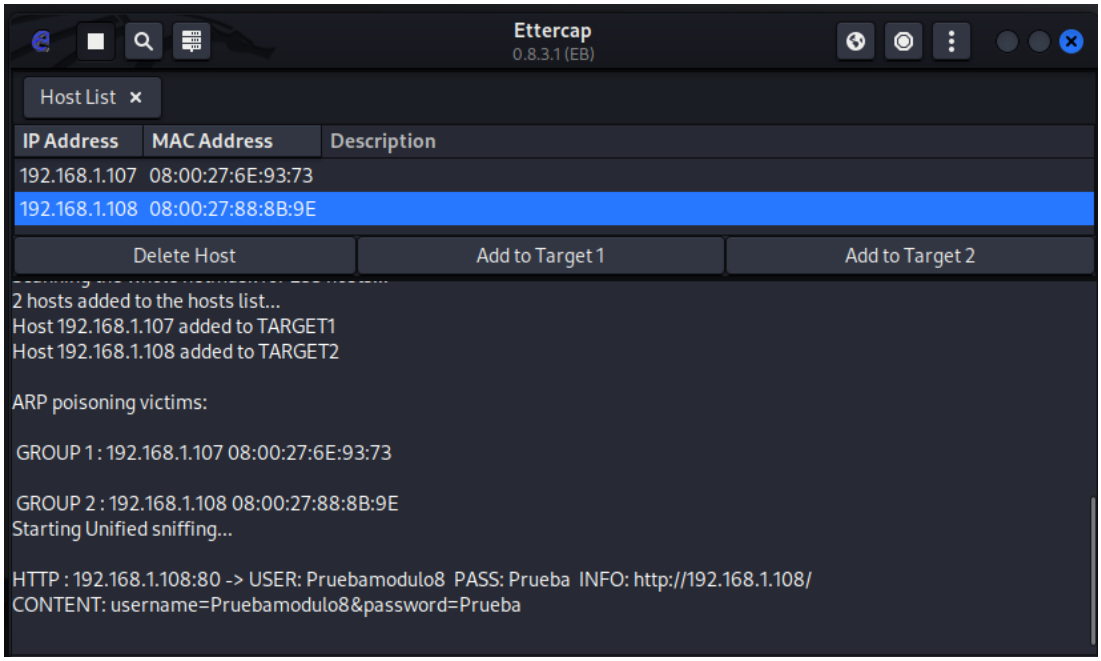
Activación del reenvío de paquetes (IP Forwarding): Antes de iniciar el ataque, se habilitó el reenvío de IP en la máquina Kali para que pudiera reenviar el tráfico interceptado entre la víctima y el servidor, evitando una interrupción completa de la comunicación.

Escaneo de la red: Se usó Ettercap para escanear la red interna (labnet) y detectar las máquinas activas.

Selección de objetivos: Se configuró Ettercap para que la máquina atacante (Kali) se posicionara entre el cliente Windows (192.168.1.107) y el servidor Ubuntu (192.168.1.108).

Ejecución del ARP Spoofing: Se inició el ataque de ARP Spoofing, lo que provocó que el cliente Windows y el servidor Ubuntu asociaran la dirección IP del otro con la dirección MAC de la máquina Kali pudiendo obtener la información del formulario alojado en el servidor y utilizado por la pc de Windows

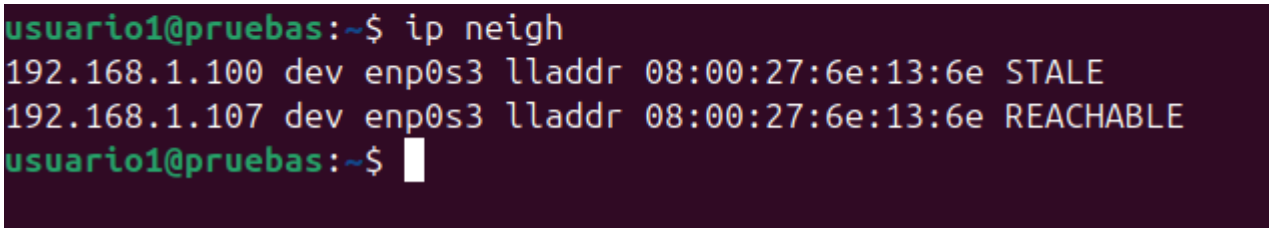




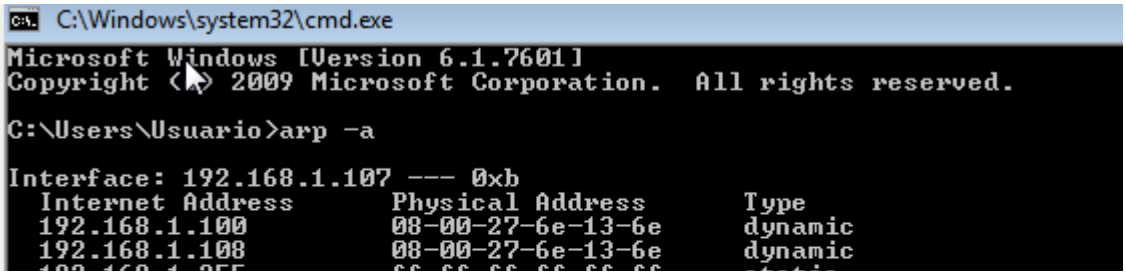
3. Pruebas y Evidencias

Ademas de las imágenes anteriores tenemos:

Evidencia en el servidor Ubuntu: La imagen muestra la tabla ARP del servidor Ubuntu (ip neigh). Se puede observar que la dirección MAC para la IP del cliente Windows (192.168.1.107) ahora corresponde a la dirección MAC del atacante Kali, y no a la MAC original de Windows.



Evidencia en el cliente Windows: La imagen muestra la salida del comando arp -a en el cliente Windows. Aquí, la dirección MAC para la IP del servidor Ubuntu (192.168.1.108) ha sido suplantada por la dirección MAC del atacante Kali. (192.168.1.100)



Estas capturas de pantalla son la prueba de que el atacante (Kali) se ha posicionado exitosamente en medio de la comunicación, permitiendo la intercepción de todo el tráfico entre la víctima y el servidor.

4. Contramedidas sugeridas:

El ataque de ARP Spoofing es efectivo en redes no seguras. Para mitigar o prevenir este tipo de ataques, se pueden implementar las siguientes contramedidas:

- Configuración de Firewall: Se recomienda configurar un firewall (como ufw o iptables) en el servidor para permitir solo el tráfico deseado.
- ARP estático: Configurar manualmente entradas ARP estáticas en los dispositivos. Esto impide que los dispositivos actualicen su caché ARP con respuestas falsificadas. Por ejemplo, en el cliente Windows, se podría añadir la entrada arp -s 192.168.1.108 <MAC_REAL_DEL_SERVIDOR>.
- Seguridad de puertos en el switch (Port Security): En un entorno de red gestionada, los switches pueden configurarse para asociar una dirección MAC específica a un puerto. Si otra dirección MAC intenta comunicarse a través de ese puerto, el switch puede apagarlo o enviarlo a un estado de alerta.
- Uso de HTTPS/SSL/TLS: Aunque el ARP Spoofing aún permite la intercepción del tráfico, el cifrado de extremo a extremo que ofrecen protocolos como HTTPS hace que los datos capturados (como las credenciales de login) sean ilegibles para el atacante, protegiendo la información sensible.

5. Conclusiones

El laboratorio demostró de manera concluyente que la red de TechSecure es vulnerable a ataques de ARP Spoofing. El éxito del ataque subraya la importancia de no depender únicamente de la seguridad perimetral, sino también de la seguridad a nivel de host.

Las medidas propuestas, incluyendo la **configuración restrictiva del firewall, el uso de ARP estático y la implementación de cifrado de tráfico**, son fundamentales para proteger el servidor Linux y cumplir con los requerimientos de la empresa. Al aplicar estos controles, el servidor estará protegido contra una amplia gama de amenazas, asegurando que el acceso sea controlado y que los datos en tránsito permanezcan confidenciales.