NOMBRE: Jonas Basora

MATRICULA: 2024-1360

DOCENTE: Jonathan Estaban Rondon

MATERIA: Seguridad De Redes

TEMA: Practica #4

Link GITHUB: https://github.com/Jonasz0/Seguridad-De-Redes-ATAQUES-VTP-DTP-Y-DNS

Link Video YOUTUBE: https://youtu.be/pBB49m4BDhQ

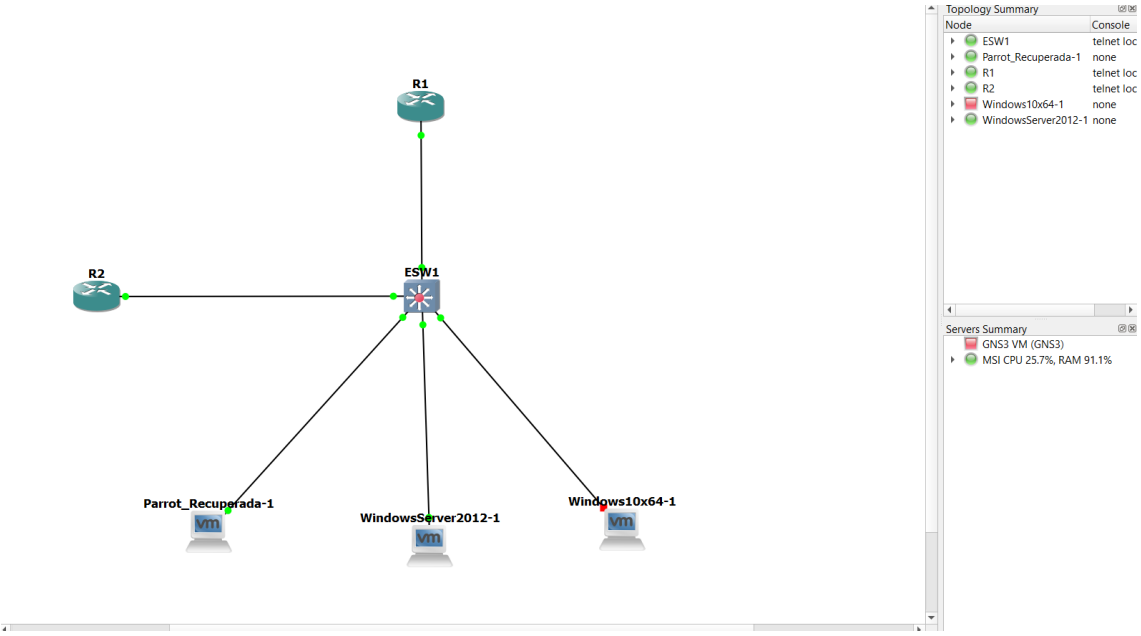
Informe Técnico de Seguridad en Redes: Implementación y Pruebas de Vulnerabilidad

Entorno de Laboratorio: GNS3, Windows Server 2012 (RADIUS/NPS), Parrot OS, Cisco IOS.

Topología y Configuración de Red

La red se diseñó bajo un esquema de seguridad perimetral y centralización de credenciales.

- **Gateway (R1): IP 192.168.1.1. Actúa como Cliente RADIUS (NAS).**
- **Servidor AAA (Windows Server 2012): IP 192.168.1.10. Servicio NPS activo.**
- **Estación de Auditoría (Parrot OS): IP 192.168.1.50.**
- **Segmentación: VLAN 1 (Administración).**
- **Interfaces: FastEthernet 0/0 conectada al core de la red.**



Implementación de Seguridad AAA (RADIUS)

Se logró la centralización de la administración del router mediante el protocolo RADIUS.

Objetivo: Evitar el uso de bases de datos locales y permitir la trazabilidad de usuarios.

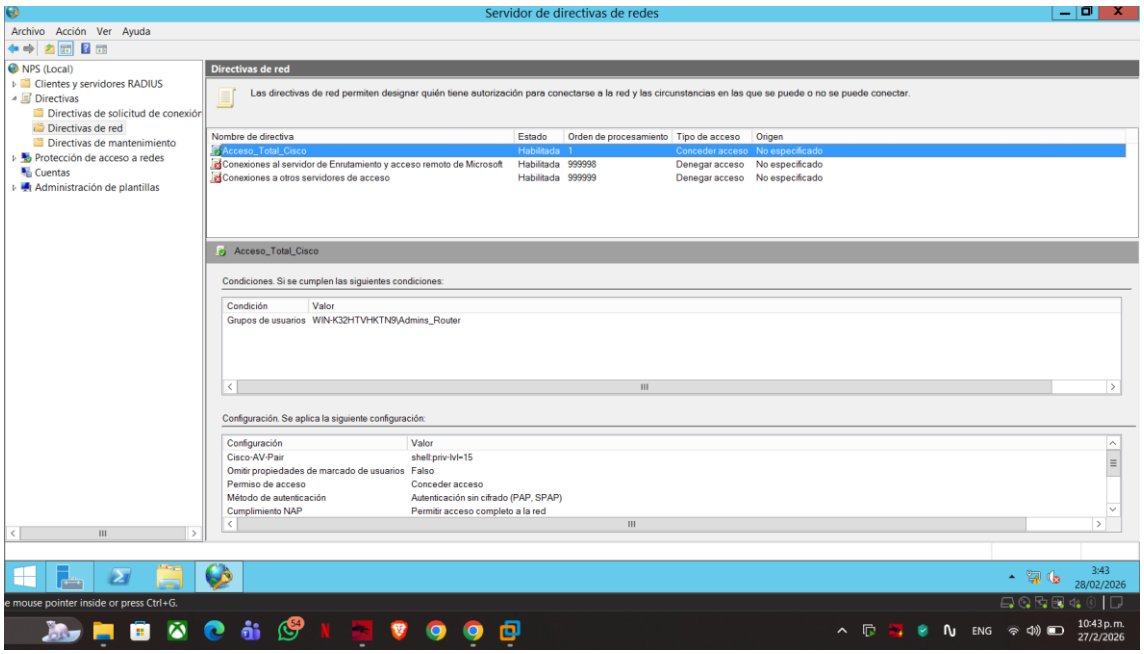
Configuración en R1: Se habilitó aaa new-model, vinculando la autenticación de login al grupo RADIUS con respaldo local.

Parámetros usados: * Puerto: UDP 1812 (Autenticación) y 1813 (Accounting).

Shared Secret: cisco123.

Método de autenticación: PAP (configurado en las directivas de red del NPS).

Resultado: Exitoso. Se validó mediante el comando test aaa group radius jonas [password] legacy.



Análisis de Ataques a Protocolos de Capa 2

En el desarrollo de la práctica, se auditaron los protocolos de infraestructura, encontrando las siguientes limitaciones técnicas:

Ataque VTP (VLAN Trunking Protocol)

Estado: No realizado.

Justificación técnica: Se intentó realizar la inyección de paquetes para modificar la base de datos de VLANs (VLAN Database) utilizando la librería Scapy en Python. Sin embargo, la complejidad del protocolo VTP y las limitaciones de la librería para manipular campos específicos de revisión de configuración en tiempo real impidieron la ejecución efectiva del ataque.

Ataque DTP (Dynamic Trunking Protocol)

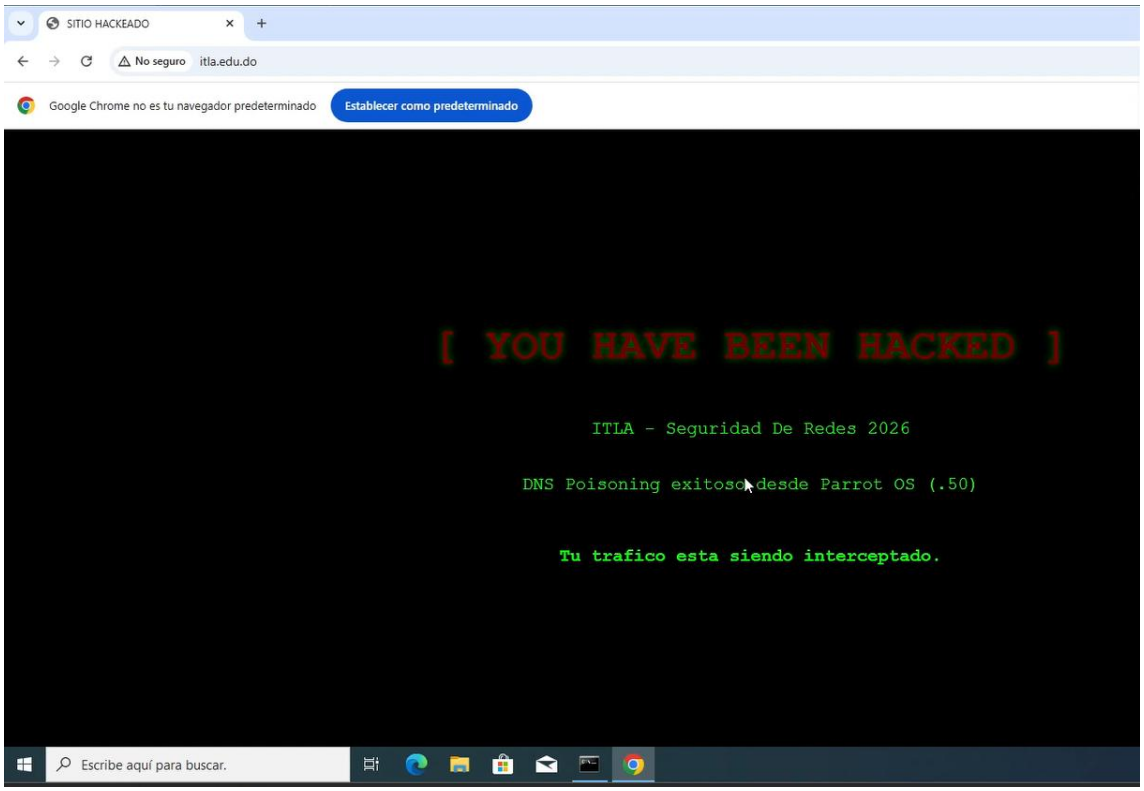
Estado: No realizado.

Justificación técnica: Este ataque requiere el uso de imágenes de Switches multicapa (como las de IOU/IOL) que soporten negociación de enlaces troncales. Debido a restricciones de hardware en la máquina anfitriona, no fue posible habilitar la virtualización anidada necesaria para ejecutar la GNS3 VM. Esto limitó el laboratorio a imágenes de routers y switches básicos que no soportan la funcionalidad completa de DTP necesaria para el salto de VLAN (VLAN Hopping).

Ataque Exitoso: DNS Spoofing (Envenenamiento de DNS)

Este ataque se realizó satisfactoriamente desde la estación Parrot OS.

- **Objetivo: Interceptar las consultas DNS de una víctima y redirigirla a una IP controlada por el atacante.**
- **Herramientas: Bettercap / Ettercap y Scapy.**
- **Procedimiento:**
    1. **Se realizó un envenenamiento ARP (ARP Spoofing) para posicionar al atacante entre el Router y la Víctima (MITM).**
    2. **Se activó el módulo de DNS Spoofing, configurando un archivo de "hosts" falso donde el dominio solicitado (ej: www.banco.com) apuntaba a la IP de Parrot OS.**
    3. **Cuando la víctima intentó navegar, el atacante respondió con la IP falsa antes que el servidor DNS real.**
- **Resultado: Exitoso. La víctima fue redirigida a una página clonada de forma transparente.**



Medidas de Mitigación Recomendadas

Para proteger la topología contra los ataques intentados y realizados, se proponen las siguientes medidas:

VTP: Configurar los switches en modo VTP Transparent y establecer contraseñas de dominio.

DTP: Deshabilitar la negociación automática en todos los puertos con switchport nonegotiate.

DNS: Implementar DNSSEC para validar las respuestas y usar herramientas de inspección de ARP (DAI) para evitar el MITM previo.

AAA: Cambiar el transporte de Telnet a SSH y utilizar protocolos de autenticación cifrados como MS-CHAPv2 o EAP.

Requisitos del Sistema

Cisco IOS Imagen v15.x.

Windows Server con rol de NPS instalado.

Librería Scapy y suite Bettercap en Linux.