Objetivo de los Scripts

El desarrollo de los scripts en este laboratorio tuvo como propósito fundamental la realización de una **prueba de penetración (Penetration Testing)** de caja blanca sobre la infraestructura de red. Los objetivos específicos se dividen en dos categorías:

A. Objetivo de los Scripts de Ataque (Scapy/Python)

- **Validación de Vulnerabilidades en Capa 2:** Evaluar la resistencia de los protocolos de gestión industrial (VTP, DTP) ante la inyección de tramas maliciosas.
- **Demostración de Concepto (PoC):** Evidenciar cómo la falta de autenticación en protocolos heredados permite a un atacante segmentar la red de forma arbitraria o realizar un salto de VLAN para interceptar tráfico sensible.
- **Simulación de Amenazas Internas:** Replicar el comportamiento de un "Insider Threat" que intenta escalar privilegios o comprometer la integridad de la base de datos de servicios (DNS).

B. Objetivo de la Configuración de Seguridad (AAA/RADIUS)

- **Centralización del Control de Acceso:** Sustituir la gestión de identidades dispersa en múltiples dispositivos por una base de datos centralizada en Windows Server 2012.
- **Garantizar el No Repudio:** Asegurar que cada acceso administrativo al Router 1 esté vinculado a una identidad única (**jonas**), permitiendo auditorías posteriores.
- **Robustecimiento de la Gestión Remota:** Establecer una política de "Acceso Denegado por Defecto", donde solo los usuarios validados por el servidor NPS puedan ejecutar comandos de configuración.

¿Qué poner en la sección de "Parámetros Usados"?

Para que tu Readme.md sea impecable, añade estos parámetros que usamos:

- **Interface:** eth0 (Parrot) / FastEthernet 0/0 (Router).
- **Target IP:** 192.168.1.1 (Router) / 192.168.1.10 (DNS/RADIUS).
- **Dictionary/Payload:** Listas de usuarios para fuerza bruta o registros DNS falsos para el Spoofing.
- **Protocolos:** UDP (1812, 1813, 53), TCP (23, 80).