Tema: VLAN's
Nombres: Cristhian Wiki Sánchez Sauñe

Del artículo descargado, responda las siguientes preguntas.
1. Implementación de la red en GNS3

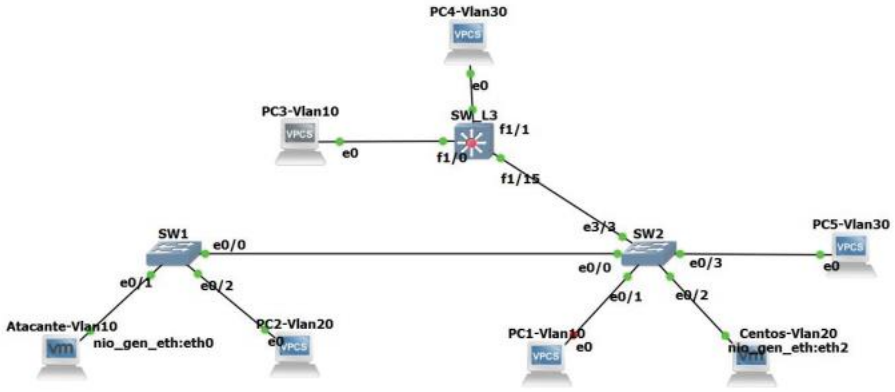
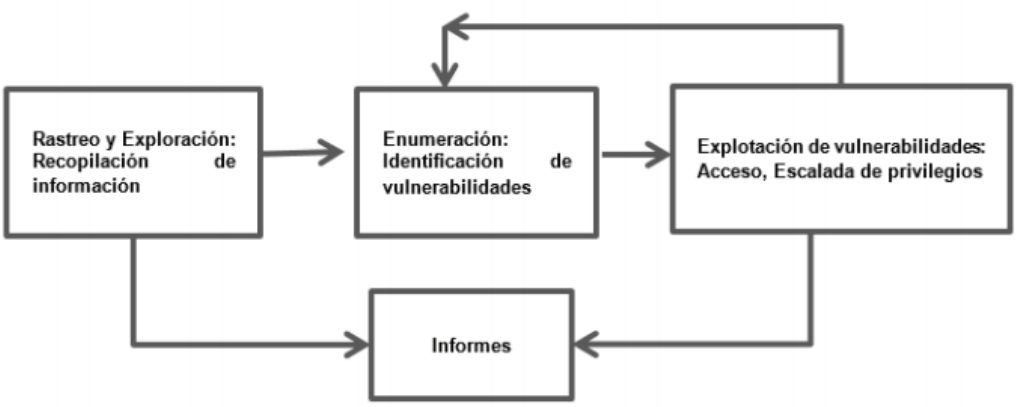


FIGURA 2: Escenario de caso de estudio.

2. Describa las fases de metodología Pentesting descritas en el artículo



i. Fase de Rastreo y Exploración

Se realizaron encuestas a los administradores de red de 30 organizaciones públicas y privadas de la ciudad Riobamba-Ecuador, pues poseen una infraestructura de red con VLANs

ii. Fase de Enumeración

En esta fase se buscó determinar las vulnerabilidades de seguridad que un atacante como usuario con privilegios y permisos puede aprovechar para tener acceso no autorizado a la red.

iii. **Fase de Explotación de Vulnerabilidades**

Se atacó directamente con Switch Spoofing y Double Tagging. Se realizaron 10 veces los mismos ataques para descartar fallas en las herramientas utilizadas o fallas humanas.

iv. Fase de Informes

En esta fase se detallaron las pruebas realizadas, se incluyó el listado de fallas y vulnerabilidades descubiertas, y se propusieron las políticas de seguridad.

3. ¿Cuáles son los dos métodos de ataque VLAN hopping? Describirlas

i. **Switch Spoofing**

(Suplantación de Switch), donde un atacante configura un equipo para simular que es un switch emulando 802.1Q y señalización DTP

ii. **Double Tagging**

Donde se intenta enviar datos de un switch a otro enviando paquetes con dos encabezados 802.1Q, uno para el switch de la víctima y el otro para el switch de ataque.

4. ¿Qué debo observar en el switch para que haya un ataque de doble etiquetado?

Los puertos de acceso estan en modo **trunk** (viene por defecto), y normalmente son puertos que no se suelen usar y no estan bien configurados. Deben configurarse todos los puertos de acceso en modo **acces** para prevenir este ataque.

5. De la siguiente topología ¿Es posible realizar un ping entre A y B? ¿Es posible realizar un ping entre A y C?

No, porque A y B pertenecen a diferentes VLAN.
No, porque A y C siguen estando en diferentes VLAN. El router C puede conectar con B porque pertenecen a la misma VLAN. A no puede conectar con ningún host.