17/07/2019

Seguridad en redes

Scanning networks

Br. Erwin Antonio Sandoval

Escaneando una red objetivo

Introducción

Scanning trata de establecer procedimientos para identificar hosts, puertos y servicios de una red. Es uno de los componentes básicos a tratar para reunir información y crear un perfil del objetivo

Se trata de obtener:

- Direcciones IP
- Puertos activos de hosts vivos
- Sistemas Operativos y arquitectura
- Servicios que están corriendo en los hosts

Objetivos:

El objetivo de este modulo es ayudar a los estudiantes a realizar escaneados de red, escaneo de puertos, análisis de vulnerabilidades de la red, etc.

- Compruebe sistemas en vivo y puertos abiertos
- Realizar la captura de banners y huellas digitales del sistema operativo
- Identificar las vulnerabilidades de la red.
- Dibujar diagramas de red de hosts vulnerables

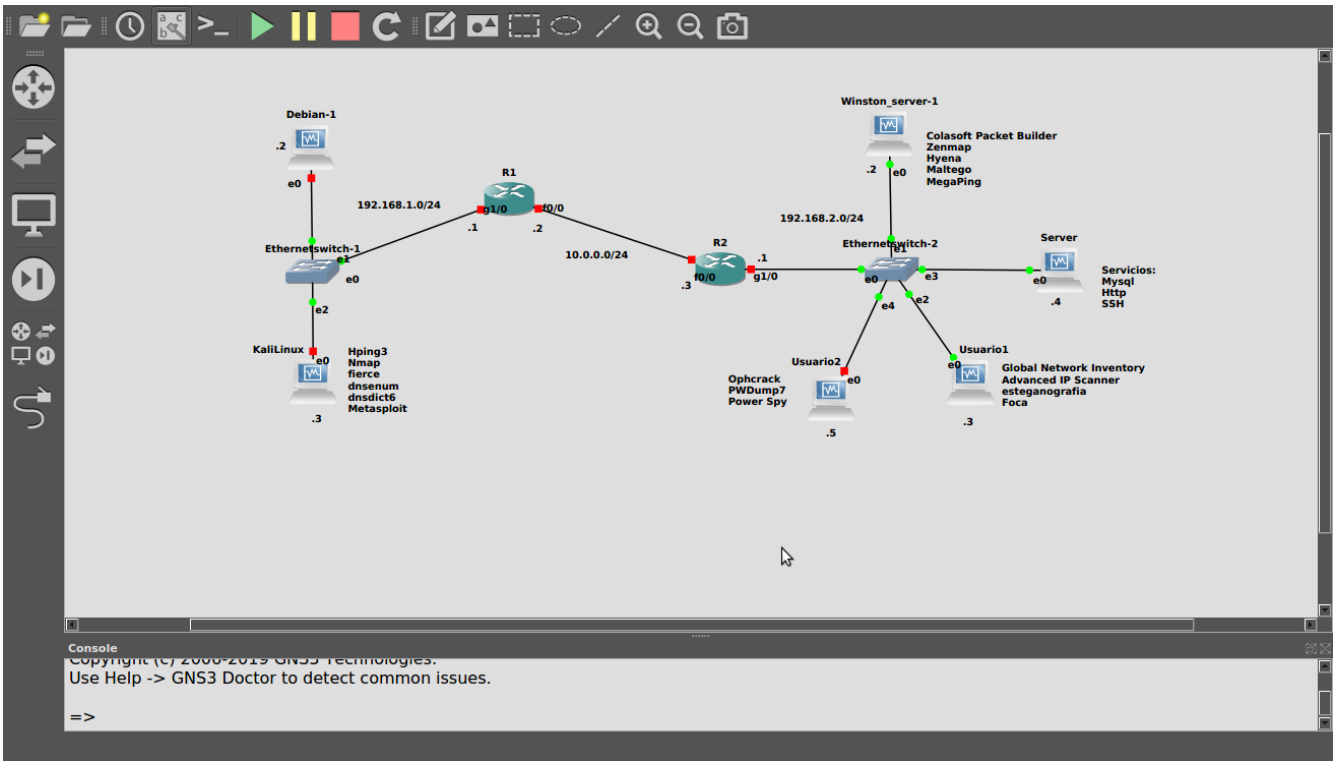
Laboratorios del modulo

Laboratorios recomendados para asistirlo en el escaneo de redes:

- Técnicas de creación de paquetes UDP y TCP utilizando **HPING3**
- Escaneando la red usando el **Colasoft Packet Builder**
- Solución de problemas básicos de red utilizando el **MegaPing**
- Entendiendo el escaneo en red usando **Nmap**
- Análisis de vulnerabilidad utilizando el **Nessus**

Escenario

En la siguiente imagen se observa la topología de la red a montar.



En la siguiente tabla se especifican las diferentes direcciones de cada uno de los interfaces de cada router y PC’s conectados a la red propuesta.

Dispositivo	Interfaz	Direccion IP	Mascarad de red	Gateway
R1	G1/0	192.168.1.1	255.255.255.0	--
	f0/0	10.0.0.2	255.255.255.0	--
R2	G1/0	192.168.2.1	255.255.255.0	--
	f0/0	10.0.0.3	255.255.255.0	--
Windows_server	e0	192.168.2.2	255.255.255.0	192.168.2.1
Usuario1	e0	192.168.2.3	255.255.255.0	192.168.2.1
Usuario2	e0	192.168.2.5	255.255.255.0	192.168.2.1
Server	e0	192.168.2.4	255.255.255.0	192.168.2.1
Kali linux	e0	192.168.1.3	255.255.255.0	192.168.1.1
Debian-1	e0	192.168.1.2	255.255.255.0	192.168.1.1