

17/07/2019

Seguridad en redes

Enumeration



Br. Erwin Antonio Sandoval

Enumeración

Introducción

Es una actividad de la informática en la cual se consigue información de usuarios , grupos o dispositivos y demás servicios relacionados de una red de computadoras. No debe ser confundido con mapeo de red, el cual sólo recupera la información sobre qué servidores están conectados a una red concreta y qué sistemas operativos corren en ellos.

Esta práctica consiste en el descubrimiento de anfitriones o dispositivos en una red de computadoras. Esta actividad tiende a utilizar protocolos de descubrimiento como ICMP y SNMP para recopilar información. También puede escanear varios puertos en anfitriones remotos para buscar servicios conocidos en un intento de identificar la función de un anfitrión remoto. La siguiente etapa de la enumeración es hacer fingerprinting al sistema operativo del anfitrión remoto.

Objetivos:

El objetivo de este módulo es proporcionar conocimiento experto sobre la enumeración de redes y otras responsabilidades que incluyen:

- Nombre de usuario y grupos de usuarios
- Listas de computadoras, sus sistemas operativos y puertos.
- Nombres de máquinas, recursos de red y servicios
- Listas de recursos compartidos en hosts individuales en la red
- Políticas y contraseñas

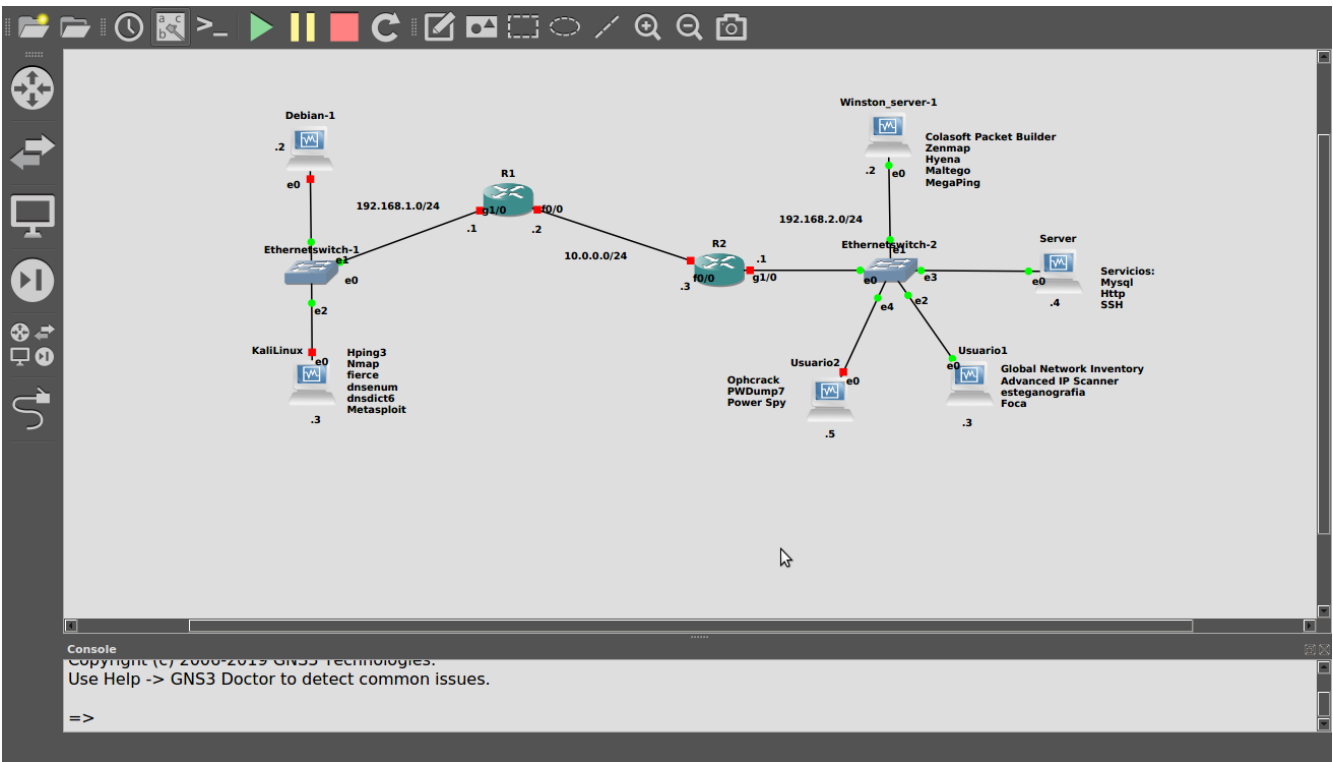
Laboratorios del modulo

Los laboratorios recomendados para asistirlo en su enumeración son:

- Enumeración de NetBIOS usando el **Inventario Global de Red**
- Enumerar los recursos de red utilizando el **escáner IP avanzado**
- Enumerar recursos en una máquina local usando **Hyena**
- Enumeración de **servicios en una máquina de destino**
- Realización de la enumeración de la red utilizando **varias herramientas de interrogación de DNS**

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