Práctico 6: Análisis de tráfico TCP y UDP en GNU/Linux

Presentación de consignas.

Ejercicio 1: Análisis de tráfico UDP sobre servidor DNS

Recomendaciones

- Lea con cuidado las consignas
- Tenga certeza de los comandos que ejecuta
- Tenga en cuenta sobre qué interfaz ejecuta el análisis de tráfico

Esquema

- El servicio será instalado y configurado en el Server.
- La lectura de tráfico será realizada desde el Cliente

Diagrama

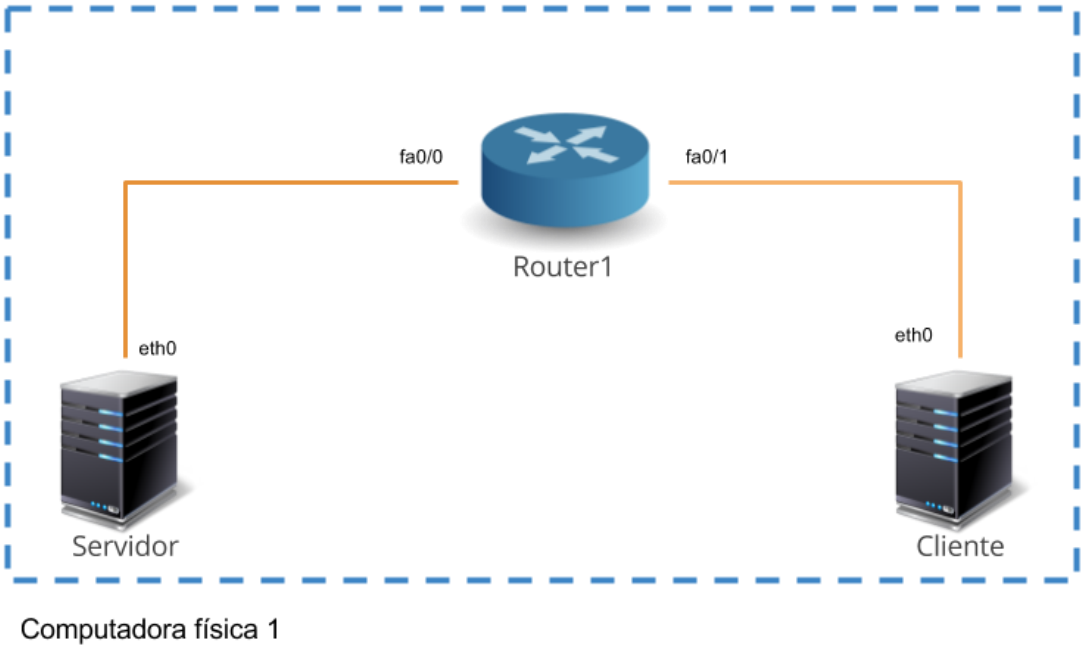

Tabla de asignación de direcciones IPv6

Computadora Interfaz de red Dirección IP

Cliente	eth0	IPv6:
Servidor	eth0	IPv6:
Router1	fa0/0	IPv6:
	fa0/1	IPv6:

Links de ayuda

Instalación y configuración de servidor DNS:
https://www.digitalocean.com/community/tutorials/how-to-configure-bind-as-an-authoritative-only-dns-server-on-ubuntu-14-04

Wireshark: https://www.howtogeek.com/104278/how-to-use-wireshark-to-capture-filter-and-inspect-packets/

Consignas

Servidor DNS

1.1.- Instalar y configurar el servicio DNS en Server

1.2.- Configurar como servidor maestro de DNS para el dominio:
grupoX.redes.fcefyn.unc.edu.local

Donde X es el número de grupo.

1.3.- Agregar los registros AAAA para las IPs de servidor y cliente:

- servidor.grupoX.redes.fcefyn.unc.edu.local
- cliente.grupoX.redes.fcefyn.unc.edu.local

Análisis de tráfico

2.1.- Realizar consultas DNS desde una máquina cliente utilizando el comando "dig"

2.2.- Analizar el tráfico DNS con Wireshark. Identificar cada campo de las Capas 2, 3, 4 y 5.

Ejercicio 2: Análisis de tráfico TCP sobre servidor HTTP

Recomendaciones

- Lea con cuidado las consignas
- Tenga certeza de los comandos que ejecuta
- Tenga en cuenta sobre qué interfaz ejecuta el análisis de tráfico

Esquema

- El servicio será instalado y configurado en el Server.
- La lectura de tráfico será realizada desde el Cliente.
- Este ejercicio NO es continuación del Ejercicio 1. Es deseable pero no mandatorio utilizar el servicio de DNS.

Diagrama

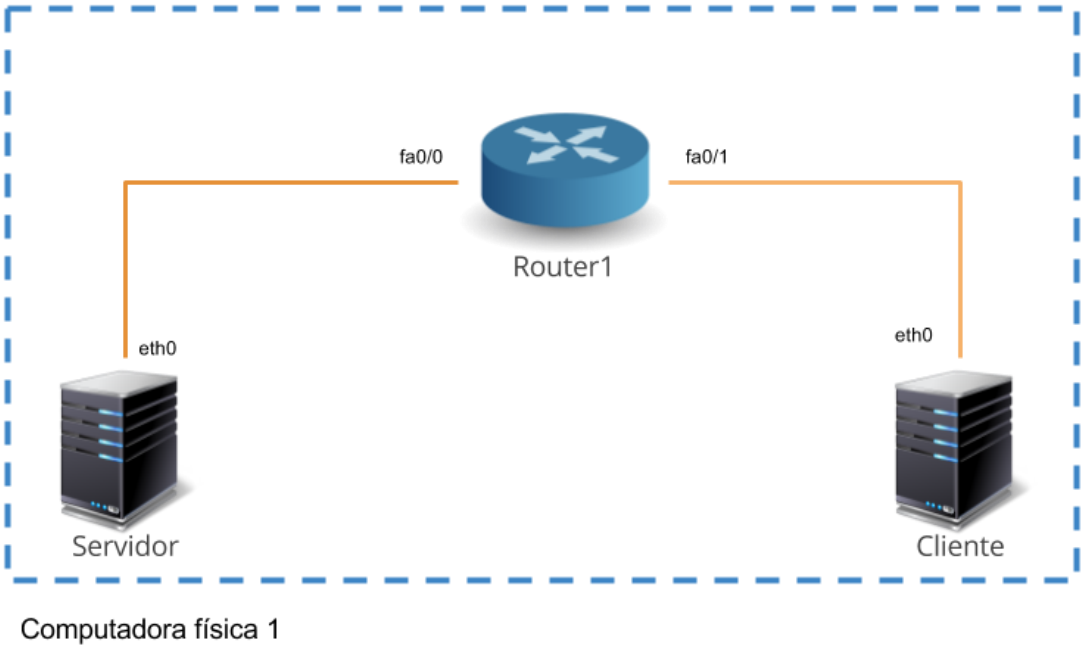

Tabla de asignación de direcciones IPv6

Computadora	Interfaz de red	Dirección IP
Cliente	eth0	IPv6:
Servidor	eth0	IPv6:
Router1	fa0/0	IPv6:
	fa0/1	IPv6:

Links de ayuda

Instalación y configuración de servidor Wordpress en Linux:

https://www.digitalocean.com/community/tutorials/how-to-install-wordpress-with-lamp-on-ubuntu-16-04

Wireshark: https://www.howtogeek.com/104278/how-to-use-wireshark-to-capture-filter-and-inspect-packets/

Consignas

Servidor Wordpress

1.1.- Instalar y configurar el servicio Wordpress en el Server.

1.2.- Utilizar la página web de autenticación para la consigna 2.-

Análisis de tráfico

2.1.- Desde el cliente utilizar el navegador web para poder autenticarse en el portal de Wordpress.

2.2.- Analizar el tráfico HTTP con Wireshark. Identificar el usuario y password. Analizar capas 3, 4 y 5.