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

Presentación de consignas.

Ejercicio 1: 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 servidor contiene un servicio de DNS y es administrable a través de WEBMIN
- El cliente es la PC Host. 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: 2001:a:a:a::1
Servidor	eth0	IPv6: 2001:a:a:a::2

Links de ayuda

Instanciar un container servidor DNS con docker:
http://www.damagehead.com/blog/2015/04/28/deploying-a-dns-server-using-docker/
http://forums.debian.net/viewtopic.php?f=5&t=134792
Wireshark:
https://www.howtogeek.com/104278/how-to-use-wireshark-to-capture-filter-and-inspect-packets/
Finalización de sesión TPC:
https://www.performancevision.com/blog/close-tcp-sessions-diagnose-disconnections/

Consignas

Servidor DNS con administración remota a través de WEBMIN

1.1.- Utilizando docker compose, crear e iniciar un container para ser utilizado como servidor DNS

- Utilizaremos la siguiente imagen para crear el containter. La misma viene con “bind” como servicio DNS y “webmin” para administración remota.
    - image: "sameersbn/bind:latest"
- Se debe setear la variable de entorno “ROOT_PASSWORD=ubuntu” en el container para tener acceso a webmin

1.2.- Configurar WEBMIN para poder ser accedido a través de IPv6

Análisis de tráfico

2.1.- Comenzar a analizar el tráfico HTTPS con Wireshark en la interfaz que nos conecta con el servidor DNS.
2.2.- Desde el cliente utilizar el navegador web para poder autenticarse en el portal de WEBMIN. Ingresar utilizando la IPv6 del servidor. Luego cierre sesion y por último cierre la pestaña del navegador.
2.3- Analizar el tráfico en capa de transporte y responder:

- ¿Como es la secuencia de iniciación de sesión de tcp? Indicar con capturas de pantalla donde se observen los mensajes
- ¿Como es la secuencia de finalización de sesión de tcp? Indicar con capturas de pantalla donde se observen los mensajes.
- ¿Que utilidad tiene el tamaño de ventana en la sesión tcp? ¿Como se calcula? Mostrar un ejemplo mediante captura de pantalla de un segmento tcp
- ¿Que significa que el tamaño de ventana sea cero?
- Como puede observarse en wireshark, durante el tiempo que tuvo abierto WEBMIN en su navegador, se iniciaron y cerraron múltiples sesiones tcp. Filtre alguna de estas sesiones y observe el comportamiento del tamaño de ventana durante la sesión. Ayuda:
    - Para filtrar los paquetes de una sesión en particular, utilizar el filtro “tcp.port”
    - Para observar el comportamiento del tamaño de ventana puede graficar el “window scaling” en wireshark

BONUS

3.1.- Configurar WEBMIN para que trabaje sin ssl
3.2.- Analizar tráfico mientras se ingresa a WEBMIN y se autentica
3.3.- En los paquetes capturados identificar el nombre de usuario y contraseña de WEBMIN

Ejercicio 2: Análisis de tráfico UDP sobre servidor DNS

1.1.- Configurar el contenedor para que almacene los archivos contenidos en /data de manera persistente.

Nota: se debe modificar el archivo de docker-compose para tal fin, luego destruir el entorno de docker-compose e iniciarlo nuevamente.

1.2.- Desde WEBMIN 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 4 y 5. Responder:

- ¿Que campos posee la cabecera UDP? indicar en print de pantalla de wireshark
- Analizar la información transportada en el segmento UDP:
  - ¿A qué capa del stack tcp/ip pertenece dicha información?
  - Indicar en un print de pantalla el nombre de dominio del cual se quiere conocer su IPv6
  - ¿Que es una zona de autoridad?
  - ¿Cual es la zona de autoridad de nuestro servidor dns? indicarlo mediante print de pantalla de wireshark, en el mensaje de respuesta
  - ¿Qué sucede si el paquete nunca llega a destino? ¿el transmisor reenvia dicho paquete?