Redes de Computadoras

Obligatorio 1 - 2023

Facultad de Ingeniería
Instituto de Computación
Departamento de Arquitectura de Sistemas

Nota previa - IMPORTANTE

Se debe cumplir íntegramente el "Reglamento del Instituto de Computación ante Instancias de No Individualidad en los Laboratorios", disponible en el EVA.

En particular está prohibido utilizar documentación de otros estudiantes, de otros años, de cualquier índole, o hacer público código a través de cualquier medio (EVA, correo electrónico, papeles sobre la mesa, etc.).

Introducción

Control Intermedio

El control intermedio se realizará en el monitoreo de la semana del 14/8 y en él se deberá demostrar que domina la herramienta `wireshark` lo suficiente como para realizar el apartado "*Parte A - Captura de tráfico con Wireshark"*. Se le podrá pedir que realice operaciones de captura, filtrado, inspección, y un discernimiento básico de los elementos presentados. Por detalles, consulte con su tutor.

Forma de entrega

Una clara, concisa y descriptiva documentación es clave para comprender el trabajo realizado. La entrega de la tarea consiste en un único archivo `obligatorio1GrupoGG.tar.gz` que deberá contener los siguientes archivos:

- Un documento llamado `Obligatorio1GrupoGG.pdf` donde se documente todo lo solicitado en la tarea. GG es el número del grupo.
- Las capturas solicitadas.
- Un directorio `extras` incluyendo cualquier otro archivo que considere relevante.

La entrega se realizará en el sitio del curso, en la plataforma EVA.

Fecha de entrega

Los trabajos deberán ser entregados **antes del 27/08/2023 a las 23:30 horas**. No se aceptará ningún trabajo pasada la citada fecha y hora. En particular, no se aceptarán trabajos enviados por e-mail a los docentes del curso.

Observaciones

Toda vez que se pida la ejecución de un comando y una respuesta, analice dichos resultados; la ejecución del mismo, incluyendo su invocación deberá ser parte de la respuesta.

Todas las capturas solicitadas hechas con wireshark deberán ser almacenadas y entregadas en el formato `pcap`.

Objetivo del Trabajo

Familiarizarse con conceptos básicos sobre redes e Internet y manejar herramientas para diagnóstico y *debug* de la red. Asimismo, esta tarea intenta que el estudiante se plantee interrogantes e investigue sobre temas que serán abordados durante el curso.

Herramientas

La tarea se puede desarrollar en cualquier entorno de computación donde se puedan ejecutar las siguientes herramientas:

- `ping` [1]
- `wireshark` [2]
- `traceroute` [3] / `tracepath` [4] (equivalente en Windows: `tracert` [5])
- `dig` [6]

Parte A - Captura de tráfico con Wireshark

1. Investigue para qué sirve y cómo se utiliza la herramienta `wireshark`.

2. Utilizaremos `wireshark` para estudiar la transferencia de datos de varias aplicaciones durante una sesión de trabajo típica. Para cada caso realice las siguientes actividades (además de las especificadas en cada una de ellas):
   - Identifique el o los protocolos participantes de cada una de las capas involucradas.
   - ¿Qué nodos participan de la sesión? ¿Qué rol cumplen? Identifique cuáles están en la Red Local, y cuáles están en Internet.
   - ¿Puede acceder a los datos transferidos analizando la captura?

   a) Capture el tráfico generado mientras abre una consola SSH a su usuario en facultad, ejecuta algunos comandos tales como `ls` y `top`, y cierra la sesión. ¿Puede deducir algo de los comandos ejecutados observando la traza capturada?

   b) Capture el tráfico generado por un navegador al descargar las páginas `http://www.columbia.edu/~fdc/sample.html` y `https://www.fing.edu.uy`. Cuando sea posible, responda las siguientes preguntas:
      1. ¿Qué objetos HTTP son transferidos durante la descarga? Identifique el media-type de cada objeto.
      2. ¿Qué versión de HTTP es usada?
      3. ¿Qué user-agent declara su cliente?
      4. ¿Qué *encodings* acepta el cliente, y cuáles usa el servidor?
      5. Identifique el mecanismo usado para marcar la posición del final de un objeto dentro del *stream*.

   c) Para alguna de las partes anteriores, identifique el tráfico DNS asociado.
      1. A partir de la traza, deduzca si la consulta se realiza de forma iterativa o recursiva. Identifique dentro de los mensajes DNS los campos de la flag responsables de este comportamiento, y explíquelos según la RFC correspondiente.

      2. ¿DNS usa algún mecanismo para indicar la longitud de un mensaje de su protocolo? ¿Cómo resuelve este problema?

Parte B - Comando ping

1. Investigue el principio de funcionamiento de la utilidad `ping`. Una respuesta completa incluye el protocolo utilizado, descripción de encabezados, qué mensajes se envían y cuales se reciben. Finalmente en base a lo anterior debería ser capaz de entender como se calculan los resultados que el comando muestra en pantalla.

2. Pruebe los siguientes comandos y analice las salidas. Describa las conclusiones a las que puede arribar con respecto a cada sitio analizado.

```
ping -c 5 www.antel.com.uy
ping -c 5 www.google.com
ping -c 5 registro.br
ping -c 5 zadna.org.za
```

3. Defina 2 criterios diferentes para determinar cual sitio es el mas cercano a usted y discuta qué tan estables en el tiempo son. **La única información disponible es la de la salida del comando**, no puede usar ninguna otra herramienta o servicio como parte de su criterio.

4. Utilizando `wireshark` analice los paquetes intercambiados entre origen y destino al hacer un `ping`. Identifique los protocolos utilizados y relacione con su investigación realizada en el apartado 1.

5. Suponga que desea que su equipo no responda al `ping` realizado desde cualquier otro host de Internet, utilizando la información del apartado anterior, ¿que tipo de tráfico entrante a su equipo es necesario filtrar?. Justifique y explique a partir de la captura de `wireshark`.

Parte C - Comando dig

1. Investigue el principio de funcionamiento del comando `dig`. Una respuesta completa incluye el protocolo utilizado, descripción de encabezados, qué mensajes se envían y cuales se reciben. Finalmente en base a lo anterior debería ser capaz de entender como se calculan los resultados que el comando muestra en pantalla.

2. Realice con `dig` una consulta del registro A del dominio `debian.org`.
   a) Analice la respuesta, explicando detalladamente cada sección de la salida así como las banderas (*flags*) de las respuestas.

   b) Proponga y realice una consulta donde la respuesta para el registro A del dominio `debian.org` sea autoritativa. Justifique.

   c) Justifique similitudes y diferencias de las respuestas obtenidas.

3. Utilice `dig` para identificar los servidores que atienden los dominios `zoom.com` y `www.zoom.com`.

4. Es frecuente ver en algunas películas de acción y espionaje que utilizan las direcciones IP para encontrar ubicaciones geográficas específicas. ¿Podría usted localizar las IPs del punto 3? .

5. ¿Quién registró el nombre de dominio `zoom.com`? (estudie como averiguarlo, no es con `dig`)

Parte D - Comando traceroute

1. Investigue el principio de funcionamiento del comando `traceroute` o `tracepath`. Una respuesta completa incluye el protocolo utilizado, descripción de encabezados, qué mensajes se envían y cuales se reciben. Finalmente en base a lo anterior debería ser capaz de entender como se calculan los resultados que el comando muestra en pantalla.

2. Utilice `wireshark` para validar el análisis anterior.

3. ¿Cómo podría replicar la funcionalidad de `traceroute` usando únicamente comandos `ping`?

4. Ejecute `traceroute` a `www.zoom.com` y responda a lo siguiente:
   a) Para cada salto intente identificar la ubicación geográfica y empresa responsable.

   b) Repita el mismo análisis para `zoom.com`.

Referencias

[1] ping(8) - Linux man page. Accesible en línea: https://linux.die.net/man/8/ping. Última visita: Julio 2023.

[2] Analizador de Tráfico Wireshark. Accesible en línea: http://www.wireshark.org/. Última visita: Julio 2023.

[3] traceroute(8) - Linux man page. Accesible en línea: https://linux.die.net/man/8/traceroute. Última visita: Julio 2023.

[4] tracepath(8) - Linux man page. Accesible en línea: https://linux.die.net/man/8/tracepath. Última visita: Julio 2023.

[5] tracert Documentation. Accesible en línea: https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/tracert. Última visita: Julio 2023.

[6] dig(1) - Linux man page. Accesible en línea: https://linux.die.net/man/1/dig. Última visita: Julio 2023.