Redes de Computadoras

Obligatorio 1 - 2018

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, news, correo, papeles sobre la mesa, etc.).

Introducción

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.
- Los programas y capturas solicitados.
- 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 26/8/2018 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

Los programas pueden ser escritos en cualquier lenguaje, pero se recomienda utilizar algún lenguaje de scripting, que son adecuados al tipo de tareas solicitadas (`shell script` o `python` por ejemplo). Los programas deberán poder ejecutarse dentro de las máquinas virtuales brindadas para el curso en los PCs Linux de facultad.

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 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 cualquiera de los entornos mencionados, dependiendo de los permisos requeridos por las herramientas necesarias son las siguientes:

- `ping`
- `wireshark` [1]
- `traceroute (equivalente en Windows: tracert)`
- `dig`

En caso de requerir permisos de root, deberá desarrollarse en la máquina virtual brindada.

Parte A - Captura de tráfico con Wireshark

1. Investigue y documente para que sirve y como se utiliza la herramienta `Wireshark`.

2. Realice la captura del tráfico generado por un equipo, para la interfaz que conecta el equipo con Internet mientras realiza el acceso a través de un navegador a la página `http://home.mcom.com/home/welcome.html`. Grabe en un archivo `netscape.pcap` el tráfico capturado. Analice la captura de tráfico realizada:
   a) Identifique el mensaje de solicitud al servidor DNS utilizado para obtener la IP del dominio. ¿Que servidor DNS se utilizó?
   b) Explique como es posible identificar las conexiones TCP que se establecieron para descargar la página solicitada. Muestre una de estas conexiones.
   c) Explique los distintos métodos del protocolo HTTP y muestre en su captura que métodos se utilizaron para solicitar la página al servidor.
   d) Identifique el User-Agent utilizado y explique su significado. ¿Por qué es útil para el servidor web tener esta información?
   e) Identifique en su captura los segmentos TCP donde el servidor envía la página HTML principal.

NOTAS:
Tenga en cuenta que en las PCs de Facultad el acceso a Internet se realiza a través de un servidor proxy. Esto puede generar diferencias con pruebas en otras redes.
Para facilitar los análisis con la herramienta Wireshark, pruebe de aplicar filtros a la captura de paquetes que realiza.

Parte B - Comando ping

1. Investigue y documente el principio de funcionamiento de la utilidad `ping`. El análisis debe incluir una descripción del los protocolos utilizados por la herramienta y una explicación de la salida del comando.

2. Utilizando `wireshark` analice los paquetes intercambiados entre origen y destino al hacer un `ping`. Muestre los protocolos utilizados incluyendo al menos 4 cabezales de 2 protocolos diferentes.

3. Pruebe los siguientes comandos y analice las salidas.
   Describa las conclusiones a las que puede arribar con respecto a cada sitio analizado. Defina 2 criterios diferentes para determinar cual sitio es el mas cercano e indique si este tipo de resultado es absoluto o si es temporal.

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

4. Suponga que se le dice que el servidor DNS que usa en la PC donde hace el `ping` es muy lento en la resolución de nombres. ¿Podría esto influir en las pruebas de alguna manera? En caso que sí, ¿qué haría usted para eliminar o minimizar el impacto?

5. La unidad máxima de transferencia (*Maximum Transmission Unit* - MTU) es un término que expresa el tamaño en bytes de la unidad de datos más grande que puede enviarse usando un determinado protocolo de comunicaciones.
   Proponga un mecanismo (utilizando ping) para determinar el MTU de un camino.

Parte C - Comando traceroute

1. Investigue el principio de funcionamiento del comando `traceroute`.

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

3. Ejecute traceroute a cada uno de los hosts del punto 3 de la Parte B.
   a) Documente y analice los resultados.
      Para los casos donde no pudo llegar, pruebe traceroute con un protocolo distinto al por defecto.
   b) ¿Coinciden los resultados con su respuesta de la Parte B?
   c) Para cada prueba, identifique el o los hops con mayor influencia en el tiempo para alcanzar el destino. ¿Que puede decir de estos hops?

Parte D - Comando dig

1. Investigue y documente el funcionamiento del sistema DNS en Internet. El análisis debe incluir una explicación del funcionamiento del sistema y una explicación de la diferencia entre un servidor recursivo y uno iterativo.

2. Investigue y documente para que sirve y como funciona la utilidad del sistema `dig`.

3. Realice con `dig` una consulta del registro A del dominio `redhat.com` a los servidores DNS con IP 192.42.93.30 y 8.8.8.8. Analice y justifique similitudes y diferencias de las respuestas obtenidas.

4. Se desea emular el comportamiento de un servidor de DNS iterativo. Para esto escriba un programa utilizando un lenguaje de scripting y el comando `dig`, que dado un nombre de dominio pasado por parámetro, realice una consulta iterativa. La consulta deberá comenzar con algún servidor raíz de la lista dada en [2].
   Asegúrese que ningún servidor de los que consulta resuelva parte de su problema.
   Verifique su funcionamiento utilizando la captura del tráfico al ejecutar el comando con `wireshark`.

5. Explique como es posible obtener el nombre de un host a partir de su dirección IP.

NOTA:
En los equipos de facultad la consulta a DNS externos esta deshabilitada, por lo tanto existen partes que deben realizarse en un equipo conectado a una red hogareña o a través de la red inalámbrica wifing utilizando el protocolo TCP.

Referencias y Bibliografía Recomendada

[1] Analizador de Tráfico Wireshark. Accesible en línea: *http://www.wireshark.org/*. Última visita: Agosto 2017.

[2] https://www.iana.org/domains/root/servers