Redes de Computadoras

Obligatorio 1 - 2015

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 `https://eva.fing.edu.uy/mod/resource/view.php?id=43153`

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.).

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 `obligatorio1.tar.gz` que deberá contener los siguientes archivos:

- Un documento llamado `Obligatorio1GrupoNN.pdf` donde se documente todo lo solicitado en la tarea. `NN` es el número del grupo.
- Los programas 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 domingo 6 de setiembre 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 solicitados pueden ser escritos en cualquier lenguaje, pero se recomienda utilizar algún lenguaje de scripting por su facilidad para este tipo de programas (`shell script` o `python` por ejemplo). Los programas deberán poder ejecutarse dentro de las máquinas 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.

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, y las herramientas necesarias son las siguientes:

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

Se pide

1) Comando ping

Una manera de probar que se puede alcanzar otro *end system* es mediante la utilización del comando `ping`.

1. Investigue y documente el principio de funcionamiento del comando ping: `man ping`. ¿Qué protocolo/s utiliza?

2. Implemente un programa que dados dos parámetros que son los *hosts* que se pretende monitorizar, dé como resultado cual es el *host* que presenta mejores tiempos de respuesta en base a alguna métrica.

3. Extienda el programa anterior de manera que su programa esté monitorizando de forma alternada ambos *hosts*, y muestre en pantalla un mensaje solo cuando exista algún problema. El problema podrá ser o que no se alcanza al destino o que el tiempo de respuesta supera un umbral especificado también como parámetro.

4. Considere un *host* a su elección, y ejecute el comando `ping -c 10 host.dominio` y luego ejecútelo nuevamente agregando la flag `-n`. ¿Puede apreciar una diferencia en el tiempo de respuesta entre ambas ejecuciones? Analice los resultados.

5. Tamaño de las pruebas

    a) ¿Cuál es el tamaño máximo y el tamaño por defecto del mensaje enviado por el comando `ping`?
    b) Pruebe hacer *pings* con los tamaños 100, 1.000 y 10.000 a diferentes *hosts* y determine de forma fundamentada si el tamaño del mensaje incide en los tiempos observados.

2) Comando traceroute

1. Investigue y documente el principio de funcionamiento del comando `traceroute`: `man traceroute`. ¿Qué protocolo/s utiliza?

2. Escriba un programa que toma como parámetro una IP o un FQDN, que sea capaz de identificar el o los hops **con mayor influencia en el tiempo para alcanzar ese host**. ¿Cómo explica este comportamiento?

3. Excriba un programa que toma como parámetro una IP o un FQDN e identifique los *ISPs* y/o *carriers* internacionales utilizados, imprimiéndolos en pantalla.

4. Investiguen y documenten de manera concisa la utilidad de los servidores *Looking Glass* .

   Realice pruebas del comando `traceroute` pero ahora seleccionando dos *Looking Glass* a su elección de [2], de manera de primero tomar uno como origen y el segundo como destino y viceversa.
   Documente los resultados obtenidos y trate de explicar las diferencias de comportamiento de las pruebas en un sentido y en el otro. Por ejemplo podría usar `Registro.br`(AS22548) y `Hurricane Electric (he.net)` (AS6939) para las pruebas.

3) Comando dig

1. Hoy día, el sistema DNS es un pilar en el funcionamiento de la red. De hecho muchas veces sucede que cuando no funciona el DNS los usuarios dicen cosas como: “¡no me anda Internet!”. Comente brevemente razones para este tipo de afirmaciones..

Para enfrentar problemas de DNS es importante tener una buena herramienta para diagnosticar. Dado que usted aprendió mucho sobre `dig` y del sistema DNS, una empresa se interesó en contratarlo para resolver problemas. Para las siguientes partes deberá explicar como logra la solución, detallando los conceptos que usa para lograrla.

2. Lo primero que le solicitan es que escriba un programa que tome como parámetro un nombre de dominio, y que retorne el o los servidores de nombre autoritativos para ese dominio.

3. Luego de algunos problemas ocasionados por servidores de DNS que tenían información errónea, la empresa le pide crear un nuevo programa, que toma como parámetros el FQDN y el tipo de RR a consultar, y retorna el resultado. Lo interesante del programa es que deberá dar una respuesta que sea autoritativa.

4. Otro problema frecuente que tiene la empresa es la gran cantidad de correo *spam* que recibe. Por esta razón necesitan que usted haga un programa que dado un nombre de dominio y una dirección IP (que es la IP del host que se conectó y pretende enviar un correo usando un remitente que pertenece al dominio pasado como primer parámetro) retorne una respuesta booleana que diga que esa IP es efectivamente una dirección IP correspondiente a un servidor de correo de ese dominio. Esa comprobación deberá ser hecha siempre contra los servidores autoritativos de ese dominio.

5. Ejecute los comandos `dig www.google.com` y `dig www.fing.edu.uy`. ¿En qué difieren? Explique el motivo de esas diferencias.

6. Ejecute los comandos `dig www.google.com` y `dig google.com` por un lado, y `dig www.fing.edu.uy` y `dig fing.edu.uy` por otro. ¿En qué difieren? Dé argumentos a favor y en contra de ambas políticas.

4) Captura de tráfico con Wireshark

1. ¿Qué utilidades tiene la herramienta `Wireshark`?

2. Cargue el archivo `Captura1.pcap` en el wireshark. Allí hay una captura de tráfico que se realizó durante la ejecución de uno de los programas de la sección 3.

Identifique cuál es ese programa y explique en detalle como llega a esa conclusión en base a la captura..

3. Cargue el archivo `Captura2.pcap` en el wireshark. Allí hay una captura de tráfico que se realizó durante la ejecución de uno de los comandos de la sección 2. Identifique si el parámetro fue una IP o un FQDN y explique en detalle como llega a esa conclusión en base a la captura.

NOTA:
Para facilitar los análisis con la herramienta Wireshark, pruebe de aplicar filtros a la captura de paquetes que realiza.

Referencias y Bibliografía Recomendada

[1] Analizador de Tráfico Wireshark. Accesible en línea: *http://www.wireshark.org/*. Última visita: Agosto 2015.

[2]Listado de servidores *Looking Glass*. Accesible en línea: `http://www.traceroute.org/#Looking%20Glass`. Última visita: Agosto 2015.

[3]Internet Control Message Protocol (ICMP) Parameters. En línea: *http://www.iana.org/assignments/icmp-parameters*. Última visita: Agosto 2015.