Introducción a las Redes de Computadoras

Obligatorio 1 – 2011

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 `http://www.fing.edu.uy/inco/pm/uploads/Ense%f1anza/NoIndividualidad.pdf`

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

Forma de entrega

Una clara, concisa y descriptiva documentación es clave para la evaluación de los trabajos entregados.

La entrega del obligatorio consiste en un único archivo `obligatorio1.tar.gz` que deberá a su vez contener los siguientes archivos:

- Un documento llamado `obligatorio1.pdf` donde se documente todo lo solicitado en el presente obligatorio.
- Los archivos correspondientes a la/s capturas de tráfico realizadas.

La entrega se realizará a través del sitio Web del curso, en la URL `http://www.fing.edu.uy/inco/cursos/redescomp/entrega.html`

Fecha de entrega

Los trabajos deberán ser entregados antes del domingo 27 de marzo 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, ni entregados en medios magnéticos en el instituto.

El sistema de entregas soporta múltiples entregas por grupo, llevando un histórico de las mismas. Se recomienda realizar una entrega vacía con tiempo, a los efectos de verificar que su sistema le permite entregar correctamente.

Observaciones

Todas las ejecuciones deberán ser realizadas en las máquinas virtuales distribuidas como parte del material del curso.

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.

Herramientas

El obligatorio se desarrollará en un entorno GNU/Linux, para lo cual se dispone de máquina virtual. Este entorno tiene las herramientas necesarias ya instaladas, tales como:

- `ping`
- `traceroute`
- `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 básico de funcionamiento del comando `ping`: `man ping`. En caso de ser necesario complemente dicha información con otra disponible en fuentes confiables. ¿Qué protocolo/s y mensajes utiliza?

2. Pruebe los siguientes comandos

```
ping -c5 www.nba.com
ping -c5 www.google.com
ping -c5 www.google.com.uy
ping -c5 www.adinet.com.uy
ping -c5 www.presidencia.gub.uy
ping -c5 www.agesic.gub.uy
```

   Utilice *copiar-y-pegar* de la salida de cada uno de los comandos y conteste fundamentando:

   a) ¿Cuál es el servicio con peor tiempo de respuesta?

   b) Explique las diferencias entre las salidas observadas y todo aquello que considere relevante.

   c) Ejecute el primer comando pero ahora desde dos líneas de comando y "al mismo tiempo". Analice los resultados y concluya.

   d) Ejecute el último comando pero ahora también con la opción `-n`. ¿Qué conclusión puede sacar de lo observado?

3. Tamaño de las pruebas

   a) ¿Cuál es el tamaño por defecto del mensaje enviado por el comando `ping`?

   b) Ejecute el comando `ping` pero ahora cambiando la cantidad de bytes de datos enviados a 100 y luego a 10.000 con destino a `www.agesic.gub.uy`, y concluya de manera fundamentada si el tamaño del mensaje incide en los tiempos observados.

   c) ¿Cuál es el tamaño máximo del mensaje enviado por el comando `ping`?

2) Comando `traceroute`

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

2. Ejecute los siguientes comandos

```
traceroute www.google.com
traceroute www.nba.com
traceroute mirror.sptel.com.au
```

   Utilizando *copiar-y-pegar* de la salida de los comandos fundamente cuál es el destino más lejano a su punto de acceso a la red, considerando la distancia

basada en la cantidad de *hops* o saltos que atraviesan sus mensajes para llegar a cada destino. ¿Qué destinos fue posible alcanzar con la prueba `traceroute`?, ¿cómo podría explicar dicho comportamiento?

3. ¿Puede correlacionar los tiempos de respuesta medidos con el comando `ping` con la distancia medida en *hops*? Fundamente su respuesta.

4. Ejecute el último comando de la parte 2 pero ahora con la opción `-n`. ¿Qué conclusión puede sacar de lo observado?

5. ANTEL es el *carrier* nacional utilizado en las pruebas (además de ser *Internet Service Provider*). Deduzca el rol de las empresas identificadas a partir de la salida del último comando ejecutado, en particular lo que refiere a los dominios: “he.net”, “tpgi.com.au” y “comindico.com.au”.

6. Un servidor *Looking Glass* es un *end system* que ejecuta un software que permite ver información de enrutamiento, permitiendo al usuario realizar pruebas como si estuviera localizado en dicho servidor.

   Realice pruebas del comando `traceroute` pero ahora desde el servicio provisto por PST (AS 9942) de Australia hacia la dirección IP 164.73.32.3.
   Documente los resultados obtenidos y compare con la salida del último comando ejecutado en la parte 2.

3) Comando dig

1. Investigue y documente el principio básico de funcionamiento del comando `dig`: `man dig`.

2. Ejecute el comando

```
dig www.fing.edu.uy @164.73.32.2
```

   Utilice *copiar-y-pegar* de la salida del comando y analice el resultado. ¿Qué otro nombre tiene el servidor Web de facultad? ¿Cómo lo indica el DNS?

3. ¿Con qué comando puede obtener la dirección de red de el o los servidores de correo de Gmail? Proponga de que formas se podría utilizar el DNS para balancear la carga de correo u otro servicio.

4. Analizando nuevamente la salida de la parte 2, ¿cuáles son los servidores de nombres del dominio `fing.edu.uy`? Las respuestas obtenidas, ¿son autoritativas? Justifique su respuesta.

5. Compare e interprete las salidas de los siguientes comandos

```
dig www.universidad.edu.uy @200.40.30.254
dig www.universidad.edu.uy @200.40.30.245
```

6. ¿Con qué comando puede obtener el nombre del *host* cuya dirección IP es 164.73.128.3?

4) Captura de tráfico con Wireshark

1. ¿Cuál es la funcionalidad del software `Wireshark`?

2. ¿Cuál es la versión del `Wireshark` disponible en el BackTrack 3 (BT3)? ¿Desde

qué año está disponible el BT3? ¿Qué versión estable está disponible en el portal del `Wireshark` para ser bajada? Identifique las dos principales causas para las actualizaciones que se le han realizado al software.

3. Utilizando `Wireshark`, capture el tráfico generado cuando utiliza un navegador para acceder a la página `http://www.ricaldoni.org.uy` (con el `Wireshark` y el navegador corriendo dentro de la máquina virtual).

4. Analice la captura de tráfico del punto anterior, ¿cuántas conexiones TCP se establecieron? Identifíquelas completamente.

5. ¿Qué método HTTP se invocó?

6. Utilizando el tráfico capturado en la parte 3:
   a) Identifique el User-Agent utilizado, así como su significado.

   b) Identifique qué información envía el servidor por cada sesión TCP.

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. En línea: `http://www.wireshark.org/`. Última visita: Marzo 2011.

[2]Listado de servidores *Looking Glass*. En línea: `http://www.traceroute.org/#Looking%20Glass`. Última visita: Marzo 2011.

[3]*Internet Control Message Protocol (ICMP) Parameters*. En línea: `http://www.iana.org/assignments/icmp-parameters`. Última visita: Marzo 2011.

[4]*Secunia Vulnerability Report: Wireshark 1.x*. En línea: `http://secunia.com/advisories/product/18083/`. Última visita: Marzo 2011.

[5]*User Agent String*. En línea: `http://www.useragentstring.com`. Última visita: Marzo 2011.