Redes de Computadoras

Obligatorio 1 - Familiarizarse con conceptos básicos sobre redes e Internet y manejar herramientas para diagnóstico y debug de la red.

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 utiliza?
2. Pruebe los siguientes comandos:
   ```
   ping -c 5 www.fedoraproject.org
   ping -c 5 www.google.com
   ping -c 5 www.adinet.com.uy
   ping -c 5 ww.presidencia.gub.uy
   ping -c 5 www.smn.gov.ar
   ```
   Copie y pegue la salida y responda fundamentando:
   a) ¿Cuál es el servicio con mejor tiempo de respuesta?
   b) ¿Cómo explica las diferencias entre las salidas?
3. Repita las pruebas anteriores a los *hosts*:
   ```
   ns1.dyndns.com
   ns2.dyndns.com
   ns3.dyndns.com
   ns4.dyndns.com
   ns5.dyndns.com
   ```
   Copie y pegue la salida y responda:
   a) ¿Cómo explica que 5 equipos del mismo dominio tengan tiempos de respuesta tan diferentes?
   b) ¿Para qué sirve el servicio ofrecido por *dyndns*? Investigue y explique brevemente su utilidad. ¿Porque cree que existe?
4. Tamaño de las pruebas
   a) ¿Cuál es 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.
   c) ¿Cuál es el tamaño máximo del mensaje enviado por el comando *ping*?

2) Comando traceroute

1. Investigue y documente el principio de funcionamiento del comando *traceroute*:
   ```
   man traceroute.
   ```
   ¿Qué protocolo/s utiliza?
2. Ejecute *traceroute* a cada uno de los *hosts* anteriores copiando la salida fundamentando responda cual de los host es el equipo más próximo a usted, considerando la distancia basada en la cantidad de *saltos* u *hops* (*routers* u *hosts*) que atraviesan sus mensajes para llegar a él.
   ¿Pudo llegar a todos los destinos con la prueba *traceroute*?, ¿a cuales si y a cuales no? ¿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. Si comparamos las salidas de los comandos:
   ```
   traceroute www.google.com
   traceroute www.fing.edu.uy
   ```

¿Puede asociar a un *hop* particular la diferencia de los tiempos de respuesta?, ¿puede explicar este motivo?

5. Habrá visto que ANTEL es el principal *carrier* nacional utilizado en las pruebas. ¿Qué otros *carriers* internacionales vio en sus pruebas? Fundamente con las salidas de los comandos anteriores.

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 "parado" en dicho servidor. Realice pruebas tomando dos *looking glass* a su elección de [2], de manera de primero tomar uno como origen y el segundo como destino y viceversa.

3) Comando dig

1. Investigue y documente el principio de funcionamiento del *dig*: `man dig`
   (Obs: *dig* reemplaza otro comando de funcionalidad similar llamado *nslookup*)
2. Ejecute el comando `dig www.fing.edu.uy @164.73.32.2`
   Pegue la salida y responda
   ¿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 él 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 2, ¿cuáles son los servidores de nombres del dominio `fing.edu.uy`? las respuestas obtenidas, ¿son autoritativas? ¿por qué?
5. ¿Con que comando puede obtener a quién pertenece la dirección IP `12.22.58.30`?

4) Comando nmap

1. Investigue y documente el principio del funcionamiento del comando `nmap`.
2. Escanee toda su red utilizando `nmap` describiendo completamente la salida del comando.
3. ¿Para que sirven los modificadores `-sU`, `-sA` y `-p` del comando?

5) Captura de tráfico con Wireshark

1. ¿Cuál es la funcionalidad del software *Wireshark*?
2. Utilizando *Wireshark*, capture todo el tráfico generado cuando se conecta al ip `200.40.206.74:33`
   (*Sugerencia: conectarse utilizando* `telnet`)
3. Siga las instrucciones que le da este servicio, copiando todos los datos enviados, y los recibidos.
4. ¿De que servicio se trata?
5. ¿Qué método de transporte utiliza?

Entrega

La entrega se debe realizar en un entorno tipo *UNIX*, se le brindara a cada alumno un usuario y una contraseña para poder realizar el obligatorio en un servidor de *ESI Buceo.*
Se debe entregar un archivo llamado `redes-e1.tar.gz` conteniendo un archivo `redes-e1.pdf` con las respuestas a las preguntas, y un archivo `redes-e1.pcap` con la captura de wireshark. En el *pdf* se deben detallar los datos del estudiante (*Nombre, Apellido y Cédula*).
El trabajo es individual y se deberá entregar **no después** del ***viernes 11 de mayo del 2012*** a las 23:59 UYT.
Los detalles de la entrega se aclararan mas adelante.

Los trabajos que no respeten el formato de entrega no serán considerados.

Referencias y Bibliografía Recomendada

[1] http://www.wireshark.org/
[2] http://www.traceroute.org/
[3] http://nmap.org/man/es/