ESTUDIO DEL PROTOCOLO DNS CON WIRESHARK

En este taller estudiaremos el funcionamiento del protocolo DNS, mediante algunas capturas con Wireshark. Proceda de la siguiente manera:

- Vacíe el caché DNS de su computador, ejecutando el comando `ipconfig /flushdns`
- Abra Wireshark e inicie la captura de paquetes.
- En el campo de filtro, introduzca `ip.addr==x.x.x.x`, para mostrar únicamente el tráfico originado desde o dirigido a su PC (`x.x.x.x` debe ser la dirección IP de su PC).
- Navegue a http://www.ietf.org
- Detenga la captura de paquetes

Conteste las siguientes preguntas con respecto a la captura:

1. Ubique los mensajes DNS de consulta y respuesta. ¿Se envían sobre TCP o UDP?
2. ¿Cuál es el puerto de destino para el mensaje DNS de consulta? ¿Cuál es el puerto de origen para el mensaje DNS de respuesta?
3. ¿A cuál dirección se envía la consulta DNS? Emplee `ipconfig` para determinar la dirección de su servidor DNS local. ¿Son iguales estas dos direcciones?
4. Examine el mensaje de consulta DNS. ¿Qué tipo de consulta es? ¿El mensaje de consulta contiene respuestas?
5. Examine el mensaje de respuesta DNS. ¿Cuántas respuestas contiene? ¿Cuál es el contenido de cada una de las respuestas?
6. Examine el paquete TCP SYN que su PC envía a continuación de las consultas al DNS. ¿La dirección IP de destino del paquete SYN coincide con alguna de las direcciones IP incluidas en el mensaje de respuesta DNS?
7. La página web contiene imágenes. Antes de recuperar cada imagen, ¿su PC hace más consultas al DNS?

Ahora experimentemos con nslookup:

- Inicie la captura de paquetes. Mantenga el filtro del paso anterior.
- Ejecute el comando `nslookup www.mit.edu`
- Detenga la captura de paquetes.

Conteste las siguientes preguntas:

8. Examine el mensaje de consulta DNS. ¿Cuál es el tipo de consulta? ¿El mensaje de consulta contiene alguna respuesta?
9. Examine el mensaje de respuesta DNS. ¿Cuántas respuestas incluye? ¿Qué contiene cada una de las respuestas?
10. Incluya una captura de pantalla.

Ahora repitamos el experimento anterior, pero ejecutando el comando `nslookup -type=NS mit.edu`

Conteste las siguientes preguntas:

11. Examine el mensaje de consulta DNS. ¿Cuál es el tipo de consulta? ¿El mensaje de consulta contiene alguna respuesta?
12. Examine el mensaje de respuesta DNS. ¿Cuáles son los nombres de los servidores DNS del MIT? ¿El mensaje de respuesta contiene también las direcciones IP de los servidores DNS del MIT?
13. Incluya una captura de pantalla.