Práctica 3 – DNS –

En la práctica de esta semana vamos estudiar el servicio de DNS! Lo vamos a usar utilizando wireshark así cómo otras herramientas muy útiles para DNS.

1. nslookup

En este laboratorio vamos a probar la herramienta nslookup, disponible para linux y windows. Para ejecutar nslookup en cualquiera de los sistemas operativos deberás estar en tu ventana de terminal con en la línea de comando.

Esta herramienta nos va a servir para realizar una consulta de DNS a un servidor que nos constestará con el registro de DNS y sus respectivas variables de registro, indicando por ejemplo qué tipo de servidor DNS es, si es su authoritative o no, entre otros.

```
root@michiruy:/home/alestolk# nslookup www.ula.ve
Server:         150.185.130.8
Address:        150.185.130.8#53

www.ula.ve      canonical name = trebol.adm.ula.ve.
Name:   trebol.adm.ula.ve
Address: 150.185.168.156

root@michiruy:/home/alestolk# nslookup -type=NS ula.ve
Server:         150.185.130.8
Address:        150.185.130.8#53

ula.ve  nameserver = azmodan.ula.ve.
ula.ve  nameserver = avalon.ula.ve.

root@michiruy:/home/alestolk# nslookup www.ula.ve dns2.usb.ve
Server:         dns2.usb.ve
Address:        159.90.200.7#53

Non-authoritative answer:
www.ula.ve      canonical name = trebol.adm.ula.ve.
Name:   trebol.adm.ula.ve
Address: 150.185.168.156
```

En el pantallazo de arriba podemos ver los resultados de 3 consultas de nslookup realizados en linux. En ese ejemplo la consulta se realizó en un equipo cliente ubicado en el campus de la Universidad de los Andes, en dónde el DNS por omisión es azmodan.ula.ve. Cuando ejecutas un nslooup y no especificas un servidor DNS, la herramienta utiliza el DNS configurado en el equipo por omisión.

Práctica 3 – DNS –

Ejecuta:

nslookup www.ula.ve

¿Qué estás preguntándole a nslookup? “Por favor dime cual es la IP del host: www.ula.ve”
y cómo lo muestra en la figura esta es la respuesta que obtienes, es:

1. El nombre y la IP del servidor que te está dando la respuesta
2. La respuesta como tal, consiste en el nombre y la IP de lo que solicitaste aunque la respuesta te la dió el DNS local (en el caso del ejemplo, el servidor DNS la Universidad de Los Andes, lo más probable es que este servidor a su vez haya contactado a otros servidores antes de darte esa respuesta! Si quieres tener más detalles sobre esto puedes consultar el libro de texto en la sección 2.4. Ahora considera el segundo comando del ejemplo:

nslookup –type=NS ula.ve

En este ejemplo, nosotros hemos solicitado la opción “-type=NS” y el dominio “ula.ve”. Cuando ejecutamos esta opción estamos preguntando: “ por favor dime los equipos son DNS autorizados para el dominio ula.ve” (Cuando no se utiliza la opción -type, nslookup usa el valor predeterminado, que es consultar los registros de tipo A). La respuesta, que se muestra en la captura, primero indica el Servidor DNS que proporciona la respuesta (que es el servidor DNS local predeterminado) junto con varios servidores de nombres la ULA. Cada uno de estos servidores es de hecho un servidor DNS autorizado para los equipo en el campus de la ULA o el dominio ula.ve.

Finalmente, la respuesta incluye el IP direcciones de los servidores DNS autorizados en la ULA. (Aunque la consulta type-NS generado por nslookup no pidió explícitamente las direcciones IP, el servidor DNS local devolvió estos datos "gratis" y nslookup muestra el resultado.) Finalmente, veamos el tercer comando:

nslookup www.ula.ve dns2.usb.ve

En este ejemplo, indicamos que queremos la consulta enviada al servidor DNS www.ula.ve en lugar del servidor DNS predeterminado (avalon.ula.ve) esta vez al servidor DNS dns2.usb.ve uno de los dns de la Universidad Simón Bolívar. Por lo tanto, la consulta y la transacción de respuesta se lleva a cabo directamente entre nuestro host local y dns2.usb.ve. En este ejemplo, el servidor DNS dns2.usb.ve proporciona la dirección IP del host www.ula.ve.

Práctica 3 – DNS –

Ahora que hemos analizado algunos ejemplos ilustrativos, quizás te preguntes cómo funciona la sintaxis general de los comandos nslookup. La sintaxis es:

nslookup –option1 –option2 host-to-find dns-server

En general, nslookup se puede ejecutar con cero, una, dos o más opciones. Y como hemos visto en los ejemplos anteriores, el servidor dns es opcional también; si no se proporciona, la consulta es enviada al servidor DNS local predeterminado. Ahora que hemos proporcionado una descripción general de nslookup, es hora de que pruebe probarlo tú mismo.

Haz lo siguiente (y pon tus resultados en el informe de la práctica):

1. Ejecuta nslookup para obtener la dirección IP de un servidor web en Asia ¿Cual es la dirección IP de ese servidor?
2. Ejecuta nslookup para determinar los servidores DNS autorizados para la Universidad Central de Venezuela (UCV).
3. Ejecuta nslookup para que se consulte uno de los servidores DNS obtenidos en la Pregunta 2 y los servidores de correo para Yahoo! OJO de correo. ¿Cuál es su dirección IP?

3. **Rastreo de DNS con Wireshark**

Ahora que estamos familiarizados con nslookup, estamos listos para revisar más seriamente la actividad de DNS por debajo. Primero capturemos los paquetes DNS que son generados vía Websurfing.

• Usa ipconfig o ifconfig para vaciar el caché de DNS en tu equipo
• Abra su navegador y vacía el caché del navegador
• Abre Wireshark y escribe "ip.addr == your_IP_address" en el filtro. Este filtro elimina todos los paquetes que ni se originan ni están destinados a tu equipo
• Comienza la captura de paquetes en Wireshark
• El navegador, visita la página web: http://www.ietf.org
• Detén la captura de paquetes.

Acuérdate que si no puedes ejecutar Wireshark en una conexión de red en vivo, puede descargar un archivo de rastreo de paquetes que se capturó al seguir los pasos anteriores en uno de los computadoras en los enlaces indicados en las prácticas anteriores. Responde las siguientes preguntas.

Siempre que sea posible, cuando respondas a continuación, pon una copia impresa del paquete (s) dentro del rastro que te indicó wireshark. Para imprimir un paquete A, usa las

opciones: Archivo-> Imprimir, elije el Paquete, elije Resumen de paquete (en inglés: File->Print, choose Selected packet only, choose Packet summary line), y selecciona la cantidad mínima de detalles del paquete que necesitas para responder las siguientes preguntas en el informe de la práctica.

4. Ubica los mensajes de consulta y respuesta de DNS. ¿Estos se envían a través de UDP o TCP?
5. ¿Cuál es el puerto de destino para el mensaje de consulta DNS? ¿Cuál es el puerto de origen del mensaje de respuesta DNS?
6. ¿A qué dirección IP se envía el mensaje de consulta DNS? Use ipconfig/ifconfig para determinar la dirección IP de tu servidor DNS local. ¿Son estas dos direcciones IP iguales?
7. Examina el mensaje de consulta DNS. ¿Qué "Tipo" de consulta DNS es? ¿El mensaje de consulta contiene alguna "respuesta"?
8. Examina el mensaje de respuesta DNS. ¿Cuántas "respuestas" se proporcionan? ¿Qué contiene cada una de estas respuestas?
9. Considera el paquete TCP SYN posterior enviado por tu equipo. La dirección IP destino del paquete SYN corresponde a cualquiera de las direcciones IP provistas en el mensaje de respuesta DNS?
10. Esta página web contiene imágenes. Antes de recuperar cada imagen, ¿tu equipo emite nuevas consultas DNS?

4. Ahora probemos nslookup4.

- Inicia la captura de paquetes.
- Haz un nslookup a www.ula.ve
- Detén la captura de paquetes.

Deberías obtener un rastro que se parece a lo siguiente:
Vemos en la captura de pantalla anterior que nslookup realmente envió tres consultas DNS y recibió tres respuestas de DNS. A los efectos de esta tarea, al responder al siguientes preguntas, ignore los primeros dos conjuntos de consultas/respuestas, ya que son específicas de nslookup y normalmente no son generados por aplicaciones estándar de Internet. Debieras en su lugar, concéntrese en los últimos mensajes de consulta y respuesta.

11. ¿Cuál es el puerto de destino para el mensaje de consulta DNS? ¿Cuál es el puerto de origen del mensaje de respuesta DNS?
12. ¿A qué dirección IP se envía el mensaje de consulta DNS? ¿Es esta la dirección IP de tu servidor DNS local predeterminado?

Práctica 3 – DNS –

13. Examina el mensaje de consulta DNS. ¿Qué "Tipo" de consulta DNS es? ¿El mensaje de consulta contiene alguna "respuesta"?
14. Examina el mensaje de respuesta de DNS. ¿Cuántas "respuestas" se proporcionan? ¿Qué contiene cada una de estas respuestas?
15. Proporciona una captura de pantalla.
Ahora repite el experimento anterior, pero usa el comando:
nslookup -type = NS mit.edu
Responde las siguientes preguntas:
16. ¿A qué dirección IP se envía el mensaje de consulta DNS? ¿Es esta la dirección IP de tu servidor DNS local predeterminado?
17. Examina el mensaje de consulta DNS. ¿Qué "Tipo" de consulta DNS es? ¿El mensaje de consulta contiene alguna "respuesta"?
18. Examina el mensaje de respuesta de DNS. ¿Qué servidores de nombres ULA hace la respuesta mensaje de proporcionar? ¿Este mensaje de respuesta también proporciona las direcciones IP de Nombres de ULA?
19. Proporciona una captura de pantalla.
Ahora repite el experimento anterior, pero usando el comando: nslookup www.aiit.or.kr bitsy.mit.edu
Responde las siguientes preguntas:
20. ¿A qué dirección IP se envía el mensaje de consulta DNS? ¿Es esta la dirección IP de tu servidor DNS local predeterminado? Si no, ¿a qué se corresponde la dirección IP?
21. Examina el mensaje de consulta DNS. ¿Qué "Tipo" de consulta DNS es? ¿El mensaje de consulta contiene alguna "respuesta"?
22. Examina el mensaje de respuesta DNS. ¿Cuántas "respuestas" se proporcionan? ¿Qué contiene cada una de estas respuestas?
23. Proporciona una captura de pantalla.

5. Por último, ubica en las bases de datos de los organismos correspondientes las siguientes direcciones IP:

1. 137.158.154.230
2. 144.32.128.84
3. 207.75.164.248
4. 210.152.243.234
5. 157.92.5.125

Dime en el informe:

24. A que corresponde esa IP
25. Cúal es el registro de DNS que encontraste para cada uno
26. Si ocurre un incidente que implique a esa dirección a quien le escribirías un correo