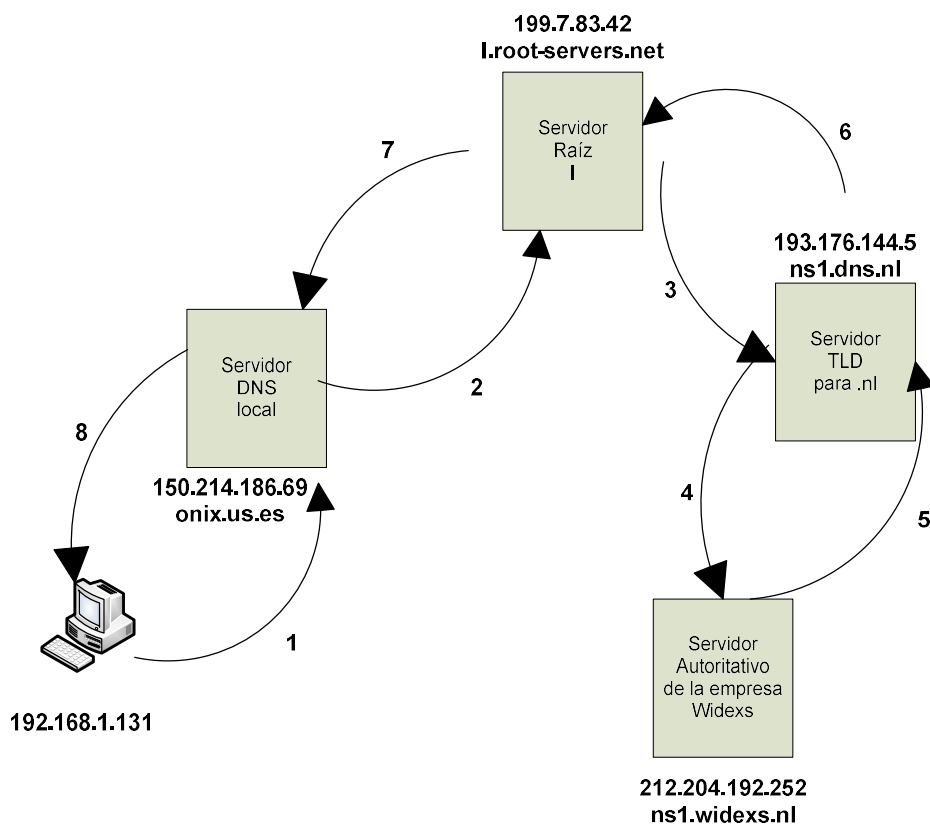


Problema 16.

Parte 1

Pregunta 1. La Figura 1 muestra esquemáticamente la búsqueda DNS realizada por un PC con dirección IP 192.168.1.131. La petición DNS etiquetada con el número 1 es una petición de un registro tipo A en el que se pregunta por la dirección IP de la URL `www.santander.nl`. Dicha URL es la página web del Banco Santander en Holanda (con dirección IP 78.31.116.203), y está alojada en un servidor de la empresa holandesa de hosting Widexs.



¿Qué tipo de búsqueda ha tenido lugar en la jerarquía DNS?

Respuesta: Se trata de una búsqueda recursiva, puesto que se deja la responsabilidad de la búsqueda al servidor raíz.

Pregunta 2. ¿Qué RRs ha debido facilitar el Banco Santander al servidor autoritativo de Widexs para que sus servicios en Holanda sean visibles? Además del servidor web antes mencionado,

también dispone del dominio de correo santander.nl, ubicado en el servidor cluster2.eu.messagelabs.com, con dirección IP 195.245.230.131.

Respuesta:

(www.santander.nl, 78.31.116.203, A)

(santander.nl, cluster2.eu.messagelabs.com, MX)

(cluster2.eu.messagelabs.com, 195.245.230.131, A)

Pregunta 3. Si el servidor autoritativo de la empresa Widexs ya estaba en el servidor TLD de .nl, ¿hace falta que Widexs facilite alguna información a dicho servidor TLD para que los servicios del banco sean operativos?

Respuesta:

Es necesario decirle al TLD de .nl que Santander.nl está alojado en el servidor autoritativo de widexs.nl, por lo que hace falta un registro NS:

(santander.nl, ns1.widexs.nl, NS)

Nota: También hace falta un registro A para ns1.widexs.nl, pero, al tratarse de una empresa de hosting holandesa ya existente, se entiende que ya estaba en el servidor TLD de .nl.

Pregunta 4. Inmediatamente después de la conexión web, el mismo PC del apartado 1 accede al servidor FTP de la empresa Nluug (asociación holandesa para estándares y sistemas abiertos). Dicho servidor, de nombre ftp.nluug.nl, está ubicado en la dirección 145.220.21.40. El servidor DNS autoritativo de la empresa Nluug es ns1.nluug.nl (con dirección 46.19.34.198). ¿Cuál es el nombre y la IP del servidor DNS al que el servidor DNS local hace la primera petición DNS? Razone su respuesta.

Respuesta:

ns1.dns.nl, 193.176.144.5

Dado que ya conocemos donde está el TLD correspondiente a .nl, no hace falta ir al servidor raíz, sino al servidor TLD de .nl.

Pregunta 5. Indique los dominios que conoce el servidor onix.us.es después de las conexiones web y FTP, y el tipo de cada uno de ellos.

Respuesta:

Conoce todos los dominios correspondientes a los servidores que se han consultado

TLD: .net, .nl

Autoritativos: root-servers.net, dns.nl, widexs.nl, santander.nl, nluug.nl

Evidentemente, también tiene que conocer el dominio raíz

Nota: En el enunciado se pregunta por los dominios, no por los servidores.

Parte 2

Pregunta 1. Se dispone de una captura de Wireshark que muestra parte del diálogo FTP establecido entre cliente y servidor. Dicho diálogo se muestra en la Figura 2.

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|-----------|---------------|---------------|----------|--------|-----------------------------------------------------------------------------------------------|
| 60 | 19.103432 | 192.168.1.131 | 145.220.21.40 | FTP | 70 | Request: USER anonymous |
| 61 | 19.172449 | 145.220.21.40 | 192.168.1.131 | FTP | 88 | Response: 331 Please specify the password. |
| 62 | 19.209653 | 192.168.1.131 | 145.220.21.40 | TCP | 54 | 50021 → 21 [ACK] Seq=31 Ack=602 Win=7591 Len=0 |
| 65 | 21.588469 | 192.168.1.131 | 145.220.21.40 | FTP | 61 | Request: PASS |
| 66 | 21.663874 | 145.220.21.40 | 192.168.1.131 | FTP | 77 | Response: 230 Login successful. |
| 67 | 21.709343 | 192.168.1.131 | 145.220.21.40 | TCP | 54 | 50021 → 21 [ACK] Seq=38 Ack=625 Win=7568 Len=0 |
| 373 | 45.009691 | 192.168.1.131 | 145.220.21.40 | FTP | 69 | Request: CWD vol/2/rfc |
| 375 | 45.078167 | 145.220.21.40 | 192.168.1.131 | FTP | 91 | Response: 250 Directory successfully changed. |
| 377 | 45.115084 | 192.168.1.131 | 145.220.21.40 | TCP | 54 | 50021 → 21 [ACK] Seq=53 Ack=662 Win=7531 Len=0 |
| 461 | 61.492812 | 192.168.1.131 | 145.220.21.40 | FTP | 82 | Request: PORT 192,168,1,131,195,108 |
| 462 | 61.561391 | 145.220.21.40 | 192.168.1.131 | FTP | 105 | Response: 200 PORT command successful. Consider using PASV. |
| 463 | 61.568336 | 192.168.1.131 | 145.220.21.40 | FTP | 70 | Request: RETR rfc99.txt |
| 464 | 61.635568 | 145.220.21.40 | 192.168.1.131 | TCP | 74 | 20 → 50028 [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM=1 TSval=3365526421 TSecr=0 WS=256 |
| 465 | 61.635771 | 192.168.1.131 | 145.220.21.40 | TCP | 74 | 50028 → 20 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1 TSval=1161813846 |
| 466 | 61.677199 | 145.220.21.40 | 192.168.1.131 | TCP | 54 | 21 → 50021 [ACK] Seq=713 Ack=97 Win=14848 Len=0 |
| 467 | 61.699876 | 145.220.21.40 | 192.168.1.131 | TCP | 66 | 20 → 50028 [ACK] Seq=1 Ack=1 Win=14848 Len=0 TSval=3365526485 TSecr=1161813846 |
| 468 | 61.700877 | 145.220.21.40 | 192.168.1.131 | FTP-DA | 1076 | FTP Data: 1010 bytes |
| 469 | 61.700878 | 145.220.21.40 | 192.168.1.131 | TCP | 66 | 20 → 50028 [FIN, ACK] Seq=1011 Ack=1 Win=14848 Len=0 TSval=3365526485 TSecr=1161813846 |
| 470 | 61.700975 | 192.168.1.131 | 145.220.21.40 | TCP | 66 | 50028 → 20 [ACK] Seq=1 Ack=1012 Win=17152 Len=0 TSval=1161813911 TSecr=3365526485 |
| 471 | 61.701613 | 145.220.21.40 | 192.168.1.131 | FTP | 123 | Response: 150 Opening BINARY mode data connection for rfc99.txt (1010 bytes). |
| 472 | 61.714670 | 192.168.1.131 | 145.220.21.40 | TCP | 66 | 50028 → 20 [FIN, ACK] Seq=1 Ack=1012 Win=17152 Len=0 TSval=1161813912 TSecr=3365526485 |
| 473 | 61.748516 | 192.168.1.131 | 145.220.21.40 | TCP | 54 | 50021 → 21 [ACK] Seq=97 Ack=782 Win=7411 Len=0 |

> Frame 463: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface 0
> Ethernet II, Src: HonHaiPr_73:b3:9b (44:1c:a0:73:b3:9b), Dst: ZteCorpo_c4:7d:66 (44:f4:36:c4:7d:66)
> Internet Protocol Version 4, Src: 192.168.1.131, Dst: 145.220.21.40
▼ Transmission Control Protocol, Src Port: 50021 (50021), Dst Port: 21 (21), Seq: 81, Ack: 713, Len: 16
Source Port: 50021

0000 44 f4 36 c4 7d 66 44 1c a8 73 b3 9b 08 00 45 00 D.6.}fD. .s....E.
0010 00 38 63 25 40 00 08 06 2e 6b c0 a8 01 83 91 dc .8c%... .k.....
0020 15 28 c3 65 00 15 1d 88 97 6f 92 1a 86 cd 50 18 .(e.... .o....P.
0030 1d 38 7d 61 00 00 52 45 54 52 20 72 66 63 39 39 .8)a..RE TR rfc99
0040 2e 74 78 74 0d 0a .txt..

¿Qué comandos ha ejecutado el cliente durante el diálogo? (Incluya los argumentos de los comandos)

Respuesta:

USER anonymous

PASS

CWD vol/2/rfc

PORT 192,168,1,131,195,108

RETR rfc99.txt

Pregunta 2. ¿Cuántas conexiones TCP se han establecido durante el diálogo (como mínimo)?

Razone su respuesta. (0.5 ptos).

Respuesta:

Deberá abrir un mínimo de dos conexiones:

- Una conexión de control (puerto 21) para los comandos y respuestas.
- Una conexión de datos (puerto 20), para descargar el archivo

Pregunta 3. Si en vez de haberse conectado a un servidor FTP, lo hubiese hecho a un servidor TFTP, ¿Qué acciones podría haber realizado y cuáles no?

Respuesta:

No puede:

- Establecer conexiones TCP
- Fijar login/password (autenticación)
- Establecer una estructura de directorios y moverse por ellos

Sí puede:

- Descargar el archivo

Pregunta 4. Indique cuántos mensajes y de que tipo se hubieran intercambiado entre cliente y servidor de haberse descargado el archivo utilizando TFTP.

Respuesta:

El archivo tiene 1010 bytes, por lo que harán falta un bloque de datos 512 bytes y otro de 498 bytes para enviarlo por TFTP. Para descargar el archivo se mandan 1 RRQ y 2 ACK (cliente) y 2 DATA (servidor). 5 mensajes TFTP en total.