

PRACTICA INTEGRADORA 1ª EVALUACIÓN

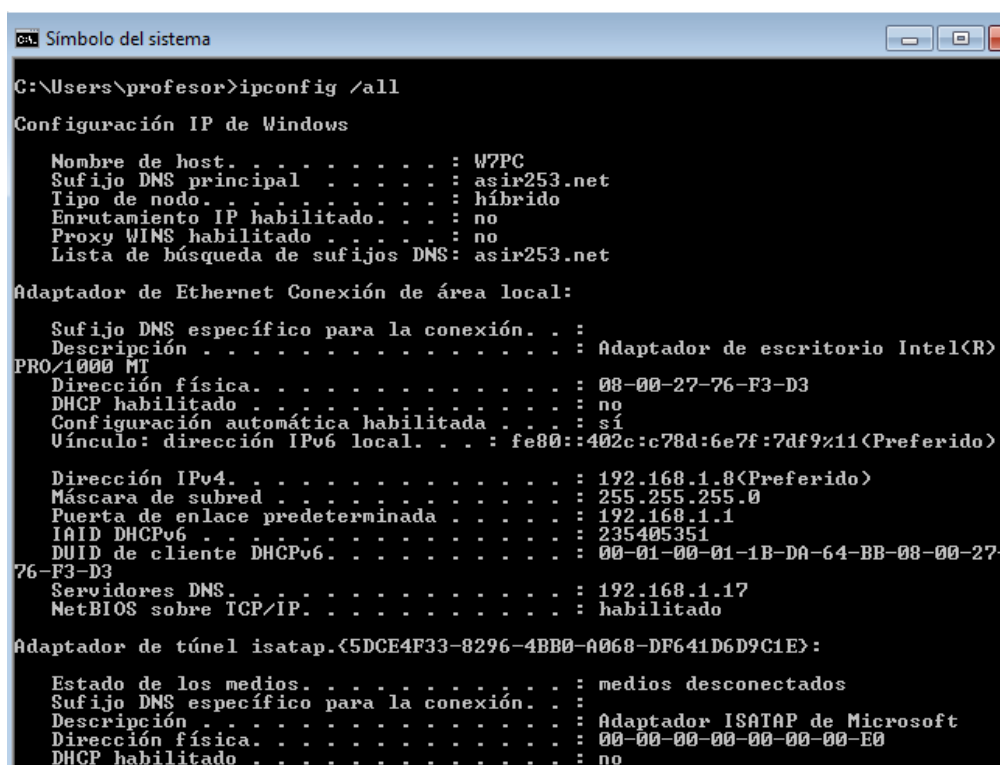
Se trata de realizar capturas mediante wireshark del funcionamiento de los dos servicios instalados FTP y DNS tanto en windows como en Linux.

PRIMERA PARTE

Teniendo el servidor de Ubuntu corriendo se iniciará el FTP instalado en la unidad 3 y se realizará una captura en la que se puedan observar todos los protocolos que intervienen:

Paso 1: Previamente desde el servidor de Ubuntu (en el ejemplo 192.168.1.17) en clase 10.12.1.xx se creará en el directorio correspondiente al usuario anónimo un fichero por ejemplo, ej

Paso 2: Comprobar que se ha configurado correctamente el cliente de windows (en el ejemplo 192.168.1.8) en clase 10.12.4.xx para que le atienda el servidor DNS de ubuntu server y que tenga como sufijo de red el de la zona para la que es autorizado el servidor de ubuntu, es decir, asirxx.net



```
C:\Users\profesor>ipconfig /all

Configuración IP de Windows

Nombre de host. . . . . : W7PC
Sufijo DNS principal . . . . : asir253.net
Tipo de nodo. . . . . : híbrido
Enrutamiento IP habilitado. . . : no
Proxy WINS habilitado . . . . : no
Lista de búsqueda de sufijos DNS: asir253.net

Adaptador de Ethernet Conexión de área local:

Sufijo DNS específico para la conexión. . : 
Descripción . . . . . : Adaptador de escritorio Intel(R)
PRO/1000 MT
Dirección física. . . . . : 08-00-27-76-F3-D3
DHCP habilitado . . . . . : no
Configuración automática habilitada . . : sí
Vínculo: dirección IPv6 local. . . : fe80::402c:c78d:6e7f:7df9%11<Preferido>

Dirección IPv4. . . . . : 192.168.1.8<Preferido>
Máscara de subred . . . . . : 255.255.255.0
Puerta de enlace predeterminada . . . . : 192.168.1.1
IAID DHCPv6 . . . . . : 235405351
DUID de cliente DHCPv6. . . . . : 00-01-00-01-1B-DA-64-BB-08-00-27-
76-F3-D3
Servidores DNS. . . . . : 192.168.1.17
NetBIOS sobre TCP/IP. . . . . : habilitado

Adaptador de túnel isatap.{5DCE4F33-8296-4BB0-A068-DF641D6D9C1E}:

Estado de los medios. . . . . : medios desconectados
Sufijo DNS específico para la conexión. . : 
Descripción . . . . . : Adaptador ISATAP de Microsoft
Dirección física. . . . . : 00-00-00-00-00-00-00-E0
DHCP habilitado . . . . . : no
```

Paso 3: Eliminar la caché ARP:

Paso 4: Eliminar la caché DNS:

Paso 5: Arrancar wireshark:

Paso 6: Realizar una petición FTP desde el cliente de windows configurado utilizando el nombre del equipo de ubuntuServer. Ver imagen

```
C:\Users\profesor>ftp ubuntuServer253
Conectado a ubuntuServer253.asir253.net.
220 (vsFTPd 3.0.3)
Usuario (ubuntuServer253.asir253.net:(none)): anonymous
331 Please specify the password.
Contraseña:
230 Login successful.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
a
b
ej
ftpW
226 Directory send OK.
ftp: 16 bytes recibidos en 0,00segundos 16000,00a KB/s.
ftp> get ej
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for ej (27 bytes).
226 Transfer complete.
ftp: 27 bytes recibidos en 0,00segundos 27000,00a KB/s.
ftp> !dir
El volumen de la unidad C no tiene etiqueta.
El número de serie del volumen es: 4CB1-4328

Directorio de C:\Users\profesor
26/11/2019  18:41    <DIR>          .
26/11/2019  18:41    <DIR>          ..
23/10/2014  08:37    <DIR>          Contacts
05/11/2019  19:22    <DIR>          Desktop
05/11/2019  21:29    <DIR>          Documents
05/11/2019  19:42    <DIR>          Downloads
26/11/2019  18:41         27 ej
```

Paso 7: Entrar con el usuario anónimo, pedir un listado del servidor, descargar el fichero ej y salir de FTP

Paso 8: Parar la captura. Guardar el fichero creado.

Paso 9: Explicación de los protocolos que han intervenido. Obtener los pantallazos correspondientes al protocolo ARP, saludo de tres vías, transferencia del fichero, quit ...

Para facilitar la búsqueda, utilizar los siguientes filtros en wireshark:

```
arp
tcp.port==21
tcp.port==20
```

Paso 10:

- ¿Cuál es el puerto de control del cliente?
- ¿Cuál es el puerto de control del servidor?
- ¿Cuántos saludos de tres vías has observado?

SEGUNDA PARTE

Teniendo el servidor de Windows 2008 corriendo se iniciará el FTP instalado en la unidad 3 y se realizará una captura en la que se puedan observar todos los protocolos que intervienen siguiendo los pasos anteriores.

TERCERA PARTE:

Captura con el wireshark una petición a madrid.org guárdala en un fichero y muestra los pantallazos correspondientes para contestar las siguientes preguntas:

- a) ¿Qué método de solicitud HTTP se ha utilizado?
- b) ¿Qué formato tiene el mensaje de petición HTTP?
- c) ¿Qué formato tiene el mensaje de respuesta HTTP? Explica qué tipo de respuesta se ha producido.
- d) Enumera los encabezados típicos de la petición.
- e) Enumera los encabezados típicos de la respuesta

NOTA: Para eliminar la caché DNS en UBUNTU:

```
$sudo systemd-resolve --flush-caches
```

Comprobar que se ha borrado:

```
$sudo systemd-resolve --statistics
```