

Práctica 2

Aspectos teóricos previos

¿Qué usuarios se pueden conectar al servicio FTP de nuestra máquina?

- En el fichero `/etc/ftpusers` se encuentra una lista de usuarios que NO se pueden conectar al servicio.
- El fichero contiene usualmente una lista de los usuarios que o bien no realizan ninguna actividad mediante ftp o bien que tienen demasiados privilegios para que se les permita el ingreso a través del demonio servidor de FTP
- Revisar la lista de usuarios
- ¿Por qué está en esta lista el usuario root?

Porque el usuario `root` tiene demasiados privilegios.

Directiva	Valor por defecto	Utilidad	Ejemplo de uso
<code>userlist_file</code>	<code>/etc/vsftpd.user_list</code>	Define el nombre del archivo que se carga cuando la opción <code>userlist_enable</code> está activada.	<code>userlist_file=/etc/vsftpd.user_list</code>
<code>userlist_enable</code>	NO	Si se activa, vsftpd carga una lista de nombres de usuario desde el archivo definido en <code>userlist_file</code> . Los usuarios en la lista son rechazados antes de pedirles la contraseña, evitando el envío de credenciales en texto plano (por ejemplo al usuario root)	<code>userlist_enable=YES</code>

userlist_deny	YES	Determina el comportamiento de la lista si userlist_enable está activo. Si se establece en NO, solo se permite el acceso a los usuarios listados; si está en YES, se deniega el acceso a los usuarios listados.	userlist_deny=NO
---------------	-----	---	------------------

Además de este archivo (/etc/ftpusers), existen otros modos de configuración sobre usuarios a los que se permite o niega el acceso al servicio, entre ellos está la lista de usuarios (user_list): Para entender mejor cómo interactúan estas directivas, imagina que el archivo userlist_file es una lista de invitados en la puerta de un club: si userlist_deny es YES, la lista es de personas "vetadas" a las que no se deja pasar; pero si userlist_deny es NO, la lista se convierte en una "lista VIP", donde solo los que están anotados pueden entrar.

Desarrollo de la práctica

1. Instala una nueva instancia del servidor 'vsftpd', pero en este caso en el servidor BOOKWORMXXA. Todas las pruebas sobre el servicio FTP las tienes que realizar conectándote desde el cliente LinuxXX
2. Modifica el registro DNS en tu servidor de modo que resuelva el nombre "ftp.asirXX.asir" por la IP 10.0.128+XX.1. Comprueba desde el cliente que se resuelve de manera correcta el nombre por la IP.

```

bookworm11b_FTP [Corriendo] - Oracle VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
alumno@bookworm11b: ~
Archivo  Editar  Pestañas  Ayuda
GNU nano 7.2 /etc/bind/asir11.asir.hosts
; $origin delega do asir11.asir11.asir.
; @      IN      NS      servidor.asir11.asir.
; ASIR WEB P1
bookworm11a      IN      A      10.0.139.1
virtual1.asir11.asir.  IN      CNAME   bookworm11a.asir11.asir.
; ASIR WEB CONTROL
control.asir11.asir.  IN      CNAME   bookworm11a.asir11.asir.
ftp              IN      CNAME   bookworm11a

```

```
Linux11DHCP [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
linux11@linux11-virtualbox: ~
Archivo Acciones Editar Vista Ayuda
linux11@linux11-virtualbox: ~ x
linux11@linux11-virtualbox:~$ dig ftp.asir11.asir

; <<>> DiG 9.18.39-0ubuntu0.24.04.1-Ubuntu <<>> ftp.asir11.asir
;; global options: +cmd
;; Got answer:
;; ->HEADER<<- opcode: QUERY, status: NOERROR, id: 64037
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: ea3951bd0a04e96601000000695f7c7169789043623331b4 (good)
;; QUESTION SECTION:
;ftp.asir11.asir.                IN      A

;; ANSWER SECTION:
ftp.asir11.asir.                3600    IN      CNAME   bookworm11a.asir11.asir.
bookworm11a.asir11.asir. 3600    IN      A       10.0.139.1

;; Query time: 2 msec
;; SERVER: 10.0.139.2#53(10.0.139.2) (UDP)
;; WHEN: Thu Jan 08 10:44:16 CET 2026
;; MSG SIZE rcvd: 114
```

3. Crea un usuario local en el servidor BOOKWORMXXA denominado "cliente1" con contraseña "123456" y perteneciente al grupo www-data. Su directorio en la máquina ha de ser /var/www/virtual1 (si este directorio no tiene todavía la propiedad y grupo asociado a www-data, modifícalo, para que la tenga). Recuerda que éste es el directorio "DocumentRoot" del sitio virtual: "virtual1.asirXX.asir"
 - #useradd -g www-data -d /var/www/virtual1 -c "Cliente 1" cliente1
 - #passwd cliente1

```
BookWorm11A-FTP [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
alumno@bookworm11a: ~
Archivo Editar Pestañas Ayuda
alumno@bookworm11a:~$ sudo useradd -g www-data -d /var/www/virtual1 -c "Cliente 1" cliente1
alumno@bookworm11a:~$ passwd cliente1
passwd: no debe ver o cambiar la información de la contraseña para cliente1.
alumno@bookworm11a:~$ sudo passwd cliente1
Nueva contraseña:
Vuelva a escribir la nueva contraseña:
passwd: contraseña actualizada correctamente
alumno@bookworm11a:~$
```

4. Pon a capturar wireshark y conéctate al servicio FTP desde el cliente LinuxXX usando el nombre DNS (ftp ftp.asirXX.asir) y prueba que te

puedes conectar con el usuario creado (cliente1) y que accede al directorio que se le ha configurado.

Bookworm11A-FTP [Corriendo] - Oracle VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

any

Archivo Edición Visualización Ir Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayuda

ftp

No.	Time	Source	Destination	Protocol	Length	Info
5	1.079024882	10.0.139.1	10.0.139.4	FTP	88	Response: 220 (vsFTPd 3.0.3)
7	3.980319124	10.0.139.4	10.0.139.1	FTP	83	Request: USER cliente1
9	3.980533105	10.0.139.1	10.0.139.4	FTP	102	Response: 331 Please specify the password.
11	6.551157855	10.0.139.4	10.0.139.1	FTP	81	Request: PASS 123456
13	6.618130319	10.0.139.1	10.0.139.4	FTP	91	Response: 230 Login successful.
15	6.618943772	10.0.139.4	10.0.139.1	FTP	74	Request: SYST
17	6.619129295	10.0.139.1	10.0.139.4	FTP	87	Response: 215 UNIX Type: L8
18	6.619670831	10.0.139.4	10.0.139.1	FTP	74	Request: FEAT
19	6.619774304	10.0.139.1	10.0.139.4	FTP	83	Response: 211-Features:
20	6.619819418	10.0.139.1	10.0.139.4	FTP	89	Response: EPRT
21	6.619977653	10.0.139.1	10.0.139.4	FTP	75	Response: PASV
22	6.620011801	10.0.139.1	10.0.139.4	FTP	82	Response: REST STREAM
24	6.620123444	10.0.139.1	10.0.139.4	FTP	75	Response: SIZE
25	6.620162072	10.0.139.1	10.0.139.4	FTP	84	Response: TVFS

Frame 5: 88 bytes on wire (704 bits), 88 bytes captured (704 bits) on interface
Linux cooked capture v1
Internet Protocol Version 4, Src: 10.0.139.1, Dst: 10.0.139.4
Transmission Control Protocol, Src Port: 21, Dst Port: 39134, Seq: 1, Ack: 39134
File Transfer Protocol (FTP)
[Current working directory:]

0000 00 04 00 01 00 06 08 00 27 ad bc be 00
0010 45 00 00 48 4c 7c 40 00 40 06 c4 2e 0a
0020 0a 00 8b 04 00 15 98 de e4 df af f5 7e
0030 80 18 01 fe 2a 40 00 00 01 01 08 0a 4c
0040 63 0b b8 d3 32 32 30 20 28 76 73 46 54
0050 33 2e 30 2e 33 29 0d 0a

Linux11DHCP [Corriendo] - Oracle VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

linux11@linux11-virtualbox: ~

Archivo Acciones Editar Vista Ayuda

```
linux11@linux11-virtualbox: ~  
linux11@linux11-virtualbox:~$ ftp ftp.asir11.asir  
Connected to bookworm11a.asir11.asir.  
220 (vsFTPd 3.0.3)  
Name (ftp.asir11.asir:linux11): cliente1  
331 Please specify the password.  
Password:  
230 Login successful.  
Remote system type is UNIX.  
Using binary mode to transfer files.  
ftp>
```

```

Linux11DHCP [Corriendo] - Oracle VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda

linux11@linux11-virtualbox: ~

Archivo  Acciones  Editar  Vista  Ayuda

linux11@linux11-virtualbox: ~ x

ftp> ls
229 Entering Extended Passive Mode (|||22358|)
150 Here comes the directory listing.
drwxr-xr-x  2 0      0      4096 Nov 27 10:05 digest
drwxr-xr-x  2 0      0      4096 Nov 26 20:03 errors
-rw-r--r--  1 0      0      370  Nov 27 10:12 index.php
drwxr-xr-x  2 0      0      4096 Dec 04 10:29 permitido
drwxr-xr-x  2 0      0      4096 Nov 26 19:08 restringido
drwxr-xr-x  2 0      0      4096 Dec 02 09:09 usuarios
226 Directory send OK.
ftp> pwd
Remote directory: /var/www/virtual1

```

5. Comprueba en la captura de wireshark los puertos del lado del servidor y del cliente que se están utilizando hasta este momento.

BookWorm11A-FTP [Corriendo] - Oracle VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

any

Archivo Edición Visualización Ir Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayuda

ftp

No.	Time	Source	Destination	Protocol	Length	Info
5	1.079024882	10.0.139.1	10.0.139.4	FTP	88	Response: 220 (vsFTPd 3.0.3)
7	3.980319124	10.0.139.4	10.0.139.1	FTP	83	Request: USER cliente1
9	3.980533105	10.0.139.1	10.0.139.4	FTP	102	Response: 331 Please specify the password.
11	6.551157855	10.0.139.4	10.0.139.1	FTP	81	Request: PASS 123456
13	6.618130319	10.0.139.1	10.0.139.4	FTP	91	Response: 230 Login successful.
15	6.618943772	10.0.139.4	10.0.139.1	FTP	74	Request: SYST
17	6.619129295	10.0.139.1	10.0.139.4	FTP	87	Response: 215 UNIX Type: L8
18	6.619670831	10.0.139.4	10.0.139.1	FTP	74	Request: FEAT
19	6.619774304	10.0.139.1	10.0.139.4	FTP	83	Response: 211-Features:
20	6.619819418	10.0.139.1	10.0.139.4	FTP	89	Response: EPRT
21	6.619977653	10.0.139.1	10.0.139.4	FTP	75	Response: PASV
22	6.620011801	10.0.139.1	10.0.139.4	FTP	82	Response: REST STREAM
24	6.620123444	10.0.139.1	10.0.139.4	FTP	75	Response: SIZE
25	6.620162072	10.0.139.1	10.0.139.4	FTP	84	Response: TVFS

Frame 5: 88 bytes on wire (704 bits), 88 bytes captured (704 bits) on interface any, id 0

Linux cooked capture v1

Internet Protocol Version 4, Src: 10.0.139.1, Dst: 10.0.139.4

Transmission Control Protocol, Src Port: 21, Dst Port: 39134, Seq: 1, Ack: 1, Len: 20

Source Port: 21

Destination Port: 39134

[Stream index: 0]

[Conversation completeness: Complete, WITH_DATA (63)]

[TCP Segment Len: 20]

0000 00 04 00 01 00 06 08 0
0010 45 00 00 48 4c 7c 40 0
0020 0a 00 8b 04 00 15 98 d
0030 80 18 01 fe 2a 40 00 0
0040 63 0b b8 d3 32 32 30 2
0050 33 2e 30 2e 33 29 0d 0

BookWorm11A-FTP [Corriendo] - Oracle VirtualBox						
Archivo Máquina Ver Entrada Dispositivos Ayuda						
any						
Archivo Edición Visualización Ir Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayuda						
ftp						
No.	Time	Source	Destination	Protocol	Length	Info
5	1.079024882	10.0.139.1	10.0.139.4	FTP	88	Response: 220 (vsFTPd 3.0.3)
7	3.980319124	10.0.139.4	10.0.139.1	FTP	83	Request: USER cliente1
9	3.980533105	10.0.139.1	10.0.139.4	FTP	102	Response: 331 Please specify the password.
11	6.551157855	10.0.139.4	10.0.139.1	FTP	81	Request: PASS 123456
13	6.618130319	10.0.139.1	10.0.139.4	FTP	91	Response: 230 Login successful.
15	6.618943772	10.0.139.4	10.0.139.1	FTP	74	Request: SYST
17	6.619129295	10.0.139.1	10.0.139.4	FTP	87	Response: 215 UNIX Type: L8
18	6.619670831	10.0.139.4	10.0.139.1	FTP	74	Request: FEAT
19	6.619774304	10.0.139.1	10.0.139.4	FTP	83	Response: 211-Features:
20	6.619819418	10.0.139.1	10.0.139.4	FTP	89	Response: EPRT
21	6.619977653	10.0.139.1	10.0.139.4	FTP	75	Response: PASV
22	6.620011801	10.0.139.1	10.0.139.4	FTP	82	Response: REST STREAM
24	6.620123444	10.0.139.1	10.0.139.4	FTP	75	Response: SIZE
25	6.620162072	10.0.139.1	10.0.139.4	FTP	84	Response: TVFS

▶ Frame 7: 83 bytes on wire (664 bits), 83 bytes captured (664 bits) on interface any, id 0
 ▶ Linux cooked capture v1
 ▶ Internet Protocol Version 4, Src: 10.0.139.4, Dst: 10.0.139.1
 ▼ Transmission Control Protocol, Src Port: 39134, Dst Port: 21, Seq: 1, Ack: 21, Len: 15
 Source Port: 39134
 Destination Port: 21
 [Stream index: 0]

0000	00 00 00 01 0
0010	45 10 00 43 b
0020	0a 00 8b 01 9
0030	80 18 7e e0 3
0040	4c 3f b7 18 5
0050	31 0d 0a

- Comprueba que alguno de los usuarios incluidos en el archivo ftpusers no puede acceder al servicio ftp, se les niega el acceso, pero se le solicita que introduzca la contraseña que podría ser vista.

```

Linux11DHCP [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
linux11@linux11-virtualbox: ~
Archivo Acciones Editar Vista Ayuda
linux11@linux11-virtualbox: ~ x
linux11@linux11-virtualbox:~$ ftp ftp.asir11.asir
Connected to bookworm11a.asir11.asir.
220 (vsFTPd 3.0.3)
Name (ftp.asir11.asir:linux11): root
331 Please specify the password.
Password:
530 Login incorrect.
ftp: Login failed
ftp>

```

- Considerando los aspectos teóricos vistos en esta práctica configura el servicio para que el usuario "cliente1" sea el único usuario local que puede conectarse al servicio (el tuyo, alumno, no debería poder). Haz las pruebas de conexión correspondientes y haz las capturas de wireshark que consideres necesarias tanto cuando se conecta "cliente1" como cuando se intenta conectar cualquier otro usuario. ¿Se solicitan las contraseñas?

```
BookWorm11A-FTP [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
alumno@bookworm11a: ~
GNU nano 7.2 /etc/vsftpd.conf
# Example config file /etc/vsftpd.conf
#
# The default compiled in settings are fairly paranoid. This sample file
# loosens things up a bit, to make the ftp daemon more usable.
# Please see vsftpd.conf.5 for all compiled in defaults.
#
# READ THIS: This example file is NOT an exhaustive list of vsftpd options.
# Please read the vsftpd.conf.5 manual page to get a full idea of vsftpd's
# capabilities.
userlist_enable=YES
userlist_deny=NO
userlist_file=/etc/vsftpd.user_list
#
```

```
BookWorm11A-FTP [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
alumno@bookworm11a: ~
GNU nano 7.2 /etc/vsftpd.user_list
cliente1
|
```

COMPROBACIONES CON CLIENTE1 Y ALUMNO:

```

Linux11DHCP [Corriendo] - Oracle VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda

linux11@linux11-virtualbox: ~

linux11@linux11-virtualbox: ~$ ftp ftp.asir11.asir
Connected to bookworm11a.asir11.asir.
220 (vsFTPd 3.0.3)
Name (ftp.asir11.asir:linux11): cliente1
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> exit
221 Goodbye.
linux11@linux11-virtualbox:~$ ftp ftp.asir11.asir
Connected to bookworm11a.asir11.asir.
220 (vsFTPd 3.0.3)
Name (ftp.asir11.asir:linux11): alumno
530 Permission denied.
ftp: Login failed
ftp> exit
221 Goodbye.
linux11@linux11-virtualbox:~$

```

BookWorm11A-FTP [Corriendo] - Oracle VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

any

Archivo Edición Visualización Ir Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayuda

ftp

No.	Time	Source	Destination	Protocol	Length Info
1	0.000000000	10.0.139.4	10.0.139.1	FTP	74 Request: QUIT
3	0.000288975	10.0.139.1	10.0.139.4	FTP	82 Response: 221 Goodbye.
11	2.257879736	10.0.139.1	10.0.139.4	FTP	88 Response: 220 (vsFTPd 3.0.3)
13	7.900256330	10.0.139.4	10.0.139.1	FTP	83 Request: USER cliente1
15	7.900542291	10.0.139.1	10.0.139.4	FTP	102 Response: 331 Please specify the password.
17	10.302005986	10.0.139.4	10.0.139.1	FTP	81 Request: PASS 123456
19	10.370770246	10.0.139.1	10.0.139.4	FTP	91 Response: 230 Login successful.
21	10.371687424	10.0.139.4	10.0.139.1	FTP	74 Request: SYST
23	10.371862474	10.0.139.1	10.0.139.4	FTP	87 Response: 215 UNIX Type: L8
24	10.372345245	10.0.139.4	10.0.139.1	FTP	74 Request: FEAT
25	10.372408998	10.0.139.1	10.0.139.4	FTP	83 Response: 211-Features:
26	10.372523655	10.0.139.1	10.0.139.4	FTP	89 Response: EPRT
27	10.372614640	10.0.139.1	10.0.139.4	FTP	89 Response: PASV
28	10.372649241	10.0.139.1	10.0.139.4	FTP	91 Response: SIZE
31	15.119298332	10.0.139.4	10.0.139.1	FTP	74 Request: QUIT
32	15.119448341	10.0.139.1	10.0.139.4	FTP	82 Response: 221 Goodbye.
39	17.318130652	10.0.139.1	10.0.139.4	FTP	88 Response: 220 (vsFTPd 3.0.3)
43	22.668321054	10.0.139.4	10.0.139.1	FTP	81 Request: USER alumno
47	23.668822067	10.0.139.1	10.0.139.4	FTP	92 Response: 530 Permission denied.
49	28.822394890	10.0.139.4	10.0.139.1	FTP	74 Request: QUIT
51	28.822714470	10.0.139.1	10.0.139.4	FTP	82 Response: 221 Goodbye.

Frame 43: 81 bytes on wire (648 bits), 81 bytes captured (648 bits) on interface any, id 0

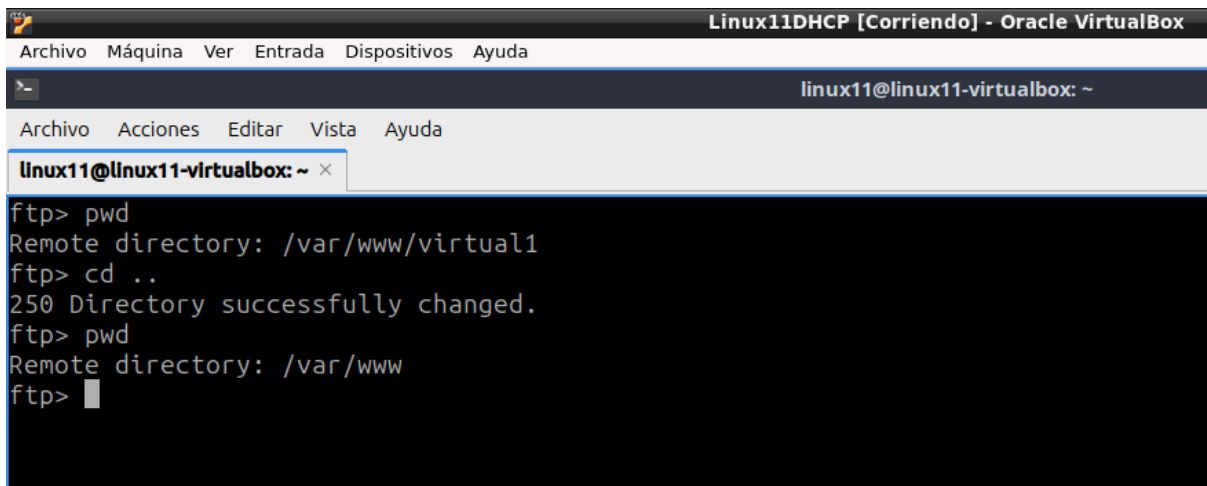
- Linux cooked capture v1
- Internet Protocol Version 4, Src: 10.0.139.4, Dst: 10.0.139.1
- Transmission Control Protocol, Src Port: 60384, Dst Port: 21, Seq: 1, Ack: 21, Len: 13
- File Transfer Protocol (FTP)
 - [Current working directory:]

```

0000  00 00 00
0010  45 10 00
0020  0a 00 8b
0030  80 18 7e
0040  4c 4f 0b
0050  0a

```

8. ¿Puede dicho usuario una vez conectado navegar a directorios distintos del suyo? Por ejemplo /var/www.

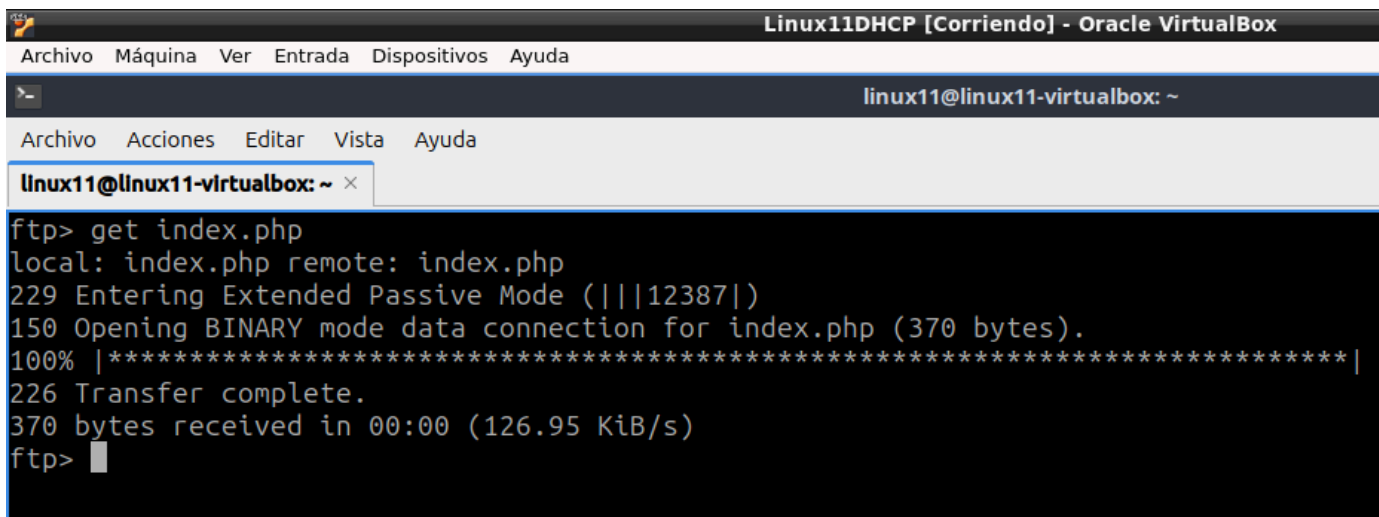


```
Linux11DHCP [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
linux11@linux11-virtualbox: ~
Archivo Acciones Editar Vista Ayuda
linux11@linux11-virtualbox: ~ x
ftp> pwd
Remote directory: /var/www/virtual1
ftp> cd ..
250 Directory successfully changed.
ftp> pwd
Remote directory: /var/www
ftp> █
```

Por defecto en **vsftpd**, **SÍ** puede salir y pasearse por **/var** o **/etc**.

Solución: Descomentar **chroot_local_user=YES** en la config para enjaularlo.

9. Pon a capturar wireshark y prueba a realizar por FTP una descarga de un archivo contenido en **/var/www/virtual1** usando el comando **get**. ¿qué puertos del lado del cliente y del servidor se han involucrado en la descarga de los datos del fichero?



```
Linux11DHCP [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
linux11@linux11-virtualbox: ~
Archivo Acciones Editar Vista Ayuda
linux11@linux11-virtualbox: ~ x
ftp> get index.php
local: index.php remote: index.php
229 Entering Extended Passive Mode (|||12387|)
150 Opening BINARY mode data connection for index.php (370 bytes).
100% |*****|
226 Transfer complete.
370 bytes received in 00:00 (126.95 KiB/s)
ftp> █
```

BookWorm11A-FTP [Corriendo] - Oracle VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

any

Archivo Edición Visualización Ir Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayuda

ftp

No.	Time	Source	Destination	Protocol	Length Info
199	340.297544862	10.0.139.1	10.0.139.4	FTP	92 Response: 226 Directory send OK.
205	347.996562475	10.0.139.4	10.0.139.1	FTP	76 Request: TYPE I
206	347.996716608	10.0.139.1	10.0.139.4	FTP	99 Response: 200 Switching to Binary mode.
207	347.997262062	10.0.139.4	10.0.139.1	FTP	84 Request: SIZE index.php
208	347.997409006	10.0.139.1	10.0.139.4	FTP	77 Response: 213 370
209	347.997890401	10.0.139.4	10.0.139.1	FTP	74 Request: EPSV
210	347.998168766	10.0.139.1	10.0.139.4	FTP	116 Response: 229 Entering Extended Passive Mode (12387)
214	347.999439522	10.0.139.4	10.0.139.1	FTP	84 Request: RETR index.php
215	347.999846835	10.0.139.1	10.0.139.4	FTP	136 Response: 150 Opening BINARY mode data connection for index.php (370 bytes).
221	348.002859922	10.0.139.4	10.0.139.1	FTP	92 Response: 226 Transfer complete.
223	348.003498206	10.0.139.1	10.0.139.4	FTP	84 Request: MDTM index.php
224	348.003597261	10.0.139.4	10.0.139.1	FTP	88 Response: 213 20251127101234

Frame 207: 84 bytes on wire (672 bits), 84 bytes captured (672 bits) on interface any, id 0

Linux cooked capture v1

Internet Protocol Version 4, Src: 10.0.139.4, Dst: 10.0.139.1

Transmission Control Protocol, Src Port: 35532, Dst Port: 21, Seq: 129, Ack: 817, Len: 16

Source Port: 35532

Destination Port: 21

[Stream index: 3]

[Conversation completeness: Incomplete, DATA (15)]

[TCP Segment Len: 16]

0000 00 00 00 01 00 06 08 00 27 5e 44 e1 08 00
0010 45 10 00 44 76 c2 40 00 40 06 99 dc 0a 00
0020 0a 00 8b 01 8a cc 00 15 df 5e 49 84 66 50
0030 80 18 7e 96 f2 3a 00 00 01 01 08 0a 63 20
0040 4c 54 16 c8 53 49 5a 45 20 69 6e 64 65 70
0050 68 70 0d 0a

10. Crea una carpeta, sube un archivo y bórralo. ¿Es posible? Si no es posible modifica las directivas correspondientes para conseguirlo.

Linux11DHCP [Corriendo] - Oracle VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

linux11@linux11-virtualbox: ~

Archivo Acciones Editar Vista Ayuda

linux11@linux11-virtualbox: ~ × linux11@linux11-virtualbox: ~ ×

```
ftp> put prueba.txt
local: prueba.txt remote: prueba.txt
229 Entering Extended Passive Mode (|||54096|)
550 Permission denied.
ftp>
```

BookWorm11A-FTP [Corriendo] - Oracle VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

alumno@bookworm11a: ~

Archivo Editar Pestañas Ayuda

alumno@boo... × alumno@boo... ×

GNU nano 7.2 /etc/vsftpd.conf

```
#
# Uncomment this to enable any form of FTP write command.
write_enable=YES
#
# Default umask for local users is 077. You may wish to change this to 022
```

```

Linux11DHCP [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda

linux11@linux11-virtualbox: ~

linux11@linux11-virtualbox: ~ x

linux11@linux11-virtualbox:~$ ftp ftp.asir11.asir
Connected to bookworm11a.asir11.asir.
220 (vsFTPd 3.0.3)
Name (ftp.asir11.asir:linux11): cliente1
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> put prueba.txt
local: prueba.txt remote: prueba.txt
229 Entering Extended Passive Mode (|||23101|)
150 Ok to send data.
0 0.00 KiB/s
226 Transfer complete.
ftp>

```

BookWorm11A-FTP [Corriendo] - Oracle VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

any

Archivo Edición Visualización Jr Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayuda

ftp

No.	Time	Source	Destination	Protocol	Length	Info
1553	3834.0445535...	10.0.139.1	10.0.139.4	FTP	75	Response: PASV
1554	3834.0445827...	10.0.139.1	10.0.139.4	FTP	82	Response: REST STREAM
1555	3834.0446487...	10.0.139.1	10.0.139.4	FTP	75	Response: SIZE
1557	3834.0447189...	10.0.139.1	10.0.139.4	FTP	75	Response: TVFS
1558	3834.0447364...	10.0.139.1	10.0.139.4	FTP	77	Response: 211 End
1563	3839.1193088...	10.0.139.4	10.0.139.1	FTP	76	Request: TYPE I
1564	3839.1194196...	10.0.139.1	10.0.139.4	FTP	99	Response: 200 Switching to Binary mode.
1565	3839.1199065...	10.0.139.4	10.0.139.1	FTP	74	Request: EPSV
1566	3839.1200589...	10.0.139.1	10.0.139.4	FTP	116	Response: 229 Entering Extended Passive Mode (23101)
1570	3839.1206738...	10.0.139.4	10.0.139.1	FTP	85	Request: STOR prueba.txt
1571	3839.1209479...	10.0.139.1	10.0.139.4	FTP	90	Response: 150 Ok to send data.
1575	3839.1216592...	10.0.139.1	10.0.139.4	FTP	92	Response: 226 Transfer complete.

Frame 1570: 85 bytes on wire (680 bits), 85 bytes captured (680 bits) on interface any, id 0

- Linux cooked capture v1
- Internet Protocol Version 4, Src: 10.0.139.4, Dst: 10.0.139.1
- Transmission Control Protocol, Src Port: 35954, Dst Port: 21, Seq: 55, Ack: 256, Len: 17
 - Source Port: 35954
 - Destination Port: 21
 - [Stream index: 19]
 - [Conversation completeness: Incomplete, DATA (15)]
 - [TCP Segment Len: 17]
 - Sequence Number: 55 (relative sequence number)

0000 00 00 00 01 00 06 08 00 27 5e 44
 0010 45 10 00 45 c9 f6 40 00 40 06 46
 0020 0a 00 8b 01 8c 72 00 15 af bc 82
 0030 80 18 7e a8 d7 2b 00 00 01 01 08
 0040 4c 89 5b fb 53 54 4f 52 20 70 72
 0050 74 78 74 0d 0a

11. Cambia al modo activo (utilizando el comando `passive` se alterna entre los dos modos de funcionamiento) y repite el punto 10 revisando qué puertos se utilizan en este caso para la transferencia del archivo.

```
Linux11DHCP [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda

linux11@linux11-virtualbox: ~

Archivo Acciones Editar Vista Ayuda

linux11@linux11-virtualbox: ~ × linux11@linux11-virtualbox: ~ ×

ftp> passive
Passive mode: off; fallback to active mode: off.
ftp> put prueba_modooactivo.txt
local: prueba_modooactivo.txt remote: prueba_modooactivo.txt
200 EPRT command successful. Consider using EPSV.
150 Ok to send data.
0 0.00 KiB/s
226 Transfer complete.
ftp> █
```

Linux11DHCP [Corriendo] - Oracle VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

*enp0s8

Archivo Edición Visualización Ir Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayuda

tcp.port == 20

No.	Time	Source	Destination	Protocol	Length	Info
55	83.362803484	10.0.139.1	10.0.139.4	TCP	74	20 → 40301 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1284...
56	83.362830812	10.0.139.4	10.0.139.1	TCP	74	40301 → 20 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 SACK_PERM...
57	83.363027872	10.0.139.1	10.0.139.4	TCP	66	20 → 40301 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1284799430 TSecr=...
59	83.363627924	10.0.139.4	10.0.139.1	TCP	66	40301 → 20 [FIN, ACK] Seq=1 Ack=1 Win=130320 Len=0 TSval=1667267631 ...
60	83.363883395	10.0.139.1	10.0.139.4	TCP	66	20 → 40301 [FIN, ACK] Seq=1 Ack=2 Win=64256 Len=0 TSval=1284799431 T...
61	83.363896999	10.0.139.4	10.0.139.1	TCP	66	40301 → 20 [ACK] Seq=2 Ack=2 Win=130320 Len=0 TSval=1667267631 TSecr=...

Frame 61: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface enp0s8, id 0

Ethernet II, Src: PCSSystemtec_5e:44:e1 (08:00:27:5e:44:e1), Dst: PCSSystemtec_ad:bc:be (08:00:27:ad:bc:be)

Internet Protocol Version 4, Src: 10.0.139.4, Dst: 10.0.139.1

Transmission Control Protocol, Src Port: 40301, Dst Port: 20, Seq: 2, Ack: 2, Len: 0

Source Port: 40301

Destination Port: 20

[Stream index: 2]

[Conversation completeness: Complete, NO_DATA (23)]

0000 08 00 27 ad bc be 08 00 2
0010 00 34 8f a8 40 00 40 06 8
0020 8b 01 9d 6d 00 14 98 da f
0030 7f 44 2a 2c 00 00 01 01 0
0040 7b c7

BookWorm11A-FTP [Corriendo] - Oracle VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

*any

Archivo Edición Visualización Ir Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayuda

tcp.port == 20

No.	Time	Source	Destination	Protocol	Length	Info
1715	4179.1338429	10.0.139.1	10.0.139.4	TCP	76	20 → 33641 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1284410409 TSecr=0 WS...
1716	4179.1341129	10.0.139.4	10.0.139.1	TCP	76	33641 → 20 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 SACK_PERM TSval=1666878609 ...
1717	4179.1341431	10.0.139.1	10.0.139.4	TCP	68	20 → 33641 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1284410409 TSecr=1666878609
1719	4179.1343092	10.0.139.1	10.0.139.4	FTP_DATA	160	FTP Data (92 bytes)
1720	4179.1344208	10.0.139.1	10.0.139.4	TCP	68	20 → 33641 [FIN, ACK] Seq=93 Ack=1 Win=64256 Len=0 TSval=1284410410 TSecr=1666878609
1721	4179.1345092	10.0.139.4	10.0.139.1	TCP	68	33641 → 20 [ACK] Seq=1 Ack=93 Win=130228 Len=0 TSval=1666878610 TSecr=1284410410
1722	4179.1348472	10.0.139.4	10.0.139.1	TCP	68	33641 → 20 [FIN, ACK] Seq=1 Ack=94 Win=130228 Len=0 TSval=1666878610 TSecr=1284410410
1723	4179.1348797	10.0.139.1	10.0.139.4	TCP	68	20 → 33641 [ACK] Seq=94 Ack=2 Win=64256 Len=0 TSval=1284410410 TSecr=1666878610
1731	4184.7904004	10.0.139.1	10.0.139.4	TCP	76	20 → 49001 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1284416066 TSecr=0 WS...
1732	4184.7906617	10.0.139.4	10.0.139.1	TCP	76	49001 → 20 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 SACK_PERM TSval=1666884266 ...
1733	4184.7906917	10.0.139.1	10.0.139.4	TCP	68	20 → 49001 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1284416066 TSecr=1666884266
1735	4184.7913470	10.0.139.4	10.0.139.1	TCP	68	49001 → 20 [FIN, ACK] Seq=1 Ack=1 Win=130320 Len=0 TSval=1666884266 TSecr=1284416066
1736	4184.7914112	10.0.139.1	10.0.139.4	TCP	68	20 → 49001 [FIN, ACK] Seq=1 Ack=2 Win=64256 Len=0 TSval=1284416067 TSecr=1666884266

Frame 1719: 160 bytes on wire (1280 bits), 160 bytes captured (1280 bits) on interface any, id 0

Linux cooked capture v1

Internet Protocol Version 4, Src: 10.0.139.1, Dst: 10.0.139.4

Transmission Control Protocol, Src Port: 20, Dst Port: 33641, Seq: 1, Ack: 1, Len: 92

FTP Data (92 bytes data)

[Setup frame: 1715]

Line-based text data (8 lines)

0000 00 04 00 01 00 06 08 00 27 ad bc be 68 96 08 00
0010 45 08 00 90 53 a0 40 00 40 06 bc ba 0a 00 8b 01 E...S...
0020 0a 00 8b 04 00 14 83 69 d7 a6 de 11 06 cb 41 ee
0030 80 18 01 f6 2a 88 00 00 01 01 08 0a 4c 8e 8c 2a*...
0040 63 5a 8c 91 64 69 67 65 73 74 0d 0a 65 72 72 6f cZ...d1
0050 72 73 0d 0a 69 6e 64 65 78 2e 70 68 70 0d 0a 70 rs...1n
0060 65 72 6d 69 74 69 64 6f 0d 0a 70 72 75 65 62 61 ermit1...
0070 2e 74 78 74 0d 9a 70 72 75 65 62 61 6f 61 63 74 .txt...
0080 69 76 65 2e 74 78 74 0d 0a 72 65 73 74 72 69 6e ive.tx...
0090 67 69 64 6f 0d 0a 75 73 75 61 72 69 6f 73 0d 0a qido...

12. ¿Es posible en las capturas de wireshark ver el usuario y contraseña de los usuarios implicados?

BookWorm11A-FTP [Corriendo] - Oracle VirtualBox						
Archivo Máquina Ver Entrada Dispositivos Ayuda						
*any						
Archivo Edición Visualización Jr Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayuda						
ftp						
No.	Time	Source	Destination	Protocol	Length	Info
1845	4545.5124281...	10.0.139.1	10.0.139.4	FTP	88	Response: 220 (vsFTPd 3.0.3)
1849	4547.8337594...	10.0.139.4	10.0.139.1	FTP	83	Request: USER cliente1
1851	4547.8339316...	10.0.139.1	10.0.139.4	FTP	102	Response: 331 Please specify the password.
1853	4550.0577537...	10.0.139.4	10.0.139.1	FTP	81	Request: PASS 123456
1854	4550.0954231...	10.0.139.1	10.0.139.4	FTP	91	Response: 230 Login successful.
1856	4550.0959469...	10.0.139.4	10.0.139.1	FTP	74	Request: SYST
1857	4550.0959970...	10.0.139.1	10.0.139.4	FTP	87	Response: 215 UNIX Type: L8
1858	4550.0962908...	10.0.139.4	10.0.139.1	FTP	74	Request: FEAT
1859	4550.0963316...	10.0.139.1	10.0.139.4	FTP	83	Response: 211-Features:
1860	4550.0963633...	10.0.139.1	10.0.139.4	FTP	89	Response: EPRT
1861	4550.0964273...	10.0.139.1	10.0.139.4	FTP	75	Response: PASV
1862	4550.0964547...	10.0.139.1	10.0.139.4	FTP	82	Response: REST STREAM
1863	4550.0965355...	10.0.139.1	10.0.139.4	FTP	75	Response: SIZE
▶ Frame 1853: 81 bytes on wire (648 bits), 81 bytes captured (648 bits) on interface any, id 0 ▶ Linux cooked capture v1 ▶ Internet Protocol Version 4, Src: 10.0.139.4, Dst: 10.0.139.1 ▶ Transmission Control Protocol, Src Port: 54120, Dst Port: 21, Seq: 16, Ack: 55, Len: 13 ▶ File Transfer Protocol (FTP) [Current working directory:]						
		0000 00 00 00 01 00 06 00 0010 45 10 00 41 11 a2 40 0020 0a 00 8b 01 d3 68 00 0030 80 18 7e d8 88 4a 00 0040 4c 94 2c 65 50 41 50 0050 0a				

El protocolo FTP original (RFC 959) no está cifrado. Todo lo que envías, incluido tu usuario y tu contraseña, viaja en "texto plano" (clear text). Cualquiera que esté "esnifando" la red (como tú estás haciendo con Wireshark) puede leerlas.

Realiza una copia de seguridad de la configuración en otro archivo para no perderla de cara a las próximas prácticas (vsftpd.conf.practica2)

```

BookWorm11A-FTP [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
alumno@bookworm11a: ~
Archivo Editar Pestañas Ayuda
* alumno@... x alumno@boo... x
alumno@bookworm11a:~$ sudo cp /etc/vsftpd.conf /etc/vsftpd.conf.practica2
[sudo] contraseña para alumno:
alumno@bookworm11a:~$ ls -l /etc/vsftpd.conf*
-rw-r--r-- 1 root root 5920 ene  8 12:07 /etc/vsftpd.conf
-rw-r--r-- 1 root root 5920 ene  8 12:28 /etc/vsftpd.conf.practica2
alumno@bookworm11a:~$

```