

Práctica 3 - Sesiones I y II - Servicios de red avanzados

Entregable

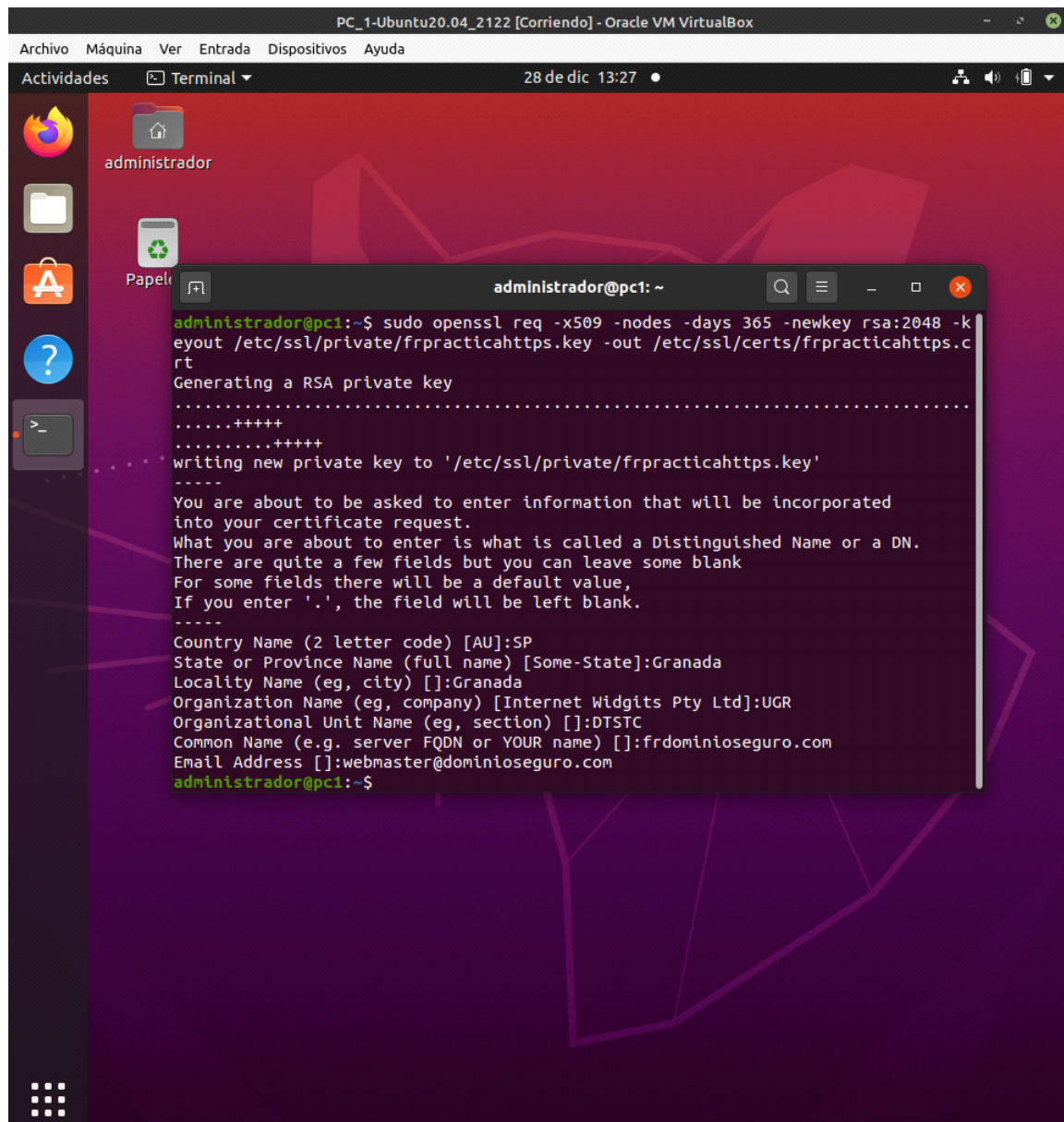
- **Información básica y requisitos para la entrega de las tareas**

- 1) Ser concisos y breves en la respuesta a cada tarea.
- 2) Ceñirse al espacio dedicado para cada tarea.
- 3) No olvidar escribir el nombre de cada integrante de la pareja y la isla en donde normalmente trabaja la pareja.
- 4) No se evaluarán tareas que ya se evaluaron en el laboratorio.
- 5) Adaptar el escenario virtualizado a la isla en donde normalmente trabaja la pareja.

- **Realización práctica: HTTPS**

- Cree un certificado SSL con la utilidad `openssl` para asociarlo al sitio `frpracticahttps.com`. Nombre el fichero del certificado como `frpracticahttps.crt` y el nombre del fichero de la clave privada como `frpracticahttps.key`.

Para crear un certificado SSL con `openssl` hay que ejecutar la orden de abajo en el PC que actúa como servidor, y en los campos poner los datos referente a la UGR, como se puede ver abajo.



- Inspeccione los ficheros `frpracticahttps.crt` y `frpracticahttps.key`.

Lo hecho en el apartado anterior hace que la clave privada y el certificado que crea se guarden respectivamente en los ficheros `/etc/ssl/private/frpracticahttps.key` y `/etc/ssl/certs/frpracticahttps.crt`, como se muestran en las fotos de abajo.

PC_1-Ubuntu20.04_2122 [Corriendo] - Oracle VM VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

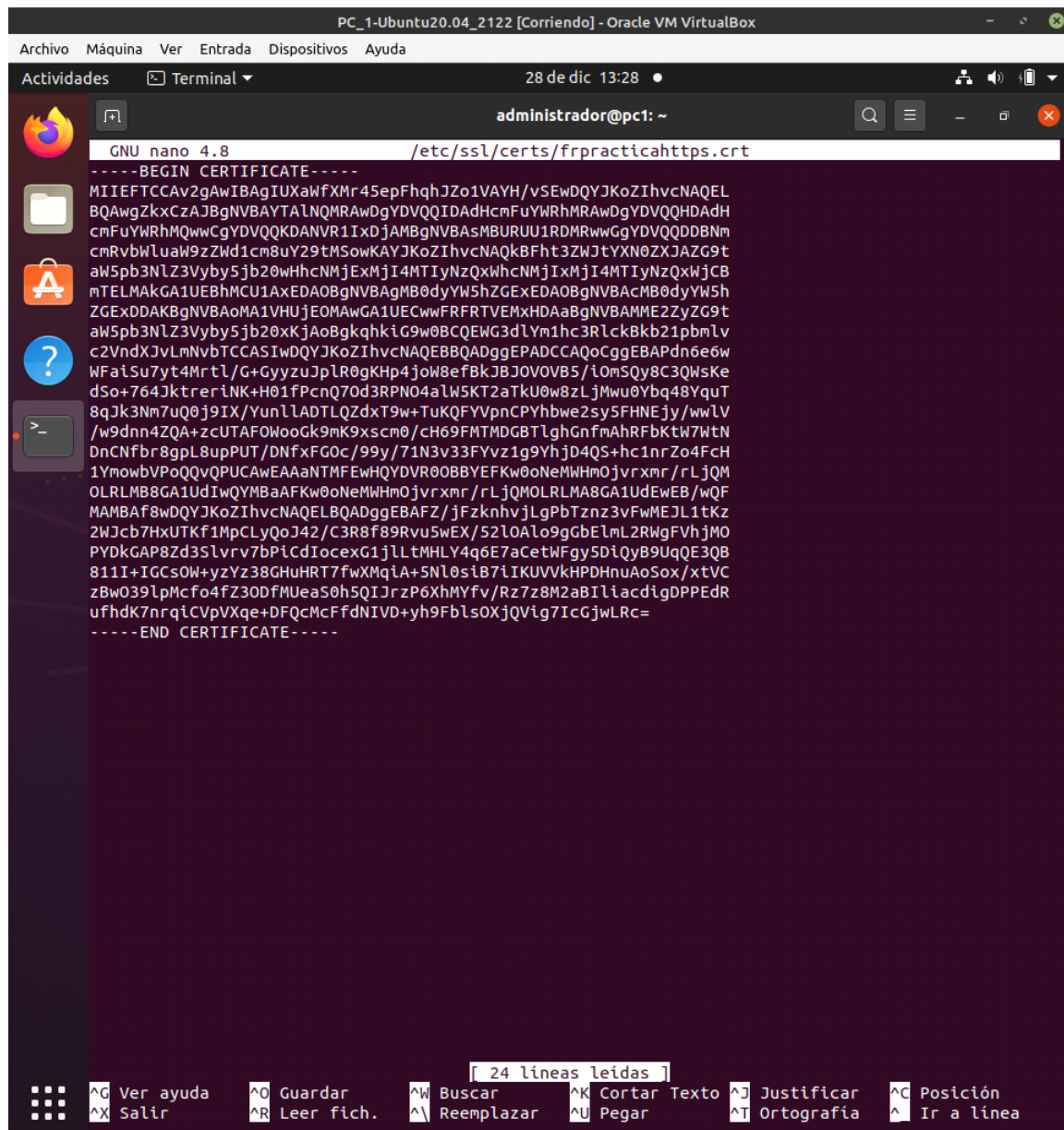
Actividades Terminal 28 de dic 13:28

administrador@pc1: ~

GNU nano 4.8 /etc/ssl/private/frpracticahttps.key

```
-----BEGIN PRIVATE KEY-----
MIIEvwIBADANBgkqhkiG9w0BAQEFAASCBBKkwggSlAgEAAoIBAQD3Z+nusFhWokru
8reDK7Zfxvhss7iaZuDICh6eI6FvHnwZCQSTLTlQef4jpkkMvAt0FrCnnUqPu+u
CZLa3q4j5vh9NXz3J00znd0TzTuGpVuSk9mk5FNMPMy4zMLtGG6uPGKrk/KiZNZ
u7kNI/SF/2Lp5ZQA0y0GxcU/cPk7IkBWFaZwj2IW8HtrMuRRzRI8v8MJVf8PXZ5+
GUAPs3FEwBTlqKBpZiVcbHJtP3B+vRTEzAxcgU5YIRp35gIURWyrVu1rTQ5WjX26
/IKS/LqT1E/wzX8RRjnP/fcv+9Td799xWL89YPWIYw+EEvoXNZ62a0BxB9WJqMG1
T6EEL0D1AgMBAAECggEAGUgQWSSsq4w4+w4dpB8z0LJ8MSi1oLzBR4pKXfSNrt6i
bAbAysp3QcV4VwxSrrd35gxRU+0ZfE/UrCckesviokoeFuSp59P1Z46qa2NMM+nP
qAcyuSwV/zPL/01fFp3Ya/3ovIhsV2ideJBSB/ll46AtUIV05AfAHM+h64sXF8im
naqPfeNcoENDvsI0Yb5S0prhjzFSA0D17dKaI+gagPJPSz2ooDuTJ09w4DW9ZcRc
3YiNELLCut0EFqgiGbR8tcUIm3wNjXNT1WGTfBZyqf+txN86SgFJjn/KL13NjamD
woVHz5ELrlxwxKsnzKgh0Qnj8rm1cvS1lgIf/evDwQKBgQD/Vj04H7RFZtI59iqH
BDrAmyGpktTCSWBSygsQwzyFOzfVLoARYD9bbeXXFjhWJz6LaqSV3MF6Wl3Gpfw1
REy+FEIf3joAWL5tkNigQQco3bwavRON1xvmXyt+qCfSfLTBLKhxiZIhwVrj1gEh
WGEAWynTE2QaBeIvegu0B/xBmQKBgQD4DGBzpvCQYw2MTYTs/JaQ+lrM1mULtUk0
Hxotx0IKF8BYKi4QfZYBa+nUgRPXaqTrceWeVHY2/xT9B50lnN2EYVhhDij93mqp
Ins6eUH+DpzKDPHn2EZ07LU8VRDVSy10DNFxtvp9LyBpMm7bj1BGRup7196RnPy4
vrY8wHNLvQKBgQDVFUTphGKP5rXCF+hrJv1vebTCbUvHHuCiQ/TsnrHCaHTP8uK
OPLWTaxhFtr8zo8H5lKaTvVrZ0LALH/adTT0/ndVOUWdGoowW99uTb1ItT9NgN
CgDqaYsqaA3VDGld2C7nppd8m24/utX46SEqLgB0tNfGkjHBjDxPVXlhyQKBgQ6
H9QtDW8FZ5Xj6WcmZJvOPWlQOq+7E8TSL2RdZV7QY/IYNc5K4XFlr6vNo01aftMx
OE2r+ISbz9vX4PN9ma8+XLEPQqjPlc1DDH5a89Ho6N4NXpLF9qsLHeMAWnQ/FunI
3yVpXns+49XWgdnFNkxt71iTh0+LI78egTwNafSzoQKBGQCVA1v0pmFX/TAJEVS7
PtB1pEKKxE2IJUNJ7fc65FwTvNU7rLcKfqJtw7w2IJRxV8yk1VWrpRgzweKJncfc
KegF21+uCiS8YrjuqanrLh8/WG8QUVkd+1CbFtsTG7B5qGygiVXQ20pouSJGSRe
PgBM/IMz+Lv+IPfJm9cExGYrJQ==
-----END PRIVATE KEY-----
```

Ver ayuda Guardar Buscar Cortar Texto Justificar Posición
Salir Leer fich. Reemplazar Pegar Ortografía Ir a línea



The screenshot shows a terminal window titled "PC_1-Ubuntu20.04_2122 [Corriendo] - Oracle VM VirtualBox". The terminal is running the nano text editor, editing the file "/etc/ssl/certs/frpracticahttps.crt". The file contains a PEM-formatted X.509 certificate. The terminal window has a sidebar with icons for file manager, application store, help, and terminal. At the bottom, there is a status bar with keyboard shortcuts for nano editor actions.

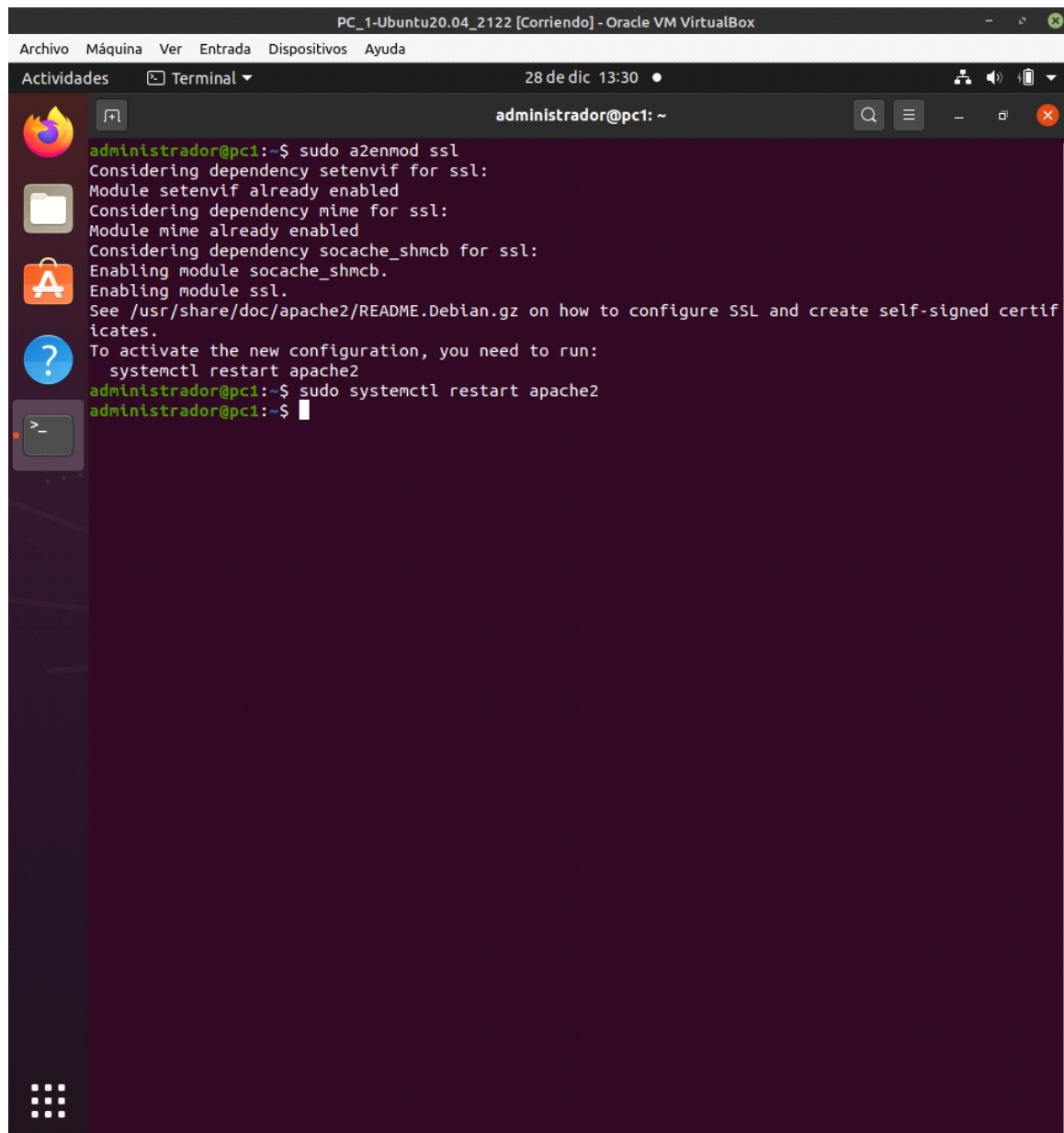
```
GNU nano 4.8 /etc/ssl/certs/frpracticahttps.crt
-----BEGIN CERTIFICATE-----
MIIEFTCCA2gAwIBAgIUxawfXMr45epFhqhJZo1VAYH/vSEwDQYJKoZIhvcNAQEL
BQAwZ2kxZCzAJBgNVBAYTALNQMRAwDgYDVQQIDAdHcmFuYWRhMRwDgYDVQHDAdH
cmFuYWRhMRwDgYDVQKDANVR1IxDjAMBGNVBAwMBURUU1RDMRwwGgYDVQDDBNm
cmRvbWluaW9zZWd1cm8uY29tMSowKAYJKoZIhvcNAQkBFht3ZWJtYXN0ZXJAZG9t
aW5pb3NlZ3Vyby5jb20wHhcNMjExMjI4MTIyNzQxhcnMjExMjI4MTIyNzQxWjCB
mTElMAkGA1UEBhMCU1AxEDAOBgNVBAGMB0dyYW5hZGExEDAOBgNVBACMB0dyYW5h
ZGExDDAKBgNVBAoMA1VHUjEOMAwGA1UECwwFRFRFTVEMxHDAaBgNVBAMME2ZyZG9t
aW5pb3NlZ3Vyby5jb20wKjAoBgkqhkiG9w0BCQEWG3d1Ym1hc3RlckBkb21pbm1v
c2VndXJvLmNvbTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAPdn6e6w
WfaiSu7yt4Mrt1/G+GyyzuJpLR0gKHp4jow8efBkJBjOVVB5/iOmSQy8C3QWskE
dSo+764JktreriNK+H01fPcnQ70d3RPN04alW5KT2aTkU0w8zLjMwu0Ybq48YquT
8qJk3Nm7uQ0j9IX/YunllADTLQZdxT9w+TuKQFYVpnCPYhbwe2sy5FHNEjy/wwLV
/w9dnn4ZQA+zcUTAF0WooGk9mK9xscm0/cH69FMTMDGBTLghGnfmaHRFBKtW7WtN
DnCNfbr8gpL8upPUT/DNfxFG0c/99y/71N3v33FYvz1g9Yhjd4QS+hc1nrZo4FcH
1YmowbVPOQQVPUCAwEAAaNTMFEwHQYDVIR00BBYEFKw0oNeMWHm0jvrxmr/rLjQM
OLRLMB8GA1UdIwQYMBaAFKw0oNeMWHm0jvrxmr/rLjQMOLRLMA8GA1UdEwEB/wQF
MAMBAf8wDQYJKoZIhvcNAQELBQADggEBAFZ/jFzknhvjlGpBtznz3vFwMEJL1tKz
2WJcb7HxUTKf1MpCLYqoJ42/C3R8f89Rvu5wEX/52l0Alo9gGbElmL2RWgFVhjMO
PYDkGAP8Zd3S1vrv7bPiCdIocexG1jLLtMHLy4q6E7aCetWfgy5DiQyB9UqQE3QB
811I+IGCSOW+yzYz38GHuHRT7fwXmqIA+5Nl0siB7iIKUVVKhPHDhnuAoSox/xtVC
zBw039lpMcfo4fZ30DFMUeaS0h5QIJrzP6XhMYfv/Rz7z8M2aBilIacdigDPPEdR
ufhdK7nrqICVpVXqe+DFQcMcFfdNIVD+yh9FblsOXjQVig7IcGjwLRc=
-----END CERTIFICATE-----
```

24 líneas leídas

Ver ayuda Guardar Buscar Cortar Texto Justificar Posición
Salir Leer fich. Reemplazar Pegar Ortografía Ir a línea

- Cree un host virtual con una página de inicio que muestre el mensaje “FR HTTPS” y configúrelo para que funcione con HTTPS haciendo uso del certificado creado anteriormente. Compruebe su correcto funcionamiento usando un navegador.

Primero hay que usar el script a2enmod como se muestra abajo, seguido de la orden para reiniciar el módulo apache2



The screenshot shows a terminal window titled "PC_1-Ubuntu20.04_2122 [Corriendo] - Oracle VM VirtualBox". The window has a menu bar with "Archivo", "Máquina", "Ver", "Entrada", "Dispositivos", and "Ayuda". Below the menu bar is a toolbar with "Actividades" and "Terminal". The terminal window shows the following commands and output:

```
administrador@pc1: ~  
administrador@pc1:~$ sudo a2enmod ssl  
Considering dependency setenvif for ssl:  
Module setenvif already enabled  
Considering dependency mime for ssl:  
Module mime already enabled  
Considering dependency socache_shmcb for ssl:  
Enabling module socache_shmcb.  
Enabling module ssl.  
See /usr/share/doc/apache2/README.Debian.gz on how to configure SSL and create self-signed certificates.  
To activate the new configuration, you need to run:  
systemctl restart apache2  
administrador@pc1:~$ sudo systemctl restart apache2  
administrador@pc1:~$
```

A continuación crearemos el archivo *sites-available* del directorio */etc/apache2* se modifica, que será el archivo de configuración del virtual host que se va a crear.

The screenshot shows a terminal window titled "PC_1-Ubuntu20.04_2122 [Corriendo] - Oracle VM VirtualBox". The terminal is running the GNU nano 4.8 editor, editing the file `/etc/apache2/sites-available/frdominioseguro.com.conf`. The user is `administrador@pc1: ~`. The date and time are "28 de dic 13:35". The terminal content is as follows:

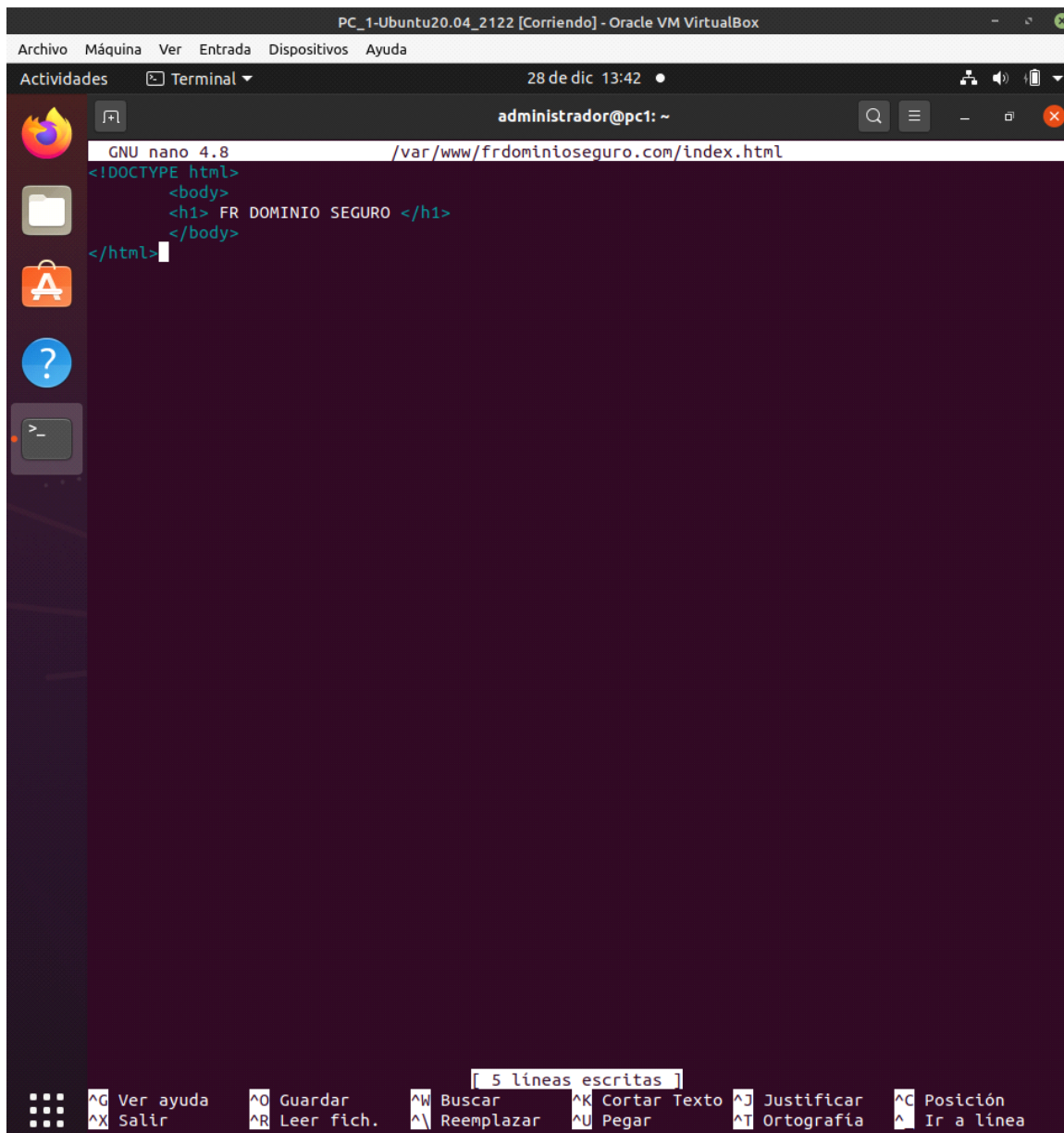
```
GNU nano 4.8 /etc/apache2/sites-available/frdominioseguro.com.conf
<VirtualHost *:443>
  ServerName frdominioseguro.com
  DocumentRoot /var/www/frdominioseguro.com

  SSLEngine on
  SSLProtocol -all +TLSv1.2
  SSLCertificateFile      /etc/ssl/certs/frpracticahttps.crt
  SSLCertificateKeyFile    /etc/ssl/private/frpracticahttps.key
</VirtualHost>
```

At the bottom of the terminal, there is a status bar showing "9 líneas escritas" and a list of keyboard shortcuts:

	Ver ayuda	Guardar	Buscar	Cortar Texto	Justificar	Posición
Salir	Leer fich.	Reemplazar	Pegar	Ortografía	Ir a línea	

Después de esto, crearemos el directorio raíz de dicho host con `mkdir -p /var/www/frdominioseguro.com`, en el que situaremos el archivo `index.html`, que es donde se va a escribir lo que aparecerá cuando se busque la dirección de este host. En este caso, lo vamos a configurar para que aparezca la sentencia "FR DOMINIO SEGURO".



The screenshot shows a terminal window titled "PC_1-Ubuntu20.04_2122 [Corriendo] - Oracle VM VirtualBox". The terminal is running the GNU nano 4.8 text editor, editing the file `/var/www/frdominioseguro.com/index.html`. The editor shows the following HTML code:

```
<!DOCTYPE html>
<body>
  <h1> FR DOMINIO SEGURO </h1>
</body>
</html>
```

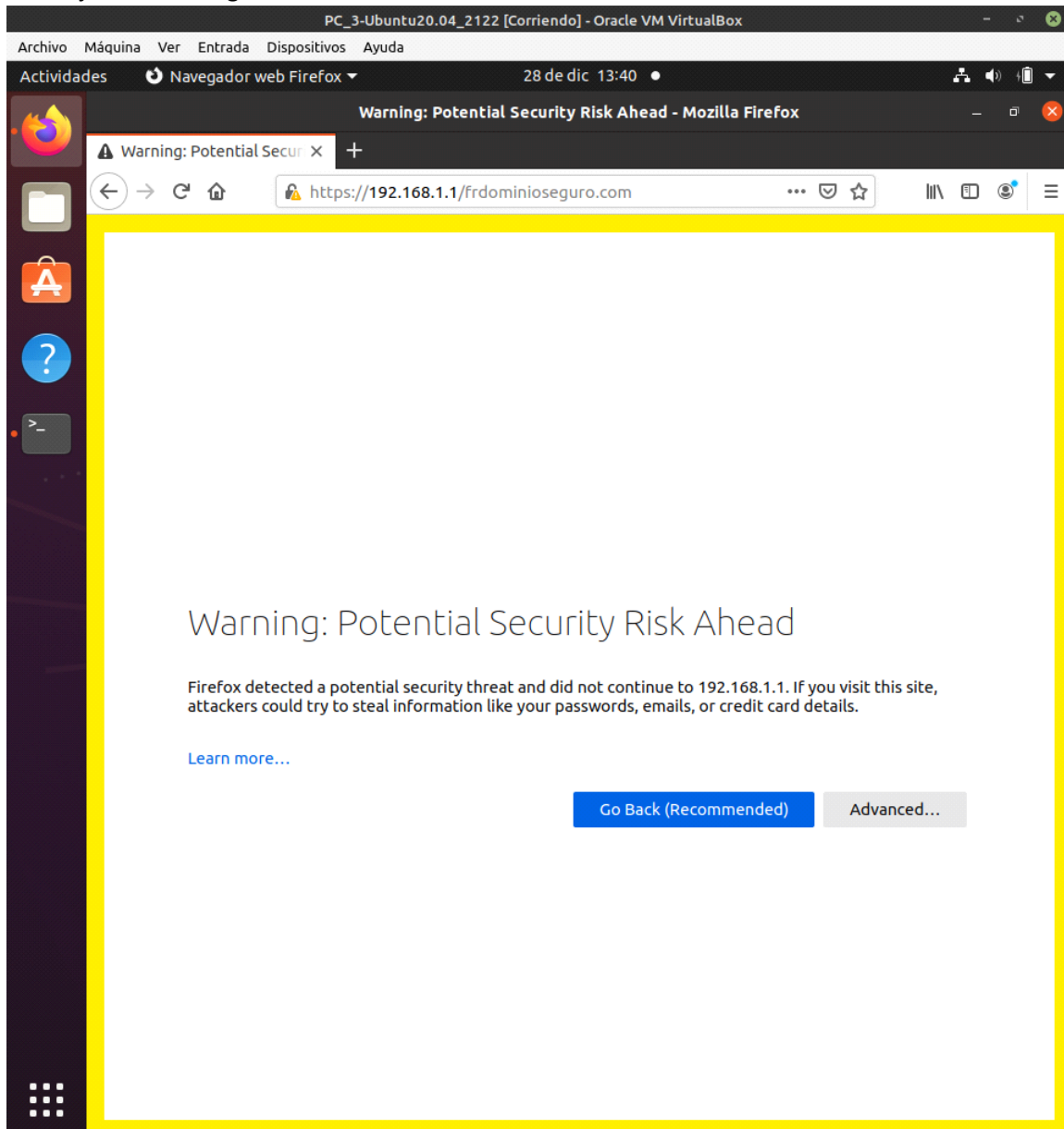
The terminal window also displays a sidebar with application icons (Firefox, Files, App Store, Help, and Terminal) and a status bar at the bottom with keyboard shortcuts for various actions like "Ver ayuda", "Guardar", "Buscar", etc.

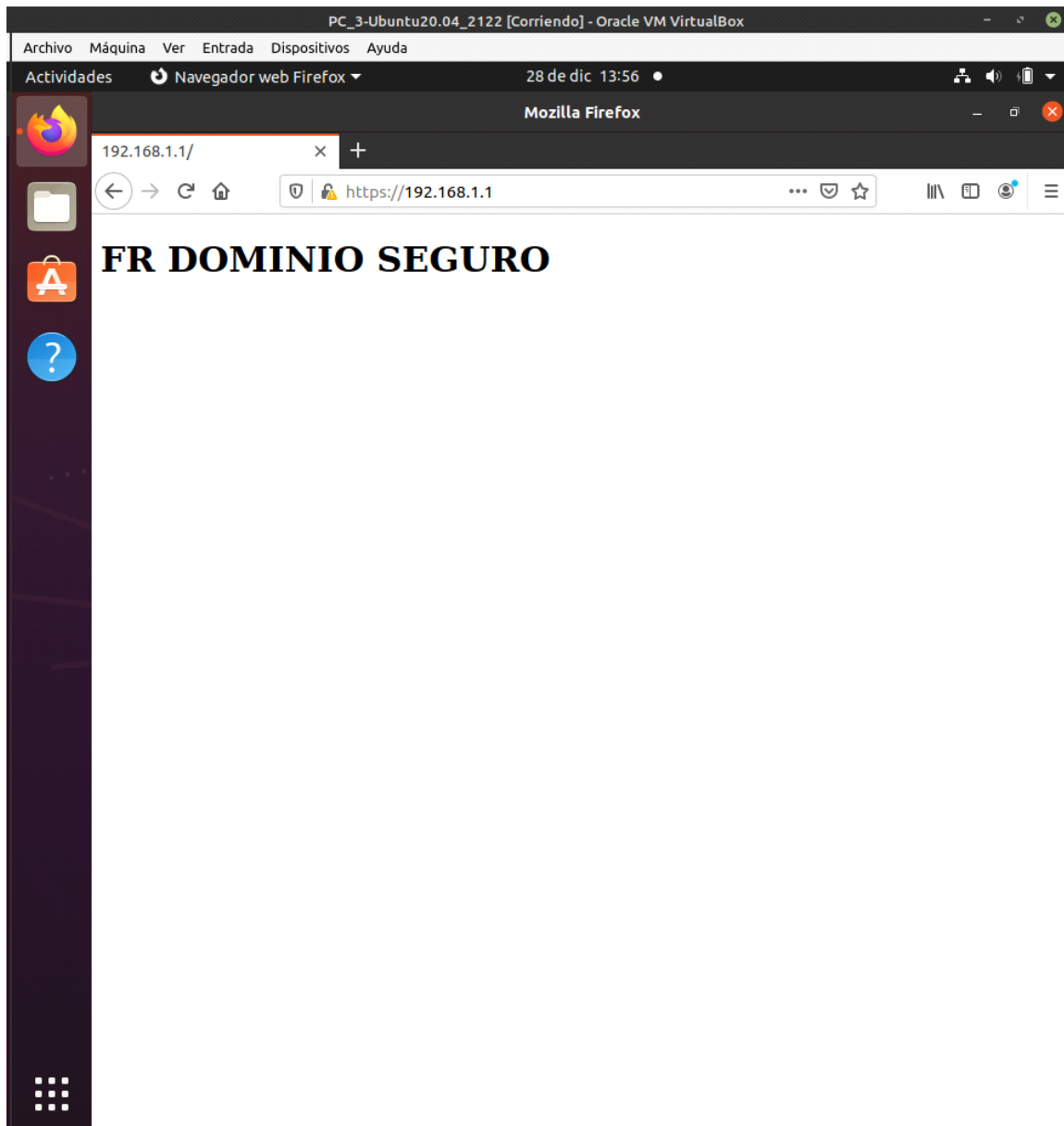
A continuación, al igual que en la parte 1 de esta práctica, usaremos la utilidad *chown*, seguida de *a2ensite* para nuestro host, para comprobar que todo ha funcionado bien se usa la orden *apachectl configtest*; y en el caso de que no haya ningún fallo reiniciaremos *apache2*.

```
administrador@pc1:~$ sudo chown -R www-data: /var/www/frdominioseguro.com
administrador@pc1:~$ sudo a2ensite frdominioseguro.com.conf
Enabling site frdominioseguro.com.
To activate the new configuration, you need to run:
    systemctl reload apache2
administrador@pc1:~$ sudo apachectl configtest
AH00558: apache2: Could not reliably determine the server's fully qualified domain name, using 12
7.0.0.1. Set the 'ServerName' directive globally to suppress this message
Syntax OK
administrador@pc1:~$ sudo systemctl reload apache2
```

Para comprobar que todo lo hecho con anterioridad funciona, nos vamos a meter en el buscador del PC que actúa como cliente y vamos a buscar nuestro dominio seguro, el cual, si va todo bien nos aparecerá

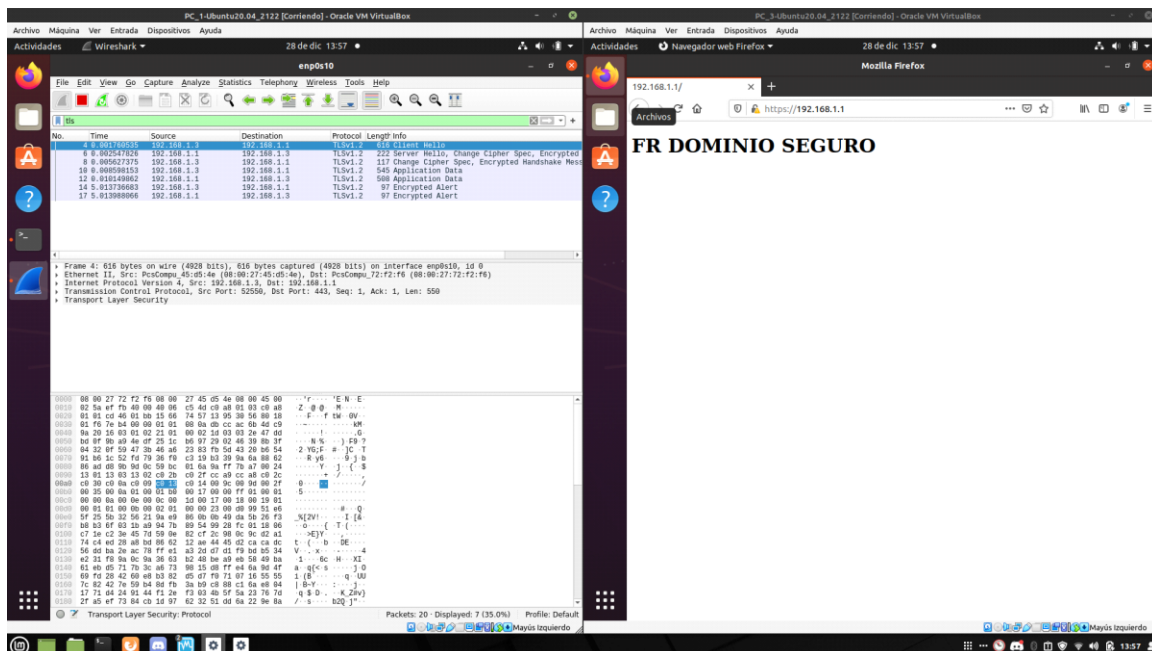
una advertencia de seguridad, la cuál si ignoramos y le damos a "advanced" y entrar, nos aparecerá el mensaje antes configurado.





- Abra Wireshark en su equipo y capture los mensajes que se generan cuando accede al sitio creado anteriormente. ¿Qué mensajes TLS se intercambian la aplicación cliente (navegador web) y el servidor (Apache) durante el inicio de la conexión? ¿Qué información relevante se intercambia en esos mensajes? ¿Es posible ver los mensajes del protocolo HTTP?

Dentro del wireshark vamos a capturar los datos del enp0s10 para realizar este ejercicio.



Como se puede ver en la foto, al buscar nuestro página "dominioseguro", aparecen 7 mensajes en el wireshark:

- En el 1 el cliente saluda.
- En el 2 el servidor saluda y le manda la clave cifrada al cliente.
- En el 3 el cliente le dice al servidor que ha recibido correctamente la clave cifrada.
- En el 4 el cliente comienza a enviarle datos al servidor.
- En el 5 el servidor le empieza a enviar datos al cliente.
- En el 6 el cliente recibe una alerta de encriptación.
- En el 7 el servidor recibe una alerta de encriptación.