



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.

Pareja: Leire Requena García, Clara M.^a Romero Lara

Isla habitual: 4

Trabajo a entregar: Sesión II práctica 3

Realización práctica: HTTPS



- 1) 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`.

Iniciamos el servicio `apache2` y comprobamos que funciona accediendo a `localhost`.
Siguiendo el guión, creamos el certificado SSL:

```
administrador@pc1: ~  
administrador@pc1:~$ sudo systemctl restart apache2  
[sudo] contraseña para administrador:  
administrador@pc1:~$ sudo openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout /etc/ssl/private/frpracticahttps.key -out /etc/ssl/certs/frpracticahttps.crt  
Generating a RSA private key  
.....+++++  
writing new private key to '/etc/ssl/private/frpracticahttps.key'  
-----  
You are about to be asked to enter information that will be incorporated  
into your certificate request.  
What you are about to enter is what is called a Distinguished Name or a DN.  
There are quite a few fields but you can leave some blank  
For some fields there will be a default value,  
If you enter '.', the field will be left blank.  
-----  
Country Name (2 letter code) [AU]:SP  
State or Province Name (full name) [Some-State]:Granada  
Locality Name (eg, city) []:Granada  
Organization Name (eg, company) [Internet Widgits Pty Ltd]:UGR  
Organizational Unit Name (eg, section) []:DTSTC  
Common Name (e.g. server FQDN or YOUR name) []:frpracticahttps.com  
Email Address []:webmaster@frpracticahttps.com
```

2) Inspeccione los ficheros `frpracticahttps.crt` y `frpracticahttps.key`.

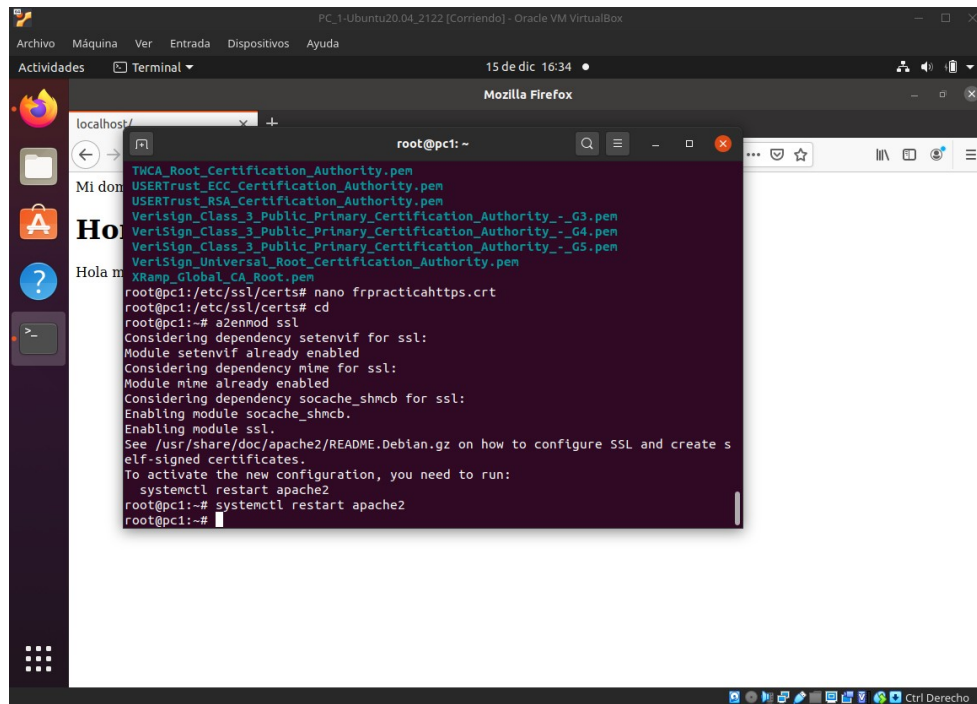
```
frpracticahttps.key:
```

frpracticahttps.crt:

[illegible]

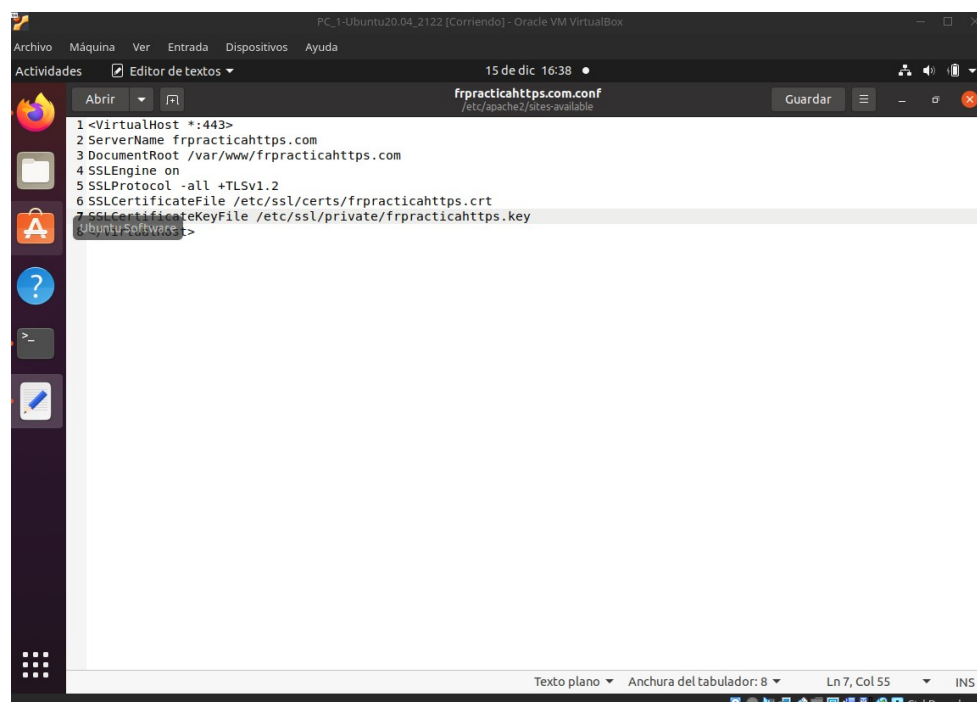
- 3) Cree un host virtual con una página de inicio que muestre el mensaje “FR HTTPS” y configúrelo para que funcione con HTTPS haciendo uso del certificado creado anteriormente. Compruebe su correcto funcionamiento usando un navegador.

Configuramos el certificado y reiniciamos el servicio apache2 con a2enmod. Creamos un archivo de configuración (.conf) para nuestra página:



```

root@pci:~# nano frpracticahttps.crt
root@pci:/etc/ssl/certs# cd
root@pci:~# 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 s
elf-signed certificates.
To activate the new configuration, you need to run:
systemctl restart apache2
root@pci:~# systemctl restart apache2
root@pci:~#
  
```

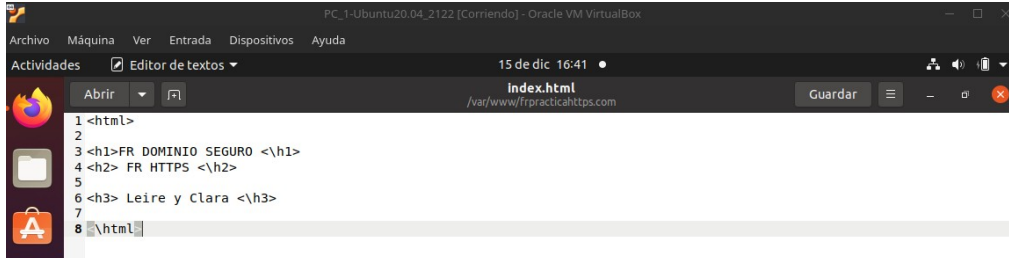


```

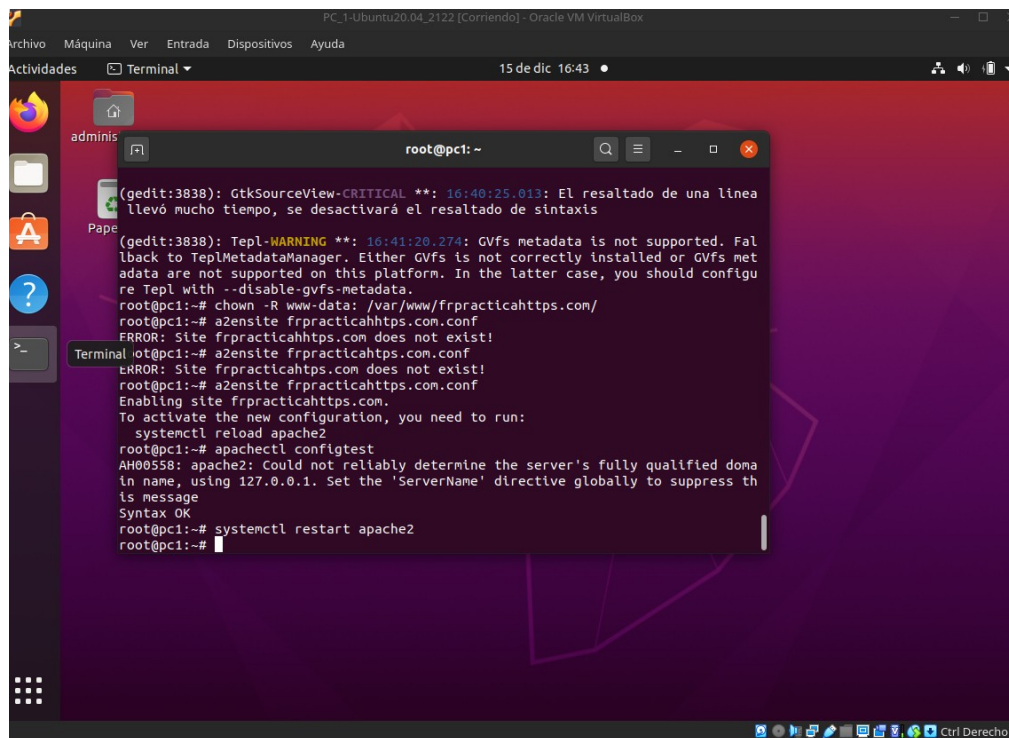
1<VirtualHost *:443>
2ServerName frpracticahttps.com
3DocumentRoot /var/www/frpracticahttps.com
4SSLEngine on
5SSLProtocol -all +TLSv1.2
6SSLCertificateFile /etc/ssl/certs/frpracticahttps.crt
7SSLCertificateKeyFile /etc/ssl/private/frpracticahttps.key
  
```



A continuación, escribimos el index.html de la página, le damos permisos y hacemos chown. Comprobamos el estado de nuestra configuración de apache, añadimos el host virtual bajo una IP local y recargamos:



```
1 <html>
2
3 <h1>FR DOMINIO SEGURO <\h1>
4 <h2> FR HTTPS <\h2>
5
6 <h3> Leire y Clara <\h3>
7
8 </html>
```



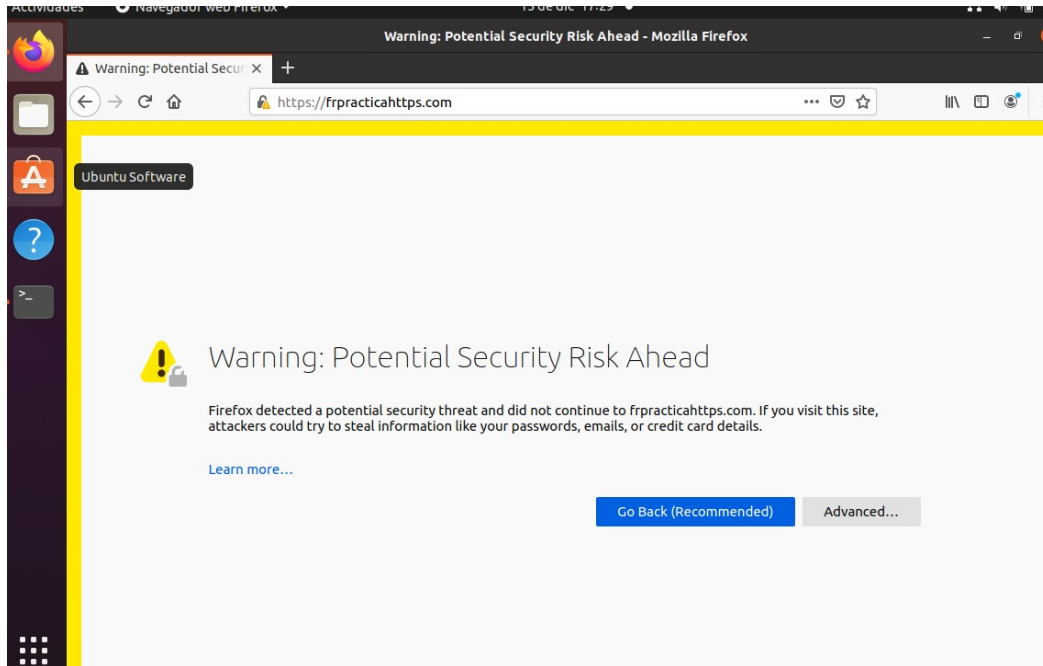
```
root@pc1:~# chown -R www-data: /var/www/frpracticahttps.com/
root@pc1:~# a2ensite frpracticahttps.com.conf
ERROR: Site frpracticahttps.com does not exist!
root@pc1:~# a2ensite frpracticahttps.com.conf
ERROR: Site frpracticahttps.com does not exist!
root@pc1:~# a2ensite frpracticahttps.com.conf
Enabling site frpracticahttps.com.
To activate the new configuration, you need to run:
systemctl reload apache2
root@pc1:~# apachectl configtest
AH00558: apache2: Could not reliably determine the server's fully qualified domain name, using 127.0.0.1. Set the 'ServerName' directive globally to suppress this message
Syntax OK
root@pc1:~# systemctl restart apache2
root@pc1:~#
```



```
1 127.0.0.1    pc1
2 127.0.1.1    administrador-PC1
3
4 # The following lines are desirable for IPv6 capable hosts
5 ::1          ip6-localhost ip6-loopback
6 fe00::0      ip6-localnet
7 ff00::0      ip6-mcastprefix
8 ff02::1      ip6-allnodes
9 ff02::2      ip6-allrouters
10
11 192.168.1.1  frpracticahttps.com
```



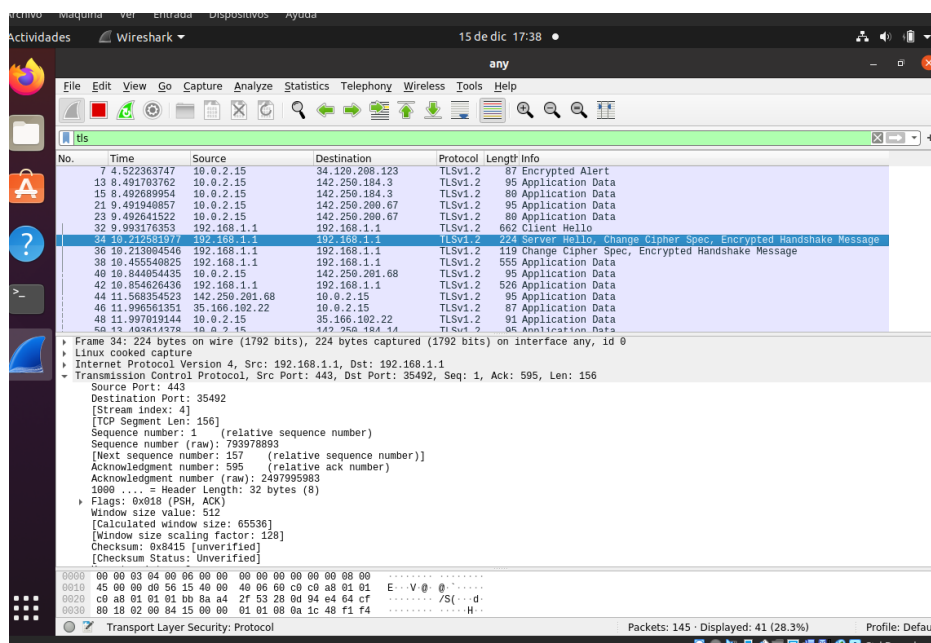
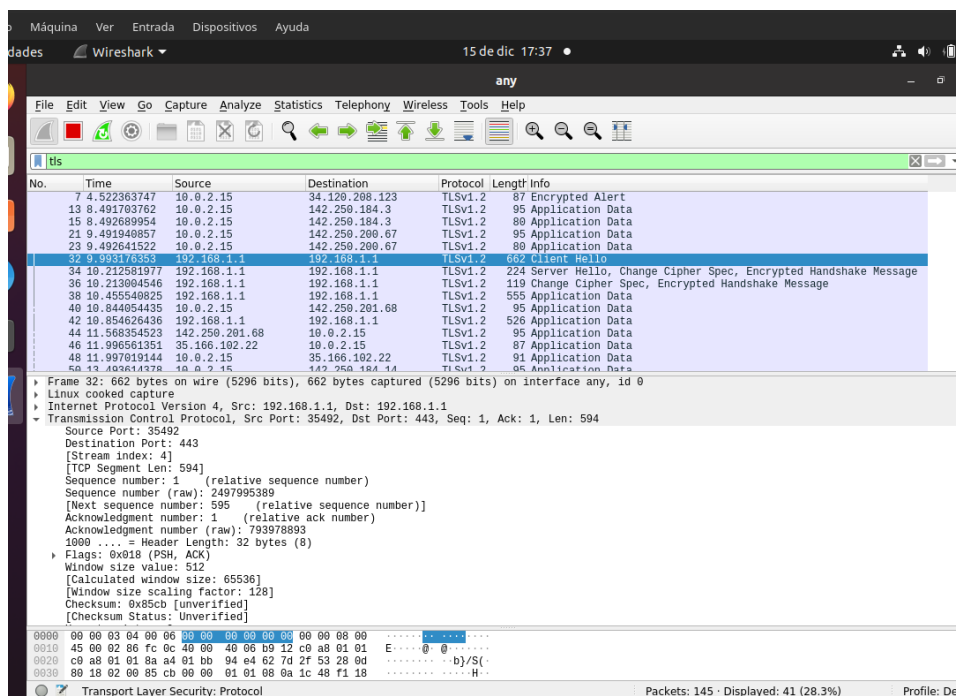

Finalmente, comprobamos que funciona accediendo desde el navegador. Nos saldrá un aviso de seguridad debido al certificado autofirmado:





- 4) 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?

Se intercambian mensajes de *handshake* encriptados que utilizan la clave que hemos generado.





Wireshark interface showing a TLSv1.2 connection. The packet list shows a sequence of packets including Encrypted Alerts, Application Data, Client Hello, Server Hello, Certificate, Server Key Exchange, Server Hello Done, Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message, New Session Ticket, and Application Data. The packet details pane shows the structure of a TLSv1.2 packet, including the TLSv1.2 Header, TLSv1.2 Handshake, and TLSv1.2 Application Data. The packet bytes pane shows the raw data of the selected packet.

Wireshark interface showing an HTTP connection. The packet list shows a sequence of packets including GET / HTTP/1.1 and HTTP/1.1 204 No Content. The packet details pane shows the structure of an HTTP packet, including the HTTP Request and HTTP Response. The packet bytes pane shows the raw data of the selected packet.