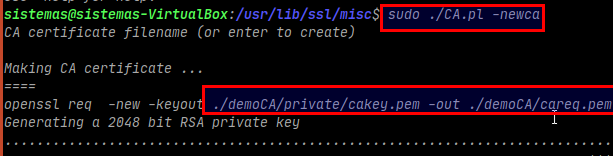
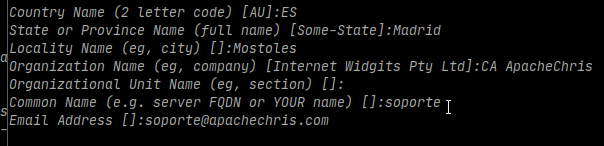
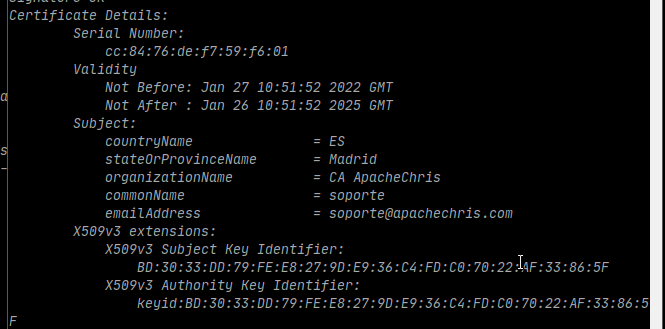
Voy a rehacer el ejercicio de HTTPS porque no funcionaba el ultimo dia. Y lo voy a ordenar mejor.

1º → Generamos el CA de nuestra empresa

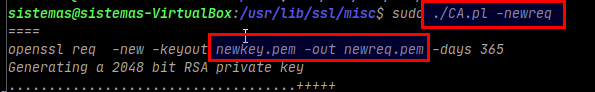


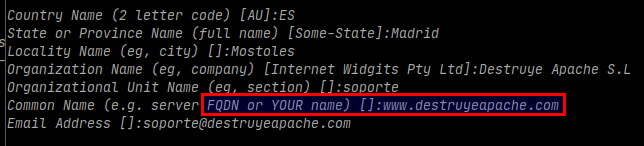




Aquí hay datos de la empresa certificadora.

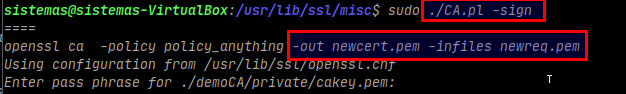
2º → Hacemos ahora la SOLICITUD de la empresa que quiere tener un HTTPS.

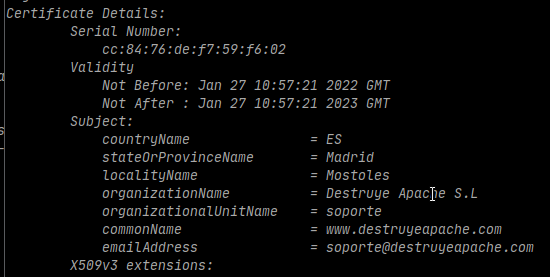




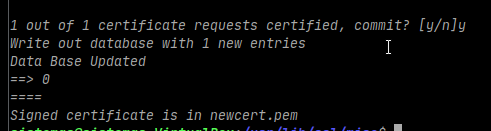
ES MUY IMPORTANTE el FQDN porque este tiene que ser IDENTICO en la configuración del apache o nunca va a funcionar.

3º → Ahora como CA firmamos esa solicitud de certificado.

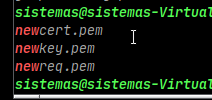




Podemos ver la info de la solicitud que nos ha llegado

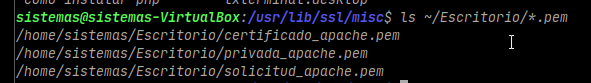


Ya tenemos firmado el certificado. Ahora mismo tenemos varios archivos generados.

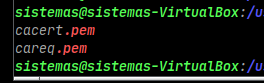


Estos 3 archivos SON DE LA EMPRESA QUE HA PEDIDO UN CERTIFICADO, la que va a crear la web. Tengo la solicitud (req), la clave PRIVADA de esa empresa (key) y el certificado FIRMADO por el CA (cert).

Los muevo a un sitio seguro y les cambio el nombre.



Por si acaso lo necesitara, en demoCA tengo el certificado de mi CA, y el request del mismo.

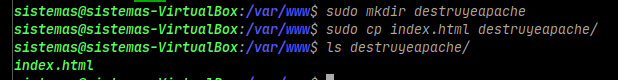


Y dentro de esta carpeta, hay una subcarpeta PRIVATE donde está la privada de mi CA



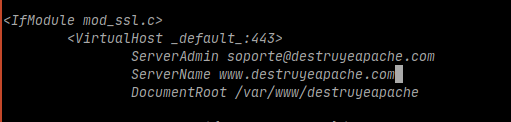
Todo esto es necesario porque son los archivos que necesito INCLUIR en la configuración de apache para que funcione por HTTPS.

4º → Creo un directorio en la carpeta de apache que será / de mi web



5º → Comenzamos con la configuración de apache. Para hacerlo con HTTPS hay que tocar nuevas líneas y añadir cosas extras, como un módulo.

Vamos a trabajar con el fichero default-ssl que es el archivo predefinido para configurar HTTPS.



En estas primeras líneas vemos 3 cosas: El correo, el server name, que como ya dije antes, tiene que ser IDENTICO al que pusimos en el certificado, y luego la ruta de apache donde estará su /.

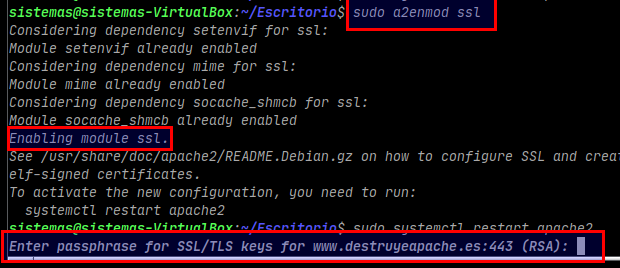


En estas 2 líneas le decimos que nuestro CERTIFICADO de HTTPS está en este archivo. Y que la clave PRIVADA con la que lo ciframos está en ese otro archivo. Son los que generamos en el punto 1.

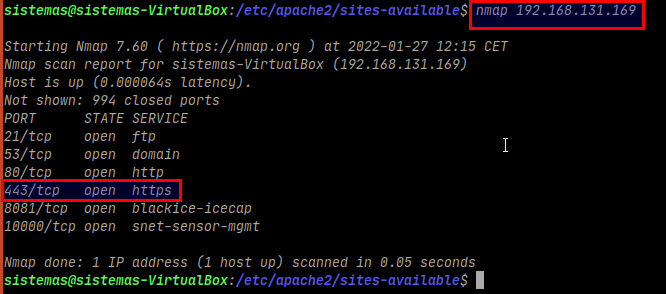
6º → Tenemos que comprobar el FIREWALL y ABRIR el puerto 443.



En este caso no tengo firewall, así que nos lo ahorramos. Si lo tuviéramos, seria añadir la excepción correspondiente.

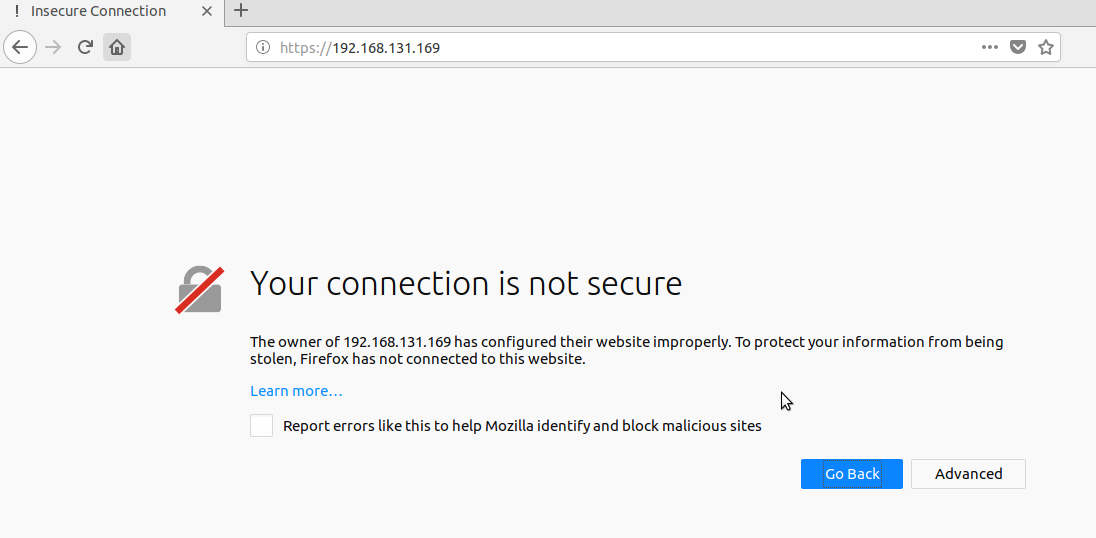


Ahora abrimos el puerto 443. Con el comando a2enmod. Nada más activarlo, nos pide la passphrase de nuestra web, esta es la clave privada que generamos en el punto 1.



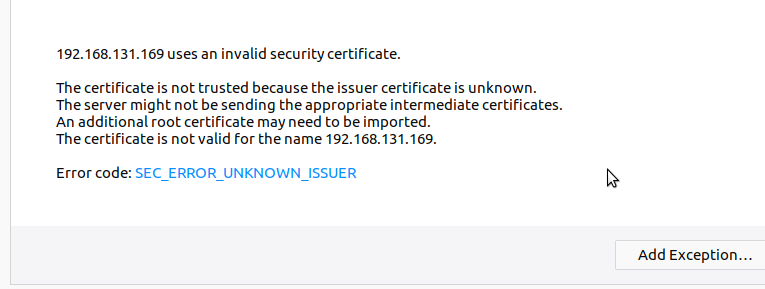
Con el comando NMAP y la ip de la web, podemos comprobar el estado de los puertos. Si aparece en la lista, es que está abierto, y te indica el servicio para el que funciona.

7º → Probamos la conexión

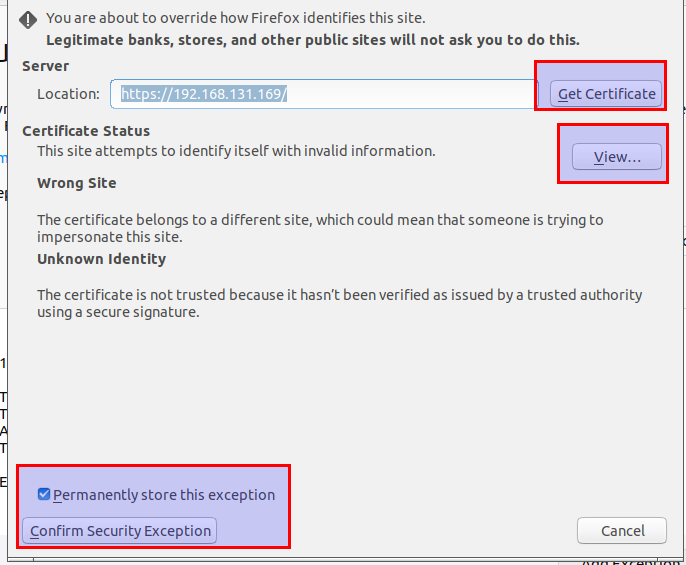


Nos sale esta pestaña, esto es porque nuestro navegador NO TIENE EL CERT de la web a la que intenta acceder. Nos pregunta si queremos obtenerlo y añadirlo.

Si le damos a advanced:



Puedo añadir la excepción y configurarla:



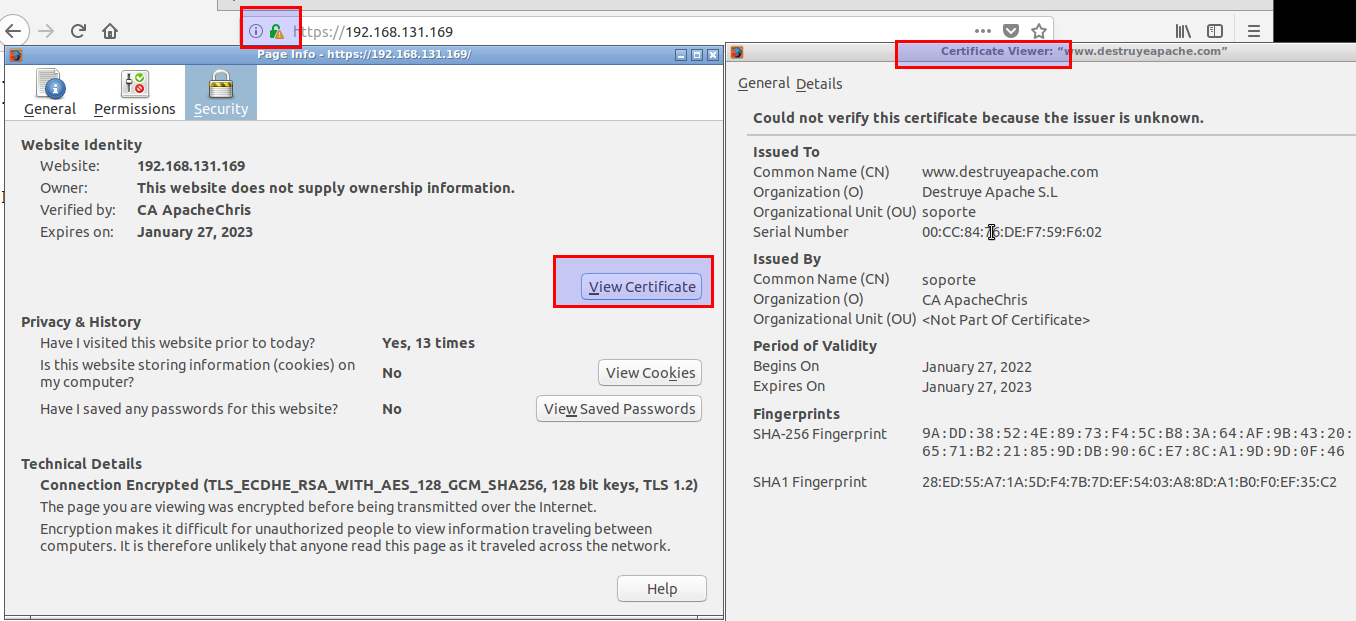
Si quiero verlo, si quiero cogerlo, para siempre, solo un tiempo, etc.

Cuando acepto, me carga la web

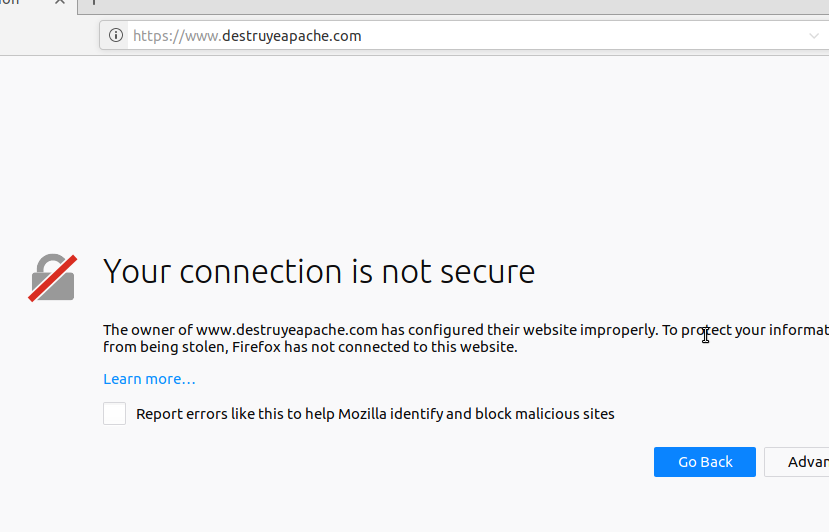


Yo soy muy original y he copiado el index del último ejercicio en lugar de hacer uno nuevo.

Si le pulso al candadito, puedo ver el certificado de seguridad de la pagina

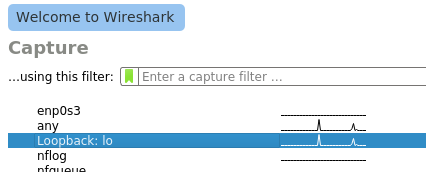


Ahora añado la página web a /*etc*/hosts porque el DNS no me funciona, pero bueno.

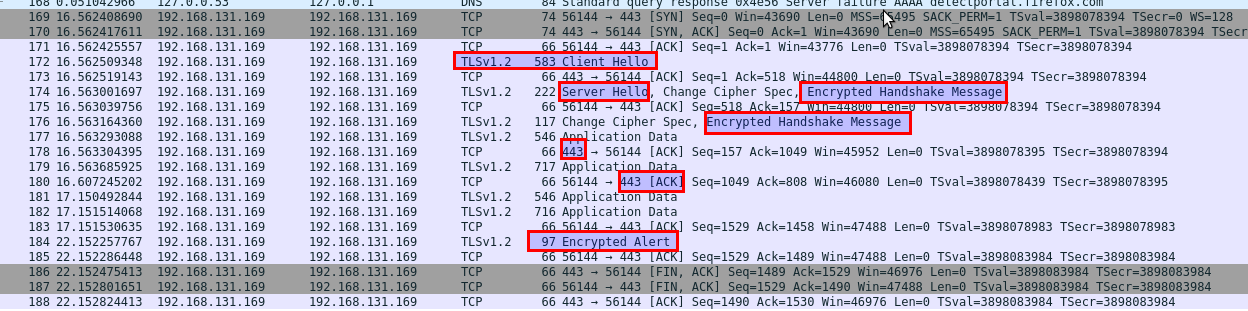


Ahora accedo por DNS y me vuelve a pedir la excepción.

8º → Vamos a abrir wireshark para ver el tráfico. Como es httpS significa que el tráfico estará cifrado, es seguro, y no podremos ver nada.



Tengo que seleccionar la de loopback.



Como se puede apreciar, se hace el 3way handshake, pero esta vez por el puerto 443, y además te pone bien clarito que está encryptado.

