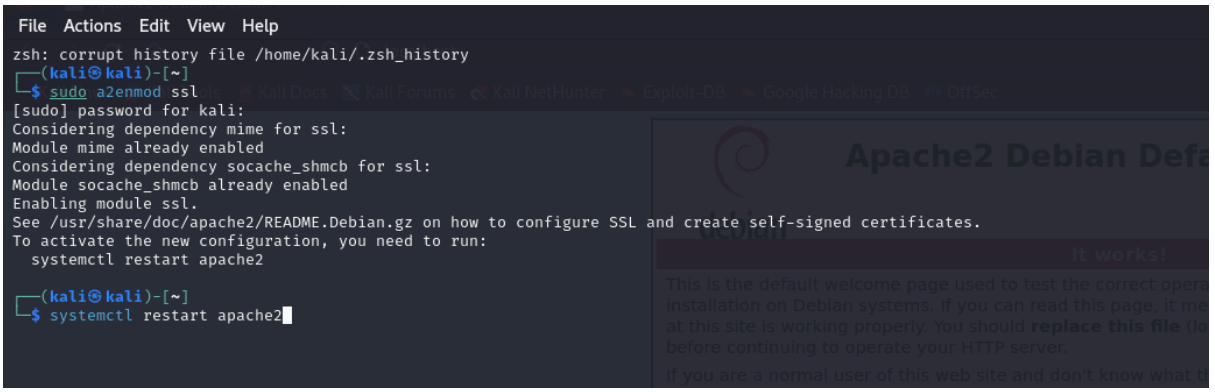
Esercizio svolto con HTTPS

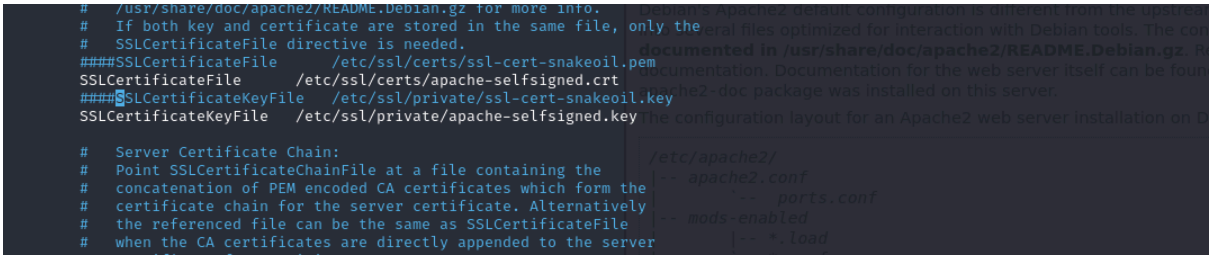
Abilitiamo la crittografia SSL su Apache2



Adesso creiamo un certificato SSL autofirmato con OPENSSL

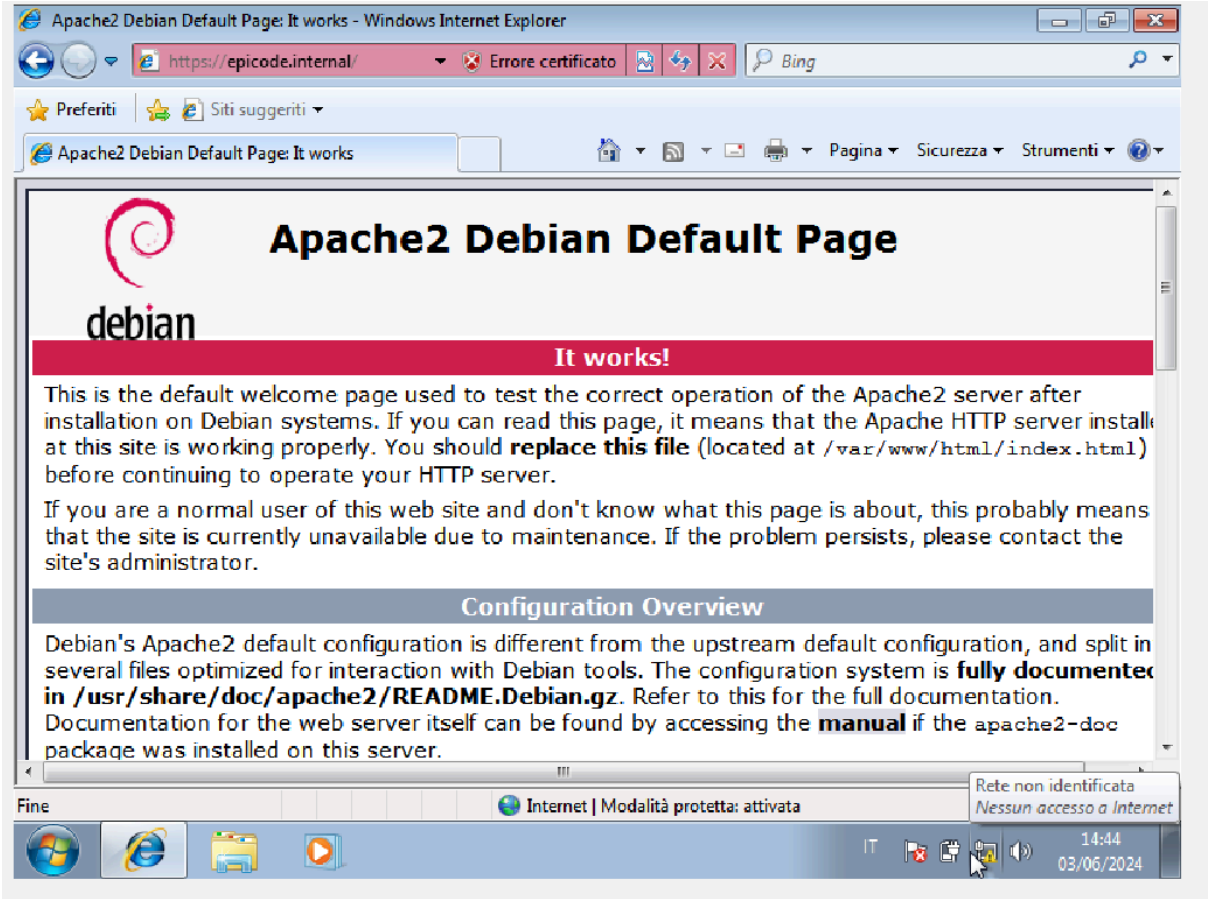
Il file che contiene il certificato si chiamerà apache-selfigned e si chiama uguale, cambia solo l'estensione, anche la chiave

AGGIORNIAMO IL FILE CERTIFICATI DI APACHE2 TRASFORMANDO IN COMMENTI LE COSE VECCHIE:



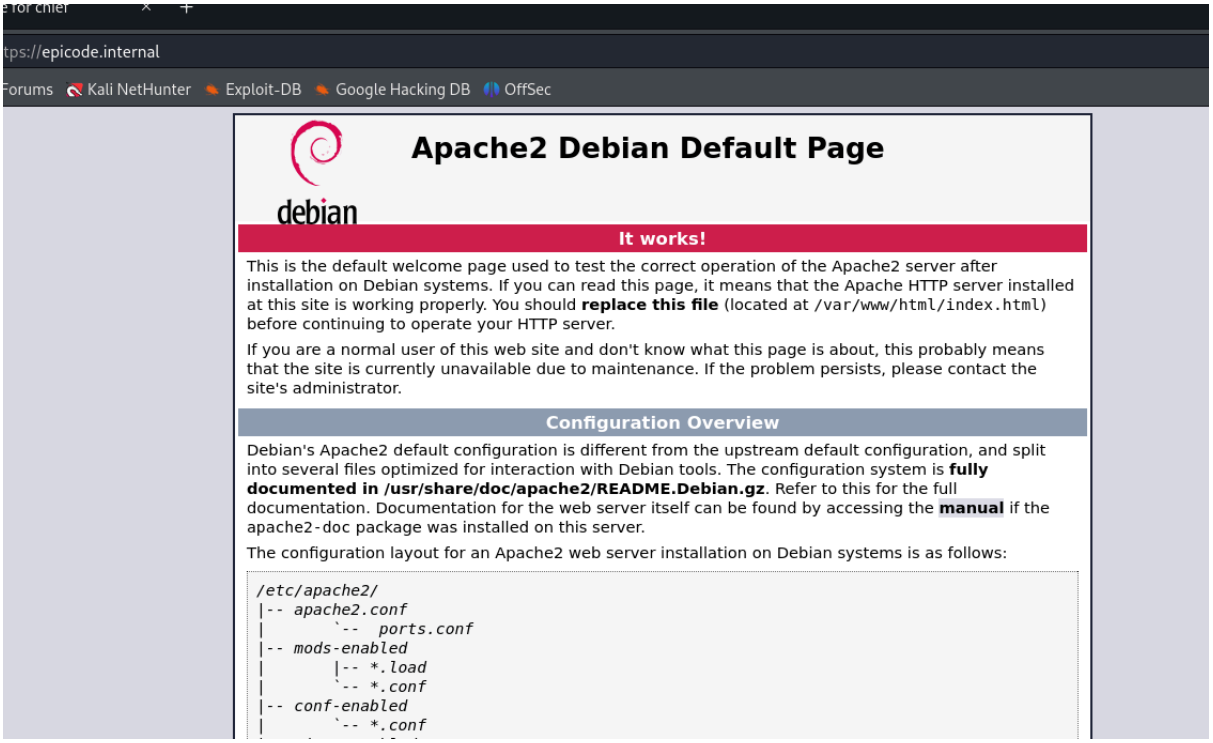
```
File  Actions  Edit  View  Help
zsh: corrupt history file /home/kali/.zsh_history
┌──(kali㉿kali)-[~]
└─$ sudo a2ensite default-ssl.conf
[sudo] password for kali:
Enabling site default-ssl.
To activate the new configuration, you need to run:
  systemctl reload apache2

┌──(kali㉿kali)-[~]
└─$ systemctl reload apache2
```

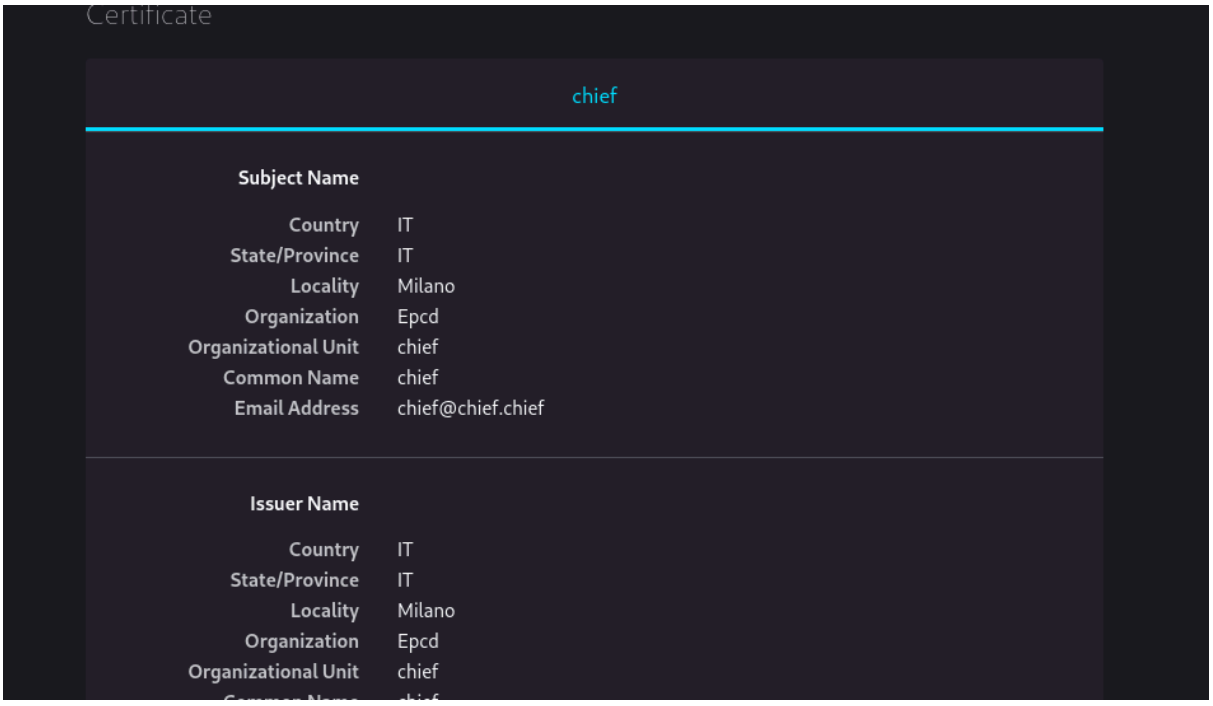
Provo a visitare https://epicode.internal da Browser - funziona!



SU KALI, MOZILLA MI FA ANCHE VEDERE IL CERTIFICATO CON DATI FARLOCCHI CHE AVEVO CREATO CON OPENSSL

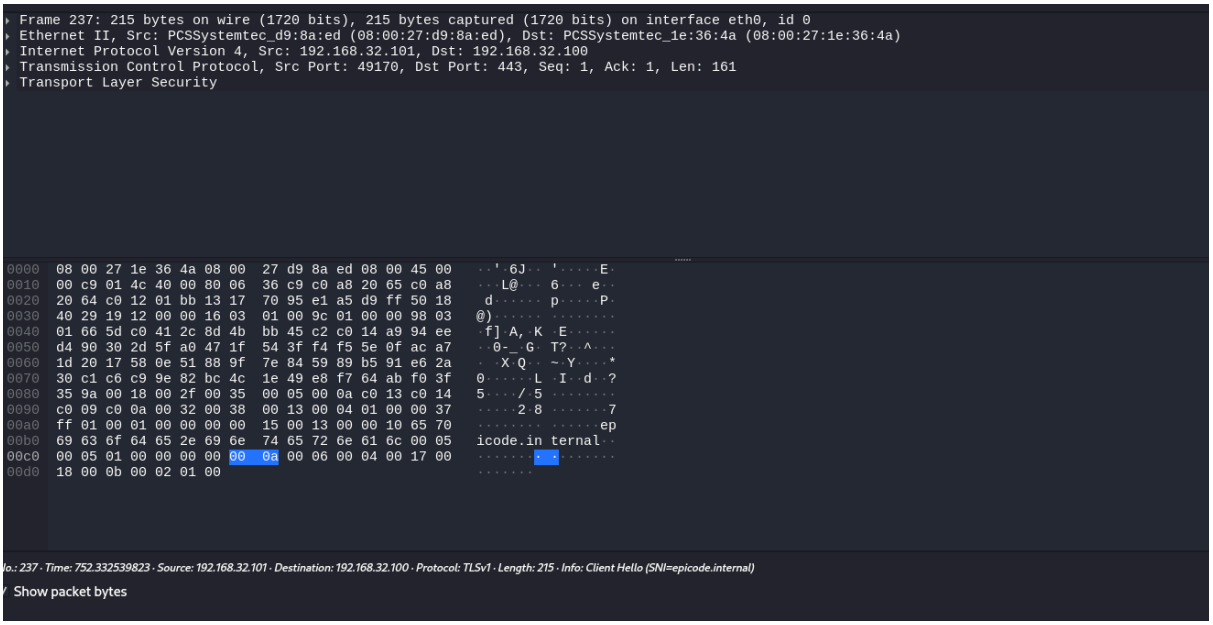
(organizzazione = epcd 😁)





Faccio partire la CATTURA Wireshark

Noto che in HTTPS LA COMUNICAZIONE, quindi il payload che esprime il contenuto del pacchetto è criptato nonostante i MAC address siano i medesimi. infatti il protocollo che Wireshark mi visualizza è il TLS che serve per trasportare dati criptati in https.


Frame 237: 215 bytes on wire (1720 bits), 215 bytes captured (1720 bits) on interface eth0, id 0
Ethernet II, Src: PCSSystemtec_d9:8a:ed (08:00:27:d9:8a:ed), Dst: PCSSystemtec_1e:36:4a (08:00:27:1e:36:4a)
Internet Protocol Version 4, Src: 192.168.32.101, Dst: 192.168.32.100
Transmission Control Protocol, Src Port: 49170, Dst Port: 443, Seq: 1, Ack: 1, Len: 161
Transport Layer Security
0000 08 00 27 1e 36 4a 08 00 27 d9 8a ed 08 00 45 00
0010 00 c9 01 4c 40 00 80 06 36 c9 c0 a8 20 65 c0 a8
0020 20 64 c0 12 01 bb 13 17 70 95 e1 a5 d9 ff 50 18
0030 40 29 19 12 00 00 16 03 01 00 9c 01 00 00 98 03
0040 01 66 5d c0 41 2c 8d 4b bb 45 c2 c0 14 a9 94 ee
0050 d4 90 30 2d 5f a0 47 1f 54 3f f4 f5 5e 0f ac a7
0060 1d 20 17 58 0e 51 88 9f 7e 84 59 89 b5 91 e6 2a
0070 30 c1 c6 c9 9e 82 bc 4c 1e 49 e8 f7 64 ab f0 3f
0080 35 9a 00 18 00 2f 00 35 00 05 00 0a c0 13 c0 14
0090 c0 09 c0 0a 00 32 00 38 00 13 00 04 01 00 00 37
00a0 ff 01 00 01 00 00 00 00 15 00 13 00 00 10 65 70
00b0 69 63 6f 64 65 2e 69 6e 74 65 72 6e 61 6c 00 05
00c0 00 05 01 00 00 00 00 0a 00 06 00 04 00 17 00
00d0 18 00 0b 00 02 01 00
icode.in ternal
o.: 237 · Time: 752.332539823 · Source: 192.168.32.101 · Destination: 192.168.32.100 · Protocol: TLSv1 · Length: 215 · Info: Client Hello (SNI=epicode.internal)
Show packet bytes