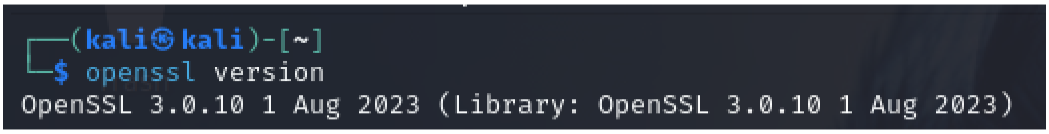
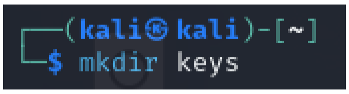
Checkpoint Secure Solution Implementation

- First launch Kali Linux machine open the terminal and check the openssl version : **openssl version**



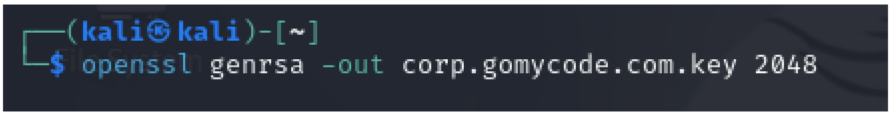
```
┌──(kali㉿kali)-[~]
└─$ openssl version
OpenSSL 3.0.10 1 Aug 2023 (Library: OpenSSL 3.0.10 1 Aug 2023)
```

- create directory to save keys : **mkdir keys**



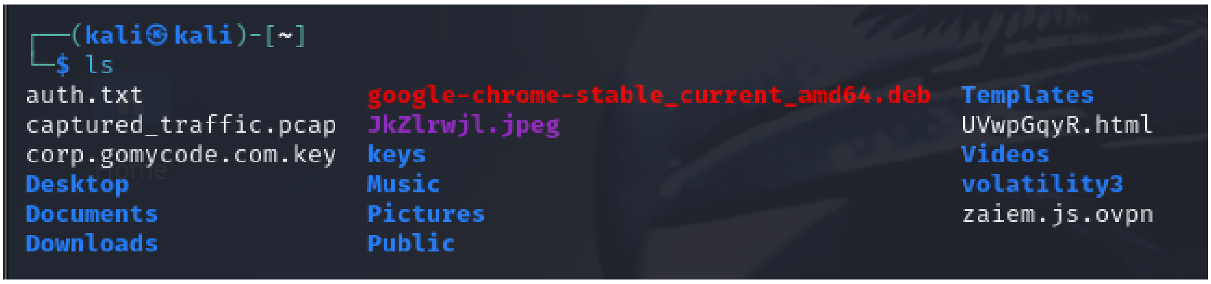
```
┌──(kali㉿kali)-[~]
└─$ mkdir keys
```

- generate asymmetric encryption keys: **openssl genrsa -out corp.gomycode.com.key 2048**



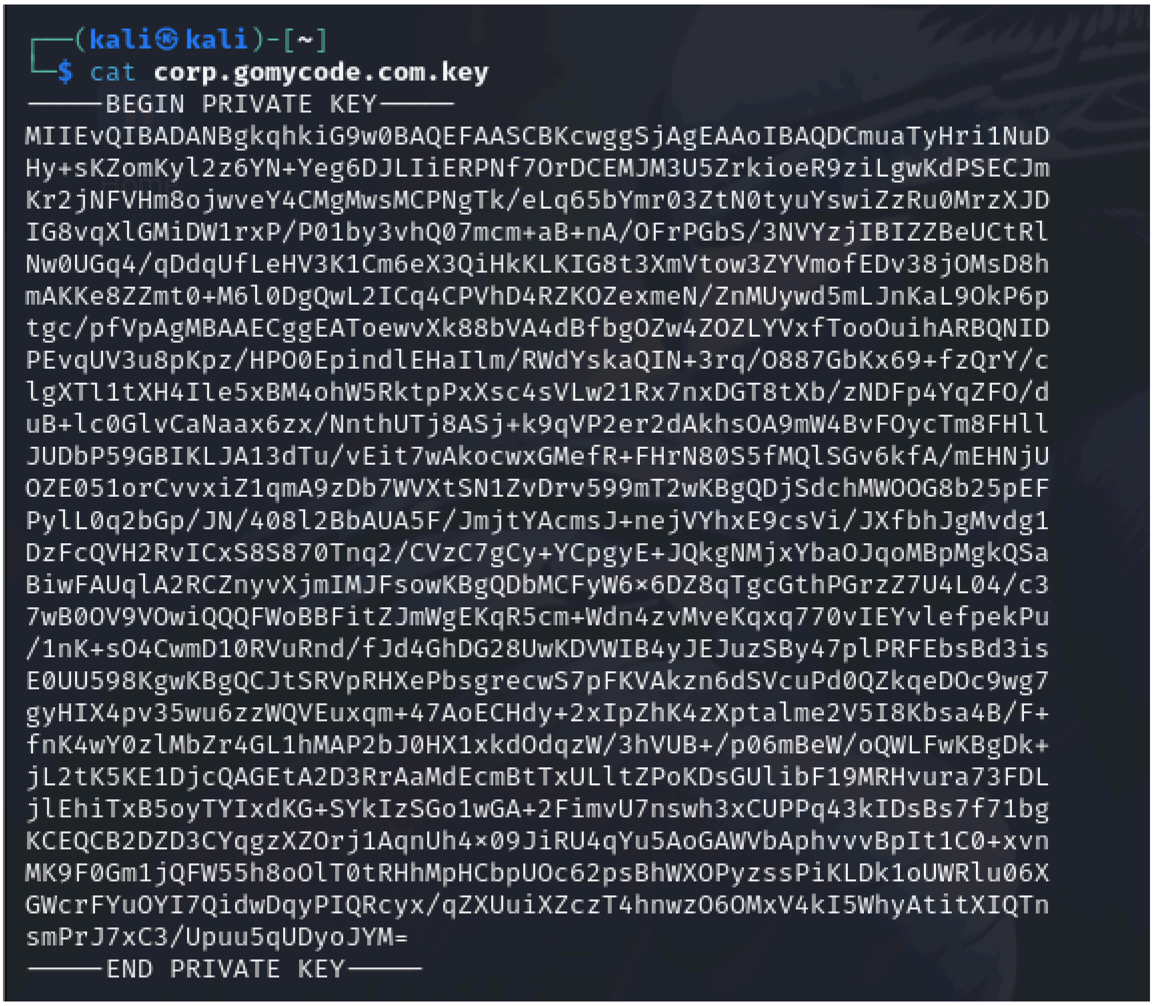
```
┌──(kali㉿kali)-[~]
└─$ openssl genrsa -out corp.gomycode.com.key 2048
```

- run **ls** to verify the creation of the file



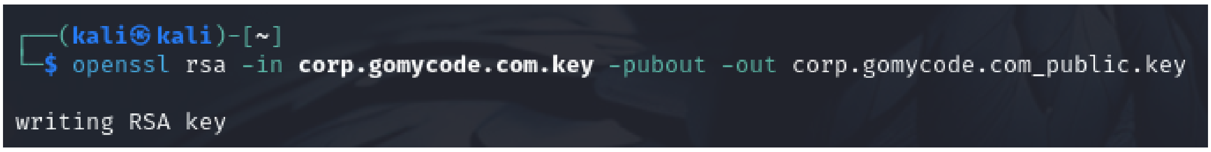
```
┌──(kali㉿kali)-[~]
└─$ ls
auth.txt               google-chrome-stable_current_amd64.deb  Templates
captured_traffic.pcap  JkZlrwjl.jpeg                           UVwpGqyR.html
corp.gomycode.com.key  keys                                    Videos
Desktop                Music                                   volatility3
Documents              Pictures                                zaiem.js.ovpn
Downloads              Public
```

- show the certification : **cat corp.gomycode.com.key**



```
┌──(kali㉿kali)-[~]
└─$ cat corp.gomycode.com.key
-----BEGIN PRIVATE KEY-----
MIIEvQIBADANBgkqhkiG9w0BAQEFAASCBKcwggSjAgEAAoIBAQDCmuaTyHri1NuD
Hy+sKZomKyl2z6YN+Yeg6DJLIiERPNf7OrDCEMJM3U5ZrkioeR9ziLgwKdPSECJm
Kr2jNFVHm8ojwveY4CMgMwsMCPNgTk/eLq65bYmr03ZtN0tyuYswiZzRu0MrzXJD
IG8vqXlGMiDW1rxP/P01by3vhQ07mcm+aB+nA/OFrPGbS/3NVYzjIBIZZBeUCtRl
Nw0UGq4/qDdqUfLeHV3K1Cm6eX3QiHkKLKIG8t3XmVtow3ZYVmofEDv38jOMsD8h
mAKKe8ZZmt0+M6l0DgQwL2ICq4CPVhD4RZKOZexmeN/ZnMUywd5mLJnKaL9OkP6p
tgc/pfVpAgMBAAECggEAToewvXk88bVA4dBfbgOZw4ZOZLYVxfTooOuihARBQNID
PEvqUV3u8pKpz/HPO0EpindlEHaIlm/RWdYskaQIN+3rq/O887GbKx69+fzQrY/c
lgXTl1tXH4Ile5xBM4ohW5RktpPxXsc4sVLw21Rx7nxDGT8tXb/zNDFp4YqZFO/d
uB+lc0GlvCaNaax6zx/NnthUTj8ASj+k9qVP2er2dAkhsOA9mW4BvFOycTm8FHll
JUDbP59GBIKLJA13dTu/vEit7wAkocwxGMefR+FHrN80S5fMQlSGv6kfA/mEHNjU
OZE051orCvvxiZ1qmA9zDb7WVXtSN1ZvDrv599mT2wKBgQDjSdchMWOOG8b25pEF
PylL0q2bGp/JN/408l2BbAUA5F/JmjtYAcmsJ+nejVYhxE9csVi/JXfbhJgMvdg1
DzFcQVH2RvICxS8S870Tnq2/CVzC7gCy+YCpgyE+JQkgNMjxYbaOJqoMBpMgkQSa
BiwFAUqlA2RCZnyvXjmIMJFsowKBgQDbMCFyW6x6DZ8qTgcGthPGrzZ7U4L04/c3
7wB0OV9VOwiQQQFWoBBFitZJmWgEKqR5cm+Wdn4zvMveKqxq770vIEYvlefpekPu
/1nK+sO4CwmD10RVuRnd/fJd4GhDG28UwKDVWIB4yJEJuzSBy47plPRFEbsBd3is
E0UU598KgwKBgQCJtSRVpRHXePbsgrecwS7pFKVAkzn6dSVcuPd0QZkqeDOc9wg7
gyHIX4pv35wu6zzWQVEuxqm+47AoECHdy+2xIpZhK4zXptalme2V5I8Kbsa4B/F+
fnK4wY0zlMbZr4GL1hMAP2bJ0HX1xkdOdqzW/3hVUB+/p06mBeW/oQWLFwKBgDk+
jL2tK5KE1DjcQAGEtA2D3RrAaMdEcmBtTxULltZPoKDsGUlibF19MRHvura73FDL
jlEhiTxB5oyTYIxdKG+SYkIzSGo1wGA+2FimvU7nswh3xCUPPq43kIDsBs7f71bg
KCEQCB2DZD3CYqgzXZOrj1AqnUh4x09JiRU4qYu5AoGAWVbAphvvvBpIt1C0+xvn
MK9F0Gm1jQFW55h8oOlT0tRHhMpHCbpUOc62psBhWXOPyzssPiKLDk1oUWRlu06X
GWcrFYuOYI7QidwDqyPIQRcyx/qZXUuiXZczT4hnwzO6OMxV4kI5WhyAtitXIQTn
smPrJ7xC3/Upuu5qUDyoJYM=
-----END PRIVATE KEY-----
```

- extract public key : **openssl rsa -in corp.gomycode.com.key -pubout -out corp.gomycode.com_public.key**



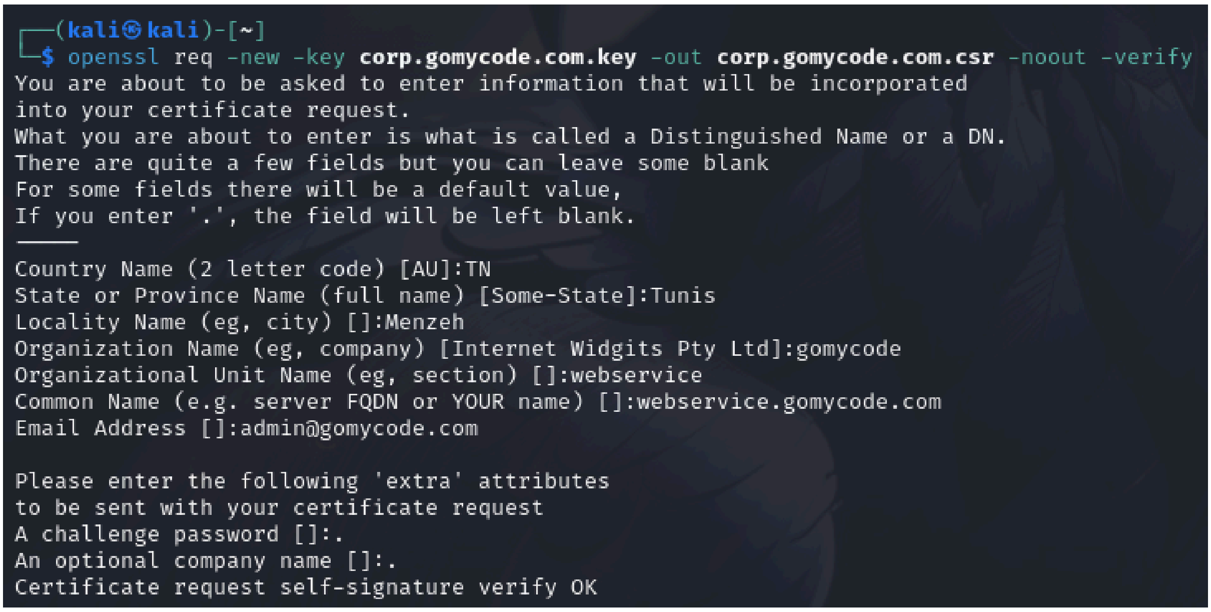
```
┌──(kali㉿kali)-[~]
└─$ openssl rsa -in corp.gomycode.com.key -pubout -out corp.gomycode.com_public.key

writing RSA key
```

- Generate a certificate signing request. Type the following command, then press ENTER:

openssl req -new -key corp.gomycode.com.key -out corp.gomycode.com.csr

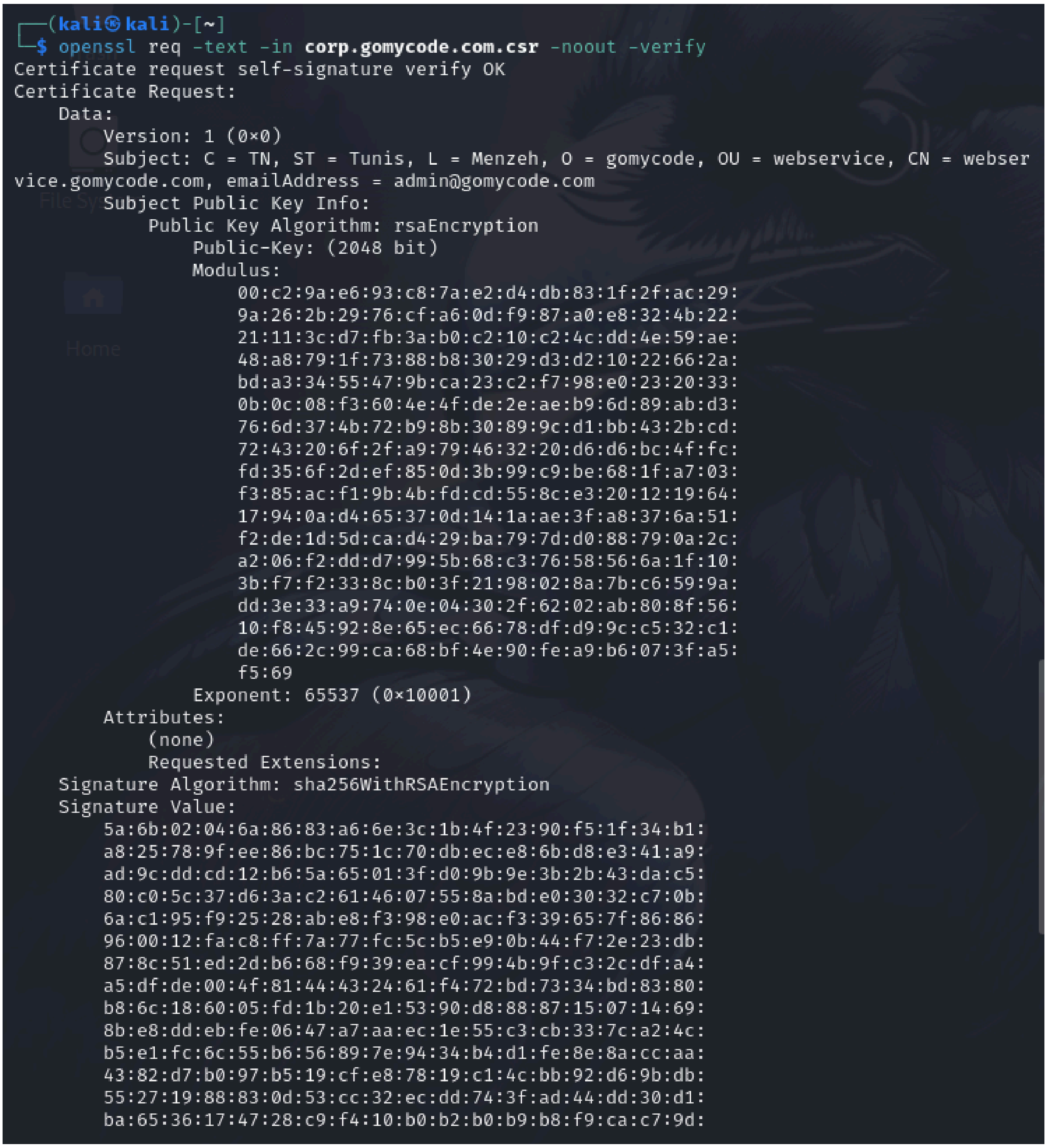
- fill the form like the following :
  https://i.imgur.com/e296Jyn.png



```
┌──(kali㉿kali)-[~]
└─$ openssl req -new -key corp.gomycode.com.key -out corp.gomycode.com.csr -noout -verify
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]:TN
State or Province Name (full name) [Some-State]:Tunis
Locality Name (eg, city) []:Menzeh
Organization Name (eg, company) [Internet Widgits Pty Ltd]:gomycode
Organizational Unit Name (eg, section) []:webservice
Common Name (e.g. server FQDN or YOUR name) []:webservice.gomycode.com
Email Address []:admin@gomycode.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:.
An optional company name []:.
Certificate request self-signature verify OK
```

- verify the certificate request : **openssl req -text -in corp.gomycode.com.csr -noout -verify**

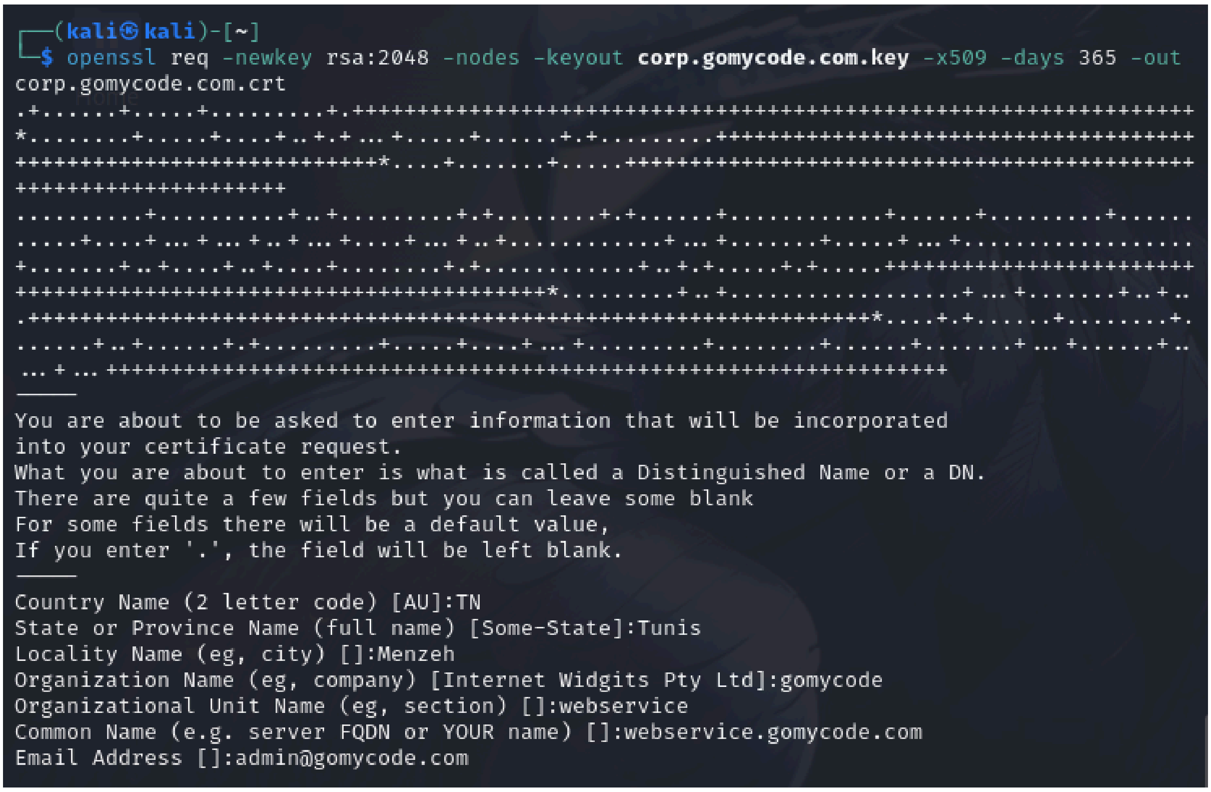


```
┌──(kali㉿kali)-[~]
└─$ openssl req -text -in corp.gomycode.com.csr -noout -verify
Certificate request self-signature verify OK
Certificate Request:
    Data:
        Version: 1 (0×0)
        Subject: C = TN, ST = Tunis, L = Menzeh, O = gomycode, OU = webservice, CN = webser
vice.gomycode.com, emailAddress = admin@gomycode.com
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:c2:9a:e6:93:c8:7a:e2:d4:db:83:1f:2f:ac:29:
                    9a:26:2b:29:76:cf:a6:0d:f9:87:a0:e8:32:4b:22:
                    21:11:3c:d7:fb:3a:b0:c2:10:c2:4c:dd:4e:59:ae:
                    48:a8:79:1f:73:88:b8:30:29:d3:d2:10:22:66:2a:
                    bd:a3:34:55:47:9b:ca:23:c2:f7:98:e0:23:20:33:
                    0b:0c:08:f3:60:4e:4f:de:2e:ae:b9:6d:89:ab:d3:
                    76:6d:37:4b:72:b9:8b:30:89:9c:d1:bb:43:2b:cd:
                    72:43:20:6f:2f:a9:79:46:32:20:d6:d6:bc:4f:fc:
                    fd:35:6f:2d:ef:85:0d:3b:99:c9:be:68:1f:a7:03:
                    f3:85:ac:f1:9b:4b:fd:cd:55:8c:e3:20:12:19:64:
                    17:94:0a:d4:65:37:0d:14:1a:ae:3f:a8:37:6a:51:
                    f2:de:1d:5d:ca:d4:29:ba:79:7d:d0:88:79:0a:2c:
                    a2:06:f2:dd:d7:99:5b:68:c3:76:58:56:6a:1f:10:
                    3b:f7:f2:33:8c:b0:3f:21:98:02:8a:7b:c6:59:9a:
                    dd:3e:33:a9:74:0e:04:30:2f:62:02:ab:80:8f:56:
                    10:f8:45:92:8e:65:ec:66:78:df:d9:9c:c5:32:c1:
                    de:66:2c:99:ca:68:bf:4e:90:fe:a9:b6:07:3f:a5:
                    f5:69
                Exponent: 65537 (0×10001)
        Attributes:
            (none)
            Requested Extensions:
    Signature Algorithm: sha256WithRSAEncryption
    Signature Value:
        5a:6b:02:04:6a:86:83:a6:6e:3c:1b:4f:23:90:f5:1f:34:b1:
        a8:25:78:9f:ee:86:bc:75:1c:70:db:ec:e8:6b:d8:e3:41:a9:
        ad:9c:dd:cd:12:b6:5a:65:01:3f:d0:9b:9e:3b:2b:43:da:c5:
        80:c0:5c:37:d6:3a:c2:61:46:07:55:8a:bd:e0:30:32:c7:0b:
        6a:c1:95:f9:25:28:ab:e8:f3:98:e0:ac:f3:39:65:7f:86:86:
        96:00:12:fa:c8:ff:7a:77:fc:5c:b5:e9:0b:44:f7:2e:23:db:
        87:8c:51:ed:2d:b6:68:f9:39:ea:cf:99:4b:9f:c3:2c:df:a4:
        a5:df:de:00:4f:81:44:43:24:61:f4:72:bd:73:34:bd:83:80:
        b8:6c:18:60:05:fd:1b:20:e1:53:90:d8:88:87:15:07:14:69:
        8b:e8:dd:eb:fe:06:47:a7:aa:ec:1e:55:c3:cb:33:7c:a2:4c:
        b5:e1:fc:6c:55:b6:56:89:7e:94:34:b4:d1:fe:8e:8a:cc:aa:
        43:82:d7:b0:97:b5:19:cf:e8:78:19:c1:4c:bb:92:d6:9b:db:
        55:27:19:88:83:0d:53:cc:32:ec:dd:74:3f:ad:44:dd:30:d1:
        ba:65:36:17:47:28:c9:f4:10:b0:b2:b0:b9:b8:f9:ca:c7:9d:
```

- generate a sel-signed certificate :

openssl req -newkey rsa:2048 -nodes -keyout corp.gomycode.com.key -x509 -days 365 -out corp.gomycode.com.crt

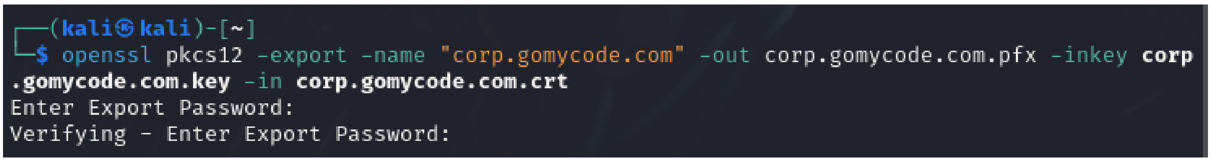
- as usual fill the form



```
┌──(kali㉿kali)-[~]
└─$ openssl req -newkey rsa:2048 -nodes -keyout corp.gomycode.com.key -x509 -days 365 -out
corp.gomycode.com.crt
.+......+.....+.........+.+++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
*........+.....+....+..+.+...+.....+......+.+.........+++++++++++++++++++++++++++++++++++++
++++++++++++++++++++++++++++*....+.......+.....++++++++++++++++++++++++++++++++++++++++++++
+++++++++++++++++++++
..........+..........+..+.........+.+........+.+......+............+......+.........+......
.....+....+...+...+..+...+....+...+..+............+...+.......+.....+...+..................
+.......+..+....+..+....+........+.+...........+..+.+.....+.+.....+++++++++++++++++++++++++
++++++++++++++++++++++++++++++++++++++++++*.........+..+.................+...+.......+..+..
.+++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++*....+.+......+........+.
......+..+......+.+.........+.....+....+...+.........+........+......+.......+...+.......+..
...+...+++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
─────
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]:TN
State or Province Name (full name) [Some-State]:Tunis
Locality Name (eg, city) []:Menzeh
Organization Name (eg, company) [Internet Widgits Pty Ltd]:gomycode
Organizational Unit Name (eg, section) []:webservice
Common Name (e.g. server FQDN or YOUR name) []:webservice.gomycode.com
Email Address []:admin@gomycode.com
```

- convert the keys format :

openssl pkcs12 -export -name "corp.gomycode.com" -out corp.gomycode.com.pfx -inkey corp.gomycode.com.key -in corp.gomycode.com.crt



```
┌──(kali㉿kali)-[~]
└─$ openssl pkcs12 -export -name "corp.gomycode.com" -out corp.gomycode.com.pfx -inkey corp
.gomycode.com.key -in corp.gomycode.com.crt
Enter Export Password:
Verifying - Enter Export Password:
```