

Checkpoint: Secure Solution Implementation II & Operations

Instructions

- First launch Kali Linux machine open the terminal and check the openssl version : **openssl version**
- create directory to save keys : **mkdir keys**
- generate asymmetric encryption keys: **openssl genrsa -out corp.gomycode.com.key 2048**
- run **ls** to verify the creation of the file
- show the certification : **cat corp.gomycode.com.key**
- extract public key : **openssl rsa -in corp.gomycode.com.key -pubout -out corp.gomycode.com_public.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

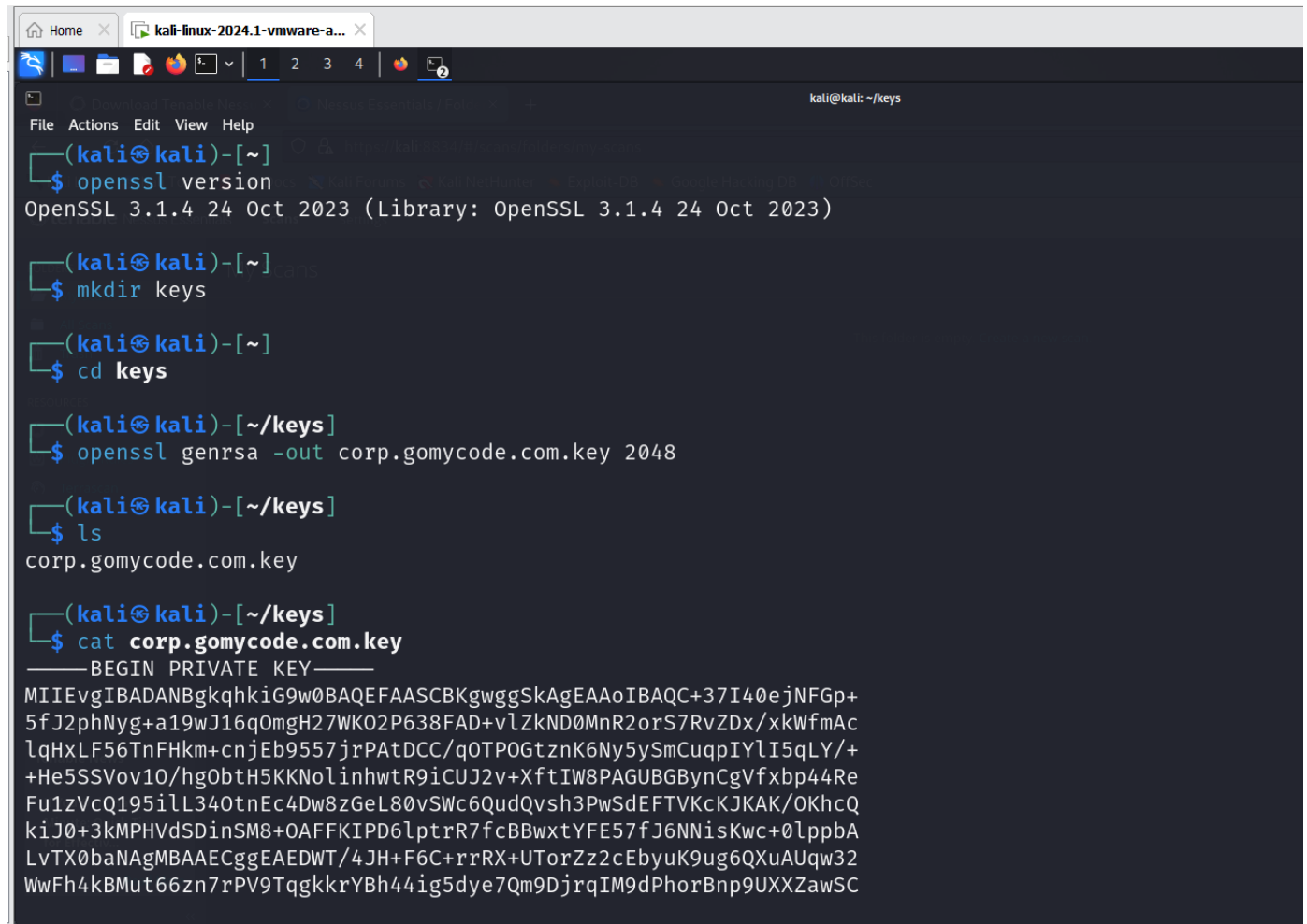
- fill the form like the following :
<https://i.imgur.com/e296Jyn.png>
- verify the certificate request : **openssl req -text -in corp.gomycode.com.csr -noout -verify**
- generate a self-signed certificate :

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

- as usual fill the form
- 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

****SOLUTION**



```
kali@kali: ~/keys
$ openssl version
OpenSSL 3.1.4 24 Oct 2023 (Library: OpenSSL 3.1.4 24 Oct 2023)

(kali@kali)-[~/keys]
$ mkdir keys

(kali@kali)-[~/keys]
$ cd keys

(kali@kali)-[~/keys]
$ openssl genrsa -out corp.gomycode.com.key 2048

(kali@kali)-[~/keys]
$ ls
corp.gomycode.com.key

(kali@kali)-[~/keys]
$ cat corp.gomycode.com.key
-----BEGIN PRIVATE KEY-----
MIIEvgIBADANBgkqhkiG9w0BAQEFAASCBAgEAAoIBAQC+37I40ejNFGp+
5fJ2phNyg+a19wJ16q0mgH27WK02P638FAD+vLZkND0MnR2orS7RvZDx/xkWfmAc
lqHxLF56TnFHkm+cnjEb9557jrPATDCC/q0TP0GtznK6Ny5ySmCuqpIYlI5qLY/+
+He5SSVov10/hg0btH5KKNoIinhwtr9iCUJ2v+XftIW8PAGUBGBynCgVfxbp44Re
Fu1zVcQ195illL340tnEc4Dw8zGeL80vSWc6QudQvsh3PwSdEFTVKcKJKAK/OKhcQ
kiJ0+3kMPHVdSDinSM8+OAFKIPD6lptrR7fcBBwxtYFE57fJ6NNisKwc+0lppbA
LvTX0baNagMBAAECggEAEDWT/4JH+F6C+rrRX+UTorZz2cEbyuK9ug6QXuAUqw32
WwFh4kBMut66zn7rPV9TqgkkrYBh44ig5dye7Qm9DjrQIM9dPhorBnp9UXXZawSC
```

```
Home X kalilinux-2024.1-vmware-a... X
File Actions Edit View Help
kali@kali: ~/keys
lqHxLF56TnFHkm+cnjEb9557jrPAtdDCC/qOTPOGtznK6Ny5ySmCuqpIYlI5qLY/+
+He5SSVov10/hgObtH5KKNoLinhwtR9iCUJ2v+XftIW8PAGUBGBynCgVfxbp44Re
Fu1zVcQ195ilL340tnEc4Dw8zGeL80vSWc6QudQvsh3PwSdEFTVKcKJKAK/OKhcQ
kiJ0+3kMPHVdSDinSM8+0AFFKIPD6lptrR7fcBBwxtYFE57fJ6NNisKwc+0lppbA
LvTX0baNAgMBAAECggEAEDWT/4JH+F6C+rrRX+UTorZz2cEbyuK9ug6QXuAUqw32
WwFh4kBMut66zn7rPV9TqgkkrYBh44ig5dye7Qm9DjrQIM9dPhorBnp9UXXZawSC
WCWCw6a4bZeqI4k7HwaU9lBS7tZyz66F23vDQw9kp2QUgyAo30ixLuAQn7jYoLB
fF+ZmyiU1omr26fN5APURGkYYns/hkEdc7d72dHvSdHsvxnag83ZRdtB5Nco5YDo
+SMCQLXDKHcPgEVD7SgKvJtcqSo6Z+yaA9TS92mLLa1pJFYnKhu15/NUuDiTrnM
j67yKxZXPI1A3tLGzw596VhHXXYZWBl9yAAbY89BIQKBgQDuU/c4Fy67ksw5VaCh
DleF4og/jTgaPou1xHNpeIADE8p6599CE09P3E5kqrjdg/few8/MX30V255cFdfT
R3vrFntyAicWvVkiUI6R3mMRxD2kobVqobZnG137LbqmAjnnHn+Mg4K3QEyb6bLc
4sIZ1mxeaHgsFE5bELUAZQt2fQKBgQDNBu/Xml3PGsUAAbQ5JRHrr5etlTJpjaJ
0YF/RiqACPuS2S7zH681IwPKLkgsMD0uMW3JvMusQJwv96arHCGzam/9dVbAXRp5
Afti8pz53ZlCxcaqx7yWA6eCsQ0RfEZ7Smq7gKIDJ9p1KhcnYVNM5NZfati8Yptr
EDzU0xZtUQKBgB0gA8FGC/7+RJjpHvICTa3d7jqd/nIunJI9DMGh6Tr3CzKT7Z08
UBKZYLcqeqbgPsVpdpaKQNYp/b1RKgv222zyVWmsKNYdk6jRd2raG49LRSE+ZdY/
JvRYwtZ0UzAAa6UT9BBu7eWJJROUrrgRuhjAPIQZDj6MyLqWQxhmQM1dAoGBAlk/
zk/Bg4dQibVC10NZMkMA6gyGJOorTKuD5/zmmhoLg7ugjsJP25AobhEtFjs07wig
0rEX5hPg4P6aRja0+YhR4JRjhBnVRckWWFyEF//QEN17M9E1HZlx/dWiuat13X0i
tSNry3cMeF+qwzdIugJdNbELKn+0nPb0ufGM3euxAoGBAOhDvghiS6xx9TrlSjXd
qtIBTrtvr1yyajFqpfq603ZGHsxpwn3FT+r0cCW92XHSm/EL75opr8Ldj0semgsy
yk8ERCLo8FIzbMn2WPTRco1n05CAKMCOPIMKvoI61r97nJvp+rsxT6oeKEhjX4PA
J070lr50kRFOn6JcMy874gdd
-----END PRIVATE KEY-----
(kali@kali)-[~/keys]
$
```

```
Home X kali-linux-2024.1-vmware-a... X
File Actions Edit View Help
kali@kali: ~/keys
END PRIVATE KEY-----
(kali@kali)-[~/keys]
$ openssl rsa -in corp.gomymcode.com.key -pubout -out corp.gomymcode.com_public.key
writing RSA key
(kali@kali)-[~/keys]
$ ls
corp.gomymcode.com.key  corp.gomymcode.com_public.key
(kali@kali)-[~/keys]
$ cat corp.gomymcode.com
cat: corp.gomymcode.com: No such file or directory
(kali@kali)-[~/keys]
$ cat corp.gomymcode.com_public.key
-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAvt+yONHozRRqfuXydqYT
coPmtfcCdeqjpoB9u1ijtj+t/BQA/r5WZDQ9DJ0dqK0u0b2Q8f8ZF5gHJah8Sxe
ek5xR5JvnJ4xG/eee46zWLQwgv6jkzzhrc5yujcuckpgrqqSGJS0ai2P/vh3uUkl
aL9Tv4YDm7R+SijaJYp4cLUfYglCdr/l37SFvDwBlARgcpwoFX8W6e0EXhbtclXE
NfeYpS9+DrZxHOA8PMxni/NL0lnOkLnUL7Idz8EnRBU1SnCiSgCvzioXEJIidPt5
DDx1XUg4p0jPPjgBRsIdw+paba0e33AQcMbWBROe3yejTYrCsHPtJaaWwC7019G2
jQIDAQAB
-----END PUBLIC KEY-----
(kali@kali)-[~/keys]
$
```

```
kali@kali: ~/keys
$ openssl req -new -key corp.gomycode.com.key -out corp.gomycode.com.csr
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]:NG
State or Province Name (full name) [Some-State]:Eniola
Locality Name (eg, city) []:Lagos
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 []:kali
An optional company name []:ohmycode

(kali@kali)-[~/keys]
$
```

```
kali@kali: ~/keys
$ openssl req -text -in corp.gomycode.com.csr -noout -verify
Certificate request self-signature verify OK
Certificate Request:
Data:
  Version: 1 (0x0)
  Subject: C = NG, ST = Eniola, L = Lagos, O = gomycode, OU = webservice, CN = webservice.gomycode.com, emailAddress = admin@gomycode.com
  Subject Public Key Info:
    Public Key Algorithm: rsaEncryption
    Public-Key: (2048 bit)
    Modulus:
      00:be:df:b2:38:d1:e8:cd:14:6a:7e:e5:f2:76:a6:
      13:72:83:e6:b5:f7:02:75:ea:a3:a6:80:7d:bb:58:
      a3:b6:3f:ad:fc:14:00:fe:be:56:64:34:3d:0c:9d:
      1d:a8:ad:2e:d1:bd:90:f1:ff:19:16:7e:60:1c:96:
      a1:f1:2c:5e:7a:4e:71:47:92:6f:9c:9e:31:1b:f7:
      9e:7b:8e:b3:c0:b4:30:82:fe:a3:93:3c:e1:ad:ce:
      72:ba:37:2e:72:4a:60:ae:aa:92:18:94:8e:6a:2d:
      8f:fe:f8:77:b9:49:25:68:bf:53:bf:86:03:9b:b4:
      7e:4a:28:da:25:8a:78:70:b5:1f:62:09:42:76:bf:
      e5:df:b4:85:bc:3c:01:94:04:60:72:9c:28:15:7f:
      16:e9:e3:84:5e:16:ed:73:55:c4:35:f7:98:a5:2f:
      7e:0e:b6:71:1c:e0:3c:3c:cc:67:8b:f3:4b:d2:59:
      ce:90:b9:d4:2f:b2:1d:cf:c1:27:44:15:35:4a:70:
      a2:4a:00:af:ce:2a:17:10:92:22:74:fb:79:0c:3c:
      75:5d:48:38:a7:48:cf:3e:38:01:45:28:83:c3:ea:
      5a:6d:ad:1e:df:70:10:70:c6:d6:05:13:9e:df:27:

```

Activate Windows
Go to Settings to activate Windows.

- `corp.gomymcode.com.csr` (certificate signing request)
- `corp.gomymcode.com.crt` (certificate)
- `corp.gomymcode.com.pfx` (converted format)