

## **MINI PROJECT**

### **352 CIS Lab (Information Security)**

**Marks: 7 Marks**

**Name: Sarah Fahad Akala** **ID : 445804653**

**Name: Lama Ahmed Alfusili** **ID : 445803877**

**Name: Bsmah Ibrahim Al Amer** **ID : 444806632**

#### **Instructions:**

- 1- Group activity: Max 3 students.
  - 2- Use SEED Ubuntu and Kali Linux to solve the questions.
  - 3- Due Date: 9<sup>th</sup> May 2025
  - 4- Take screenshots for your work.
  - 5- For each task and submit Online
- 

#### **Question 1**

**( 3.5 Marks)**

**Create a certificate for the following server: [SEEDPKILab2020.com](http://SEEDPKILab2020.com) by apply the following steps:**

## 1. Become a Certificate Authority CA

```

seed@VM: ~
[05/09/26]seed@VM:~$ cp /usr/lib/ssl/openssl.cnf ./
[05/09/26]seed@VM:~$ mkdir demoCA && cd demoCA
[05/09/26]seed@VM:~/demoCA$ mkdir certs crl newcerts
[05/09/26]seed@VM:~/demoCA$ ls
certs crl newcerts
[05/09/26]seed@VM:~/demoCA$ touch index.txt serial
[05/09/26]seed@VM:~/demoCA$ ls
certs crl index.txt newcerts serial
[05/09/26]seed@VM:~/demoCA$ echo 1000 > serial
[05/09/26]seed@VM:~/demoCA$ cd ..
[05/09/26]seed@VM:~$ openssl req -new -x509 -keyout ca.key -out ca.crt -config o
penssl.cnf
Generating a RSA private key
.....+++++
...+++++
writing new private key to 'ca.key'
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
-----
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]:SA
State or Province Name (full name) [Some-State]:Aseer
Locality Name (eg, city) []:Abha
Organization Name (eg, company) [Internet Widgits Pty Ltd]:KKU
Organizational Unit Name (eg, section) []:IS
Common Name (e.g. server FQDN or YOUR name) []:GROUP2
Email Address []:
[05/09/26]seed@VM:~$ openssl x509 -in ca.crt -text -noout
Certificate:

```

```

seed@VM: ~
Email Address []:
[05/09/26]seed@VM:~$ openssl x509 -in ca.crt -text -noout
Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number:
      0a:ad:02:b8:45:0e:fc:3c:3e:65:64:a3:09:05:61:8f:b4:38:7e:91
    Signature Algorithm: sha256WithRSAEncryption
    Issuer: C = SA, ST = Aseer, L = Abha, O = KKU, OU = IS, CN = GROUP2
    Validity
      Not Before: May  9 11:37:32 2026 GMT
      Not After : Jun  8 11:37:32 2026 GMT
    Subject: C = SA, ST = Aseer, L = Abha, O = KKU, OU = IS, CN = GROUP2
    Subject Public Key Info:
      Public Key Algorithm: rsaEncryption
      RSA Public-Key: (2048 bit)
      Modulus:
        00:ea:64:6a:11:fb:2c:54:0c:8c:5e:64:b6:2a:4e:
        af:46:22:51:97:4f:8d:d9:62:0b:50:5e:e8:98:d5:
        00:43:ef:b6:f4:18:f0:9e:88:dc:de:20:28:b0:5a:
        fe:00:35:18:3c:e3:4d:21:52:d5:a9:84:6e:8f:54:
        84:d7:7e:c1:fb:dc:98:f4:cc:0c:d4:2d:13:40:56:
        f5:d5:c6:c1:6d:e6:d9:0a:54:02:2b:92:5a:ca:d3:
        a3:be:e1:73:f5:be:bc:ac:e5:15:98:2e:20:61:9a:
        4b:f2:ee:52:f9:7b:99:b3:14:f4:0a:7a:f2:b1:20:
        47:14:cb:ae:aa:eb:c6:5f:0d:77:c5:7a:4c:fe:e4:
        38:95:3f:ff:72:03:b6:ab:38:e8:a2:09:35:b4:bc:
        55:49:4e:ba:0e:bf:93:d6:81:6c:52:67:c6:85:b2:
        dd:83:9f:92:d1:f9:1e:7a:9c:84:f1:88:dd:09:97:
        bc:30:49:2d:87:33:88:2c:a1:41:35:10:85:7a:82:
        b5:5e:80:fd:b7:a4:47:ac:29:19:05:cc:11:94:04:
        20:05:4f:cf:da:68:d9:4a:4c:47:28:31:ca:b5:c1:
        bf:e3:5f:02:06:4d:98:f5:31:a2:a2:fe:a6:56:39:
        91:38:c6:ab:43:e4:70:f8:18:f9:02:46:85:a9:6b:
        46:4d

```

## Classification: Personal

```
20:05:4f:cf:da:68:d9:4a:4c:47:28:31:ca:b5:c1:
bf:e3:5f:02:06:4d:98:f5:31:a2:a2:fe:a6:56:39:
91:38:c6:ab:43:e4:70:f8:18:f9:02:46:85:a9:6b:
46:4d
Exponent: 65537 (0x10001)
X509v3 extensions:
X509v3 Subject Key Identifier:
    79:DD:F5:A0:DA:AE:51:A4:A2:12:67:F8:94:51:23:98:CE:01:22:60
X509v3 Authority Key Identifier:
    keyid:79:DD:F5:A0:DA:AE:51:A4:A2:12:67:F8:94:51:23:98:CE:01:22:60

X509v3 Basic Constraints: critical
CA:TRUE
Signature Algorithm: sha256WithRSAEncryption
e2:9f:7c:d3:b3:c0:85:95:2e:82:3a:e1:f6:25:98:d4:2b:f0:
d7:04:0b:b1:31:0d:f4:94:22:69:91:2f:10:3d:01:92:0a:de:
64:e7:74:a3:5d:40:08:94:12:ff:de:d1:bc:59:9a:08:db:61:
ce:c2:e2:ca:41:a3:5b:90:db:a8:f4:a8:a5:7f:7e:7b:55:06:
ef:d9:a3:64:48:bb:c6:da:44:9a:6e:a6:e3:93:ce:f6:8d:cf:
d0:c7:62:2d:ee:99:ed:f5:c9:74:9a:0a:6f:15:91:55:1d:33:
3d:4a:86:b2:7d:b6:4b:bd:e6:da:e3:60:0b:3e:c6:26:0a:99:
e0:87:f2:7a:4f:89:47:83:a4:2f:a7:63:e2:67:6d:9d:15:07:
d5:2c:cd:be:b9:23:df:05:95:76:1d:5a:a4:1f:5b:c2:08:3e:
73:44:02:60:b0:31:e3:11:dc:62:64:fd:18:7b:c3:ca:c6:eb:
50:b1:d6:ca:47:93:5f:05:bd:e0:8f:b9:1a:35:77:b0:e0:22:
96:cb:5c:85:81:c6:44:f9:ab:82:2f:b6:8f:b2:09:21:af:01:
b9:8f:65:57:a8:b2:54:ed:95:a8:7b:5b:3f:8d:ee:95:ce:b4:
a6:9b:96:54:b2:54:f4:4d:fb:6d:bb:db:46:7e:ca:32:cc:a7:
01:34:46:f9
[05/09/26]seed@VM:~$
```

## 2. Create a certificate for seedworkshop2019.com

```
seed@VM: ~
[05/09/26]seed@VM:~$ openssl genrsa -aes128 -out server.key 1024
Generating RSA private key, 1024 bit long modulus (2 primes)
.....+++++
.....+++++
e is 65537 (0x010001)
Enter pass phrase for server.key:
Verifying - Enter pass phrase for server.key:
[05/09/26]seed@VM:~$ openssl req -new -key server.key -out server.csr -config op
enssl.cnf
Enter pass phrase for server.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]:SA
State or Province Name (full name) [Some-State]:Aseer
Locality Name (eg, city) []:Abha
Organization Name (eg, company) [Internet Widgits Pty Ltd]:KKU
Organizational Unit Name (eg, section) []:IS
Common Name (e.g. server FQDN or YOUR name) []:SEEDWorkshop2019.com
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
[05/09/26]seed@VM:~$ openssl ca -in server.csr -out server.crt -cert ca.crt -key
file ca.key -config openssl.cnf
Using configuration from openssl.cnf
```

```

seed@VM: ~
Enter pass phrase for ca.key:
Check that the request matches the signature
Signature ok
Certificate Details:
  Serial Number: 4096 (0x1000)
  Validity
    Not Before: May  9 12:04:16 2026 GMT
    Not After : May  9 12:04:16 2027 GMT
  Subject:
    countryName           = SA
    stateOrProvinceName   = Aseer
    organizationName      = KKU
    organizationalUnitName = IS
    commonName            = SEEDWorkshop2019.com
  X509v3 extensions:
    X509v3 Basic Constraints:
      CA:FALSE
    Netscape Comment:
      OpenSSL Generated Certificate
    X509v3 Subject Key Identifier:
      BA:3C:39:C7:83:00:21:51:D7:8E:F3:75:B4:83:BD:7B:C1:2A:CD:A2
    X509v3 Authority Key Identifier:
      keyid:80:8F:8B:48:AE:61:14:07:72:1E:F7:82:F6:21:27:B8:86:A6:A6:D
0

Certificate is to be certified until May  9 12:04:16 2027 GMT (365 days)
Sign the certificate? [y/n]:y

1 out of 1 certificate requests certified, commit? [y/n]
Write out database with 1 new entries
Data Base Updated

```

```

seed@VM: ~
1 out of 1 certificate requests certified, commit? [y/n]
Write out database with 1 new entries
Data Base Updated
[05/09/26]seed@VM:~$ openssl x509 -in server.crt -text -noout
Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number: 4096 (0x1000)
    Signature Algorithm: sha256WithRSAEncryption
    Issuer: C = SA, ST = Aseer, L = Abha, O = KKU, OU = SI, CN = GROUP2
    Validity
      Not Before: May  9 12:04:16 2026 GMT
      Not After : May  9 12:04:16 2027 GMT
    Subject: C = SA, ST = Aseer, O = KKU, OU = IS, CN = SEEDWorkshop2019.com
    Subject Public Key Info:
      Public Key Algorithm: rsaEncryption
      RSA Public-Key: (1024 bit)
      Modulus:
        00:9f:9a:d0:cc:95:b8:2d:0a:0f:42:50:b1:e4:0a:
        67:36:54:e3:97:6e:2c:63:a9:5f:5c:43:5a:f1:43:
        02:42:14:10:73:44:df:6f:65:79:f1:48:63:21:95:
        61:0d:e7:48:2b:17:a5:49:db:7e:03:e8:d4:09:1d:
        bd:cd:d4:fb:9b:a6:29:2b:ac:87:c6:bf:a7:9e:1e:
        2a:aa:de:ea:62:f1:2b:1f:ff:6d:20:e3:85:0b:7f:
        1b:56:90:0b:3b:e6:71:d1:9e:ad:60:5b:19:a2:54:
        1a:e2:9a:14:9a:c9:ce:e4:d9:f8:94:f3:05:00:8f:
        76:32:4e:25:b4:ea:71:0f:53
      Exponent: 65537 (0x10001)
    X509v3 extensions:
      X509v3 Basic Constraints:
        CA:FALSE

```

```
seed@VM: ~
1b:56:90:0b:3b:e6:71:d1:9e:ad:60:5b:19:a2:54:
1a:e2:9a:14:9a:c9:ce:e4:d9:f8:94:f3:05:00:8f:
76:32:4e:25:b4:ea:71:0f:53
Exponent: 65537 (0x10001)
X509v3 extensions:
X509v3 Basic Constraints:
CA:FALSE
Netscape Comment:
OpenSSL Generated Certificate
X509v3 Subject Key Identifier:
BA:3C:39:C7:83:00:21:51:D7:8E:F3:75:B4:83:BD:7B:C1:2A:CD:A2
X509v3 Authority Key Identifier:
keyid:80:8F:8B:48:AE:61:14:07:72:1E:F7:82:F6:21:27:B8:86:A6:A6:D

Signature Algorithm: sha256WithRSAEncryption
91:d3:73:bb:9b:89:14:ef:7f:0a:30:97:a9:62:34:d7:b8:f8:
5f:45:ca:4f:d4:b6:55:bd:b2:56:4b:43:1f:03:83:81:56:b8:
11:fd:d8:7a:2d:22:71:8b:81:b8:cd:46:17:78:07:07:08:ba:
f6:eb:dc:0d:1c:9f:b3:1f:41:8a:b4:41:ba:65:fd:e4:04:0f:
a8:b1:e8:9f:6c:fe:5c:9a:e7:a4:a7:d0:ee:b2:39:5b:d1:a4:
68:1c:23:83:5c:74:be:3e:4a:e5:63:97:c7:12:cf:bd:7d:32:
21:fe:d4:43:e5:1c:52:5b:62:38:de:c2:35:71:ea:ae:16:26:
a6:dc:ab:1e:d1:c8:dd:5a:e3:6d:8a:29:61:fb:5b:0c:84:38:
ea:d9:58:5e:95:65:be:74:4c:a9:cc:95:6d:b1:cd:08:a1:d0:
9e:76:1c:1c:24:42:4c:ba:3b:87:b8:c1:36:85:d5:b3:82:20:
43:04:12:7d:4f:06:73:e7:b9:52:8d:db:c5:83:64:02:65:91:
b9:e2:ca:93:be:6f:79:d4:d7:4e:33:58:46:45:4a:c5:80:51:
d7:a8:40:63:dd:77:fb:9f:20:db:55:61:67:0b:e9:62:14:bf:
b1:c3:eb:da:d6:75:77:5f:8c:27:57:51:d0:88:9c:90:dd:32:
71:af:ca:fa
[05/09/26]seed@VM:~$
```

The image shows a file manager interface with a sidebar on the left containing 'Recent', 'Starred', 'Home', 'Desktop', 'Documents', 'Downloads', 'Music', 'Pictures', 'Videos', 'Trash', 'demoCA', and 'Other Locations'. The main area displays a file named '1000.pem'. A preview window titled '1000.pem' is open, showing the following certificate details:

**SEEDWorkshop2019.com**  
Identity: SEEDWorkshop2019.com  
Verified by: GROUP2  
Expires: 05/09/2027

**Details**

**Subject Name**  
C (Country): SA  
ST (State): Aseer  
O (Organization): KKU  
OU (Organizational Unit): IS  
CN (Common Name): SEEDWorkshop2019.com

**Issuer Name**  
C (Country): SA  
ST (State): Aseer  
L (Locality): Abha  
O (Organization): KKU  
OU (Organizational Unit): SI  
CN (Common Name): GROUP2

**Issued Certificate**  
Version: 3  
Serial Number: 10 00  
Not Valid Before: 2026-05-09  
Not Valid After: 2027-05-09

**Certificate Fingerprints**  
SHA1: 8C BE A8 BB 64 AD 33 03 D4 4A BA 35 D1 C4 1F E6 94 7B 2F 35  
MD5: B7 36 56 D8 C4 54 66 07 B5 09 28 F9 78 A3 EA 3B

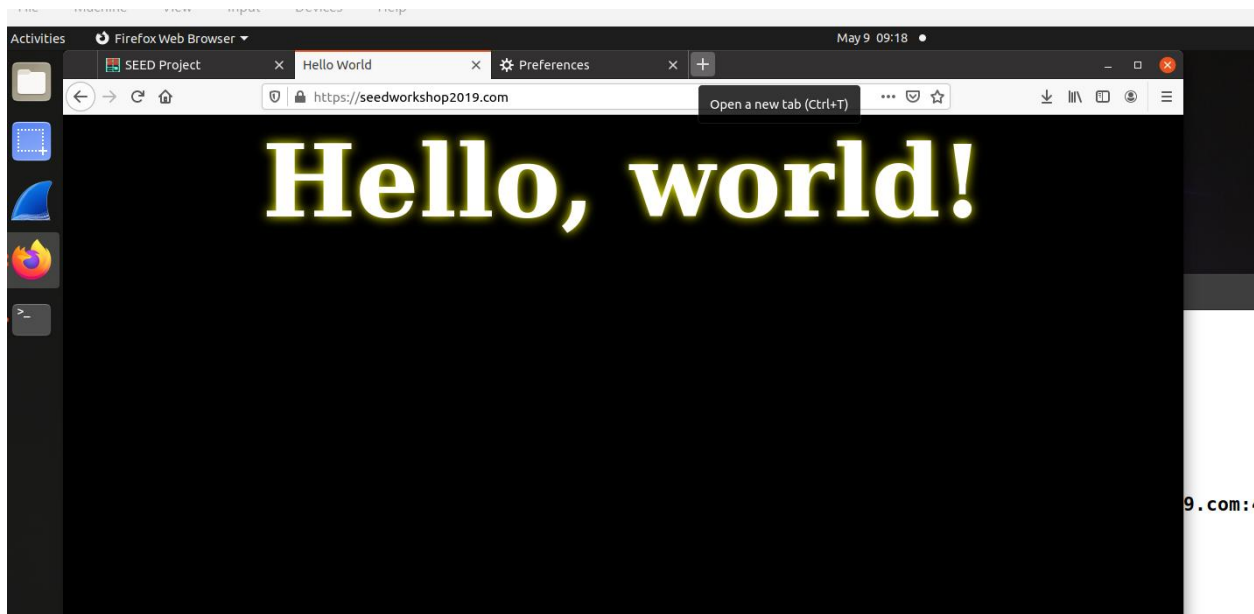
**Public Key Info**  
Key Algorithm: RSA  
Key Parameters: 05 00  
Key Size: 1024  
Key SHA1 Fingerprint: D5 67 0E A6 DC 4B 4B CB 8C 7F F8 65 A6 D1 48 07 10 04 61 2E

Buttons: Close, Import

### 3. Deploying Certificate in an Apache-Based HTTPS Website

*Note: Submit ca.crt and server.crt that must include you Group number*

```
seed@VM: ~  
[05/09/26]seed@VM:~$ deploy_https.sh  
mkdir: cannot create directory '/var/www/SEEDWorkshop2019/': File exists  
AH00558: apache2: Could not reliably determine the server's fully qualified domain name, using 127.0.1.1. Set the 'ServerName' directive globally to suppress this message  
Syntax OK  
Considering dependency setenvif for ssl:  
Module setenvif already enabled  
Considering dependency mime for ssl:  
Module mime already enabled  
Considering dependency socache_shmcb for ssl:  
Module socache_shmcb already enabled  
Module ssl already enabled  
Site seed-ssl already enabled  
Enter passphrase for SSL/TLS keys for SEEDWorkshop2019.com:443 (RSA): (press TAB  
****  
[05/09/26]seed@VM:~$ ls -l /var/www/SEEDWorkshop2019/  
total 12  
-rw-r--r-- 1 root root 225 May 9 08:55 index.html  
-rw-r--r-- 1 root root 3684 May 9 08:55 server.crt  
-r----- 1 root root 986 May 9 08:55 server.key  
[05/09/26]seed@VM:~$ /var/www/SEEDWorkshop2019  
bash: /var/www/SEEDWorkshop2019: Is a directory  
[05/09/26]seed@VM:~$
```



Certificate

GROUP2

**Subject Name**

Country SA  
State/Province Aseer  
Locality Abha  
Organization KKU  
Organizational Unit SI  
Common Name GROUP2

**Issuer Name**

Country SA  
State/Province Aseer  
Locality Abha  
Organization KKU  
Organizational Unit SI  
Common Name GROUP2

**Validity**

Not Before 5/9/2026, 7:56:57 AM (Eastern Daylight Time)  
Not After 6/8/2026, 7:56:57 AM (Eastern Daylight Time)

**Public Key Info**

Algorithm RSA  
Key Size 2048  
Exponent 65537  
Modulus B6:E9:C0:DD:22:C0:92:F6:67:6C:E8:D6:C0:FC:A9:7F:66:8E:CE:2B:26:AD:0B:A...

**Miscellaneous**

Serial Number 57:42:82:16:96:82:3E:0E:52:69:9A:08:57:8B:B8:FC:AF:55:C5:DF  
Signature Algorithm SHA-256 with RSA Encryption  
Version 3  
Download [PEM \(cert\)](#) [PEM \(chain\)](#)

**Fingerprints**

SHA-256 CC:8D:65:D9:6A:D0:7E:C1:4A:FF:42:A4:E8:DE:DF:59:7E:0A:C0:D5:19:45:B3:F...  
SHA-1 DF:D1:7C:39:3F:15:47:A3:3D:65:D3:D7:71:2E:3D:F9:7F:D2:9C:D7

**Basic Constraints**

Certificate Authority Yes

**Subject Key ID**

Key ID 80:8F:8B:48:AE:61:14:07:72:1E:F7:82:F6:21:27:B8:86:A6:A6:D0

**Authority Key ID**

Key ID 80:8F:8B:48:AE:61:14:07:72:1E:F7:82:F6:21:27:B8:86:A6:A6:D0

Certificate

SEEDWorkshop2019.com

GROUP2

**Subject Name**

Country SA  
 State/Province Aseer  
 Organization KKU  
 Organizational Unit IS  
 Common Name SEEDWorkshop2019.com

**Issuer Name**

Country SA  
 State/Province Aseer  
 Locality Abha  
 Organization KKU  
 Organizational Unit SI  
 Common Name GROUP2

**Validity**

Not Before 5/9/2026, 8:04:16 AM (Eastern Daylight Time)  
 Not After 5/9/2027, 8:04:16 AM (Eastern Daylight Time)

**Public Key Info**

Algorithm RSA  
 Key Size 1024  
 Exponent 65537  
 Modulus 9F:9A:D0:CC:95:B8:2D:0A:0F:42:50:B1:E4:0A:67:36:54:E3:97:6E:2C:63:A9:5F:...

**Miscellaneous**

Serial Number 10:00  
 Signature Algorithm SHA-256 with RSA Encryption  
 Version 3  
 Download [PEM \(cert\)](#) [PEM \(chain\)](#)

**Fingerprints**

SHA-256 28:4C:30:5A:F9:35:E0:CA:D0:8C:CC:7F:9D:ED:04:D9:58:C9:64:57:3F:F4:57:A2...  
 SHA-1 8C:BE:A8:BB:64:AD:33:03:D4:4A:BA:35:D1:C4:1F:E6:94:7B:2F:35

**Basic Constraints**

Certificate Authority No

**Subject Key ID**

Key ID BA:3C:39:C7:83:00:21:51:D7:8E:F3:75:B4:83:BD:7B:C1:2A:CD:A2

**Authority Key ID**

Key ID 80:8F:8B:48:AE:61:14:07:72:1E:F7:82:F6:21:27:B8:86:A6:A6:D0

Question 2:

**(3.5 Marks)**

**Network Scanning and MITM Attacks**

1. Network scanning using nmap tool.
2. Network package analysis tool such as Wireshark.
3. Perform MITM attack using ARP Cache Poisoning Attack tool such as Ettercap, and analyze the result using Wireshark.

*Note: Show the username and password as group # as credentials that you have used on the Victim Side*

