Seng 360 Assignment 4

[redacted]

Public Key Infrastructure (PKI)

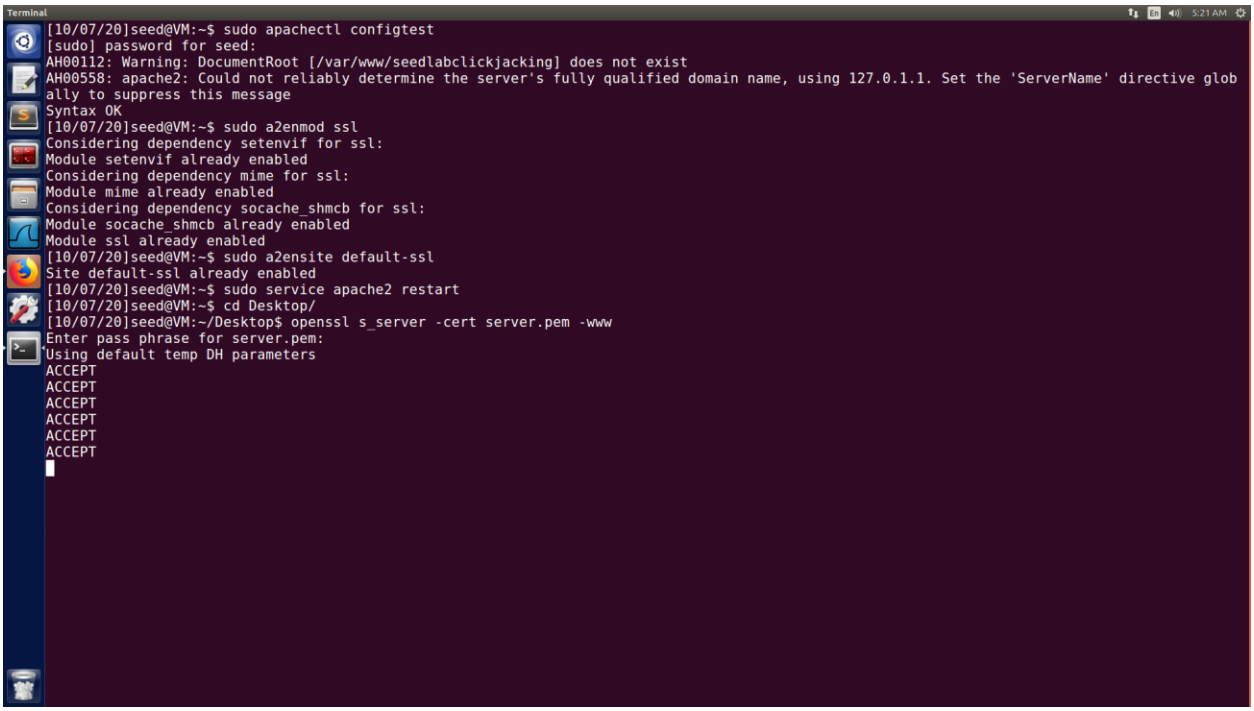
Please describe in detail the steps that you have taken, the contents that you add to Apache's configuration file, and the screenshots of the final outcome showing that you can successfully browse the HTTPS site.

The HTTPS server setup based on Apache was done using the steps below. The Apache server, was already installed on our VM.

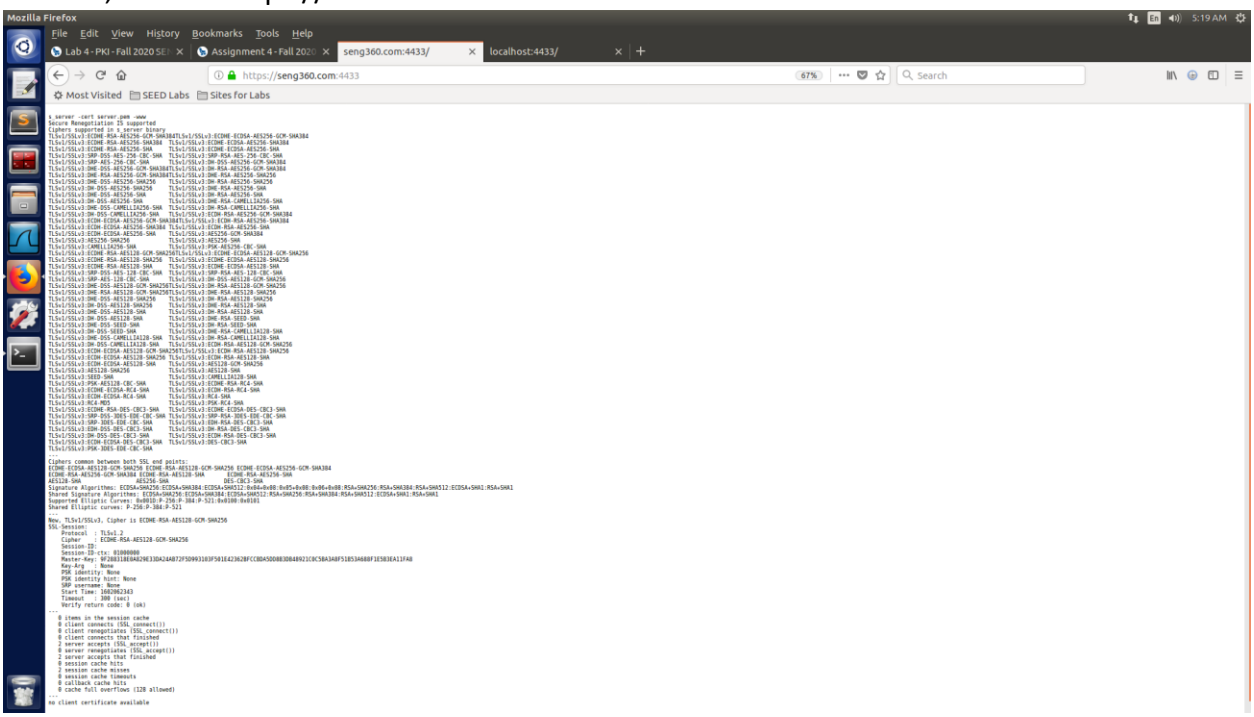
1. To configure the Apache server we need to setup the configuration files in order to provide details about where to get the private key and certificates. To provide the directory where a website's files are stored we use a VirtualHost file. The VirtualHost file is located in the /etc/apache2/. First we locate that directory.
2. To add an HTTPS website, we need to add a VirtualHost entry to the default-ssl.conf file located in the directory above. This file is shown below. Is the name of the website and DocumentRoot points to the websites files.

```
1 <VirtualHost *:443>
2     ServerName SENG360.com
3     DocumentRoot /var/www/SENG360
4     DirectoryIndex index.html
5
6     SSSLEngine On
7     SSLCertificateFile /home/seed/Desktop/server.pem
8     SSLCertificateKeyFile /home/seed/Desktop/server.key
9 </VirtualHost>
```

3. After the default-ssl.conf file is created we need to run a series of commands to enable SSL. We need the password Apache used for encrypting the private key. These commands are shown in the terminal screenshot below.



4. Now all the traffic between the browser and the server will be encrypted. To access the website, we visit https://SENG360.com: 4433. This is shown below.



As you can see in the final outcome the site can be browsed and is secure.

With everything set up, now visit the target real website, and see what your browser would say. Please explain what you have observed.

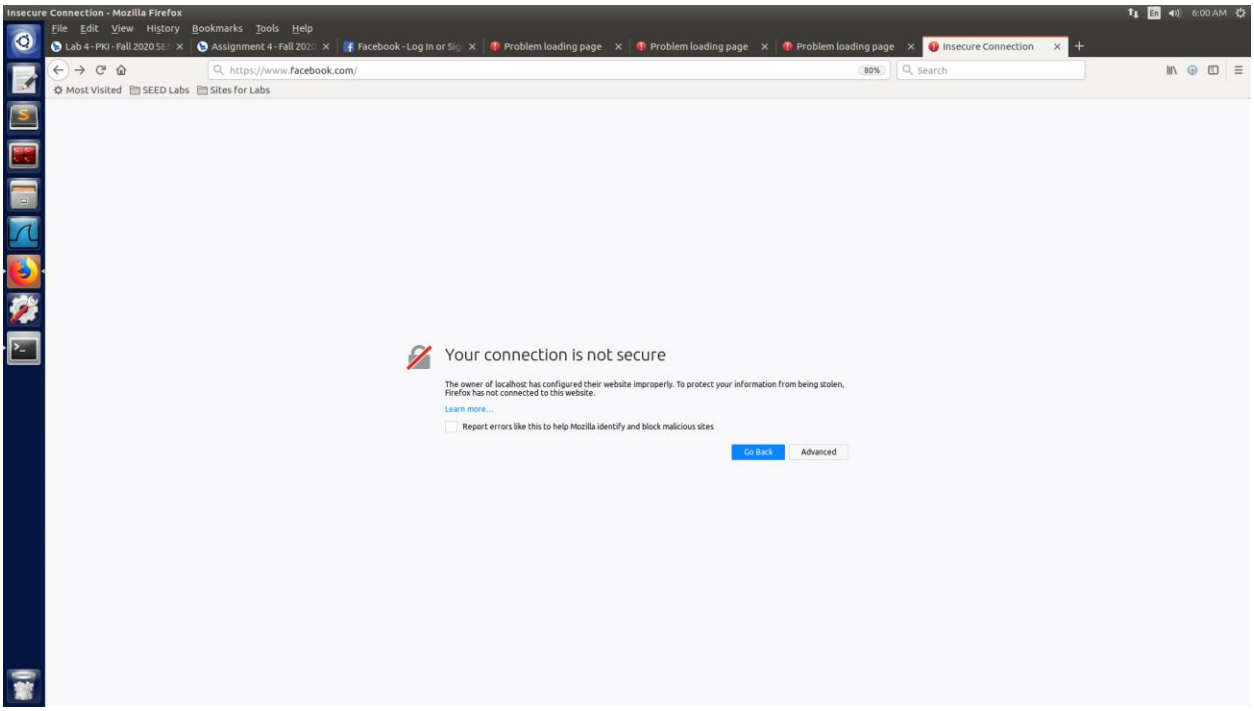
The website I chose to use was Facebook. To achieve that, we modify the VirtualHost entry in the Apache's SSL configuration file. This is shown below the only difference is the ServerName is the name of the fake website, but the rest of the configuration is the same above.

```
<VirtualHost *:443>
    ServerName Facebook.com
    DocumentRoot /var/www/SENG360
    DirectoryIndex index.html

    SSSLEngine On
    SSLCertificateFile /home/seed/Desktop/server.pem
    SSLCertificateKeyFile /home/seed/Desktop/server.key
</VirtualHost>
```

To get the user to the site we modify the victim's machine's /etc/hosts file to redirect the user to the IP address of the malicious server instead of the site they wish to visit.

```
127.0.0.1   localhost
127.0.1.1   VM
127.0.0.1   Facebook.com

# The following lines are desirable for IPv6 capable hosts
::1     ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
127.0.0.1       User
127.0.0.1       Attacker
127.0.0.1       Server
127.0.0.1       www.SeedLabSQLInjection.com
127.0.0.1       www.xsslabelgg.com
127.0.0.1       www.csrflabelgg.com
127.0.0.1       www.csrflabattacker.com
127.0.0.1   www.repackagingattacklab.com
127.0.0.1   www.seedlabclickjacking.com
```

After the setup of the Apache server to impersonate the website we can see the browser identifies the website as not trusted. It then warns the user with more details regarding the website.



Please design an experiment to show that the attacker can successfully launch MITM attacks on any HTTPS website. You can use the same setting created in Task 5, but this time, you need to demonstrate that the MITM attack is successful, i.e., the browser will not raise any suspicion when the victim tries to visit a website but land in the MITM attacker's fake website.

After stealing the private key we are able to create a certificate for the fake website this is done by creating a request and signing it ourselves using the stolen key this is done using the commands below.

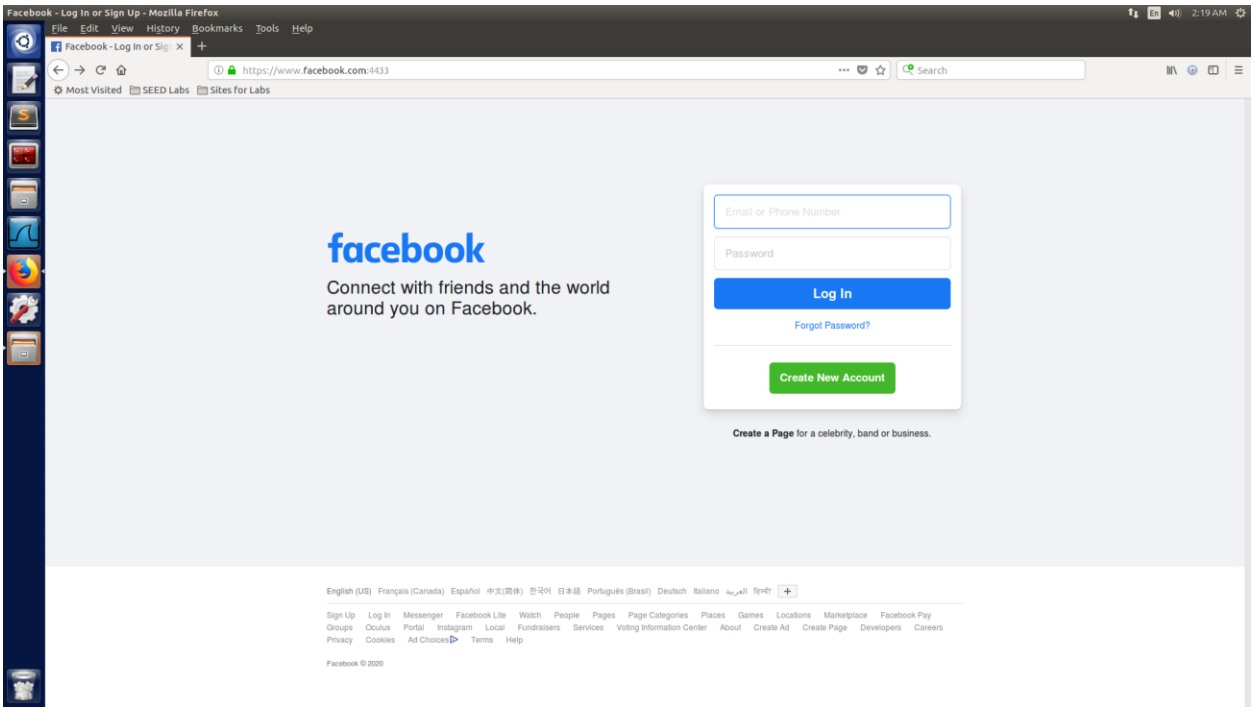
$ openssl req -new -key server.key -out server.csr -config openssl.cnf

$ openssl ca -in server.csr -out server.crt -cert ca.crt -keyfile ca.key -config openssl.cnf

This produces the certificate file shown below.

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 4096 (0x1000)
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=CA, ST=British Columbia, L=Victoria, O=am signing, CN=Amaan/emailAddress=amaanmakhani@gmail.com
        Validity
            Not Before: Oct  6 08:35:49 2020 GMT
            Not After : Oct  6 08:35:49 2021 GMT
        Subject: C=CA, ST=British Columbia, L=Victoria, O=Facebook.com, CN=Facebook.com
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (1024 bit)
                Modulus:
                    00:b5:a3:4a:4f:e2:18:82:14:14:ac:96:7e:b4:7a:
                    91:14:27:15:11:0a:bb:8f:4d:89:7a:16:9b:ce:5d:
                    d9:71:a8:4b:a5:29:e0:c3:dc:e7:87:95:75:9d:78:
                    38:fc:1c:2e:dd:56:68:55:c0:01:1f:9b:4c:15:39:
                    48:4b:11:f8:9e:94:53:f2:50:ae:9f:ae:46:30:3d:
                    20:1a:93:36:f8:ea:0b:11:fb:20:6f:15:17:89:1a:
                    ba:65:5f:46:8f:83:d8:e3:b5:bb:38:8d:3a:d3:40:
                    bd:5e:9f:b7:5f:d4:76:17:45:2b:84:f8:d2:3d:2a:
                    49:44:aa:f5:a6:44:b4:fd:6b
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            Netscape Comment:
                OpenSSL Generated Certificate
            X509v3 Subject Key Identifier:
                BB:BB:62:9B:53:9A:CE:3E:F6:7D:95:30:93:10:71:5C:1C:DD:ED:A6
            X509v3 Authority Key Identifier:
                keyid:97:2C:1C:EF:31:51:1C:94:82:D0:8E:7D:E4:13:EE:8B:5B:C8:63:83

    Signature Algorithm: sha256WithRSAEncryption
         1f:94:81:3a:9e:f2:d8:f1:31:83:72:c9:80:e2:3c:c4:50:3a:
         be:f2:2f:57:b4:c9:1e:10:ac:05:c5:38:5f:97:06:74:5e:51:
         2f:9a:7b:71:11:a8:15:0d:08:3f:f6:46:e6:46:81:fc:75:f7:
         6b:90:64:8d:d4:22:95:bb:bb:2a:2c:f3:9a:ec:0b:1a:ee:b5:
         d7:d5:fe:0e:cf:6a:45:c6:68:b5:1a:33:56:4c:10:48:1f:52:
         3e:5b:6d:60:e2:8e:e0:89:1d:e8:d3:6f:b6:20:6d:7d:c3:69:
         90:16:e9:85:bc:be:da:46:83:6f:30:6f:44:39:c3:41:ce:f2:
         95:d7:f7:c0:df:8e:a1:e9:f5:91:35:d7:1e:57:07:26:db:74:
         56:99:30:48:2f:77:a0:43:4d:e0:1a:a4:6f:2e:dc:20:14:b2:
         32:b9:87:b6:34:c2:85:c6:53:a6:9f:e8:4d:f4:c8:0e:ce:2b:
         79:ed:e6:df:2c:29:ea:ba:65:d7:b7:c7:5f:e4:84:6e:33:f5:
         37:6d:8d:27:b0:60:a2:89:fc:cb:55:d7:9e:9b:d3:75:51:dc:
         7f:ee:fb:a8:7c:7c:b2:db:eb:f4:74:a7:ef:66:c1:fd:b3:91:
         a9:9d:37:3d:11:f6:d2:d9:0b:6e:d9:d1:5e:47:84:04:85:01:
         97:07:7b:9e
-----BEGIN CERTIFICATE-----
MIIDYjCCAkqgAwIBAgICEAAwDQYJKoZIhvcNAQELBQAwgYcxCzAJBgNVBAYTAkNB
MRkwFwYDVQQIDBBCcml0aXNoIENvbHVtYmlhMREwDwYDVQQHDAhWaWN0b3JpYTET
MBEGA1UECgwKYW0gc2lnbmluZzEOMAwGA1UEAwwFQW1hYW4xJTAjBgkqhkiG9w0B
CQEWFmFtYWFubWFraGFuaUBnbWFpbC5jb20wHhcNMjAxMDA2MDgzNTQ5WhcNMjEx
MDA2MDgzNTQ5WjBnMQswCQYDVQQGEwJDQTEZMBcGA1UECAwQQnJpdGlzaCBDb2x1
bWJpYTERMA8GA1UEBwwIVmljdG9yaWExFDASBgNVBAoMC1NFTkczNjAuY29tMRQw
EgYDVQQDDAtTRU5HMzYwLmNvbTCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEA
taNKT+IYghQUrJZ+tHqRFCcVEQq7j02Jehabzl3ZcahLpSngw9znh5V1nXq4/Bwu
3VZoVcABH5tMFTlISxH4npRT8lCun65GMD0gGpM2+OoLEfsgbxUXiRq6ZV9Gj4PY
47W7OI0600C9Xp+3X9R2F0UrhPjSPSpJRKrlpkS0/WsCAwEAAaN7MHkwCQYDVR0T
BAIwADAsBglghkgBhvhCAQ0EHxYdT3BlblNTTCBHZW5lcmF0ZWQgQ2VydGlmaWNh
dGUwHQYDVR0OBBYEFLu7YptTms4+9n2VMJMQcVwc3e2mMB8GA1UdIwQYMBaAFJcs
HO8xURyUgtCOfeQT7otbyGODMA0GCSqGSIb3DQEBCwUAA4IBAQAflIE6nvLY8TGD
csmA4jzEUDq+8i9XtMkeEKwFxThflwZ0XlEvmntxEagVDQg/9kbmRoH8dfdrkGSN
1CKVu7sqLPOa7Asa7rXX1f4Oz2pFxmi1GjNWTBBIH1I+W21g4o7giR3o02+2IG19
w2mQFumFvL7aRoNvMG9EOcNBzvKV1/fA346h6fWRNdceVwcm23RWmTBIL3egQ03g
GqRvLtwgFLIyuYe2NMKFxlOmn+hN9MgOzit57ebfLCnqumXXt8df5IRuM/U3bY0n
sGCiifzLVdeem9N1Udx/7vuofHyy2+v0dKfvZsH9s5GpnTc9EfbS2Qtu2dFeR4QE
hQGXB3ue
-----END CERTIFICATE-----
```

Once this file is added assuming the browser trusts certificates from this CA the website will not be flagged as a insecure one as there is belief that the certificate was signed properly. This trusted website is shown below.


Facebook - Log In or Sign Up - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Facebook - Log In or Sig
https://www.facebook.com:4433
Search
Most Visited
SEED Labs
Sites for Labs
facebook
Connect with friends and the world around you on Facebook.
Email or Phone Number
Password
Log In
Forgot Password?
Create New Account
Create a Page for a celebrity, band or business.
English (US) Français (Canada) Español 中文(简体) 한국어 日本語 Português (Brasil) Deutsch Italiano العربية हिन्दी
Sign Up Log In Messenger Facebook Lite Watch People Pages Page Categories Places Games Locations Marketplace Facebook Pay
Groups Oculus Portal Instagram Local Fundraisers Services Voting Information Center About Create Ad Create Page Developers Careers
Privacy Cookies Ad Choices Terms Help
Facebook © 2020