Taha Jawaid **Assignment 3** **21k-3881**

Task 1: Becoming A Certificate Authority:

- Set up an OpenSSL configuration file to define directories for certificates and keys.
- Create a self-signed root CA certificate, which will act as a trusted CA.
- Verify the certificate details to ensure it is properly created.

```
Activities  Terminal  Oct 30 09:51
seed@VM: ~
[10/30/24]seed@VM:~$ cp /usr/lib/ssl/openssl.cnf ./myCA_openssl.cnf
[10/30/24]seed@VM:~$ nano myCA_openssl.cnf
[10/30/24]seed@VM:~$ mkdir -p demoCA/certs demoCA/crl demoCA/newcerts demoCA/private
[10/30/24]seed@VM:~$ touch demoCA/index.txt
[10/30/24]seed@VM:~$ echo 1000>demoCA/serial

[10/30/24]seed@VM:~$ openssl req -x509 -newkey -rsa:4096 -sha256 -days 3650 \
req: Use -help for summary.
[10/30/24]seed@VM:~$ ir             = ./demoCA              #>
ir: command not found
[10/30/24]seed@VM:~$ certs           = $dir/certs            #>
certs: command not found
[10/30/24]seed@VM:~$ crl_dir         = $dir/crl              #>
crl_dir: command not found
[10/30/24]seed@VM:~$ database        = $dir/index.txt^C
[10/30/24]seed@VM:~$ openssl req -x509 -newkey -rsa:4096 -sha256 -days 3650 \
req: Use -help for summary.
[10/30/24]seed@VM:~$ -keyout ca.key -out ca.crt\
> -subj "/CN=www.modelCA.com/O=model CA LTD./C=US" \
> -passout pass:dees
-keyout: command not found
[10/30/24]seed@VM:~$ openssl version
OpenSSL 1.1.1f  31 Mar 2020
[10/30/24]seed@VM:~$ openssl req -x509 -newkey -rsa:4096 -sha256 -days 3650 \
req: Use -help for summary.
[10/30/24]seed@VM:~$ openssl req-x509 -newkey -rsa:4096 -sha256 -days 3650 \
Invalid command 'req-x509'; type "help" for a list.
[10/30/24]seed@VM:~$ openssl -req -x509 -newkey -rsa:4096 -sha256 -days 3650 \
Invalid command '-req'; type "help" for a list.
[10/30/24]seed@VM:~$ openssl req -x509 -newkey -rsa:4096 -sha256 -days 3650 \
req: Use -help for summary.
[10/30/24]seed@VM:~$ openssl genpkey -algorithm RSA -out ca.key -aes256 -pass pass:dees -pkeyopt rsa_keygen_bits:4096
```

```
req: Use -help for summary.
[10/30/24]seed@VM:~$ openssl genpkey -algorithm RSA -out ca.key -aes256 -pass pass:dees -pkeyopt rsa_keygen_bits:4096
............++++
................++++
[10/30/24]seed@VM:~$ openssl req -x509 -new -key ca.key -out ca.crt -days 3650 -subj "/CN=www.modelCA.com/O=Model CA LTD./C=US" -passin pass:
dees
[10/30/24]seed@VM:~$ openssl x509 -in ca.crt -text -noout
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            61:db:77:86:2b:f0:50:8a:80:94:f7:8d:5d:9a:45:bd:3b:d2:08:ca
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: CN = www.modelCA.com, O = Model CA LTD., C = US
        Validity
            Not Before: Oct 30 13:35:33 2024 GMT
            Not After : Oct 28 13:35:33 2034 GMT
        Subject: CN = www.modelCA.com, O = Model CA LTD., C = US
Right Ctrl
```

```
            X509v3 Basic Constraints: critical
                CA:TRUE
    Signature Algorithm: sha256WithRSAEncryption
         92:10:82:f7:66:56:a2:bb:fe:4e:88:ab:2c:f2:af:3d:5b:77:
         c7:9e:47:f8:2d:e9:46:79:bb:4f:2f:4a:15:02:35:c6:ca:5a:
         fb:17:24:f8:9e:9c:6e:f5:c2:e2:5d:b4:aa:08:5e:98:67:cc:
         13:44:97:3f:fb:cb:a9:31:41:74:6b:87:e6:f3:c2:9f:11:10:
         93:29:b5:2f:29:ea:7c:23:b8:79:4c:28:73:ce:a9:8e:27:fc:
         6d:3f:5e:5d:39:9d:d6:c3:73:08:36:81:f9:2d:1e:99:2d:52:
         5d:d2:82:ae:81:62:5f:7a:09:ff:3b:9c:b0:29:79:07:93:93:
         91:70:3a:e0:64:90:c2:ec:d5:64:64:da:f6:67:c2:0d:55:8b:
         1b:36:59:e5:b2:a8:5a:df:7c:4b:7a:2d:d7:bb:14:00:8f:f5:
         41:9e:3d:f4:4a:2e:0c:ce:13:5b:6c:6d:b9:9b:82:7b:bc:e5:
         33:9f:0e:c8:64:5d:25:29:b5:e5:08:17:bc:64:0d:fb:1c:84:
         0c:47:ea:fe:e0:a4:e3:8b:94:92:39:1a:61:84:f9:8b:1e:a6:
         b7:d1:bc:ef:4b:08:8c:d2:2b:b8:89:33:6f:48:1f:c4:86:76:
         28:1d:d1:7e:08:9d:a7:5a:e1:59:4d:ae:23:d5:9d:e3:0a:bd:
         5a:2e:2d:8c:8f:2a:5b:79:37:dd:bc:05:8c:52:22:24:f9:1a:
         63:9c:39:c2:67:66:ed:af:1c:cd:df:04:93:c6:3f:81:a6:09:
         dd:b1:20:83:9c:b1:ef:cc:66:49:ba:1f:d7:e6:60:fc:83:87:
         79:2c:de:81:96:96:d7:26:3f:d6:ab:9d:29:c6:75:68:02:c2:
         32:80:c9:2c:b0:28:a7:e1:9c:90:93:a9:91:03:87:c5:e6:53:
         92:82:2d:c5:31:fb:09:ce:fd:46:54:80:f2:b2:73:3b:1f:da:
         bf:49:96:2c:63:e9:ce:f3:cf:36:f6:76:f5:9d:5b:8e:60:57:
         8c:8d:19:88:62:63:c6:8b:71:a1:8d:05:0c:b5:3b:5f:a2:47:
         8e:8f:d0:22:8e:0e:ca:16:ff:e7:25:0a:34:2b:c2:1b:05:04:
         a8:dd:78:62:12:2f:f7:a1:18:bb:5d:f1:05:14:f4:10:84:38:
         e2:6b:89:e0:71:99:0b:8c:7d:ea:02:e3:b2:f6:a7:57:6f:4e:
         f0:c8:ca:13:8d:51:67:49:8b:81:13:27:42:9b:2b:ed:5b:34:
         fc:43:90:d1:e5:80:2e:2c:f1:2a:bc:b8:61:e3:ee:fe:4b:fc:
         25:ce:2f:06:f7:76:c0:1e:68:62:55:d4:7f:d7:ac:6d:d8:f4:
         12:77:9a:34:6c:0b:d8:16
```

```
    49:df:fa:86:e2:88:9f:29:db:70:c5:29:2d:fd:58:
    e3:46:5a:a5:9a:23:b4:da:c5:e0:0a:5f:61:6d:47:
    60:8a:d9:da:ea:15:21:10:12:ef:0c:18:4d:f8:96:
    a9:5f:2d:2b:0f:cd:dc:6a:8a:b4:d2:2f:00:8b:91:
    fa:cd:3f:b1:0c:35:f6:23:70:3f:15:c7:96:99:7b:
    66:5a:bb:d3:e2:6b:2a:6b:a0:f0:70:b2:02:72:a1:
    b7:0c:69:c3:b8:96:8e:5e:0a:1b:0d:5f:74:6e:b9:
    79:71:0a:cd:82:20:b3:c7:e8:bd:53:00:f8:7d:4e:
    90:9f:70:26:96:70:24:b4:e2:21:5e:65:65:27:62:
    6e:d9
exponent1:
    00:b7:55:f8:88:db:18:c7:f9:0f:2a:ed:6c:f0:87:
    bd:2d:7b:ac:42:84:67:98:ce:78:79:df:0c:31:ca:
    60:01:b7:08:ac:b1:ca:a5:f1:c8:77:b3:b3:40:45:
    a9:37:67:76:37:da:9e:16:72:3b:0c:f8:55:4e:55:
    57:f3:f3:7b:cc:60:34:d5:80:6a:57:8e:1a:93:17:
    98:12:da:d2:9d:73:2b:1b:21:fa:23:11:8c:43:53:
    a4:40:92:97:09:0a:5c:39:63:ca:73:56:0f:e6:a3:
    a4:33:b1:00:df:f2:1d:04:8b:cf:24:ed:3f:30:b2:
    7d:25:f3:25:83:9f:ef:3e:ff:d4:e9:05:84:b7:33:
    58:30:bc:f8:8b:01:1d:c8:14:c1:5c:d3:97:32:0a:
    f9:37:d1:cc:0b:e4:60:b8:4d:f8:bd:e1:8f:4f:29:
    36:e8:2a:b5:0d:78:4a:78:2b:b8:78:75:92:85:c3:
    df:54:80:56:e9:5b:24:c4:fa:79:1b:e7:c2:a5:d4:
    20:7f:4f:89:bb:0f:af:3a:04:27:b7:4e:bb:46:b8:
    fc:ea:01:9e:7c:be:ab:99:0e:94:65:ff:51:59:8f:
    b6:0d:ba:88:62:6c:2e:c8:f0:d7:47:38:21:f7:ec:
    d3:86:21:41:9f:7d:ea:84:48:9b:80:d6:67:9f:78:
    d5:e1
exponent2:
    09:1e:8d:7e:10:32:d4:b2:37:c2:45:b3:35:13:37:
    da:ba:65:5e:60:aa:cd:f0:53:eb:27:df:9d:f2:34:
```

Task 2: (Generating a Certificate Signing Request (CSR) for the Web Server)

- Generate a Certificate Signing Request (CSR) and private key for your web server (e.g., `www.bank32.com`).
- Add Subject Alternative Names (SAN) to allow multiple domain names for the server.

Seed Ubuntu [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Activities Terminal Oct 30 10:54

seed@VM: ~

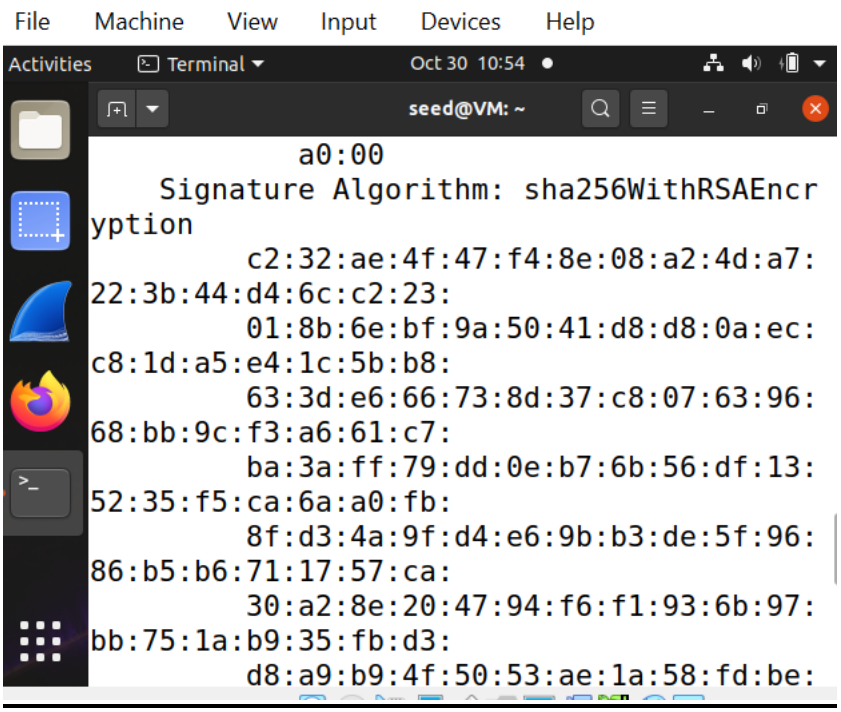
```
-----
[10/30/24]seed@VM:~$ openssl req -newkey r
sa:2048 -sha256 -keyout server.key -out se
rver.csr \
> -subj "/CN=www.bank32.com/O=Bank32 Inc./
C=US" -passout pass:dees \
> -addtext "subjectAltName=DNS:www.bank32.
com, DNS:www.bank32A.com, DNS:www.bank32B.
com"
req: Unrecognized flag addtext
req: Use -help for summary.
[10/30/24]seed@VM:~$ openssl req -in serve
r.csr -text -noout
Certificate Request:
    Data:
        Version: 1 (0x0)
```

Right Ctrl

seed@VM: ~

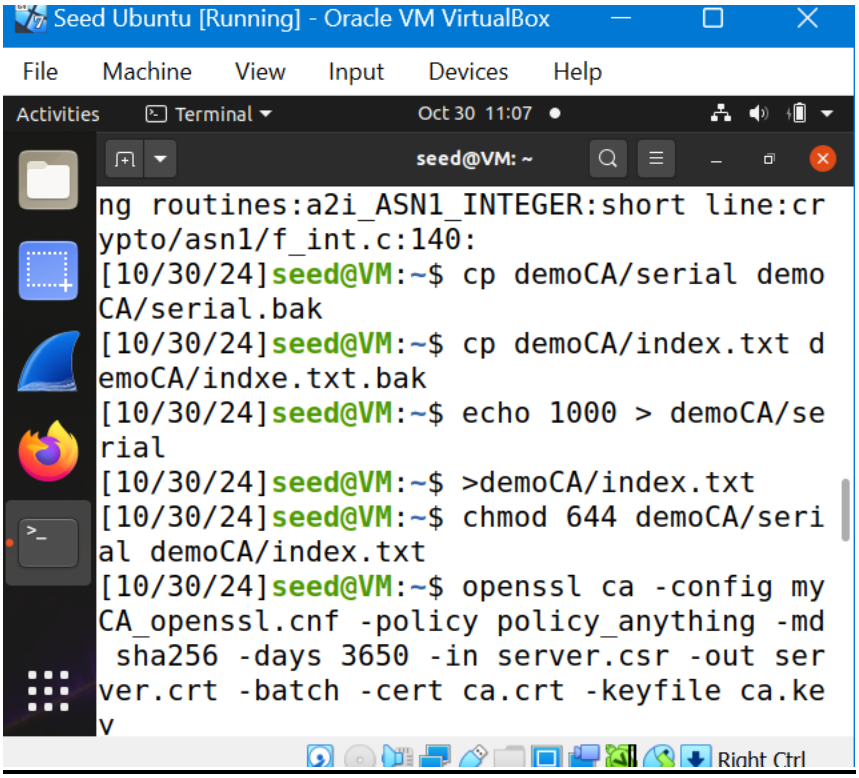
```
req: Use -help for summary.
[10/30/24]seed@VM:~$ openssl req -in serve
r.csr -text -noout
Certificate Request:
    Data:
        Version: 1 (0x0)
        Subject: CN = www.bank32.com, O =
Bank32 Inc., C = US
        Subject Public Key Info:
            Public Key Algorithm: rsaEncry
ption
                RSA Public-Key: (2048 bit)
                Modulus:
                    00:c8:5e:4c:4d:28:7f:0
6:95:eb:e3:9b:a5:3f:2b:
                    0c:05:69:93:eb:4d:7f:b
```

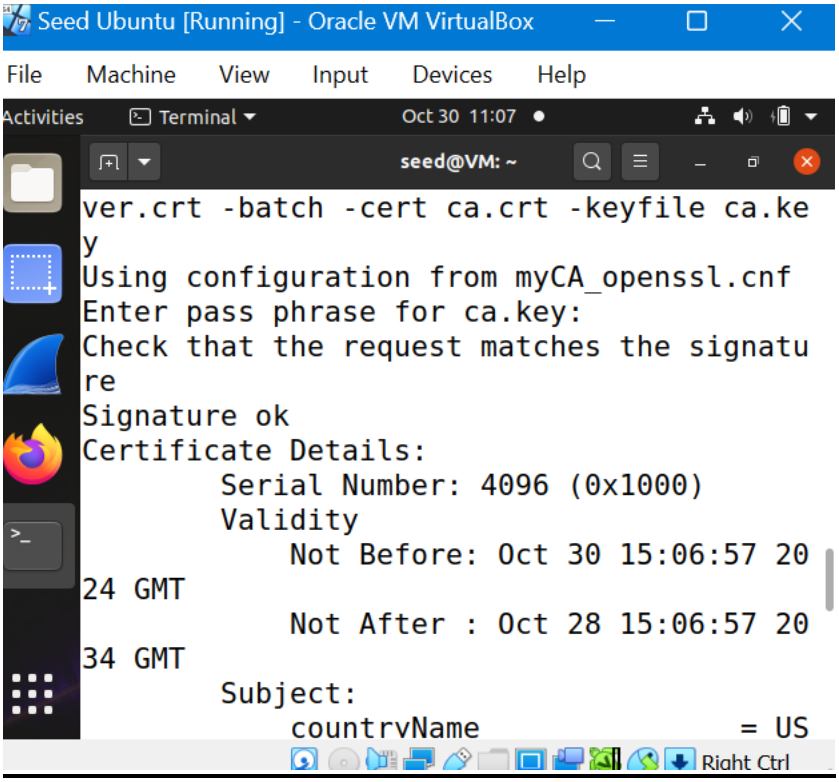
Right Ctrl

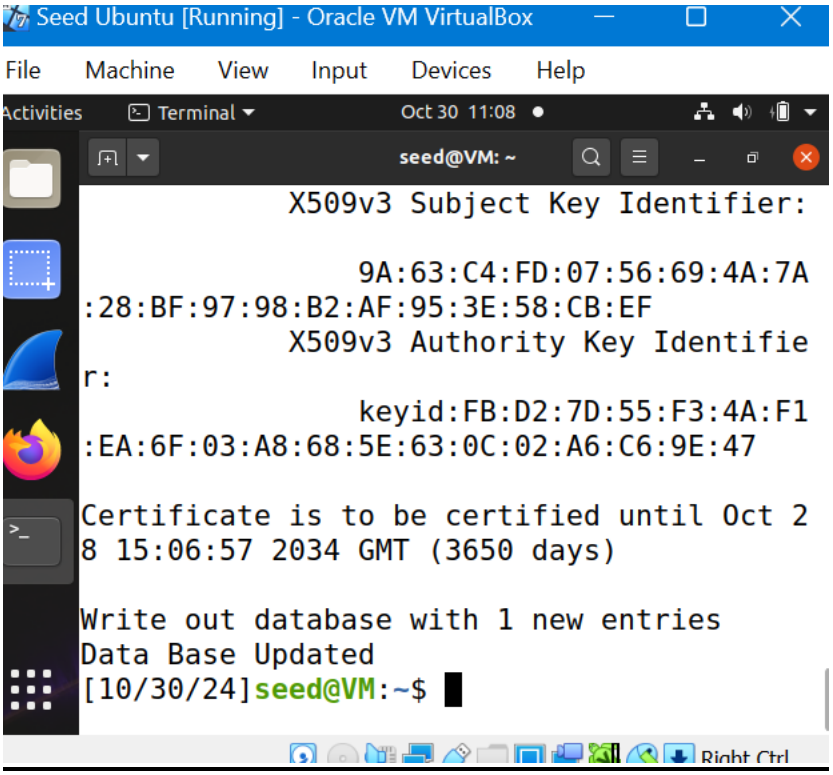


Task 3: (Generating a Certificate For The Server)

- • Use the CA from Task 1 to sign the CSR from Task 2, creating a certificate for your web server.
- Verify the certificate to ensure it includes any additional domain names specified.


Seed Ubuntu [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal Oct 30 11:07
seed@VM: ~
ng routines:a2i_ASN1_INTEGER:short line:crypto/asn1/f_int.c:140:
[10/30/24]seed@VM:~$ cp demoCA/serial demoCA/serial.bak
[10/30/24]seed@VM:~$ cp demoCA/index.txt demoCA/indxe.txt.bak
[10/30/24]seed@VM:~$ echo 1000 > demoCA/serial
[10/30/24]seed@VM:~$ >demoCA/index.txt
[10/30/24]seed@VM:~$ chmod 644 demoCA/serial demoCA/index.txt
[10/30/24]seed@VM:~$ openssl ca -config myCA_openssl.cnf -policy policy_anything -md sha256 -days 3650 -in server.csr -out server.crt -batch -cert ca.crt -keyfile ca.key
Right Ctrl


Seed Ubuntu [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal Oct 30 11:07
seed@VM: ~
ver.crt -batch -cert ca.crt -keyfile ca.key
Using configuration from myCA_openssl.cnf
Enter pass phrase for ca.key:
Check that the request matches the signature
Signature ok
Certificate Details:
Serial Number: 4096 (0x1000)
Validity
Not Before: Oct 30 15:06:57 2024 GMT
Not After : Oct 28 15:06:57 2034 GMT
Subject:
countryName = US
Right Ctrl



Task 4: (Deploying Certificate in an Apache-Based HTTPS Website)

- Configure Apache to use the server certificate and private key, enabling HTTPS for the site.
- Set up Virtual Host configuration to specify the certificate files.
- Start or reload Apache to apply the HTTPS configuration.

```
sudo: mvserver.crt: command not found
[10/30/24]seed@VM:~$ sudo mv server.crt /c
erts/
[10/30/24]seed@VM:~$ sudo mv server.key /c
erts/
[10/30/24]seed@VM:~$ cd /etc/apache2/sites
-available/
[10/30/24]seed@VM:.../sites-available$ nan
o bank32_apache_ssl.com
[10/30/24]seed@VM:.../sites-available$ sud
o nano bank32_apache_ssl.com
[10/30/24]seed@VM:.../sites-available$ a2e
nmod ssl
Considering dependency setenvif for ssl:
Module setenvif already enabled
```

Seed Ubuntu [Running] - Oracle VM VirtualBox

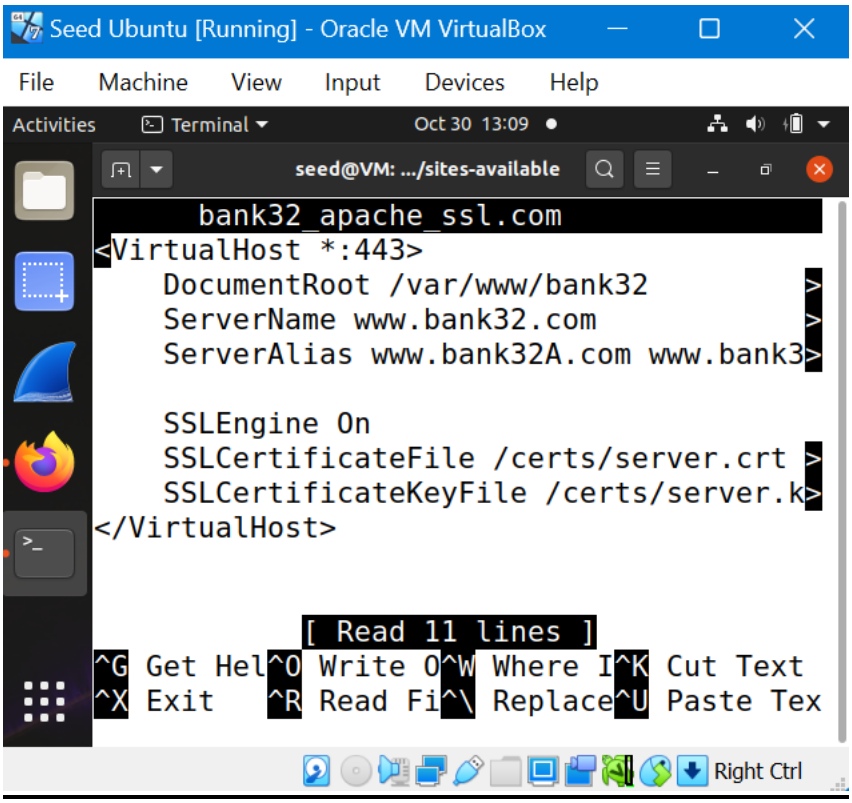
File Machine View Input Devices Help

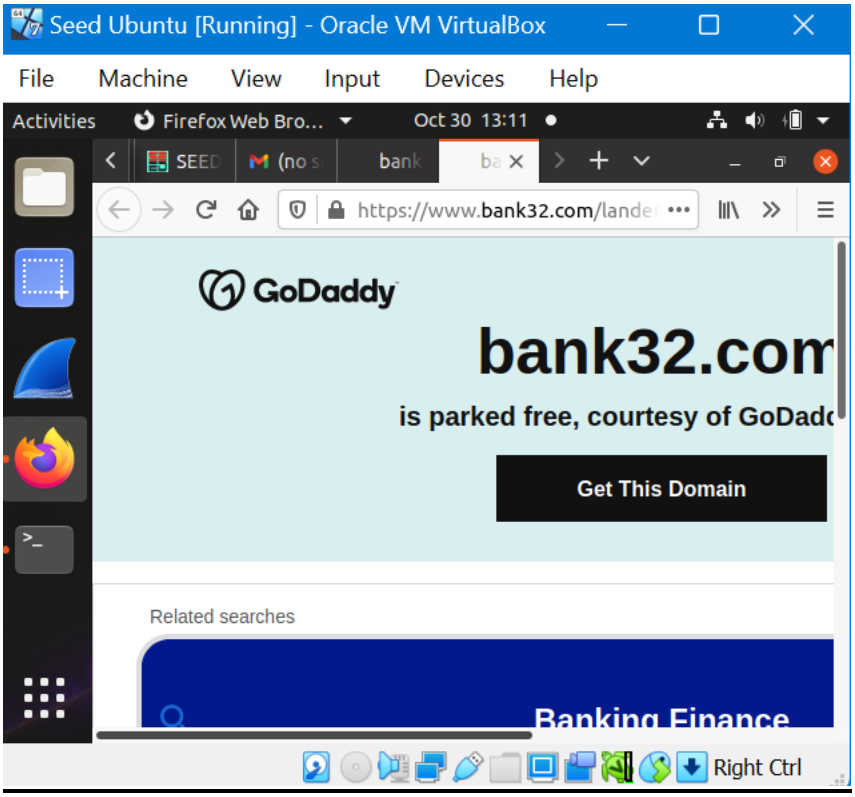
Activities Terminal Oct 30 13:09

seed@VM: .../sites-available

```
Could not create /etc/apache2/mods-enabled
/socache_shmcb.load: Permission denied
[10/30/24]seed@VM:.../sites-available$ sud
o a2enmod ssl
Considering dependency setenvif for ssl:
Module setenvif already enabled
Considering dependency mime for ssl:
Module mime already enabled
Considering dependency socache_shmcb for s
sl:
Enabling module socache_shmcb.
Enabling module ssl.
See /usr/share/doc/apache2/README.Debian.g
z on how to configure SSL and create self-
signed certificates.
To activate the new configuration, you nee
```

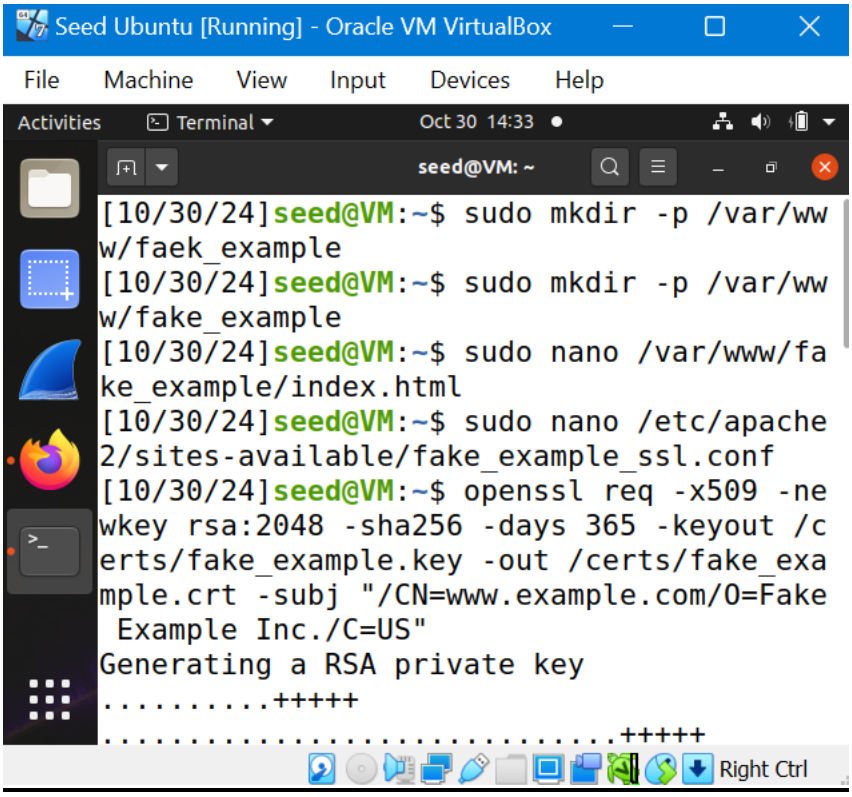
Right Ctrl

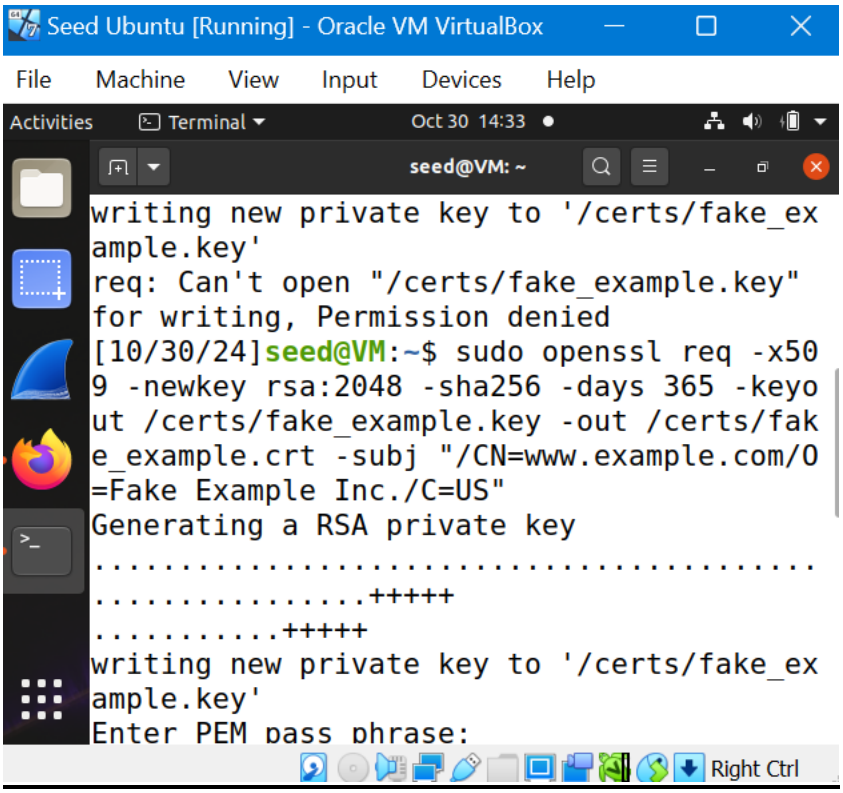

Seed Ubuntu [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal Oct 30 13:09
seed@VM: .../sites-available
bank32_apache_ssl.com
<VirtualHost *:443>
DocumentRoot /var/www/bank32
ServerName www.bank32.com
ServerAlias www.bank32A.com www.bank3
SSLEngine On
SSLCertificateFile /certs/server.crt
SSLCertificateKeyFile /certs/server.k
</VirtualHost>
[Read 11 lines]
^G Get Hel ^O Write O ^W Where I ^K Cut Text
^X Exit ^R Read Fi ^\ Replace ^U Paste Tex
Right Ctrl

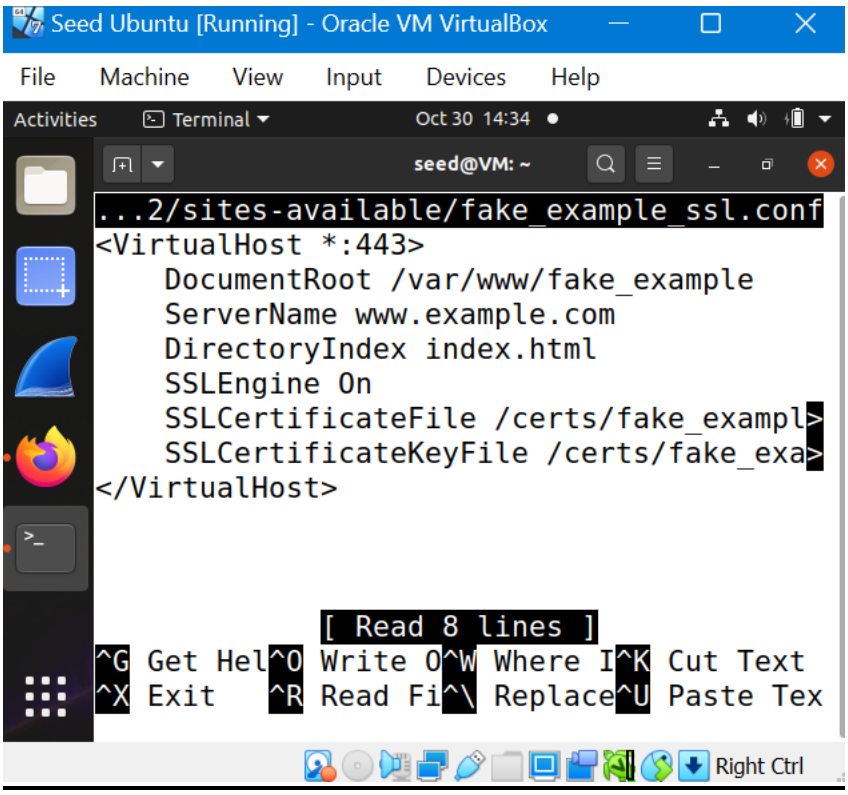

Seed Ubuntu [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Firefox Web Bro... Oct 30 13:11
https://www.bank32.com/lande
GoDaddy
bank32.com
is parked free, courtesy of GoDadd
Get This Domain
Related searches
Banking Finance
Right Ctrl

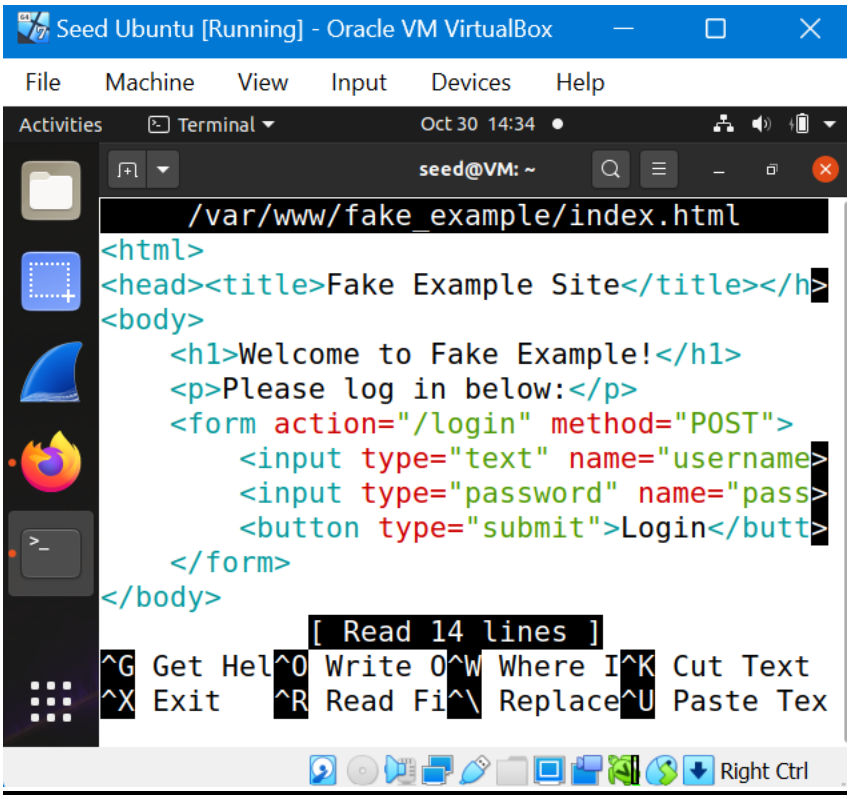
Task 5: (Launching a Man-In-The-Middle (MITM) Attack)

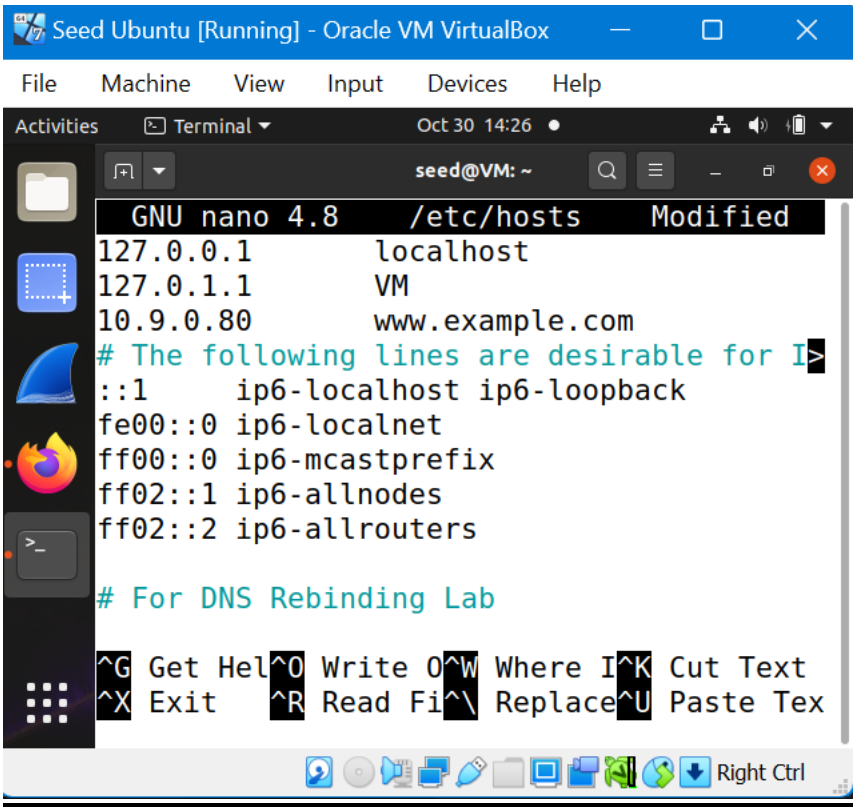
- Set up a fake website with the same domain name as the target (e.g., `www.example.com`).
- Modify the victim's `/etc/hosts` file to redirect requests for the target site to the fake server.
- Test by visiting the fake site to observe a security warning in the browser, showing that PKI prevents the attack.

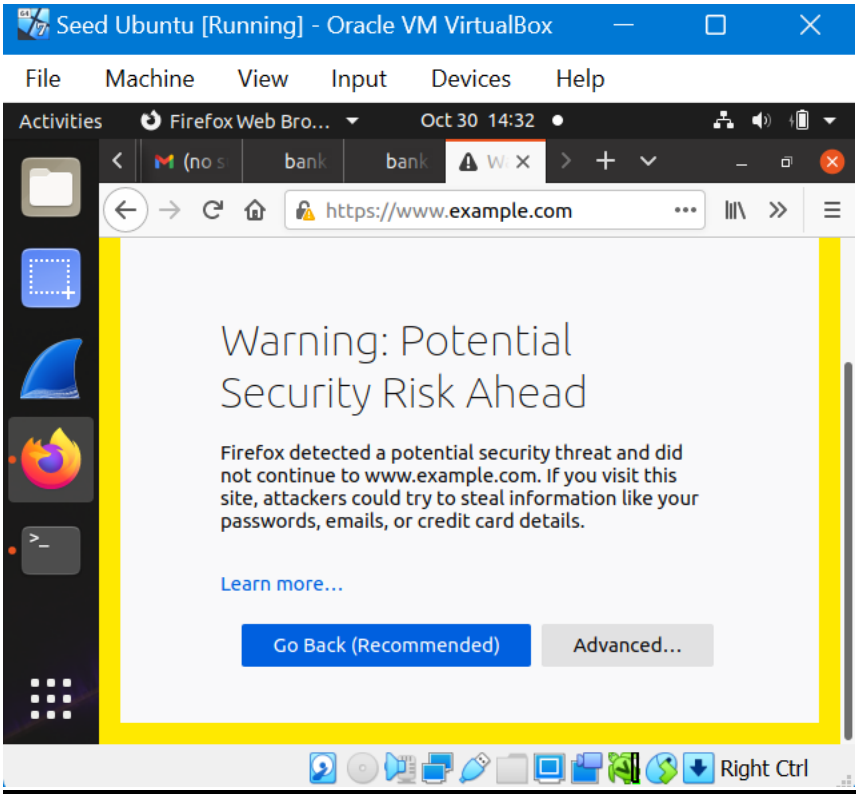



Seed Ubuntu [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal Oct 30 14:33
seed@VM: ~
writing new private key to '/certs/fake_example.key'
req: Can't open "/certs/fake_example.key" for writing, Permission denied
[10/30/24]seed@VM:~$ sudo openssl req -x509 -newkey rsa:2048 -sha256 -days 365 -keyout /certs/fake_example.key -out /certs/fake_example.crt -subj "/CN=www.example.com/O=Fake Example Inc./C=US"
Generating a RSA private key
.....+++++
.....+++++
writing new private key to '/certs/fake_example.key'
Enter PEM pass phrase:
Right Ctrl

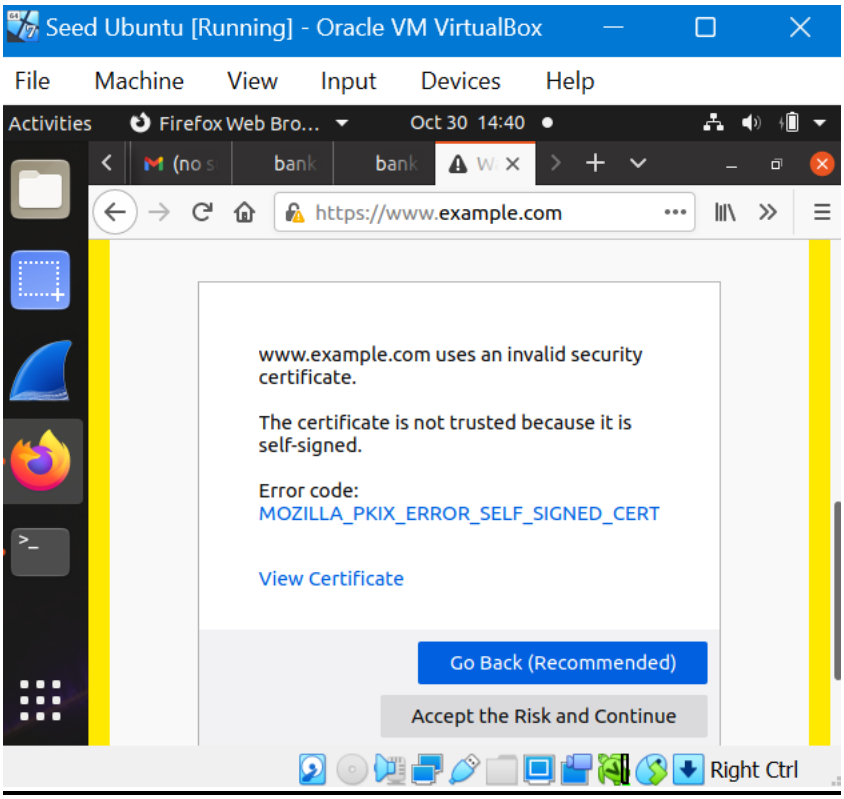

Seed Ubuntu [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal Oct 30 14:34
seed@VM: ~
...2/sites-available/fake_example_ssl.conf
<VirtualHost *:443>
DocumentRoot /var/www/fake_example
ServerName www.example.com
DirectoryIndex index.html
SSLEngine On
SSLCertificateFile /certs/fake_exampl>
SSLCertificateKeyFile /certs/fake_exa>
</VirtualHost>
[Read 8 lines]
^G Get Hel ^O Write O ^W Where I ^K Cut Text
^X Exit ^R Read Fi ^\ Replace ^U Paste Tex
Right Ctrl

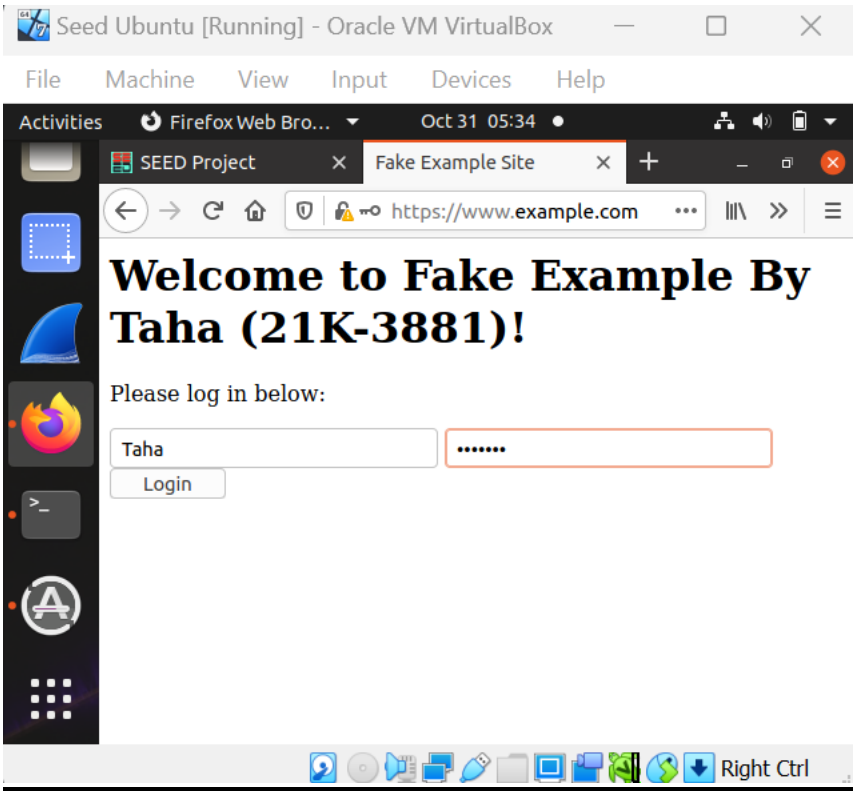

Seed Ubuntu [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal Oct 30 14:34
seed@VM: ~
/var/www/fake_example/index.html
<html>
<head><title>Fake Example Site</title></h
<body>
<h1>Welcome to Fake Example!</h1>
Please log in below:
<form action="/login" method="POST">
<input type="text" name="username
<input type="password" name="pass
<button type="submit">Login</butt
</form>
</body>
[Read 14 lines]
^G Get Hel ^O Write O ^W Where I ^K Cut Text
^X Exit ^R Read Fi ^\ Replace ^U Paste Tex
Right Ctrl


Seed Ubuntu [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal Oct 30 14:26
seed@VM: ~
GNU nano 4.8 /etc/hosts Modified
127.0.0.1 localhost
127.0.1.1 VM
10.9.0.80 www.example.com
The following lines are desirable for I
::1 ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
For DNS Rebinding Lab
^G Get Hel ^O Write O ^W Where I ^K Cut Text
^X Exit ^R Read Fi ^\ Replace ^U Paste Tex
Right Ctrl


Seed Ubuntu [Running] - Oracle VM VirtualBox
File
Machine
View
Input
Devices
Help
Activities
Firefox Web Bro...
Oct 30 14:32
https://www.example.com
Warning: Potential Security Risk Ahead
Firefox detected a potential security threat and did not continue to www.example.com. If you visit this site, attackers could try to steal information like your passwords, emails, or credit card details.
Learn more...
Go Back (Recommended)
Advanced...
Right Ctrl

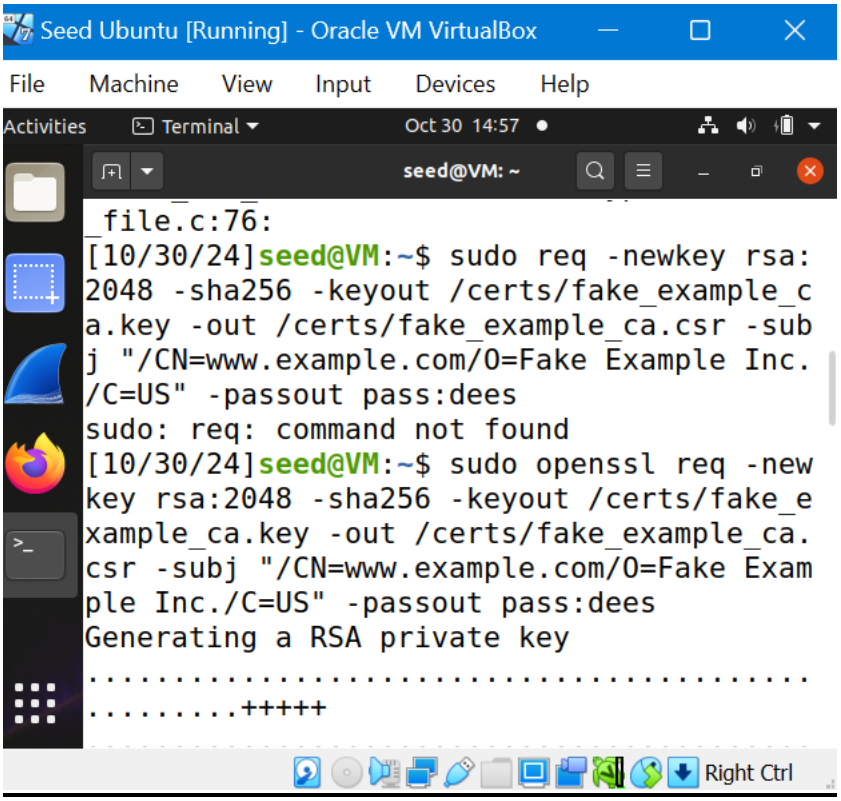
Taha Jawaid **Assignment 3** **21k-3881**

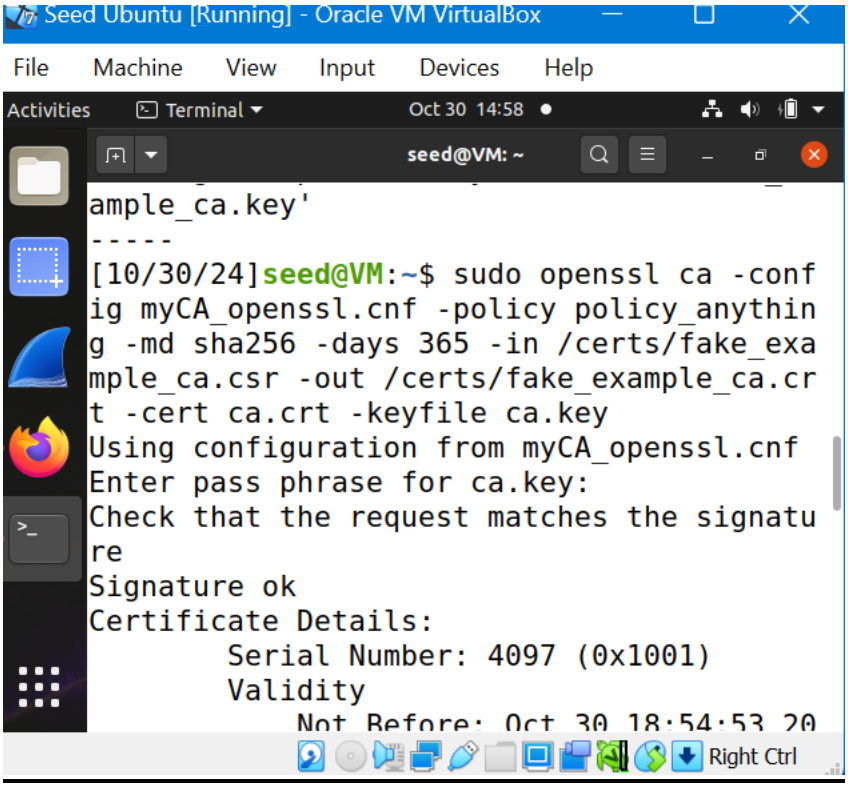




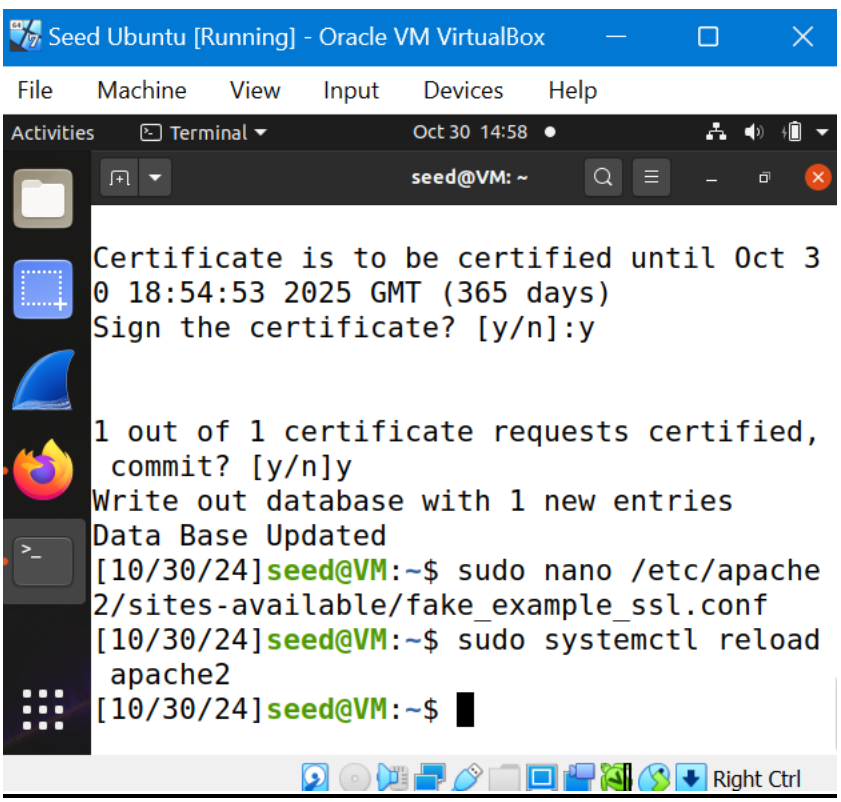
Task 6: (Launching a MITM Attack with a Compromised CA)

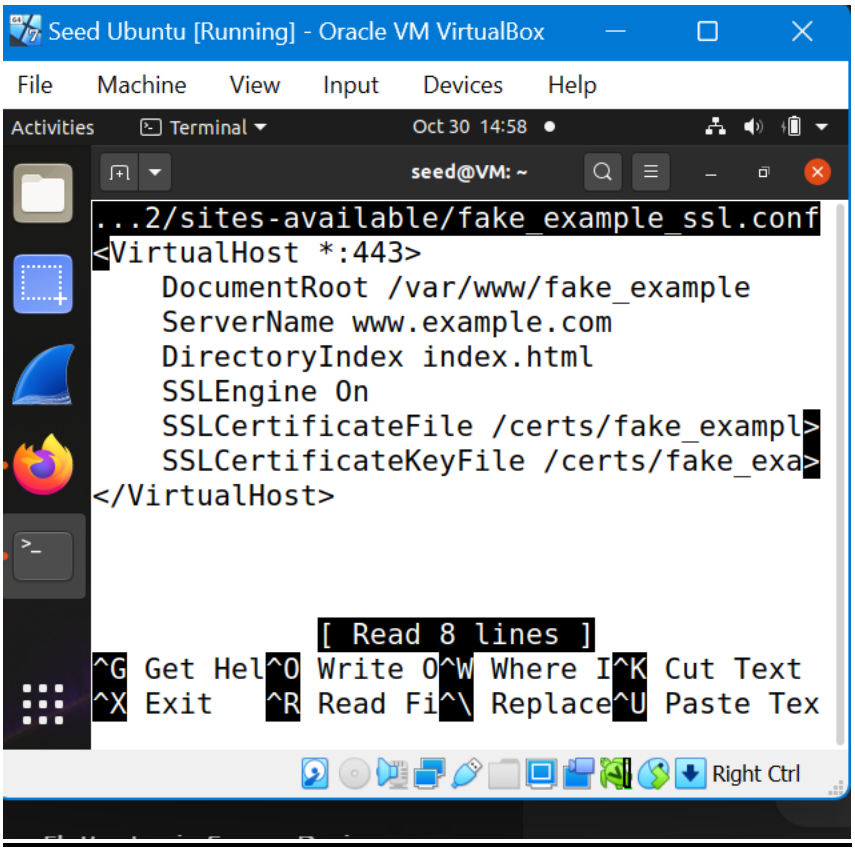
- • Create a new certificate for the fake website, signed by the compromised CA.
- Configure Apache to use this compromised certificate for the fake site.
- Test by visiting the fake site from the victim's browser; confirm that no security warning appears, demonstrating the effect of a compromised CA on PKI security.

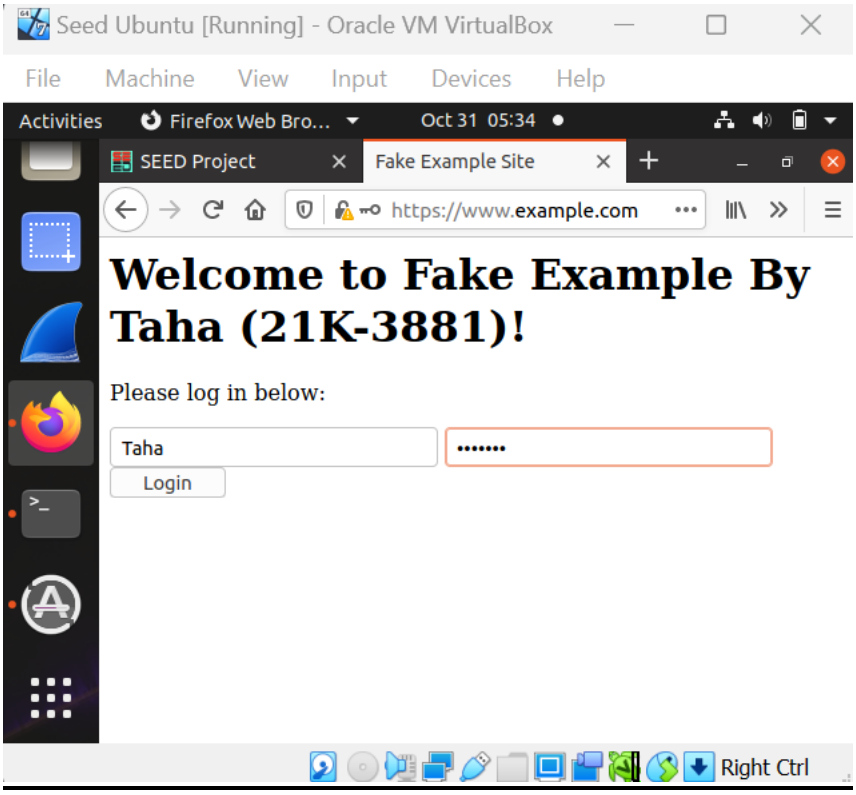



Seed Ubuntu [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal Oct 30 14:58
seed@VM: ~
ample_ca.key'

[10/30/24]seed@VM:~$ sudo openssl ca -conf
ig myCA_openssl.cnf -policy policy_anythin
g -md sha256 -days 365 -in /certs/fake_exa
mple_ca.csr -out /certs/fake_example_ca.cr
t -cert ca.crt -keyfile ca.key
Using configuration from myCA_openssl.cnf
Enter pass phrase for ca.key:
Check that the request matches the signatu
re
Signature ok
Certificate Details:
Serial Number: 4097 (0x1001)
Validity
Right Ctrl


Seed Ubuntu [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal Oct 30 14:58
seed@VM: ~
Certificate is to be certified until Oct 3
0 18:54:53 2025 GMT (365 days)
Sign the certificate? [y/n]:y
1 out of 1 certificate requests certified,
commit? [y/n]y
Write out database with 1 new entries
Data Base Updated
[10/30/24]seed@VM:~$ sudo nano /etc/apache
2/sites-available/fake_example_ssl.conf
[10/30/24]seed@VM:~$ sudo systemctl reload
apache2
[10/30/24]seed@VM:~$
Right Ctrl


Seed Ubuntu [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal Oct 30 14:58
seed@VM: ~
...2/sites-available/fake_example_ssl.conf
<VirtualHost *:443>
DocumentRoot /var/www/fake_example
ServerName www.example.com
DirectoryIndex index.html
SSLEngine On
SSLCertificateFile /certs/fake_exampl>
SSLCertificateKeyFile /certs/fake_exa>
</VirtualHost>
[Read 8 lines]
^G Get Hel ^O Write O ^W Where I ^K Cut Text
^X Exit ^R Read Fi ^\ Replace ^U Paste Tex
Right Ctrl


Seed Ubuntu [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Firefox Web Bro... Oct 31 05:34
SEED Project
Fake Example Site
https://www.example.com
Welcome to Fake Example By Taha (21K-3881)!
Please log in below:
Taha
Login
Right Ctrl

Taha Jawaid **Assignment 3** **21k-3881**