EAST WEST UNIVERSITY

Securing a networked system with Public Key Infrastructure

Course Title: Cybersecurity, law, and Ethics

Course Code: CSE487

Section: 03

Submitted to:

Rashedul Amin Tuhin

Senior Lecturer

Department of Computer Science and Engineering

East West University

Submitted by:

Asef Amer

ID: 2018-2-60-068

Department of Computer Science and Engineering

East West Engineering

Date of Submission:

08/9/2022

Certificate Generation Process

1. **Open Command prompt in VM for Linux Host 2.0**
2. ifconfig *-192.168.56.101*

DNS Configuration package:

    1. sudo apt install bind9
    2. sudo apt install dnsutils
    3. sudo systemctl restart bind9.service

3. sudo nano /etc/resolv.conf
    1. nameserver 192.168.56.101
    2. options edns0 trust-ad
    3. search localdomain

5.sudo nano /etc/named.conf

5. dig google.com

6. nslookup google.com

7. systemctl enable named

8. systemctl start named

sudo nano /etc/bind/verysecureserver.com.zone

```
...............................................................................

; Authoritative data for verysecureserver.com zone

;

$TTL 1D

@ IN SOA verysecureserver.com root.verysecureserver.com. (

2022041301 ; serial

1D ; refresh

1H ; retry
```

```
    1W ; expire

    3H ) ; minimum

    $ORIGIN verysecureserver.com.

    verysecureserver.com. IN NS verysecureserver.com.

    @ IN A 1. 192.168.56.101

    sudo nano /etc/bind/named.conf.local
```

```
zone "verysecureserver.com" IN {
    type master;
    file "/etc/bind/verysecureserver.com.zone";
};
```

```
9. systemctl enable named
10. systemctl start named
11. systemctl restart named
```

```
12. dig verysecureserver.com
13. nslookup verysecureserver.com
```

Create certificate ans sign this site with the certificate

```
14. mkdir {root-ca,sub-ca,server}
15. mkdir {root-ca,sub-ca,server}/{private,certs,newcerts,crl,csr}
```

```
16. touch root-ca/index
17. touch sub-ca/index
```

```
18. openssl genrsa -aes256 -out root-ca/private/ca.key 4096
19. openssl genrsa -aes256 -out sub-ca/private/sub-ca.key 4096
20. openssl genrsa -out server/private/server.key 2048
```

21. cd root-ca

22. openssl req -config root-ca.conf -key private/ca.key -new -x509 -days 7200 -sha256 -extensions v3_ca -out certs/ca.crt

#common name : Acme-RootCA

23. cd ../sub-ca/

24. openssl req -config sub-ca.conf -new -key private/sub-ca.key -sha256 -out csr/sub-ca.csr

#common name : Acme

25. cd ../root-ca

26. openssl ca -config root-ca.conf -extensions v3_intermediate_ca -days 3650 -notext -in ../sub-ca/csr/sub-ca.csr -out ../sub-ca/certs/sub-ca.crt -rand_serial

27. cd ../server

28. openssl req -config server.conf -key private/server.key -new -sha256 -out csr/server.csr

#common name : verysecureserver.com

29. cd ../sub-ca

30. openssl ca -config sub-ca.conf -extensions server_cert -days 365 -notext -in ../server/csr/server.csr -out ../server/certs/server.crt -rand_serial

31. cd ..

32. cat ./server/certs/server.crt ./sub-ca/certs/sub-ca.crt > chained.crt

# Revoke certificate

32. cd sub-ca

33. openssl ca -config sub-ca.conf -revoke ../server/certs/server.crt

# Add CRL to server

34. cd sub-ca

35. nano crlnumber

36. Add this certificate to the trusted certificate list.

For the Client :

1. **Open Command prompt in VM for Linux client 3.0**
2. ifconfig *-192.168.56.101*
3. sudo nano /etc/netplan/1-network-manager-all.yaml
4. for clint server confi

```
# Let NetworkManager manage all devices on this system

network:

  version: 2

  renderer: NetworkManager

  ethernets:

    enp0s3:

      dhcp4: no

      addresses: [192.168.56.101/24]

      routes:

        - to: default

          via: 192.168.0.1

      nameservers:

           addresses: [192.168.56.101]
           search: [verysecureserver.com]
```

5.sudo netplan try

6.sudo resolvectl status

7.nslookup 192.168.56.101

8. nslookup verysecureserver.com

DNS.1 = verysecureserver.com

DNS.2 = www.verysecureserver.com

Firewall configuration to allow necessary ports

```
<VirtualHost *:80>
    ServerName verysecureserver.com
    ServerAlias www.verysecureserver.com
    ServerAdmin webmaster@localhost
    DocumentRoot /var/www/secureserver
    ErrorLog ${APACHE_LOG_DIR}/error.log
    CustomLog ${APACHE_LOG_DIR}/access.log combined
</VirtualHost>
<VirtualHost *:443>
    ServerName verysecureserver.com
    ServerAlias www.verysecureserver.com
    ServerAdmin webmaster@localhost
    DocumentRoot /var/www/secureserver
    ErrorLog ${APACHE_LOG_DIR}/error.log
    CustomLog ${APACHE_LOG_DIR}/access.log combined
    SSLEngine on
      SSLCertificateFile /home/asef/openssl/server/certs/server.crt
      SSLCertificateKeyFile /home/asef/openssl/server/private/server.key
      SSLCertificateChainFile /home/asef/openssl/chained.crt

</VirtualHost>
```