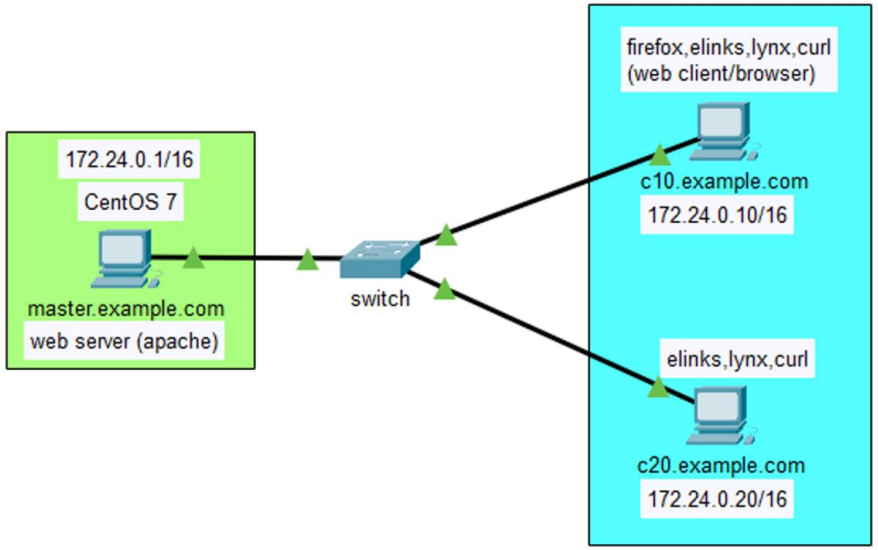
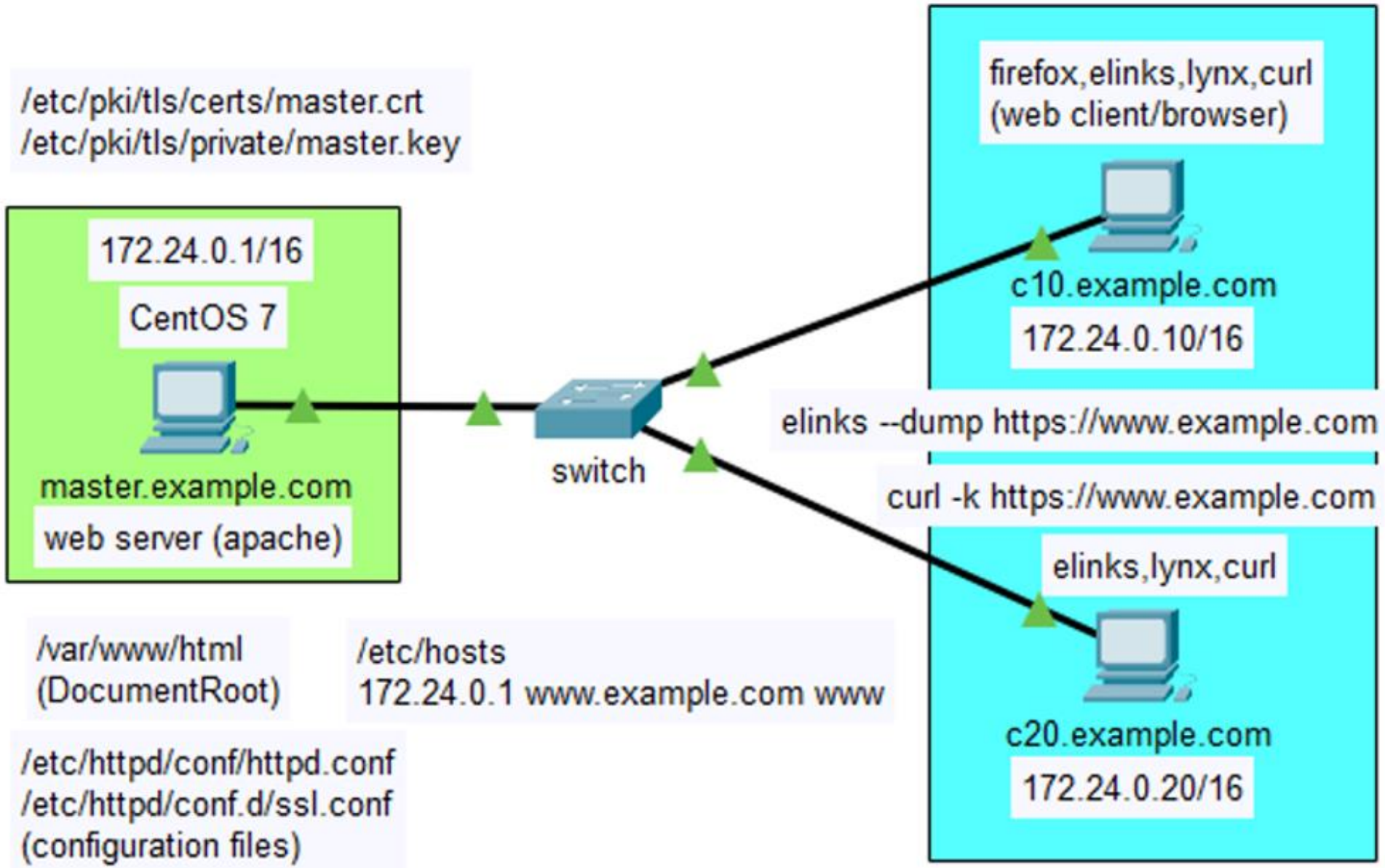


Implement Secure Apache Server

(Implement https)

Vipin Gupta
BE,RHCE,CEH,CCNA,MCSE,MCSA
vipin2411@gmail.com
Mobile: 93563-10379
www.linuxexpert.in

Lab Setup


/etc/pki/tls/certs/master.crt
/etc/pki/tls/private/master.key
172.24.0.1/16
CentOS 7
master.example.com
web server (apache)
switch
firefox,elinks,lynx,curl
(web client/browser)
c10.example.com
172.24.0.10/16
elinks --dump https://www.example.com
curl -k https://www.example.com
elinks,lynx,curl
c20.example.com
172.24.0.20/16
/var/www/html
(DocumentRoot)
/etc/hosts
172.24.0.1 www.example.com www
/etc/httpd/conf/httpd.conf
/etc/httpd/conf.d/ssl.conf
(configuration files)

View Critical Settings in “ssl.conf”

```
[root@master ~]# cd /etc/httpd/conf.d/
[root@master conf.d]#
[root@master conf.d]# pwd
/etc/httpd/conf.d
[root@master conf.d]#
[root@master conf.d]# ls
autoindex.conf  php.conf  README  ssl.conf  userdir.conf  welcome.conf
[root@master conf.d]#
```

```
[root@master conf.d]# ls -l
total 32
-rw-r--r-- 1 root root 2926 Nov 16 21:48 autoindex.conf
-rw-r--r-- 1 root root  691 Apr  1  2020 php.conf
-rw-r--r-- 1 root root  366 Nov 16 21:49 README
-rw-r--r-- 1 root root 9443 Nov 16 20:14 ssl.conf
-rw-r--r-- 1 root root 1248 Jan  9 16:50 userdir.conf
-rw-r--r-- 1 root root  824 Nov 16 20:14 welcome.conf
[root@master conf.d]#
[root@master conf.d]# cat ssl.conf |grep ^SSLCertificate
SSLCertificateFile /etc/pki/tls/certs/localhost.crt
SSLCertificateKeyFile /etc/pki/tls/private/localhost.key
[root@master conf.d]#
```

By default, “/etc/httpd/conf.d/ssl.conf” contains information certificate file “localhost.crt” and private key file “localhost.key” .

Verify Packages & Create Private Key

```
[root@master conf.d]# rpm -q openssl
openssl-1.0.2k-21.el7_9.x86_64
[root@master conf.d]#
[root@master conf.d]# rpm -q mod_ssl
mod_ssl-2.4.6-97.el7.centos.x86_64
[root@master conf.d]#
[root@master conf.d]# openssl genrsa -out master.key 1024
Generating RSA private key, 1024 bit long modulus
..........++++++
.....++++++
e is 65537 (0x10001)
[root@master conf.d]#
[root@master conf.d]# ls
autoindex.conf  master.key  php.conf  README  ssl.conf  userdir.conf  welcome.conf
[root@master conf.d]#
[root@master conf.d]# ls -l
total 36
-rw-r--r-- 1 root root 2926 Nov 16 21:48 autoindex.conf
-rw-r--r-- 1 root root  891 Jan 10 11:57 master.key
-rw-r--r-- 1 root root  691 Apr  1  2020 php.conf
-rw-r--r-- 1 root root  366 Nov 16 21:49 README
-rw-r--r-- 1 root root 9443 Nov 16 20:14 ssl.conf
-rw-r--r-- 1 root root 1248 Jan  9 16:50 userdir.conf
-rw-r--r-- 1 root root  824 Nov 16 20:14 welcome.conf
```

Create private key “master.key” by using “openssl”.

View Private Key

```
[root@master conf.d]# cat master.key
-----BEGIN RSA PRIVATE KEY-----
MIICXgIBAAKBgQDTxgErG1YP67/C0gdMy99H9wbo1Keo2lBhS7X1iuZhrFKg9bEf
Zlku5M620JDY2U3DAXTkcZuLW305M7F7uQNcFI7WcFH3GtgZw9GSlxoRUrzplf6Y
2qv4cQHGLaHvZPIYgTHb66hdOKufmk160eY8fblelIEtPh2/Pu4Suu5QVQIDAQAB
AoGBAKKItn7aJSxk+LFSty2Wz1CRZGkwRVmP7N8v14CT0YunUWeeCgoaaFpYW9p5
AZqc9VS0en2WQBYt6qcLaK2Xat5Mb5suaYgFXAdTJzcnRNLPr05Lh2BXisJaZGv6
oKwDAD+bFdsqTuaYiMeE2I5/vwpUYhkGeZ5SWChtlCbX0asFAkEA8gnKSNPkePM4
68Mx1F/rnLMEYpkwiA7LxbMCnNPUV1tgGHeZLohpJZuIuLIqWv+H7De9M40BZjET
49ymyq0llwJBAN/9SlamFG0L8JR5Y7xPL0L5Iq782SDTy9WXyX/0kHNdCtU4L3gG
Ad68MVa3mbEKqFs6p0cjCsbYuCwvZFXBLvMCQQDVdtz5LigqpBhnlle0PoTGRvxv
GTw8QxBk5GRBfHGi0eyep5xp9dUGXg5PFpNUflmac+5iMNIzFsW8CTbxMTMxAkBr
1WY3hucj8ZgV8sbYPorzRDu1YNcrXauxHc0NQ/FTCMURV2ZK8yFtWM6r/+IHAKmC
mh4PhKhIiMdJxlsYid0PAkEArfd80UiEQZ9WH1AsZYfBSugTvzdfIkVcLt2w4aEc
Pku4x+ZF10rgV/AVpYArL2qQfeWgAoEacGHVFA01TAddzg==
-----END RSA PRIVATE KEY-----
```

Create Self Signed Certificate

```
[root@master conf.d]# openssl req -new -key master.key -out master.crt -x509
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) [XX]:IN
State or Province Name (full name) []:Punjab
Locality Name (eg, city) [Default City]:Chandigarh
Organization Name (eg, company) [Default Company Ltd]:U-Net Solutions
Organizational Unit Name (eg, section) []:IT
Common Name (eg, your name or your server's hostname) []:www.example.com
Email Address []:admin@example.com
[root@master conf.d]#
```

Create self signed certificate “master.crt” by using “openssl”.

Locate Certificate File & Private Key

```
[root@master conf.d]# ls
autoindex.conf  master.crt  master.key  php.conf  README  ssl.conf
[root@master conf.d]#
[root@master conf.d]# ls -l
total 40
-rw-r--r-- 1 root root 2926 Nov 16 21:48 autoindex.conf
-rw-r--r-- 1 root root 1094 Jan 10 12:09 master.crt
-rw-r--r-- 1 root root  891 Jan 10 11:57 master.key
-rw-r--r-- 1 root root  691 Apr  1  2020 php.conf
-rw-r--r-- 1 root root  366 Nov 16 21:49 README
-rw-r--r-- 1 root root 9443 Nov 16 20:14 ssl.conf
-rw-r--r-- 1 root root 1248 Jan  9 16:50 userdir.conf
-rw-r--r-- 1 root root  824 Nov 16 20:14 welcome.conf
[root@master conf.d]#
```

The certificate file and private key are in “/etc/httpd/conf.d/” directory.

View Contents of Certificate File

```
[root@master conf.d]# cat master.crt
-----BEGIN CERTIFICATE-----
MIIC/DCCAmWgAwIBAgIJAInai57pFTAfMA0GCSqGSIb3DQEBCwUAMIGWMQswCQYD
VQQGEwJJTjEPMA0GA1UECAwGUHVuamFiMRMwEQYDVQQHDApDaGFuZGlnYXJoMRgw
FgYDVQQKDA9VLU5ldCBTb2x1dGlvbnMxCzAJBgNVBAsMAklUMRgwFgYDVQQDDA93
d3cuZXhhbXBsZS5jb20xIDAeBgkqhkiG9w0BCQEWEWFkbWluQGV4YW1wbGUuY29t
MB4XDTIxMDExMDA2Mzky0FoXDTIxMDIw0TA2Mzky0FowgZYxCzAJBgNVBAYTAkl0
MQ8wDQYDVQQIDAZQdW5qYWIxEzARBgNVBAcMCkNoYW5kaWdhcmgxGDAWBgNVBAoM
D1UtTmV0IFNvbHV0aW9uczELMAkGA1UECwwCSVQxGDAWBgNVBAMMD3d3dy5leGFt
cGxlLmNvbTEgMB4GCSqGSIb3DQEJARYRYWRtaW5AZXhhbXBsZS5jb20wgZ8wDQYJ
KoZIhvcNAQEBBQADgY0AMIGJAoGBANPGASsbVg/rv8LSB0zL30f3BujUp6jaUGFL
tfWK5mGsUqD1sR9mWS7kzrY4kNjZTcMBd0Rxm4tbfTkzsXu5A1wUjtZwUfca2BnD
0ZKXGhFSv0mV/pjaq/hxAcYtoe9k8hiBMdvrqF04q5+aTXrR5jx9uV6UgS0+Hb8+
7hK67lBVAgMBAAGjUDBOMB0GA1UdDgQWBBRmq5Y2LN98yNqHeYt4nQn0ZtMLyTAf
BgNVHSMEGDAWgBRmq5Y2LN98yNqHeYt4nQn0ZtMLyTAMBgNVHRMEBTADAQH/MA0G
CSqGSIb3DQEBCwUAA4GBAMY2f/rGnpkLy13IhrLZIU/1azdDwoDuiDW2MQHH7vU6
lqIeV42uq+2I1Az24gsvtAzuoFmlXSZpFcdV6U/iXau8T5x6Vh5Y0GYPL1B/W59D
GkYFdzxAkk51kBwV3Ci8Y7EBJK8GM77xtLjb0SQDwlv7f1d2p1/TFPLzf8pWAC/S
-----END CERTIFICATE-----
[root@master conf.d]#
```

Move Certificate File & Private Key

```
[root@master conf.d]# ls -l /etc/pki/tls/certs/
total 16
lrwxrwxrwx 1 root root   49 Jul 12 09:45 ca-bundle.crt -> /etc/
m
lrwxrwxrwx 1 root root   55 Jul 12 09:45 ca-bundle.trust.crt -
dle.trust.crt
-rw------- 1 root root 1452 Jan  7 18:40 localhost.crt
-rwxr-xr-x 1 root root  610 Dec 17 02:54 make-dummy-cert
-rw-r--r-- 1 root root 2516 Dec 17 02:54 Makefile
-rwxr-xr-x 1 root root  829 Dec 17 02:54 renew-dummy-cert
[root@master conf.d]#
[root@master conf.d]# ls -l /etc/pki/tls/private/
total 4
-rw------- 1 root root 1679 Jan  7 18:40 localhost.key
[root@master conf.d]#
```

Move Certificate File & Private Key

```
[root@master conf.d]# mv master.crt /etc/pki/tls/certs/
[root@master conf.d]#
[root@master conf.d]# mv master.key /etc/pki/tls/private/
[root@master conf.d]#
[root@master conf.d]# ls /etc/pki/tls/certs/
ca-bundle.crt        localhost.crt    Makefile    renew-dummy-cert
ca-bundle.trust.crt  make-dummy-cert  master.crt
[root@master conf.d]#
[root@master conf.d]# ls /etc/pki/tls/private/
localhost.key  master.key
[root@master conf.d]#
```

Move certificate file and private key to proper directories.

Modify “ssl.conf”

```
[root@master conf.d]# cat ssl.conf |grep ^SSLCertificate
SSLCertificateFile /etc/pki/tls/certs/master.crt
SSLCertificateKeyFile /etc/pki/tls/private/master.key
[root@master conf.d]#
[root@master conf.d]# systemctl restart httpd
[root@master conf.d]#
```

Modify “ssl.conf” and restart web server.

Verify “https” Access

```
[root@c10 ~]# openssl  s_client  -connect  www.example.com:443 |head -6
depth=0 C = IN, ST = Punjab, L = Chandigarh, O = U-Net Solutions, OU = IT, CN = www.example.com, emailAddr
ess = admin@example.com
verify error:num=18:self signed certificate
verify return:1
depth=0 C = IN, ST = Punjab, L = Chandigarh, O = U-Net Solutions, OU = IT, CN = www.example.com, emailAddr
ess = admin@example.com
verify return:1
CONNECTED(00000003)
---
Certificate chain
 0 s:/C=IN/ST=Punjab/L=Chandigarh/O=U-Net Solutions/OU=IT/CN=www.example.com/emailAddress=admin@example.co
m
   i:/C=IN/ST=Punjab/L=Chandigarh/O=U-Net Solutions/OU=IT/CN=www.example.com/emailAddress=admin@example.co
m
---
[root@c10 ~]# _
```

Use “openssl s_client” to test https web server.

Verify “https” Access

```
[root@c10 ~]# elinks --dump https://www.example.com
ELinks: SSL error
[root@c10 ~]#
[root@c10 ~]# curl https://www.example.com
curl: (60) Peer's certificate issuer has been marked as not trusted by the user.
More details here: http://curl.haxx.se/docs/sslcerts.html

curl performs SSL certificate verification by default, using a "bundle"
 of Certificate Authority (CA) public keys (CA certs). If the default
 bundle file isn't adequate, you can specify an alternate file
 using the --cacert option.
If this HTTPS server uses a certificate signed by a CA represented in
 the bundle, the certificate verification probably failed due to a
 problem with the certificate (it might be expired, or the name might
 not match the domain name in the URL).
If you'd like to turn off curl's verification of the certificate, use
 the -k (or --insecure) option.
[root@c10 ~]#
```

Use “elinks” and ”curl” to test https web server.

Verify “https” Access

```
[root@c10 ~]# curl -k https://www.example.com
101 marketing 30000 <br />102 sales 25000 <br />103 production 12000 <br />104 cs 20000 <br />
#
```

Use ”curl” to test https web server.

Verify “https” Access

```
[root@c10 ~]# cat /etc/elinks.conf |grep cert_verify
    ## connection.ssl.cert_verify [0|1]
    set connection.ssl.cert_verify = 1
[root@c10 ~]#
[root@c10 ~]# vi /etc/elinks.conf
```

```
[root@c10 ~]# cat /etc/elinks.conf |grep cert_verify
    ## connection.ssl.cert_verify [0|1]
    set connection.ssl.cert_verify = 0
[root@c10 ~]#
[root@c10 ~]# elinks --dump https://www.example.com
   101 marketing 30000
   102 sales 25000
   103 production 12000
   104 cs 20000
```

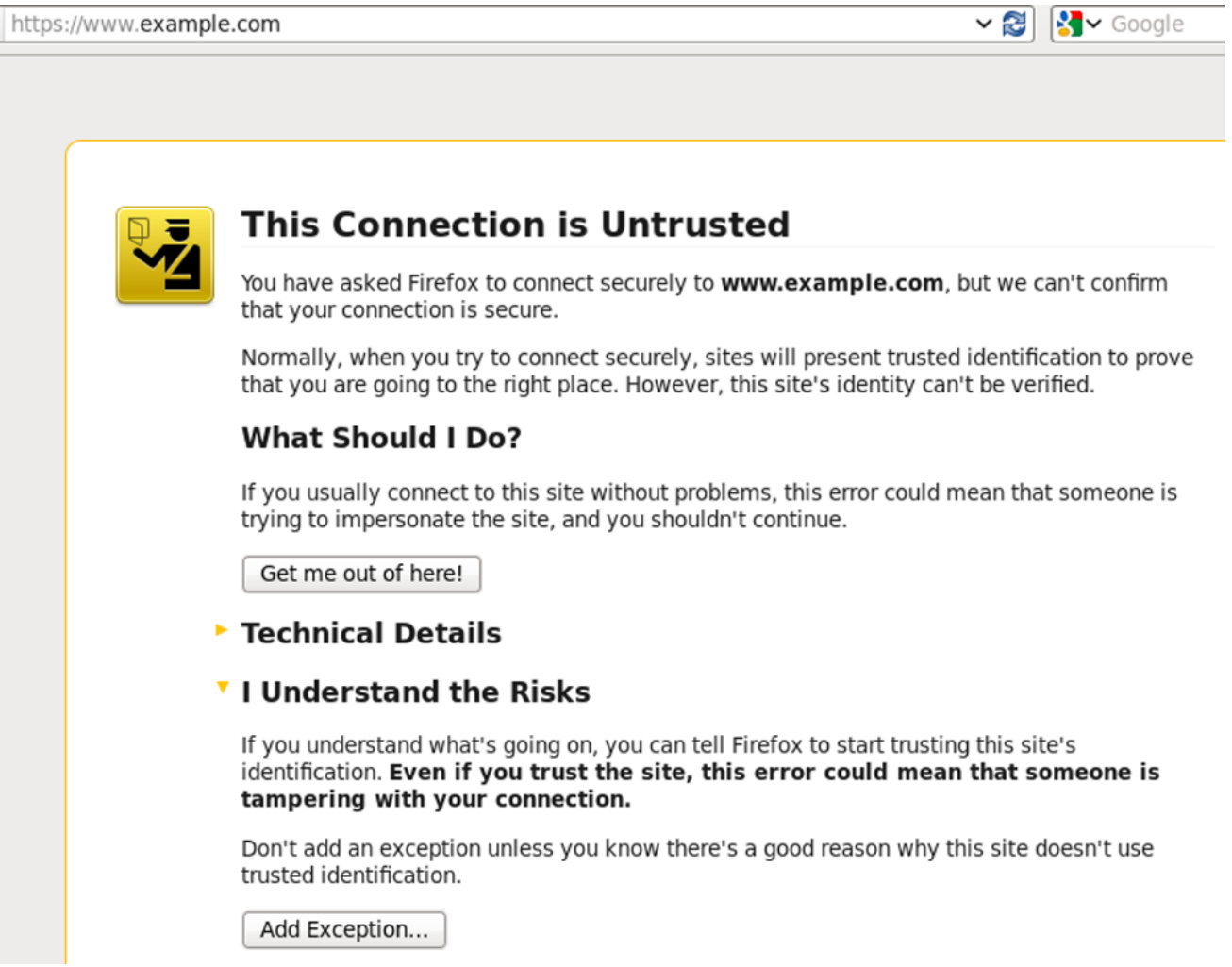
Use “elinks” to test https web server.

Using GUI Mode To Verify “https” Access

```
[root@client31 ~]# ifconfig eth0 |head -2
eth0      Link encap:Ethernet  HWaddr 00:0C:29:5E:10:AA
          inet addr:172.24.0.31  Bcast:172.24.255.255  Mask:255.255.0.0
[root@client31 ~]#
[root@client31 ~]# tail -1 /etc/hosts
172.24.0.1 www.example.com www
[root@client31 ~]#
```

Use “firefox” to test https web server.

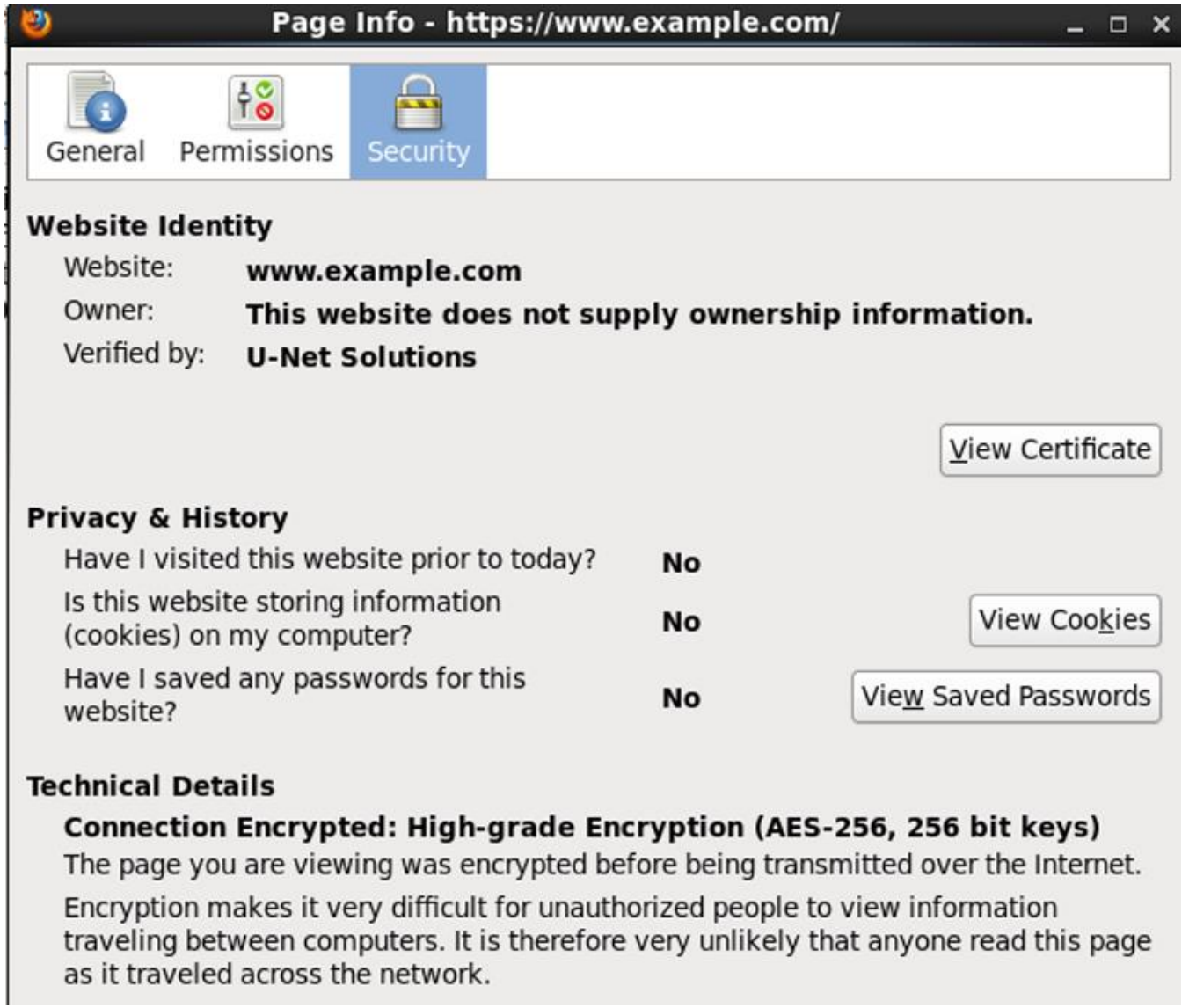
Using “Firefox” Browser To Verify “https” Access



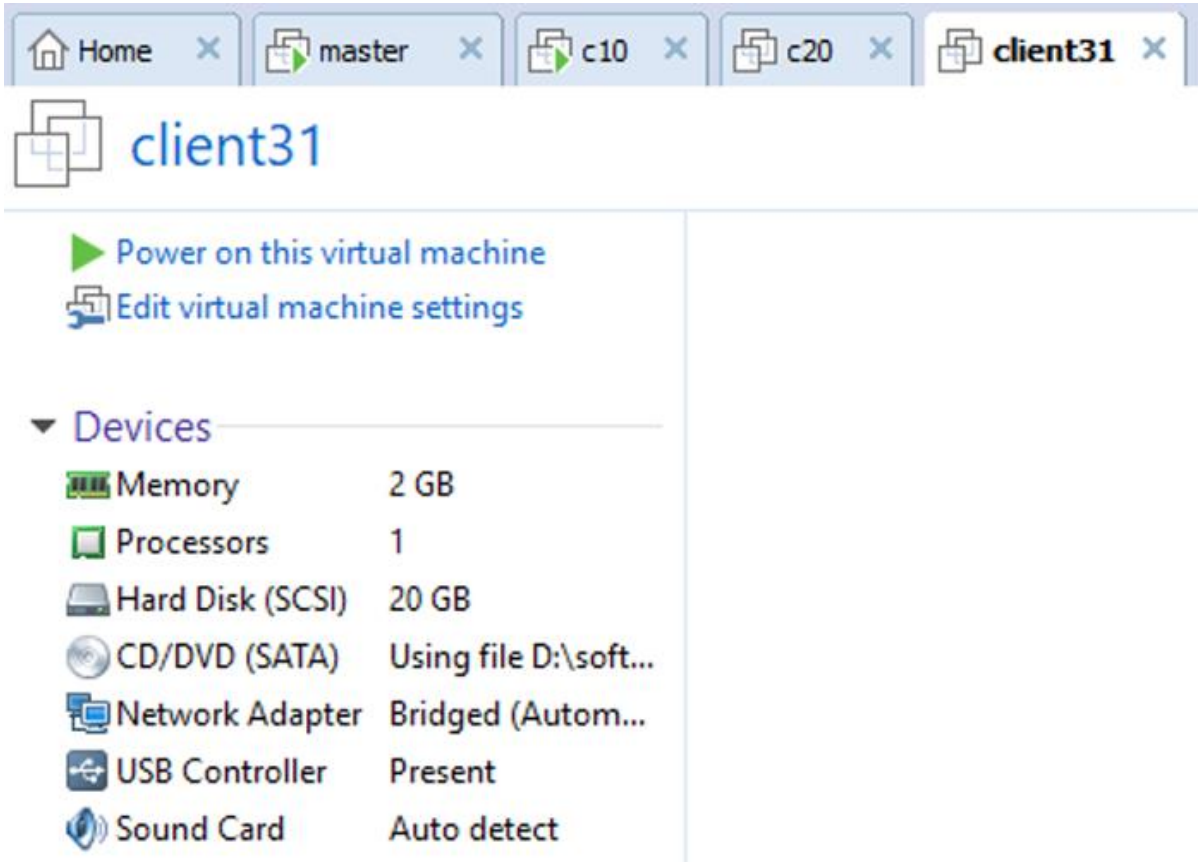
Use “firefox” to test https web server.

Using “Firefox” Browser To Verify “https” Access

Use “firefox” to test https web server.



Using “Firefox” Browser To Verify “https” Access



Use “firefox” to test https web server.