Fall2019 Cent OS 7 web server installation with a self signed certificate.

The presentation installs and checks the operation of a web server. Once the web server is installed, the presentation creates a self signed certificate and configures the web server to use ssl.

Preuss
12/6/2019

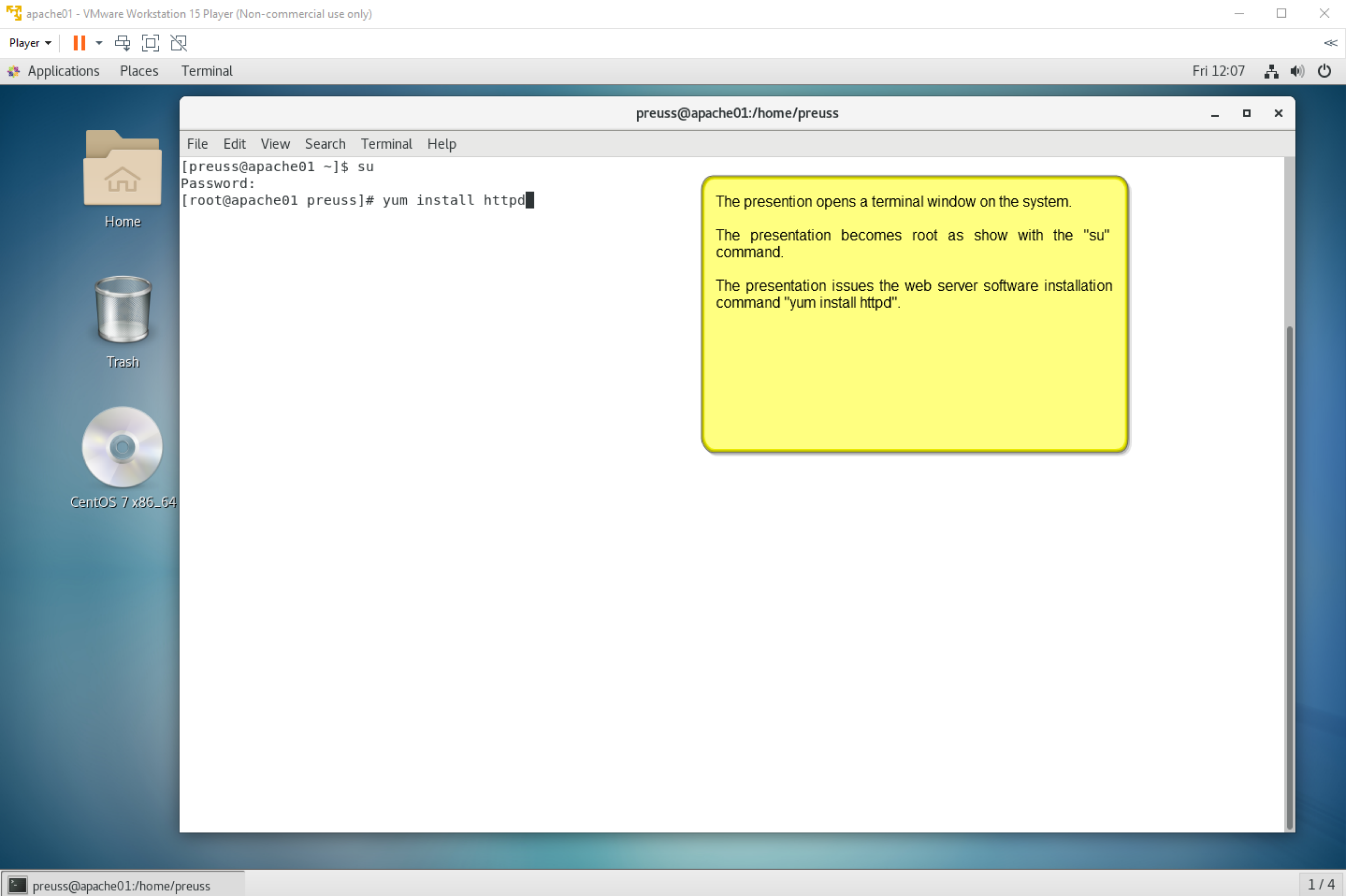
Cent OS 7 Settings on both systems

20 GB disk
8 GB RAM
2 Processors
NAT Network Settings

Software Install: Server with GUI (no additional software)
Automatic partitioning
No security policy chosen

Post-Installation
Install open-vm-tools
Install updates

Resource:
https://www.tecmint.com/install-apache-on-centos-7/
https://blog.canadianwebhosting.com/installing-self-signed-ssl-on-apache-with-centos-7/



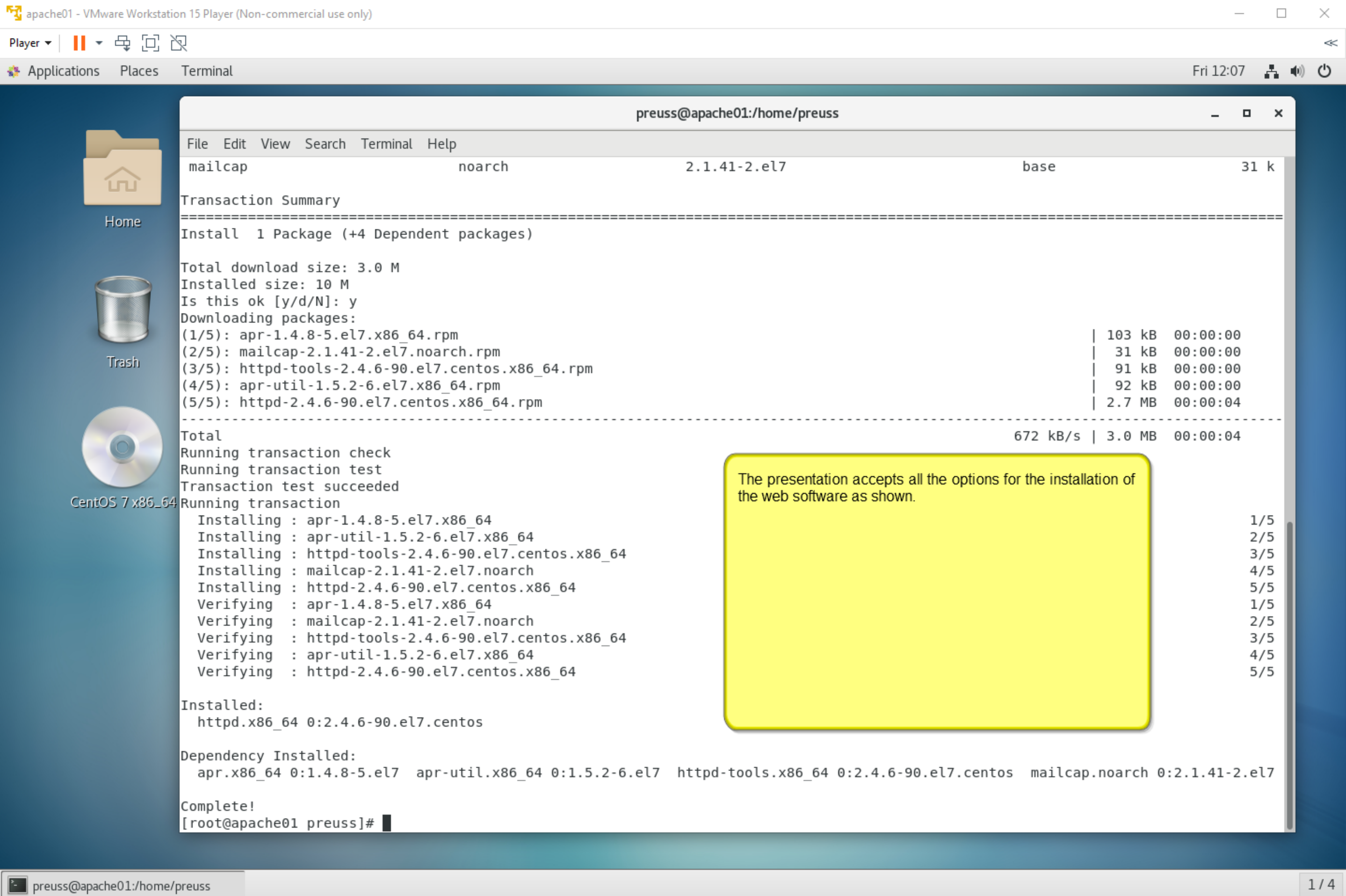
apache01 - VMware Workstation 15 Player (Non-commercial use only)
Player
Applications
Places
Terminal
Fri 12:07
Home
Trash
CentOS 7 x86_64
preuss@apache01:/home/preuss
File
Edit
View
Search
Terminal
Help
preuss@apache01:/home/preuss
1 / 4

```
[preuss@apache01 ~]$ su
Password:
[root@apache01 preuss]# yum install httpd
```

The presention opens a terminal window on the system.

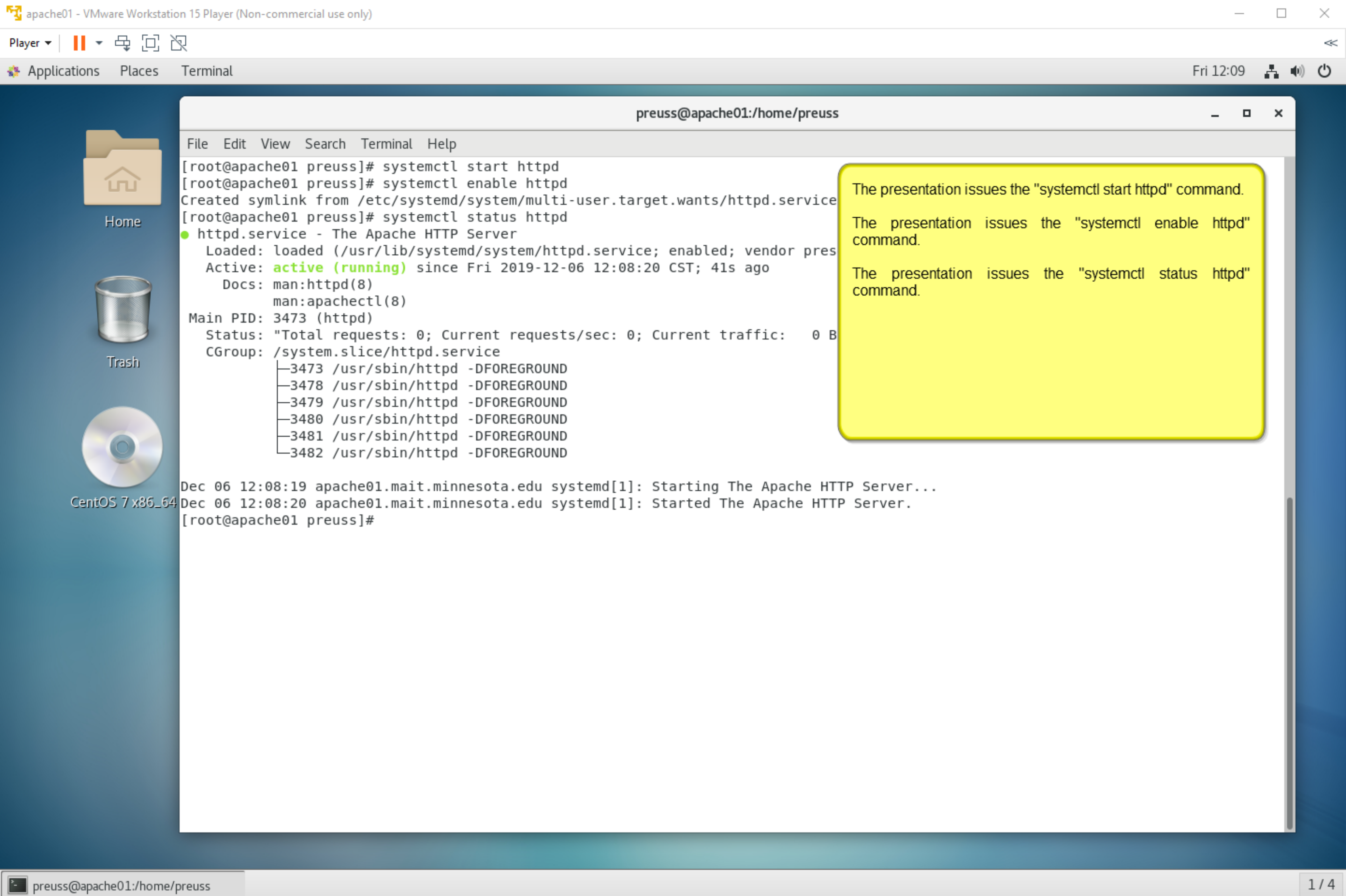
The presentation becomes root as show with the "su" command.

The presentation issues the web server software installation command "yum install httpd".


apache01 - VMware Workstation 15 Player (Non-commercial use only)
Player
Applications
Places
Terminal
Fri 12:07
Home
Trash
CentOS 7 x86_64
preuss@apache01:/home/preuss
File
Edit
View
Search
Terminal
Help
preuss@apache01:/home/preuss
1 / 4

```
 mailcap                     noarch                  2.1.41-2.el7                       base                     31 k

Transaction Summary
=================================================================================================================================
Install  1 Package (+4 Dependent packages)

Total download size: 3.0 M
Installed size: 10 M
Is this ok [y/d/N]: y
Downloading packages:
(1/5): apr-1.4.8-5.el7.x86_64.rpm                                                                   | 103 kB  00:00:00
(2/5): mailcap-2.1.41-2.el7.noarch.rpm                                                              |  31 kB  00:00:00
(3/5): httpd-tools-2.4.6-90.el7.centos.x86_64.rpm                                                   |  91 kB  00:00:00
(4/5): apr-util-1.5.2-6.el7.x86_64.rpm                                                              |  92 kB  00:00:00
(5/5): httpd-2.4.6-90.el7.centos.x86_64.rpm                                                         | 2.7 MB  00:00:04
---------------------------------------------------------------------------------------------------------------------------------
Total                                                                                      672 kB/s | 3.0 MB  00:00:04
Running transaction check
Running transaction test
Transaction test succeeded
Running transaction
  Installing : apr-1.4.8-5.el7.x86_64                                                                                     1/5
  Installing : apr-util-1.5.2-6.el7.x86_64                                                                                2/5
  Installing : httpd-tools-2.4.6-90.el7.centos.x86_64                                                                     3/5
  Installing : mailcap-2.1.41-2.el7.noarch                                                                                4/5
  Installing : httpd-2.4.6-90.el7.centos.x86_64                                                                           5/5
  Verifying  : apr-1.4.8-5.el7.x86_64                                                                                     1/5
  Verifying  : mailcap-2.1.41-2.el7.noarch                                                                                2/5
  Verifying  : httpd-tools-2.4.6-90.el7.centos.x86_64                                                                     3/5
  Verifying  : apr-util-1.5.2-6.el7.x86_64                                                                                4/5
  Verifying  : httpd-2.4.6-90.el7.centos.x86_64                                                                           5/5

Installed:
  httpd.x86_64 0:2.4.6-90.el7.centos

Dependency Installed:
  apr.x86_64 0:1.4.8-5.el7  apr-util.x86_64 0:1.5.2-6.el7  httpd-tools.x86_64 0:2.4.6-90.el7.centos  mailcap.noarch 0:2.1.41-2.el7

Complete!
[root@apache01 preuss]#
```

The presentation accepts all the options for the installation of the web software as shown.

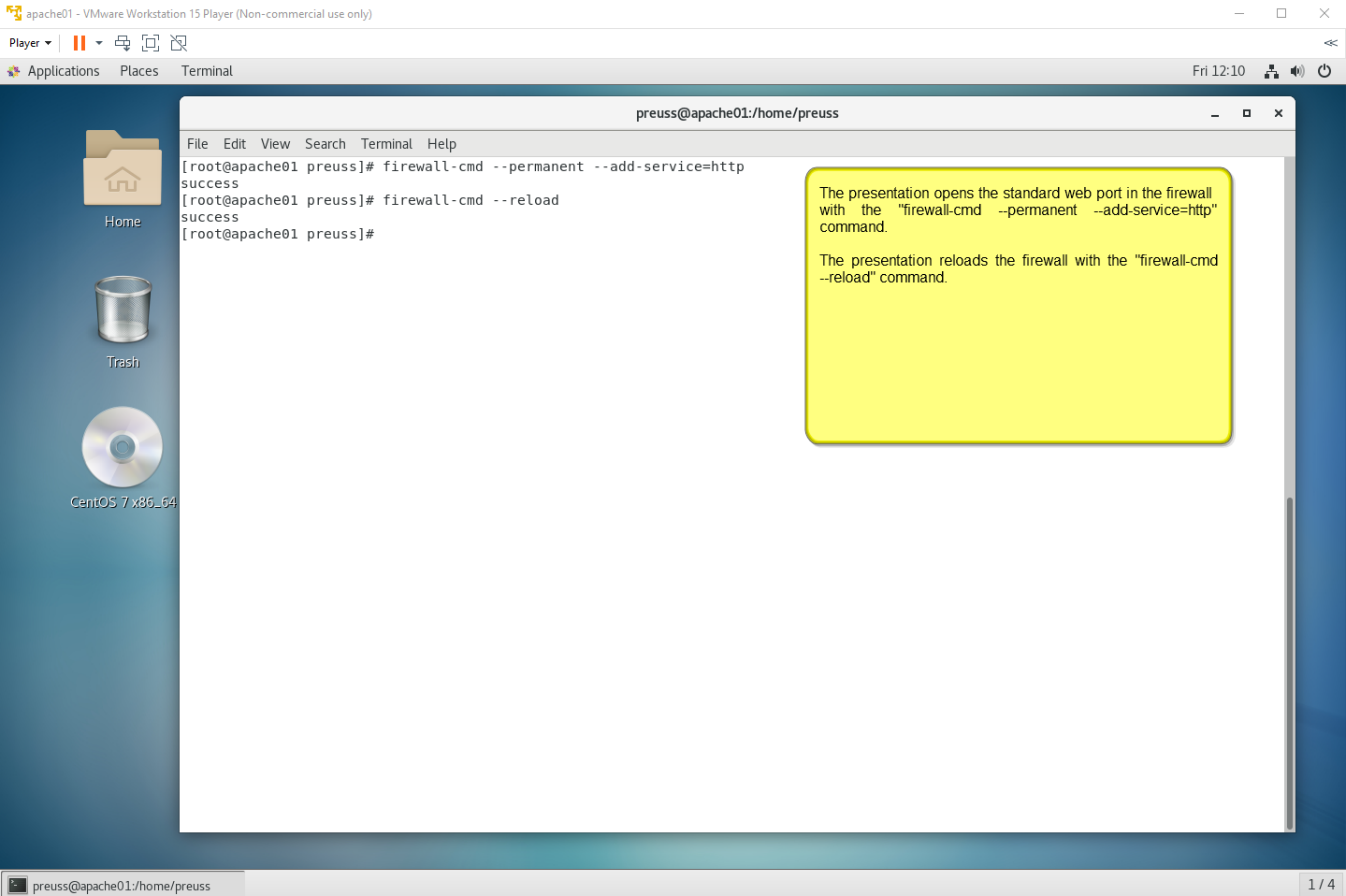

apache01 - VMware Workstation 15 Player (Non-commercial use only)
Player
Applications
Places
Terminal
Fri 12:09
preuss@apache01:/home/preuss
File
Edit
View
Search
Terminal
Help
Home
Trash
CentOS 7 x86_64
preuss@apache01:/home/preuss
1 / 4

```
[root@apache01 preuss]# systemctl start httpd
[root@apache01 preuss]# systemctl enable httpd
Created symlink from /etc/systemd/system/multi-user.target.wants/httpd.service
[root@apache01 preuss]# systemctl status httpd
● httpd.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; enabled; vendor pres
   Active: active (running) since Fri 2019-12-06 12:08:20 CST; 41s ago
     Docs: man:httpd(8)
           man:apachectl(8)
 Main PID: 3473 (httpd)
   Status: "Total requests: 0; Current requests/sec: 0; Current traffic:   0 B
   CGroup: /system.slice/httpd.service
           ├─3473 /usr/sbin/httpd -DFOREGROUND
           ├─3478 /usr/sbin/httpd -DFOREGROUND
           ├─3479 /usr/sbin/httpd -DFOREGROUND
           ├─3480 /usr/sbin/httpd -DFOREGROUND
           ├─3481 /usr/sbin/httpd -DFOREGROUND
           └─3482 /usr/sbin/httpd -DFOREGROUND

Dec 06 12:08:19 apache01.mait.minnesota.edu systemd[1]: Starting The Apache HTTP Server...
Dec 06 12:08:20 apache01.mait.minnesota.edu systemd[1]: Started The Apache HTTP Server.
[root@apache01 preuss]#
```

The presentation issues the "systemctl start httpd" command.

The presentation issues the "systemctl enable httpd" command.

The presentation issues the "systemctl status httpd" command.

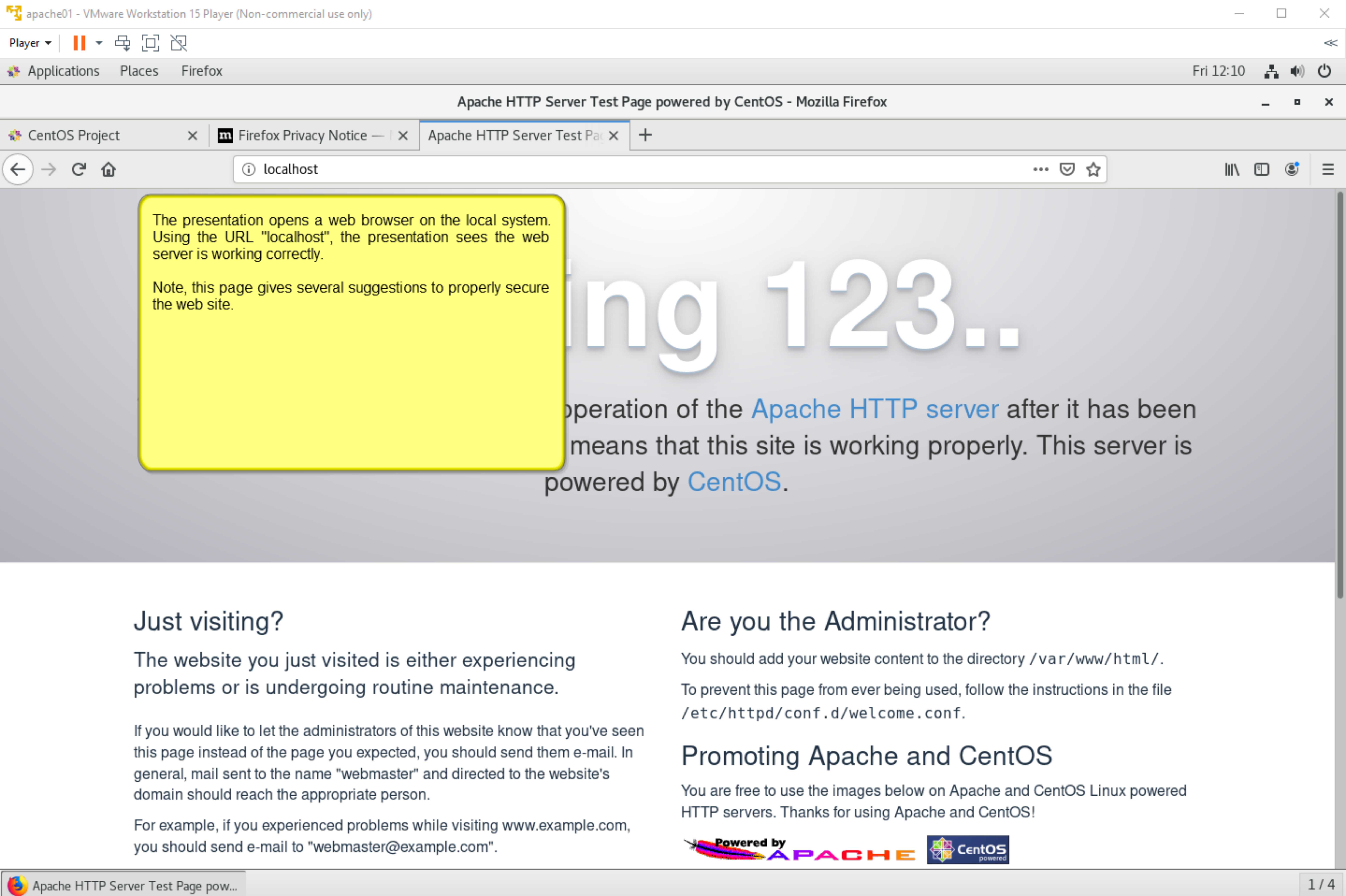


apache01 - VMware Workstation 15 Player (Non-commercial use only)
Player
Applications
Places
Terminal
Fri 12:10
Home
Trash
CentOS 7 x86_64
preuss@apache01:/home/preuss
File
Edit
View
Search
Terminal
Help
preuss@apache01:/home/preuss
1 / 4

```
[root@apache01 preuss]# firewall-cmd --permanent --add-service=http
success
[root@apache01 preuss]# firewall-cmd --reload
success
[root@apache01 preuss]#
```

The presentation opens the standard web port in the firewall with the "firewall-cmd --permanent --add-service=http" command.

The presentation reloads the firewall with the "firewall-cmd --reload" command.


apache01 - VMware Workstation 15 Player (Non-commercial use only)
Player
Applications
Places
Firefox
Fri 12:10
Apache HTTP Server Test Page powered by CentOS - Mozilla Firefox
CentOS Project
Firefox Privacy Notice —
Apache HTTP Server Test Pa
localhost
Apache HTTP Server Test Page pow...
1 / 4

The presentation opens a web browser on the local system. Using the URL "localhost", the presentation sees the web server is working correctly.

Note, this page gives several suggestions to properly secure the web site.

ing 123..

operation of the Apache HTTP server after it has been means that this site is working properly. This server is powered by CentOS.

Just visiting?

The website you just visited is either experiencing problems or is undergoing routine maintenance.

If you would like to let the administrators of this website know that you've seen this page instead of the page you expected, you should send them e-mail. In general, mail sent to the name "webmaster" and directed to the website's domain should reach the appropriate person.

For example, if you experienced problems while visiting www.example.com, you should send e-mail to "webmaster@example.com".

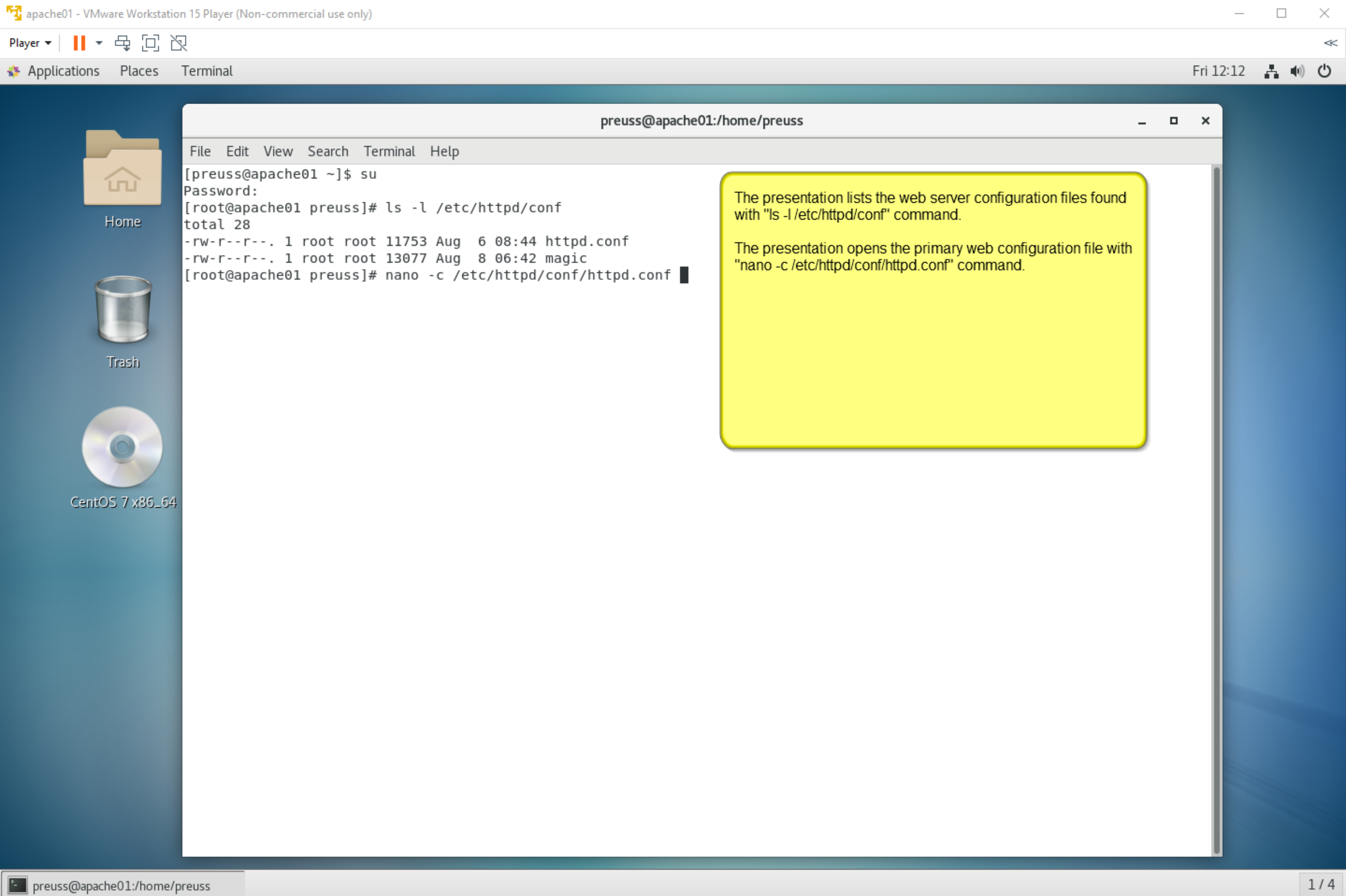
Are you the Administrator?

You should add your website content to the directory `/var/www/html/`.

To prevent this page from ever being used, follow the instructions in the file `/etc/httpd/conf.d/welcome.conf`.

Promoting Apache and CentOS

You are free to use the images below on Apache and CentOS Linux powered HTTP servers. Thanks for using Apache and CentOS!

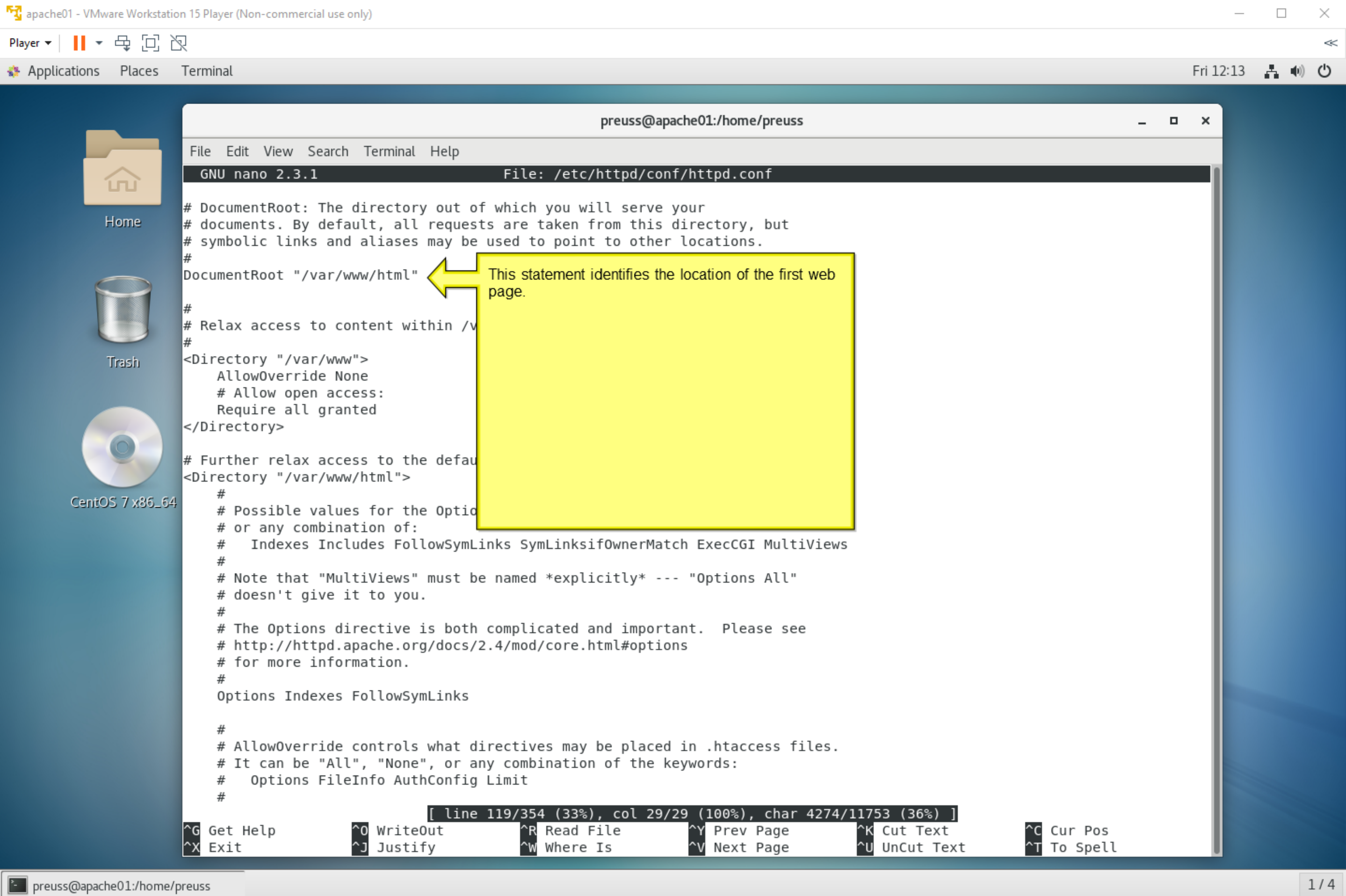


apache01 - VMware Workstation 15 Player (Non-commercial use only)
Player
Applications
Places
Terminal
Fri 12:12
Home
Trash
CentOS 7 x86_64
preuss@apache01:/home/preuss
File
Edit
View
Search
Terminal
Help
preuss@apache01:/home/preuss
1 / 4

```
[preuss@apache01 ~]$ su
Password:
[root@apache01 preuss]# ls -l /etc/httpd/conf
total 28
-rw-r--r--. 1 root root 11753 Aug  6 08:44 httpd.conf
-rw-r--r--. 1 root root 13077 Aug  8 06:42 magic
[root@apache01 preuss]# nano -c /etc/httpd/conf/httpd.conf
```

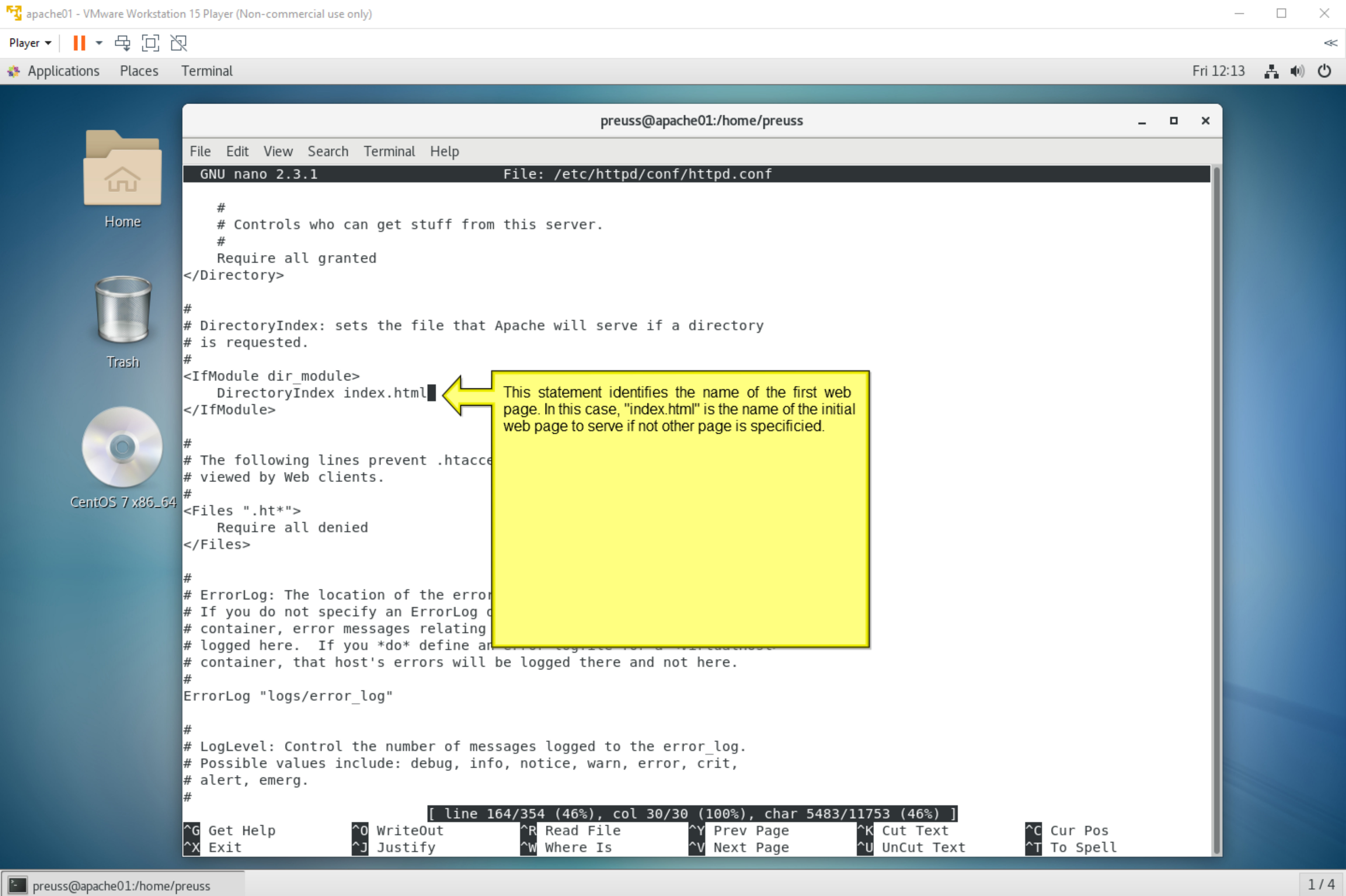
The presentation lists the web server configuration files found with "ls -l /etc/httpd/conf" command.

The presentation opens the primary web configuration file with "nano -c /etc/httpd/conf/httpd.conf" command.


apache01 - VMware Workstation 15 Player (Non-commercial use only)
Player
Applications
Places
Terminal
Fri 12:13
Home
Trash
CentOS 7 x86_64
preuss@apache01:/home/preuss
File
Edit
View
Search
Terminal
Help
preuss@apache01:/home/preuss
1 / 4

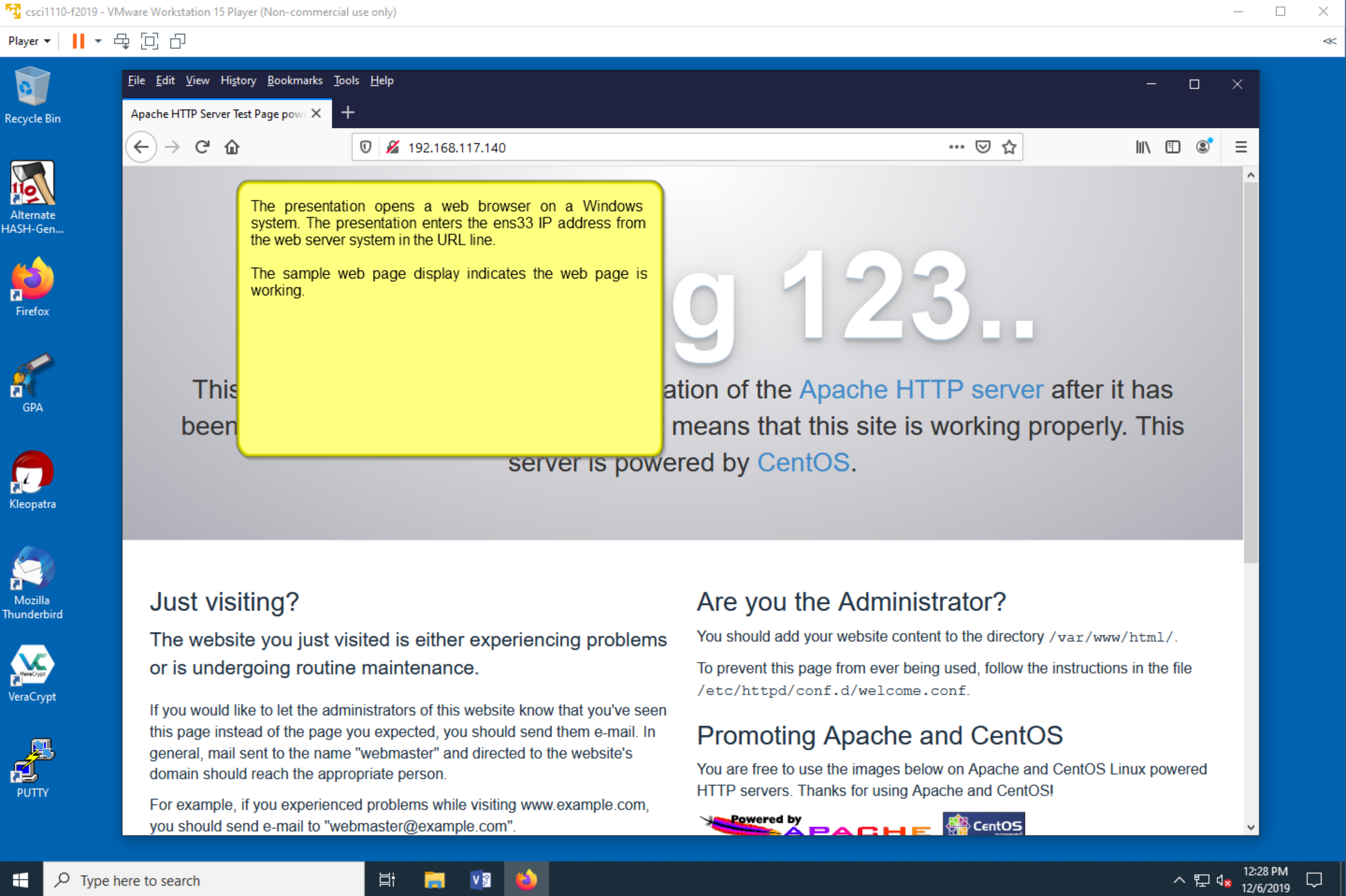
```
  GNU nano 2.3.1                    File: /etc/httpd/conf/httpd.conf

# DocumentRoot: The directory out of which you will serve your
# documents. By default, all requests are taken from this directory, but
# symbolic links and aliases may be used to point to other locations.
#
DocumentRoot "/var/www/html"

#
# Relax access to content within /v
#
<Directory "/var/www">
    AllowOverride None
    # Allow open access:
    Require all granted
</Directory>

# Further relax access to the defau
<Directory "/var/www/html">
    #
    # Possible values for the Optio
    # or any combination of:
    #   Indexes Includes FollowSymLinks SymLinksifOwnerMatch ExecCGI MultiViews
    #
    # Note that "MultiViews" must be named *explicitly* --- "Options All"
    # doesn't give it to you.
    #
    # The Options directive is both complicated and important.  Please see
    # http://httpd.apache.org/docs/2.4/mod/core.html#options
    # for more information.
    #
    Options Indexes FollowSymLinks

    #
    # AllowOverride controls what directives may be placed in .htaccess files.
    # It can be "All", "None", or any combination of the keywords:
    #   Options FileInfo AuthConfig Limit
    #
                     [ line 119/354 (33%), col 29/29 (100%), char 4274/11753 (36%) ]
^G Get Help     ^O WriteOut     ^R Read File    ^Y Prev Page    ^K Cut Text     ^C Cur Pos
^X Exit         ^J Justify      ^W Where Is     ^V Next Page    ^U UnCut Text   ^T To Spell
```

This statement identifies the location of the first web page.


apache01 - VMware Workstation 15 Player (Non-commercial use only)
Player
Applications
Places
Terminal
Fri 12:13
Home
Trash
CentOS 7 x86_64
preuss@apache01:/home/preuss
File
Edit
View
Search
Terminal
Help
preuss@apache01:/home/preuss
1 / 4

```
  GNU nano 2.3.1                    File: /etc/httpd/conf/httpd.conf

    #
    # Controls who can get stuff from this server.
    #
    Require all granted
</Directory>

#
# DirectoryIndex: sets the file that Apache will serve if a directory
# is requested.
#
<IfModule dir_module>
    DirectoryIndex index.html
</IfModule>


#
# The following lines prevent .htacce
# viewed by Web clients.
#
<Files ".ht*">
    Require all denied
</Files>

#
# ErrorLog: The location of the error
# If you do not specify an ErrorLog d
# container, error messages relating
# logged here.  If you *do* define an
# container, that host's errors will be logged there and not here.
#
ErrorLog "logs/error_log"

#
# LogLevel: Control the number of messages logged to the error_log.
# Possible values include: debug, info, notice, warn, error, crit,
# alert, emerg.
#
                    [ line 164/354 (46%), col 30/30 (100%), char 5483/11753 (46%) ]
^G Get Help      ^O WriteOut      ^R Read File     ^Y Prev Page     ^K Cut Text      ^C Cur Pos
^X Exit          ^J Justify       ^W Where Is      ^V Next Page     ^U UnCut Text    ^T To Spell
```

This statement identifies the name of the first web page. In this case, "index.html" is the name of the initial web page to serve if not other page is specificied.


csci1110-f2019 - VMware Workstation 15 Player (Non-commercial use only)
Player
File Edit View History Bookmarks Tools Help
Apache HTTP Server Test Page pow
192.168.117.140
Recycle Bin
Alternate HASH-Gen...
Firefox
GPA
Kleopatra
Mozilla Thunderbird
VeraCrypt
PUTTY
Type here to search
12:28 PM
12/6/2019

The presentation opens a web browser on a Windows system. The presentation enters the ens33 IP address from the web server system in the URL line.

The sample web page display indicates the web page is working.

g 123..

This ation of the Apache HTTP server after it has been means that this site is working properly. This server is powered by CentOS.

Just visiting?

The website you just visited is either experiencing problems or is undergoing routine maintenance.

If you would like to let the administrators of this website know that you've seen this page instead of the page you expected, you should send them e-mail. In general, mail sent to the name "webmaster" and directed to the website's domain should reach the appropriate person.

For example, if you experienced problems while visiting www.example.com, you should send e-mail to "webmaster@example.com".

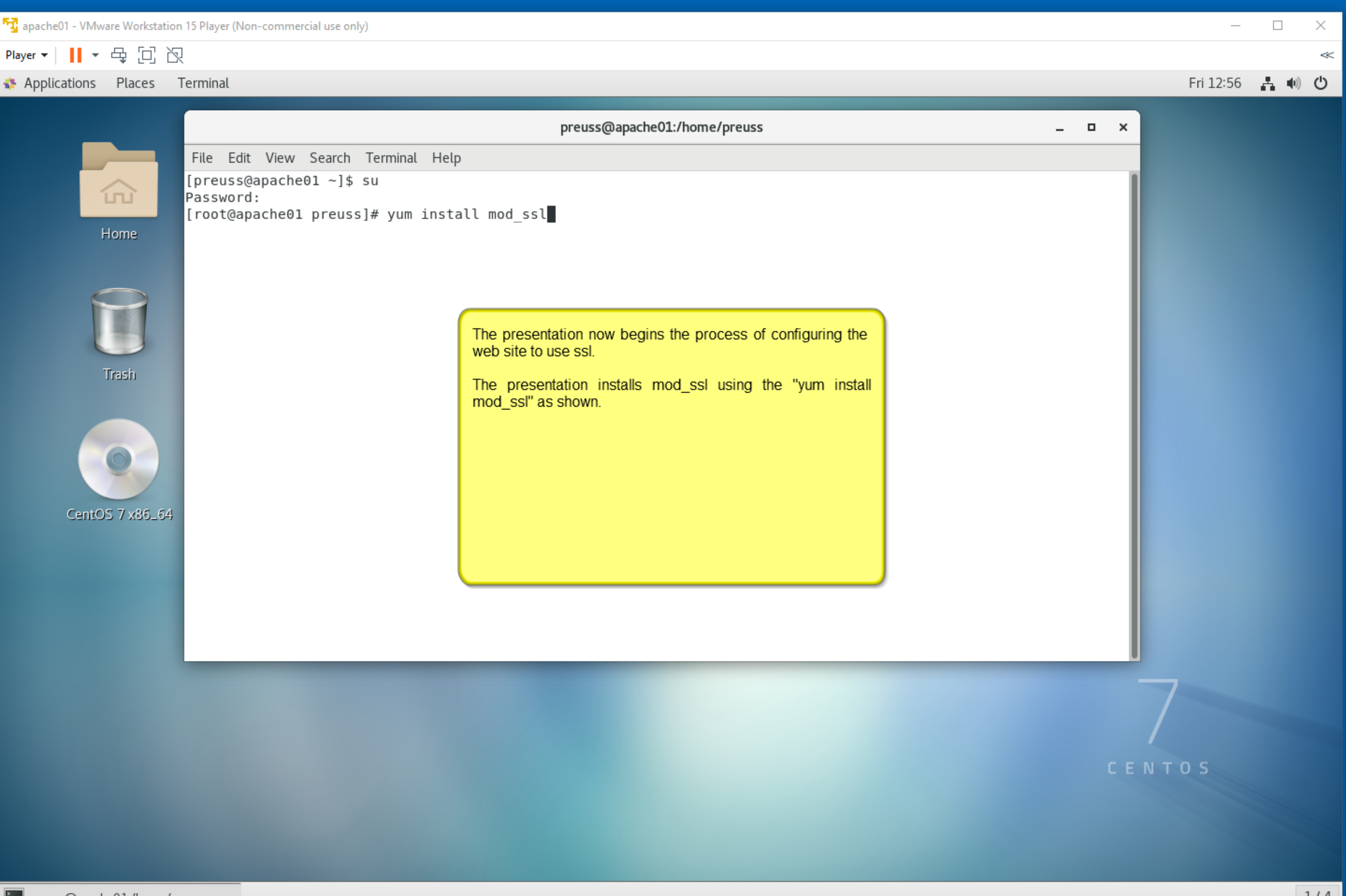
Are you the Administrator?

You should add your website content to the directory `/var/www/html/`.

To prevent this page from ever being used, follow the instructions in the file `/etc/httpd/conf.d/welcome.conf`.

Promoting Apache and CentOS

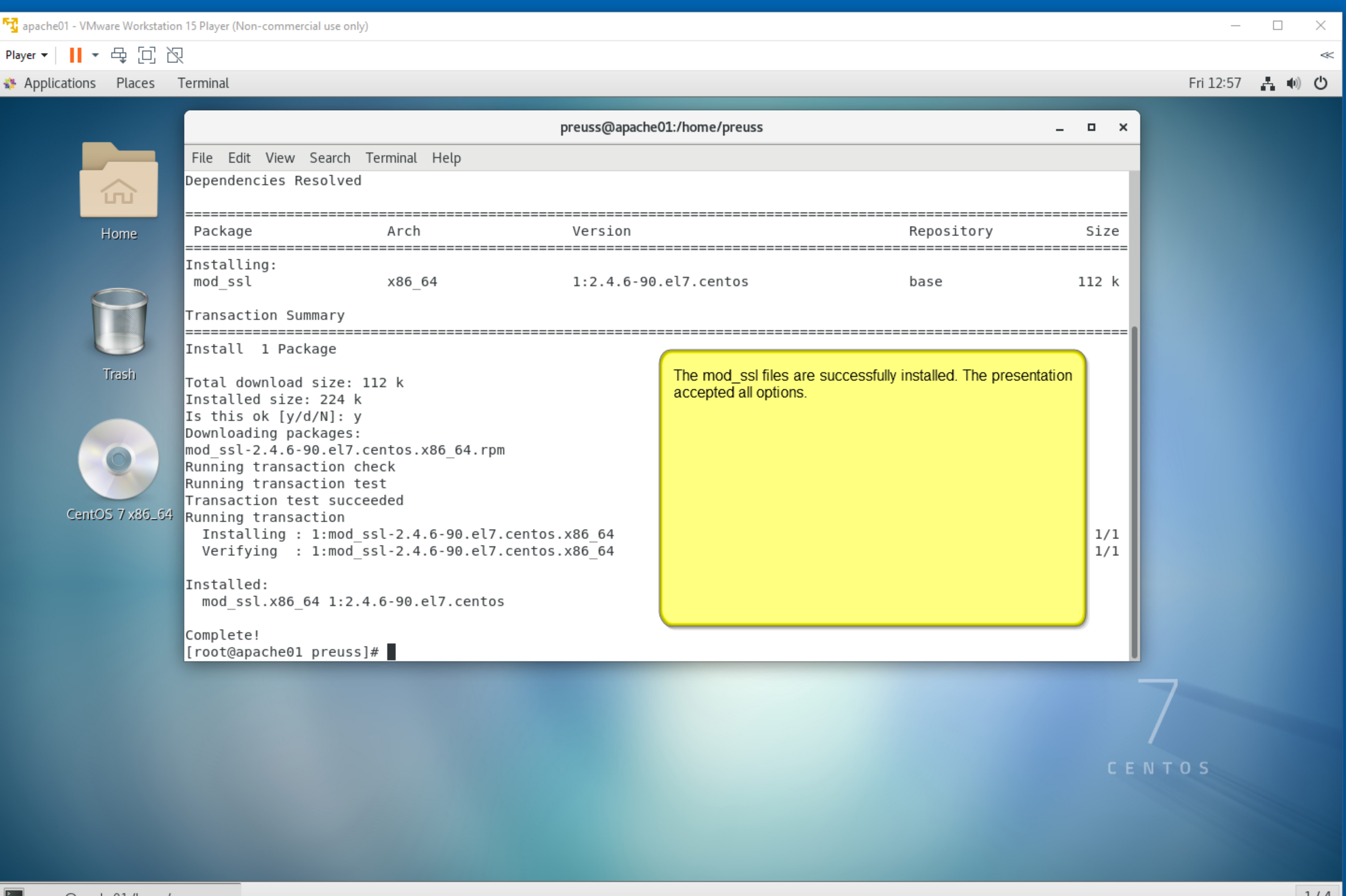
You are free to use the images below on Apache and CentOS Linux powered HTTP servers. Thanks for using Apache and CentOS!



```
[preuss@apache01 ~]$ su
Password:
[root@apache01 preuss]# yum install mod_ssl
```

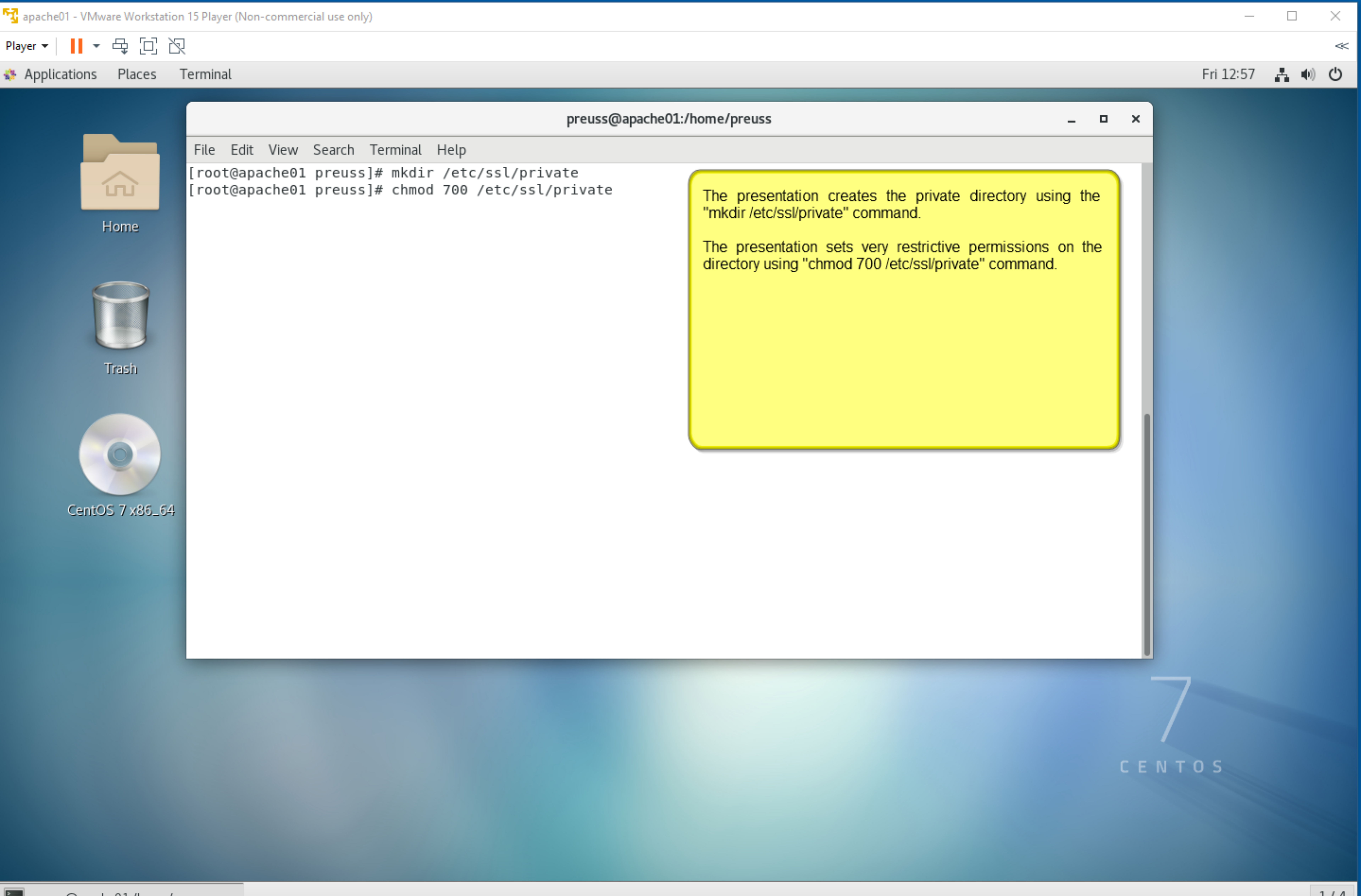
The presentation now begins the process of configuring the web site to use ssl.

The presentation installs mod_ssl using the "yum install mod_ssl" as shown.



```
Dependencies Resolved

================================================================================================================
 Package                Arch                    Version                                 Repository         Size
================================================================================================================
Installing:
 mod_ssl                x86_64                  1:2.4.6-90.el7.centos                   base              112 k

Transaction Summary
================================================================================================================
Install  1 Package

Total download size: 112 k
Installed size: 224 k
Is this ok [y/d/N]: y
Downloading packages:
mod_ssl-2.4.6-90.el7.centos.x86_64.rpm
Running transaction check
Running transaction test
Transaction test succeeded
Running transaction
  Installing : 1:mod_ssl-2.4.6-90.el7.centos.x86_64                                                           1/1
  Verifying  : 1:mod_ssl-2.4.6-90.el7.centos.x86_64                                                           1/1

Installed:
  mod_ssl.x86_64 1:2.4.6-90.el7.centos

Complete!
[root@apache01 preuss]#
```

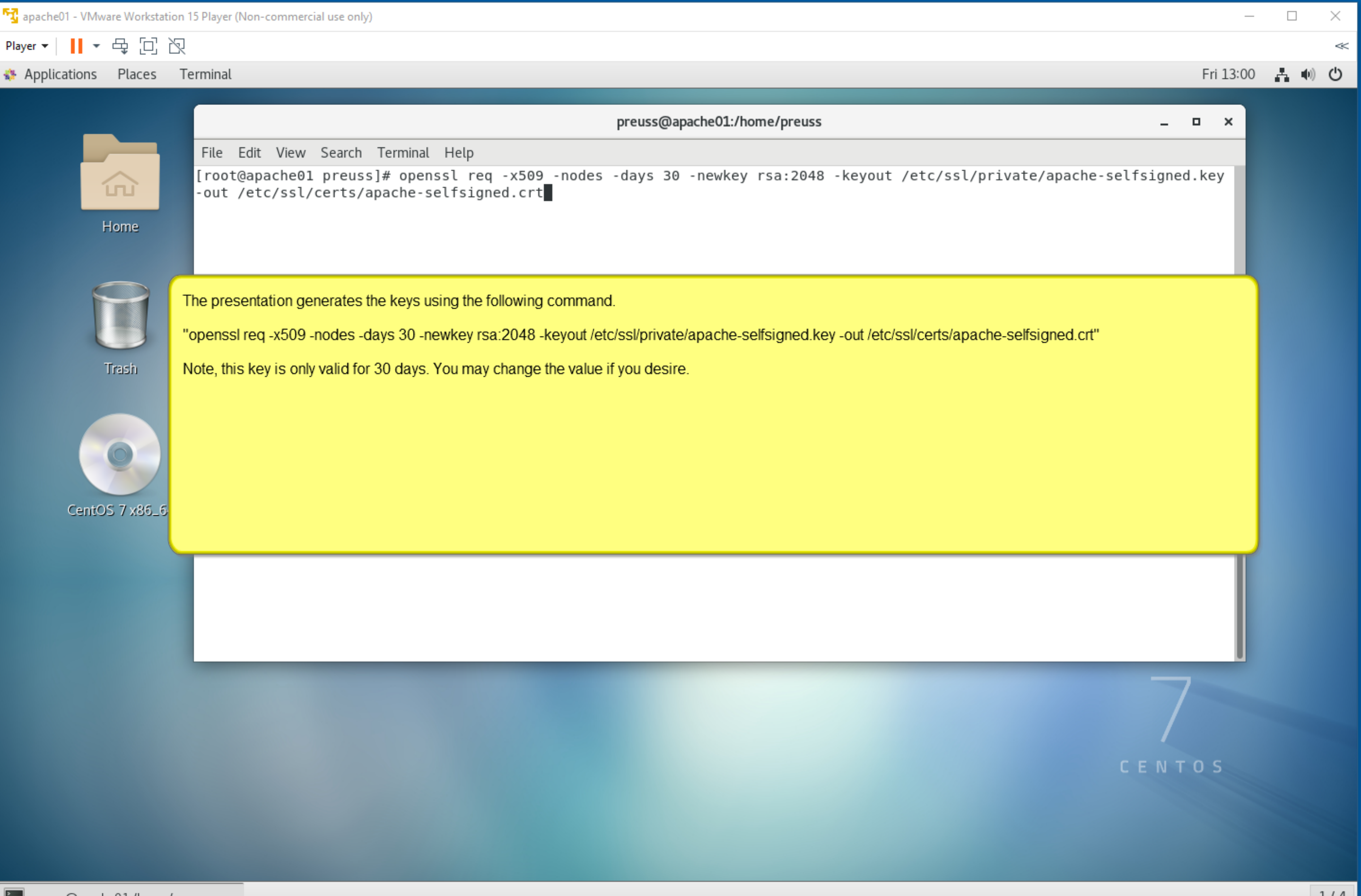
The mod_ssl files are successfully installed. The presentation accepted all options.



```
[root@apache01 preuss]# mkdir /etc/ssl/private
[root@apache01 preuss]# chmod 700 /etc/ssl/private
```

The presentation creates the private directory using the "mkdir /etc/ssl/private" command.

The presentation sets very restrictive permissions on the directory using "chmod 700 /etc/ssl/private" command.

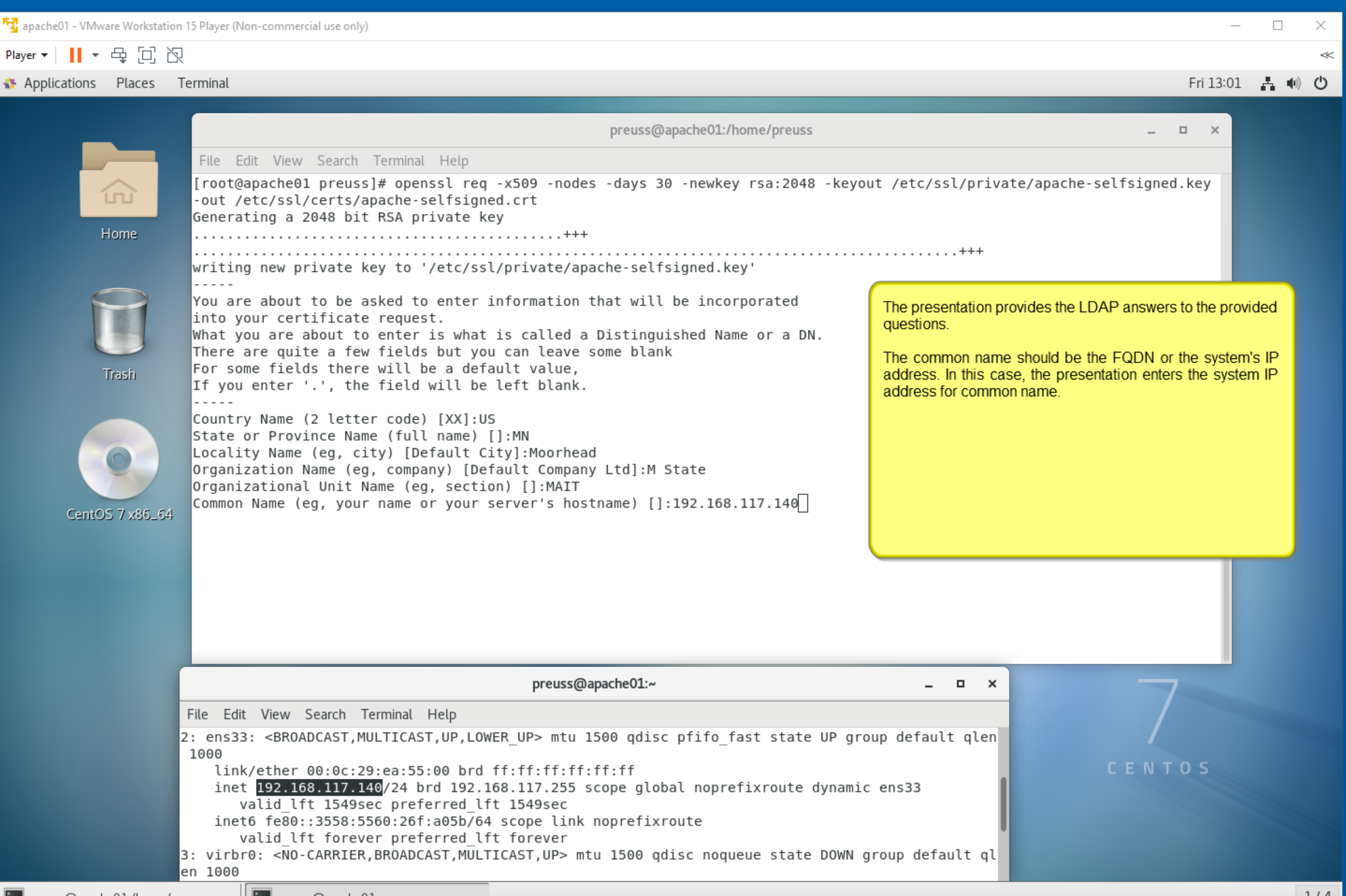


```
[root@apache01 preuss]# openssl req -x509 -nodes -days 30 -newkey rsa:2048 -keyout /etc/ssl/private/apache-selfsigned.key
-out /etc/ssl/certs/apache-selfsigned.crt
```

The presentation generates the keys using the following command.

"openssl req -x509 -nodes -days 30 -newkey rsa:2048 -keyout /etc/ssl/private/apache-selfsigned.key -out /etc/ssl/certs/apache-selfsigned.crt"

Note, this key is only valid for 30 days. You may change the value if you desire.

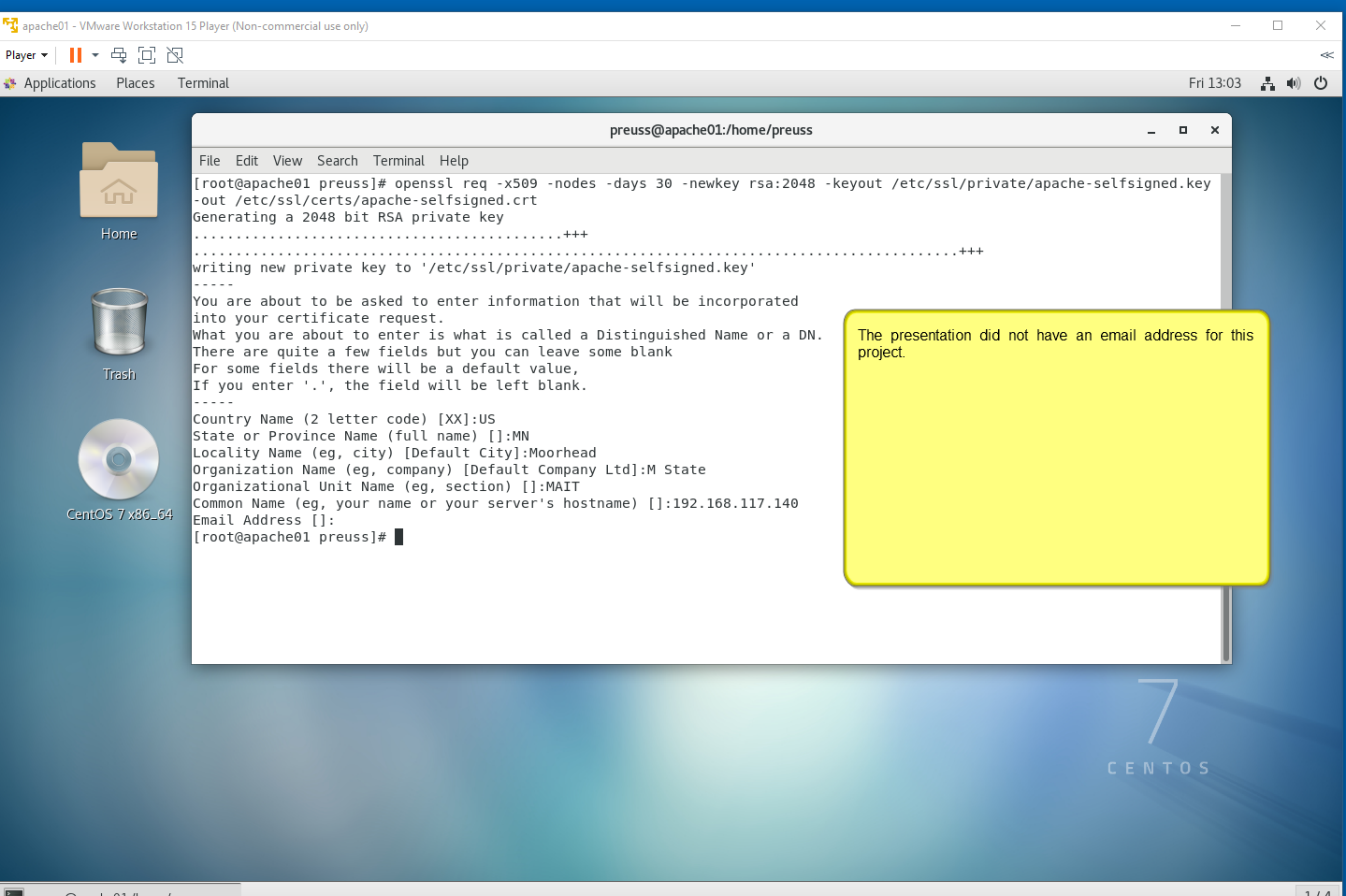

apache01 - VMware Workstation 15 Player (Non-commercial use only)
Player
Applications
Places
Terminal
Fri 13:01
Home
Trash
CentOS 7 x86_64
preuss@apache01:/home/preuss
File Edit View Search Terminal Help
preuss@apache01:~
7 CENTOS

```
[root@apache01 preuss]# openssl req -x509 -nodes -days 30 -newkey rsa:2048 -keyout /etc/ssl/private/apache-selfsigned.key
-out /etc/ssl/certs/apache-selfsigned.crt
Generating a 2048 bit RSA private key
.....................................+++
..............................................................................+++
writing new private key to '/etc/ssl/private/apache-selfsigned.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) [XX]:US
State or Province Name (full name) []:MN
Locality Name (eg, city) [Default City]:Moorhead
Organization Name (eg, company) [Default Company Ltd]:M State
Organizational Unit Name (eg, section) []:MAIT
Common Name (eg, your name or your server's hostname) []:192.168.117.140
```

The presentation provides the LDAP answers to the provided questions.

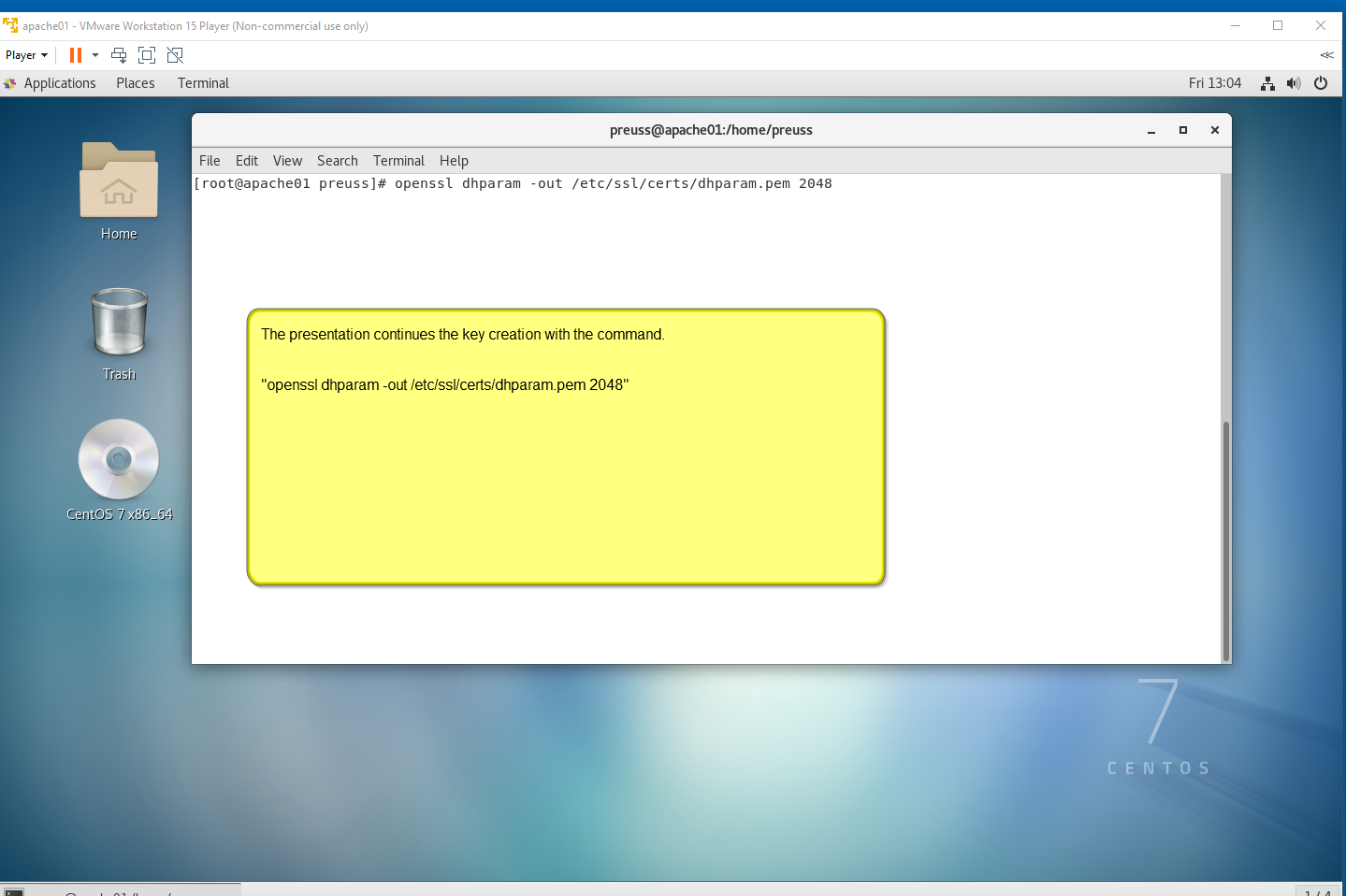
The common name should be the FQDN or the system's IP address. In this case, the presentation enters the system IP address for common name.

```
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen
 1000
    link/ether 00:0c:29:ea:55:00 brd ff:ff:ff:ff:ff:ff
    inet 192.168.117.140/24 brd 192.168.117.255 scope global noprefixroute dynamic ens33
       valid_lft 1549sec preferred_lft 1549sec
    inet6 fe80::3558:5560:26f:a05b/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
3: virbr0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default ql
en 1000
```



```
[root@apache01 preuss]# openssl req -x509 -nodes -days 30 -newkey rsa:2048 -keyout /etc/ssl/private/apache-selfsigned.key
-out /etc/ssl/certs/apache-selfsigned.crt
Generating a 2048 bit RSA private key
.............................................+++
..............................................................................................+++
writing new private key to '/etc/ssl/private/apache-selfsigned.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) [XX]:US
State or Province Name (full name) []:MN
Locality Name (eg, city) [Default City]:Moorhead
Organization Name (eg, company) [Default Company Ltd]:M State
Organizational Unit Name (eg, section) []:MAIT
Common Name (eg, your name or your server's hostname) []:192.168.117.140
Email Address []:
[root@apache01 preuss]# 
```

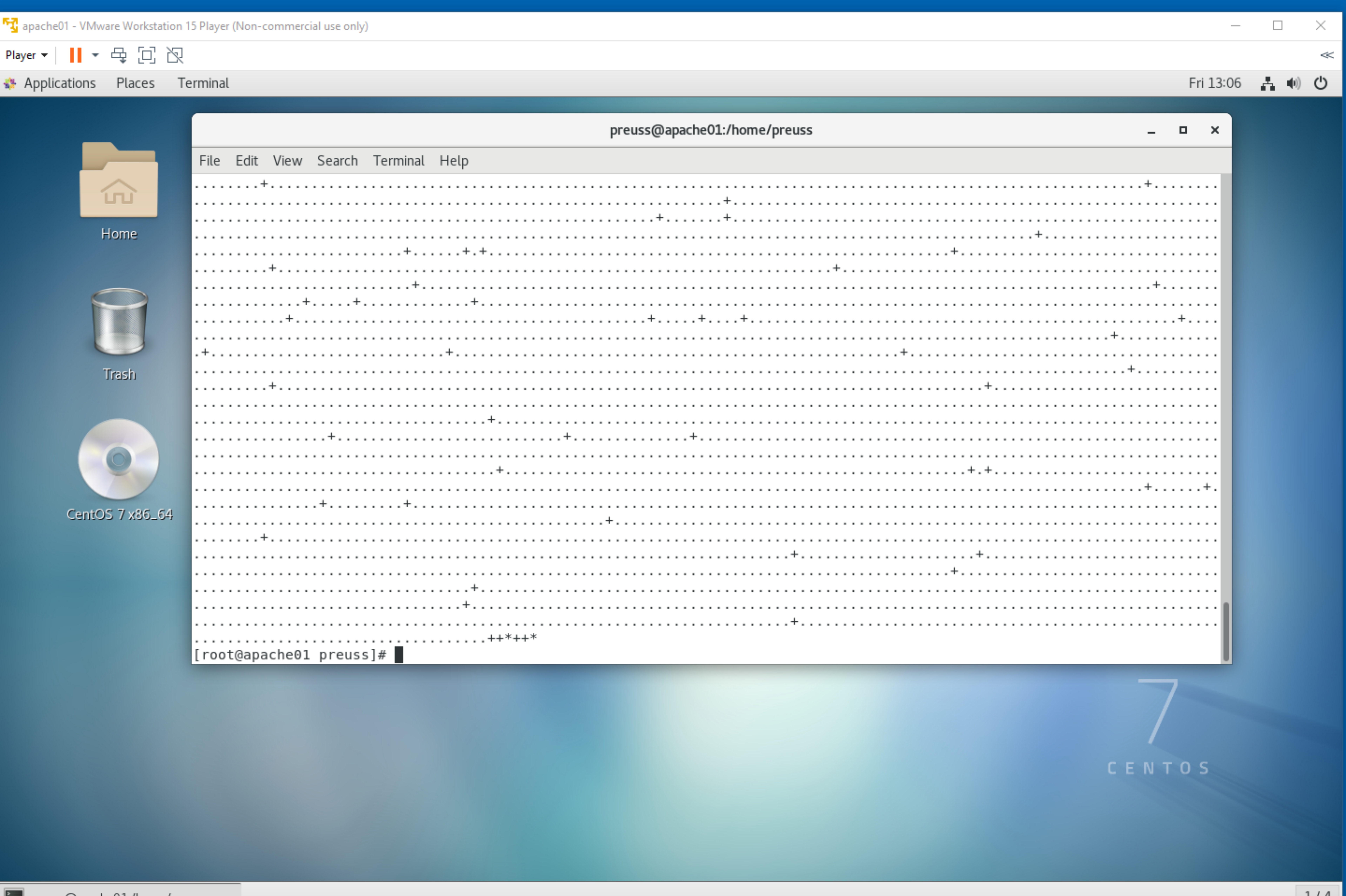
The presentation did not have an email address for this project.



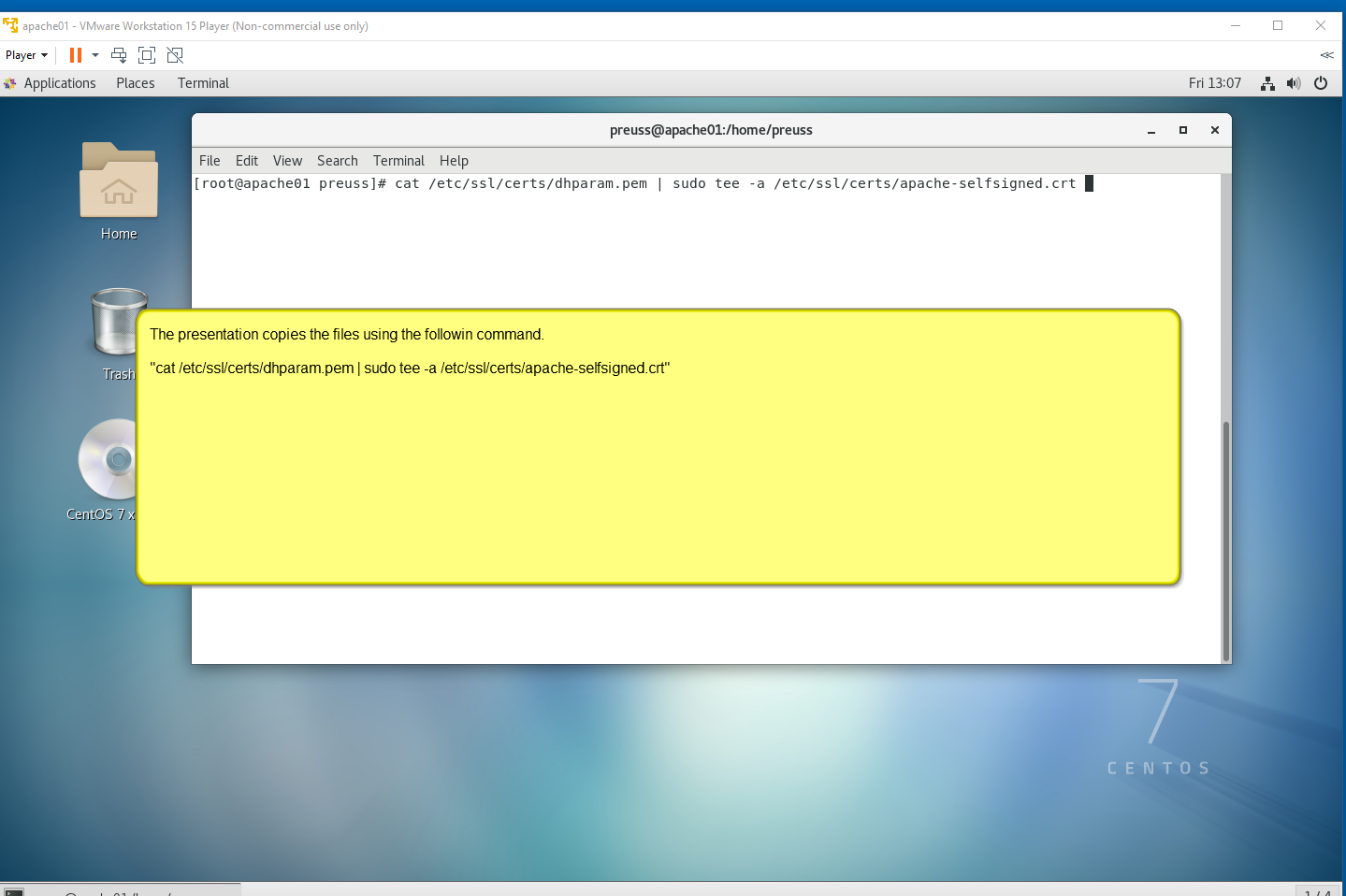
```
[root@apache01 preuss]# openssl dhparam -out /etc/ssl/certs/dhparam.pem 2048
```

The presentation continues the key creation with the command.

"openssl dhparam -out /etc/ssl/certs/dhparam.pem 2048"



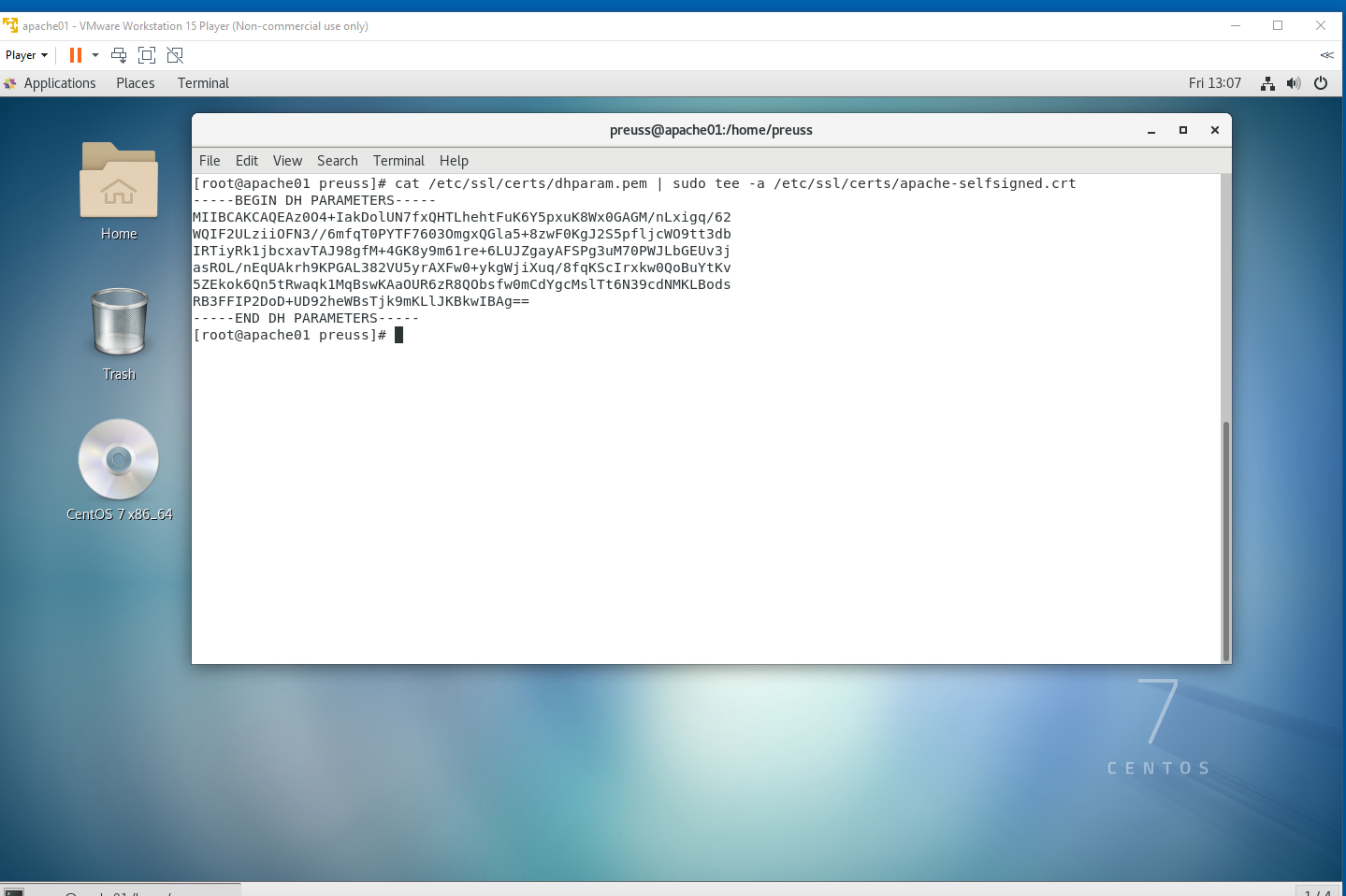
```
........+........................................................................................................+........
...............................................................+..........................................................
.......................................................+.......+..........................................................
....................................................................................................+.....................
.........................+......+.+.......................................................+...............................
.........+..................................................................+.............................................
..........................+.......................................................................................+.......
.............+.....+.............+........................................................................................
...........+..........................................+.....+....+...................................................+....
.............................................................................................................+............
.+............................+.....................................................+.....................................
...............................................................................................................+..........
.........+....................................................................................+...........................
..........................................................................................................................
...................................+......................................................................................
................+...........................+..............+..............................................................
..........................................................................................................................
....................................+.......................................................+.+...........................
.................................................................................................................+......+.
...............+.........+................................................................................................
.................................................+........................................................................
........+.................................................................................................................
.......................................................................+.....................+............................
..........................................................................................+...............................
.................................+........................................................................................
................................+.........................................................................................
.......................................................................+..................................................
...................................++*++*
[root@apache01 preuss]# 
```



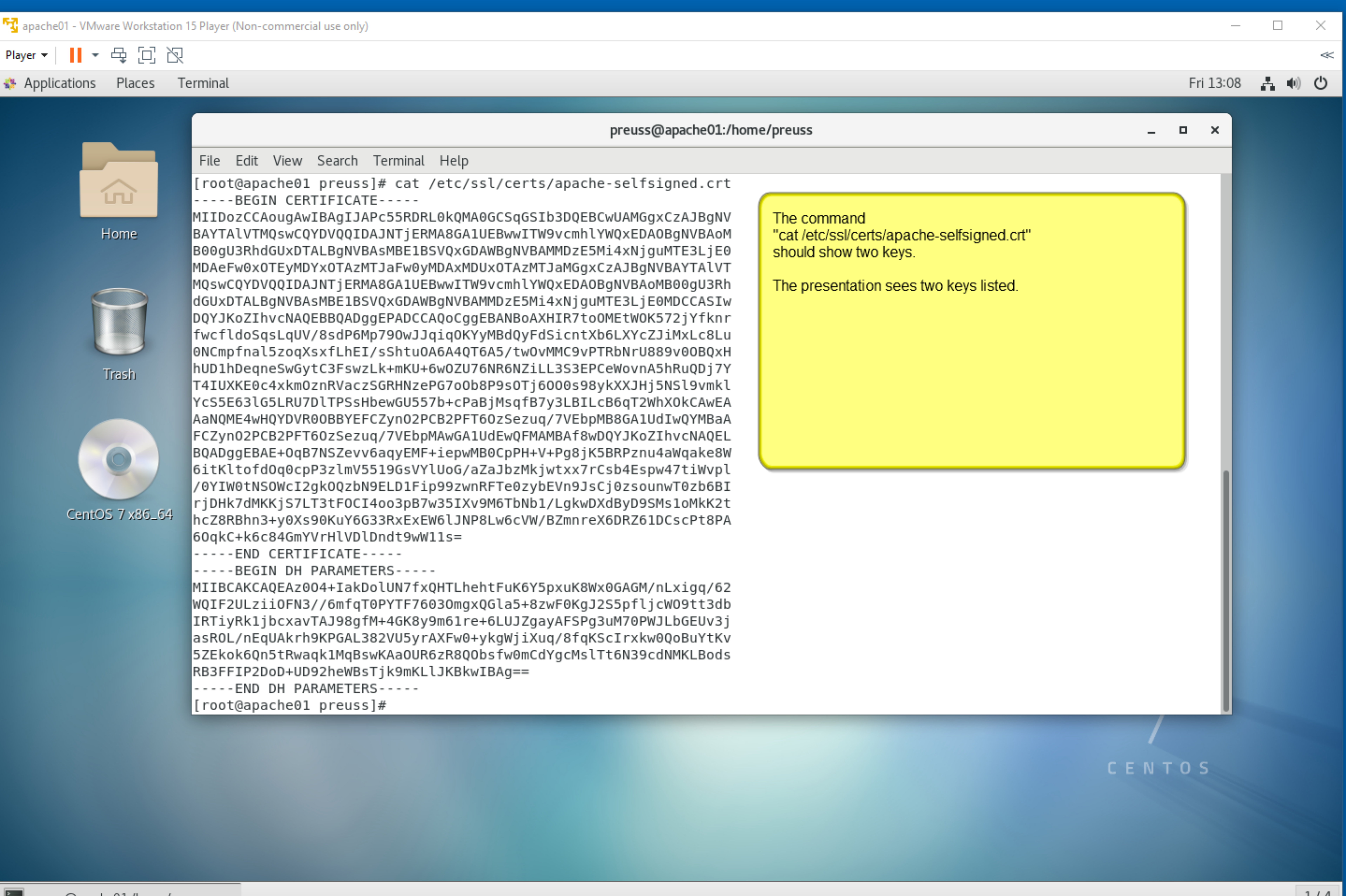
```
[root@apache01 preuss]# cat /etc/ssl/certs/dhparam.pem | sudo tee -a /etc/ssl/certs/apache-selfsigned.crt
```

The presentation copies the files using the followin command.

"cat /etc/ssl/certs/dhparam.pem | sudo tee -a /etc/ssl/certs/apache-selfsigned.crt"



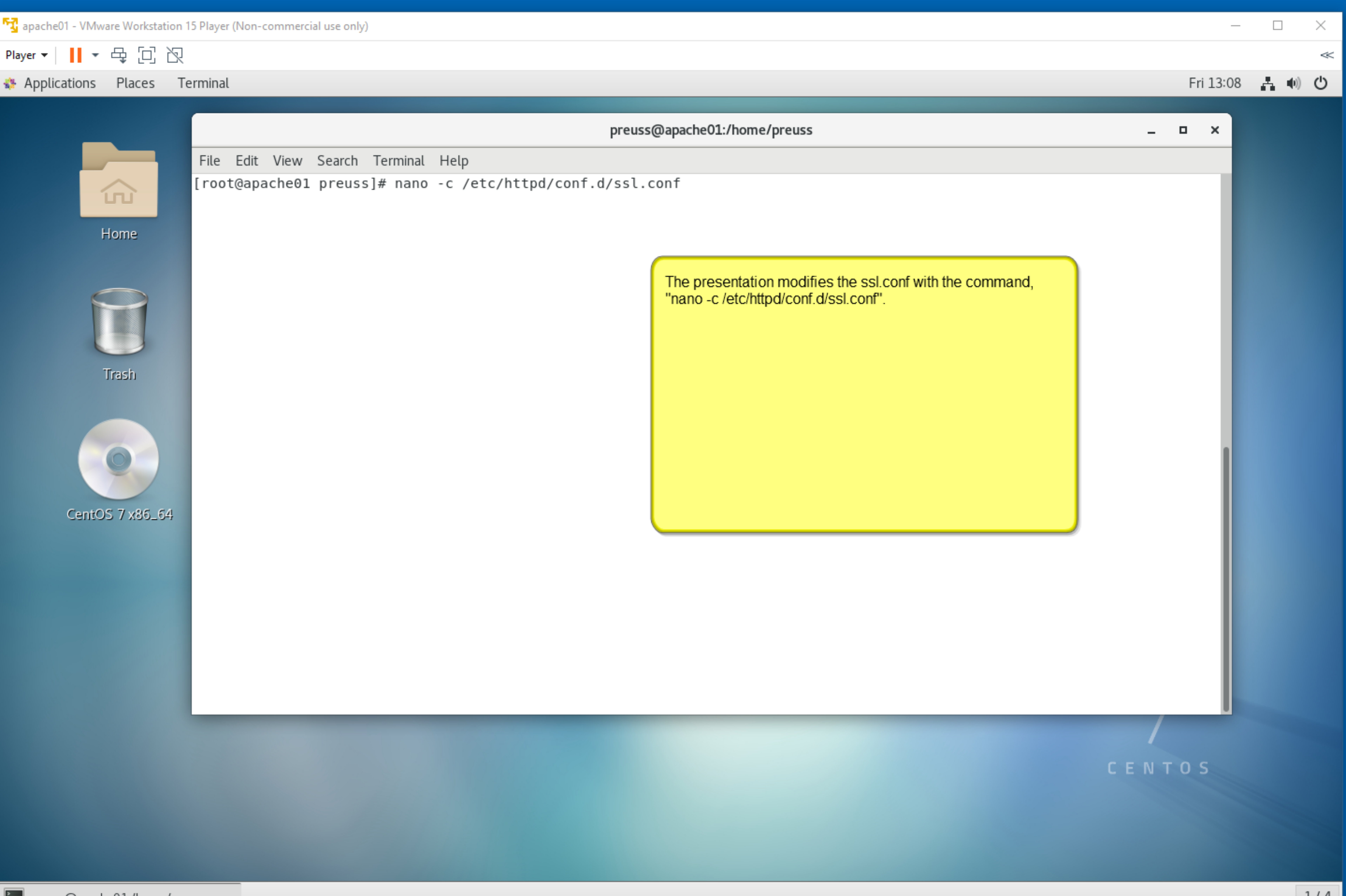
```
[root@apache01 preuss]# cat /etc/ssl/certs/dhparam.pem | sudo tee -a /etc/ssl/certs/apache-selfsigned.crt
-----BEGIN DH PARAMETERS-----
MIIBCAKCAQEAz0O4+IakDolUN7fxQHTLhehtFuK6Y5pxuK8Wx0GAGM/nLxigq/62
WQIF2ULziiOFN3//6mfqT0PYTF7603OmgxQGla5+8zwF0KgJ2S5pfljcWO9tt3db
IRTiyRk1jbcxavTAJ98gfM+4GK8y9m61re+6LUJZgayAFSPg3uM70PWJLbGEUv3j
asROL/nEqUAkrh9KPGAL382VU5yrAXFw0+ykgWjiXuq/8fqKScIrxkw0QoBuYtKv
5ZEkok6Qn5tRwaqk1MqBswKAaOUR6zR8QObsfw0mCdYgcMslTt6N39cdNMKLBods
RB3FFIP2DoD+UD92heWBsTjk9mKLlJKBkwIBAg==
-----END DH PARAMETERS-----
[root@apache01 preuss]# 
```



```
[root@apache01 preuss]# cat /etc/ssl/certs/apache-selfsigned.crt
-----BEGIN CERTIFICATE-----
MIIDozCCAougAwIBAgIJAPc55RDRL0kQMA0GCSqGSIb3DQEBCwUAMGgxCzAJBgNV
BAYTAlVTMQswCQYDVQQIDAJNTjERMA8GA1UEBwwITW9vcmhlYWQxEDAOBgNVBAoM
B00gU3RhdGUxDTALBgNVBAsMBE1BSVQxGDAWBgNVBAMMDzE5Mi4xNjguMTE3LjE0
MDAeFw0xOTEyMDYxOTAzMTJaFw0yMDAxMDUxOTAzMTJaMGgxCzAJBgNVBAYTAlVT
MQswCQYDVQQIDAJNTjERMA8GA1UEBwwITW9vcmhlYWQxEDAOBgNVBAoMB00gU3Rh
dGUxDTALBgNVBAsMBE1BSVQxGDAWBgNVBAMMDzE5Mi4xNjguMTE3LjE0MDCCASIw
DQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBANBoAXHIR7toOMEtWOK572jYfknr
fwcfldoSqsLqUV/8sdP6Mp79OwJJqiqOKYyMBdQyFdSicntXb6LXYcZJiMxLc8Lu
0NCmpfnal5zoqXsxfLhEI/sShtuOA6A4QT6A5/twOvMMC9vPTRbNrU889v0OBQxH
hUD1hDeqneSwGytC3FswzLk+mKU+6wOZU76NR6NZiLL3S3EPCeWovnA5hRuQDj7Y
T4IUXKE0c4xkmOznRVaczSGRHNzePG7oOb8P9sOTj6OO0s98ykXXJHj5NSl9vmkl
YcS5E63lG5LRU7DlTPSsHbewGU557b+cPaBjMsqfB7y3LBILcB6qT2WhXOkCAwEA
AaNQME4wHQYDVR0OBBYEFCZynO2PCB2PFT6OzSezuq/7VEbpMB8GA1UdIwQYMBaA
FCZynO2PCB2PFT6OzSezuq/7VEbpMAwGA1UdEwQFMAMBAf8wDQYJKoZIhvcNAQEL
BQADggEBAE+OqB7NSZevv6aqyEMF+iepwMB0CpPH+V+Pg8jK5BRPznu4aWqake8W
6itKltofdOq0cpP3zlmV5519GsVYlUoG/aZaJbzMkjwtxx7rCsb4Espw47tiWvpl
/0YIW0tNSOWcI2gkOQzbN9ELD1Fip99zwnRFTe0zybEVn9JsCj0zsounwT0zb6BI
rjDHk7dMKKjS7LT3tFOCI4oo3pB7w35IXv9M6TbNb1/LgkwDXdByD9SMs1oMkK2t
hcZ8RBhn3+y0Xs90KuY6G33RxExEW6lJNP8Lw6cVW/BZmnreX6DRZ61DCscPt8PA
6OqkC+k6c84GmYVrHlVDlDndt9wW11s=
-----END CERTIFICATE-----
-----BEGIN DH PARAMETERS-----
MIIBCAKCAQEAz0O4+IakDolUN7fxQHTLhehtFuK6Y5pxuK8Wx0GAGM/nLxigq/62
WQIF2ULziiOFN3//6mfqT0PYTF7603OmgxQGla5+8zwF0KgJ2S5pfljcWO9tt3db
IRTiyRk1jbcxavTAJ98gfM+4GK8y9m61re+6LUJZgayAFSPg3uM70PWJLbGEUv3j
asROL/nEqUAkrh9KPGAL382VU5yrAXFw0+ykgWjiXuq/8fqKScIrxkw0QoBuYtKv
5ZEkok6Qn5tRwaqk1MqBswKAaOUR6zR8QObsfw0mCdYgcMslTt6N39cdNMKLBods
RB3FFIP2DoD+UD92heWBsTjk9mKLlJKBkwIBAg==
-----END DH PARAMETERS-----
[root@apache01 preuss]#
```

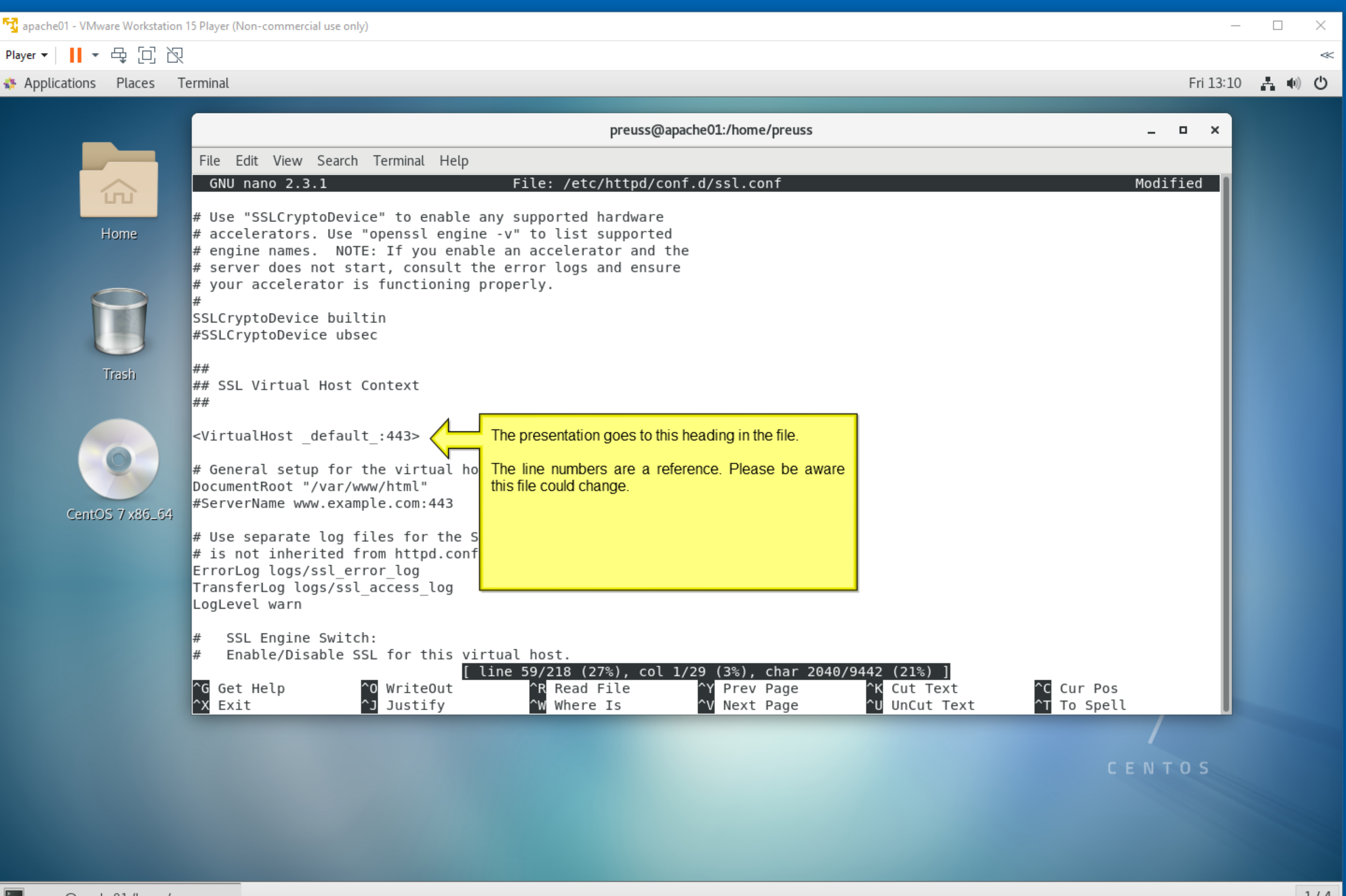
The command
"cat /etc/ssl/certs/apache-selfsigned.crt"
should show two keys.

The presentation sees two keys listed.



```
[root@apache01 preuss]# nano -c /etc/httpd/conf.d/ssl.conf
```

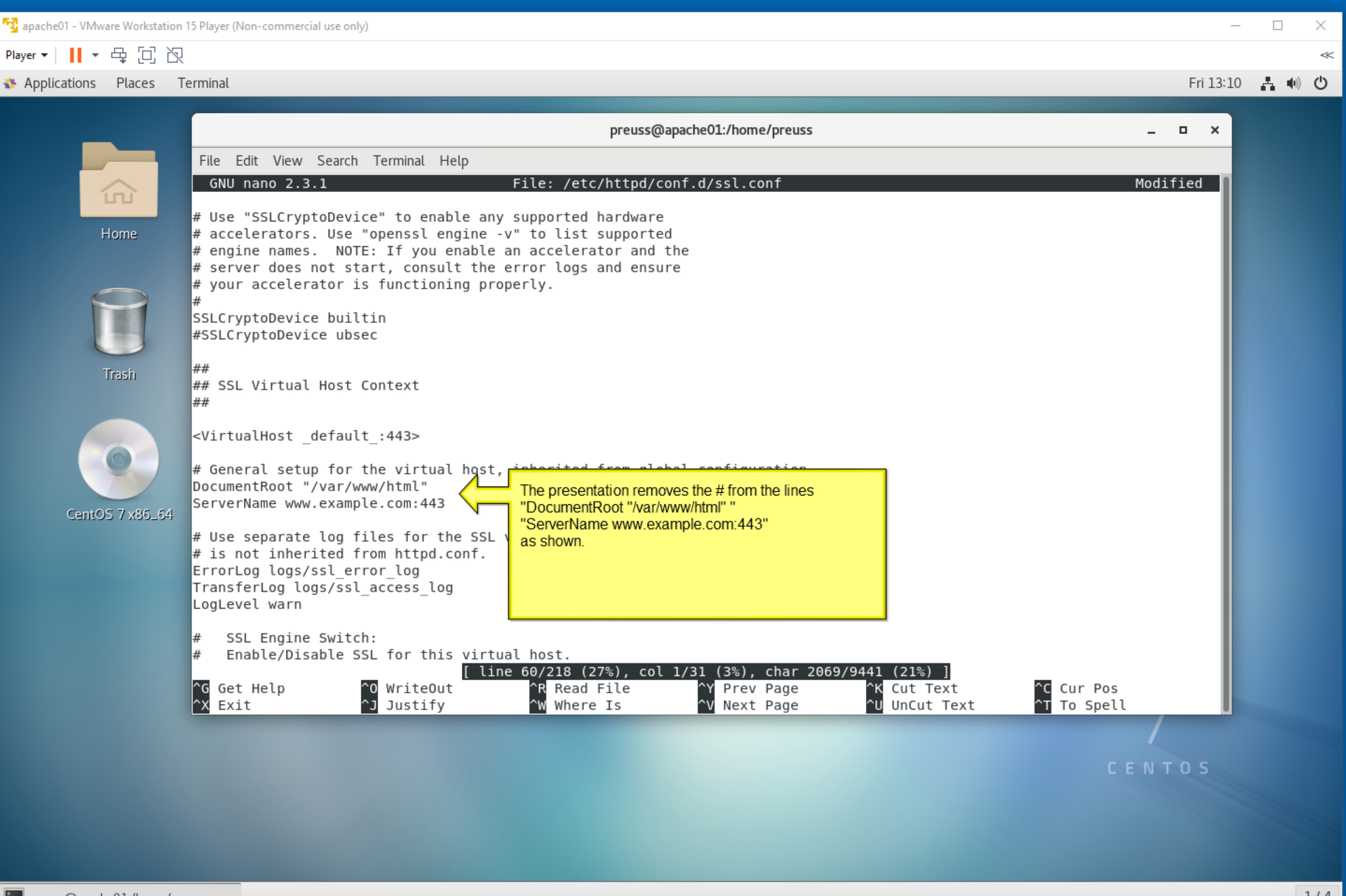
The presentation modifies the ssl.conf with the command, "nano -c /etc/httpd/conf.d/ssl.conf".



```
  GNU nano 2.3.1              File: /etc/httpd/conf.d/ssl.conf                      Modified

# Use "SSLCryptoDevice" to enable any supported hardware
# accelerators. Use "openssl engine -v" to list supported
# engine names.  NOTE: If you enable an accelerator and the
# server does not start, consult the error logs and ensure
# your accelerator is functioning properly.
#
SSLCryptoDevice builtin
#SSLCryptoDevice ubsec

##
## SSL Virtual Host Context
##

<VirtualHost _default_:443>

# General setup for the virtual ho
DocumentRoot "/var/www/html"
#ServerName www.example.com:443

# Use separate log files for the S
# is not inherited from httpd.conf
ErrorLog logs/ssl_error_log
TransferLog logs/ssl_access_log
LogLevel warn

#   SSL Engine Switch:
#   Enable/Disable SSL for this virtual host.
                [ line 59/218 (27%), col 1/29 (3%), char 2040/9442 (21%) ]
^G Get Help      ^O WriteOut      ^R Read File     ^Y Prev Page     ^K Cut Text      ^C Cur Pos
^X Exit          ^J Justify       ^W Where Is      ^V Next Page     ^U UnCut Text    ^T To Spell
```

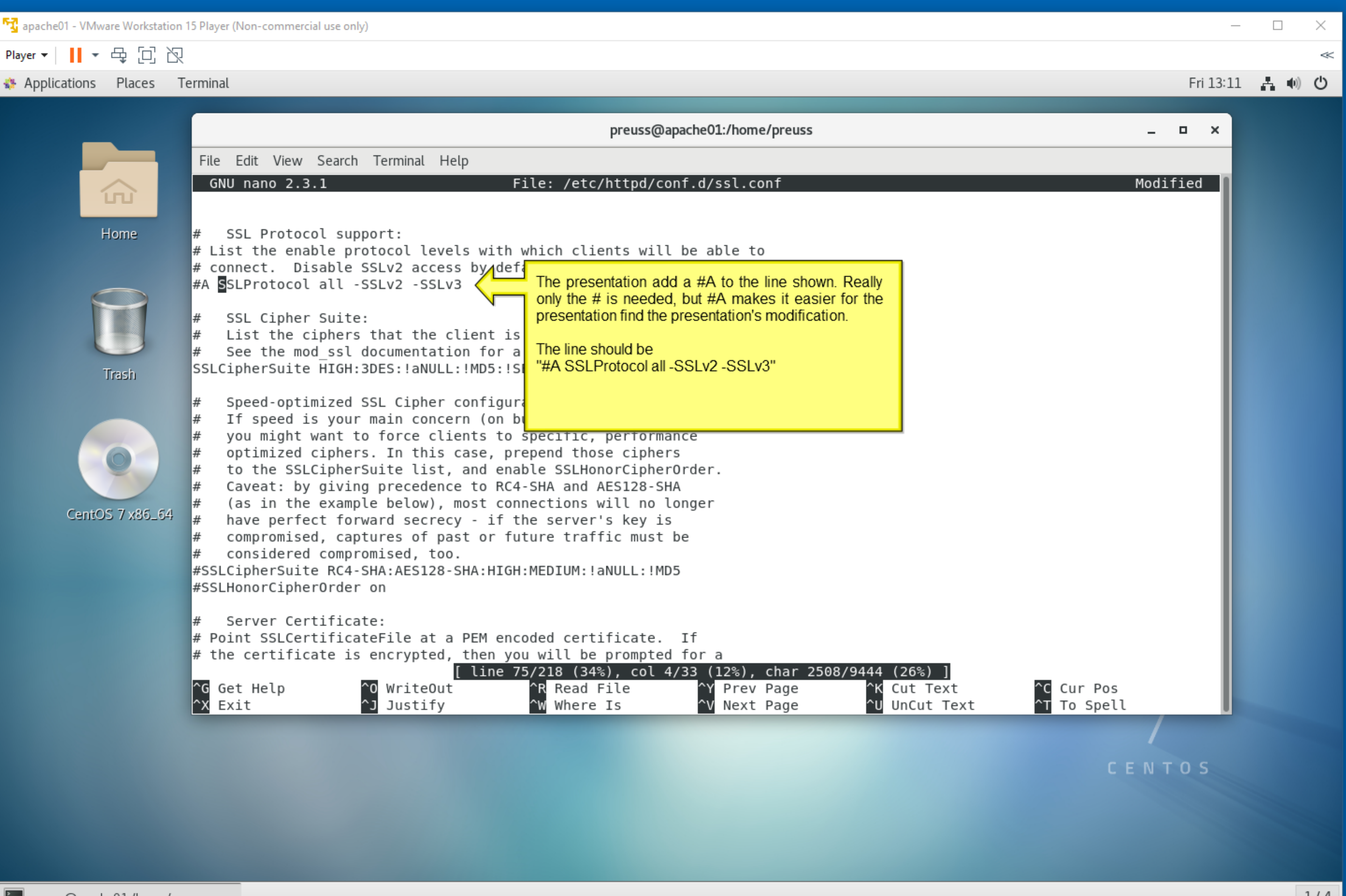
The presentation goes to this heading in the file.

The line numbers are a reference. Please be aware this file could change.



```
  GNU nano 2.3.1              File: /etc/httpd/conf.d/ssl.conf                  Modified

# Use "SSLCryptoDevice" to enable any supported hardware
# accelerators. Use "openssl engine -v" to list supported
# engine names.  NOTE: If you enable an accelerator and the
# server does not start, consult the error logs and ensure
# your accelerator is functioning properly.
#
SSLCryptoDevice builtin
#SSLCryptoDevice ubsec

##
## SSL Virtual Host Context
##

<VirtualHost _default_:443>

# General setup for the virtual host, inherited from global configuration
DocumentRoot "/var/www/html"
ServerName www.example.com:443

# Use separate log files for the SSL v
# is not inherited from httpd.conf.
ErrorLog logs/ssl_error_log
TransferLog logs/ssl_access_log
LogLevel warn

#   SSL Engine Switch:
#   Enable/Disable SSL for this virtual host.
                              [ line 60/218 (27%), col 1/31 (3%), char 2069/9441 (21%) ]
^G Get Help      ^O WriteOut      ^R Read File     ^Y Prev Page     ^K Cut Text      ^C Cur Pos
^X Exit          ^J Justify       ^W Where Is      ^V Next Page     ^U UnCut Text    ^T To Spell
```

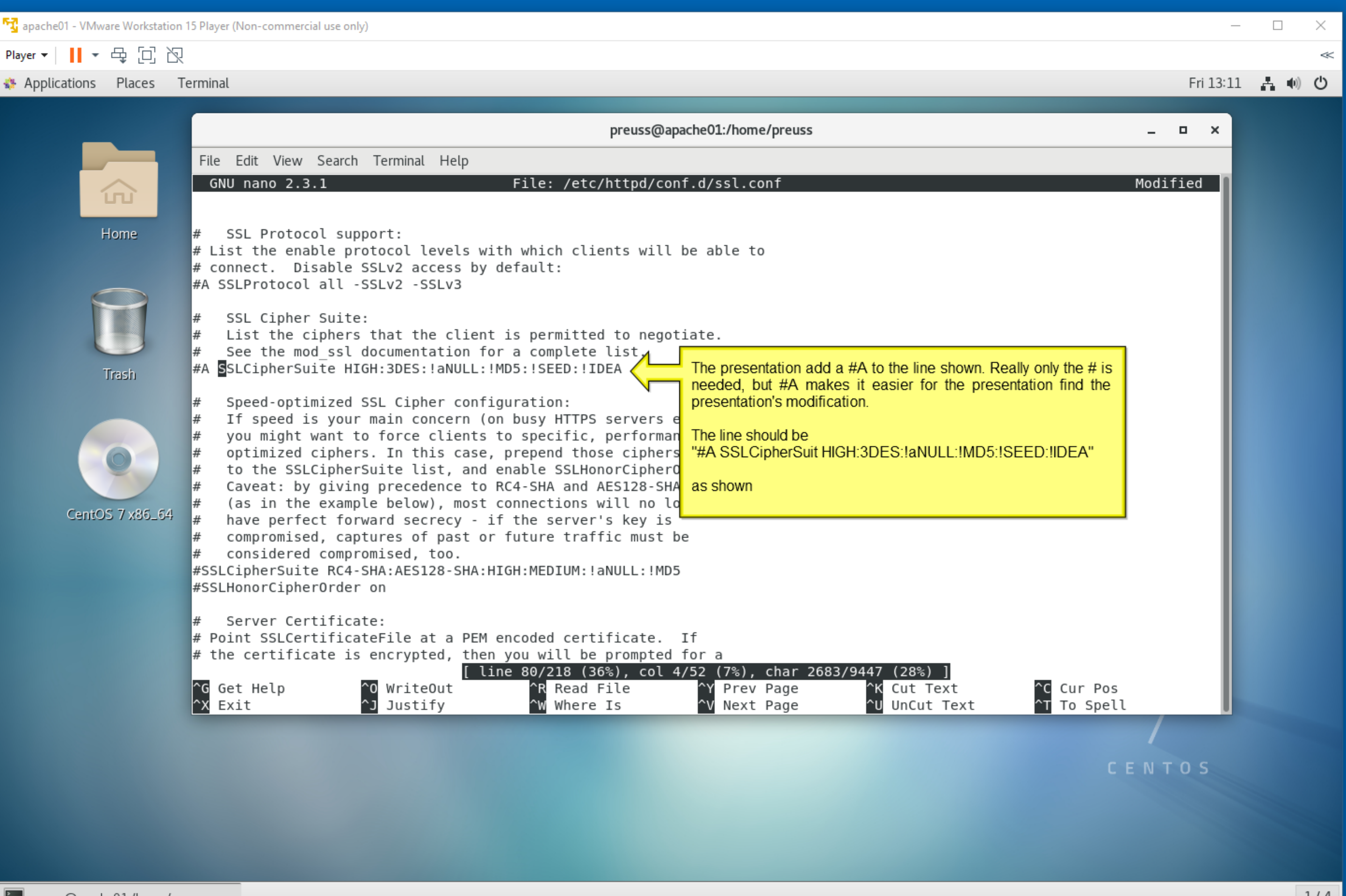
The presentation removes the # from the lines
"DocumentRoot "/var/www/html" "
"ServerName www.example.com:443"
as shown.



```
  GNU nano 2.3.1                 File: /etc/httpd/conf.d/ssl.conf                              Modified


#   SSL Protocol support:
# List the enable protocol levels with which clients will be able to
# connect.  Disable SSLv2 access by defa
#A SSLProtocol all -SSLv2 -SSLv3

#   SSL Cipher Suite:
#   List the ciphers that the client is
#   See the mod_ssl documentation for a
SSLCipherSuite HIGH:3DES:!aNULL:!MD5:!SE

#   Speed-optimized SSL Cipher configura
#   If speed is your main concern (on bu
#   you might want to force clients to specific, performance
#   optimized ciphers. In this case, prepend those ciphers
#   to the SSLCipherSuite list, and enable SSLHonorCipherOrder.
#   Caveat: by giving precedence to RC4-SHA and AES128-SHA
#   (as in the example below), most connections will no longer
#   have perfect forward secrecy - if the server's key is
#   compromised, captures of past or future traffic must be
#   considered compromised, too.
#SSLCipherSuite RC4-SHA:AES128-SHA:HIGH:MEDIUM:!aNULL:!MD5
#SSLHonorCipherOrder on

#   Server Certificate:
# Point SSLCertificateFile at a PEM encoded certificate.  If
# the certificate is encrypted, then you will be prompted for a
                           [ line 75/218 (34%), col 4/33 (12%), char 2508/9444 (26%) ]
^G Get Help         ^O WriteOut         ^R Read File        ^Y Prev Page        ^K Cut Text         ^C Cur Pos
^X Exit             ^J Justify          ^W Where Is         ^V Next Page        ^U UnCut Text       ^T To Spell
```

The presentation add a #A to the line shown. Really only the # is needed, but #A makes it easier for the presentation find the presentation's modification.

The line should be
"#A SSLProtocol all -SSLv2 -SSLv3"

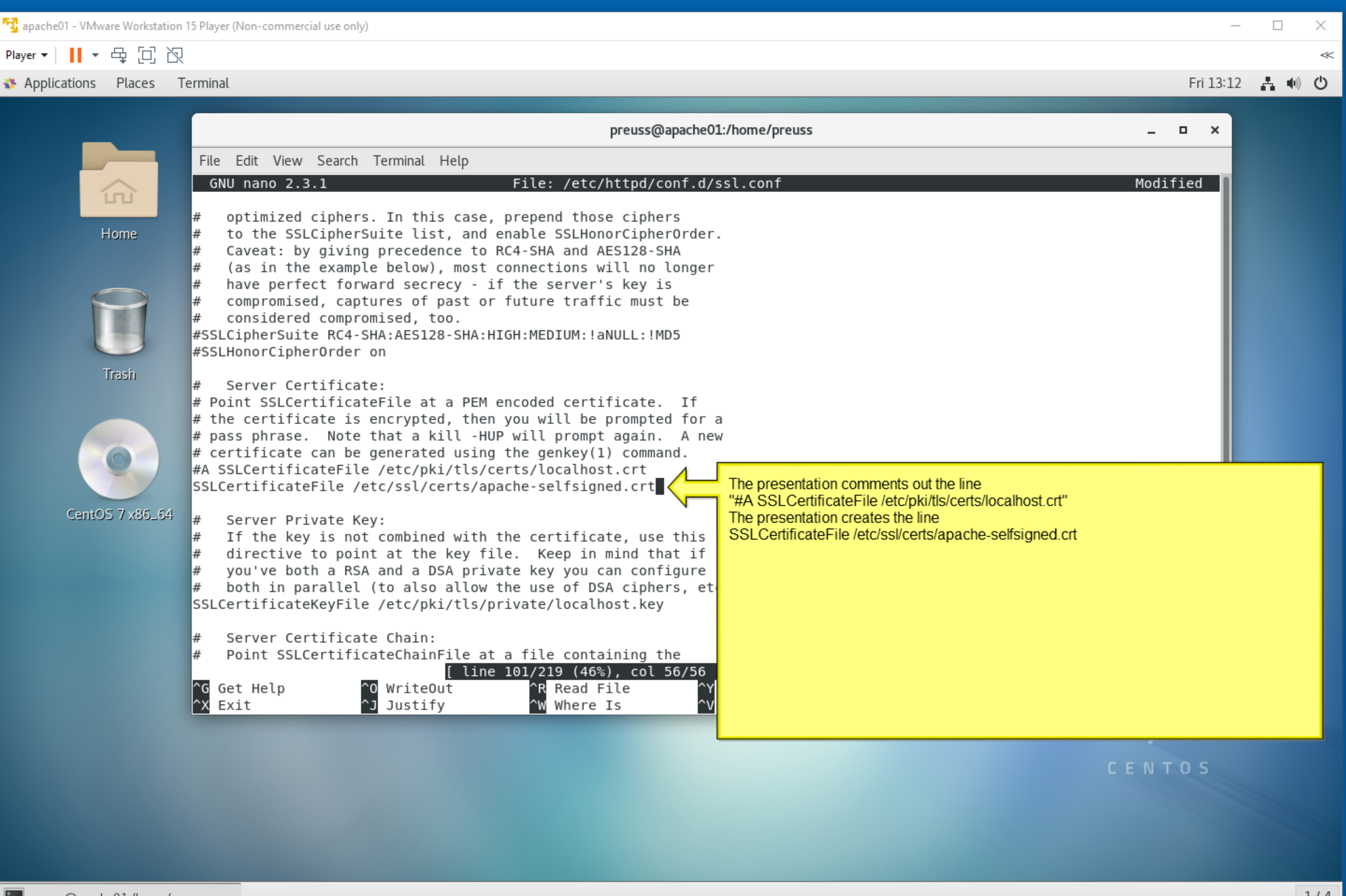


```
  GNU nano 2.3.1                 File: /etc/httpd/conf.d/ssl.conf                                     Modified


#   SSL Protocol support:
# List the enable protocol levels with which clients will be able to
# connect.  Disable SSLv2 access by default:
#A SSLProtocol all -SSLv2 -SSLv3

#   SSL Cipher Suite:
#   List the ciphers that the client is permitted to negotiate.
#   See the mod_ssl documentation for a complete list.
#A SSLCipherSuite HIGH:3DES:!aNULL:!MD5:!SEED:!IDEA

#   Speed-optimized SSL Cipher configuration:
#   If speed is your main concern (on busy HTTPS servers e
#   you might want to force clients to specific, performan
#   optimized ciphers. In this case, prepend those ciphers
#   to the SSLCipherSuite list, and enable SSLHonorCipherO
#   Caveat: by giving precedence to RC4-SHA and AES128-SHA
#   (as in the example below), most connections will no lo
#   have perfect forward secrecy - if the server's key is
#   compromised, captures of past or future traffic must be
#   considered compromised, too.
#SSLCipherSuite RC4-SHA:AES128-SHA:HIGH:MEDIUM:!aNULL:!MD5
#SSLHonorCipherOrder on

#   Server Certificate:
# Point SSLCertificateFile at a PEM encoded certificate.  If
# the certificate is encrypted, then you will be prompted for a
                [ line 80/218 (36%), col 4/52 (7%), char 2683/9447 (28%) ]
^G Get Help       ^O WriteOut       ^R Read File      ^Y Prev Page      ^K Cut Text       ^C Cur Pos
^X Exit           ^J Justify        ^W Where Is       ^V Next Page      ^U UnCut Text     ^T To Spell
```

The presentation add a #A to the line shown. Really only the # is needed, but #A makes it easier for the presentation find the presentation's modification.

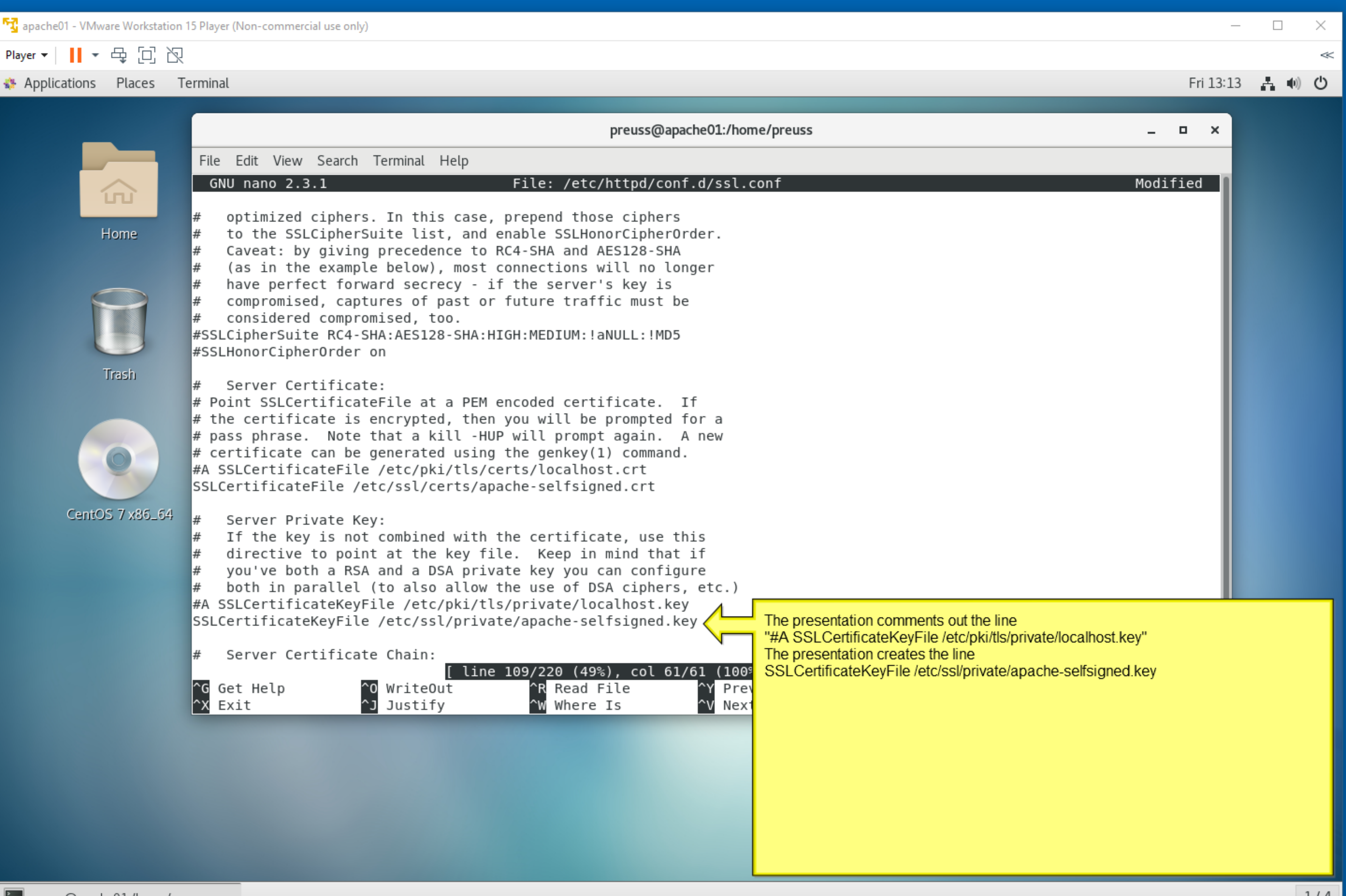
The line should be
"#A SSLCipherSuit HIGH:3DES:!aNULL:!MD5:!SEED:!IDEA"

as shown



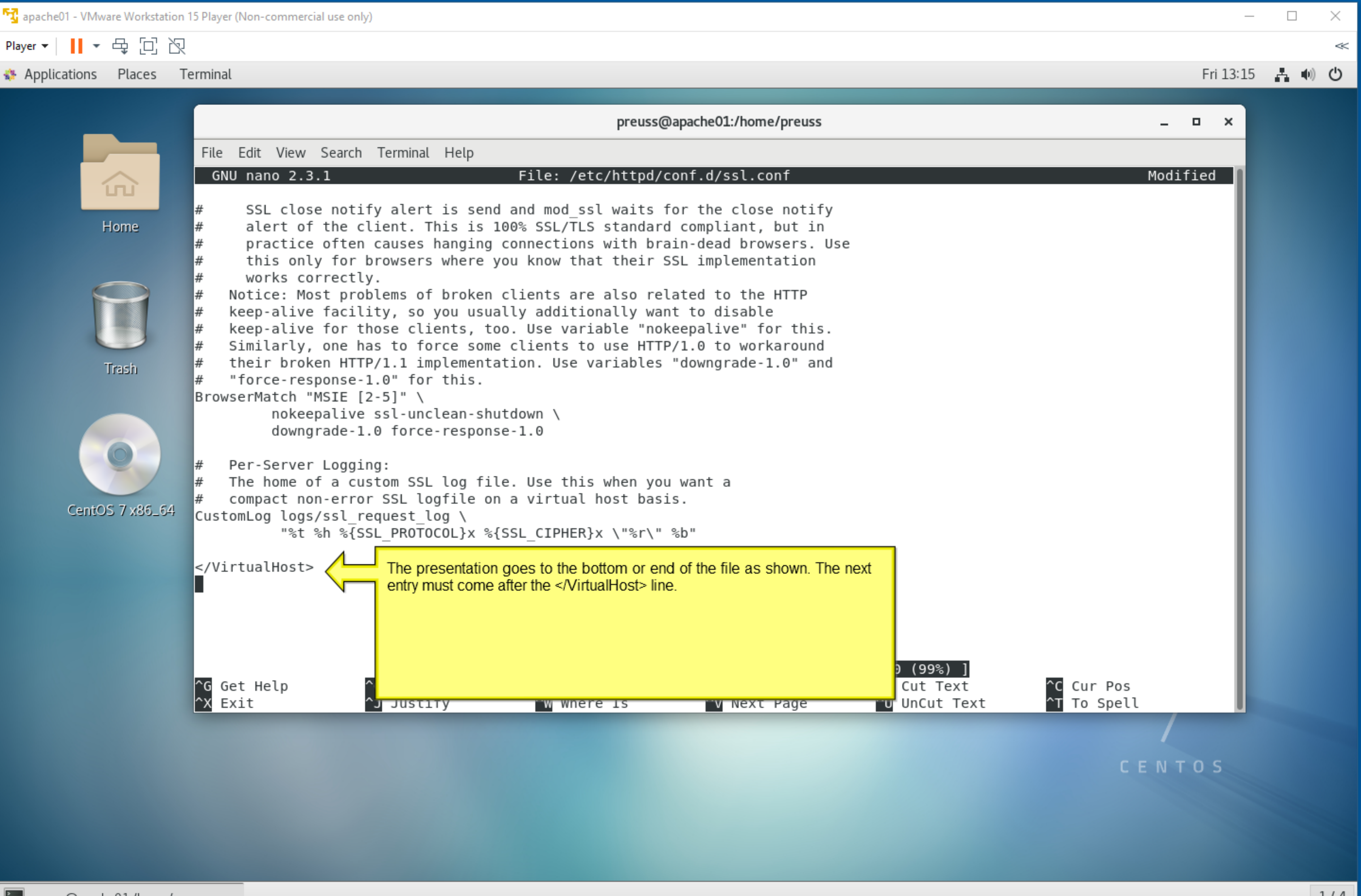
```
  GNU nano 2.3.1                  File: /etc/httpd/conf.d/ssl.conf                              Modified

#   optimized ciphers. In this case, prepend those ciphers
#   to the SSLCipherSuite list, and enable SSLHonorCipherOrder.
#   Caveat: by giving precedence to RC4-SHA and AES128-SHA
#   (as in the example below), most connections will no longer
#   have perfect forward secrecy - if the server's key is
#   compromised, captures of past or future traffic must be
#   considered compromised, too.
#SSLCipherSuite RC4-SHA:AES128-SHA:HIGH:MEDIUM:!aNULL:!MD5
#SSLHonorCipherOrder on

#   Server Certificate:
# Point SSLCertificateFile at a PEM encoded certificate.  If
# the certificate is encrypted, then you will be prompted for a
# pass phrase.  Note that a kill -HUP will prompt again.  A new
# certificate can be generated using the genkey(1) command.
#A SSLCertificateFile /etc/pki/tls/certs/localhost.crt
SSLCertificateFile /etc/ssl/certs/apache-selfsigned.crt

#   Server Private Key:
#   If the key is not combined with the certificate, use this
#   directive to point at the key file.  Keep in mind that if
#   you've both a RSA and a DSA private key you can configure
#   both in parallel (to also allow the use of DSA ciphers, et
SSLCertificateKeyFile /etc/pki/tls/private/localhost.key

#   Server Certificate Chain:
#   Point SSLCertificateChainFile at a file containing the
                          [ line 101/219 (46%), col 56/56
^G Get Help         ^O WriteOut         ^R Read File        ^Y
^X Exit             ^J Justify          ^W Where Is         ^V
```

The presentation comments out the line
"#A SSLCertificateFile /etc/pki/tls/certs/localhost.crt"
The presentation creates the line
SSLCertificateFile /etc/ssl/certs/apache-selfsigned.crt



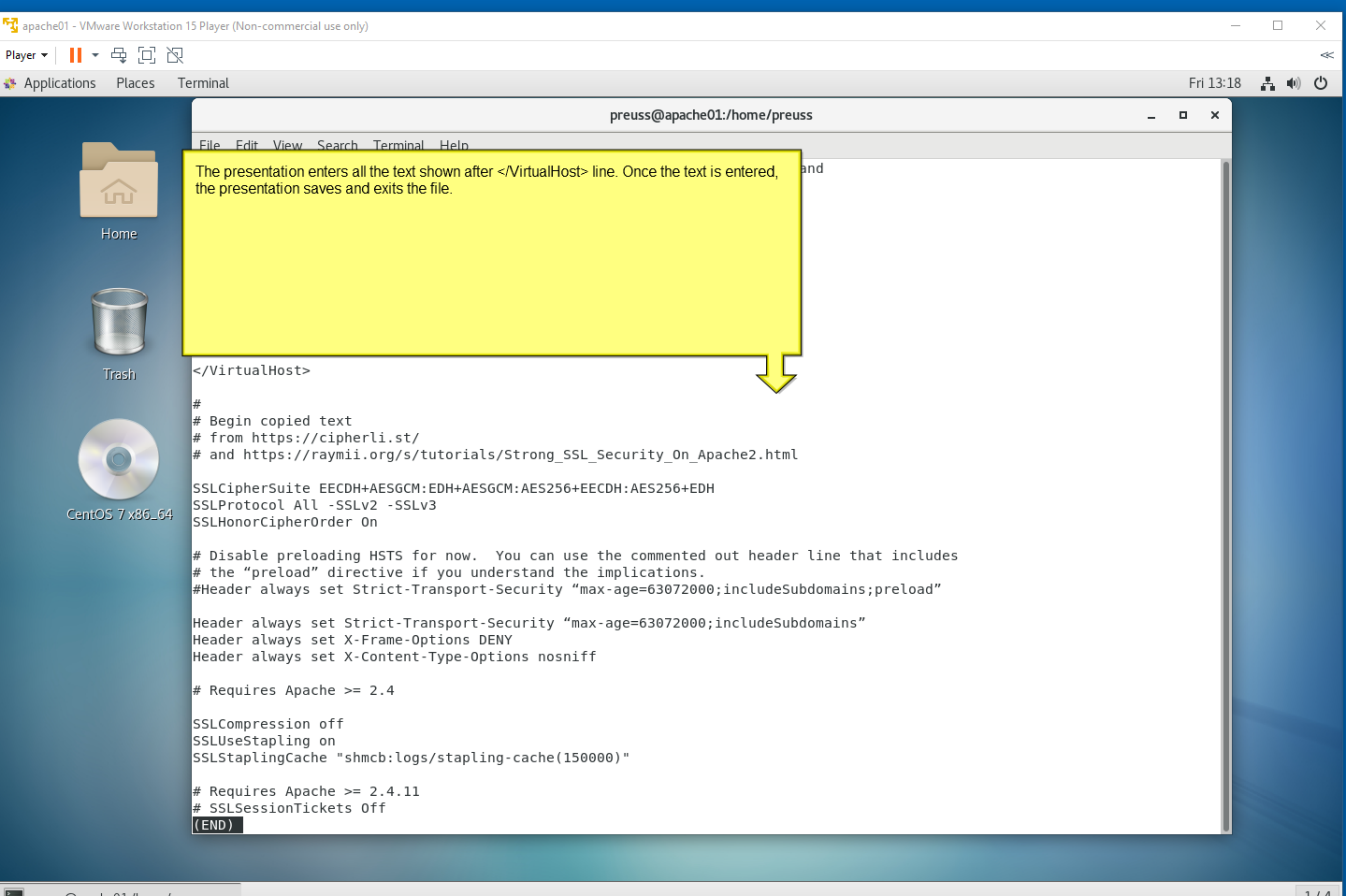
```
  GNU nano 2.3.1                File: /etc/httpd/conf.d/ssl.conf                        Modified

#   optimized ciphers. In this case, prepend those ciphers
#   to the SSLCipherSuite list, and enable SSLHonorCipherOrder.
#   Caveat: by giving precedence to RC4-SHA and AES128-SHA
#   (as in the example below), most connections will no longer
#   have perfect forward secrecy - if the server's key is
#   compromised, captures of past or future traffic must be
#   considered compromised, too.
#SSLCipherSuite RC4-SHA:AES128-SHA:HIGH:MEDIUM:!aNULL:!MD5
#SSLHonorCipherOrder on

#   Server Certificate:
# Point SSLCertificateFile at a PEM encoded certificate.  If
# the certificate is encrypted, then you will be prompted for a
# pass phrase.  Note that a kill -HUP will prompt again.  A new
# certificate can be generated using the genkey(1) command.
#A SSLCertificateFile /etc/pki/tls/certs/localhost.crt
SSLCertificateFile /etc/ssl/certs/apache-selfsigned.crt

#   Server Private Key:
#   If the key is not combined with the certificate, use this
#   directive to point at the key file.  Keep in mind that if
#   you've both a RSA and a DSA private key you can configure
#   both in parallel (to also allow the use of DSA ciphers, etc.)
#A SSLCertificateKeyFile /etc/pki/tls/private/localhost.key
SSLCertificateKeyFile /etc/ssl/private/apache-selfsigned.key

#   Server Certificate Chain:
                          [ line 109/220 (49%), col 61/61 (100%
^G Get Help         ^O WriteOut         ^R Read File        ^Y Prev
^X Exit             ^J Justify          ^W Where Is         ^V Next
```

The presentation comments out the line
"#A SSLCertificateKeyFile /etc/pki/tls/private/localhost.key"
The presentation creates the line
SSLCertificateKeyFile /etc/ssl/private/apache-selfsigned.key



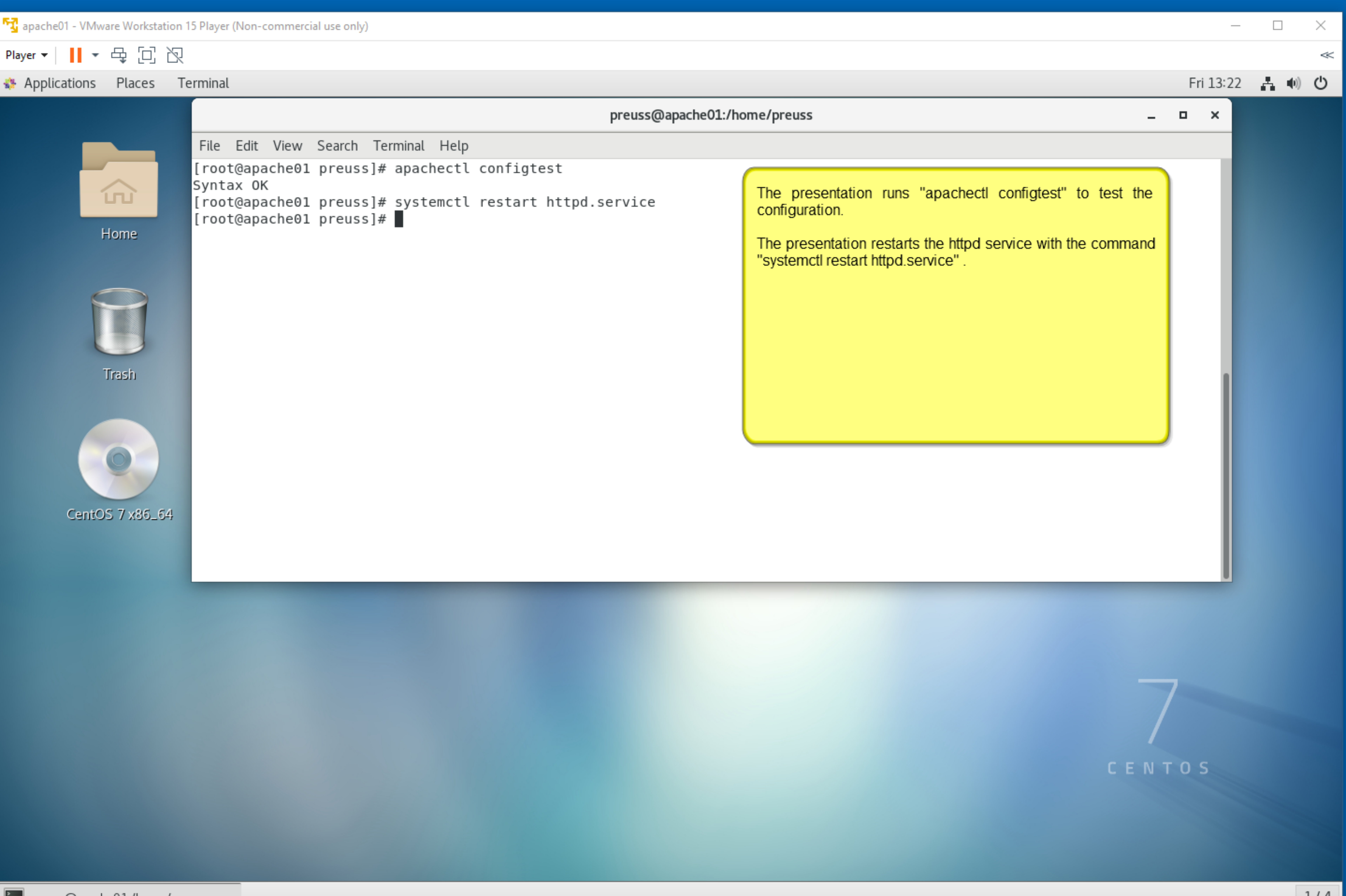
```
 GNU nano 2.3.1              File: /etc/httpd/conf.d/ssl.conf                    Modified

#     SSL close notify alert is send and mod_ssl waits for the close notify
#     alert of the client. This is 100% SSL/TLS standard compliant, but in
#     practice often causes hanging connections with brain-dead browsers. Use
#     this only for browsers where you know that their SSL implementation
#     works correctly.
#   Notice: Most problems of broken clients are also related to the HTTP
#   keep-alive facility, so you usually additionally want to disable
#   keep-alive for those clients, too. Use variable "nokeepalive" for this.
#   Similarly, one has to force some clients to use HTTP/1.0 to workaround
#   their broken HTTP/1.1 implementation. Use variables "downgrade-1.0" and
#   "force-response-1.0" for this.
BrowserMatch "MSIE [2-5]" \
         nokeepalive ssl-unclean-shutdown \
         downgrade-1.0 force-response-1.0

#   Per-Server Logging:
#   The home of a custom SSL log file. Use this when you want a
#   compact non-error SSL logfile on a virtual host basis.
CustomLog logs/ssl_request_log \
          "%t %h %{SSL_PROTOCOL}x %{SSL_CIPHER}x \"%r\" %b"

</VirtualHost>

                                                                      0 (99%) ]
^G Get Help    ^                                                    Cut Text      ^C Cur Pos
^X Exit        ^J Justify      ^W Where Is     ^V Next Page     ^U UnCut Text    ^T To Spell
```

The presentation goes to the bottom or end of the file as shown. The next entry must come after the </VirtualHost> line.



The presentation enters all the text shown after </VirtualHost> line. Once the text is entered, the presentation saves and exits the file.

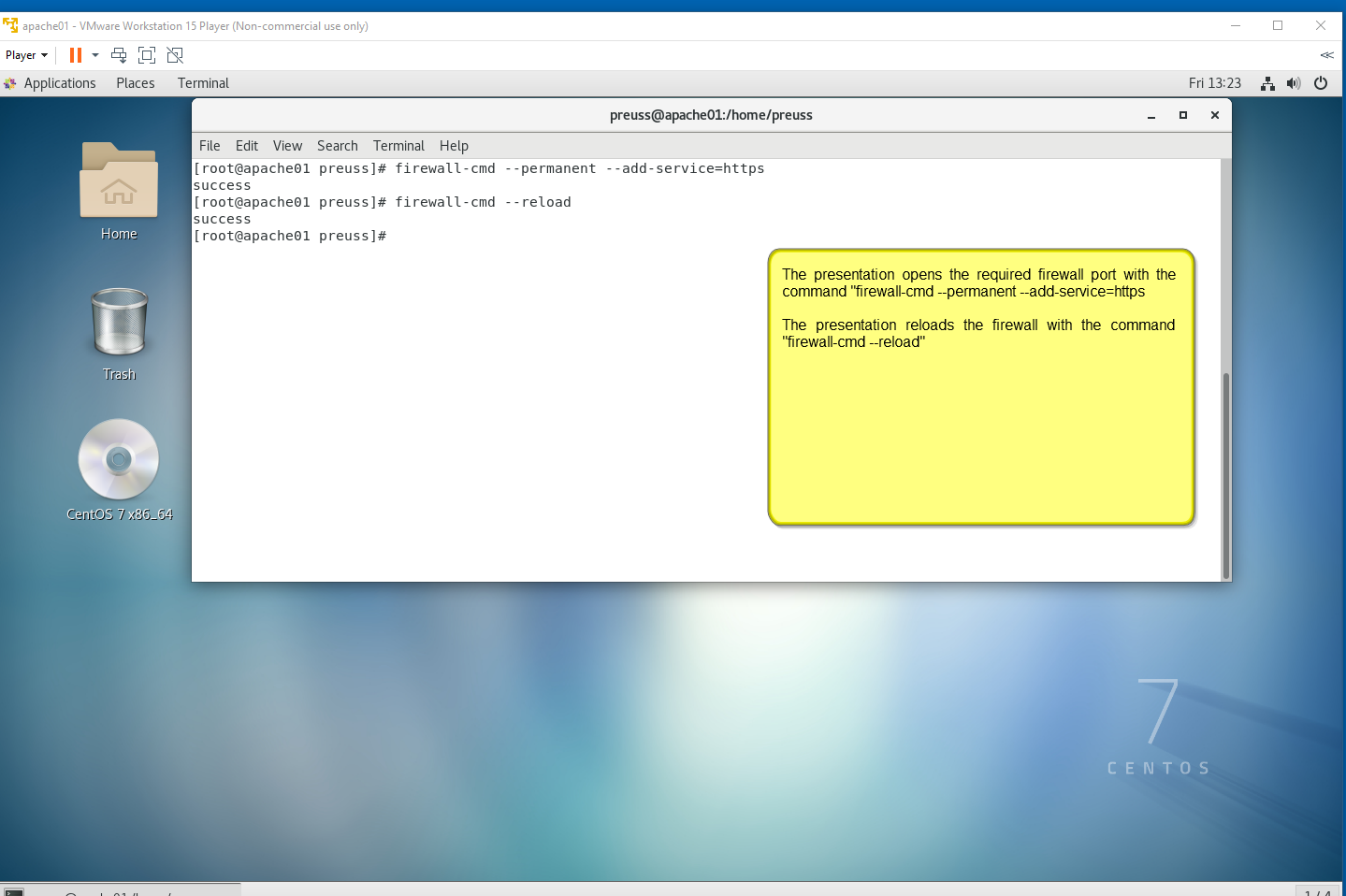
```
                                                                      and
</VirtualHost>

#
# Begin copied text
# from https://cipherli.st/
# and https://raymii.org/s/tutorials/Strong_SSL_Security_On_Apache2.html

SSLCipherSuite EECDH+AESGCM:EDH+AESGCM:AES256+EECDH:AES256+EDH
SSLProtocol All -SSLv2 -SSLv3
SSLHonorCipherOrder On

# Disable preloading HSTS for now.  You can use the commented out header line that includes
# the “preload” directive if you understand the implications.
#Header always set Strict-Transport-Security “max-age=63072000;includeSubdomains;preload”

Header always set Strict-Transport-Security “max-age=63072000;includeSubdomains”
Header always set X-Frame-Options DENY
Header always set X-Content-Type-Options nosniff

# Requires Apache >= 2.4

SSLCompression off
SSLUseStapling on
SSLStaplingCache "shmcb:logs/stapling-cache(150000)"

# Requires Apache >= 2.4.11
# SSLSessionTickets Off
(END)
```



```
[root@apache01 preuss]# apachectl configtest
Syntax OK
[root@apache01 preuss]# systemctl restart httpd.service
[root@apache01 preuss]# 
```

The presentation runs "apachectl configtest" to test the configuration.

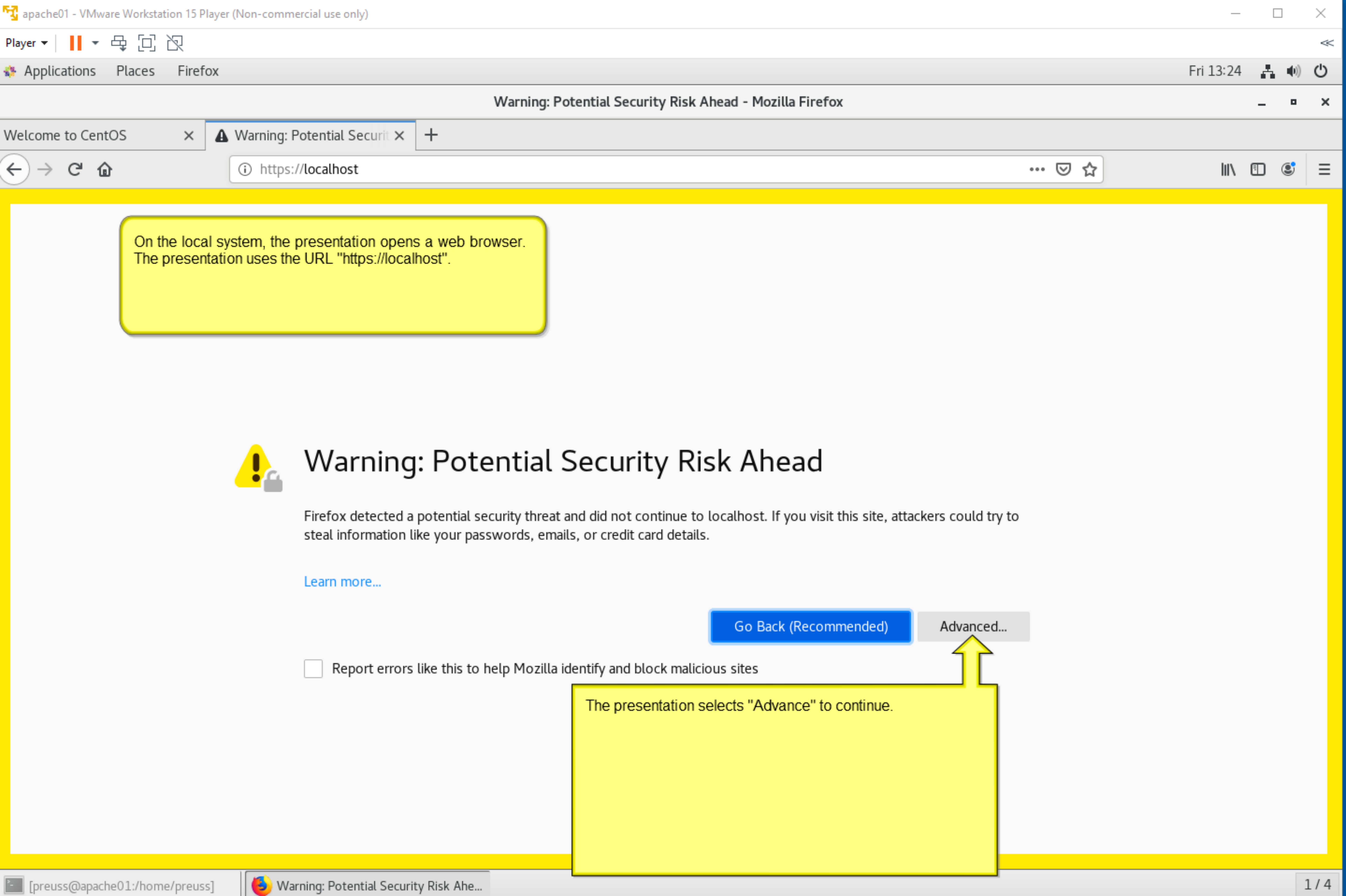
The presentation restarts the httpd service with the command "systemctl restart httpd.service" .



```
[root@apache01 preuss]# firewall-cmd --permanent --add-service=https
success
[root@apache01 preuss]# firewall-cmd --reload
success
[root@apache01 preuss]#
```

The presentation opens the required firewall port with the command "firewall-cmd --permanent --add-service=https

The presentation reloads the firewall with the command "firewall-cmd --reload"



apache01 - VMware Workstation 15 Player (Non-commercial use only)
Player
Applications
Places
Firefox
Fri 13:24
Warning: Potential Security Risk Ahead - Mozilla Firefox
Welcome to CentOS
Warning: Potential Securi
https://localhost
[preuss@apache01:/home/preuss]
Warning: Potential Security Risk Ahe...
1 / 4

On the local system, the presentation opens a web browser. The presentation uses the URL "https://localhost".

Warning: Potential Security Risk Ahead

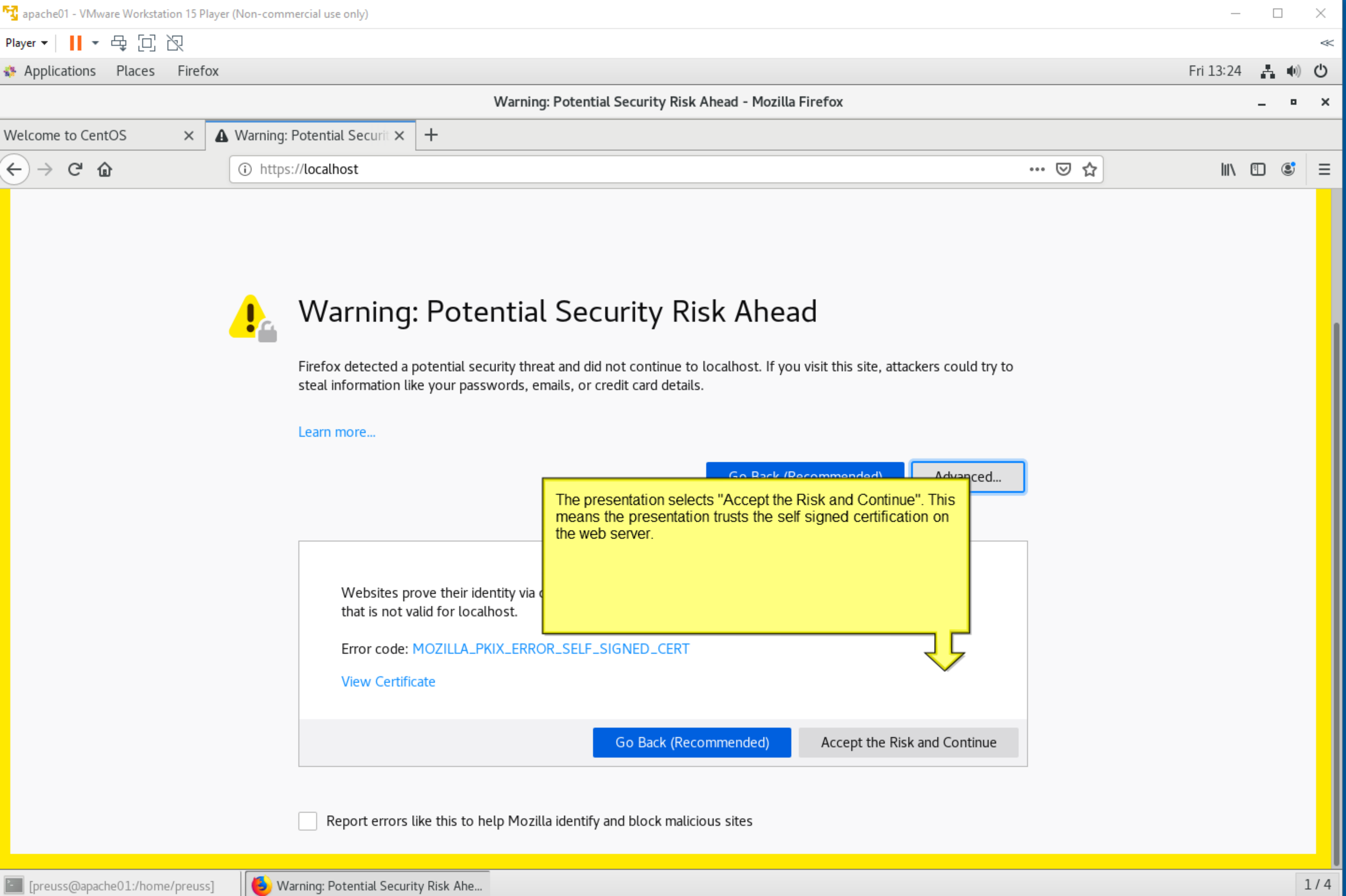
Firefox detected a potential security threat and did not continue to localhost. If you visit this site, attackers could try to steal information like your passwords, emails, or credit card details.

Learn more...

Go Back (Recommended)
Advanced...

□ Report errors like this to help Mozilla identify and block malicious sites

The presentation selects "Advance" to continue.


apache01 - VMware Workstation 15 Player (Non-commercial use only)
Player
Applications
Places
Firefox
Fri 13:24
Warning: Potential Security Risk Ahead - Mozilla Firefox
Welcome to CentOS
Warning: Potential Securi
https://localhost
[preuss@apache01:/home/preuss]
Warning: Potential Security Risk Ahe...
1 / 4

Warning: Potential Security Risk Ahead

Firefox detected a potential security threat and did not continue to localhost. 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...

The presentation selects "Accept the Risk and Continue". This means the presentation trusts the self signed certification on the web server.

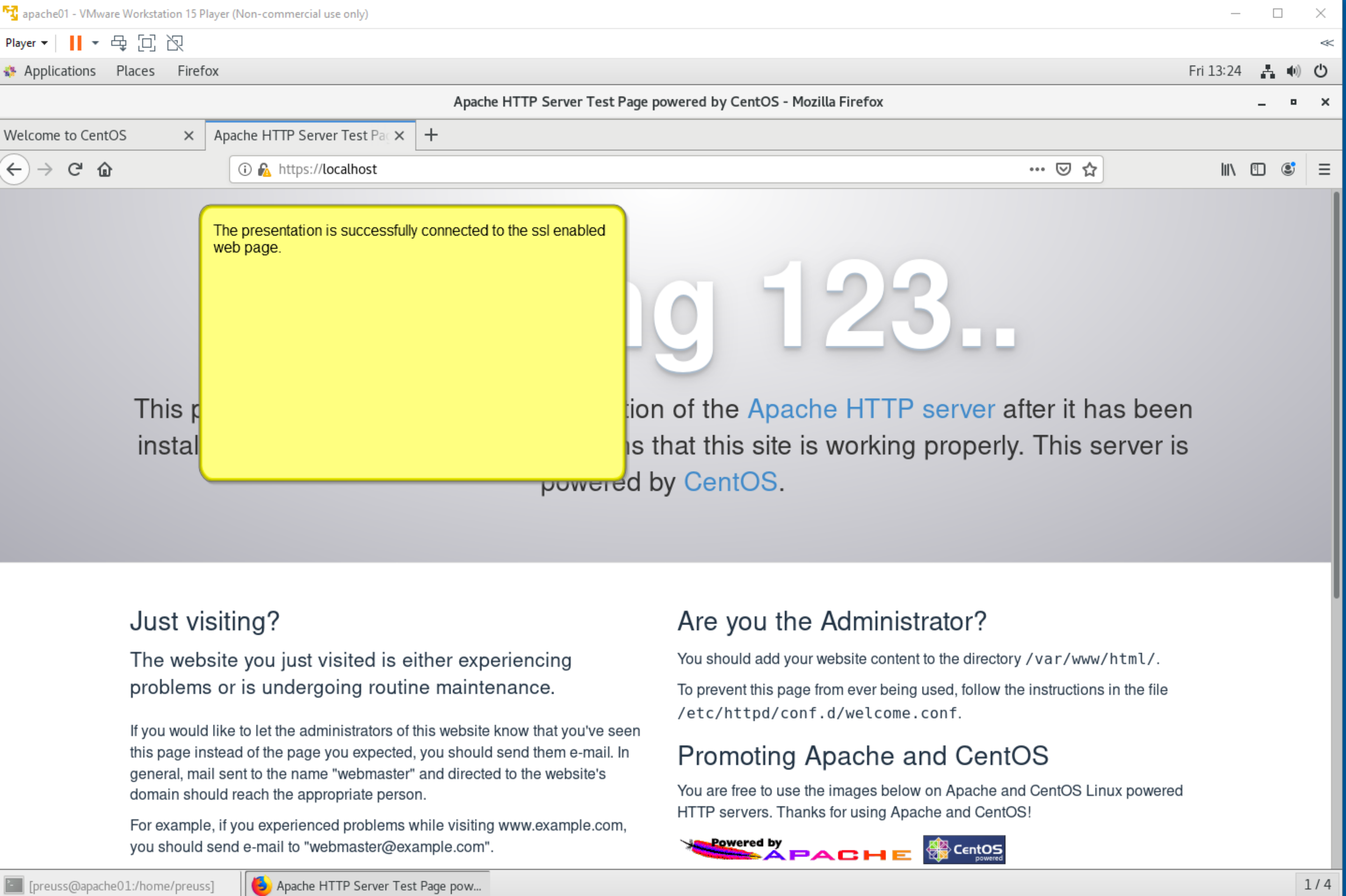
Websites prove their identity via c
that is not valid for localhost.

Error code: MOZILLA_PKIX_ERROR_SELF_SIGNED_CERT

View Certificate

Go Back (Recommended) Accept the Risk and Continue

□ Report errors like this to help Mozilla identify and block malicious sites


apache01 - VMware Workstation 15 Player (Non-commercial use only)
Player
Applications
Places
Firefox
Fri 13:24
Apache HTTP Server Test Page powered by CentOS - Mozilla Firefox
Welcome to CentOS
Apache HTTP Server Test Pa
https://localhost
[preuss@apache01:/home/preuss]
Apache HTTP Server Test Page pow...
1 / 4

The presentation is successfully connected to the ssl enabled web page.

ng 123..

This p tion of the Apache HTTP server after it has been instal s that this site is working properly. This server is powered by CentOS.

Just visiting?

The website you just visited is either experiencing problems or is undergoing routine maintenance.

If you would like to let the administrators of this website know that you've seen this page instead of the page you expected, you should send them e-mail. In general, mail sent to the name "webmaster" and directed to the website's domain should reach the appropriate person.

For example, if you experienced problems while visiting www.example.com, you should send e-mail to "webmaster@example.com".

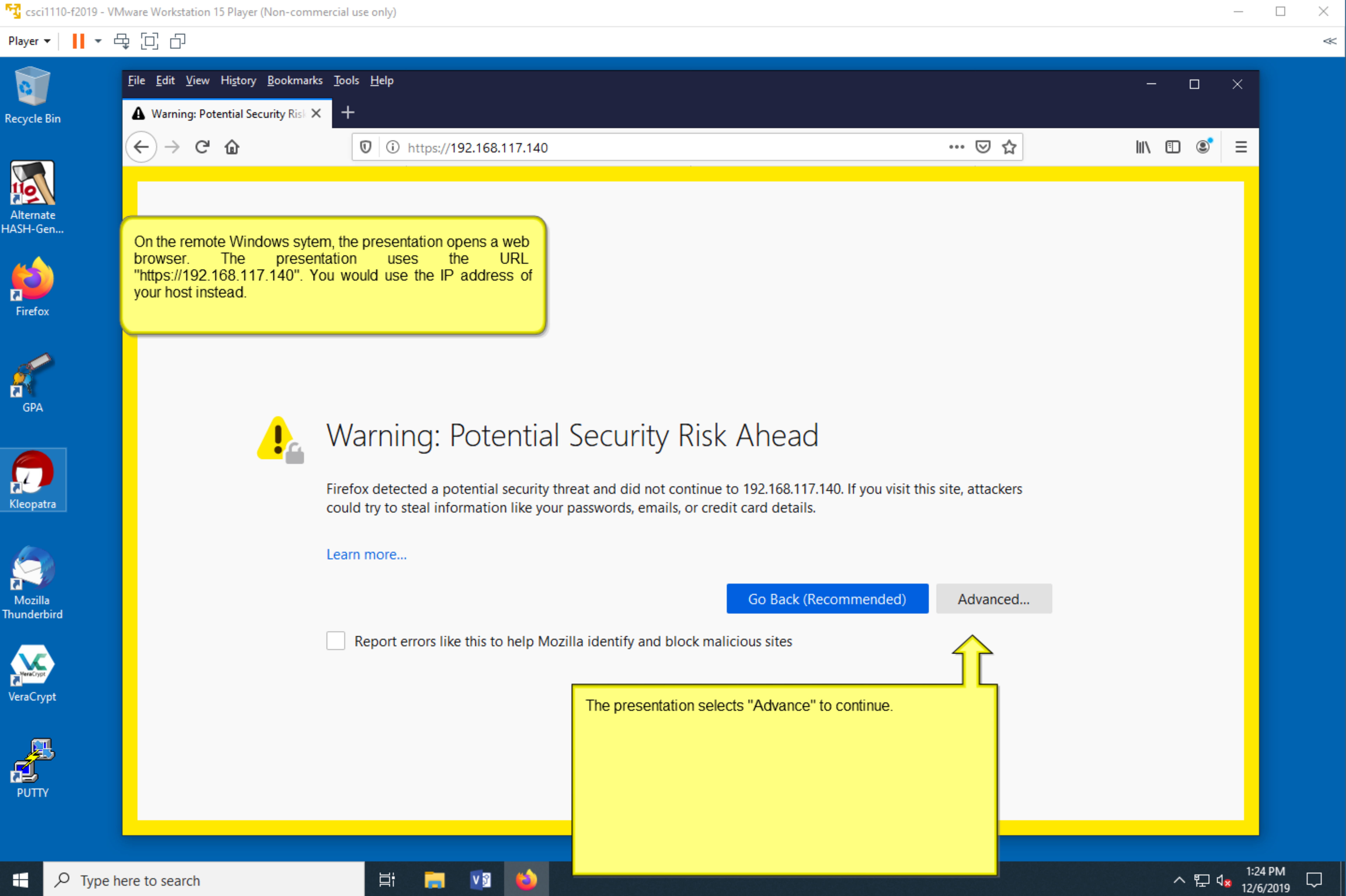
Are you the Administrator?

You should add your website content to the directory `/var/www/html/`.

To prevent this page from ever being used, follow the instructions in the file `/etc/httpd/conf.d/welcome.conf`.

Promoting Apache and CentOS

You are free to use the images below on Apache and CentOS Linux powered HTTP servers. Thanks for using Apache and CentOS!



On the remote Windows sytem, the presentation opens a web browser. The presentation uses the URL "https://192.168.117.140". You would use the IP address of your host instead.

Warning: Potential Security Risk Ahead

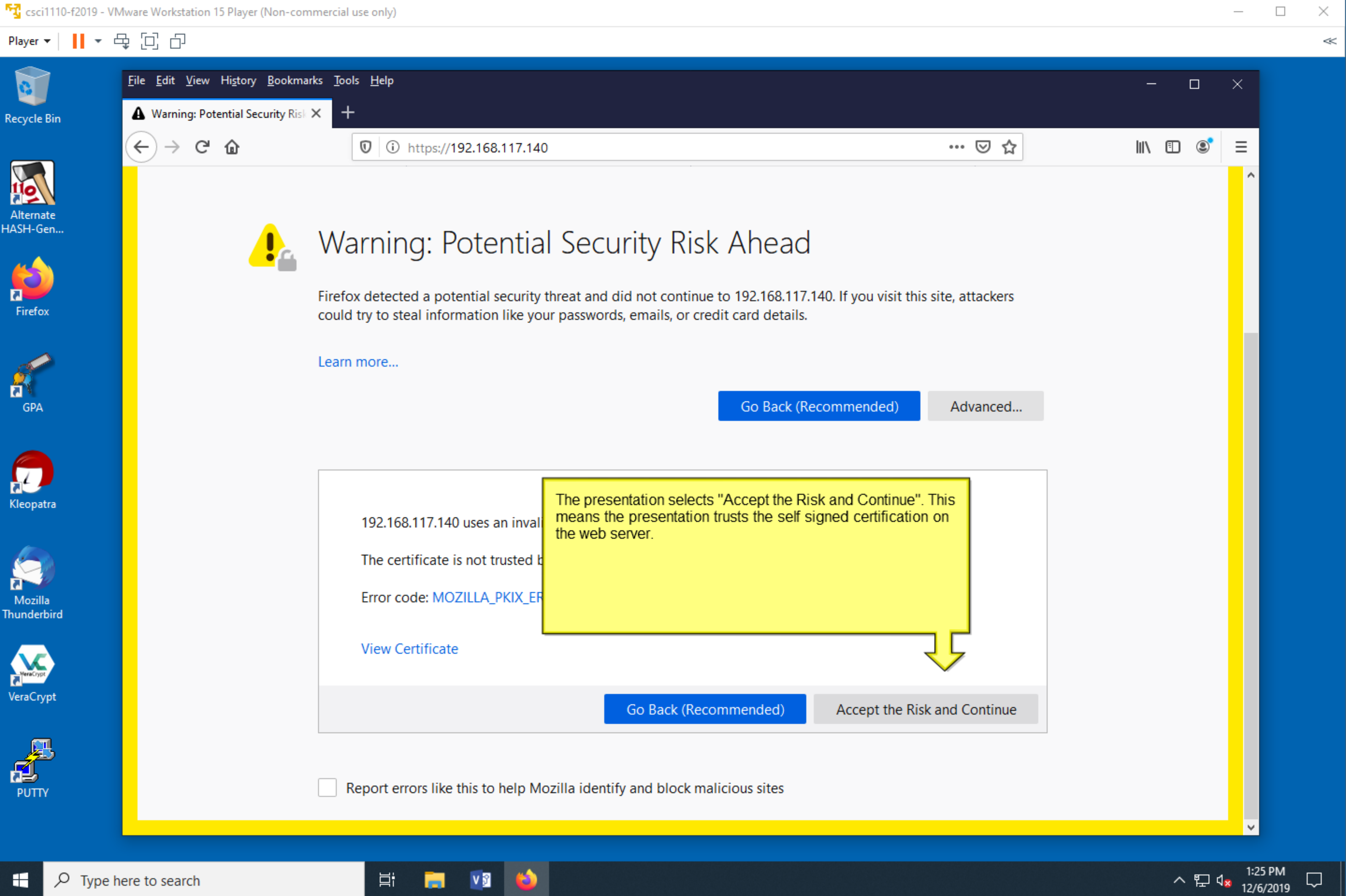
Firefox detected a potential security threat and did not continue to 192.168.117.140. If you visit this site, attackers could try to steal information like your passwords, emails, or credit card details.

Learn more...

Go Back (Recommended) Advanced...

□ Report errors like this to help Mozilla identify and block malicious sites

The presentation selects "Advance" to continue.



Warning: Potential Security Risk Ahead

Firefox detected a potential security threat and did not continue to 192.168.117.140. 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...

192.168.117.140 uses an inval

The certificate is not trusted b

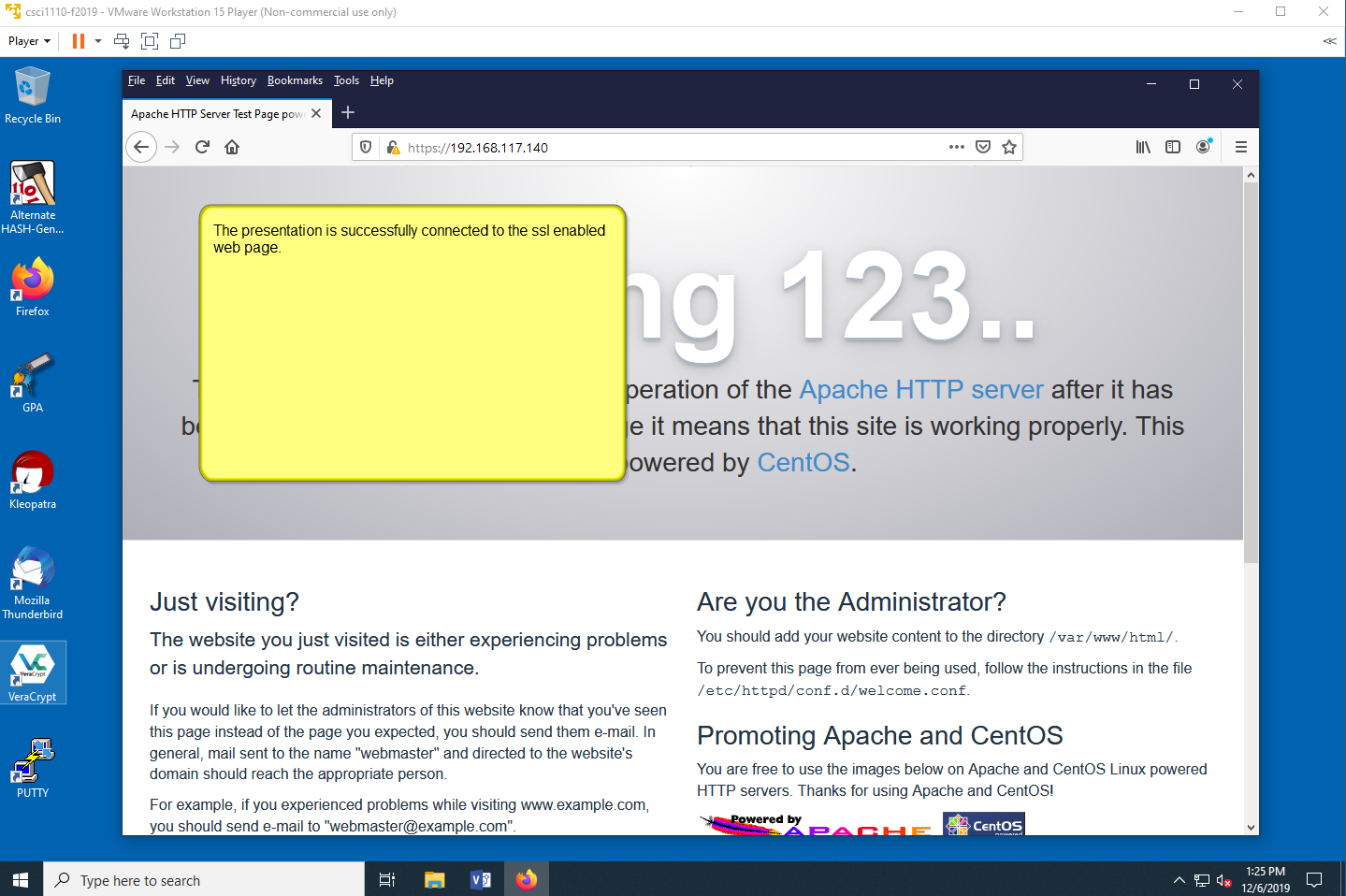
Error code: MOZILLA_PKIX_ER

View Certificate

Go Back (Recommended) Accept the Risk and Continue

□ Report errors like this to help Mozilla identify and block malicious sites

The presentation selects "Accept the Risk and Continue". This means the presentation trusts the self signed certification on the web server.



The presentation is successfully connected to the ssl enabled web page.

ng 123..

peration of the Apache HTTP server after it has

b e it means that this site is working properly. This

owered by CentOS.

Just visiting?

The website you just visited is either experiencing problems or is undergoing routine maintenance.

If you would like to let the administrators of this website know that you've seen this page instead of the page you expected, you should send them e-mail. In general, mail sent to the name "webmaster" and directed to the website's domain should reach the appropriate person.

For example, if you experienced problems while visiting www.example.com, you should send e-mail to "webmaster@example.com".

Are you the Administrator?

You should add your website content to the directory `/var/www/html/`.

To prevent this page from ever being used, follow the instructions in the file `/etc/httpd/conf.d/welcome.conf`.

Promoting Apache and CentOS

You are free to use the images below on Apache and CentOS Linux powered HTTP servers. Thanks for using Apache and CentOS!