Exercise 1.

1. What is the status of selinux?

```
sestatus
SELinux status:                 enabled
SELinuxfs mount:                /sys/fs/selinux
SELinux root directory:         /etc/selinux
Loaded policy name:             targeted
Current mode:                   enforcing
Mode from config file:          enforcing
Policy MLS status:              enabled
Policy deny_unknown status:     allowed
Max kernel policy version:      28
```

2. Use getenforce to get the status

```
getenforce
Enforcing
```

use

Use setenforce to change the status

```
setenforce 0
getenforce
Permissive
```

Exercise 2.

Context type

Apache uses a DocumentRoot that has "`httpd_sys_content_t`" as type.

1.

```
ls -Zd /var/www/html
drwxr-xr-x. root root system_u:object_r:httpd_sys_content_t:s0
/var/www/html
```

Apache's httpd runs with type httpd_t.

2.

```
ps -efZ |grep httpd
system_u:system_r:httpd_t:s0    root     27356     1  0 11:30 ?
00:00:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0    apache   27357 27356  0 11:30 ?
00:00:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0    apache   27358 27356  0 11:30 ?
00:00:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0    apache   27359 27356  0 11:30 ?
00:00:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0    apache   27360 27356  0 11:30 ?
00:00:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0    apache   27361 27356  0 11:30 ?
00:00:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0    apache   27362 27356  0 11:30 ?
00:00:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0    apache   27363 27356  0 11:30 ?
00:00:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0    apache   27364 27356  0 11:30 ?
00:00:00 /usr/sbin/httpd -DFOREGROUND
```

With SELinux enabled, httpd is allowed to access /var/www/html.

When you create a new DocumentRoot, access to this directory will be denied because the new directory will not have the same context as the original DocumentRoot.

3.

```
mkdir /newhtml
ls -Zd /newhtml
drwxr-xr-x. root root unconfined_u:object_r:default_t:s0 /newhtml
```

The context type is "`default_t`".

Now, when you access the webserver, access will be denied.

4.

```
tail -f /var/log/audit/audit.log
type=AVC msg=audit(1480764099.856:1548): avc:  denied  { read } for
pid=16337 comm="httpd" name="index.html" dev="dm-1" ino=28350272
scontext=system_u:system_r:httpd_t:s0
tcontext=unconfined_u:object_r:default_t:s0 tclass=file
```

To allow access, change the type to "`httpd_sys_content_t`".

5.

```
chcon -Rt httpd_sys_content_t /newhtml/
```

This will recursively change context type for all files and directories in /newhtml including newly added files.

To restore the orginal context of `/newhtml` (thus blocking again):

6.

```
restorecon -R /newhtml
```

To make the context type permanent, even through relabelling:

7.

```
semanage fcontext -a -t httpd_sys_content_t "/newhtml(/.*)?"
```

Exercise 3.

Ports and SELINUX example.

We want our webserver to listen to a non default port.

1. Configure httpd to listen to a non default port – say 8999.

After a default install of httpd port 80 is the port that httpd listens to.
Change the port in /etc/httpd/conf/httpd.conf

```
sed -i -e 's/Listen 80/Listen 8999/' /etc/httpd/conf/httpd.conf
```

2. In another shell follow the audit.log file.

```
tail -f /var/log/audit/audit.log
```

3. Restart httpd and view the error message in the audit.log file

```
[systemctl restart httpd
```

(audit.log)
avc: denied { name_bind } for pid=17010 comm="httpd" src=8999

4. What are the ports that httpd is allowed to listen to?

```
semanage port -l |grep ^http_port_t
http_port_t tcp 80, 81, 443, 488, 8008, 8009, 8443, 9000
```

5. Add port 8999 to the list of ports for httpd and check.

```
semanage port -a -t http_port_t -p tcp 8999
```

6. Restart httpd.

```
systemctl restart httpd
semanage port -l |grep ^http_port_t
http_port_t tcp 8999, 80, 81, 443, 488, 8008, 8009, 8443, 9000
```

Exercise 4.

Allow access to a daemon that is by default denied by selinux.
You generate SELinux policy allow rules from logs of denied operations.

1. You change the httpd.conf file to listen to a different port

Open /etc/httpd/conf/httpd.conf and change the port to 8888

2.

```
vi /etc/httpd/conf/httpd.conf
   Listen 8888
   :wq!
```

Restart httpd

3.

```
systemctl restart httpd
  Job for httpd.service failed because the control process exited
  with error code. See "systemctl status httpd.service" and
  journalctl -xe" for details.
```

Check the audit.log file for the httpd error

4.

```
grep httpd /var/log/audit/audit.log | grep -i 8888

grep httpd /var/log/audit/audit.log | audit2allow -M httpd
checkmodule -M -m -o httpd.mod httpd.te
semodule_package -o httpd.pp -m httpd.mod
semodule -i httpd.pp
```

Restart httpd

```
systemctl start httpd
```