RHEL 134
Week 03 Labs

CIT 218

Chaz Davis

BCTC
Spring 2020

April 3, 2020

Part 1: Questions

i) Create a file named “firstname_lastname”. Set an ACL for your current user to have read-only access to the file. Provide the ACL details of the file.

I created a directory named chaz with the command `mkdir chaz` and then cd’d into the directory. I then created a file names Chaz_Davis.txt with the command `touch Chaz_Davis.txt` then set the acl for the user using the comnmand `setfacl -m u::rX Chaz_Davis.txt`, where the `-m` means to modify and the `u::rX` means that for the default user let this file be read-only and remove execution permissions unless explicitly stated, for this file and recursively through directories. this isn’t a necessary step, but is considered best practice. I then viewed the output of the act by running the command `getfacl Chaz_Davis.txt`. You can see the Screenshot in Fig. 1a on Pg. 2.

ii) Create a directory named “CIT218” in your home directory. Set an ACL to allow recursive read/write access on the directory for the “student” group. Provide the ACL details of the directory.

From my jome directory I created a directory named ”CIT218” by running the command `mkdir CIT218`, and then I set an ACL for that directory by running `setfacl -R -m g:student:rw CIT218`, where `-R -m` means modify the acl Recursively, and then `g:student:rw` means for group student, restrict access to read and write only. I then checked the acl config by running `getfacl CIT218`. See the Screenshot in Fig. 1b on Pg. 2.

iii) Change the mode of SELinux to disabled. Provide the output.

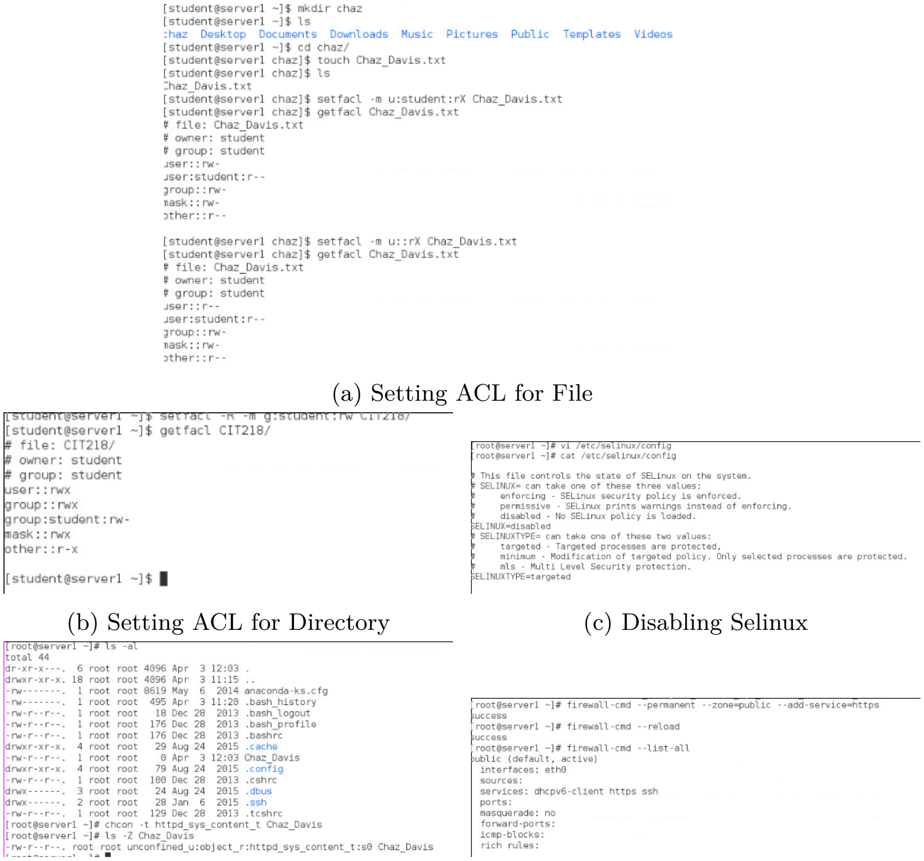
I logged in as root and typed `vi /etc/selinux/config`, once in vi i went to the line with `SELINUX=enforcing` and changed it to `SELINUX=disabled`, I then saved my work with `:wq`. Once back in the terminal i checked the output by typing `cat /etc/selinux/config`. You can see the ouput in Fig. 1c on Pg. 2.

iv) Create a file named “firstname_lastname”. Change the file context to httpd_sys_content_t. Provide the SELinux details of the file.

I logged into the terminal as root and installed the apache server by running `yum -y install httpd`. Next, I created the file Chaz_Davis by running `touch Chaz\_Davis`. I then changed the selinux context for the file by using `chcon -t httpd_sys_content_t Chaz_Davis`, i could have also done this with `semange fcontext -t httpd_sys_content_t Chaz_Davis`, which I believe is technically the preferred method fo management fo the context of a file. I then got the configuration of the file output in the terminal by running `ls -Z Chaz_Davis`. You can see in Fig. 1 d on Pg. 2.

v) Allow the HTTPS service through the firewall. Make it permanent and reload the firewall.

I started off by logging into the terminal as root, I then ran the comnmand `firewall-cmd --permanent --zone=public --add-service=https` , I then ran `firewall-cmd --reload`, and finally to check that it stuck I ran `firewall-cmd --list-all` You can see in Fig. 1 e on Pg. 2.



```
[student@server1 ~]$ mkdir chaz
[student@server1 ~]$ ls
:haz  Desktop  Documents  Downloads  Music  Pictures  Public  Templates  Videos
[student@server1 ~]$ cd chaz/
[student@server1 chaz]$ touch Chaz_Davis.txt
[student@server1 chaz]$ ls
Chaz_Davis.txt
[student@server1 chaz]$ setfacl -m u:student:rX Chaz_Davis.txt
[student@server1 chaz]$ getfacl Chaz_Davis.txt
# file: Chaz_Davis.txt
# owner: student
# group: student
user::rw-
user:student:r--
group::rw-
mask::rw-
other::r--

[student@server1 chaz]$ setfacl -m u::rX Chaz_Davis.txt
[student@server1 chaz]$ getfacl Chaz_Davis.txt
# file: Chaz_Davis.txt
# owner: student
# group: student
user::r--
user:student:r--
group::rw-
mask::rw-
other::r--
```

(a) Setting ACL for File

```
[student@server1 ~]$ setfacl -R -m g:student:rw CIT218/
[student@server1 ~]$ getfacl CIT218/
# file: CIT218/
# owner: student
# group: student
user::rwx
group::rwx
group:student:rw-
mask::rwx
other::r-x

[student@server1 ~]$ █
```

(b) Setting ACL for Directory

```
[root@server1 ~]# vi /etc/selinux/config
[root@server1 ~]# cat /etc/selinux/config

# This file controls the state of SELinux on the system.
# SELINUX= can take one of these three values:
#     enforcing - SELinux security policy is enforced.
#     permissive - SELinux prints warnings instead of enforcing.
#     disabled - No SELinux policy is loaded.
SELINUX=disabled
# SELINUXTYPE= can take one of these two values:
#     targeted - Targeted processes are protected,
#     minimum - Modification of targeted policy. Only selected processes are protected.
#     mls - Multi Level Security protection.
SELINUXTYPE=targeted
```

(c) Disabling Selinux

```
[root@server1 ~]# ls -al
total 44
dr-xr-x---.  6 root root 4096 Apr  3 12:03 .
drwxr-xr-x. 18 root root 4096 Apr  3 11:15 ..
-rw-------.  1 root root 8619 May  6  2014 anaconda-ks.cfg
-rw-------.  1 root root  495 Apr  3 11:20 .bash_history
-rw-r--r--.  1 root root   18 Dec 28  2013 .bash_logout
-rw-r--r--.  1 root root  176 Dec 28  2013 .bash_profile
-rw-r--r--.  1 root root  176 Dec 28  2013 .bashrc
drwxr-xr-x.  4 root root   29 Aug 24  2015 .cache
-rw-r--r--.  1 root root    0 Apr  3 12:03 Chaz_Davis
drwxr-xr-x.  4 root root   79 Aug 24  2015 .config
-rw-r--r--.  1 root root  100 Dec 28  2013 .cshrc
drwx------.  3 root root   24 Aug 24  2015 .dbus
drwx------.  2 root root   28 Jan  6  2015 .ssh
-rw-r--r--.  1 root root  129 Dec 28  2013 .tcshrc
[root@server1 ~]# chcon -t httpd_sys_content_t Chaz_Davis
[root@server1 ~]# ls -Z Chaz_Davis
-rw-r--r--. root root unconfined_u:object_r:httpd_sys_content_t:s0 Chaz_Davis
```

(d) Changing Selinux context of a file

```
[root@server1 ~]# firewall-cmd --permanent --zone=public --add-service=https
success
[root@server1 ~]# firewall-cmd --reload
success
[root@server1 ~]# firewall-cmd --list-all
public (default, active)
  interfaces: eth0
  sources:
  services: dhcpv6-client https ssh
  ports:
  masquerade: no
  forward-ports:
  icmp-blocks:
  rich rules:
```

(e) Allowing HTTPS through the firewall

Figure 1: Screenshots for Week 3 Labs