EECS 3482 Lab 4

Jonathan Baldwin

Chapter 1

Part 1: Activation of SELinux on Kali Linux

Get the default policy and the basic set of SELinux utilities

```
# apt-get -qy install selinux-basics selinux-policy-default auditd
```

(Lots of messages are printed as apt-get downloads and installs the packages.)

Run selinux-activate to configure GRUB and PAM and to create `/.autorelabel`

```
# selinux-activate
Activating SE Linux
Generating grub configuration file ...
Found background image: /usr/share/images/desktop-base/desktop-grub.png
Found linux image: /boot/vmlinuz-4.18.0-kali2-amd64
Found initrd image: /boot/initrd.img-4.18.0-kali2-amd64
done
SE Linux is activated.  You may need to reboot now.
```

Reboot.

During the reboot, SELinux relabels the filesystem. It complains about not being able to find users but otherwise proceeds.

Run check-selinux-installation to check that everything has been setup correctly

```
# check-selinux-installation
Traceback (most recent call last):
  File "/usr/sbin/check-selinux-installation", line 33, in <module>
    results += test.test()
  File "/usr/share/selinux-basics/tests/24_fsckfix.py", line 24, in test
    raise IOError("/etc/default/rcS not found, is this Debian?")
OSError: /etc/default/rcS not found, is this Debian?
```

The `check-selinux-installation` script appears to not properly support the current version of Kali.

Test the current SELinux status

```
# sestatus
SELinux status:                 enabled
SELinuxfs mount:                /sys/fs/selinux
SELinux root directory:         /etc/selinux
```

```
Loaded policy name:             default
Current mode:                   permissive
Mode from config file:          permissive
Policy MLS status:              enabled
Policy deny_unknown status:     allowed
Memory protection checking:     actual (secure)
Max kernel policy version:      31
```

SELinux is enabled in permissive mode.

Determine the current position of the directory

```
# pwd
/root
```

Verify and switch to the root directory.

```
# cd /root
# pwd
/root
```

List the contents of the current directory with `ls -l`

```
# ls -l

total 32
drwxr-xr-x. 2 root root 4096 Oct 26 05:32 Desktop
drwxr-xr-x. 2 root root 4096 Oct 26 05:32 Documents
drwxr-xr-x. 2 root root 4096 Oct 26 05:32 Downloads
drwxr-xr-x. 2 root root 4096 Oct 26 05:32 Music
drwxr-xr-x. 2 root root 4096 Oct 26 05:32 Pictures
drwxr-xr-x. 2 root root 4096 Oct 26 05:32 Public
drwxr-xr-x. 2 root root 4096 Oct 26 05:32 Templates
drwxr-xr-x. 2 root root 4096 Oct 26 05:32 Videos
```

Nothing special here.

List the contents of the current directory with `ls -Z`

```
# ls -Z
    system_u:object_r:user_home_t:s0 Desktop
system_u:object_r:xdg_documents_t:s0 Documents
system_u:object_r:xdg_downloads_t:s0 Downloads
    system_u:object_r:xdg_music_t:s0 Music
 system_u:object_r:xdg_pictures_t:s0 Pictures
    system_u:object_r:user_home_t:s0 Public
    system_u:object_r:user_home_t:s0 Templates
   system_u:object_r:xdg_videos_t:s0 Videos
```

SELinux information appears in the first column.

Type the contents of the file config

```
# 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=permissive
# SELINUXTYPE= can take one of these two values:
# default - equivalent to the old strict and targeted policies
# mls     - Multi-Level Security (for military and educational use)
# src     - Custom policy built from source
SELINUXTYPE=default

# SETLOCALDEFS= Check local definition changes
SETLOCALDEFS=0
```

What is the current status of SELINUX?

The current status of SELinux is permissive.

What is the current type of SELINUX?

The current type of SELinux is default.

Type the list of switches for the command semanage

```
# semanage -h
usage: semanage [-h]
                {import,export,login,user,port,ibpkey,ibendport,interface,module,node,fcontext
                ,boolean,permissive,dontaudit}
                ...

semanage is used to configure certain elements of SELinux policy with-out
requiring modification to or recompilation from policy source.

positional arguments:
  {import,export,login,user,port,ibpkey,ibendport,interface,module,node,fcontext,boolean,
  permissive,dontaudit}
    import              Import local customizations
    export              Output local customizations
    login               Manage login mappings between linux users and SELinux
                        confined users
    user                Manage SELinux confined users (Roles and levels for an
                        SELinux user)
    port                Manage network port type definitions
    ibpkey              Manage infiniband ibpkey type definitions
    ibendport           Manage infiniband end port type definitions
    interface           Manage network interface type definitions
    module              Manage SELinux policy modules
    node                Manage network node type definitions
    fcontext            Manage file context mapping definitions
    boolean             Manage booleans to selectively enable functionality
    permissive          Manage process type enforcement mode
    dontaudit           Disable/Enable dontaudit rules in policy

optional arguments:
  -h, --help            show this help message and exit
```

Type the list of switches for the command semanage with boolean option

```
# semanage boolean -h
usage: semanage boolean [-h] [-n] [-N] [-S STORE] [  --extract  | --deleteall  | --list -C | --modify ( --
```

```
positional arguments:
  boolean               boolean

optional arguments:
  -h, --help            show this help message and exit
  -C, --locallist       List boolean local customizations
  -n, --noheading       Do not print heading when listing boolean object types
  -N, --noreload        Do not reload policy after commit
  -S STORE, --store STORE
                        Select an alternate SELinux Policy Store to manage
  -m, --modify          Modify a record of the boolean object type
  -l, --list            List records of the boolean object type
  -E, --extract         Extract customizable commands, for use within a
                        transaction
  -D, --deleteall       Remove all boolean objects local customizations
  -1, --on              Enable the boolean
  -0, --off             Disable the boolean
```

List all boolean values.

```
# semanage boolean -l
SELinux boolean                State  Default Description
```

A long list of `name (state, default) description` tuples follows.

What is the default value of the `fenced_can_ssh` process?

```
# semanage boolean -l | grep fenced_can_ssh
fenced_can_ssh                 (off  ,  off)  Determine whether fenced can use ssh.
```

The default value for `fenced_can_ssh` is off.

What is the current value of the user_ping process?

```
# semanage boolean -l | grep user_ping
user_ping                      (off  ,  off)  Control users use of ping and traceroute
```

The current value of `user_ping` is off.

Attempt: `getsebool user_ping` and `getsebool fenced_can_ssh`

```
# getsebool user_ping
user_ping --> off
getsebool fenced_can_ssh
fenced_can_ssh --> off
```

Matches the above.

Determine the current Boolean value for Apache capability to connect to database:

```
# getsebool httpd_can_network_connect_db
httpd_can_network_connect_db --> off
```

Determine the current Boolean value for Apache capability to connect to database:

```
# setsebool httpd_can_network_connect_db on
```

Determine the current Boolean value for Apache capability to connect to database:

```
# getsebool httpd_can_network_connect_db
httpd_can_network_connect_db --> on
```

The setting seems to have stuck.

Make the change persistent across reboots

```
# setsebool -P httpd_can_network_connect_db on
```

Determine the current context of the Apache server

```
# ps axZ | grep httpd
system_u:system_r:initrc_t:s0    2270 pts/0    S+     0:00 grep httpd
```

The Apache server isn't running, we just find the `grep` process itself.

List the currently supported roles in the environment

```
# seinfo -r

Roles: 14
   auditadm_r
   dbadm_r
   guest_r
   logadm_r
   nx_server_r
   object_r
   secadm_r
   staff_r
   sysadm_r
   system_r
   unconfined_r
   user_r
   webadm_r
   xguest_r
```

Start the Apache Server

```
# apache2ctl start
Invoking 'systemctl start apache2'.
Use 'systemctl status apache2' for more info.
```

Verify the status of the Apache server

```
# systemctl status apache2
* apache2.service - The Apache HTTP Server
   Loaded: loaded (/lib/systemd/system/apache2.service; disabled; vendor preset: disabled)
   Active: active (running) since Fri 2019-03-08 21:08:56 EST; 10ms ago
  Process: 2288 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
 Main PID: 2292 (apache2)
    Tasks: 3 (limit: 2348)
   Memory: 8.0M
   CGroup: /system.slice/apache2.service
           2292 /usr/sbin/apache2 -k start

Mar 08 21:08:56 kali systemd[1]: Starting The Apache HTTP Server...  Mar 08 21:08:56 kali
apachectl[2288]: AH00558: apache2: Could not reliably determine the server's fully qualified
```

```
domain name, using 127.0.1.1. Set the 'ServerName' directive globally to suppress this message
Mar 08 21:08:56 kali systemd[1]: Started The Apache HTTP Server.
```

The Apache server is indeed running.

Verify the current context

```
ps axZ | grep httpd
system_u:system_r:httpd_t:s0     2292 ?        Ds     0:00 /usr/sbin/apache2 -k start
system_u:system_r:initrc_t:s0    2295 pts/0    S+     0:00 grep httpd
```

And it appears with the `httpd_t` type.

Chapter 2

Part 2: Relabeling Files in SELinux

0.

```
# sed -i 's/\/var\/www\/\html/\/html/g' \
    /etc/apache2/sites-available/000-default.conf
# systemctl reload apache2
```

Create Directory

```
# mkdir /html
```

Create the `index.html` file

```
# touch /html/index.html
```

List the context labels for the file

```
# ls -Z /html/index.html
# system_u:object_r:root_t:s0 /html/index.html
```

List the context label for the directory

```
# ls -Zd /html
# system_u:object_r:root_t:s0 /html
```

Attempt to start the browser and document the output

Trying to browse the page yields a 403 Forbidden status.

Change the context for the directory

```
# chcon -v --type=httpd_sys_content_t /html
# changing security context of '/html'
```

Change the context for the file

```
# chcon -v --type=httpd_sys_content_t /html/index.html
# changing security context of '/html/index.html'
```

```
# ls -Z /html/index.html
# system_u:object_r:httpd_sys_content_t:s0 /html/index.html
```

```
# ls -Zd /html
# system_u:object_r:httpd_sys_content_t:s0 /html
```

Trying to browse the site still yields a 403 error.

Relabeling the entire file system

```
# touch /.autorelabel
# reboot
# genhomedircon
# touch /.autorelabel
# reboot
```

After rebooting the system twice and relabeling the filesystem, trying to browse still yields a 403 error.

Allowing access to ports and list the ports

```
# semanage port -a -t http_port_t -p tcp 81
# semanage port -l
SELinux Port Type              Proto    Port Number
```

A list of `type protocol port_number` tuples follows. The `http_port_t` tuple has port 81:

```
http_port_t                    tcp      81, 80, 443, 488, 8008, 8009, 8443
```