

EECS 3482

Lab 4

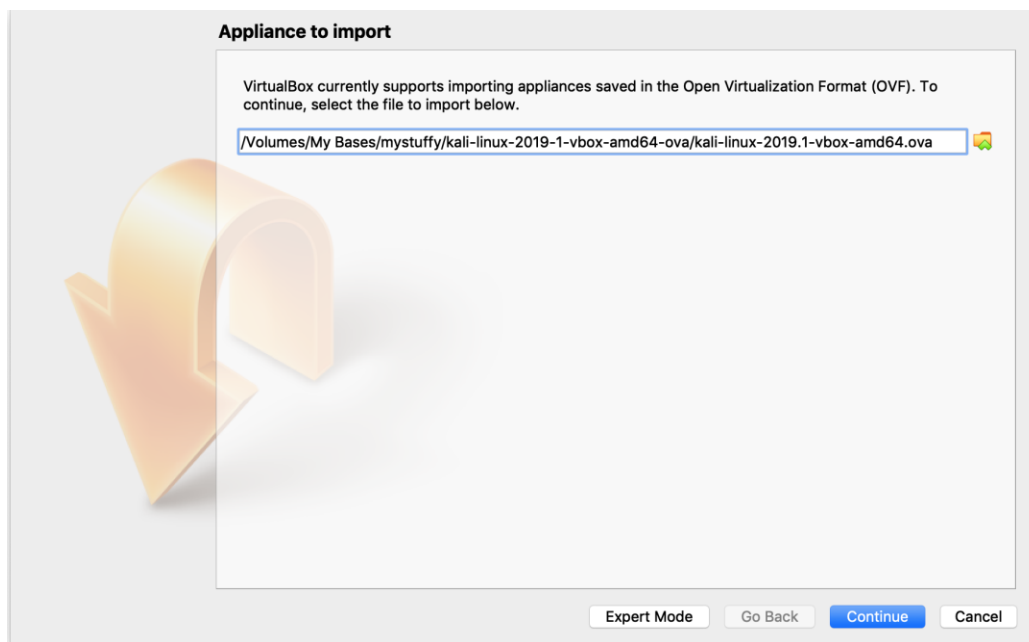
Name : AKALPIT SHARMA

ID: 212650628

## Lab 4 EECS Lab Work

# Part 1: Activation of SELinux on Kali Linux

Importing Appliance: kali-linux-2019.1-vbox-amd64.ova



Appliance Settings

### Appliance settings

These are the virtual machines contained in the appliance and the suggested settings of the imported VirtualBox machines. You can change many of the properties shown by double-clicking on the items and disable others using the check boxes below.

Virtual System 1	
Name	Kali-Linux-2019.1-vbox-amd64 1
Product	Kali Linux
Product-URL	<a href="https://www.kali.org/">https://www.kali.org/</a>
Vendor	Offensive Security
Vendor-URL	<a href="https://www.offensive-security.com/">https://www.offensive-security.com/</a>
Version	Rolling (2019.1) x64

You can modify the base folder which will host all the virtual machine files (per virtual machine) modified. Original Value: Rolling (2019.1) x64


MAC Address Policy:

Additional Options: ☒ Import hard drives as VDI

Appliance is not signed

## Progress

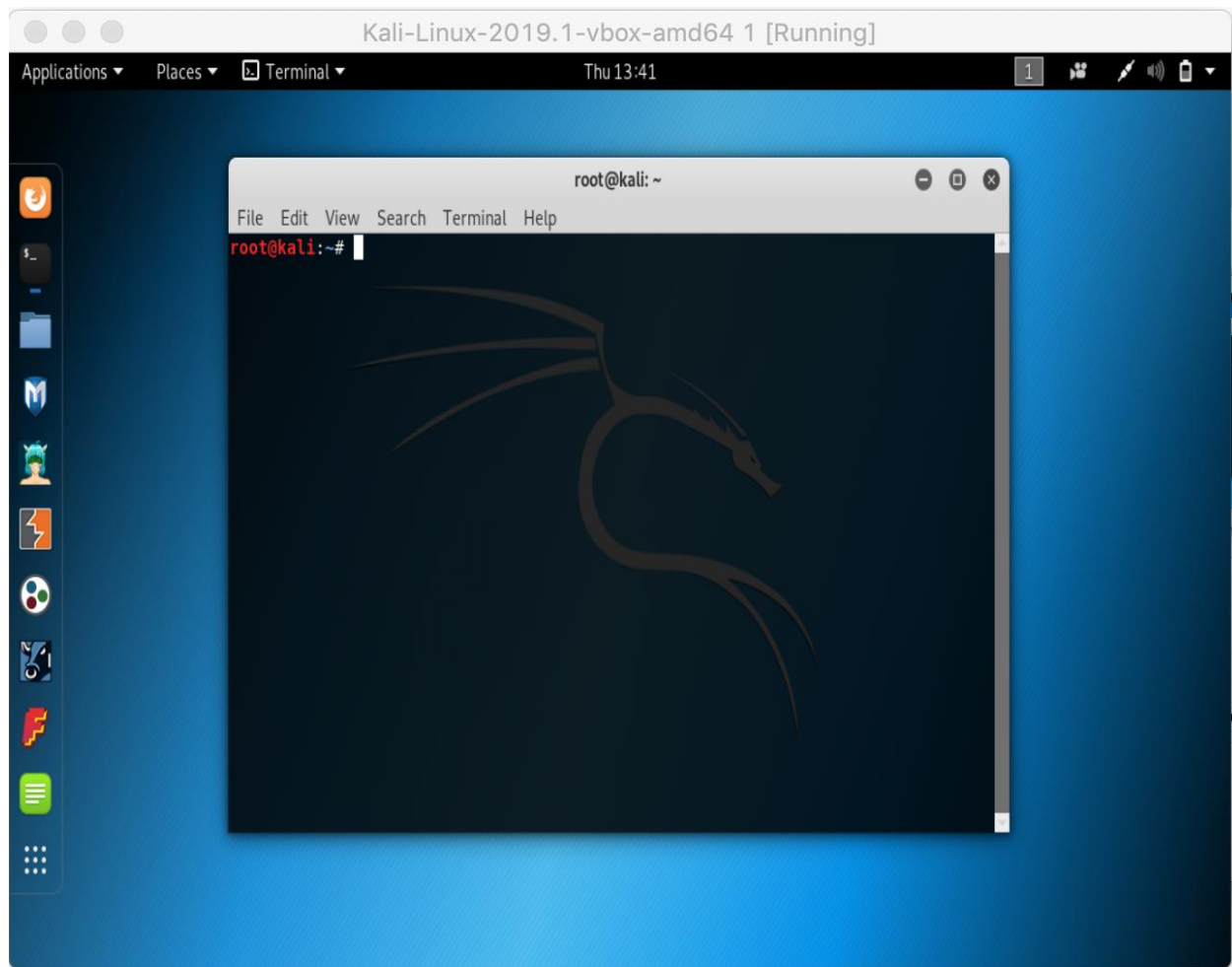
### Oracle VM VirtualBox Manager



Importing virtual disk image 'Kali-Linux-2019.1-vbox-amd64-disk001.vmdk' ... (2/3)

4 minutes remaining

Powered on Server



**apt-get install selinux-basics selinux-policy-default auditd:**

First Screenshot

```

root@kali:~# apt-get install selinux-basics selinux-policy-default auditd
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
  libcharls1 libpoppler80 libpython3.6 libpython3.6-dev libpython3.6-minimal
  libpython3.6-stdlib python3.6 python3.6-dev python3.6-minimal
Use 'apt autoremove' to remove them.
The following additional packages will be installed:
  checkpolicy gdal-bin gdal-data libauparse0 libcharls2 libgdal20 libhdf5-103
  libnetcdf13 libpython3-dev libpython3-stdlib libpython3.7 libpython3.7-dev
  libpython3.7-minimal libpython3.7-stdlib policycoreutils policycoreutils-dev
  policycoreutils-python-utils python-gdal python-numpy python3 python3-audit
  python3-dev python3-distutils python3-gdal python3-minimal python3-networkx
  python3-numpy python3-selinux python3-semanage python3-sepolgen
  python3-sepolicy python3-setools python3.7 python3.7-dev python3.7-minimal
  selinux-policy-dev selinux-utils semodule-utils setools
Suggested packages:
  audispd-plugins libgdal-grass gfortran python-numpy-dbg python-numpy-doc
  python3-doc python3-tk python3-venv python-networkx-doc python3-pytest
  python3-numpy-dbg python3.7-venv python3.7-doc logcheck syslog-summary
  setools-gui
The following packages will be REMOVED:
  libhdf5-100

```

## Installing Packages:

```

The following NEW packages will be installed:
  auditd checkpolicy libauparse0 libcharls2 libhdf5-103 libpython3.7-dev
  policycoreutils policycoreutils-dev policycoreutils-python-utils
  python3-audit python3-gdal python3-networkx python3-selinux python3-semanage
  python3-sepolgen python3-sepolicy python3-setools python3.7-dev
  selinux-basics selinux-policy-default selinux-policy-dev selinux-utils
  semodule-utils setools
The following packages will be upgraded:
  gdal-bin gdal-data libgdal20 libnetcdf13 libpython3-dev libpython3-stdlib
  libpython3.7 libpython3.7-minimal libpython3.7-stdlib python-gdal
  python-numpy python3 python3-dev python3-distutils python3-minimal
  python3-numpy python3.7 python3.7-minimal
18 upgraded, 24 newly installed, 1 to remove and 736 not upgraded.
Need to get 77.0 MB of archives.
After this operation, 116 MB of additional disk space will be used.
Do you want to continue? [Y/n] Y
Get:1 http://kali.download/kali kali-rolling/main amd64 libnetcdf13 amd64 1:4.6.2-1 [403 kB]
Get:2 http://kali.download/kali kali-rolling/main amd64 gdal-bin amd64 2.4.0+dfsg-1+b1 [406 kB]
Get:3 http://kali.download/kali kali-rolling/main amd64 python-gdal amd64 2.4.0+dfsg-1+b1 [814 kB]
Get:4 http://kali.download/kali kali-rolling/main amd64 libgdal20 amd64 2.4.0+dfsg-1+b1 [6,171 kB]
7% [4 libgdal20 3,932 kB/6,171 kB 64%]
50% [4 libgdal20 4,063 kB/6,171 kB 66%]
Get:5 http://kali.download/kali kali-rolling/main amd64 libhdf5-103 amd64 1.10.4+repack-10 [1,325 kB]
Get:6 http://kali.download/kali kali-rolling/main amd64 python-numpy amd64 1:1.16.1-1 [2,098 kB]
174 kB/s 6min
174 kB/s 6min

```

Final Screenshot:

```
Setting up python3 (3.7.2-1) ...  
running python rtupdate hooks for python3.7...  
running python post-rtupdate hooks for python3.7...  
Setting up python3-selinux (2.8-1+b1) ...  
Setting up python3-numpy (1:1.16.1-1) ...  
Setting up python3.7-dev (3.7.2-2) ...  
Setting up python3-gdal (2.4.0+dfsg-1+b1) ...  
Setting up python3-networkx (2.2-1) ...  
Setting up python3-setools (4.2.0-1) ...  
Setting up python3-semanage (2.8-2) ...  
Setting up setools (4.2.0-1) ...  
Processing triggers for gnome-menus (3.31.3-1) ...  
Setting up python3-sepolgen (2.8-3) ...  
Setting up python3-distutils (3.7.2-3) ...  
Setting up python3-audit (1:2.8.4-2) ...  
Setting up selinux-basics (0.5.6) ...  
Setting up python3-dev (3.7.2-1) ...  
Setting up python3-sepolicy (2.8-3) ...  
Setting up policycoreutils-python-utils (2.8-3) ...  
Setting up policycoreutils-dev (2.8-3) ...  
Setting up selinux-policy-dev (2:2.20190201-2) ...  
Processing triggers for libc-bin (2.28-2) ...  
Processing triggers for systemd (240-4) ...  
root@kali:~#
```

Run **selinux-activate**

```
root@kali:~/Desktop# 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-4.19.0-kali1-amd64  
Found initrd image: /boot/initrd.img-4.19.0-kali1-amd64  
done  
SE Linux is activated. You may need to reboot now.
```

**check-selinux-installation & sestatus**



```
root@kali:~# 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?")
IOError: /etc/default/rcS not found, is this Debian?
root@kali:~# 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
```

pwd

```
root@kali:~# pwd
/root
root@kali:~#
```

Ls -l

```
root@kali:~# ls -l
total 32
drwxr-xr-x. 2 root root 4096 Mar  6 11:09 Desktop
drwxr-xr-x. 2 root root 4096 Feb 11 02:46 Documents
drwxr-xr-x. 2 root root 4096 Feb 11 02:46 Downloads
drwxr-xr-x. 2 root root 4096 Feb 11 02:46 Music
drwxr-xr-x. 2 root root 4096 Feb 11 02:46 Pictures
drwxr-xr-x. 2 root root 4096 Feb 11 02:46 Public
drwxr-xr-x. 2 root root 4096 Feb 11 02:46 Templates
drwxr-xr-x. 2 root root 4096 Feb 11 02:46 Videos
```

Ls -Z

```
root@kali:~# 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
```

cat /etc/selinux/config

Current status of SELINUX: **permissive**

Current type of SELINUX: **default**

```
root@kali:~# 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
root@kali:~#
```



## semanage -h

```
root@kali:~# 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
```

## Semanage boolean

```
root@kali:~# semanage Boolean
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
semanage: error: argument subcommand: invalid choice: 'Boolean' (choose from 'import', 'export', 'login', 'user', 'port', 'ibpkey', 'ibendport', 'interface',
'module', 'node', 'fcontext', 'boolean', 'permissive', 'dontaudit')
```

## semanage boolean -l

```
root@kali:~# semanage boolean -l
```

## SELinux boolean State Default Description

`allow_cvs_read_shadow` (off , off) Determine whether cvs can read shadow password files.

`allow_execheap` (off , off) Allow unconfined executables to make their heap memory executable. Doing this is a really bad idea. Probably indicates a badly coded executable, but could indicate an attack. This executable should be reported in bugzilla

`allow_execmem` (off , off) Allow unconfined executables to map a memory region as both executable and writable, this is dangerous and the executable should be reported in bugzilla")

`allow_execmod` (off , off) Allow all unconfined executables to use libraries requiring text relocation that are not labeled `textrel_shlib_t`")

`allow_execstack` (off , off) Allow unconfined executables to make their stack executable. This should never, ever be necessary. Probably indicates a badly coded executable, but could indicate an attack. This executable should be reported in bugzilla")

`allow_ftpd_anon_write` (off , off) Determine whether ftpd can modify public files used for public file transfer services. Directories/Files must be labeled `public_content_rw_t`.

`allow_ftpd_full_access` (off , off) Determine whether ftpd can login to local users and can read and write all files on the system, governed by DAC.

`allow_ftpd_use_cifs` (off , off) Determine whether ftpd can use CIFS used for public file transfer services.

`allow_ftpd_use_nfs` (off , off) Determine whether ftpd can use NFS used for public file transfer services.

`allow_gssd_read_tmp` (off , off) Determine whether gssd can read generic user temporary content.

`allow_gssd_write_tmp` (off , off) Determine whether gssd can write generic user temporary content.

`allow_httpd_anon_write` (off , off) Determine whether httpd can modify public files used for public file transfer services. Directories/Files must be labeled `public_content_rw_t`.

`allow_httpd_apcupsd_cgi_script_anon_write` (off , off) Determine whether the script domain can modify public files used for public file transfer services. Directories/Files must be labeled `public_content_rw_t`.

allow\_httpd\_awstats\_script\_anon\_write (off , off) Determine whether the script domain can modify public files used for public file transfer services. Directories/Files must be labeled public\_content\_rw\_t.

allow\_httpd\_bugzilla\_script\_anon\_write (off , off) Determine whether the script domain can modify public files used for public file transfer services. Directories/Files must be labeled public\_content\_rw\_t.

allow\_httpd\_collectd\_script\_anon\_write (off , off) Determine whether the script domain can modify public files used for public file transfer services. Directories/Files must be labeled public\_content\_rw\_t.

allow\_httpd\_cvs\_script\_anon\_write (off , off) Determine whether the script domain can modify public files used for public file transfer services. Directories/Files must be labeled public\_content\_rw\_t.

allow\_httpd\_dspam\_script\_anon\_write (off , off) Determine whether the script domain can modify public files used for public file transfer services. Directories/Files must be labeled public\_content\_rw\_t.

allow\_httpd\_git\_script\_anon\_write (off , off) Determine whether the script domain can modify public files used for public file transfer services. Directories/Files must be labeled public\_content\_rw\_t.

allow\_httpd\_lightsquid\_script\_anon\_write (off , off) Determine whether the script domain can modify public files used for public file transfer services. Directories/Files must be labeled public\_content\_rw\_t.

allow\_httpd\_man2html\_script\_anon\_write (off , off) Determine whether the script domain can modify public files used for public file transfer services. Directories/Files must be labeled public\_content\_rw\_t.

allow\_httpd\_mediawiki\_script\_anon\_write (off , off) Determine whether the script domain can modify public files used for public file transfer services. Directories/Files must be labeled public\_content\_rw\_t.

allow\_httpd\_mod\_auth\_pam (off , off) Determine whether httpd can use mod\_auth\_pam.

allow\_httpd\_mojomojo\_script\_anon\_write (off , off) Determine whether the script domain can modify public files used for public file transfer services. Directories/Files must be labeled public\_content\_rw\_t.

allow\_httpd\_munin\_script\_anon\_write (off , off) Determine whether the script domain can modify public files used for public file transfer services. Directories/Files must be labeled public\_content\_rw\_t.

allow\_httpd\_nagios\_script\_anon\_write (off , off) Determine whether the script domain can modify public files used for public file transfer services. Directories/Files must be labeled public\_content\_rw\_t.

allow\_httpd\_nutups\_cgi\_script\_anon\_write (off , off) Determine whether the script domain can modify public files used for public file transfer services. Directories/Files must be labeled public\_content\_rw\_t.

allow\_httpd\_prewikka\_script\_anon\_write (off , off) Determine whether the script domain can modify public files used for public file transfer services. Directories/Files must be labeled public\_content\_rw\_t.

allow\_httpd\_smokeping\_cgi\_script\_anon\_write (off , off) Determine whether the script domain can modify public files used for public file transfer services. Directories/Files must be labeled public\_content\_rw\_t.

allow\_httpd\_squid\_script\_anon\_write (off , off) Determine whether the script domain can modify public files used for public file transfer services. Directories/Files must be labeled public\_content\_rw\_t.

allow\_httpd\_sys\_script\_anon\_write (off , off) Determine whether the script domain can modify public files used for public file transfer services. Directories/Files must be labeled public\_content\_rw\_t.

allow\_httpd\_unconfined\_script\_anon\_write (off , off) Determine whether the script domain can modify public files used for public file transfer services. Directories/Files must be labeled public\_content\_rw\_t.

allow\_httpd\_user\_script\_anon\_write (off , off) Determine whether the script domain can modify public files used for public file transfer services. Directories/Files must be labeled public\_content\_rw\_t.

allow\_httpd\_w3c\_validator\_script\_anon\_write (off , off) Determine whether the script domain can modify public files used for public file transfer services. Directories/Files must be labeled public\_content\_rw\_t.

allow\_httpd\_webalizer\_script\_anon\_write (off , off) Determine whether the script domain can modify public files used for public file transfer services. Directories/Files must be labeled public\_content\_rw\_t.

allow\_java\_execstack (off , off) Determine whether java can make its stack executable.

allow\_kerberos (off , off) Determine whether kerberos is supported.

allow\_mount\_anyfile (off , off) Allow the mount command to mount any directory or file.

allow\_mplayer\_execstack (off , off) Determine whether mplayer can make its stack executable.

allow\_nfsd\_anon\_write (off , off) Determine whether nfs can modify public files used for public file transfer services. Directories/Files must be labeled public\_content\_rw\_t.

allow\_polyinstantiation (off , off) Enable polyinstantiated directory support.

allow\_ptrace (off , off) Allow sysadm to debug or ptrace all processes.

allow\_rsync\_anon\_write (off , off) Determine whether rsync can modify public files used for public file transfer services. Directories/Files must be labeled public\_content\_rw\_t.

allow\_saslauthd\_read\_shadow (off , off) Determine whether sasl can read shadow files.

allow\_smbd\_anon\_write (off , off) Determine whether samba can modify public files used for public file transfer services. Directories/Files must be labeled public\_content\_rw\_t.

allow\_ssh\_keysign (off , off) allow host key based authentication

allow\_user\_mysql\_connect (off , off) Allow users to connect to mysql

allow\_user\_postgresql\_connect (off , off) Allow users to connect to PostgreSQL

allow\_write\_xshm (off , off) Allows clients to write to the X server shared memory segments.

allow\_yppbind (off , off) Allow system to run with NIS

allow\_zebra\_write\_config (off , off) Determine whether zebra daemon can manage its configuration files.

amavis\_use\_jit (off , off) Determine whether amavis can use JIT compiler.

authlogin\_nsswitch\_use\_ldap (off , off) Allow users to resolve user passwd entries directly from ldap rather than using a sssd server

awstats\_purge\_apache\_log\_files (off , off) Determine whether awstats can purge httpd log files.

boinc\_execmem (on , on) Determine whether boinc can execmem/execstack.

cdrecord\_read\_content (off , off) Determine whether cdrecord can read various content. nfs, samba, removable devices, user temp and untrusted content files

chromium\_bind\_tcp\_unreserved\_ports (off , off) Allow chromium to bind to tcp ports

chromium\_exec\_plugins (off , off) Allow chromium to execute it's config (for plugins like Flash)



chromium\_manage\_all\_user\_content (off , off) Grant the chromium domains manage rights on all user content

chromium\_manage\_generic\_user\_content (off , off) Grant the chromium domains manage rights on generic user content

chromium\_read\_all\_user\_content (off , off) Grant the chromium domains read access to all user content

chromium\_read\_generic\_user\_content (on , on) Grant the chromium domains read access to generic user content

chromium\_read\_system\_info (off , off) Allow chromium to read system information

chromium\_rw\_usb\_dev (off , off) Allow chromium to read/write USB devices

clamav\_read\_all\_non\_security\_files\_clamscan (off , off) Determine whether clamscan can read all non-security files.

clamav\_read\_user\_content\_files\_clamscan (off , off) Determine whether clamscan can read user content files.

clamd\_use\_jit (off , off) Determine whether can clamd use JIT compiler.

collectd\_tcp\_network\_connect (off , off) Determine whether collectd can connect to the network using TCP.

condor\_tcp\_network\_connect (off , off) Determine whether Condor can connect to the network using TCP.

console\_login (on , on) Allow logging in and using the system from /dev/console.

cron\_can\_relabel (off , off) Determine whether system cron jobs can relabel filesystem for restoring file contexts.

cron\_manage\_all\_user\_content (off , off) Grant the cron domains manage rights on all user content

cron\_manage\_generic\_user\_content (off , off) Grant the cron domains manage rights on generic user content

cron\_read\_all\_user\_content (off , off) Grant the cron domains read access to all user content

cron\_read\_generic\_user\_content (on , on) Grant the cron domains read access to generic user content

cron\_userdomain\_transition (on , on) Determine whether crond can execute jobs in the user domain as opposed to the the generic cronjob domain.

dbadm\_manage\_user\_files (off , off) Determine whether dbadm can manage generic user files.

dbadm\_read\_user\_files (off , off) Determine whether dbadm can read generic user files.

dhcpd\_use\_ldap (off , off) Determine whether DHCP daemon can use LDAP backends.

dovecot\_can\_connect\_db (off , off) Determine whether dovecot can connect to databases.

entropyd\_use\_audio (off , off) Determine whether entropyd can use audio devices as the source for the entropy feeds.

evolution\_manage\_all\_user\_content (off , off) Grant the evolution domains manage rights on all user content

evolution\_manage\_generic\_user\_content (off , off) Grant the evolution domains manage rights on generic user content

evolution\_manage\_user\_certs (off , off) Allow evolution to create and write user certificates in addition to being able to read them

evolution\_read\_all\_user\_content (off , off) Grant the evolution domains read access to all user content

evolution\_read\_generic\_user\_content (on , on) Grant the evolution domains read access to generic user content

exim\_can\_connect\_db (off , off) Determine whether exim can connect to databases.

exim\_manage\_user\_files (off , off) Determine whether exim can create, read, write, and delete generic user content files.

exim\_read\_user\_files (off , off) Determine whether exim can read generic user content files.

fcron\_cron (off , off) Determine whether extra rules should be enabled to support fcron.

fenced\_can\_network\_connect (off , off) Determine whether fenced can connect to the TCP network.

fenced\_can\_ssh (off , off) Determine whether fenced can use ssh.

ftp\_home\_dir (off , off) Determine whether ftpd can read and write files in user home directories.

ftpd\_connect\_all\_unreserved (off , off) Determine whether ftpd can connect to all unreserved ports.

ftpd\_connect\_db (off , off) Determine whether ftpd can connect to databases over the TCP network.

ftpd\_use\_passive\_mode (off , off) Determine whether ftpd can bind to all unreserved ports for passive mode.

git\_cgi\_enable\_homedirs (off , off) Determine whether Git CGI can search home directories.

git\_cgi\_use\_cifs (off , off) Determine whether Git CGI can access cifs file systems.

git\_cgi\_use\_nfs (off , off) Determine whether Git CGI can access nfs file systems.

git\_session\_bind\_all\_unreserved\_ports (off , off) Determine whether Git session daemon can bind TCP sockets to all unreserved ports.

git\_session\_send\_syslog\_msg (off , off) Determine whether Git session daemons can send syslog messages.

git\_session\_users (off , off) Determine whether calling user domains can execute Git daemon in the git\_session\_t domain.

git\_system\_enable\_homedirs (off , off) Determine whether Git system daemon can search home directories.

git\_system\_use\_cifs (off , off) Determine whether Git system daemon can access cifs file systems.

git\_system\_use\_nfs (off , off) Determine whether Git system daemon can access nfs file systems.

gitosis\_can\_sendmail (off , off) Determine whether Gitosis can send mail.

global\_ssp (off , off) Enable reading of urandom for all domains.

gpg\_agent\_env\_file (off , off) Determine whether GPG agent can manage generic user home content files. This is required by the --write-env-file option.

gpg\_agent\_use\_card (off , off) Determine whether GPG agent can use OpenPGP cards or Yubikeys over USB

gpg\_manage\_all\_user\_content (off , off) Grant the gpg domains manage rights on all user content

gpg\_manage\_generic\_user\_content (off , off) Grant the gpg domains manage rights on generic user content

gpg\_read\_all\_user\_content (off , off) Grant the gpg domains read access to all user content

gpg\_read\_generic\_user\_content (on , on) Grant the gpg domains read access to generic user content

httpd\_builtin\_scripting (off , off) Determine whether httpd can use built in scripting.

httpd\_can\_check\_spam (off , off) Determine whether httpd can check spam.

httpd\_can\_network\_connect (off , off) Determine whether httpd scripts and modules can connect to the network using TCP.

httpd\_can\_network\_connect\_cobbler (off , off) Determine whether httpd scripts and modules can connect to cobbler over the network.

httpd\_can\_network\_connect\_db (off , off) Determine whether scripts and modules can connect to databases over the network.

httpd\_can\_network\_connect\_ldap (off , off) Determine whether httpd can connect to ldap over the network.

httpd\_can\_network\_connect\_memcache (off , off) Determine whether httpd can connect to memcache server over the network.

httpd\_can\_network\_connect\_zabbix (off , off) Determine whether httpd daemon can connect to zabbix over the network.

httpd\_can\_network\_relay (off , off) Determine whether httpd can act as a relay.

httpd\_can\_sendmail (off , off) Determine whether httpd can send mail.

httpd\_dbus\_avahi (off , off) Determine whether httpd can communicate with avahi service via dbus.

httpd\_enable\_cgi (off , off) Determine whether httpd can use support.

httpd\_enable\_ftp\_server (off , off) Determine whether httpd can act as a FTP server by listening on the ftp port.

httpd\_enable\_homedirs (off , off) Determine whether httpd can traverse user home directories.

httpd\_execmem (off , off) Determine whether httpd scripts and modules can use execmem and execstack.

httpd\_gpg\_anon\_write (off , off) Determine whether httpd gpg can modify public files used for public file transfer services. Directories/Files must be labeled public\_content\_rw\_t.

httpd\_graceful\_shutdown (off , off) Determine whether httpd can connect to port 80 for graceful shutdown.

httpd\_manage\_ipa (off , off) Determine whether httpd can manage IPA content files.

httpd\_mod\_auth\_ntlm\_winbind (off , off) Determine whether httpd can use mod\_auth\_ntlm\_winbind.

httpd\_read\_user\_content (off , off) Determine whether httpd can read generic user home content files.

httpd\_setrlimit (off , off) Determine whether httpd can change its resource limits.

httpd\_ssi\_exec (off , off) Determine whether httpd can run SSI executables in the same domain as system CGI scripts.

httpd\_tmp\_exec (off , off) Determine whether httpd can execute its temporary content.

httpd\_tty\_comm (off , off) Determine whether httpd can communicate with the terminal. Needed for entering the passphrase for certificates at the terminal.

httpd\_unified (off , off) Determine whether httpd can have full access to its content types.

httpd\_use\_cifs (off , off) Determine whether httpd can use cifs file systems.

httpd\_use\_fusefs (off , off) Determine whether httpd can use fuse file systems.

httpd\_use\_gpg (off , off) Determine whether httpd can use gpg.

httpd\_use\_nfs (off , off) Determine whether httpd can use nfs file systems.

i18n\_input\_read\_generic\_user\_content (on , on) Grant the i18n\_input domains read access to generic user content

icecast\_use\_any\_tcp\_ports (off , off) Determine whether icecast can listen on and connect to any TCP port.

init\_daemons\_use\_tty (off , off) Allow all daemons the ability to read/write terminals

init\_upstart (off , off) Enable support for upstart as the init program.

irc\_manage\_all\_user\_content (off , off) Grant the irc domains manage rights on all user content

irc\_manage\_generic\_user\_content (off , off) Grant the irc domains manage rights on generic user content

irc\_read\_all\_user\_content (off , off) Grant the irc domains read access to all user content



irc\_read\_generic\_user\_content (on , on) Grant the irc domains read access to generic user content

irc\_use\_any\_tcp\_ports (off , off) Determine whether irc clients can listen on and connect to any unreserved TCP ports.

java\_manage\_all\_user\_content (off , off) Grant the java domains manage rights on all user content

java\_manage\_generic\_user\_content (off , off) Grant the java domains manage rights on generic user content

java\_read\_all\_user\_content (off , off) Grant the java domains read access to all user content

java\_read\_generic\_user\_content (on , on) Grant the java domains read access to generic user content

logwatch\_can\_network\_connect\_mail (off , off) Determine whether logwatch can connect to mail over the network.

mail\_read\_content (off , off) Allow email client to various content. nfs, samba, removable devices, and user temp files

mcelog\_client (off , off) Determine whether mcelog supports client mode.

mcelog\_exec\_scripts (on , on) Determine whether mcelog can execute scripts.

mcelog\_foreground (off , off) Determine whether mcelog can use all the user ttys.

mcelog\_server (off , off) Determine whether mcelog supports server mode.

mcelog\_syslog (off , off) Determine whether mcelog can use syslog.

minidlna\_read\_generic\_user\_content (off , off) Determine whether minidlna can read generic user content.

mmap\_low\_allowed (off , off) Control the ability to mmap a low area of the address space, as configured by /proc/sys/kernel/mmap\_min\_addr.

monit\_startstop\_services (off , off) Allow monit to start/stop services

mozilla\_execstack (off , off) Determine whether mozilla can make its stack executable.

mozilla\_manage\_all\_user\_content (off , off) Grant the mozilla domains manage rights on all user content

mozilla\_manage\_generic\_user\_content (off , off) Grant the mozilla domains manage rights on generic user content

mozilla\_read\_all\_user\_content (off , off) Grant the mozilla domains read access to all user content

mozilla\_read\_generic\_user\_content (on , on) Grant the mozilla domains read access to generic user content

mpd\_enable\_homedirs (off , off) Determine whether mpd can traverse user home directories.

mpd\_use\_cifs (off , off) Determine whether mpd can use cifs file systems.

mpd\_use\_nfs (off , off) Determine whether mpd can use nfs file systems.

mplayer\_manage\_all\_user\_content (off , off) Grant the mplayer domains manage rights on all user content

mplayer\_manage\_generic\_user\_content (off , off) Grant the mplayer domains manage rights on generic user content

mplayer\_mencoder\_manage\_all\_user\_content (off , off) Grant the mplayer\_mencoder domains manage rights on all user content

mplayer\_mencoder\_manage\_generic\_user\_content (off , off) Grant the mplayer\_mencoder domains manage rights on generic user content

mplayer\_mencoder\_read\_all\_user\_content (off , off) Grant the mplayer\_mencoder domains read access to all user content

mplayer\_mencoder\_read\_generic\_user\_content (on , on) Grant the mplayer\_mencoder domains read access to generic user content

mplayer\_read\_all\_user\_content (off , off) Grant the mplayer domains read access to all user content

mplayer\_read\_generic\_user\_content (on , on) Grant the mplayer domains read access to generic user content

mysql\_connect\_any (off , off) Determine whether mysqld can connect to all TCP ports.

named\_tcp\_bind\_http\_port (off , off) Determine whether Bind can bind tcp socket to http ports.

named\_write\_master\_zones (off , off) Determine whether Bind can write to master zone files. Generally this is used for dynamic DNS or zone transfers.

nfs\_export\_all\_ro (off , off) Allow any files/directories to be exported read/only via NFS.

nfs\_export\_all\_rw (off , off) Allow any files/directories to be exported read/write via NFS.

nscd\_use\_shm (off , off) Determine whether confined applications can use nscd shared memory.

openvpn\_can\_network\_connect (off , off) Determine whether openvpn can connect to the TCP network.

openvpn\_enable\_homedirs (off , off) Determine whether openvpn can read generic user home content files.

polipo\_session\_send\_syslog\_msg (off , off) Determine whether Polipo session daemon can send syslog messages.

polipo\_session\_users (off , off) Determine whether calling user domains can execute Polipo daemon in the polipo\_session\_t domain.

polipo\_system\_use\_cifs (off , off) Determine whether Polipo system daemon can access CIFS file systems.

polipo\_system\_use\_nfs (off , off) Determine whether Polipo system daemon can access NFS file systems.

postfix\_local\_write\_mail\_spool (on , on) Determine whether postfix local can manage mail spool content.

postfix\_manage\_all\_user\_content (off , off) Grant the postfix domains manage rights on all user content

postfix\_manage\_generic\_user\_content (off , off) Grant the postfix domains manage rights on generic user content

postfix\_read\_all\_user\_content (off , off) Grant the postfix domains read access to all user content

postfix\_read\_generic\_user\_content (on , on) Grant the postfix domains read access to generic user content

pppd\_can\_insmmod (off , off) Determine whether pppd can load kernel modules.

pppd\_for\_user (off , off) Determine whether common users can run pppd with a domain transition.

privoxy\_connect\_any (off , off) Determine whether privoxy can connect to all tcp ports.

pulseaudio\_execmem (off , off) Allow pulseaudio to execute code in writable memory

puppet\_manage\_all\_files (off , off) Determine whether puppet can manage all non-security files.

qemu\_full\_network (off , off) Determine whether qemu has full access to the network.

racoona\_read\_shadow (off , off) Allow racoona to read shadow

rgmanager\_can\_network\_connect (off , off) Determine whether rgmanager can connect to the network using TCP.

rsync\_client (off , off) Determine whether rsync can run as a client

rsync\_export\_all\_ro (off , off) Determine whether rsync can export all content read only.

rsync\_use\_cifs (off , off) Determine whether rsync can use cifs file systems.

rsync\_use\_fusefs (off , off) Determine whether rsync can use fuse file systems.

rsync\_use\_nfs (off , off) Determine whether rsync can use nfs file systems.

samba\_create\_home\_dirs (off , off) Determine whether samba can create home directories via pam.

samba\_domain\_controller (off , off) Determine whether samba can act as the domain controller, add users, groups and change passwords.

samba\_enable\_home\_dirs (off , off) Determine whether samba can share users home directories.

samba\_export\_all\_ro (off , off) Determine whether samba can share any content read only.

samba\_export\_all\_rw (off , off) Determine whether samba can share any content readable and writable.

samba\_portmapper (off , off) Determine whether samba can act as a portmapper.

samba\_read\_shadow (off , off) Determine whether smbd\_t can read shadow files.

samba\_run\_unconfined (off , off) Determine whether samba can run unconfined scripts.

samba\_share\_fusefs (off , off) Determine whether samba can use fuse file systems.

samba\_share\_nfs (off , off) Determine whether samba can use nfs file systems.

sanlock\_use\_nfs (off , off) Determine whether sanlock can use nfs file systems.

sanlock\_use\_samba (off , off) Determine whether sanlock can use cifs file systems.

secure\_mode (off , off) Enabling secure mode disallows programs, such as newrole, from transitioning to administrative user domains.

secure\_mode\_insmo (off , off) Disable kernel module loading.

secure\_mode\_policyload (off , off) Boolean to determine whether the system permits loading policy, setting enforcing mode, and changing boolean values. Set this to true and you have to reboot to set it back.

sepgsql\_enable\_users\_ddl (off , off) Allow unprivileged users to execute DDL statement

sepgsql\_transmit\_client\_label (off , off) Allow transmit client label to foreign database

sepgsql\_unconfined\_dbadm (off , off) Allow database admins to execute DML statement

sftpd\_anon\_write (off , off) Determine whether sftpd can modify public files used for public file transfer services. Directories/Files must be labeled public\_content\_rw\_t.

sftpd\_enable\_homedirs (off , off) Determine whether sftpd-can read and write files in user home directories.

sftpd\_full\_access (off , off) Determine whether sftpd-can login to local users and read and write all files on the system, governed by DAC.

sftpd\_write\_ssh\_home (off , off) Determine whether sftpd can read and write files in user ssh home directories.

smartmon\_3ware (off , off) Determine whether smartmon can support devices on 3ware controllers.

spamassassin\_can\_network (off , off) Determine whether spamassassin clients can use the network.

spamd\_enable\_home\_dirs (off , off) Determine whether spamd can manage generic user home content.

squid\_connect\_any (off , off) Determine whether squid can connect to all TCP ports.

squid\_use\_pinger (on , on) Determine whether squid can use the pinger daemon (needs raw net access)

squid\_use\_tproxy (off , off) Determine whether squid can run as a transparent proxy.

ssh\_sysadm\_login (off , off) Allow ssh logins as sysadm\_r:sysadm\_t

ssh\_use\_gpg\_agent (off , off) Allow ssh to use gpg-agent

systemd\_nspawn\_labeled\_namespace (off , off) Allow systemd-nspawn to create a labelled namespace with the same types as parent environment

systemd\_tmpfiles\_manage\_all (off , off) Enable support for systemd-tmpfiles to manage all non-security files.



telepathy\_connect\_all\_ports (off , off) Determine whether telepathy connection managers can connect to any port.

telepathy\_tcp\_connect\_generic\_network\_ports (off , off) Determine whether telepathy connection managers can connect to generic tcp ports.

tftp\_anon\_write (off , off) Determine whether tftp can modify public files used for public file transfer services. Directories/Files must be labeled public\_content\_rw\_t.

tftp\_enable\_homedir (off , off) Determine whether tftp can manage generic user home content.

thunderbird\_manage\_all\_user\_content (off , off) Grant the thunderbird domains manage rights on all user content

thunderbird\_manage\_generic\_user\_content (off , off) Grant the thunderbird domains manage rights on generic user content

thunderbird\_read\_all\_user\_content (off , off) Grant the thunderbird domains read access to all user content

thunderbird\_read\_generic\_user\_content (on , on) Grant the thunderbird domains read access to generic user content

tor\_bind\_all\_unreserved\_ports (off , off) Determine whether tor can bind tcp sockets to all unreserved ports.

use\_lpd\_server (off , off) Determine whether to support lpd server.

use\_nfs\_home\_dirs (off , off) Support NFS home directories

use\_samba\_home\_dirs (off , off) Support SAMBA home directories

user\_bind\_unreserved (off , off) Allow user to bind all unreserved ports

user\_direct\_mouse (off , off) Allow regular users direct mouse access

user\_dmesg (off , off) Allow users to read system messages.

user\_exec\_noexattrfile (off , off) Allow user to execute files on filesystems that do not have extended attributes (FAT, CDROM, FLOPPY)

user\_ping (off , off) Control users use of ping and traceroute

user\_rw\_noexattrfile (off , off) Allow user to r/w files on filesystems that do not have extended attributes (FAT, CDROM, FLOPPY)

user\_tcp\_server (off , off) Allow users to run TCP servers (bind to ports and accept connection from the same domain and outside users) disabling this forces FTP passive mode and may change other protocols.

user\_ttyfile\_stat (off , off) Allow w to display everyone

user\_udp\_server (off , off) Allow users to run UDP servers (bind to ports and accept connection from the same domain and outside users)

user\_write\_removable (off , off) Allow user to write files on removable devices (e.g. external USB memory devices or floppies)

varnishd\_connect\_any (off , off) Determine whether varnishd can use the full TCP network.

vbtool\_mmap\_zero\_ignore (off , off) Determine whether attempts by vbtool to mmap low regions should be silently blocked.

virt\_use\_comm (off , off) Determine whether confined virtual guests can use serial/parallel communication ports.

virt\_use\_execmem (off , off) Determine whether confined virtual guests can use executable memory and can make their stack executable.

virt\_use\_fusefs (off , off) Determine whether confined virtual guests can use fuse file systems.

virt\_use\_nfs (off , off) Determine whether confined virtual guests can use nfs file systems.

virt\_use\_samba (off , off) Determine whether confined virtual guests can use cifs file systems.

virt\_use\_sysfs (off , off) Determine whether confined virtual guests can manage device configuration.

virt\_use\_usb (off , off) Determine whether confined virtual guests can use usb devices.

virt\_use\_vfio (off , off) Determine whether confined virtual guests can use vfio for pci device pass through (vt-d).

virt\_use\_xserver (off , off) Determine whether confined virtual guests can interact with xserver.

webadm\_manage\_user\_files (off , off) Determine whether webadm can manage generic user files.

webadm\_read\_user\_files (off , off) Determine whether webadm can read generic user files.

wine\_mmap\_zero\_ignore (off , off) Determine whether attempts by wine to mmap low regions should be silently blocked.

wireshark\_manage\_all\_user\_content (off , off) Grant the wireshark domains manage rights on all user content

wireshark\_manage\_generic\_user\_content (off , off) Grant the wireshark domains manage rights on generic user content

wireshark\_read\_all\_user\_content (off , off) Grant the wireshark domains read access to all user content

wireshark\_read\_generic\_user\_content (on , on) Grant the wireshark domains read access to generic user content

xdm\_sysadm\_login (off , off) Allow xdm logins as sysadm

xen\_use\_fusefs (off , off) Determine whether xen can use fusefs file systems.

xen\_use\_nfs (off , off) Determine whether xen can use nfs file systems.

xen\_use\_samba (off , off) Determine whether xen can use samba file systems.

xend\_run\_blkmap (off , off) Determine whether xend can run blkmapctrl and tapdisk.

xguest\_connect\_network (off , off) Determine whether xguest can configure network manager.

xguest\_mount\_media (off , off) Determine whether xguest can mount removable media.

xguest\_use\_bluetooth (off , off) Determine whether xguest can use blue tooth devices.

xscreensaver\_read\_generic\_user\_content (on , on) Grant the xscreensaver domains read access to generic user content

xserver\_allow\_dri (off , off) Allow DRI access

xserver\_gnome\_xdm (off , off) Use gnome-shell in gdm mode as the X Display Manager (XDM)

xserver\_object\_manager (off , off) Support X userspace object manager

zabbix\_can\_network (off , off) Determine whether zabbix can connect to all TCP ports

What is the default value of the **fenced\_can\_ssh** process? **off**

What is the current value of the **user\_ping** process? **Off**

getsebool user\_ping

```
root@kali:~# getsebool user_ping
user_ping --> off
root@kali:~#
```

getsebool fenced\_can\_ssh

```
root@kali:~# getsebool fenced_can_ssh
fenced_can_ssh --> off
root@kali:~#
```

getsebool httpd\_can\_network\_connect\_db

```
root@kali:~# getsebool httpd_can_network_connect_db
httpd_can_network_connect_db --> off
root@kali:~#
```

setsebool httpd\_can\_network\_connect\_db on

setsebool -P httpd\_can\_network\_connect\_db on

```
root@kali:~# getsebool user_ping
user_ping --> off
root@kali:~# getsebool fenced_can_ssh
fenced_can_ssh --> off
root@kali:~# getsebool httpd_can_network_connect_db
httpd_can_network_connect_db --> off
root@kali:~# setsebool httpd_can_network_connect_db on
root@kali:~# getsebool httpd_can_network_connect_db
httpd_can_network_connect_db --> on
root@kali:~#
```

ps axZ | grep httpd

```
root@kali:~# ps axZ | grep httpd
system_u:system_r:initrc_t:s0    2310 pts/1    S+      0:00 grep httpd
root@kali:~#
```

seinfo -r



```
root@kali:~# 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
```

```
root@kali:~# █
```

apache2ctl start

systemctl status apache2

```

root@kali:~# apache2ctl start
Invoking 'systemctl start apache2'.
Use 'systemctl status apache2' for more info.
root@kali:~# systemctl status apache2
● apache2.service - The Apache HTTP Server
   Loaded: loaded (/lib/systemd/system/apache2.service; disabled; vendor preset: disabled)
   Active: active (running) since Wed 2019-03-06 11:57:26 EST; 22s ago
     Process: 2325 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
    Main PID: 2329 (apache2)
       Tasks: 7 (limit: 2343)
      Memory: 24.3M
     CGroup: /system.slice/apache2.service
             └─2329 /usr/sbin/apache2 -k start
               └─2330 /usr/sbin/apache2 -k start
                 └─2331 /usr/sbin/apache2 -k start
                   └─2332 /usr/sbin/apache2 -k start
                     └─2333 /usr/sbin/apache2 -k start
                       └─2334 /usr/sbin/apache2 -k start
                         └─2335 /usr/sbin/apache2 -k start

Mar 06 11:57:26 kali systemd[1]: Starting The Apache HTTP Server...
Mar 06 11:57:26 kali apachectl[2325]: AH00558: apache2: Could not reliably determine the server's fully qualified domain name, using 127.0.1.1. Set the 'ServerName' directive dynamically to determine the server's name.
Mar 06 11:57:26 kali systemd[1]: Started The Apache HTTP Server.
lines 1-19/19 (END)

```

ps axZ | grep httpd

```

root@kali:~# ps axZ | grep httpd
system_u:system_r:httpd_t:s0      2329 ?        Ss      0:00 /usr/sbin/apache2 -k start
system_u:system_r:httpd_t:s0      2330 ?        S       0:00 /usr/sbin/apache2 -k start
system_u:system_r:httpd_t:s0      2331 ?        S       0:00 /usr/sbin/apache2 -k start
system_u:system_r:httpd_t:s0      2332 ?        S       0:00 /usr/sbin/apache2 -k start
system_u:system_r:httpd_t:s0      2333 ?        S       0:00 /usr/sbin/apache2 -k start
system_u:system_r:httpd_t:s0      2334 ?        S       0:00 /usr/sbin/apache2 -k start
system_u:system_r:httpd_t:s0      2335 ?        S       0:00 /usr/sbin/apache2 -k start
system_u:system_r:initrc_t:s0     2396 pts/1    S+      0:00 grep httpd
root@kali:~#

```

## Part 2: Relabeling Files in SELinux

### 1. Make Directory on the root folder

```
root@kali:~# mkdir html
```

### 2. Create index.html inside the html folder

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

### 3. List the context labels for the file

```
root@kali:~# ls -Z html/index.html
```

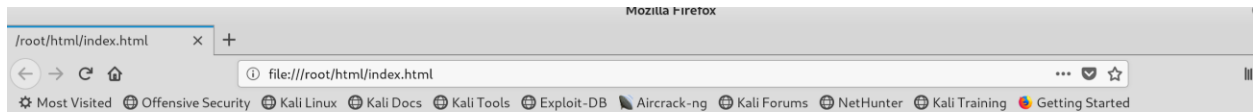
```
system_u:object_r:user_home_dir_t:s0 html/index.html
```

#### 4. List the context label for the directory

```
root@kali:~# ls -Z | grep html
```

```
system_u:object_r:user_home_dir_t:s0 html
```

#### 5. Attempt to start the browser and document the output



#### 6. Change the context for the directory

```
root@kali:~# chcon -v --type=httpd_sys_content_t html
```

```
changing security context of 'html'
```

#### 7. Change the context for the file

```
root@kali:~# chcon -v --type=httpd_sys_content_t html/index.html
```

```
changing security context of 'html/index.html'
```

##### a. ls -Z /html/index.html

```
root@kali:~# ls -Z html/index.html
```

```
system_u:object_r:httpd_sys_content_t:s0 html/index.html
```

##### b. ls -Z | grep html

```
root@kali:~# ls -Z | grep html
```

```
system_u:object_r:httpd_sys_content_t:s0 html
```

## 8: Relabeling the entire file system

### genhomedircon

```
root@kali:~# genhomedircon
libsemanage.get_home_dirs: Error while fetching users. Returning list so far.
root@kali:~# touch /.autorelabel
root@kali:~#
```

## Reboot

```
*** Warning -- SELinux default policy relabel is required.
*** Relabeling could take a very long time, depending on file
*** system size and speed of hard drives.
libsemanage.get_home_dirs: Error while fetching users. Returning list so far.
Warning: Skipping the following R/O filesystems:
/sys/fs/cgroup
Relabeling / /dev /dev/hugepages /dev/mqueue /dev/pts /dev/shm /run /run/lock /sys /sys/fs/cgroup/bl
kio /sys/fs/cgroup/cpu,cpuacct /sys/fs/cgroup/cpuset /sys/fs/cgroup/devices /sys/fs/cgroup/freezer /
sys/fs/cgroup/memory /sys/fs/cgroup/net_cls,net_prio /sys/fs/cgroup/perf_event /sys/fs/cgroup/pids /
sys/fs/cgroup/systemd /sys/fs/cgroup/unified /sys/fs/pstore /sys/kernel/debug
26.3%
```

## 9: Allowing access to ports and list the ports

### A. semanage port -a -t http\_port\_t -p tcp 81

```
root@kali:~# semanage port -a -t http_port_t -p tcp 81
```

```
libsemanage.get_home_dirs: Error while fetching users. Returning list so far.
```

### B. semanage port -l

```
root@kali:~# semanage port -l
```

SELinux Port Type Proto Port Number

```
afs3_callback_port_t tcp 7001
```

```
afs3_callback_port_t udp 7001
```

afs\_bos\_port\_t udp 7007  
afs\_fs\_port\_t tcp 2040  
afs\_fs\_port\_t udp 7000, 7005  
afs\_ka\_port\_t udp 7004  
afs\_pt\_port\_t udp 7002  
afs\_vl\_port\_t udp 7003  
agentx\_port\_t tcp 705  
agentx\_port\_t udp 705  
amanda\_port\_t tcp 10080-10083  
amanda\_port\_t udp 10080-10082  
amavisd\_recv\_port\_t tcp 10024  
amavisd\_send\_port\_t tcp 10025  
amqp\_port\_t tcp 5671-5672  
amqp\_port\_t udp 5671-5672  
aol\_port\_t tcp 5190-5193  
aol\_port\_t udp 5190-5193  
apcupsd\_port\_t tcp 3551  
apcupsd\_port\_t udp 3551  
apertus\_ldp\_port\_t tcp 539  
apertus\_ldp\_port\_t udp 539  
armtechdaemon\_port\_t tcp 9292  
armtechdaemon\_port\_t udp 9292  
asterisk\_port\_t tcp 1720  
asterisk\_port\_t udp 2427, 2727, 4569  
audit\_port\_t tcp 60  
auth\_port\_t tcp 113  
bgp\_port\_t tcp 179, 2605  
bgp\_port\_t udp 179, 2605

boinc\_client\_port\_t tcp 1043  
boinc\_client\_port\_t udp 1034  
boinc\_port\_t tcp 31416  
certmaster\_port\_t tcp 51235  
chronyd\_port\_t udp 323  
clamd\_port\_t tcp 3310  
clockspeed\_port\_t udp 4041  
cluster\_port\_t tcp 5149, 40040, 50006-50008  
cluster\_port\_t udp 5149, 50006-50008  
cma\_port\_t tcp 1050  
cma\_port\_t udp 1050  
cobbler\_port\_t tcp 25151  
complex\_link\_port\_t tcp 5001  
complex\_link\_port\_t udp 5001  
complex\_main\_port\_t tcp 5000  
complex\_main\_port\_t udp 5000  
comsat\_port\_t udp 512  
condor\_port\_t tcp 9618  
condor\_port\_t udp 9618  
couchdb\_port\_t tcp 5984  
couchdb\_port\_t udp 5984  
cslistener\_port\_t tcp 9000  
cslistener\_port\_t udp 9000  
ctdb\_port\_t tcp 4379  
ctdb\_port\_t udp 4397  
cvs\_port\_t tcp 2401  
cvs\_port\_t udp 2401  
cyphesis\_port\_t tcp 6767, 6769, 6780-6799

cypheis\_port\_t udp 32771  
daap\_port\_t tcp 3689  
daap\_port\_t udp 3689  
dbskkd\_port\_t tcp 1178  
dcc\_port\_t udp 6276, 6277  
dccm\_port\_t tcp 5679  
dccm\_port\_t udp 5679  
dhcpc\_port\_t tcp 68, 546, 5546  
dhcpc\_port\_t udp 68, 546, 5546  
dhcpd\_port\_t tcp 547, 548, 647, 847, 7911  
dhcpd\_port\_t udp 67, 547, 548, 647, 847  
dict\_port\_t tcp 2628  
distccd\_port\_t tcp 3632  
dns\_port\_t tcp 53  
dns\_port\_t udp 53  
dropbox\_port\_t tcp 17500  
dropbox\_port\_t udp 17500  
efs\_port\_t tcp 520  
embrace\_dp\_c\_port\_t tcp 3198  
embrace\_dp\_c\_port\_t udp 3198  
epmap\_port\_t tcp 135  
epmap\_port\_t udp 135  
epmd\_port\_t tcp 4369  
epmd\_port\_t udp 4369  
fingerd\_port\_t tcp 79  
ftp\_data\_port\_t tcp 20  
ftp\_port\_t tcp 21, 990  
ftp\_port\_t udp 990

gatekeeper\_port\_t tcp 1721, 7000

gatekeeper\_port\_t udp 1718, 1719

gdomap\_port\_t tcp 538

gdomap\_port\_t udp 538

gds\_db\_port\_t tcp 3050

gds\_db\_port\_t udp 3050

gift\_d\_port\_t tcp 1213

git\_port\_t tcp 9418

git\_port\_t udp 9418

glance\_registry\_port\_t tcp 9191

glance\_registry\_port\_t udp 9191

gopher\_port\_t tcp 70

gopher\_port\_t udp 70

gpsd\_port\_t tcp 2947

hadoop\_datanode\_port\_t tcp 50010

hadoop\_namenode\_port\_t tcp 8020

hddtemp\_port\_t tcp 7634

hi\_reserved\_port\_t sctp 512-1023

hi\_reserved\_port\_t tcp 512-1023

hi\_reserved\_port\_t udp 512-1023

howl\_port\_t tcp 5335

howl\_port\_t udp 5353

hplip\_port\_t tcp 1782, 2207, 2208, 8290, 8292, 9100, 9101, 9102, 9220, 9221, 9222, 9280, 9281, 9282, 9290, 9291, 50000, 50002

http\_cache\_port\_t tcp 3128, 8080, 8118, 10001-10010

http\_cache\_port\_t udp 3130

http\_port\_t tcp 81, 80, 443, 488, 8008, 8009, 8443

i18n\_input\_port\_t tcp 9010



imaze\_port\_t tcp 5323

imaze\_port\_t udp 5323

inetd\_child\_port\_t tcp 1, 7, 9, 13, 19, 37, 512, 543, 544, 891, 892, 2105, 5666

inetd\_child\_port\_t udp 1, 7, 9, 13, 19, 37, 891, 892

innd\_port\_t tcp 119

interwise\_port\_t tcp 7778

interwise\_port\_t udp 7778

ionixnetmon\_port\_t tcp 7410

ionixnetmon\_port\_t udp 7410

ipmi\_port\_t udp 623, 664

ipp\_port\_t tcp 631, 8610-8614

ipp\_port\_t udp 631, 8610-8614

ipsecnat\_port\_t tcp 4500

ipsecnat\_port\_t udp 4500

ircd\_port\_t tcp 6665, 6666, 6667, 6668, 6669, 6697

isakmp\_port\_t udp 500

iscsi\_port\_t tcp 3260

isns\_port\_t tcp 3205

isns\_port\_t udp 3205

jabber\_client\_port\_t tcp 5222, 5223

jabber\_interserver\_port\_t tcp 5269

jboss\_iiop\_port\_t tcp 3528

jboss\_iiop\_port\_t udp 3528

kerberos\_admin\_port\_t tcp 464, 749

kerberos\_admin\_port\_t udp 464

kerberos\_master\_port\_t tcp 4444

kerberos\_master\_port\_t udp 4444

kerberos\_port\_t tcp 88, 750

kerberos\_port\_t udp 88, 750

kismet\_port\_t tcp 2501

kprop\_port\_t tcp 754

ktalkd\_port\_t udp 517, 518

l2tp\_port\_t tcp 1701

l2tp\_port\_t udp 1701

ldap\_port\_t tcp 389, 636, 3268, 3269

ldap\_port\_t udp 389, 636

lirc\_port\_t tcp 8765

llmnr\_port\_t tcp 5355

llmnr\_port\_t udp 5355

lmp\_port\_t tcp 24

lmp\_port\_t udp 24

mail\_port\_t tcp 2000, 3905

matahari\_port\_t tcp 49000

matahari\_port\_t udp 49000

memcache\_port\_t tcp 11211

memcache\_port\_t udp 11211

mmcc\_port\_t tcp 5050

mmcc\_port\_t udp 5050

mon\_port\_t tcp 2583

mon\_port\_t udp 2583

monit\_port\_t tcp 2812

monopd\_port\_t tcp 1234

mountd\_port\_t tcp 20048

mountd\_port\_t udp 20048

movaz\_ssc\_port\_t tcp 5252

movaz\_ssc\_port\_t udp 5252

mpd\_port\_t tcp 6600

ms\_streaming\_port\_t tcp 1755

ms\_streaming\_port\_t udp 1755

msgsvr\_port\_t tcp 8787

msgsvr\_port\_t udp 8787

msnp\_port\_t tcp 1863

msnp\_port\_t udp 1863

mssql\_port\_t tcp 1433-1434

mssql\_port\_t udp 1433-1434

munin\_port\_t tcp 4949

munin\_port\_t udp 4949

mxi\_port\_t tcp 8005

mxi\_port\_t udp 8005

mysqld\_port\_t tcp 1186, 3306, 63132-63164

mysqlmanagerd\_port\_t tcp 2273

nessus\_port\_t tcp 1241

netport\_port\_t tcp 3129

netport\_port\_t udp 3129

netsupport\_port\_t tcp 5404, 5405

netsupport\_port\_t udp 5404, 5405

nfs\_port\_t tcp 2049

nfs\_port\_t udp 2049

nfsrdma\_port\_t tcp 20049

nfsrdma\_port\_t udp 20049

nmbd\_port\_t udp 137, 138

ntop\_port\_t tcp 3000-3001

ntop\_port\_t udp 3000-3001

ntp\_port\_t udp 123

oa\_system\_port\_t tcp 8022  
oa\_system\_port\_t udp 8022  
ocsp\_port\_t tcp 9080  
openhpid\_port\_t tcp 4743  
openhpid\_port\_t udp 4743  
openvpn\_port\_t tcp 1194  
openvpn\_port\_t udp 1194  
oracledb\_port\_t tcp 1521, 2483, 2484  
oracledb\_port\_t udp 1521, 2483, 2484  
pdps\_port\_t tcp 1314  
pdps\_port\_t udp 1314  
pegasus\_http\_port\_t tcp 5988  
pegasus\_https\_port\_t tcp 5989  
pgpkeyserver\_port\_t tcp 11371  
pgpkeyserver\_port\_t udp 11371  
pingd\_port\_t tcp 9125  
pktcable\_cops\_port\_t tcp 2126  
pktcable\_cops\_port\_t udp 2126  
pop\_port\_t tcp 106, 109, 110, 143, 220, 993, 995, 1109  
portmap\_port\_t tcp 111  
portmap\_port\_t udp 111  
postfix\_policyd\_port\_t tcp 10031  
postgresql\_port\_t tcp 5432  
postgrey\_port\_t tcp 10023, 60000  
pptp\_port\_t tcp 1723  
pptp\_port\_t udp 1723  
prelude\_port\_t tcp 4690  
prelude\_port\_t udp 4690

presence\_port\_t tcp 5298-5299  
presence\_port\_t udp 5298-5299  
printer\_port\_t tcp 515  
ptal\_port\_t tcp 5703  
pulseaudio\_port\_t tcp 4713  
puppet\_port\_t tcp 8140  
pxe\_port\_t udp 4011  
pyzor\_port\_t udp 24441  
radacct\_port\_t udp 1646, 1813  
radius\_port\_t udp 1645, 1812  
radsec\_port\_t tcp 2083  
razor\_port\_t tcp 2703  
redis\_port\_t tcp 6379, 26379  
repository\_port\_t tcp 6363  
reserved\_port\_t sctp 1-511  
reserved\_port\_t tcp 1-511  
reserved\_port\_t udp 1-511  
ricci\_modcluster\_port\_t tcp 16851  
ricci\_modcluster\_port\_t udp 16851  
ricci\_port\_t tcp 11111  
ricci\_port\_t udp 11111  
rlogind\_port\_t tcp 513  
rndc\_port\_t tcp 953, 8953  
rndc\_port\_t udp 953, 8953  
router\_port\_t tcp 521  
router\_port\_t udp 520, 521  
rsh\_port\_t tcp 514  
rsync\_port\_t tcp 873

rsync\_port\_t udp 873  
rtsp\_port\_t tcp 554  
rtsp\_port\_t udp 554  
rwho\_port\_t udp 513  
sap\_port\_t tcp 9875  
sap\_port\_t udp 9875  
servistaitesm\_port\_t tcp 3636  
servistaitesm\_port\_t udp 3636  
sieve\_port\_t tcp 4190  
sip\_port\_t tcp 5060, 5061  
sip\_port\_t udp 5060, 5061  
sixxsconfig\_port\_t tcp 3874  
sixxsconfig\_port\_t udp 3874  
smbd\_port\_t tcp 445, 137-139  
smtp\_port\_t tcp 25, 465, 587  
snmp\_port\_t tcp 199, 1161  
snmp\_port\_t udp 161, 162  
soundd\_port\_t tcp 8000, 9433, 16001  
spamd\_port\_t tcp 783  
speech\_port\_t tcp 8036  
squid\_port\_t tcp 3401, 4827  
squid\_port\_t udp 3401, 4827  
ssdp\_port\_t tcp 1900  
ssdp\_port\_t udp 1900  
ssh\_port\_t tcp 22  
svn\_port\_t tcp 3690  
svn\_port\_t udp 3690  
svrloc\_port\_t tcp 427

svrloc\_port\_t udp 427

swat\_port\_t tcp 901

syncthing\_admin\_port\_t tcp 8384

syncthing\_discovery\_port\_t udp 21027

syncthing\_port\_t tcp 22000

sype\_transport\_port\_t tcp 9911

sype\_transport\_port\_t udp 9911

syslog\_tls\_port\_t tcp 6514

syslog\_tls\_port\_t udp 6514

syslogd\_port\_t udp 514

tcs\_port\_t tcp 30003

telnetd\_port\_t tcp 23

tftp\_port\_t udp 69

tor\_port\_t tcp 6969, 9001, 9030, 9050, 9051

traceroute\_port\_t udp 64000-64010

transproxy\_port\_t tcp 8081

trisoap\_port\_t tcp 10200

trisoap\_port\_t udp 10200

trivnet1\_port\_t tcp 8200

trivnet1\_port\_t udp 8200

unreserved\_port\_t sctp 1024-65535

unreserved\_port\_t tcp 1024-65535

unreserved\_port\_t udp 1024-65535

ups\_port\_t tcp 3493

uucpd\_port\_t tcp 540

varnishd\_port\_t tcp 6081-6082

virt\_migration\_port\_t tcp 49152-49216

virt\_port\_t tcp 16509, 16514

virt\_port\_t udp 16509, 16514  
virtual\_places\_port\_t tcp 1533  
virtual\_places\_port\_t udp 1533  
vnc\_port\_t tcp 5900  
wccp\_port\_t udp 2048  
websm\_port\_t tcp 9090  
websm\_port\_t udp 9090  
whois\_port\_t tcp 43, 4321  
whois\_port\_t udp 43, 4321  
winshadow\_port\_t tcp 3161  
winshadow\_port\_t udp 3261  
wsdapi\_port\_t tcp 5357  
wsdapi\_port\_t udp 5357  
wsicopy\_port\_t tcp 3378  
wsicopy\_port\_t udp 3378  
xdmcp\_port\_t tcp 177  
xdmcp\_port\_t udp 177  
xen\_port\_t tcp 8002  
xfs\_port\_t tcp 7100  
xserver\_port\_t tcp 6000-6020  
zabbix\_agent\_port\_t tcp 10050  
zabbix\_port\_t tcp 10051  
zarafo\_port\_t tcp 236, 237  
zebra\_port\_t tcp 2606, 2600-2604  
zebra\_port\_t udp 2606, 2600-2604  
zented\_port\_t tcp 1229  
zented\_port\_t udp 1229  
zookeeper\_client\_port\_t tcp 2181



zookeeper\_election\_port\_t tcp 3888

zookeeper\_leader\_port\_t tcp 2888

zope\_port\_t tcp 8021

root@kali:~#