

Concepts in System Security

Understanding SELinux

Karthikeyan G
Roll No: CB.SC.P2CYS24008

March 15, 2025

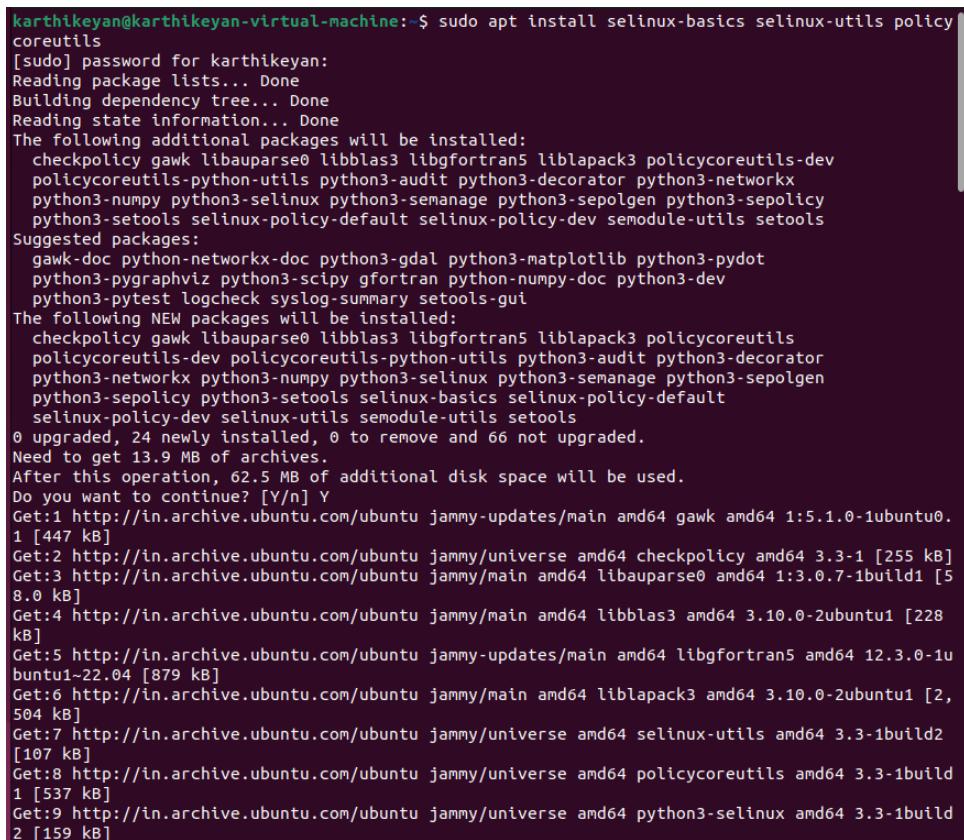
1 SELinux Setup

Security-Enhanced Linux (SELinux) is a security architecture for Linux systems that provides mandatory access control (MAC). It enforces security policies that restrict what actions users, programs, and processes can perform on a system.

To install SELinux, use the following command:

```
sudo apt install selinux-basics selinux-utils policycoreutils
```

This command installs the basic SELinux packages, utilities, and policy tools needed for managing SELinux.



```
kartikeyan@kartikeyan-virtual-machine:~$ sudo apt install selinux-basics selinux-utils policycoreutils
[sudo] password for kartikeyan:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  checkpolicy gawk libbauparse0 libblas3 libgfortran5 liblapack3 policycoreutils-dev
  policycoreutils-python-utils python3-audit python3-decorator python3-networkx
  python3-numpy python3-selinux python3-semanage python3-sepolgen python3-sepolice
  python3-setools selinux-policy-default selinux-policy-dev semodule-utils setools
Suggested packages:
  gawk-doc python-networkx-doc python3-gdal python3-matplotlib python3-pydot
  python3-pygraphviz python3-scipy gfortran python-numpy-doc python3-dev
  python3-pytest logcheck syslog-summary setools-gui
The following NEW packages will be installed:
  checkpolicy gawk libbauparse0 libblas3 libgfortran5 liblapack3 policycoreutils
  policycoreutils-dev policycoreutils-python-utils python3-audit python3-decorator
  python3-networkx python3-numpy python3-selinux python3-semanage python3-sepolgen
  python3-sepolice python3-setools selinux-basics selinux-policy-default
  selinux-policy-dev selinux-utils semodule-utils setools
0 upgraded, 24 newly installed, 0 to remove and 66 not upgraded.
Need to get 13.9 MB of archives.
After this operation, 62.5 MB of additional disk space will be used.
Do you want to continue? [Y/n] Y
Get:1 http://in.archive.ubuntu.com/ubuntu jammy-updates/main amd64 gawk amd64 1:5.1.0-1ubuntu0.1 [447 kB]
Get:2 http://in.archive.ubuntu.com/ubuntu jammy/universe amd64 checkpolicy amd64 3.3-1 [255 kB]
Get:3 http://in.archive.ubuntu.com/ubuntu jammy/main amd64 libbauparse0 amd64 1:3.0.7-1build1 [58.0 kB]
Get:4 http://in.archive.ubuntu.com/ubuntu jammy/main amd64 libblas3 amd64 3.10.0-2ubuntu1 [228 kB]
Get:5 http://in.archive.ubuntu.com/ubuntu jammy-updates/main amd64 libgfortran5 amd64 12.3.0-1ubuntu1-22.04 [879 kB]
Get:6 http://in.archive.ubuntu.com/ubuntu jammy/main amd64 liblapack3 amd64 3.10.0-2ubuntu1 [2,504 kB]
Get:7 http://in.archive.ubuntu.com/ubuntu jammy/universe amd64 selinux-utils amd64 3.3-1build2 [107 kB]
Get:8 http://in.archive.ubuntu.com/ubuntu jammy/universe amd64 policycoreutils amd64 3.3-1build1 [537 kB]
Get:9 http://in.archive.ubuntu.com/ubuntu jammy/universe amd64 python3-selinux amd64 3.3-1build2 [159 kB]
```

Figure 1: Installing SELinux

To activate SELinux, run the following command:

```
sudo selinux-activate
```

This command enables SELinux and prepares the system for enforcing policies.

```
karthikeyan@karthikeyan-virtual-machine:~$ sestatus
SELinux status:          disabled
karthikeyan@karthikeyan-virtual-machine:~$ sudo selinux-activate
Activating SE Linux
Sourcing file '/etc/default/grub'
Sourcing file '/etc/default/grub.d/init-select.cfg'
Generating grub configuration file ...
Found linux image: /boot/vmlinuz-6.8.0-52-generic
Found initrd image: /boot/initrd.img-6.8.0-52-generic
Found linux image: /boot/vmlinuz-6.8.0-40-generic
Found initrd image: /boot/initrd.img-6.8.0-40-generic
Found memtest86+ image: /boot/memtest86+.elf
Found memtest86+ image: /boot/memtest86+.bin
Warning: os-prober will not be executed to detect other bootable partitions.
Systems on them will not be added to the GRUB boot configuration.
Check GRUB_DISABLE_OS_PROBER documentation entry.
done
SE Linux is activated. You may need to reboot now.
karthikeyan@karthikeyan-virtual-machine:~$
```

Figure 2: Activating SELinux

SELinux operates in different modes:

Permissive mode: SELinux loads the security policy but does not enforce it. Instead, it logs policy violations, making it useful for debugging and troubleshooting.

```
karthikeyan@karthikeyan-virtual-machine:~$ 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: 33
karthikeyan@karthikeyan-virtual-machine:~$
```

Figure 3: Permissive Mode in SELinux

Enforcing mode: SELinux actively enforces the security policy, blocking any unauthorized access attempts.

```
karthikeyan@karthikeyan-virtual-machine:~$ sudo selinux-config-enforcing
Configured enforcing mode in /etc/selinux/config for the next boot.
This can be overridden by "enforcing=0" on the kernel command line.
karthikeyan@karthikeyan-virtual-machine:~$
```

Figure 4: Enforcing Mode in SELinux

To list available SELinux object classes, use:

```
ls /sys/fs/selinux/class
```

Object classes define different types of objects that SELinux controls, such as files, directories, and network sockets.

```
karthikeyan@karthikeyan-virtual-machine:~$ ls /sys/fs/selinux/class
alg_socket          irda_socket           process
appleTalk_socket    isdn_socket           process2
association         iucv_socket           qlpcrtr_socket
atmpvc_socket       kcm_socket            rawip_socket
atmsvc_socket       kernel_service       rds_socket
ax25_socket         key                  rose_socket
binder              key_socket            rxrpc_socket
blk_file            llc_socket            sctp_socket
bluetooth_socket   lnk_file              security
bpf                 lockdown              sem
caif_socket         memprotect           service
can_socket          msg                  shm
cap2_userns         msq                 smc_socket
capability          netif                socket
capability2         netlink_audit_socket  sock_file
cap_userns          netlink_connector_socket system
chr_file            netlink_crypto_socket tcp_socket
context             netlink_dartr_socket  tipc_socket
db_blob             netlink_fib_lookup_socket tun_socket
db_column           netlink_generic_socket udp_socket
db_database          netlink_iscsi_socket  unix_dgram_socket
db_datatype          netlink_kobject_uevent_socket unix_stream_socket
db_exception         netlink_nffilter_socket vsock_socket
db_language          netlink_nflog_socket  x25_socket
db_procedure         netlink_rdma_socket  x_application_data
db_schema            netlink_route_socket x_client
db_sequence          netlink_scsitrasport_socket x_colormap
db_table             netlink_selinux_socket x_cursor
db_tuple             netlink_socket        x_device
dbus                netlink_tcpdiag_socket xdp_socket
db_view              netlink_xfrm_socket  x_drawable
dccp_socket          netrom_socket        x_event
decnet_socket        nfc_socket           x_extension
dtr                 node                 x_font
fd                  nsqd                x_gc
fifo_file           obsolete_netlink_firewall_socket x_keyboard
file               obsolete_netlink_ip6fw_socket x_pointer
```

Figure 5: SELinux Object Classes

To show available permissions for the `file` class:

```
ls /sys/fs/selinux/class/file perms
```

This command lists the actions allowed on files, such as read, write, and execute.

```
karthikeyan@karthikeyan-virtual-machine:~$ ls /sys/fs/selinux/class/file/perms
append      execmod      ioctl      mounton     relabelfrom  unlink      watch_sb
audit_access  execute    link      open       relabelto    watch      watch_with_perm
create      execute_no_trans  lock      quotaon   rename      watch_mount  write
entrypoint   getattr     map      read      setattr     watch_reads
```

Figure 6: File Permissions in SELinux

To display permissions for TCP sockets:

```
ls /sys/fs/selinux/class/tcp_socket perms/
```

This command helps administrators manage network security by defining socket access rules.

```
karthikeyan@karthikeyan-virtual-machine:~$ ls /sys/fs/selinux/class/tcp_socket/perms
accept      connect     getopt    lock      name_connect  recvfrom    sendto    shutdown
append      create      ioctl     map      node_bind    relabelfrom  setattr   write
bind       getattr     listen   name bind   read      relabelto   setopt
```

Figure 7: TCP Socket Permissions

To query the set of domains accessible to a role in SELinux:

```
seinfo -ruser_r -x
```

```
karthikeyan@karthikeyan-virtual-machine:~$ seinfo -ruser_r -x
Roles: 1
    role user_r types { telepathy_gabble_t xscreensaver_t thunderbird_t xauth_t httpd_user_script_t telepathy_msn_t updpwd_t wireshark_t policykit_auth_t lpr_t pulseaudio_t evolution_t evolution_alarm_t pppd_t user_mail_t telepathy_stream_engine_t gpg_pinentry_t dirmngr_t traceroute_t gconfd_t sepgsql_trusted_proc_t gpg_agent_t telepathy_idle_t chfn_t shutdown_t user_userhelper_t postfix_postqueue_t exim_t irc_t xscreensaver_helper_t ping_t pam_t telepathy_mission_control_t sysadm_screen_t gpg_helper_t vml_t git_session_t user_t sepgsql_ranged_proc_t user_wm_t vma_re_t user_systemd_t user_crontab_t postfix_postdrop_t vlock_t sysadm_consolehelper_t gpg_t telepathy_salut_t user_dbusd_t xserver_t spamassassin_t chromium_games_t chkpwd_t evolution_webcal_t staff_screen_t telepathy_sofiasip_t mailman_mail_t bluetooth_helper_t cdrecord_t user_screen_t passwd_t loadkeys_t mencoder_t user_ssh_agent_t user_sudo_t telepathy_sunshine_t evolution_exchange_t tvtime_t utempter_t chromium_sandbox_t qmail_inject_t sysadm_userhelper_t staff_userhelper_t ssh_t razor_t iceauth_t mplayer_t spmc_t mozilla_t staff_consolehelper_t auditadm_sreen_t user_gkeyringd_t pyzor_t ddclient_t newrole_t telepathy_logger_t qmail_queue_t secadm_sreen_t user_su_t java_t chromium_naclhelper_t evolution_server_t rssh_t chromium_renderer_t nscd_t user_consolehelper_t mozilla_plugin_t mozilla_plugin_config_t };
karthikeyan@karthikeyan-virtual-machine:~$
```

Figure 8: SELinux User Information

The `seinfo` command provides an overview of SELinux policies, roles, and users.

To get details of a specific SELinux user (e.g., `staff_u`):

```
seinfo -ustaff_u -x
```

This command displays detailed information about the given SELinux user, including assigned roles and policies.

```
karthikeyan@karthikeyan-virtual-machine:~$ seinfo -ustaff_u -x
Users: 1
    user staff_u roles { sysadm_r staff_r } level s0 range s0 - s0:c0.c1023;
karthikeyan@karthikeyan-virtual-machine:~$
```

Figure 9: SELinux User Information

Semanage Utility: The `semanage` command manages SELinux policies. To list all SELinux users, use:

```
sudo semanage user -l
```

This command shows defined SELinux users and their associated roles.

```
karthikeyan@karthikeyan-virtual-machine:~$ sudo semanage user -l
          Labeling      MLS/      MLS/
SELinux User     Prefix      MCS Level     MCS Range           SELinux Roles
root            sysadm      s0        s0-s0:c0.c1023
staff_u         staff       s0        s0-s0:c0.c1023
sysadm_u        sysadm      s0        s0-s0:c0.c1023
system_u        user        s0        s0-s0:c0.c1023
unconfined_u    unconfined  s0        s0-s0:c0.c1023
user_u          user        s0        s0
xdm              user        s0        s0
karthikeyan@karthikeyan-virtual-machine:~$
```

Figure 10: SELinux Users List

When analyzing SELinux contexts, the following example output shows two files with security contexts:

```
unconfined_u:object_r:user_home_t:s0
```

This indicates that both files belong to `unconfined_u`, meaning they are not restricted by strict SELinux policies. This is useful in security audits to detect potential policy violations.

```
karthikeyan@karthikeyan-virtual-machine:~$ ls /home
karthikeyan  linuxbrew
karthikeyan@karthikeyan-virtual-machine:~$ ls -l /home/karthikeyan/K1.txt /home/linuxbrew/K.txt
-rw-r--r--. 1 root root 0 Mar 23 21:36 /home/karthikeyan/K1.txt
-rw-r--r--. 1 root root 0 Mar 23 21:39 /home/linuxbrew/K.txt
karthikeyan@karthikeyan-virtual-machine:~$ ls -ldZ /home/karthikeyan/K1.txt /home/linuxbrew/K.txt
-rw-r--r--. 1 root root unconfined_u:object_r:user_home_t:s0 0 Mar 23 21:36 /home/karthikeyan/K1.txt
-rw-r--r--. 1 root root unconfined_u:object_r:home_root_t:s0 0 Mar 23 21:39 /home/linuxbrew/K.txt
karthikeyan@karthikeyan-virtual-machine:~$ sudo chcon unconfined_u:object_r:user_home_t:s0 /home/linuxbrew/K
.txt
karthikeyan@karthikeyan-virtual-machine:~$ ls -ldZ /home/karthikeyan/K1.txt /home/linuxbrew/K.txt
-rw-r--r--. 1 root root unconfined_u:object_r:user_home_t:s0 0 Mar 23 21:36 /home/karthikeyan/K1.txt
-rw-r--r--. 1 root root unconfined_u:object_r:home_root_t:s0 0 Mar 23 21:39 /home/linuxbrew/K.txt
karthikeyan@karthikeyan-virtual-machine:~$ █
```

Figure 11: SELinux Context Analysis