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.

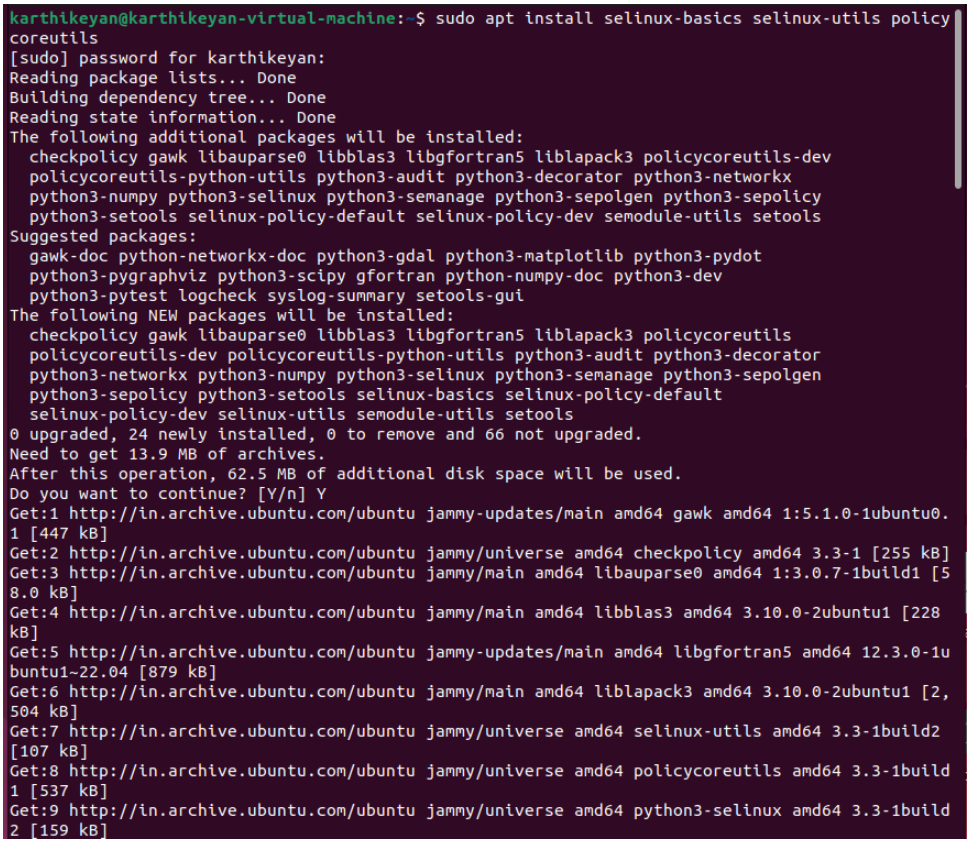

Figure 1: Installing SELinux

To activate SELinux, run the following command:

```
sudo selinux-activate
```

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

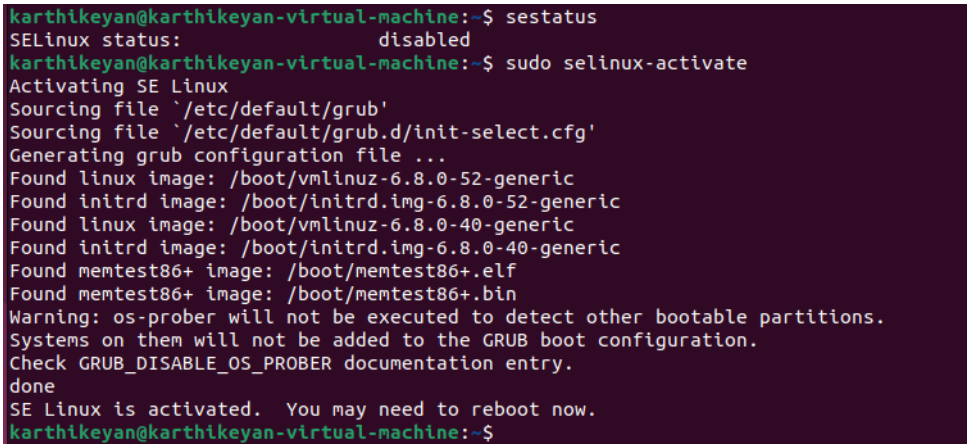

Figure 2: Activating SELinux

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.

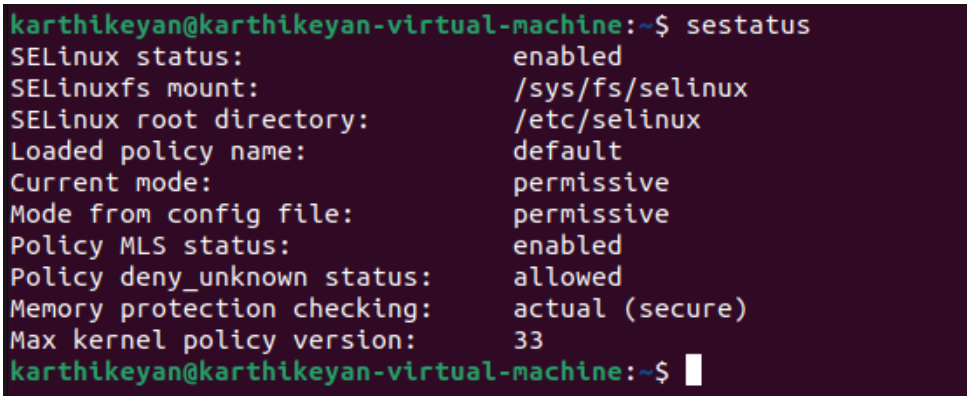

Figure 3: Permissive Mode in SELinux

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

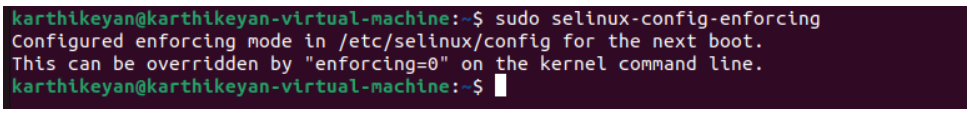

Figure 4: Enforcing Mode in SELinux

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                     qipcrtr_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         msgq                            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_dnrt_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_netfilter_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_scsitransport_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
dir                 node                            x_font
fd                  nscd                            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
karthikeyan@karthikeyan-virtual-machine:~$
```

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
```

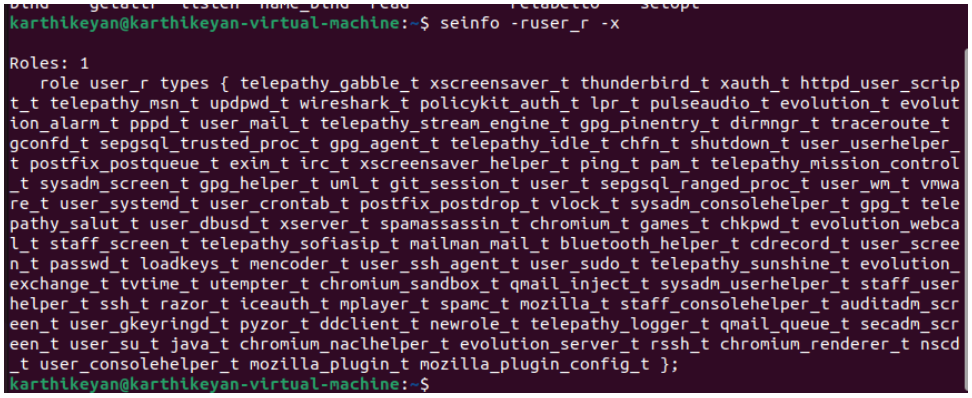

Figure 8: SELinux User Information

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.

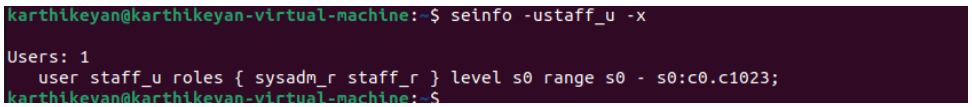

Figure 9: SELinux User Information

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.

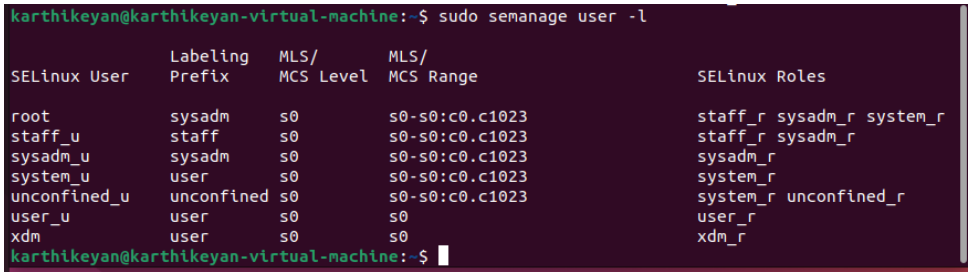

Figure 10: SELinux Users List

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.

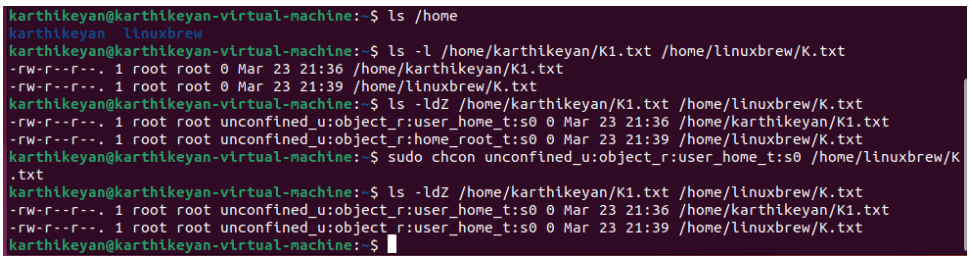

Figure 11: SELinux Context Analysis