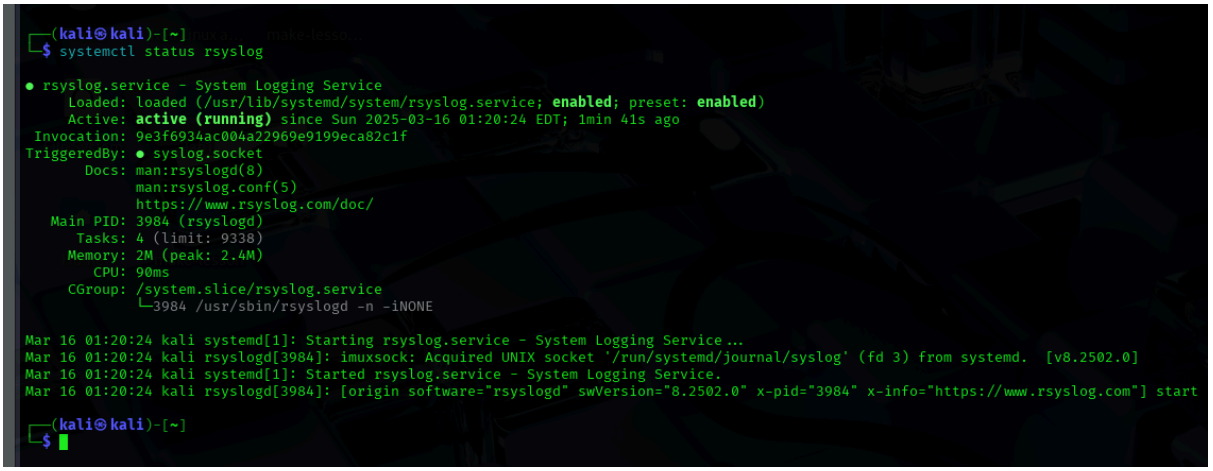
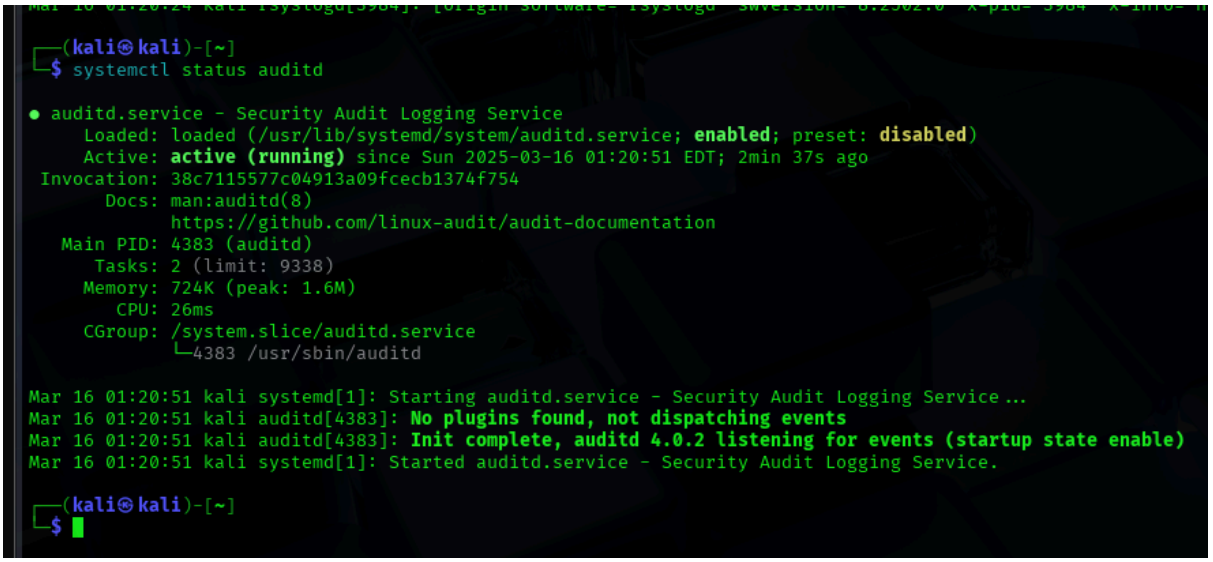
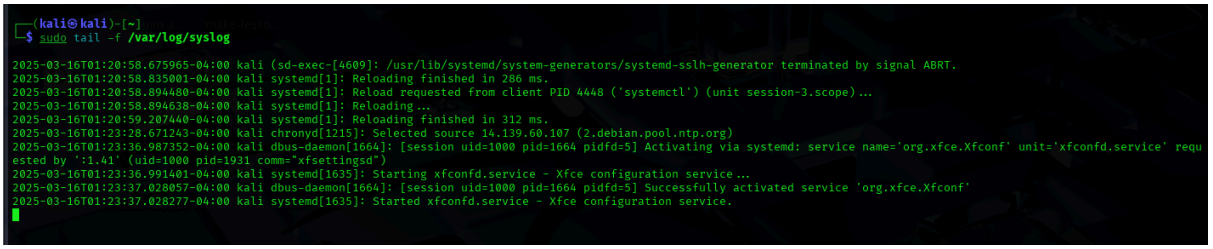
System Security Lab 9 - SE-linux

Praneesh R V
cb.sc.u4cys23036

12.2:







```
┌──(kali㉿kali)-[~]
└─$ sudo tail -f /var/log/audit/audit.log

type=USER_ACCT msg=audit(1742102639.335:26): pid=6223 uid=1000 auid=1000 ses=3 subj=unconfined msg='op=PAM:accounting grantc
ame=? addr=? terminal=/dev/pts/0 res=success'UID="kali" AUID="kali"
type=USER_CMD msg=audit(1742102639.335:27): pid=6223 uid=1000 auid=1000 ses=3 subj=unconfined msg='cwd="/home/kali" cmd=7461
r/bin/sudo" terminal=pts/0 res=success'UID="kali" AUID="kali"
type=CRED_REFR msg=audit(1742102639.335:28): pid=6223 uid=1000 auid=1000 ses=3 subj=unconfined msg='op=PAM:setcred grantors=
=? addr=? terminal=/dev/pts/0 res=success'UID="kali" AUID="kali"
type=USER_START msg=audit(1742102639.335:29): pid=6223 uid=1000 auid=1000 ses=3 subj=unconfined msg='op=PAM:session_open gra
winbind acct="root" exe="/usr/bin/sudo" hostname=? addr=? terminal=/dev/pts/0 res=success'UID="kali" AUID="kali"
type=USER_END msg=audit(1742102653.124:30): pid=6223 uid=1000 auid=1000 ses=3 subj=unconfined msg='op=PAM:session_close gran
inbind acct="root" exe="/usr/bin/sudo" hostname=? addr=? terminal=/dev/pts/0 res=success'UID="kali" AUID="kali"
type=CRED_DISP msg=audit(1742102653.124:31): pid=6223 uid=1000 auid=1000 ses=3 subj=unconfined msg='op=PAM:setcred grantors=
=? addr=? terminal=/dev/pts/0 res=success'UID="kali" AUID="kali"
type=USER_ACCT msg=audit(1742102661.384:32): pid=6405 uid=1000 auid=1000 ses=3 subj=unconfined msg='op=PAM:accounting grantc
ame=? addr=? terminal=/dev/pts/0 res=success'UID="kali" AUID="kali"
type=USER_CMD msg=audit(1742102661.384:33): pid=6405 uid=1000 auid=1000 ses=3 subj=unconfined msg='cwd="/home/kali" cmd=7461
42E6C6F67 exe="/usr/bin/sudo" terminal=pts/0 res=success'UID="kali" AUID="kali"
type=CRED_REFR msg=audit(1742102661.384:34): pid=6405 uid=1000 auid=1000 ses=3 subj=unconfined msg='op=PAM:setcred grantors=
=? addr=? terminal=/dev/pts/0 res=success'UID="kali" AUID="kali"
type=USER_START msg=audit(1742102661.384:35): pid=6405 uid=1000 auid=1000 ses=3 subj=unconfined msg='op=PAM:session_open gra
winbind acct="root" exe="/usr/bin/sudo" hostname=? addr=? terminal=/dev/pts/0 res=success'UID="kali" AUID="kali"
```

```
┌──(kali㉿kali)-[~]
└─$ service auditd status
● auditd.service - Security Audit Logging Service
     Loaded: loaded (/usr/lib/systemd/system/auditd.service; enabled; preset: disabled)
     Active: active (running) since Sun 2025-03-16 01:20:51 EDT; 4min 4s ago
 Invocation: 38c7115577c04913a09fcecb1374f754
       Docs: man:auditd(8)
             https://github.com/linux-audit/audit-documentation
   Main PID: 4383 (auditd)
      Tasks: 2 (limit: 9338)
     Memory: 728K (peak: 1.6M)
        CPU: 26ms
     CGroup: /system.slice/auditd.service
             └─4383 /usr/sbin/auditd

Mar 16 01:20:51 kali systemd[1]: Starting auditd.service - Security Audit Logging Service...
Mar 16 01:20:51 kali auditd[4383]: No plugins found, not dispatching events
Mar 16 01:20:51 kali auditd[4383]: Init complete, auditd 4.0.2 listening for events (startup state enable)
Mar 16 01:20:51 kali systemd[1]: Started auditd.service - Security Audit Logging Service.

┌──(kali㉿kali)-[~]
└─$
```

```
Mar 16 01:20:51 kali systemd[1]: Started auditd.service - Security Audit Logging Service.

┌──(kali㉿kali)-[~]
└─$  service syslog status
● rsyslog.service - System Logging Service
     Loaded: loaded (/usr/lib/systemd/system/rsyslog.service; enabled; preset: enabled)
     Active: active (running) since Sun 2025-03-16 01:20:24 EDT; 5min ago
 Invocation: 9e3f6934ac004a22969e9199eca82c1f
TriggeredBy: ● syslog.socket
       Docs: man:rsyslogd(8)
             man:rsyslog.conf(5)
             https://www.rsyslog.com/doc/
   Main PID: 3984 (rsyslogd)
      Tasks: 4 (limit: 9338)
     Memory: 2M (peak: 2.4M)
        CPU: 92ms
     CGroup: /system.slice/rsyslog.service
             └─3984 /usr/sbin/rsyslogd -n -iNONE

Mar 16 01:20:24 kali systemd[1]: Starting rsyslog.service - System Logging Service...
Mar 16 01:20:24 kali rsyslogd[3984]: imuxsock: Acquired UNIX socket '/run/systemd/journal/syslog' (fd 3) from systemd.  [v8.2502.0]
Mar 16 01:20:24 kali systemd[1]: Started rsyslog.service - System Logging Service.
Mar 16 01:20:24 kali rsyslogd[3984]: [origin software="rsyslogd" swVersion="8.2502.0" x-pid="3984" x-info="https://www.rsyslog.com"] start

┌──(kali㉿kali)-[~]
└─$
```

```
┌──(kali㉿kali)-[~]
└─$ sudo grep -i selinux /var/log/syslog

[sudo] password for kali:
2025-03-16T01:20:24.617759-04:00 kali kernel: evm: security.selinux
2025-03-16T01:32:38.786127-04:00 kali kernel: Command line: BOOT_IMAGE=/boot/vmlinuz-6.12.13-amd64 root=UUID=1c5327a1-a953-414a-9c3a-87388e8d7645 ro security=selinux quiet spl
ash
2025-03-16T01:32:38.786188-04:00 kali systemd[1]: selinux-autorelabel-mark.service - Mark the need to relabel after reboot was skipped because of an unmet condition check (Con
ditionSecurity=!selinux).
2025-03-16T01:32:38.786440-04:00 kali kernel: Kernel command line: BOOT_IMAGE=/boot/vmlinuz-6.12.13-amd64 root=UUID=1c5327a1-a953-414a-9c3a-87388e8d7645 ro security=selinux qu
iet splash
2025-03-16T01:32:38.788694-04:00 kali kernel: LSM: initializing lsm=lockdown,capability,landlock,yama,selinux,bpf,ipe,ima,evm
2025-03-16T01:32:38.788704-04:00 kali kernel: SELinux:  Initializing.
2025-03-16T01:32:38.790996-04:00 kali kernel: evm: security.selinux
2025-03-16T01:32:38.791534-04:00 kali kernel: SELinux:  policy capability network_peer_controls=1
2025-03-16T01:32:38.791534-04:00 kali kernel: SELinux:  policy capability open_perms=1
2025-03-16T01:32:38.791535-04:00 kali kernel: SELinux:  policy capability extended_socket_class=1
2025-03-16T01:32:38.791543-04:00 kali kernel: SELinux:  policy capability always_check_network=0
2025-03-16T01:32:38.791544-04:00 kali kernel: SELinux:  policy capability cgroup_seclabel=1
2025-03-16T01:32:38.791544-04:00 kali kernel: SELinux:  policy capability nnp_nosuid_transition=1
2025-03-16T01:32:38.791545-04:00 kali kernel: SELinux:  policy capability genfs_seclabel_symlinks=0
2025-03-16T01:32:38.791545-04:00 kali kernel: SELinux:  policy capability ioctl_skip_cloexec=0
2025-03-16T01:32:38.791546-04:00 kali kernel: SELinux:  policy capability userspace_initial_context=0
2025-03-16T01:32:38.791555-04:00 kali kernel: audit: type=1403 audit(1742103155.903:2): auid=4294967295 ses=4294967295 lsm=selinux res=1
2025-03-16T01:32:38.801210-04:00 kali dbus-daemon[811]: [system] SELinux support is enabled
2025-03-16T01:32:41.109484-04:00 kali containerd[1215]: time="2025-03-16T01:32:41.107357712-04:00" level=info msg="Start cri plugin with config {PluginConfig:{ContainerdConfig
:{Snapshotter:overlayfs DefaultRuntimeName:runc DefaultRuntime:{Type: Path: Engine: PodAnnotations:[] ContainerAnnotations:[] Root: Options:map[] PrivilegedWithoutHostDevices:
false PrivilegedWithoutHostDevicesAllDevicesAllowed:false BaseRuntimeSpec: NetworkPluginConfDir: NetworkPluginMaxConfNum:0 Snapshotter: SandboxMode:} UntrustedWorkloadRuntime:
{Type: Path: Engine: PodAnnotations:[] ContainerAnnotations:[] Root: Options:map[] PrivilegedWithoutHostDevices:false PrivilegedWithoutHostDevicesAllDevicesAllowed:false BaseR
untimeSpec: NetworkPluginConfDir: NetworkPluginMaxConfNum:0 Snapshotter: SandboxMode:} Runtimes:map[runc:{Type:io.containerd.runc.v2 Path: Engine: PodAnnotations:[] ContainerA
nnotations:[] Root: Options:map[BinaryName: CriuImagePath: CriuPath: CriuWorkPath: IoGid:0 IoUid:0 NoNewKeyring:false NoPivotRoot:false Root: ShimCgroup: SystemdCgroup:false]
PrivilegedWithoutHostDevices:false PrivilegedWithoutHostDevicesAllDevicesAllowed:false BaseRuntimeSpec: NetworkPluginConfDir: NetworkPluginMaxConfNum:0 Snapshotter: SandboxMod
e:podsandbox} NoPivot:false DisableSnapshotAnnotations:true DiscardUnpackedLayers:false IgnoreBlockIONotEnabledErrors:false IgnoreRdtNotEnabledErrors:false} CniConfig:{Networ
kPluginBinDir:/usr/lib/cni NetworkPluginConfDir:/etc/cni/net.d NetworkPluginMaxConfNum:1 NetworkPluginSetupSerially:false NetworkPluginConfTemplate: IPPreference:} Registry:{C
onfigPath: Mirrors:map[] Configs:map[] Auths:map[] Headers:map[]} ImageDecryption:{KeyModel:node} DisableTCPService:true StreamServerAddress:127.0.0.1 StreamServerPort:0 Strea
mIdleTimeout:4h0m0s EnableSelinux:false SelinuxCategoryRange:1024 SandboxImage:registry.k8s.io/pause:3.8 StatsCollectPeriod:10 SystemdCgroup:false EnableTLSStreaming:false X50
9KeyPairStreaming:{TLSCertFile: TLSKeyFile:} MaxContainerLogLineSize:16384 DisableCgroup:false DisableApparmor:false RestrictOOMScoreAdj:false MaxConcurrentDownloads:3 Disable
ProcMount:false UnsetSeccompProfile: TolerateMissingHugetlbController:true DisableHugetlbController:true DeviceOwnershipFromSecurityContext:false IgnoreImageDefinedVolumes:fal
se NetNSMountsUnderStateDir:false EnableUnprivilegedPorts:false EnableUnprivilegedICMP:false EnableCDI:false CDISpecDirs:[/etc/cdi /var/run/cdi] ImagePullProgressTimeout:5m0s
DrainExecSyncIOTimeout:0s ImagePullWithSyncFs:false IgnoreDeprecationWarnings:[]} ContainerdRootDir:/var/lib/containerd ContainerdEndpoint:/run/containerd/containerd.sock Root
Dir:/var/lib/containerd/io.containerd.grpc.v1.cri StateDir:/run/containerd/io.containerd.grpc.v1.cri}"
2025-03-16T01:32:43.035695-04:00 kali dbus-daemon[1431]: [session uid=125 pid=1431 pidfd=5] SELinux support is enabled
2025-03-16T01:34:09.683302-04:00 kali dbus-daemon[1650]: [session uid=1000 pid=1650 pidfd=5] SELinux support is enabled

┌──(kali㉿kali)-[~]
└─$
```

```
┌──(kali㉿kali)-[~]
└─$ sudo grep -i selinux /var/log/audit/audit.log

type=USER_CMD msg=audit(1742103004.907:208): pid=10794 uid=1000 auid=1000 ses=3 subj=unconfined msg='cwd="/home/kali" cmd="selinux-activate" exe="/usr/bin/sudo" terminal=pts/0
 res=success'UID="kali" AUID="kali"
type=USER_ROLE_CHANGE msg=audit(1742103162.419:122): pid=1343 uid=0 auid=4294967295 ses=4294967295 subj=system_u:system_r:init_t:s0 msg='op=pam_selinux default-context=unconfi
ned_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 selected-context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 exe="/usr/lib/systemd/systemd-executor" hostname=? addr=?
 terminal=? res=success'UID="root" AUID="unset"
type=USER_START msg=audit(1742103162.431:125): pid=1343 uid=0 auid=125 ses=2 subj=system_u:system_r:init_t:s0 msg='op=PAM:session_open grantors=pam_selinux,pam_selinux,pam_log
inuid,pam_limits,pam_permit,pam_umask,pam_unix,pam_winbind,pam_keyinit,pam_systemd acct="lightdm" exe="/usr/lib/systemd/systemd-executor" hostname=? addr=? terminal=? res=succ
ess'UID="root" AUID="lightdm"
type=USER_ROLE_CHANGE msg=audit(1742103249.315:191): pid=1621 uid=0 auid=4294967295 ses=4294967295 subj=system_u:system_r:init_t:s0 msg='op=pam_selinux default-context=unconfi
ned_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 selected-context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 exe="/usr/lib/systemd/systemd-executor" hostname=? addr=?
 terminal=? res=success'UID="root" AUID="unset"
type=USER_START msg=audit(1742103249.323:193): pid=1621 uid=0 auid=1000 ses=4 subj=system_u:system_r:init_t:s0 msg='op=PAM:session_open grantors=pam_selinux,pam_selinux,pam_lo
ginuid,pam_limits,pam_permit,pam_umask,pam_unix,pam_winbind,pam_keyinit,pam_systemd acct="kali" exe="/usr/lib/systemd/systemd-executor" hostname=? addr=? terminal=? res=succes
s'UID="root" AUID="kali"
type=USER_ROLE_CHANGE msg=audit(1742103249.635:195): pid=1610 uid=0 auid=1000 ses=3 subj=system_u:system_r:xdm_t:s0 msg='op=pam_selinux default-context=unconfined_u:unconfined
_r:unconfined_t:s0-s0:c0.c1023 selected-context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 exe="/usr/sbin/lightdm" hostname=? addr=? terminal=:0 res=success'UID="ro
ot" AUID="kali"
type=USER_START msg=audit(1742103249.719:196): pid=1610 uid=0 auid=1000 ses=3 subj=system_u:system_r:xdm_t:s0 msg='op=PAM:session_open grantors=pam_env,pam_env,pam_selinux,pam
_limits,pam_loginuid,pam_permit,pam_umask,pam_unix,pam_winbind,pam_systemd,pam_selinux,pam_gnome_keyring acct="kali" exe="/usr/sbin/lightdm" hostname=? addr=? terminal=:0 res=
success'UID="root" AUID="kali"
```

12.3.

```
┌──(kali㉿kali)-[~]
└─$ sudo selinux-activate

[sudo] password for kali:
Activating SE Linux
Generating grub configuration file ...
Found theme: /boot/grub/themes/kali/theme.txt
Found background image: /usr/share/images/desktop-base/desktop-grub.png
Found linux image: /boot/vmlinuz-6.12.13-amd64
Found initrd image: /boot/initrd.img-6.12.13-amd64
Found linux image: /boot/vmlinuz-6.10.9-amd64
Found initrd image: /boot/initrd.img-6.10.9-amd64
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.
Adding boot menu entry for UEFI Firmware Settings ...
done
SE Linux is activated.  You may need to reboot now.

┌──(kali㉿kali)-[~]
└─$
```

```
┌──(kali㉿kali)-[~]
└─$ getenforce
Permissive

┌──(kali㉿kali)-[~]
└─$
```

```
┌──(kali㉿kali)-[~]
└─$ cat /selinux/enforce
```

```
┌──(kali㉿kali)-[~]
└─$ sudo  setenforce Enforcing

┌──(kali㉿kali)-[~]
└─$ getenforce
Enforcing

┌──(kali㉿kali)-[~]
└─$ sudo  setenforce Permissive

┌──(kali㉿kali)-[~]
└─$ getenforce
Permissive

┌──(kali㉿kali)-[~]
└─$
```

12.6.

```
┌──(kali㉿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:          enforcing
Policy MLS status:              enabled
Policy deny_unknown status:     allowed
Memory protection checking:     actual (secure)
Max kernel policy version:      33

┌──(kali㉿kali)-[~]
└─$
```

```
┌──(kali㉿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=enforcing
# 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

┌──(kali㉿kali)-[~]
└─$
```

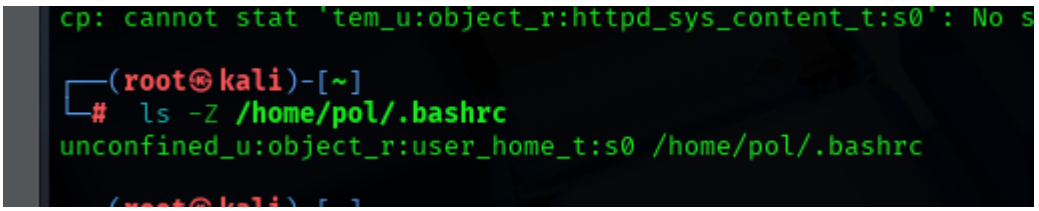
12.10.

```
┌──(root㉿kali)-[~]
└─# ls -Z
system_u:object_r:user_home_t:s0 attr        system_u:object_r:user_home_t:s0 permissions  system_u:object_r:user_home_t:s0 sshd.bak
system_u:object_r:user_home_t:s0 ip_forward  system_u:object_r:user_home_t:s0 rightnet.sh
system_u:object_r:user_home_t:s0 leftnet.sh  system_u:object_r:user_home_t:s0 router.sh

┌──(root㉿kali)-[~]
└─#
```

```
┌──(root㉿kali)-[~]
└─# useradd -m -s /bin/bash pol

┌──(root㉿kali)-[~]
└─#
```


cp: cannot stat 'tem_u:object_r:httpd_sys_content_t:s0': No s
(root kali)-[~]
ls -Z /home/pol/.bashrc
unconfined_u:object_r:user_home_t:s0 /home/pol/.bashrc

12.12.

```
┌──(root㉿kali)-[~]
└─# ls -ls -l /sys/fs/selinux/

total 0
-rw-rw-rw-.   1 root root    0 Mar 16 01:46 access
dr-xr-xr-x.   2 root root    0 Mar 16 01:46 avc
dr-xr-xr-x.   2 root root    0 Mar 16 01:46 booleans
-rw-r--r--.   1 root root    0 Mar 16 01:46 checkreqprot
dr-xr-xr-x. 137 root root    0 Mar 16 01:46 class
--w-------.   1 root root    0 Mar 16 01:46 commit_pending_bools
-rw-rw-rw-.   1 root root    0 Mar 16 01:46 context
-rw-rw-rw-.   1 root root    0 Mar 16 01:46 create
-r--r--r--.   1 root root    0 Mar 16 01:46 deny_unknown
--w-------.   1 root root    0 Mar 16 01:46 disable
-rw-r--r--.   1 root root    0 Mar 16 01:46 enforce
dr-xr-xr-x.   2 root root    0 Mar 16 01:46 initial_contexts
-rw-------.   1 root root    0 Mar 16 01:46 load
-rw-rw-rw-.   1 root root    0 Mar 16 01:46 member
-r--r--r--.   1 root root    0 Mar 16 01:46 mls
crw-rw-rw-.   1 root root 1, 3 Mar 16 01:46 null
-r--r--r--.   1 root root    0 Mar 16 01:46 policy
dr-xr-xr-x.   2 root root    0 Mar 16 01:46 policy_capabilities
-r--r--r--.   1 root root    0 Mar 16 01:46 policyvers
-r--r--r--.   1 root root    0 Mar 16 01:46 reject_unknown
-rw-rw-rw-.   1 root root    0 Mar 16 01:46 relabel
dr-xr-xr-x.   2 root root    0 Mar 16 01:46 ss
-r--r--r--.   1 root root    0 Mar 16 01:46 status
-rw-rw-rw-.   1 root root    0 Mar 16 01:46 user
--w--w--w-.   1 root root    0 Mar 16 01:46 validatetrans

┌──(root㉿kali)-[~]
└─#
```

12.13.

```
┌──(root㉿kali)-[~]
└─# id -id -Z

unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023

┌──(root㉿kali)-[~]
└─#
```

12.15.

```
┌──(root㉿kali)-[~]
└─# ps fax -Z | grep /sbin/init
system_u:system_r:init_t:s0          1 ?        Ss     0:02 /sbin/init splash
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 15201 pts/1 S+   0:00                  \_ grep --color=auto /sbin/init

┌──(root㉿kali)-[~]
└─#
```

```
┌──(root㉿kali)-[~]
└─# whicwhichradd usermod userdel httpd postcat postfix

/usr/sbin/useradd
/usr/sbin/usermod
/usr/sbin/userdel
httpd not found
postcat not found
postfix not found

┌──(root㉿kali)-[~]
└─#
```

```
┌──(root㉿kali)-[~]
└─#  net netstat -nptlZ | tr -s ' ' | cut -d' ' -f6-


Foreign Address State PID/Program name Security Context
LISTEN 1244/sshd: /usr/sbi system_u:system_r:sshd_t:s0
LISTEN 1228/containerd system_u:system_r:dockerd_t:s0
LISTEN 2066/kdeconnectd fined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
LISTEN 1244/sshd: /usr/sbi system_u:system_r:sshd_t:s0

┌──(root㉿kali)-[~]
└─#
```

```
┌──(root㉿kali)-[~]
└─# semasemanaget -l |-l | tail

zabbix_port_t                  tcp      10051
zarafa_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)-[~]
└─#
```

12.16.

```
┌──(root㉿kali)-[~]
└─# id  id | cut -d' ' -f4

context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023

┌──(root㉿kali)-[~]
└─#
```

```
┌──(root㉿kali)-[/home]
└─# ls -Z test1
system_u:object_r:user_home_t:s0 welcome.txt

┌──(root㉿kali)-[/home]
└─#
```

```
┌──(root㉿kali)-[/home]
└─# ps -ZC init
LABEL                          PID TTY          TIME CMD

┌──(root㉿kali)-[/home]
└─# sS
```

```
┌──(root㉿kali)-[~]
└─# ls -Zd /proc/1/
system_u:system_r:init_t:s0 /proc/1/

┌──(root㉿kali)-[~]
└─#
```

12.17

```
┌──(root㉿kali)-[~]
└─# touch test /tmp/test

┌──(root㉿kali)-[~]
└─# ls -Z test
unconfined_u:object_r:user_home_t:s0 test

┌──(root㉿kali)-[~]
└─# ls -Z /tmp/test
unconfined_u:object_r:user_tmp_t:s0 /tmp/test

┌──(root㉿kali)-[~]
└─#
```

12.18.

```
┌──(root㉿kali)-[~]
└─# ls --context
system_u:object_r:user_home_t:s0 attr            system_u:object_r:user_home_t:s0 router.sh
system_u:object_r:user_home_t:s0 ip_forward      system_u:object_r:user_home_t:s0 sshd.bak
system_u:object_r:user_home_t:s0 leftnet.sh   unconfined_u:object_r:user_home_t:s0 system_u:object_r:httpd_sys_content_t:s0
system_u:object_r:user_home_t:s0 permissions  unconfined_u:object_r:user_home_t:s0 test
system_u:object_r:user_home_t:s0 rightnet.sh

┌──(root㉿kali)-[~]
└─#
```

```
┌──(root㉿kali)-[~]
└─# ls -Z
system_u:object_r:user_home_t:s0 attr            system_u:object_r:user_home_t:s0 router.sh
system_u:object_r:user_home_t:s0 ip_forward      system_u:object_r:user_home_t:s0 sshd.bak
system_u:object_r:user_home_t:s0 leftnet.sh   unconfined_u:object_r:user_home_t:s0 system_u:object_r:httpd_sys_content_t:s0
system_u:object_r:user_home_t:s0 permissions  unconfined_u:object_r:user_home_t:s0 test
system_u:object_r:user_home_t:s0 rightnet.sh

┌──(root㉿kali)-[~]
└─#
```

12.19.

```
┌──(root㉿kali)-[~]
└─# ps -ZC mingetty
LABEL                                PID TTY          TIME CMD

┌──(root㉿kali)-[~]
└─#
```

12.20

```
┌──(root㉿kali)-[~]
└─# ls -Z test
unconfined_u:object_r:user_home_t:s0 test

┌──(root㉿kali)-[~]
└─# chcon -t samba_share_t test

┌──(root㉿kali)-[~]
└─# ls -Z test
unconfined_u:object_r:samba_share_t:s0 test

┌──(root㉿kali)-[~]
└─#
```

12.21.

```
┌──(root㉿kali)-[~]
└─#  touch /var/www/html/test42.txt

┌──(root㉿kali)-[~]
└─# ls -Z /var/www/html/test42.txt
unconfined_u:object_r:httpd_sys_content_t:s0 /var/www/html/test42.txt

┌──(root㉿kali)-[~]
└─# touch /root/test42.txt

┌──(root㉿kali)-[~]
└─# ls -Z /root/test42.txt
unconfined_u:object_r:user_home_t:s0 /root/test42.txt
```

```
┌──(root㉿kali)-[/root]
└─#  wget http://localhost/test42.txt
--2025-03-16 02:36:58--  http://localhost/test42.txt
Resolving localhost (localhost)...  ::1, 127.0.0.1
Connecting to localhost (localhost)|::1|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 0 [text/plain]
Saving to: 'test42.txt.1'

test42.txt.1                                [ <=>

2025-03-16 02:36:58 (0.00 B/s) - 'test42.txt.1' saved [0/0]


┌──(root㉿kali)-[/root]
└─#
```

```
┌──(root㉿kali)-[/root]
└─#  ps -ZC httpd | head -4
LABEL                           PID TTY          TIME CMD

┌──(root㉿kali)-[/root]
└─#
```

```
┌──(root㉿kali)-[/root]
└─#  chcon -t samba_share_t /var/www/html/test42.txt

┌──(root㉿kali)-[/root]
└─# ls -Z /var/www/html/test42.txt
unconfined_u:object_r:samba_share_t:s0 /var/www/html/test42.txt

┌──(root㉿kali)-[/root]
└─# setenforce 1

┌──(root㉿kali)-[/root]
└─# getenforce
Enforcing

┌──(root㉿kali)-[/root]
└─#
```

```
┌──(root㉿kali)-[/root]
└─#  wget http://localhost/test42.txt
--2025-03-16 02:38:42--  http://localhost/test42.txt
Resolving localhost (localhost)... ::1, 127.0.0.1
Connecting to localhost (localhost)|::1|:80... connected.
HTTP request sent, awaiting response... 403 Forbidden
2025-03-16 02:38:42 ERROR 403: Forbidden.


┌──(root㉿kali)-[/root]
└─# tail -3 /var/log/audit/audit.log
type=AVC msg=audit(1742107131.044:1019): avc:  denied  { execmem } for  pid=30381 comm="grep" scontext=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 tcontext=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 tclass=process permissive=0
type=SYSCALL msg=audit(1742107131.044:1019): arch=c000003e syscall=9 success=no exit=-13 a0=0 a1=10000 a2=7 a3=22 items=0 ppid=30379 pid=30381 auid=1000 uid=1000 gid=1000 euid=1000 suid=1000 fsuid=1000 egid=1000 sgid=1000 fsgid=1000 tty=(none) ses=3 comm="grep" exe="/usr/bin/grep" subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 key=(null)ARCH=x86_64 SYSCALL=mmap AUID="kali" UID="kali" GID="kali" EUID="kali" SUID="kali" FSUID="kali" EGID="kali" SGID="kali" FSGID="kali"
type=PROCTITLE msg=audit(1742107131.044:1019): proctitle=6772657000 2D6F002D5000283F3C3D696E657420295B302D395D7B312C337D285C2E5B302D395D7B312C337D297B337D

┌──(root㉿kali)-[/root]
└─#
```

12.23:

```
┌──(root㉿kali)-[/]
└─# getsebool -a | head
aide_mmap_files ⟶ off
allow_cvs_read_shadow ⟶ off
allow_execheap ⟶ off
allow_execmem ⟶ off
allow_execmod ⟶ off
allow_execstack ⟶ off
allow_ftpd_anon_write ⟶ off
allow_ftpd_full_access ⟶ off
allow_ftpd_use_cifs ⟶ off
allow_ftpd_use_nfs ⟶ off

┌──(root㉿kali)-[/]
└─#
```

```
┌──(root㉿kali)-[/]
└─# setssetseboolpd_read_user_content=1


┌──(root㉿kali)-[/]
└─# getsebool httpd_read_user_content
httpd_read_user_content ⟶ on

┌──(root㉿kali)-[/]
└─# http setsebool httpd_enable_homedirs=1

┌──(root㉿kali)-[/]
└─# getsebool httpd_enable_homedirs
httpd_enable_homedirs ⟶ on
```

```
┌──(root㉿kali)-[/]
└─#  setsebool -P httpd_enable_homedirs=1
^C

┌──(root㉿kali)-[/]
└─#  setsebool -P httpd_read_user_content=1
^C
```