SUBMITTED BY :

Shams Ali

ROLL NO :

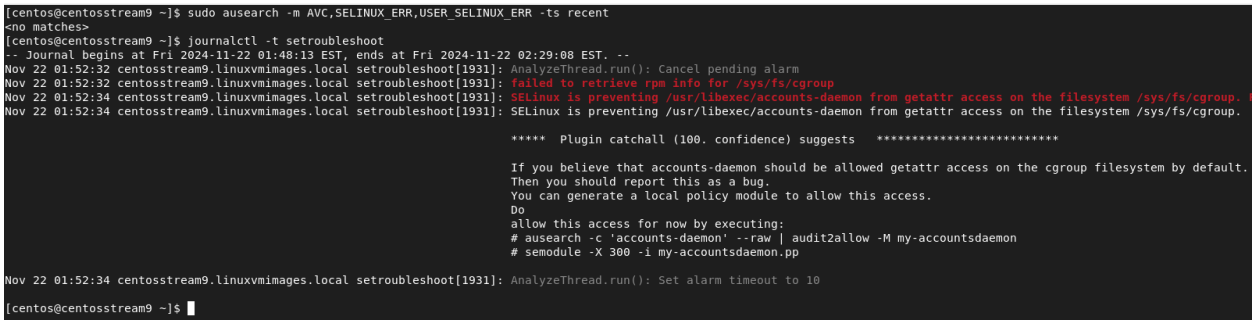
BSIT51F22S016

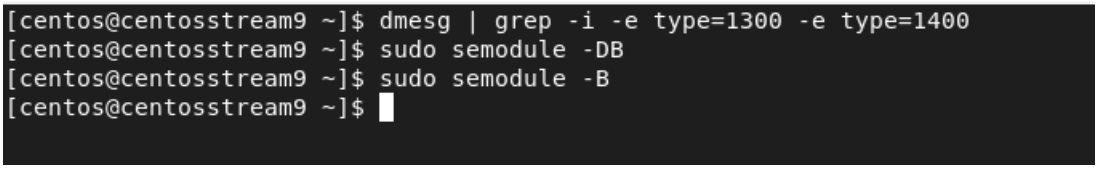
SUBMITTED TO :

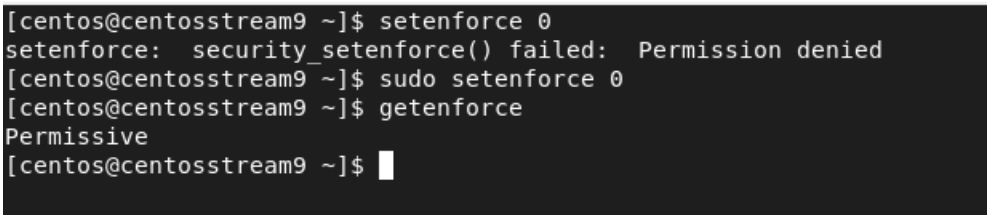
MS. Misbah Jabeen

SE Linux Troubleshooting

1.IDENTIFYING SELINUX DENIALS







2. ANALYZING SELINUX DENIAL MESSAGES

```
[centos@centosstream9 ~]$ sudo yum install policycoreutils-python-utils
Last metadata expiration check: 0:36:46 ago on Fri 22 Nov 2024 02:01:16 AM EST.
Package policycoreutils-python-utils-3.3-2.el9.noarch is already installed.
Dependencies resolved.
================================================================================================================
 Package                          Architecture        Version              Repository                  Size
================================================================================================================
Upgrading:
 libsemanage                      x86_64              3.6-3.el9            baseos                     118 k
 policycoreutils                  x86_64              3.6-2.1.el9          baseos                     242 k
 policycoreutils-python-utils     noarch              3.6-2.1.el9          appstream                   77 k
 python3-libsemanage              x86_64              3.6-3.el9            appstream                   79 k
 python3-policycoreutils          noarch              3.6-2.1.el9          appstream                  2.1 M
Installing dependencies:
 python3-distro                   noarch              1.5.0-7.el9          appstream                   37 k

Transaction Summary
================================================================================================================
Install  1 Package
Upgrade  5 Packages

Total download size: 2.7 M
Is this ok [y/N]: y
Downloading Packages:
(1/6): python3-distro-1.5.0-7.el9.noarch.rpm                                 62 kB/s |  37 kB     00:00
(2/6): policycoreutils-python-utils-3.6-2.1.el9.noarch.rpm                  186 kB/s |  77 kB     00:00
(3/6): python3-libsemanage-3.6-3.el9.x86_64.rpm                             178 kB/s |  79 kB     00:00
(4/6): libsemanage-3.6-3.el9.x86_64.rpm                                      50 kB/s | 118 kB     00:02
(5/6): policycoreutils-3.6-2.1.el9.x86_64.rpm                                83 kB/s | 242 kB     00:02
(6/6): python3-policycoreutils-3.6-2.1.el9.noarch.rpm                       917 kB/s | 2.1 MB     00:02
----------------------------------------------------------------------------------------------------------------
Total                                                                       398 kB/s | 2.7 MB     00:06
Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
```

```
[centos@centosstream9 ~]$ sudo yum install setroubleshoot-server
Last metadata expiration check: 0:38:46 ago on Fri 22 Nov 2024 02:01:16 AM EST.
Package setroubleshoot-server-3.3.26-5.el9.x86_64 is already installed.
Dependencies resolved.
================================================================================
 Package                                                 Architecture
================================================================================
Upgrading:
 setroubleshoot-server                                   x86_64

Transaction Summary
================================================================================
Upgrade  1 Package

Total download size: 324 k
Is this ok [y/N]: y
Downloading Packages:
setroubleshoot-server-3.3.32-1.el9.x86_64.rpm
--------------------------------------------------------------------------------
Total
Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction
  Preparing        :
  Running scriptlet: setroubleshoot-server-3.3.32-1.el9.x86_64
  Upgrading        : setroubleshoot-server-3.3.32-1.el9.x86_64
  Running scriptlet: setroubleshoot-server-3.3.32-1.el9.x86_64
  Cleanup          : setroubleshoot-server-3.3.26-5.el9.x86_64
  Running scriptlet: setroubleshoot-server-3.3.26-5.el9.x86_64
  Verifying        : setroubleshoot-server-3.3.32-1.el9.x86_64
  Verifying        : setroubleshoot-server-3.3.26-5.el9.x86_64
```

```
[root@centosstream9 centos]# sudo auditctl -w /etc/shadow -p w -k shadow-write
[root@centosstream9 centos]# rm -f /var/lib/setroubleshoot/setroubleshoot.xml
[root@centosstream9 centos]# sudo auditctl -W /etc/shadow -p w -k shadow-write
[root@centosstream9 centos]#
```

3. FIXING ANALYZED SELINUX DENIALS

```
[root@centosstream9 centos]# semanage fcontext -a -t httpd_sys_content_t "/srv/myweb(/.*)?"
File context for /srv/myweb(/.*)? already defined, modifying instead
[root@centosstream9 centos]# mkdir srv
[root@centosstream9 centos]# cd srv
[root@centosstream9 srv]# mkdir myweb
[root@centosstream9 srv]# cd ..
[root@centosstream9 centos]# restorecon -v srv/myweb/
[root@centosstream9 centos]# restorecon -R -v /srv/myweb
restorecon: lstat(/srv/myweb) failed: No such file or directory
[root@centosstream9 centos]# restorecon -R -v srv/myweb
[root@centosstream9 centos]#
```

```
[root@centosstream9 centos]# matchpathcon -V srv/myweb/
srv/myweb verified.
[root@centosstream9 centos]#
```

```
[root@centosstream9 centos]# setsebool -P httpd_can_network_connect_db on
[root@centosstream9 centos]# getsebool -a | grep ftp
ftpd_anon_write --> off
ftpd_connect_all_unreserved --> off
ftpd_connect_db --> off
ftpd_full_access --> off
ftpd_use_cifs --> off
ftpd_use_fusefs --> off
ftpd_use_nfs --> off
ftpd_use_passive_mode --> off
httpd_can_connect_ftp --> off
httpd_enable_ftp_server --> off
tftp_anon_write --> off
tftp_home_dir --> off
[root@centosstream9 centos]# semanage boolean -l
SELinux boolean                 State  Default Description

abrt_anon_write                 (off  ,  off)  Allow abrt to anon write
abrt_handle_event               (off  ,  off)  Allow abrt to handle event
abrt_upload_watch_anon_write    (on   ,   on)  Allow abrt to upload watch anon write
antivirus_can_scan_system       (off  ,  off)  Allow antivirus to can scan system
antivirus_use_jit               (off  ,  off)  Allow antivirus to use jit
auditadm_exec_content           (on   ,   on)  Allow auditadm to exec content
authlogin_nsswitch_use_ldap     (off  ,  off)  Allow authlogin to nsswitch use ldap
authlogin_radius                (off  ,  off)  Allow authlogin to radius
authlogin_yubikey               (off  ,  off)  Allow authlogin to yubikey
awstats_purge_apache_log_files  (off  ,  off)  Allow awstats to purge apache log files
boinc_execmem                   (on   ,   on)  Allow boinc to execmem
cdrecord_read_content           (off  ,  off)  Allow cdrecord to read content
cluster_can_network_connect     (off  ,  off)  Allow cluster to can network connect
cluster_manage_all_files        (off  ,  off)  Allow cluster to manage all files
cluster_use_execmem             (off  ,  off)  Allow cluster to use execmem
```

```
bash: audit2allow: command not found...
[root@centosstream9 centos]# audit2allow -w -a
type=AVC msg=audit(1732258351.216:108): avc:  denied  { getattr } for  pid=733 comm="accounts-daemon" name="/" dev="cgroup2" ino=1 scontext=system_u:system_r:accountsd_t:s0 tcontext=system_u:object_r:cgroup_t:s0
 tclass=filesystem permissive=0
        Was caused by:
                Missing type enforcement (TE) allow rule.

                You can use audit2allow to generate a loadable module to allow this access.

type=AVC msg=audit(1732260825.803:236): avc:  denied  { read write } for  pid=3793 comm="unix_chkpwd" path="/dev/pts/0" dev="devpts" ino=3 scontext=unconfined_u:unconfined_r:chkpwd_t:s0-s0:c0.c1023 tcontext=unco
nfined_u:object_r:user_devpts_t:s0 tclass=chr_file permissive=0
        Was caused by:
                Unknown - should be dontaudit'd by active policy
                Possible mismatch between this policy and the one under which the audit message was generated.

                Possible mismatch between current in-memory boolean settings vs. permanent ones.

type=AVC msg=audit(1732260828.876:243): avc:  denied  { siginh } for  pid=3805 comm="SetroubleshootP" scontext=system_u:system_r:init_t:s0 tcontext=system_u:system_r:unconfined_service_t:s0 tclass=process permis
sive=0
        Was caused by:
                Unknown - should be dontaudit'd by active policy
                Possible mismatch between this policy and the one under which the audit message was generated.

                Possible mismatch between current in-memory boolean settings vs. permanent ones.

[root@centosstream9 centos]#
```

4. CREATING A LOCAL SELINUX POLICY MODULE

```
[root@centosstream9 centos]# yum install setools-console
Last metadata expiration check: 5:29:15 ago on Fri 22 Nov 2024 02:01:16 AM EST.
Package setools-console-4.4.4-1.el9.x86_64 is already installed.
Dependencies resolved.
Nothing to do.
Complete!
[root@centosstream9 centos]# yum install audit
Last metadata expiration check: 5:29:21 ago on Fri 22 Nov 2024 02:01:16 AM EST.
Package audit-3.0.5-5.el9.x86_64 is already installed.
Dependencies resolved.
================================================================================================================================================
 Package                                          Architecture                                  Version
================================================================================================================================================
Upgrading:
 audit                                            x86_64                                        3.1.5-1.el9
 audit-libs                                       x86_64                                        3.1.5-1.el9
 python3-audit                                    x86_64                                        3.1.5-1.el9

Transaction Summary
================================================================================================================================================
Upgrade  3 Packages

Total download size: 478 k
Is this ok [y/N]: y
Downloading Packages:
(1/3): audit-libs-3.1.5-1.el9.x86_64.rpm
(2/3): python3-audit-3.1.5-1.el9.x86_64.rpm
(3/3): audit-3.1.5-1.el9.x86_64.rpm
------------------------------------------------------------------------------------------------------------------------------------------------
Total
Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
```

File Machine View Input Devices Help

```
[root@centosstream9 centos]# touch local_httpd_fix.cil
[root@centosstream9 centos]# vim local_httpd_fix.cil
[root@centosstream9 centos]# semodule -i local_httpd_fix.cil
[root@centosstream9 centos]# systemctl restart httpd
[root@centosstream9 centos]# semodule -lfull |grep local_httpd
400 local_httpd_fix    cil
[root@centosstream9 centos]#
```

File Machine View Input Devices Help

```
(allow cupsd_lpd_t
 cupsd_var_run_t(file(read)))
~
~
~
~
```

```
[root@centosstream9 centos]# sesearch -A --source=cupsd_lpd_t --target=cupsd_var_run_t --class=file --perm=read
allow cupsd_lpd_t cupsd_var_run_t:file read;
[root@centosstream9 centos]# systemctl status httpd
● httpd.service - The Apache HTTP Server
     Loaded: loaded (/usr/lib/systemd/system/httpd.service; disabled; vendor preset: disabled)
     Active: active (running) since Fri 2024-11-22 07:44:27 EST; 6min ago
       Docs: man:httpd.service(8)
   Main PID: 7361 (httpd)
     Status: "Total requests: 0; Idle/Busy workers 100/0;Requests/sec: 0; Bytes served/sec:   0 B/sec"
      Tasks: 177 (limit: 11110)
     Memory: 35.3M
        CPU: 5.272s
     CGroup: /system.slice/httpd.service
             ├─7361 /usr/sbin/httpd -DFOREGROUND
             ├─7362 /usr/sbin/httpd -DFOREGROUND
             ├─7363 /usr/sbin/httpd -DFOREGROUND
             ├─7365 /usr/sbin/httpd -DFOREGROUND
             └─7368 /usr/sbin/httpd -DFOREGROUND

Nov 22 07:44:26 centosstream9.linuxvmimages.local systemd[1]: Starting The Apache HTTP Server...
Nov 22 07:44:27 centosstream9.linuxvmimages.local systemd[1]: Started The Apache HTTP Server.
Nov 22 07:44:27 centosstream9.linuxvmimages.local httpd[7361]: Server configured, listening on: port 80
[root@centosstream9 centos]# ps -efZ | rep httpd
bash: rep: command not found...
[root@centosstream9 centos]# ps -efZ | grep httpd
system_u:system_r:httpd_t:s0    root        7361       1  0 07:44 ?        00:00:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0    apache      7362    7361  0 07:44 ?        00:00:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0    apache      7363    7361  0 07:44 ?        00:00:01 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0    apache      7365    7361  0 07:44 ?        00:00:02 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0    apache      7368    7361  0 07:44 ?        00:00:01 /usr/sbin/httpd -DFOREGROUND
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 root 7631 5223  0 07:52 pts/0 00:00:00 grep --color=auto httpd
```

```
[root@centosstream9 centos]# ausearch -m AVC -i -ts recent
<no matches>
```

5. SELINUX DENIALS IN THE AUDIT LOG

```
Password:
[root@centosstream9 centos]#  ausearch -m AVC,USER_AVC,SELINUX_ERR,USER_SELINUX_ERR
----
time->Fri Nov 22 01:52:31 2024
type=PROCTITLE msg=audit(1732258351.216:108): proctitle="/usr/libexec/accounts-daemon"
type=SYSCALL msg=audit(1732258351.216:108): arch=c000003e syscall=137 success=no exit=-13 a0=7f5ae879259
id=0 egid=0 sgid=0 fsgid=0 tty=(none) ses=4294967295 comm="accounts-daemon" exe="/usr/libexec/accounts-d
type=AVC msg=audit(1732258351.216:108): avc:  denied  { getattr } for  pid=733 comm="accounts-daemon" na
 tclass=filesystem permissive=0
----
time->Fri Nov 22 02:33:45 2024
type=PROCTITLE msg=audit(1732260825.803:236): proctitle=2F7573722F7362696E2F756E69785F63686B707764006365
type=EXECVE msg=audit(1732260825.803:236): argc=3 a0="/usr/sbin/unix_chkpwd" a1="centos" a2="chkexpiry"
type=SYSCALL msg=audit(1732260825.803:236): arch=c000003e syscall=59 success=yes exit=0 a0=7f8aa17fd04a
suid=0 fsuid=0 egid=1000 sgid=1000 fsgid=1000 tty=(none) ses=3 comm="unix_chkpwd" exe="/usr/sbin/unix_ch
type=AVC msg=audit(1732260825.803:236): avc:  denied  { read write } for  pid=3793 comm="unix_chkpwd" pa
nfined_u:object_r:user_devpts_t:s0 tclass=chr_file permissive=0
----
time->Fri Nov 22 02:33:48 2024
type=PROCTITLE msg=audit(1732260828.876:243): proctitle=2F7573722F62696E2F707974686F6E33002F7573722F7368
type=EXECVE msg=audit(1732260828.876:243): argc=2 a0="/usr/bin/python3" a1="/usr/share/setroubleshoot/Se
type=SYSCALL msg=audit(1732260828.876:243): arch=c000003e syscall=59 success=yes exit=0 a0=560f8921a200
d=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=(none) ses=4294967295 comm="SetroubleshootP" exe="/usr/bin/
type=AVC msg=audit(1732260828.876:243): avc:  denied  { siginh } for  pid=3805 comm="SetroubleshootP" sc
sive=0
[root@centosstream9 centos]#
```