Лабораторная работа №6

Мандатное разграничение прав в Linux

Губина О. В.

10 октября 2023

Российский университет дружбы народов, Москва, Россия

Информация

Докладчик

- Губина Ольга Вячеславовна
- студент(-ка) уч. группы НПИбд-01-20
- Российский университет дружбы народов
- 1032201737@pfur.ru
- https://github.com/ovgubina

Вводная часть

Актуальность

- Необходимость понимания возможножностей технологии SELinux и веб-сервера Apache.

Объект и предмет исследования

- SELinux, Apache

Цели и задачи

- Получить первое практическое знакомство с технологией SELinux1
- Проверить работу SELinx на практике совместно с веб-сервером Apache

Материалы и методы

- Командная строка ОС Linux

Процесс выполнения работы

Режим enforcing политики targeted и запуск

```
[ovgubina@ovgubina ~]$ getenforce
Enforcing
[ovgubina@ovgubina ~]$ sestatus
SELinux status:                 enabled
SELinuxfs mount:                /sys/fs/selinux
SELinux root directory:         /etc/selinux
Loaded policy name:             targeted
Current mode:                   enforcing
Mode from config file:          enforcing
Policy MLS status:              enabled
Policy deny_unknown status:     allowed
Memory protection checking:     actual (secure)
Max kernel policy version:      33
[ovgubina@ovgubina ~]$
```

```
[ovgubina@ovgubina ~]$ service httpd status
Redirecting to /bin/systemctl status httpd.service
○ httpd.service - The Apache HTTP Server
     Loaded: loaded (/usr/lib/systemd/system/httpd.service; disabled; preset: disabled)
     Active: inactive (dead)
       Docs: man:httpd.service(8)
[ovgubina@ovgubina ~]$ service httpd start
Redirecting to /bin/systemctl start httpd.service
[ovgubina@ovgubina ~]$ service httpd status
Redirecting to /bin/systemctl status httpd.service
● httpd.service - The Apache HTTP Server
     Loaded: loaded (/usr/lib/systemd/system/httpd.service; disabled; preset: disabled)
     Active: active (running) since Mon 2023-10-09 19:37:46 MSK; 7s ago
       Docs: man:httpd.service(8)
   Main PID: 6096 (httpd)
     Status: "Started, listening on: port 80"
      Tasks: 213 (limit: 12145)
     Memory: 27.5M
        CPU: 191ms
     CGroup: /system.slice/httpd.service
             ├─6096 /usr/sbin/httpd -DFOREGROUND
             ├─6105 /usr/sbin/httpd -DFOREGROUND
             ├─6106 /usr/sbin/httpd -DFOREGROUND
             ├─6110 /usr/sbin/httpd -DFOREGROUND
             └─6111 /usr/sbin/httpd -DFOREGROUND

Oct 09 19:37:46 ovgubina.localdomain systemd[1]: Starting The Apache HTTP Server...
Oct 09 19:37:46 ovgubina.localdomain httpd[6096]: Server configured, listening on: port 80
Oct 09 19:37:46 ovgubina.localdomain systemd[1]: Started The Apache HTTP Server.
[ovgubina@ovgubina ~]$
```

Статистика Apache

```
[ovgubina@ovgubina ~]$ sestatus -b httpd
SELinux status:                 enabled
SELinuxfs mount:                /sys/fs/selinux
SELinux root directory:         /etc/selinux
Loaded policy name:             targeted
Current mode:                   enforcing
Mode from config file:          enforcing
Policy MLS status:              enabled
Policy deny_unknown status:     allowed
Memory protection checking:     actual (secure)
Max kernel policy version:      33

Policy booleans:
abrt_anon_write                             off
abrt_handle_event                           off
abrt_upload_watch_anon_write                on
antivirus_can_scan_system                   off
antivirus_use_jit                           off
auditadm_exec_content                       on
authlogin_nsswitch_use_ldap                 off
authlogin_radius                            off
authlogin_yubikey                           off
awstats_purge_apache_log_files              off
boinc_execmem                               on
cdrecord_read_content                       off
cluster_can_network_connect                 off
cluster_manage_all_files                    off
cluster_use_execmem                         off
cobbler_anon_write                          off
cobbler_can_network_connect                 off
cobbler_use_cifs                            off
```

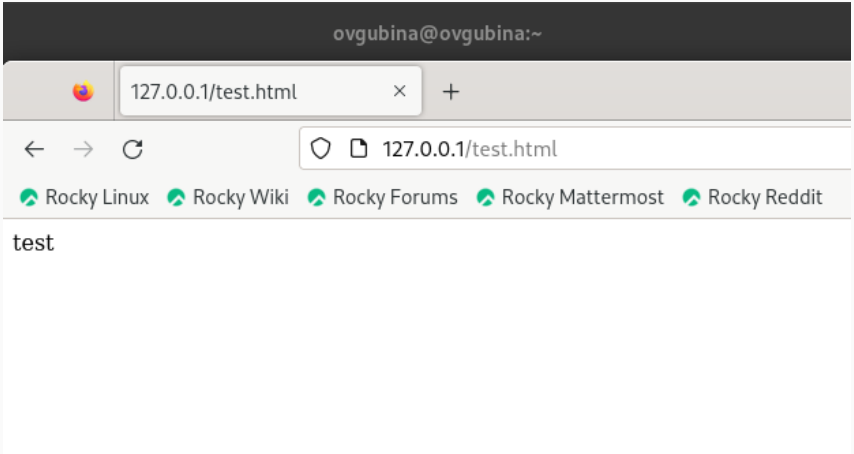
```
[ovgubina@ovgubina ~]$ seinfo
Statistics for policy file: /sys/fs/selinux/policy
Policy Version:             33 (MLS enabled)
Target Policy:              selinux
Handle unknown classes:     allow
  Classes:             135    Permissions:         457
  Sensitivities:         1    Categories:         1024
  Types:              5100    Attributes:          258
  Users:                 8    Roles:                14
  Booleans:            353    Cond. Expr.:         384
  Allow:             65008    Neverallow:            0
  Auditallow:          170    Dontaudit:          8572
  Type_trans:       265344    Type_change:          87
  Type_member:          35    Range_trans:        6164
  Role allow:           38    Role_trans:          420
  Constraints:          70    Validatetrans:         0
  MLS Constrain:        72    MLS Val. Tran:         0
  Permissives:           2    Polcap:                6
  Defaults:              7    Typebounds:            0
  Allowxperm:            0    Neverallowxperm:       0
  Auditallowxperm:       0    Dontauditxperm:        0
  Ibendportcon:          0    Ibpkeycon:             0
  Initial SIDs:         27    Fs_use:               35
  Genfscon:            109    Portcon:             660
  Netifcon:              0    Nodecon:               0
[ovgubina@ovgubina ~]$
```

Создание файла test.html

```
<html>
<body>test</body>
</html>
~
~
~
~
~
~
```

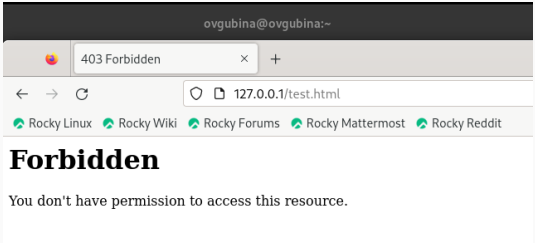
```
[ovgubina@ovgubina ~]$ ls -lZ /var/www/html
total 4
-rw-r--r--. 1 root root unconfined_u:object_r:httpd_sys_content_t:s0 33 Oct  9 19:50 test.html
[ovgubina@ovgubina ~]$
```

Обращение к файлу через веб-сервер



Смена контекста безропасности html файла

```
[root@ovgubina ~]# chcon -t samba_share_t /var/www/html/test.html
[root@ovgubina ~]# ls -Z /var/www/html/test.html
unconfined_u:object_r:samba_share_t:s0 /var/www/html/test.html
[root@ovgubina ~]#
```

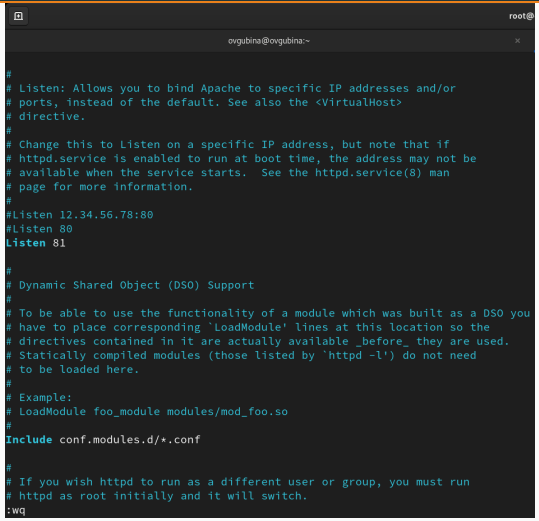


Log-файлы


[root@ovgubina ~]# ls -l /var/www/html/test.html
-rw-r--r--. 1 root root 33 Oct 9 19:50 /var/www/html/test.html
[root@ovgubina ~]# tail /var/log/messages
Oct 9 20:06:01 ovgubina systemd[1]: Created slice Slice /system/dbus-:1.1-org.fedoraproject.SetroubleshootPrivileged.
Oct 9 20:06:01 ovgubina systemd[1]: Started dbus-:1.1-org.fedoraproject.SetroubleshootPrivileged@0.service.
Oct 9 20:06:04 ovgubina setroubleshoot[6998]: SELinux is preventing /usr/sbin/httpd from getattr access on the file /var/www/html/test.html. For complete SEL
inux messages run: sealert -l 147bdebb-2a12-4b0e-8be3-f2deed03e785
Oct 9 20:06:04 ovgubina setroubleshoot[6998]: SELinux is preventing /usr/sbin/httpd from getattr access on the file /var/www/html/test.html.#012#012***** Pl
ugin restorecon (92.2 confidence) suggests   ************************#012#012If you want to fix the label. #012/var/www/html/test.html default label should be
httpd_sys_content_t.#012Then you can run restorecon. The access attempt may have been stopped due to insufficient permissions to access a parent directory in
which case try to change the following command accordingly.#012Do#012# /sbin/restorecon -v /var/www/html/test.html#012#012***** Plugin public_content (7.83
confidence) suggests   ********************#012#012If you want to treat test.html as public content#012Then you need to change the label on test.html to publi
c_content_t or public_content_rw_t.#012Do#012# semanage fcontext -a -t public_content_t '/var/www/html/test.html'#012# restorecon -v '/var/www/html/test.html'
#012#012***** Plugin catchall (1.41 confidence) suggests   **************************#012#012If you believe that httpd should be allowed getattr access on th
e test.html file by default.#012Then you should report this as a bug.#012You can generate a local policy module to allow this access.#012Do#012allow this acce
ss for now by executing:#012# ausearch -c 'httpd' --raw | audit2allow -M my-httpd#012# semodule -X 300 -i my-httpd.pp#012
Oct 9 20:06:04 ovgubina setroubleshoot[6998]: SELinux is preventing /usr/sbin/httpd from getattr access on the file /var/www/html/test.html. For complete SEL
inux messages run: sealert -l 147bdebb-2a12-4b0e-8be3-f2deed03e785
Oct 9 20:06:04 ovgubina setroubleshoot[6998]: SELinux is preventing /usr/sbin/httpd from getattr access on the file /var/www/html/test.html.#012#012***** Pl
ugin restorecon (92.2 confidence) suggests   ************************#012#012If you want to fix the label. #012/var/www/html/test.html default label should be
httpd_sys_content_t.#012Then you can run restorecon. The access attempt may have been stopped due to insufficient permissions to access a parent directory in
which case try to change the following command accordingly.#012Do#012# /sbin/restorecon -v /var/www/html/test.html#012#012***** Plugin public_content (7.83
confidence) suggests   ********************#012#012If you want to treat test.html as public content#012Then you need to change the label on test.html to publi
c_content_t or public_content_rw_t.#012Do#012# semanage fcontext -a -t public_content_t '/var/www/html/test.html'#012# restorecon -v '/var/www/html/test.html'
#012#012***** Plugin catchall (1.41 confidence) suggests   **************************#012#012If you believe that httpd should be allowed getattr access on th
e test.html file by default.#012Then you should report this as a bug.#012You can generate a local policy module to allow this access.#012Do#012allow this acce
ss for now by executing:#012# ausearch -c 'httpd' --raw | audit2allow -M my-httpd#012# semodule -X 300 -i my-httpd.pp#012
Oct 9 20:06:14 ovgubina systemd[1]: dbus-:1.1-org.fedoraproject.SetroubleshootPrivileged@0.service: Deactivated successfully.
Oct 9 20:06:14 ovgubina systemd[1]: dbus-:1.1-org.fedoraproject.SetroubleshootPrivileged@0.service: Consumed 2.490s CPU time.
Oct 9 20:06:14 ovgubina systemd[1]: setroubleshootd.service: Deactivated successfully.
Oct 9 20:06:14 ovgubina systemd[1]: setroubleshootd.service: Consumed 1.473s CPU time.
[root@ovgubina ~]#


[root@ovgubina ~]# cat /var/log/audit/audit.log
type=DAEMON_START msg=audit(1694100940.504:6778): op=start ver=3.0.7 format=enriched kernel=5.14.0-284.11.1.el9_2.x86_64 auid=4294967295 pid=712 uid=0 ses=429
4967295 subj=system_u:system_r:auditd_t:s0 res=successAUID="unset" UID="root"
type=CONFIG_CHANGE msg=audit(1694100940.574:5): op=set audit_backlog_limit=8192 old=64 auid=4294967295 ses=4294967295 subj=system_u:system_r:unconfined_servic
e_t:s0 res=1AUID="unset"
type=SYSCALL msg=audit(1694100940.574:5): arch=c000003e syscall=44 success=yes exit=60 a0=3 a1=7fff09031d90 a2=3c a3=0 items=0 ppid=717 pid=727 auid=429496729
5 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=(none) ses=4294967295 comm="auditctl" exe="/usr/sbin/auditctl" subj=system_u:system_r:unconfined
_service_t:s0 key=(null)ARCH=x86_64 SYSCALL=sendto AUID="unset" UID="root" GID="root" EUID="root" SUID="root" FSUID="root" EGID="root" SGID="root" FSGID="root
"
type=PROCTITLE msg=audit(1694100940.574:5): proctitle=2F7362696E2F617564697463746C002D52002F6574632F61756469742F61756469742E72756C6573
type=CONFIG_CHANGE msg=audit(1694100940.575:6): op=set audit_failure=1 old=1 auid=4294967295 ses=4294967295 subj=system_u:system_r:unconfined_service_t:s0 res
=1AUID="unset"
type=SYSCALL msg=audit(1694100940.575:6): arch=c000003e syscall=44 success=yes exit=60 a0=3 a1=7fff09031d90 a2=3c a3=0 items=0 ppid=717 pid=727 auid=429496729
5 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=(none) ses=4294967295 comm="auditctl" exe="/usr/sbin/auditctl" subj=system_u:system_r:unconfined
_service_t:s0 key=(null)ARCH=x86_64 SYSCALL=sendto AUID="unset" UID="root" GID="root" EUID="root" SUID="root" FSUID="root" EGID="root" SGID="root" FSGID="root
"
type=PROCTITLE msg=audit(1694100940.575:6): proctitle=2F7362696E2F617564697463746C002D52002F6574632F61756469742F61756469742E72756C6573
type=CONFIG_CHANGE msg=audit(1694100940.576:7): op=set audit_backlog_wait_time=60000 old=60000 auid=4294967295 ses=4294967295 subj=system_u:system_r:unconfine
d_service_t:s0 res=1AUID="unset"
type=SYSCALL msg=audit(1694100940.576:7): arch=c000003e syscall=44 success=yes exit=60 a0=3 a1=7fff09031d90 a2=3c a3=0 items=0 ppid=717 pid=727 auid=429496729
5 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=(none) ses=4294967295 comm="auditctl" exe="/usr/sbin/auditctl" subj=system_u:system_r:unconfined
_service_t:s0 key=(null)ARCH=x86_64 SYSCALL=sendto AUID="unset" UID="root" GID="root" EUID="root" SUID="root" FSUID="root" EGID="root" SGID="root" FSGID="root
"
type=PROCTITLE msg=audit(1694100940.576:7): proctitle=2F7362696E2F617564697463746C002D52002F6574632F61756469742F61756469742E72756C6573
type=SERVICE_START msg=audit(1694100940.578:8): pid=1 uid=0 auid=4294967295 ses=4294967295 subj=system_u:system_r:init_t:s0 msg='unit=auditd comm="systemd" ex
e="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=success'UID="root" AUID="unset"
type=SYSTEM_BOOT msg=audit(1694100940.593:9): pid=734 uid=0 auid=4294967295 ses=4294967295 subj=system_u:system_r:init_t:s0 msg=' comm="systemd-update-utmp" e
xe="/usr/lib/systemd/systemd-update-utmp" hostname=? addr=? terminal=? res=success'UID="root" AUID="unset"
type=SERVICE_START msg=audit(1694100940.602:10): pid=1 uid=0 auid=4294967295 ses=4294967295 subj=system_u:system_r:init_t:s0 msg='unit=systemd-update-utmp com
m="systemd" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=success'UID="root" AUID="unset"

Смена прослушиваемого порта и перезапуск сервера




```
[root@ovgubina ~]# service httpd restart
Redirecting to /bin/systemctl restart httpd.service
[root@ovgubina ~]#
```

log-файл

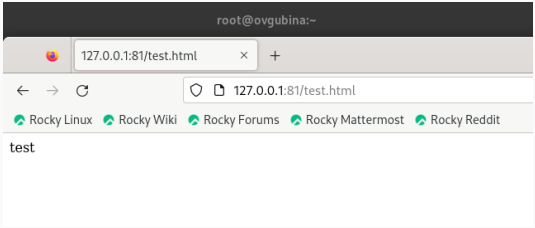
```
[root@ovgubina ~]# tail /var/log/messages
Oct  9 20:14:08 ovgubina systemd[1]: Starting The Apache HTTP Server...
Oct  9 20:14:08 ovgubina systemd[1]: Started The Apache HTTP Server.
Oct  9 20:14:08 ovgubina httpd[7156]: Server configured, listening on: port 81
Oct  9 20:14:27 ovgubina systemd[1]: Stopping The Apache HTTP Server...
Oct  9 20:14:28 ovgubina systemd[1]: httpd.service: Deactivated successfully.
Oct  9 20:14:28 ovgubina systemd[1]: Stopped The Apache HTTP Server.
Oct  9 20:14:28 ovgubina systemd[1]: Starting The Apache HTTP Server...
Oct  9 20:14:28 ovgubina httpd[7400]: Server configured, listening on: port 81
Oct  9 20:14:28 ovgubina systemd[1]: Started The Apache HTTP Server.
Oct  9 20:14:34 ovgubina systemd[1]: fprintd.service: Deactivated successfully.
[root@ovgubina ~]#
```

Список портов

```
[root@ovgubina ~]# semanage port -l | grep http_port_t
http_port_t                    tcp      80, 81, 443, 488, 8008, 8009, 8443, 9000
pegasus_http_port_t            tcp      5988
[root@ovgubina ~]#
```

Возвращаем контекст безопасности

```
[root@ovgubina ~]# chcon -t httpd_sys_content_t /var/www/html/test.html
[root@ovgubina ~]# ls -Z /var/www/html/test.html
unconfined_u:object_r:httpd_sys_content_t:s0 /var/www/html/test.html
[root@ovgubina ~]#
```



Удаление файла

```
[root@ovgubina ~]# semanage port -d -t http_port_t -p tcp 81
ValueError: Port tcp/81 is defined in policy, cannot be deleted
[root@ovgubina ~]# vim /etc/httpd/conf/httpd.conf
[root@ovgubina ~]# rm /var/www/html/test.html
rm: remove regular file '/var/www/html/test.html'? y
[root@ovgubina ~]# ls /var/www/html
[root@ovgubina ~]#
```

Результаты работы

Результаты работы

- Получила первое практическое знакомство с технологией SELinux1
- Проверила работу SELinx на практике совместно с веб-сервером Apache.

Вывод

Вывод

Развила навыки администрирования ОС Linux. Получила первое практическое знакомство с технологией SELinux1. Проверила работу SELinx на практике совместно с веб-сервером Apache.