Лабораторная работа №6

Мандатное разграничение прав в Linux

Дорофеева А.Т.

12 октября 2023

Российский университет дружбы народов, Москва, Россия

Информация

Докладчик

- Дорофеева Алёна Тимофеевна
- студент(-ка) уч. группы НПИбд-01-20
- Российский университет дружбы народов
- 1032201392@pfur.ru
- https://github.com/DorofeevaAT

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

```
[aldoro@aldoro ~]$ getenforce
Enforcing
[aldoro@aldoro ~]$ 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
[aldoro@aldoro ~]$
```

```
[aldoro@aldoro ~]$ 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)
[aldoro@aldoro ~]$ service httpd start
Redirecting to /bin/systemctl start httpd.service
[aldoro@aldoro ~]$ 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 Thu 2023-10-12 07:02:26 MSK; 16s ago
       Docs: man:httpd.service(8)
   Main PID: 109637 (httpd)
     Status: "Total requests: 0; Idle/Busy workers 100/0;Requests/sec: 0; Bytes served/sec:   0 B/sec"
      Tasks: 213 (limit: 12221)
     Memory: 23.2M
        CPU: 108ms
     CGroup: /system.slice/httpd.service
             ├─109637 /usr/sbin/httpd -DFOREGROUND
             ├─109642 /usr/sbin/httpd -DFOREGROUND
             ├─109648 /usr/sbin/httpd -DFOREGROUND
             ├─109649 /usr/sbin/httpd -DFOREGROUND
             └─109650 /usr/sbin/httpd -DFOREGROUND

Oct 12 07:02:26 aldoro.localdomain systemd[1]: Starting The Apache HTTP Server...
Oct 12 07:02:26 aldoro.localdomain systemd[1]: Started The Apache HTTP Server.
Oct 12 07:02:26 aldoro.localdomain httpd[109637]: Server configured, listening on: port 80
[aldoro@aldoro ~]$
```

Статистика Apache

```
[aldoro@aldoro ~]$ 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
cobbler_use_nfs                             off
collectd_tcp_network_connect                off
colord_use_nfs                              off
condor_tcp_network_connect                  off
conman_can_network                          off
conman_use_nfs                              off
container_connect_any                       off
container_manage_cgroup                     off
container_use_cephfs                        off
container_use_devices                       off
container_use_ecryptfs                      off
cron_can_relabel                            off
cron_system_cronjob_use_shares              off
```

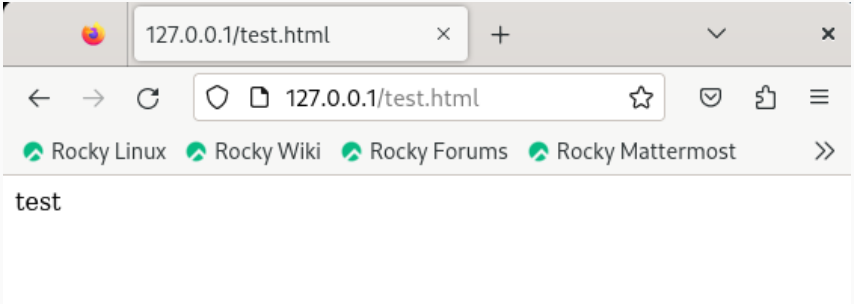
```
Statistics for policy file: /sys/fs/selinux/policy
Policy Version:             33 (MLS enabled)
Target Policy:              selinux
Handle unknown classes:     allow
  Classes:             135    Permissions:         457
  Sensitivities:         1    Categories:         1024
  Types:              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

[aldoro@aldoro ~]$
```

Создание файла test.html

```
[aldoro@aldoro ~]$ su -
Password:
[root@aldoro ~]# nano /var/www/html/test.html
[root@aldoro ~]# cat /var/www/html/test.html
<html>
<body>test</body>
</html>
[root@aldoro ~]#
```

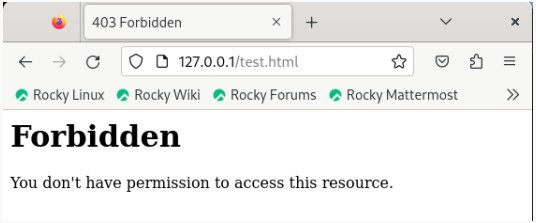
```
[aldoro@aldoro ~]$ ls -lZ /var/www/html
total 4
-rw-r--r--. 1 root root unconfined_u:object_r:httpd_sys_content_t:s0 33 Oct 12 07:14 test.html
[aldoro@aldoro ~]$
```

Обращение к файлу через веб-сервер



Смена контекста безропасности html файла

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



Log-файлы

:::::::::::::: {.columns align=center} ::: {.column width="50%"}

```
[root@aldoro ~]# ls -l /var/www/html/test.html
-rw-r--r--. 1 root root 33 Oct 12 07:14 /var/www/html/test.html
[root@aldoro ~]# tail /var/log/messages
Oct 12 07:26:35 aldoro setroubleshoot[111056]: SELinux is preventing /usr/sbin/httpd from getattr access on the file /var/www/html/test.html.#012#012*****  Plugin 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 public_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 the 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 access for now by executing:#012# ausearch -c 'httpd' --raw | audit2allow -M my-httpd#012# semodule -X 300 -i my-httpd.pp#012
Oct 12 07:26:35 aldoro setroubleshoot[111056]: SELinux is preventing /usr/sbin/httpd from getattr access on the file /var/www/html/test.html. For complete SELinux messages run: sealert -l 75b759cf-8678-4b72-91d7-4828e4b3e437
Oct 12 07:26:35 aldoro setroubleshoot[111056]: SELinux is preventing /usr/sbin/httpd from getattr access on the file /var/www/html/test.html.#012#012*****  Plugin 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 public_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 the 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 access for now by executing:#012# ausearch -c 'httpd' --raw | audit2allow -M my-httpd#012# semodule -X 300 -i my-httpd.pp#012
Oct 12 07:26:45 aldoro systemd[1]: dbus-:1.1-org.fedoraproject.SetroubleshootPrivileged@0.service: Deactivated successfully.
Oct 12 07:26:45 aldoro systemd[1]: dbus-:1.1-org.fedoraproject.SetroubleshootPrivileged@0.service: Consumed 2.365s CPU time.
Oct 12 07:26:45 aldoro systemd[1]: setroubleshootd.service: Deactivated successfully.
```

Смена прослушиваемого порта и перезапуск сервера

```
#
# Change this to Listen on a specific IP address, but note that if
# httpd.service is enabled to run at boot time, the address may not be
# available when the service starts.  See the httpd.service(8) man
# page for more information.
#
#Listen 12.34.56.78:80
#Listen 80
Listen 81
#
# Dynamic Shared Object (DSO) Support
#
# To be able to use the functionality of a module which was built as a DSO yo
# have to place corresponding `LoadModule' lines at this location so the
# directives contained in it are actually available _before_ they are used.
# Statically compiled modules (those listed by `httpd -l') do not need
# to be loaded here.
```

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

log-файл

```
[root@aldoro ~]# tail /var/log/messages
Oct 12 07:26:59 aldoro firefox.desktop[110770]: [ERROR viaduct::backend::ffi] Missing HTTP status
Oct 12 07:26:59 aldoro firefox.desktop[110770]: [ERROR viaduct::backend::ffi] Missing HTTP status
Oct 12 07:27:00 aldoro systemd[1574]: app-gnome-firefox-110770.scope: Consumed 22.636s CPU time.
Oct 12 07:40:10 aldoro systemd[1]: Stopping The Apache HTTP Server...
Oct 12 07:40:12 aldoro systemd[1]: httpd.service: Deactivated successfully.
Oct 12 07:40:12 aldoro systemd[1]: Stopped The Apache HTTP Server.
Oct 12 07:40:12 aldoro systemd[1]: httpd.service: Consumed 1.843s CPU time.
Oct 12 07:40:12 aldoro systemd[1]: Starting The Apache HTTP Server...
Oct 12 07:40:12 aldoro systemd[1]: Started The Apache HTTP Server.
Oct 12 07:40:12 aldoro httpd[111134]: Server configured, listening on: port 81
[root@aldoro ~]#
```

Список портов

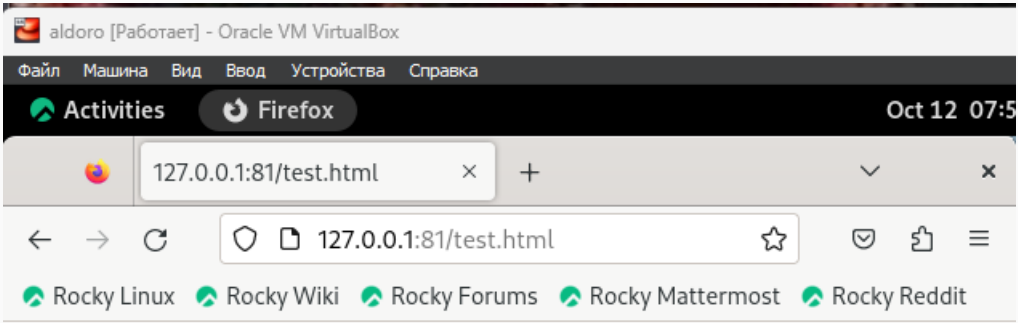
```
[root@aldoro ~]# semanage port -a -t http_port_t -p tcp 81
ValueError: Port tcp/81 already defined
[root@aldoro ~]# swmanage port -l |grep http_port_t
bash: swmanage: command not found...
[root@aldoro ~]# semanage port -l |grep http_port_t
http_port_t                    tcp      80, 81, 443, 488, 8008, 8009, 8443, 9000
pegasus_http_port_t            tcp      5988
[root@aldoro ~]#
```

Возвращаем контекст безопасности

:::::::::::::: {.columns align=center} ::: {.column width="50%"}

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

::: ::: {.column width="50%"}



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.