Презентация по лабораторной работе №6

Мандатное разграничение прав в Linux

Нгуен Дык Ань

11 октября 2024

Докладчик

- Нгуен Дык Ань
- Студенческий билет: 1032215251
- Группа: НКНбд-01-21
- Российский университет дружбы народов
- https://github.com/NguyenDucAnh0512

Цель работы

Развить навыки администрирования ОС Linux. Получить первое практическое знакомство с технологией SELinux

Выполнение работы

1. Подготовка лабораторного стенда

- Задать параметр ServerName в конфигурационном файле /etc/httpd/httpd.conf
- Проследить, чтобы пакетный фильтр был отключён или в своей рабочей конфигурации позволял подключаться к 80-у и 81-у портам протокола tcp

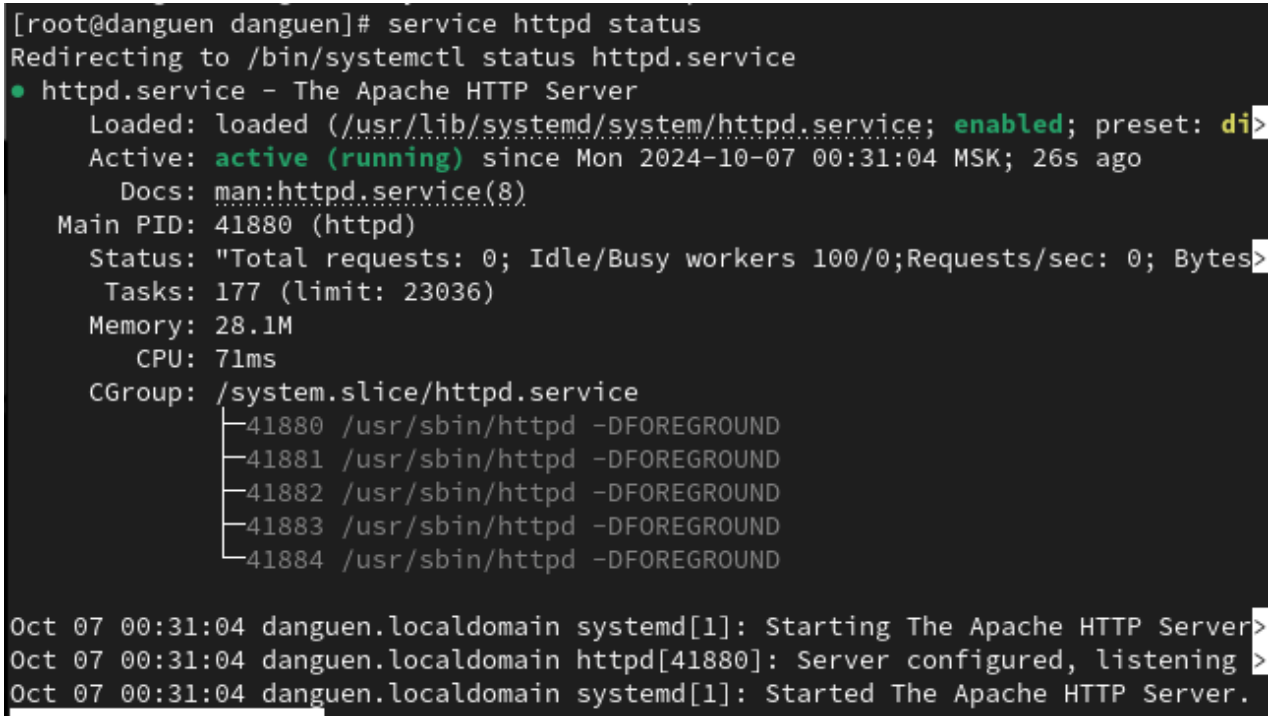
```
ServerAdmin root@localhost

#
# ServerName gives the name and port that the server uses to identify itself.
# This can often be determined automatically, but we recommend you specify
# it explicitly to prevent problems during startup.
#
# If your host doesn't have a registered DNS name, enter its IP address here.
#
ServerName test.ru
```

```
[root@danguen danguen]# iptables -I INPUT -p tcp --dport 80 -j ACCEPT
[root@danguen danguen]# iptables -I INPUT -p tcp --dport 81 -j ACCEPT
[root@danguen danguen]# iptables -I OUTPUT -p tcp --sport 80 -j ACCEPT
[root@danguen danguen]# iptables -I OUTPUT -p tcp --sport 81 -j ACCEPT
```

2. Выполнение работы

- Убедиться, что SELinux работает в режиме enforcing политики targeted с помощью команд getenforce и sestatus
- Проверять, что услуга httpd работает
- Использовать команду ps auxZ | grep httpd, найти веб-сервер Apache в списке процессов
- Посмотрить статистику по политике с помощью команды seinfo

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


[root@danguen danguen]# service httpd status
Redirecting to /bin/systemctl status httpd.service
● httpd.service - The Apache HTTP Server
Loaded: loaded (/usr/lib/systemd/system/httpd.service; enabled; preset: di
Active: active (running) since Mon 2024-10-07 00:31:04 MSK; 26s ago
Docs: man:httpd.service(8)
Main PID: 41880 (httpd)
Status: "Total requests: 0; Idle/Busy workers 100/0;Requests/sec: 0; Bytes
Tasks: 177 (limit: 23036)
Memory: 28.1M
CPU: 71ms
CGroup: /system.slice/httpd.service
├─41880 /usr/sbin/httpd -DFOREGROUND
├─41881 /usr/sbin/httpd -DFOREGROUND
├─41882 /usr/sbin/httpd -DFOREGROUND
├─41883 /usr/sbin/httpd -DFOREGROUND
└─41884 /usr/sbin/httpd -DFOREGROUND
Oct 07 00:31:04 danguen.localdomain systemd[1]: Starting The Apache HTTP Server
Oct 07 00:31:04 danguen.localdomain httpd[41880]: Server configured, listening
Oct 07 00:31:04 danguen.localdomain systemd[1]: Started The Apache HTTP Server.

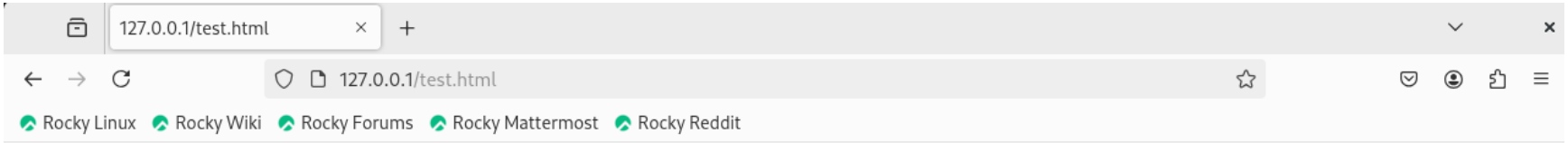
```
[root@danguen danguen]# ps auxZ | grep httpd
system_u:system_r:httpd_t:s0    root       41880  0.0  0.3  20152 11404 ?        Ss   00:31   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0    apache     41881  0.0  0.1  22032  7100 ?        S    00:31   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0    apache     41882  0.0  0.4 1571340 17256 ?       Sl   00:31   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0    apache     41883  0.0  0.3 1440204 13144 ?       Sl   00:31   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0    apache     41884  0.0  0.2 1440204 10900 ?       Sl   00:31   0:00 /usr/sbin/httpd -DFOREGROUND
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 root 42103 0.0  0.0 221664 2176 pts/0 S+ 00:32   0:00 grep --color=auto httpd
```

```
[root@danguen danguen]# 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:              5145    Attributes:          259
  Users:                 8    Roles:                15
  Booleans:            356    Cond. Expr.:         388
  Allow:             65504    Neverallow:            0
  Auditallow:          176    Dontaudit:          8682
  Type_trans:       271770    Type_change:          94
  Type_member:          37    Range_trans:        5931
  Role allow:           40    Role_trans:          417
  Constraints:          70    Validatetrans:         0
  MLS Constrain:        72    MLS Val. Tran:         0
  Permissives:           4    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:             665
  Netifcon:              0    Nodecon:               0
```

2. Выполнение работы

- Создать от имени суперпользователя html-файл /var/www/html/test.html
- Обратиться к файлу через веб-сервер, введя в браузере адрес http://127.0.0.1/test.html
- Проверить контекст файла test.html можно командой ls -Z /var/www/html/test.html
- Измените контекст файла /var/www/html/test.html с httpd_sys_content_t на samba_share_t

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

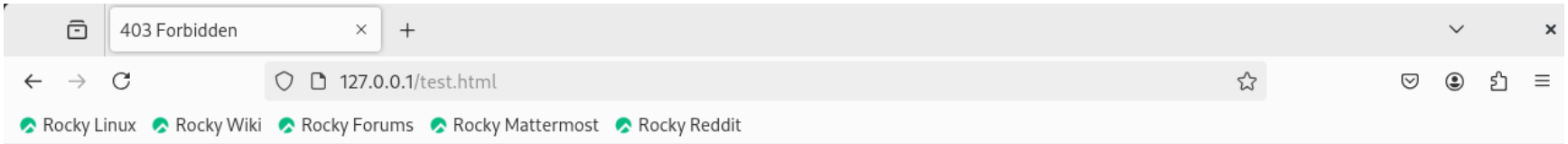

127.0.0.1/test.html
127.0.0.1/test.html
Rocky Linux
Rocky Wiki
Rocky Forums
Rocky Mattermost
Rocky Reddit
test

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

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

2. Выполнение работы

- Попробовать ещё раз получить доступ к файлу через веб-сервер
- Попробовать запустить веб-сервер Apache на прослушивание TCP-порта 81 и убедиться, что порт 81 появился в списке
- Выполнять перезапуск веб-сервера Apache и проанализировать лог-файлы
- Вернуть контекст httpd_sys_content__t к файлу /var/www/html/ test.html



Forbidden

You don't have permission to access this resource.

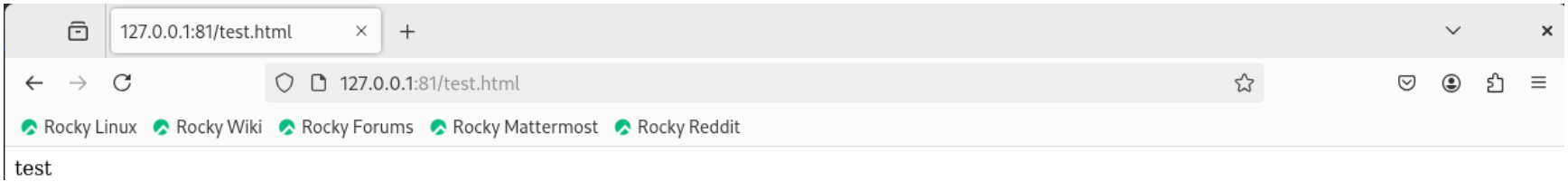
```
[root@danguen danguen]# semanage port -l | grep http_port_t
http_port_t                    tcp      80, 81, 443, 488, 8008, 8009, 8443, 9000
pegasus_http_port_t            tcp      5988
```

```
Oct  7 00:53:35 danguen systemd[1]: dbus-:1.1-org.fedoraproject.SetroubleshootPrivileged@0.service: Deactivated successfully.
Oct  7 00:53:35 danguen systemd[1]: setroubleshootd.service: Deactivated successfully.
Oct  7 00:57:16 danguen systemd[1]: Stopping The Apache HTTP Server...
Oct  7 00:57:17 danguen systemd[1]: httpd.service: Deactivated successfully.
Oct  7 00:57:17 danguen systemd[1]: Stopped The Apache HTTP Server.
Oct  7 00:57:17 danguen systemd[1]: Starting The Apache HTTP Server...
Oct  7 00:57:17 danguen httpd[43317]: Server configured, listening on: port 81
Oct  7 00:57:17 danguen systemd[1]: Started The Apache HTTP Server.
```

```
[root@danguen danguen]# chcon -t httpd_sys_content_t /var/www/html/test.html
```

2. Выполнение работы

- Попробовать получить доступ к файлу через веб-сервер, введя в браузере адрес http://127.0.0.1:81/test.html
- Удалить файл /var/www/html/test.html.- Удалить файл /var/www/html/test.html.


127.0.0.1:81/test.html
127.0.0.1:81/test.html
Rocky Linux
Rocky Wiki
Rocky Forums
Rocky Mattermost
Rocky Reddit
test

Вывод

После работы я получил практическое знакомство с технологией SELinux и развил навыки работы с ним.