

Лабораторная работа №6

Мандатное разграничение прав в Linux

Хватов Максим

Содержание

| | | |
|---|---------------------------------|----|
| 1 | Цель работы | 5 |
| 2 | Подготовка лабораторного стенда | 6 |
| 3 | Выполнение работы | 8 |
| 4 | Вывод | 11 |

Список иллюстраций

| | | |
|-----|--------|----|
| 3.1 | Рис. 1 | 8 |
| 3.2 | Рис. 2 | 9 |
| 3.3 | Рис. 3 | 10 |

Список таблиц

1 Цель работы

Развить навыки администрирования ОС Linux. Получить первое практическое знакомство с технологией SELinux. Проверить работу SELinux на практике совместно с веб-сервером Apache.

2 Подготовка лабораторного стенда

1. При подготовке стенда обратите внимание, что необходимая для работы и указанная выше политика `targeted` и режим `enforcing` используются в данном дистрибутиве по умолчанию, т.е. каких-то специальных настроек не требуется. При этом следует убедиться, что политика и режим включены, особенно когда работа будет проводиться повторно и велика вероятность изменений при предыдущем использовании системы.
2. При необходимости администратор должен разбираться в работе SELinux и уметь как исправить конфигурационный файл `/etc/selinux/config`, так и проверить используемый режим и политику.
3. Необходимо, чтобы был установлен веб-сервер Apache. При установке системы в конфигурации «рабочая станция» указанный пакет не ставится.
4. В конфигурационном файле `/etc/httpd/httpd.conf` необходимо задать параметр `ServerName: ServerName test.ru` чтобы при запуске веб-сервера не выдавались лишние сообщения об ошибках, не относящихся к лабораторной работе.
5. Также необходимо проследить, чтобы пакетный фильтр был отключён или в своей рабочей конфигурации позволял подключаться к 80-у и 81-у портам протокола tcp. Отключить фильтр можно командами `iptables -F iptables -P INPUT ACCEPT iptables -P OUTPUT ACCEPT` либо добавить разрешающие правила: `iptables -I INPUT -p tcp -dport 80 -j ACCEPT iptables -I INPUT -p tcp -dport 81 -j ACCEPT iptables -I OUTPUT -p tcp -sport 80 -j ACCEPT iptables -I OUTPUT -p tcp -sport 81 -j ACCEPT`

6. Обратите внимание, что данные правила не являются «точными» и рекомендуемыми на все случаи жизни, они лишь позволяют правильно организовать работу стенда.
7. В работе специально не делается акцент, каким браузером (или какой консольной программой) будет производиться подключение к вебсерверу. По желанию могут использоваться разные программы, такие как консольные links, lynx, wget и графические konqueror, opera, firefox или др.

3 Выполнение работы

Вхожу в систему с полученными учётными данными и убеждаюсь, что SELinux работает в режиме enforcing политики targeted с помощью команд `getenforce` и `sestatus`.

Проверяю работоспособность сервера Apache

`ps auxZ | grep httpd`

```
[hmaksim@localhost ~]$ 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)
   Drop-In: /usr/lib/systemd/system/httpd.service.d
            └─php-fpm.conf
   Active: inactive (dead)
     Docs: man:httpd.service(8)
[hmaksim@localhost ~]$
[hmaksim@localhost ~]$ service httpd start
Redirecting to /bin/systemctl start httpd.service
[hmaksim@localhost ~]$ 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)
   Drop-In: /usr/lib/systemd/system/httpd.service.d
            └─php-fpm.conf
   Active: active (running) since Tue 2024-04-23 07:37:16 MSK; 3s ago
     Docs: man:httpd.service(8)
  Main PID: 34659 (httpd)
    Status: "Started, listening on: port 80"
    Tasks: 213 (limit: 10887)
   Memory: 29.5M
      CPU: 72ms
  CGroup: /system.slice/httpd.service
          └─34659 /usr/sbin/httpd -DFOREGROUND
            └─34673 /usr/sbin/httpd -DFOREGROUND
              └─34674 /usr/sbin/httpd -DFOREGROUND
                └─34675 /usr/sbin/httpd -DFOREGROUND
                  └─34676 /usr/sbin/httpd -DFOREGROUND

anp 23 07:37:16 localhost.localdomain systemd[1]: Starting The Apache HTTP Server:
anp 23 07:37:16 localhost.localdomain httpd[34659]: AH00558: httpd: Could not re
anp 23 07:37:16 localhost.localdomain httpd[34659]: Server configured, listening
anp 23 07:37:16 localhost.localdomain systemd[1]: Started The Apache HTTP Serve
[hmaksim@localhost ~]$
[hmaksim@localhost ~]$ getenforce
Enforcing
[hmaksim@localhost ~]$ setstatus
bash: setstatus: command not found...
[hmaksim@localhost ~]$
```

Рис. 3.1: Рис. 1

`sestatus -bigrep httpd` команда не работает

Устанавливаю seinfo и использую команду seinfo

```
[hmaksim@localhost ~]$ ps auxZ | grep httpd
system_u:system_r:httpd_t:s0 root 34659 0.0 0.6 20120 11284 ? Ss 07:37 0:00 /usr/sbin/httpd -DFO
system_u:system_r:httpd_t:s0 root 34660 0.0 1.3 173888 23620 ? Ss 07:37 0:00 php-fpm: master proc
system_u:system_r:httpd_t:s0 apache 34668 0.0 0.5 175780 10572 ? S 07:37 0:00 php-fpm: pool www
system_u:system_r:httpd_t:s0 apache 34669 0.0 0.5 175780 10572 ? S 07:37 0:00 php-fpm: pool www
system_u:system_r:httpd_t:s0 apache 34670 0.0 0.5 175780 10572 ? S 07:37 0:00 php-fpm: pool www
system_u:system_r:httpd_t:s0 apache 34671 0.0 0.5 175780 10572 ? S 07:37 0:00 php-fpm: pool www
system_u:system_r:httpd_t:s0 apache 34672 0.0 0.5 175780 10572 ? S 07:37 0:00 php-fpm: pool www
system_u:system_r:httpd_t:s0 apache 34673 0.0 0.3 21588 7180 ? S 07:37 0:00 /usr/sbin/httpd -DFO
system_u:system_r:httpd_t:s0 apache 34674 0.0 0.8 1669256 14984 ? SL 07:37 0:00 /usr/sbin/httpd -DFO
system_u:system_r:httpd_t:s0 apache 34675 0.0 0.6 1538120 10904 ? SL 07:37 0:00 /usr/sbin/httpd -DFO
system_u:system_r:httpd_t:s0 apache 34676 0.0 0.6 1538120 10888 ? SL 07:37 0:00 /usr/sbin/httpd -DFO
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 hmaksim 35265 0.0 0.1 6432 2156 pts/0 S+ 07:56 0:00 grep --col

[hmaksim@localhost ~]$ 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: 5135 Attributes: 259
Users: 8 Roles: 15
Booleans: 357 Cond. Expr.: 390
Allow: 65380 Neverallow: 0
Auditallow: 172 Dontaudit: 8647
Type_trans: 267809 Type_change: 94
Type_member: 37 Range_trans: 6164
Role_allow: 39 Role_trans: 419
Constraints: 70 Validatetrans: 0
MLS Constrains: 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: 665
Netifcon: 0 Nodecon: 0
```

Рис. 3.2: Рис. 2

Создаю файл test.html и пытаюсь его редактировать, сохранить его не получается из-за недостатка прав. При заходе на localhost я должен был получить “test” в браузере.

Использую команду `man httpd_selinux` и получаю конфигурацию ‘httpd_sys_content_t’

Использую команду `chcon -t samba_share_t /var/www/html/test.html`, затем `“ls -Z /var/www/html/test.html”`

Так как контекст поменялся, то в браузере получу ошибку You don’t have permission to access /test.html on this server.

```

[hmaksim@localhost ~]$ /var/www/html
bash: /var/www/html: 3ro karanor
[hmaksim@localhost ~]$ ls -lZ /var/www/html
-rw-r--r-- 0
[hmaksim@localhost ~]$ touch /var/www/html/test.html
touch: невозможно выполнить touch для '/var/www/html/test.html': Отказано в доступе
[hmaksim@localhost ~]$ sudo touch /var/www/html/test.html
[hmaksim@localhost ~]$ ls -Z /var/www/html/test.html
unconfined_u:object_r:httpd_sys_content_t:s0 /var/www/html/test.html
[hmaksim@localhost ~]$ chcon -t samba_share_t /var/www/html/test.html
chcon: не удалось изменить контекст безопасности '/var/www/html/test.html' на «unconfined_u:object_r:samba_share_t:s0»:
[hmaksim@localhost ~]$ sudo chcon -t samba_share_t /var/www/html/test.html
[hmaksim@localhost ~]$ ls -Z /var/www/html/test.html
unconfined_u:object_r:samba_share_t:s0 /var/www/html/test.html
[hmaksim@localhost ~]$ █

```

Рис. 3.3: Рис. 3

4 Вывод

Я развил наавыки работы с SELinux и научился работать с Apache на практике.