Лабораторная работа №6

Мандатное разграничение прав в Linux

Хватов Максим

Содержание

Список иллюстраций

Список таблиц

1 Цель работы

Развить навыки администрирования ОС Linux. Получить первое практическое знакомство с технологией SELinux. Проверить работу SELinx 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`

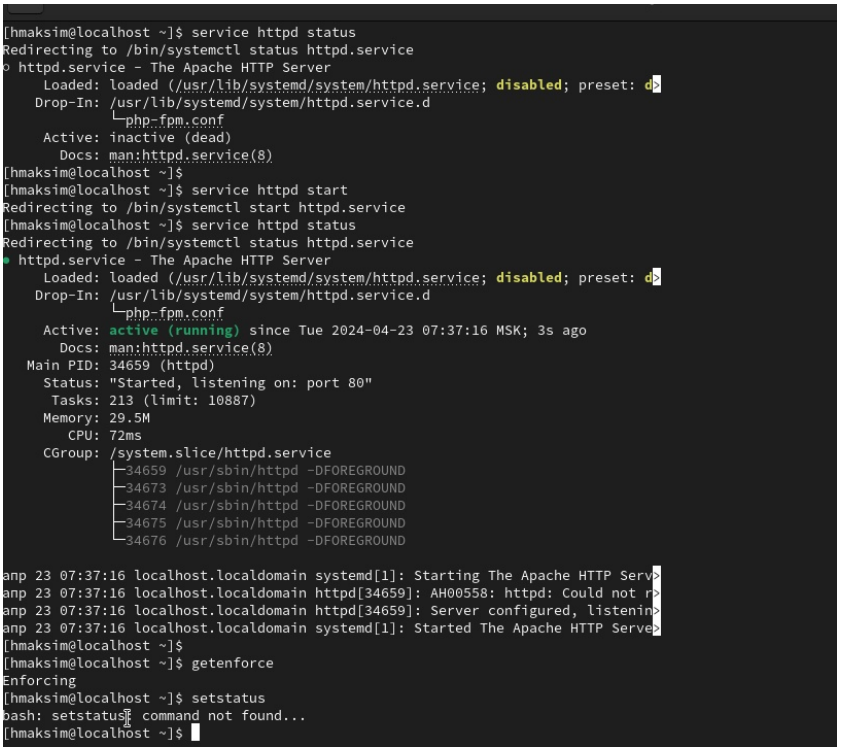

Рис. 3.1: Рис. 1

`sestatus -bigrep httpd`команда не работает

Устанавливаю seinfo и использую команду `seinfo`

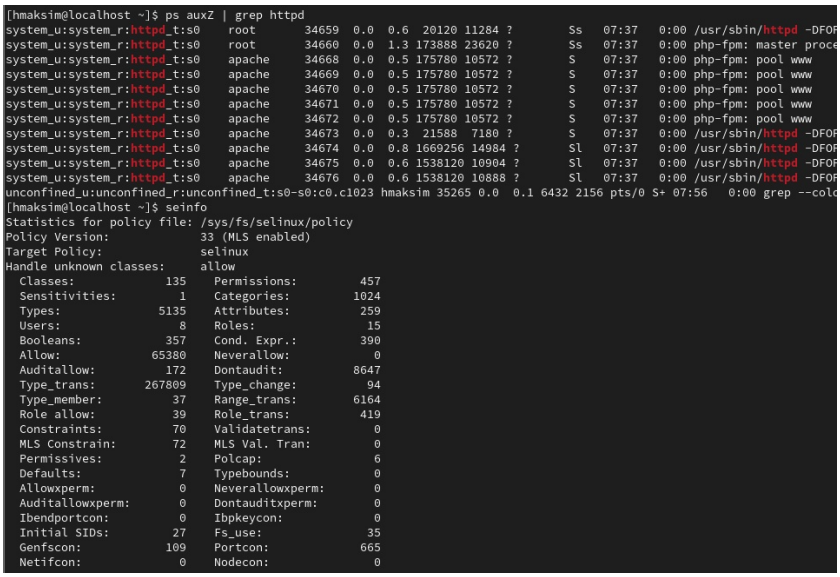

Рис. 3.2: Рис. 2

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: Это каталог
[hmaksim@localhost ~]$ ls -lZ /var/www/html
итого 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.