Презентация по лабораторной работе №6.

Информационная безопасность

Ле Тиен Винь

05 Октября 2024

Информация

- Ле Тиен Винь
- Студент
- Российский университет дружбы народов
- 1032215241@pfur.ru
- https://github.com/tvle2000/information

vinh

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
```

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

```
[root@ltvinh ~]$ getenforce
Enforcing
[root@ltvinh ~]$ 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@ltvinh ltvinh ]# 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
```

#

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

```
[root@ltvinh ltvinh]# sestatus -b | grep httpd
httpd_anon_write                            off
httpd_builtin_scripting                     on
httpd_can_check_spam                        off
httpd_can_connect_ftp                       off
httpd_can_connect_ldap                      off
httpd_can_connect_mythtv                    off
httpd_can_connect_zabbix                    off
httpd_can_manage_courier_spool              off
httpd_can_network_connect                   off
httpd_can_network_connect_cobbler           off
httpd_can_network_connect_db                off
httpd_can_network_memcache                  off
httpd_can_network_relay                     off
httpd_can_sendmail                          off
httpd_dbus_avahi                            off
httpd_dbus_sssd                             off
httpd_dontaudit_search_dirs                 off
httpd_enable_cgi                            on
httpd_enable_ftp_server                     off
httpd_enable_homedirs                       off
httpd_execmem                               off
httpd_graceful_shutdown                     off
httpd_manage_ipa                            off
httpd_mod_auth_ntlm_winbind                 off
httpd_mod_auth_pam                          off
httpd_read_user_content                     off
httpd_run_ipa                               off
httpd_run_preupgrade                        off
httpd_run_stickshift                        off
httpd_serve_cobbler_files                   off
httpd_setrlimit                             off
httpd_ssi_exec                              off
httpd_sys_script_anon_write                 off
httpd_tmp_exec                              off
httpd_tty_comm                              off
httpd_unified                               off
httpd_use_cifs                              off
httpd_use_fusefs                            off
httpd_use_gpg                               off
httpd_use_nfs                               off
httpd_use_opencryptoki                      off
httpd_use_openstack                         off
httpd_use_sasl                              off
httpd_verify_dns                            off
```

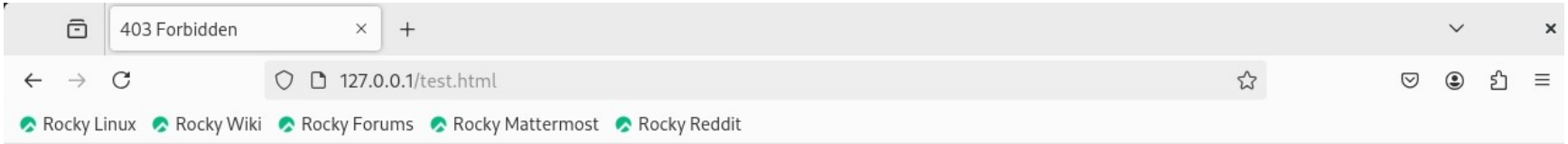
2. Выполнение работы

- 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

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



Forbidden

You don't have permission to access this resource.

Вывод

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