Лабораторная работа №6

Мандатное разграничение прав в Linux

Ким М. А.

14 октября 2023

Российский университет дружбы народов, Москва, Россия

Информация

Докладчик

- Ким Михаил Алексеевич
- студент уч. группы НФИбд-01-20
- Российский университет дружбы народов
- 1032201664@pfur.ru
- https://github.com/exmanka

Вводная часть

Актуальность

- Необходимость навыков работы с различными ОС, git, Markdown.

Объект и предмет исследования

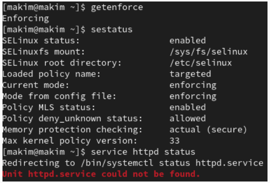
- Операционная система Rocky Linux
- SELinux
- Apache
- Язык разметки Markdown

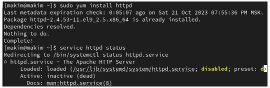
Цели и задачи

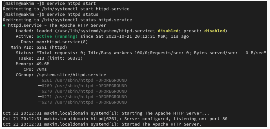
- Развитие навыков администрирования ОС Linux. Получение первого практического знакомства с технологией принудительного контроля доступа SELinux. Проверка работы SELinx на практике совместно с веб-сервером Apache.

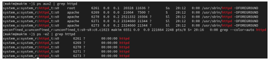
Процесс выполнения работы

Получение информации о работе SELinux. Установка и проверка Apache









Получение информации о работе Apache

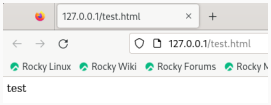
```
[makim@makim ~]$ sestatus -b httpd
SELinux status:                 enabled
SELinuxfs mount:                /sys/fs/selinux
SELinux root directory:         /etc/selinux
Loaded policy name:             targeted
Current mode:                   enforcing
Mode from config file:          enforcing
Policy 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
cron_userdomain_transition                  on
cups_execmem                                off
cvs_read_shadow                             off
daemons_dontaudit_scheduling                on
daemons_dump_core                           off
daemons_enable_cluster_mode                 off
daemons_use_tcp_wrapper                     off
daemons_use_tty                             off
```

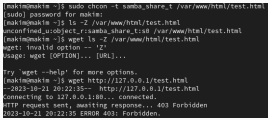
```
[makim@makim ~]$ setsfo
bash: setsfo: command not found...
Install package 'setools-console' to provide command 'setsfo'? [N/y] y

 * Waiting in queue...
The following packages have to be installed:
 setools-console-4.4.1-1.el9.x86_64     Policy analysis command-line tools for SELinux
Proceed with changes? [N/y] y

 * Waiting in queue...
 * Waiting for authentication...
 * Waiting in queue...
 * Downloading packages...
 * Requesting data...
 * Testing changes...
 * Installing packages...
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:             5109    Attributes:         258
  Users:                8    Roles:               14
  Booleans:           353    Cond. Expr.:        384
  Allow:            65008    Neverallow:           0
  Auditallow:         179    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:              32
  Genfscon:           103    Portcon:            660
  Netifcon:             0    Nodecon:              0

[makim@makim ~]$ setsfo
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:             5109    Attributes:         258
  Users:                8    Roles:               14
  Booleans:           353    Cond. Expr.:        384
  Allow:            65008    Neverallow:           0
  Auditallow:         179    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:              32
  Genfscon:           103    Portcon:            660
  Netifcon:             0    Nodecon:              0
```

```
[makim@makim ~]$ ls -lZ /var/www
total 0
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_script_exec_t:s0 6 May 16 23:21 cgi-bin
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:s0     6 May 16 23:21 html
[makim@makim ~]$ ls -lZ /var/www/html
total 0
[makim@makim ~]$ sudo nano /var/www/html/test.html
```

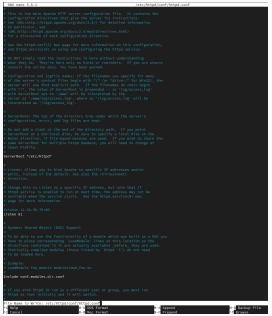
```
[makim@makim ~]$ ls -Z /var/www/html
unconfined_u:object_r:httpd_sys_content_t:s0 test.html
```

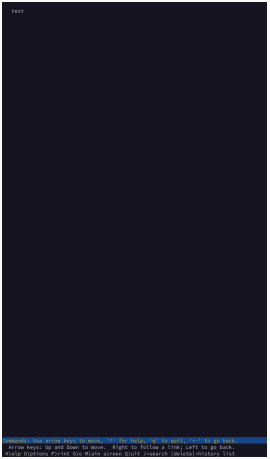
Отображение HTML-файла. Измение контекста файла. Просмотр логов



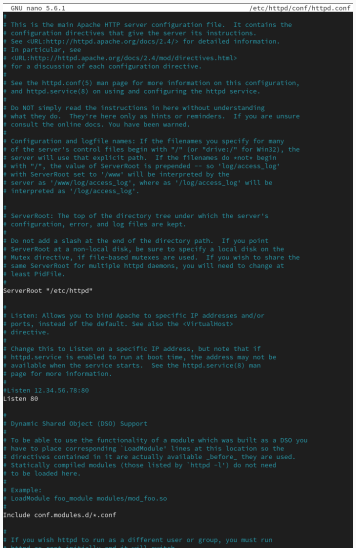


Изменение прослушиваемого TCP-порта для Apache





Обратное изменение прослушиваемого TCP-порта для Apache. Удаление созданных файлов



Результаты

Результаты

- Выполнены все необходимые задания.

Вывод

Развиты навыки администрирования ОС Linux. Получено первое практическое знакомство с технологией SELinux. Проверена работа SELinx на практике совместно с веб-сервером Apache.