

Лабораторная работа №6

Информационная безопасность

Аристова А. О.

11 октября 2024

Российский университет дружбы народов имени Патриса Лумумбы, Москва, Россия

- Аристова Арина Олеговна
- Студентка группы НФИбд-01-21
- Студ. билет 1032216433
- Российский университет дружбы народов имени Патриса Лумумбы

Цель лабораторной работы

- Развить навыки администрирования ОС Linux. Получить первое практическое знакомство с технологией SELinux1. Проверить работу SELinx на практике совместно с веб-сервером Apache

1. **SELinux (Security-Enhanced Linux)** обеспечивает усиление защиты путем внесения изменений как на уровне ядра, так и на уровне пространства пользователя, что превращает ее в действительно «непробиваемую» операционную систему

SELinux имеет три основных режим работы:

- **Enforcing:** режим по умолчанию. При выборе этого режима все действия, которые каким-то образом нарушают текущую политику безопасности, будут блокироваться, а попытка нарушения будет зафиксирована в журнале.
- **Permissive:** в случае использования этого режима, информация о всех действиях, которые нарушают текущую политику безопасности, будут зафиксированы в журнале, но сами действия не будут заблокированы.
- **Disabled:** полное отключение системы принудительного контроля доступа.

2. **Apache** — это свободное программное обеспечение, с помощью которого можно создать веб-сервер. Данный продукт возник как доработанная версия другого HTTP-клиента от национального центра суперкомпьютерных приложений (NCSA)

Для чего нужен Apache сервер:

- чтобы открывать динамические PHP-страницы,
- для распределения поступающей на сервер нагрузки,
- для обеспечения отказоустойчивости сервера,
- чтобы потренироваться в настройке сервера и запуске PHP-скриптов.

Ход выполнения лабораторной работы

Выполнение лабораторной работы

Убедились, что SELinux работает в режиме enforcing политики targeted

```
[mvmalashenko@mvmalashenko ~]$ cat /etc/httpd/httpd.conf
cat: /etc/httpd/httpd.conf: No such file or directory
[mvmalashenko@mvmalashenko ~]$ getenforce
Enforcing
[mvmalashenko@mvmalashenko ~]$ 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
```

Рис. 1: (рис. 1. Проверка режима enforcing политики targeted)

Обратились с помощью браузера к веб-серверу, запущенному на компьютере, и убедились, что последний работает

(рис. 2. Проверка работы веб-сервера)

Рис. 2: (рис. 2. Проверка работы веб-сервера)

Определили контекст безопасности веб-сервера Apache

```
[mmalashenko@mmalashenko ~]$ ps auxZ | grep httpd
system_u:system_r:httpd_t:s0 root      2906  0.1  0.2 20328 11588 ?        Ss   02:34   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache  2907  0.0  0.1 21664 7388 ?        S    02:34   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache  2908  0.0  0.4 2521332 19308 ?      Sl   02:34   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache  2909  0.0  0.5 2324660 21352 ?      Sl   02:34   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache  2910  0.0  0.5 2324660 21352 ?      Sl   02:34   0:00 /usr/sbin/httpd -DFOREGROUND
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 mmalas+ 3161  0.0  0.2 236220 9000 pts/0 T 02:34   0:00 /bin/systemctl status ht
tpd.service
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 mmalas+ 3175  0.0  0.0 221664 2256 pts/0 S+ 02:35   0:00 grep --color=auto httpd
[mmalashenko@mmalashenko ~]$
```

Рис. 3: (рис. 3. Контекст безопасности веб-сервера Apache)

Выполнение лабораторной работы

Посмотрели текущее состояние переключателей, многие из переключателей находятся в положении “off”

```
[mvmalashenko@mvmalashenko ~]$ sestatus -b httpd
SELinux status:                enabled
SELinuxfs mounts:              /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
awsstats_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
cobble_anon_write              off
cobble_can_network_connect     off
cobble_use_cifs                off
cobble_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_group         off
container_use_cephfs           off
container_use_devices          off
container_use_execvtsfs        off
```

Рис. 4: (рис. 4. Текущее состояние переключателей SELinux)

Выполнение лабораторной работы

Посмотрели статистику по политике. Множество пользователей - 8, ролей - 14, типов 5100

```
* 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:              5100 Attributes:       258
Users:              8    Roles:           14
Booleans:           353  Cond. Expr.:     384
Allow:              65000 Neverallow:       0
Auditallow:         170 Dontaudit:         8572
Type_trans:         265341 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:          35
Genfscon:           109  Portcon:         660
Netifcon:           0    Nodecon:         0
```

Рис. 5: (рис. 5. Статистика по политике)

Выполнение лабораторной работы

Посмотрели файлы и поддиректории, находящиеся в директории `/var/www`.
Определили, что в данной директории файлов нет. Только
владелец/суперпользователь может создавать файлы в директории
`/var/www/html`

```
[mvmalashenko@mvmalashenko ~]$ 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
[mvmalashenko@mvmalashenko ~]$ ls -lZ /var/www/html
total 0
```

Рис. 6: (рис. 6. Просмотр файлов и поддиректорий в директории `/var/www`)

От имени суперпользователя создали html-файл. Контекст созданного файла - httpd_sys_content_t

```
[mvmalashenko@mvmalashenko ~]$ su -  
Password:  
[root@mvmalashenko ~]# touch /var/www/html/test.html  
[root@mvmalashenko ~]# nano /var/www/html/test.html  
[root@mvmalashenko ~]# cat /var/www/html/test.html  
<html>  
<body>test</body>  
</html>  
[root@mvmalashenko ~]# su - mvmalashenko  
[mvmalashenko@mvmalashenko ~]$ ls -lZ /var/www/html  
total 4  
-rw-r--r--. 1 root root unconfined_u:object_r:httpd_sys_content_t:s0 33 Oct 13 02:43 test.html
```

Рис. 7: (рис. 7. Создание файла /var/www/html/test.html)

Выполнение лабораторной работы

Обратились к файлу через веб-сервер, введя в браузере адрес “http://127.0.0.1/test.html”. Файл был успешно отображен

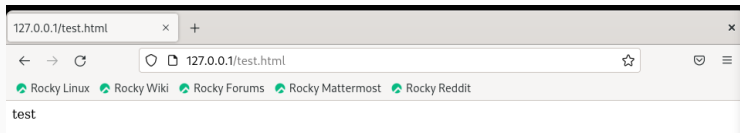


Рис. 8: (рис. 8. Обращение к файлу через веб-сервер)

Выполнение лабораторной работы

Изучив справку `httpd_selinux`, выяснили, какие контексты определены для файлов `httpd`.

Контекст моего файла - `httpd_sys_content_t` (в таком случае содержимое должно быть доступно для всех скриптов `httpd` и для самого демона).

Изменили контекст файла на `samba_share_t`

```
[mvmalashenko@mvmalashenko ~]$ ls -Z /var/www/html/test.html
unconfined_u:object_r:httpd_sys_content_t:s0 /var/www/html/test.html
[mvmalashenko@mvmalashenko ~]$ chcon -t samba_share_t /var/www/html/test.html
chcon: failed to change context of '/var/www/html/test.html' to 'unconfined_u:
object_r:samba_share_t:s0': Operation not permitted
[mvmalashenko@mvmalashenko ~]$ sudo chcon -t samba_share_t /var/www/html/test.
html
[sudo] password for mvmalashenko:
[mvmalashenko@mvmalashenko ~]$ chcon -t samba_share_t /var/www/html/test.html
[mvmalashenko@mvmalashenko ~]$ ls -Z /var/www/html/test.html
unconfined_u:object_r:samba_share_t:s0 /var/www/html/test.html
```

Рис. 9: (рис. 9. Изменение контекста)

Выполнение лабораторной работы

Попробовали еще раз получить доступ к файлу через веб-сервер, введя в браузере адрес “http://127.0.0.1/test.html” и получили сообщение об ошибке (т.к. кустановленному ранее контексту процесс httpd не имеет доступа)

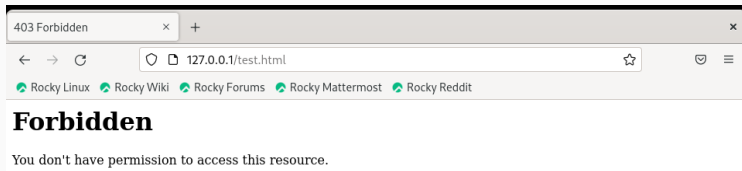


Рис. 10: (рис. 10. Обращение к файлу через веб-сервер)

Выполнение лабораторной работы

Убедились, что читать данный файл может любой пользователь.
Просмотрели системный лог-файл веб-сервера Apache, отображающий ошибки

```
[mmalashenko@mmalashenko ~]$ ls -l /var/www/html/test.html
-rw-r--r-- 1 root root 33 Oct 13 02:43 /var/www/html/test.html
[mmalashenko@mmalashenko ~]$ tail /var/log/messages
tail: cannot open '/var/log/messages' for reading: Permission denied
[mmalashenko@mmalashenko ~]$ sudo tail /var/log/messages
Oct 13 02:54:41 mmalashenko systemd[1]: Created slice Slice /system/dbus-1.1-org.fedoraproject.SetroubleshootPrivileged.
Oct 13 02:54:41 mmalashenko systemd[1]: Started dbus-1.1-org.fedoraproject.SetroubleshootPrivileged@0.service.
Oct 13 02:54:43 mmalashenko setroubleshoot[3995]: SELinux is preventing /usr/sbin/httpd from getattr access on the file /var/www/html/test.html. For complete SELinux messages run: sealert -l 32dcec71-a556-44ad-89a2-9c3f99d9d6d57
Oct 13 02:54:43 mmalashenko setroubleshoot[3995]: SELinux is preventing /usr/sbin/httpd from getattr access on the file /var/www/html/test.html.#012#012***** Plugin restorecon (02.2 confidence) suggests *****#012#012If you want to fix the label. #012/var/www/html/test.html default label should be httpd_sys_content_t.#012Then you can run restorecon. The access attempt may have been stopped due to insufficient permissions to access a parent directory in which case try to change the following command accordingly.#012Do#012# /sbin/restorecon -v /var/www/html/test.html#012#012***** Plugin public_content (7.83 confidence) suggests *****#012#012If you want to treat test.html as public content#012Then you need to change the label on test.html to public_content_t or public_content_rw_t.#012Do#012# semanage fcontext -a -t public_content_t '/var/www/html/test.html'#012# restorecon -v '/var/www/html/test.html'#012#012***** Plugin catchall (1.41 confidence) suggests *****#012#012If you believe that httpd should be allowed getattr access on the test.html file by default.#012Then you should report this as a bug.#012You can generate a local policy module to allow this access.#012Do#012allow this access for now by executing:#012# ausearch -c 'httpd' --raw | audit2allow -M my-httpd#012# semodule -X 300 -i my-httpd.pp#012
Oct 13 02:54:43 mmalashenko setroubleshoot[3995]: SELinux is preventing /usr/sbin/httpd from getattr access on the file /var/www/html/test.html. For complete SELinux messages run: sealert -l 32dcec71-a556-44ad-89a2-9c3f99d9d6d57
Oct 13 02:54:43 mmalashenko setroubleshoot[3995]: SELinux is preventing /usr/sbin/httpd from getattr access on the file /var/www/html/test.html.#012#012***** Plugin restorecon (02.2 confidence) suggests *****#012#012If you want to fix the label. #012/var/www/html/test.html default label should be httpd_sys_content_t.#012Then you can run restorecon. The access attempt may have been stopped due to insufficient permissions to access a parent directory in which case try to change the following command accordingly.#012Do#012# /sbin/restorecon -v /var/www/html/test.html#012#012***** Plugin public_content (7.83 confidence) suggests *****#012#012If you want to treat test.html as public content#012Then you need to change the label on test.html to public_content_t or public_content_rw_t.#012Do#012# semanage fcontext -a -t public_content_t '/var/www/html/test.html'#012# restorecon -v '/var/www/html/test.html'#012#012***** Plugin catchall (1.41 confidence) suggests *****#012#012If you believe that httpd should be allowed getattr access on the test.html file by default.#012Then you should report this as a bug.#012You can generate a local policy module to allow this access.#012Do#012allow this access for now by executing:#012# ausearch -c 'httpd' --raw | audit2allow -M my-httpd#012# semodule -X 300 -i my-httpd.pp#012
Oct 13 02:54:53 mmalashenko systemd[1]: dbus-1.1-org.fedoraproject.SetroubleshootPrivileged@0.service: Deactivated successfully.
Oct 13 02:54:53 mmalashenko systemd[1]: dbus-1.1-org.fedoraproject.SetroubleshootPrivileged@0.service: Consumed 1.87s CPU time.
Oct 13 02:54:53 mmalashenko systemd[1]: setroubleshootd.service: Deactivated successfully.
Oct 13 02:54:53 mmalashenko systemd[1]: setroubleshootd.service: Consumed 1.188s CPU time.
```

Выполнение лабораторной работы

В файле `/etc/httpd/conf/httpd.conf` заменили строчку “Listen 80” на “Listen 81”, чтобы установить веб-сервер Apache на прослушивание TCP-порта 81



```
mmmalashenko@mmmalashenko:~$ nano /etc/httpd/conf/httpd.conf
GNU nano 5.6.1 /etc/httpd/conf/httpd.conf Modified
#
ServerRoot "/etc/httpd"
#
# Listen: Allows you to bind Apache to specific IP addresses and/or
# ports, instead of the default. See also the <VirtualHost>
# directive.
#
# Change this to Listen on a specific IP address, but note that if
# httpd.service is enabled to run at boot time, the address may not be
# available when the service starts. See the httpd.service(8) man
# page for more information.
#
#Listen 12.34.56.78:80
Listen 81
#
# Dynamic Shared Object (DSO) Support
#
# To be able to use the functionality of a module which was built as a DSO you
# have to place corresponding 'LoadModule' lines at this location so the
# directives contained in it are actually available _before_ they are used.
# Statically compiled modules (those listed by 'httpd -l') do not need
# to be loaded here.
#
# Example:
# LoadModule foo_module modules/mod_foo.so
#
Include conf.modules.d/*.conf
#
# Help      ^O Write Out  ^W Where Is   ^K Cut        ^T Execute
# Exit      ^R Read File  ^\ Replace    ^U Paste      ^J Justify
```

Перезапускаем веб-сервер Apache и анализируем лог-файлы командой “tail -nl /var/log/messages”

```
[mvmalashenko@mvmalashenko ~]$ systemctl restart httpd
[mvmalashenko@mvmalashenko ~]$ tail -nl /var/log/messages
tail: invalid number of lines: 'l'
[mvmalashenko@mvmalashenko ~]$ tail -nl /var/log/messages
tail: cannot open '/var/log/messages' for reading: Permission denied
[mvmalashenko@mvmalashenko ~]$ sudo tail -nl /var/log/messages
Oct 13 03:03:22 mvmalashenko systemd[1]: fprintd.service: Deactivated successfully.
```

Рис. 13: (рис. 13. Перезапуск веб-сервера и анализ лог-файлов)

Выполнение лабораторной работы

Просмотрели файлы “var/log/http/error_log”, “/var/log/http/access_log” и “/var/log/audit/audit.log” и выяснили, что запись появилась в последнем файле

[illegible]

Выполнение лабораторной работы

Проверили список портов командой, убедились, что порт 81 есть в списке и запускаем веб-сервер Apache снова

```
[mvmalashenko@mvmalashenko ~]$ sudo semanage port -a -t http_port_t -p tcp 81
ValueError: Port tcp/81 already defined
[mvmalashenko@mvmalashenko ~]$ sudo 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
[mvmalashenko@mvmalashenko ~]$ systemctl restart httpd
[mvmalashenko@mvmalashenko ~]$ curl ifconfig.me
185.237.219.250[mvmalashenko@mvsystemctl status httpdctl status httpd
● httpd.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; enabled; preset: disabled)
   Active: active (running) since Fri 2023-10-13 03:18:59 EEST; 5min ago
     Docs: man:httpd.service(8)
  Main PID: 4563 (httpd)
    Status: "Total requests: 0; Idle/Busy workers 100/0; Requests/sec: 0; Bytes served/sec: 0"
    Tasks: 213 (limit: 24684)
   Memory: 43.3M
      CPU: 621ms
   CGroup: /system.slice/httpd.service
           └─4563 /usr/sbin/httpd -DFOREGROUND
             └─4564 /usr/sbin/httpd -DFOREGROUND
               └─4565 /usr/sbin/httpd -DFOREGROUND
                 └─4566 /usr/sbin/httpd -DFOREGROUND
                   └─4567 /usr/sbin/httpd -DFOREGROUND

Oct 13 03:18:59 mvmalashenko.localdomain systemd[1]: Starting The Apache HTTP Server...
Oct 13 03:18:59 mvmalashenko.localdomain systemd[1]: Started The Apache HTTP Server.
Oct 13 03:18:59 mvmalashenko.localdomain httpd[4563]: Server configured, listening on: port 81
lines 1-19/19 (END)
```

Вернули контекст “httpd_sys_content_t” файлу “/var/www/html/test.html” и попробовали получить доступ к файлу через веб-сервер, введя адрес “http://127.0.0.1:81/test.html”, увидели содержимое файла - слово “test”

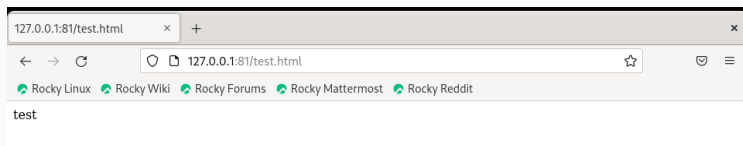


Рис. 16: (рис. 17. Обращение к файлу через веб-сервер)

Выполнение лабораторной работы

Исправили обратно конфигурационный файл apache, вернув “Listen 80”.
Попытались удалить привязку http_port к 81 порту, но этот порт определен на уровне политики, поэтому его нельзя удалить

```
[@vmalashenko@vmalashenko ~]$ nano /etc/httpd/conf/httpd.conf
[vmalashenko@vmalashenko ~]$ sudo semanage port -d -t http_port_t -p tcp 81
ValueError: Port tcp/81 is defined in policy, cannot be deleted
[vmalashenko@vmalashenko ~]$ sudo semanage port -l | grep http_port_t
http_port_t      tcp      80, 81, 443, 488, 8008, 8009, 8443, 9000
pegasus_http_port_t tcp      5985
[vmalashenko@vmalashenko ~]$ cat /etc/httpd/conf/httpd.conf
#
# This is the main Apache HTTP server configuration file. It contains the
# configuration directives that give the server its instructions.
# See http://httpd.apache.org/docs/2.4/ for detailed information.
# In particular, see
# http://httpd.apache.org/docs/2.4/mod/directives.html
# for a discussion of each configuration directive.
#
# See the httpd.conf(5) man page for more information on this configuration,
# and httpd.service(8) on using and configuring the httpd service.
#
# Do NOT simply read the instructions in here without understanding
# what they do. They're here only as hints or reminders. If you are unsure
# consult the online docs. You have been warned.
#
# Configuration and logfile names: If the filenames you specify for many
# of the server's control files begin with "/" (or "drive:/") for Win32), the
# server will use that explicit path. If the filenames do not begin
# with "/", the value of ServerRoot is prepended -- so 'log/access_log'
# with ServerRoot set to '/www' will be interpreted by the
# server as '/www/log/access_log', where as '/log/access_log' will be
# interpreted as '/log/access_log'.
#
#
# ServerRoot: The top of the directory tree under which the server's
# configuration, error, and log files are kept.
#
# Do not add a slash at the end of the directory path. If you point
# ServerRoot at a non-local disk, be sure to specify a local disk on the
# Mutex directive, if file-based mutexes are used. If you wish to share the
# same ServerRoot for multiple httpd daemons, you will need to change at
# least PidFile.
#
# ServerRoot "/etc/httpd"
#
# Listen: Allows you to bind Apache to specific IP addresses and/or
# ports, instead of the default. See also the VirtualHost
# directive.
#
# Change this to Listen on a specific IP address, but note that if
# httpd.service is enabled to run at boot time, the address may not be
# available when the service starts. See the httpd.service(8) man
# page for more information.
#
# Listen 12.34.56.78:80
Listen 80
```

Удалили файл “/var/www/html/test.html”

```
[mvmalashenko@mvmalashenko ~]$ sudo rm /var/www/html/test.html  
[mvmalashenko@mvmalashenko ~]$ ls /var/www/html/test.html  
ls: cannot access '/var/www/html/test.html': No such file or directory  
[mvmalashenko@mvmalashenko ~]$ ls /var/www/html
```

Рис. 18: (рис. 19. Удаление файла test.html)

Вывод

В ходе выполнения данной лабораторной работы были развиты навыки администрирования ОС Linux, получено первое практическое знакомство с технологией SELinux и проверена работа SELinux на практике совместно с веб-сервером Apache.

Список литературы. Библиография

0] Методические материалы курса

[1] SELinux: <https://habr.com/ru/companies/kingservers/articles/209644/>

[2] Apache: <https://2domains.ru/support/vps-i-servery/shto-takoye-apache>