

Отчёт по лабораторной работе №6

Информационная безопасность

Мандатное разграничение прав в Linux

Выполнила: Мальков Роман Сергеевич,
НФИбд-02-20, 1032217048

Содержание

Цель работы	4
Теоретическое введение	5
Выполнение лабораторной работы	7
Вывод	18
Список литературы. Библиография	19

Список иллюстраций

1	(рис. 1. Проверка режима enforcing политики targeted)	7
2	(рис. 2. Проверка работы веб-сервера)	8
3	(рис. 3. Контекст безопасности веб-сервера Apache)	8
4	(рис. 4. Текущее состояние переключателей SELinux)	9
5	(рис. 5. Статистика по политике)	10
6	(рис. 6. Просмотр файлов и поддиректорий в директории /var/www) . .	10
7	(рис. 7. Создание файла /var/www/html/test.html)	11
8	(рис. 8. Обращение к файлу через веб-сервер)	11
9	(рис. 9. Изменение контекста)	12
10	(рис. 10. Обращение к файлу через веб-сервер)	12
11	(рис. 11. Просмотр log-файла)	13
12	(рис. 12. Установка веб-сервера Apache на прослушивание TCP-порта 81)	14
13	(рис. 13. Перезапуск веб-сервера и анализ лог-файлов)	14
14	(рис. 14. Содержание файла var/log/audit/audit.log)	15
15	(рис. 15. Проверка установки порта 81)	16
16	(рис. 16. Возвращение исходного контекста файлу)	16
17	(рис. 17. Обращение к файлу через веб-сервер)	16
18	(рис. 18. Возвращение Listen 80 и попытка удалить порт 81)	17
19	(рис. 19. Удаление файла test.html)	17

Цель работы

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

Теоретическое введение

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. Впервые эта система появилась в четвертой версии CentOS, а в 5 и 6 версии реализация была существенно дополнена и улучшена.

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.

Политика SELinux определяет доступ пользователей к ролям, доступ ролей к доменам и доступ доменов к типам. Контекст безопасности — все атрибуты SELinux — роли, типы и домены. Более подробно см. в [1].

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.

Apache является кроссплатформенным ПО и поддерживает такие операционные системы, как Linux, BSD, MacOS, Microsoft, BeOS и другие.

Более подробно см. в [2].

Выполнение лабораторной работы

Вошли в систему под своей учетной записью и убедились, что SELinux работает в режиме enforcing политики targeted с помощью команд “getenforce” и “sestatus”

```
[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 с помощью команды “service httpd status”

```
Complete!
[mvmalashenko@mvmalashenko ~]$ sudo systemctl start httpd
[mvmalashenko@mvmalashenko ~]$ sudo systemctl enable httpd
Created symlink /etc/systemd/system/multi-user.target.wants/httpd.service → /usr/lib/systemd/system/httpd.service.
[mvmalashenko@mvmalashenko ~]$ service httpd status
Redirecting to /bin/systemctl status httpd.service
● httpd.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; enabled; preset: >
   Active: active (running) since Fri 2023-10-13 02:34:11 EEST; 19s ago
     Docs: man:httpd.service(8)
   Main PID: 2906 (httpd)
   Status: "Total requests: 0; Idle/Busy workers 100/0;Requests/sec: 0; Byt>
     Tasks: 213 (limit: 24684)
    Memory: 49.7M
       CPU: 266ms
    CGroup: /system.slice/httpd.service
           └─2906 /usr/sbin/httpd -DFOREGROUND
             └─2907 /usr/sbin/httpd -DFOREGROUND
               └─2908 /usr/sbin/httpd -DFOREGROUND
                 └─2909 /usr/sbin/httpd -DFOREGROUND
                   └─2910 /usr/sbin/httpd -DFOREGROUND

Oct 13 02:34:10 mvmalashenko.localdomain systemd[1]: Starting The Apache HTTP>
Oct 13 02:34:11 mvmalashenko.localdomain systemd[1]: Started The Apache HTTP >
Oct 13 02:34:11 mvmalashenko.localdomain httpd[2906]: Server configured, list>
lines 1-19/19 (END)
```

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

С помощью команды “ps auxZ | grep httpd” определили контекст безопасности веб-сервера Apache - httpd_t

```
[mvmalashenko@mvmalashenko ~]$ 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 mvmalas+ 3175 0.0  0.0 221664 2256 pts/0 S+  02:35   0:00 grep --color=auto httpd
[mvmalashenko@mvmalashenko ~]$
```

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

Посмотрели текущее состояние переключателей SELinux для Apache с помощью команды “sestatus -bigrep httpd”, многие из переключателей находятся в положении “off”


```

[mvmalashenko@mvmalashenko ~]$ 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

```

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

Посмотрели статистику по политике с помощью команды “seinfo”. 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)

С помощью команды “ls -lZ /var/www” посмотрели файлы и поддиректории, находящиеся в директории /var/www. Используя команду “ls -lZ /var/www/html”, 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 /var/www/html/test.html. Контекст со-

данного 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)

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

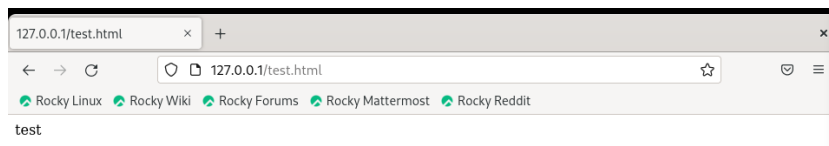


Рис. 8: (рис. 8. Обращение к файлу через веб-сервер)

Изучив справку `man httpd_selinux`, выяснили, что для `httpd` определены следующие контексты файлов:

`httpd_sys_content_t`, `httpd_sys_script_exec_t`,
`httpd_sys_script_ro_t`, `httpd_sys_script_rw_t`,
`httpd_sys_script_ra_t`, `httpd_unconfined_script_exec_t`.

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` командой “`sudo chcon -t samba_share_t /var/www/html/test.html`” и проверили, что контекст поменялся

```
[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)

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. к установленному ранее контексту процесс httpd не имеет доступа)

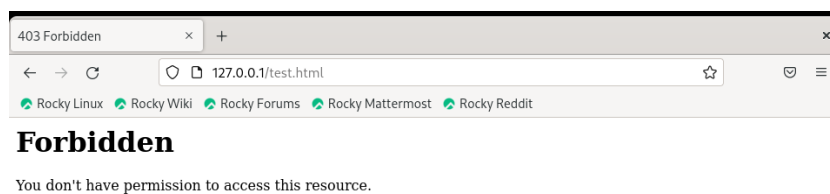


Рис. 10: (рис. 10. Обращение к файлу через веб-сервер)

Командой “ls -l /var/www/html/test.html” убедились, что читать данный файл может любой пользователь. Просмотрели системный лог-файл веб-сервера Apache командой “sudo tail /var/log/messages”, отображающий ошибки

```

[mvmalashenko@mvmalashenko ~]$ ls -l /var/www/html/test.html
-rw-r--r--. 1 root root 33 Oct 13 02:43 /var/www/html/test.html
[mvmalashenko@mvmalashenko ~]$ tail /var/log/messages
tail: cannot open '/var/log/messages' for reading: Permission denied
[mvmalashenko@mvmalashenko ~]$ sudo tail /var/log/messages
Oct 13 02:54:41 mvmalashenko systemd[1]: Created slice Slice /system/dbus-:1.1-org.fedoraproject.SetroubleshootPrivileged.
Oct 13 02:54:41 mvmalashenko systemd[1]: Started dbus-:1.1-org.fedoraproject.SetroubleshootPrivileged@0.service.
Oct 13 02:54:43 mvmalashenko 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-a556-44a0-89a2-9c3f09d96d57
Oct 13 02:54:43 mvmalashenko setroubleshoot[3995]: SELinux is preventing /usr/sbin/httpd from getattr access on the file /var/www/html/test.html.#012#012***** Plugin restorecon (92.2 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 mvmalashenko 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-a556-44a0-89a2-9c3f09d96d57
Oct 13 02:54:43 mvmalashenko setroubleshoot[3995]: SELinux is preventing /usr/sbin/httpd from getattr access on the file /var/www/html/test.html.#012#012***** Plugin restorecon (92.2 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 mvmalashenko systemd[1]: dbus-:1.1-org.fedoraproject.SetroubleshootPrivileged@0.service: Deactivated successfully.
Oct 13 02:54:53 mvmalashenko systemd[1]: dbus-:1.1-org.fedoraproject.SetroubleshootPrivileged@0.service: Consumed 1.817s CPU time.
Oct 13 02:54:53 mvmalashenko systemd[1]: setroubleshootd.service: Deactivated successfully.
Oct 13 02:54:53 mvmalashenko systemd[1]: setroubleshootd.service: Consumed 1.188s CPU time.

```

Рис. 11: (рис. 11. Просмотр log-файла)

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



Рис. 12: (рис. 12. Установка веб-сервера Apache на прослушивание TCP-порта 81)

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

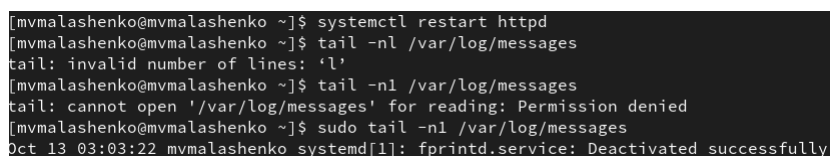


Рис. 13: (рис. 13. Перезапуск веб-сервера и анализ лог-файлов)

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

```
mvmlashenko@mvmlashenko:~  
type=USER_START msg=audit(1697155533.240:287): pid=4381 uid=1000 audit=1000 ses=3 subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0-  
1023 msg=op=PAM:session_open grantors=pam_keyinit,pam_limits,pam_systemd,pam_unix acct="root" exe="/usr/bin/sudo" hostname=? addr=? t  
terminal=/dev/pts/0 res=success'UID="mvmlashenko" AUDID="mvmlashenko"  
type=USER_END msg=audit(1697155533.245:288): pid=4381 uid=1000 audit=1000 ses=3 subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0-  
1023 msg=op=PAM:session_close grantors=pam_keyinit,pam_limits,pam_systemd,pam_unix acct="root" exe="/usr/bin/sudo" hostname=? addr=? t  
terminal=/dev/pts/0 res=success'UID="mvmlashenko" AUDID="mvmlashenko"  
type=CRED_DISP msg=audit(1697155533.245:289): pid=4381 uid=1000 audit=1000 ses=3 subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0-  
1023 msg=op=PAM:setcred grantors=pam_env,pam_fprintd acct="root" exe="/usr/bin/sudo" hostname=? addr=? terminal=/dev/pts/0 res=succes  
s'UID="mvmlashenko" AUDID="mvmlashenko"  
type=SERVICE_START msg=audit(1697155572.643:290): pid=1 uid=0 audit=4294967295 ses=4294967295 subj=system_u:system_r:init_t:s0 msg=unit  
d=dnf-makecache comm="systemd" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=success'UID="root" AUDID="unset"  
type=SERVICE_STOP msg=audit(1697155572.643:291): pid=1 uid=0 audit=4294967295 ses=4294967295 subj=system_u:system_r:init_t:s0 msg=unit  
d=dnf-makecache comm="systemd" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=success'UID="root" AUDID="unset"  
type=USER_ACT msg=audit(1697155678.271:292): pid=4406 uid=1000 audit=1000 ses=3 subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0-  
1023 msg=op=PAM:accounting grantors=pam_unix,pam_localuser acct="mvmlashenko" exe="/usr/bin/sudo" hostname=? addr=? terminal=/dev/pt  
s/0 res=success'UID="mvmlashenko" AUDID="mvmlashenko"  
type=USER_CMD msg=audit(1697155678.272:293): pid=4406 uid=1000 audit=1000 ses=3 subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0-  
1023 msg=cmd="/home/mvmlashenko" cmd=636174202f7661722f6c6f672f61756469742f61756469742e6c6f67 exe="/usr/bin/sudo" terminal=pts/0 res=  
success'UID="mvmlashenko" AUDID="mvmlashenko"  
type=CRED_REF msg=audit(1697155678.273:294): pid=4406 uid=1000 audit=1000 ses=3 subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0-  
1023 msg=op=PAM:setcred grantors=pam_env,pam_fprintd acct="root" exe="/usr/bin/sudo" hostname=? addr=? terminal=/dev/pts/0 res=succes  
s'UID="mvmlashenko" AUDID="mvmlashenko"  
type=USER_START msg=audit(1697155678.278:295): pid=4406 uid=1000 audit=1000 ses=3 subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0-  
1023 msg=op=PAM:session_open grantors=pam_keyinit,pam_limits,pam_systemd,pam_unix acct="root" exe="/usr/bin/sudo" hostname=? addr=? t  
terminal=/dev/pts/0 res=success'UID="mvmlashenko" AUDID="mvmlashenko"  
type=USER_END msg=audit(1697155678.467:296): pid=4406 uid=1000 audit=1000 ses=3 subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0-  
1023 msg=op=PAM:session_close grantors=pam_keyinit,pam_limits,pam_systemd,pam_unix acct="root" exe="/usr/bin/sudo" hostname=? addr=? t  
terminal=/dev/pts/0 res=success'UID="mvmlashenko" AUDID="mvmlashenko"  
type=CRED_DISP msg=audit(1697155678.467:297): pid=4406 uid=1000 audit=1000 ses=3 subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0-  
1023 msg=op=PAM:setcred grantors=pam_env,pam_fprintd acct="root" exe="/usr/bin/sudo" hostname=? addr=? terminal=/dev/pts/0 res=succes  
s'UID="mvmlashenko" AUDID="mvmlashenko"  
type=USER_ACT msg=audit(1697155776.505:298): pid=4445 uid=1000 audit=1000 ses=3 subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0-  
1023 msg=op=PAM:accounting grantors=pam_unix,pam_localuser acct="mvmlashenko" exe="/usr/bin/sudo" hostname=? addr=? terminal=/dev/pt  
s/0 res=success'UID="mvmlashenko" AUDID="mvmlashenko"  
type=USER_CMD msg=audit(1697155776.505:299): pid=4445 uid=1000 audit=1000 ses=3 subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0-  
1023 msg=cmd="/home/mvmlashenko" cmd=636174202f7661722f6c6f672f61756469742f61756469742e6c6f67 exe="/usr/bin/sudo" terminal=pts/0 res=  
success'UID="mvmlashenko" AUDID="mvmlashenko"  
type=CRED_REF msg=audit(1697155776.506:300): pid=4445 uid=1000 audit=1000 ses=3 subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0-  
1023 msg=op=PAM:setcred grantors=pam_env,pam_fprintd acct="root" exe="/usr/bin/sudo" hostname=? addr=? terminal=/dev/pts/0 res=succes  
s'UID="mvmlashenko" AUDID="mvmlashenko"  
type=USER_START msg=audit(1697155776.519:301): pid=4445 uid=1000 audit=1000 ses=3 subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0-  
1023 msg=op=PAM:session_open grantors=pam_keyinit,pam_limits,pam_systemd,pam_unix acct="root" exe="/usr/bin/sudo" hostname=? addr=? t  
terminal=/dev/pts/0 res=success'UID="mvmlashenko" AUDID="mvmlashenko"  
type=USER_END msg=audit(1697155776.693:302): pid=4445 uid=1000 audit=1000 ses=3 subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0-  
1023 msg=op=PAM:session_close grantors=pam_keyinit,pam_limits,pam_systemd,pam_unix acct="root" exe="/usr/bin/sudo" hostname=? addr=? t  
terminal=/dev/pts/0 res=success'UID="mvmlashenko" AUDID="mvmlashenko"  
type=CRED_DISP msg=audit(1697155776.693:303): pid=4445 uid=1000 audit=1000 ses=3 subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0-  
1023 msg=op=PAM:setcred grantors=pam_env,pam_fprintd acct="root" exe="/usr/bin/sudo" hostname=? addr=? terminal=/dev/pts/0 res=succes  
s'UID="mvmlashenko" AUDID="mvmlashenko"  
type=USER_ACT msg=audit(1697155883.681:304): pid=4451 uid=1000 audit=1000 ses=3 subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0-  
1023 msg=op=PAM:accounting grantors=pam_unix,pam_localuser acct="mvmlashenko" exe="/usr/bin/sudo" hostname=? addr=? terminal=/dev/pt  
s/0 res=success'UID="mvmlashenko" AUDID="mvmlashenko"  
type=USER_CMD msg=audit(1697155883.681:305): pid=4451 uid=1000 audit=1000 ses=3 subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0-  
1023 msg=cmd="/home/mvmlashenko" cmd=636174202f7661722f6c6f672f61756469742f61756469742e6c6f67 exe="/usr/bin/sudo" terminal=pts/0 res=  
success'UID="mvmlashenko" AUDID="mvmlashenko"  
type=CRED_REF msg=audit(1697155883.682:306): pid=4451 uid=1000 audit=1000 ses=3 subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0-  
1023 msg=op=PAM:setcred grantors=pam_env,pam_fprintd acct="root" exe="/usr/bin/sudo" hostname=? addr=? terminal=/dev/pts/0 res=succes  
s'UID="mvmlashenko" AUDID="mvmlashenko"  
type=USER_START msg=audit(1697155883.688:307): pid=4451 uid=1000 audit=1000 ses=3 subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0-  
1023 msg=op=PAM:session_open grantors=pam_keyinit,pam_limits,pam_systemd,pam_unix acct="root" exe="/usr/bin/sudo" hostname=? addr=? t  
terminal=/dev/pts/0 res=success'UID="mvmlashenko" AUDID="mvmlashenko"  
[mvmlashenko@mvmlashenko ~]$
```

Рис. 14: (рис. 14. Содержание файла var/log/audit/audit.log)

Выполнили команду “semanage port -a -t http_port_t -p tcp 81” и убедились, что порт TCP-81 установлен. Проверили список портов командой “semanage port -l | grep http_port_t”, 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@mvmalashenko ~]$ systemctl 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)
```

Рис. 15: (рис. 15. Проверка установки порта 81)

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

```
[mvmalashenko@mvmalashenko ~]$ sudo chcon -t httpd_sys_content_t /var/www/html/test.html
[sudo] password for mvmalashenko:
[mvmalashenko@mvmalashenko ~]$ ls -Z /var/www/html/test.html
unconfined_u:object_r:httpd_sys_content_t:s0 /var/www/html/test.html
```

Рис. 16: (рис. 16. Возвращение исходного контекста файлу)

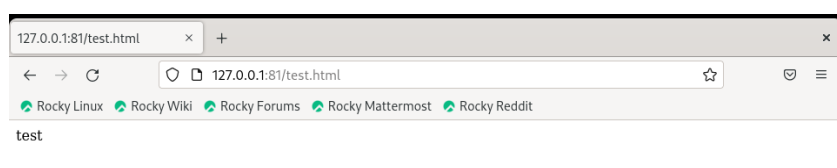


Рис. 17: (рис. 17. Обращение к файлу через веб-сервер)

Исправили обратно конфигурационный файл apache, вернув “Listen 80”. Попытались удалить привязку http_port к 81 порту командой “semanage port -d -t http_port_t -p tcp 81”, но этот порт определен на уровне политики, поэтому его нельзя удалить


```

[mvmalashenko@mvmalashenko ~]$ nano /etc/httpd/conf/httpd.conf
[mvmalashenko@mvmalashenko ~]$ sudo semanage port -d -t http_port_t -p tcp 81
ValueError: Port tcp/81 is defined in policy, cannot be deleted
[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 ~]$ 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 <URL:http://httpd.apache.org/docs/2.4/> for detailed information.
# In particular, see
# <URL: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

```

Рис. 18: (рис. 18. Возвращение Listen 80 и попытка удалить порт 81)

Удалили файл “/var/www/html/test.html” командой “rm /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. 19: (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>