

Шаблон отчёта по лабораторной работе

Лабораторная работа № 6

Мерич Дорук Каймакджыоглу

Содержание

Цель работы	1
Задание.....	1
Выполнение лабораторной работы	1
Выводы.....	7
Список литературы.....	7

Цель работы

Мандатное разграничение прав в Linux.

Задание

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

Выполнение лабораторной работы

1. Войдите в систему с полученными учётными данными и убедитесь, что SELinux работает в режиме enforcing политики targeted с помощью команд

```
[mericdoruk@localhost ~]$ getenforce
Enforcing
[mericdoruk@localhost ~]$ 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
[mericdoruk@localhost ~]$
```

getenforce и sestatus.

2. Обратитесь с помощью браузера к веб-серверу, запущенному на вашем компьютере, и убедитесь, что последний работает: `service httpd status` или `/etc/rc.d/init.d/httpd status` Если не работает, запустите его так же, но с

```
mericdoruk@localhost:/home/mericdoruk — /bin/systemctl sta...
[root@localhost mericdoruk]# 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: disabled)
   Active: active (running) since Fri 2023-10-13 23:08:54 MSK; 21s ago
     Docs: man:httpd.service(8)
   Main PID: 45435 (httpd)
   Status: "Total requests: 0; Idle/Busy workers 100/0; Requests/sec: 0; Bytes served: 0"
   Tasks: 213 (limit: 10902)
  Memory: 23.3M
    CPU: 71ms
   CGroup: /system.slice/httpd.service
           └─45435 /usr/sbin/httpd -DFOREGROUND
             └─45436 /usr/sbin/httpd -DFOREGROUND
               └─45440 /usr/sbin/httpd -DFOREGROUND
                 └─45441 /usr/sbin/httpd -DFOREGROUND
                   └─45442 /usr/sbin/httpd -DFOREGROUND

Oct 13 23:08:54 localhost.localdomain systemd[1]: Starting The Apache HTTP Server: httpd.
Oct 13 23:08:54 localhost.localdomain httpd[45435]: AH00558: httpd: Could not reliably ope
Oct 13 23:08:54 localhost.localdomain systemd[1]: Started The Apache HTTP Server: httpd.
Oct 13 23:08:54 localhost.localdomain httpd[45435]: Server configured, listening on: 192.168.1.1
lines 1-20/20 (END)
```

параметром `start`.

3. Найдите веб-сервер Apache в списке процессов, определите его контекст безопасности и занесите эту информацию в отчёт. Например, можно использовать команду `ps auxZ | grep httpd` или `ps -eZ | grep httpd`

```
mericdoruk@localhost:/home/mericdoruk
[root@localhost mericdoruk]# ps auxZ | grep httpd
system_u:system_r:httpd_t:s0 root 45435 0.0 0.6 20128 11452 ?
Ss 23:08 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 45436 0.0 0.4 21612 7248 ?
S 23:08 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 45440 0.0 0.7 1210520 13036 ?
Sl 23:08 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 45441 0.0 0.6 1079384 10988 ?
Sl 23:08 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 45442 0.0 0.6 1079384 10988 ?
Sl 23:08 0:00 /usr/sbin/httpd -DFOREGROUND
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 root 45689 0.0 0.1 221664
2252 pts/0 S+ 23:10 0:00 grep --color=auto httpd
[root@localhost mericdoruk]#
```

4. Посмотрите текущее состояние переключателей SELinux для Apache с помощью команды `sestatus -bigrep httpd` Обратите внимание, что многие из них находятся в положении «off».

5. Посмотрите статистику по политике с помощью команды `seinfo`, также определите множество пользователей, ролей, типов.

```
mericdoruk@localhost:/home/mericdoruk
Policy Version:      33 (MLS enabled)
Target Policy:       selinux
Handle unknown classes: allow
Classes:             135   Permissions:           457
Sensitivities:       1     Categories:           1024
Types:               5135  Attributes:            259
Users:               8     Roles:                 15
Booleans:            357   Cond. Expr.:          390
Allow:               65381 Neverallow:             0
Auditallow:          172  Dontaudit:             8647
Type_trans:          267809 Type_change:            94
Type_member:          37   Range_trans:           6164
Role allow:           39   Role_trans:            419
Constraints:          70  Validatetrans:          0
MLS Constrains:       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:                 665
Netifcon:             0   Nodecon:                 0
[root@localhost mericdoruk]#
```

6. Определите тип файлов и поддиректорий, находящихся в директории `/var/www`, с помощью команды `ls -lZ /var/www`
7. Определите тип файлов, находящихся в директории `/var/www/html`: `ls -lZ`

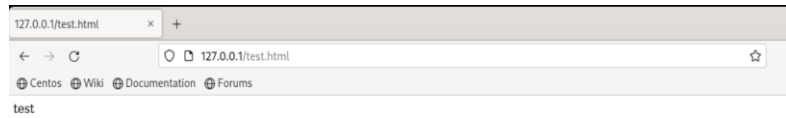
```
[root@localhost mericdoruk]# ls -lZ /var/www
total 0
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_script_exec_t:s0 6 Jul 20 11
:44 cgi-bin
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:s0 6 Jul 20 11
:44 html
/var/www/html [root@localhost mericdoruk]#
```

8. Определите круг пользователей, которым разрешено создание файлов в директории `/var/www/html`.
9. Создайте от имени суперпользователя (так как в дистрибутиве после установки только ему разрешена запись в директорию) html-файл `/var/www/html/test.html` следующего содержания:
10. Проверьте контекст созданного вами файла. Занесите в отчёт контекст, присваиваемый по умолчанию вновь созданным файлам в директории

```
[mericdoruk@localhost ~]$ cd /var/www/html
[mericdoruk@localhost html]$ touch test.html
touch: cannot touch 'test.html': Permission denied
[mericdoruk@localhost html]$ su
Password:
[root@localhost html]# touch test.html
[root@localhost html]# ls
test.html
[root@localhost html]# vim test.html
[root@localhost html]# cat test.html
[root@localhost html]# vim test.html
[root@localhost html]# cat test.html
<html><body>test</body></html>
[root@localhost html]#
```

/var/www/html.

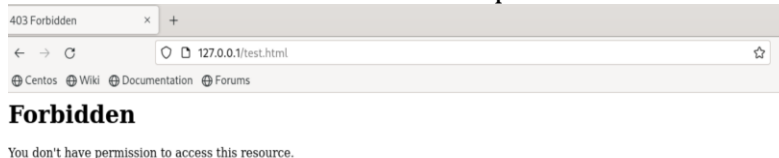
11. Обратитесь к файлу через веб-сервер, введя в браузере адрес `http://127.0.0.1/test.html`. Убедитесь, что файл был успешно отображён.



- файл не отображён
12. Изучите справку `man httpd_selinux` и выясните, какие контексты файлов определены для `httpd`. Сопоставьте их с типом файла `test.html`. Проверить контекст файла можно командой `ls -Z. ls -Z /var/www/html/test.html`
13. Измените контекст файла `/var/www/html/test.html` с `httpd_sys_content_t` на любой другой, к которому процесс `httpd` не должен иметь доступа, например, на `samba_share_t`: `chcon -t samba_share_t /var/www/html/test.html` `ls -Z /var/www/html/test.html` После этого проверьте, что контекст поменялся.

```
[root@localhost html]# man httpd_selinux
No manual entry for httpd_selinux
[root@localhost html]# ls -Z /var/www/html/test.html
unconfined_u:object_r:httpd_sys_content_t:s0 /var/www/html/test.html
[root@localhost html]# su mericdoruk
[mericdoruk@localhost html]$ ls -Z /var/www/html/test.html
unconfined_u:object_r:httpd_sys_content_t:s0 /var/www/html/test.html
[mericdoruk@localhost html]$ man httpd_selinux
No manual entry for httpd_selinux
[mericdoruk@localhost html]$ chcon -t samba_share_t /var/www/html/test.html
chcon: failed to change context of '/var/www/html/test.html' to 'unconfined_u:ob
ject_r:samba_share_t:s0': Operation not permitted
[mericdoruk@localhost html]$ su
Password:
[root@localhost html]# chcon -t samba_share_t /var/www/html/test.html
[root@localhost html]#
```

14. Попробуйте ещё раз получить доступ к файлу через веб-сервер, введя в браузере адрес `http://127.0.0.1/test.html`. Вы должны получить сообщение об ошибке: `Forbidden You don't have permission to access /test.html on this server.`

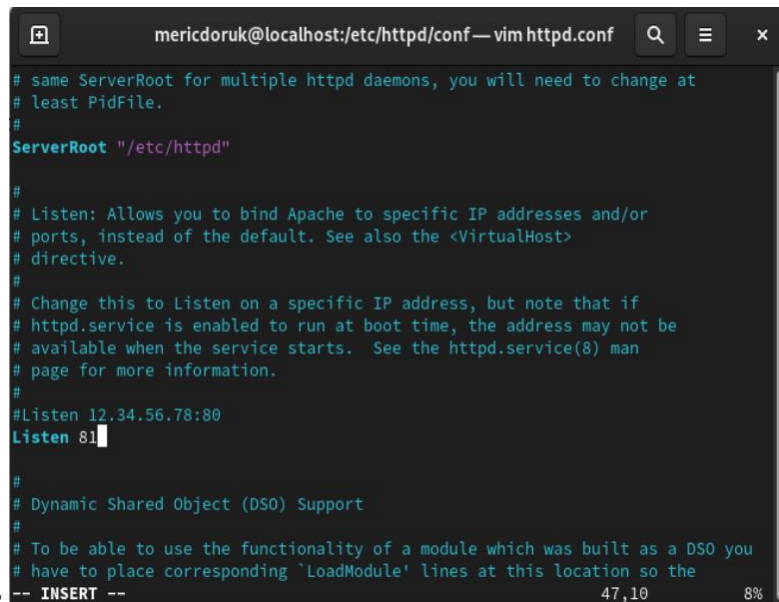


15. Проанализируйте ситуацию. `ls -l /var/www/html/test.html` Просмотрите log-файлы веб-сервера Apache. Также просмотрите системный лог-файл: `tail`

```
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_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 23:25:41 localhost systemd[1]: dbus-:1.1-org.fedoraproject.SetroubleshootPrivileged@0.service: Deactivated successfully.
Oct 13 23:25:41 localhost systemd[1]: dbus-:1.1-org.fedoraproject.SetroubleshootPrivileged@0.service: Consumed 2.365s CPU time.
Oct 13 23:25:41 localhost systemd[1]: setroubleshootd.service: Deactivated successfully.
Oct 13 23:26:50 localhost systemd[1]: Starting Fingerprint Authentication Daemon ...
Oct 13 23:26:50 localhost systemd[1]: Started Fingerprint Authentication Daemon.
Oct 13 23:26:52 localhost su[47278]: (to root) mericdoruk on pts/0
[root@localhost html]#
```

`/var/log/messages`

16. Попробуйте запустить веб-сервер Apache на прослушивание TCP-порта 81 (а не 80, как рекомендует IANA и прописано в `/etc/services`). Для этого в файле `/etc/httpd/httpd.conf` найдите строчку `Listen 80` и замените её на `Listen 81`.



```
mericdoruk@localhost:/etc/httpd/conf — vim httpd.conf
# 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 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
-- INSERT --
```

- файл пуст

17. Выполните перезапуск веб-сервера Apache.
18. Проанализируйте лог-файлы: `tail -nl /var/log/messages` Просмотрите файлы `/var/log/http/error_log`, `/var/log/http/access_log` и `/var/log/audit/audit.log` и выясните, в каких файлах появились записи.

```
mericdoruk@localhost:/var/log/httpd — vim access_log
127.0.0.1 - - [13/Oct/2023:23:20:59 +0300] "GET /test.html HTTP/1.1" 200 31 "-"
"Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0"
127.0.0.1 - - [13/Oct/2023:23:20:59 +0300] "GET /favicon.ico HTTP/1.1" 404 196 "
http://127.0.0.1/test.html" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/201
00101 Firefox/102.0"
127.0.0.1 - - [13/Oct/2023:23:25:26 +0300] "GET /test.html HTTP/1.1" 403 199 "-"
"Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0"
127.0.0.1 - - [13/Oct/2023:23:25:27 +0300] "GET /favicon.ico HTTP/1.1" 404 196 "
http://127.0.0.1/test.html" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/201
00101 Firefox/102.0"
```

```
mericdoruk@localhost:/var/log/httpd — vim error_log
[Fri Oct 13 23:08:54.783502 2023] [core:notice] [pid 45435:tid 45435] SELinux po
licy enabled; httpd running as context system_u:system_r:httpd_t:s0
[Fri Oct 13 23:08:54.785499 2023] [suexec:notice] [pid 45435:tid 45435] AH01232:
suEXEC mechanism enabled (wrapper: /usr/sbin/suexec)
AH00558: httpd: Could not reliably determine the server's fully qualified domain
name, using localhost.localdomain. Set the 'ServerName' directive globally to s
uppress this message
[Fri Oct 13 23:08:54.798545 2023] [lbmethod_heartbeat:notice] [pid 45435:tid 454
35] AH02282: No slotmem from mod_heartbeat
[Fri Oct 13 23:08:54.809201 2023] [mpm_event:notice] [pid 45435:tid 45435] AH004
89: Apache/2.4.57 (CentOS Stream) configured -- resuming normal operations
[Fri Oct 13 23:08:54.809228 2023] [core:notice] [pid 45435:tid 45435] AH00094: C
ommand line: '/usr/sbin/httpd -D FOREGROUND'
[Fri Oct 13 23:25:26.652245 2023] [core:error] [pid 45442:tid 45630] (13)Permiss
ion denied: [client 127.0.0.1:45718] AH00035: access to /test.html denied (files
ystem path '/var/www/html/test.html') because search permissions are missing on
a component of the path
```

```
mericdoruk@localhost:/var/log/audit — vim audit.log
type=DAEMON_START msg=audit(1694533504.236:5182): op=start ver=3.0.7 format=enri
ched kernel=5.14.0-362.el9.x86_64 auid=4294967295 pid=693 uid=0 ses=4294967295 s
ubj=system_u:system_r:auditd_t:s0 res=success^]AUID="unset" UID="root"
type=SERVICE_START msg=audit(1694533504.283:5): pid=1 uid=0 auid=4294967295 ses=
4294967295 subj=system_u:system_r:init_t:s0 msg='unit=systemd-journal-catalog-up
date comm="systemd" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=?
res=success^]AUID="root" AUID="unset"
type=CONFIG_CHANGE msg=audit(1694533504.328:6): op=set audit_backlog_limit=8192
old=64 auid=4294967295 ses=4294967295 subj=system_u:system_r:unconfined_service_
t:s0 res=1^]AUID="unset"
type=SYSCALL msg=audit(1694533504.328:6): arch=c000003e syscall=44 success=yes e
xit=60 a0=3 a1=7fff5ec512f0 a2=3c a3=0 items=0 ppid=698 pid=708 auid=4294967295
uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=(none) ses=429496729
5 comm="auditctl" exe="/usr/sbin/auditctl" subj=system_u:system_r:unconfined_ser
vice_t:s0 key=(null)^]ARCH=x86_64 SYSCALL=sendto AUID="unset" UID="root" GID="ro
ot" EUID="root" SUID="root" FSUID="root" EGID="root" SGID="root" FSGID="root"
type=PROCTITLE msg=audit(1694533504.328:6): proctitle=2F7362696E2F61756469746374
6C002D52002F6574632F61756469742F61756469742E72756C6573
type=CONFIG_CHANGE msg=audit(1694533504.328:7): op=set audit_failure=1 old=1 aui
d=4294967295 ses=4294967295 subj=system_u:system_r:unconfined_service_t:s0 res=1
^]AUID="unset"
type=SYSCALL msg=audit(1694533504.328:7): arch=c000003e syscall=44 success=yes e
@@@
"audit.log" 1867L, 429762B
1,1 Top
[root@localhost log]# cd httpd/
[root@localhost httpd]# ls
access_log error_log
[root@localhost httpd]# vim access_log
[root@localhost httpd]# vim error_log
[root@localhost httpd]# cd ..
[root@localhost log]# cd audit/
[root@localhost audit]# ls
audit.log
[root@localhost audit]# vim audit.log
[root@localhost audit]#
```


19. Выполните команду `semanage port -a -t http_port_t -p tcp 81` После этого проверьте список портов командой `semanage port -l | grep http_port_t` Убедитесь, что порт 81 появился в списке.

```
[root@localhost var]# semanage port -a -t http_port_t -p tcp 81
ValueError: Port tcp/81 already defined
[root@localhost var]# 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
[root@localhost var]#
```

20. Попробуйте запустить веб-сервер Apache ещё раз.

```
[root@localhost var]# systemctl restart httpd
[root@localhost var]#
```

21. Верните контекст `httpd_sys_content_t` к файлу `/var/www/html/ test.html`: `chcon -t httpd_sys_content_t /var/www/html/test.html` После этого попробуйте получить доступ к файлу через веб-сервер, введя в браузере адрес `http://127.0.0.1:81/test.html`. Вы должны увидеть содержимое файла — слово «test».
22. Исправьте обратно конфигурационный файл `apache`, вернув `Listen 80`.
23. Удалите привязку `http_port_t` к 81 порту: `semanage port -d -t http_port_t -p tcp 81` и проверьте, что порт 81 удалён.
24. Удалите файл `/var/www/html/test.html`: `rm /var/www/html/test.html`

```
[root@localhost conf]# vim httpd.conf
[root@localhost conf]# semanage port -d -t http_port_t -p tcp 81
ValueError: Port tcp/81 is defined in policy, cannot be deleted
[root@localhost conf]# semanage port -a -t http_port_t -p tcp 80
ValueError: Port tcp/80 already defined
[root@localhost conf]# rm /var/www/html/test/html
rm: cannot remove '/var/www/html/test/html': No such file or directory
[root@localhost conf]# rm /var/www/html/test.html
rm: remove regular file '/var/www/html/test.html'? y
[root@localhost conf]#
```

Выводы

я изучил методы работы с сервером `apache` в среде `Linux` и познакомился с основами информационной безопасности

Список литературы

lab05 {#refs:Лабораторная работа № 6. Мандатное разграничение прав в Linux}