

Отчёт по лабораторной работе

Лабораторная работа № 6

Живцова Анна

Содержание

1	Цель работы	5
2	Теоретическое введение	6
3	Выполнение лабораторной работы	8
4	Выводы	17
	Список литературы	18

Список иллюстраций

3.1	Проверка готовности к выполнению лабораторной работы	9
3.2	Контекст процесса Apache. Состояние переключателей SELinux для Apache	10
3.3	Статистика по политике	11
3.4	Множество пользователей	12
3.5	Изучение контекстов и отображение созданного html файла . . .	13
3.6	Ошибка при обращении к html файлу с измененным контекстом .	13
3.7	Лог файлы	14
3.8	Смена порта	15
3.9	Смена порта	15
3.10	Возвращение контекста html файлу и обращение через браузер .	16
3.11	Восстановление всех изменений	16

Список таблиц

1 Цель работы

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

2 Теоретическое введение

Security-Enhanced Linux (SELinux) - это метод контроля доступа в Linux на основе модуля ядра Linux Security (LSM). SELinux включен по умолчанию во многих дистрибутивах на основе Red Hat, использующих пакетную базу rpm, например, Fedora, CentOS и т.д.

SELinux представляет собой систему маркировки, каждый процесс имеет метку. Каждый файл, каталог или даже пользователь в системе имеет метку. Даже портам и устройствам и именам хостов в системе присвоены метки. SELinux определяет правила доступа процесса к объектам с определенными метками. Это и называется политикой. За соблюдением правил следит ядро. Иногда это еще называется обязательный контроль доступа (Mandatory Access Control, MAC)

Владелец файла не имеет полной свободы действий над атрибутами безопасности. Стандартные атрибуты контроля доступа, такие как группа и владелец ничего не значат для SELinux. Полностью все управляется метками. Значения атрибутов могут быть установлены и без прав root, но на это нужно иметь специальные полномочия SELinux [1].

Apache - это популярнейший свободный веб-сервер. Состоянием на 2020 год он используется на 33% всех сайтов интернета, а это приблизительно 304 миллиарда сайтов. Этот веб-сервер был разработан в далеком 1995, как замена для популярного того сервера NCSA и исправил множество его проблем. Ходят слухи что его имя походит от a patchy, заплатка, так как он исправлял ошибки NCSA. Сейчас же, это кроссплатформенная программа, поддерживающая Windows, Linux и MacOS и обеспечивающая достаточную гибкость, настраиваемость и функцио-

нальность. Программа имеет модульную структуру, что позволяет расширять ее функциональность почти до бесконечности с помощью модулей [2] .

3 Выполнение лабораторной работы

1. Убедились, что SELinux работает в режиме enforcing при политике targeted.
Установили и запустили web-сервер apache (см. рис. 3.1).


```

[annazhivtsova@annazhivtsova ~]$ getenforce
Enforcing
[annazhivtsova@annazhivtsova ~]$ 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
[annazhivtsova@annazhivtsova ~]$ service httpd status
Redirecting to /bin/systemctl status httpd.service
Unit httpd.service could not be found.
[annazhivtsova@annazhivtsova ~]$ /etc/rc.d/init.d/httpd status
bash: /etc/rc.d/init.d/httpd: No such file or directory
[annazhivtsova@annazhivtsova ~]$ start /etc/rc.d/init.d/httpd status
bash: start: command not found...
[annazhivtsova@annazhivtsova ~]$ /etc/rc.d/init.d/httpd start
bash: /etc/rc.d/init.d/httpd: No such file or directory
[annazhivtsova@annazhivtsova ~]$ sudo su
[sudo] password for annazhivtsova:
[root@annazhivtsova annazhivtsova]# dnf install httpd
CentOS Stream 9 - BaseOS                11 kB/s | 9.2 kB      00:00
CentOS Stream 9 - BaseOS                5.1 MB/s | 7.8 MB     00:01
CentOS Stream 9 - AppStream             27 kB/s | 9.3 kB      00:00
CentOS Stream 9 - AppStream             6.3 MB/s | 18 MB      00:02
CentOS Stream 9 - Extras packages       15 kB/s | 10 kB       00:00
Dependencies resolved.
=====
Package                                Arch      Version           Repository        Size
=====
Installing:
httpd                                  x86_64    2.4.57-5.el9      appstream         47 k
Installing dependencies:
apr                                    x86_64    1.7.0-11.el9      appstream         123 k
apr-util                              x86_64    1.6.1-23.el9      appstream          95 k
apr-util-bdb                          x86_64    1.6.1-23.el9      appstream          13 k
centos-logos-httpd                    noarch    90.4-1.el9        appstream         252 k

```

Рис. 3.1: Проверка готовности к выполнению лабораторной работы

2. Получили контекст процесса Apache. Посмотрели текущее состояние переключателей SELinux для Apache (см. рис. 3.2).

```

[annazhivtsova@annazhivtsova ~]$ ps auxZ | grep httpd
system_u:system_r:httpd_t:s0 root 3676 0.0 0.5 20340 11680 ? Ss
10:07 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 3677 0.0 0.3 21676 7428 ? S
10:07 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 3678 0.0 0.5 1079488 11044 ? Sl
10:07 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 3679 0.0 0.6 1210624 13092 ? Sl
10:07 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 3680 0.0 0.8 1079488 17176 ? Sl
10:07 0:00 /usr/sbin/httpd -DFOREGROUND
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 annazhi+ 3938 0.0 0.1 221796 2
256 pts/0 S+ 10:11 0:00 grep --color=auto httpd
[annazhivtsova@annazhivtsova ~]$ sestatus -bigrep httpd
sestatus: invalid option -- 'i'

Usage: sestatus [OPTION]

-v Verbose check of process and file contexts.
-b Display current state of booleans.

Without options, show SELinux status.
[annazhivtsova@annazhivtsova ~]$ 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

```

Рис. 3.2: Контекст процесса Apache. Состояние переключателей SELinux для Apache

3. Посмотрели статистику по политике с помощью команды `seinfo` (см. рис. 3.3), определили множество пользователей, ролей, типов (см. рис. 3.4).

```

seinfo: error: unrecognized arguments: --types
[annazhivtsova@annazhivtsova ~]$ seinfo
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:            5135     Attributes:         259
Users:            8        Roles:              15
Booleans:         357     Cond. Expr.:       390
Allow:            65380    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

[annazhivtsova@annazhivtsova ~]$ seinfo -r

Roles: 15
auditadm_r
container_user_r
dbadm_r
guest_r
logadm_r
nx_server_r
object_r
secadm_r
staff_r
sysadm_r
system_r
unconfined_r
user_r

```

Рис. 3.3: Статистика по политике

```
[annazhivtsova@annazhivtsova ~]$ seinfo -u
Users: 8
  guest_u
  root
  staff_u
  sysadm_u
  system_u
  unconfined_u
  user_u
  xguest_u
```

Рис. 3.4: Множество пользователей

4. Определили тип файлов и поддиректорий, находящихся в директориях `/var/www` и `/var/www/html`. Для последней директории установлены права `rwxr_xr_x`. Создали в ней простой html файл. По умолчанию ему был присвоен контекст `unconfined_u:object_r:httpd_sys_content_t:s0`. Обратились к файлу через браузер (см. рис. 3.5).

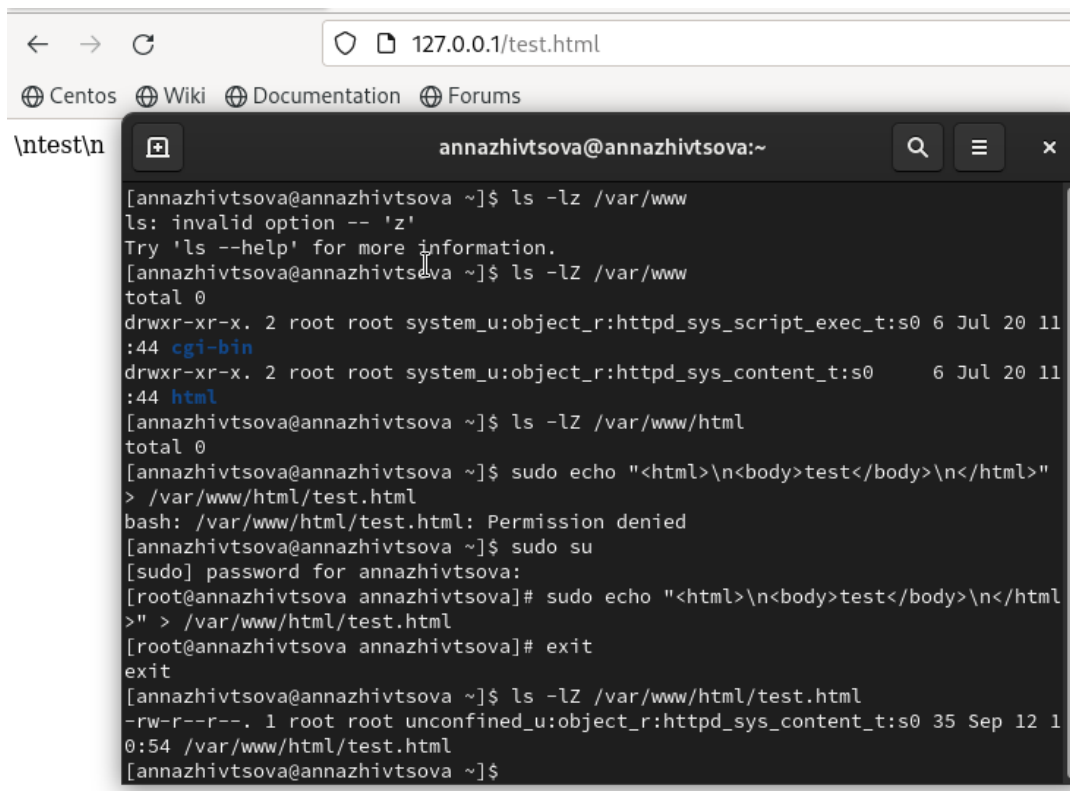


Рис. 3.5: Изучение контекстов и отображение созданного html файла

5. Изменили контекст созданного html файла на тот, к которому процесс httpd не должен иметь доступа и получили ошибку при обращении к файлу через браузер (см. рис. 3.6).

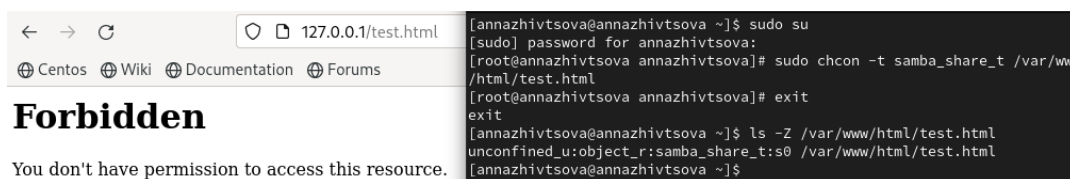


Рис. 3.6: Ошибка при обращении к html файлу с измененным контекстом

6. Посмотрели лог файлы (см. рис. 3.7).

```

[root@annazhivtsova annazhivtsova]# cat /var/log/httpd/error_log
[Tue Sep 12 10:07:22.598331 2023] [core:notice] [pid 3676:tid 3676] SELinux policy enabled;
httpd running as context system_u:system_r:httpd_t:s0
[Tue Sep 12 10:07:22.600588 2023] [suexec:notice] [pid 3676:tid 3676] AH01232: suEXEC mechanism enabled (wrapper: /usr/sbin/suexec)
[Tue Sep 12 10:07:27.649223 2023] [lbmethod_heartbeat:notice] [pid 3676:tid 3676] AH02282:
No slotmem from mod_heartbeat
[Tue Sep 12 10:07:27.663183 2023] [mpm_event:notice] [pid 3676:tid 3676] AH00489: Apache/2.
4.57 (CentOS Stream) configured -- resuming normal operations
[Tue Sep 12 10:07:27.663221 2023] [core:notice] [pid 3676:tid 3676] AH00094: Command line:
'/usr/sbin/httpd -D FOREGROUND'
[Tue Sep 12 11:10:10.971442 2023] [core:error] [pid 3680:tid 3873] (13)Permission denied: [
client 127.0.0.1:49008] AH00035: access to /test.html denied (filesystem path '/var/www/htm
l/test.html') because search permissions are missing on a component of the path
[root@annazhivtsova annazhivtsova]# tail /var/log/messages
Sep 12 11:10:26 annazhivtsova systemd[1]: setroubleshootd.service: Deactivated successfully
.
Sep 12 11:10:26 annazhivtsova systemd[1]: setroubleshootd.service: Consumed 1.312s CPU time
.
Sep 12 11:22:50 annazhivtsova systemd[1]: Starting Fingerprint Authentication Daemon...
Sep 12 11:22:50 annazhivtsova systemd[1]: Started Fingerprint Authentication Daemon.
Sep 12 11:22:54 annazhivtsova NetworkManager[884]: <info> [1694506974.5010] agent-manager:
agent[cf19cc90d6ac6248,:1.68/org.gnome.Shell.NetworkAgent/1000]: agent registered
Sep 12 11:23:20 annazhivtsova systemd[1]: fprintd.service: Deactivated successfully.
Sep 12 11:25:16 annazhivtsova systemd[1]: Starting Fingerprint Authentication Daemon...
Sep 12 11:25:16 annazhivtsova systemd[1]: Started Fingerprint Authentication Daemon.
Sep 12 11:25:19 annazhivtsova su[5919]: (to root) root on pts/1
Sep 12 11:25:47 annazhivtsova systemd[1]: fprintd.service: Deactivated successfully.

```

Рис. 3.7: Лог файлы

7. Запустили веб-сервер Apache на прослушивание TCP-порта (см. рис. 3.8).

```
GNU nano 5.6.1 /etc/httpd/conf/httpd.conf Modified
# 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:
```

Рис. 3.8: Смена порта

8. Посмотрели лог файлы, недавно был обновлен файл `/var/log/http/error_log` (см. рис. 3.9).

```
[root@annazhivtsova guest]# tail -n1 /var/log/messages
Sep 14 15:58:52 annazhivtsova httpd[7536]: Server configured, listening on: port 81
[root@annazhivtsova guest]# cat /var/log/httpd/error_log | grep 15:58
[Thu Sep 14 15:58:51.080778 2023] [mpm_event:notice] [pid 7158:tid 7158] AH00492: caught SIGWINCH, shutting down gracefully
[Thu Sep 14 15:58:52.201975 2023] [core:notice] [pid 7536:tid 7536] SELinux policy enabled; httpd running as context system_u:system_r:httpd_t:s0
[Thu Sep 14 15:58:52.203613 2023] [suexec:notice] [pid 7536:tid 7536] AH01232: suEXEC mechanism enabled (wrapper: /usr/sbin/suexec)
[Thu Sep 14 15:58:52.247401 2023] [lbmethod_heartbeat:notice] [pid 7536:tid 7536] AH02282: No slotmem from mod_heartmonitor
[Thu Sep 14 15:58:52.307857 2023] [mpm_event:notice] [pid 7536:tid 7536] AH00489: Apache/2.4.57 (CentOS Stream) configured -- resuming normal operations
[Thu Sep 14 15:58:52.307966 2023] [core:notice] [pid 7536:tid 7536] AH00094: Command line: '/usr/sbin/httpd -D FOREGROUND'
[root@annazhivtsova guest]# cat /var/log/httpd/access_log | grep 15:5
[root@annazhivtsova guest]# cat /var/log/httpd/audit_log | grep 15:5
cat: /var/log/httpd/audit_log: No such file or directory
[root@annazhivtsova guest]# cat /var/log/audit/audit.log | grep 15:5
type=USER_ACCT msg=audit(1694459963.115:581): pid=38219 uid=1001 auid=1001 ses=6 subj=unconfined_u:unconfined_r:unc
onfined_t:s0-s0:c0.c1023 msg='op=PAM:accounting grantors=pam_unix,pam_localuser acct="guest2" exe="/usr/bin/su" hos
tname=? addr=? terminal=/dev/pts/2 res=success'UID="guest" AUID="guest"
type=BPF msg=audit(1694675046.515:52): prog-id=37 op=LOAD
[root@annazhivtsova guest]# cat /var/log/audit/audit.log
type=DAEMON_START msg=audit(1693993144.909:7201): op=start ver=3.0.7 format=enriched kernel=5.14.0-362.el9.x86_64 a
uid=4294967295 pid=693 uid=0 ses=4294967295 subj=system_u:system_r:auditd_t:s0 res=successAUID="unset" UID="root"
type=CONFIG_CHANGE msg=audit(1693993144.983:5): op=set audit_backlog_limit=8192 old=64 auid=4294967295 ses=42949672
95 subj=system_u:system_r:unconfined_service_t:s0 res=1AUID="unset"
type=SYSCALL msg=audit(1693993144.983:5): arch=c000003e syscall=44 success=yes exit=60 a0=3 a1=7ffdebbe4990 a2=3c a
3=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) se
s=4294967295 comm="auditctl" exe="/usr/sbin/auditctl" subj=system_u:system_r:unconfined_service_t:s0 kevn(null)ARCH=
```

Рис. 3.9: Смена порта

9. Выполнили поднастройку политики командой `semanage port -a -t http_port_t -p tcp 81`, вернули html файлу прежний контекст, обратились к нему из браузера (см. рис. 3.10).

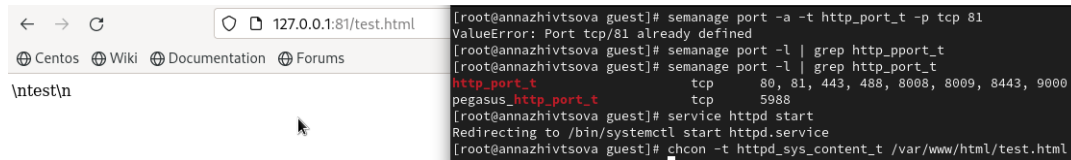


Рис. 3.10: Возвращение контекста html файлу и обращение через браузер

10. Восстановление всех изменений (см. рис. 3.11).

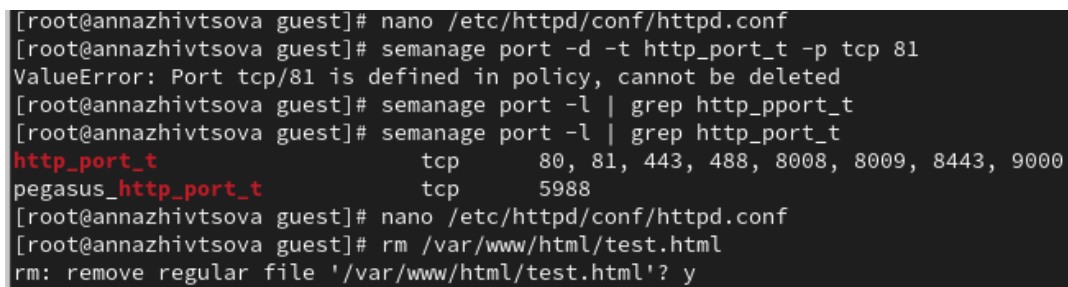


Рис. 3.11: Восстановление всех изменений

4 Выводы

Развили навыки администрирования ОС Linux. Получили первое практическое знакомство с технологией SELinux. Проверили работу SELinx на практике совместно с веб-сервером Apache.

Список литературы

1. Vermeulen S. SELinux System Administration. Packt Publishing Ltd., 2001. 336 с.
2. Хокинс, Скотт. Администрирование web-сервера apache и руководство по электронной коммерции. Издательский дом Вильям, 2020. 459 с.