

Информационная безопасность. Лабораторная работа № 6 на тему “Мандатное разграничение прав в Linux”

Горбунова Ярослава Михайловна

RUDN University, Moscow, Russian Federation


Содержание

- Цели и задачи
- Выполнение
- Результаты
- Список литературы

Цели и задачи

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

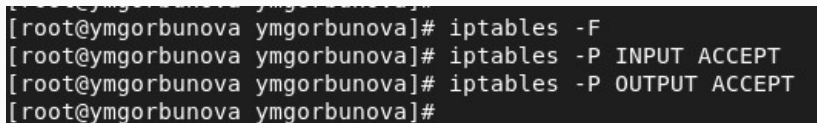
Выполнение



The screenshot shows a text editor window titled "httpd.conf [Только для чтения]" (httpd.conf [Read Only]) with the path "/etc/httpd/conf". The editor contains the following lines:

```
92
93 #
94 # ServerName gives the name and port that the server uses to identify itself.
95 # This can often be determined automatically, but we recommend you specify
96 # it explicitly to prevent problems during startup.
97 #
98 # If your host doesn't have a registered DNS name, enter its IP address here.
99 #
100 #ServerName www.example.com:80
101 ServerName test.ru
102
```

Figure 1: Подготовка лабораторного стенда. Пункт 4



The screenshot shows a terminal window with the following commands and output:

```
[root@ymgorbunova ymgorbunova]# iptables -F
[root@ymgorbunova ymgorbunova]# iptables -P INPUT ACCEPT
[root@ymgorbunova ymgorbunova]# iptables -P OUTPUT ACCEPT
[root@ymgorbunova ymgorbunova]#
```

Figure 2: Подготовка лабораторного стенда. Пункт 5

Выполнение

```
[ymgorbunova@ymgorbunova ~]$ getenforce
Enforcing
[ymgorbunova@ymgorbunova ~]$ 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
[ymgorbunova@ymgorbunova ~]$ 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; vendor pre>
   Active: active (running) since Tue 2022-10-11 15:58:26 MSK; 47min ago
     Docs: man:httpd.service(8)
  Main PID: 943 (httpd)
    Status: "Total requests: 0; Idle/Busy workers 100/0;Requests/sec: 0; Bytes>
      Tasks: 213 (limit: 12209)
    Memory: 19.2M
       CPU: 1.050s
    CGroup: /system.slice/httpd.service
            └─943 /usr/sbin/httpd -DFOREGROUND
              └─962 /usr/sbin/httpd -DFOREGROUND
                └─963 /usr/sbin/httpd -DFOREGROUND
                  └─964 /usr/sbin/httpd -DFOREGROUND
                    └─965 /usr/sbin/httpd -DFOREGROUND

окт 11 15:58:26 ymgorbunova.localdomain systemd[1]: Starting The Apache HTTP Se>
окт 11 15:58:26 ymgorbunova.localdomain systemd[1]: Started The Apache HTTP Ser>
окт 11 15:58:26 ymgorbunova.localdomain httpd[943]: Server configured, listenin>
[ymgorbunova@ymgorbunova ~]$
```



```
[ymgorbunova@ymgorbunova ~]$ ps auxZ | grep httpd
system_u:system_r:httpd_t:s0      root          943   0.0  0.2  20248  5156 ?        Ss   15:57   0:00
/usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0      apache        962   0.0  0.1  21572  2992 ?        S    15:57   0:00
/usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0      apache        963   0.0  0.3 1210512 7304 ?        Sl   15:57   0:00
/usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0      apache        964   0.0  0.2 1079376 5328 ?        Sl   15:57   0:00
/usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0      apache        965   0.0  0.2 1079376 5364 ?        Sl   15:57   0:00
/usr/sbin/httpd -DFOREGROUND
unconfined_u:unconfined_r:unconfined_t:s0-c0.c1023 ymgorbu+ 4381 0.0  0.1 221824 2272 pts/1 S+ 1
6:46   0:00 grep --color=auto httpd
[ymgorbunova@ymgorbunova ~]$ ps -eZ | grep httpd
system_u:system_r:httpd_t:s0      943 ?          00:00:00 httpd
system_u:system_r:httpd_t:s0      962 ?          00:00:00 httpd
system_u:system_r:httpd_t:s0      963 ?          00:00:00 httpd
system_u:system_r:httpd_t:s0      964 ?          00:00:00 httpd
system_u:system_r:httpd_t:s0      965 ?          00:00:00 httpd
[ymgorbunova@ymgorbunova ~]$
```

Figure 4: Пункт 3

Выполнение

```
[ymgorbunova@ymgorbunova ~]$ 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
httpd_dbus_sssd off
httpd_dontaudit_search_dirs off
httpd_enable_cgi on
httpd_enable_ftp_server off
httpd_enable_homedirs off
httpd_execmem off
httpd_graceful_shutdown off
httpd_manage_ipa off
httpd_mod_auth_ntlm_winbind off
httpd_mod_auth_pam off
httpd_read_user_content off
httpd_run_ipa off
httpd_run_preupgrade off
httpd_run_stickshift off
httpd_serve_cobbler_files off
httpd_setrlimit off
httpd_ssi_exec off
httpd_sys_script_anon_write off
httpd_tmp_exec off
httpd_tty_comm off
httpd_unified on
httpd_use_cifs off
httpd_use_fusefs off
httpd_use_gpg off
httpd_use_nfs off
httpd_use_openssl off
httpd_use_openssl off
httpd_use_openssl off
httpd_use_openssl off
httpd_use_openssl off
httpd_use_openssl off
httpd_use_openssl off
httpd_use_openssl off
httpd_verify_dns off
```

```
[ymgorbunova@ymgorbunova ~]$ seinfo
Statistics for policy file: /sys/fs/selinux/policy
Policy Version:          33 (MLS enabled)
Target Policy:           selinux
Handle unknown classes:  allow

Classes:                  133      Permissions:              454
Sensitivities:            1        Categories:              1024
Types:                    4995     Attributes:               254
Users:                    8         Roles:                    14
Booleans:                 347      Cond. Expr.:             382
Allow:                    63727    Neverallow:               0
Auditallow:               163      Dontaudit:                8391
Type_trans:               251060   Type_change:              87
Type_member:               35      Range_trans:              5958
Role_allow:                38      Role_trans:               418
Constraints:              72      Validatetrans:            0
MLS Constrain:            72      MLS Val. Tran:            0
Permissives:              0        Polcap:                   5
Defaults:                 7        Typebounds:               0
Allowxperm:               0        Neverallowxperm:          0
Auditallowxperm:          0        Dontauditxperm:           0
Ibendportcon:             0        Ibpkeycon:                0
Initial SIDs:             27      Fs_use:                   33
Genfscon:                 106     Portcon:                  651
Netifcon:                 0        Nodecon:                  0
```

```
[ymgorbunova@ymgorbunova ~]$
```

```
[ymgorbunova@ymgorbunova ~]$ ls -lZ /var/www
итого 0
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_script_exec_t:s0 6 мая 16 15:10 cgi-bin
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:s0 6 мая 16 15:10 html
[ymgorbunova@ymgorbunova ~]$ ls -lZ /var/www/html
итого 0
```

Figure 7: Пункт 6-8

```
[root@ymgorbunova ymgorbunova]# echo "<html>
<body>test</body>
</html>" > /var/www/html/test.html
[root@ymgorbunova ymgorbunova]# cat /var/www/html/test.html
<html>
<body>test</body>
</html>
[root@ymgorbunova ymgorbunova]# touch /var/www/html/my.html
[root@ymgorbunova ymgorbunova]# cat /var/www/html/my.html
[root@ymgorbunova ymgorbunova]#
```

Figure 8: Пункт 9-10

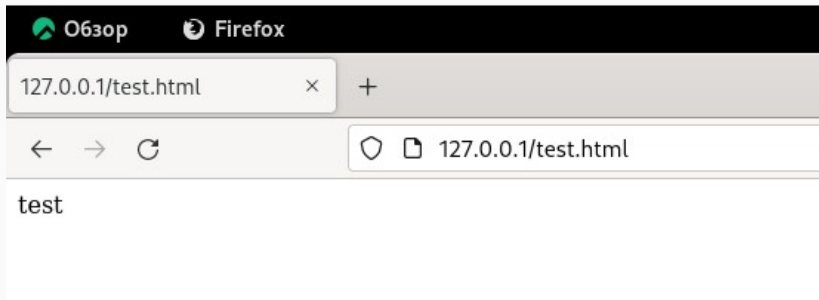


Figure 9: Пункт 11

```
[root@ymgorbunova ymgorbunova]# ls -Z /var/www/html/test.html
unconfined_u:object_r:httpd_sys_content_t:s0 /var/www/html/test.html
[root@ymgorbunova ymgorbunova]#
```

Figure 10: Пункт 12

```
[root@ymgorbunova ymgorbunova]# chcon -t samba_share_t /var/www/html/test.html  
[root@ymgorbunova ymgorbunova]# ls -Z /var/www/html/test.html  
unconfined_u:object_r:samba_share_t:s0 /var/www/html/test.html
```

Figure 11: Пункт 13

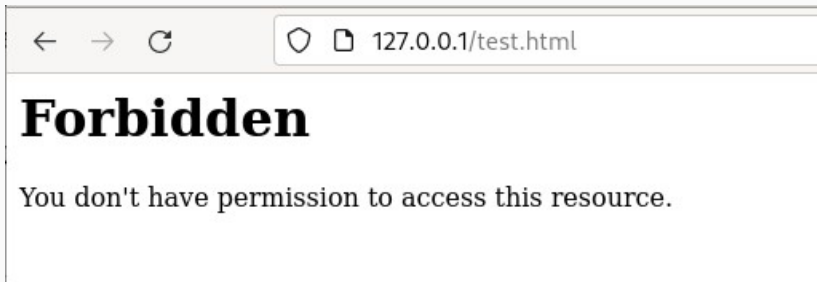


Figure 12: Пункт 14

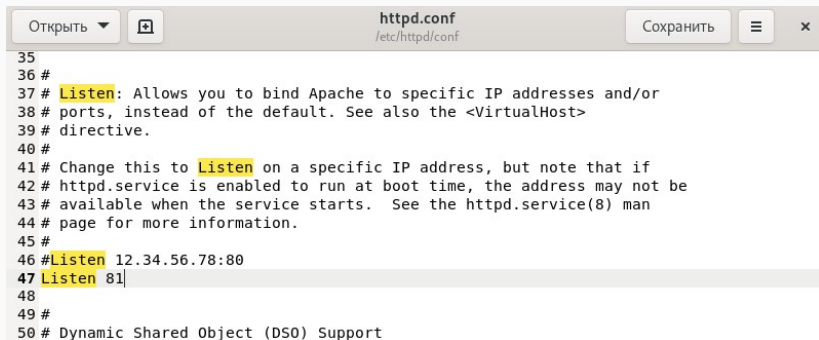
```
[root@ymgorbunova ymgorbunova]# ls -l /var/www/html/test.html  
-rw-r--r-- 1 root root 33 окт 11 17:11 /var/www/html/test.html
```

```
[root@ymgorbunova ymgorbunova]# tail /var/log/messages
Oct 11 17:30:15 ymgorbunova setroubleshoot[5129]: failed to retrieve rpm info for /var/www/html/test.htm
l
Oct 11 17:30:15 ymgorbunova setroubleshoot[5129]: SELinux запрещает /usr/sbin/httpd доступ getattr к фай
лу /var/www/html/test.html. Для выполнения всех сообщений SELinux: sealert -l 21b3fad3-a74f-4ebe-a9a6-ac8
d253ee43b
Oct 11 17:30:15 ymgorbunova setroubleshoot[5129]: SELinux запрещает /usr/sbin/httpd доступ getattr к фай
лу /var/www/html/test.html.#012#012**** Модуль restorecon предлагает (точность 92.2) *****
*****#012#012Если вы хотите исправить метку.$TARGETзнак _PATH по умолчанию должен быть httpd_sys_cont
ent_t#012То вы можете запустить restorecon. Возможно, попытка доступа была остановлена из-за недостаточн
ых разрешений для доступа к родительскому каталогу, и в этом случае попытайтесь соответствующим образом
изменить следующую команду.#012Сделать#012# /sbin/restorecon -v /var/www/html/test.html#012#012**** Мо
дуль public_content предлагает (точность 7.83) *****#012#012Если вы хотите лечить test.
html как общедоступный контент#012То необходимо изменить метку test.html с public_content_t на public_co
ntent_rw_t.#012Сделать#012# semanage fcontext -a -t public_content_t '/var/www/html/test.html'#012# rest
orecon -v '/var/www/html/test.html'#012#012**** Модуль catchall предлагает (точность 1.41) *****
*****#012#012Если вы считаете, что httpd должно быть разрешено getattr доступ к test.html fi
le по умолчанию.#012То рекомендуется создать отчет об ошибке.#012Чтобы разрешить доступ, можно создать л
окальный модуль политики.#012Сделать#012'зрешить этот доступ сейчас, выполнив:#012# ausearch -c 'httpd'
--raw | audit2allow -M my-httpd#012# semodule -X 300 -i my-httpd.pp#012
Oct 11 17:30:25 ymgorbunova systemd[1]: dbus-:1.10-org.fedoraproject.SetroubleshootPrivileged@0.service:
Main process exited, code=killed, status=14/ALRM
Oct 11 17:30:25 ymgorbunova systemd[1]: dbus-:1.10-org.fedoraproject.SetroubleshootPrivileged@0.service:
Failed with result 'signal'.
Oct 11 17:30:25 ymgorbunova systemd[1]: dbus-:1.10-org.fedoraproject.Setroubleshootd@0.service: Main pro
cess exited, code=killed, status=14/ALRM
Oct 11 17:30:25 ymgorbunova systemd[1]: dbus-:1.10-org.fedoraproject.Setroubleshootd@0.service: Failed w
ith result 'signal'.
Oct 11 17:32:11 ymgorbunova systemd[1]: Starting Fingerprint Authentication Daemon...
Oct 11 17:32:11 ymgorbunova systemd[1]: Started Fingerprint Authentication Daemon.
Oct 11 17:32:15 ymgorbunova su[5219]: (to root) ymgorbunova on pts/1
[root@ymgorbunova ymgorbunova]#
```

Figure 14: Пункт 15 (2)

```
[root@ymgorbunova ymgorbunova]# tail /var/log/audit/audit.log
type=USER_END msg=audit(1665498673.772:192): pid=4674 uid=1000 auid=1000 ses=3 subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 msg='op=PAM:session close grantors=pam_keyinit,pam_limits,pam_systemd,pam_unix,pam_umask,pam_xauth acct="root" exe="/usr/bin/su" hostname=? addr=? terminal=/dev/pts/1 res=success'UID="ymgorbunova" AUID="ymgorbunova"
type=CRED_DISP msg=audit(1665498673.772:193): pid=4674 uid=1000 auid=1000 ses=3 subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 msg='op=PAM:setcred grantors=pam_unix acct="root" exe="/usr/bin/su" hostname=? addr=? terminal=/dev/pts/1 res=success'UID="ymgorbunova" AUID="ymgorbunova"
type=BPF msg=audit(1665498731.403:194): prog-id=51 op=LOAD
type=SERVICE_START msg=audit(1665498731.489:195): pid=1 uid=0 auid=4294967295 ses=4294967295 subj=system_u:system_r:init_t:s0 msg='unit=fprintd comm="systemd" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=success'UID="root" AUID="unset"
type=USER_AUTH msg=audit(1665498735.781:196): pid=5219 uid=1000 auid=1000 ses=3 subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 msg='op=PAM:authentication grantors=pam_unix acct="root" exe="/usr/bin/su" hostname=? addr=? terminal=/dev/pts/1 res=success'UID="ymgorbunova" AUID="ymgorbunova"
type=USER_ACCT msg=audit(1665498735.798:197): pid=5219 uid=1000 auid=1000 ses=3 subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 msg='op=PAM:accounting grantors=pam_unix,pam_localuser acct="root" exe="/usr/bin/su" hostname=? addr=? terminal=/dev/pts/1 res=success'UID="ymgorbunova" AUID="ymgorbunova"
type=CRED_ACQ msg=audit(1665498735.803:198): pid=5219 uid=1000 auid=1000 ses=3 subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 msg='op=PAM:setcred grantors=pam_unix acct="root" exe="/usr/bin/su" hostname=? addr=? terminal=/dev/pts/1 res=success'UID="ymgorbunova" AUID="ymgorbunova"
type=USER_START msg=audit(1665498735.842:199): pid=5219 uid=1000 auid=1000 ses=3 subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 msg='op=PAM:session open grantors=pam_keyinit,pam_limits,pam_systemd,pam_unix,pam_umask,pam_xauth acct="root" exe="/usr/bin/su" hostname=? addr=? terminal=/dev/pts/1 res=success'UID="ymgorbunova" AUID="ymgorbunova"
type=SERVICE_STOP msg=audit(1665498761.704:200): pid=1 uid=0 auid=4294967295 ses=4294967295 subj=system_u:system_r:init_t:s0 msg='unit=fprintd comm="systemd" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=success'UID="root" AUID="unset"
type=BPF msg=audit(1665498761.716:201): prog-id=51 op=UNLOAD
[root@ymgorbunova ymgorbunova]#
```

Figure 15: Пункт 15 (3)



```
35
36 #
37 # Listen: Allows you to bind Apache to specific IP addresses and/or
38 # ports, instead of the default. See also the <VirtualHost>
39 # directive.
40 #
41 # Change this to Listen on a specific IP address, but note that if
42 # httpd.service is enabled to run at boot time, the address may not be
43 # available when the service starts. See the httpd.service(8) man
44 # page for more information.
45 #
46 #Listen 12.34.56.78:80
47 Listen 81
48
49 #
50 # Dynamic Shared Object (DSO) Support
```

Figure 16: Пункт 16

```
[root@ymgorbunova ymgorbunova]# service httpd stop
Redirecting to /bin/systemctl stop httpd.service
[root@ymgorbunova ymgorbunova]# service httpd start
Redirecting to /bin/systemctl start httpd.service
```

Figure 17: Пункт 17

```
[root@ymgorbunova ymgorbunova]# tail -n1 /var/log/messages
Oct 11 17:41:53 ymgorbunova httpd[5523]: Server configured, listening on: port 81
[root@ymgorbunova ymgorbunova]# tail -n1 /var/log/audit/audit.log
type=SERVICE_START msg=audit(1665499313.903:203): pid=1 uid=0 auid=4294967295 ses=4294967295 subj=system_u:system_r:init_t:s0 msg='unit=httpd comm="systemd" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=success' UID="root" AUID="unset"
```

Figure 18: Пункт 18

```
[root@ymgorbunova ymgorbunova]# semanage port -a -t http_port_t -p tcp 81
usage: semanage [-h]
                {import,export,login,user,port,ibpkey,ibendport,interface,module,node,fcontext,boolean,p
ermissive,dontaudit}
```

Figure 19: Пункт 19 (1)

```
[root@ymgorbunova ymgorbunova]# 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@ymgorbunova ymgorbunova]#
```

Figure 20: Пункт 19 (2)

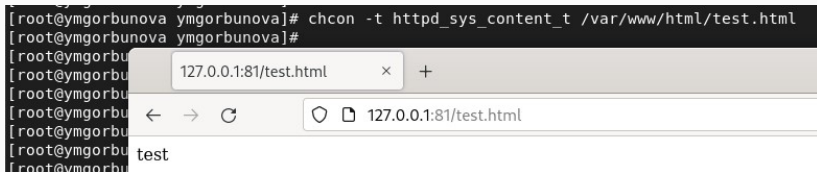


Figure 21: Пункт 21

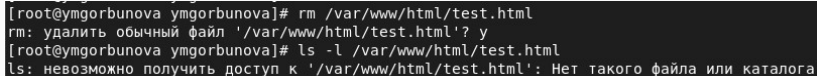


Figure 22: Пункт 24

Результаты

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

Список литературы

1. Методические материалы курса