№6

12.03.2024

, ,

-
- , -03-22
-
- 1032225355@pfur.ru

, SetUID- Sticky- .

. 1:

. **2:** setenforce 0

```
jose@jose-IdeaPad-3-15ITL6:~$ sudo apt install setools
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
Los paquetes indicados a continuación se instalaron de forma automática y ya no son necesarios.
  libsdl-ttf2.0-0 libsdl1.2debian nvidia-firmware-535-535.113.01
Utilice «sudo apt autoremove» para eliminarlos.
Se instalarán los siguientes paquetes adicionales:
  python3-networkx python3-setools
Paquetes sugeridos:
  python-networkx-doc python3-gdal python3-pydot python3-pygraphviz setools-gui
Se instalarán los siguientes paquetes NUEVOS:
  python3-networkx python3-setools setools
0 actualizados, 3 nuevos se instalarán, 0 para eliminar y 0 no actualizados.
Se necesita descargar 1.929 kB de archivos.
Se utilizarán 11,9 MB de espacio de disco adicional después de esta operación.
¿Desea continuar? [S/n] s
Des:1 http://es.archive.ubuntu.com/ubuntu mantic/main amd64 python3-networkx all 2.8.8-1ubuntu1 [1.468 kB]
Des:2 http://es.archive.ubuntu.com/ubuntu mantic/universe amd64 python3-setools amd64 4.4.3-1 [421 kB]
Des:3 http://es.archive.ubuntu.com/ubuntu mantic/universe amd64 setools amd64 4.4.3-1 [40,1 kB]
Descargados 1.929 kB en 2s (871 kB/s)
Seleccionando el paquete python3-networkx previamente no seleccionado.
(Leyendo la base de datos ... 507278 ficheros o directorios instalados actualmente.
```

. 3:

```
[root@localhost ~]# ps -auxZ | grep httpd
system_u:system_r:httpd_t:s0    root      139338  0.0  0.5  20128 11212 ?        Ss   00:25   0:00 /usr/sbin/
httpd -DFOREGROUND
system_u:system_r:httpd_t:s0    apache    139339  0.0  0.3  21612  7248 ?        S    00:25   0:00 /usr/sbin/
httpd -DFOREGROUND
system_u:system_r:httpd_t:s0    apache    139343  0.0  0.6 1210520 13020 ?       Sl   00:25   0:00 /usr/sbin/
httpd -DFOREGROUND
system_u:system_r:httpd_t:s0    apache    139345  0.0  0.5 1079384 10972 ?       Sl   00:25   0:00 /usr/sbin/
httpd -DFOREGROUND
system_u:system_r:httpd_t:s0    apache    139346  0.0  0.5 1079384 10972 ?       Sl   00:25   0:00 /usr/sbin/
httpd -DFOREGROUND
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 root 139757 0.0  0.1 221664 2256 pts/0 S+ 12:24   0:00
grep --color=auto httpd
```

. 4:

```
jose@jose-IdeaPad-3-15ITL6:~$ seinfo
Statistics for policy file: /etc/selinux/default/policy/policy.33
Policy Version:             33 (MLS enabled)
Target Policy:              selinux
Handle unknown classes:     allow
  Classes:             135    Permissions:         426
  Sensitivities:         1    Categories:         1024
  Types:              3971    Attributes:          227
  Users:                 7    Roles:                15
  Booleans:            318    Cond. Expr.:         349
  Allow:            107509    Neverallow:            0
  Auditallow:           21    Dontaudit:         17044
  Type_trans:         9433    Type_change:          72
  Type_member:          16    Range_trans:          56
  Role allow:           32    Role_trans:          372
  Constraints:         133    Validatetrans:         0
  MLS Constrain:       110    MLS Val. Tran:         0
  Permissives:           0    Polcap:                5
  Defaults:              0    Typebounds:            0
  Allowxperm:            0    Neverallowxperm:       0
  Auditallowxperm:       0    Dontauditxperm:        0
  Ibendportcon:          0    Ibpkeycon:             0
  Initial SIDs:         27    Fs_use:               29
  Genfscon:             95    Portcon:             487
  Netifcon:              0    Nodecon:               0
```

. 5:


jose@jose-IdeaPad-3-15ITL6:~$ ls -lZ /var/www
total 4
drwxr-xr-x 2 root root ? 4096 abr 24 12:12 html

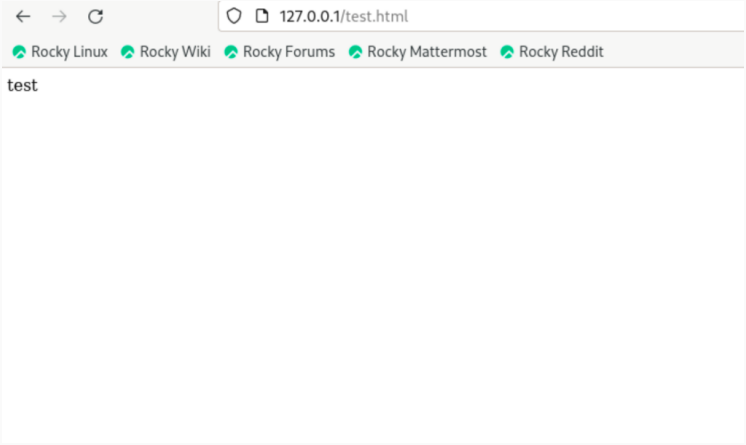
. 6: id

```
jose@jose-IdeaPad-3-15ITL6:~$ ls -lZ /var/www/html
total 12
-rw-r--r-- 1 root root ? 10671 abr 24 12:12 index.html
```

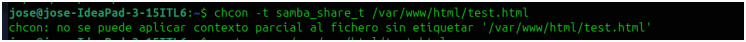
. 7:

```
jose@jose-IdeaPad-3-15ITL6:~$ ls -lZ /var/www/html/test.html
-rw-r--r-- 1 root root ? 31 abr 27 13:58 /var/www/html/test.html
```

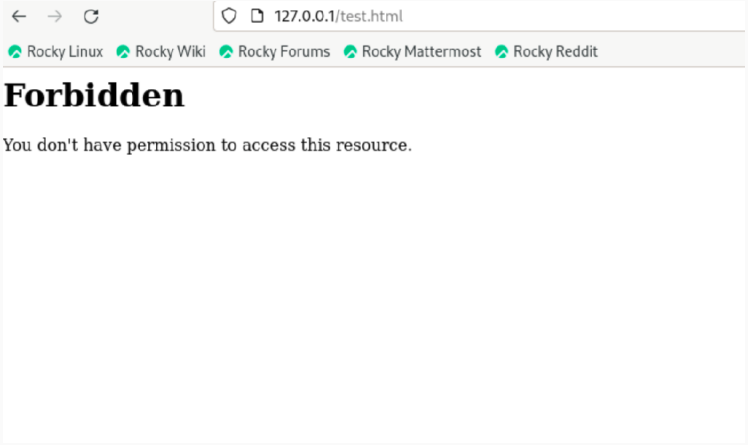
. 8:


127.0.0.1/test.html
Rocky Linux
Rocky Wiki
Rocky Forums
Rocky Mattermost
Rocky Reddit
test

. 9:


jose@jose-IdeaPad-3-15ITL6:~$ chcon -t samba_share_t /var/www/html/test.html
chcon: no se puede aplicar contexto parcial al fichero sin etiquetar '/var/www/html/test.html'

. **10:** ls -l


127.0.0.1/test.html
Rocky Linux
Rocky Wiki
Rocky Forums
Rocky Mattermost
Rocky Reddit
Forbidden
You don't have permission to access this resource.

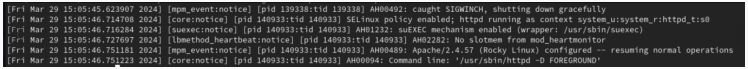
. 11:


Mar 29 14:54:55 localhost setroubleshoot[140747]: SELinux is preventing /usr/sbin/httpd from getattr access o
n 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_s
ys_content_t.#012Then you can run restorecon. The access attempt may have been stopped due to insufficient pe
rmissions to access a parent directory in which case try to change the following command accordingly.#012Do#0
12# /sbin/restorecon -v /var/www/html/test.html#012#012***** Plugin public_content (7.83 confidence) suggest
s **********#012#012If you want to treat test.html as public content#012Then you need to change t
he label on test.html to public_content_t or public_content_rw_t.#012Do#012# semanage fcontext -a -t public_c
ontent_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 g
etattr 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
Mar 29 14:55:05 localhost systemd[1]: dbus-:1.1-org.fedoraproject.SetroubleshootPrivileged@0.service: Deactiv
ated successfully.
Mar 29 14:55:05 localhost systemd[1]: dbus-:1.1-org.fedoraproject.SetroubleshootPrivileged@0.service: Consume
d 1.553s CPU time.
Mar 29 14:55:05 localhost systemd[1]: setroubleshootd.service: Deactivated successfully.
Mar 29 14:55:05 localhost systemd[1]: setroubleshootd.service: Consumed 1.155s CPU time.
[root@localhost html]# S

. 12:


GNU nano 5.6.1
/etc/httpd/conf/httpd.conf
Modified
#Listen 12.34.56.78:80
Listen 81

. 13:

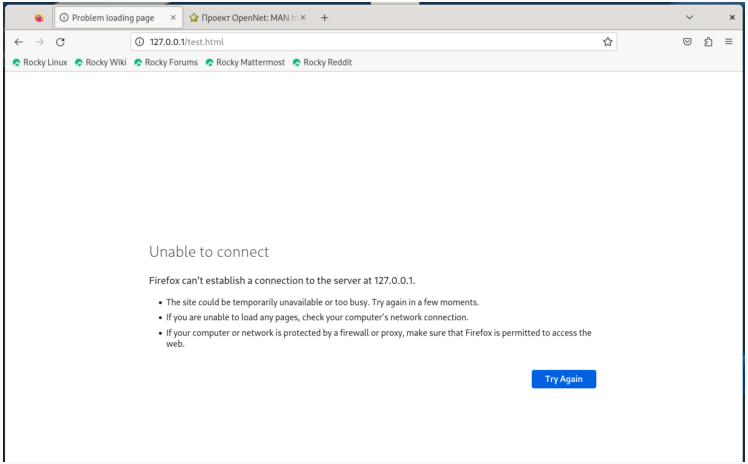

[Fri Mar 29 15:05:45.623907 2024] [mpm_event:notice] [pid 139338:tid 139338] AH00492: caught SIGWINCH, shutting down gracefully
[Fri Mar 29 15:05:46.714708 2024] [core:notice] [pid 140933:tid 140933] SELinux policy enabled; httpd running as context system_u:system_r:httpd_t:s0
[Fri Mar 29 15:05:46.716284 2024] [suexec:notice] [pid 140933:tid 140933] AH01232: suEXEC mechanism enabled (wrapper: /usr/sbin/suexec)
[Fri Mar 29 15:05:46.727697 2024] [lbmethod_heartbeat:notice] [pid 140933:tid 140933] AH02282: No slotmem from mod_heartmonitor
[Fri Mar 29 15:05:46.751181 2024] [mpm_event:notice] [pid 140933:tid 140933] AH00489: Apache/2.4.57 (Rocky Linux) configured -- resuming normal operations
[Fri Mar 29 15:05:46.751223 2024] [core:notice] [pid 140933:tid 140933] AH00094: Command line: '/usr/sbin/httpd -D FOREGROUND'

. 14:

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

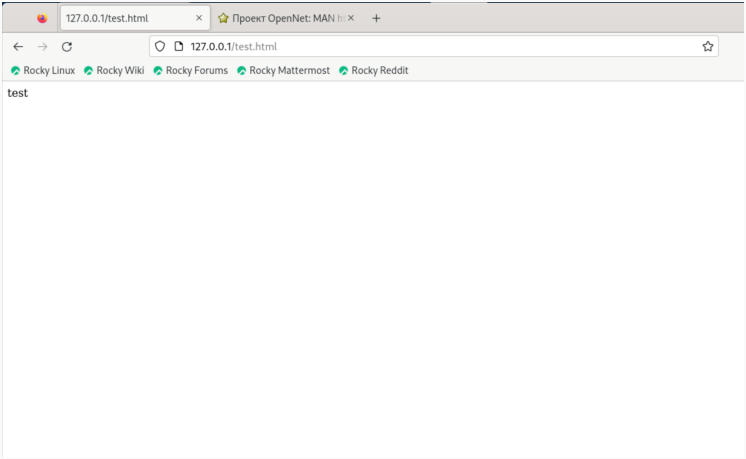
. 15:

Sticky-


Problem loading page
Проект OpenNet: MAN h
127.0.0.1/test.html
Rocky Linux
Rocky Wiki
Rocky Forums
Rocky Mattermost
Rocky Reddit
Unable to connect
Firefox can't establish a connection to the server at 127.0.0.1.
The site could be temporarily unavailable or too busy. Try again in a few moments.
If you are unable to load any pages, check your computer's network connection.
If your computer or network is protected by a firewall or proxy, make sure that Firefox is permitted to access the web.
Try Again

. 16:

Sticky-


127.0.0.1/test.html
Проект OpenNet: MAN
127.0.0.1/test.html
Rocky Linux
Rocky Wiki
Rocky Forums
Rocky Mattermost
Rocky Reddit
test

. 17:

```
[root@localhost html]# rm /var/www/html/test.html
rm: remove regular file '/var/www/html/test.html'? y
[root@localhost html]#
```

. 18: t

Sticky

. 19: Sticky

, SetUID- Sticky- .

.