

Tên: Trần Minh Triết

MSSV: SE172241

```
triettm@triettm:~  
File Edit View Search Terminal Help  
[triettm@triettm ~]$ ls -Z  
drwxr-xr-x. triettm triettm unconfined_u:object_r:user_home_t:s0 Desktop  
drwxr-xr-x. triettm triettm unconfined_u:object_r:user_home_t:s0 Documents  
drwxr-xr-x. triettm triettm unconfined_u:object_r:user_home_t:s0 Downloads  
drwxr-xr-x. triettm triettm unconfined_u:object_r:audio_home_t:s0 Music  
drwxr-xr-x. triettm triettm unconfined_u:object_r:user_home_t:s0 Pictures  
drwxr-xr-x. triettm triettm unconfined_u:object_r:user_home_t:s0 Public  
drwxr-xr-x. triettm triettm unconfined_u:object_r:user_home_t:s0 Templates  
drwxr-xr-x. triettm triettm unconfined_u:object_r:user_home_t:s0 Videos  
[triettm@triettm ~]$
```

Kiểm tra quyền SELinux của file.

```
[triettm@triettm ~]$ ps -Z  
LABEL PID TTY TIME CMD  
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 10333 pts/0 00:00:00 bash  
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 10790 pts/0 00:00:00 ps  
[triettm@triettm ~]$
```

Kiểm tra quyền SELinux của các process.

Installing the SELinux tools

```
[triettm@triettm ~]$ sudo yum install setools policycoreutils policycoreutils-python
[sudo] password for triettm:
Loaded plugins: fastestmirror, langpacks
Loading mirror speeds from cached hostfile
* base: mirrors.vhost.vn
* extras: mirrors.vhost.vn
* updates: mirrors.nhanhoa.com
base | 3.6 kB    00:00
extras | 2.9 kB    00:00
updates | 2.9 kB    00:00
(1/4): base/7/x86_64/group_gz | 153 kB    00:00
(2/4): extras/7/x86_64/primary_db | 249 kB    00:00
(3/4): base/7/x86_64/primary_db | 6.1 MB    00:26
(4/4): updates/7/x86_64/primary_db | 19 MB    01:04
Package policycoreutils-2.5-34.el7.x86_64 already installed and latest version
Package policycoreutils-python-2.5-34.el7.x86_64 already installed and latest version
Resolving Dependencies
--> Running transaction check
```

```

triettm@triettm:~
File Edit View Search Terminal Help
Verifying : setools-3.3.8-4.el7.x86_64 3/7
Verifying : setools-libs-tcl-3.3.8-4.el7.x86_64 4/7
Verifying : setools-console-3.3.8-4.el7.x86_64 5/7
Verifying : 1:tk-8.5.13-6.el7.x86_64 6/7
Verifying : setools-gui-3.3.8-4.el7.x86_64 7/7

Installed:
  setools.x86_64 0:3.3.8-4.el7

Dependency Installed:
  bwidget.noarch 0:1.9.0-6.el7      setools-console.x86_64 0:3.3.8-4.el7
  setools-gui.x86_64 0:3.3.8-4.el7  setools-libs-tcl.x86_64 0:3.3.8-4.el7
  tcl.x86_64 1:8.5.13-8.el7        tk.x86_64 1:8.5.13-6.el7

Complete!
[triettm@triettm ~]$ sudo yum install setroubleshoot
Loaded plugins: fastestmirror, langpacks
Loading mirror speeds from cached hostfile
* base: mirrors.nipa.cloud
* extras: mirrors.nipa.cloud
* updates: mirror.vodien.com
Package setroubleshoot-3.2.30-8.el7.x86_64 already installed and latest version
Nothing to do

```

```
triettm@triettm:~  
File Edit View Search Terminal Help  
(1/3): mailcap-2.1.41-2.el7.noarch.rpm | 31 kB 00:00  
(2/3): httpd-tools-2.4.6-98.el7.centos.6.x86_64.rpm | 94 kB 00:00  
(3/3): httpd-2.4.6-98.el7.centos.6.x86_64.rpm | 2.7 MB 00:00  
-----  
Total 3.1 MB/s | 2.8 MB 00:00  
Running transaction check  
Running transaction test  
Transaction test succeeded  
Running transaction  
Installing : mailcap-2.1.41-2.el7.noarch 1/3  
Installing : httpd-tools-2.4.6-98.el7.centos.6.x86_64 2/3  
Installing : httpd-2.4.6-98.el7.centos.6.x86_64 3/3  
Verifying : httpd-tools-2.4.6-98.el7.centos.6.x86_64 1/3  
Verifying : mailcap-2.1.41-2.el7.noarch 2/3  
Verifying : httpd-2.4.6-98.el7.centos.6.x86_64 3/3  
  
Installed:  
httpd.x86_64 0:2.4.6-98.el7.centos.6  
  
Dependency Installed:  
httpd-tools.x86_64 0:2.4.6-98.el7.centos.6 mailcap.noarch 0:2.1.41-2.el7  
  
Complete!  
[triettm@triettm ~]$  
  
Complete:  
[triettm@triettm ~]$ sudo firewall-cmd --permanent --add-service=http  
success  
[triettm@triettm ~]$ sudo systemctl enable --now httpd  
Created symlink from /etc/systemd/system/multi-user.target.wants/httpd.service  
to /usr/lib/systemd/system/httpd.service.  
[triettm@triettm ~]$ sudo firewall-cmd --reload  
success  
[triettm@triettm ~]$
```

Cài đặt dịch vụ Apache cho Linux server để build một web server. Lúc này ta có thể truy cập vào Web Server ngay trên máy ảo Centos. Tuy nhiên các máy tính khác cùng dãy mạng lại không thể truy cập vào trang web được (cụ thể là máy tính thật). Lý do là vì firewall của web server đã chặn không cho kết nối tới, vì thế ta cần config lại quyền truy cập trên firewall, add thêm service http vào.

Hands-on lab – SELinux type enforcement

1. Cài đặt Apache và SELinux tools

```
triettm@triettm:~  
File Edit View Search Terminal Help  
[triettm@triettm ~]$ sudo yum install httpd setroubleshoot setools policycoreut  
ils policycoreutils-python  
[sudo] password for triettm:  
Loaded plugins: fastestmirror, langpacks  
Loading mirror speeds from cached hostfile  
* base: mirrors.vhost.vn  
* extras: mirrors.vhost.vn  
* updates: mirrors.nhanhoa.com  
Package httpd-2.4.6-98.el7.centos.6.x86_64 already installed and latest version  
Package setroubleshoot-3.2.30-8.el7.x86_64 already installed and latest version  
Package setools-3.3.8-4.el7.x86_64 already installed and latest version  
Package policycoreutils-2.5-34.el7.x86_64 already installed and latest version  
Package policycoreutils-python-2.5-34.el7.x86_64 already installed and latest v  
ersion  
Nothing to do  
[triettm@triettm ~]$
```

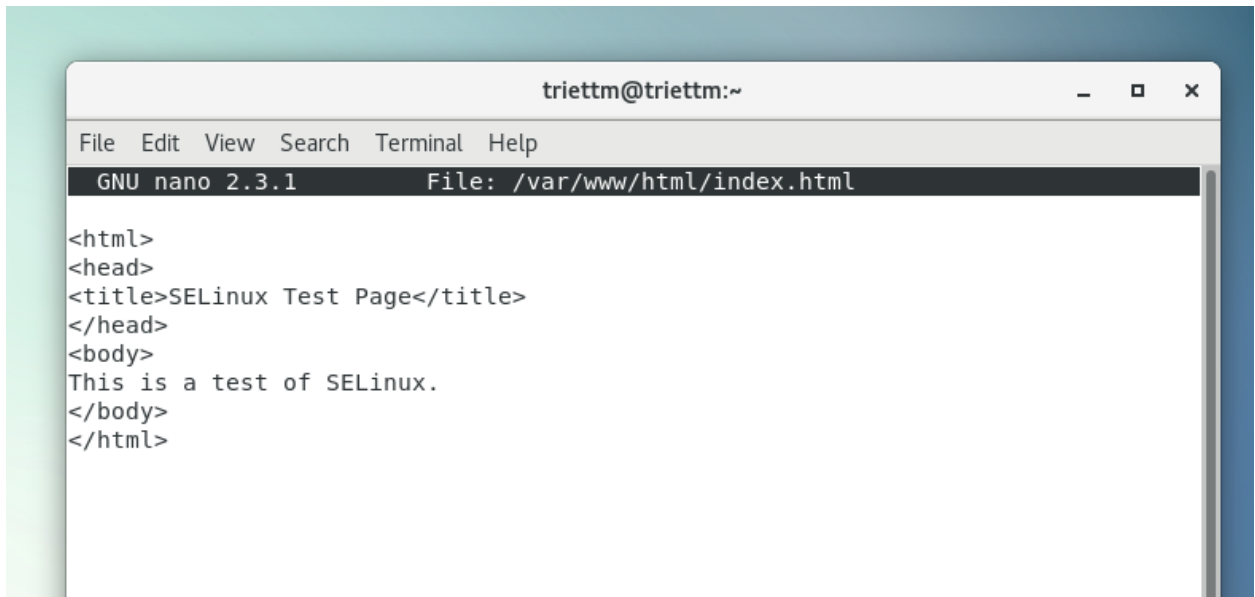
2. Khởi động lại quá trình troubleshoot bằng cách restart auditd

```
[triettm@triettm ~]$ sudo service auditd restart  
Stopping logging: [ OK ]  
Redirecting start to /bin/systemctl start auditd.service  
[triettm@triettm ~]$
```

3. Khởi động lại dịch vụ Apache và mở port 80 của tường lửa

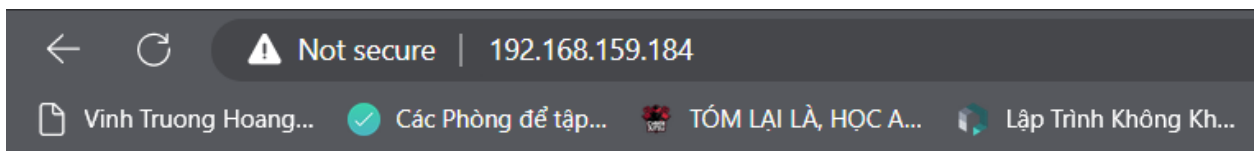
```
[triettm@triettm ~]$ sudo systemctl enable --now httpd  
[triettm@triettm ~]$ sudo firewall-cmd --permanent --add-service=http  
Warning: ALREADY_ENABLED: http  
success  
[triettm@triettm ~]$ sudo firewall-cmd --reload  
success  
[triettm@triettm ~]$
```

4. Đến đường dẫn /var/www/html directory, và tạo file index.html chứa nội dung web



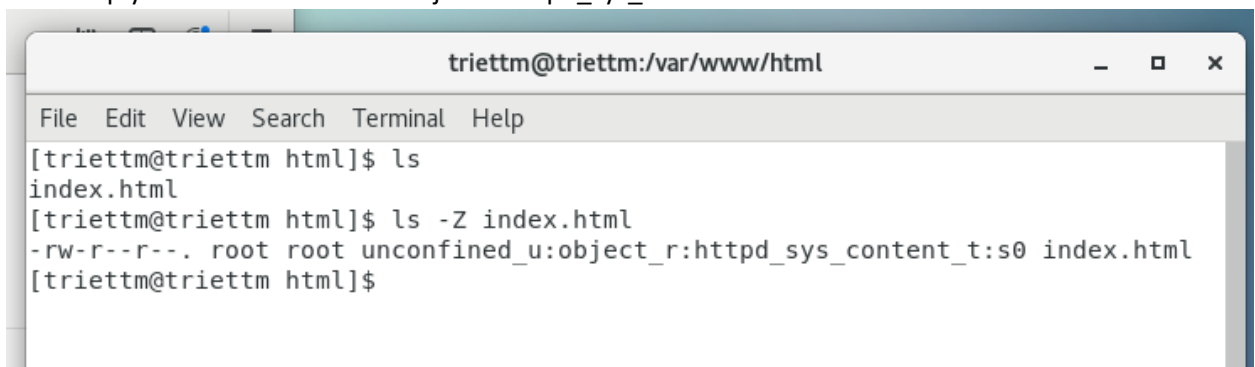
```
triettm@triettm:~  
File Edit View Search Terminal Help  
GNU nano 2.3.1 File: /var/www/html/index.html  
  
<html>  
<head>  
<title>SELinux Test Page</title>  
</head>  
<body>  
This is a test of SELinux.  
</body>  
</html>
```

Chúng ta đã dựng thành công trang web tĩnh đầu tiên



This is a test of SELinux.

Ta xem quyền SELinux của file có object là httpd_sys_content

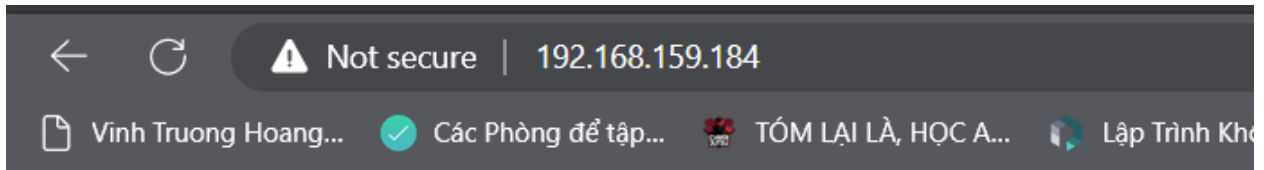


```
triettm@triettm:/var/www/html  
File Edit View Search Terminal Help  
[triettm@triettm html]$ ls  
index.html  
[triettm@triettm html]$ ls -Z index.html  
-rw-r--r--. root root unconfined_u:object_r:httpd_sys_content_t:s0 index.html  
[triettm@triettm html]$
```

Ta tiến hành sửa lại quyền SELinux thành object tmp_t

```
[triетtm@triетtm html]$ sudo chcon -t tmp_t index.html
[sudo] password for triетtm:
[triетtm@triетtm html]$ ls -Z index.html
-rw-r--r--. root root unconfined_u:object_r:tmp_t:s0 index.html
[triетtm@triетtm html]$
```

Lúc này ta không còn quyền để đọc file index.html nên load lại trang web trả về status code 403 không cho đọc nữa



Forbidden

You don't have permission to access /index.html on this server.

Nếu ta sử dụng câu lệnh restorecon thì quyền object SELinux sẽ được khôi phục lại như cũ

```
-rw-r--r--. root root unconfined_u:object_r:tmp_t:s0 index.html
[triетtm@triетtm html]$ sudo chcon -t tmp_t index.htm
[triетtm@triетtm html]$ sudo restorecon index.html
[triетtm@triетtm html]$ ls
index.htm index.html
[triетtm@triетtm html]$ ls -lZ
-rw-rw-r--. triетtm triетtm unconfined_u:object_r:tmp_t:s0 index.htm
-rw-r--r--. root root unconfined_u:object_r:httpd_sys_content_t:s0 index.html
[triетtm@triетtm html]$
```

Hands-on lab – SELinux Booleans and ports

```
triettm@triettm:/var/www/html
File Edit View Search Terminal Help
[triettm@triettm html]$ sudo semanage port -l | grep 'http'
[sudo] password for triettm:
http_cache_port_t      tcp      8080, 8118, 8123, 10001-10010
http_cache_port_t      udp      3130
http_port_t            tcp      80, 81, 443, 488, 8008, 8009, 8443, 9000
pegasus_http_port_t    tcp      5988
pegasus_https_port_t   tcp      5989
[triettm@triettm html]$
```

Câu lệnh trên cho ta biết SELinux cho phép service Apache chạy trên những port nào

```
[triettm@triettm html]$ sudo systemctl restart httpd
[triettm@triettm html]$
```

Restart lại service

```
triettm@triettm:/var/www/html
File Edit View Search Terminal Help
Mar  6 10:50:37 triettm dhclient[10547]: DHCPDISCOVER on virbr0 to 255.255.255.255 port 67 interval 21 (xid=0x1b5e1e4)
Mar  6 10:50:58 triettm dhclient[10547]: DHCPDISCOVER on virbr0 to 255.255.255.255 port 67 interval 19 (xid=0x1b5e1e4)
Mar  6 10:51:17 triettm dhclient[10547]: DHCPDISCOVER on virbr0 to 255.255.255.255 port 67 interval 14 (xid=0x1b5e1e4)
Mar  6 10:51:31 triettm dhclient[10547]: No DHCP OFFERS received.
Mar  6 10:51:31 triettm dhclient[10547]: No working leases in persistent database - sleeping.
Mar  6 10:52:28 triettm dhclient[10547]: DHCPDISCOVER on virbr0-nic to 255.255.255.255 port 67 interval 5 (xid=0xd8d39a3)
Mar  6 10:52:33 triettm dhclient[10547]: DHCPDISCOVER on virbr0-nic to 255.255.255.255 port 67 interval 11 (xid=0xd8d39a3)
Mar  6 10:52:41 triettm systemd: Stopping The Apache HTTP Server...
Mar  6 10:52:42 triettm systemd: Stopped The Apache HTTP Server.
Mar  6 10:52:42 triettm systemd: Starting The Apache HTTP Server...
Mar  6 10:52:42 triettm systemd: Started The Apache HTTP Server.
Mar  6 10:52:44 triettm dhclient[10547]: DHCPDISCOVER on virbr0-nic to 255.255.255.255 port 67 interval 10 (xid=0xd8d39a3)
Mar  6 10:52:54 triettm dhclient[10547]: DHCPDISCOVER on virbr0-nic to 255.255.255.255 port 67 interval 14 (xid=0xd8d39a3)
Mar  6 10:53:08 triettm dhclient[10547]: DHCPDISCOVER on virbr0-nic to 255.255.255.255 port 67 interval 11 (xid=0xd8d39a3)
[triettm@triettm html]$
```

Thêm vào SELinux port 82 cho phép service Apache chạy trên port này

```
triettm@triettm:/var/www/html
File Edit View Search Terminal Help
zented_port_t      tcp      1229
zented_port_t      udp      1229
zookeeper_client_port_t  tcp      2181
zookeeper_election_port_t  tcp      3888
zookeeper_leader_port_t    tcp      2888
zope_port_t        tcp      8021
[triettm@triettm html]$ sudo semanage port -l | grep 82
amanda_port_t      udp      10080-10082
collectd_port_t    udp      25826
fac_restore_port_t tcp      5582
fac_restore_port_t udp      5582
hplip_port_t       tcp      1782, 2207, 2208, 8290, 8292, 9100, 9101, 9102, 9220, 9221, 9222, 9280, 9281, 9282, 9290, 9291, 50000, 50002
http_port_t        tcp      82, 80, 81, 443, 488, 8008, 8009, 8443, 9000
pki_ca_port_t      tcp      829, 9180, 9701, 9443-9447
squid_port_t       tcp      3128, 3401, 4827
squid_port_t       udp      3401, 4827
trivnet1_port_t    tcp      8200
trivnet1_port_t    udp      8200
us_cli_port_t      tcp      8082, 8083
us_cli_port_t      udp      8082, 8083
varnishd_port_t    tcp      6081-6082
[triettm@triettm html]$
```

Ta có thể thấy chúng ta đã thành công thêm port 82 cho chạy service httpd Apache


```
triettm@triettm:/var/www/html
File Edit View Search Terminal Help
GNU nano 2.3.1 File: /etc/httpd/conf/httpd.conf

# 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'.

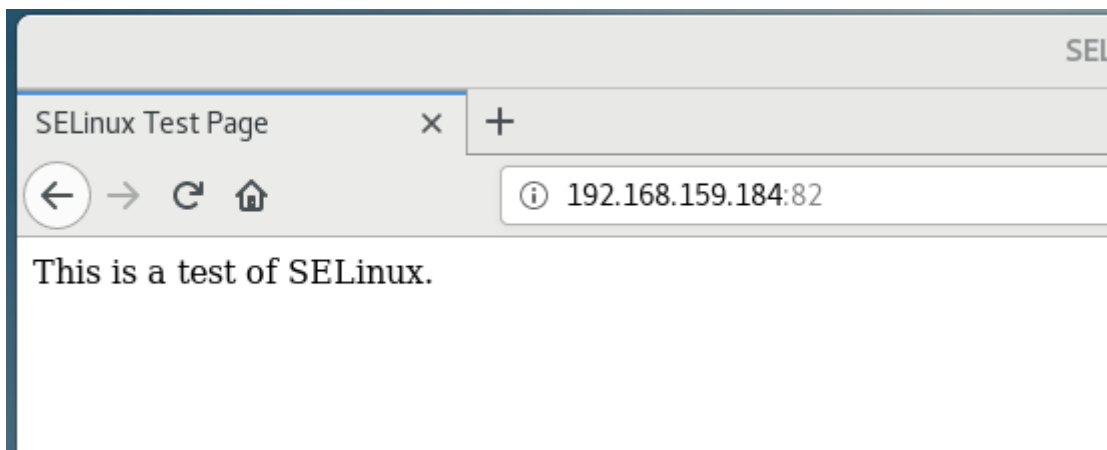
#
# ServerRoot: The top of the directory tree under which the server's
# configuration, error, and log files are kept.
#
# Do not add a slash at the end of the directory path.  If you point
# ServerRoot at a non-local disk, be sure to specify a local disk on the
# Mutex directive, if file-based mutexes 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 specific IP addresses as shown below to
# prevent Apache from glomming onto all bound IP addresses.
#
#Listen 12.34.56.78:80
Listen 82

#
# 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.

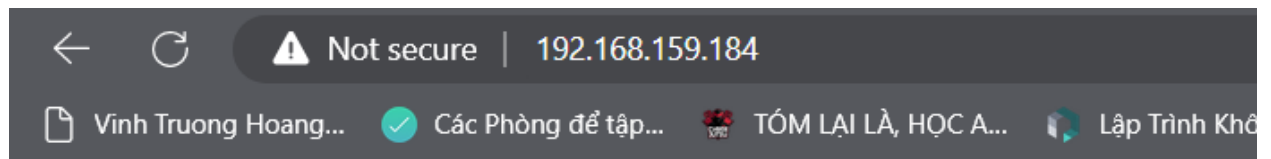
^G Get Help      ^O WriteOut      ^R Read File     ^Y Prev Page
^X Exit          ^J Justify       ^W Where Is      ^V Next Page
^K C
^U L
```

Ngoài ra ta cần phải sửa config của file httpdconf chuyển service Apache listen trên port 82.



Vậy là ta đã có thể truy cập vào trang web bằng port mới

```
triettm@triettm:~  
File Edit View Search Terminal Help  
[triettm@triettm ~]$ sudo semanage -d 82 -t http_port_t -p tcp  
[sudo] password for triettm:  
usage: semanage [-h]  
                {import,export,login,user,port,ibpkey,ibendport,interface,module,node,fcontext,boolean,permissive,dontaudit  
                ...  
semanage: error: argument subcommand: invalid choice: '82' (choose from 'import', 'export', 'login', 'user', 'port', 'ibpke  
ort', 'interface', 'module', 'node', 'fcontext', 'boolean', 'permissive', 'dontaudit')  
[triettm@triettm ~]$
```



This is a test of SELinux.

Chúng ta trả về lại port 80 và vô lại bth.