

## LAB 07

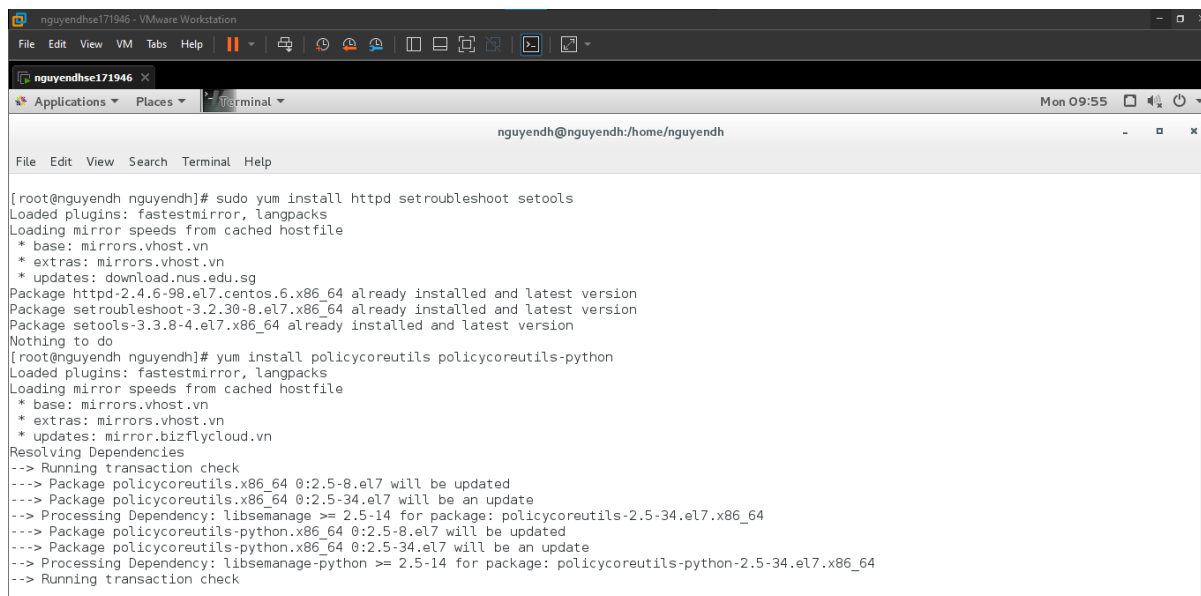
Thầy Mai Hoàng Đình  
Trường đại học FPT

Người thực hiện

Đặng Hoàng Nguyên

## SELinux type enforcement

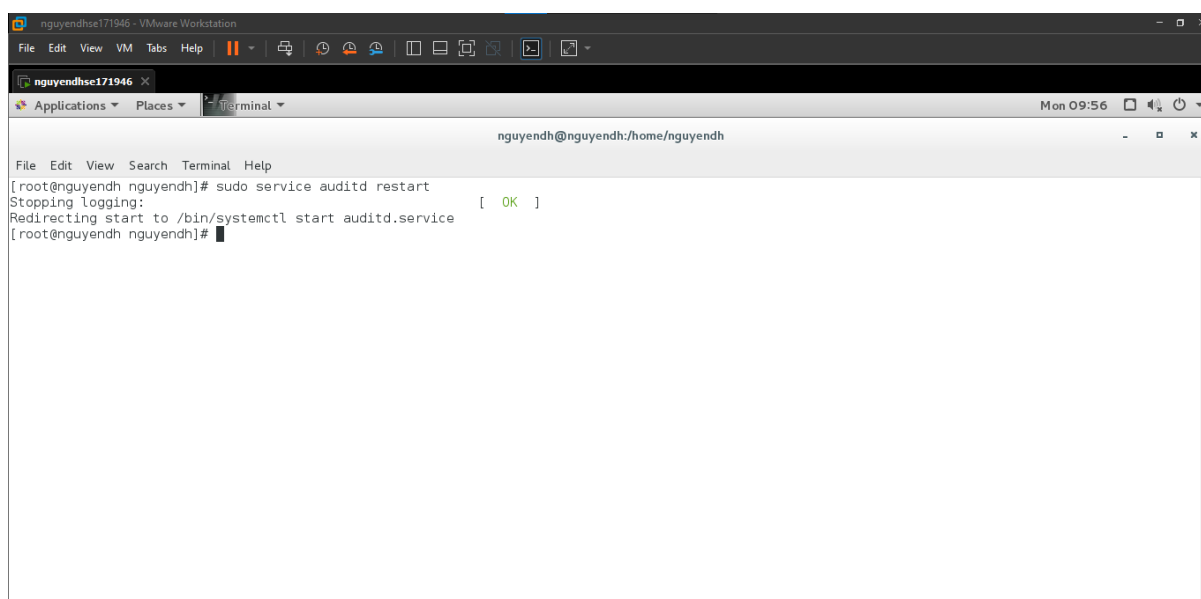
Cài đặt gói cần thiết thông qua lệnh yum install, nếu có tiến trình đang chạy yum thì hấn câu lệnh kill -9 pid. Sau đó cài đặt lại như bình thường



```
nguyendh@nguyendh:/home/nguyendh
File Edit View Search Terminal Help

[root@nguyendh nguyendh]# sudo yum install httpd setroubleshoot setools
Loaded plugins: fastestmirror, langpacks
Loading mirror speeds from cached hostfile
 * base: mirrors.vhost.vn
 * extras: mirrors.vhost.vn
 * updates: download.nus.edu.sg
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
Nothing to do
[root@nguyendh nguyendh]# yum install policycoreutils policycoreutils-python
Loaded plugins: fastestmirror, langpacks
Loading mirror speeds from cached hostfile
 * base: mirrors.vhost.vn
 * extras: mirrors.vhost.vn
 * updates: mirror.bizflycloud.vn
Resolving Dependencies
--> Running transaction check
--> Package policycoreutils.x86_64 0:2.5-8.el7 will be updated
--> Package policycoreutils.x86_64 0:2.5-34.el7 will be an update
--> Processing Dependency: libsemanage >= 2.5-14 for package: policycoreutils-2.5-34.el7.x86_64
--> Package policycoreutils-python.x86_64 0:2.5-8.el7 will be updated
--> Package policycoreutils-python.x86_64 0:2.5-34.el7 will be an update
--> Processing Dependency: libsemanage-python >= 2.5-14 for package: policycoreutils-python-2.5-34.el7.x86_64
--> Running transaction check
```

Sau khi cài đặt xong, khởi động lại audit để kiểm soát hệ thống thông qua câu lệnh:  
**service auditd restart**

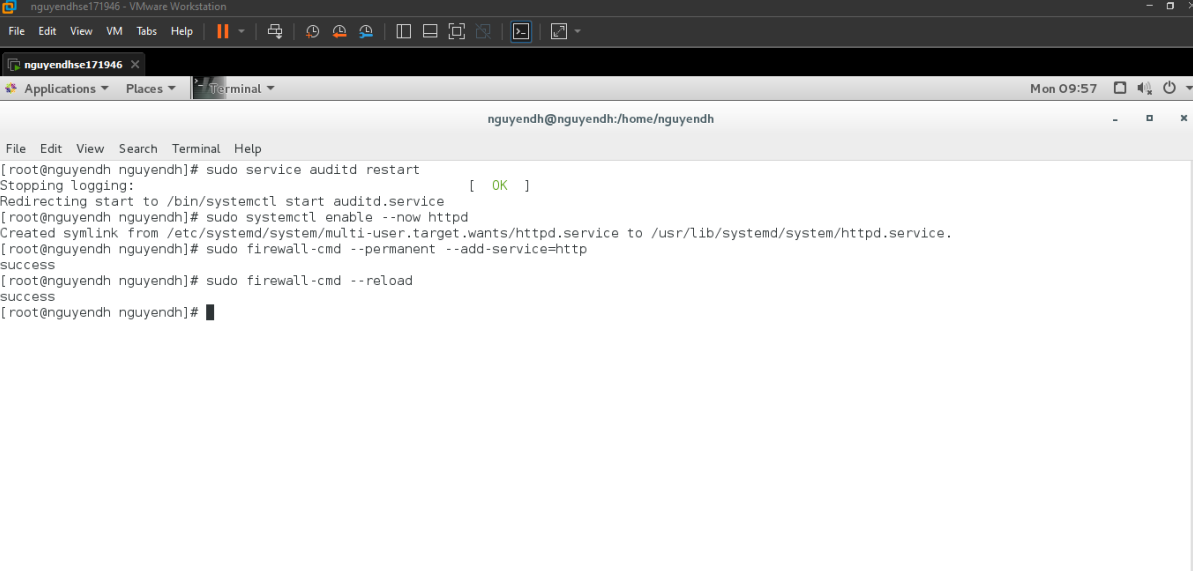


```
nguyendh@nguyendh:/home/nguyendh
File Edit View Search Terminal Help

[root@nguyendh nguyendh]# sudo service auditd restart
Stopping logging: [ OK ]
Redirecting start to /bin/systemctl start auditd.service
[root@nguyendh nguyendh]#
```

Sau đó chúng ta sẽ bắt đầu kích hoạt và khởi động dịch vụ Apache trên port 80. port 80 là port dành cho http với các câu lệnh sau:

- **systemctl enable --now httpd** Đây là câu lệnh cho phép chúng ta có thể kích hoạt ngay lập tức dịch vụ httpd
- **sudo firewall-cmd --permanent --add-service=http**: câu lệnh này cho phép chúng ta sẽ cho firewall mở port 80 để truy cập
- **sudo firewall-cmd --reload**: Câu lệnh này cho phép chúng ta reload lại firewall sau khi cấu hình xong firewall mở thêm port 80

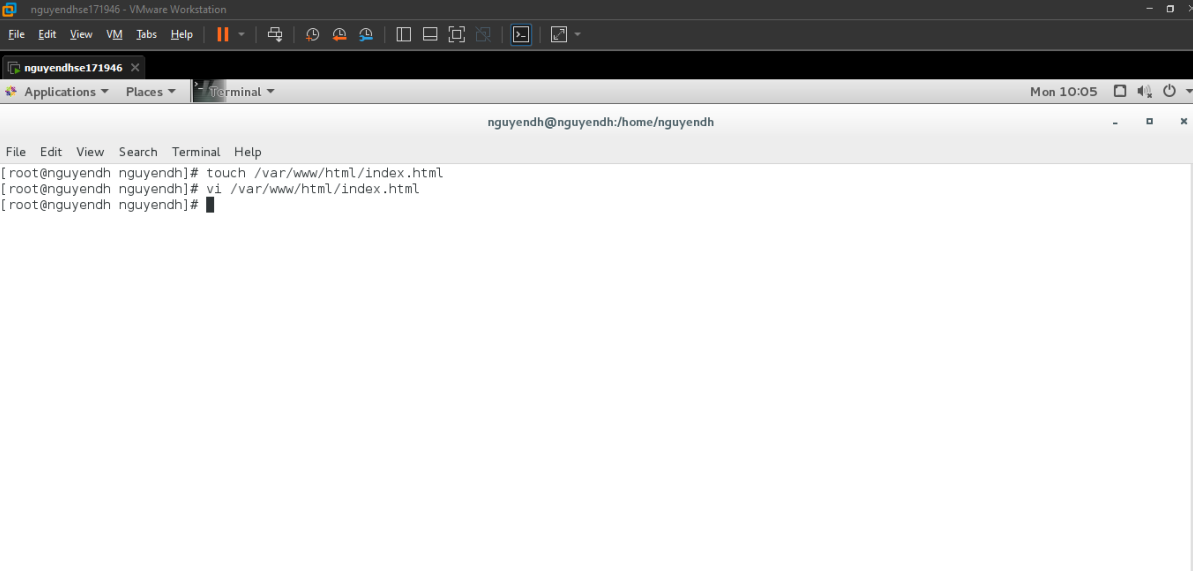


```

[nguyendhse171946 - VMware Workstation]
File Edit View VM Tabs Help
nguyendhse171946
Applications Places Terminal
Mon 09:57
nguyendh@nguyendh:/home/nguyendh
File Edit View Search Terminal Help
[root@nguyendh nguyendh]# sudo service auditd restart
Stopping logging: [ OK ]
Redirecting start to /bin/systemctl start auditd.service
[root@nguyendh nguyendh]# sudo systemctl enable --now httpd
Created symlink from /etc/systemd/system/multi-user.target.wants/httpd.service to /usr/lib/systemd/system/httpd.service.
[root@nguyendh nguyendh]# sudo firewall-cmd --permanent --add-service=http
success
[root@nguyendh nguyendh]# sudo firewall-cmd --reload
success
[root@nguyendh nguyendh]#

```

Tạo một file index.html trong /var/www/html để giúp ta có thể có một file html giúp chúng ta có thể truy cập vào giao diện trang web. Sau đó thiết lập nội dung của trang theo như sau:



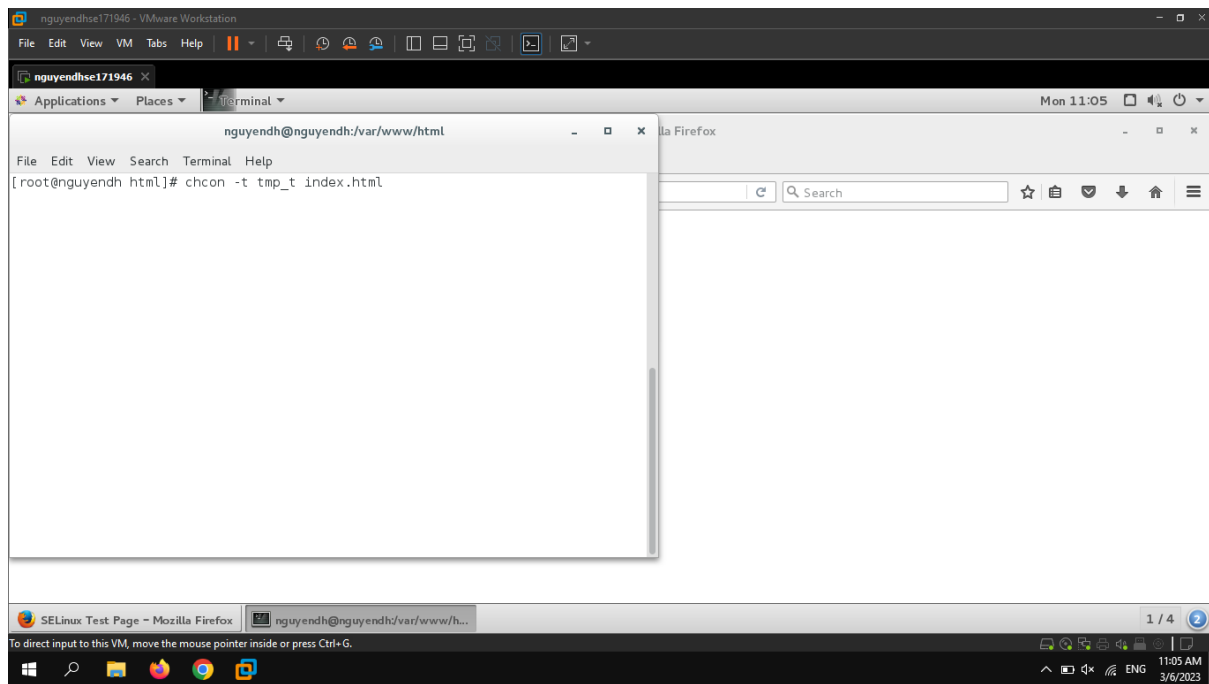
```

[nguyendhse171946 - VMware Workstation]
File Edit View VM Tabs Help
nguyendhse171946
Applications Places Terminal
Mon 10:05
nguyendh@nguyendh:/home/nguyendh
File Edit View Search Terminal Help
[root@nguyendh nguyendh]# touch /var/www/html/index.html
[root@nguyendh nguyendh]# vi /var/www/html/index.html
[root@nguyendh nguyendh]#

```

Như ta thấy ở hình dưới, ta sẽ cấu hình cho file html với thẻ tag của trang với tên là “Selinux test page” và trong phần body của nó có một dòng với tiêu đề là “This is a test of Selinux”

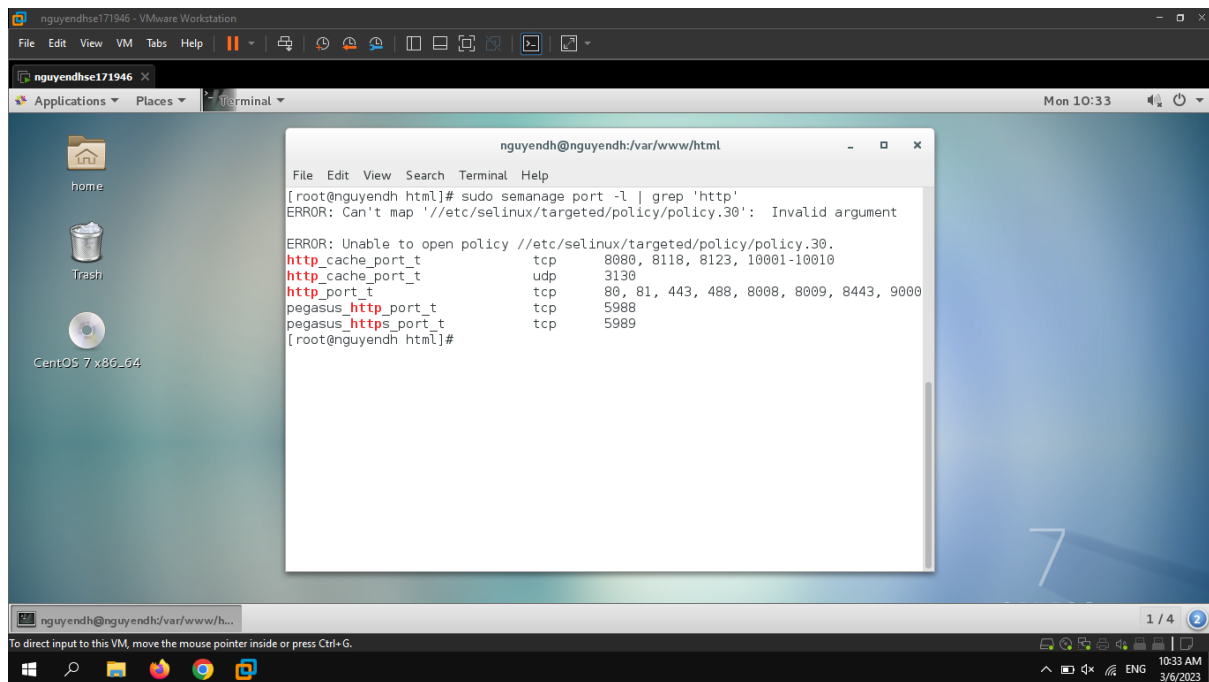




Sau đó chúng ta có thể thấy được rằng Website báo lỗi vì policy của linux không đúng. Sử dụng câu lệnh **“restorecon index.html”** để có thể khôi phục lại đúng cấu trúc của file index.html

## SELinux Booleans and ports

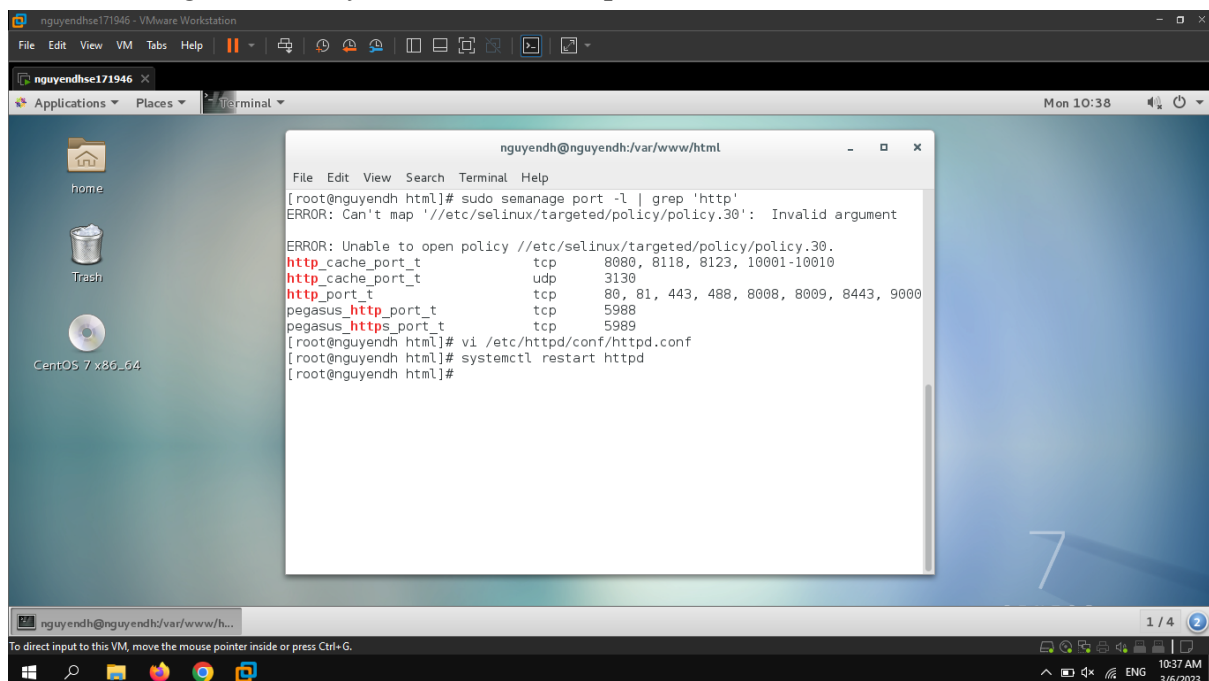
Câu lệnh "sudo semanage port -l | grep 'http'" được sử dụng để liệt kê danh sách các cổng mà SELinux hiện đang cấu hình trên hệ thống, và sau đó lọc kết quả để chỉ hiển thị những cổng liên quan đến HTTP.



```
nguyendh@nguyendh:var/www/html
File Edit View Search Terminal Help
[root@nguyendh html]# sudo semanage port -l | grep 'http'
ERROR: Can't map '//etc/selinux/targeted/policy/policy.30': Invalid argument

ERROR: Unable to open policy //etc/selinux/targeted/policy/policy.30.
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
[root@nguyendh html]#
```

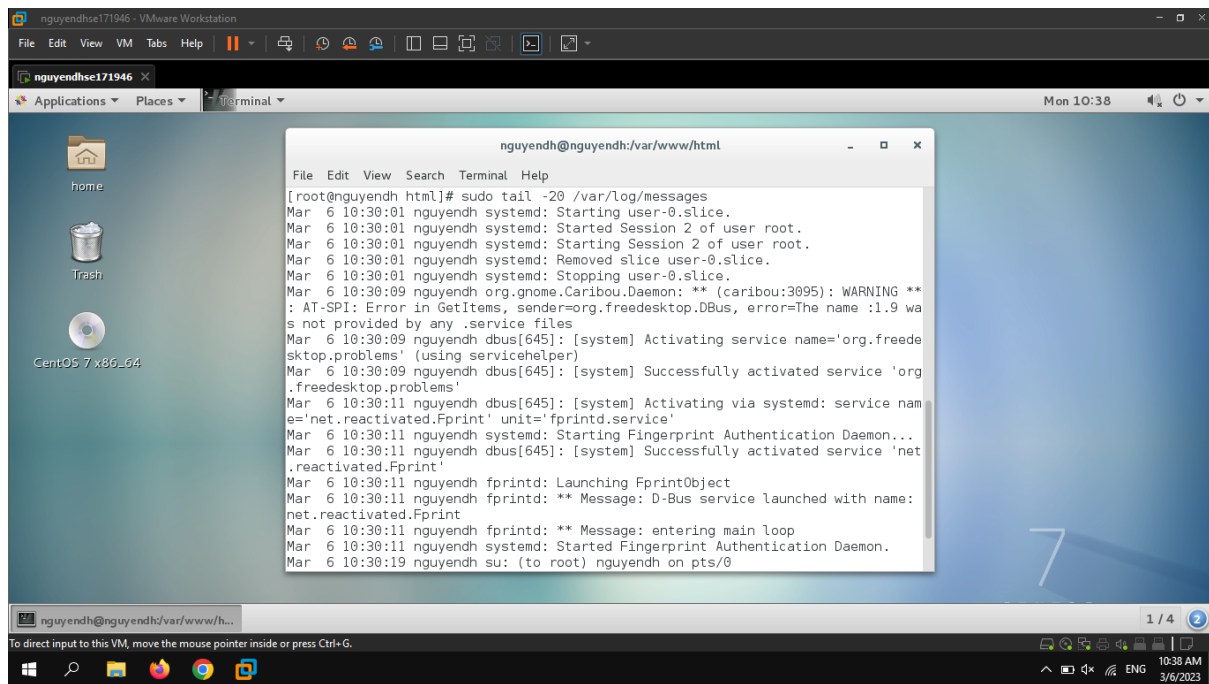
Vào thư mục /etc/httpd/conf và chỉnh lại file text httpd.conf, chỉnh cổng từ 80 thành 82 và sử dụng câu lệnh systemctl restart httpd



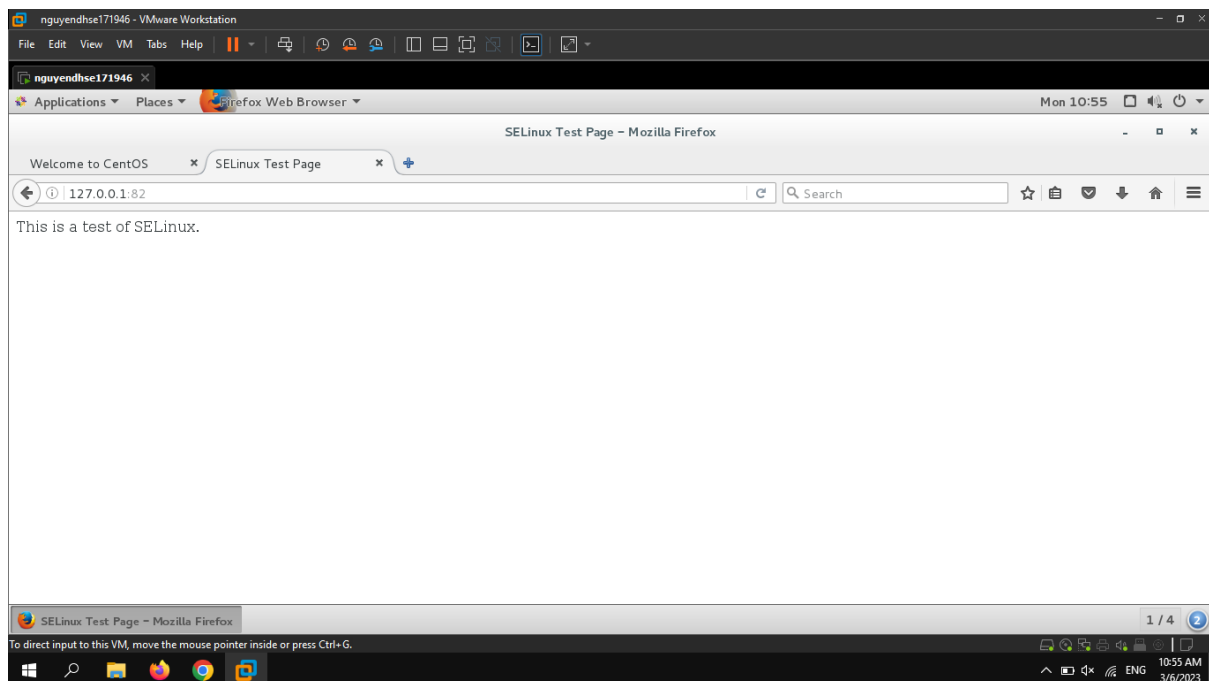
```
nguyendh@nguyendh:var/www/html
File Edit View Search Terminal Help
[root@nguyendh html]# sudo semanage port -l | grep 'http'
ERROR: Can't map '//etc/selinux/targeted/policy/policy.30': Invalid argument

ERROR: Unable to open policy //etc/selinux/targeted/policy/policy.30.
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
[root@nguyendh html]# vi /etc/httpd/conf/httpd.conf
[root@nguyendh html]# systemctl restart httpd
[root@nguyendh html]#
```

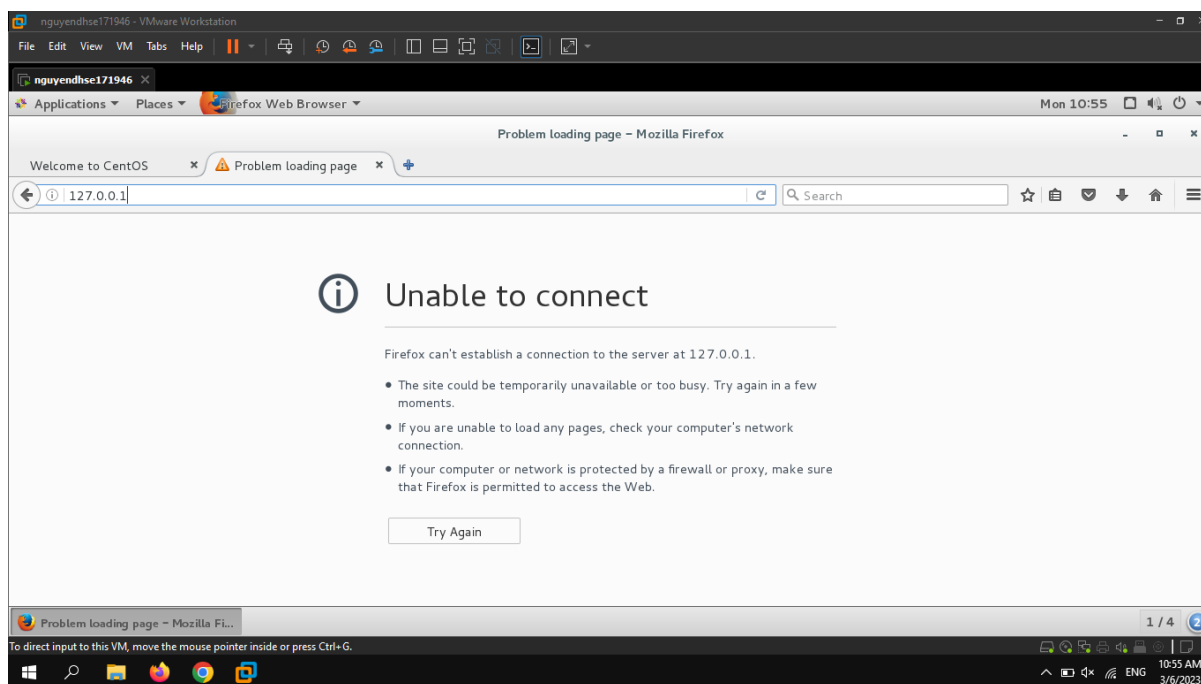
Sử dụng câu lệnh tail -20 /var/log/messages để xem được thông báo lỗi



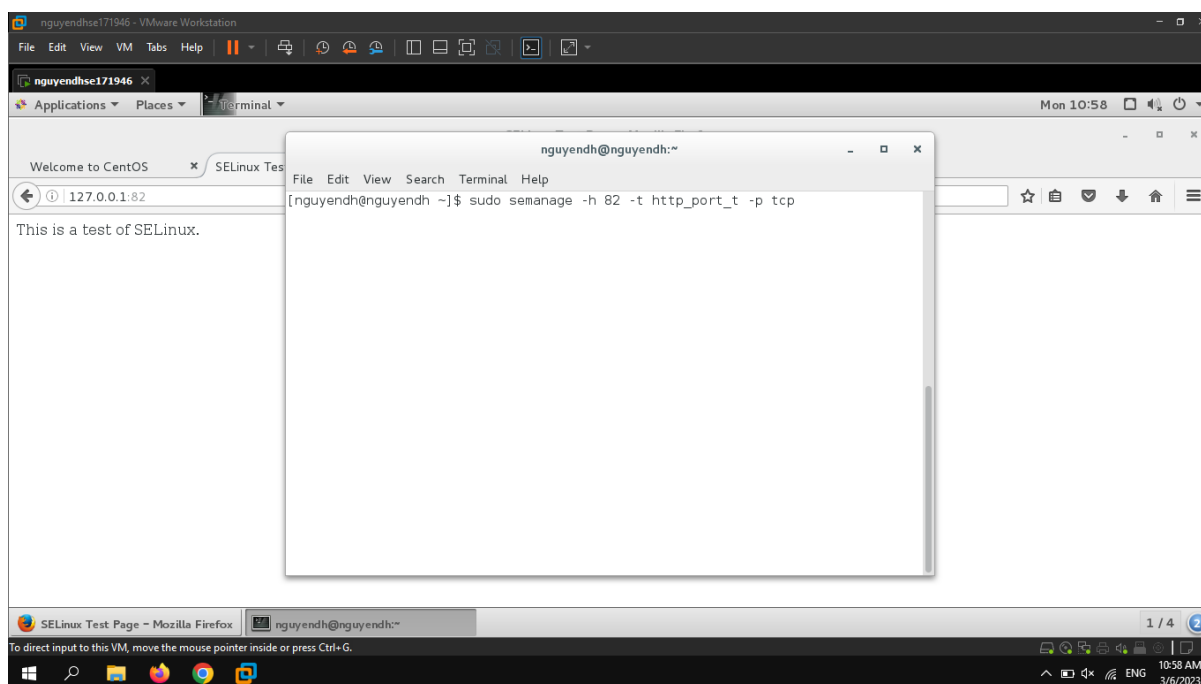
Sau đó sử dụng câu lệnh `semanage port -a 82 -t http_port_t -p tcp` để có thể thêm một port mới là port 82 vào trong danh sách những port được mở. Kiểm tra bằng lệnh `semanage port -l` và sau đó restart lại httpd. Kiểm tra bằng cash vào thử website “127.0.0.1”



Ta có thể thấy rằng, do thay thế bằng port 82 nên giờ chỉ có thằng port 82 có thể vào được

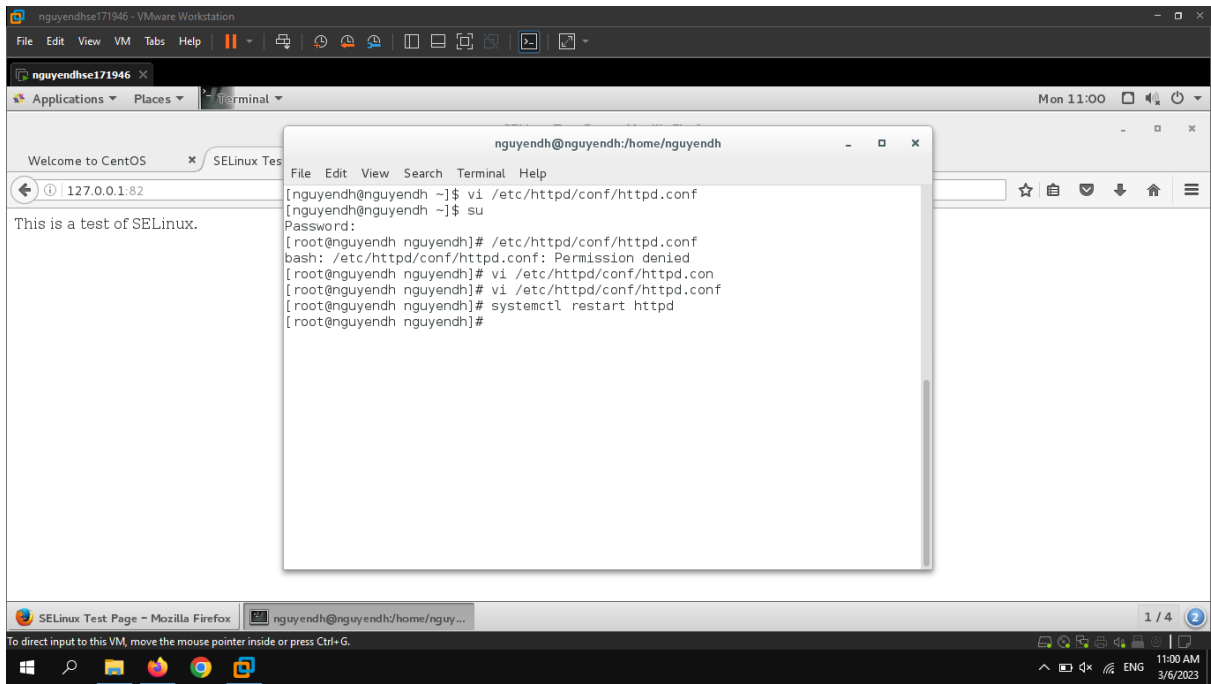


Sau đó xóa cổng 82. Chúng ta sẽ xóa cổng TCP 82 khỏi danh sách cổng được phép truy cập trên SELinux. Kể từ đó, tiến trình không được phép sử dụng cổng này trên hệ thống của chúng ta trừ khi ta cấu hình lại SELinux cho phép truy cập vào cổng này.



Sau đó chúng ta vào file `/etc/httpd/conf/httpd.conf` để chỉnh cổng thành 80 và khởi động lại dịch vụ bằng **`systemctl restart httpd`**





Mở lại thử bằng port 80 thì ta đã có lại

