

**HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG
KHOA AN TOÀN THÔNG TIN**



**BÁO CÁO BÀI THỰC HÀNH
HỌC PHẦN: AN TOÀN MẠNG NÂNG CAO
MÃ HỌC PHẦN: INT1483**

BÀI THỰC HÀNH
Tìm hiểu về proxy

Sinh viên thực hiện: Trần Thị Thu Phương

Mã sinh viên: B21DCAT151

Giảng viên hướng dẫn: TS. Phạm Hoàng Duy

HỌC KỲ 2 NĂM HỌC 2024-202

Tải bài lab nếu chưa có:

imodule <https://github.com/thang010501/ptit-proxy/raw/main/imodule.tar>

Khởi động bài lab: vào terminal, gõ:

labtainer -r ptit-proxy

(chú ý: sinh viên sử dụng mã sinh viên của mình để nhập thông tin MSV người thực hiện bài lab khi có yêu cầu, để sử dụng khi chấm điểm)

Cài đặt proxy server (Cài đặt squid và khởi động)

Chạy lệnh: `sudo nano /etc/squid/squid.conf`

Ở máy proxy thêm các dòng cấu hình:

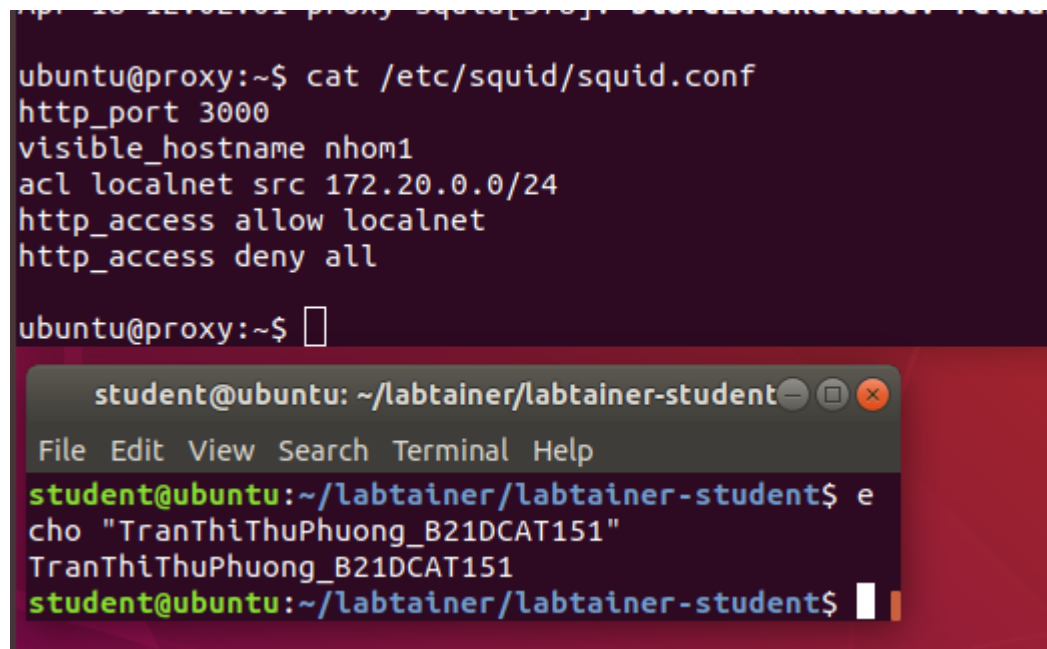
`http_port 3000` # Cổng dùng để lắng nghe các yêu cầu HTTP

`visible_hostname nhom1` # Tên của máy chủ proxy

`acl localnet src 172.20.0.0/24` # Địa chỉ IP của mạng nội bộ

`http_access allow localnet` # Cho phép truy cập từ mạng nội bộ

`http_access deny all` # Tất cả các yêu cầu khác bị từ chối



```
ubuntu@proxy:~$ cat /etc/squid/squid.conf
http_port 3000
visible_hostname nhom1
acl localnet src 172.20.0.0/24
http_access allow localnet
http_access deny all

ubuntu@proxy:~$
```

```
student@ubuntu: ~/labtainer/labtainer-student
File Edit View Search Terminal Help
student@ubuntu:~/labtainer/labtainer-student$ e
cho "TranThiThuPhuong_B21DCAT151"
TranThiThuPhuong_B21DCAT151
student@ubuntu:~/labtainer/labtainer-student$
```

Chạy dòng lệnh ở terminal: `sudo squid -k parse` (kiểm tra xem có báo lỗi cấu hình không).

Chạy lệnh ở terminal proxy: `netstat -an | grep ESTABLISHED | grep :3000` (dùng để lắng nghe)

```
ubuntu@proxy:~$ netstat -an | grep ESTABLISHED | grep :3000
tcp        0      0 172.20.0.2:3000      172.20.0.3:44830     ESTABLISHED
tcp        0      0 172.20.0.2:3000      172.20.0.3:44834     ESTABLISHED
tcp        0      0 172.20.0.2:3000      172.20.0.3:44838     ESTABLISHED
ubuntu@proxy:~$ echo "TranThiThuPhuong_B21DCAT151"
TranThiThuPhuong_B21DCAT151
ubuntu@proxy:~$
```

Cấu hình logging

ở máy proxy, chạy lệnh `sudo nano /etc/squid/squid.conf`

thêm 5 dòng cấu hình :

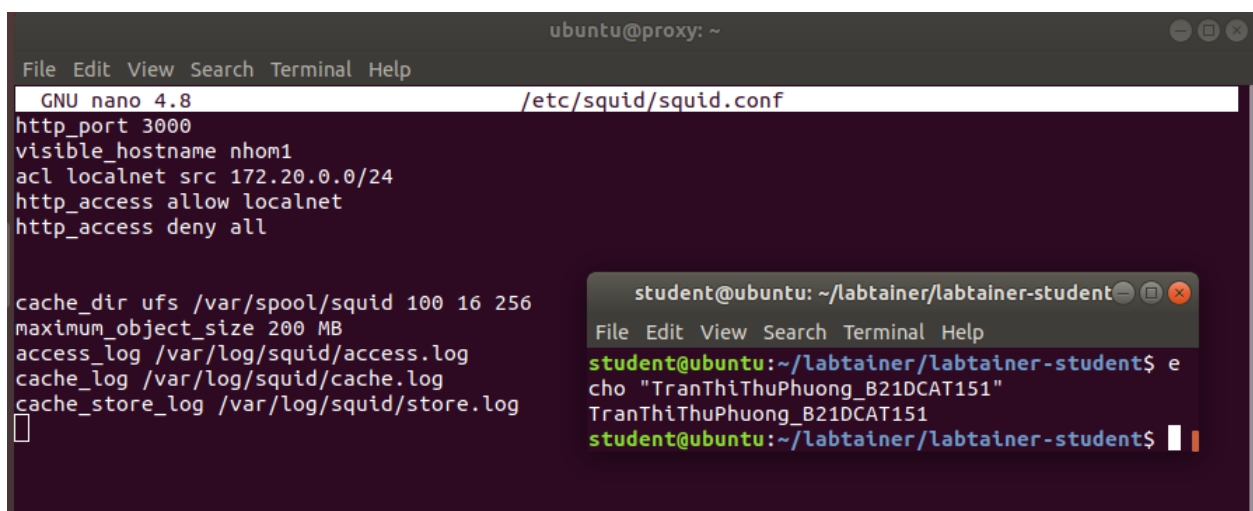
`cache_dir ufs /var/spool/squid 100 16 256`

`maximum_object_size 200 MB`

`access_log /var/log/squid/access.log` # xác định nơi Squid ghi log về các hoạt động truy cập mạng

`cache_log /var/log/squid/cache.log` #xác định nơi Squid ghi log về hoạt động của bộ đệm

`cache_store_log /var/log/squid/store.log` # Tùy chọn này xác định nơi Squid ghi log về việc lưu trữ các đối tượng vào bộ đệm



```
ubuntu@proxy: ~
File Edit View Search Terminal Help
GNU nano 4.8 /etc/squid/squid.conf
http_port 3000
visible_hostname nhom1
acl localnet src 172.20.0.0/24
http_access allow localnet
http_access deny all

cache_dir ufs /var/spool/squid 100 16 256
maximum_object_size 200 MB
access_log /var/log/squid/access.log
cache_log /var/log/squid/cache.log
cache_store_log /var/log/squid/store.log

```

```
student@ubuntu: ~/labtainer/labtainer-student
File Edit View Search Terminal Help
student@ubuntu:~/labtainer/labtainer-student$ e
cho "TranThiThuPhuong_B21DCAT151"
TranThiThuPhuong_B21DCAT151
student@ubuntu:~/labtainer/labtainer-student$
```

`sudo systemctl restart squid` (khởi động lại squid)

```
ubuntu@proxy:~$ sudo systemctl restart squid

student@ubuntu: ~/labtainer/labtainer-student
File Edit View Search Terminal Help
student@ubuntu:~/labtainer/labtainer-student$ echo "TranThiThuPhuong_B21DCAT151"
TranThiThuPhuong_B21DCAT151
student@ubuntu:~/labtainer/labtainer-student$
```

sudo tail -f /var/log/squid/access.log (xem log hoạt động truy cập của proxy)

```
ubuntu@proxy:~$ sudo tail -f /var/log/squid/access.log
1744992912.808      84 172.20.0.3 TCP_MISS/200 626 POST http://o.pki.goog/we2 - HIER_DIRECT/142.25
0.76.227 application/ocsp-response
1744992912.823      88 172.20.0.3 TCP_MISS/200 626 POST http://o.pki.goog/we2 - HIER_DIRECT/142.25
0.76.227 application/ocsp-response
1744992912.872     125 172.20.0.3 TCP_MISS/200 626 POST http://o.pki.goog/we2 - HIER_DIRECT/142.25
0.76.227 app
student@ubuntu: ~/labtainer/labtainer-student
File Edit View Search Terminal Help
student@ubuntu:~/labtainer/labtainer-student$ echo "TranThiThuPhuong_B21DCAT151"
TranThiThuPhuong_B21DCAT151
1744992912.872     125 172.20.0.3 TCP_MISS/200 626 POST http://o.pki.goog/we2 - HIER_DIRECT/142.25
0.76.227 app
student@ubuntu:~/labtainer/labtainer-student$ echo "TranThiThuPhuong_B21DCAT151"
TranThiThuPhuong_B21DCAT151
1744992912.872     125 172.20.0.3 TCP_MISS/200 626 POST http://o.pki.goog/we2 - HIER_DIRECT/142.25
0.76.227 app
student@ubuntu:~/labtainer/labtainer-student$
```

Tạo blacklist cấm truy cập web đen

Tạo file blacklist thuộc dạng txt để cấm truy cập vào facebook.com.

Chạy lệnh: sudo nano /etc/squid/blacklist.txt, nhập www.facebook.com, lưu vào file.

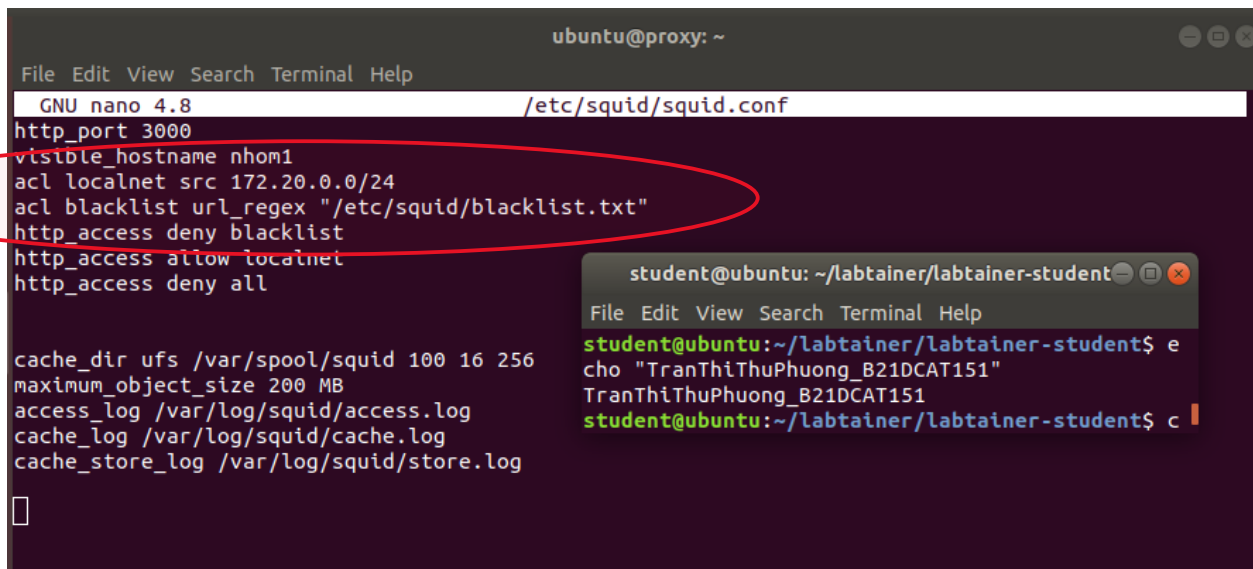
```
ubuntu@proxy: ~
File Edit View Search Terminal Help
GNU nano 4.8 /etc/squid/blacklist.txt
www.facebook.com
[]

student@ubuntu: ~/labtainer/labtainer-student
File Edit View Search Terminal Help
student@ubuntu:~/labtainer/labtainer-student$ echo "TranThiThuPhuong_B21DCAT151"
TranThiThuPhuong_B21DCAT151
student@ubuntu:~/labtainer/labtainer-student$ c
```

Mở sudo nano /etc/squid/squid.conf và thêm 2 dòng:

acl blacklist url_regex "/etc/squid/blacklist.txt"

http_access deny blacklist



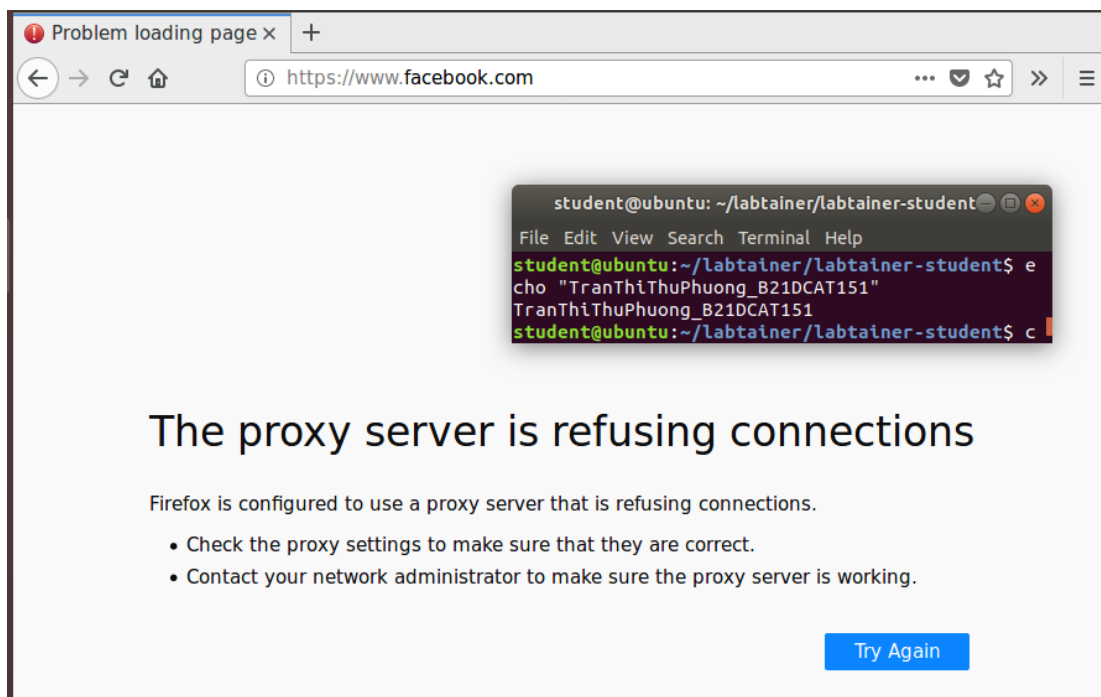
```
ubuntu@proxy: ~  
File Edit View Search Terminal Help  
GNU nano 4.8 /etc/squid/squid.conf  
http_port 3000  
visible_hostname nhom1  
acl localnet src 172.20.0.0/24  
acl blacklist url_regex "/etc/squid/blacklist.txt"  
http_access deny blacklist  
http_access allow localnet  
http_access deny all  
  
cache_dir ufs /var/spool/squid 100 16 256  
maximum_object_size 200 MB  
access_log /var/log/squid/access.log  
cache_log /var/log/squid/cache.log  
cache_store_log /var/log/squid/store.log  
  
[ ]
```

```
student@ubuntu: ~/labtainer/labtainer-student  
File Edit View Search Terminal Help  
student@ubuntu:~/labtainer/labtainer-student$ e  
cho "TranThiThuPhuong_B21DCAT151"  
TranThiThuPhuong_B21DCAT151  
student@ubuntu:~/labtainer/labtainer-student$ c
```

Chạy lệnh ở proxy để khởi động lại: `sudo systemctl restart squid`

`sudo tail -f /var/log/squid/access.log` (xem log hoạt động truy cập của proxy) (nếu không chạy lệnh này → không được Y)

Truy cập máy client: dùng firefox đăng nhập đường link www.facebook.com



Tạo whitelist chỉ cho phép truy cập vào một trang web nhất định

Tạo file whitelist thuộc dạng txt. //tạo một danh sách whitelist và thêm vào danh sách www.facebook.com

`sudo nano /etc/squid/whitelist.txt`

```
File Edit View Search Terminal Help
GNU nano 4.8 /etc/squid/whitelist.txt Modified
www.facebook.com
[ ]

student@ubuntu: ~/labtainer/labtainer-student
File Edit View Search Terminal Help
student@ubuntu:~/labtainer/labtainer-student$ e
cho "TranThiThuPhuong_B21DCAT151"
TranThiThuPhuong_B21DCAT151
student@ubuntu:~/labtainer/labtainer-student$ c
```

truy cập sudo nano /etc/squid/squid.conf và thêm 2 dòng:

acl whitelist url_regex "/etc/squid/whitelist.txt"

http_access deny !whitelist

// cấm truy cập hết ngoại trừ có trong danh sách whitelist.txt

```
File Edit View Search Terminal Help
GNU nano 4.8 /etc/squid/squid.conf
http_port 3000
visible_hostname nhom1
acl localnet src 172.20.0.0/24
acl whitelist url_regex "/etc/squid/whitelist.txt"
http_access deny !whitelist
http_access allow localnet
http_access deny all

cache_dir ufs /var/spool/squid 100 16 256
maximum_object_size 200 MB
access_log /var/log/squid/access.log
cache_log /var/log/squid/cache.log
cache_store_log /var/log/squid/store.log

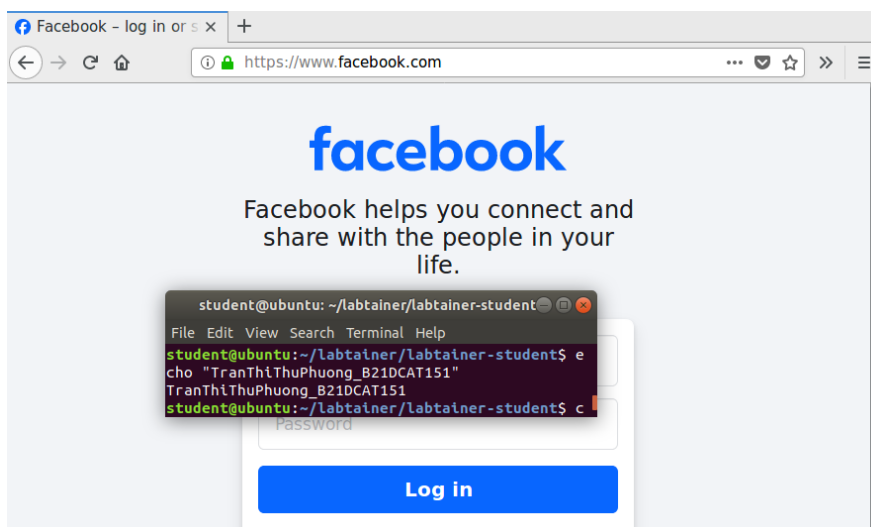
student@ubuntu: ~/labtainer/labtainer-student
File Edit View Search Terminal Help
student@ubuntu:~/labtainer/labtainer-student$ e
cho "TranThiThuPhuong_B21DCAT151"
TranThiThuPhuong_B21DCAT151
student@ubuntu:~/labtainer/labtainer-student$ c
```

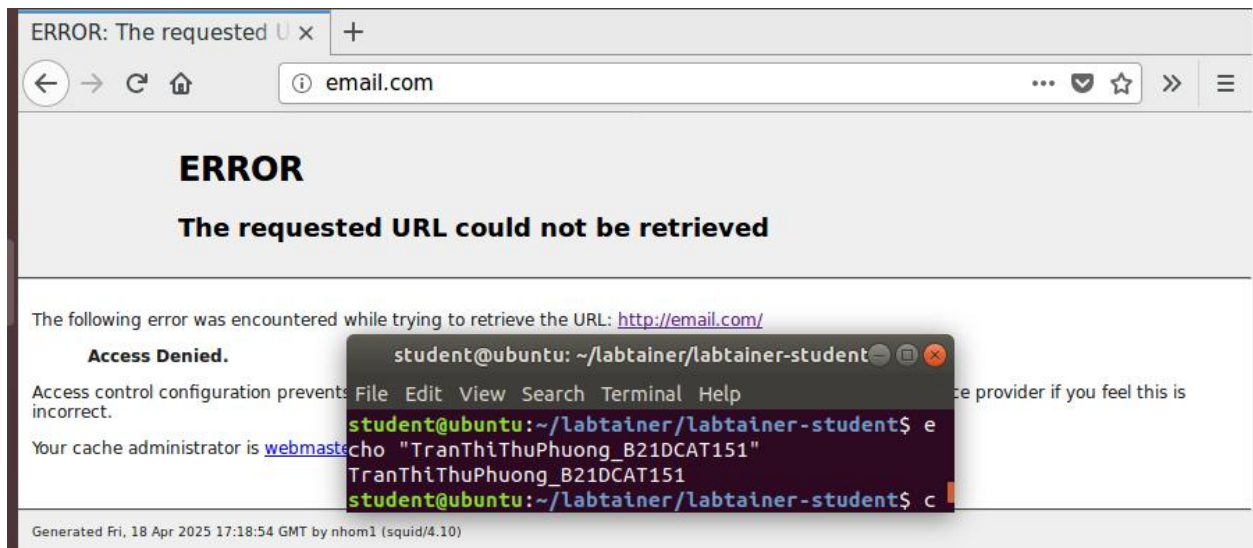
xóa www.facebook.com ra khỏi blacklist.txt

khởi động lại squid:

sudo tail -f /var/log/squid/access.log (xem log hoạt động truy cập của proxy)

truy cập máy client: dùng firefox đăng nhập đường link www.facebook.com. Và thử một số link khác như [youtube.com](https://www.youtube.com), [email.com](https://www.email.com),...





```
student@ubuntu:~/labtainer/labtainer-student$ checkwork
Results stored in directory: /home/student/labtainer_xfer/ptit-proxy

Labname ptit-proxy

Student | proxy_settings | log_configurati | black_lists | white_lists | user_management | Verify_proxy |
=====|=====|=====|=====|=====|=====|=====|
B21DCAT151 | Y | Y | Y | Y | | |
What is automatically assessed for this lab:

student@ubuntu:~/labtainer/labtainer-student$
student@ubuntu:~/labtainer/labtainer-student$ echo "Tran Thi Thu Phuong - B21DCAT151"
Tran Thi Thu Phuong - B21DCAT151
student@ubuntu:~/labtainer/labtainer-student$ echo "18/4/2025"
18/4/2025
student@ubuntu:~/labtainer/labtainer-student$
```

Kết thúc bài lab:

Trên terminal đầu tiên sử dụng câu lệnh sau để kết thúc bài lab:

stoplab

Khi bài lab kết thúc, một tệp zip lưu kết quả được tạo và lưu vào một vị trí được hiển thị bên dưới stoplab.

Lưu ý: checkwork đủ các mục proxy_settings | log_configurati | black_lists | white_lists là đạt.