Giới thiệu chung về bài thực hành

Tên bài thực hành: Tìm hiểu về proxy

Mã: ptit-proxy

Trong bài thực hành này, sinh viên làm quen với hoạt động của proxy.

# Nội dung và hướng dẫn bài thực hành

## *Mục đích*

Giúp sinh viên tìm hiểu các kiến thức về proxy, cài đặt và cấu hình proxy server sử dụng Squid

Hiểu và thực hành cách quản lý quyền truy cập qua proxy, sử dụng blacklist và whitelist để kiểm soát lưu lượng mạng

## Yêu cầu đối với sinh viên

Có kiến thức cơ bản về Wireshark

## Nội dung thực hành

Tải bài lab: 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 email 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 dòng cấu hình:

http\_port 3000 # Cổng lắng nghe yêu cầu HTTP

visible\_hostname nhom1 # Tên máy chủ proxy

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

http\_access deny blacklist # Cấm truy cập từ blacklist

http\_access allow localnet # Cho phép truy cập từ mạng nội bộ

http\_access deny all # Cấm tất cả các yêu cầu khác

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

Chạy dòng lệnh để khởi động squid: sudo systemctl start squid (khởi động squid)

Truy cập firefox bên client.

Chọn tùy chọn vào cài đặt. tìm proxy network chọn Manual proxy configuration nhập địa chỉ ip 172.20.0.2. và cổng kết nối là 3000.

Chọn Use this proxy server for all protocols ấn lưu.

Hình 5 Cấu hình browser

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

**Cấu hình loging**

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

thêm dòng cấu hình :

cache\_dir ufs /var/spool/squid 100 16 256

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

sudo systemctl restart squid (khởi động lại squid)



Hình 10 Khởi chạy squid

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

**Quản lý truy cập**

**Tạo blacklist cấm truy cập web đen**

// tạo file blacklist thuộc dạng txt. cấm truy cập vào facebook Chạy lệnh sudo nano /etc/squid/blacklist.txt

mở sudo nano /etc/squid/squid.conf và thêm dòng:

acl blacklist url\_regex "/etc/squid/blacklist.txt"

http\_access deny blacklist

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



Hình 16 Khởi động lại squid

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

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](http://www.facebook.com/)

sudo nano /etc/squid/whitelist.txt

truy cập sudo nano /etc/squid/squid.conf và thêm 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

xóa [www.facebook.com](http://www.facebook.com/) ra khỏi blacklist.txt

khởi động lại squid: sudo systemctl restart squid

sudo tail -f /var/log/squid/access\_squid.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 email.com,…

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.