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 tấn công MITM

Sinh viên thực hiện: Trần Thị Thu Phương

Mã sinh viên: B21DCAT151

Giảng viên hướng dẫn: TS. Phạm Hoàng Duy

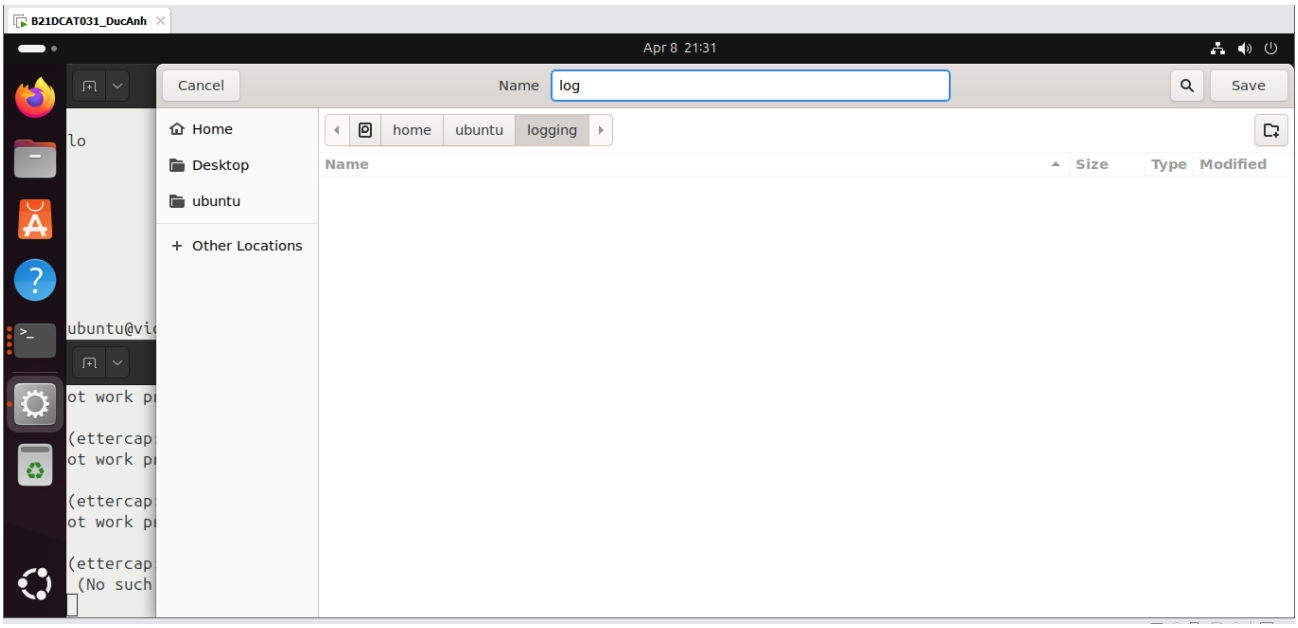
HỌC KỲ 2 NĂM HỌC 2024-2025

1. Tiến hành bật Ettercap máy attacker

- Bật ettercap với quyền root

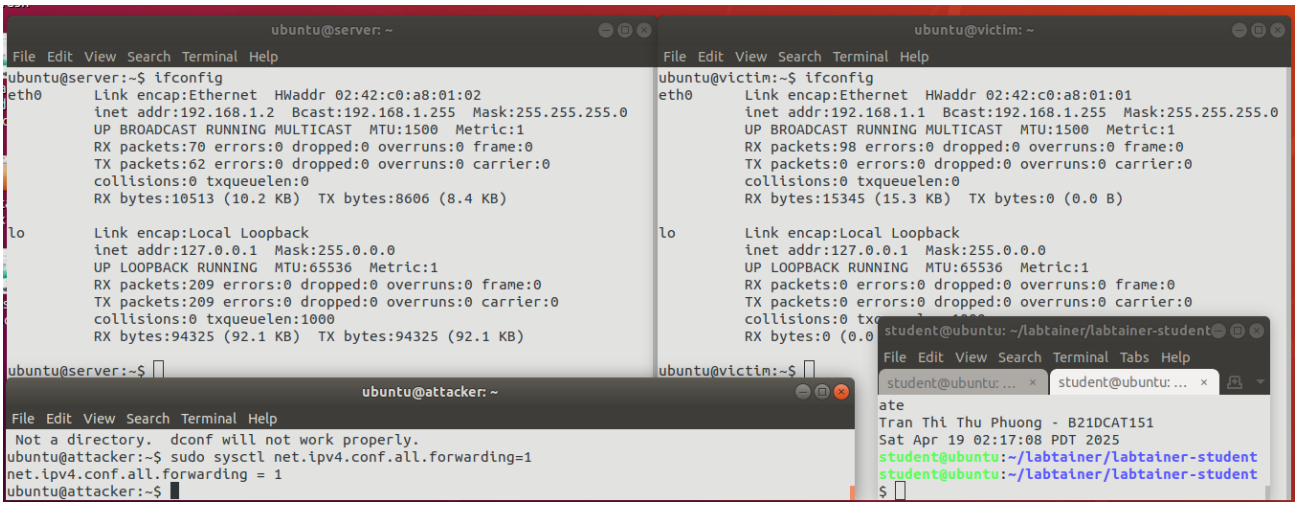
Vào phần menu, chọn Logging => Log user messages

Lưu tại thư mục /home/ubuntu/logging với tên là log.



Trên máy Attacker Enable IP Forward bằng lệnh:

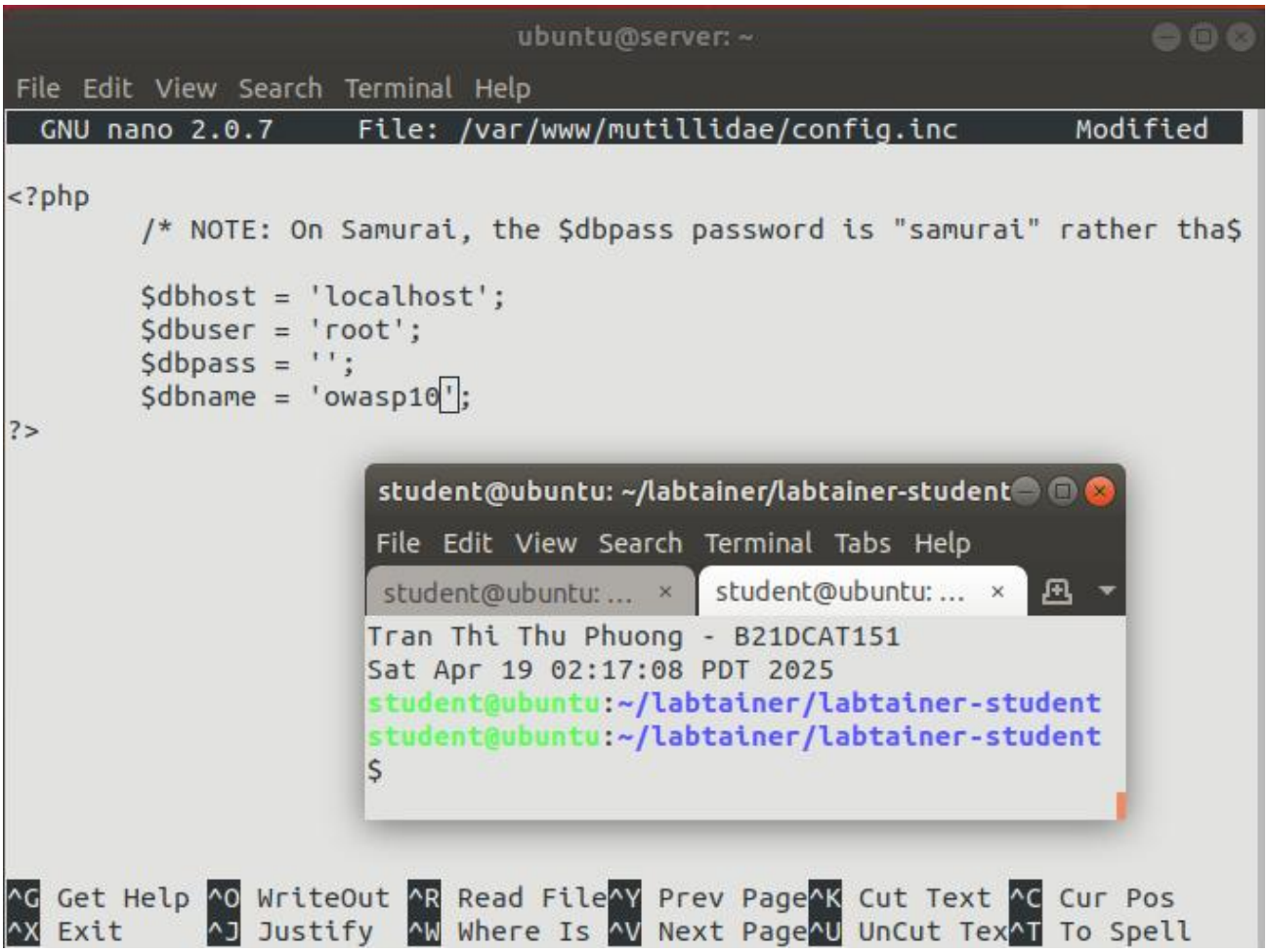
sudo sysctl net.ipv4.conf.all.forwarding=1



2. Scan host

Scan for hosts

Trên máy server Config server database tại đường dẫn /var/www/mutillidae/config.inc sửa mục dbname



Khởi động lại webserver

sudo /etc/init.d/apache2 reload

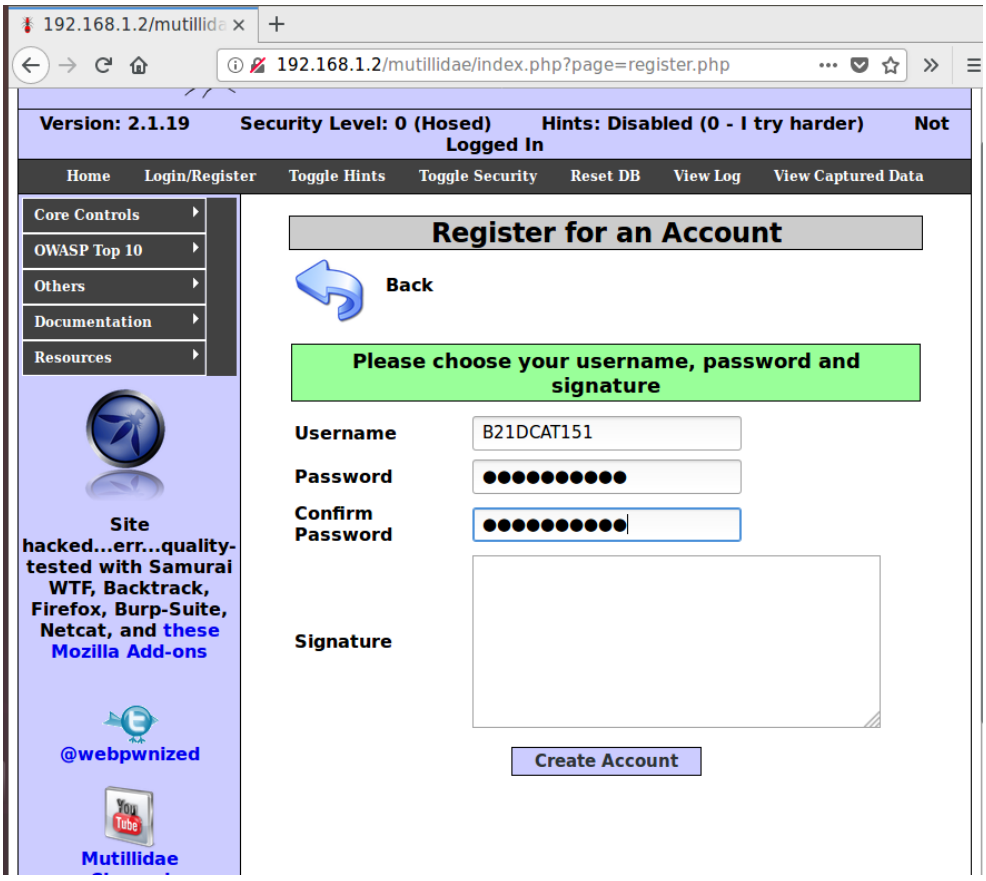
```
ubuntu@server:~$ sudo /etc/init.d/apache2 reload
 * Reloading web server config apache2
apache2: Could not reliably determine the server's fully qualified domain
name, using 192.168.1.2 for ServerName
                                                                    [ OK ]
ubuntu@server:~$
```

3. Lấy thông tin username và password

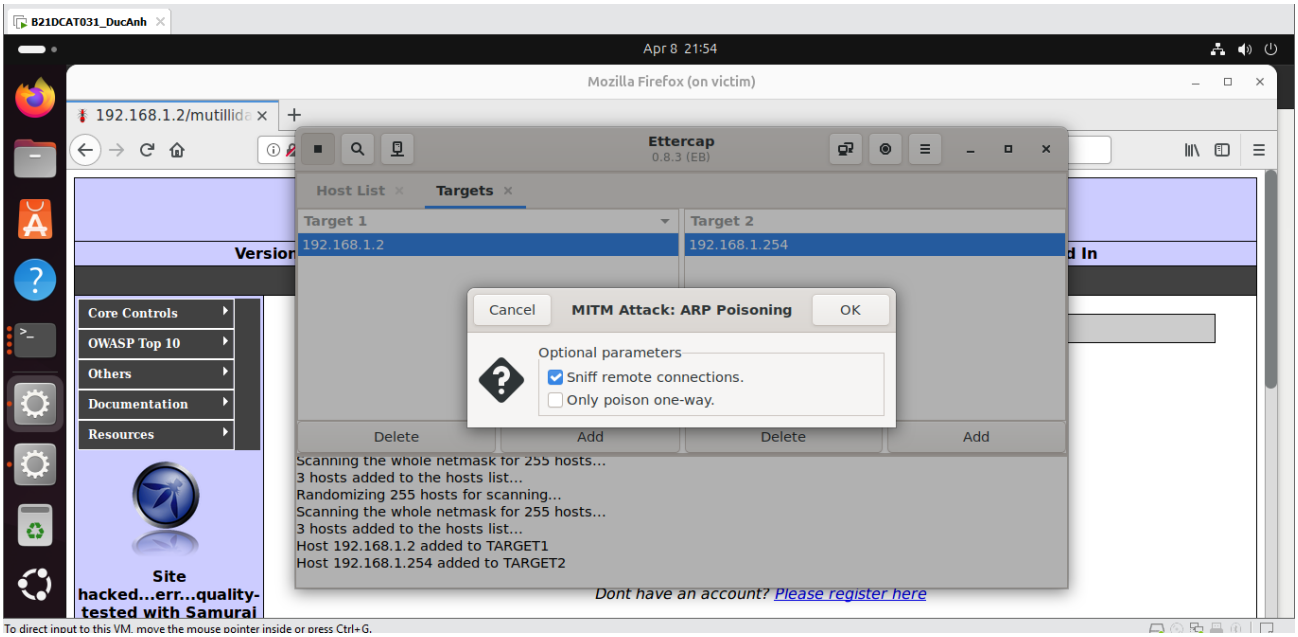
Trên máy victim mở trình duyệt firefox truy cập web server:

http://192.168.1.2/mutillidae/index.php?page=login.php

Đăng kí tài khoản



Chọn ARP poisoning, sau đó chọn Start sniffing.



Sau khi đăng nhập vào web, ettercap đã bắt được thông tin username và password.

```
index.php?page=login.php
CONTENT: username=B21DCAT151&password=B21DCAT151&login-php-submit-button=Login

HTTP : 192.168.1.2:80 -> USER: B21DCAT151  PASS: B21DCAT151  INFO: http://192.168.1.2/mutillidae/-
index.php?page=login.php
CONTENT: username=B21DCAT151&password=B21DCAT151&login-php-submit-button=Login
```

4. Kiểm tra checkwork

```
Results stored in directory: /home/student/labtainer_xfer/ptit-ettercap
Labname ptit-ettercap

Student              |        get_info | enable_ip_forwa |   scan_for_host |
==================== | =============== | =============== | =============== |
B21DCAT151           |                 |               Y |               Y |
What is automatically assessed for this lab:


student@ubuntu:~/labtainer/labtainer-student$ echo "Tran Thi Thu Phuong - B21DCAT151"; date
Tran Thi Thu Phuong - B21DCAT151
Sat Apr 19 03:27:27 PDT 2025
student@ubuntu:~/labtainer/labtainer-student$
```