

**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

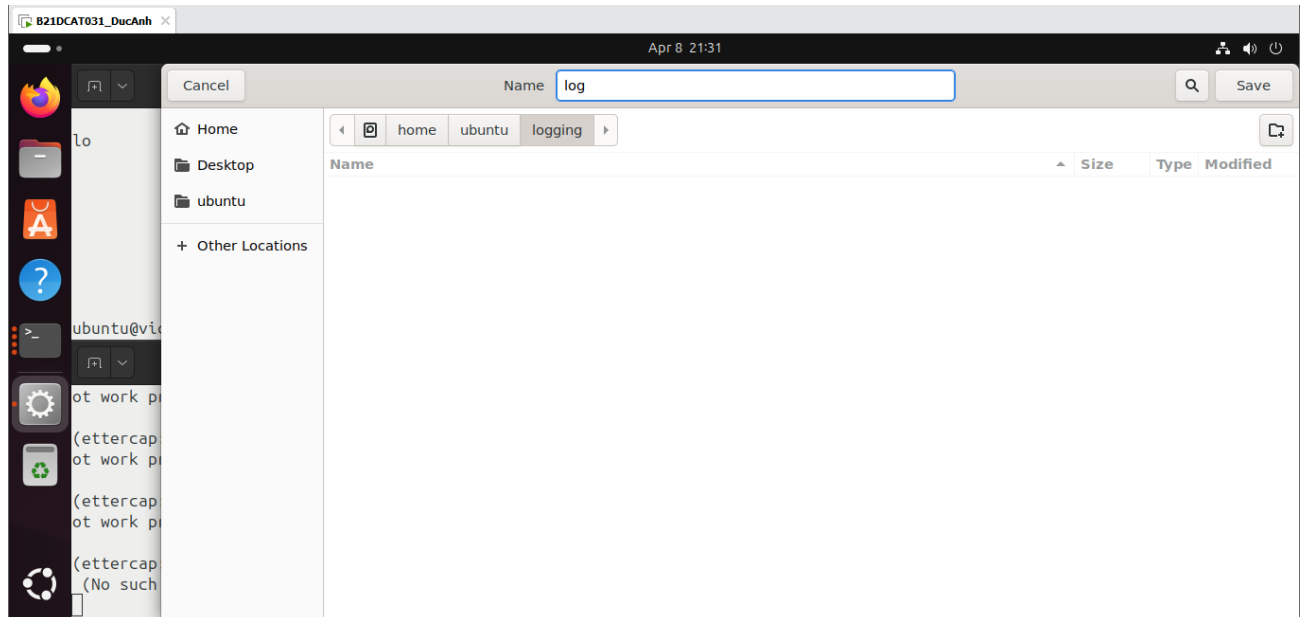
HỌC KỲ 2 NĂM HỌC 2024-2025

1. Tiến hành bật Ettercap máy attacker

- Bật ettercap với quyền root

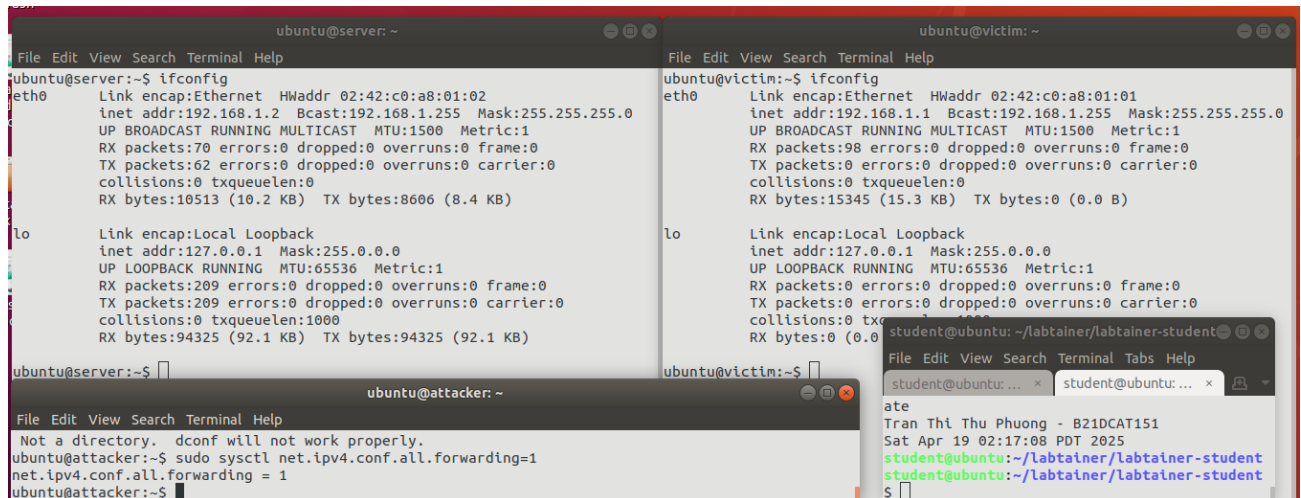
Vào phần menu, chọn Logging => Log user messages

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



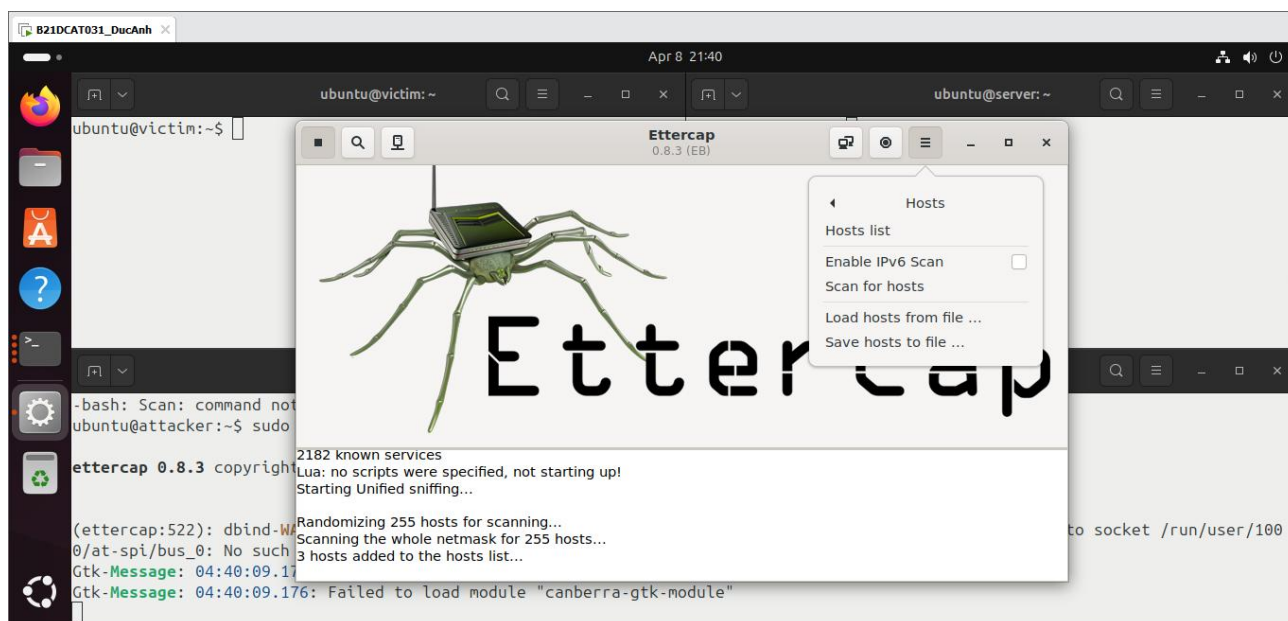
Trên máy Attacker Enable IP Forward bằng lệnh:

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

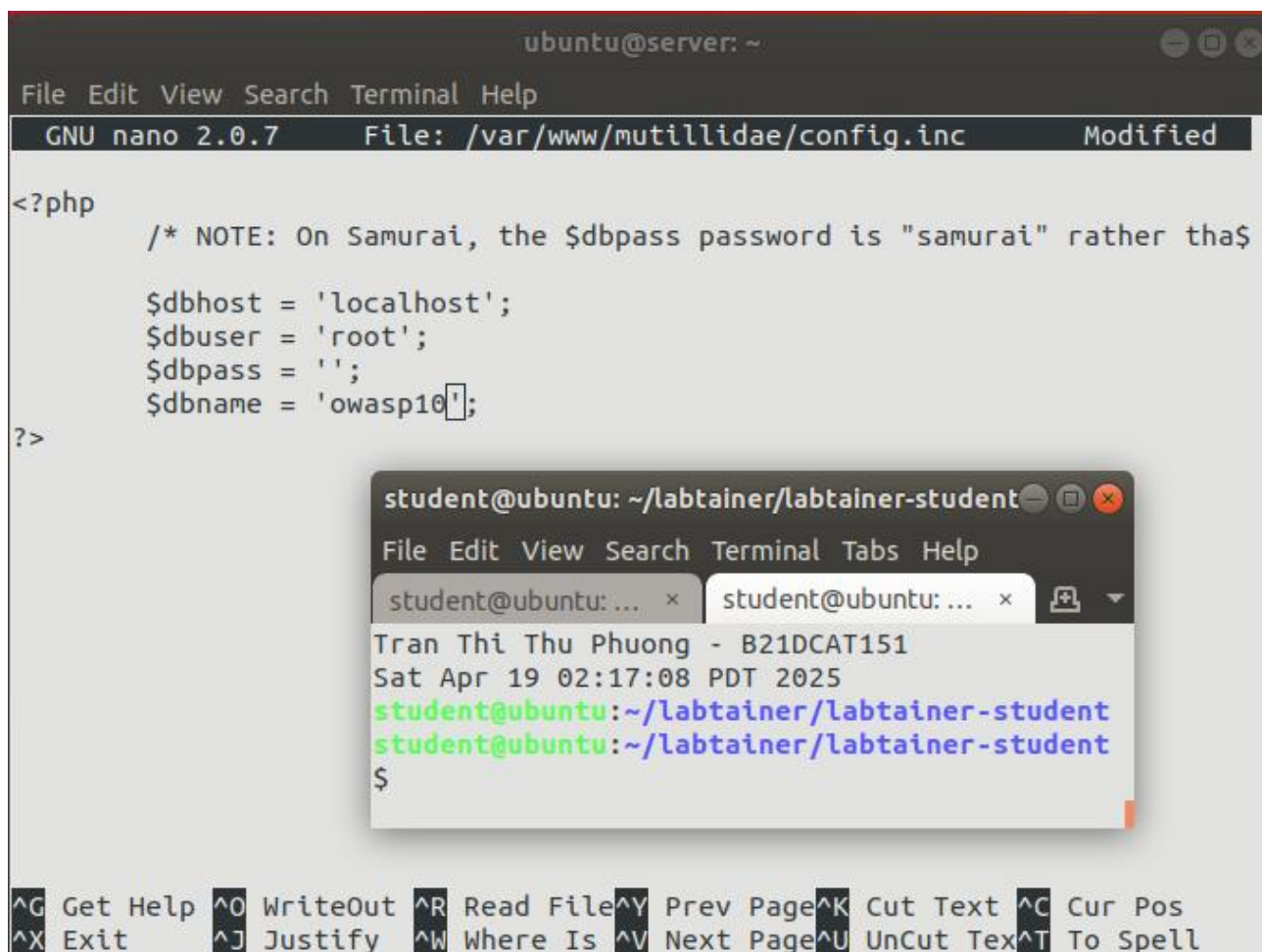


2. Scan host

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 nano /var/www/mutillidae/config.txt
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

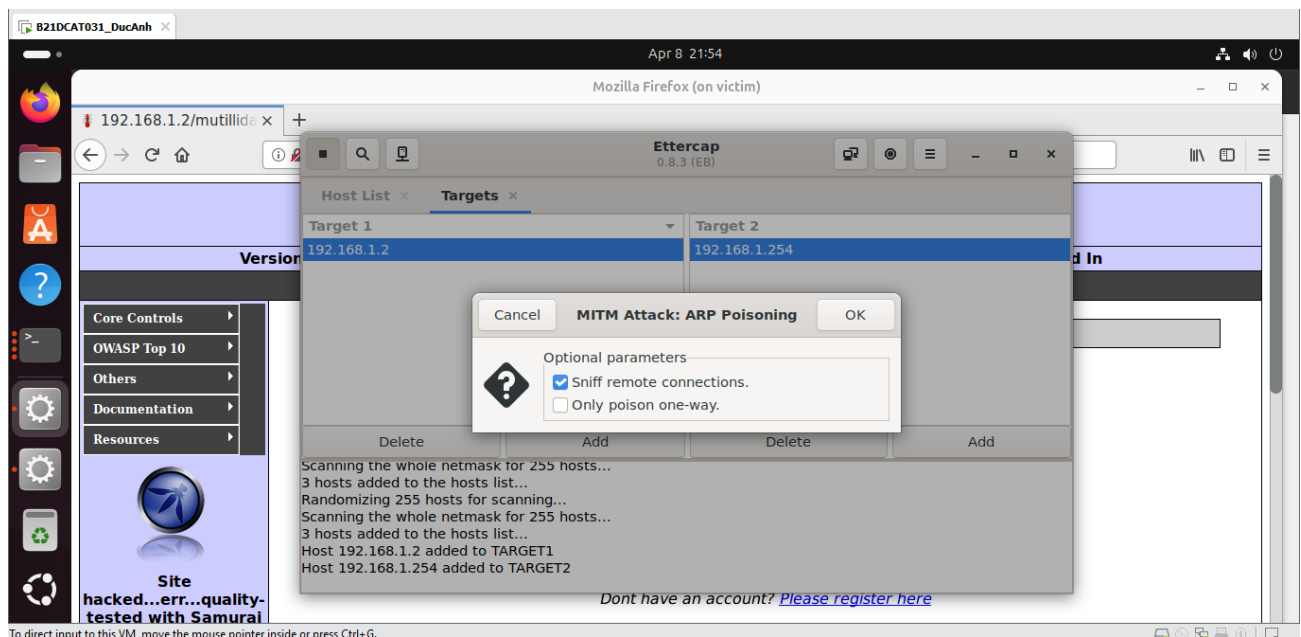
Trên máy victim mở trình duyệt firefox truy cập web server:

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

Đăng kí tài khoản

The screenshot shows a web browser window with the address bar displaying `192.168.1.2/mutillidae/index.php?page=register.php`. The page has a purple header with the following information: **Version: 2.1.19**, **Security Level: 0 (Hosed)**, **Hints: Disabled (0 - I try harder)**, and **Not Logged In**. Below the header is a navigation bar with links: Home, Login/Register, Toggle Hints, Toggle Security, Reset DB, View Log, and View Captured Data. On the left side, there is a sidebar menu with links: Core Controls, OWASP Top 10, Others, Documentation, and Resources. Below the menu is a logo and a message: "Site hacked...err...quality-tested with Samurai WTF, Backtrack, Firefox, Burp-Suite, Netcat, and these Mozilla Add-ons". At the bottom of the sidebar, there is a Twitter handle "@webpwnized" and a YouTube logo with the text "Mutillidae". The main content area is titled "Register for an Account" and contains a "Back" button with a blue arrow. Below this is a green box with the text "Please choose your username, password and signature". There are three input fields: "Username" with the value "B21DCAT151", "Password" with masked characters, and "Confirm Password" with masked characters. Below these is a "Signature" field with a large empty box. At the bottom right of the form is a "Create Account" button.

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$
```