Báo cáo tuần 8

Họ và tên: Phạm Đặng Tấn Dũng

MSSV: 20225569

**Giảng viên hướng dẫn: Nguyễn Đức Toàn**

Chủ đề: Rust và Evil Twin Attack

* Khó khăn đầu tiên là soft ap không cung cấp các công cụ có khả năng của iptables hay dnsmaq như linux.
* Thứ 2 là driver usb wifi trên laptop không hỗ trợ monitor mode và packet injection.
* Vì vậy nếu làm thì cần cấu hình dns và địa chỉ ip tĩnh trên máy nạn nhân

dnsmasq: Công cụ nhỏ gọn cung cấp DHCP (cấp IP) và DNS (phân giải tên miền). Trong Evil Twin, nó dùng để cấp IP cho nạn nhân và "đánh lừa" DNS để mọi yêu cầu tên miền đều trỏ về IP của kẻ tấn công (máy ảo ubuntu trên virtual box).

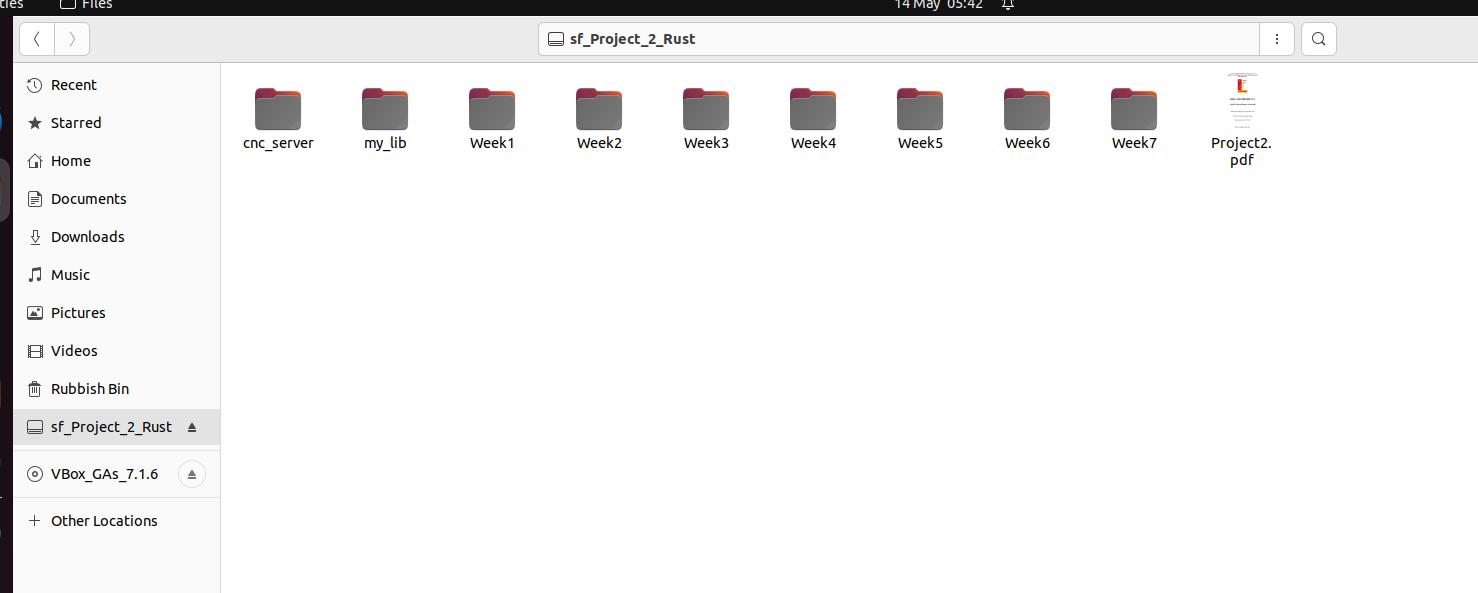
iptables: Công cụ tường lửa mạnh mẽ của Linux. Được dùng để chuyển hướng (redirect) lưu lượng mạng. Trong Evil Twin, nó dùng để chuyển hướng mọi traffic HTTP (port 80) và có thể cả HTTPS (port 443) từ nạn nhân đến port 3000 là port captive portal đang chạy.

**Do đó trong tuần này em đã:**

1. Chuyển code sang chạy trên máy ảo.
2. Cài đặt database, libraries và dependencies cần thiết.
3. Cho phép máy host truy cập vào captive portal được chạy trên máy ảo sử dụng cổng 3000 thông qua bridged network.
4. Lưu thông tin đăng nhập vào postgresql trên máy ảo.

**Cụ thể:**

* Tạo máy ảo Ubuntu 64-bit với 2 interface 1 là NAT(để kết nối với Internet), 2 là Bridged Network(để máy host và máy nạn nhân có thể truy cập vào captive portal).
* Cài Rust trong máy ảo.
* Sử dụng shared folders để lấy code từ windows.



* Copy thư mục code ra ngoài(tránh các lỗi liên quan đến trình biên dịch Rust khi đọc ghi các file).

*cp -r ../../.. ~/*

* Cài đặt các libraries và các gói dependencies cần thiết(net-tools, sqlx).
* Cài dnsmasq:

Dừng và vô hiệu hóa system-resolved để giải phóng cổng 53 cho dnsmasq.

*sudo systemctl stop systemd-resolved*

*sudo systemctl disable systemd-resolved*

Điều chỉnh file */etc/resolv.conf: nameserver 8.8.8.8* để máy ảo vẫn phân giải tên miền bình thường.

* Cài database postgresql:

Tạo database credentials: *sudo -i -u postgres*

*psql*

*CREATE DATABASE credentials;*

*CREATE USER postgres WITH PASSWORD ‘123456';*

*GRANT ALL PRIVILEGES ON DATABASE credentials TO postgres;*

*\q*

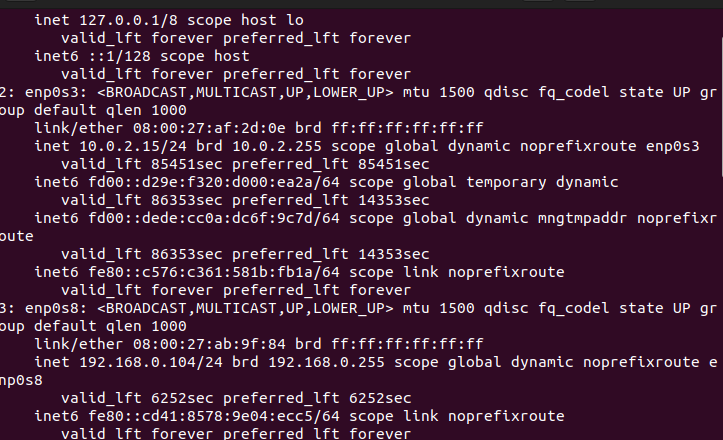
*exit*

Khởi động lại postgresql: *sudo systemctl restart postgresql*

* Tạo table credentials:

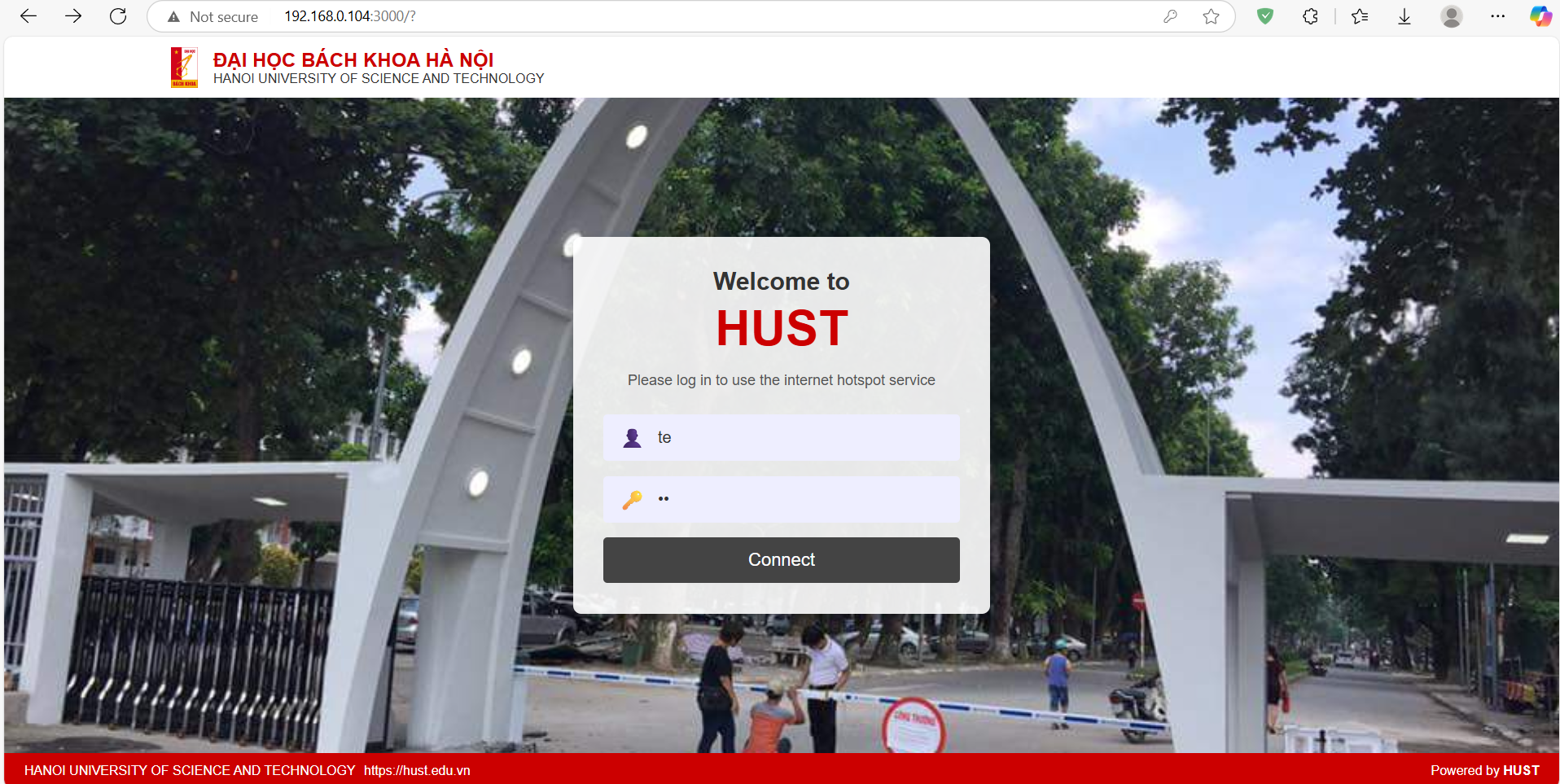
*sqlx database create(nếu chưa có)*

*sqlx migrate run*

* Đổi từ địa chỉ loopback(127.0.0.1) thành địa chỉ của máy ảo(192.169.0.104) là địa chỉ của interface enp0s8(bridged network). 
* Trong file main.rs: Đổi 127.0.0.1 thành 0.0.0.0, có nghĩa là chương trình Rust này sẽ lắng nghe trên tất cả interface có sẵn trên máy ảo.



* Ảnh của captive portal:



**Tuần sau, khi có usb wifi, em sẽ:**

Cấu hình dnsmaq và iptables.

Thực hiện mô phỏng tấn công deauthentication attack.

Xây dựng wifi giả mạo.