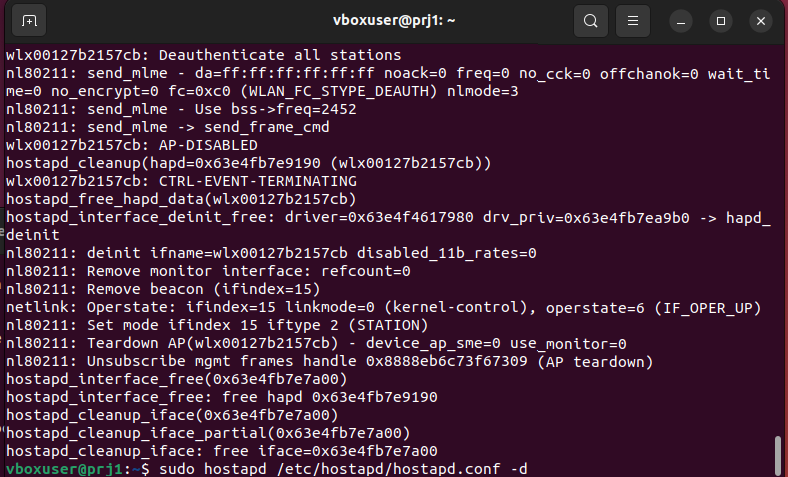


sudo killall hostapd

WEEK 10:

*sudo hostapd /etc/hostapd/hostapd.conf -d*



Thiết lập network service(dns và dhcp):

*interface=<wireless\_interface>*

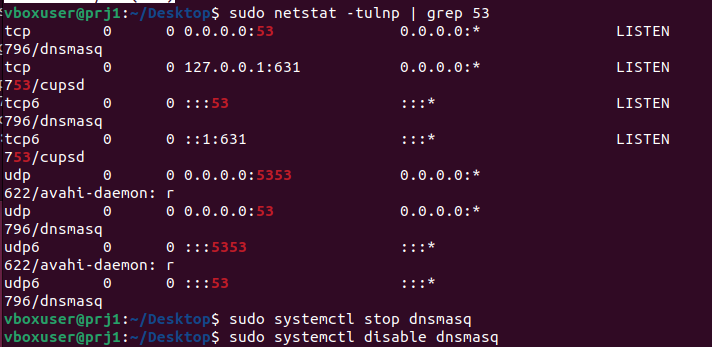
*dhcp-range=10.0.0.100,10.0.0.200,255.255.255.0,12h # Dải IP cấp phát*

*dhcp-option=3,10.0.0.1 # Gateway (IP của máy Kali)*

*dhcp-option=6,10.0.0.1 # DNS Server (Trỏ về máy Kali)*

*log-queries*

Disable dnsmasq để khởi động thủ công bằng dnsmasq.conf



Chạy lệnh: *sudo dnsmasq -C /etc/hostapd/dnsmasq.conf -d*

**

Bật IP forwarding: *echo 1 | sudo tee /proc/sys/net/ipv4/ip\_forward*

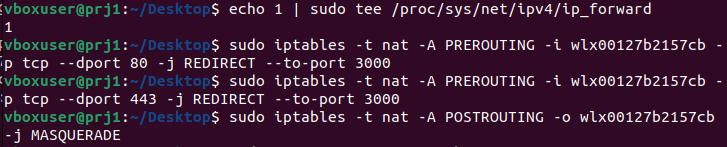
Thiết lập rule chuyển hướng:

*sudo iptables -t nat -A PREROUTING -i <wireless\_interface> -p tcp --dport 80 -j REDIRECT --to-port <port >*

*sudo iptables -t nat -A PREROUTING -i <wireless\_interface> -p tcp --dport 443 -j REDIRECT --to-port <port >*

Thiết lập NAT để nạn nhân vẫn có mạng khi qua portal:

*sudo iptables -t nat -A POSTROUTING -o <internet\_facing\_interface> -j MASQUERADE*

**

Lưu iptables:

*sudo apt-get install iptables-persistent*

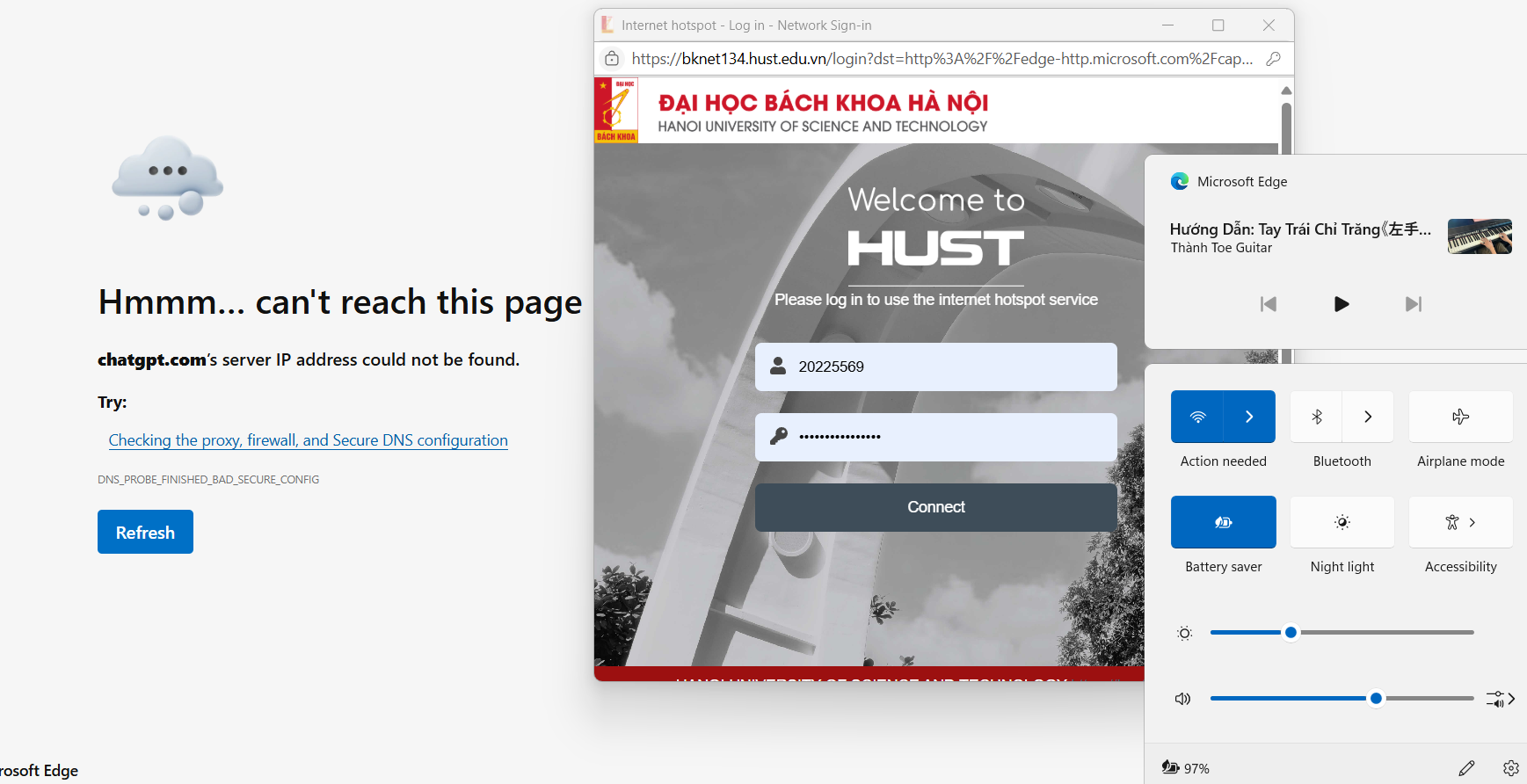
*sudo netfilter-persistent save*

**

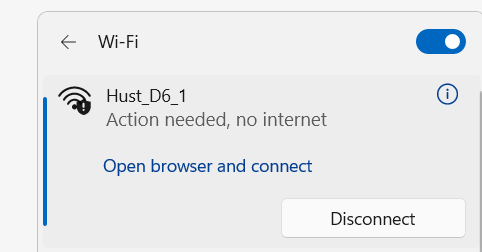
Continue:

Khi có captive portal, browser báo không tìm được địa chỉ ip của tên miền(thay vì forward mọi gói tin sang 10.0.0.1:3000, từ đó gây lỗi chứng chỉ ssl cho các request https), trang đăng nhập pop-up ở cửa sổ mới, mục wifi trong máy tính hiện action needed.

Giải thích: Cơ chế phát hiện captive portal của Windows, các gói tin bị không được forward mà bị chặn lại.



Mục open browser and connect:



Windows sử dụng giao thức HTTP GET kiểm tra xem có nhận được dữ liệu về file connecttest.txt(hoặc dùng http://www.msftncsi.com/ncsi.txt) không từ [www.msftconnecttest.com](http://www.msftconnecttest.com), nếu kết quả nhận được là HTTP/1.1 200 OK thì có kết nối bình thường(không cần captive portal).

