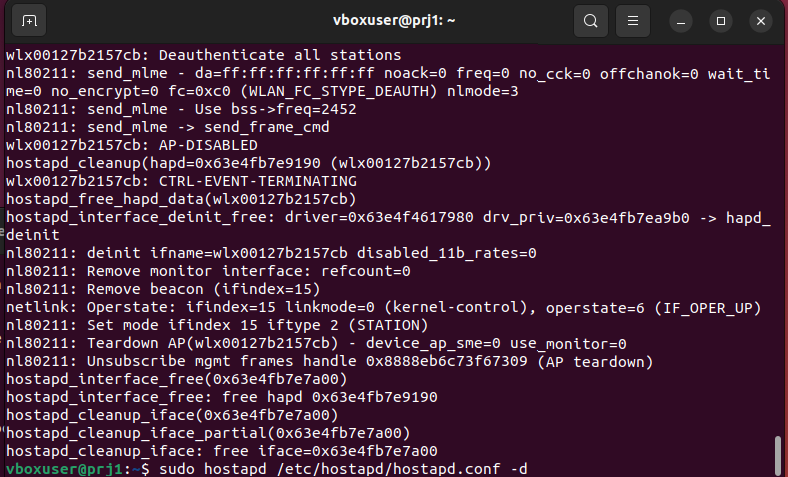


sudo killall hostapd

WEEK 10:

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



Thiết lập network service(dns và dhcp):

*interface=<wireless\_interface>*

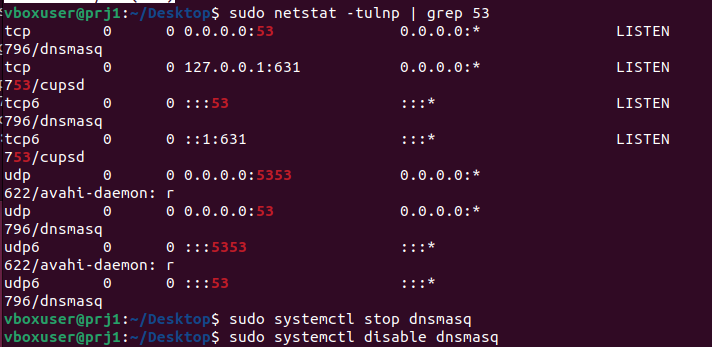
*dhcp-range=10.0.0.100,10.0.0.200,255.255.255.0,12h # Dải IP cấp phát*

*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*

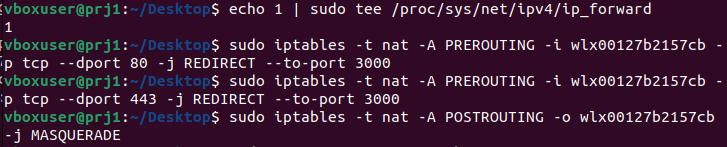
Thiết lập rule chuyển hướng:

*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*

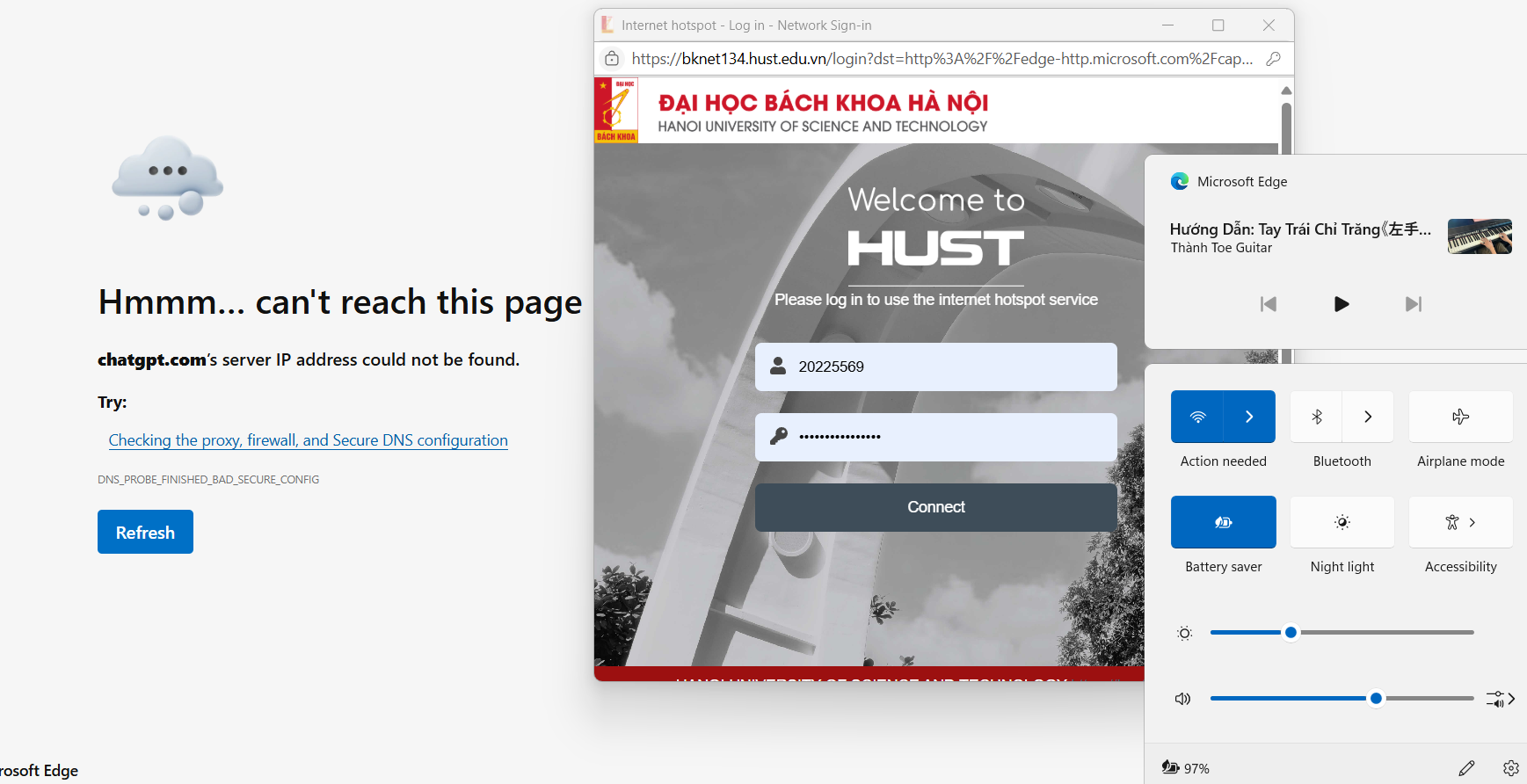
*sudo netfilter-persistent save*

**

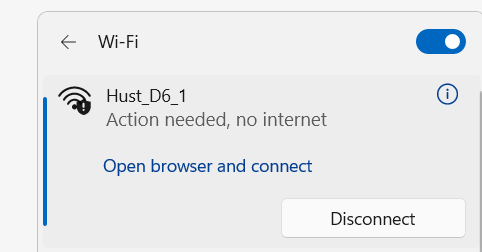
Continue:

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.

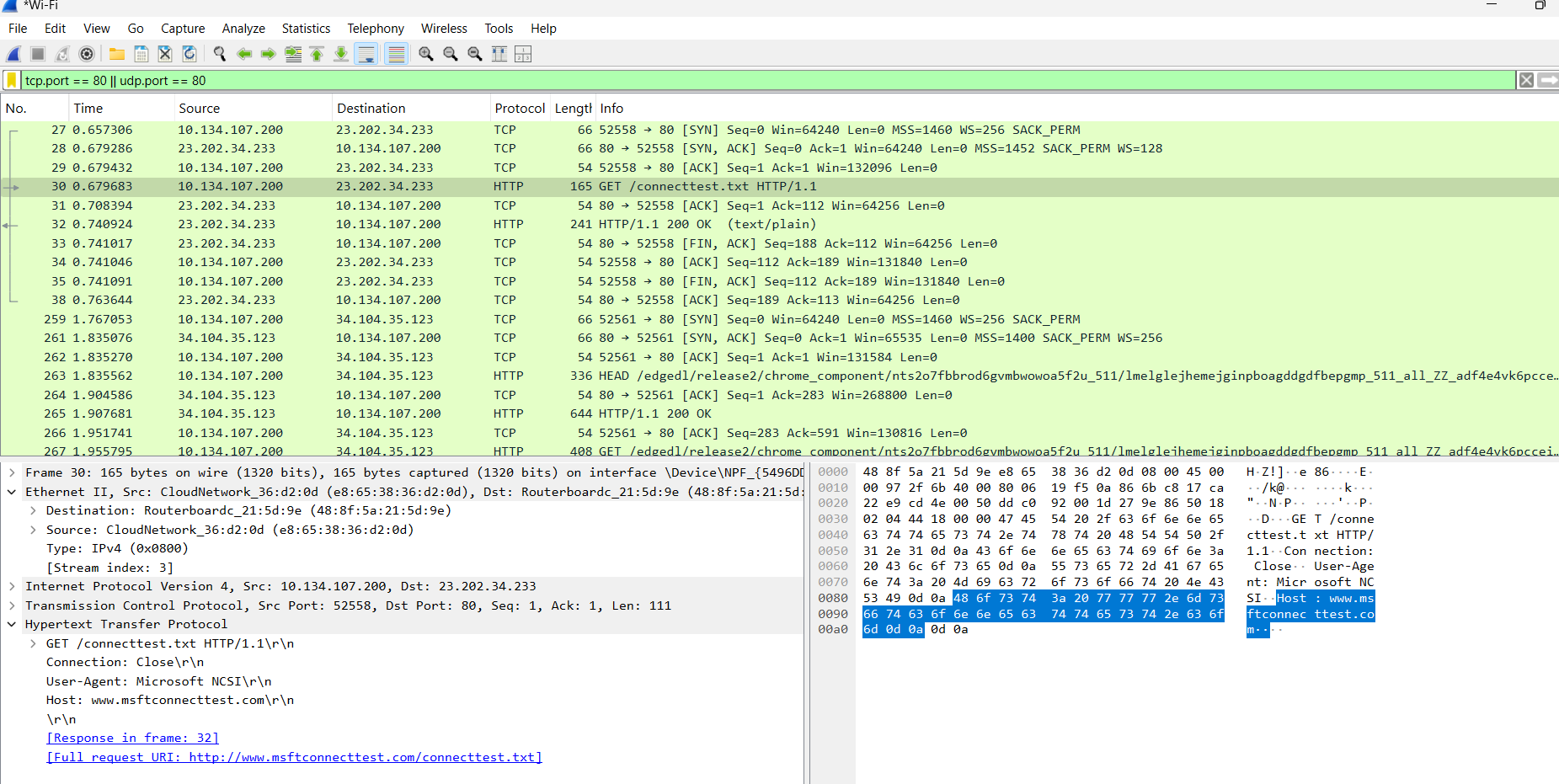


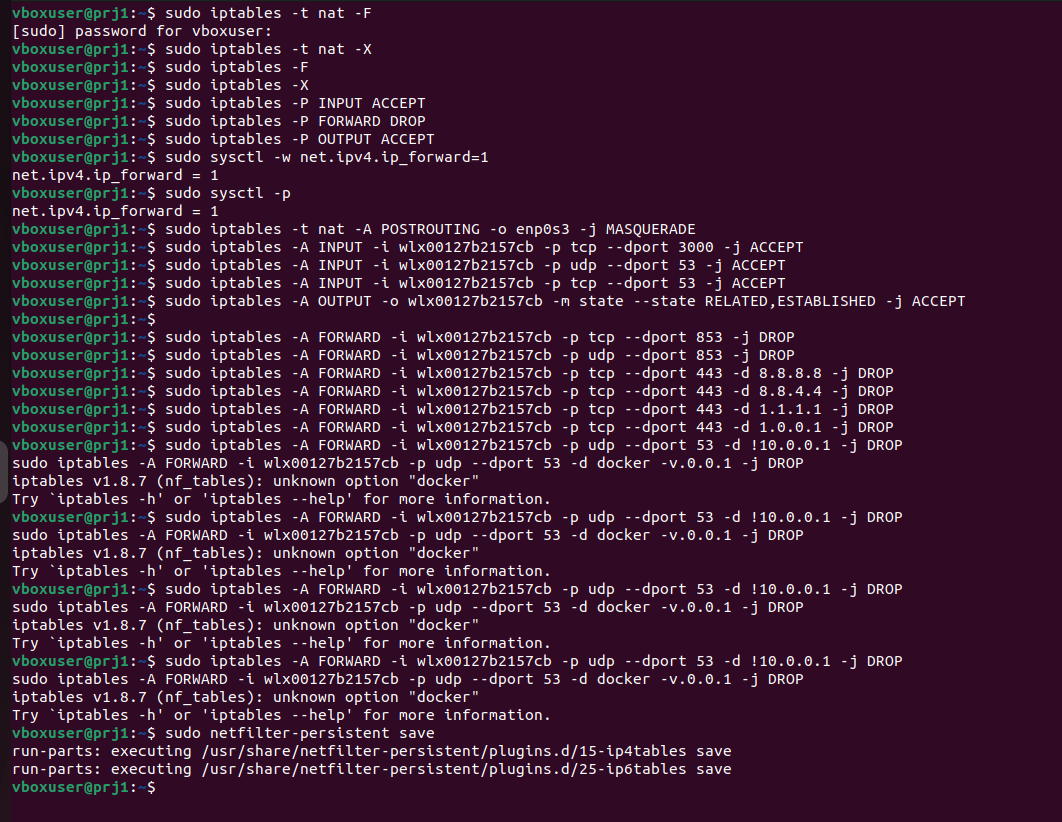
Mục open browser and connect:

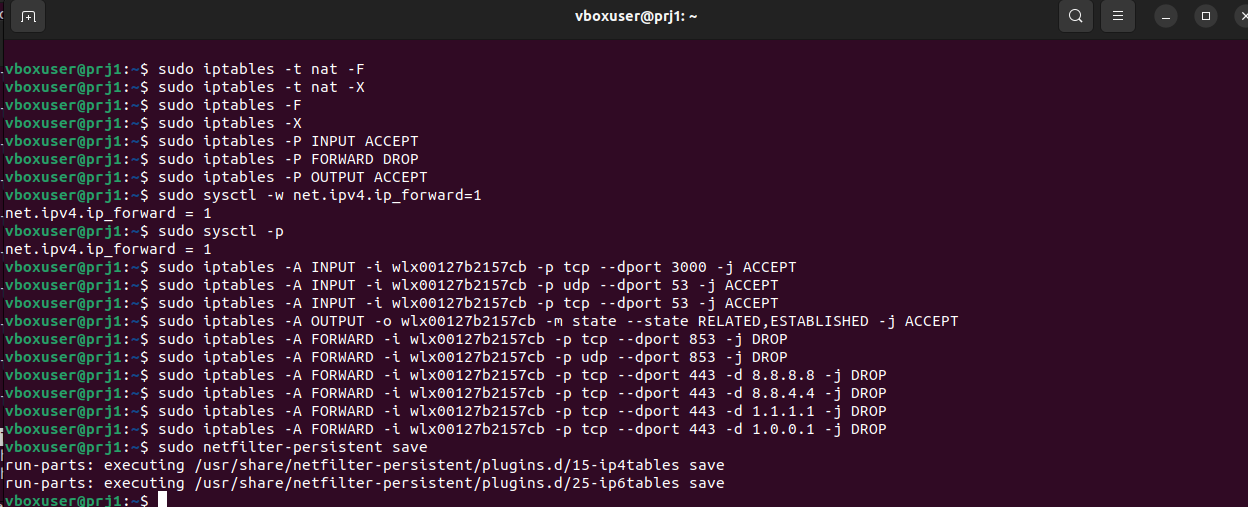


Windows sử dụng giao thức HTTP GET kiểm tra xem có nhận được dữ liệu về file connecttest.txt(hoặc dùng http://www.msftncsi.com/ncsi.txt) không từ [www.msftconnecttest.com](http://www.msftconnecttest.com), nếu kết quả nhận được là HTTP/1.1 200 OK thì có kết nối bình thường(không cần captive portal).

Hyperlink: [Android Enterprise Network Requirements - Android Enterprise Help](https://support.google.com/work/android/answer/10513641?hl=en#:~:text=Used%20by%20Android%20OS%20for%20connectivity%20check%20whenever,network%20to%20point%20to%20a%20reachable%20PAC%20file.)







# ĐẦU TIÊN VÀ TRÊN HẾT: FLUSH TẤT CẢ CÁC QUY TẮC HIỆN CÓ

sudo iptables -t nat -F

sudo iptables -t nat -X

sudo iptables -F

sudo iptables -X

# ĐẶT CHÍNH SÁCH MẶC ĐỊNH CHO TẤT CẢ CÁC CHAIN THÀNH ACCEPT

# Điều này đảm bảo không có quy tắc DROP ngầm nào gây nhiễu

sudo iptables -P INPUT ACCEPT

sudo iptables -P FORWARD DROP

sudo iptables -P OUTPUT ACCEPT

# Bật IP Forwarding (Đảm bảo đã chạy và duy trì sau khởi động lại)

sudo sysctl -w net.ipv4.ip\_forward=1

sudo sysctl -p # Áp dụng ngay lập tức từ /etc/sysctl.conf

# Cho phép client truy cập vào Axum server của bạn (10.0.0.1:3000)

# Đây là cách client có thể truy cập trang login và các URL kiểm tra kết nối

sudo iptables -A INPUT -i wlx00127b2157cb -p tcp --dport 3000 -j ACCEPT

# Cho phép client gửi DNS query đến dnsmasq (10.0.0.1:53)

sudo iptables -A INPUT -i wlx00127b2157cb -p udp --dport 53 -j ACCEPT

sudo iptables -A INPUT -i wlx00127b2157cb -p tcp --dport 53 -j ACCEPT

# \*\*\* QUY TẮC CHUYỂN HƯỚNG CHO CAPTIVE PORTAL (PREROUTING) \*\*\*

# Những quy tắc này sẽ chuyển hướng traffic HTTP/HTTPS đến Axum server của bạn (Port 3000)

# Đây là cách chính để Axum nhận được các yêu cầu trên port 80/443

sudo iptables -t nat -A PREROUTING -i wlx00127b2157cb -p tcp --dport 80 -j DNAT --to-destination 10.0.0.1:3000

sudo iptables -t nat -A PREROUTING -i wlx00127b2157cb -p tcp --dport 443 -j DNAT --to-destination 10.0.0.1:3000

# Cho phép Axum server gửi phản hồi về client cho các kết nối đã thiết lập (DHCP, DNS, HTTP/3000)

sudo iptables -A OUTPUT -o wlx00127b2157cb -m state --state RELATED,ESTABLISHED -j ACCEPT

# LƯU LẠI CÁC QUY TẮC IPTABLES để chúng không bị mất khi khởi động lại

sudo netfilter-persistent save