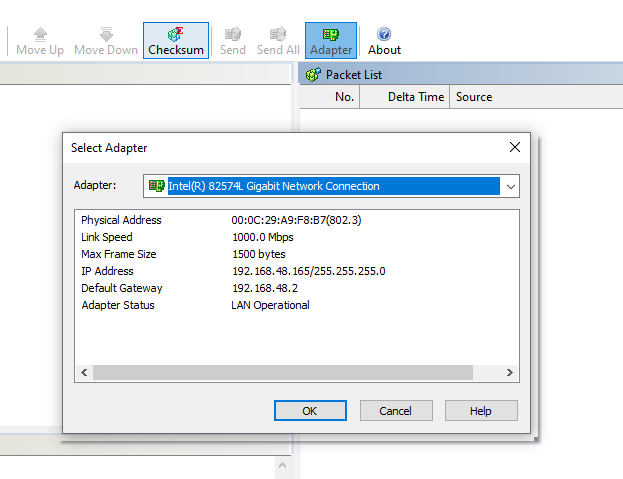
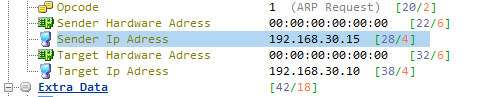
Module 3 Scanning Network

# Sử dụng Colasoft Packet Builder

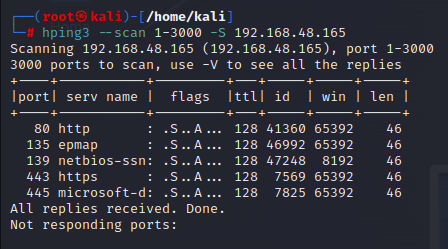




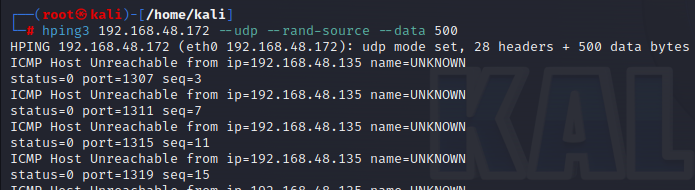


# Hping3

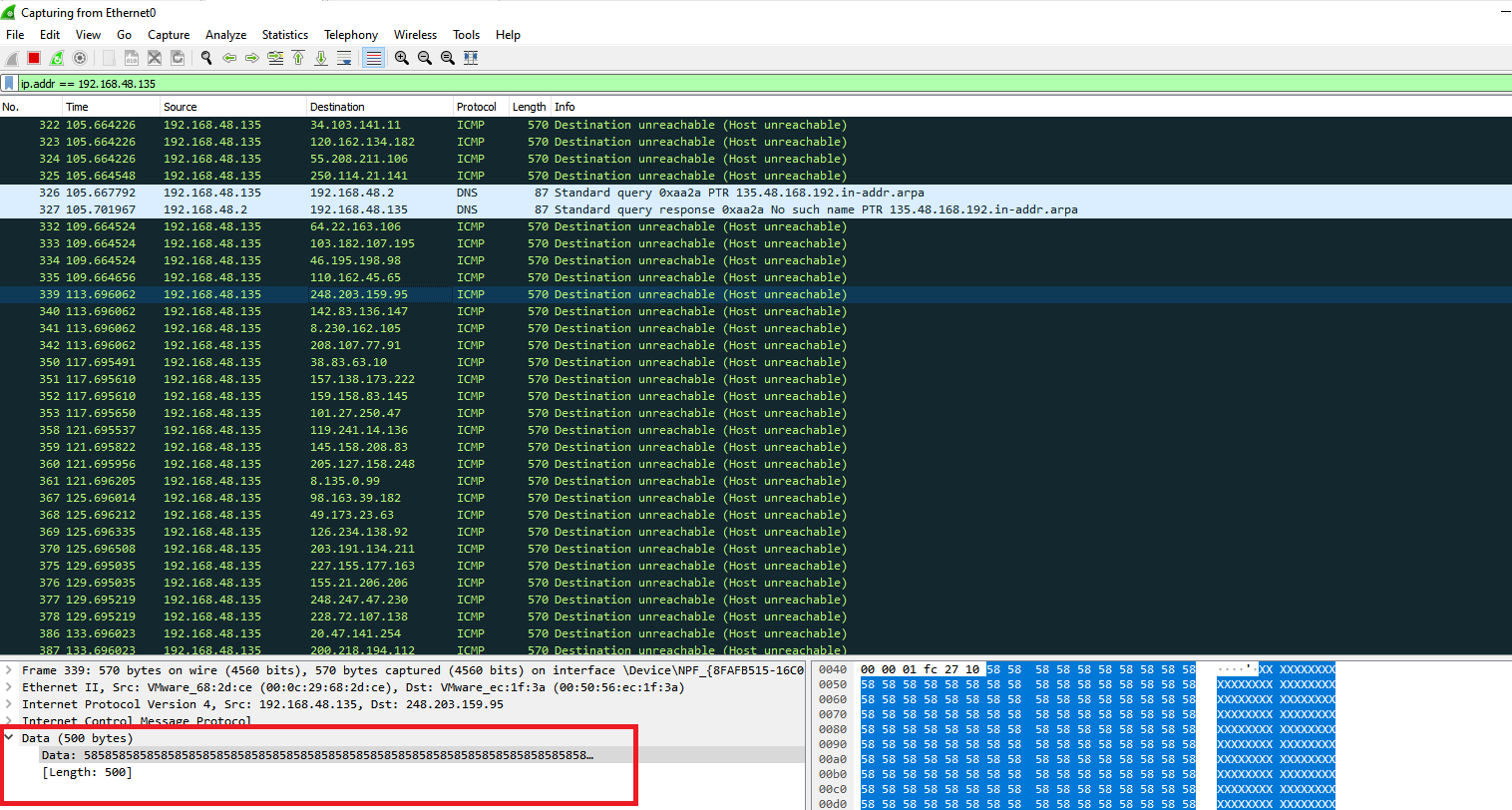
Quét cổng 1-300 với gói tin SYN (gói tin TCP)



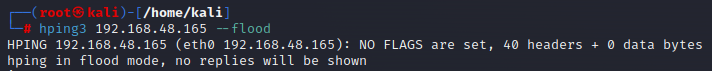
Gửi các gói tin với độ dài 500 và dùng giao thức udp tới các target random



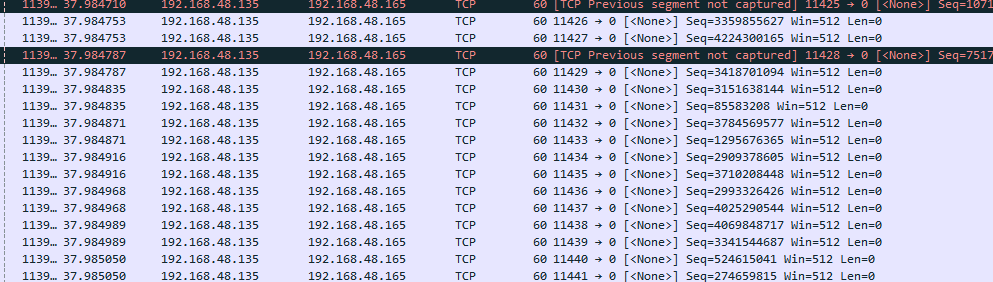
Kết quả được wireshark ghi lại



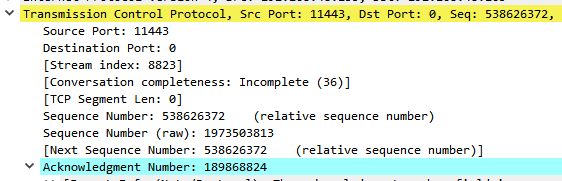
Tấn công flood (gửi hàng loạt gói tin tcp tới máy mục tiêu)



Số lượng lớn gói tin được chuyển đi

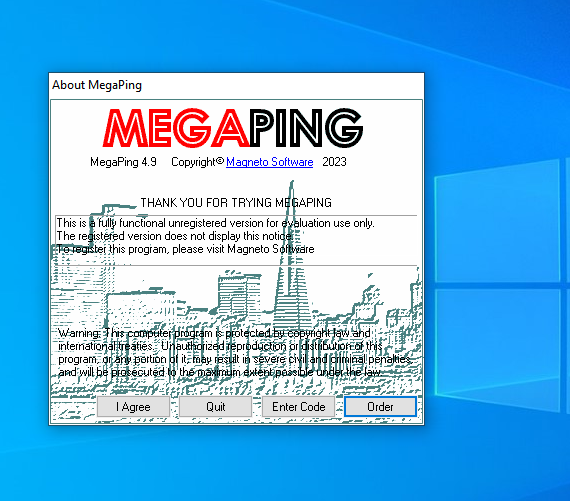


Thông tin số lượng các gói được gửi đi là không hề nhỏ

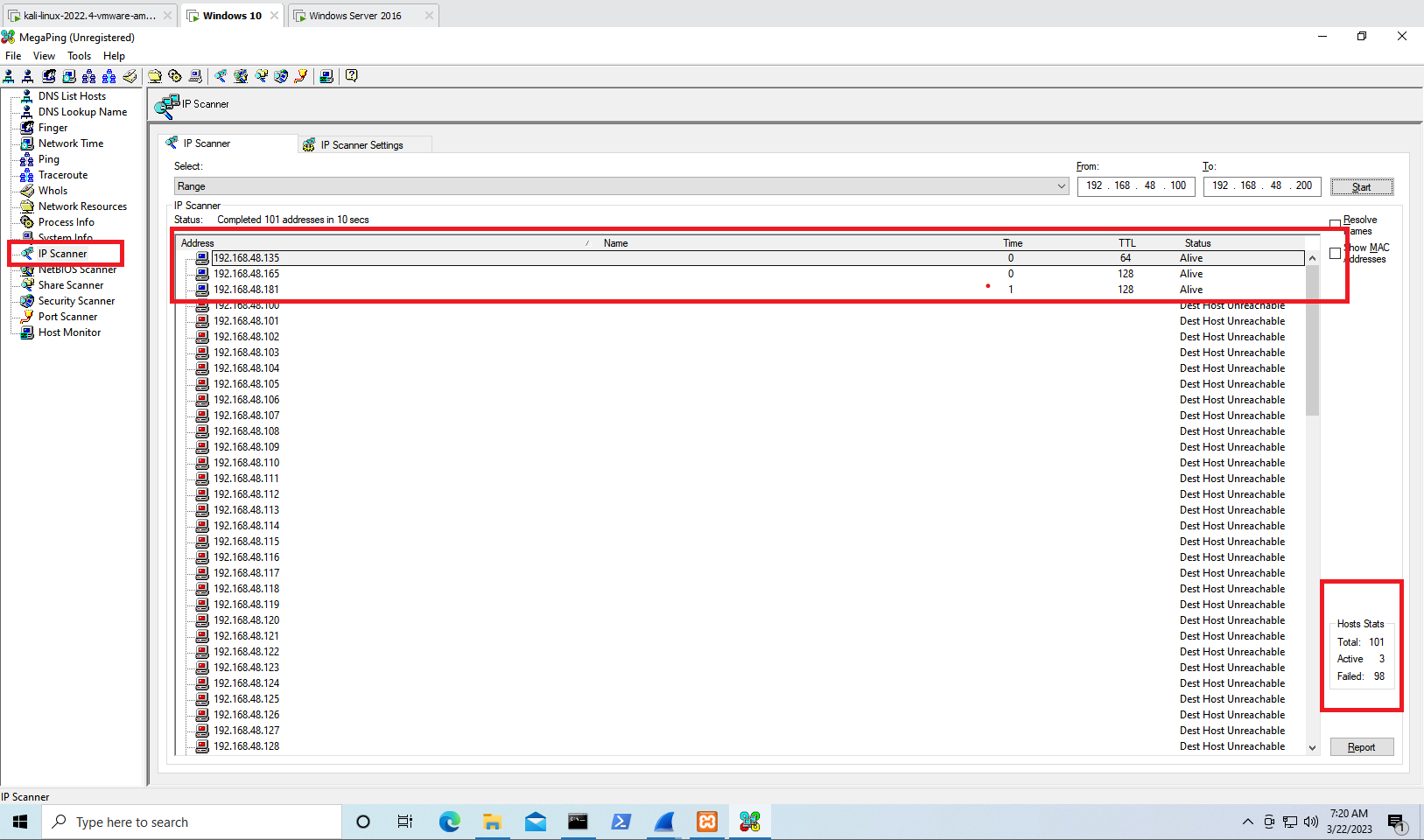


# Sử dụng MegaPing để scan network

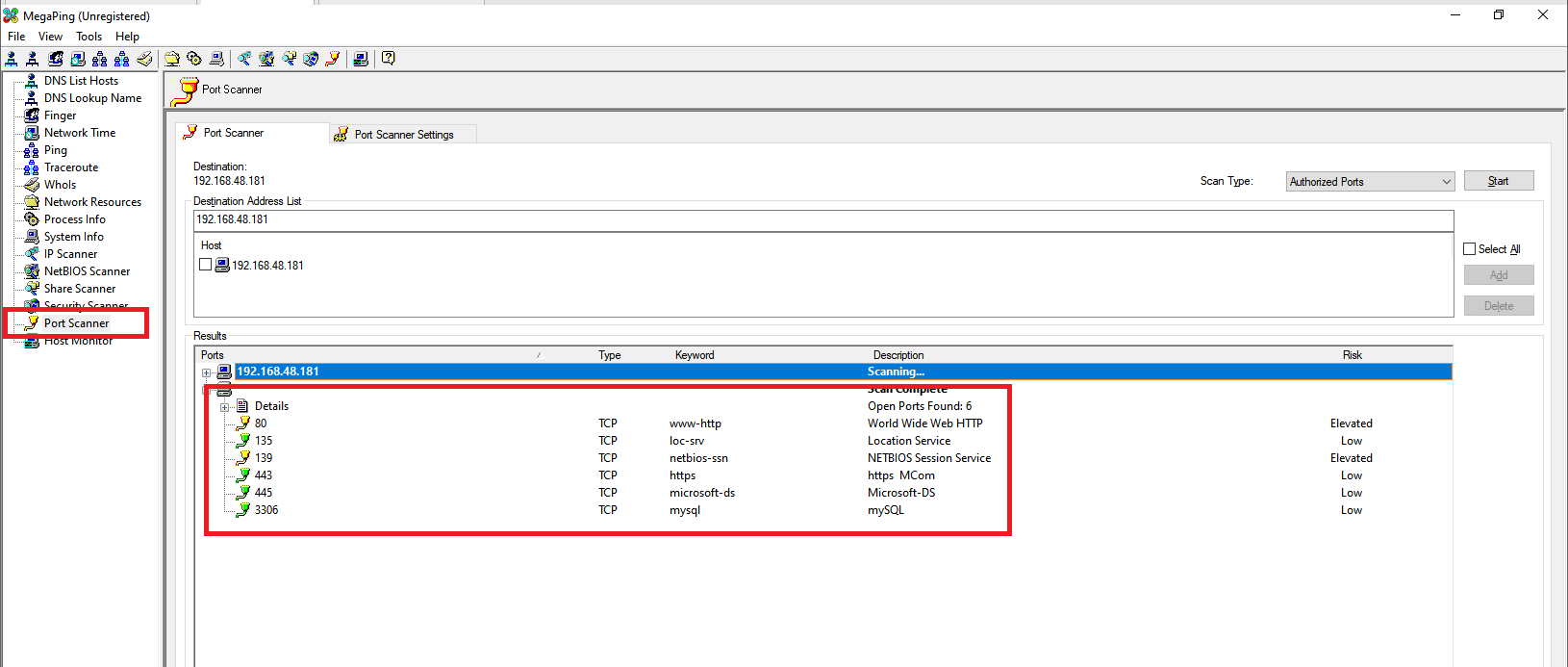
Giao diện khởi động



Quét dãy ip các máy đang hoạt động kết quả có 3 máy

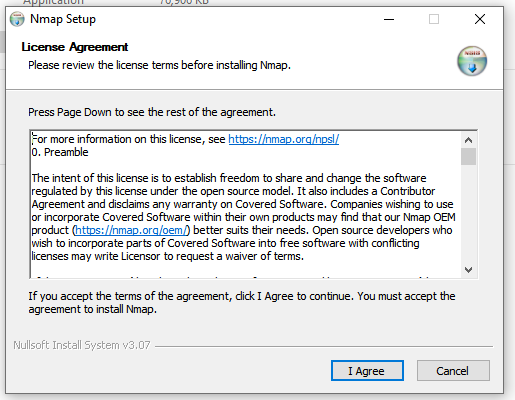


Quét các cổng đang của ip 192.168.48.181 và có các dịch vụ đang mở như http,mysql,...

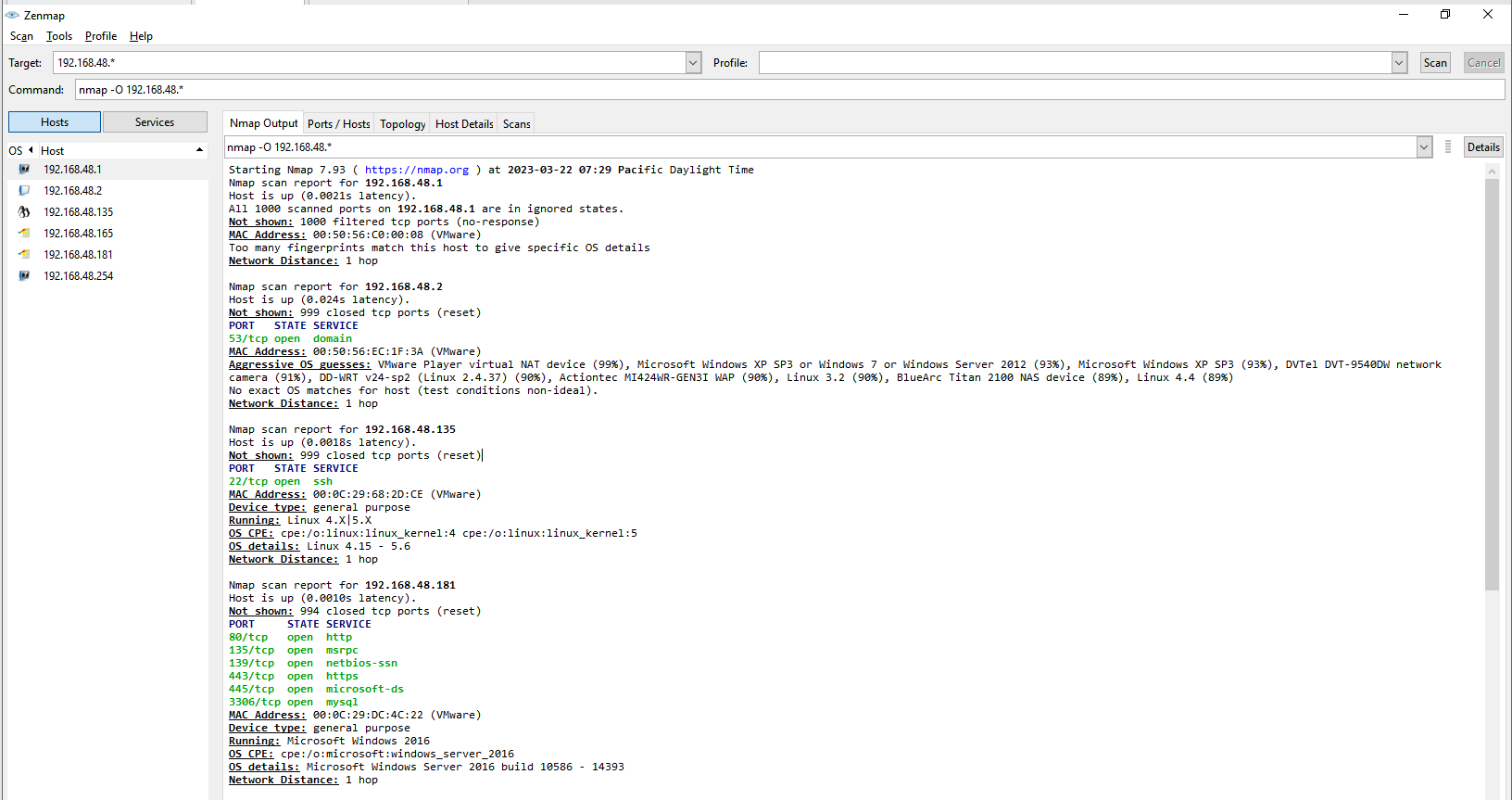


# Sử dụng zenmap

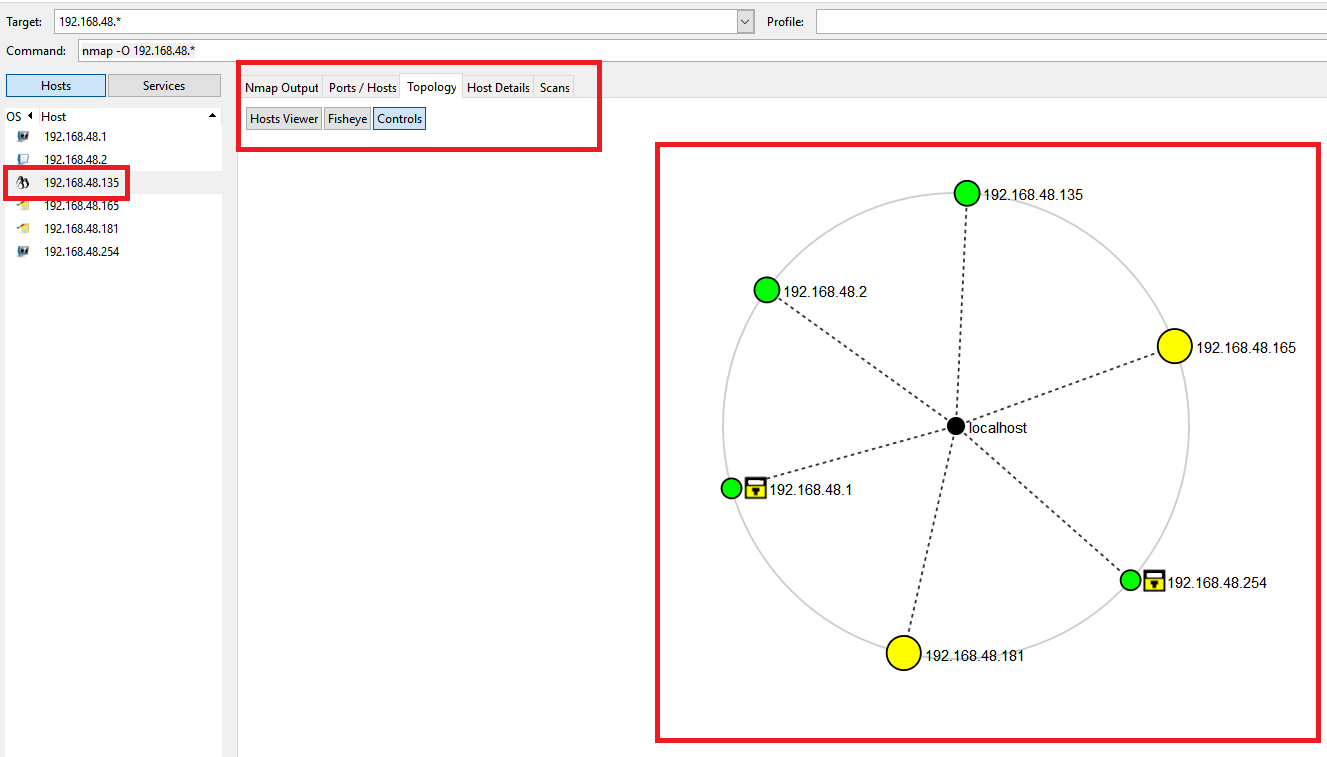
Cài đặt zenmap



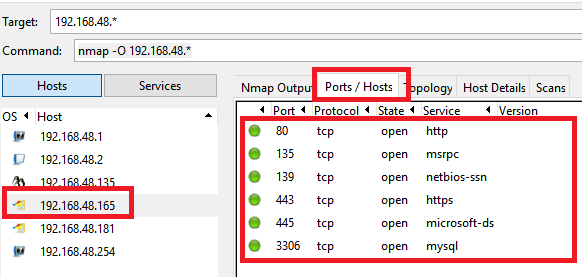
Sử dụng lệnh “nmap -O 192.168.48.\*” để quét hết tất cả các hệ điều hành trong dãy ip 192.168.48, kết quả quét ra được 3 máy ảo và router



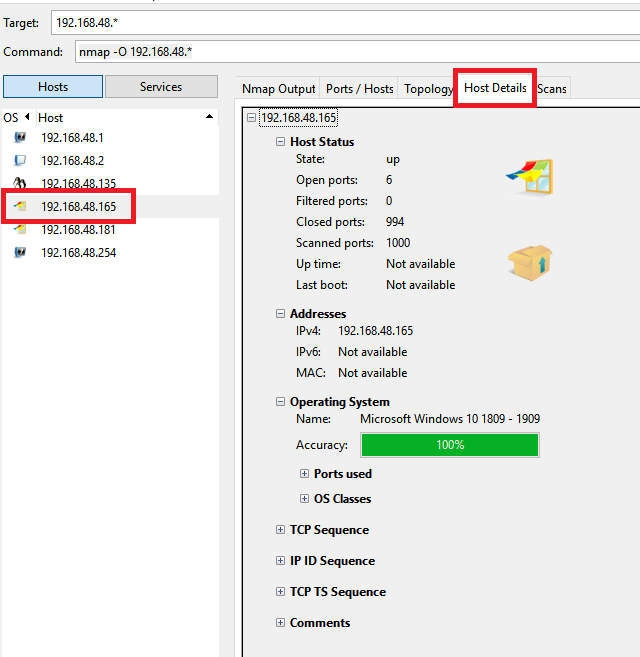
Zenmap còn có chức năng hiện thị sơ đồ mạng



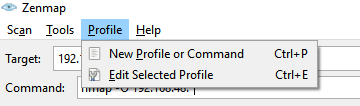
Tại tab ports/host hiện thị các dịch vụ đang mở tại host có ip “192.168.48.165”



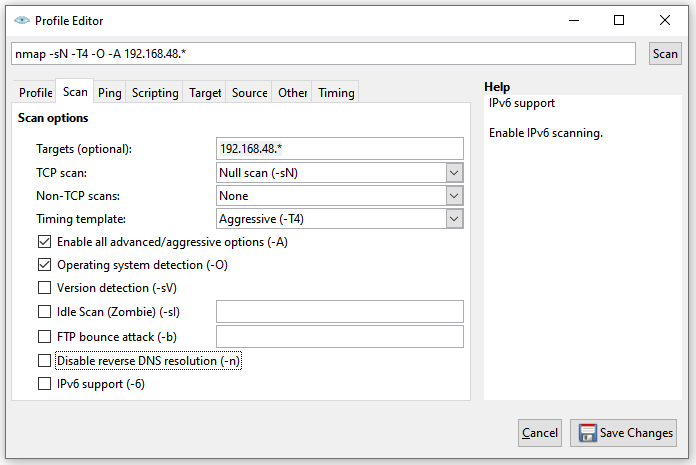
Ở tab host Detail hiện thị một vào thông tin cơ bản của máy đích



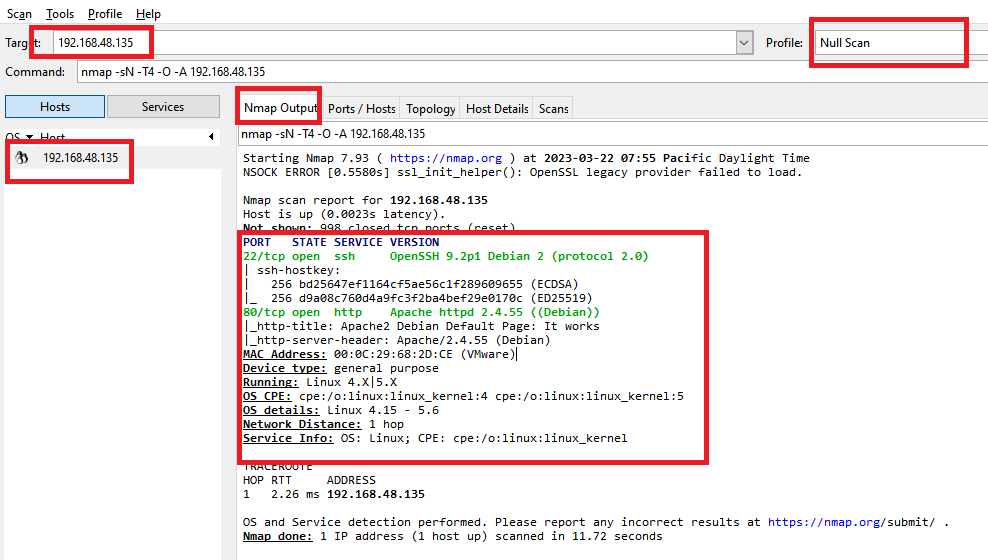
Tạo profile mới ( các option được tích hợp sẵn khi cần dùng k cần gõ lại )



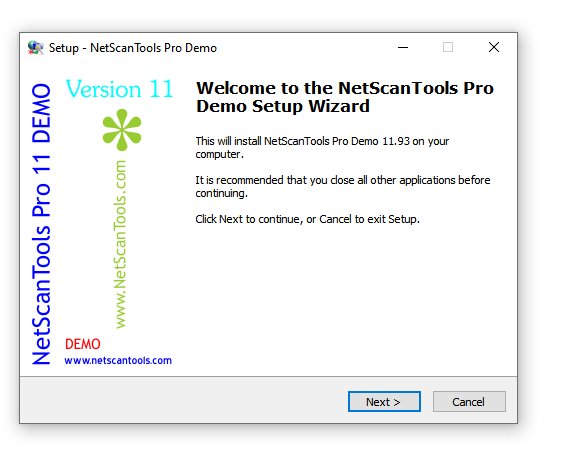
targets địa chỉ ip không cần phải nhập, tab profile đặt tên là Null Scan tùy chọn -sN sẽ gửi các gói tin rỗng

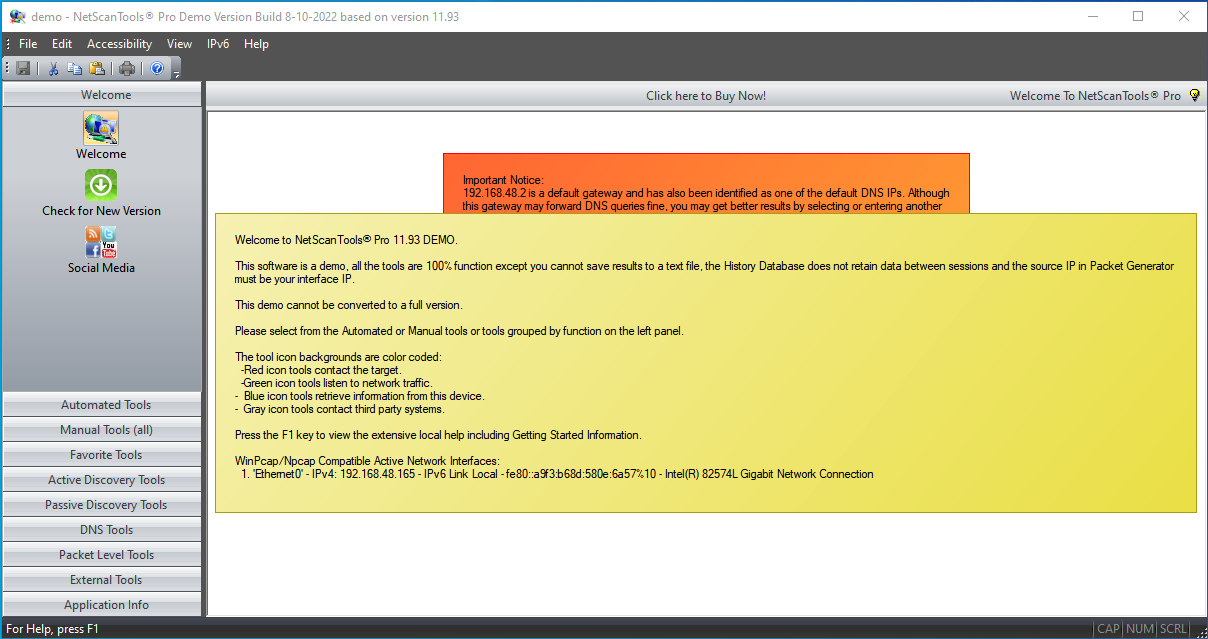


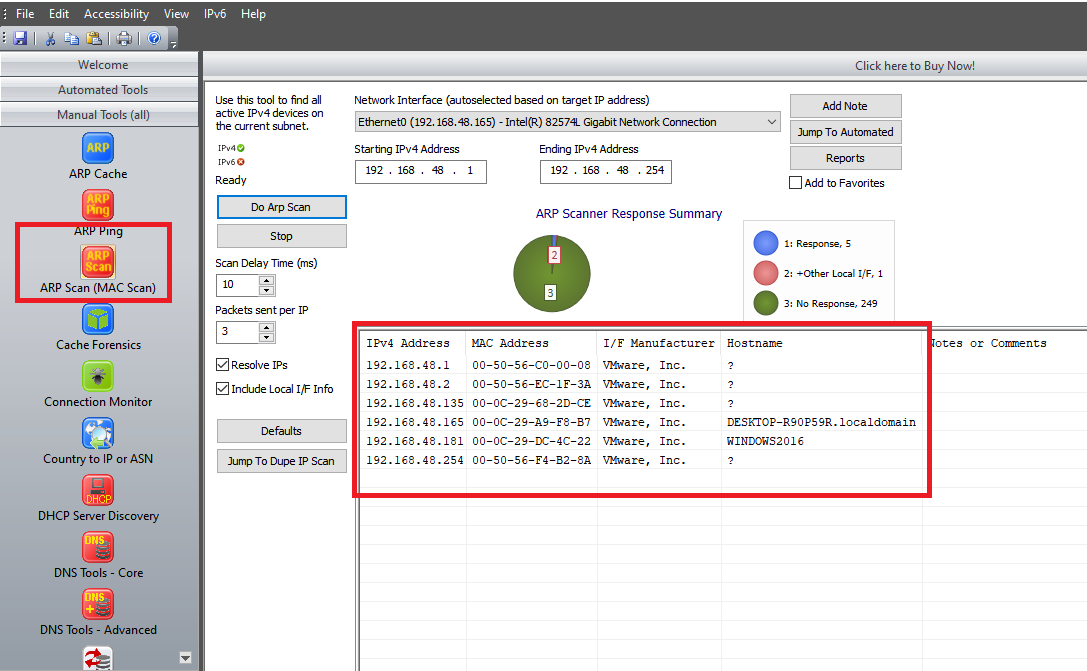
Ta dùng profile “Null Scan” và thay ip của máy cần quét các cổng



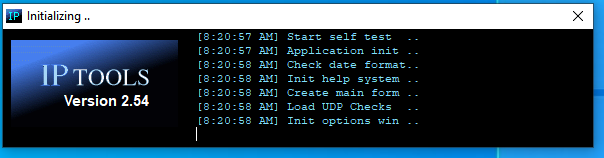
# NetScanTools Pro

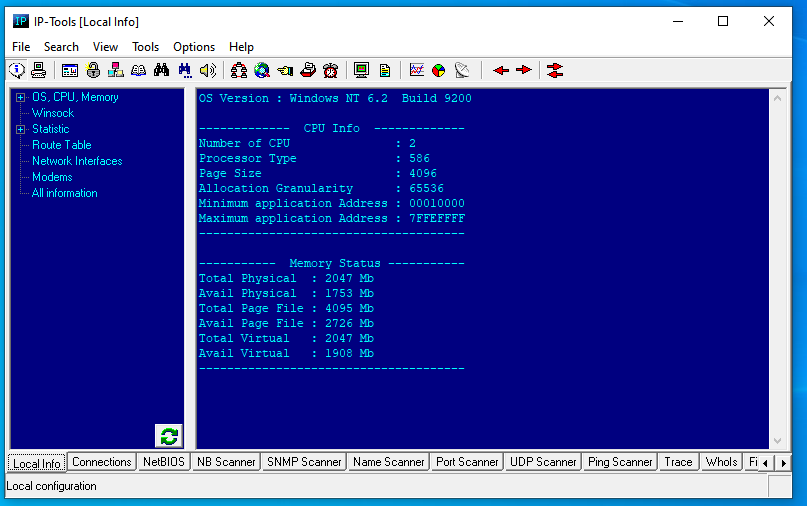


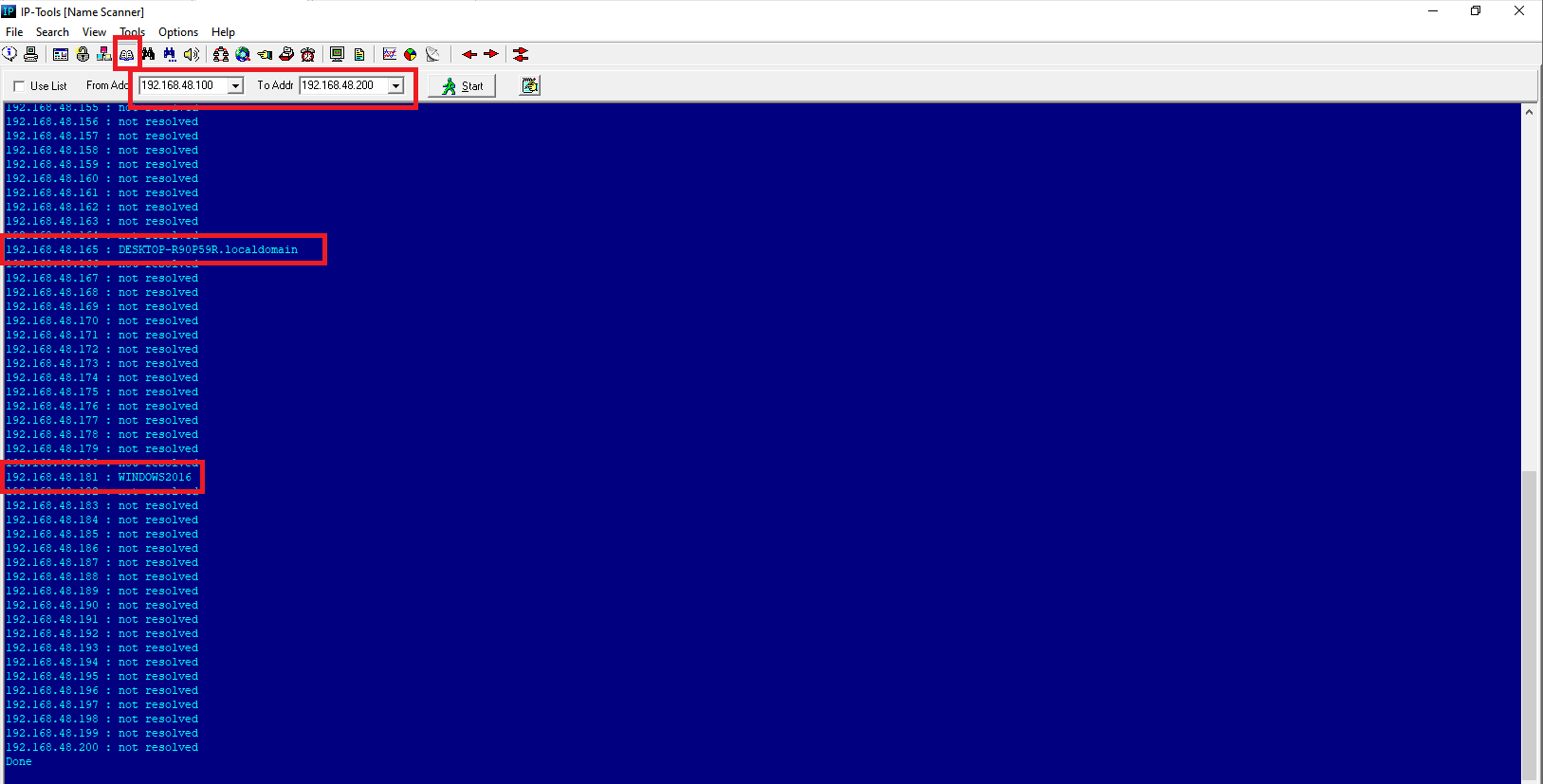


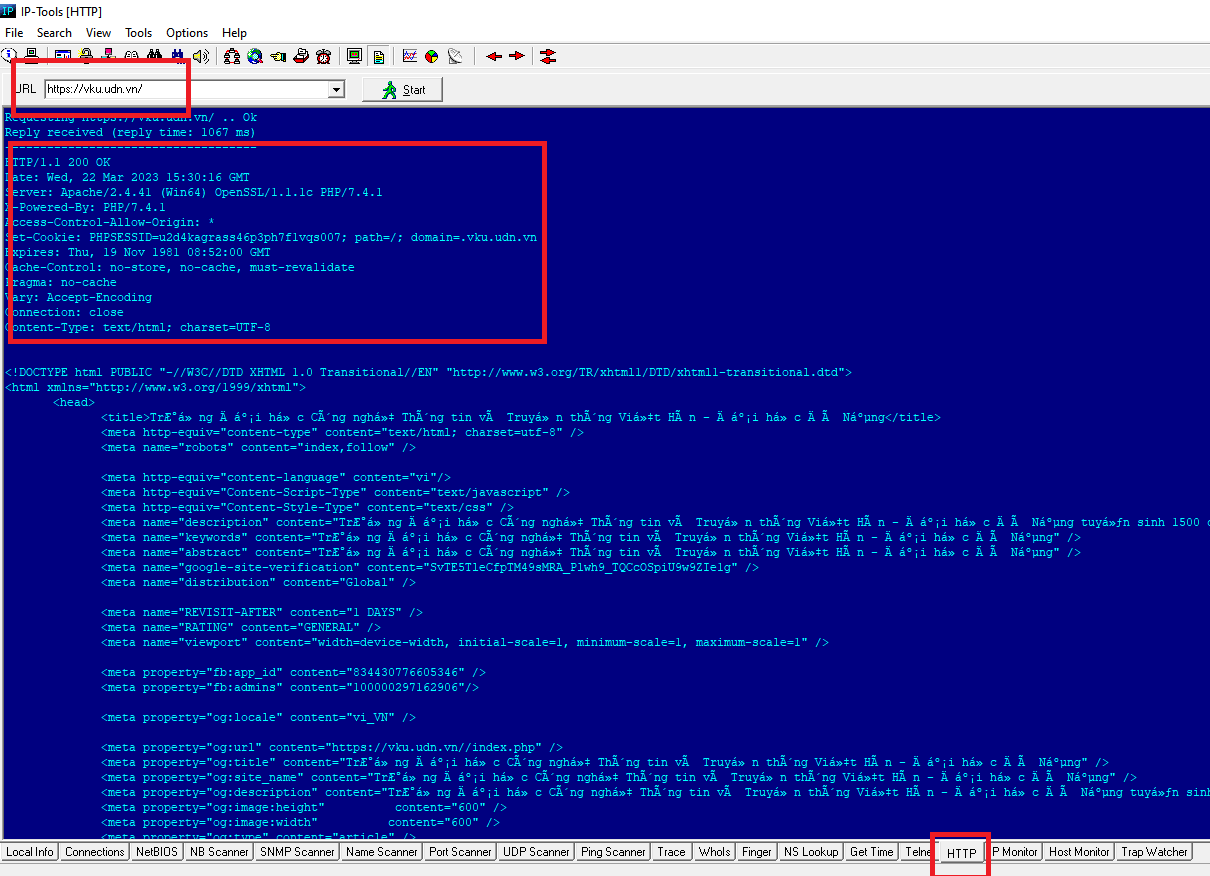


# IP-Tools



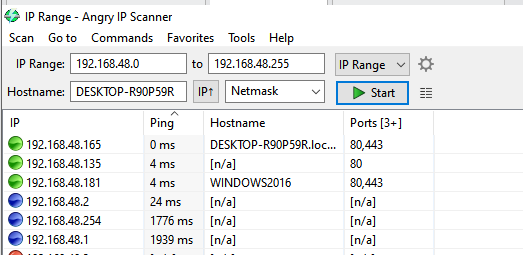




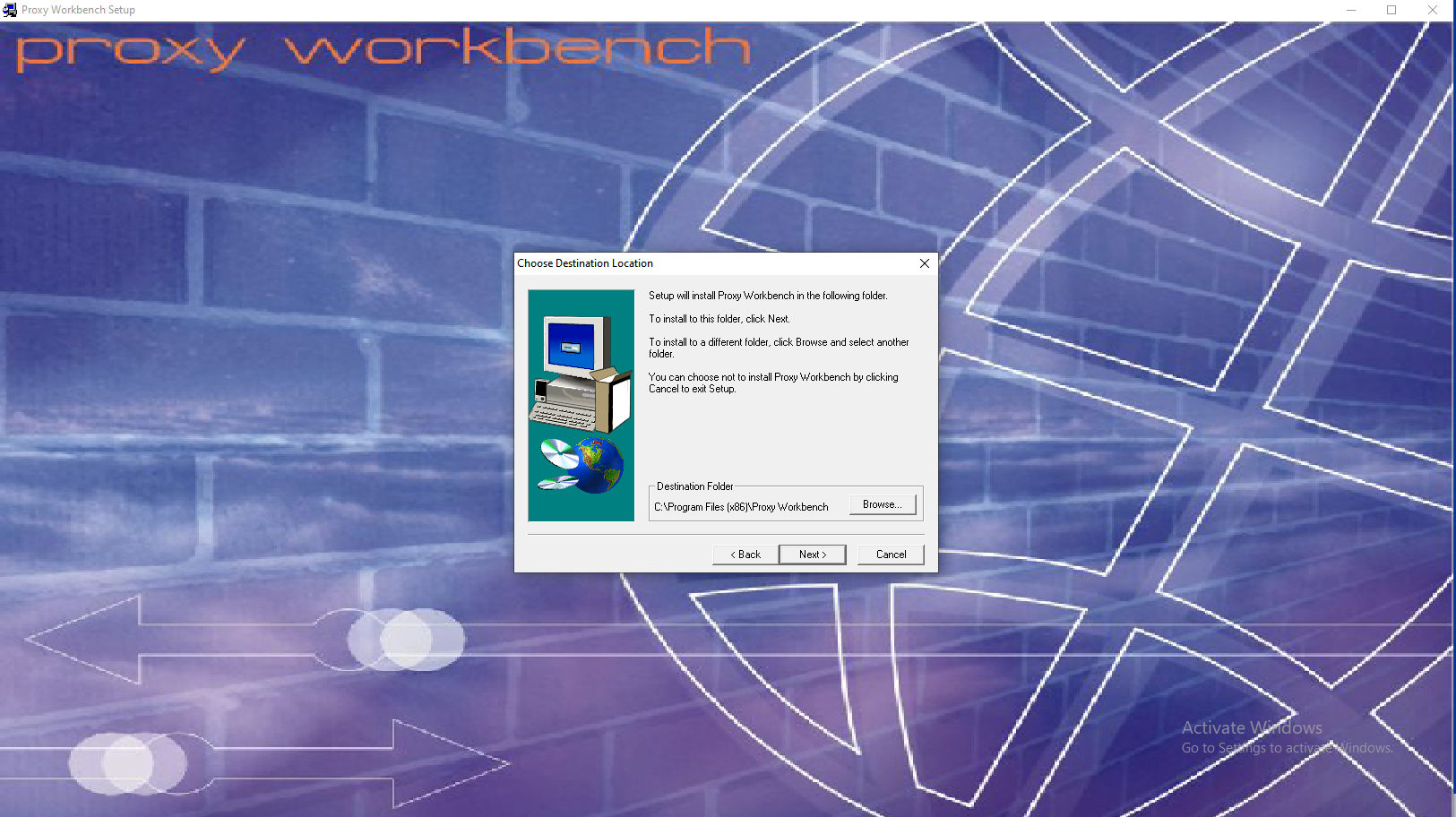


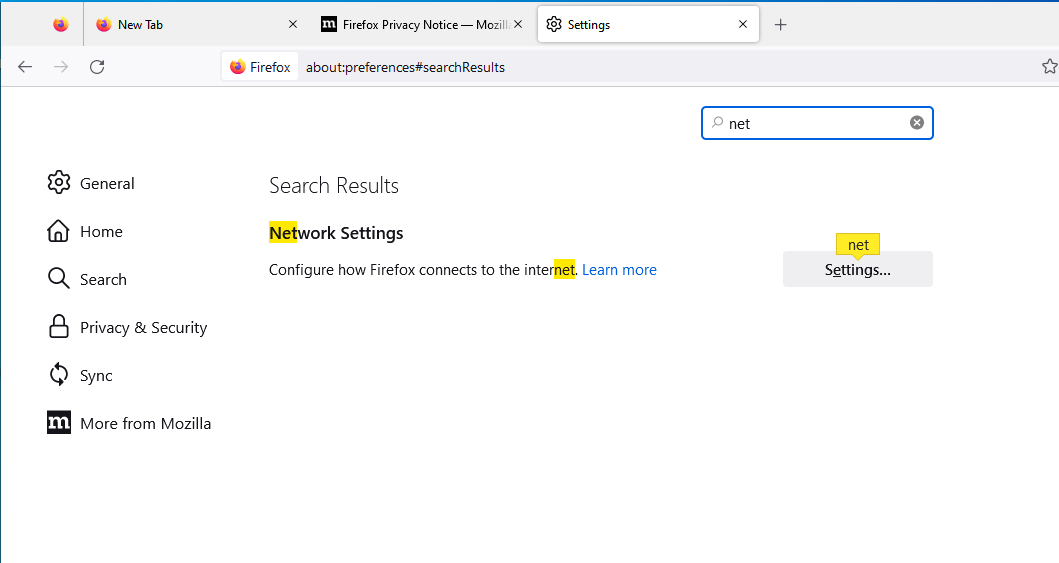
# Angry IP Scanner

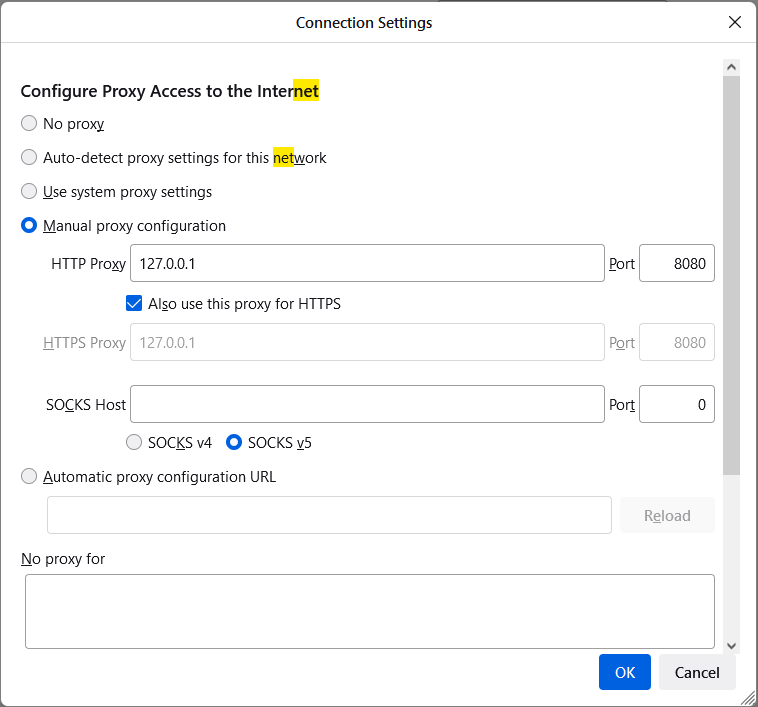


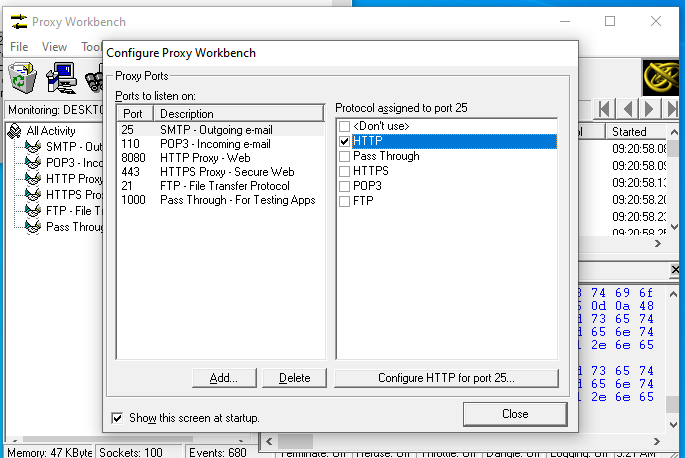


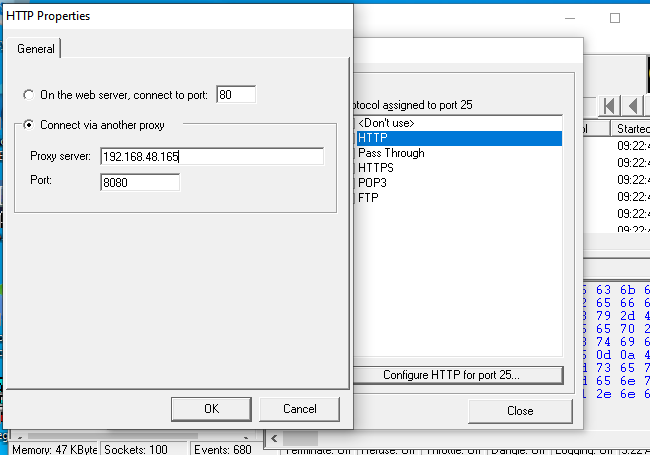
# Proxy Workbench

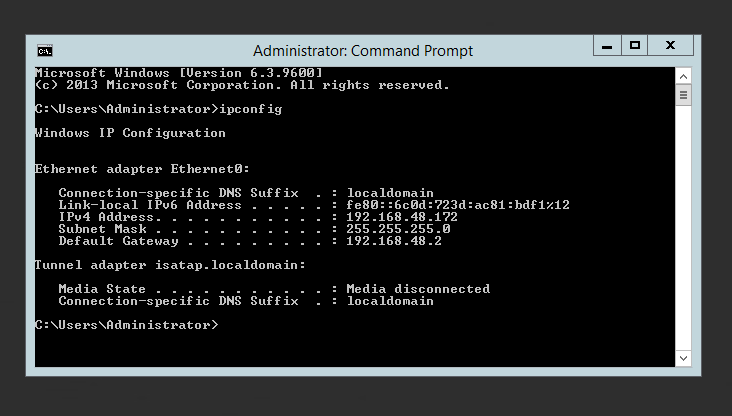


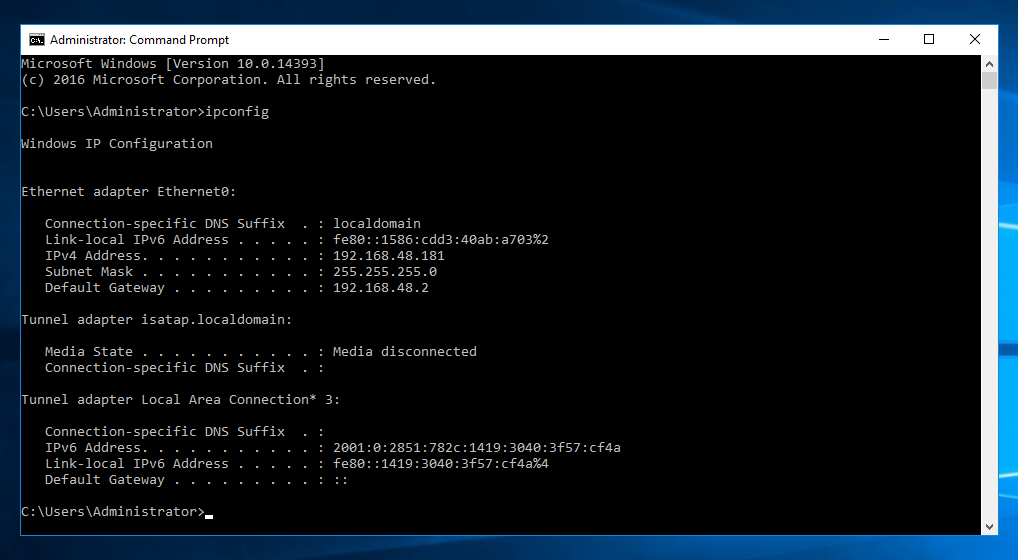


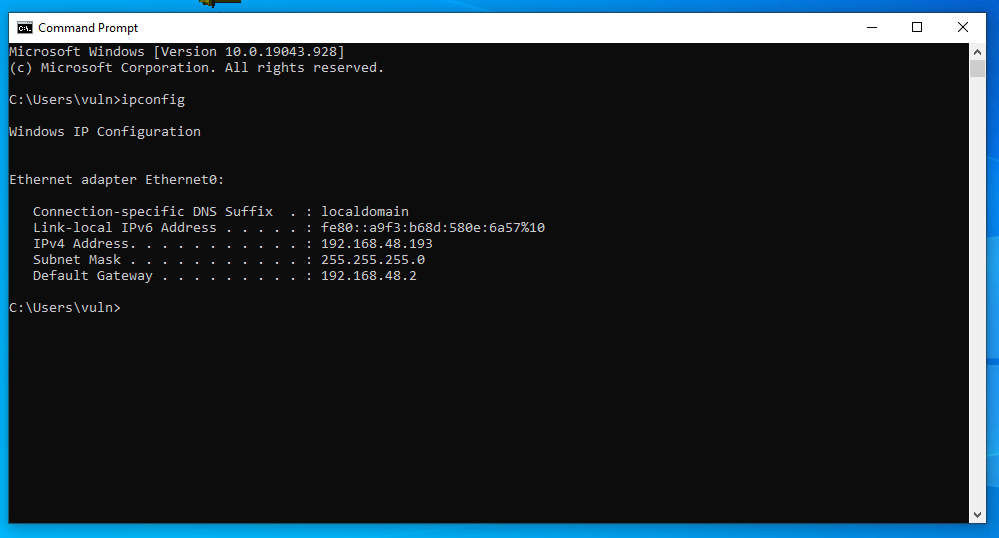




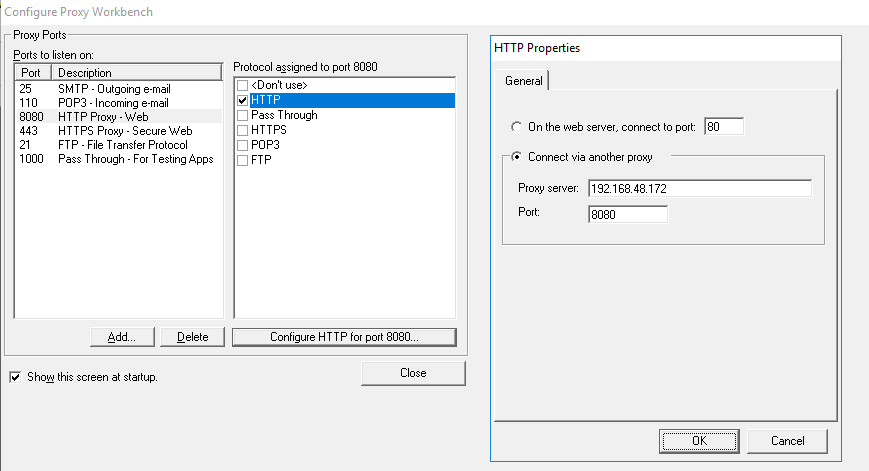




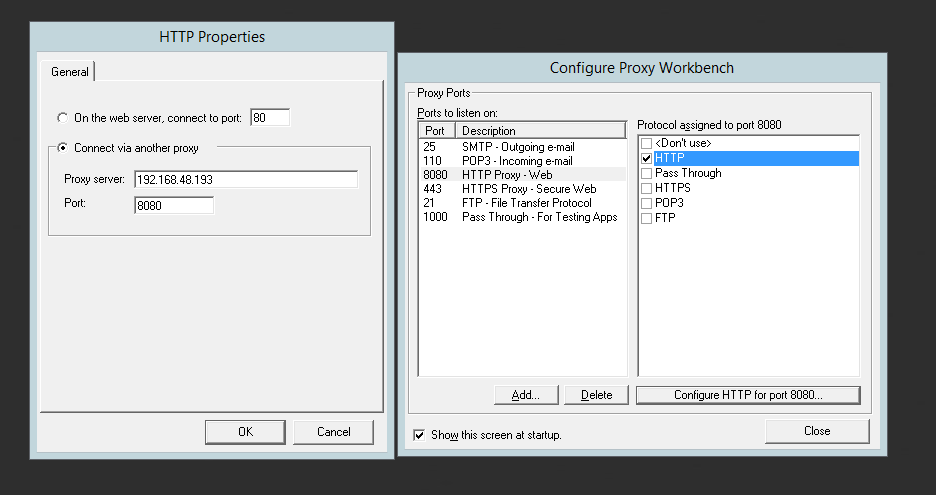




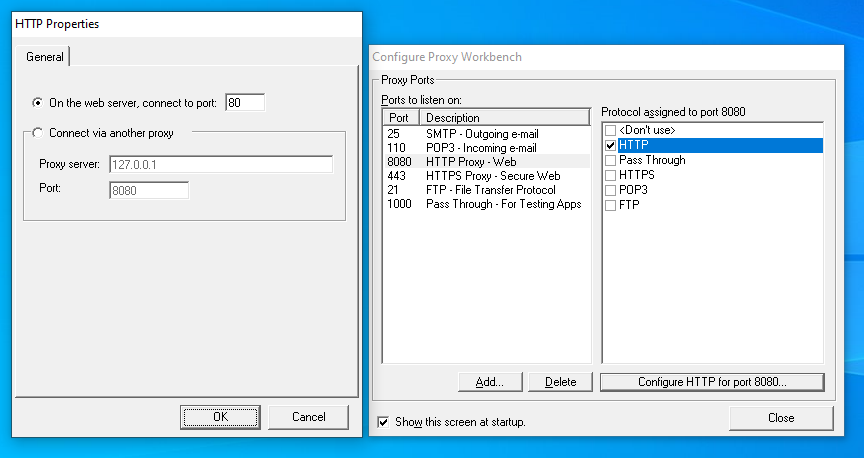
WINDOWS 2016

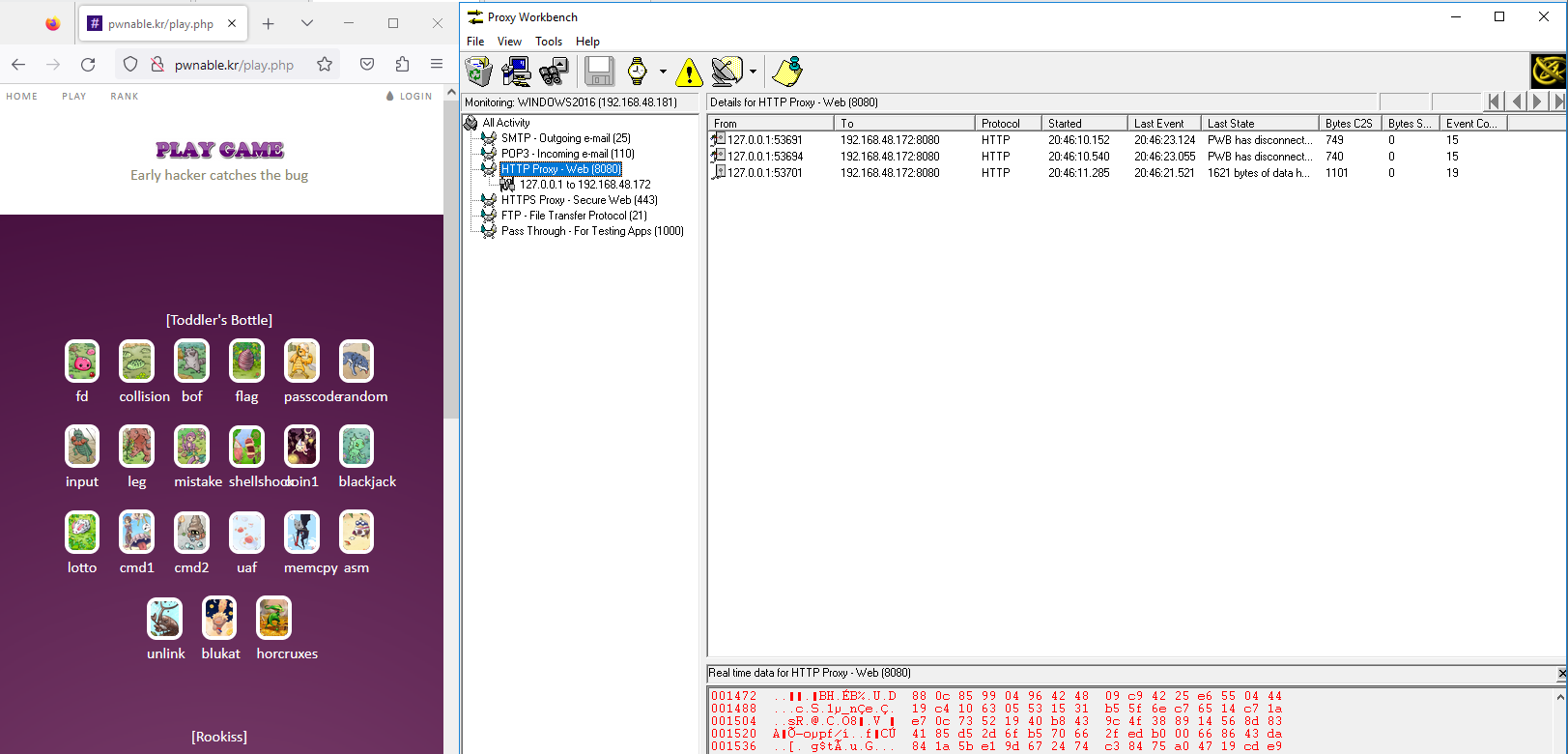


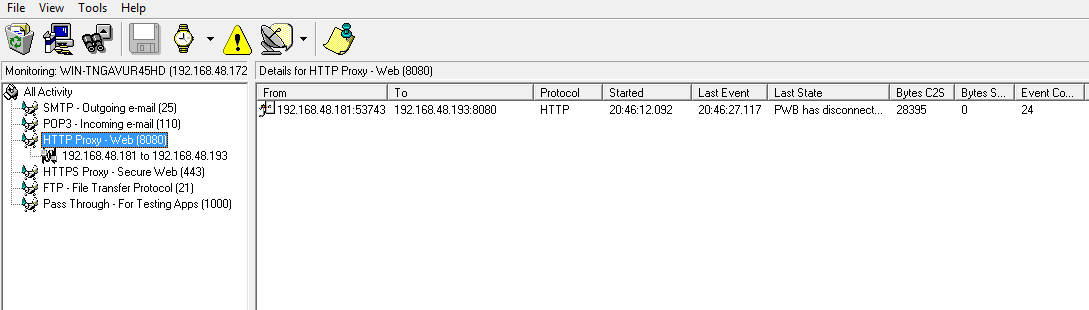
WINDOWS 2012

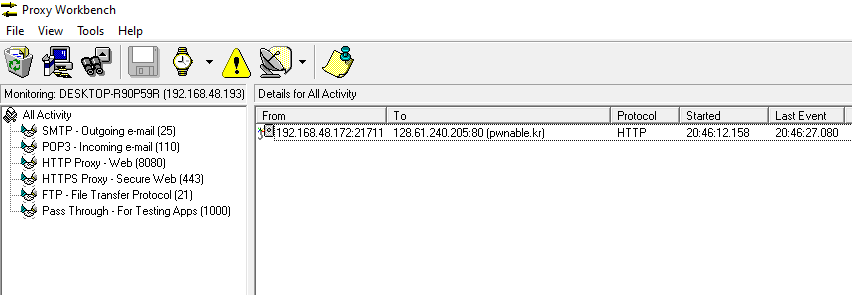


WINDOWS 10

  
DUYỆT WEB Ở WINDOWS 2016

****

****

****