

# BÁO CÁO THỰC HÀNH

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

Tên chủ đề: Viết rule trên Snort

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:<sup>1</sup>

STT	Nội dung	Tình trạng	Trang
1	<a href="#">Yêu cầu 1</a>	100%	
2	<a href="#">Yêu cầu 2</a>	100%	
3	<a href="#">Yêu cầu 3</a>	100%	
4	<a href="#">Yêu cầu 4</a>	100%	
5	<a href="#">Yêu cầu 5.1</a>	100%	
5	Yêu cầu 5.2	100%	
Điểm tự đánh giá			10/10

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

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

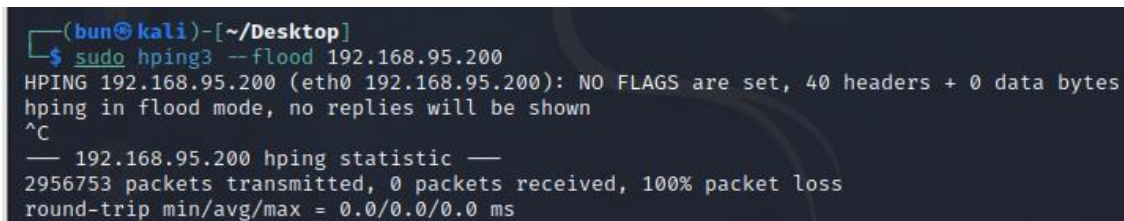
## BÁO CÁO CHI TIẾT

### Yêu cầu 1.1 Ngăn chặn tấn công ICMP Flood

- Viết Snort rule thực hiện giới hạn gói ICMP đến máy *Victim*. Ngưỡng (threshold) là không quá 23 gói/5s.
- Sử dụng công cụ **hping3** trên máy *Attacker* để thực hiện tấn công.
- Kiểm tra kết quả trước và sau khi cài đặt rule.

#### a) Trước khi dùng rule

- Tại máy attacker

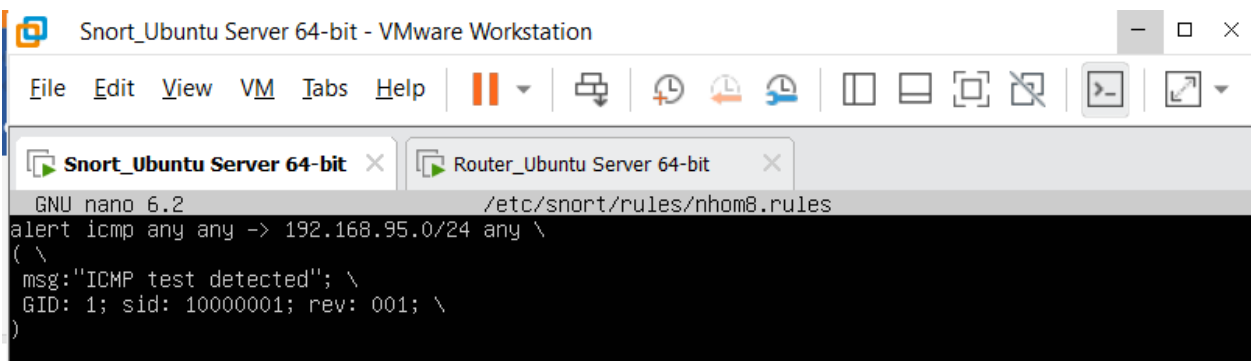


```
(bun@kali)~[~/Desktop]
$ sudo hping3 --flood 192.168.95.200
HPING 192.168.95.200 (eth0 192.168.95.200): NO FLAGS are set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
^C
— 192.168.95.200 hping statistic —
2956753 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

Sử dụng hping3 với option “--flood” để gửi liên tục hàng loạt các gói tin ICMP tới Victim nhằm thực hiện tấn công ICMP Flood

- Tại máy Snort

Dùng rule chỉ để thông báo để phát hiện có ICMP flood



```
Snort_Ubuntu Server 64-bit - VMware Workstation
File Edit View VM Tabs Help
GNU nano 6.2 /etc/snort/rules/nhom8.rules
alert icmp any any -> 192.168.95.0/24 any \
( \
  msg:"ICMP test detected"; \
  GID: 1; sid: 10000001; rev: 001; \
)
```

Xuất hiện các cảnh báo trên snort ngay sau khi attacker tấn công

```

root@server2:/etc/snort/rules# snort -c /etc/snort/nhom8-snort.conf -Q -q -i ens37:ens38 -A console
04/01-07:43:15.420574  [**] [1:2:1] Alert ICMP test [**] [Priority: 0] {TCP} 10.81.95.100:2694 -> 192.168.95.200:0
04/01-07:43:32.758574  [**] [1:2:1] Alert ICMP test [**] [Priority: 0] {TCP} 10.81.95.100:1770 -> 192.168.95.200:0
04/01-07:43:32.859532  [**] [1:2:1] Alert ICMP test [**] [Priority: 0] {TCP} 10.81.95.100:1771 -> 192.168.95.200:0
04/01-07:43:32.960091  [**] [1:2:1] Alert ICMP test [**] [Priority: 0] {TCP} 10.81.95.100:1772 -> 192.168.95.200:0
04/01-07:43:33.061461  [**] [1:2:1] Alert ICMP test [**] [Priority: 0] {TCP} 10.81.95.100:1773 -> 192.168.95.200:0
04/01-07:43:33.162246  [**] [1:2:1] Alert ICMP test [**] [Priority: 0] {TCP} 10.81.95.100:1774 -> 192.168.95.200:0
04/01-07:43:33.263212  [**] [1:2:1] Alert ICMP test [**] [Priority: 0] {TCP} 10.81.95.100:1775 -> 192.168.95.200:0
04/01-07:43:33.364025  [**] [1:2:1] Alert ICMP test [**] [Priority: 0] {TCP} 10.81.95.100:1776 -> 192.168.95.200:0
04/01-07:43:33.464571  [**] [1:2:1] Alert ICMP test [**] [Priority: 0] {TCP} 10.81.95.100:1777 -> 192.168.95.200:0
04/01-07:43:33.565067  [**] [1:2:1] Alert ICMP test [**] [Priority: 0] {TCP} 10.81.95.100:1778 -> 192.168.95.200:0
04/01-07:43:33.665812  [**] [1:2:1] Alert ICMP test [**] [Priority: 0] {TCP} 10.81.95.100:1779 -> 192.168.95.200:0

```

- Kiểm tra tại máy victim

```

msfadmin@metasploitable:~$ telnet goole.com 80
telnet: could not resolve goole.com/80: Name or service not known
msfadmin@metasploitable:~$ telnet goole.com 443
telnet: could not resolve goole.com/443: Name or service not known
msfadmin@metasploitable:~$ _

```

=> máy Victim không thể truy cập internet được nữa

## b) Sau khi thiết lập rule

Tại máy attacker thực hiện tấn công lại

```

(bun@kali)-[~/Desktop]
$ sudo hping3 --flood 192.168.95.200
HPING 192.168.95.200 (eth0 192.168.95.200): NO FLAGS are set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
^C
— 192.168.95.200 hping statistic —
690812 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms

```

=> Vì chế độ flood sẽ không hiển thị phản hồi gì nên thông tin nhận được sẽ không khác gì trước đó

- Tại Snort

Rất nhiều thông báo ngăn chặn ICMP Flood được snort đưa ra

```

04/01-07:38:02.278706 [Drop] [**] [1:2:1] Drop ICMP test [**] [Priority: 0] {TCP} 10.81.95.100:3837
-> 192.168.95.200:0
04/01-07:38:02.288939 [Drop] [**] [1:2:1] Drop ICMP test [**] [Priority: 0] {TCP} 10.81.95.100:3838
-> 192.168.95.200:0
04/01-07:38:02.293018 [Drop] [**] [1:2:1] Drop ICMP test [**] [Priority: 0] {TCP} 10.81.95.100:3839
-> 192.168.95.200:0
04/01-07:38:02.296995 [Drop] [**] [1:2:1] Drop ICMP test [**] [Priority: 0] {TCP} 10.81.95.100:3840
-> 192.168.95.200:0
04/01-07:38:02.305492 [Drop] [**] [1:2:1] Drop ICMP test [**] [Priority: 0] {TCP} 10.81.95.100:3841
-> 192.168.95.200:0
04/01-07:38:02.424026 [Drop] [**] [1:2:1] Drop ICMP test [**] [Priority: 0] {TCP} 10.81.95.100:3842
-> 192.168.95.200:0
04/01-07:38:02.445973 [Drop] [**] [1:2:1] Drop ICMP test [**] [Priority: 0] {TCP} 10.81.95.100:3843
-> 192.168.95.200:0
04/01-07:38:02.487530 [Drop] [**] [1:2:1] Drop ICMP test [**] [Priority: 0] {TCP} 10.81.95.100:3844
-> 192.168.95.200:0
04/01-07:38:02.513907 [Drop] [**] [1:2:1] Drop ICMP test [**] [Priority: 0] {TCP} 10.81.95.100:3845
-> 192.168.95.200:0
04/01-07:38:02.514921 [Drop] [**] [1:2:1] Drop ICMP test [**] [Priority: 0] {TCP} 10.81.95.100:3895
-> 192.168.95.200:0
04/01-07:38:02.514922 [Drop] [**] [1:2:1] Drop ICMP test [**] [Priority: 0] {TCP} 10.81.95.100:3846
-> 192.168.95.200:0
04/01-07:38:02.514922 [Drop] [**] [1:2:1] Drop ICMP test [**] [Priority: 0] {TCP} 10.81.95.100:3847
-> 192.168.95.200:0
04/01-07:38:02.514922 [Drop] [**] [1:2:1] Drop ICMP test [**] [Priority: 0] {TCP} 10.81.95.100:3848
-> 192.168.95.200:0
04/01-07:38:02.514922 [Drop] [**] [1:2:1] Drop ICMP test [**] [Priority: 0] {TCP} 10.81.95.100:3906
-> 192.168.95.200:0
04/01-07:38:02.514922 [Drop] [**] [1:2:1] Drop ICMP test [**] [Priority: 0] {TCP} 10.81.95.100:3849
-> 192.168.95.200:0
04/01-07:38:02.549618 [Drop] [**] [1:2:1] Drop ICMP test [**] [Priority: 0] {TCP} 10.81.95.100:3851
-> 192.168.95.200:0
04/01-07:38:02.549618 [Drop] [**] [1:2:1] Drop ICMP test [**] [Priority: 0] {TCP} 10.81.95.100:3955
-> 192.168.95.200:0
04/01-07:38:02.552596 [Drop] [**] [1:2:1] Drop ICMP test [**] [Priority: 0] {TCP} 10.81.95.100:3852
-> 192.168.95.200:0
  
```

=> Snort thành công ngăn chặn tấn công ICMP Flood

- Tại máy Victim:

```

msfadmin@metasploitable:~$ telnet google.com 443
Trying 172.217.27.14...
Connected to google.com.
Escape character is '^['.
  
```

=> Máy Victim vẫn kết nối được tới domain Google.com => truy cập được tới Internet

**Yêu cầu 1.2** Chỉ cho phép truy cập đến các dịch vụ đang chạy trên Victim

- Sử dụng **nmap** quét các cổng đang mở trên máy *Victim*.
- Viết Snort rule chỉ cho phép các máy truy cập đến các port đang mở của máy Victim. Chặn tất cả các port còn lại.
- Sử dụng công cụ **telnet** hoặc **nmap** trên máy Attacker thực hiện tấn công.
- Kiểm tra kết quả trước và sau khi cài đặt rule.
- Khởi chạy snort:

```
snort@snort:/etc/snort/rules$ sudo snort -c /etc/snort/nhom8-snort.conf -Q -i ens37:ens38_
```

- Trên máy kali, ta sử dụng công cụ nmap để quét các port đang mở:

```
(kali@kali)-[~]
$ nmap 192.168.95.200
Starting Nmap 7.94 ( https://nmap.org ) at 2024-04-01 04:08 EDT
Nmap scan report for 192.168.95.200
Host is up (0.032s latency).
Not shown: 977 closed tcp ports (conn-refused)
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

Nmap done: 1 IP address (1 host up) scanned in 0.48 seconds
(kali@kali)-[~]
$
```

- Thử kiểm tra trạng thái port 8080, ta thấy port này đang đóng:

```
(kali@kali)-[~]
$ nmap -p 8080 192.168.95.200
Starting Nmap 7.94 ( https://nmap.org ) at 2024-04-01 10:06 EDT
Nmap scan report for 192.168.95.200
Host is up (0.0014s latency).

PORT      STATE SERVICE
8080/tcp  closed http-proxy

Nmap done: 1 IP address (1 host up) scanned in 0.17 seconds
(kali@kali)-[~]
$
```

- Trên máy victim, ta dùng công cụ tcp dump để log các gói tin. Ta dễ dàng nhận thấy các gói tin được gửi từ máy kali được nhận tại port 8080 dù máy nạn nhận không phản hồi:

```
876(0) win 64240 <mss 1460,sackOK,timestamp 3501275627 0,nop,wscale 7>
05:39:31.379665 IP 192.168.95.200.www > 10.81.95.100.34134: S 810019534:81001953
4(0) ack 2362482877 win 5792 <mss 1460,sackOK,timestamp 637386 3501275627,nop,ws
cale 5>
05:39:31.379655 IP 10.81.95.100.58876 > 192.168.95.200.https: S 3717542015:37175
42015(0) win 64240 <mss 1460,sackOK,timestamp 3501275628 0,nop,wscale 7>
05:39:31.379725 IP 192.168.95.200.https > 10.81.95.100.58876: R 0:0(0) ack 37175
42016 win 0
05:39:31.379851 IP 192.168.95.200.40556 > dns.google.domain: 28055+ PTR? 100.95.
81.10.in-addr.arpa. (43)
05:39:31.380210 IP 10.81.95.100.34134 > 192.168.95.200.www: . ack 1 win 502 <nop
,nop,timestamp 3501275629 637386>
05:39:31.380258 IP 10.81.95.100.34134 > 192.168.95.200.www: R 1:1(0) ack 1 win 5
02 <nop,nop,timestamp 3501275629 637386>
05:39:31.431419 IP dns.google.domain > 192.168.95.200.40556: 28055 NXDomain 0/0/
0 (43)
05:39:31.529479 IP 10.81.95.100.34512 > 192.168.95.200.webcache: S 81465868:8146
5868(0) win 64240 <mss 1460,sackOK,timestamp 3501275778 0,nop,wscale 7>
05:39:31.529494 IP 192.168.95.200.webcache > 10.81.95.100.34512: R 0:0(0) ack 81
465869 win 0
05:39:32.224061 IP 192.168.95.1.51859 > 239.255.255.250.1900: UDP, length 175
05:39:32.224276 IP 192.168.195.1.51858 > 239.255.255.250.1900: UDP, length 175
05:39:34.380992 arp who-has 192.168.95.200 tell 192.168.95.1
05:39:34.381016 arp reply 192.168.95.200 is-at 00:0c:29:1f:58:a9 (oui Unknown)
```

- Snort rules:
  - PortVar: là biến chứa các port đang được mở trên máy victim
  - Alert: dùng để thông báo khi có những gói tin gửi vào các port đang mở
  - Block: chặn các gói tin gửi vào các port đang không mở

```
GNU nano 6.2                                nhom8.rules
PortVar open_ports [21,22,23,25,53,80,111,139,445,512,513,514,1099,1524,2049,2121,3306,5432,5900,60
alert tcp any any -> 192.168.95.200 $open_ports (msg:"Allow access to open ports"; sid:1000001;)
block tcp any any -> 192.168.95.200 !$open_ports (msg:"Block access to non-open ports"; sid:1000002)
```

- Tiến hành khởi chạy lại snort sau khi đã viết rules:

```
snort@snort:/etc/snort/rules$ sudo snort -c /etc/snort/nhom8-snort.conf -Q -i ens37:ens38_
```

- Ta sẽ thử dùng ftp vào port 21 đang mở, dùng công cụ tcpdump, ta có thể thấy máy victim đã nhận và phản hồi gói tin:

```
(kali@kali)-[~]
$ telnet 192.168.95.200 21
Trying 192.168.95.200 ...
Connected to 192.168.95.200.
Escape character is '^]'.
220 (vsFTPd 2.3.4)
```



```

687(0) ack 1400209457 win 5792 <mss 1460,sackOK,timestamp 738648 3502285200,nop,
wscale 5>
05:56:24.485326 IP 192.168.95.200.ftp > 10.81.95.100.46530: S 3746286687:3746286
687(0) ack 1400209457 win 5792 <mss 1460,sackOK,timestamp 738697 3502285200,nop,
wscale 5>
05:56:26.085520 IP 192.168.95.200.ftp > 10.81.95.100.60708: S 3476643641:3476643
641(0) ack 3101222 win 5792 <mss 1460,sackOK,timestamp 738857 3502267583,nop,ws
cale 5>
05:56:28.126161 IP 10.81.95.100.46530 > 192.168.95.200.ftp: S 1400209456:1400209
456(0) win 65535 <mss 1460,sackOK,timestamp 3502292359 0,nop,wscale 2>
05:56:28.126228 IP 192.168.95.200.ftp > 10.81.95.100.46530: S 3746286687:3746286
687(0) ack 1400209457 win 5792 <mss 1460,sackOK,timestamp 739061 3502285200,nop,
wscale 5>
05:56:30.285356 IP 192.168.95.200.ftp > 10.81.95.100.43442: S 2403365387:2403365
387(0) ack 3156708579 win 5792 <mss 1460,sackOK,timestamp 739277 3502198868,nop,
wscale 5>
05:56:30.885290 IP 192.168.95.200.ftp > 10.81.95.100.46530: S 3746286687:3746286
687(0) ack 1400209457 win 5792 <mss 1460,sackOK,timestamp 739337 3502285200,nop,
wscale 5>
05:56:36.318454 IP 10.81.95.100.46530 > 192.168.95.200.ftp: S 1400209456:1400209
456(0) win 65535 <mss 1460,sackOK,timestamp 3502300551 0,nop,wscale 2>
05:56:36.318476 IP 192.168.95.200.ftp > 10.81.95.100.46530: S 3746286687:3746286
687(0) ack 1400209457 win 5792 <mss 1460,sackOK,timestamp 739880 3502285200,nop,
wscale 5>

```

- Kiểm tra alert tại /var/log/snort/alert, ta thấy các gói tin gửi đến port 21 được thông báo cho phép truy cập:

```

[**] [1:1000001:0] Allow access to open ports [**]
[Priority: 0]
04/01-14:43:49.383299 10.81.95.100:48270 -> 192.168.95.200:21
TCP TTL:63 TOS:0x0 ID:40119 IpLen:20 DgmLen:60 DF
*****S* Seq: 0xA9011539 Ack: 0x0 Win: 0xFAF0 TcpLen: 40
TCP Options (5) => MSS: 1460 SackOK TS: 3503512694 0 NOP WS: 7

[**] [1:1000001:0] Allow access to open ports [**]
[Priority: 0]
04/01-14:43:49.385572 10.81.95.100:48270 -> 192.168.95.200:21
TCP TTL:63 TOS:0x0 ID:40120 IpLen:20 DgmLen:52 DF
***A**** Seq: 0xA901153A Ack: 0x5A8693A3 Win: 0x1F6 TcpLen: 32
TCP Options (3) => NOP NOP TS: 3503512698 861096

[**] [1:1000001:0] Allow access to open ports [**]
[Priority: 0]
04/01-14:43:49.388081 10.81.95.100:48270 -> 192.168.95.200:21
TCP TTL:63 TOS:0x0 ID:40121 IpLen:20 DgmLen:52 DF
***A**** Seq: 0xA901153A Ack: 0x5A8693B7 Win: 0x1F6 TcpLen: 32
TCP Options (3) => NOP NOP TS: 3503512701 861097

snort@snort:/etc/snort/rules$ _

```

- Ta sẽ thử với một port đang đóng là 8080:

```

(kali@kali)-[~]
$ telnet 192.168.95.200 8080
Trying 192.168.95.200 ...

```

- Trên công cụ tcpdump, ta không nhận thấy bất kỳ gói tin nào được gửi đến port 8080 của máy nạn nhân:

```
06:00:21.202804 IP 192.168.95.1.mdns > mdns.mcast.net.mdns: 0*- [0q] 2/0/0 AAAA[
idomain]
06:00:21.202842 IP 192.168.195.1.mdns > mdns.mcast.net.mdns: 0*- [0q] 2/0/0 AAAA
[idomain]
06:00:21.202912 IP 192.168.95.1.mdns > mdns.mcast.net.mdns: 0*- [0q] 2/0/0 AAAA[
idomain]
06:00:21.203161 IP 192.168.195.1.mdns > mdns.mcast.net.mdns: 0*- [0q] 2/0/0 AAAA
[idomain]
06:00:21.203532 IP 192.168.95.1.mdns > mdns.mcast.net.mdns: 0*- [0q] 2/0/0 AAAA[
idomain]
06:00:21.203533 IP 192.168.195.1.mdns > mdns.mcast.net.mdns: 0*- [0q] 2/0/0 AAAA
[idomain]
06:00:21.203686 IP 192.168.95.1.mdns > mdns.mcast.net.mdns: 0*- [0q] 2/0/0 AAAA[
idomain]
06:00:21.203912 IP 192.168.195.1.mdns > mdns.mcast.net.mdns: 0*- [0q] 2/0/0 AAAA
[idomain]
06:00:21.624733 IP 192.168.95.1 > igmp.mcast.net: igmp v3 report, 1 group record
(s)
06:00:21.624735 IP6 fe80::336b:5ac8:7e9c:1dd7 > ff02::16: HBH ICMP6, multicast l
istener report v2, 1 group record(s), length 28
06:00:21.625224 IP 192.168.195.1 > igmp.mcast.net: igmp v3 report, 1 group recor
d(s)
06:00:21.625439 IP6 fe80::70de:5193:adb0:8f18 > ff02::16: HBH ICMP6, multicast l
istener report v2, 1 group record(s), length 28
```

- Kiểm tra alert tại /var/log/snort/alert, ta thấy các gói tin đã bị chặn:



```
[**] [1:1000002:0] Block access to non-open ports [**]
[Priority: 0]
04/01-14:48:53.342632 10.81.95.100:55238 -> 192.168.95.200:8080
TCP TTL:63 TOS:0x0 ID:37364 IpLen:20 DgmLen:60 DF
*****S* Seq: 0x4C540C86 Ack: 0x0 Win: 0xFAF0 TcpLen: 40
TCP Options (5) => MSS: 1460 SackOK TS: 3503816639 0 NOP WS: 7

[**] [1:1000002:0] Block access to non-open ports [**]
[Priority: 0]
04/01-14:48:55.355267 10.81.95.100:55238 -> 192.168.95.200:8080
TCP TTL:63 TOS:0x0 ID:37365 IpLen:20 DgmLen:60 DF
*****S* Seq: 0x4C540C86 Ack: 0x0 Win: 0xFAF0 TcpLen: 40
TCP Options (5) => MSS: 1460 SackOK TS: 3503818651 0 NOP WS: 7

[**] [1:1000002:0] Block access to non-open ports [**]
[Priority: 0]
04/01-14:48:59.428615 10.81.95.100:55238 -> 192.168.95.200:8080
TCP TTL:63 TOS:0x0 ID:37366 IpLen:20 DgmLen:60 DF
*****S* Seq: 0x4C540C86 Ack: 0x0 Win: 0xFAF0 TcpLen: 40
TCP Options (5) => MSS: 1460 SackOK TS: 3503822719 0 NOP WS: 7

[**] [1:1000002:0] Block access to non-open ports [**]
[Priority: 0]
04/01-14:49:07.615334 10.81.95.100:55238 -> 192.168.95.200:8080
TCP TTL:63 TOS:0x0 ID:37367 IpLen:20 DgmLen:60 DF
*****S* Seq: 0x4C540C86 Ack: 0x0 Win: 0xFAF0 TcpLen: 40
TCP Options (5) => MSS: 1460 SackOK TS: 3503830911 0 NOP WS: 7

[**] [1:1000002:0] Block access to non-open ports [**]
[Priority: 0]
04/01-14:49:23.755664 10.81.95.100:55238 -> 192.168.95.200:8080
TCP TTL:63 TOS:0x0 ID:37368 IpLen:20 DgmLen:60 DF
*****S* Seq: 0x4C540C86 Ack: 0x0 Win: 0xFAF0 TcpLen: 40
TCP Options (5) => MSS: 1460 SackOK TS: 3503847051 0 NOP WS: 7

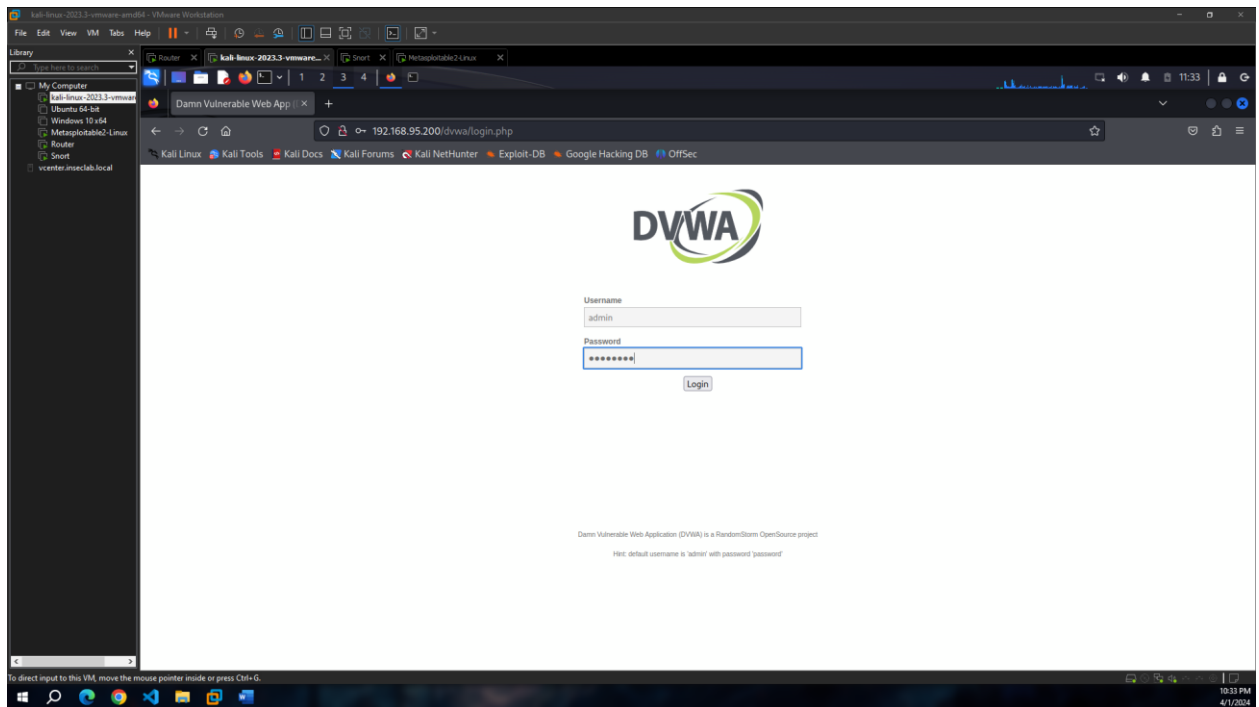
snort@snort:/etc/snort/rules$ _
```

#### **Yêu cầu 1.4** Ngăn chặn tấn công Path Traversal

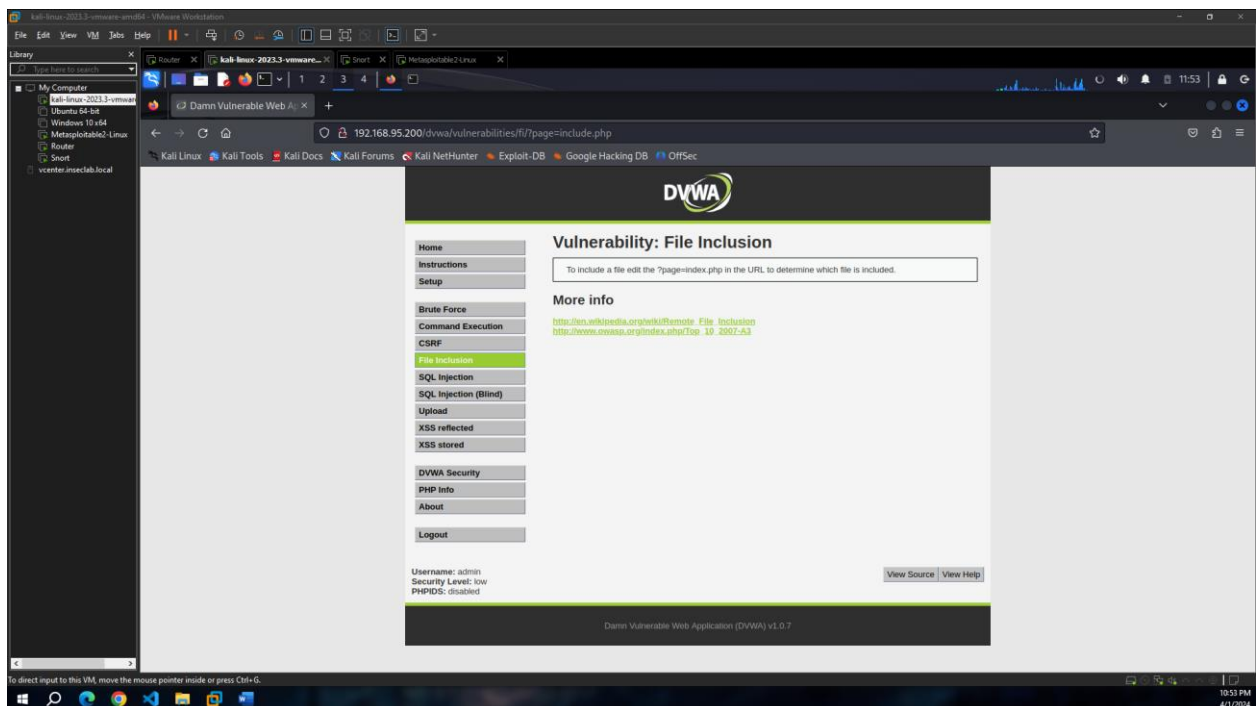
- Viết Snort rule ngăn chặn các tấn công Path Traversal1
- Trên máy Attacker truy cập đến đường dẫn <http://192.168.x.200/dvwa/> để thực hiện tấn công.
- Kiểm tra kết quả trước và sau khi thực hiện tấn công

#### Thực hiện:

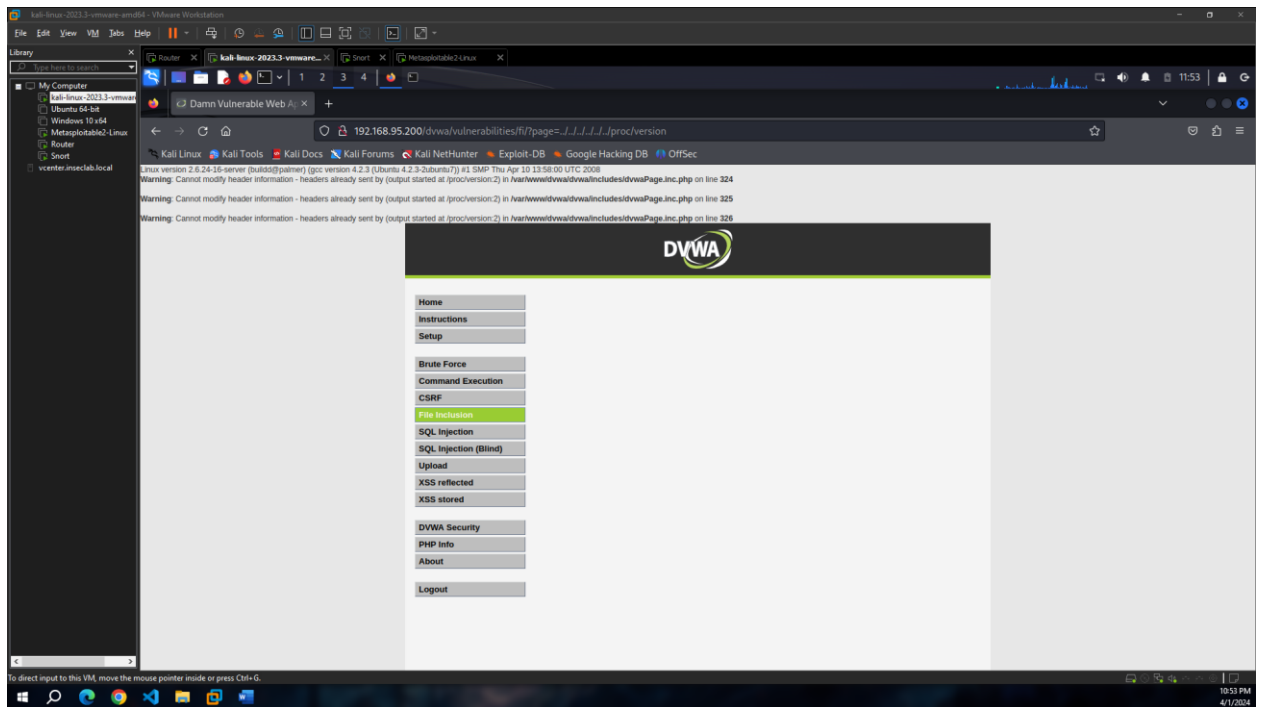
- Truy cập vào đường dẫn <http://192.168.x.200/dvwa/> và đăng nhập với username: admin và password: password:



- Tại trang chủ, ta chọn File Inclusion để tiến hành tấn công, sau một vài lần thử nghiệm, payload tìm được: ../../../../../../proc/version



- Đây là payload có thể lấy thông tin version của server:



- Viết snort rule để ngăn chặn tấn công Path Traversal:
  - Flow: hướng đi của TCP, established là hướng gửi từ client đến server
  - Content: nội dung trong gói TCP
  - “../” là payload được chèn ở url nhằm khai thác thông tin

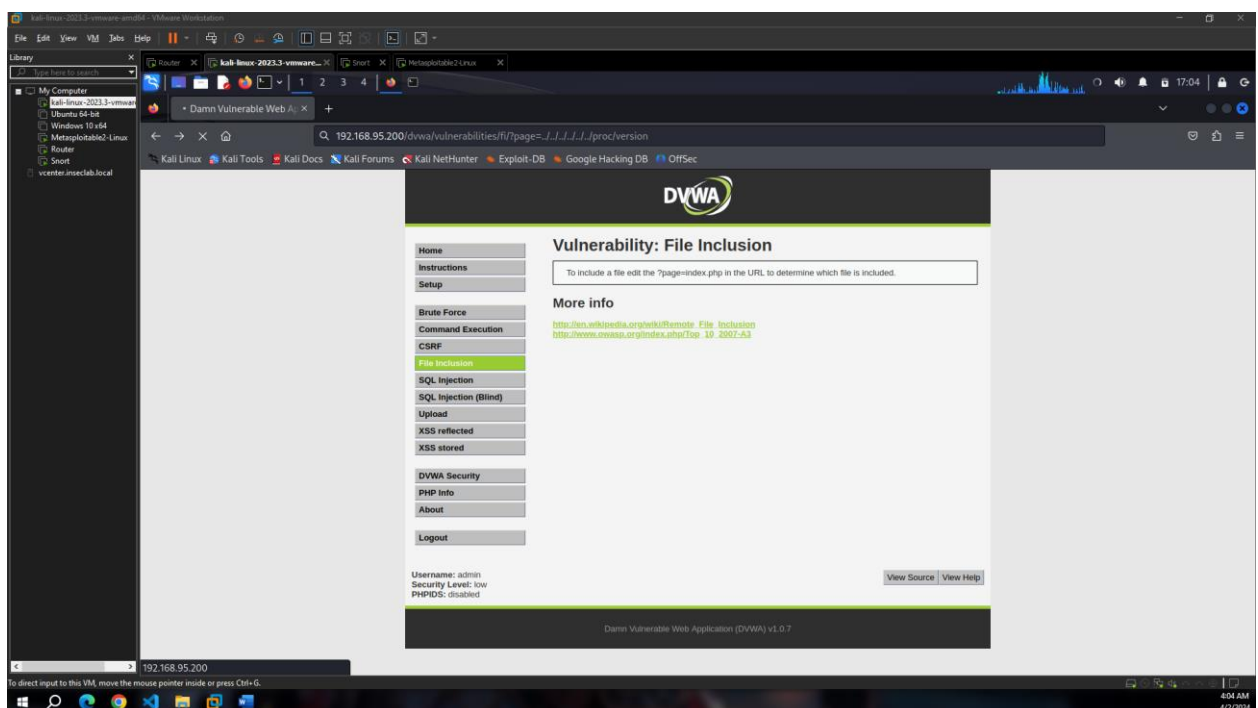
```

GNU nano 6.2                                nhom8.rules *
PortVar open_ports [21,22,23,25,53,80,111,139,445,512,513,514,1099,1524,2049,2121,3306,5432,5900,60
alert tcp any any -> 192.168.95.200 $open_ports (msg:"Allow access to open ports"; sid:1000001;)
block tcp any any -> 192.168.95.200 !$open_ports (msg:"Block access to non-open ports"; sid:1000002)
drop tcp any any -> 192.168.95.200 80 (
msg:"Potential Path Traversal Attack Detected";
flow:established;
content:"GET";
content:"HTTP";
fast_pattern;
content:"../";
nocase;
session:all;
sid:1000005; rev:1)

```

Help Exit Write Out Read File Where Is Replace Cut Paste Execute Justify Location Go To Line Undo Redo

- Sau khi viết rule và tiến hành khởi chạy snort, thì khi chèn payload vào url đã không thể khai thác được thông tin version như trước nữa:



- Sử dụng tcpdump để kiểm tra từ lúc chèn payload và gửi, máy victim không nhận được gói tin nào từ máy kali:

```

17:17:29.176823 IP 192.168.95.1 > igmp.mcast.net: igmp v3 report, 1 group record
(s)
17:17:29.176824 IP6 fe80::336b:5ac8:7e9c:1dd7 > ff02::16: HBH ICMP6, multicast l
istener report v2, 1 group record(s), length 28
17:17:29.177123 IP 192.168.195.1 > igmp.mcast.net: igmp v3 report, 1 group recor
d(s)
17:17:29.177364 IP6 fe80::70de:5193:adb0:8f18 > ff02::16: HBH ICMP6, multicast l
istener report v2, 1 group record(s), length 28
17:17:35.442054 IP 192.168.95.1.65156 > 239.255.255.250.1900: UDP, length 175
17:17:35.442276 IP 192.168.95.200.39996 > dns.google.domain: 32572+ PTR? 250.255
.255.239.in-addr.arpa. (46)
17:17:35.442579 IP 192.168.195.1.65155 > 239.255.255.250.1900: UDP, length 175
17:17:35.497083 IP dns.google.domain > 192.168.95.200.39996: 32572 NXDomain 0/1/
0 (103)
17:17:36.451651 IP 192.168.95.1.65156 > 239.255.255.250.1900: UDP, length 175
17:17:36.452125 IP 192.168.195.1.65155 > 239.255.255.250.1900: UDP, length 175
17:17:37.456805 IP 192.168.95.1.65156 > 239.255.255.250.1900: UDP, length 175
17:17:37.457450 IP 192.168.195.1.65155 > 239.255.255.250.1900: UDP, length 175
17:17:38.457394 IP 192.168.95.1.65156 > 239.255.255.250.1900: UDP, length 175
17:17:38.457631 IP 192.168.195.1.65155 > 239.255.255.250.1900: UDP, length 175
17:17:40.434760 arp who-has 192.168.95.1 tell 192.168.95.200
17:17:40.435545 arp reply 192.168.95.1 is-at 00:0c:29:3c:7e:49 (oui Unknown)
17:17:40.679153 arp who-has 192.168.95.200 tell 192.168.95.1
17:17:40.679165 arp reply 192.168.95.200 is-at 00:0c:29:1f:58:a9 (oui Unknown)
-

```

- Kiểm tra alert của snort, rule đã được thực thi, gói tin chứa payload đã bị drop:

```

[**] [1:1000005:1] Potential Path Traversal Attack Detected [**]
[Priority: 0]
04/01-21:04:09.530201 10.81.95.100:56126 -> 192.168.95.200:80
TCP TTL:63 TOS:0x0 ID:13103 IpLen:20 DgmLen:516 DF
***AP*** Seq: 0xBF165545 Ack: 0xADF939FA Win: 0x1F6 TcpLen: 32
TCP Options (3) => NOP NOP TS: 2221828690 449547

[**] [1:1000001:0] Allow access to open ports [**]
[Priority: 0]
04/01-21:04:12.515820 10.81.95.100:56126 -> 192.168.95.200:80
TCP TTL:63 TOS:0x0 ID:13104 IpLen:20 DgmLen:52 DF
***A*** Seq: 0xBF165715 Ack: 0xADF939FA Win: 0x1F6 TcpLen: 32
TCP Options (3) => NOP NOP TS: 2221831676 449547

[**] [1:1000005:1] Potential Path Traversal Attack Detected [**]
[Priority: 0]
04/01-21:04:16.189862 10.81.95.100:56126 -> 192.168.95.200:80
TCP TTL:63 TOS:0x0 ID:13105 IpLen:20 DgmLen:516 DF
***AP*** Seq: 0xBF165545 Ack: 0xADF939FA Win: 0x1F6 TcpLen: 32
TCP Options (3) => NOP NOP TS: 2221835350 449547

[**] [1:1000005:1] Potential Path Traversal Attack Detected [**]
[Priority: 0]
04/01-21:04:29.501759 10.81.95.100:56126 -> 192.168.95.200:80
TCP TTL:63 TOS:0x0 ID:13106 IpLen:20 DgmLen:516 DF
***AP*** Seq: 0xBF165545 Ack: 0xADF939FA Win: 0x1F6 TcpLen: 32
TCP Options (3) => NOP NOP TS: 2221848662 449547

[**] [1:1000005:1] Potential Path Traversal Attack Detected [**]
[Priority: 0]
04/01-21:04:31.549948 10.81.95.100:33160 -> 192.168.95.200:80
TCP TTL:63 TOS:0x0 ID:46542 IpLen:20 DgmLen:516 DF
***AP*** Seq: 0xF0300DBA Ack: 0x9613555A Win: 0x1F6 TcpLen: 32
TCP Options (3) => NOP NOP TS: 2221850710 446976

snort@snort:/etc/snort/rules$

```

**Yêu cầu 1.3** Ngăn chặn tấn công dò mật khẩu trên ứng dụng Web

- Truy cập vào ứng dụng web Mutillidae ([/mutillidae/index.php?page=login.php](http://mutillidae/index.php?page=login.php)) trên máy Victim. Viết Snort rule ngăn chặn tấn công dò mật khẩu đăng nhập trên ứng dụng web này. **Lưu ý:** chỉ chặn dò mật khẩu, ứng dụng web vẫn phải truy cập bình thường.
- Sử dụng công cụ **hydra** trên máy Attacker thực hiện tấn công.
- Kiểm tra kết quả trước và sau khi cài đặt rule.

**a) Trước khi thiết lập rule**

Thực hiện tấn công trên máy attacker (Kali linux)

=> Việc brute force diễn ra **thành công** nhưng do không có mật khẩu nào đúng để đăng nhập nên hydra đưa ra thông báo **"1 of 1 target completed, 0 valid password found"**

```

(bun@kali)-[~/Downloads]
$ hydra -l msfadmin -P passforbruteforce.txt 192.168.95.200 http-post-form "/mutillidae/index.php?page=login.php:username=^USER^&password=^PASS^&login-php-submit-button=Login:F=Not Logged In" -V
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these ** ignore laws and ethics anyway).

File Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-04-06 11:58:40
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 15 tasks per 1 server, overall 15 tasks, 15 login tries (l:1/p:15), ~1 try per task
[DATA] attacking http-post-form://192.168.95.200:80/mutillidae/index.php?page=login.php:username=^USER^&password=^PASS^&login-php-submit-button=Login:F=Not Logged In
[ATTEMPT] target 192.168.95.200 - login "msfadmin" - pass "nt123456" - 1 of 15 [child 0] (0/0)
[ATTEMPT] target 192.168.95.200 - login "msfadmin" - pass "aimabiet" - 2 of 15 [child 1] (0/0)
[ATTEMPT] target 192.168.95.200 - login "msfadmin" - pass "khongcopass" - 3 of 15 [child 2] (0/0)
[ATTEMPT] target 192.168.95.200 - login "msfadmin" - pass "khongco" - 4 of 15 [child 3] (0/0)
[ATTEMPT] target 192.168.95.200 - login "msfadmin" - pass "123456@#$$$^$#@!!" - 5 of 15 [child 4] (0/0)
[ATTEMPT] target 192.168.95.200 - login "msfadmin" - pass "bruteforce" - 6 of 15 [child 5] (0/0)
[ATTEMPT] target 192.168.95.200 - login "msfadmin" - pass "test" - 7 of 15 [child 6] (0/0)
[ATTEMPT] target 192.168.95.200 - login "msfadmin" - pass "msfadmin" - 8 of 15 [child 7] (0/0)
[ATTEMPT] target 192.168.95.200 - login "msfadmin" - pass "123asdfg" - 9 of 15 [child 8] (0/0)
[ATTEMPT] target 192.168.95.200 - login "msfadmin" - pass "abcdef" - 10 of 15 [child 9] (0/0)
[ATTEMPT] target 192.168.95.200 - login "msfadmin" - pass "hom nay troi dep" - 11 of 15 [child 10] (0/0)
[ATTEMPT] target 192.168.95.200 - login "msfadmin" - pass "asdfghjkl" - 12 of 15 [child 11] (0/0)
[ATTEMPT] target 192.168.95.200 - login "msfadmin" - pass "vbnm" - 13 of 15 [child 12] (0/0)
[ATTEMPT] target 192.168.95.200 - login "msfadmin" - pass "ddd" - 14 of 15 [child 13] (0/0)
[ATTEMPT] target 192.168.95.200 - login "msfadmin" - pass "000000" - 15 of 15 [child 14] (0/0)
1 of 1 target completed, 0 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-04-06 11:58:53

(bun@kali)-[~/Downloads]
$
  
```

Lệnh thực hiện dò mật khẩu:

```
hydra -l msfadmin -P passforbruteforce.txt 192.168.95.200 -V http-post-form  
"/mutillidae/index.php?page=login.php:username=^USER^&password=^PASS^&login-  
php-submit-button=Login:F=Not Logged In"
```

**Ý nghĩa lệnh:**

-l msfadmin : username của tài khoản mà chúng ta muốn crack

-P passforbruteforce.txt : file chứa các password mà chúng ta sẽ dùng để brute force

192.168.95.200 : Địa chỉ Ipv4 của server chứa trang Mutillidae

-V : bật chế độ verbose, thể hiện login+pass của mỗi quá trình crack

http-post-form : phương thức POST data tới website được chỉ định

"/mutillidae/index.php?page=login.php" : Đường dẫn URL của trang web mà chúng ta muốn thực hiện crack

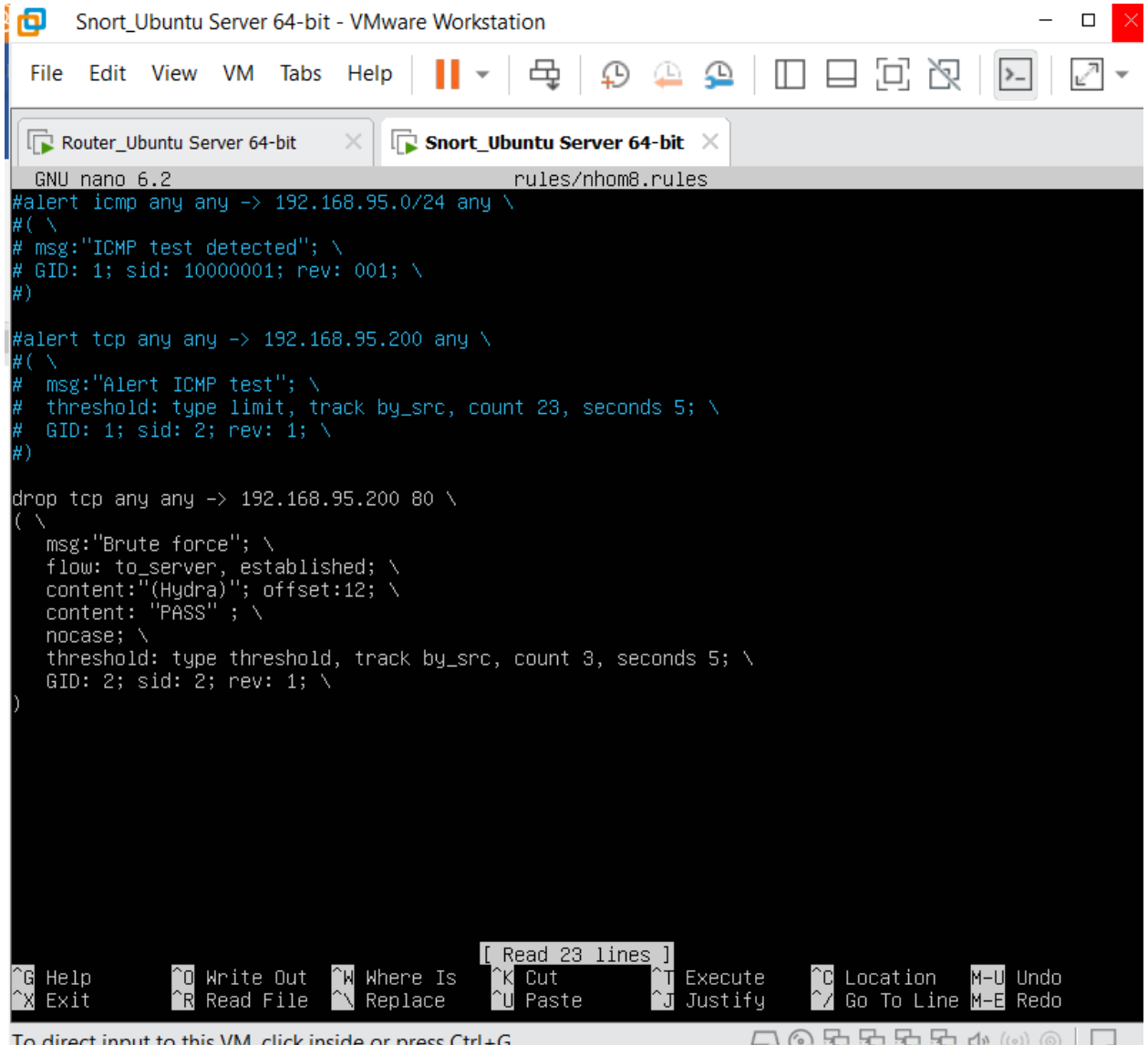
"username=^USER^&password=^PASS^&login-php-submit-button=Login" : thông báo cho hydra biết vị trí đặt password và username

"F=Not Logged In" : Đặt phản hồi cho Bad Response để hydra biết và tiếp tục việc brute force

**b) Sau khi thiết lập rule**

- RULE





```
GNU nano 6.2 rules/nhom8.rules
#alert icmp any any -> 192.168.95.0/24 any \
#( \
#  msg:"ICMP test detected"; \
#  SID: 1; sid: 10000001; rev: 001; \
#)

#alert tcp any any -> 192.168.95.200 any \
#( \
#  msg:"Alert ICMP test"; \
#  threshold: type limit, track by_src, count 23, seconds 5; \
#  SID: 1; sid: 2; rev: 1; \
#)

drop tcp any any -> 192.168.95.200 80 \
( \
  msg:"Brute force"; \
  flow: to_server, established; \
  content:"(Hydra)"; offset:12; \
  content: "PASS" ; \
  nocase; \
  threshold: type threshold, track by_src, count 3, seconds 5; \
  SID: 2; sid: 2; rev: 1; \
)
```

Ý nghĩa rule:

- flow: to\_server, established : luồng gửi tin đi từ client tới server và đã có kết nối TCP
- threshold: type thresh, track by\_src, count 3, second 23 : đặt ra ngưỡng giới hạn chỉ cho phép nhận không quá 3 gói/23 giây từ nguồn được chỉ định, chế độ thông báo là thresh
- content: "PASS" : để tìm các gói tin có chứa chuỗi "PASS" trong payload vì các gói tin dò mật khẩu thường có chứa chuỗi này.
- content: "(Hydra)" : để tìm các gói tin do hydra thực hiện gửi (vì thỉnh thoảng các gói tin do các công cụ brute force gửi sẽ liệt kê tên công cụ trong trường user-agent)
- nocase : không phân biệt chữ hoa, chữ thường trong payload của gói tin
- Tại máy Attacker (Kali linux)

Thực hiện lại tấn công brute force bằng hydra

```

bun@kali: ~/Downloads
File Actions Edit View Help
[ATTEMPT] target 192.168.95.200 - login "msfadmin" - pass "bruteforce" - 6 of 15 [child 5] (0/0)
[ATTEMPT] target 192.168.95.200 - login "msfadmin" - pass "test" - 7 of 15 [child 6] (0/0)
[ATTEMPT] target 192.168.95.200 - login "msfadmin" - pass "msfadmin" - 8 of 15 [child 7] (0/0)
[ATTEMPT] target 192.168.95.200 - login "msfadmin" - pass "123asdfg" - 9 of 15 [child 8] (0/0)
[ATTEMPT] target 192.168.95.200 - login "msfadmin" - pass "abcdef" - 10 of 15 [child 9] (0/0)
[ATTEMPT] target 192.168.95.200 - login "msfadmin" - pass "hom nay troi dep" - 11 of 15 [child 10] (0/0)
[ATTEMPT] target 192.168.95.200 - login "msfadmin" - pass "asdfghjkl" - 12 of 15 [child 11] (0/0)
[ATTEMPT] target 192.168.95.200 - login "msfadmin" - pass "vbnm" - 13 of 15 [child 12] (0/0)
[ATTEMPT] target 192.168.95.200 - login "msfadmin" - pass "ddd" - 14 of 15 [child 13] (0/0)
[ATTEMPT] target 192.168.95.200 - login "msfadmin" - pass "000000" - 15 of 15 [child 14] (0/0)
[STATUS] 15.00 tries/min, 15 tries in 00:01h, 1 to do in 00:01h, 15 active
[STATUS] 7.50 tries/min, 15 tries in 00:02h, 1 to do in 00:01h, 15 active
[STATUS] 5.00 tries/min, 15 tries in 00:03h, 1 to do in 00:01h, 15 active
[STATUS] 3.75 tries/min, 15 tries in 00:04h, 1 to do in 00:01h, 15 active
[STATUS] 3.00 tries/min, 15 tries in 00:05h, 1 to do in 00:01h, 15 active
[80][http-post-form] host: 192.168.95.200 login: msfadmin password: asdfghjkl
[80][http-post-form] host: 192.168.95.200 login: msfadmin password: aimabiet
[80][http-post-form] host: 192.168.95.200 login: msfadmin password: khongco
[80][http-post-form] host: 192.168.95.200 login: msfadmin password: 123asdfg
[80][http-post-form] host: 192.168.95.200 login: msfadmin password: abcdef
[80][http-post-form] host: 192.168.95.200 login: msfadmin password: msfadmin
[80][http-post-form] host: 192.168.95.200 login: msfadmin password: 000000
[80][http-post-form] host: 192.168.95.200 login: msfadmin password: vbnm
[80][http-post-form] host: 192.168.95.200 login: msfadmin password: ddd
[80][http-post-form] host: 192.168.95.200 login: msfadmin password: bruteforce
[80][http-post-form] host: 192.168.95.200 login: msfadmin password: test
[80][http-post-form] host: 192.168.95.200 login: msfadmin password: khongcopass
[80][http-post-form] host: 192.168.95.200 login: msfadmin password: nt123456
[80][http-post-form] host: 192.168.95.200 login: msfadmin password: hom nay troi dep
[80][http-post-form] host: 192.168.95.200 login: msfadmin password: 123456@#$%^&*!
1 of 1 target successfully completed, 15 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-04-07 09:13:11
(bun@kali) - [~/Downloads]
$

```

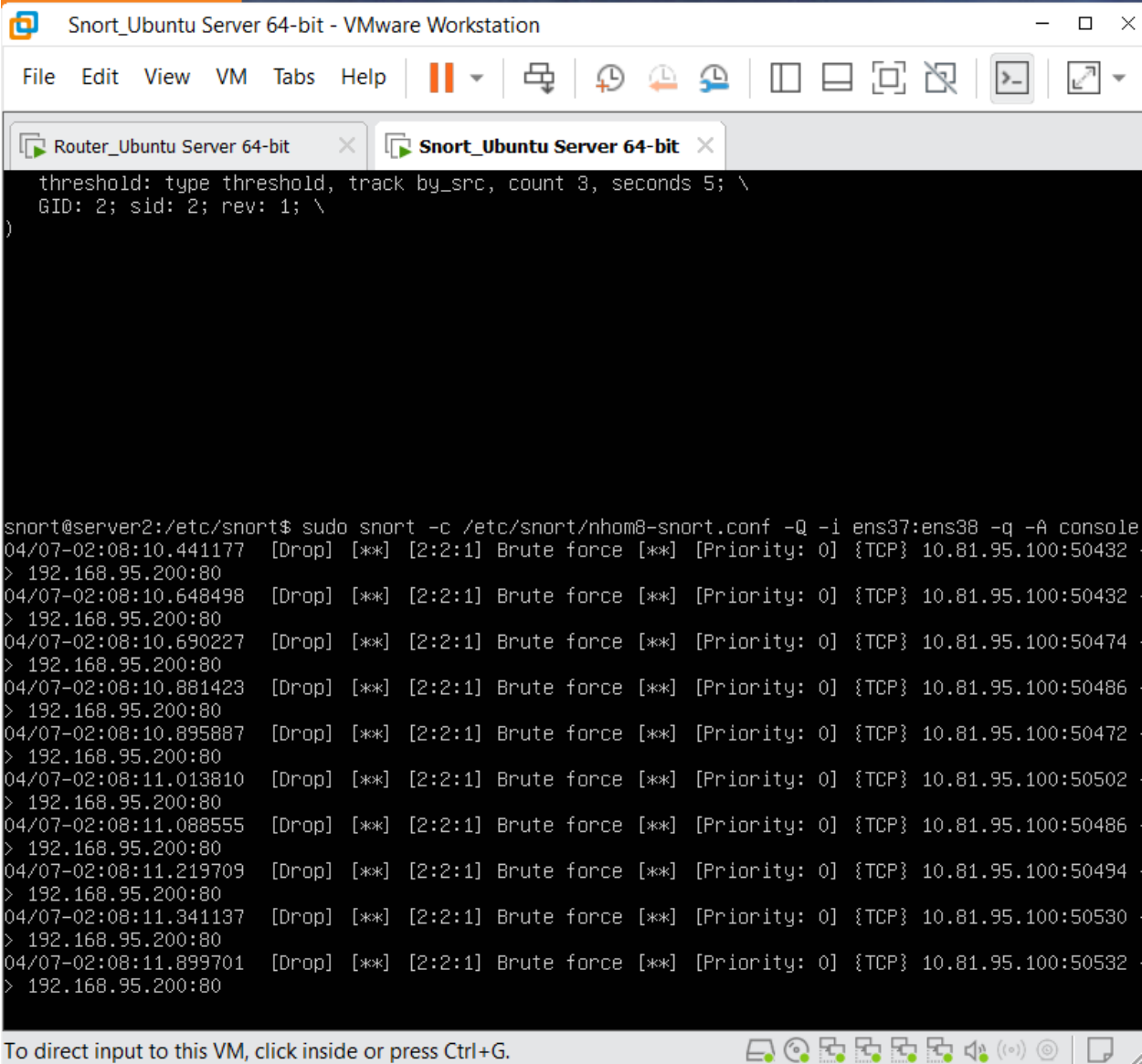
=> Kết quả nhận được bị sai do cùng 1 username mà tìm thấy rất nhiều password hợp lệ. Kết quả này cũng khác với kết quả của lần tấn công trước đó

=>Việc chặn tấn công bruteforce đã thành công

- Tại máy Snort

Sau khi thực hiện chạy snort

=> Nhận được rất nhiều thông điệp đã phát hiện tấn công brute force của Hydra



```
threshold: type threshold, track by_src, count 3, seconds 5; \
GID: 2; sid: 2; rev: 1; \
)

snort@server2:/etc/snort$ sudo snort -c /etc/snort/nhom8-snort.conf -Q -i ens37:ens38 -q -A console
04/07-02:08:10.441177 [Drop] [**] [2:2:1] Brute force [**] [Priority: 0] {TCP} 10.81.95.100:50432 > 192.168.95.200:80
04/07-02:08:10.648498 [Drop] [**] [2:2:1] Brute force [**] [Priority: 0] {TCP} 10.81.95.100:50432 > 192.168.95.200:80
04/07-02:08:10.690227 [Drop] [**] [2:2:1] Brute force [**] [Priority: 0] {TCP} 10.81.95.100:50474 > 192.168.95.200:80
04/07-02:08:10.881423 [Drop] [**] [2:2:1] Brute force [**] [Priority: 0] {TCP} 10.81.95.100:50486 > 192.168.95.200:80
04/07-02:08:10.895887 [Drop] [**] [2:2:1] Brute force [**] [Priority: 0] {TCP} 10.81.95.100:50472 > 192.168.95.200:80
04/07-02:08:11.013810 [Drop] [**] [2:2:1] Brute force [**] [Priority: 0] {TCP} 10.81.95.100:50502 > 192.168.95.200:80
04/07-02:08:11.088555 [Drop] [**] [2:2:1] Brute force [**] [Priority: 0] {TCP} 10.81.95.100:50486 > 192.168.95.200:80
04/07-02:08:11.219709 [Drop] [**] [2:2:1] Brute force [**] [Priority: 0] {TCP} 10.81.95.100:50494 > 192.168.95.200:80
04/07-02:08:11.341137 [Drop] [**] [2:2:1] Brute force [**] [Priority: 0] {TCP} 10.81.95.100:50530 > 192.168.95.200:80
04/07-02:08:11.899701 [Drop] [**] [2:2:1] Brute force [**] [Priority: 0] {TCP} 10.81.95.100:50532 > 192.168.95.200:80
> 192.168.95.200:80
```

=> Snort thành công phát hiện và ngăn chặn cuộc tấn công của hydra

```

Snort_Ubuntu Server 64-bit - VMware Workstation
File Edit View VM Tabs Help

Router_Ubuntu Server 64-bit x Snort_Ubuntu Server 64-bit x
04/07-01:47:47.656072 [Drop] [**] [2:2:1] Brute force [**] [Priority: 0] {TCP} 10.81.95.100:46338
> 192.168.95.200:80
04/07-01:47:47.656072 [Drop] [**] [2:2:1] Brute force [**] [Priority: 0] {TCP} 10.81.95.100:46372
> 192.168.95.200:80
04/07-01:47:47.656152 [Drop] [**] [2:2:1] Brute force [**] [Priority: 0] {TCP} 10.81.95.100:46354
> 192.168.95.200:80
04/07-01:47:52.619263 [Drop] [**] [2:2:1] Brute force [**] [Priority: 0] {TCP} 10.81.95.100:46338
> 192.168.95.200:80
04/07-01:47:52.619263 [Drop] [**] [2:2:1] Brute force [**] [Priority: 0] {TCP} 10.81.95.100:46354
> 192.168.95.200:80
04/07-01:47:52.619263 [Drop] [**] [2:2:1] Brute force [**] [Priority: 0] {TCP} 10.81.95.100:46372
> 192.168.95.200:80
04/07-01:47:52.619263 [Drop] [**] [2:2:1] Brute force [**] [Priority: 0] {TCP} 10.81.95.100:46386
> 192.168.95.200:80
04/07-01:47:52.619263 [Drop] [**] [2:2:1] Brute force [**] [Priority: 0] {TCP} 10.81.95.100:46450
> 192.168.95.200:80
04/07-01:47:52.619263 [Drop] [**] [2:2:1] Brute force [**] [Priority: 0] {TCP} 10.81.95.100:46432
> 192.168.95.200:80
04/07-01:47:52.619263 [Drop] [**] [2:2:1] Brute force [**] [Priority: 0] {TCP} 10.81.95.100:46308
> 192.168.95.200:80
04/07-01:47:52.619263 [Drop] [**] [2:2:1] Brute force [**] [Priority: 0] {TCP} 10.81.95.100:46324
> 192.168.95.200:80
04/07-01:47:52.619971 [Drop] [**] [2:2:1] Brute force [**] [Priority: 0] {TCP} 10.81.95.100:46356
> 192.168.95.200:80
04/07-01:47:52.619971 [Drop] [**] [2:2:1] Brute force [**] [Priority: 0] {TCP} 10.81.95.100:46366
> 192.168.95.200:80
04/07-01:47:52.619971 [Drop] [**] [2:2:1] Brute force [**] [Priority: 0] {TCP} 10.81.95.100:46402
> 192.168.95.200:80
04/07-01:47:52.619971 [Drop] [**] [2:2:1] Brute force [**] [Priority: 0] {TCP} 10.81.95.100:46414
> 192.168.95.200:80
04/07-01:47:52.619971 [Drop] [**] [2:2:1] Brute force [**] [Priority: 0] {TCP} 10.81.95.100:46426
> 192.168.95.200:80
04/07-01:47:52.619971 [Drop] [**] [2:2:1] Brute force [**] [Priority: 0] {TCP} 10.81.95.100:46446
> 192.168.95.200:80
04/07-01:47:52.619971 [Drop] [**] [2:2:1] Brute force [**] [Priority: 0] {TCP} 10.81.95.100:46460
> 192.168.95.200:80
To direct input to this VM, click inside or press Ctrl+G.

```

**Yêu cầu 1.5** Sinh viên tự xây dựng thêm 2 kịch bản tấn công và viết Snort rule để ngăn chặn tấn công

- Sinh viên tự xây dựng 2 kịch bản tấn công khác không liên quan đến tấn công DoS và tấn công web, sau đó, viết rule Snort để ngăn chặn tấn công.
- Thực hiện viết rule Snort, kiểm tra kết quả trước và sau khi tấn công giống như các yêu cầu phía trên.
- Điểm đánh giá tùy thuộc vào mức độ phức tạp của kịch bản.

### Kịch bản 1 : Khai thác lỗ hổng VSFTPD v2.3.4 Backdoor Command Execution

#### a) Trước khi chặn tấn công bằng snort

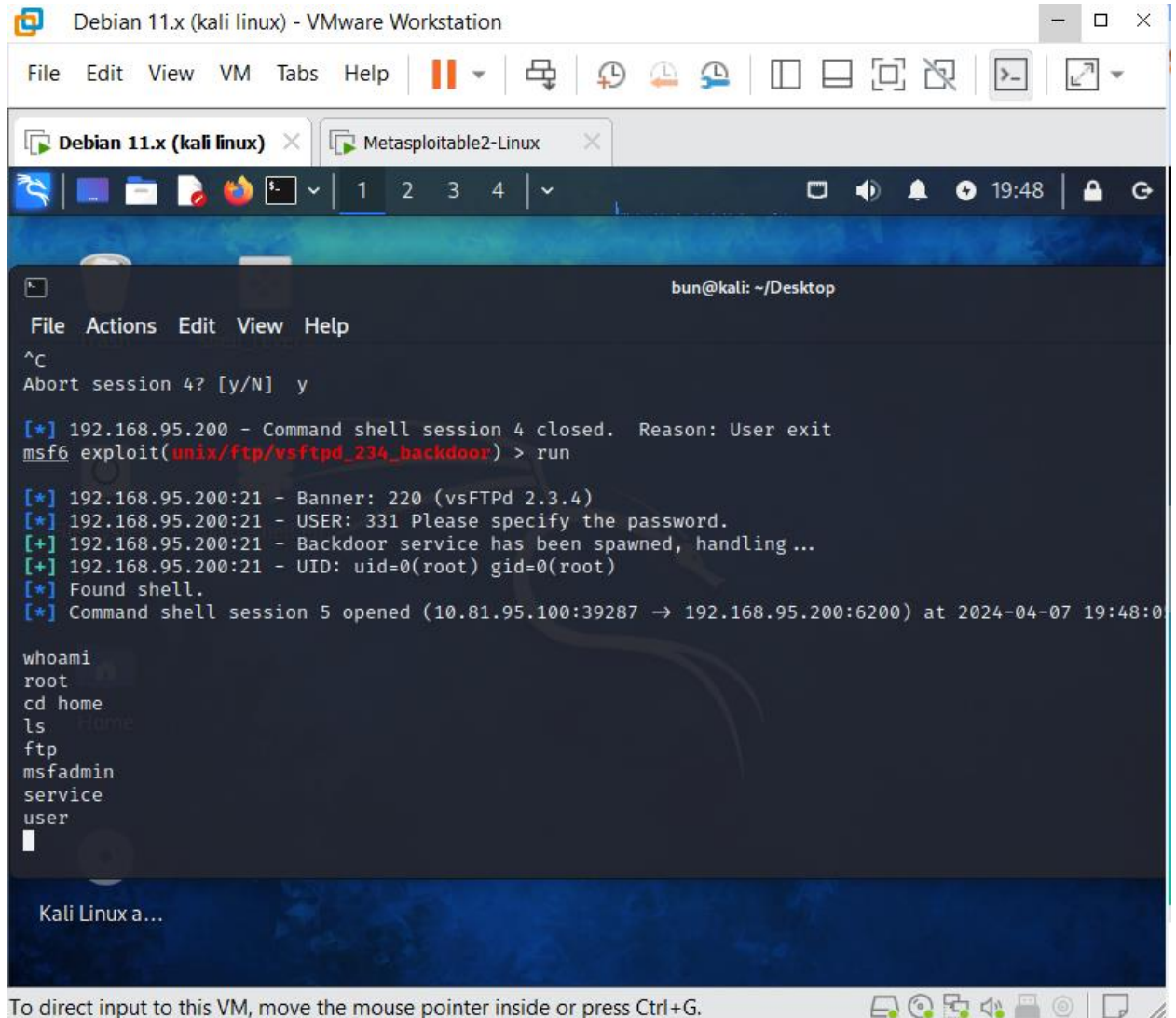


Sử dụng Metasploit Framework với module “exploit/unix/ftp/vsftpd\_234\_backdoor” để tấn công máy Target

Cài RHOSTS = địa chỉ IP của Target

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.95.200
RHOSTS => 192.168.95.200
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > 
```

Thực hiện tấn công bằng lệnh run



```
Debian 11.x (kali linux) - VMware Workstation
File Edit View VM Tabs Help
Debian 11.x (kali linux) x Metasploitable2-Linux x
1 2 3 4
bun@kali: ~/Desktop
File Actions Edit View Help
^C
Abort session 4? [y/N] y
[*] 192.168.95.200 - Command shell session 4 closed. Reason: User exit
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run
[*] 192.168.95.200:21 - Banner: 220 (vsFTPD 2.3.4)
[*] 192.168.95.200:21 - USER: 331 Please specify the password.
[+] 192.168.95.200:21 - Backdoor service has been spawned, handling ...
[+] 192.168.95.200:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 5 opened (10.81.95.100:39287 -> 192.168.95.200:6200) at 2024-04-07 19:48:0
whoami
root
cd home
ls
ftp
msfadmin
service
user
Kali Linux a...
```

=> Chiếm được quyền truy cập shell của máy Target

**b) Thiết lập rule để ngăn chặn tấn công**

- RULE:

```

GNU nano 6.2 rules/nhom8.rules
#alert icmp any any -> 192.168.95.0/24 any \
\
# msg:"ICMP test detected"; \
# GID: 1; sid: 10000001; rev: 001; \
#)

#alert tcp any any -> 192.168.95.200 any \
#( \
# msg:"Alert ICMP test"; \
# threshold: type limit, track by_src, count 23, seconds 5; \
# GID: 1; sid: 2; rev: 1; \
#)

#drop tcp any any -> 192.168.95.200 80 \
#( \
# msg:"Brute force"; \
# flow: to_server, established; \
# content:"(Hydra)"; offset:12; \
# content: "PASS" ; \
# nocase; \
# threshold: type threshold, track by_src, count 3, seconds 5; \
# GID: 2; sid: 2; rev: 1; \
#)

#portvar PORTS [21,6200]

drop tcp any any -> 192.168.95.200 6200 \
( \
flow: to_server, established; \
content:"|69 64 0a|" ; \
msg: "Detect vsftpd 2.3.4 - Backdoor CE"; \
GID: 3; sid: 2; rev: 1; \
)

[ Read 32 lines ]
^G Help      ^O Write Out ^W Where Is  ^K Cut       ^T Execute   ^C Location  M-U Undo
^X Exit      ^R Read File ^N Replace   ^U Paste     ^J Justify   ^_ Go To Line M-E Redo

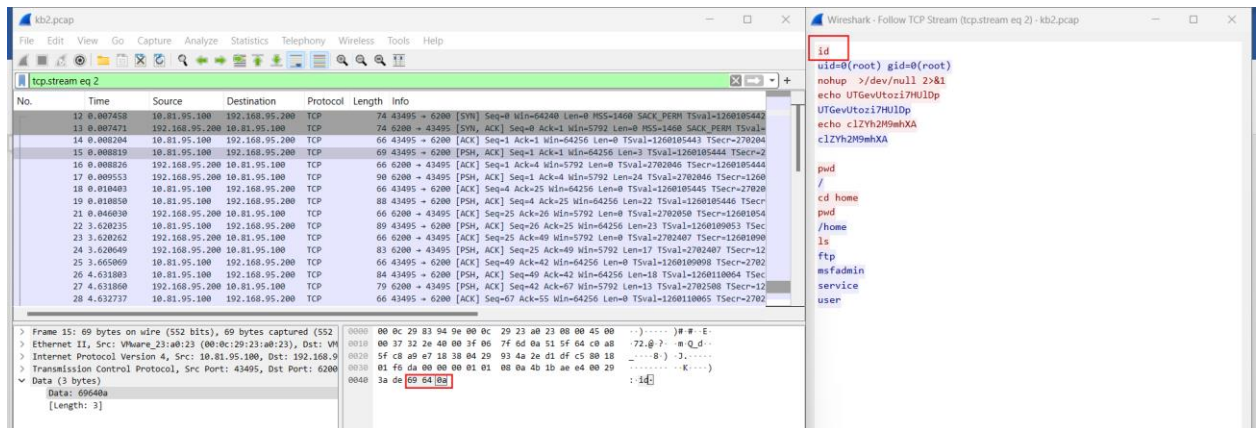
```

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

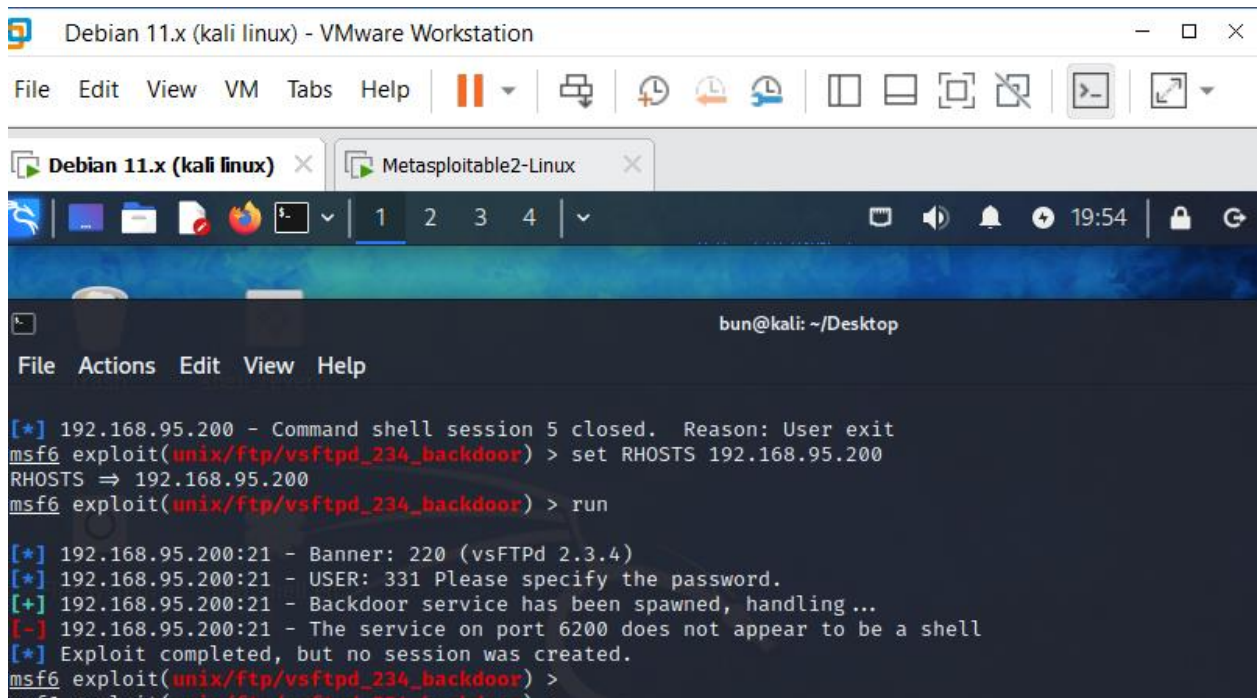
Ý nghĩa:

- flow: to\_server, established : luồng gửi tin đi từ client tới server và đã có kết nối TC
- content: "|69 64 0a|" : để tìm các gói tin có chứa dãy số hex này trong payload.

Vì sau khi phân tích file .pcap của quá trình tấn công trước, chúng ta phát hiện gói tin chứa dãy số này là dấu hiệu quan trọng nhận biết cuộc tấn công này



- Tại máy attacker



=> Cuộc tấn công đã thất bại, chúng ta nhận được thông báo “no session was created”

- Tại máy Snort

Nhiều thông điệp phát hiện cuộc tấn công đã thực hiện được thông báo



```

#)
#portvar PORTS [21,6200]

drop tcp any any -> 192.168.95.200 6200 \
( \
  flow: to_server, established; \
  content:"|69 64 0a|"; \
  msg: "Detect vsftpd 2.3.4 - Backdoor CE"; \
  SID: 3; sid: 2; rev: 1; \
)

snort@server2:/etc/snort$ sudo snort -c /etc/snort/nhom8-snort.conf -Q -i ens37:ens38 -q -A console
04/07-12:53:11.577945 [Drop] [**] [3:2:1] Detect vsftpd 2.3.4 - Backdoor CE [**] [Priority: 0] {TCP
} 10.81.95.100:40889 -> 192.168.95.200:6200
04/07-12:53:11.784373 [Drop] [**] [3:2:1] Detect vsftpd 2.3.4 - Backdoor CE [**] [Priority: 0] {TCP
} 10.81.95.100:40889 -> 192.168.95.200:6200
04/07-12:53:11.996571 [Drop] [**] [3:2:1] Detect vsftpd 2.3.4 - Backdoor CE [**] [Priority: 0] {TCP
} 10.81.95.100:40889 -> 192.168.95.200:6200
04/07-12:53:12.421043 [Drop] [**] [3:2:1] Detect vsftpd 2.3.4 - Backdoor CE [**] [Priority: 0] {TCP
} 10.81.95.100:40889 -> 192.168.95.200:6200
04/07-12:53:13.285212 [Drop] [**] [3:2:1] Detect vsftpd 2.3.4 - Backdoor CE [**] [Priority: 0] {TCP
} 10.81.95.100:40889 -> 192.168.95.200:6200
04/07-12:53:14.980403 [Drop] [**] [3:2:1] Detect vsftpd 2.3.4 - Backdoor CE [**] [Priority: 0] {TCP
} 10.81.95.100:40889 -> 192.168.95.200:6200
04/07-12:53:16.584487 [Drop] [**] [3:2:1] Detect vsftpd 2.3.4 - Backdoor CE [**] [Priority: 0] {TCP
} 10.81.95.100:40889 -> 192.168.95.200:6200
04/07-12:53:16.793041 [Drop] [**] [3:2:1] Detect vsftpd 2.3.4 - Backdoor CE [**] [Priority: 0] {TCP
} 10.81.95.100:40889 -> 192.168.95.200:6200
04/07-12:53:17.220242 [Drop] [**] [3:2:1] Detect vsftpd 2.3.4 - Backdoor CE [**] [Priority: 0] {TCP
} 10.81.95.100:40889 -> 192.168.95.200:6200
04/07-12:53:18.053302 [Drop] [**] [3:2:1] Detect vsftpd 2.3.4 - Backdoor CE [**] [Priority: 0] {TCP
} 10.81.95.100:40889 -> 192.168.95.200:6200
04/07-12:53:19.754380 [Drop] [**] [3:2:1] Detect vsftpd 2.3.4 - Backdoor CE [**] [Priority: 0] {TCP
} 10.81.95.100:40889 -> 192.168.95.200:6200

```

=> Snort thành công ngăn chặn cuộc tấn công

## Kịch bản 2 : Phát hiện Brute force mật khẩu bằng SSH

Sử dụng Metasploit Framework với module “scanner/ssh/ssh\_login” để tấn công máy Target

Cài RHOSTS = địa chỉ IP của Target

```
msf6 auxiliary(scanner/ssh/ssh_login) > set RHOSTS 192.168.95.200
RHOSTS => 192.168.95.200
```

Sử dụng tập file rockyou.txt để làm tập file bruteforce tài khoản và mật khẩu

```
msf6 auxiliary(scanner/ssh/ssh_login) > set USERPASS_FILE /usr/share/wordlists/rockyou.txt
USERPASS_FILE => /usr/share/wordlists/rockyou.txt
```

Bắt đầu bruteforce bằng lệnh “exploit”

```
msf6 auxiliary(scanner/ssh/ssh_login) > exploit
[*] 192.168.95.200:22 - Starting bruteforce
```

## Viết Snort rule để phát hiện bruteforce

```
alert tcp any any -> 192.168.95.200 22 (msg:"Detect SSH Bruteforce"; \
    flow: to_server; \
    threshold: type threshold, track by_src, count 5, seconds 3; \
    sid: 1000006; rev:1;)
```

## Giải thích lệnh:

- alert tcp any any -> any 22: Rule này xác định loại giao thức (TCP) và cổng (22 - SSH) mà nó áp dụng.
- msg:"SSH Brute Force Attempt Detected": Đây là thông điệp cảnh báo sẽ được hiển thị khi một cố gắng brute force SSH được phát hiện.
- flow:to\_server: Rule sẽ kiểm tra dữ liệu chỉ theo hướng từ máy khách đến máy chủ.
- threshold:type threshold, track by\_src, count 5, seconds 3: Đây là một ngưỡng (threshold) được áp dụng cho rule. Rule sẽ kích hoạt khi có ít nhất 5 sự kiện phù hợp trong vòng 3 giây từ cùng một nguồn IP.

Như vậy, rule này sẽ phát hiện các cố gắng brute force SSH bằng cách theo dõi số lần cố gắng đăng nhập không thành công từ cùng một nguồn IP trong một khoảng thời gian ngắn và kích hoạt cảnh báo khi số lượng cố gắng vượt qua ngưỡng đã được xác định.

Dùng lệnh tcpdump trên máy Target, ta thấy có rất nhiều gói tin SSH được gửi đến.

```
11:29:16.794950 IP 10.81.95.100.42221 > 192.168.95.200.ssh: P 1506:1650(144) ack
975 win 501 <nop,nop,timestamp 376963456 2986551>
11:29:16.812636 IP 192.168.95.200.ssh > 10.81.95.100.42221: P 975:1695(720) ack
1650 win 362 <nop,nop,timestamp 2986553 376963456>
11:29:16.818595 IP 10.81.95.100.42221 > 192.168.95.200.ssh: P 1650:1674(24) ack
1695 win 501 <nop,nop,timestamp 376963480 2986553>
11:29:16.852781 IP 192.168.95.200.ssh > 10.81.95.100.42221: . ack 1674 win 362 <
nop,nop,timestamp 2986558 376963480>
11:29:16.857293 IP 10.81.95.100.42221 > 192.168.95.200.ssh: P 1674:1726(52) ack
1695 win 501 <nop,nop,timestamp 376963518 2986558>
11:29:16.857323 IP 192.168.95.200.ssh > 10.81.95.100.42221: . ack 1726 win 362 <
nop,nop,timestamp 2986558 376963518>
11:29:16.857427 IP 192.168.95.200.ssh > 10.81.95.100.42221: P 1695:1747(52) ack
1726 win 362 <nop,nop,timestamp 2986558 376963518>
11:29:16.863040 IP 10.81.95.100.42221 > 192.168.95.200.ssh: P 1726:1810(84) ack
1747 win 501 <nop,nop,timestamp 376963524 2986558>
11:29:16.864090 IP 192.168.95.200.59594 > 192.168.95.1.domain: 36333+ PTR? 100.9
5.81.10.in-addr.arpa. (43)
11:29:16.867475 IP 192.168.95.1 > 192.168.95.200: ICMP 192.168.95.1 udp port dom
ain unreachable, length 79
11:29:16.867783 IP 192.168.95.200.39825 > 192.168.95.1.domain: 36333+ PTR? 100.9
5.81.10.in-addr.arpa. (43)
11:29:16.902993 IP 192.168.95.200.ssh > 10.81.95.100.42221: . ack 1810 win 362 <
nop,nop,timestamp 2986563 376963524>
```

Bên máy Snort cũng có thông báo có cuộc tấn công

```

04/07-15:30:47.438233  [**] [1:1000006:1] Detect SSH Bruteforce [**] [Priority: 0] {TCP} 10.81.95.10
0:38107 -> 192.168.95.200:22
04/07-15:30:47.480924  [**] [1:1000006:1] Detect SSH Bruteforce [**] [Priority: 0] {TCP} 10.81.95.10
0:38107 -> 192.168.95.200:22
04/07-15:30:52.555723  [**] [1:1000006:1] Detect SSH Bruteforce [**] [Priority: 0] {TCP} 10.81.95.10
0:36029 -> 192.168.95.200:22
04/07-15:30:52.594709  [**] [1:1000006:1] Detect SSH Bruteforce [**] [Priority: 0] {TCP} 10.81.95.10
0:36029 -> 192.168.95.200:22
04/07-15:30:52.666883  [**] [1:1000006:1] Detect SSH Bruteforce [**] [Priority: 0] {TCP} 10.81.95.10
0:45505 -> 192.168.95.200:22
04/07-15:30:52.679411  [**] [1:1000006:1] Detect SSH Bruteforce [**] [Priority: 0] {TCP} 10.81.95.10
0:45505 -> 192.168.95.200:22
04/07-15:30:52.754238  [**] [1:1000006:1] Detect SSH Bruteforce [**] [Priority: 0] {TCP} 10.81.95.10
0:45505 -> 192.168.95.200:22
04/07-15:30:52.788045  [**] [1:1000006:1] Detect SSH Bruteforce [**] [Priority: 0] {TCP} 10.81.95.10
0:44701 -> 192.168.95.200:22
04/07-15:30:52.833020  [**] [1:1000006:1] Detect SSH Bruteforce [**] [Priority: 0] {TCP} 10.81.95.10
0:44701 -> 192.168.95.200:22
04/07-15:30:57.897955  [**] [1:1000006:1] Detect SSH Bruteforce [**] [Priority: 0] {TCP} 10.81.95.10
0:43679 -> 192.168.95.200:22
04/07-15:30:57.939660  [**] [1:1000006:1] Detect SSH Bruteforce [**] [Priority: 0] {TCP} 10.81.95.10
0:43679 -> 192.168.95.200:22
04/07-15:30:58.011541  [**] [1:1000006:1] Detect SSH Bruteforce [**] [Priority: 0] {TCP} 10.81.95.10
0:33663 -> 192.168.95.200:22
04/07-15:30:58.031904  [**] [1:1000006:1] Detect SSH Bruteforce [**] [Priority: 0] {TCP} 10.81.95.10
0:33663 -> 192.168.95.200:22
04/07-15:30:58.114123  [**] [1:1000006:1] Detect SSH Bruteforce [**] [Priority: 0] {TCP} 10.81.95.10
0:33663 -> 192.168.95.200:22
04/07-15:30:58.151464  [**] [1:1000006:1] Detect SSH Bruteforce [**] [Priority: 0] {TCP} 10.81.95.10
0:42575 -> 192.168.95.200:22
04/07-15:30:58.238754  [**] [1:1000006:1] Detect SSH Bruteforce [**] [Priority: 0] {TCP} 10.81.95.10
0:42575 -> 192.168.95.200:22
^Z[37] Killed snort -c /etc/snort/nhom8-snort.conf -Q -i ens37:ens38 -A console -q
q

[38]+ Stopped snort -c /etc/snort/nhom8-snort.conf -Q -i ens37:ens38 -A console -q
root@ubuntu:/home/ubuntu# _

```