



BÁO CÁO LAB 3

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

GVTH: ĐỖ HOÀNG HIỀN

Sinh viên thực hiện	Sinh viên 1 MSSV: 21522573 Họ tên: Phạm Thanh Tâm Sinh viên 2 MSSV: 21520514 Họ tên: Nguyễn Văn Anh Tú
Lớp	NT204.O21.ATCL
Tổng thời gian thực hiện Lab trung bình	
Phân chia công việc (nếu là nhóm)	[Sinh viên 1]: 1,5 [Sinh viên 2]: 2,3,4
Link Video thực hiện (nếu có yêu cầu)	
Ý kiến (nếu có) + Khó khăn gặp phải + Đề xuất, góp ý...	Không
Điểm tự đánh giá (bắt buộc)	10 /10



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

Bài làm

Yêu cầu 1.1: Giới hạn gói tin đến dịch vụ DNS

- *Viết Snort rule thực hiện giới hạn gói tin đến dịch vụ DNS đến máy Victim. Ngưỡng (threshold) là không quá 90 gói/10s*
- *Sử dụng công cụ hping3 trên máy Attacker để thực hiện tấn công*
- *Kiểm tra kết quả trước và sau khi cài rule*

Đầu tiên ta bật snort bên máy snort sau đó dùng tcpdump ở máy Victim và hping3 –flood -2 -p 53 192.168.14.200 để gửi gói tin đến máy Victim

```
(root@kali)-[~]  
# hping3 --flood -2 -p 53 192.168.14.200  
HPING 192.168.14.200 (eth0 192.168.14.200): udp mode set, 28 headers + 0 data bytes  
hping in flood mode, no replies will be shown
```

+ Trước khi áp dụng rule snort:

```
07:41:13.195380 IP 10.81.14.100.27974 > 192.168.14.200.domain: [!domain]  
07:41:13.195546 IP 10.81.14.100.27975 > 192.168.14.200.domain: [!domain]  
07:41:13.208211 IP 10.81.14.100.27976 > 192.168.14.200.domain: [!domain]  
07:41:13.208213 IP 10.81.14.100.27977 > 192.168.14.200.domain: [!domain]  
07:41:13.208215 IP 10.81.14.100.27978 > 192.168.14.200.domain: [!domain]  
07:41:13.208216 IP 10.81.14.100.27979 > 192.168.14.200.domain: [!domain]  
07:41:13.208217 IP 10.81.14.100.27980 > 192.168.14.200.domain: [!domain]  
07:41:13.208218 IP 10.81.14.100.27981 > 192.168.14.200.domain: [!domain]  
07:41:13.208218 IP 10.81.14.100.27982 > 192.168.14.200.domain: [!domain]  
07:41:13.208225 IP 10.81.14.100.27983 > 192.168.14.200.domain: [!domain]  
07:41:13.208226 IP 10.81.14.100.27984 > 192.168.14.200.domain: [!domain]  
07:41:22.499030 IP 10.81.14.100.43291 > 192.168.14.200.domain: [!domain]  
07:41:22.499176 IP 10.81.14.100.43292 > 192.168.14.200.domain: [!domain]  
07:41:22.499313 IP 10.81.14.100.43586 > 192.168.14.200.domain: [!domain]  
07:41:22.499433 IP 10.81.14.100.43294 > 192.168.14.200.domain: [!domain]  
07:41:22.499537 IP 10.81.14.100.43295 > 192.168.14.200.domain: [!domain]  
07:41:22.499685 IP 10.81.14.100.43296 > 192.168.14.200.domain: [!domain]  
07:41:22.499813 IP 10.81.14.100.43651 > 192.168.14.200.domain: [!domain]  
07:41:22.500142 IP6 fe80::20c:29ff:fe60:1991 > ff02::16: HBH ICMP6, multicast li  
stener report v2, 1 group record(s), length 28  
  
1926 packets captured  
20825 packets received by filter  
18536 packets dropped by kernel  
msfadmin@metasploitable:~$
```

Ta có thể thấy máy Victim nhận được 1 ít gói tin và drop rất nhiều gói tin.



Ta có thể viết rule snort như sau để thực hiện giới hạn gói đến dịch vụ DNS đến máy Victim: drop udp any any → 192.168.14.200 53 (msg:"Limit DNS package"; threshold: type threshold, track by_dst, count 90, seconds 10; sid:1; rev: 101)

Với ý nghĩa là nếu có nhiều hơn 90 gói tin gửi đến port 53 (dịch vụ DNS) của máy trong 10s thì sẽ bị drop

Ta tiến hành set rule và thực hiện lại bước tcpdump trước khi dùng máy attacker sử dụng hping3 đến máy victim

```
Eth Disc:          0 ( 0.000%)
IP4 Disc:          0 ( 0.000%)
IP6 Disc:          0 ( 0.000%)
TCP Disc:          0 ( 0.000%)
UDP Disc:          0 ( 0.000%)
ICMP Disc:         0 ( 0.000%)
All Discard:       0 ( 0.000%)
  Other:           0 ( 0.000%)
Bad Chk Sum:       0 ( 0.000%)
Bad TTL:           0 ( 0.000%)
S5 G 1:            0 ( 0.000%)
S5 G 2:            0 ( 0.000%)
Total:            36938
=====
Action Stats:
  Alerts:          410 ( 1.110%)
  Logged:          410 ( 1.110%)
  Passed:           0 ( 0.000%)
Limits:
  Match:           0
  Queue:           0
  Log:             0
  Event:           36507
  Alert:           0
Verdicts:
  Allow:           21 ( 0.057%)
  Block:           0 ( 0.000%)
  Replace:         0 ( 0.000%)
  Whitelist:       0 ( 0.000%)
  Blacklist:       36917 ( 99.940%)
  Ignore:          0 ( 0.000%)
  Retry:           0 ( 0.000%)
=====
+-----[filtered events]-----+
| gen-id=1      sig-id=1      type=Threshold tracking=dst count=90  seconds=10  filtered=36507
Snort exiting
kenzy@snort:/etc/snort/rules$
```

Kết quả ta thu được filtering trên máy snort

Yêu cầu 1.2: Chỉ cho phép truy cập đến một số dịch vụ

- *Viết Snort rule chỉ cho phép các máy truy cập đến các port của các dịch vụ sau trên máy Victim: Telnet, FTP, SSH, Web, mail, NetBIOS, SMB, MySQL, postgresql.*
- *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.*

Đầu tiên ta sử dụng nmap để quét xem máy victim đang mở các port nào:



```
(root@kali)-[~]
# nmap 192.168.14.200
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-03 07:55 EDT
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 192.168.14.200
Host is up (0.019s 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

Nmap done: 1 IP address (1 host up) scanned in 0.80 seconds
```

Đề bài yêu cầu ta chỉ cho phép các port của các dịch vụ Telnet, FPT, SSH, Web, mail, NetBIOS, SMB, MySQL, postgresql

Để được như vậy thì ta sẽ viết 1 rule snort drop hết tất cả các port còn lại: drop tcp any any -> any ![21,22,23,25,53,80,139,445,3306,5432] (msg:"Allow only some port"; sid:101; rev:1)

Ta tiến hành nmap lại để check và kiểm tra tcpdump bên máy Victim

```
08:39:11.333233 IP 192.168.14.200.mysql > 10.81.14.100.57814: S 2069711198:20697
11198(0) ack 2616059873 win 5840 <mss 1460>
08:39:11.523587 IP 192.168.14.200.microsoft-ds > 10.81.14.100.57816: S 207537686
8:2075376868(0) ack 2616190947 win 5840 <mss 1460>
08:39:11.732996 IP 192.168.14.200.mysql > 10.81.14.100.57816: S 2077108642:20771
08642(0) ack 2616190947 win 5840 <mss 1460>
08:39:11.733157 IP 192.168.14.200.netbios-ssn > 10.81.14.100.57814: S 2073947214
:2073947214(0) ack 2616059873 win 5840 <mss 1460>
08:39:11.923856 IP 192.168.14.200.telnet > 10.81.14.100.57816: S 2078497536:2078
497536(0) ack 2616190947 win 5840 <mss 1460>
08:39:11.933497 IP 192.168.14.200.ftp > 10.81.14.100.57816: S 2080771933:2080771
933(0) ack 2616190947 win 5840 <mss 1460>
08:39:12.124236 IP 192.168.14.200.smtp > 10.81.14.100.57814: S 2074506451:207450
6451(0) ack 2616059873 win 5840 <mss 1460>
08:39:12.133429 IP 192.168.14.200.ftp > 10.81.14.100.57814: S 2078248436:2078248
436(0) ack 2616059873 win 5840 <mss 1460>
08:39:12.723470 IP 192.168.14.200.smtp > 10.81.14.100.57816: S 2074520996:207452
0996(0) ack 2616190947 win 5840 <mss 1460>
08:39:12.733544 IP 192.168.14.200.netbios-ssn > 10.81.14.100.57816: S 2081012105
:2081012105(0) ack 2616190947 win 5840 <mss 1460>
08:39:28.614065 IP 192.168.14.200.postgresql > 10.81.14.100.57816: S 2352238565:
2352238565(0) ack 2616190947 win 5840 <mss 1460>
08:39:28.813447 IP 192.168.14.200.postgresql > 10.81.14.100.57814: S 2355005497:
2355005497(0) ack 2616059873 win 5840 <mss 1460>
```

Yêu cầu 1.3: Chỉ cho phép các truy vấn DNS đến các tên miền thuộc quản lý của UIT



- *Viết Snort rule chỉ cho phép gửi các yêu cầu DNS đến máy Victim khi truy vấn đến các tên miền thuộc quản lý của UIT*
- *Sử dụng công cụ nslookup trên máy Attacker thực hiện tấn công.*
- *Kiểm tra kết quả trước và sau khi cài đặt rule*

Ta dùng nslookup để truy vấn thử đến 1 vài tên miền trước khi áp dụng rule

```
(root@kali)-[~]
# nslookup uit.edu.vn 192.168.14.200
Server:          192.168.14.200
Address:         192.168.14.200#53

** server can't find uit.edu.vn: REFUSED

(root@kali)-[~]
# nslookup facebook.com 192.168.14.200
Server:          192.168.14.200
Address:         192.168.14.200#53

** server can't find facebook.com: REFUSED

(root@kali)-[~]
#
```

Ta thực hiện viết rule cho snort:

Pass udp any any -> 192.168.14.200 53 (msg:"Only DNS UIT";content:"|03|uit|03|edu|02|vn"; sid:101)

Drop udp any any -> 192.168.14.200 53 (msg:"Drop any other DNS"; sid:102)

Sau khi áp dụng rule ta thử dùng nslookup lại thì thấy facebook đã bị time out



```
(root@kali)-[~]
# nslookup facebook.com 192.168.14.200
;; communications error to 192.168.14.200#53: timed out
;; communications error to 192.168.14.200#53: timed out
;; communications error to 192.168.14.200#53: timed out
;; no servers could be reached

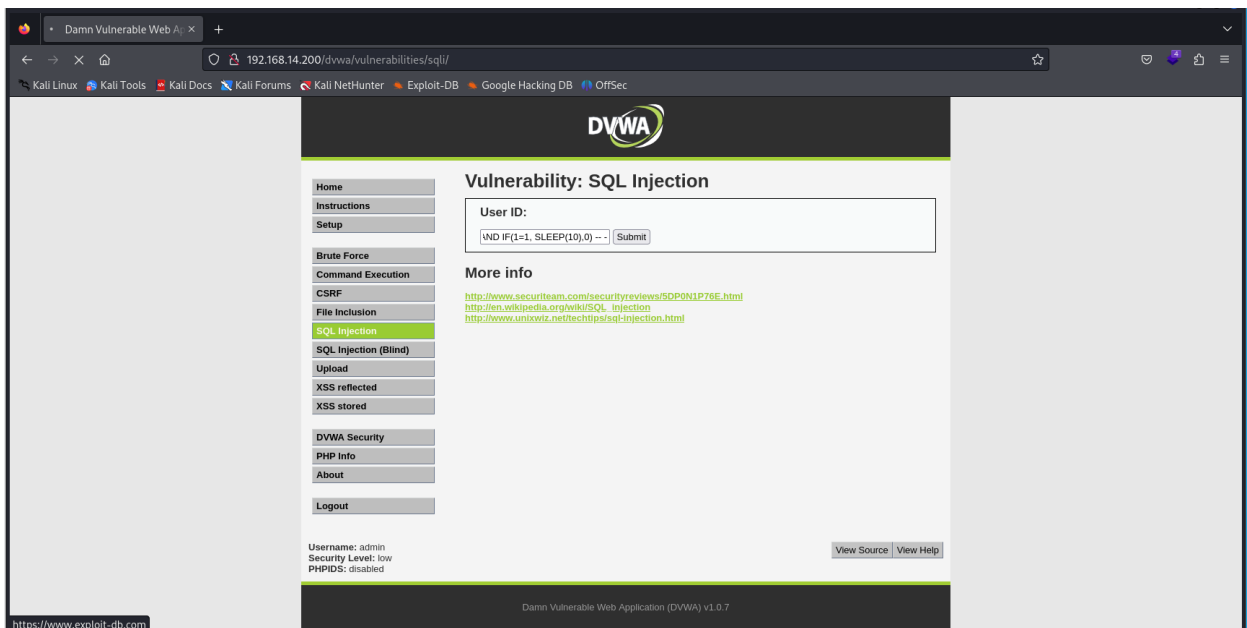
(root@kali)-[~]
# nslookup uit.edu.vn 192.168.14.200
Server:          192.168.14.200
Address:         192.168.14.200#53

** server can't find uit.edu.vn: REFUSED
```

Yêu cầu 1.4: Ngăn chặn tấn công Time-based SQL injection

- *Viết Snort rule ngăn chặn tấn công Time-based SQL injection trên 1 website của máy Victim*
- *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.*

Trước khi ta viết snort rule, ta thử dùng time-based injection bằng truy vấn: `1' AND IF(1=1, SLEEP(10),0) --` - với if để kiểm tra điều kiện đúng thì sẽ sleep(10) là sẽ delay câu truy vấn này trong 10s





Ta thấy sau khi submit câu truy vấn thì page load khoảng chừng 10s

Ta viết rule snort để ngăn chặn time-based injection:

Drop tcp any any -> 192.168.14.200 80 (msg:"Prevent Time-based SQL Injection";
flow:to_server, established; content:"SLEEP"; sid:1)

Sau đó ta thực hiện lại truy vấn và check log alert để kiểm tra

```
[**] [1:1:0] Prevent Time-based SQL Injection [**]  
[Priority: 0]  
05/03-14:12:14.833280 10.81.14.100:59022 -> 192.168.14.200:80  
TCP TTL:63 TOS:0x0 ID:5182 IpLen:20 DgmLen:607 DF  
***AP*** Seq: 0xD9E58CFD Ack: 0x36E0C162 Win: 0xFB TcpLen: 32  
TCP Options (3) => NOP NOP TS: 1896112719 909705  
  
[**] [1:1:0] Prevent Time-based SQL Injection [**]  
[Priority: 0]  
05/03-14:12:21.744752 10.81.14.100:59022 -> 192.168.14.200:80  
TCP TTL:63 TOS:0x0 ID:5183 IpLen:20 DgmLen:607 DF  
***AP*** Seq: 0xD9E58CFD Ack: 0x36E0C162 Win: 0xFB TcpLen: 32  
TCP Options (3) => NOP NOP TS: 1896119631 909705  
  
[**] [1:1:0] Prevent Time-based SQL Injection [**]  
[Priority: 0]  
05/03-14:12:35.570136 10.81.14.100:59022 -> 192.168.14.200:80  
TCP TTL:63 TOS:0x0 ID:5184 IpLen:20 DgmLen:607 DF  
***AP*** Seq: 0xD9E58CFD Ack: 0x36E0C162 Win: 0xFB TcpLen: 32  
TCP Options (3) => NOP NOP TS: 1896133455 909705  
  
[**] [1:1:0] Prevent Time-based SQL Injection [**]  
[Priority: 0]  
05/03-14:13:04.242538 10.81.14.100:59022 -> 192.168.14.200:80  
TCP TTL:63 TOS:0x0 ID:5185 IpLen:20 DgmLen:607 DF  
***AP*** Seq: 0xD9E58CFD Ack: 0x36E0C162 Win: 0xFB TcpLen: 32  
TCP Options (3) => NOP NOP TS: 1896162127 909705  
  
[**] [1:1:0] Prevent Time-based SQL Injection [**]  
[Priority: 0]  
05/03-14:13:59.539122 10.81.14.100:59022 -> 192.168.14.200:80  
TCP TTL:63 TOS:0x0 ID:5186 IpLen:20 DgmLen:607 DF  
***AP*** Seq: 0xD9E58CFD Ack: 0x36E0C162 Win: 0xFB TcpLen: 32  
TCP Options (3) => NOP NOP TS: 1896217423 909705  
  
kenzy@snort:/var/log/snort$ _
```

Ta check log alert thì thấy được kết quả

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: Ngăn chặn tấn công IP Spoofing từ vùng mạng của Victim

```
File Actions Edit View Help
(root@kali)-[~]
# ping 192.168.14.200
PING 192.168.14.200 (192.168.14.200) 56(84) bytes of data.
64 bytes from 192.168.14.200: icmp_seq=1 ttl=63 time=14.0 ms
64 bytes from 192.168.14.200: icmp_seq=2 ttl=63 time=4.01 ms
64 bytes from 192.168.14.200: icmp_seq=3 ttl=63 time=3.16 ms
64 bytes from 192.168.14.200: icmp_seq=4 ttl=63 time=6.31 ms
64 bytes from 192.168.14.200: icmp_seq=5 ttl=63 time=4.38 ms
64 bytes from 192.168.14.200: icmp_seq=6 ttl=63 time=3.08 ms
^C
— 192.168.14.200 ping statistics —
6 packets transmitted, 6 received, 0% packet loss, time 5011ms
rtt min/avg/max/mdev = 3.076/5.822/14.005/3.812 ms
(root@kali)-[~]
#
```

Thông thường ta có thể ping tới địa chỉ IP của Victim

Tiếp đến ta sẽ thực hiện chặn ip ngoài vùng mạng của victim với rule snort như sau:

drop ip !192.168.14.0/24 any -> any any (msg:"IP spoofing detected"; sid:101; rev:1)

ip !192.168.14.0/24 any -> any any: áp dụng rule cho tất cả các gói tin IP không có địa chỉ nguồn thuộc mạng con đến bất kì địa chỉ IP đích nào

```
(root@kali)-[~]
# ping 192.168.14.200
PING 192.168.14.200 (192.168.14.200) 56(84) bytes of data.
^C
— 192.168.14.200 ping statistics —
11 packets transmitted, 0 received, 100% packet loss, time 10227ms
```

Sau khi set rule thì máy attacker không còn ping được tới máy Victim được nữa



Kịch bản 2: Ngăn chặn tấn công bruteforce từ dịch vụ FTP

Ta thử dùng hydra để thực hiện bruteforce mật khẩu của máy victim với user mà msfadmin với option FTP để chỉ định dịch vụ FTP

```
(root@kali)-[~]
# hydra -t 4 -V -f -l msfadmin -P password.txt 192.168.14.200 ftp
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for i
llegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-05-03 11:21:42
[DATA] max 4 tasks per 1 server, overall 4 tasks, 8 login tries (l:1/p:8), ~2 tries per task
[DATA] attacking ftp://192.168.14.200:21/
[ATTEMPT] target 192.168.14.200 - login "msfadmin" - pass "test111" - 1 of 8 [child 0] (0/0)
[ATTEMPT] target 192.168.14.200 - login "msfadmin" - pass "1234567" - 2 of 8 [child 1] (0/0)
[ATTEMPT] target 192.168.14.200 - login "msfadmin" - pass "2421521" - 3 of 8 [child 2] (0/0)
[ATTEMPT] target 192.168.14.200 - login "msfadmin" - pass "hihitest" - 4 of 8 [child 3] (0/0)
[ATTEMPT] target 192.168.14.200 - login "msfadmin" - pass "aimabiet" - 5 of 8 [child 1] (0/0)
[ATTEMPT] target 192.168.14.200 - login "msfadmin" - pass "password" - 6 of 8 [child 0] (0/0)
[ATTEMPT] target 192.168.14.200 - login "msfadmin" - pass "hehheboiz" - 7 of 8 [child 2] (0/0)
[ATTEMPT] target 192.168.14.200 - login "msfadmin" - pass "msfadmin" - 8 of 8 [child 3] (0/0)
[21][ftp] host: 192.168.14.200 login: msfadmin password: msfadmin
[STATUS] attack finished for 192.168.14.200 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-05-03 11:21:46
```

Sau đó ta sẽ ngăn chặn việc này bằng cách viết 1 rule snort:

```
drop tcp any any -> 192.168.14.200 21 (msg:"Prevent FTP Bruteforce";
flow:to_server,established; content:"PASS"; nocase; threshold:type both, track
by_src, count 5, seconds 100; sid:101; rev:1)
```

Với ý nghĩa rằng rule trên kiểm tra gói tin đến từ attacker đến victim với content là pass(không phân biệt hoa hay thường, không vượt quá 5 gói tin từ 1 địa chỉ trong vòng 100s) thì snort sẽ drop

```
(root@kali)-[~]
# hydra -t 4 -V -f -l msfadmin -P password.txt 192.168.14.200 ftp
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for i
llegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-05-03 11:25:25
[DATA] max 4 tasks per 1 server, overall 4 tasks, 8 login tries (l:1/p:8), ~2 tries per task
[DATA] attacking ftp://192.168.14.200:21/
[ATTEMPT] target 192.168.14.200 - login "msfadmin" - pass "test111" - 1 of 8 [child 0] (0/0)
[ATTEMPT] target 192.168.14.200 - login "msfadmin" - pass "1234567" - 2 of 8 [child 1] (0/0)
[ATTEMPT] target 192.168.14.200 - login "msfadmin" - pass "2421521" - 3 of 8 [child 2] (0/0)
[ATTEMPT] target 192.168.14.200 - login "msfadmin" - pass "hihitest" - 4 of 8 [child 3] (0/0)
[ATTEMPT] target 192.168.14.200 - login "msfadmin" - pass "aimabiet" - 5 of 8 [child 1] (0/0)
[ATTEMPT] target 192.168.14.200 - login "msfadmin" - pass "password" - 6 of 8 [child 2] (0/0)
[ATTEMPT] target 192.168.14.200 - login "msfadmin" - pass "hehheboiz" - 7 of 8 [child 0] (0/0)
[ATTEMPT] target 192.168.14.200 - login "msfadmin" - pass "msfadmin" - 8 of 8 [child 3] (0/0)
[STATUS] 8.00 tries/min, 8 tries in 00:01h, 1 to do in 00:01h, 4 active
[RE-ATTEMPT] target 192.168.14.200 - login "msfadmin" - pass "aimabiet" - 8 of 8 [child 1] (0/0)
[RE-ATTEMPT] target 192.168.14.200 - login "msfadmin" - pass "password" - 8 of 8 [child 2] (0/0)
[RE-ATTEMPT] target 192.168.14.200 - login "msfadmin" - pass "msfadmin" - 8 of 8 [child 3] (0/0)
[RE-ATTEMPT] target 192.168.14.200 - login "msfadmin" - pass "hehheboiz" - 8 of 8 [child 0] (0/0)
1 of 1 target completed, 0 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-05-03 11:27:02
```

Ta set rule và thực hiện lại bruteforce thì thấy rằng vẫn có password trong file .txt nhưng lại thông báo là invalid