BÁO CÁO LAB 3

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

GVTH: ĐỖ HOÀNG HIỂN

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**

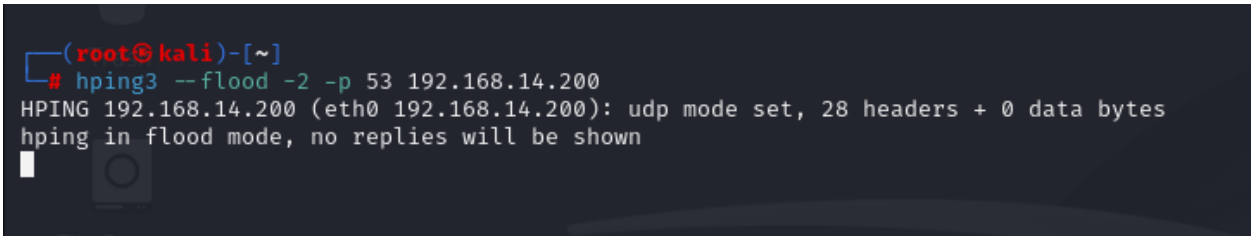
[Nội dung báo cáo chi tiết – Trình bày tùy sinh viên, Xuất file .PDF khi nộp]

Bài làm

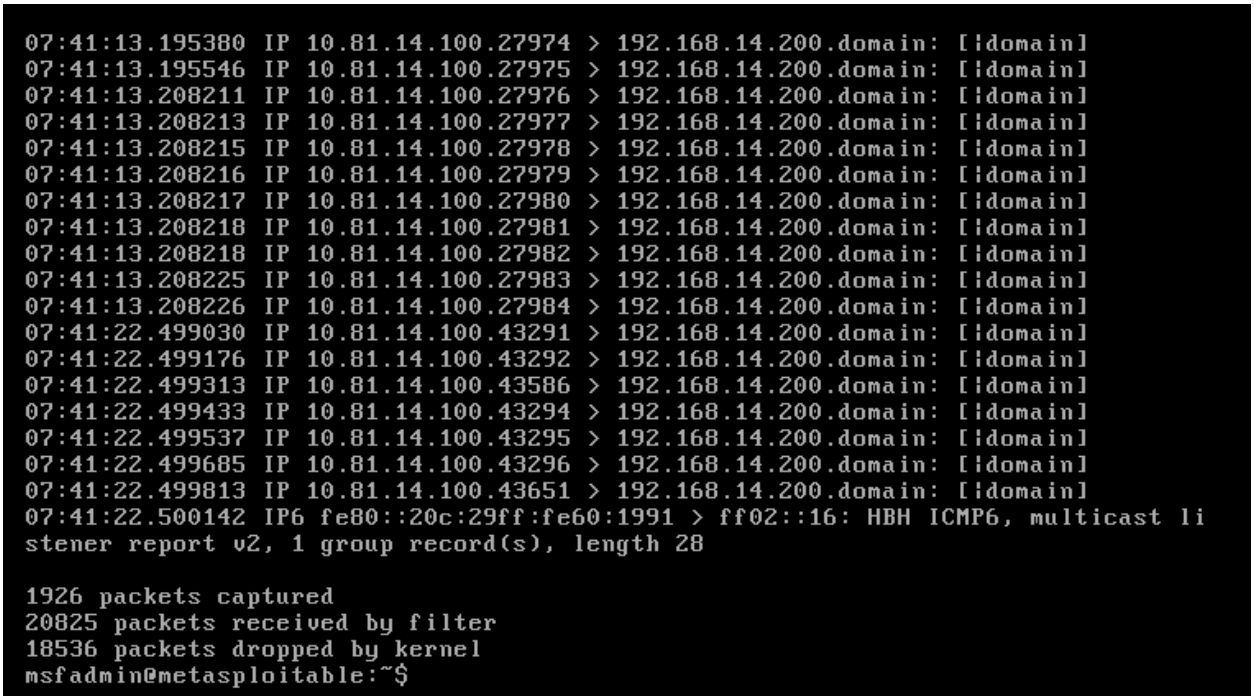
Yêu cầu 1.1: Giới hạn gói tin đến dịch vụ DNS

- ***Viết Snort rule thực hiện giới hạn gói đến dịch vụ DNS đến máy Victim. Ngưỡng (threshold) la 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



+ Trước khi áp dụng rule snort:



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

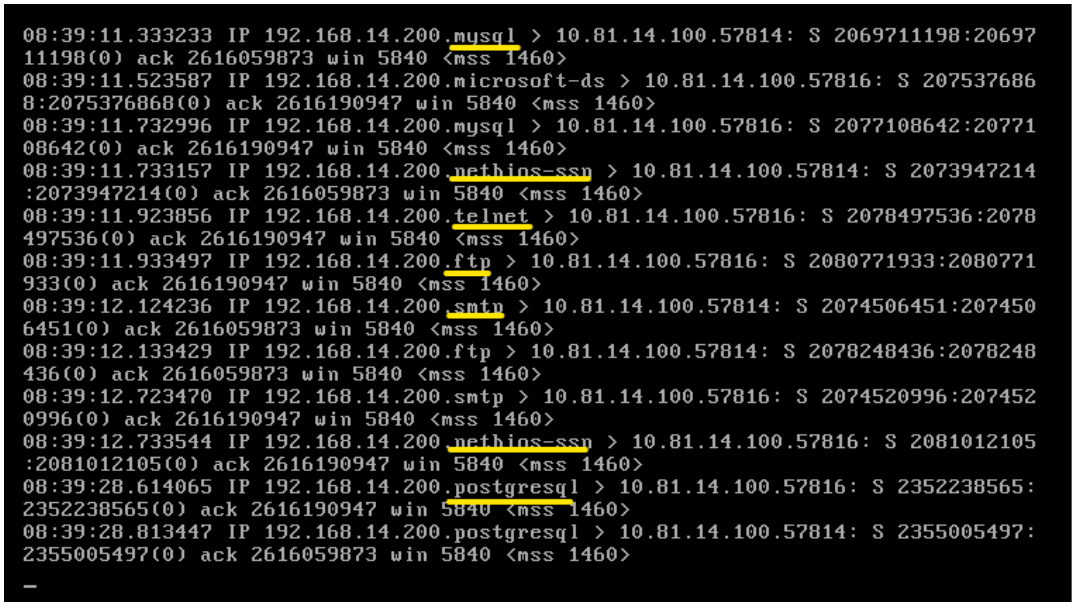
- ***Viết Snort rule chỉ cho phép các máy truy cập đến các port của các dịch vụ sau trên máy Victim: Telnet, FPT, SSH, Web, mail, NetBIOS, SMB, MySQL, postgresql.***
- ***Sử dụng công cụ telnet hoặc nmap trên máy Attacker thực hiện tấn công.***
- ***Kiểm trà kết quả trước và sàu khi cài đặt rule.***

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

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)

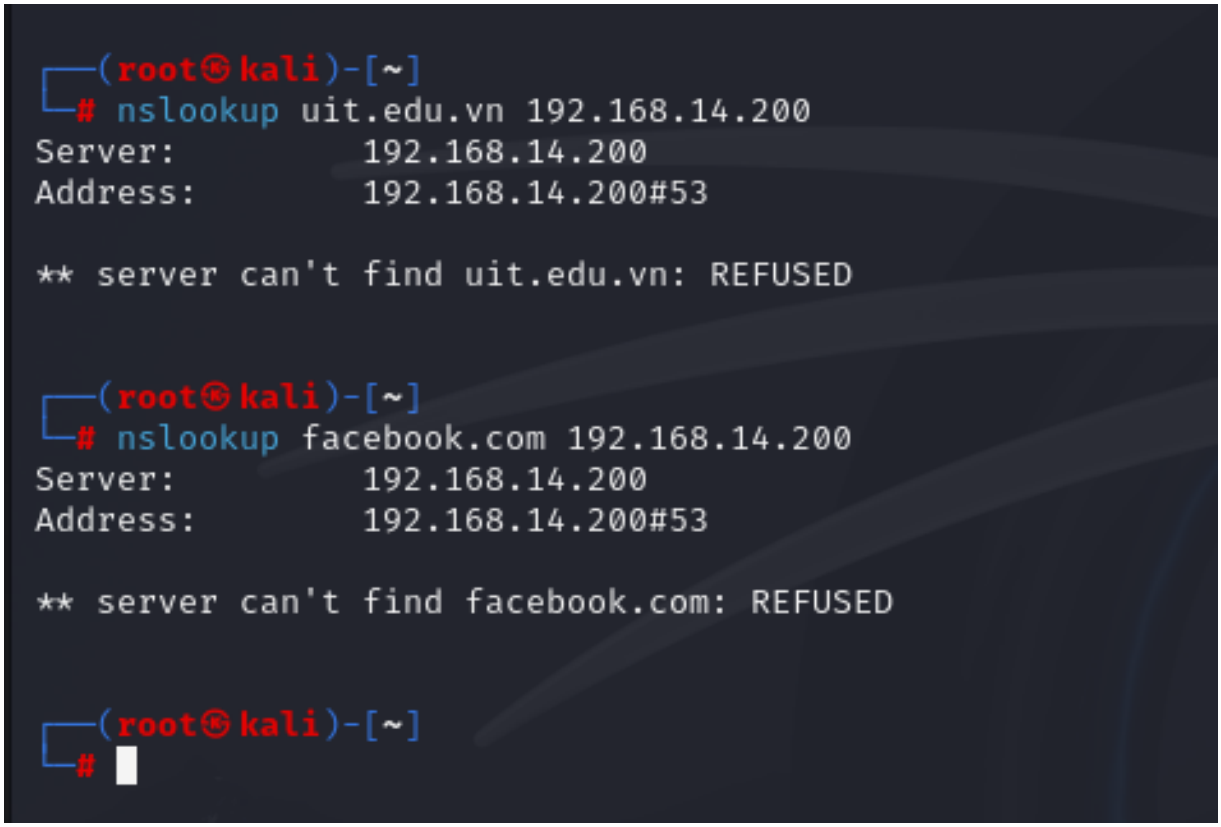
Ta tiến hành nmap lại để check và kiểm tra tcpdump bên máy Victim



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



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)

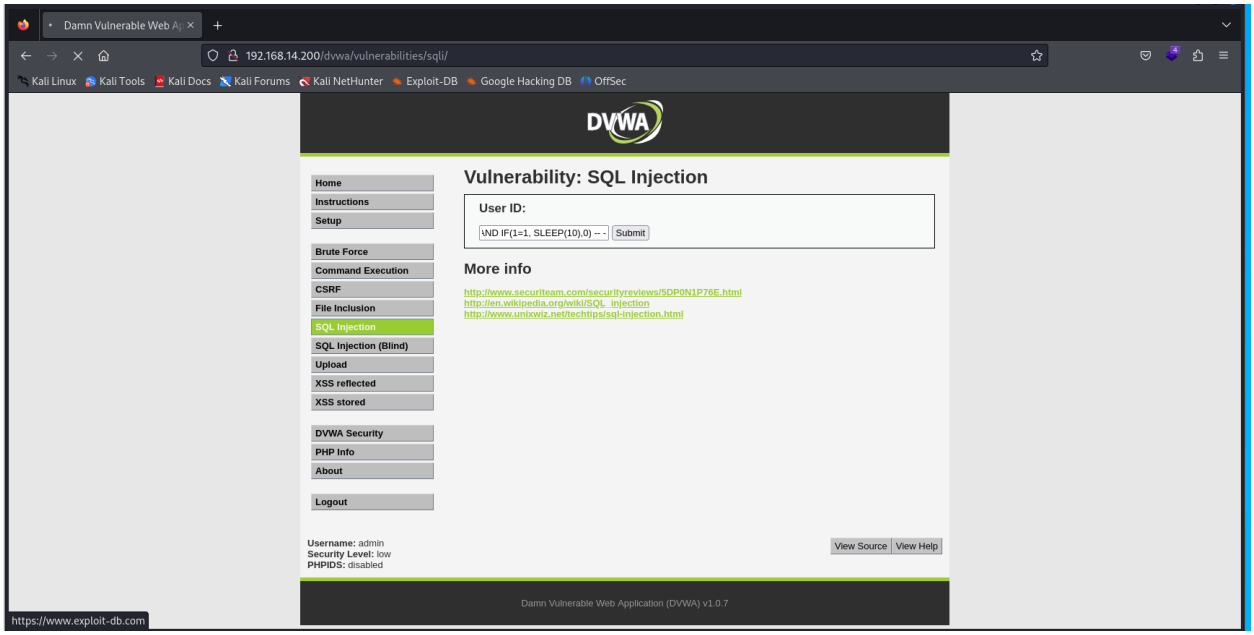
Sau khi áp dụng rule ta thử dùng nslookup lại thì thấy facebook đã bị time out

```
┌──(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

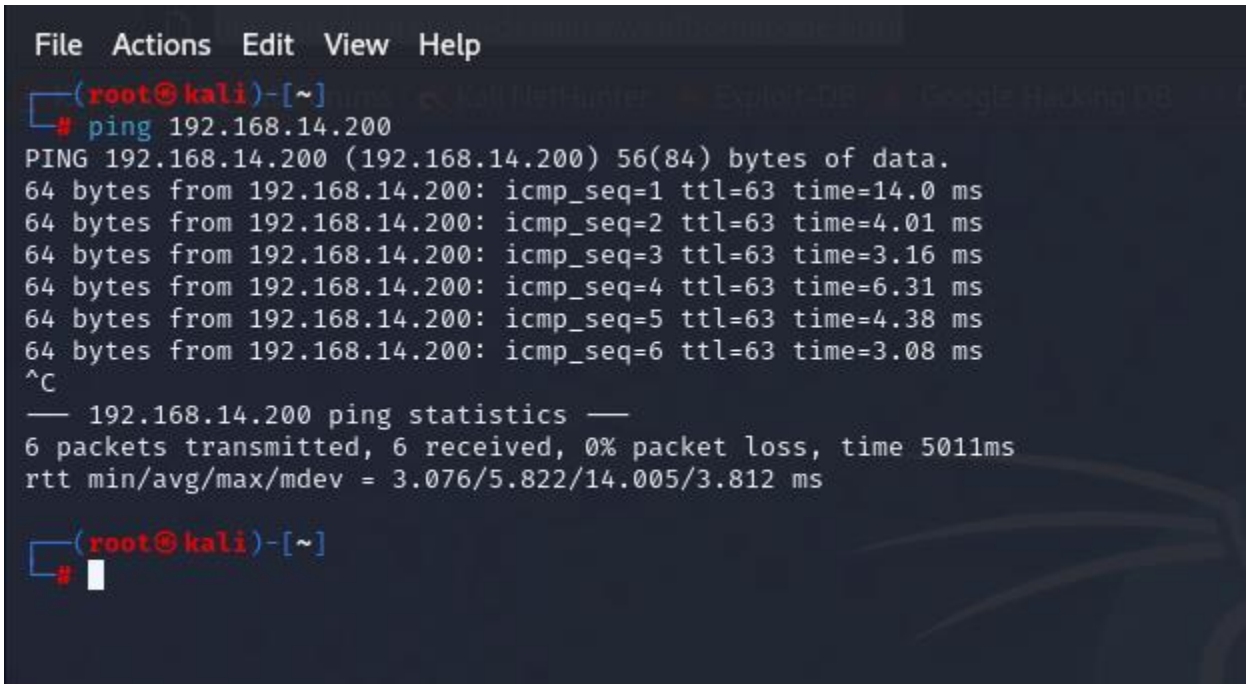
```
[**] [1:1:0] Prevent Time-based SQL Injection [**]
[Priority: 0]
05/03-14:12:14.833280 10.81.14.100:59022 -> 192.168.14.200:80
TCP TTL:63 TOS:0x0 ID:5182 IpLen:20 DgmLen:607 DF
***AP*** Seq: 0xD9E58CFD  Ack: 0x36E0C162  Win: 0xFB  TcpLen: 32
TCP Options (3) => NOP NOP TS: 1896112719 909705

[**] [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

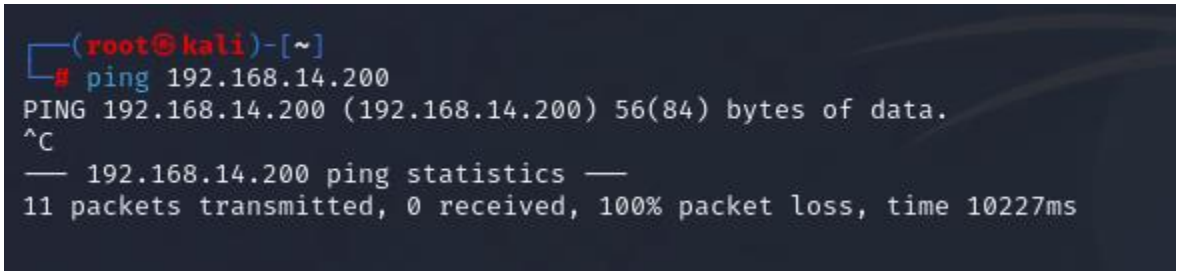


Thông thường ta có thể ping tới địa chỉ IP của Victim

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



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 passsword.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 Bruteforcce"; 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 passsword.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