Lab cấu hình tường lửa trên linux

Chuẩn bị

- Một máy linux có 2 card mạng đóng vai trò firewall.
- Một máy kali.
- Một máy linux cài sẵn các dịch Ngnix, vsftpd, open-ssh.

Mục tiêu

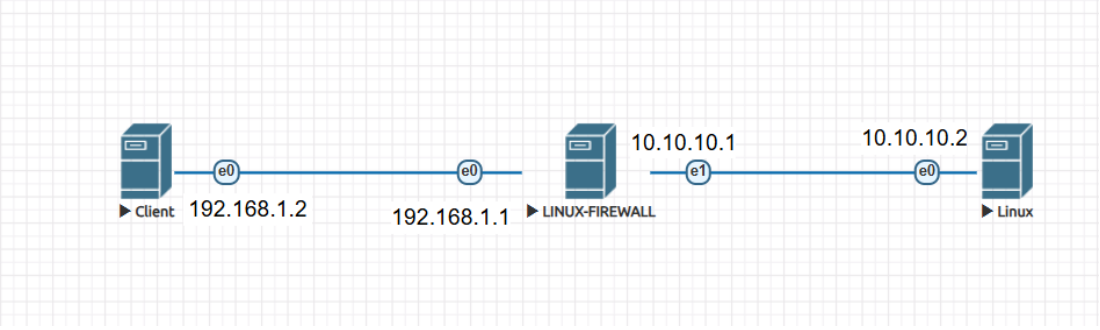
- Tạo các rules với iptables.
- Tạo rules(Nat, forwarding services ,anti-dos, anti-brute-force) với iptables.

Cảnh báo: Tất cả các bài lab tấn công chỉ được thực hiện trong **môi trường ảo**, **cách ly** và **hợp pháp**. **Tuyệt đối không** áp dụng trên **hệ thống thật** hoặc **mạng không được phép**, mọi vi phạm sẽ bị xử lý theo quy định và pháp luật hiện hành.

Khuyến nghị: Tùy theo ngữ cảnh để xác định các rule cần thiết trên firewall, bạn nên đọc qua tất cả bài tập để nắm rõ nội dung rồi mới thực hành, vì bài lab này thực hiện sắp xếp lại rules khá nhiều.

Các bài tập thực hành

Mô hình bài lab:



Giải thích :

Trong mô hình trên, client là người dùng cuối truy cập dịch vụ từ server linux, Linux-firewall sẽ đóng vai trò là tường lửa, chuyển tiếp các luồng lưu lượng hợp pháp.

Bài tập 1: cấu hình NAT (Network Address Translation)

Cấu hình NAT cho phép 2 giao tiếp giữa 2 vùng mạng thông qua Linux-firewall

Trên máy linux-firewall chạy các lệnh sau:

#Bật IP forwarding:

```
echo 1 > /proc/sys/net/ipv4/ip_forward
```

#Thêm NAT (MASQUERADE):

```
iptables -t nat -A POSTROUTING -s 192.168.1.0/24 -o ens4 -j MASQUERADE
```

#Forward tất cả traffic giữa 2 mạng:

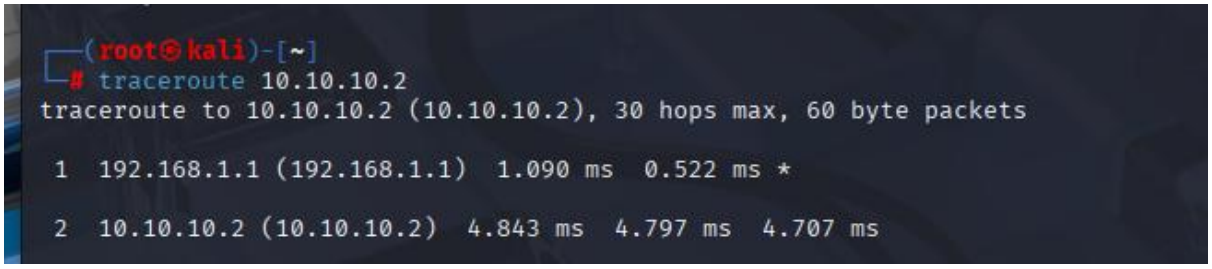
+Từ Client đến Server:

```
iptables -A FORWARD -s 192.168.1.0/24 -d 10.10.10.0/24 -j ACCEPT
```

+Cho phép gói phản hồi từ Server về Client:

```
iptables -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT
```

Để kiểm tra lại, trên máy client, thực hiện traceroute tới địa chỉ 10.10.10.2



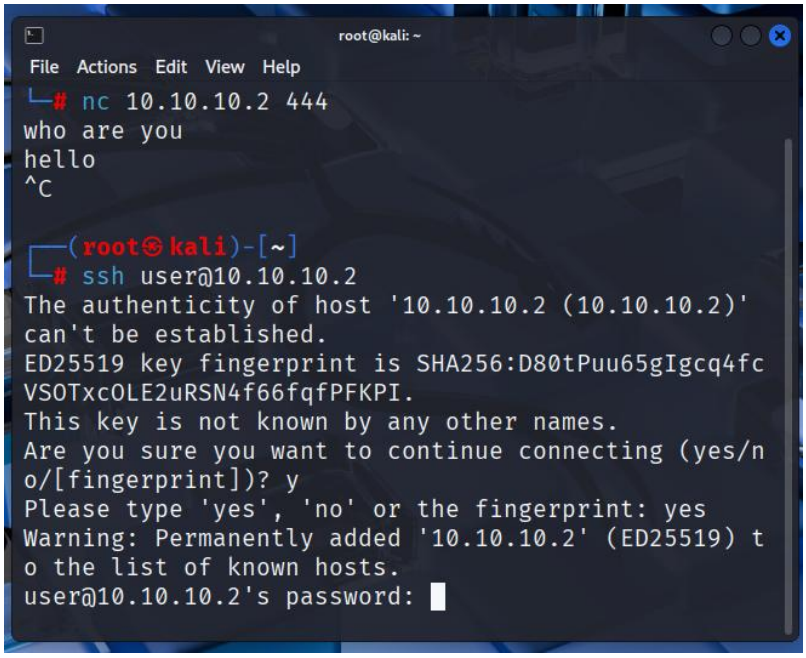
Như vậy là toàn bộ dịch vụ trên server client có thể truy cập được.

Bài tập 2: tạo rule chỉ cho phép truy cập dịch vụ hợp lệ

Trong tình huống máy chủ có nhiều cổng và dịch vụ mở, chúng ta cần kiểm soát chặt chẽ các dịch vụ mà client được phép truy cập. Giả sử chúng ta chỉ muốn client truy cập dịch vụ **Web (HTTP)** và **FTP**.

Mô phỏng tình huống:

Truy cập SSH từ Client: Trên máy client, chạy lệnh: ssh user@10.10.10.2



Như vậy, dịch vụ SSH có thể truy cập được từ client.

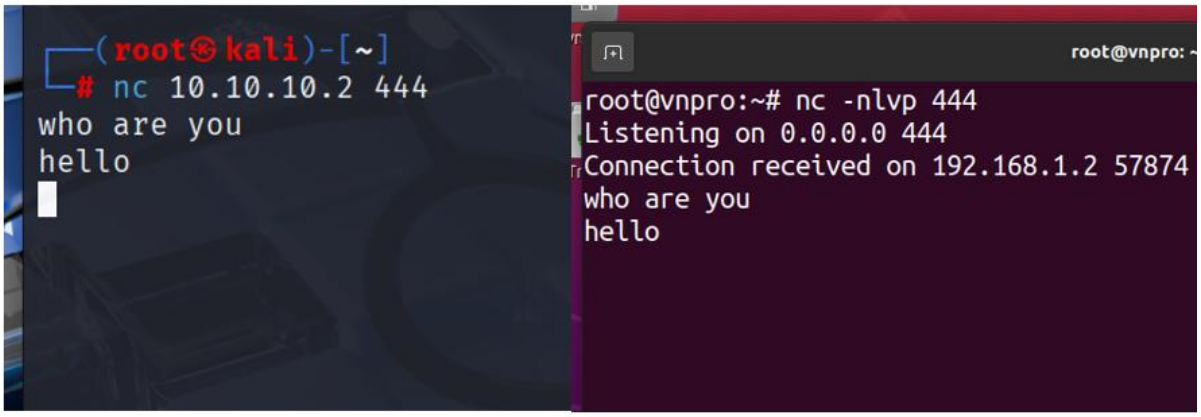
Hoặc chúng ta có thể thử với một port tùy ý

Trên máy server, chạy lệnh:

nc -nvlp 444

Trên máy client, chạy lệnh:

nc 10.10.10.2 444



Sau đó, bạn có thể kết nối với máy server qua cổng 444, là một cổng không chính quy (không được phép truy cập từ bên ngoài).

Cấu hình Iptables để kiểm soát dịch vụ:

#Thiết lập chính sách mặc định của chuỗi FORWARD là DROP:

```
iptables -P FORWARD DROP
```

➔Điều này đảm bảo rằng tất cả các gói tin không khớp với rule cụ thể nào sẽ bị chặn.

#Cho phép dịch vụ HTTP (cổng 80):

```
iptables -A FORWARD -p tcp -s 192.168.1.0/24 -d 10.10.10.2 --dport 80 -j ACCEPT
```

Cho phép dịch vụ FTP (cổng 21):

```
iptables -A FORWARD -p tcp -s 192.168.1.0/24 -d 10.10.10.2 --dport 21 -j ACCEPT
```

Kiểm tra lại bảng rules:

```
iptables -L FORWARD --line-number
```

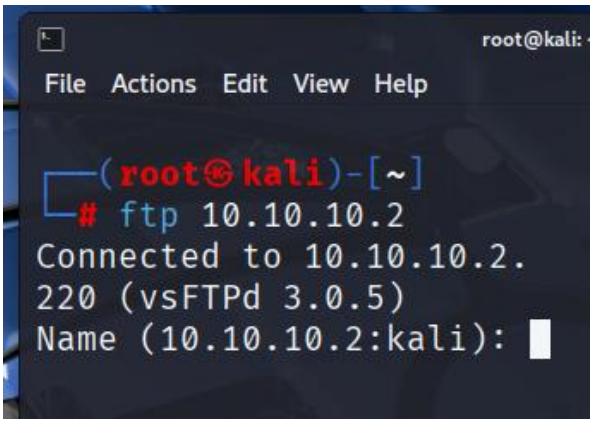
```
root@vnpro:~# iptables -L FORWARD --line-number
Chain FORWARD (policy DROP)
num  target     prot opt source               destination
1    ACCEPT     all  --  192.168.1.0/24       10.10.10.0/24
2    ACCEPT     all  --  anywhere             anywhere             state RELATED
,ESTABLISHED
3    ACCEPT     tcp  --  192.168.1.0/24       10.10.10.2           tcp dpt:http
4    ACCEPT     tcp  --  192.168.1.0/24       10.10.10.2           tcp dpt:ftp
```

Dựa vào bảng iptables, ta thấy rằng việc chuyển tiếp toàn bộ dịch vụ không còn phù hợp nữa, nên sẽ xóa rules đầu tiên đi.

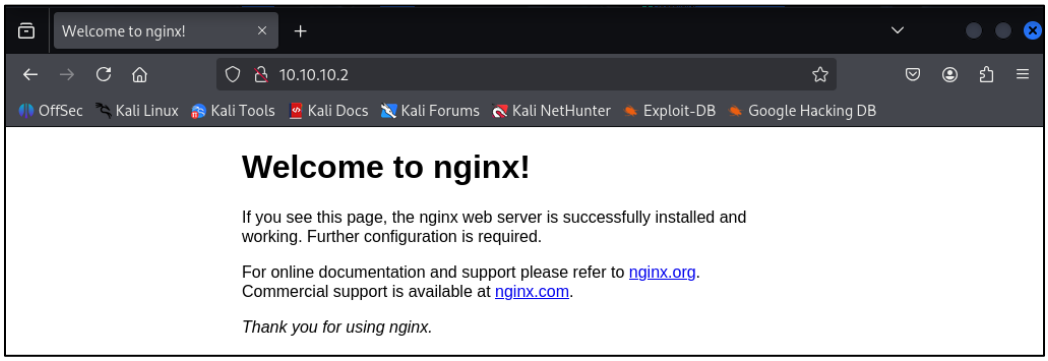
```
iptables -D FORWARD 1
```

Kiểm tra kết quả sau khi cấu hình:

Kiểm tra dịch vụ FTP trên máy client bằng lệnh ftp 10.10.10.2



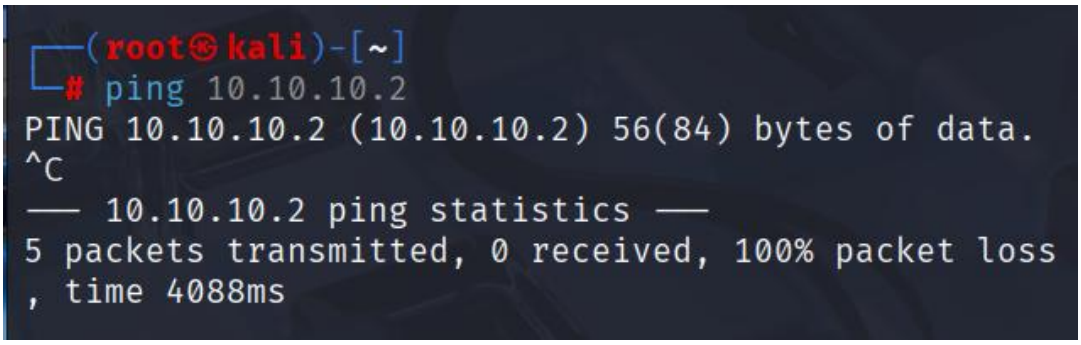
Kiểm tra dịch vụ Web trên máy client: Truy cập địa chỉ IP của server trên trình duyệt.



Thử truy cập các dịch vụ còn lại (ví dụ: Ping, SSH):

Lệnh ping:

ping 10.10.10.2



Lệnh SSH:

ssh user@10.10.10.2

➔Các dịch vụ này đã bị chặn.

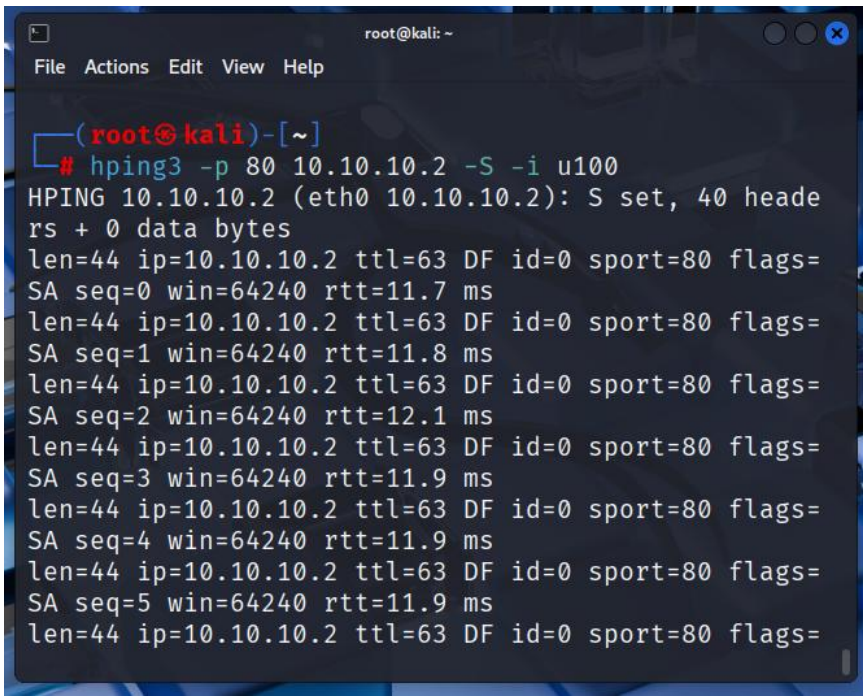
Bài tập 3: cấu hình rule chống tấn công DoS (Denial of Service)

Để phòng chống tấn công DoS, đặc biệt là SYN Flood, chúng ta sẽ thiết lập rule để chặn các nguồn gửi quá nhiều gói SYN trong một khoảng thời gian ngắn.

Mô phỏng tấn công DoS:

Trên máy Kali, thực hiện tấn công DoS bằng lệnh:

```
hping3 -S -p 80 10.10.10.2 -i u100
```



Thiết lập Rule chống DoS:

Để tối ưu, chúng ta cần xem xét khả năng đáp ứng của máy chủ. Trong bài tập này, chúng ta sẽ **drop toàn bộ các gói tin từ nguồn gửi liên tục 20 gói SYN khi chưa tới 5 giây.**

#Drop các nguồn gửi liên tục 20 gói tin SYN khi chưa tới 5 giây:

```
iptables -A FORWARD -p tcp --syn -m recent --name synflood --update --seconds 5 --hitcount 20 -j DROP
```

#Ghi nhận IP gửi gói SYN mới:

```
iptables -A FORWARD -p tcp --syn -m recent --name synflood --set -j ACCEPT
```

#Kiểm tra và sắp xếp lại bảng rules:

```
iptables -L FORWARD --line-number
```

```
Chain FORWARD (policy DROP)
num  target     prot opt source               destination
1    ACCEPT     all  --  anywhere             anywhere             state RELATED
,ESTABLISHED
2    ACCEPT     tcp  --  192.168.1.0/24       10.10.10.2           tcp dpt:http
3    ACCEPT     tcp  --  192.168.1.0/24       10.10.10.2           tcp dpt:ftp
4    DROP       tcp  --  anywhere             anywhere             tcp flags:FIN
,SYN,RST,ACK/SYN recent: UPDATE seconds: 5 hit_count: 20 name: synflood side: so
urce mask: 255.255.255.255
5                tcp  --  anywhere             anywhere             tcp flags:FIN
,SYN,RST,ACK/SYN recent: SET name: synflood side: source mask: 255.255.255.255
root@vnpro:~#
```

Khi kiểm tra, chúng ta có thể nhận thấy thứ tự các rule chưa tối ưu. Rule chống DoS cần được đặt sau các rule cho phép các kết nối hợp lệ.

Thứ tự đúng của các rule:

➞1. Cho phép kết nối đã có (ESTABLISHED, RELATED)

➞2. Cho phép HTTP

➞3. Cho phép FTP

➞4. Ghi nhận IP gửi SYN (sử dụng --set)

➞5. Chặn nếu IP vượt ngưỡng SYN (--update --seconds 5 --hitcount 20 -j DROP)

Sắp xếp lại các rule:

Đầu tiên, xóa các rule cũ nếu chúng không đúng thứ tự:

```
iptables -D FORWARD 5
iptables -D FORWARD 4
iptables -D FORWARD 3
iptables -D FORWARD 2
```

Sau đó, thêm lại các rule theo thứ tự tối ưu:

```
# Cho phép HTTP
iptables -A FORWARD -p tcp -s 192.168.1.0/24 -d 10.10.10.2 --dport 80 -j ACCEPT
```

Cho phép FTP (port 21)

```
iptables -A FORWARD -p tcp -s 192.168.1.0/24 -d 10.10.10.2 --dport 21 -j ACCEPT
```

Ghi nhận IP gửi gói SYN mới

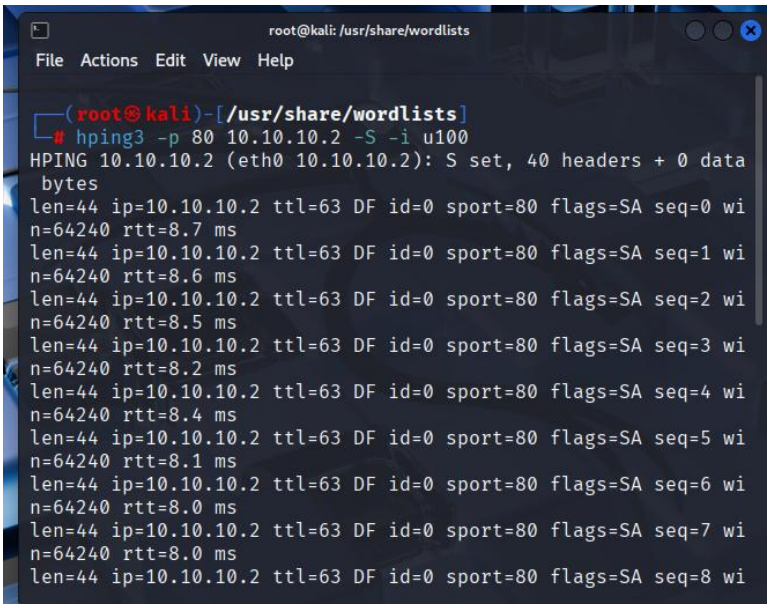
```
iptables -A FORWARD -p tcp --syn -m recent --name synflood --set -j ACCEPT
```

Drop các nguồn gửi liên tục 20 gói tin khi chưa tới 5s

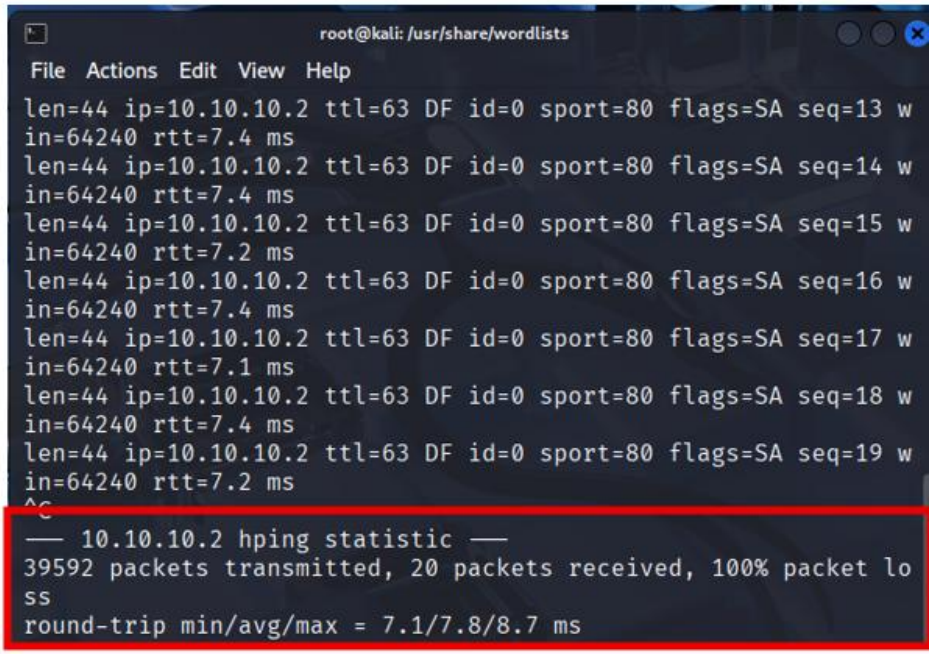
```
iptables -A FORWARD -p tcp --syn -m recent --name synflood --update --seconds 5 --hitcount 20 -j DROP
```

Sau đó trên máy client thực hiện lại cuộc tấn công bằng lệnh:

```
hping3 -p 80 10.10.10.2 -S -i u100
```



Nhận thấy rằng sau gói tin thứ 20, không còn gói nào được response, nhấn tổ hợp phím ctrl+c, kết quả thấy rằng 100% gói tin bị lost, như vậy chúng ta đã chặn thành công cuộc tấn công DOS.

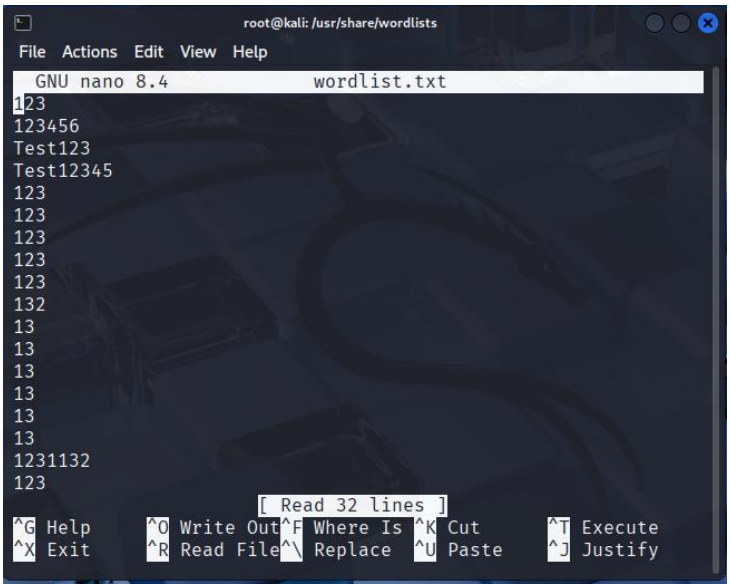


Bài tập 4: tạo rule phòng chống Brute-force FTP

Khi public dịch vụ FTP, hacker có thể dò mật khẩu (brute-force) để chiếm quyền truy cập. Chúng ta sẽ cấu hình iptables để ngăn chặn hành vi này.

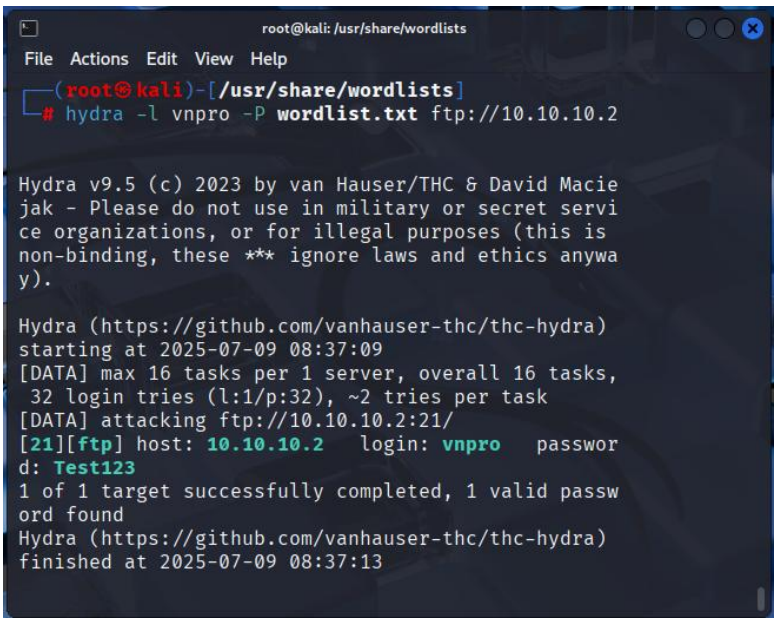
Mô phỏng tấn công Brute-force:

#Tạo một wordlist trên máy client: dùng lệnh nano wordlist.txt, nhập các mật khẩu vào file, sau đó lưu lại (Ctrl+X, Y, Enter).



#Tiến hành brute-force mật khẩu bằng Hydra:

hydra -l vnpro -P wordlist.txt ftp://10.10.10.2



Nhận thấy rằng, Hydra dò mật khẩu thành công với user "vnpro" password là “Test123”

Thiết lập Rule chống Brute-force FTP:

Trên máy firewall, thêm các rule sau:

#DROP nếu IP truy cập quá 5 lần trong 60 giây (đối với cổng FTP 21):

iptables -A FORWARD -p tcp --dport 21 -m recent --name ftpbrute --rcheck --seconds 60 --hitcount 5 -j DROP

#Nếu không vượt quá ngưỡng, thì ghi nhận IP:

iptables -A FORWARD -p tcp --dport 21 -m recent --name ftpbrute --set -j ACCEPT

Thứ tự các rule:

➞1. Cho phép kết nối đã có (ESTABLISHED, RELATED)

➞2. Chặn brutefoce FTP

➞3. Cho phép các truy cập FTP hợp lệ

➞4. Chặn DoS

➞5. Cho phép luồng hợp lệ

➞6. Cho phép HTTP

➞7. Cho phép FTP

```
root@vnpro:~# iptables -L FORWARD --line-number
Chain FORWARD (policy DROP)
num  target     prot opt source               destination
1    ACCEPT     all  --  anywhere             anywhere             state RELATED
,ESTABLISHED
2    DROP       tcp  --  anywhere             anywhere             tcp dpt:ftp r
ecent: CHECK seconds: 60 hit_count: 5 name: ftpbrute side: source mask: 255.255.
255.255
3    ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:ftp r
ecent: SET name: ftpbrute side: source mask: 255.255.255.255
4    DROP       tcp  --  anywhere             anywhere             tcp flags:FIN
,SYN,RST,ACK/SYN recent: UPDATE seconds: 5 hit_count: 20 name: synflood side: so
urce mask: 255.255.255.255
5    ACCEPT     tcp  --  anywhere             anywhere             tcp flags:FIN
,SYN,RST,ACK/SYN recent: SET name: synflood side: source mask: 255.255.255.255
6    ACCEPT     tcp  --  192.168.1.0/24       10.10.10.2           tcp dpt:ftp
7    ACCEPT     tcp  --  192.168.1.0/24       10.10.10.2           tcp dpt:http
root@vnpro:~#
```

Kiểm tra lại:

Trên máy client, thực hiện lại lệnh brute-force bằng Hydra. Bạn sẽ thấy quá trình này bị chặn và không có phản hồi từ server sau một số lần thử.