HỌC VIỆN KỸ THUẬT MẬT MÃ
KHOA AN TOÀN THÔNG TIN

MODULE THỰC HÀNH

AN TOÀN MẠNG MÁY TÍNH

BÀI THỰC HÀNH SỐ 01

THIẾT LẬP VÀ CẤU HÌNH TƯỜNG LỬA IPTABLES

Người xây dựng bài thực hành:

Th.S Cao Minh Tuấn

HÀ NỘI, 2018

MỤC LỤC

THÔNG TIN CHUNG VỀ BÀI THỰC HÀNH

Tên bài thực hành: Thiết lập và cấu hình tường lửa Iptables.

Học phần: An toàn mạng máy tính

Số lượng sinh viên cùng thực hiện:

Địa điểm thực hành: Phòng máy

Yêu cầu:

Máy tính vật lý có cấu hình tối thiểu: RAM 4GB, 50 HDD

- Yêu cầu kết nối mạng LAN: có
- Yêu cầu kết nối mạng Internet: có
- Yêu cầu khác: máy chiếu, bảng viết, bút/phấn viết bảng

Công cụ được cung cấp cùng tài liệu này:

CHUẨN BỊ BÀI THỰC HÀNH

Đối với giảng viên

Trước buổi học, giảng viên (người hướng dẫn thực hành) cần kiểm tra sự phù hợp của điều kiện thực tế của phòng thực hành với các yêu cầu của bài thực hành.

Ngoài ra không đòi hỏi gì thêm.

Đối với sinh viên

Trước khi bắt đầu thực hành, cần tạo các bản sao của máy ảo để sử dụng. Đồng thời xác định vị trí lưu trữ các công cụ đã chỉ ra trong phần yêu cầu.

THIẾT LẬP VÀ CẤU HÌNH TƯỜNG LỬA IPTABLES

1.1. Mô tả

Tường lửa Iptables là loại tường lửa miễn phí được tích hợp sẵn trong các hệ điều hành Linux. Có thể ứng dụng để kiểm soát truy cập cho mạng máy tính nội bộ và phân vùng mạng máy chủ.

Trong bài thực hành này hướng dẫn thiết lập tập luật cho tường lửa Iptables để kiểm soát các dịch vụ cho mạng nội bộ, mạng DMZ, mạng Internet. Cụ thể là cho phép người dùng trong mạng nội bộ LAN có thể truy cập được ra ngoài Internet với các giao thức HTTP, HTTPS, ICMP, DNS.

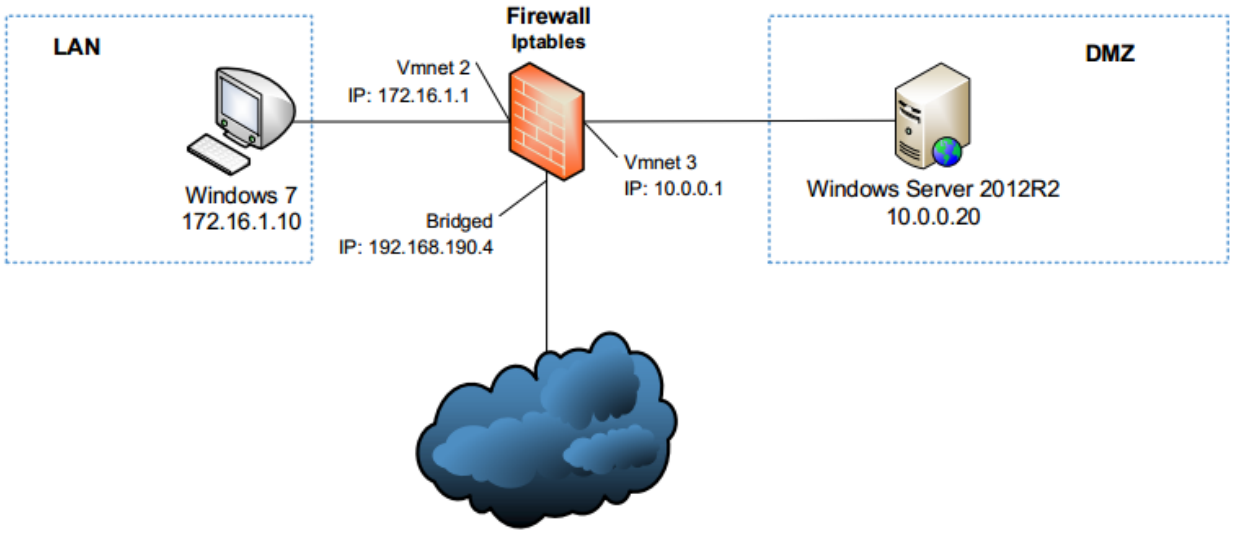
Cho phép người dùng từ mạng Internet và mạng nội bộ truy cập được trang web từ máy chủ web trong phần vùng DMZ.

Cho phép người dùng sử dụng ứng dụng thư điện tử để gửi và nhận thư với nhau.

1.2. Chuẩn bị

- 01 máy ảo hệ điều hành Windows 7: Cài đặt ứng dụng thư Mozilla Thunderbird
- 01 máy ảo hệ điều hành Windows Server 2012.
  - + Đã cài dịch vụ web sử dụng máy chủ web IIS với trang web mặc định của Microsoft.
  - + Đã cài dịch vụ phân giải tên miền DNS với các bản ghi thích hợp cho web và mail.
  - + Đã cài phần mềm máy chủ thư điện tử (MDaemon V10).
- 01 máy ảo hệ điều hành CentOS 6.5 để làm tường lửa Iptables.

1.3. Mô hình cài đặt



1.4. Một số câu lệnh cơ bản sử dụng trong tường lửa Iptables

Lệnh khởi động tường lửa:

```
[root@server]# service iptables start
[root@server]# service iptables stop
[root@server]# service iptables restart
```

Để khởi động Iptables mỗi khi khởi động máy:

```
[root@server]# chkconfig iptables on
```

Để xem tình trạng của Iptables:

```
[root@server]# service iptables status
```

Lưu thông tin cấu hình:

```
[root@server]# /etc/init.d/iptables save
```

Lệnh xóa toàn bộ luật có trong Iptables:

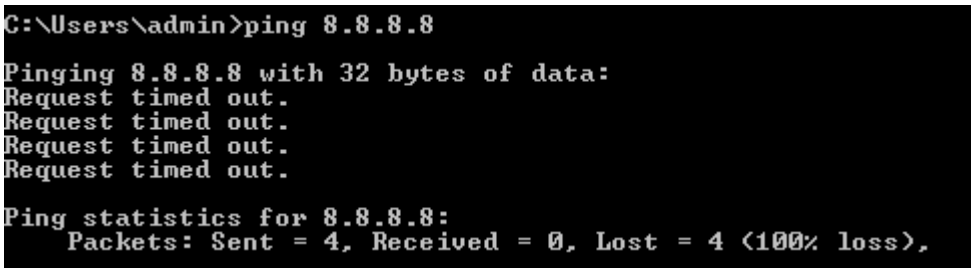
```
[root@server]# iptables -F
[root@server]# iptables -t nat -F
```

1.5. Các kịch bản thực hiện

1.5.1. Kịch bản 1. Cho phép máy tính trong LAN Ping ra ngoài mạng Internet

Bước 1. Kiểm tra Ping

Tại máy trạm Windows 7 thực Ping đến địa chỉ IP bất kỳ.



Kết quả, không Ping được ra ngoài mạng.

Bước 2. Thiết lập luật trên tường lửa Iptables để cho phép máy trạm Ping ra bên ngoài.

Trước hết cần kiểm tra tên của các giao diện mạng trên máy tường lửa Iptables:

```
[root@server]# ifconfig
eth1      Link encap:Ethernet  HWaddr 00:0C:29:56:E3:8A
          inet addr:192.168.190.4  Bcast:192.168.190.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe56:e38a/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1

eth2      Link encap:Ethernet  HWaddr 00:0C:29:56:E3:94
          inet addr:172.16.1.1  Bcast:172.16.1.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe56:e394/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1

eth3      Link encap:Ethernet  HWaddr 00:0C:29:56:E3:9E
          inet addr:10.0.0.1  Bcast:10.0.0.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe56:e39e/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
```

Trong hình trên giao diện eth1 kết nối mạng Internet. Giao diện eth2 kết nối mạng nội bộ, giao diện eth3 kết nối mạng máy chủ.

Tiếp theo đặt lệnh cho Iptables để cho phép máy trạm trong mạng nội bộ Ping ra mạng Internet.

```
[root@server]#iptables -A FORWARD -i eth2 -o eth1 -s
172.16.1.0/24 -p icmp --icmp-type any -j ACCEPT
[root@server]#iptables -A FORWARD -i eth1 -o eth2 -d
172.16.1.0/24 -p icmp --icmp-type any -j ACCEPT
[root@server]#iptables -t nat -A POSTROUTING -o eth1 -s
172.16.1.0/24 -j SNAT --to-source 192.168.190.4
[root@server]#nano /proc/sys/net/ipv4/ip_forward 0 -> 1
```

Ghi chú: địa chỉ IP 192.168.190.4 là địa chỉ của giao diện mạng kết nối Internet (eth1), tùy thuộc vào trường hợp cụ thể của máy ảo mà sử dụng địa chỉ IP này.

Bước 3. Kiểm tra kết quả

Trở lại máy trạm Windows 7 kiểm tra Ping tới địa chỉ IP tại bước 1. Kết quả thành công.

```
C:\Users\admin>ping 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time=35ms TTL=127
Reply from 8.8.8.8: bytes=32 time=38ms TTL=127
Reply from 8.8.8.8: bytes=32 time=36ms TTL=127
Reply from 8.8.8.8: bytes=32 time=36ms TTL=127

Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 35ms, Maximum = 38ms, Average = 36ms
```

1.5.2. Kịch bản 2. Cho phép máy tính trong LAN truy vấn DNS ra Internet

Bước 1. Kiểm tra truy vấn

Trước khi thiết lập luật cho tường lửa, tại máy trạm Windows 7 không truy vấn được DNS. Sử dụng lệnh **nslookup** để truy vấn.

```
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\admin>nslookup
DNS request timed out.
    timeout was 2 seconds.
Default Server:  UnKnown
Address:  8.8.8.8

>
```

Bước 2. Cấu hình luật để cho phép truy vấn DNS tại tường lửa.

```
[root@server]#iptables -A FORWARD -i eth2 -o eth1 -s
172.16.1.0/24 -p udp --dport 53 -j ACCEPT
[root@server]#iptables -A FORWARD -i eth1 -o eth2 -d
172.16.1.0/24 -p udp --sport 53 -j ACCEPT
```

Bước 3. Kiểm tra kết quả

Kết quả, lúc này tại máy Windows 7 thực hiện truy vấn thành công

```
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\admin>nslookup
Default Server:  google-public-dns-a.google.com
Address:  8.8.8.8

> _
```

1.5.3. Kịch bản 3. Cho phép máy tính trong mạng LAN truy cập được các website từ mạng Internet

Yêu cầu:

- Thiết lập luật cho tường lửa Iptables sao cho các máy tính trạng mạng nội bộ có thể truy cập được mạng Internet thông qua hai giao thức HTTP và HTTPS.
- Sử dụng Win 7 để kiểm tra truy cập trước và sau khi thiết lập luật cho tường lửa.

1.5.4. Kịch bản 4. Cho phép truy cập tới máy chủ web trong phân vùng mạng DMZ

Yêu cầu:

- Thiết lập luật cho tường lửa Iptables sao cho các máy tính trong mạng nội bộ có thể truy cập được website từ máy chủ web trong mạng DMZ
- Thiết lập luật cho tường lửa Iptables sao cho các máy tính từ mạng Internet có thể truy cập được website trong mạng DMZ.
- Sử dụng Win7 là máy ảo trong mạng nội bộ để kiểm tra.
- Sử dụng máy tính vật lý làm máy từ Internet truy cập vào website.

1.5.5. Kịch bản 5. Cho phép người dùng gửi và nhận thư điện tử

Yêu cầu:

- Thiết lập luật cho tường lủa Iptables sao cho các máy tính trong mạng nội bộ và máy tính từ Internet có thể gửi và nhận thư điện tử được cho nhau thông qua máy chủ mail trong DMZ.
- Sử dụng mail client Mozilla Thunderbirth để kiểm tra.