Giới thiệu:

- IP tables là công cụ mạnh mẽ

- Nó được xây dựng dưới dạng 1 node trong kernel, có thể tương tác với firewall thông qua các cmd (thêm rule, sử rule..)

- Ip tables sử dụng các tính chất của IP, protocol (tcp, udp, icmp), port cho việc lọc, dễ dàng cho việc tiếp cận

- Các rule của Iptables được lưu trong các chains (INPUT, OUTPUT, FORWARD), nó sẽ check bất kỳ network trafic (IP packets) và sau đó app các rule đã định nghĩa vào.

- 2 các định nghĩa nhiều nhất sử dụng cho các targer là DROP (drop packet) và ACCEPT (accept packet)

Chains

- Có 3 loại định nghĩa trước cho chain trong filter table, nó sẽ được sử dụng khi ta add các rule vào các chain xác định:

+ INPUT – tất cả các packets đi đến host

+ OUTPUT – tất các các packets đi ra khỏi host

+ FORWARD – tất cả packet đi qua host và mong muốn được truy cập vào host khác (khi sử dụng host cho việc định tuyến)

- Thông thường, ta chủ yếu sử dụng bảng INPUT để lọc các gói tin

- Các rule được thêm vào mỗi chain

- Các packet sẽ được check, bắt đầu từ trên xuống dưới, nếu match thì sẽ apply luật, nếu không match bất kỳ rule nào thì sẽ apply rule mặc định của chains. Khi rule match, nó sẽ kết thúc phiên làm việc với packet. Có 2 rule default cho chain là ACCEPT và DROP

Làm rõ trước khi apply rule default cho chains

- Ta có thể set DROP policy mặc định cho chains, sau đó thêm các rule cho phép (accept) các gói tin từ các ip tin cậy hoặc 1 số port xác định

- Ta có thể set ACCEPT tất cả các packet và sau đó thêm các rule block (drop) các packet từ 1 khoảng ip ko tin cậy, và 1 số ports cho các service private hoặc không có service chạy

- Thông thường, ta sử dụng rule DROP cho input chains và ACCEPT cho output chains

**Writing a Simple Rule Set**

- Viết các rule đơn giản

# iptables -P INPUT ACCEPT

# iptables -F

# iptables -A INPUT -i lo -j ACCEPT

# iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT

# iptables -A INPUT -p tcp --dport 22 -j ACCEPT

# iptables -P INPUT DROP

# iptables -P FORWARD DROP

# iptables -P OUTPUT ACCEPT

# iptables -L -v

- Kết quả

Chain INPUT (policy DROP 0 packets, 0 bytes)

pkts bytes target prot opt in out source destination

0 0 ACCEPT all -- lo any anywhere anywhere

0 0 ACCEPT all -- any any anywhere anywhere state RELATED,ESTABLISHED

0 0 ACCEPT tcp -- any any anywhere anywhere tcp dpt:ssh

Chain FORWARD (policy DROP 0 packets, 0 bytes)

pkts bytes target prot opt in out source destination

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)

pkts bytes target prot opt in out source destination

- Phân tích 8 cmd

+ Nếu đang kết nối dạng remote thông qua ssh thì rule này sẽ tự động cho phép kết nối ssh hiện tại được quyền sử dụng tiếp

**iptables -P INPUT ACCEPT**

+ Xóa tất cả các rule hiện có, sử dụng tham số **-F**

**iptables -F**

+ Tạo 1 rule cơ bản, ta sử dụng -A (Append or add) để thêm 1 rule xác định cho chain, trong vd là thêm vào INPUT chains, sau đó ta sử dụng -i dể xác đinh interface, -j (jump) để định nghĩa hành động cho packet match rule. Trong tường hợp dưới là cho phép tất các packet từ địa chỉ loopback được quyền kết nối

**iptables -A INPUT -i lo -j ACCEPT**

+ Ta sử dụng -A (thêm rule append), sử dụng -m để sử dụng module (state). State module cho phép kiểm tra trạng thái của packet và xác định nó thuộc dạng NEW, ESTABLISHED or RELATED. NEW = các paket từ 1 kết nối mới được khởi tạo, chưa được khởi tạo lần nào bưởi host system. ESTABLISHED and RELATED = các packet là thuộc 1 ohaafn của các kết nối đã được thiết lập hoặc liên quan đến 1 kết nối đã được thiết lập

**iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT**

+ Add rule cho ssh thông qua port 22, tcp

**iptables -A INPUT -p tcp --dport 22 -j ACCEPT**

+ option “-P” set default policy cho 1 chain xác định. Trong ví dụ ta xét default policy cho input là drop = tất cả các gói tin đến nếu ko match rule sẽ bị block (drop)

**iptables -P INPUT DROP**

+ set default policy cho FORWARD là DROP trong trường hợp ko sử dụng host như router

**iptables -P FORWARD DROP**

+ set default policy cho OUTPUT là ACCEPT, cho phép các kết nối khởi tạo từ máy

**iptables -P OUTPUT ACCEPT**

+ xem kết quả

**iptables -L -v**

+ Chúng ta cần save rule để trong trường hợp restart firewall các cấu hình vẫn được giữ lại

NOTE:

- có thể tạo 1 script cấu hình firewall với các note, các chỉ dẫn cho các rule

**Interfaces**

- Sử dụng cho việc định nghĩa việc xử lý các gói tin cho interface

iptables -A INPUT -i lo -j ACCEPT

- Giả sử chúng ta có 2 interface, eth0 = lan, ppp0 là đường cung cấp bởi nhà mạng. Ta muốn các hình cho phép tất cả các packet đến chửa LAN và vẫn filter tất các packet đến của internet

iptables -A INPUT -i lo -j ACCEPT

iptables -A INPUT -i eth0 -j ACCEPT

- nếu chúng ta cho phép tất cả packet đến của internet => đồng nghĩa disable firewall

iptables -A INPUT -i ppp0 -j ACCEPT

**IP Addresses**

- Sử dụng trong mạng nhỏ, khi chúng ta cần accept các ip tin cậy, được quyền truy cập vào máy chủ

# Accept packets from trusted IP addresses

iptables -A INPUT -s 192.168.0.4 -j ACCEPT # change the IP address as appropriate

- sử dụng tham số “-A” để thêm rule cho INPUT chain, “-s” để xác đinh source

- Trong trường hợp ta cho phép 1 dải ip tin cậy, có thể định nghĩa thêm netmask cho dải mạng

# Accept packets from trusted IP addresses

iptables -A INPUT -s 192.168.0.4 -j ACCEPT # change the IP address as appropriate

- Chúng ta còn có thể filter các packet theo MAC để xác định ip tin cậy (yêu cầu MAC module)

# Accept packets from trusted IP addresses

iptables -A INPUT -s 192.168.0.4 -m mac --mac-source 00:50:8D:FD:E6:32 -j ACCEPT

- sử dụng “-m mac” để load module mac, sau đó sử dụng --mac-source để chỉ định địa chỉ MAC. Sử dụng module sẽ tránh việc giả mạo IP để truy cập bất hợp pháp

**Ports and Protocols**

- Cách định nghĩa các rule cho phép truy cập port

- Để làm được đầu tiên phải xác định được protocol và port number set cho service. Ví dự bitorrent sử dụng tcp protocol và port 6881

# Accept tcp packets on destination port 6881 (bittorrent)

iptables -A INPUT -p tcp --dport 6881 -j ACCEPT

- sử dụng tham số “-A” để add rule vào spefic chains, “-p” để xác đinh protocol, và “-dport” để xác định port đích.

Note: Lưu ý có 2 loại port đích(dport) và port nguồn (sport)

- có thể mở rộng port => range port

# Accept tcp packets on destination port 6881 (bittorrent)

iptables -A INPUT -p tcp --dport 6881 -j ACCEPT

**Putting It All Together**

- khi chúng ta mở port 22 => hacker có thể sử dụng kỹ thuật brute force cracking để dò ra passwd các user => nếu chúng ta xác định được các ip mong muốn được truy cập thì có thể set lại rule này

# Accept tcp packets on destination port 22 (SSH)

iptables -A INPUT -p tcp --dport 22 -j ACCEPT

sửa lại

# Accept tcp packets on destination port 22 (SSH)

iptables -A INPUT -p tcp --dport 22 -j ACCEPT

e