Iptables - Network Security

Published on Tuesday, January 05, 2016

Hi Folks,

We're continuing with remaining parts of network security section. Today's topic is Iptables. This feature is mostly used with Linux systems which represent a major chunk of commercial servers. Any doubts/suggestions - pour your heart out in comments section!

==>> This article is a part of PK Series (IT Officers)

What is Iptable?

Iptable is the building block of a framework inside the **Linux Kernel**. It is represented by a generic table structure for **definition of rulesets**. Each rule with an Iptable consists of a number of classifiers (iptable matches) and one connection action (iptable target). The security functions that can be achieved with Iptables are as follows:

- Build internet firewalls based on **stateless** and **stateful** packet filtering- In stateful filtering ports are opened and closed as clients use the internet in such a way that it mostly presents a blank wall to attackers.
- NAT and masquerading for sharing internet access
- NAT to implement transparent proxies - transparent proxies are intermediary systems that sit between user and content providers. Upon request by a user, they perform functions like caching, redirection and authentication.
- Packet manipulation like altering the bits of IP header.
- Provides for improved logging options by using user defined prefixes

Iptable Tables

1. Filter table

Its the default table i.e if you haven't defined your own one, you will be using the default. It has following built in chains:

- INPUT chain - for packets coming to local server.
- OUTPUT chain - for packets going out of the server.
- FORWARD chain - packets for another interface i.e packets routed through the server.

2. NAT table

It has following built in chains:

- PREROUTING chain - packet translation happens immediately after packet

comes to the system and before it is routed further. This helps to translate the destination IP address of packets to something that matches on local server.

- POSTROUTING chain - packet translation happens when packets are leaving the system. It translates the source IP address to something which matches on server.
- OUTPUT chain - NAT for locally generated packets on the firewall.

3. Mangle Table

It is for specialized packet alteration. This alters QOS bits in TCP header. Quality of service (QOS) is a group of components that can differentiate traffic flows so that high priority traffic receives preferential treatment. Mangle table has following built in chains:

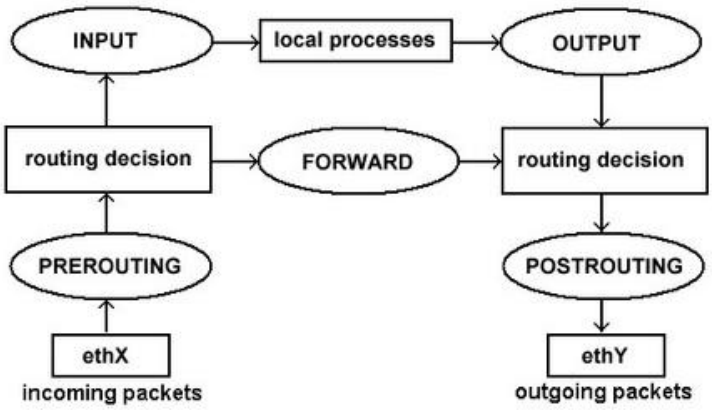
- PREROUTING chain
- OUTPUT chain
- FORWARD chain
- INPUT chain
- POSTROUTING chain

4. Raw table

It is used for configuration exemptions. It has following built in chains:

- PREROUTING chain
- OUTPUT chain

The following flowchart will help you better understand the flow using Iptables:



Iptable Rules

Rules contain a criteria and a target. If criteria is matched, it executes values mentioned in the target and if criteria is not matched, it moves to the next rule.

Target Values

- ACCEPT - firewall will accept the packet
- DROP - drop the packet
- QUEUE - pass the packet to user space
- RETURN - stop executing next set of rules in current chain and control is returned to calling chain.

Let's see some **commands** we use for Iptables:

1. To see all firewall rules in system:

 # iptables -t filter --list (or)
 # iptables --list (will display default filter table)

2. To view NAT table:

 # iptables -t nat --list

3. To view Raw table:

 # iptables -t raw --list

4. To view the Mangle Table:

 # iptables -t mangle --list

Quote of the day

The best revenge is massive success. - *Frank Sinatra*