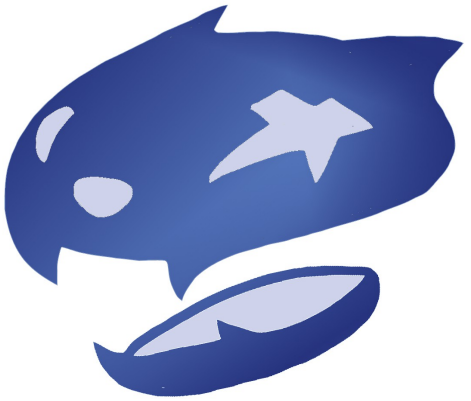
Basic Firewalls in Linux Using IPTables

Camilo Payan
Panther Linux User Group
Florida International University
February 17, 2011



Basic Definitions

- **Address**: represents a given device (an IP Address)
- **Ports**: When a packet is received by a host, it's sent to a specific port
- **Protocols**: The “type” of traffic that is being sent
  - **TCP** (Transmission Control Protocol) maintains a connection between hosts
  - **UDP** (User Datagram Protocol) sends data without establishing a connection
  - **ICMP** (Internet Control Message Protocol) handles admin functions, like ping
- It takes a **source address**, **destination address**, **destination port**, **source port**, and **protocol type** to characterize traffic for a firewall.

What is Packet Filtering and why should I do it?

- Blocking unwanted traffic or probes from outside
- Limiting internet access from certain hosts
- Network Address Translation
- Inbound port redirection

Tables, Chains, and Rules

- **Tables**: A set of chains, there are three basic tables
  - Filter Table
  - NAT Table
  - Mangle Table
- We focus on the **Filter Table** which has three main chains
  - INPUT
  - OUTPUT
  - FORWARD
- Chains are made up of user-defined rules

IPTables Syntax

- **Adding a rule**
  - `iptables -t table -A/I chain condition -j TARGET`
- **Listing rules**
  - `iptables -t table -L --line-number`
- **Deleting a rule**
  - `iptables -t table -D chain condition action`
  - `iptables -t table -D chain rule-number`

IPTables Conditions

- **-p** {tcp|udp|icmp|all}
- **-s** source_ip
- **-d** destination_ip
- **--sport** source_port
- **--dport** dest_port
- **-i** input interface
- **-o** output interface
- **-m** state **--state** {NEW|ESTABLISHED|RELATED}

Example:

```
-p tcp -s IP -sport 80 -d IP -m state --state NEW
```

IPTables Targets

- **ACCEPT**: let packet pass
- **DROP**: ignore packet, send no response back
- **REJECT**: ignore packet, send error message back
- **Custom Chain**: direct it to another custom chain by naming that chain

Examples!

- Allowing incoming ssh traffic
  - `iptables -A INPUT -p tcp --dport ssh -j ACCEPT`
- Limiting pings to 1 per second
  - `iptables -A INPUT -p icmp --icmp-type echo-request -m limit --limit 1/s -i eth0 -j ACCEPT`
- And much more in your trusty `man` page and online.