Tutorial & Case Study in Implementing Linux Network Security, part I

Oskar Andreasson
oskar.andreasson@direct2internet.com

The speaker - that is me

- Oskar Andreasson
- From Sweden
- Linux user since 1994.
- Written about Iptables since 2.4 kernels
- Unix Specialist at Direct2Internet

Table of Contents

Table of Content

- Introduction
- Iptables
  - What is it
  - Packet traversal
  - Command syntax
- Ipsysctl
  - What is it
  - Tools
  - Structure
  - What you can find
- Final notes
- Break

LAMP Case study - Theory - Iptables

□ A tool for implementing security policies

□ A packet filter

□ Network Address Translation

□ Packet mangling

LAMP Case study - Theory - Iptables - What is it

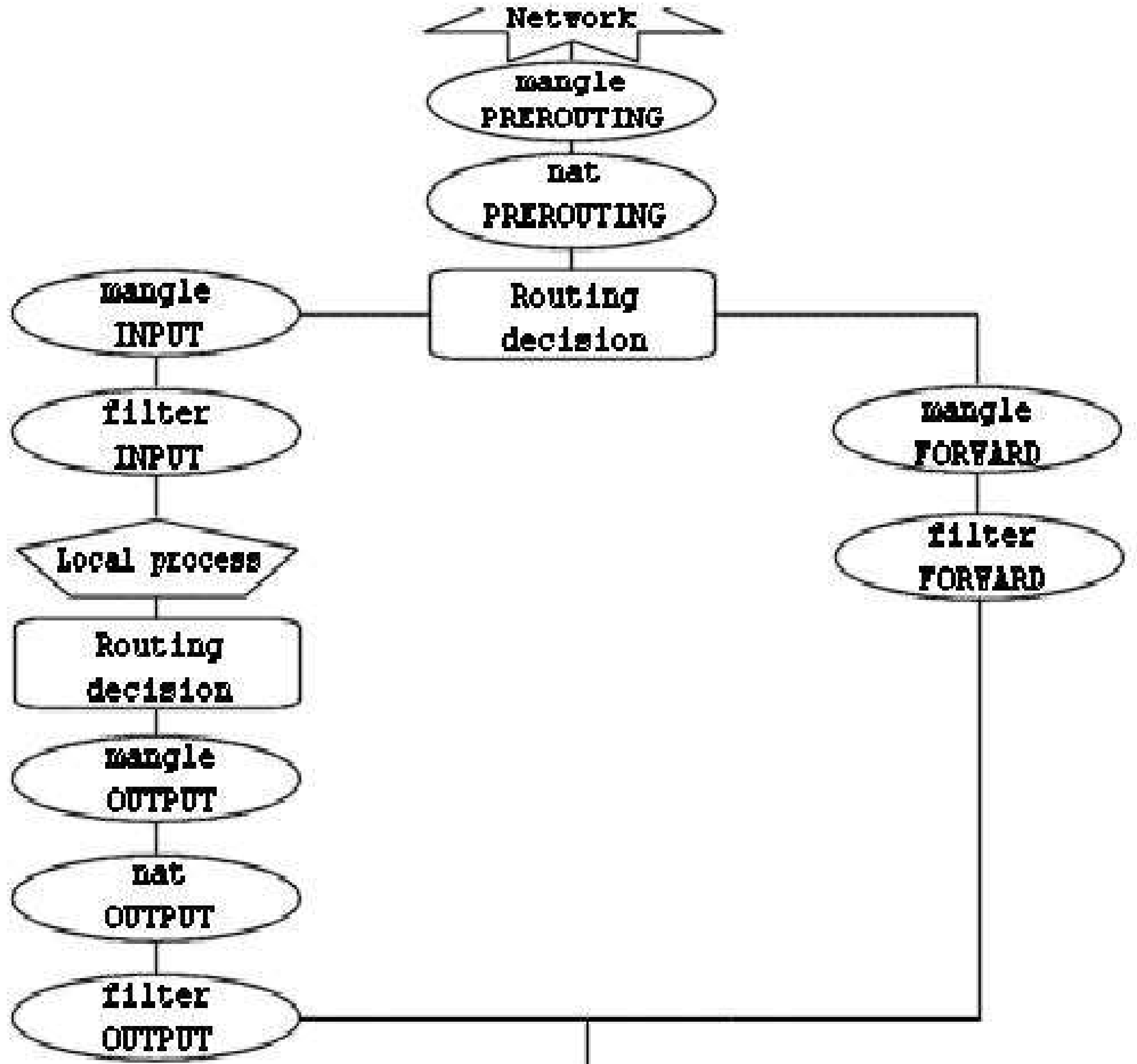
- Consists of two parts
  - Iptables - userspace tool
  - Netfilter - kernel side

- Iptables
  - Used to configure and to change the Netfilter settings
  - A userspace program

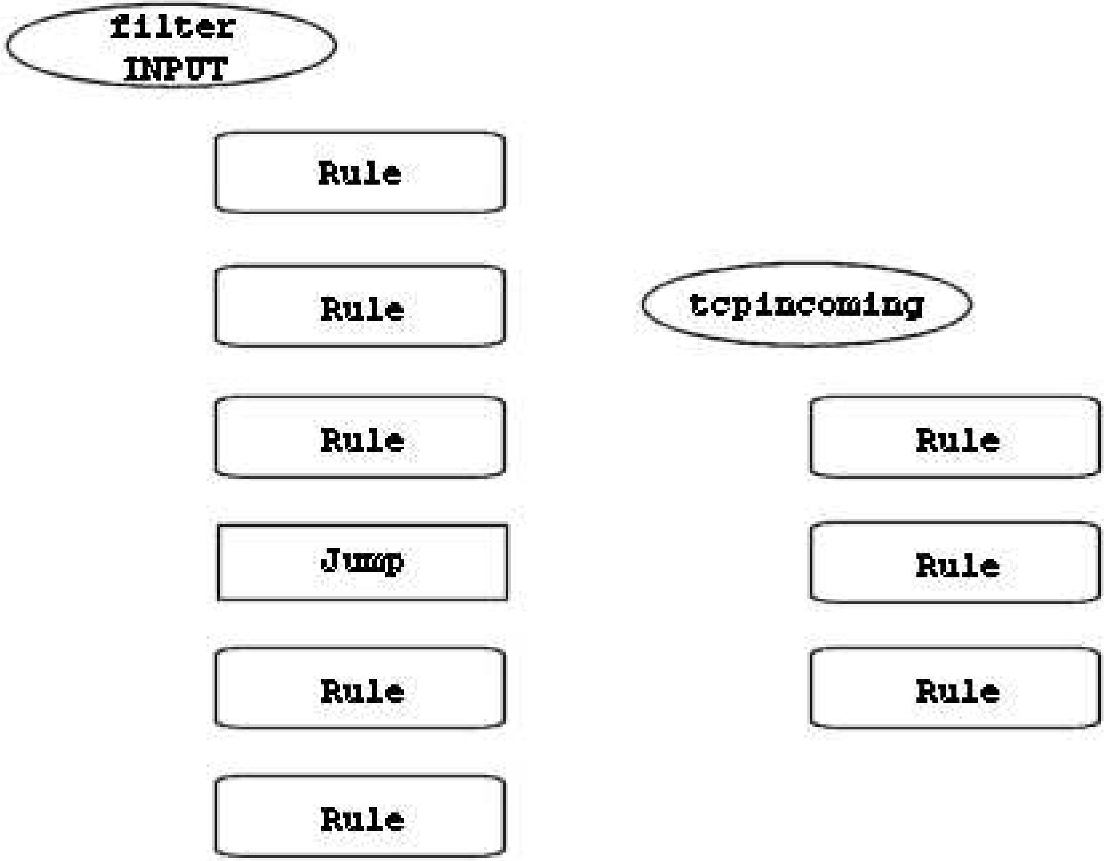
LAMP Case study - Theory - Iptables - What is it

- Netfilter
  - The real workhorse in the combo
  - Located inside the kernel
  - Does all of the filtering, mangling and masquerading specified by iptables
  - Support must be in kernel!

LAMP Case study - Theory - Iptables - Packet traversal



LAMP Case study - Theory - Iptables - Packet traversal



Traversal of a single chain with subchain

LAMP Case study - Theory - Iptables - Command syntax

```
iptables [-t table] command [match] [target/jump]
```

- □ -t table - which table to alter (filter (default), nat or mangle)
- □ command - What command to perform, delete, append, insert, flush, etc
- □ match - All the matches that we want to perform
- □ target/jump - The action we want to take if all matches are right

LAMP Case study - Theory - Iptables - Command syntax

Tables

- □ nat - Used for network address translation
- □ mangle - Used for mangling packet headers or content
- □ filter - Used for filtering packets

LAMP Case study - Theory - Iptables - Command syntax

Commands

- □ delete
- □ flush
- □ policy
- □ append
- □ insert
- □ list
- □ zero
- □ new
- □ delete-chain
- □ rename-chain

LAMP Case study - Theory - Iptables - Command syntax

Matches

Protocol
Source
Destination
In interface
Out interface
Fragment
Source port
Destination port
TCP flags
SYN
TCP option

ICMP type
Limit
Source MAC
Mark
Multiport
Owner
State
TOS
TTL
Unclean

And much much more in patch-o-matic

LAMP Case study - Theory - Iptables - Command syntax

Targets/jumps

ACCEPT
DNAT
DROP
LOG
MARK
MASQUERADE
MIRROR
QUEUE

REDIRECT
REJECT
RETURN
SNAT
TOS
TTL
ULOG

And even more in patch-o-matic

LAMP Case study - Theory - Ipsysctl

- A virtual filesystem containing a set of structures
- Structures bound inside the kernel
- Makes it possible to configure kernel behaviour on the fly
- Done via either specific tools, or standard unix tools
  - echo, cat, ls, etc.

LAMP Case study - Theory - Ipsysctl - What is it

- Consists of two different interfaces
  - /proc filesystem
    - Can be used together with standard unix commands
    - each setting is a file
    - structured in directories
  - system calls
    - sysctl program
    - Can either use a config file, or command line
- Changes the behaviour of the kernel
  - network, filesystem, virtual memory, etc.
- The interfaces goes straight into the kernel
  - Source code is a little bit spread out throughout the kernel

LAMP Case study - Theory - Ipsysctl - Tools - sysctl

- sysctl
  - -a displays all variables and values currently used
  - -A same as -a but in table form
  - -p <conffile> loads the settings in file conffile. Default = /etc/sysctl.conf
  - -w set a single variable from command line
- Examples
  - sysctl -a
  - sysctl -p ~/gc-settings.conf
  - sysctl -w net.ipv4.neigh.default.gc_thresh3 = 4096

LAMP Case study - Theory - Ipsysctl - Tools - Unix commands

- Unix commands
  - cat - show variables
  - echo - set variables
  - ls - show variable names/files
  - cd - change place in directory structure

- Examples
  - cat /proc/sys/net/ipv4/ip_conntrack_max
  - echo 8192 > /proc/sys/net/ipv4/ip_conntrack_max
  - cd /proc/sys/net/ipv4/neigh
  - ls

LAMP Case study - Theory - Ipsysctl - Structure

- Each fundamental area has it’s own section in the sysctls
  - networking
  - devices
  - filesystems
  - virtual memory system
  - etc.

LAMP Case study - Theory - Ipsysctl - Structure

- The networking sysctls are split into sections per protocol
  - 802
  - ethernet
  - IPv4
  - IPv6
  - etc

LAMP Case study - Theory - Ipsysctl - Structure

- IPv4 structure
  - IP, TCP, UDP, ICMP, and miscellany directly in this directory
  - neigh variables, neighbour table settings
  - route variables, route table settings
  - conf variables, per device settings
  - netfilter settings, iptables/netfilter settings (with tcp-window-tracking patch)

LAMP Case study - Theory - Ipsysctl - What you can find

- What to expect in the IPv4 structure
  - timeouts
  - garbage collection timings
  - on/off switches for algorithms and functionality
  - memory usage settings

LAMP Case study - Theory - Summary

- Gone through the basics of iptables and netfilter
  - basic functionality
  - command syntax
  - usage
- and the ip sysctl’s
  - usage
  - syntax
  - structure and where to look for settings

Final notes - Other resources

http://www.frozentux.net

http://www.netfilter.org

http://www.linuxguruz.org/iptables/

http://www.islandsoft.net/veerapen.html

http://www.lartc.org

http://www.docum.org