CPR E 431

BASICS OF INFORMATION SYSTEM SECURITY

Firewall and Intrusion Prevention System

Firewalls with iptables

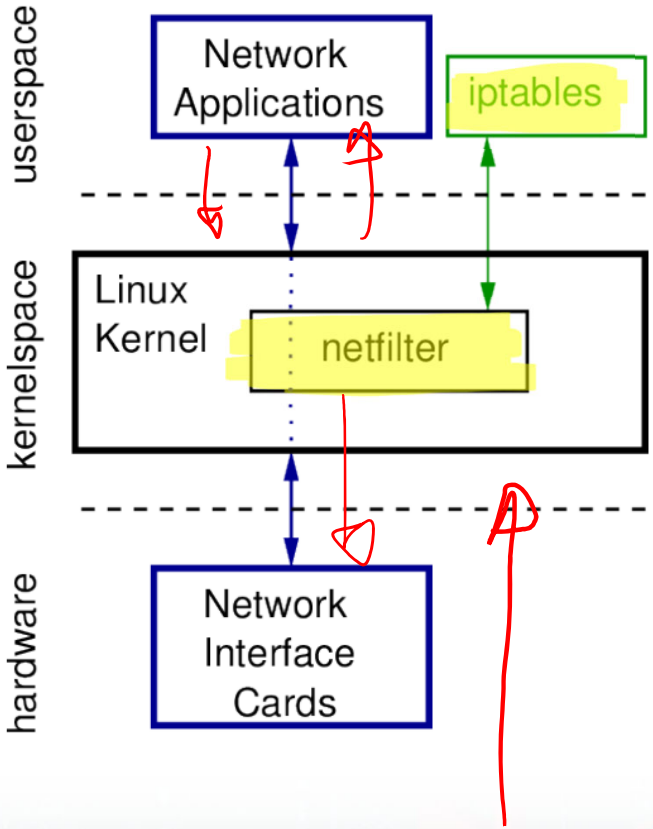
Video Summary

- Linux, netfilter, and iptables
- Iptables Concepts (tables, chains, rules)
- Common iptables syntax
- Examples and Demo

Linux, netfilter and iptables

- `netfilter`: module for filtering packets in Linux kernel
- `iptables`: user space application to manipulate packet filters of `netfilter`
- Administrator privileges needed for manipulating kernel packet filters
  - Prefix `iptables` commands with `sudo`

Linux, netfilter and iptables



iptables Concepts: Tables

- Different tables of filters (depend on kernel configuration)
- Selected using `-t` option
  - `filter`: default table (if no option used)
  - `nat`: Network Address Translation
  - `mangle`: Altering packets
  - `...`
- Tables contain chains

iptables Concepts: Chains

Different filtering rules depending on how/where packet processed by kernel

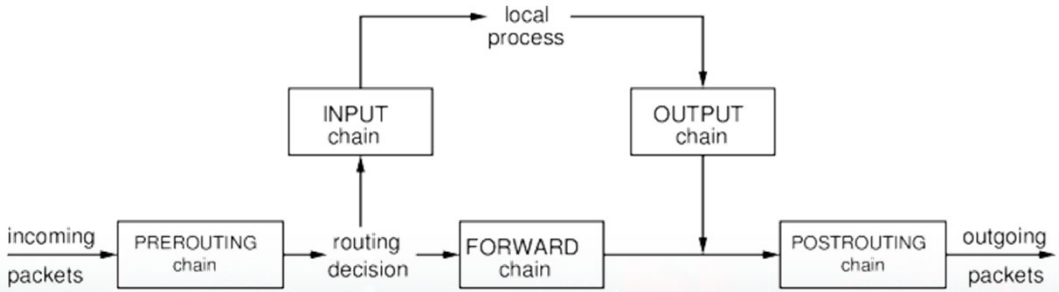
INPUT packets destined to this computer

OUTPUT packets originating from this computer

FORWARD packets being forwarded by this computer

PREROUTING altering packets as they come in to this computer (e.g. nat, mangle)

POSTROUTING altering packets as they go out of this computer (e.g. nat, mangle)



iptables Concepts: Rules

- Chains contain packet filtering rules
- Rules consist of:

  Matching condition(s) desired packet characteristics
  - protocol, source/dest. address, interface
  - many protocol specific extensions

  Target action to take if packet matches specified conditions
  - ACCEPT, DROP, RETURN, ...
- A packet is checked against rules in chain, from 1st to last
- If rule does not match, check against next rule in chain
- If rule matches, take action as specified by target

Common iptables Syntax

iptables [-t *table*] [-*operation chain*] [-p *protocol*] [-s *srcip*] [-d *dstip*] [-i *inif*] [-o *outif*] [–param1 value1 . . .] -j *target*

- *table*: `filter`, `nat`, `mangle`
- *operation*: (first uppercase letter) Append, Delete, Insert, List, Flush, Policy, . . .
- *chain*: `INPUT`, `OUPTUT`, `FORWARD`, `PREROUTING`, `POSTROUTING`
- *protocol*: `tcp`, `udp`, `icmp`, `all`, . . .
- *srcip*, *dstip*: IP address, e.g. `1.1.1.1`, `2.2.2.0/24`
- *inif*, *outif*: interface name, e.g. `eth0`
- *param*, *value*: protocol specific parameter and value
  - `sport`, `dport`, `tcp-flags`, `icmp-type`, . . .
- *target*: `ACCEPT`, `DROP`, `RETURN`, . . .

`man iptables` to see detailed syntax and parameters

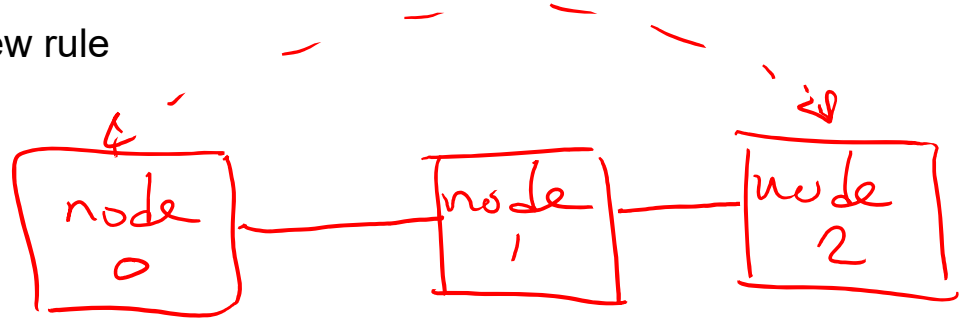
Example

Aim:

Drop all ICMP packets sent from node-0 to node-2

Design:

Assume default policy is ACCEPT
Assume filter table empty ➔ append a new rule
Packets sent ➔ FORWARD chain
Protocol is icmp
Target is DROP



Implementation

sudo iptables -A FORWARD -P icmp -j DROP

Example

Aim:

Drop all ICMP packets sent from node-0 to node-2

Design:

Assume default policy is ACCEPT
Assume filter table empty ➔ append a new rule
Packets sent ➔ FORWARD chain
Protocol is icmp
Target is DROP

Implementation

iptables –A FORWARD –p icmp –j DROP

Example

Aim:

View current rule

Implementation

iptables -L -n

iptables -L FORWARD -v

Example

Aim:

View current rule

Implementation

iptables –L –n

Or

iptables –L FORWARD -v

Example

Aim:

Drop tcp packets between node-0 and node-2

Implementation

sudo iptables -A FORWARD -p tcp -j DROP

Example

Aim:

Drop tcp packets between node-0 and node-2

Implementation

sudo iptables –A FORWARD –p tcp –j DROP

Example

Aim:

Block all packets arriving on interface eth0 and destined to ip 10.10.1.1 and then view the rules

Implementation

Introduction to iptables

s46 iptables -A FORWARD -i eth0

-d 10.10.1.1 -j DROP

Example

Aim:

Block all packets arriving on interface eth0 and destined to ip 10.10.1.1 and then view the rules

Implementation

Introduction to iptables

sudo iptables -A FORWARD -i eth0 -d 10.10.1.1 -j DROP

Example

Aim:

Prevent others from sending anything to this computer, except to the local HTTP webserver

Design

Packets received → INPUT chain
HTTP uses TCP → protocol is tcp
Web server listens on port 80 → destination port 80
Set the default policy to DROP
Target is ACCEPT

Implementation

iptables -P INPUT DROP

iptables -A INPUT -p tcp --dport 80 -j ACCEPT

Video Summary

- Linux, netfilter, and iptables
- Iptables Concepts (tables, chains, rules)
- Common iptables syntax
- Examples and Demo