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

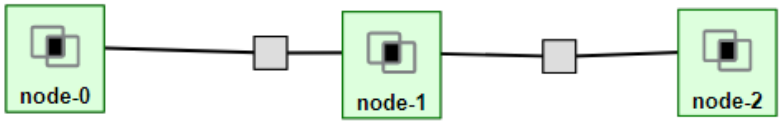
Common iptables Syntax

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

Network Toplogy



GENI Platform

Node #1:

Status	Client ID	Component ID	Expiration	Type	Hostname
READY	node-0	pc2	2020-08-08T12:03:13.000Z	default-vm	node-0.Firewall.ch-geni-net.instageni.colorado.edu
Login	ssh myoussef@pc2.instageni.colorado.edu -p 26210				
Interfaces		**MAC**		**Layer 3**	
interface-0	pc2:lo0	025f7f360197		ipv4: 10.10.1.1	

Node #2:

Status	Client ID	Component ID	Expiration	Type	Hostname
READY	node-1	pc2	2020-08-08T12:03:13.000Z	default-vm	node-1.Firewall.ch-geni-net.instageni.colorado.edu
Login	ssh myoussef@pc2.instageni.colorado.edu -p 26211				
Interfaces		**MAC**		**Layer 3**	
interface-1	pc2:lo0	0232fbf1c0a0		ipv4: 10.10.1.2	
interface-2	pc2:lo0	027c974238dd		ipv4: 10.10.2.1	

Node #3:

Status	Client ID	Component ID	Expiration	Type	Hostname
READY	node-2	pc2	2020-08-08T12:03:13.000Z	default-vm	node-2.Firewall.ch-geni-net.instageni.colorado.edu
Login	ssh myoussef@pc2.instageni.colorado.edu -p 26212				
Interfaces		**MAC**		**Layer 3**	
interface-3	pc2:lo0	02ec3d2c00d9		ipv4: 10.10.2.2	

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

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

Video Summary

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