Computer Science and Engineering Department

Group Name&Surname: Mehmet Taha USTA & Burcu ÖZTAŞ

Identity Numbers: 21527472 & 21483435

Course: BBM-465 Information Security Lab.

Experiment: Assignment 3

Subject: Firewall Configurations, Iptables

Due Date: 11/12/2019 - 23:59

Advisor: Dr. Ahmet Selman BOZKIR

1. IPTables Commands Structures

iptables [command] [chain] [parameter] [target]

1.1. IPTables Commands

A: This is the command used to add a rule to the chain.
F: Delete all of the rules in the chain.
N - Specifies to add the new process.
D: Deletes a rule in a particular chain
X - It indicates the deletion.
L - Specifies the listing process.
E - It renamed the chain.

1.2. IPTables Chains

INPUT Chain – Incoming to firewall. For packets coming to the local server.
OUTPUT Chain – Outgoing from firewall. For packets generated locally and going out of the local server.
FORWARD Chain – Packet for another NIC on the local server. For packets routed through the local server.

1.3. IPTables Parametters

d: Sets the destination hostname
i: Sets the incoming network interface, such as eth0
o: Sets the outgoing network interface
p: Sets the IP protocol for the rule
s: Sets the source for a particular packet using the same syntax as the destination (-d) parameter.
j: Jumps to the specified target when a packet matches a particular rule.
f: Applies this rule only to fragmented packets.

1.4. IPTables Targets

ACCEPT: Allows the packet to successfully move on to its destination or another chain.
DROP: Drops the packet without responding to the requester.
QUEUE: The packet is queued for handling by a user-space application.
RETURN: Stops checking the packet against rules in the current chain.
REJECT: Sends an error packet back to the remote system and drops the packet.

1.5. IPTables Protocols(-p parametter)

1.TCP 2.UDP 3.ICMP

2. Experiment

2.1. Introduction

In this experiment, we supposed to learn the use of the iptables service, which provides a firewall configuration of a device.

2.2. Tasks

Firstly we want to explain all command options which we used. Also, in every question's description part these options will be elucidated.

- -F, --flush
  This term is used to delete all the rules from all the chains.
- -F, --flush [chain]
  Flush the selected chain (all the chains in the table if none is given). This is equivalent to deleting all the rules one by one.
- -A, --append chain rule-specification
  Append one or more rules to the end of the selected chain.
- -p, --protocol protocol
  The protocol of the rule or of the packet to check.
- --icmp-type {type[/code]|typename}
  This allows specification of the ICMP type.
- -j, --jump target
  This specifies the target of the rule.
- -i, --in-interface name
  Name of an interface via which a packet was received.
- -o, --out-interface name
  Name of an interface via which a packet is going to be sent.
- -m matchname, match [per-match-options]

2.3. Questions and Answers

Question 1

In this question, Computer1 is allowed to ping Computer3. And we gave IPs to computer1 and computer3 according to given IP pool for configurations.

Commands for the computer1

```
#computer1
iptables -F
iptables -A INPUT -s 192.168.14.2 -p icmp --icmp-type echo-reply -j ACCEPT
iptables -A OUTPUT -d 192.168.14.2 -p icmp --icmp-type echo-request -j ACCEPT
```

Firstly, we deleted the all the rules which we used with –F.

Computer1 can send ping to only computer3 but also computer3 send a reply to the computer1. Therefore, we should add an OUTPUT rule and an INPUT rule for computer1.

Second command adds rule to the INPUT chain. The rule is, allow computer 3 to reply to computer1. Computer3 is the source, which we gave IP the 192.168.14.2.

• -A INPUT, Packet is going to be locally delivered the computer1 itself will be visiting this chain.
• -S 192.168.14.2, Source is the computer3 which we gave IP the 192.168.14.2.
• -p icmp, The specified protocol is icmp. The ping utility is implemented using the ICMP "Echo request" and "Echo reply" messages.
• --icmp-type echo-reply, We want a reply so we used the echo-reply type.
• - j ACCEPT, In here, we want to accept the rule so our target is ACCEPT.

Third command adds rule to the OUTPUT chain. The rule is, allow computer1 to ping to computer3, destination, we gave 192.168.14.2 IP to computer 3 which in given IP pool.

• -A OUTPUT, Packets sent from the computer1 itself will be visiting this chain.
• -d 192.168.14.2, In this question destination is computer3 which we gave IP the 192.168.14.2.
• -p icmp, The specified protocol is icmp. The ping utility is implemented using the ICMP "Echo request" and "Echo reply" messages.
• --icmp-type echo-request, We want a request so we used the echo-request type.
• - j ACCEPT, In here, we want to accept the rule so our target is ACCEPT.

And we used this commands to computer3 but src and dst IPs are set according to computer3.
Commands for the computer3

```
#computer3
iptables -A INPUT -s 192.168.6.2 -p icmp --icmp-type echo-request -j ACCEPT
iptables -A OUTPUT -d 192.168.6.2 -p icmp --icmp-type echo-reply -j ACCEPT
```

Commands for the firewall

```
#firewall
iptables -A FORWARD -s 192.168.14.2 -i eth3 -o eth2 -d 192.168.6.2 -j ACCEPT
iptables -A FORWARD -s 192.168.6.2 -i eth2 -o eth3 -d 192.168.14.2 -j ACCEPT
iptables-save
```

First command adds rule to the FORWARD chain. The rule is, allow computer3(source, 192.168.14.2) to ping computer 1(destination, 192.168.6.2).

- -A FORWARD, Packets sent from the computer3 to computer1 will be visiting this chain.
- -d 192.168.6.2, In this question destination is computer1 which we gave IP the 192.168.6.2.
- -s 192.168.14.2, Source is the computer3 which we gave IP the 192.168.14.2.
- -i eth3, The specified interface name is eth3. The packet will be received from eth3.
- -o eth2, The specified interface name is eth2. The packet will be sent to eth2.
- - j ACCEPT, In here, we want to accept the rule so our target is ACCEPT.

Second command adds rule to the FORWARD chain. The rule is, allow computer 1(source, 192.168.6.2) to ping computer 3(destination, 192.168.14.2).

- -A FORWARD, Packets sent from the Computer 1 to Computer 3 will be visiting this chain.
- -d 192.168.14.2, In this question destination is computer 3 which we gave IP the 192.168.14.2.
- -s 192.168.6.2, Source is the computer 1 which we gave IP the 192.168.6.2.
- -i eth2, The specified interface name is eth2. The packet will be received from eth2.
- -o eth3, The specified interface name is eth3. The packet will be sent to eth3.
- - j ACCEPT, In here, we want to accept the rule so our target is ACCEPT.

Last command saves rules to iptables.

Question 2

In this question, computer3 is allowed to ping all computers in LAN1.

Commands for the computer3

```
#computer3
iptables -F
ipset -N LAN1 iphash
ipset -A LAN1 192.168.14.0/24
iptables -A INPUT -m set --match-set LAN1 src -p icmp --icmp-type echo-reply-j
ACCEPT
iptables -A OUTPUT -m set --match-set LAN1 dst -p icmp --icmp-type echo-request-j
ACCEPT
```

Firstly, we deleted the all the rules which we used with –F.

Then we set up an ipset with LAN1 name in second command.

To add an IP to ipset –A option was used in third command. We add the all IP's in the LAN1 to ipset with given IP pool. When another computer will be added to LAN1, there is no need to again configuration for this computer, because of defining IP pool.

In 4th and 5th commands, -m set --match-set option was used for setting ipset for iptables. LAN1 specify the destination and source IP address.

The iphash set type uses a hash to store IP addresses.

Commands for the LAN1_computer3

```
#LAN1_computer3
ipset -N computer3 iphash
ipset -A computer3 192.168.14.2
iptables -A INPUT -m set --match-set computer3 src -p icmp --icmp-type echo-
request -j ACCEPT
iptables -A OUTPUT -m set --match-set computer3 dst -p icmp --icmp-type echo-
reply -j ACCEPT
```

Commands for the firewall

```
#firewall
ipset -N LAN1 iphash
ipset -A LAN1 192.168.14.0/24
ipset -N computer3 iphash
ipset -A computer3 192.168.14.2
iptables -A FORWARD -m set --match-set computer3 src -i eth3 -o eth3 -m set
--match-set LAN1 dst -j ACCEPT
iptables -A FORWARD -m set --match-set LAN1 src -i eth3 -o eth3 -m set --match-set
computer3 dst -j ACCEPT
iptables-save
```

Question 3

In this question, computers in LAN1 and LAN2 are allowed for only connect with Google machine.

```
#computer1
iptables -F
iptables -A INPUT -s 173.194.39.210 -j ACCEPT
iptables -A OUTPUT -d 173.194.39.210 -j ACCEPT
```

```
#computer2
iptables -A INPUT -s 173.194.39.210 -j ACCEPT
iptables -A OUTPUT -d 173.194.39.210 -j ACCEPT
```

All commands are explained before questions.

```
#computer3
iptables -A INPUT -s 173.194.39.210 -j ACCEPT
iptables -A OUTPUT -d 173.194.39.210 -j ACCEPT
```

```
#firewall
ipset -N LAN1 iphash
ipset -A LAN1 192.168.14.0/24
ipset -N LAN2 iphash
ipset -A LAN2 192.168.6.0/24
iptables -A FORWARD -m set --match-set LAN2 src -i eth2 -o eth1 -d 173.194.39.210 -j
ACCEPT
iptables -A FORWARD -s 173.194.39.210 -i eth1 -o eth2 -m set --match-set LAN2 dst
-j ACCEPT
iptables -A FORWARD -m set --match-set LAN1 src -i eth3 -o eth1 -d 173.194.39.210 -j
ACCEPT
iptables -A FORWARD -s 173.194.39.210 -i eth1 -o eth3 -m set --match-set LAN1 dst
-j ACCEPT
iptables-save
```

Question 4

In this question, we have configured the Web Server so that more than 8 computers can not access the server over https.

```
#firewall
iptables -F
iptables -A OUTPUT -o eth0 -d 192.168.1.2 -p tcp --dport 443 -m limit --limit 8/second
-j ACCEPT
iptables-save
```

--dport 443 means https port.
--limit 8/second means more than 8 computers can not access the server at the same time

Question 5

In this question, in firewall we wrote the necessary configuration for blocking the DDos attacks to mail server.

```
#firewall
iptables -F
iptables -A INPUT -o eth0 -s 192.168.1.3 -p tcp -m multiport --dports
25,110,995,143,993,465 -m limit --limit 25/minute --limit-burst 100 -j DROP
iptables-save
```

Question 6

In this question, we configured the web server for the Remote PC can access the web sites on the Apache.

```
# Apache_web_server
iptables -F
iptables -A INPUT -s 93.101.30.55 -p tcp -m multiport --dports 80, 443, 8005, 8080,
8009 -m state --state NEW,ESTABLISHED -j ACCEPT
iptables -A OUTPUT -d 93.101.30.55 -p tcp -m multiport --dports 80, 443, 8005, 8080,
8009 -m state --state ESTABLISHED -j ACCEPT
iptables-save
```

-m multiport --dports 80, 443, 8005, 8080, 8009 option used for Apache and browser ports. multiport option allows us to write more than one port.
-m state --state ESTABLISHED option allows all incoming web traffic.
ESTABLISHED meaning that the packet is associated with a connection which has seen packets in both directions.