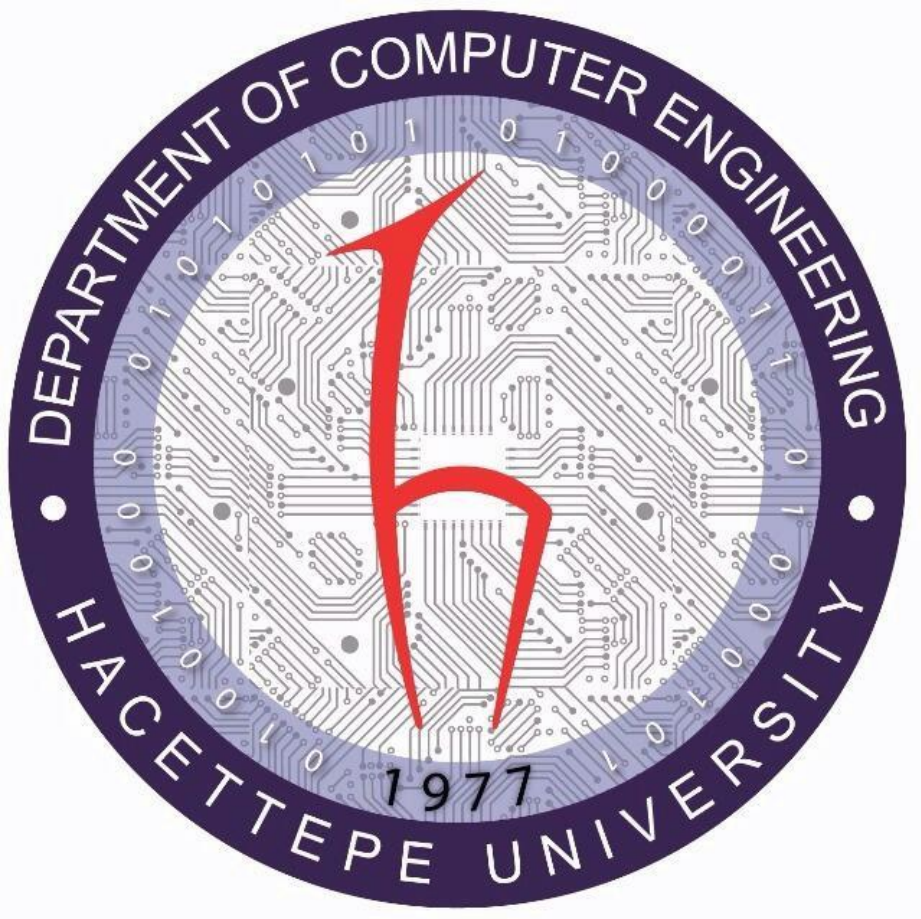
HACETTEPE UNIVERSITY DEPARTMENT OF COMPUTER ENGINEERING

BBM 465 Information Security Lab.



Assignment 4

GROUP 38

Burak Yılmaz

21627868

Yiğit Barkın Ünal

21627763

The Parameters Used In the Assignment

-F: Means flush. We are flushing the previous iptables commands.
-A: Means append. We are appending a new rule.
-o: Means output. It is for specifying the name of the interface that the packet being sent to.
-i: Means input. It is for specifying the name of the interface that the packet is received
-p: Means protocol. It is for specifying the protocol that we are using.
-m: Means match. It matches the basis of the packet on their source and destination ports.
--state: We are adding this after -m command. We want to match the state of the packet.
-j: Means jump. We are accepting or rejecting the packet.
--dport: Destination port.
--sport: Source port.

Question 1

Write the iptables configurations to enable computers in Computer Engineering Lan and Electronic Engineering Lan can communicate with each other.

```
iptables -F

(Lan 1)
Computer Engineering:
iptables -A OUTPUT -o eth1 -p all -d 192.168.10.0/24 -m state --state NEW,ESTABLISHED -j ACCEPT
iptables -A INPUT -i eth1 -p all -s 192.168.10.0/24 -m state --state NEW,ESTABLISHED -j ACCEPT

(Lan 2)
Electronic Engineering:
iptables -A OUTPUT -o eth2 -p all -d 192.168.5.0/24 -m state --state NEW,ESTABLISHED -j ACCEPT
iptables -A INPUT -i eth2 -p all -s 192.168.5.0/24 -m state --state NEW,ESTABLISHED -j ACCEPT

Firewall:
iptables -A FORWARD -i eth1 -o eth2 -p all -d 192.168.10.0/24 -m state --state ESTABLISHED -j ACCEPT
iptables -A FORWARD -i eth2 -o eth1 -p all -s 192.168.10.0/24 -m state --state ESTABLISHED -j ACCEPT
iptables -A FORWARD -i eth2 -o eth1 -p all -d 192.168.5.0/24 -m state --state ESTABLISHED -j ACCEPT
iptables -A FORWARD -i eth1 -o eth2 -p all -s 192.168.5.0/24 -m state --state ESTABLISHED -j ACCEPT
```

We started with flushing the previous commands for the iptables.

After flushing, we need to have 2 rules for each Lan: for input, and for output. Before we go on more explanation we should mention some keywords;

When we use the NEW keyword it refers to A packet requesting a new connection, such as an HTTP request.
When we use the ESTABLISHED keyword it refers to A packet that is part of an existing connection.

For output: with

- -o, we are adding the name of the interface by which a packet is being sent.
- -p, we are adding the protocol. In this case, we are making a connection for all connections.
- -d, we are adding the destination address to our iptable
- -m, matches packets on the basis of their source or destination ports,
- -j, we are accepting the packet if it matches.

For input we just changed the OUTPUT to INPUT, and -o to -i, rest is the same.

After adding the corresponding rules for Lan2 too, it's time for the firewall.

For the Firewall part,

We are adding rules for forwarding. With:

- -i, we are specifying the interface where packets are receiving.
- -o, we are specifying the interface where packets are being sent.
- —state, for this time since we are only forwarding, we are putting the established parameter.

Question 2

Write the necessary configurations for all computers inside of campus (Lan1, Lan2, Lan3) to be able to start HTTP/HTTPS communication to the Twitter and Youtube machines.

```
iptables -F

(Lan 1)
Computer Engineering:
iptables -A OUTPUT -o eth1 -p tcp --dport 80,443 -d 170.192.40.234 -m state --state NEW,ESTABLISHED -j ACCEPT
iptables -A OUTPUT -o eth1 -p tcp --dport 80,443 -d 144.188.127.195 -m state --state NEW,ESTABLISHED -j ACCEPT

iptables -A INPUT -i eth1 -p tcp --sport 80,443 -s 170.192.40.234 -m state --state NEW,ESTABLISHED -j ACCEPT
iptables -A INPUT -i eth1 -p tcp --sport 80,443 -s 144.188.127.195 -m state --state NEW,ESTABLISHED -j ACCEPT

(Lan 2)
Electronic Engineering:
iptables -A OUTPUT -o eth2 -p tcp --dport 80,443 -d 170.192.40.234 -m state --state NEW,ESTABLISHED -j ACCEPT
iptables -A OUTPUT -o eth2 -p tcp --dport 80,443 -d 144.188.127.195 -m state --state NEW,ESTABLISHED -j ACCEPT

iptables -A INPUT -i eth2 -p tcp --sport 80,443 -s 170.192.40.234 -m state --state NEW,ESTABLISHED -j ACCEPT
iptables -A INPUT -i eth2 -p tcp --sport 80,443 -s 144.188.127.195 -m state --state NEW,ESTABLISHED -j ACCEPT

(Lan 3)
Physics Engineering:
iptables -A OUTPUT -o eth3 -p tcp --dport 80,443 -d 170.192.40.234 -m state --state ESTABLISHED -j ACCEPT
iptables -A OUTPUT -o eth3 -p tcp --dport 80,443 -d 144.188.127.195 -m state --state ESTABLISHED -j ACCEPT

iptables -A INPUT -i eth3 -p tcp --sport 80,443 -s 170.192.40.234 -m state --state ESTABLISHED -j ACCEPT
iptables -A INPUT -i eth3 -p tcp --sport 80,443 -s 144.188.127.195 -m state --state ESTABLISHED -j ACCEPT

Firewall:
iptables -A FORWARD -i eth1,eth2,eth3 -o eth4 -p tcp --dport 80,443 -m state --state ESTABLISHED -d 170.192.40.234
-j ACCEPT
iptables -A FORWARD -i eth1,eth2,eth3 -o eth4 -p tcp --dport 80,443 -m state --state ESTABLISHED -d 144.188.127.195
-j ACCEPT

iptables -A FORWARD -i eth4 -o eth1,eth2,eth3 -p tcp --sport 80,443 -m state --state ESTABLISHED -s 170.192.40.234
-j ACCEPT
iptables -A FORWARD -i eth4 -o eth1,eth2,eth3 -p tcp --sport 80,443 -m state --state ESTABLISHED -s 144.188.127.195
-j ACCEPT
```

In addition to what we explained in Question 1, with:

-p, since our connections are HTTP/HTTPS we are using tcp protocol

—dport, we are specifying the destination ports. For HTTP, it's 80 and for HTTPS, it's 443

—sport, we are specifying the source ports. For HTTP, it's 80 and for HTTPS, it's 443

-i and -o, we are specifying the corresponding interface.

For Firewall, with:

-i, we are adding all the interfaces that we are receiving the packets from.

-o, we are adding the interface that we are sending the packets to.

Question 3

Write the iptables configurations to enable that all computers inside of campus (Lan1,Lan2,Lan3) and outside of campus can start HTTP/HTTPS communication to Web Server and SMTP communication to E-mail Server machine.

```
iptables -F

(Lan 1)
Computer Engineering:
iptables -A OUTPUT -o eth1 -p tcp --dport 80,443 -d 192.168.1.2 -j ACCEPT
iptables -A INPUT -i eth1 -p tcp --sport 80,443 -s 192.168.1.2 -j ACCEPT

iptables -A OUTPUT -o eth1 -p tcp --dport 25,587,465 -d 192.168.1.3 -j ACCEPT
iptables -A INPUT -i eth1 -p tcp --sport 25,587,465 -s 192.168.1.3 -j ACCEPT

(Lan 2)
Electronic Engineering:
iptables -A OUTPUT -o eth2 -p tcp --dport 80,443 -d 192.168.1.2 -j ACCEPT
iptables -A INPUT -i eth2 -p tcp --sport 80,443 -s 192.168.1.2 -j ACCEPT

iptables -A OUTPUT -o eth2 -p tcp --dport 25,587,465 -d 192.168.1.3 -j ACCEPT
iptables -A INPUT -i eth2 -p tcp --sport 25,587,465 -s 192.168.1.3 -j ACCEPT

(Lan 3)
Physics Engineering:
iptables -A OUTPUT -o eth3 -p tcp --dport 80,443 -d 192.168.1.2 -j ACCEPT
iptables -A INPUT -i eth3 -p tcp --sport 80,443 -s 192.168.1.2 -j ACCEPT

iptables -A OUTPUT -o eth3 -p tcp --dport 25,587,465 -d 192.168.1.3 -j ACCEPT
iptables -A INPUT -i eth3 -p tcp --sport 25,587,465 -s 192.168.1.3 -j ACCEPT

Firewall:
iptables -A FORWARD -i eth1,eth2,eth3 -o eth0 -p tcp --dport 80,443 -d 192.168.1.2 -j ACCEPT
iptables -A FORWARD -i eth1,eth2,eth3 -o eth0 -p tcp --dport 25,587,465 -d 192.168.1.3 -j ACCEPT

iptables -A FORWARD -i eth0 -o eth1,eth2,eth3 -p tcp --sport 80,443 -s 192.168.1.2 -j ACCEPT
iptables -A FORWARD -i eth0 -o eth1,eth2,eth3 -p tcp --sport 25,587,465 -s 192.168.1.3 -j ACCEPT
```

In addition to what's written on question 1 and question 2, with:

—dport, we are also adding the ports for SMTP protocol (25, 587, 465)

-p, the protocol is tcp for SMTP.

Question 4

Write the iptables configurations to enable that all computers inside of campus (Lan1,Lan2,Lan3) can start POP3 and IMAP communication to the Email Server machine.

```
iptables -F

(Lan 1)
Computer Engineering:
iptables -A OUTPUT -o eth1 -p tcp --dport 110,143 -d 192.168.1.3 -m state --state NEW,ESTABLISHED -j ACCEPT
iptables -A INPUT -i eth1 -p tcp --sport 110,143 -s 192.168.1.3 -m state --state NEW,ESTABLISHED -j ACCEPT

(Lan 2)
Electronic Engineering:
iptables -A OUTPUT -o eth2 -p tcp --dport 110,143 -d 192.168.1.3 -m state --state NEW,ESTABLISHED -j ACCEPT
iptables -A INPUT -o eth2 -p tcp --sport 110,143 -s 192.168.1.3 -m state --state NEW,ESTABLISHED -j ACCEPT

(Lan 3)
Physics Engineering:
iptables -A OUTPUT -o eth3 -p tcp --dport 110,143 -d 192.168.1.3 -m state --state NEW,ESTABLISHED -j ACCEPT
iptables -A INPUT -o eth3 -p tcp --sport 110,143 -s 192.168.1.3 -m state --state NEW,ESTABLISHED -j ACCEPT

Firewall:
iptables -A FORWARD -i eth1,eth2,eth3 -o eth0 -p tcp -s 192.168.5.0/24,192.168.10.0/24,192.168.25.0/24 --dport
110,143 -d 192.168.1.3 -m state --state ESTABLISHED -j ACCEPT
iptables -A FORWARD -i eth0 -o eth1,eth2,eth3 -p tcp -d 192.168.5.0/24,192.168.10.0/24,192.168.25.0/24 --sport
110,143 -s 192.168.1.3 -m state --state ESTABLISHED -j ACCEPT
```

In addition to what's written on question 1 and question 2, question 3, with:

—dport, we are also adding the ports for POP3 and IMAP protocol (110,143)

-p, the protocol is tcp for POP3 and IMAP.

Question 5

```
iptables -F

(Lan 1)
Computer Engineering:
iptables -A INPUT -i eth1 -p icmp -s 85.77.42.63 -m state --state NEW,ESTABLISHED -j ACCEPT
iptables -A OUTPUT -o eth1 -p icmp -d 85.77.42.63 -m state --state NEW,ESTABLISHED -j ACCEPT

(Lan 2)
Electronic Engineering:
iptables -A INPUT -i eth2 -p icmp -s 85.77.42.63 -m state --state NEW,ESTABLISHED -j ACCEPT
iptables -A OUTPUT -o eth2 -p icmp -d 85.77.42.63 -m state --state NEW,ESTABLISHED -j ACCEPT

(Lan 3)
Physics Engineering:
iptables -A INPUT -i eth3 -p icmp -s 85.77.42.63 -m state --state NEW,ESTABLISHED -j ACCEPT
iptables -A OUTPUT -o eth3 -p icmp -d 85.77.42.63 -m state --state NEW,ESTABLISHED -j ACCEPT

Remote Computer:
iptables -A INPUT -i eth4 -p icmp -s 192.168.5.0/24,192.168.10.0/24,192.168.25.0/24 -m state --state NEW,ESTABLISHED
-j ACCEPT
iptables -A OUTPUT -o eth4 -p icmp -d 192.168.5.0/24,192.168.10.0/24,192.168.25.0/24 -m state --state
NEW,ESTABLISHED -j ACCEPT

Firewall:
iptables -A FORWARD -i eth1,eth2,eth3 -o eth4 -p icmp -s 192.168.5.0/24,192.168.10.0/24,192.168.25.0/24 -d
85.77.42.63 -m state --state ESTABLISHED -j ACCEPT
iptables -A FORWARD -i eth4 -o eth1,eth2,eth3 -s 85.77.42.63 -p icmp -d
192.168.5.0/24,192.168.10.0/24,192.168.25.0/24 -m state --state ESTABLISHED -j ACCEPT
```

Write the necessary configurations for that the remote computer can ping computers in Computer Engineering Lan, Electronic Engineering Lan, and Physics Engineering Lan.

In addition to what's written on question 1 and question 2, question 3, question 4, with:

-p, icmp for pinging.

Question 6

Write the necessary configurations so that more than 100 computers cannot access HTTPS port of the Web Server simultaneously. (The configuration will be done on the Firewall device, not on the Web Server.)

```
iptables -F

Firewall:
iptables -A FORWARD -p tcp --syn --dport 443 -m connlimit --connlimit-upto 100 -j ACCEPT
```

In addition to what's written on question 1 and question 2, question 3, question 4, with:

—syn, only matches TCP packets with the SYN bit set and the ACK, RST, and FIN bits cleared.
-m, is for match.
connlimit, is the extended packet module name, which is connection limit.
—connlimit-upto, means match if the number of existing connections is below or equal *n*.

What is a Firewall?

A **firewall** is a software or firmware that prevents unauthorized access to a network. Broadly speaking, a computer firewall is a software program that prevents unauthorized access to or from a private network. Firewalls are tools that can be used to enhance the security of computers connected to a network, such as LAN or the Internet. They are an integral part of a comprehensive security framework for your network.

What is ip-table and what chain are they contained in?

Iptables is an extremely flexible firewall utility built for Linux operating systems. Iptables is a command-line firewall utility that uses policy chains to allow or block traffic. When a connection tries to establish itself on your system, iptables looks for a rule in its list to match it to. If it doesn't find one, it resorts to the default action.

Tables consist of chains, which are lists of rules which are followed in order. The default table, filter, contains three built-in chains: **Input**, **Output** and **Forward** which are activated at different points of the packet filtering process.Packet filtering is based on rules, which are specified by multiple matches and one target.

Input -This chain is used to control the behavior of incoming connections. For instance, if a user attempts to SSH into your PC/server, iptables will attempt to match the IP address and port to a rule in the input chain

Forward – This chain is used for incoming connections that aren't actually being delivered locally.

Output – This chain is used for outgoing connections. For instance, if you try to ping a site, iptables will check its output chain to see what the rules are regarding ping and the site before making a decision to allow or deny the connection attempt.

References :

https://personalfirewall.comodo.com/what-is-firewall.php
https://www.cyberciti.biz/tips/linux-iptables-examples.html
https://www.thegeekstuff.com/2011/06/iptables-rules-examples/
https://wiki.archlinux.org/index.php/iptables
https://serversforhackers.com/c/firewalls-basics-of-iptables
https://www.baeldung.com/linux/iptables-intro
https://iximiuz.com/en/posts/laymans-iptables-101/
https://www.tothenew.com/blog/basics-of-iptables/
http://linux-training.be/networking/ch14.html
https://www.csie.ntu.edu.tw/~b93070/CNL/v4.0/CNLv4.0.files/Page1504.htm
https://www.linode.com/docs/guides/control-network-traffic-with-iptables/