HACETTEPE UNIVERSITY
ENGINEERING DEPARTMENT
COMPUTER ENGINEERING

LESSON
BBM 465 INFORMATION SECURITY LAB.

ADVISOR
Yasin Şahin, Işıl Karabey

EXPERIMENT
Experiment 1

GROUP MEMBERS

Hasan Hüseyin TOPÇU
21228764

Taha BAŞKAK
21228104

GROUP NO
30

Contents

Technical Information

Firewall

The term firewall originally referred to a wall intended to confine a fire or potential fire within a building.Later uses refer to similar structures, such as the metal sheet separating the engine compartment of a vehicle or aircraft from the passenger compartment.Firewall technology emerged in the late 1980s when the Internet was a fairly new technology in terms of its global use and connectivity.

In computing, a firewall is a network security system, either hardware- or software-based, that the incoming and outgoing network traffic based on predetermined security rules.

Firewall have two types. That are software and hardware firewall.Other firewall have rules (There have IP addresses,domain names,protocols,ports,keywords) and logic types. Firewall logic types of filter mechanism whic are packet filter and purity , data flow consists of packets of information and firewalls analyze these packets to sniff out offensive or unwanted packets depending on what you have defined as unwanted packets, proxy, firewall assume the role of a recipient and in turn sends it to the node that has requested the information and vice versa , inspection , Firewalls instead of sifting through all of the information in the packets, mark key features in all outgoing requests & check for the same matching characteristics in the inflow to decide if it relevant information that is coming through.

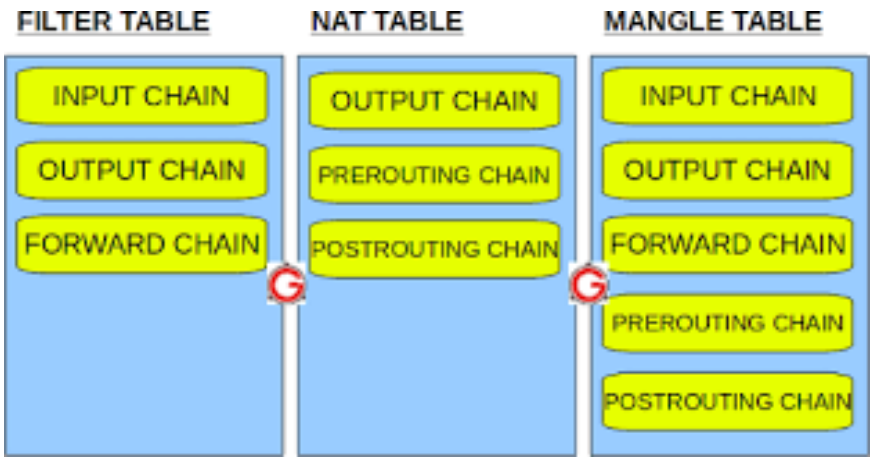
Iptables

Iptables is a user-space application program that allows a system administrator to configure the tables provided by the Linux kernel firewall and the chains and rules it stores. Other way iptables default structure of iptables is like, tables which has chains and the chains which contains rules. Iptables have tpyes table which are filter , nat , mangle tables. That tables have a lot of chain.
Chains ;
FILTER Table

INPUT Chain; Managing packet in to server , adding rules of input from connection other server.

OUTPUT Chain ; Control packet out to server , adding rulse of outgoing from connection other server.

FORWARD Chain ; Controling packer from source server to other server.


FILTER TABLE
NAT TABLE
MANGLE TABLE
INPUT CHAIN
OUTPUT CHAIN
FORWARD CHAIN
OUTPUT CHAIN
PREROUTING CHAIN
POSTROUTING CHAIN
INPUT CHAIN
OUTPUT CHAIN
FORWARD CHAIN
PREROUTING CHAIN
POSTROUTING CHAIN

Questions And Solutions

Question 1 and Solution

Question : 1 numaralı bilgisayarın sadece 3 numaralı bilgisayara ping atabilmesi için gerekli yapılandırmaları yazınız.

Solution :

Using protocol is icmp to ping.
Using icmp-type codes:
8 => echo-request
0 => echo-reply

* PC-1 Configuration *

##Filter Table OUTPUT chain

#delete existing rules that defined OUTPUT table
iptables –F OUTPUT

#sending ping request to pc-3(192.168.14.2) from pc-1(192.168.6.2)
#pc-1's ip is source, pc-3's ip is destination so pc-1 just send ping request to pc-3
iptables -A OUTPUT -p icmp --icmp-type 8 -s 192.168.6.2 -d 192.168.14.2 -j ACCEPT

#saving rules
service iptables save

##################################

##Filter Table INPUT chain

#delete existing rules that defined INPUT table
iptables -F INPUT

#receiving ping reply from pc-3(192.168.14.2)
##pc-3's ip is source, pc-1's ip is destination so pc-1 just receive ping reply from pc-3
iptables -A INPUT -p icmp --icmp-type 0 -s 192.68.14.2 -d 192.168.6.2 -j ACCEPT

#saving rules
service iptables save

* Firewall Configuration *

##Filter Table FORWARD Chain

#delete existing rules that defined FORWARD table
iptables -F FORWARD

#forward ping request that came from eth2 to eth3
iptables -A FORWARD -p icmp --icmp-type 8 -i eth2 -o eth3 -j ACCEPT

#forward ping reply that came form eth3 to eth2
iptables -A FORWARD -p icmp --icmp-type 0 -i eth3 -o eth2 -j ACCEPT

#saving rules
service iptables save

* PC-3 Configuration *

##Filter Table INPUT Chain

#delete existing rules that defined INPUT table
iptables -F INPUT

#receiving ping request from any pc
#source is 0/0 so that mean is any ip address, pc-3 receive ping request any computer because there is not constraint that just receive from pc-1.
iptables -A INPUT -p icmp –icmp-type 8 -s 0/0 -d 192.168.14.2 -j ACCEPT

#saving rules
service iptables save

###################################

##Filter Table OUTPUT Chain

#delete existing rules that defined OUTPUT table
iptables -F OUTPUT

#sending ping reply to any pc from pc-3
#destination is 0/0 so its contains pc-1's ip address
iptables -F OUTPUT -p icmp –icmp-type 0 -s 192.168.14.2 -d 0/0 -j ACCEPT

#saving rules
service iptables save

Question 2 and Solution

Question : Dış bilgisayarın Yerel Ağ 2'deki bilgisayarların hepsine ping atabilmesi için gerekli yapılandırmaları yazınız (ipset kullanılarak yapılacaktır).

Solution :

Using protocol is icmp to ping
Using icmp-type codes:
8 => echo-request
0 => echo-reply

* Creating ipset *

#creating ipset for local network 2 and add local network 2's computers ip
ipset create localNetwork2 hash:ip
ipset add localNetwork2 192.168.6.0/24

* External Computer Configuration *

##Filter Table OUTPUT Chain

#delete existing rules that defined OUTPUT table
iptables –F OUTPUT

#sending ping request to ipset of localNetwork2 these is pc-1, pc-2
#destination(dst) is localNetwork2 ipset that is all computer in local network 2
iptables -A OUTPUT -m set --match-set localNetwork2 dst -p icmp --icmp-type 8 -j ACCEPT

#saving rules
service iptables save

##################################

##Filter Table INPUT Chain

#delete existing rules that defined INPUT table
iptables -F INPUT

#receiving ping reply from ipset of localNetwork2 these is pc-1, pc-2
#source(src) is localNetwork2 ipset so pc-1 and pc-2
iptables -A INPUT -m set --match-set localNetwork2 src -p icmp --icmp-type 0 -j ACCEPT

#saving rules
service iptables save

* Firewall Configuration *

##Filter Table FORWARD Chain

#delete existing rules that defined FORWARD table
iptables -F FORWARD

#forward ping request came from eth1 to eth2
iptables -A FORWARD -p icmp --icmp-type 8 -i eth1 -o eth2 -j ACCEPT

#forward ping reply came from eth2 to eth1
iptables -A FORWARD -p icmp --icmp-type 0 -i eth2 -o eth1 -d 93.101.30.55 -j ACCEPT

#saving rules
service iptables save

* Local Network 2 Configuration *

##Filter Table INPUT Chain

#delete existing rules that defined INPUT table
iptables -F INPUT

#receiving ping request from external computer
#source(-s) is external cımputer
iptables -A INPUT -p icmp --icmp-type 8 -s 93.101.30.55 -j ACCEPT

#saving rules
service iptables save

###################################

##Filter Table OUTPUT Chain

#delete existing rules that defined OUTPUT table
iptables -F OUTPUT

#sending ping reply to external computer
#destination(-d) is external computer
iptables -F OUTPUT -p icmp --icmp-type 0 -d 93.101.30.55 -j ACCEPT

#saving rules
service iptables save

Question 3 and Solution

Question : Yerel Ağ 1 ve Yerel Ağ 2 ağlarında yer alan bilgisayarların sadece Google makinasına erişebilmesi için gerekli yapılandırmaları yazınız.

Solution :

* Local Network 1and 2 Configuration *

##Filter Table OUTPUT Chain

#delete existing rules that defined OUTPUT table
iptables -F OUTPUT

#sending connection request to google machine from local network 1 and 2
#using tcp protocol and 80 port so http
#soruces(-s) are local network 1 and 2 that its ip is given command,
#destination(-d) is google machine that its ip is given command
#use NEW key word because of this conneciton request is new, first
iptables -A OUTPUT -s 192.168.14.0/24, 192.168.6.0/24 -d 173.194.39.210 -p tcp --dport 80 -m state --state NEW,ESTABLISHED -j ACCEPT

#saving rules
service iptables save

##################################

##Filter Table INPUT Chain

#delete existing rules that defined INPUT table
iptables -F INPUT

receiving connection reply from google machine by use soruce port is 80 and there is not NEW key word
iptables -A INPUT -s 173.194.39.210 -d 192.168.14.0/24, 192.168.6.0/24 -p tcp --sport 80 -m state --state ESTABLISHED -j ACCEPT

#saving rules
service iptables save

* Firewall Configuration *

##Filter Table FORWARD Chain

#delete existing rules that defined FORWARD table
iptables -F FORWARD

#forward conneciton request came from eth2 and eth3 to eth1 but just one ip that -d = 173.194.39.210
iptables -A FORWARD -p tcp --dport 80 -i eth2, eth3 -o eth1 -d 173.194.39.210 -m state --state NEW,ESTABLISHED -j ACCEPT

#forward connection reply came from eth1to eth2 and eth3
iptables -A FORWARD -p tcp --sport 80 -i eth1 -o eth2,eth3 -s 173.194.39.210 -m state --state ESTABLISHED -j ACCEPT

#saving rules
service iptables save

* Google Configuration *

##Filter Table INPUT Table

#delete existing rules that defined INPUT table
iptables -F INPUT

#google machine receive conneciton request came from local network 1 and 2
#this action is first, new because of using NEW key world
iptables -A INPUT -s 192.168.14.0/24, 192.168.6.0/24 -d 173.194.39.210 -p tcp --dport 80 -m state --state NEW, ESTABLISHED -j ACCEPT

#saving rules
service iptables save

##################################

##Filter Table OUTPUT Table

#delete existing rules that defined OUTPUT table
iptables -F OUTPUT

#google macihne send conneciton reply to computers of local network 1 and 2
iptables -A OUTPUT -s 173.194.39.210 -d 192.168.14.0/24, 192.168.6.0/24 -p tcp –sport 80 -m state –state ESTABLISHED -j ACCEPT

#saving rules
service iptables save

Question 4 and Solution

Quesiton : Web Sunucusuna https üzerinden 12'den fazla bilgisayarın aynı anda erişememesi için gerekli yapılandırmaları yazınız. (Yapılandırma Web Sunucusunda değil Güvenlik Duvarı cihazında yapılacaktır.)

Solution :

* Firewall Configuration *

##Filter Table FORWARD Chain

#delete existing rules that defined FORWARD table
iptables -F FORWARD

#drop access request outgoing interface o eth0 and destination ip is 192.168.1.2(web server) if exceed the limit that 12
#destination port is 443 that is https's port number
iptables -A FORWARD -o eth0 -p tcp --dport 443 --syn -d 192.168.1.2 -m connlimit --connlimit-above 12 –connlimit-mask 0 -j DROP

#forward access request to outgoing eth0
iptables -A FORWARD -o eth0 -d 192.168.1.2 -p tcp --dport 443 -m state --state NEW,ESTABLISHED -j ACCEPT

#forward access reply came from eth0
iptables -A FORWARD -i eth0 -s 192.168.1.2 -p tcp --sport 443 -m state --state ESTABLISHED -j ACCEPT

#saving rules
service iptables save

* Web Server Configuration *

##Filter Table INPUT Chain

#delete existing rules that defined INPUT table
iptables -F INPUT

receiving access request came from any commputer to web server by used 443(https) port
iptables -A INPUT -s 0/0 -d 192.168.1.2 -p tcp --dport 443 -m state --state NEW, ESTABLISHED -j ACCEPT

#saving rules
service iptables save

###################################

##Filter Table OUTPUT Chain

#delete existing rules that defined OUTPUT table
iptables -F OUTPUT

#sending access reply to any computer from web server by used 443(https) port number
iptables -A OUTPUT -s 192.168.1.2 -d 0/0 -p tcp --sport 443 -m state --state ESTABLISHED -j ACCEPT

#saving rules
service iptables save

Question 5 and Solution

Quesiton : Posta Sunucusunda dos atağın engellenmesi için gerekli yapılandırmaları yazınız. (Yapılandırma Posta Sunucusunda değil Güvenlik Duvarı cihazında yapılacaktır.)

Solution :

* Firewall Configuration *

##Filter Table FORWARD Chain

#delete existing rules that defined OUTPUT table
iptables -F FORWARD

#--limit 25/minute => Maximum average matching rate in minute
#--limit-burst 100 => Maximum initial number of packets to match
#if does not provide these constraints then drop
iptables -A FORWARD -o eth0 -d 192.168.1.3 -p tcp -m multiport --dports 25,2525,587,110,143,465,587,2526 -m limit --limit 25/minute --limit-burst 100 -j DROP

#forward request outgoing eth0
#mail server's port numbers are 25,110,995,143,993,465
iptables -A FORWARD -o eth0 -d 192.168.1.3 -p tcp --dport 25,110,995,143,993,465 -m state --state NEW,ESTABLISHED -j ACCEPT

#forward reply came from eth0
iptables -A FORWARD -i eth0 -s 192.168.1.3 -p tcp --sport 25,110,995,143,993,465 -m state --state ESTABLISHED -j ACCEPT

#saving rules
service iptables save

Question 6 and Solution

Quesiton : Web Sunucusu olarak Tomcat bulunmaktadır. 3 nolu bilgisayarın web tarayıcısından Tomcat üzerinde bulunan web sitelerine erişebilmek için Web Sunucusunda yapılması gereken yapılandırmayı yazınız. (3 nolu bilgisayar ve paketleri yönlendiren güvenlik duvarı ile ilgili bir yapılandırma yapılmayacaktır.) (Web tarayıcısının ve tomcat sunucusunun kullandığı portların bulunması gerekmektedir.)

Solution :

* Web Server Configuration *

##Filter Table OUTPUT Chain

#delete existing rules that defined OUTPUT table
iptables -F OUTPUT

#sending access reply to pc-3 from web server
#using tcp protocol and ports number are 8080,8007,8009,8085,8443,80 that are tomcat's posts
iptables -A OUTPUT -d 192.168.14.2 -p tcp --dport 8080,8007,8009,8085,8443,80 -m state --state ESTABLISHED -j ACCEPT

#saving rules
service iptables save

##################################

##Filter Table INPUT Chain

#delete existing rules that defined INPUT table
iptables -F INPUT

#receiving access requeset came from pc-3 with used tomcat's ports
iptables -A INPUT -s 192 .168.14.2 -p tcp --sport 8080,8007,8009,8085,8443,80 -m state --state NEW,ESTABLISHED -j ACCEPT

#saving rules
service iptables save

References

https://javapipe.com/iptables-ddos-protection
http://www.karlrupp.net/en/computer/nat_tutorial
http://www.netfilter.org/documentation/HOWTO/NAT-HOWTO-6.html
http://ipset.netfilter.org/iptables.man.html
http://www.thegeekstuff.com/2011/06/iptables-rules-examples
https://wiki.archlinux.org/index.php/Ipset
http://ipset.netfilter.org/ipset.man.html
http://www.linuxjournal.com/content/advanced-firewall-configurations-ipset?page=0,2
https://crybit.com/iptables-rules-for-icmp/
http://www.cyberciti.biz/tips/linux-iptables-9-allow-icmp-ping.html
http://www.computernetworkingnotes.com/manage-system-security/how-to-use-iptables-commands.html
https://tr.wikipedia.org/wiki/Iptables
http://web.mit.edu/rhel-doc/4/RH-DOCS/rhel-sg-en-4/s1-firewall-ipt-basic.html
http://serverfault.com/questions/475717/iptables-block-incoming-on-eth1-and-allow-all-from-eth0
http://www.cyberciti.biz/tips/linux-iptables-9-allow-icmp-ping.html
https://ubuntuforums.org/showthread.php?t=1431990
https://crybit.com/iptables-rules-for-icmp/
http://serverfault.com/questions/209140/iptables-how-to-drop-incoming-pings-from-host-but-allow-ping-response
http://www.cyberciti.biz/tips/linux-iptables-9-allow-icmp-ping.html