

Lab Assignment 10

Aim: To study and configure Firewalls using IP tables

LO Attainment : **LO6**

Firewall:

A firewall is a system designed to prevent unauthorized access to or from a private network. You can implement a firewall in either hardware or software form, or a combination of both. Generally the firewall has two network interfaces: one for the external side of the network, one for the internal side. Its purpose is to control what traffic is allowed to traverse from one side to the other. As the most basic level, firewalls can block traffic intended for particular IP addresses or server ports.

TCP network traffic moves around a network in packets, which are containers that consist of a packet header—this contains control information such as source and destination addresses, and packet sequence information—and the data (also known as a payload). While the control information in each packet helps to ensure that its associated data gets delivered properly, the elements it contains also provides firewalls a variety of ways to match packets against firewall rules.

Types of Firewalls

Three basic types of network firewalls: packet filtering (stateless), stateful, and application layer.

Packet filtering, or stateless, firewalls work by inspecting individual packets in isolation. As such, they are unaware of connection state and can only allow or deny packets based on individual packet headers.

Stateful firewalls are able to determine the connection state of packets, which makes them much more flexible than stateless firewalls. They work by collecting related packets until the connection state can be determined before any firewall rules are applied to the traffic.

AMAN SINGH
T23, 128

Application firewalls go one step further by analyzing the data being transmitted, which allows network traffic to be matched against firewall rules that are specific to individual services or applications. These are also known as proxy-based firewalls.

```
lab1004@MUM131: ~  
^C  
--- 192.168.92.17 ping statistics ---  
16 packets transmitted, 16 received, 0% packet loss, time 14999ms  
rtt min/avg/max/mdev = 0.108/0.176/0.251/0.033 ms  
lab1004@MUM131:~$ sudo iptables -L  
[sudo] password for lab1004:  
Chain INPUT (policy ACCEPT)  
target prot opt source destination  
  
Chain FORWARD (policy ACCEPT)  
target prot opt source destination  
  
Chain OUTPUT (policy ACCEPT)  
target prot opt source destination  
lab1004@MUM131:~$ clear  
  
lab1004@MUM131:~$ iptables -L  
iptables v1.4.21: can't initialize iptables table 'filter': Permission denied (y  
ou must be root)  
Perhaps iptables or your kernel needs to be upgraded.  
lab1004@MUM131:~$ sudo iptables -L  
[sudo] password for lab1004:  
Chain INPUT (policy ACCEPT)  
target prot opt source destination  
  
Chain FORWARD (policy ACCEPT)  
target prot opt source destination  
  
Chain OUTPUT (policy ACCEPT)  
target prot opt source destination  
lab1004@MUM131:~$
```

```
lab1004@MUM131: ~  
[sudo] password for lab1004:  
Chain INPUT (policy ACCEPT)  
target prot opt source destination  
  
Chain FORWARD (policy ACCEPT)  
target prot opt source destination  
  
Chain OUTPUT (policy ACCEPT)  
target prot opt source destination  
lab1004@MUM131:~$ clear  
  
lab1004@MUM131:~$ iptables -L  
iptables v1.4.21: can't initialize iptables table 'filter': Permission denied (y  
ou must be root)  
Perhaps iptables or your kernel needs to be upgraded.  
lab1004@MUM131:~$ sudo iptables -L  
[sudo] password for lab1004:  
Chain INPUT (policy ACCEPT)  
target prot opt source destination  
  
Chain FORWARD (policy ACCEPT)  
target prot opt source destination  
  
Chain OUTPUT (policy ACCEPT)  
target prot opt source destination  
lab1004@MUM131:~$ sudo iptables -A INPUT -p tcp --dport ssh -j ACCEPT  
[sudo] password for lab1004:  
lab1004@MUM131:~$ sudo iptables -L  
[sudo] password for lab1004:  
Chain INPUT (policy ACCEPT)  
target prot opt source destination  
ACCEPT tcp -- anywhere anywhere tcp dpt:ssh  
  
Chain FORWARD (policy ACCEPT)  
target prot opt source destination  
  
Chain OUTPUT (policy ACCEPT)  
target prot opt source destination  
lab1004@MUM131:~$
```

AMAN SINGH
T23, 128

```
lab1004@MUM131: ~  
ou must be root)  
Perhaps iptables or your kernel needs to be upgraded.  
lab1004@MUM131:~$ sudo iptables -L  
sudo: unable to resolve host MUM131  
[sudo] password for lab1004:  
Chain INPUT (policy ACCEPT)  
target    prot opt source                destination  
  
Chain FORWARD (policy ACCEPT)  
target    prot opt source                destination  
  
Chain OUTPUT (policy ACCEPT)  
target    prot opt source                destination  
lab1004@MUM131:~$ sudo iptables -A INPUT -p tcp --dport ssh -j ACCEPT  
sudo: unable to resolve host MUM131  
lab1004@MUM131:~$ sudo iptables -L  
sudo: unable to resolve host MUM131  
Chain INPUT (policy ACCEPT)  
target    prot opt source                destination  
ACCEPT    tcp  --  anywhere              anywhere            tcp dpt:ssh  
  
Chain FORWARD (policy ACCEPT)  
target    prot opt source                destination  
  
Chain OUTPUT (policy ACCEPT)  
target    prot opt source                destination  
lab1004@MUM131:~$ sudo iptables -A INPUT -p tcp --dport 80 -j ACCEPT  
sudo: unable to resolve host MUM131  
lab1004@MUM131:~$ sudo iptables -L  
sudo: unable to resolve host MUM131  
Chain INPUT (policy ACCEPT)  
target    prot opt source                destination  
ACCEPT    tcp  --  anywhere              anywhere            tcp dpt:ssh  
ACCEPT    tcp  --  anywhere              anywhere            tcp dpt:http  
  
Chain FORWARD (policy ACCEPT)  
target    prot opt source                destination  
  
Chain OUTPUT (policy ACCEPT)  
target    prot opt source                destination  
lab1004@MUM131:~$
```

```
Terminal  
lab1004@MUM131: ~  
target    prot opt source                destination  
  
Chain OUTPUT (policy ACCEPT)  
target    prot opt source                destination  
lab1004@MUM131:~$  
lab1004@MUM131:~$  
lab1004@MUM131:~$  
lab1004@MUM131:~$ sudo iptables -A INPUT -j DROP  
sudo: unable to resolve host MUM131  
lab1004@MUM131:~$ sudo iptables -L  
sudo: unable to resolve host MUM131  
Chain INPUT (policy ACCEPT)  
target    prot opt source                destination  
ACCEPT    tcp  --  anywhere              anywhere            tcp dpt:ssh  
ACCEPT    tcp  --  anywhere              anywhere            tcp dpt:http  
DROP      all  --  anywhere              anywhere  
DROP      all  --  anywhere              anywhere  
  
Chain FORWARD (policy ACCEPT)  
target    prot opt source                destination  
  
Chain OUTPUT (policy ACCEPT)  
target    prot opt source                destination  
lab1004@MUM131:~$  
normal.java  
Iptables Lab4  
zip  
SimSANS_v4_20110412_4016b.zip  
num.html  
SimSANS_v4_20110412_4016b.zip.lnk  
otp.html
```

AMAN SINGH

T23, 128

```
lab1004@MUM131: ~  
target      prot opt source      destination  
Chain OUTPUT (policy ACCEPT)  
target      prot opt source      destination  
lab1004@MUM131:~$  
lab1004@MUM131:~$  
lab1004@MUM131:~$  
lab1004@MUM131:~$ sudo iptables -A INPUT -j DROP  
sudo: unable to resolve host MUM131  
lab1004@MUM131:~$ sudo iptables -L  
sudo: unable to resolve host MUM131  
Chain INPUT (policy ACCEPT)  
target      prot opt source      destination  
ACCEPT      tcp  --  anywhere    anywhere     tcp dpt:ssh  
ACCEPT      tcp  --  anywhere    anywhere     tcp dpt:http  
DROP        all  --  anywhere    anywhere  
DROP        all  --  anywhere    anywhere  
Chain FORWARD (policy ACCEPT)  
target      prot opt source      destination  
Chain OUTPUT (policy ACCEPT)  
target      prot opt source      destination  
lab1004@MUM131:~$ sudo iptables -I INPUT 1 -i lo -j ACCEPT  
sudo: unable to resolve host MUM131  
lab1004@MUM131:~$ sudo iptables -L  
sudo: unable to resolve host MUM131  
Chain INPUT (policy ACCEPT)  
target      prot opt source      destination  
ACCEPT      all  --  anywhere    anywhere  
ACCEPT      tcp  --  anywhere    anywhere     tcp dpt:ssh  
ACCEPT      tcp  --  anywhere    anywhere     tcp dpt:http  
DROP        all  --  anywhere    anywhere  
DROP        all  --  anywhere    anywhere  
Chain FORWARD (policy ACCEPT)  
target      prot opt source      destination  
Chain OUTPUT (policy ACCEPT)  
target      prot opt source      destination  
lab1004@MUM131:~$
```

```
lab1004@MUM131: ~  
DROP        all  --  anywhere    anywhere  
DROP        all  --  anywhere    anywhere  
Chain FORWARD (policy ACCEPT)  
target      prot opt source      destination  
Chain OUTPUT (policy ACCEPT)  
target      prot opt source      destination  
lab1004@MUM131:~$ sudo iptables -I INPUT 1 -i lo -j ACCEPT  
sudo: unable to resolve host MUM131  
lab1004@MUM131:~$ sudo iptables -L  
sudo: unable to resolve host MUM131  
Chain INPUT (policy ACCEPT)  
target      prot opt source      destination  
ACCEPT      all  --  anywhere    anywhere  
ACCEPT      tcp  --  anywhere    anywhere     tcp dpt:ssh  
ACCEPT      tcp  --  anywhere    anywhere     tcp dpt:http  
DROP        all  --  anywhere    anywhere  
DROP        all  --  anywhere    anywhere  
Chain FORWARD (policy ACCEPT)  
target      prot opt source      destination  
Chain OUTPUT (policy ACCEPT)  
target      prot opt source      destination  
lab1004@MUM131:~$ sudo iptables -L -v  
sudo: unable to resolve host MUM131  
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)  
pkts bytes target      prot opt in      out     source    destination  
140 9376 ACCEPT     tcp  --  lo      any     anywhere  anywhere  
0 0 ACCEPT     tcp  --  any     any     anywhere  anywhere  
0 0 ACCEPT     tcp  --  any     any     anywhere  anywhere  
509 111K DROP      all  --  any     any     anywhere  anywhere  
0 0 DROP      all  --  any     any     anywhere  anywhere  
Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)  
pkts bytes target      prot opt in      out     source    destination  
Chain OUTPUT (policy ACCEPT 420 packets, 29783 bytes)  
pkts bytes target      prot opt in      out     source    destination  
lab1004@MUM131:~$
```


AMAN SINGH
T23, 128

```
lab1004@MUM131: ~  
DROP      all -- anywhere          anywhere  
  
Chain FORWARD (policy ACCEPT)  
target    prot opt source          destination  
  
Chain OUTPUT (policy ACCEPT)  
target    prot opt source          destination  
lab1004@MUM131:~$ sudo iptables -L -v  
sudo: unable to resolve host MUM131  
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)  
pkts bytes target    prot opt in     out     source          destination  
140  9376 ACCEPT    all  --  lo      any      anywhere        anywhere  
0    0 ACCEPT    tcp  --  any    any      anywhere        anywhere        tcp dpt:ssh  
0    0 ACCEPT    tcp  --  any    any      anywhere        anywhere        tcp dpt:http  
509 111K DROP     all  --  any    any      anywhere        anywhere  
0    0 DROP     all  --  any    any      anywhere        anywhere  
  
Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)  
pkts bytes target    prot opt in     out     source          destination  
  
Chain OUTPUT (policy ACCEPT 420 packets, 29783 bytes)  
pkts bytes target    prot opt in     out     source          destination  
lab1004@MUM131:~$ sudo iptables -A INPUT -p icmp -j ACCEPT  
sudo: unable to resolve host MUM131  
lab1004@MUM131:~$ sudo iptables -L  
sudo: unable to resolve host MUM131  
Chain INPUT (policy ACCEPT)  
target    prot opt source          destination  
ACCEPT    all  --  anywhere        anywhere  
ACCEPT    tcp  --  anywhere        anywhere        tcp dpt:ssh  
ACCEPT    tcp  --  anywhere        anywhere        tcp dpt:http  
DROP      all  --  anywhere        anywhere  
DROP      all  --  anywhere        anywhere  
ACCEPT    icmp --  anywhere        anywhere  
  
Chain FORWARD (policy ACCEPT)  
target    prot opt source          destination  
  
Chain OUTPUT (policy ACCEPT)  
target    prot opt source          destination  
lab1004@MUM131:~$
```

```
lab1004@MUM131: ~  
ACCEPT     tcp  --  anywhere        anywhere        tcp dpt:ssh  
ACCEPT     tcp  --  anywhere        anywhere        tcp dpt:http  
DROP       all  --  anywhere        anywhere  
DROP       all  --  anywhere        anywhere  
ACCEPT     icmp --  anywhere        anywhere  
  
Chain FORWARD (policy ACCEPT)  
target    prot opt source          destination  
  
Chain OUTPUT (policy ACCEPT)  
target    prot opt source          destination  
lab1004@MUM131:~$ ping 192.168.92.17  
PING 192.168.92.17 (192.168.92.17) 56(84) bytes of data.  
  
^C  
--- 192.168.92.17 ping statistics ---  
89 packets transmitted, 0 received, 100% packet loss, time 88703ms  
  
lab1004@MUM131:~$ ping 192.168.92.17  
PING 192.168.92.17 (192.168.92.17) 56(84) bytes of data.  
  
^C  
--- 192.168.92.17 ping statistics ---  
8 packets transmitted, 0 received, 100% packet loss, time 7056ms  
  
lab1004@MUM131:~$ sudo iptables -F  
sudo: unable to resolve host MUM131  
lab1004@MUM131:~$ sudo iptables -L  
sudo: unable to resolve host MUM131  
Chain INPUT (policy ACCEPT)  
target    prot opt source          destination  
  
Chain FORWARD (policy ACCEPT)  
target    prot opt source          destination  
  
Chain OUTPUT (policy ACCEPT)  
target    prot opt source          destination  
lab1004@MUM131:~$
```

AMAN SINGH

T23, 128

```
lab1004@MUM131: ~  
target      prot opt source      destination  
Chain OUTPUT (policy ACCEPT)  
target      prot opt source      destination  
lab1004@MUM131:~$ ping 192.168.92.17  
PING 192.168.92.17 (192.168.92.17) 56(84) bytes of data.  
64 bytes from 192.168.92.17: icmp_seq=1 ttl=64 time=0.167 ms  
64 bytes from 192.168.92.17: icmp_seq=2 ttl=64 time=0.166 ms  
64 bytes from 192.168.92.17: icmp_seq=3 ttl=64 time=0.150 ms  
64 bytes from 192.168.92.17: icmp_seq=4 ttl=64 time=0.179 ms  
64 bytes from 192.168.92.17: icmp_seq=5 ttl=64 time=0.170 ms  
64 bytes from 192.168.92.17: icmp_seq=6 ttl=64 time=0.175 ms  
64 bytes from 192.168.92.17: icmp_seq=7 ttl=64 time=0.154 ms  
^C  
--- 192.168.92.17 ping statistics ---  
7 packets transmitted, 7 received, 0% packet loss, time 6000ms  
rtt min/avg/max/mdev = 0.150/0.165/0.179/0.019 ms  
lab1004@MUM131:~$ sudo iptables -A INPUT -p icmp DROP  
sudo: unable to resolve host MUM131  
Bad argument 'DROP'  
Try 'iptables -h' or 'iptables --help' for more information.  
lab1004@MUM131:~$ sudo iptables -A INPUT -p icmp -j DROP  
sudo: unable to resolve host MUM131  
lab1004@MUM131:~$ sudo iptables -L  
sudo: unable to resolve host MUM131  
Chain INPUT (policy ACCEPT)  
target      prot opt source      destination  
DROP        icmp -- anywhere anywhere  
Chain FORWARD (policy ACCEPT)  
target      prot opt source      destination  
Chain OUTPUT (policy ACCEPT)  
target      prot opt source      destination  
lab1004@MUM131:~$ ping 192.168.92.17  
PING 192.168.92.17 (192.168.92.17) 56(84) bytes of data.  
^C  
--- 192.168.92.17 ping statistics ---  
14 packets transmitted, 0 received, 100% packet loss, time 13000ms  
lab1004@MUM131:~$
```

```
lab1004@MUM131: ~  
Chain FORWARD (policy ACCEPT)  
target      prot opt source      destination  
Chain OUTPUT (policy ACCEPT)  
target      prot opt source      destination  
lab1004@MUM131:~$ ping 192.168.92.17  
PING 192.168.92.17 (192.168.92.17) 56(84) bytes of data.  
^C  
--- 192.168.92.17 ping statistics ---  
14 packets transmitted, 0 received, 100% packet loss, time 13000ms  
lab1004@MUM131:~$ ^C  
lab1004@MUM131:~$ ^C  
lab1004@MUM131:~$ sudo iptables -A OUTPUT -p icmp -j DROP  
sudo: unable to resolve host MUM131  
lab1004@MUM131:~$ sudo iptables -L  
sudo: unable to resolve host MUM131  
Chain INPUT (policy ACCEPT)  
target      prot opt source      destination  
DROP        icmp -- anywhere anywhere  
Chain FORWARD (policy ACCEPT)  
target      prot opt source      destination  
Chain OUTPUT (policy ACCEPT)  
target      prot opt source      destination  
DROP        icmp -- anywhere anywhere  
lab1004@MUM131:~$ ping 192.168.92.17  
PING 192.168.92.17 (192.168.92.17) 56(84) bytes of data.  
ping: sendmsg: Operation not permitted  
ping: sendmsg: Operation not permitted  
ping: sendmsg: Operation not permitted  
ping: sendmsg: Operation not permitted  
ping: sendmsg: Operation not permitted  
ping: sendmsg: Operation not permitted  
^C  
--- 192.168.92.17 ping statistics ---  
7 packets transmitted, 0 received, 100% packet loss, time 6047ms  
lab1004@MUM131:~$
```

AMAN SINGH
T23, 128

```
lab1004@MUM131: ~  
DROP      icmp -- anywhere          anywhere  
ACCEPT    icmp -- anywhere          anywhere  
lab1004@MUM131:~$ sudo iptables -F  
sudo: unable to resolve host MUM131  
lab1004@MUM131:~$ ping 192.168.92.17  
PING 192.168.92.17 (192.168.92.17) 56(84) bytes of data.  
64 bytes from 192.168.92.17: icmp_seq=1 ttl=64 time=0.133 ms  
64 bytes from 192.168.92.17: icmp_seq=2 ttl=64 time=0.115 ms  
64 bytes from 192.168.92.17: icmp_seq=3 ttl=64 time=0.119 ms  
64 bytes from 192.168.92.17: icmp_seq=4 ttl=64 time=0.136 ms  
64 bytes from 192.168.92.17: icmp_seq=5 ttl=64 time=0.133 ms  
^C  
--- 192.168.92.17 ping statistics ---  
5 packets transmitted, 5 received, 0% packet loss, time 3999ms  
rtt min/avg/max/mdev = 0.115/0.127/0.136/0.011 ms  
lab1004@MUM131:~$ sudo iptables -A INPUT -p tcp -j DROP  
sudo: unable to resolve host MUM131  
lab1004@MUM131:~$ sudo iptables -L  
sudo: unable to resolve host MUM131  
Chain INPUT (policy ACCEPT)  
target    prot opt source                destination  
DROP      tcp  -- anywhere              anywhere  
  
Chain FORWARD (policy ACCEPT)  
target    prot opt source                destination  
  
Chain OUTPUT (policy ACCEPT)  
target    prot opt source                destination  
lab1004@MUM131:~$ sudo iptables -F  
sudo: unable to resolve host MUM131  
lab1004@MUM131:~$ sudo iptables -L  
sudo: unable to resolve host MUM131  
Chain INPUT (policy ACCEPT)  
target    prot opt source                destination  
  
Chain FORWARD (policy ACCEPT)  
target    prot opt source                destination  
  
Chain OUTPUT (policy ACCEPT)  
target    prot opt source                destination  
lab1004@MUM131:~$
```

Conclusion :-

We have successfully learned and implemented the concept of firewalls, we learned to see content of iptables ,get more details of the table, append new rules for packet filtration, dropping and blocking the packets of specific protocol, etc.