Practical Computer Networks and Application

Firewalls and iptables

Summer Term 2020

Prof. Dr. Christian Baun
Henry-Norbert Cocos
Maurizio Petrozziello
{christianbaun,cocos,petrozziello}@fb2.fra-uas.de

Computer Science
Faculty of Computer Science and Engineering
Frankfurt University of Applied Sciences

Content

1. Introduction
2. Firewalls
3. `iptables`
4. References

Introduction

In the last Lab Exercise you did the following things:

- **Set up a Network using Linux**
- **Configuring a Gateway for a Network**
- **Configuring Clients in the Network**

Introduction

In this Lab Exercise we will learn the following things:

- **What Firewalls are and how they work**
- **How a packet filter works**
- **Some basic things about** `iptables`

After this Lab Exercise

After you solved this Lab Exercise you have some basic knowledge about packet filters and `iptables`. This knowlegde will help you to understand security issues in Computer Networks!

Security Hazards in IP-based Networks

IP-based networks are vulnerable to some risks [1]:

- **Denial of Service Attacks (DoS)** [2] – An Attack on a Server that makes the Service unavailable
- **MAC-Spoofing** – Changing the MAC-Address to a valid MAC-Address in a private Network
- **IP-Spoofing** [3] – Changing the Sender Address in IP-Packets to a different IP-Address

MAC-Spoofing

Changing the MAC-Address in Linux is a simple task.

Simply issue the following commands [4]:

```
/etc/init.d/networking stop
ifconfig eth0 hw ether <MAC-ADDRESS>
/etc/init.d/networking start
```

Firewalls

There are different types of Firewalls:

- **Personal (Desktop) Firewall** [5, 6] – Software solution installed on a computer that secures the Networking services
- **Hardware (Network) Firewall** [7] – A Hardware component that secures two different networks
- **Packet Filter** [1] – Checks the IP-Addresses and Ports by inspecting the Header information of each packet
- **Application Layer Firewall** [8] – Checks the protocol information of packets but also its payload

[1] This topic will be discussed in this Slide Set

Personal and Network Firewalls

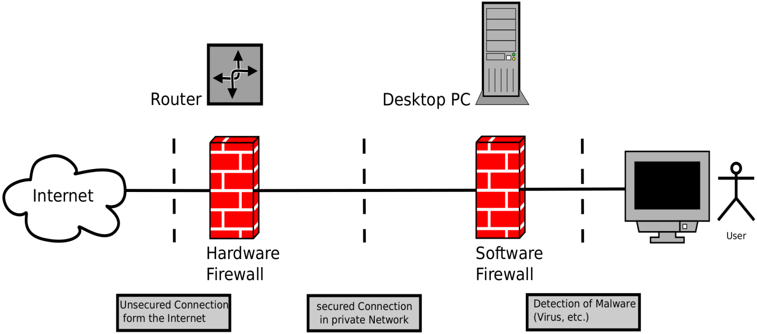

Router
Desktop PC
Internet
Hardware Firewall
Software Firewall
User
Unsecured Connection form the Internet
secured Connection in private Network
Detection of Malware (Virus, etc.)

Figure: Diagram of a Personal and a Network Firewall

Personal and Network Firewalls

Personal Firewalls [5, 6]:

- Secures the Computer from Malware
- Monitors Network Services provided by the Computer
- Checks incomming and outgoing Requests by Services

Network Firewalls [7]:

- Logically seperates two Networks (WAN from LAN)
- Monitors connections from the Internet to the private Network and vice versa

Application Layer Firewall

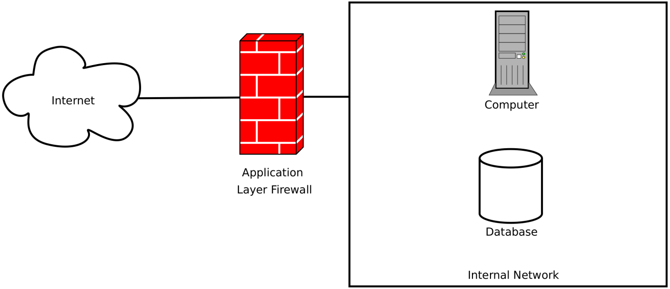


Figure: Diagram of a Application Layer Firewall

Application Layer Firewall

Application Layer Firewall [8]:

- Checks the Protocol information and payload of all packets
- Serves each connection from Client to the Server in the Internet (Proxy Server)
- Can change the incomming and outgoing packets of the transmission

IT-Security

The topics Personal, Network Firewall and Application Layer Firewall are discussed in more detail in the lecture **IT-Security**. There these topics are discussed in more detail. This Slide set only provides you with basic information.

Packet Filter

Packet Filters have the following charachteristics:

- Checks the IP-Addresses and Ports of incomming and outgoing packets
- Defines Rules for the incomming, outgoing and forwarded packets
- Nowadays part of Routing devices (e.g. FritzBox)

Packet filters define **Rule Chains** and **Policies**

Rule Chains

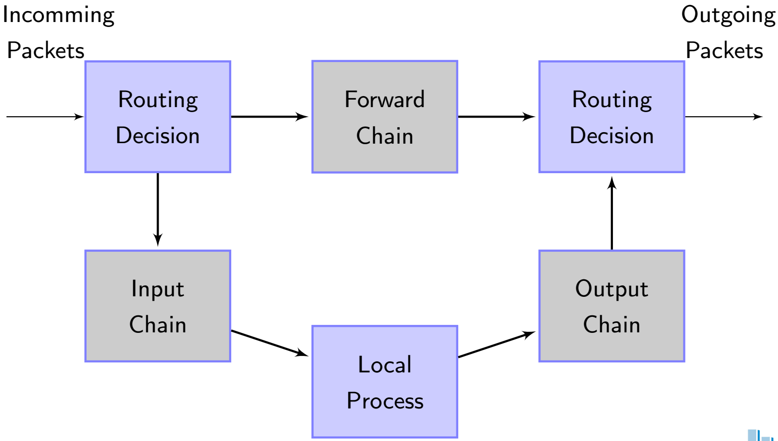


Figure: Flow of packets trough a packet filter

Rule Chains

Input Chain:

- Defines the behaviour of incomming packets that are locally processed

Forward Chain:

- Defines the behaviour of packets that pass through the router

Output Chain:

- Defines the behaviour of packets that go from a local process to the destination

Prerouting Chain:

- Defines the behavour of packets before routing them

Postrouting Chain:

- Defines the behavior of packets after routing them

Policies

The following policies exist:

- ACCEPT – Accepts all packets
- DROP – Drops all packets (Without error information)
- REJECT – Rejects all packets (With error information)
- LOG – Logs information about the packets

Policies define the behaviour of a chain

If no rule can be applied to the packet the poilicy defines how the packet should be treated

Rule Chains and Policies

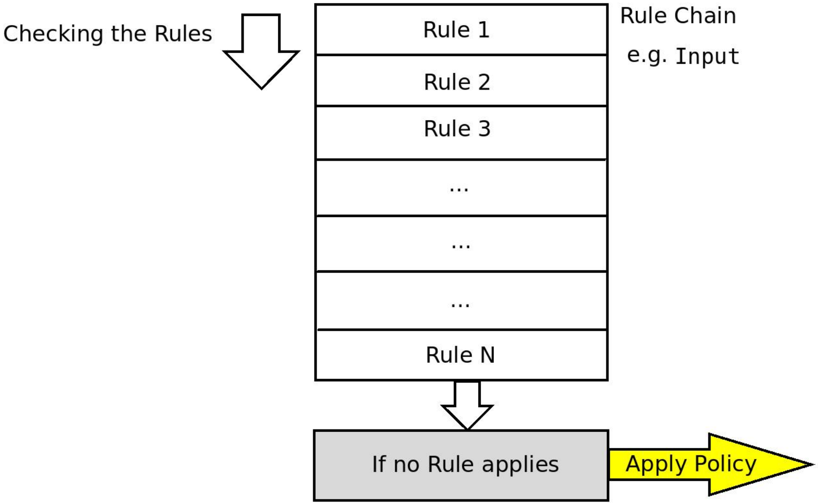


Figure: Rule Chains and Policies

Rule Chains and Policies

The concept of Rule Chains and Policies is a key element in working with `iptables`

The definition of Rule Chains and Policies in `iptables` is explained in the next section!

iptables

iptables [9] is a command-line tool for the configuration of packet filters

The tool is used to define Policies and Rule Chains in Linux

It is the standard tool for packet filters in Linux

iptables – Definition of Rules

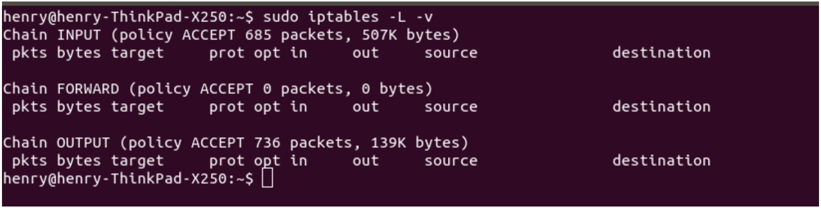
The most important Rule Chains in `iptables` **are** [10]:

- `INPUT` – rules for incomming connections
- `FORWARD` – rules for incomming connections that pass through
- `OUTPUT` – rules for outgoing connections

The rules that are already defined in the system can be listed with the following command:

- `sudo iptables -L -v`

iptables – Definition of Rules



```
henry@henry-ThinkPad-X250:~$ sudo iptables -L -v
Chain INPUT (policy ACCEPT 685 packets, 507K bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 736 packets, 139K bytes)
 pkts bytes target     prot opt in     out     source               destination
henry@henry-ThinkPad-X250:~$ 
```

Figure: Listing the rules in iptables

iptables – Definition of Rules

Some important options [2]:

`-A, -append` Appends rules to an existing chain

`-s, -source` Specifies the source address (e.g. 192.168.0.1/24)

`-d, -destination` Specifies the destination address

`-p, -protocol` Specifies a protocol (e.g. `tcp`, `udp`, `icmp`, etc.)

`-destination-port,-dport` Specifies the destination port

`-i` Specifies the interface (e.g. `eth0`, `wlan0`)

`-ctstate` Specifies the state of connections
(e.g. `NEW`, `RELATED`, etc.)

[2] For a more detailed list see [9]

iptables – Definition of Rules

Examples of Rules:

- `iptables -A INPUT -s 10.10.10.10 -j DROP`
  Blocks all connections from IP-Address 10.10.10.10
- `iptables -A INPUT -p tcp --dport ssh -s 10.10.10.10 -j DROP`
  Blocks all `ssh` connections from IP-Address 10.10.10.10

An Example using connection states:

1.
   ```
   iptables -A INPUT -p tcp --dport ssh
   -s 10.10.10.10 -m state --state NEW,ESTABLISHED -j ACCEPT
   ```
   Command 1 allows `ssh` connections from IP-Address 10.10.10.10 but no `ssh` connections to this IP-Address.

2.
   ```
   iptables -A OUTPUT -p tcp --sport 22
   -d 10.10.10.10 -m state --state ESTABLISHED -j ACCEPT
   ```
   Command 2 allows `ssh` connections to send back packets if there is a session established

iptables – Definition of Policies

Policies are useful to handle packets that do not apply to a rule in a Rule Chain

iptables defines the following policies:

- ACCEPT – Accepts all packets
- DROP – Drops all packets (Without error information)
- REJECT – Rejects all packets (With error information)
- LOG – Logs information about the packets

The Parameters for the policies need to be specified with the option -P or --policy!

DROP vs REJECT

DROP blocks any connection without error information. REJECT returns an error message that helps administrators to identify the machine.

iptables – Definition of Policies

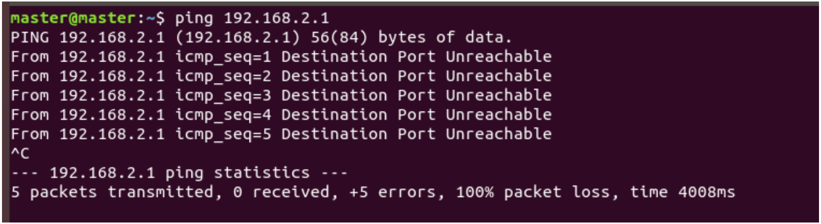
Some Examples for policies in iptables:

- `iptables -P INPUT DROP`
  Blocks all packets that do not apply to a rule in the INPUT Rule Chain (without error message)
- `iptables -P OUTPUT ACCEPT`
  Accepts all packets that do not apply to a rule in the OUTPUT Rule Chain
- `iptables --policy FORWARD REJECT`
  Rejects all packets that do not apply to a rule in the FORWARD Rule Chain (an error message is sent)

Default Deny Policies

A Policy where all packets in all Rule Chains are blocked using DROP is called **default deny**. In a default deny setup rules for allowed connections have to be specified. Everything that is not defined by a rule is blocked per default.

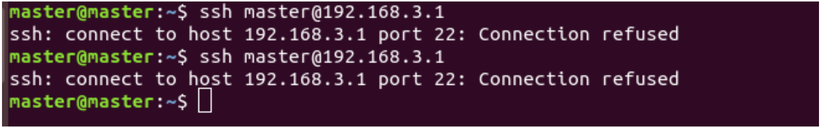
iptables – DROP



```
master@master:~$ ping 192.168.2.1
PING 192.168.2.1 (192.168.2.1) 56(84) bytes of data.
From 192.168.2.1 icmp_seq=1 Destination Port Unreachable
From 192.168.2.1 icmp_seq=2 Destination Port Unreachable
From 192.168.2.1 icmp_seq=3 Destination Port Unreachable
From 192.168.2.1 icmp_seq=4 Destination Port Unreachable
From 192.168.2.1 icmp_seq=5 Destination Port Unreachable
^C
--- 192.168.2.1 ping statistics ---
5 packets transmitted, 0 received, +5 errors, 100% packet loss, time 4008ms
```

Figure: DROP – Destination Port unrechable

iptables – REJECT



```
master@master:~$ ssh master@192.168.3.1
ssh: connect to host 192.168.3.1 port 22: Connection refused
master@master:~$ ssh master@192.168.3.1
ssh: connect to host 192.168.3.1 port 22: Connection refused
master@master:~$ 
```

Figure: REJECT – Connection refused

Lab Exercise 3

This slide set gives a you brief overview of the tools and technologies discussed in Lab exercise sheet 3.

Hopefully this slide set gives you the abillity to solve the tasks of exercise sheet 3!

Lab Exercise 3

Have fun solving the Exercise Sheet and if you have questions, don't be afraid to ask ;-)

Submission Lab Exercise Sheet 3

Please do not forget to submit your results on Moodle until 21st June 2020 !!!

References I

[1] M. Kappes, *Netzwerk- und Datensicherheit*, ser. Lehrbuch : Informatik. Teubner, 2007.

[2] Denial-of-service attack. [accessed: April 19, 2020]. [Online]. Available: https://en.wikipedia.org/wiki/Denial-of-service_attack

[3] Ip address spoofing. [accessed: April 19, 2020]. [Online]. Available: https://en.wikipedia.org/wiki/IP_address_spoofing

[4] Changing your mac address/linux. [accessed: April 19, 2020]. [Online]. Available: https://en.wikibooks.org/wiki/Changing_Your_MAC_Address/Linux

[5] Personal firewall. [accessed: April 19, 2020]. [Online]. Available: https://www.bsi.bund.de/DE/Service/FAQ/PersonalFirewall/faq_node.html

[6] Personal firewall. [accessed: April 19, 2020]. [Online]. Available: https://en.wikipedia.org/wiki/Personal_firewall

References II

[7] Network firewalls explained. [accessed: April 19, 2020]. [Online]. Available: https://www.pacetechnical.com/network-firewalls-explained/

[8] Application layer firewalls. [accessed: April 19, 2020]. [Online]. Available: https://howdoesinternetwork.com/2012/application-layer-firewalls

[9] `iptables` - linux man page. [accessed: April 19, 2020]. [Online]. Available: https://linux.die.net/man/8/iptables

[10] The beginner's guide to iptables, the linux firewall. [accessed: April 19, 2020]. [Online]. Available: https://www.howtogeek.com/177621/the-beginners-guide-to-iptables-the-linux-firewall/