The Linux Firewall

Laboratory Report in EDA491/DIT071 Network Security

Author 1
Author 2

Group XX

Version no: 0.1

May 13, 2014

Contents

1 Introduction

This section shall introduce the reader to the subject. It should include the purpose of the report, i.e. a formulation of the problem to which the report provides an answer.

The last paragraph should explain the structure of the report, e.g., The rest of the report is organized as follows: Section 2 provides...

If you need information on LaTeX, [2] is a good place to start...

2 System Configuration and Requirements

This section should include an explanation of the system configuration and the services which are running on the host. It should also include the security requirements (as stated in the lab PM). Make appropriate use of tables. For your convenience, an example table is given below, but its content may need to be updated.

At the begining of the lab a initial firewall configuration was in place to make the host work as intended when not used for this particular laboratory assignment. The configuration can be seen in Listing 1.

Listing 1: Initial firewall configuration

```
Chain INPUT (policy ACCEPT 9 packets, 2244 bytes)
num   pkts bytes target     prot opt in     out     source               destination
1        0     0 CTH        all  --  eth0   *       129.16.0.0/16        0.0.0.0/0
          /* Fix NFS traffic */
2        0     0 DROP       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0
          tcp flags:0x29/0x29
3        0     0 DROP       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0
          tcp flags:0x3F/0x00

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
num   pkts bytes target     prot opt in     out     source               destination
1        0     0 DROP       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0
          tcp flags:0x29/0x29
2        0     0 DROP       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0
          tcp flags:0x3F/0x00

Chain OUTPUT (policy ACCEPT 5 packets, 1207 bytes)
num   pkts bytes target     prot opt in     out     source               destination
1        0     0 ACCEPT     all  --  *      eth0    0.0.0.0/0            129.16.0.0/16

Chain CTH (1 references)
num   pkts bytes target     prot opt in     out     source               destination
1        0     0 ACCEPT     all  --  *      *       129.16.20.26         0.0.0.0/0
          ctstate RELATED,ESTABLISHED /* NFS server soleil */
2        0     0 RETURN     all  --  *      *       129.16.20.0/23       0.0.0.0/0
          /* Dont look at CE */
3        0     0 ACCEPT     all  --  *      *       0.0.0.0/0            0.0.0.0/0
          ctstate RELATED,ESTABLISHED /* Allow the rest to Chalmers */
```

3 Firewall Configuration

Describe the new firewall configuration, together with the output, e.g., rule on line 5 ensures that the number of ping packets are limited to 1. Don't forget to refer to your script in Appendix B.

Listing 2: Final firewall configuration

```
{output of iptables -vL --line-numbers}
```

4 Firewall Correctness

Explain which tool you used and how it helped you in verifying your firewall configuration. Elaborate on why the firewall is correctly configured and does what it should do. E.g., by trying the command XXX, we found that there are only YYY number of packets returned when pinging the host. Thus, the ping protection (rule Z) is working.
Also answer:
– Why is the order of your firewall rules correct and makes sense?
– Is your configuration stateful?

5 Discussion

Reflect on the current firewall configuration. E.g., is it complete? What have you learned? Recommendations for future configuration, maintenance requirements of the firewall, etc.

6 Conclusion

Present your conclusions in relation to the objective stated in the introduction. It should not contain new information that is not discussed elsewhere in the report.

References

[1] R. Russell. *Linux 2.4 Packet Filtering HOWTO*. June 2002. URL: `http://netfilter.org/documentation/HOWTO/packet-filtering-HOWTO.html`.

[2] *LaTeX - Wikibooks, open books for an open world*. URL: `http://en.wikibooks.org/wiki/LaTeX`.

Please use Vancouver/IEEE style for your referencing. For more information please check: `http://www.lib.unimelb.edu.au/cite/ieee/index.html`. References can easily be managed with the program `JabRef`.

A Initial Firewall Configuration

The initial configuration script of the firewall is shown in Listing 3.

Listing 3: Initial firewall configuration script

```
#!/bin/bash -
#

MY_NETWORK="129.16.21.0/24"

# Replace the ip address here with the ip address for your computer.
# You can use the program "/sbin/ifconfig", or "/sbin/ip addr show"
# to obtain the correct address.
MY_HOST="129.16.21.XX"

# Network devices
IN=eth0
OUT=eth0

# Path to iptables, "/sbin/iptables"
IPTABLES="sudo␣/sbin/iptables"


######################################################################
### NOTE: FOLLOWING ROLES MUST BE AT THE TOP OF THIS CONFIGURATION ###
###       AND THEY SHOULD NOT BE MODIFIED IN ANY WAY(!)            ###
###       CHANGING ANY OF THESE RULES MAY RESULT IN THAT YOUR      ###
###       MACHINE FREEZES (AS YOUR NFS CONNECTION IS LOST TO YOUR  ###
###       HOME DIRECTORY).                                         ###
######################################################################

# Flushing all chains and setting default rules
$IPTABLES -P INPUT ACCEPT
$IPTABLES -P FORWARD ACCEPT
$IPTABLES -P OUTPUT ACCEPT
$IPTABLES -F
$IPTABLES -F CTH
$IPTABLES -X CTH

# Make sure NFS works (allow traffic to Chalmers)
# If NFS connection is lost, your machine will hang for eternity
$IPTABLES -N CTH
$IPTABLES -A CTH -s 129.16.20.26 -m state --state ESTABLISHED,RELATED -m comment --
    comment "NFS␣server␣soleil" -j ACCEPT
$IPTABLES -A CTH -s 129.16.20.0/23 -m comment --comment "Dont␣look␣at␣CE" -j RETURN
$IPTABLES -A CTH -m state --state ESTABLISHED,RELATED -m comment --comment "Allow␣the␣
    rest␣to␣Chalmers" -j ACCEPT

$IPTABLES -A INPUT -i $IN -s 129.16.0.0/16 -m comment --comment "Fix␣NFS␣traffic" -j CTH
$IPTABLES -A OUTPUT -o $OUT -d 129.16.0.0/16 -j ACCEPT

$IPTABLES -Z
```

```
47 ########################################
   ### WRITE YOUR OWN RULES FROM HERE... ###
49 ########################################


51
   # Kill malformed packets
53 # Block XMAS packets
   $IPTABLES -A INPUT -p tcp --tcp-flags FIN,PSH,URG FIN,PSH,URG -j DROP
55 $IPTABLES -A FORWARD -p tcp --tcp-flags FIN,PSH,URG FIN,PSH,URG -j DROP
   # Block NULL packets
57 $IPTABLES -A INPUT -p tcp --tcp-flags ALL NONE -j DROP
   $IPTABLES -A FORWARD -p tcp --tcp-flags ALL NONE -j DROP
59


61 echo "Done!"
```

B Final Configuration Script

The final configuration script of the firewall is shown in Listing 4.

Listing 4: Final firewall configuration script

```
#!/bin/bash -
#

MY_NETWORK="129.16.23.0/24"

# Replace the ip address here with the ip address for your computer.
# You can use the program "/sbin/ifconfig", or "/sbin/ip addr show"
# to obtain the correct address.
MY_HOST="129.16.23.134"

# Network devices
IN=em1
OUT=em1

# Path to iptables, "/sbin/iptables"
IPTABLES="sudo␣/sbin/iptables"


########################################################################
### NOTE: FOLLOWING ROLES MUST BE AT THE TOP OF THIS CONFIGURATION ###
###       AND THEY SHOULD NOT BE MODIFIED IN ANY WAY(!)            ###
###       CHANGING ANY OF THESE RULES MAY RESULT IN THAT YOUR      ###
###       MACHINE FREEZES (AS YOUR NFS CONNECTION IS LOST TO YOUR  ###
###       HOME DIRECTORY).                                         ###
########################################################################

# Flushing all chains and setting default rules
$IPTABLES -P INPUT ACCEPT
$IPTABLES -P FORWARD ACCEPT
$IPTABLES -P OUTPUT ACCEPT
$IPTABLES -F
$IPTABLES -F CTH
$IPTABLES -X CTH

# Make sure NFS works (allow traffic to Chalmers)
# If NFS connection is lost, your machine will hang for eternity
$IPTABLES -N CTH
$IPTABLES -A CTH -s 129.16.20.26 -m state --state ESTABLISHED,RELATED -m comment --
    comment "NFS␣server␣soleil" -j ACCEPT
$IPTABLES -A CTH -s 129.16.20.0/22 -m comment --comment "Dont␣look␣at␣CE" -j RETURN
$IPTABLES -A CTH -m state --state ESTABLISHED,RELATED -m comment --comment "Allow␣the␣
    rest␣to␣Chalmers" -j ACCEPT

$IPTABLES -A INPUT -i $IN -s 129.16.0.0/16 -m comment --comment "Fix␣NFS␣traffic" -j CTH
$IPTABLES -A OUTPUT -o $OUT -d 129.16.0.0/16 -j ACCEPT

$IPTABLES -Z

```

```
########################################
### WRITE YOUR OWN RULES FROM HERE... ###
########################################

$IPTABLES -P INPUT DROP
$IPTABLES -P FORWARD DROP
$IPTABLES -P OUTPUT DROP

# Block IP-Spoofing
$IPTABLES -A INPUT -s 10.0.0.0/8,172.16.0.0/12,192.168.0.0/16,169.254.0.0/16 -j DROP
$IPTABLES -A OUTPUT -s 10.0.0.0/8,172.16.0.0/12,192.168.0.0/16,169.254.0.0/16 -d
    10.0.0.0/8,172.16.0.0/12,192.168.0.0/16,169.254.0.0/16 -j DROP

# Kill malformed packets
# Block XMAS packets
$IPTABLES -A INPUT -p tcp --tcp-flags FIN,PSH,URG FIN,PSH,URG -j DROP
$IPTABLES -A FORWARD -p tcp --tcp-flags FIN,PSH,URG FIN,PSH,URG -j DROP
# Block NULL packets
$IPTABLES -A INPUT -p tcp --tcp-flags ALL NONE -j DROP
$IPTABLES -A FORWARD -p tcp --tcp-flags ALL NONE -j DROP

# Enable ping
$IPTABLES -A INPUT -m limit --limit 1/sec -p icmp --icmp-type echo-request -j ACCEPT
$IPTABLES -A INPUT -p icmp --icmp-type echo-request -j DROP

# Let established connections through
$IPTABLES -A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT

# Enable loopback
$IPTABLES -A INPUT -i lo -j ACCEPT
$IPTABLES -A OUTPUT -o lo -j ACCEPT

# Enable all outgoing conenctions
$IPTABLES -A OUTPUT -o em1 -j ACCEPT

# Enable incomming conenctions for selected services
$IPTABLES -A INPUT -p udp -i em1 --dport 22 -j ACCEPT
$IPTABLES -A INPUT -p tcp -i em1 --dport 22 -j ACCEPT
$IPTABLES -A INPUT -p udp -i em1 --dport 8080 -j ACCEPT
$IPTABLES -A INPUT -p tcp -i em1 --dport 8080 -j ACCEPT
$IPTABLES -A INPUT -p udp -i em1 --dport 111 -j ACCEPT
$IPTABLES -A INPUT -p tcp -i em1 --dport 111 -j ACCEPT

$IPTABLES -A INPUT -j LOG
$IPTABLES -A OUTPUT -j LOG
$IPTABLES -A FORWARD -j LOG

echo "Done!"
```

C Answers to Assignment Questions

Q1. After DROPping echo-reply packets on OUTPUT chain, what was the observed effect? Use Figure 1 to illustrate the path of the packets. Mark the path with arrows and use an X to mark the point where the packets are DROPped.

Q2. After DROPing echo-request packets on INPUT chain, what was the observed effect? How is this reaction different from the reaction achieved in Q1? Use Figure 1 to illustrate the path of the packets. Mark the path with arrows and use an X to mark the point where the packets are DROPped.

Figure 1: Figure to help you illustrate your thoughts regarding the packet flow in questions Q1 and Q2.

Q3. For each entry in the log, several information items are displayed. Some entries can be useful for creating new rules. Explain the items `IN`, `OUT`, `SRC`, `DST` and `PROTO` mean and why these might be useful.

Q4. At this stage, with default policy set to DROP for all chains, would you consider the system secure? Would you consider it useful?

Q5. Assume instead that you used default policy ACCEPT, would you consider the system secure now? Would you consider it useful?

Q6. You just added some protection against flooding by limiting the number of packets the firewall will let through to 1 per second. Give two examples on how you can tell that you are protected!