Tutorial & Case Study in Implementing Linux Network Security, part II

Oskar Andreasson
oskar.andreasson@direct2internet.com

Table of Contents

Table of Content

LAMP Case Study

LAMP is:

- Linux
- Apache
- MySQL
- PHP

- And others.

LAMP Case Study - Overview

Needs:

- Allow specific traffic to get in.
- Deny all other traffic from getting in.
- Allow specific traffic to get out.
- Deny the rest from getting out.

Technical:

- Interface: eth0
- IP: 192.168.0.2

LAMP Case Study - Components

Components we will use:

- Apache - port 80
- MySQL - port 3306
- PHP - scripting language...
- SSH - port 22
- FTP - port 21 + random ports

LAMP Case Study - Goals

- Block everything.
- Allow necessary services.
- Sandbox the machine.

LAMP Case Study - Sandboxing

Block

- Block everything
- Includes incoming, outgoing and forwarded traffic

Unblock

- Unblock specific services that you want to allow
- Includes services on this machine
- Services on other machines
- Forwarded services (e.g., routed services)

Build as many walls as possible, and with as few holes as possible.

LAMP Case Study - Script - Variables

IPTABLES="/usr/sbin/iptables"
Location of iptables on this machine

IP="192.168.0.2"
IP address of this machine

IFACE="eth0"
Interface on this machine

LAMP Case Study - Script - Policies

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

Set the default policies of all chains to DROP.

LAMP Case Study - Script - Sysctl’s

echo 40 0 0 0 60 300 60 0 0 > /proc/sys/vm/bdflush

Improve disk IO on servers. kupdate will run every .6 seconds, dirty buffer flush every 3 secs.

echo 1 > /proc/sys/net/ipv4/tcp_syncookies

Use SYN cookies. Controversial, and do break RFC’s in a sense. Be careful

echo 1 > /proc/sys/net/ipv4/icmp_echo_ignore_broadcasts

Ignore broadcasted pings

LAMP Case Study - Script - Sysctl’s

echo 8192 174760 349520 > /proc/sys/net/ipv4/tcp_rmem

Increase TCP Receive memory buffer, to improve performance on high speed networks

echo 8192 32768 262144 > /proc/sys/net/ipv4/tcp_wmem

Increase TCP Send memory buffer, to improve performance on high speed networks.

LAMP Case Study - Script - Extra chains

$IPTABLES -N allowed

$IPTABLES -A allowed -p TCP --syn -j ACCEPT

$IPTABLES -A allowed -p TCP -m state --state ESTABLISHED,RELATED -j ACCEPT

$IPTABLES -A allowed -p TCP -j REJECT

- Standardized chain for checking TCP packets legality.

LAMP Case Study - Script - INPUT

```
$IPTABLES -A INPUT -m state -i $IFACE --state ESTABLISHED,RELATED -j allowed
$IPTABLES -A INPUT -p tcp --destination $IP --dport 80 -j allowed
$IPTABLES -A INPUT -p tcp --destination $IP --dport 21 -j allowed
$IPTABLES -A INPUT -p tcp --destination $IP --dport 22 -j allowed
$IPTABLES -A INPUT -p tcp -i lo --dport 3306 -j allowed
$IPTABLES -A INPUT -p tcp -i lo --dport 25 -j allowed
$IPTABLES -A INPUT -p tcp -i lo --dport allowed
```

LAMP Case Study - Script - INPUT

- Try to add the rules which will take the largest burden at the top
- Be as specific as possible.
- We don’t want to allow junk that should normally not be allowed in here.
- Try to be as specific as possible about packets (even from local host).

LAMP Case Study - Script - OUTPUT

```
$IPTABLES -A OUTPUT -m state --state ESTABLISHED,RELATED -j
ACCEPT
$IPTABLES -A OUTPUT -p tcp --dport 80 -j allowed
$IPTABLES -A OUTPUT -p tcp -o lo --dport 3306 -j allowed
$IPTABLES -A OUTPUT -p tcp -o lo --dport 25 -j allowed
```

LAMP Case Study - Script - OUTPUT

- Only allow the absolutely necessary to leave the machine
- Be cautious of allowing standard protocols, such as http.
  - These are often used to grab malicious code online, etc.

LAMP Case Study - Summary

- You now have a complete script for a Linux Apache MySQL PHP system
- Should have enough knowledge to write some simple iptables scripts
- Some more basic knowledge about the ipsysctl

Final notes - Other resources

- http://www.frozentux.net
- http://www.netfilter.org
- http://www.linuxguruz.org/iptables/
- http://www.islandsoft.net/veerapen.html
- http://www.lartc.org
- http://www.docum.org