Lazy-Admin Hacking guide

Michael Bauer mb@bellevue.cc

April 14, 2003

1 Introduction

Lazy-Admin was a set of makefiles written to ease the maintaining of a Firewall. I liked it so much that i decided to extend it a little bit, perhaps it will be usefull somewhen. It contains the following "packages":

- The Linuxkernel
- grsecurity patches for the Linux-kernel
- netfilter + patch-o-matic
- snort + snort rules
- libpcap (+ 802.11b patches)
- Tripwire
- Openssh
- Openssl
- zlib
- tcpdump
- ethereal
- Glib and GTK+ (1.2)
- kismet

2 Packages

A "Package" is simply a Directory with a Makefile, the name of the directory is the name of the package. The makefiles contain all the important information for: fetching the file, unpacking the file, configuring and compiling the package and finaly installing the package. At the moment Dependencies are not checked, i'm working on this. MD5 checksums of the packets are checked, if this fails whole make process will abort. It should never happen to you, but when it does, try to get the actual MD5 sum from the vendor.

2.1 The Makefile

usualy a makefile begins with the following lines:

```
NAME=
VERSION=
FILE=$(NAME)-$(VERSION).tar.gz
LOCATION=
DIR=$(NAME)-$(VERSION)
CONFIGUREOPTS=
TARGET=
DEPENDENCIES=
```

This are the general settings of the Makefile, you will usualy only have to modify theese. NAME is the name of the package. VERSION is the recent version of the package. FILE is the Filename of the file to be downloaded. LOCATION is the location where the FILE should be downloaded from (e.q. "ftp://ftp.kernel.org/pub/linux/kernel/v.2.4/") Don't forget the trailing slash. DIR is the directory created if the FILE is unpacked. CONFIGUREOPTS are the options to the ./configure script. TARGET is the target to be created, usually the program or library name (with full relative path!). So if for example there is a new openssh version availible, just cd to openssh edit the Makefile and change VERSION= to the recent version. run make && make install, and the new openssh package should be installed. To define a new package copy the example Makefile of the doc dir and fill in your settings. Don't forget to create the file md5 with the actual md5 sums in it.

2.2 installing

Now how to install or update a package? It's quite easy, just cd to the directory the package is in, type make && make install and the Packet will be installed. Some packets require special dependencies, or another Package to be remade (for example the patch-o-matic package needs an unpacket and configured kernel (cd to linux and type make linux)). Dependency checking

isn't done yet but will follow. To update a package just edit the Makefile and change VERSION= to the recent version. Next step is updating the MD5sum just edit the file md5 od fetch the package from a thrusted server and run md5sum ¡packagefile¿ ¿ md5 . Type make && make install and the package should be updated.

2.3 The Kernelpackage

The kernel package is a little bit different, because configuration has to be done different. The configuration of the kernel is in the file linux/linux-config. To configure a new kernel (if you need to) just follow these steps:

```
cd linux
make linux
cd linux
make menuconfig (or xconfig or config)
cp .config ../linux-config
```

This will save the configuration you created to linux-config. You may need to run make again to build the new kernel. There are two different kernel packages: linux-vanilla and linux-grsecurity, linux is only a symlink to one of these two, change the symlink to select a different package.

2.4 Tripwire

Tripwire is an Local intrusion detection system, and as such it is really recommended to install it onto a RO medium (floppy). Make install will install it into /usr/local/tripwire so you might consider the following steps for installation:

```
mkdir -r /usr/local/tripwire
mount /dev/fd0 /usr/local/tripwire
cd /usr/src/lazy-admin/tripwire
make && make install
umount /usr/local/tripwire
# now switch on write protection
mount /dev/fd0 /usr/local/tripwire
```

there is a crontab in the tripwire directory (tripwire.cron) you may want to install it.