



OWASP

The Open Web Application Security Project
<http://www.owasp.org>

Up and Running with LabRat

The OWASP LiveCD Education Project

Author: Brian Shumate

SECUR[IT]Y DISTRO

www.securitydistro.com



Table of Contents

| | |
|--|----|
| A1 Introduction..... | 3 |
| A2 Downloading LabRat..... | 4 |
| A3 Booting the ISO..... | 5 |
| A4 Using the Included Tools..... | 6 |
| A5 Installing LabRat to Hard Disk..... | 7 |
| A6 Booting the New Image from the Hard Disk..... | 9 |
| A7 Updating LabRat Software..... | 11 |
| A8 Wrapping Up..... | 12 |
| A9 References..... | 12 |
| A10 About the Author..... | 13 |



A1 Introduction

Just when you thought you'd seen all of the finest Linux based Live CD security distros available, a clean, comprehensive, and very usable solution pops into the scene from the fine folks at the Open Web Application Security Project (OWASP).

In conjunction with some sponsoring security organizations, OWASP has produced a strong offering in the OWASP AOC LiveCD distribution, version 0.10 (known also as "LabRat") that is worth a serious look if you are seeking a fantastic LiveCD security-oriented distribution.

The OWASP LiveCD is a Debian-flavored distro based on Morphix built around a rich assemblage of applications and documentation, and with a goal of providing security professionals and students an ideal platform for structured and standardized application security testing. The system even offers a series of tests which can be performed by "hacking" the included WebGoat J2EE application simulator according to the well-structured guides.

Excellent Security Testing Applications

Some of the major security testing applications available in LabRat include:

- NMAP
- TCPDUMP
- Paros
- JBroFuzzer
- WireShark
- WebGoat
- WebScarab

Scope of this Guide

This guide further introduces the OWASP LiveCD (LabRat) distribution, details installing to a hard disk drive, and updating included the included applications, and operating system components. If you're ready to try this excellent security distribution, grab a machine, a bit of bandwidth, and let's go!



A2 Downloading LabRat

Once you've provisioned a test machine, you need to download the LabRat ISO from the OWASP project website.

Retrieve the ISO from the following URL:

http://www.owasp.org/index.php/Category:OWASP_Live_CD_Project

Note: This disk image is approximately 790MB, so you'll need to write the image to a DVD, or consider using a virtual machine environment, such as VMware for your testing.



A3 Booting the ISO

Write the downloaded ISO to a disk or refer to it directly through a virtual machine environment, and then boot the disc or ISO. Eventually, you will reach a nice KDE desktop that resembles the one shown in the screen-shot below.



Figure 1: OWASP LiveCD



A4 Using the Included Tools

LabRat ships with a comprehensive testing guide that you can use to try out the various security tools which comprise the distribution. You can access this guide from the desktop icon, and through OWASP's Testing Project:

http://www.owasp.org/index.php/Category:OWASP_Testing_Project

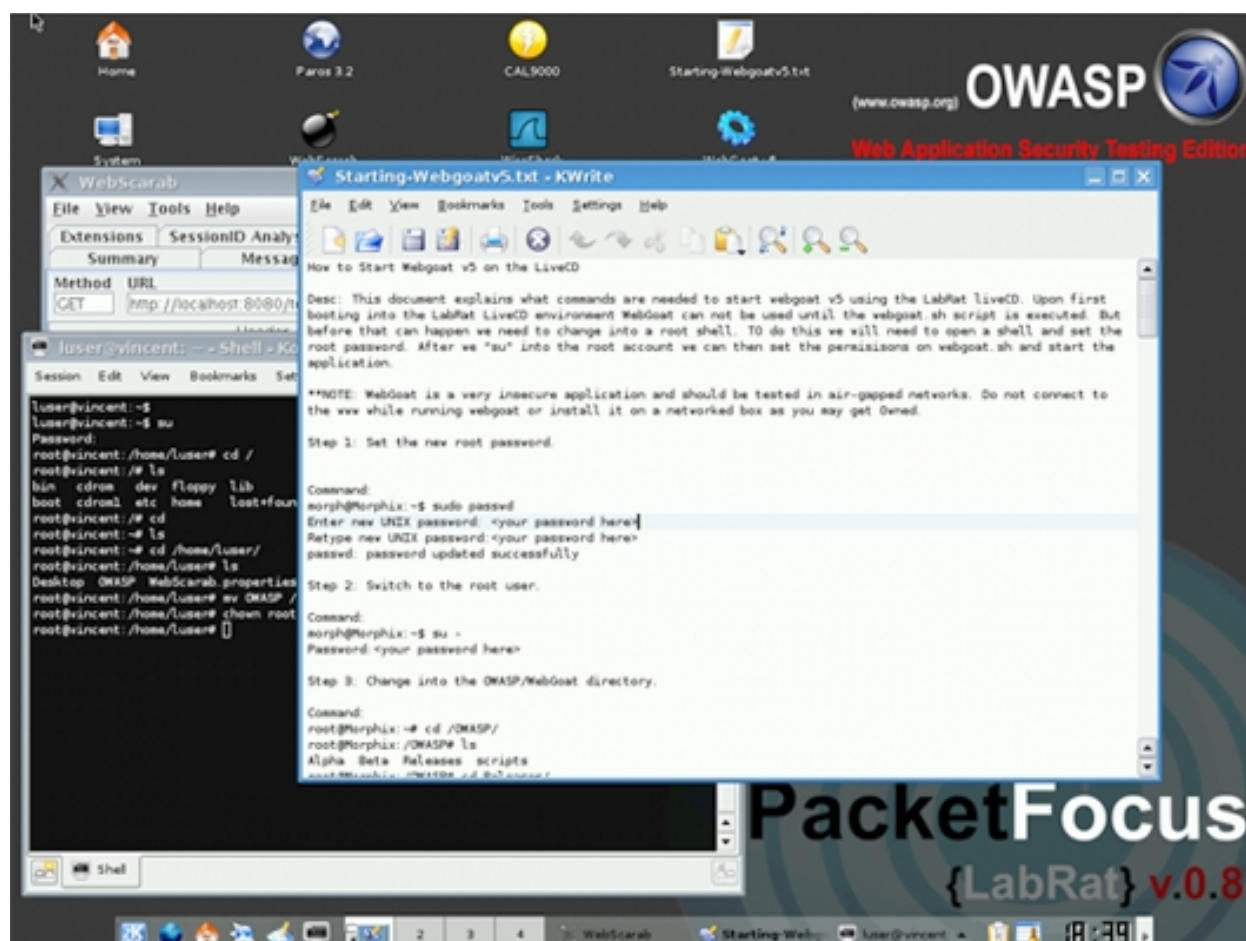


Figure 2: LabRat Desktop showing WebScarab and the WebGoat start instructions



A5 Installing LabRat to Hard Disk

Being a LiveCD system, LabRat runs completely in memory after loading into a memory based disk. If you'd rather establish a more permanent installation to your computer's hard disk, and not be required boot from removable disc each time you want to use LabRat, then follow these directions for installing the LabRat image to your computer's hard disk:

Partition the Hard Disk:

1. Open a shell from the Shell icon on the menu dock.
2. Start the Morphix Installer (morphixinstaller) with the following command line:
3. `morphix@Morphix:~$ sudo morphixinstaller`
4. You should see a graphical install window- Click **Forward**.
5. Select your hard disk and click Forward to partition the selected disk with 'cfdisk'. The cfdisk utility resembles the screenshot shown here: Figure 3

Figure 3: The cfdisk utility with two partitions (primary and swap) configured for hard



6. Create a new root partition by selecting **New** and then **Primary**. Define a value that leaves enough room for swap should your system need swap space. For example if your computer has 256MB of main memory, leave at least 512MB of space for swap. Choose to add the partition to the beginning of the free space.
7. With the root partition you just created highlighted, choose **Bootable**. This should add **Boot** to the partition's flags.
8. Highlight the free space, choose **New** and **Primary**. Allocate the remaining free space.

```
cfdisk 2.12r
          Disk Drive: /dev/hda
          Size: 4295467008 bytes, 4295 MB
          Heads: 255   Sectors per Track: 63   Cylinders: 522

-----
Name      Flags      Part Type  FS Type      [Label]      Size (MB)
-----
hda1     Boot      Primary    Linux        [Label]      3800.08
hda2                                Primary    Linux swap / Solaris
-----

[Bootable] [ Delete ] [ Help ] [Maximize] [ Print ] [ Quit ]
[ Type ]  [ Units ] [ Write ]

Toggle bootable flag of the current partition
```

Figure 3: The cfdisk utility with two partitions (primary and swap) configured for hard

9. W
i



th the second partition highlighted, choose Type, and then specify type **82** for **Linux Swap**.

10. With the swap partition highlighted, choose Write and confirm with yes that you wish to write this partition to disk. After writing is complete, choose **Quit**
11. You will now see a dialog stating that partitioning should be correct. Verify your swap partition exists and is selected, then click **Forward**.
12. Next, ensure that your primary disk partition is selected, then click Forward to format the partition with the Ext3 filesystem.
13. Now the partitions are initialized and data copied from the running LiveCD, to your computer's hard disk. This is a great time to go and grab another copious quantity of caffeine, or see what's new on www.securitydistro.com. :-)

After the files have been copied, you will receive some additional prompting for the following information:

- Network hostname for the system
- Password for the root user
- Username of the normal (default) user account
- Password for the normal (default) user account

Finally, after supplying the above information, you can elect to install the LILO bootloader to your hard disk's master boot record (mbr) or the root partition. You can also elect to skip installing LILO altogether if you have some specific reason for doing so.

Once you've chosen your boot loader option, the system will be installed to hard disk and you will be prompted to reboot. Go ahead and reboot from the hard disk now- we'll update packages and rebuild a custom ISO image next.

A6 Booting the New Image from the Hard Disk

After booting from the hard disk, you'll notice a few things have changed. Now, there is a more general KDE styled greeter, where you must login with the regular user account you defined during the hard disk installation process.

Upon logging in however, you should see a familiar LabRat desktop.



From here, you may wish to ensure you have some specific directories in place. Namely the /OWASP and /pentest directories. If you do not see these directories in the output of the ls command when run against the root of your hard disk, then you need to copy them from the DVD. These directories should be copied to your root directory and should be recursively owned by user root and group root.

Note, that if you are missing the above named directories, you'll likely find that some of the included applications do not start.

To replace the above named directories on your hard disk instance of LabRat, follow this procedure:

Mount the Morphix DVD

```
luser@vincent:~$ sudo mount /dev/cdrom /cdrom
```

Next, extract the main module from the DVD to retrieve an the ISO, which you will mount for copying the necessary directories- Change into the main module directory on the DVD, then make temporary directory for extracting the module as ISO :

```
luser@vincent:~$ cd /cdrom/mainmod
```

```
luser@vincent:mainmod$ mkdir /tmp/labrat
```

```
luser@vincent:mainmod$ extract_compressed_fs mainmod-chroot.mod > /tmp/labrat/originalmodule.iso
```

When the extraction completes, change into the temporary directory, and mount the ISO:

```
luser@vincent:mainmod$ cd /tmp/labrat
```

```
luser@vincent:labrat$ mkdir tmp1
```

```
luser@vincent:labrat$ sudo mount -o loop labrat.iso tmp1/
```

Recursively copy the required directory structures (while maintaining original permissions) from the ISO to your hard disk:

```
luser@vincent:labrat$ sudo cp -rp tmp1/OWASP /OWASP
```

```
luser@vincent:labrat$ sudo cp -rp tmp1/pentest /pentest
```

Now, clean up the cruft resulting from the previous steps:

```
luser@vincent:labrat$ sudo umount tmp1
```



```
luser@vincent:labrat$ cd
```

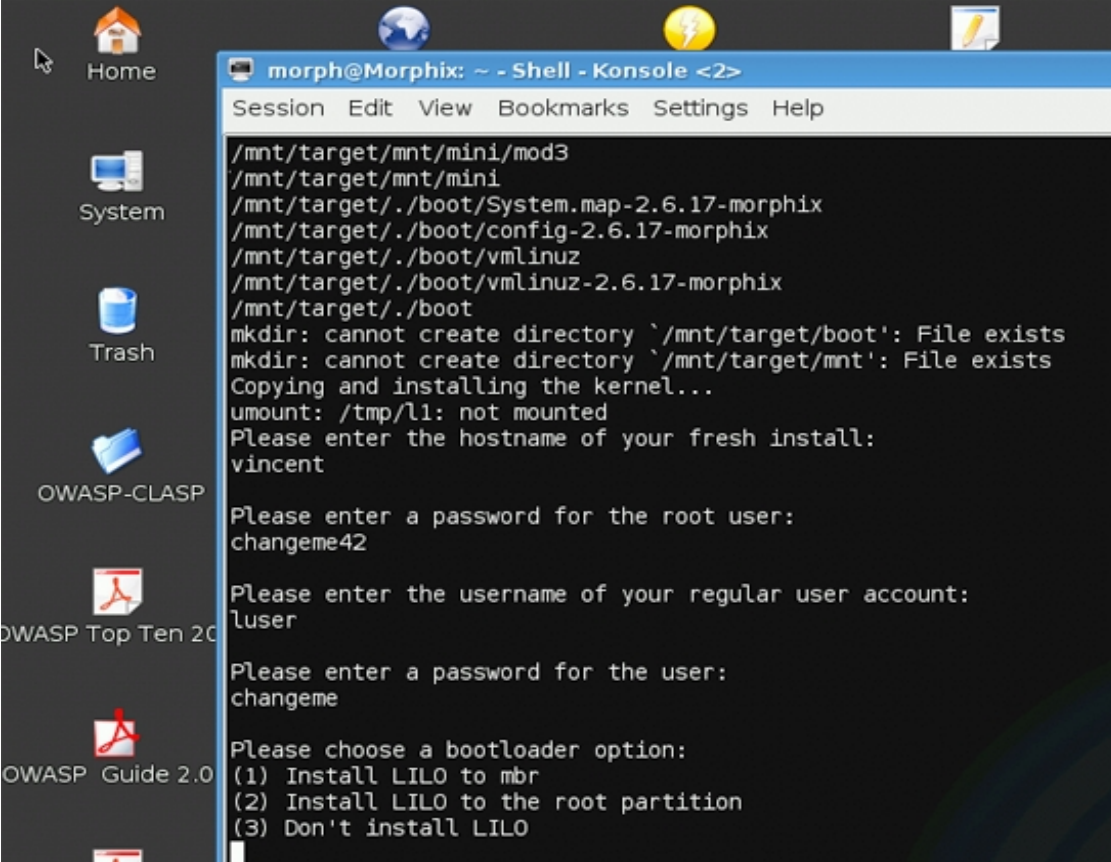
```
luser@vincent:labrat$ sudo rm -rf /tmp/labrat
```

```
luser@vincent:labrat$ sudo umount /cdrom
```

After ensuring your applications are working, you might want to make sure all software in the LabRat distribution is updated- particularly before optionally creating your own custom ISO.

A7 Updating LabRat Software

You can use the standard deb and apt utilities to update the software that powers LabRat. This section will briefly demonstrate the process of updating both your software package lists, and all software packages installed.



```
morph@Morphix: ~ - Shell - Konsole <2>
Session Edit View Bookmarks Settings Help

/mnt/target/mnt/mini/mod3
/mnt/target/mnt/mini
/mnt/target/./boot/System.map-2.6.17-morphix
/mnt/target/./boot/config-2.6.17-morphix
/mnt/target/./boot/vmlinuz
/mnt/target/./boot/vmlinuz-2.6.17-morphix
/mnt/target/./boot
mkdir: cannot create directory `/mnt/target/boot': File exists
mkdir: cannot create directory `/mnt/target/mnt': File exists
Copying and installing the kernel...
umount: /tmp/l1: not mounted
Please enter the hostname of your fresh install:
vincent

Please enter a password for the root user:
changeme42

Please enter the username of your regular user account:
luser

Please enter a password for the user:
changeme

Please choose a bootloader option:
(1) Install LILO to mbr
(2) Install LILO to the root partition
(3) Don't install LILO
```

Figure 5: Additional morphixinstaller



Open a shell, and issue the following commands to update all software on your LabRat:

```
luser@vincent~$ sudo apt-get update
```

```
luser@vincent~$ sudo apt-get -u upgrade
```

If you wish to attempt to upgrade all software to a newer LabRat release, then use these commands:

```
luser@vincent~$ sudo apt-get update
```

```
luser@vincent~$ sudo apt-get -u dist-upgrade
```

After copying the directories to their proper locations, you should find that the OWASP applications, such as Paros and MetaSploite are working as they should.

A8 Wrapping Up

Now that you've done all the hard work related to creating permanent and custom instances of LabRat, don't congratulate yourself just yet- get busy making the most of LabRat, and do some testing!

You may also want to learn how you can share your shiny new creation in the form of [PLUG Second Tutorial LINK]making a custom ISO[/PLUG] to use in multiple locations, distribute to students in classes, and so on. There is a great guide to [PLUG Third Tutorial LINK]updating LabRat applications with modules[/PLUG], and a nice [PLUG Video Tutorial?]video tutorial[/PLUG] on modules too keep you busy and learning with this great application security testing distribution as well.

Stay tuned for updates to this fantastic LiveCD distribution from OWASP, and be on the lookout for more tutorials on LabRat soon as well.

Have fun testing, and don't forget to share and enjoy!

A9 References

OWASP: http://www.owasp.org/index.php/Main_Page

OWASP LiveCD (LabRat) : http://www.owasp.org/index.php/Category:OWASP_Live_CD_Project

OWASP Testing Project: http://www.owasp.org/index.php/Category:OWASP_Testing_Project

WebGoat: http://www.owasp.org/index.php/Category:OWASP_WebGoat_Project



Morphix Linux HD FAQ: <http://www.morphix.org/wiki/index.php/MorphixHdFaq>

Morphix HOWTO: <http://www.morphix.org/wiki/index.php/MorphHowTo>

Morphix tools: http://www.morphix.org/doc/how_tos/docbook_html/ar01s06.html

A10 About the Author