Building a Custom LabRat ISO

The OWASP LiveCD Education Project

Author: Brian Shumate

SECUR[IT]Y DISTRO

www.securitydistro.com

Table of Contents

A1 Introduction

If you have not yet seen the Open Web Application Security Project (OWASP) LiveCD security distribution known as "LabRat", then you want to head on over to OWASP.org and read the OWASP-Up and Running with LabRat on Hard Disk and learn more about this excellent security testing distribution before continuing with this guide.

This guide aims to familiarize the regular user of LabRat with concepts and procedures involved with creating a custom version of the LabRat ISO image. You might want to create such a custom image when you have added additional software to the original image, or have updated the included packages to their latest versions.

This guide assumes some level of familiarity with the LabRat LiveCD, and Linux command-line practices in general. This guide also assumes you have a installed LabRat on your hard disk, OWASP-Up and Running with LabRat on Hard Disk, and that you either have the ability to download the ISO, or already have a DVD made from the ISO. You will be shown how to mount the LabRat DVD, extract an ISO from the LabRat main module, mount this image, make your customizations, and finally, assemble a new custom ISO. Additional resources will be provided at the end of the article for your reference.

A2 Obtaining the LabRat ISO

Either you can extract the ISO image from a working DVD instance of LabRat, or alternatively, you can download the ISO image from the OWASP website at the following location:

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

A3 Extracting the ISO

NOTE: *If you are downloading the ISO, you can skip the following steps, and proceed from the* **Mounting the ISO** *section of this guide.*

If you are using a LabRat DVD, you'll need to insert the DVD, and mount it to begin extracting the ISO from the DVD. Follow these steps to mount and extract the ISO directly from a DVD:

First, make a working directory for processing the modules and images from the image:

```
user@vincent:~$ sudo mkdir -p /LabRat/ISO
```

OWASP Papers Program

Then, mount the DVD with this command:

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

Now, create a directory to extract the ISO into, and begin extraction:

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

user@vincent:mainmod$ sudo extract_compressed_fs \

mainmod-chroot.mod > /LabRat/ISO/mainmod-original.iso
```

A4 Extract Compressed Filesystems

To extract the compressed filesystems which comprise the LabRat DVD, Insert and mount the disc, then extract the images. This process may take a bit of time, so go and check out www.securitydistro.com for the latest news while you wait:

```
user@vincent:~$ mount /dev/cdrom /cdrom

user@vincent:~$ cd /cdrom/mainmod

user@vincent:mainmod$ sudo sh -c extract_compressed_fs \

mainmod.mod > /LabRat/mainmod_original.iso
```

Once the extraction process completes, you're free to mount the `mainmod_original.iso`, and copy its contents to your hard disk.

A5 Mounting the ISO

NOTE: *If you downloaded the ISO to the LabRat regular user's home directory, then copy the ISO to your working directory*:

```
user@vincent:~$ cp AOC_Labrat-ALPHA-0010.iso /LabRat/ISO/
```

Once you copy the ISO in place, or if you have already extracted the ISO from a DVD, then continue with the following steps to create a change root (chroot) environment that you can use to customize your LabRat ISO instance:

A6 Creating a Change Root Enviroment

Create a change root environment in which to make your customizations to the LabRat filesystem before preparing the new ISO. This process makes the ISO image act as though it is the actual current root filesystem. You can then download package updates,

and make other changes as you would on your current installation, but those changes are actually applied to your working copy of the LabRat ISO image.

Follow these steps carefully to create chrooted environment based the LabRat ISO:

```
user@vincent:~$ cd /LabRat

user@vincent:LabRat$ sudo mkdir tmp2

user@vincent:LabRat$ sudo mount -o loop mainmod_original.iso \

/LabRat/tmp1

user@vincent:LabRat$ sudo cp -rp tmp1/* /LabRat/tmp2

user@vincent:LabRat$ cd tmp2

user@vincent:tmp2$ sudo mv tmp1 labrat_hdd

user@vincent:tmp2$ sudo mv labrat_hdd /LabRat

user@vincent:tmp2$ cd /LabRat

user@vincent:LabRat$ sudo umount tmp1
```

Now that you have prepared the chroot environment, go ahead and change root into the labrat_hdd directory, and prepare your custom ISO content:

```
user@vincent:LabRat$ cd /

user@vincent:/$ sudo mount --bind /dev /LAbRat/labrat_hdd/dev

user@vincent:/$ sudo chroot /LabRat/labrat_hdd

user@vincent:/$ sudo mount -t proc /proc proc
```

A7 Customizing Your LabRat

From this point, you can work with the chrooted instance of LabRat as if it were the same as your installed hard disk instance. You can update the applications/application sources, add new applications, customize configuration files, and so on. After making these changes, you can make new ISO image containing your customization and changes.

Once you have made your changes, updated software, and the like, prepare the image to be made into an ISO, but unmounting the chrooted environment, and then use the **mkisofs** tool to create your new ISO:

```
user@vincent:/$ sudo umount /proc Exit chroot
```

Press CTRL-D to exit the chroot

```
user@vincent:/$ sudo umount -f /LabRat/labrat_hdd/dev

user@vincent:/$ sudo cd /LabRat

user@vincent:LabRat$ sudo mkisofs -R -U -V "LabRat fs" \

-P "LabRat" -cache-inodes -nobak -pad /LabRat/labrat_hdd \

> ./labratcustom.iso
```

A8 Creating a Morphix Module

Alright, now you've got your very own LabRat ISO! Let's not start the party too early though- you now need to create a module that the underlying Morphix-based OS will use as the new DVD.

Use the Morphix tool, `create_compressed_fs` to transform your `modcustom.iso` into a Morphix-compatible module. Now's the time to open a book, a video game, or a quick IRC conversation- this part takes a bit of time!

```
user@vincent:/LabRat$ sudo create_compressed_fs \

./labratcustom.iso 65536 > labratcustom.mod
```

Let's store the final DVD ISO image in a directory within the `/LabRat` hierarchy, named `labrat_disc`:

```
user@vincent:LabRat$ sudo mkdir /LabRat/labrat_disc

user@vincent:LabRat$ cd /LabRat/labrat_disc

user@vincent:labrat_disc$ sudo mkdir mainmod

user@vincent:labrat_disc$ cd /LabRat

user@vincent:LabRat$ sudo mv labratcustom.mod \

/LabRat/labrat_disc/mainmod
```

With the new mainmod in place, copy the additional supporting files into your new disc's directory:

```
user@vincent:LabRat$ cd /DVD
```

```
user@vincent:DVD$ sudo cp -a base* /LabRat/labrat_disc

user@vincent:DVD$ sudo cp -a minimod* /LabRat/labrat_disc

user@vincent:DVD$ sudo cp boot.catalog /LabRat/labrat_disc

user@vincent:DVD$ sudo cd /LabRat/labrat_disc

user@vincent:labrat_disc$ sudo mv boot.catalog boot.img
```

Finally, we're ready to heat up the laser! You need to generate the final ISO image that you will burn repeatedly and hand out to friends and family, while proudly proclaiming, "I made this!".

```
user@vincent:LabRat$ cd /LabRat

user@vincent:LabRat$ mkisofs -pad -l -r -J -v -V "LabRat" \

-b base/boot.img -c base/boot.cat -hide-rr-moved \

-o mylabrat.iso labrat_disc
```

A9 Burning and Testing

At this point, you'll want to use the aforementioned laser, preferably in a serviceable optical device and with your preferred software, to actually burn an instance of your wonderful new ISO. Since this guide has kept you in the shell for some time, you can use a command-line tool like

A10 Conclusion

At this point, you should feel confident in building your own custom LabRat ISO images, and will have a better understanding of the underlying operating system with respect to the module model used by Morphix, and the process of extracting ISO images, and creating chrooted environments for development of custom images.

From here, the sky's the limit- You could build any number of specialized LabRat ISO images for any number of functions and purposes, from special convention discs, training camp or seminar materials, or just keeping up with the latest critical packages.

Be sure to see the other www. SecurityDistro.com resources available for the LabRat distribution, such as our [LINKS TO OTHER GUIDES AND VIDEOS].

A11 References

Open Web Application Security Project (OWASP): http://www.owasp.org

LabRat LiveCD Security Project:

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

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

A12 About the Author

The author is a career open source and Linux advocate who grew up among the first generation of children to experience computers in the classroom. Having worn nearly as many hats as one might expect to find at a nice sized rodeo, the author has at times been a system administrator, technical writer, and technologist through the past fifteen years.