HOWTO: Booting an acquired hard disk image containing a Windows installation using xmount and OpenGates

1. Copyright

2. About this HOWTO

This HOWTO deals about booting a Windows installation contained in an acquired hard disk image. The image can be in raw DD, EWF (Expert Witness Compression Format - http://sourceforge.net/projects/libewf/) or AFF (Advanced Forensic Format - http://www.afflib.org/) format. To boot the installed Windows, you can use your favorite virtual machine. (I'm going to cover VirtualBox, VMWare Workstation and qemu in this HOWTO). Furthermore I suppose you are using a recent Debian based Linux distribution (Debian, Ubuntu, Knoppix, etc...) as those are the only ones I offer prebuild binary packages of xmount for.

3. Get and install required software

To keep you up to date with new xmount releases, we're going to add my repository to your software sources list. To do this, execute the following two commands in a terminal window:

```
$ sudo wget -P /etc/apt/sources.list.d/ http://deb.pinguin.lu/pinguin.lu.list
$ sudo aptitude update
```

When the update process has finished, you can install xmount by executing the following command:

```
$ sudo aptitude install xmount
```

I'm not going to cover the process of installing a virtual machine here. Refer for example to VirtualBox's website for details (http://www.virtualbox.org/wiki/Linux_Downloads).

In order to use OpenGates, you need a bootable OpenGates ISO image. Refer to my HOWTO on building a bootable OpenGates CD to get one.

4. Configure your Linux

In order to use FUSE (Filesystem in Userspace - http://fuse.sourceforge.net/), what xmount uses, you have to be in the “fuse” group. To achieve this, execute the following command:

```
$ sudo usermod -a -G fuse username
```

and replace *username* with your user name. Another important configuration step for FUSE is to edit the file “/etc/fuse.conf” with your favorite text editor and uncomment the line that includes “user_allow_other” (Remove the “#” in front of that line). This is especially important when you plan to use VMWare Workstation to boot your acquired disk.

As we're not going to use xmount as root, we will need a personal mount-point to supply to xmount. This one can be created by issuing the following command:

```
$ mkdir ~/mnt0
```

5. Mounting the acquired hard disk image

Depending on which virtual machine you're going to use and in what format your acquired hard disk image is, the command to mount it is different. Below are examples for mounting the EWF image “MyDisk.E01 .. MyDisk.E27” located in “~/acquired/” in order to use it in VirtualBox, VMWare Workstation or qemu. If you have an AFF or DD image, change the “--in *type*” parameter accordingly. The file extension “.E??” is used as you have to specify all EWF segments and this will be expanded by bash to match them all. And as booting an OS involves writing to the disk, the “--cache *cachefile*” parameter is used to enable virtual write access that will be redirected to the specified cache file.

5.1. VirtualBox

```
$ xmount --in ewf --out vdi --cache ~/acquired/MyDisk.cache ~/acquired/MyDisk.E?? ~/mnt0
```

5.2. VMWare Workstation

```
$ xmount --in ewf --out vmdk --cache ~/acquired/MyDisk.cache ~/acquired/MyDisk.E?? ~/mnt0
```

In order to emulate a disk connected to the SCSI bus, replace “--out vmdk” with “--out vmdks”.

5.3. qemu or alike

```
$ xmount --in ewf --out dd --cache ~/acquired/MyDisk.cache ~/acquired/MyDisk.E?? ~/mnt0
```

xmount does not support any qemu specific formats, but qemu, kvm and alike support raw DD images as virtual hard disks.

6. Adding the virtual hard disk to your virtual machine

Once mounted, your virtual disk is located under “~/mnt0/” and ready to be added to a virtual machine. As I suppose you know how to do this, I'm not going any further here.

7. Running OpenGates

Warning: Before starting your virtual machine, make sure it isn't connected to your network (No bridging or NAT)!

You can try and fire up your virtual machine now. Sometimes Windows will just boot and be happy but most times, it won't start at all, produce a BSOD, won't let you login before specifying the right password or before reactivating it. In all those cases, OpenGates is your best bet to get it although running.

Insert the OpenGates ISO into your virtual CD-Rom drive, restart your virtual machine and press any key when asked to boot from the CD. Once the rescue Windows has started, it will launch OpenGates and you are guided trough the patch process. This one should be pretty self-explanatory and just accepting the defaults by pressing [ENTER] on all prompts should normally end you up with a running Windows.

There are two scenarios where you can't accept the defaults. The first one is if you need to clear user account passwords, and the other one is when Windows wants you to reactivate it. In the first case, press “y” when asked to clear user passwords and then clear the ones you need. In the second case, press “y” when you are asked to copy AntiWPA to disk and remember that it must be activated manually afterwards.

Once OpenGates has finished, it displays a summary information. These informations are important as you must update your virtual machine's configuration to reflect them. In VirtualBox, update “Guest OS”, “ACPI” and “IO-APIC” settings. In VMWare Workstation, you can only adjust “Guest OS” and in qemu, you can't adjust anything.

8. Some closing tips and tricks

- Sometimes, even after running OpenGates, Windows doesn't want to start up. The first thing to do is to run OpenGates again and double check that you configured your virtual machine according to the infos OpenGates printed out.
- Another possibility is to switch to another virtual machine. I've encountered several Windows installations that didn't boot in VirtualBox but ran without any problems in VMWare Workstation. Just make sure you use the same cache file as before, so the changes that OpenGates did aren't lost.
- I suggest that once Windows is running, you install your virtual machine's guest additions in order to have mouse pointer integration etc...
- When using VirtualBox, your mouse will often be stuck the first time you boot. Just wait for some minutes and it should work again.