

Entry Point Laptop Configuration Guide

Overview and Requirements

Host Laptop is Required:

Please read carefully.

- If your host is anything other than some flavor of Linux or a Windows version, consider yourself self-supported.
- You must have VMWare Workstation Pro (**essential for snapshotting**). VMWare Player *doesn't* cut it. Apple computers can run VMWare Fusion Pro (the Pro is far more capable, and recommended for this course). If you are unable to get VMWare Workstation Pro, a free alternative is [Oracle VirtualBox](#).
- You will need an **admin account** in order to install software, such as **VMWare Workstation Pro**. It's best if you have access to an administrative account on the laptop for the duration of CyberFIRE for lab and contest work.
- You will need an **Ethernet interface**. A hardwired, actual Ethernet cable will need to plug into your laptop (*not just wifi*) in order to connect to local servers for the labs and the contest. Remember to bring the right dongles if the laptop doesn't have a built-in Ethernet port.

Operating Systems Required:

- REMnux 6 , found at <https://remnux.org>

There are many options to set up a safe analysis environment and to emulate a network. **You will need a Remnux 6 VM for the course.**

What is REMnux?

REMnux is a Linux toolkit for reverse engineering and malware analysis. It comes preloaded with a wide variety of useful freely-available tools. It is based off of Ubuntu, and VMWare will recognize it as such. You will be downloading and importing a .OVA file. An OVA file is an Open Virtualization Archive file, and is a compressed and installable virtual machine.

The Final Product

We will be building one Remnux virtual machine, with Host-Only networking when we are working on it. The VM will not be able to access the internet, so any updates / packages should be run prior to arriving at CyberFIRE training.

Building a REMnux VM on VMware

(See below for VirtualBox instructions)

REMnux 6 , found at <https://remnux.org>

Download and Import

1. Download the .ova file at REMnux.org
2. In VMWare Workstation, got to File --> Open --> File you just downloaded
3. Follow the Prompts to import the .ova

Install VMWare Tools

1. On the top bar, click VM --> Install VMWare Tools
2. Open a terminal as root
3. Mount the virtual CD

```
mount /dev/sr0
```

OR

```
mount /dev/cdrom /mnt/cdrom
```

4. Change to a working directory

```
cd /tmp
```

5. Note the filename of the VMWare Tools Installer

```
ls /mnt/cdrom
```

6. Uncompress the Installer, replacing the x's and y's with the version number from above step.

```
tar xzpf /mnt/cdrom/VMWareTools--x.x.x-yyy.tar.gz
```

7. Unmount the Virtual CD

```
umount /dev/cdrom
```

8. Open the VMWare Tools Directory

```
cd vmware-tools-distrib
```

9. Run the installer

```
./vmware-install.pl
```

10. Hit enter a few times to accept the defaults (or don't, if you know what you're doing)
11. Restart the VM

VirtualBox Setup

1. Get the OVA file from [REMnux](#), as mentioned above.
2. If you've already installed VirtualBox, you can just double click the .ova file you downloaded to import the virtual machine. Do so and follow the steps.
3. Before starting the virtual machine, you'll need to add a CD/DVD drive.
 - o Click the 'Settings' gear (with your imported vm selected).
 - o Click 'Storage' on the dialog that pops up.
 - o In the 'Storage Tree', select the 'Controller: SCSI Controller'.
 - o Click the left most disk looking button with a plus sign below, and choose to add a CD/DVD drive.
 - o Choose 'Leave Empty' when prompted. You will now have a DVD drive.
 - o Click OK.
4. Start your VM. The resolution will be terrible.
 - o The VM will start with a terminal up. Shrink it and fit it in your tiny screen.
5. Install 'Guest Additions'
 - o Your VM window will have a 'Devices' menu, choose 'Insert Guest Additions CD Image'. (Right control uncaptures your mouse in VirtualBox).
 - o Enter the following commands in the terminal with the VM:


```
sudo mount /dev/cdrom
sudo ./mnt/cdrom/VBoxLinuxAdditions.run
sudo reboot
```
6. Your VM should reboot with a much better resolution that resizes with your VM screen.
7. Follow the rest of the steps below.

Updating the System

Updates and package installations require network access. If you are behind a proxy, see the section at the end to set system-wide proxies.

After booting into the virtual appliance, open up a terminal window (looks like a desktop / screen icon on the bottom menu) and type in the command on REMnux to update its software.

```
update-remnux full
```

This will allow you to benefit from any enhancements introduced after the virtual appliance has been packaged. Your system needs to have Internet access for this to work.

If that doesn't work, you can always try the following. Open up a terminal window, run the command:

```
sudo apt-get update
```

Install Packages

Additional packages that will help in class are listed, and should be installed:

```
sudo apt-get install bless sleuthkit
```

As well as items for Python3

```
sudo apt-get install python3-pip
sudo pip3 --proxy http://yourproxy.gov:port install future
sudo pip3 --proxy http://yourproxy.gov:port install pefile
```

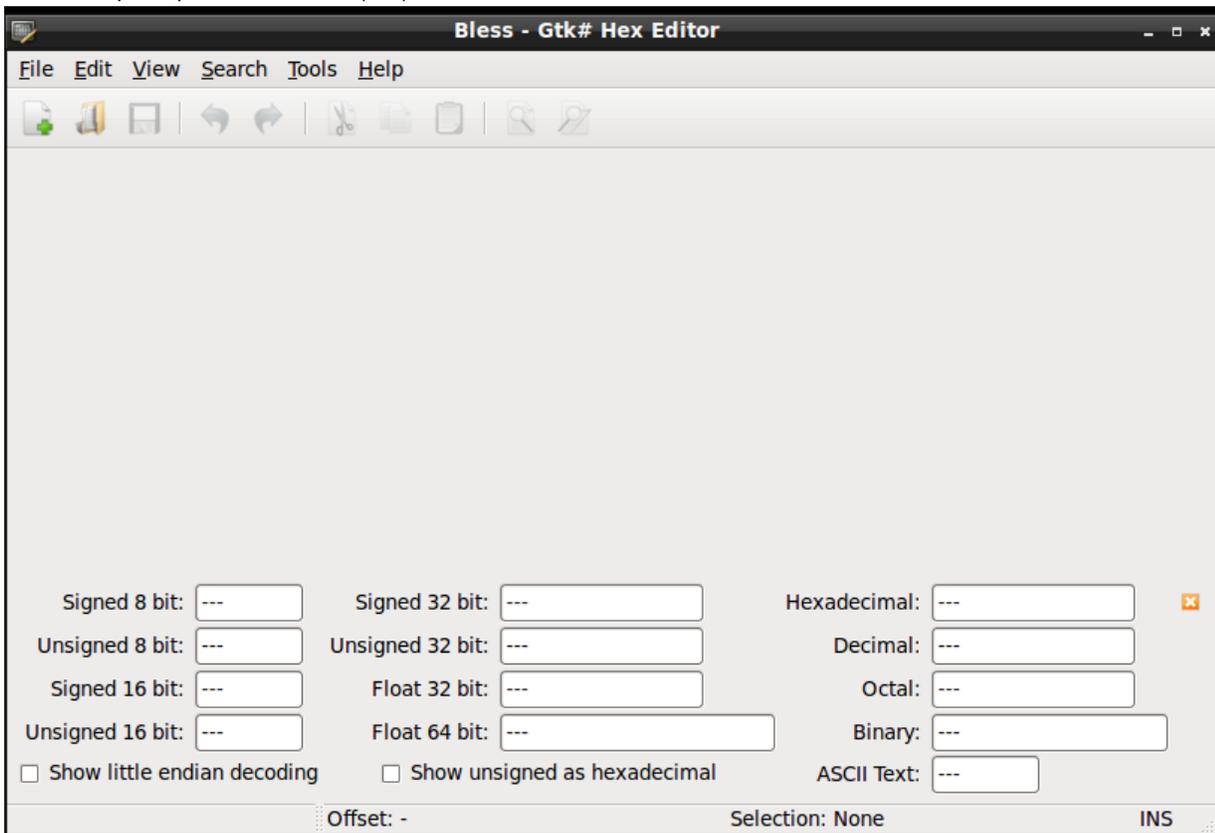
If you are behind a proxy, do use the proxy flag and information, replacing `yourproxy.gov:port` with your local information. For apt-get to work, you may have to follow the proxy setup directions at the bottom of the guide. If you are not behind a proxy, the commands would be `sudo pip3 install package` where `package` is `future` and `pefile`.

Testing installs

Open a terminal window, and type

```
bless
```

It should open up a hexadecimal (hex) editor.



You can quit out of Bless.

To test `sleuthkit`, run the command `mm1s -V` and you should see a version number.

```
$ mm1s -V
The Sleuth Kit ver 4.2.0
```

Test the installation of `pefile` type `pip3 show pefile`.

```
---
Name: pefile
```

Version: 2016.3.28
Location: /usr/local/lib/python3.4/dist-packages
Requires: future

Don't Forget to Snapshot!!

Once all the above tools are installed, take a snapshot and name it with something that makes sense to you. One recommendation is to name it "Clean with Tools_MM_DD_YY" with the current date.

Set system-wide proxies (if needed)

System-wide proxies in CLI Ubuntu/Server must be set as environment variables.

Open the /etc/environment file with vi, gedit, or your favorite editor. This file stores the system-wide variables initialized upon boot. The following commands show the proxy port as 8080. Your values may be different. Check with your local administrator if needed.

```
sudo vim /etc/environment

<type i to start insert mode in vi>
http_proxy=http://myproxy.server.com:8080/
https_proxy=http://myproxy.server.com:8080/
ftp_proxy=http://myproxy.server.com:8080/
no_proxy=localhost,127.0.0.1,localaddress,.localdomain.com
<press ESC key to stop inserting>
<type ':wq' to write and quit vi, not including quotes>
```

apt-get , aptitude , etc. will not obey the environment variables when used normally with sudo . So separately configure them; create a file called 95proxies in /etc/apt/apt.conf.d/ , and include the following:

```
Acquire::http::proxy "http://myproxy.server.com:8080/";
Acquire::ftp::proxy "ftp://myproxy.server.com:8080/";
Acquire::https::proxy "https://myproxy.server.com:8080/";
```

Finally, logout and reboot to make sure the changes take effect. One easy test is to see if you can run sudo apt-get update .

For more information, please look at <http://askubuntu.com/questions/175172/how-do-i-configure-proxies-without-gui> or run a Google search on setting a proxy in Ubuntu.