Avoiding cyberattack

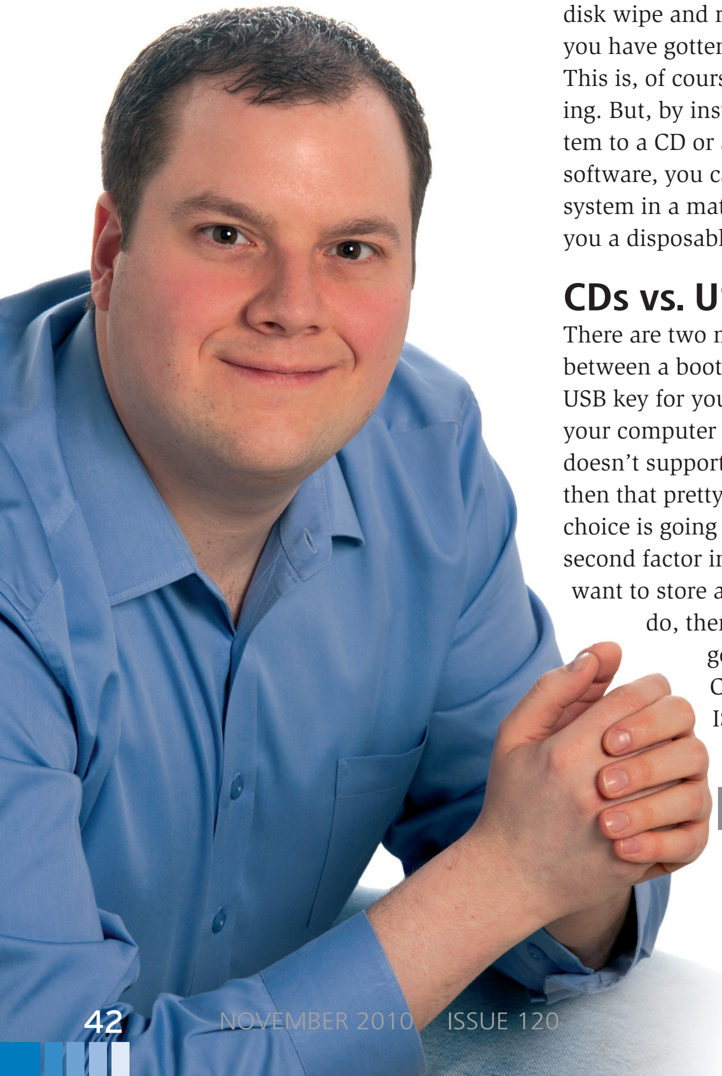
Self-Protection

One way to avoid having your personal information stolen is to use a disposable computer set up for sensitive operations. *By Kurt Seifried*

You have probably read about various options for high-performance computing with Linux in this month's issue. But, what do the bad guys do when they need high-performance computing? They break into other people's computers and use them.

So, how can you avoid becoming part of a botnet and, more importantly, avoid having your personal information, banking details, and other sensitive information sold to someone in a foreign country?

By having a disposable computer, of course! If you need to do something potentially dangerous (like open up an unknown application) or something sensitive (like online banking) simply use a clean computer set up for the task and then wipe it when you are done. The only problem is that this becomes expensive (even with cheap netbooks). So, how can you create inexpensive (or even free) computers?

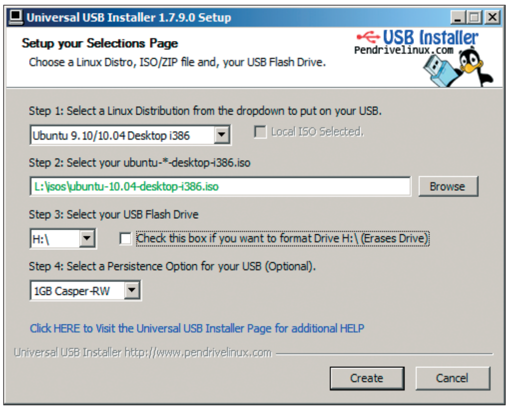


Bootable CDs and USB Keys

The problem with booting from and using your system hard drive is that, if you get attacked and compromised, a rootkit, virus, or other malware will most likely be installed on the system. Many of these are very difficult to get rid of (especially on Windows) – generally requiring a disk wipe and re-install to be certain that you have gotten rid of everything bad. This is, of course, highly time-consuming. But, by installing an operating system to a CD or a USB key using the right software, you can easily create a fresh system in a matter of minutes, giving you a disposable computer.

CDs vs. USB Keys

There are two main factors for choosing between a bootable CD or a bootable USB key for your disposable system. If your computer is old enough that it doesn't support booting from a USB key, then that pretty much means your choice is going to be a bootable CD. The second factor involves whether you want to store any changed data; if you do, then a USB key is the way to go. (Even with re-writable CDs, I haven't seen any ISO distributions set up to use them for storage, but if you know of one, I'd love to hear about it.)



Universal USB Installer 1.7.9.0 Setup

Setup your Selections Page

Choose a Linux Distro, ISO/ZIP file and, your USB Flash Drive.

Step 1: Select a Linux Distribution from the dropdown to put on your USB.

Ubuntu 9.10/10.04 Desktop i386 ☐ Local ISO Selected.

Step 2: Select your ubuntu-*-desktop-i386.iso

L:\isos\ubuntu-10.04-desktop-i386.iso

Step 3: Select your USB Flash Drive

H:\ ☐ Check this box if you want to format Drive H:\ (Erases Drive)

Step 4: Select a Persistence Option for your USB (Optional).

1GB Casper-RW

Click HERE to Visit the Universal USB Installer Page for additional HELP

Universal USB Installer http://www.pendrivelinux.com

Figure 1: Pendrivelinux running on Windows.

Personally, I use USB keys when surfing to potentially dangerous sites or running unknown software so that I can then examine the data and changes made on the USB key to see what exactly happened. But, if I want a system that can't be modified between reboots, then I'll use a CD. Even if an attacker breaks in, they can't change anything on it (because the disk is burned and closed to prevent any future modifications), so a quick reboot ensures that I have a clean system again.

Pendrivelinux

Pendrivelinux [1] will install a variety of Linux versions to either a CD or a USB key. To make things easier, you can install using a local ISO image that you have already downloaded, or Pendrivelinux can download the ISO image for you (which makes it easy to try out new Linux distributions, if you have high-speed Internet). You simply download

KURT SEIFRIED

Kurt Seifried is an Information Security Consultant specializing in Linux and networks since 1996. He often wonders how it is that technology works on a large scale but often fails on a small scale.

the application and run it (Figure 1). Pick the operating system you want to run, whether or not you want to download it, and the target drive with a USB key or blank CD.

You also have the option of making a writable storage area if you're using a USB key. If you plan to use the disposable machine for testing something or need to download something, then you should select this option.

UNetbootin

Another option for creating a bootable USB key is UNetbootin [2]. UNetbootin is actually designed for installing full versions of Linux to USB keys or hard drives and does not support burning CDs or DVDs, so you can't make a read-only system easily. However, if you want a full-fledged Linux system that you can boot and run from a USB key, then UNetbootin is actually a better tool in some cases than Pendrivelinux.

"I use USB keys when surfing to potentially dangerous sites ..."

Using UNetbootin is pretty much the same as Pendrivelinux: You pick an operating system and version to install, pick your target drive, and hit *OK*. If you have a copy of the ISO for the operating system that you want to install, you can specify that. If not, UNetbootin will automatically download it. If you need to test an operating system quickly, this is by far the easiest way (Figure 2). However, if you get compromised, the attacker will be able to modify the operating system installed on the USB key – definitely something to be aware of.

MultiBootISOs

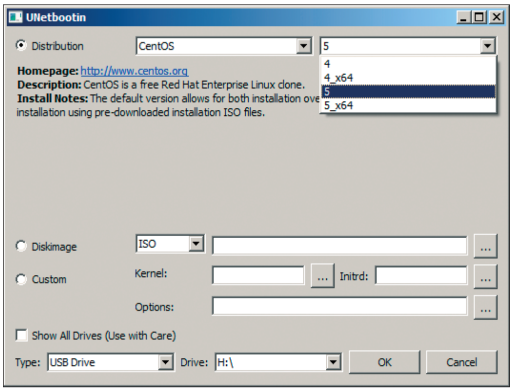
You may have noticed that when Pendrivelinux and UNetbootin are installing an operating system on a USB key, they take the entire USB key and won't share it with anything else. So, what happens if you want more than one operating system or utility disk burned to your USB key? If you're using 1 or 2GB USB keys, the simple answer is just to buy a bunch and have one operating system per key. But, what if you want your 16GB USB key to multi-boot all of them? You use MultiBootISOs [3].

MultiBootISOs has basically all the same operating system choices as Pendrivelinux (but not as many as UNetbootin, unfortunately) along with a few other choices like memtest86 (test your system memory for errors) and DBAN (Darik's Boot And Nuke, which provides disk wiping). It also has several security options, such as the AVG, AVIRA, BitDefender, and Kaspersky rescue disks (which should allow you to rescue a virus-infested Windows box) and Backtrack [4], which can be used for penetration testing (e.g., walk up to a machine on the internal network, plug the USB stick in, reboot, and, voilà, you're in).

LiLi USB Creator

Of course, I would be remiss if I only gave you two or three options. The final program to be covered is the Linux Live (LiLi) USB Creator. This program is very similar to Pendrivelinux and UNetbootin except that it makes setting up a persistent storage area very easy and also allows the size of that storage area to be configured easily (Pendrivelinux only has a few choices for size).

Linux Live is also the only one that will test download mirrors before downloading the ISO, which makes it less likely that you get stuck waiting for a slow site to give you the ISO image that you need.

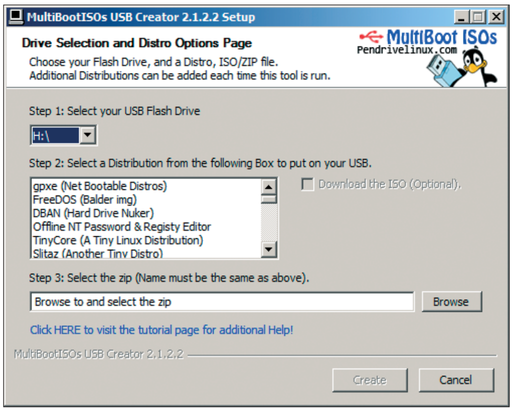

UNetbootin

● Distribution: CentOS; 5 (4, 4_x64, 5, 5_x64)

Homepage: http://www.centos.org
Description: CentOS is a free Red Hat Enterprise Linux clone.
Install Notes: The default version allows for both installation ove
installation using pre-downloaded installation ISO files.

○ Diskimage: ISO
○ Custom: Kernel: Initrd: Options:
□ Show All Drives (Use with Care)
Type: USB Drive Drive: H:\

Figure 2: UNetbootin running on Windows.


MultiBootISOs USB Creator 2.1.2.2 Setup

Drive Selection and Distro Options Page
Choose your Flash Drive, and a Distro, ISO/ZIP file.
Additional Distributions can be added each time this tool is run.

Step 1: Select your USB Flash Drive
H:\

Step 2: Select a Distribution from the following Box to put on your USB.
gpxe (Net Bootable Distros)
FreeDOS (Balder img)
DBAN (Hard Drive Nuker)
Offline NT Password & Registy Editor
TinyCore (A Tiny Linux Distribution)
Slitaz (Another Tiny Distro)
□ Download the ISO (Optional).

Step 3: Select the zip (Name must be the same as above).
Browse to and select the zip

Click HERE to visit the tutorial page for additional Help!

MultiBootISOs USB Creator 2.1.2.2

Figure 3: MultiBootISOs running on Windows.

Other Live CDs

If you just want to burn an ISO image to CD and be done with it, you won't be short of options. The LiveCD List [5] has more than 100 entries with links to the download locations. Also, almost every distribution now either makes a Live CD available or has a Live CD option during install.

Conclusion

This made me think about people who are not technologically sophisticated and may depend on you for support. Mailing someone a CD or a USB key instead of physically visiting them to set up the machine is very attractive, And, when upgrading the machine means simply mailing out another CD or USB key, I am tempted to say – just as we shouldn't give knives to toddlers – maybe we shouldn't give hard drives to people who can't take care of their computers. ■■■

INFO

[1] Pendrivelinux: *http://www.pendrivelinux.com/universal-usb-installer-easy-as-1-2-3/*

[2] UNetbootin: *http://unetbootin.sourceforge.net/*

[3] MultiBootISOs: *http://www.pendrivelinux.com/boot-multiple-iso-from-usb-multiboot-usb/*

[4] "Sleuthing" by Kurt Seifried, *Linux Pro Magazine*, August 2008: *http://www.linuxpromagazine.com/Issues/2008/93/SLEUTHING*

[5] LiveCD List: *http://www.livecdlist.com/*