AC 2009-2275: RUNNING LINUX IN A WINDOWS COMPUTER LAB

Ed Crowley, University of Houston

Running Linux in a Windows Computer Lab

Abstract

In many courses, the effective use of Linux, or other open source software, can expand and enhance active learning opportunities for students. Since many institutions have standardized on Windows Computer Laboratories, implementing Linux based learning experiences may initially seem problematic. However, with a Live Linux CD, you can quickly and easily run Linux, and related open source tools, in an existing Windows Computer Lab.

In this paper, we will explain how Linux Live CDs, and related Free and Open Source Software (FOSS), can be used to expand and enhance active learning opportunities available in existing Windows computer laboratories. For example, Free and Open Source Software (FOSS) and Live Linux CDs can enable students to continue their learning activities at home, or at their work place, with the same software that they use in their academic laboratory. Another example is that FOSS can enable students to demonstrate their laboratory activities in a work or even a job interview environment.

In this paper, we will first describe our program context and our FOSS based learning module design goals. We then present learning module summaries that include a listing of related Live CDs and open source software. We will also include survey results concerning utilization of Live Linux CDs and open source software. We will close with a discussion of future challenges.

Introduction

Over the past several years, our classroom experiences with Live Linux CDs have been very positive. Implementing Linux based learning modules in our Windows Laboratories have enabled our students to gain experience with some very sophisticated software tools. Often, these learning activities were conducted on computer systems preconfigured with Windows Operating Systems. From a student perspective, our surveys indicate an enthusiastically positive response to these Live Linux CD based learning experiences.

A Live Linux CD is a portable Linux distribution that boots and runs from a CD, DVD, USB stick, or similar device. By design, our Linux based structured learning experiences do not impact the Windows Systems upon which they run. That is, when students power down the systems and remove their Live CDs, the Windows Systems are in the identical state that they were prior to the laboratory.

Our Linux based learning activities require neither dedicated hardware nor dedicated support. For example, we have conducted Live CD based Linux Tutorials in Windows Labs at a variety of institutions including the New Jersey Institute of Technology, the University of Houston, and Lone Star Community College. We've also conducted "Hands On" tutorials in hotel and university conference rooms where attendees booted their own Windows based portable computers with the provided Live Linux CDs.

Currently, we even conduct structured "Hands On" learning activities in conventional classrooms where each student boots their own personal computer with the provided live Linux CD.

Context

Our environment is that of a small college at a large urban university. In our environment, resources, both hardware and support, are constrained. Fortunately, we are led by an entrepreneurial Dean and Chair that have created an atmosphere that facilitates the development of innovative and cost effective learning activities.

In disciple terms, we offer a graduate level security specialization within a Computer Information Systems (CIS) program. Currently, our undergraduate program is undergoing ABET accreditation while our graduate specialization curriculum is certified by the NSA through the Committee on National Security Systems (CNSS).

The focus of our four, three graduate hour, class specialization is enterprise security assessment and evaluation. Three of the courses have published technical goals. [1] From a technical perspective, our learning outcomes include a variety of areas including: computer security, network security, applied cryptography, and Internet security. Consequently, the learning modules that we have developed may be utilized in a number of technical areas. For example, our colleagues in Computer Engineering Technology have incorporated several of our applied cryptography learning modules into their courses.

Learning Module Design Goals

Before we created our active learning modules, we articulated several design goals. In specific, we wanted to:

1. Provide students with a portable laboratory environment that would enable them to continue their active learning after the class period has ended and the laboratory closed.
    a. Distribute laboratory software for free.
    b. Eliminate college's need to track software licenses.
2. Empower students to demonstrate laboratory learning activities at home or at work.
3. Free the instructor from administrative budget constraints (both time and cost).
4. Free the instructor to choose most appropriate software version. That is, depending on the particular situation, the instructor may:
    a. Implement a newly available software version or
    b. Continue using an existing version.
5. Leverage existing Windows laboratory infrastructure without impacting existing configuration or the ability of other classes to utilize Windows.

Table One presents a brief description of some of the learning modules that we have developed.

	Module	Live CD and Brief Description

1	Live CD Boot Process Live CDs Burning	Knoppix Students learn boot modes and methods available in Knoppix. Then, they use K3B to burn a new Knoppix Live CD from an ISO image. (ISO image may be downloaded or instructor provided.)
2	Footprinting	Knoppix Students use Linux command line utilities and browsers to gather information about computer systems and the entities to which they belong. Utilities include whois, dig, and nslookup.
3	Protocol Analysis HTTP, TCP/IP, DNS	Knoppix With the Wireshark protocol analyzer students capture packets as they visit specified web site. Analysis includes identifying TCP 3 way handshake and DNS server IP address. From their packet capture, students reassemble the web page.
4	TCP/IP with NetCat	Knoppix Students use NetCat utility to grab banners from web servers. Then, they use NetCat to establish a connection between two different computers and send text characters and text files between them.
5	Applied Cryptography	Knoppix Students employ OpenSSL to create symmetric (DES) keys. Students also create asymmetric (RSA) key pairs. Once keys have been created, students encrypt and exchange enciphered documents. Finally, students demonstrate file integrity with one way hashes (MD5 and SHA1).
6	Network Security Monitoring	Knoppix –NSM Snort, Sguil, NTOP, and BASE Students work with a graphical user interface that provides access to realtime network events, session data, and raw packet captures. Students gain experience by doing event driven analysis.
7	Network Monitoring	Back Track Students use EtherApe, a graphical network monitor, to perform real time network monitoring. Students work in teams where one team member uses NetCat, NMap, and DD to create network traffic. The other team member employs EtherApe to analyze the busy nodes and protocols.
8	Network Scanning	Knoppix Students use Network Mapper (NMap) to identify live systems on a network. They further identify the services (ports) that each machine is offering. Using this information, they establish a network baseline as well as a report identifying 'interesting' network nodes.
9	Forensic Analysis	Helix Students employ the Sleuth Kit and Autopsy to perform forensic analysis. Because these tools do not rely on the native operating system to process the file systems, students can demonstrate the recovery of deleted and hidden content.

10	System Scanning	Knoppix Students use Network Mapper (NMap) and the Nessus vulnerability scanner to identify open ports and other individual system vulnerabilities. They then use the CVE numbers reported by Nessus to further research the vulnerabilities.

Table One, Learning Module Descriptions

A glance at the software utilized in our sample modules will show that our students gain experience with a variety of sophisticated software tools including protocol analyzers, network monitors and intrusion detection systems in addition to the normal Linux command line utilities.

While calculating the cost of equivalent proprietary software tools would be an interesting project, FOSS and Live Linux CDs offer a free solution that is congruent with our module design goals. The next section elaborates on both FOSS and the following section elaborates on Live LinuxCDs.

Note
Some of the software that our security students employ is considered to be 'sensitive'. In our environment, none of this software violates our College's or our University's Acceptable Use Policy (AUP). Nonetheless, it would be prudent to check the policies governing your environment prior to employing tools like network mappers or protocol analyzers.

Free and Open Source Software (FOSS)

Free software has several popular definitions. For purpose of this paper, we will use the Free Software Foundation's (FSF) definition. [2] That is,

> Free software is software that gives you the user the freedom to share, study and modify it.

The FSF is the primary sponsor of the GNU project. In 1984, the GNU Project was formed to develop a complete Unix-like operating system. While the project was successful in developing utilities and related application software, the GNU project never completed a system kernel. Consequently, complete Linux Distributions are formed by combining selected GNU utilities and applications with the Linux kernel. Different distributions are then released under a variety of software licenses including the GNU General Public License (GPL).

The GPL gives every person who receives a copy of a work permission to reproduce, adapt or distribute the work as long as any resulting copies or adaptations are also bound by the same license. That is, future works are restricted to being released under the same license conditions as the original GPL code. In contrast to copyright, this aspect of GNU philosophy is known as copyleft.

Not all open source licenses are considered restrictive like the GNU GPL. For example, the Berkeley Software Distribution (BSD) license is considered a permissive open source license. That is, BSD style licenses have relatively few restrictions and do not support the GNU copyleft philosophy. Because BSD Style Licenses allow proprietary commercial use, there is widespread use of BSD code in commercial products such as Mac OS X.

Note also that a particular software package may be free without being open source. The Adobe Flash Reader is an example of a program that is free but not open source. Another example is that wireless card vendors that offer proprietary binary card drivers without making the source code available. These binary drivers are another example of free but not open source software.

Distinctions between licenses and software packages are important because thousands of separate software packages may be combined with other components including the Linux kernel to form a Linux distribution. Live CDs represent a particular class of distributions that distinguish themselves by offering a complete self configuring Linux system that may be booted from a CD or a similar media.

These distributions may be distributed as ISO files through the Internet. Or they may be distributed on a bootable media such as a CD, DVD, USB flash memory stick, or similar portable device. Now, we will examine Linux and Linux Distributions. Then, we will examine Live CDs.

Linux Distributions

A typical Linux distribution consists of multiple components including:

- Linux kernel
- GNU software tools and libraries
- Additional application and utility software
- Windows manager and desktop environment
- Applications and utilities
- Documentation

Linux distributions combine specific collections of utility and application software designed to appeal to specific audiences. For example, some distributions offer fully-featured desktops whereas other distributions may be server software focused and still others may be security focused.

Linux Distributions may be released under a variety of Open Source Licenses.
For example, the Knoppix Live CD uses GPL V2. Other distributions may contain free but not open source software. Within a particular distribution, different licenses may apply to separate software packages. Philosophical differences may also impact specific distributions. Table 2 presents several popular Live CD distributions.

Live CD	Description

Knoppix	Based upon Debian, Knoppix is generally considered the oldest and best documented Live CD. Using KDE as the default interface, Knoppix V5.11 contains many system and security tools including the Wireshark Protocol Analyzer and the Nessus vulnerability scanner.
Backtrack	Slax based, Backtrack focuses on security in general and penetration testing in particular. It simplifies complex configurations, including an automatic Kismet configuration and one click Snort Intrusion Detection System (IDS) setup.
Slax	Based upon Slackware, Slax aims to provide a broad software collection, while maintaining a CD image small enough to be written to a 185 MB CD. For the default interface, it uses KDE. It is modular in design and can be expanded through the addition of modules.
Puppy	Puppy Linux is a small Live CD that is optimized for speed and ease of use. On PCs that contain 256MB or more of RAM, it will boot entirely into RAM enabling the boot media to be removed. Because it is not based upon a preexisting distribution, Puppy is known as an independent Live CD.

Table 2 Live CD Distributions

Live CDs

Because Live CDs dynamically configure the hardware and can save their settings to a USB memory stick, or other transportable media, the utilization of Live CDs enables the same physical computer to host multiple class sections without increasing the need for dedicated lab support. As a byproduct of the dynamic configuration process, the Live CD is transportable between different hardware systems. For example, a student can make changes to a project in a laboratory, save those changes, and, later on his dormitory computer, revise those changes.

Note that the student may save their work in a variety of locations. For example, if the student has booted from a USB stick, then they may save their work to the same USB stick. They may also save to a separate USB stick. They may also save their work to an Internet based service such as Google Docs.

In addition to saving their own work, students are free to duplicate and distribute Live CDs. This means, students are free to work with their Live CDs at home or at other locations. For example, our graduate students have used their Live CDs to support presentations to local and regional professional organizations.

Live CDs provide an expedient way for students to gain experience with Linux and with Linux based software tools. Our students have responded very positively to the utilization

of open source tools and Live CDs. Anecdotally, many students report a very high perceived value added to the classes in which Live CDs are utilized.

Summary Freedom and Empowerment

Our experiences can be summarized in two general categories: Freedom and Empowerment. These results are summarized in Tables 3 and 4. Our experiences indicate that use of FOSS has potential positive attributes for students, instructors, and administrators.

Group	Freedom
Students	Freedom to continue their work at home, at work, or at other places.
	Freedom from needing to use the school's computer laboratories.
Instructors	Freedom from their school's budget and purchasing cycles.
Students and instructors	Freedom to utilize whatever software best meets their educational goals.
Schools	Freedom from the need to provide open lab time
	Freedom from the need to track software licenses
Data	Freedom from proprietary formats

Table 3 Live CD Freedoms

Group	Empowerment
Students	Empowered to gain experience as computer administrators without the possibility of impacting other students or classes
	Empowered to legally distribute laboratory software with their friends or coworkers.
Instructors	Empowered to choose software without regard to budget or purchasing constraints.
Schools	Empowered to use laboratory hardware for multiple purposes rather than for a single dedicated purpose (or class).

Table 4 Live CD Empowerments

Survey Results

When we began to employ Live CDs in our classes, we were concerned with how the students would react to them. We were especially concerned because previously our students had worked in Windows laboratories exclusively. We also were concerned because of our perceptions that our students did not to have significant exposure to command line utilities.

To ascertain our student's perspectives, we created a survey. The survey employed a five point scale with five meaning that a student strongly agrees and one meaning that a student strongly disagrees. Table 5 demonstrates that the students strongly agree that the Live CDs added value to the class.

Question	Response
The use of Live CDs added value to the class.	4.7

The use of free and open source tools added value to the class.	4.7
The ability to take a Live CD to home or to work added value to your class experience.	4.5
The ability to duplicate and distribute Live CDs added value to you class experience.	4.3

Table 5 Live CD Survey Results

For Future Study

Utilizing Live CDs along with open source software has been a very positive and rewarding experience. But there is much more that can be done.

Our experience with developing and teaching our security classes show a clear progression. Seven years ago, we taught in a dedicated lab where the students installed both Windows and Red Hat Linux on a replaceable hard drive. Then, we migrated to an environment where we employed scratch Windows Systems on replaceable hard drives along with Live Linux CDs. Now, we are contemplating using the students own laptops where Windows are required along with Live Linux CDs.

Our direction of change is to, over time, employ more FOSS along with fewer dedicated college resources. In addition to the student, instructor, and institutional goals that we have already articulated, this trend provides the college with increased options concerning how to scale the class as the program expands.

An interesting project that has developed in parallel with our use of Live CDs is the use of free web resources that our students use to produce their learning portfolio for each class. Currently, for each of our security classes, students use Google, (Groups, Sites, Pages, Blogger, …) to create an online learning portfolio. This term, we are also going to have the students remaster Knoppix to produce a custom Live CD that also displays their learning portfolio. We feel that these portfolio projects have the potential to greatly expand our assessment efforts.

In summary, there appears to be a bright future for the academic use of open source software in general and Linux Live CDs in particular.

Bibliography

[1] Crowley, E., Information System Security Curricula Development, Conference on Information Technology Education, SIGITE, West Lafayette, IN, 2003.

[2] Free Software Foundation, Retrieved Dec 09 from: http://www.fsf.org/

[3] Granneman Scott ,Live CD paradise, The Register, 7th May 2005, Retrieved Dec 08 From: http://www.theregister.co.uk/2005/05/07/live_cd_paradise/.

[4] Matthews, Jeanna, Hands-on Approach to Teaching Computer Networking Using Packet Traces, Conference on Information Technology Education, SIGITE, Newark, N.J., 2005.

[5] "The LiveCD List", Retrieved Dec 08 from:
http://www.livecdlist.com/

[6]Walden, Chris, The Distro Jungle, 28 Jun 07. Retreived Dec 08 from:
http://www.ibm.com/developerworks/linux/library/l-linux-distros/