Portable Operating Systems and Information Security Risks

Thomas S. Hyslip

East Carolina University

Abstract

A recent review of online retailers shows 2GB USB flash drives selling for under $10.00, CD/DVD-RW drives for only $30.00 and CD-R media for under $0.20 a piece. Couple this with the growing community of open source software developers and portable operating systems are becoming a real threat to information security. This paper examines the threat of portable operating systems to computers and computer networks, as well as the security measures available to prevent such exploits. The research examines the different types of portable operating systems and the available portable media such as USB flash drives, CD-R/RWs, portable media players, and micro hard drives. It also explores the available sources of programs and instructions for utilizing portable executables.   In all these examples, the paper provides hands on research, examples, and screen captures of actual running portable operating systems, as well as the steps required to duplicate the exercise.

Portable Operating Systems

Over the past 20 years we have moved from portable operating systems to fixed operating systems and back to portable operating systems. Initially all personal or “micro” computers ran on portable operating systems that were loaded into Random Access Memory (RAM). These operating systems such as Beginner's All Purpose Symbolic Instruction Code, or BASIC, and Disk Operating System, or DOS, as they are better known, were loaded from paper, tape, or floppy disks into RAM, and enabled the user to input commands that the computer would remember. Sherman (1997) points out that in 1975 BASIC was the first commercially available operating system for the first micro computer, the Altair, and it was all made possible by Bill Gates and Paul Allen. (p. 1). For the next 5 years all personal computers used some version of a portable operating system. But in 1980 this all changed. According to the DUX Computer Digest “In 1980, Seagate Technology introduced the first hard disk drive for microcomputers, the ST506.” (p. 1).

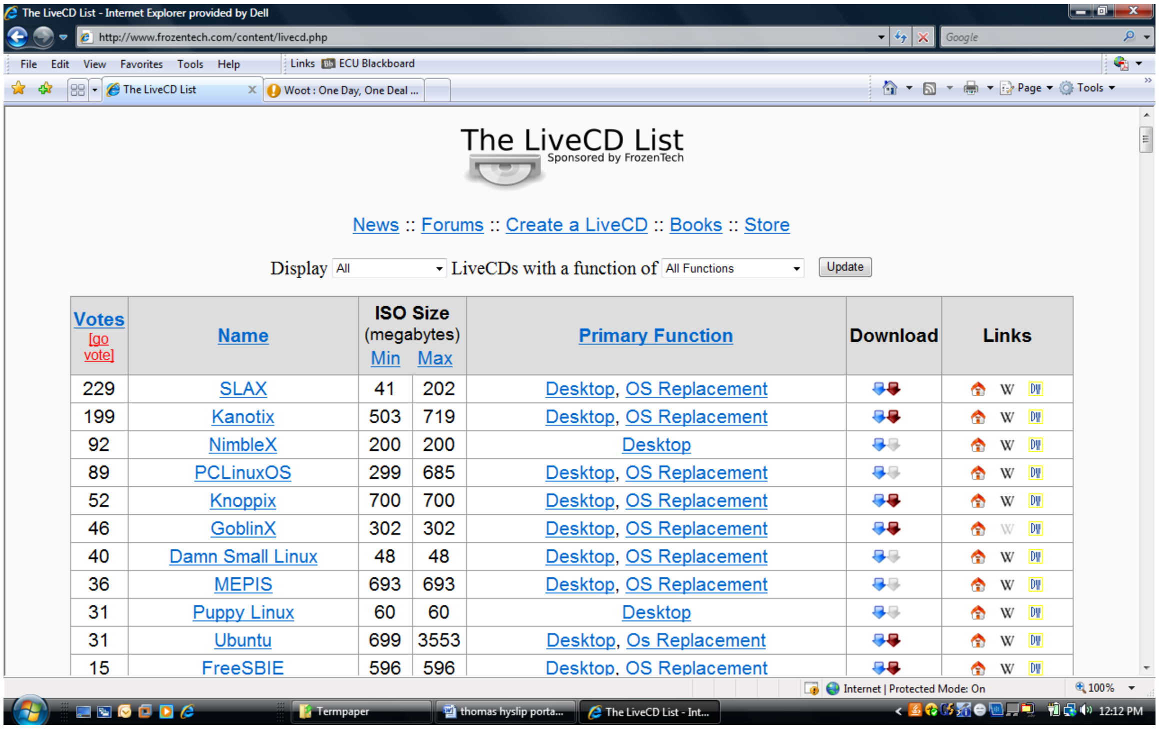
The creation of the hard disk drive has to be considered one of the most revolutionary inventions for personal computers. Without the hard disk drive, the functionality and usability of the personal computer we have come to expect would not have been possible. For the next 2 decades the personal computer as we know it today was developed. Even with the creation of the hard drive, the floppy disk continued to be used with portable operating systems and is still heavily in use to today. Although it is used more as a rescue or recovery disk, it is still a portable operating system that is loaded each time the computer is started with a floppy disk.

The Live CD

With the creation of the recordable CD-Rom or CD-R and inexpensive CD drives capable of “burning” CD-Rs, the portable operating system took on a new life. Prior to this, there were plenty of bootable CD-Roms, but personal computers were not capable of creating such disks. If you have installed Windows 95, 2000, or XP on your computer then you have used a bootable CD-Rom. But these were not portable operating systems. The CD-Roms where used to install an operating system onto a hard disk drive not run an operating system from the CD.

Sometime around the turn of the century, the first “modern” portable operating system was developed with the creation of the Live CD. The Live CD is a complete operating system that runs completely from the CD-Rom without using a hard disk drive. Unlike its predecessors like MS-DOS, the Live CD is a complete operating system with all the bells and whistles users have come to expect. This includes GUI interfaces, networking, word processors, spreadsheets, and games. Today there are hundreds of different Live CDs available for download on the internet, and it is fairly easy to create your own Live CD from scratch. Unless you need very specific software included with your Live CD, it is highly recommended that you use one of the already created Live CDs readily available on the internet. And chances are if you search long enough you will find a Live CD that includes the software title you are looking for. The best resource I have found for distributions of Live CDs is the website, http://www.frozentech.com/content/livecd.php. The site includes user feedback of the different Live CDs, as well as links to the download sites for each Live CD. Below is a screen capture of the website and you can see some of the Live CD version available, including SLAX, Knoppix, and Damn Small Linux.

Figure 1. Live CD List.


The LiveCD List - Internet Explorer provided by Dell
http://www.frozentech.com/content/livecd.php
Google
File Edit View Favorites Tools Help
Links ECU Blackboard
The LiveCD List
Woot : One Day, One Deal ...
Page
Tools
Internet | Protected Mode: On
100%
Termpaper
thomas hyslip porta...
The LiveCD List - Int...
12:12 PM

The LiveCD List
Sponsored by FrozenTech

News :: Forums :: Create a LiveCD :: Books :: Store

Display All LiveCDs with a function of All Functions Update

Votes [go vote]	Name	ISO Size (megabytes)		Primary Function	Download	Links
		Min	Max			
229	SLAX	41	202	Desktop, OS Replacement	⬇⬇	⌂ W
199	Kanotix	503	719	Desktop, OS Replacement	⬇⬇	⌂ W
92	NimbleX	200	200	Desktop	⬇⬇	⌂ W
89	PCLinuxOS	299	685	Desktop, OS Replacement	⬇⬇	⌂ W
52	Knoppix	700	700	Desktop, OS Replacement	⬇⬇	⌂ W
46	GoblinX	302	302	Desktop, OS Replacement	⬇⬇	⌂ W
40	Damn Small Linux	48	48	Desktop, OS Replacement	⬇⬇	⌂ W
36	MEPIS	693	693	Desktop, OS Replacement	⬇⬇	⌂ W
31	Puppy Linux	60	60	Desktop	⬇⬇	⌂ W
31	Ubuntu	699	3553	Desktop, Os Replacement	⬇⬇	⌂ W
15	FreeSBIE	596	596	Desktop, OS Replacement	⬇⬇	⌂ W

The main advantage of the Live CD over other types of portable operating systems is its simplicity. Almost 100% of computers today are able to boot from a CD and most users are familiar with burning a CD-Rom from an ISO image. Furthermore, the Live CDs have been around long enough that the majority of operating systems have a Live CD available. There is even a Live CD for Windows XP called, Bart's Preinstalled Environment (BartPE) bootable live Windows CD/DVD, or more commonly referred to as Bart's PE. Bart's PE is available at http://www.nu2.nu/perbuilder/. During my research however I have found that the best Live CDs are based on some version of Linux. These Linux based portable operating systems are very easy to install and do not make any changes to the hard disk drives attached to the computers unless the user manually mounts the hard drives as writeable and modifies the stored data. Furthermore, the entire operating system is loaded into RAM from the Live CD so there is no residual data on the PC. While this is great for anonymous computer access and ease of operation, it is very threatening to information security. If a computer's BIOS is set to boot to the CD drive prior to the local hard drive, all security measures will be defeated by a Live CD. The user will not need a user name or password, if the network is running DHCP, the Live CD will acquire an IP address and the user will have network access. One disadvantage of the Live CD is the inability to store data to the CD. Thus any changes a user makes to the operating system will not be present the next time it is used. Plus the user cannot store any data to the Live CD; they must utilize a secondary storage device such as an external hard drive or USB flash drive. While this is a shortfall of the Live CD, it is an advantage for information security.

Creating a Live CD

There are only four steps required to create and use a Live CD and they are provided below.

Figure 2. Steps to create Live CD

1 Download ISO image of Live CD

2 Burn image to CD/DVD

3 Ensure Computer BIOS is set to boot to CD prior to Hard Drive

4 Reboot Computer with the Live CD

During my research I created Live CDs using the following operating systems; Knoppix, Slax, Ophcrack, Backtrack, Helix, Damn Small Linux, Ubuntu, CentOS, and Damn Vulnerable Linux. The ISO images were all obtained free online at the following websites.

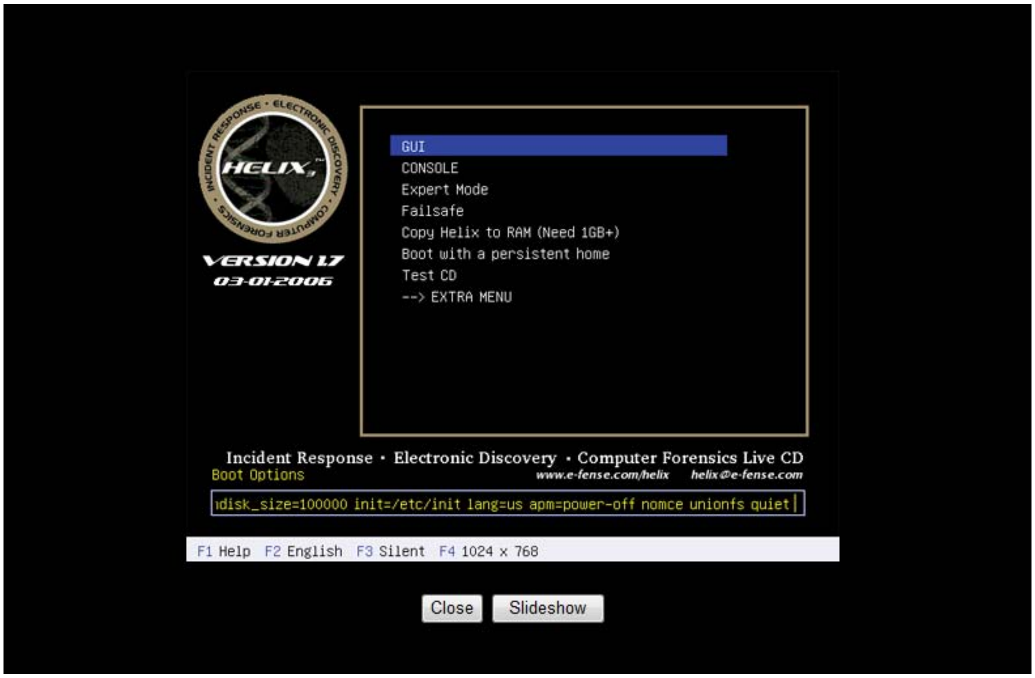
Figure 3. Live CD Websites.

Operating System	Website
Knoppix	www.knoppix.org
Slax	www.slax.org
Ophcrack	www.ophcarck.sourceforge.net
Backtrack	www.remote-exploit.org/backtrack_download.html
Helix	www.e-fense.com/helix/index.php
Damn Small Linux	www.damnsmalllinux.org
Ubuntu	www.ubuntu.com
CentOS	www.centos.org
Damn Vulnerable Liunx	www.damnvulnerablelinux.org

The 9 different operating systems can be broken down into 3 categories, desktop replacement, incident response and forensics, hacking / security. The desktop replacement versions are Knoppix, Slax, Damn Small Linux, Unbuntu, and CentOS. Helix is the only incident response and forensic operating system. While Backtrack, Ophcrack and Damn Vulnerable Linux should be considered hacking / security operating systems. The desktop replacement Live CDs are all pretty standard with GUI interfaces, office suites, email clients, web browsers, and games all preinstalled with the operating system. Although these Live CDs do not have many tools available other than standard Linux tools, they are still a threat to information security because the Live CD bypasses any computer logons with the installed operating system. They also allow the user to mount external USB drives and copy any data off the computer or delete data. The Live CDs also gives users network access and ability to browse the network.

Helix is really 2 resources in one. First it is the Live CD portable operating system that comes with computer forensics and incident response software preinstalled. It includes tools to make bit for bit images of hard drives with MD5 hashing capability, recycle bin analyzers, cookie analyzers for internet explorer and root kit hunters, plus many more. I highly recommend this portable operating system to anyone working in the information security field. Helix has the same information security concerns as the Desktop replacement Live CDs.

Figure 4. Helix Boot Screen.

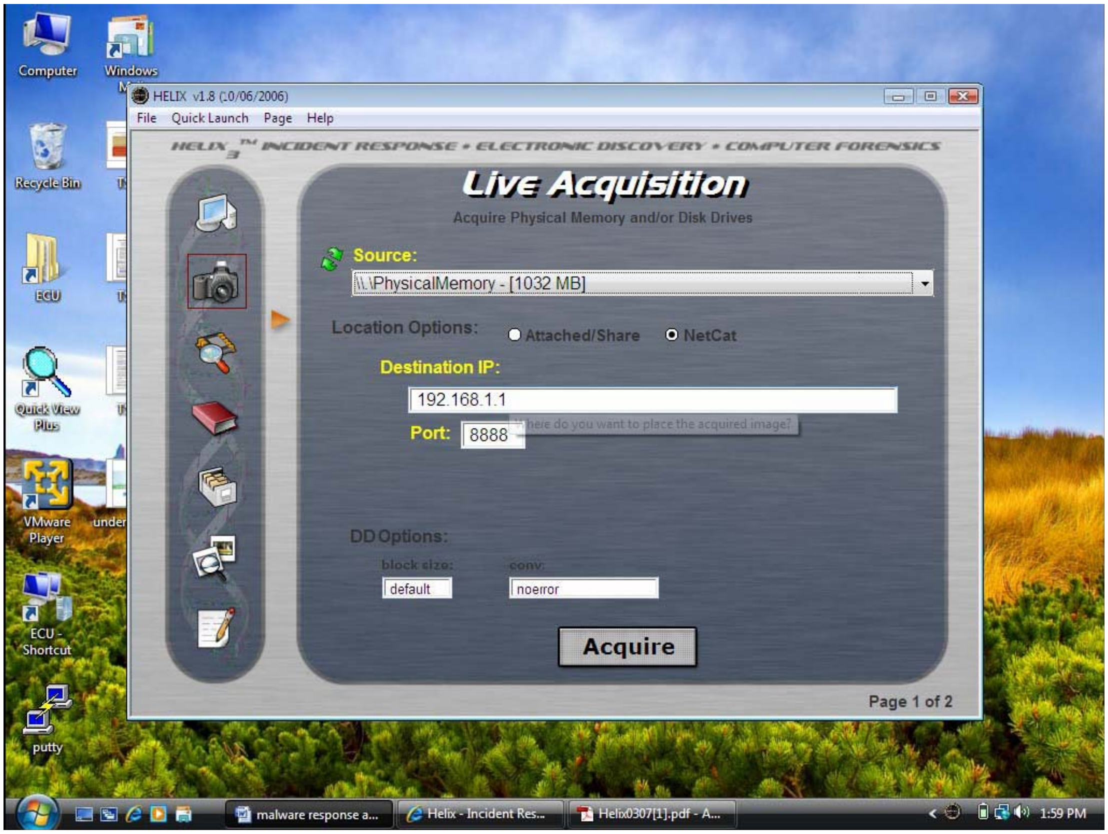

INCIDENT RESPONSE • ELECTRONIC DISCOVERY • COMPUTER FORENSICS
HELIX
VERSION 1.7
03-01-2006
GUI
CONSOLE
Expert Mode
Failsafe
Copy Helix to RAM (Need 1GB+)
Boot with a persistent home
Test CD
--> EXTRA MENU
Incident Response • Electronic Discovery • Computer Forensics Live CD
www.e-fense.com/helix
helix@e-fense.com
F1 Help
F2 English
F3 Silent
F4 1024 x 768
Close
Slideshow

Boot Options

```
ıdisk_size=100000 init=/etc/init lang=us apm=power-off nomce unionfs quiet
```

The second part of the Helix CD is a live analysis tool for running Windows systems. While not directly related to the paper topic, it is still worth mentioning. If a computer is suspected of being compromised you can run the Helix CD within Windows on the suspect computer and it will provide you with very valuable information including a list of running process and process IDs, as well as the ability to image running RAID arrays, and the RAM of the suspect computer.

Figure 5. Helix Live Acquisition of Physical RAM.



Source: \\.\PhysicalMemory - [1032 MB]

Location Options: ○ Attached/Share ● NetCat

Destination IP: 192.168.1.1

Port: 8888

Where do you want to place the acquired image?

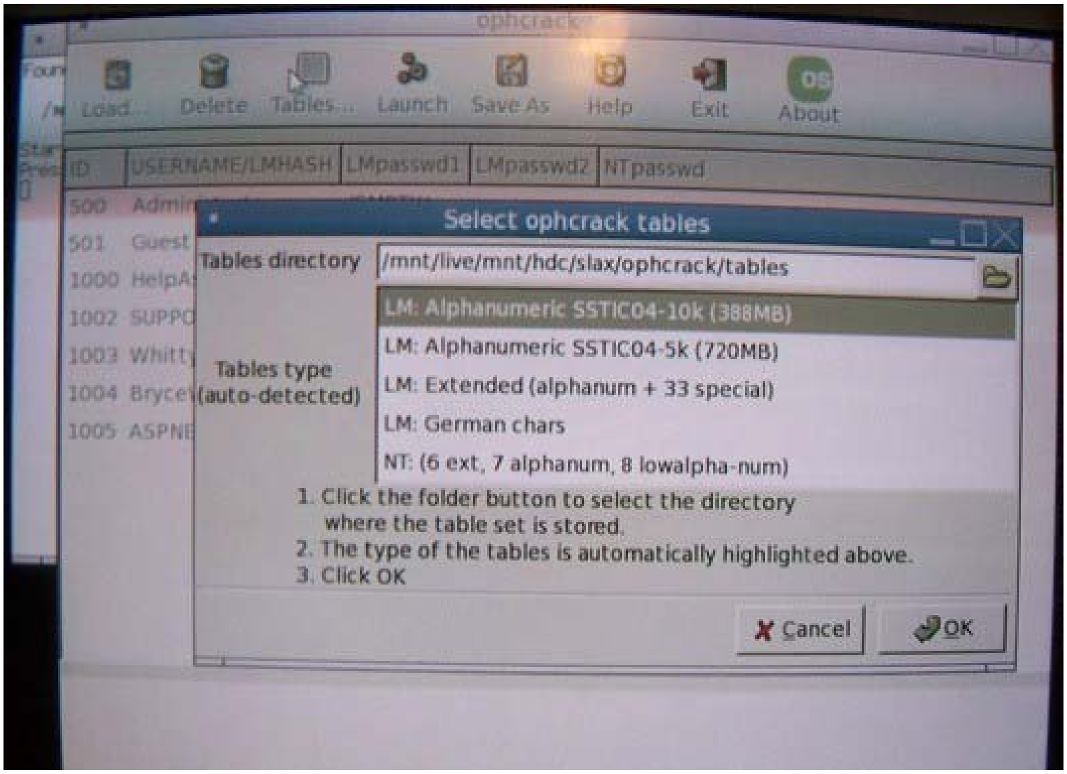
DD Options:

block size: default

conv: noerror

The final three Live CDs can be further broken down into 2 sub categories; password breaking and hacking / security. Ophcrack is unique Live CD in that its only purpose is to break passwords. It is based on the Slax version of linux but does not include the majority of the Slax functionality. When the Live CD boots the computer it searches for any password files on the local hard drives and begins breaking the passwords. If Ophcrack finds more than one SAM file, it provides the user the option to choose which SAM file to break first. Ophcrack also provides the user the option of which passwords to attempt first, either rainbow tables, or brute force. There really is no valid reason for a user to have an Ophcrack CD and attempt to use it in a work environment. The information security concerns are great because any user could put Ophcrack into a computer and break the user names and password resident on the computer.

Figure 6. Ophcrack Rainbow and Brute Force Tables.



Select ophcrack tables

Tables directory: /mnt/live/mnt/hdc/slax/ophcrack/tables

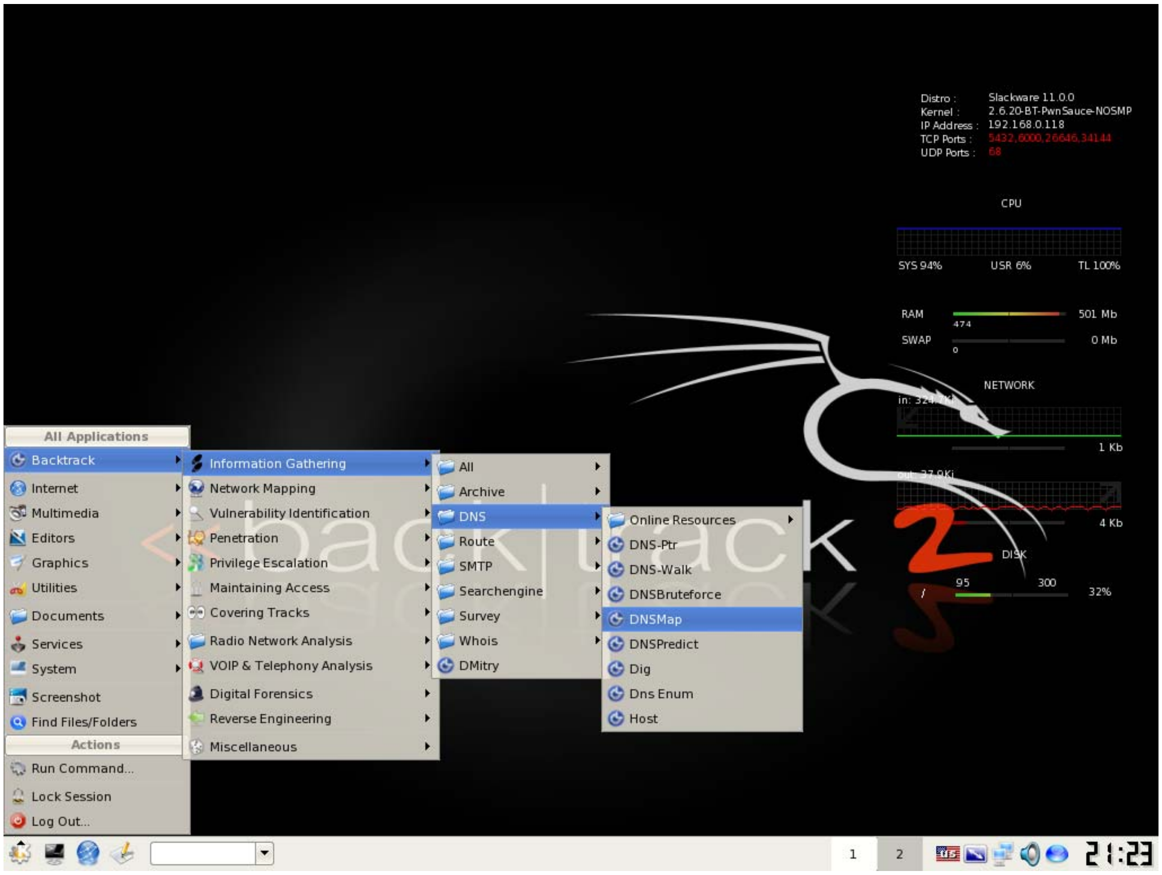
Tables type (auto-detected):

- LM: Alphanumeric SSTIC04-10k (388MB)
- LM: Alphanumeric SSTIC04-5k (720MB)
- LM: Extended (alphanum + 33 special)
- LM: German chars
- NT: (6 ext, 7 alphanum, 8 lowalpha-num)

1. Click the folder button to select the directory where the table set is stored.
2. The type of the tables is automatically highlighted above.
3. Click OK

The last 2 Live CD portable operating systems are very similar, Backtrack and Damn Vulnerable Linux. They both boot to a GUI interface and come with many of the same features as the desktop replacement Live CDs, but they also have hundreds of security and hacking tools installed. Backtrack for example comes with 24 information gathering software utilities, 21 network mapping utilities, 65 vulnerability identification utilities, 11 penetration utilities, 48 privilege escalation utilities, 15 maintaining access utilities, 1 covering tracks utility, 29 wifi / 802.11 utilities, 9 bluetooth utilities, and 28 utilities for forensics, VOIP, reverse engineering and SNORT. The list is way too large to list each utility but they can be viewed at http://wiki.remote-exploit.org/index.php/Tools. Below is a screen capture of Backtrack running with the menu for information gathering on the screen. You can also see the different options for privilege escalation, penetration, etc.

Figure 7. Backtrack Screen Capture



Distro : Slackware 11.0.0
Kernel : 2.6.20-BT-PwnSauce-NOSMP
IP Address : 192.168.0.118
TCP Ports : 5432,6000,26646,34144
UDP Ports : 68

While Backtrack and Damn Vulnerable Linux are great Live CDs and portable operating systems, be very careful which utilities you use on an open network, they could get you in trouble. Furthermore, there is no reason for a user to use either Live CD in a corporate environment. The tools available to the user are nothing a standard user should have access to and they will cause more harm than good.

Residual Data

To test the theory that Live CDs do not alter the physical data on the hard drives and do not leave any residual data I conducted a test using the 4 Live CDs, Knoppix, Helix, Ophcrack, and Backtrack, and a Solo III Image Master. First I created an image of the computer hard drive with the Solo III Image Master and saved the MD5 hash of the entire drive for the test. The MD5 hash is a unique number generated from a mathematical algorithm that is used in computer forensics to show that data has not been altered. Barbara (2008) states:

> It has been estimated that the odds of any two given hashes having the same value is 2^128. A very important fact concerning hashes is that even a small change in the message itself will result in a completely different hash value. In cryptology, this is referred to as the “avalanche effect,” meaning that when input to a message is slightly changed, the output is significantly altered.

The MD5 hash before the test was 4635f119dd0bfd96dde0eb24966fdee9. Then one at a time I booted the computer with the Live CDs, played around a bit on the computer and shut the computer down. Then I used the Solo III Image Master to create the MD5 hash again. Each time the MD5 hash was exact, proving the Live CDs did not alter any data on the hard drives nor leave any residual data on the drive. The great thing about these Linux Live CDs is they only mount the drives read only and the user must manually mount the drive as writeable to make any changes to the hard drive. The down side is that anyone could boot a computer, gain network access, copy files, delete files, and there would be no evidence the person ever used the computer.

USB Flash Drives

Sometime around 2005 motherboard manufacturers began to incorporate the ability for the motherboard BIOS to recognize USB drives during the boot process and boot the computer to an operating system on the USB device. I have not been able to determine which motherboard was the first to enable this feature, but many of the newer motherboards do boot to USB. However there is not a list of which motherboards support USB and the documentation with most motherboards do not cover this area in detail. So to tell if a computer will boot to a USB drive, you have to manually check the BIOS and then try to boot the computer to a USB drive. While this is very cumbersome there are many advantages to a portable operating system on a USB drive rather than a Live CD. The biggest advantage is with persistent data and the ability to save system changes to the USB drive. USB Drives also allow software to be installed and they operate just like a hard disk drive that users are accustomed to. While it is more difficult to install an operating system on a USB drive then burning a Live CD ISO, it is still a very simple process. For the purposes of this paper I choose to install Slax, Backtrack, and Knoppix on USB flash drives, and test their functionality.

Slax USB Drive

Slax was by far the easiest of the three to install since the website www.slax.org provides a tar file for a USB install. Below are the four simple steps required to install Slax onto a USB Flash Drive.

Figure 8. Steps to Install Slax on USB Flash Drive

1. Download tar file at www.slax.org/get_slax.php?download=tar
2. Extract files from tar file to the USB Flash Drive
3. Run bootinst.bat file from the USB Flash Drive
4. Change BIOS to boot from USB before UDD and reboot

One word of caution when installing Slax on the USB Drive; make sure you are within the USB Drive when you execute the bootinst.bat batch file. If you run this file from your hard drive it will modify the master boot record of the hard drive and you will not be able to boot your computer from the hard drive.

Backtrack USB Drive

To install Backtrack to a USB Flash Drive requires a few extra steps and a program such as Isobuster available at www.isobuster.com. But, it is still a very simple process.

Figure 9. Steps to install Backtrack on USB Flash Drive

1. Download Backtrack ISO from www.remote-exploit.org/backtrack_download.html
2. Run ISOBuster and open the Backtrack ISO

3. Extract the /boot and /BT folders from the ISO to the USB Drive
4. Run bootinst.bat file from the USB Drive
5. Change the BIOS to boot from USB before HDD and reboot

As you can see from the above steps the only difference is you have to manually extract the files from the ISO image with Backtract, while Slax provides the Files in a TAR file.

Knoppix USB Drive

The final portable operating system I installed to a USB Flash Drive is Knoppix. Since Knoppix only provides an ISO image available for download there are some extra steps involved in creating the Knoppix USB Drive.   First you have to install the HP USB format tool on your computer which is available at

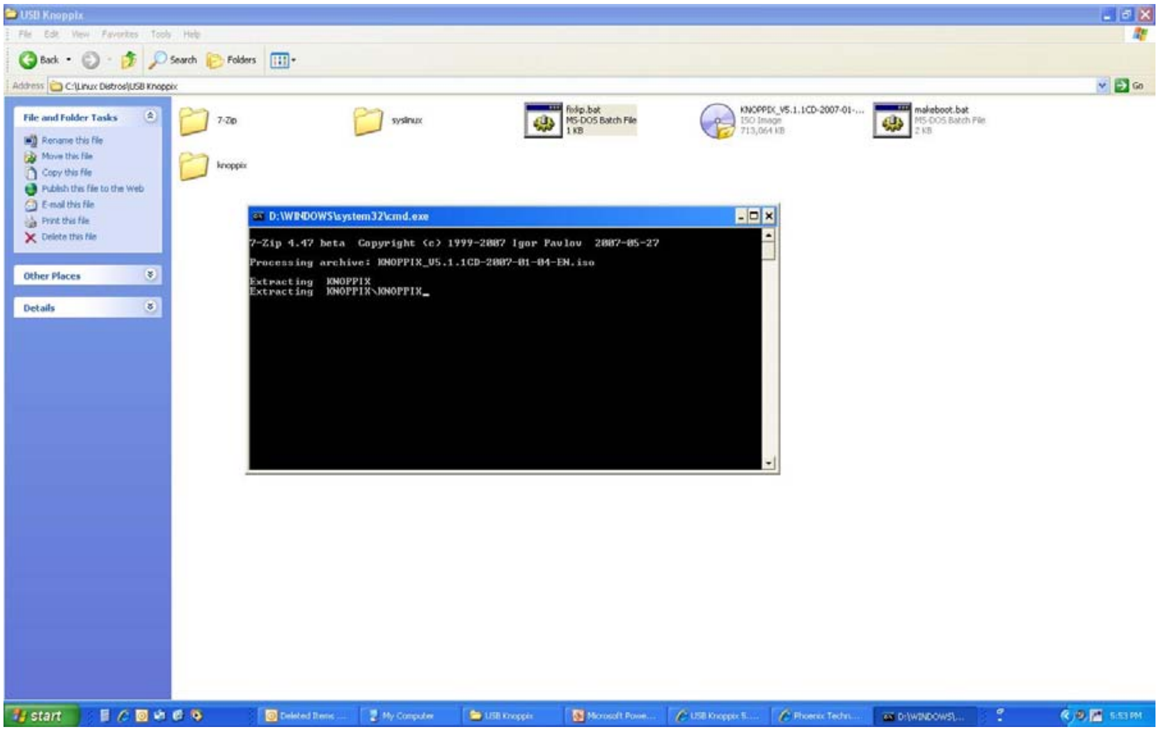
http://files.filefront.com/SP27608exe/;9868201;/fileinfo.html

Once you have installed this file, you have to format the USB flash drive with the tool as either FAT of FAT32. Then you create a folder on your hard drive named USB Knoppix. Download the Knoppix ISO from

http://www.kernel.org/pub/dist/knoppix/KNOPPIX_V5.1.1CD-2007-01-04-EN.iso

and save it to the USB Knoppix Folder. Next you must download the fixmp.zip file from http://pendrivelinux.com/downloads/fixkp.zip and extract the files to the USB Knoppix folder.   Next, from within the USB Knoppix folder, run the fixkp.bat file and follow the instructions. Below is a screen capture of the output.

Figure 10. Knoppix Install fixkp.bat output.



```
7-Zip 4.47 beta  Copyright (c) 1999-2007 Igor Pavlov  2007-05-27

Processing archive: KNOPPIX_V5.1.1CD-2007-01-04-EN.iso

Extracting  KNOPPIX
Extracting  KNOPPIX\KNOPPIX_
```

The batch file extracts the contents of the Knoppix ISO to a sub folder, “Knoppix” within the USB Knoppix Folder. Once this is complete, copy all the files from the new Knoppix folder to the USB drive. Finally run the makeboot.bat from your USB drive. Now you can reboot the computer and run knoppix from your USB drive. The one difference you will notice with the Knoppix USB Drive, you are actually running the Live CD ISO from the USB Drive. It works great, but is different than the other USB installs we did early. One significant difference I noticed during testing is the in-ability to store persistent data. Since the computer thinks it is booting to a Live CD it will not allow you to mount the disk as writeable and store data on it. This is a significant draw back when compared to the Slax and Backtrack USB drives that allow you to write to the USB.

The portable operating systems themselves operate the same whether they are on the Live CD or the USB flash drive so I will not explain the differences in the operating systems I provided previously. The only major difference is the ability of the USB portable operating systems to store data and make persistent changes to the OS.

Advantages

The advantages to using a portable operating system are many, especially with the USB flash drive installs. They allow you to take your entire OS and all your software programs with you.

Shaw (2006) explains:

> Its fun to watch the continuing evolution of the USB flash drive from just a storage device to a must have system that could eventually replace a notebook. It's not that far a stretch. USB drives can store all your data – the next big step is putting all your applications on them. Once that happens, you just need a dumb terminal with a PC, monitor and keyboard to get your work done.

I would say that time has already come, at least when working with Linux operating systems such as Slax and Backtrack. The portable operating systems also serve as a great rescue disk or virus recovery agent and allow users the opportunity to try different operating systems without replacing their current OS or using a third party software program such as VMWare.

Disadvantages

While portable operating systems provide many advantages to the user, they are far outweighed by the disadvantages to information security within the corporate world. First and foremost, if a portable operating system is able to be started it will bypass all security measures inherent to the installed operating system of the computer. The portable operating systems also gives users many tools they would not otherwise have access to on their computer, such as network scanners, password breakers, and remote exploitation tools. Furthermore, the only evidence the IT staff or law enforcement would have is network logs showing the IP address was assigned to a certain work station that exceeded its authorized access. There will be no evidence left on the computer where the portable operating system was utilized. Finally, the storage media utilized to run portable operating systems, CD-Roms and USB flash drives are common workplace items and will not raise concern among information security professionals.

Security

Should corporations be concerned about portable operating systems? After all it would take an employee or insider to get physical access to a computer and boot the portable OS right? According to Gordon (2006) in the FBI / CSI Computer Crime and Security Survey, “Despite some variation from year to year, inside jobs occur about as often as outside jobs. The lesson here, though, surely is as simple as this: organizations have to anticipate attacks from all quarters.” So now that you know you do not want users to run portable operating systems on their computers what can you do? It is really quite simple. First disable the BIOS options for the computer to boot to CD and USB. Then password protect the BIOS of the computer. If a user has a valid need to boot the computer to a CD or USB drive the IT staff can change the BIOS to allow it and then change it back after the user completes their task.

References

*Barbara, J.J. (2008). Computer Forensics Standards and Controls. Forensic Magazine. December 2007/ January 1008 Issue.

*DUX Computer Digest. Hard Disk Drive Guide, A Brief History of the Hard Disk Drive. http://www.duxcw.com/digest/guides/hd/hd2.htm

Gates, W. H. (1976). An Open Letter to Hobbyists. http://www.blinkenlights.com/classiccmp/gateswhine.html

* Gordon, L. & Loeb, M. &Lucyshyn, W. & Richardson, R. (2006). CSI/FBI Computer Crime and Security Survey. (p.15)

Kanellos, M. (2006). Half a Century of Hard Drives. CENT News. http://www.news.com/The-hard-drive-at-50/2009-1015_3-6112782.html

Polsson, K. (2008). A Brief Timeline of Personal Computers. http://www.islandnet.com/~KPOLSSON/comphist/mini.htm

Sammett, J.E. (1969). Programming Languages: History and Fundamentals. (p.27). Prentice Hall

*Shaw, K. (2006). Network World. USB Drives Become Application Powerhouses. (p.1).

*Sherman, J. (1997). History of Operating Systems. http://www.skrause.org/computers/os_history.shtml

Stotzer, M. Maximizing DOS "Conventional" Memory with DOS 5, 6, and 7 (Win95). http://winmac.mvps.org/doswin.html. April 1997

http://wiki.remote-exploit.org/index.php/Tools.

http://ophcrack.sourceforge.net/

www.knoppix.org

www.slax.org

www.ophcarck.sourceforge.net

www.remote-exploit.org/backtrack_download.html

www.e-fense.com/helix/index.php

www.damnsmalllinux.org

www.ubuntu.com

www.centos.org

www.damnvulnerablelinux.org

www.bootdisk.com/pendrive.htm

www.slax.org/get_slax.php

www.pendrivelinux.com/2007/01/01/usb-knoppix-510/

http://www.microsoft.com/whdc/archive/sub-boot.mspx