Interested in learning
more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Security Applications of Bootable Linux CD-ROMs

CD-ROM readers have been a part of the standard PC configuration for some time, and CD-R writers are close behind. CD-R writers and CD-R media are becoming increasingly inexpensive. The unit cost of media bought in bulk is low enough to make CD-Rs as disposable as paper cups - use it once and throw it away (a new opportunity for dumpster divers!). They are supplanting floppy disks and Zip disks. Their shelf life is said to be comparable to tapes. This paper skimmed over some of the possible Linux security applications ...

Copyright SANS Institute
Author Retains Full Rights

AD

Richard Bajusz

GSEC Practical Assignment Version 1.2e
Security Applications of Bootable Linux CD-ROMs

© SANS Institute 2001, Author retains full rights

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Introduction

Read-only media has been a standard feature of computing for a long time – from the write protection rings on tapes, to notches on 5 ¼" floppies, to jumpers on hard disks. The author's first exposure to read-only media as a security mechanism was several years ago when he first installed Tripwire on a Solaris file server. Tripwire's documentation strongly urged that the file of checksums be stored on read-only media so that an intruder could not modify them. The only read-only medium accessible at the time was the pitifully small 1.44 MB floppy disk. The floppy disk was sufficient to contain the file of checksums, but what if an intruder hacked the tripwire executables to hide his tracks? Clearly, tripwire itself should be stored on read-only media. Why not store the entire operating system on read-only media? This was hard to do. Sure, many SCSI disks had read-only jumpers, but using that feature would require not only rebooting when any change had to be made but also finding a screwdriver, opening up the case and twiddling with jumpers. It just wasn't worth the effort.

CD-R & Bootable CD-ROMs

Today with the advent of CD-Rs, a form of WORM (Write Once, Read Many media), we have the ability to create usefully sized and convenient read-only media. Not only that, most modern PCs can be made to boot from a CD-ROM by a simple BIOS setting.

Several vendors have begun selling commercial products that are based on bootable CD-ROMs. One example is the *SuSE Linux Firewall on CD*. This firewall boots and runs entirely off of a CD-ROM, with its configuration files coming from a floppy disk that can itself be write protected. There is no need for a hard disk at all since logs can be sent via network to a logging host. Assuming an intruder breaks into a firewall such as this, what permanent damage can he do to the firewall it self? No files can be modified, so any damage he might manage to inflict will be gone after a simple reboot of the system.

A similar technique can be used for a web server. Imagine a web server with several CD-ROM drives and no hard disks. The server would boot from a CD-ROM, serve static content the other CD-ROMs, and pull any dynamic content necessary from a database server that's behind it's own custom firewall (That's three PCs doing the work of one, but mid-range PCs are cheap, and defense in depth is crucial). The web server could be running Tripwire, or a similar daemon, configured to simply reboot the server at the first sign of an intrusion. The web site could not be defaced. After a power outage the server would reboot itself with no possibility of file corruption. It is possible to create any number of different appliance like networked devices from inexpensive or surplus PCs and custom bootable Linux CD-ROMs.

There are tools available for creating bootable Linux CD-ROMs. In order to be bootable, a CD-ROM must conform to the *El Torito Bootable CD-ROM* specification, which involves placing the image of a boot floppy on the CD-ROM. The details of creating bootable CD-ROMs are beyond the scope of this paper (see Resources below for links to the Linux CD-Writing-HOWTO and Bootdisk-HOWTO).

Two very different, yet complimentary, free packages are discussed below as examples of how bootable CD-ROMs can be used as tools in a Linux System Administrator's utility belt.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

PLAC: Portable Linux Auditing CD

PLAC is a downloadable ISO 9660 image that is under 50MB so it can be burned onto a business card sized CD-R that is small enough carry around in one's shirt pocket or wallet. Business card CDs are becoming a popular means of distributing "multi-media brochures", and blank ones can now be found in most large computer stores. PLAC was designed by its creators to reduce their need for a laptop. It is a bootable Linux system containing a variety of security and recovery tools. While it contains useful hardware (Memtest86) and filesystem maintenance (Gpart, Parted, Ext2resize…) tools, it is also an excellent package for forensics and recovery.

Forensics & recovery

Among the difficulties one faces when investigating a security incident is knowing whether to trust the tools available on the compromised system. The intruder may have replaced the existing executables with others designed to cover his tracks, open up backdoors, or destroy data. Will *ls* really show all the files in a directory? Will *tar* backup files or delete them? Is simply logging in as root a safe thing to do?

One approach to dealing with an untrustworthy system is to remove its hard disks, install them in another system, and mount them on that system in order to examine them. PLAC simplifies this process by allowing the drives to be examined in place.

Simply booting any desktop PC off the PLAC CD-ROM provides a known good (uncompromised) Linux environment with which to work. PLAC uses several techniques to pack a lot of Linux into a small space. It starts with a relatively small kernel, and a large number of modules covering most common devices, including SCSI disks, tapes drives, and PCMCIA cards. PLAC uses a 30 MB ramdisk for its root filesystem and a cloop filesystem for /usr. Cloop refers to a filesystem that is stored as a single compressed file on the CD-ROM. This technique allows a 121 MB filesystem to be stored in only 43 MB on the CD-ROM.

When PLAC boots it presents the user with the following LILO prompt:

```
Portable Linux Auditing CD
PLAC version 2.9.5

Boot Options:
linux          diskless          debug
linux-800      diskless-800      memtest
linux-1024     diskless-1024
linux-1280     diskless-1280
linux-1600     diskless-1600
```

Choosing one of the 'linux' options boots the system as described above, with /usr mounted from the CD. If the system has enough memory, one of the 'diskless' options can be used to copy /usr into a larger ramdisk, thereby freeing up the CD-ROM drive for other uses. The size of the ramdisk can also be set manually with the kernel parameter, "ramdisk=X", where X is the ramdisk size in KB. The numbers in the list of options refer to the system's video resolution. Specifying the resolution allows PLAC to boot with an appropriate number of text lines on the console. The memtest option runs the excellent *Memtest86* utility to test the system's RAM.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

When PLAC boots, it searches all IDE and SCSI disks for any partitions with recognizable filesystems, and mounts them read-only. Once the system is booted, and the user has logged in as root with no password, the script *net-conf* can be run to identify the system's network card, load the correct kernel module, and configure the systems IP settings. The user is presented with a choice of either using a DHCP client, or manually entering the IP configuration. It is probably a good idea to connect the system to a different network, or at least use a different IP address while running PLAC.

Now that that the system is up and running PLAC, a full backup of the compromised system should be made. PLAC comes with the ability to write to tapes and CD-Rs making local backups simple. Backing up to remote devices can be done in a variety of ways since PLAC also includes OpenSSH, NFS, SAMBA, and Netcat. A bit stream backup (using *dd*) of all partitions, including swap partitions, along with their md5 checksums is best. CD-R tools are available, allowing backups to CD-ROM, but this is a difficult task as the filesystems to be backed-up may be much larger than the capacity of a CD-ROM.

After the backup is out of the way, it is time to examine the system to see what damage may have been done. Beyond the usual Unix utilities, PLAC includes two packages useful for forensics. The first, *chkrootkit*, can be used to determine if a rootkit has been installed on the system. It works somewhat like a virus scanner, examining a number of commonly trojaned system binaries for known signatures. It can also detect deletions from the lastlog and wtmp files. The other forensics tool is *The Coroner's Toolkit* (TCT). TCT is a tool for examining unallocated disk space and recovering deleted files. It can also search the swap partition for signs of processes that were running and whether they were SUID. TCT can also generate reports of what files have been created, accessed or modified during a given time frame.

Network auditing

PLAC also contains a number of tools for network auditing. With PLAC, one could sit down at any networked PC, pop in a CD-ROM, and after a quick reboot, start sniffing packets. Like many security tools, PLAC can be a danger in the wrong hands, but a danger that requires physical access.

Among the network oriented tools included with PLAC are:

- *Sniffit* – A general purpose IP packet sniffer
- *Dsniff* – A clever sniffing tool that specializes in sniffing switched networks. It can use several techniques to "trick" switches into sending packet its way.
- *Ettercap* – A multipurpose sniffer/logger that has may features including password collection. It can also perform arp-poisoning to work on switched networks.
- *MTR (Multi Router Traffic Grapher)* – A tool that uses SNMP to read traffic counters from routers and generates HTML containing graphical representations network load.
- *Nmap* – A stealth port scanner and OS fingerprinter.
- *Arping* – An ARP level ping utility. It can determine if an IP address is being used on a remote subnet. It can also ping MAC addresses directly.
- *Tcpspy* – Logs TCP/IP connections by local address, remote address, and user name
- *Hping* – A custom TCP/IP packet generator/analyzer with a traceroute feature.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

There is a lot of capability packed into the tiny PLAC CD-ROM; it also has *gcc*, *perl*, several filesystem recovery tools, and even a firewall. The one draw back of PLAC, at the time this paper is being written is its almost complete lack of documentation. The documentation that does exist is out of date and inaccurate. As the project matures, its documentation should improve. There are other bootable CD-ROMs including the *Linuxcare Bootable Toolbox* (LBT), a more general purpose bootable Linux CD-ROM which contains an X window environment.

MkCDrec: Make CD-ROM Recovery

An important concern after a security incident, or even a hardware failure, is recovery time. Getting vital systems up and running again as quickly as possible is critical. The management of an organization may consider restoring service more important than containment and eradication of a threat. There are a number of good system rescue tools available including PLAC and LBT. They all contain tools for editing and repairing partition tables, boot sectors, and filesystems. However, when using these tools is insufficient or to slow, the system must be restored from backup. Restoring individual files from backup is a simple and straightforward process, but restoring an entire system is more complicated.

MkCDrec combines the rescue and backup/restore functions into one tool that simplifies the task of restoring a complete system. Unlike PLAC, mkCDrec is not a bootable CD-ROM image, but it is rather a set of tools for creating a bootable disaster recovery CD-ROM. It creates an El Torito image containing the system's current kernel, kernel-modules, and important executables. This allows the rescue CD-ROM to boot and access whatever unusual hardware the system requires without wasting space for unnecessary kernel-modules. MkCDrec can also efficiently backup Ext2, Ext3, xfs, jfs, ReiserFS, msdos, fat, and vfat filesystems to CD-Rs.

How it works

MkCDrec comes with a number of tools useful for creating small Linux systems:

- *Busybox* – A space saving tool intended for embedded Linux applications that combines about 70 common Unix utilities into a single executable
- *ISOLINUX* -- A LILO replacement that allows booting from an ISO 9660 filesystem
- *Mkisofs* – A tool for creating and working ISO 9660 filesystem images
- *Mformat* – A Part of Mtools that is used to create a bootable floppy image
- *Tinylogin* – A tiny replacement for login (of course).

Some of the recovery tools included are:

- *Parted* – The GNU partition editor
- *Gpart* – A tool to reconstruct damaged partition tables
- *Recover* – A tool for recover deleted files
- *E2salvage* – A utility to recover data from damaged ext2 filesystems
- *Ext2resize* – A tool to change the size of an ext2 filesystes.

The tools and scripts for making rescue and backup CD-ROMs are tied together with a makefile. Running the command "make test" in the mkCDrec directory will determine if your system has

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

all the mkCDrec's prerequisites. If the system has been used to burn CD-ROMs before, chances are the prerequisites will be met. In the worst case, recompiling the kernel may be necessary.

To use mkCDrec the user runs *make* and is presented with a menu:

```
Enter your selection:
  1) Rescue CD-ROM only (no backups)
  2) Into /home/isofs (to burn on CD-ROM)
  3) Enter another path (spare disk or NFS)
  4) Enter (remote) tape device

Please choose from the above list [1-4]:
```

The first option only creates a rescue CD-ROM, while the other three options determine where backups will be saved. MkCDrec will backup Linux filesystems as compressed tar files, and Microsoft file systems as compressed byte streams. In order improve compression of the msdos, fat and, vfat filesystems, unallocated space is emptied by filling the file system to capacity with a file containing only NUL characters. The file is then deleted before the filesystem is backed up and compressed. In the case of option 2, mkCDrec can split the backup over several CD-Rs.

Assuming everything works as intended, the restoration procedure is very simple (an important feature when working under pressure!). The system is booted from the first CD-ROM in the backup set from that point on it runs entirely from a ramdisk. The user can try to resurrect the old system using the utilities provided or run the *start-restore.sh* script to restore the complete system from scratch. The *restore-fs.sh* script can also be used to restore a single file system. If restoring onto a fresh hard disk (or disks) mkCDrec is smart enough to provide some flexibility in laying out the partitions, as long as the new partitions are no smaller than the old ones. One can even restore onto a different kind of filesystem. This feature makes mkCDrec an excellent tool for migrating from ext2 to one of the supported journaling file systems.

MkCDrec creates a snapshot of the system at a given time, and makes it simple to return to that snapshot. It is probably not practical as a tool for regular backups, but it will get the system to a known good state on top of which the latest routine incremental backups can be restored. As always, the standard advise applies – practice the disaster recovery plan before a disaster occurs.

Summary

CD-ROM readers have been a part of the standard PC configuration for some time, and CD-R writers are close behind. CD-R writers and CD-R media are becoming increasingly inexpensive. The unit cost of media bought in bulk is low enough to make CD-Rs as disposable as paper cups – use it once and throw it away (a new opportunity for dumpster divers!). They are supplanting floppy disks and Zip disks. Their shelf life is said to be comparable to tapes.

This paper skimmed over some of the possible Linux security applications of CD-ROMs, and discussed two projects in some detail. The resources section below contains links to more information about some of the tools mentioned in this paper, as well as some related projects not mentioned. The number of tools intended to assist in the creation of bootable CD-ROMs is

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

growing. The author hopes this paper will inspire the reader to think of more creative uses for CD-ROMs in the field of security.

References

"Constructing a Bootable CD". June 6, 1995
Phoenix Technologies
http://www.phoenix/com/PlatSS/PDFs/wp-bootcd.pdf

Darwe, Mohammed. "The Linux Bootdisk HOWTO, section 10: Creating bootable CD-ROMs"
The Linux Documentation Project
http://www.linuxdoc.org/HOWTO/Bootdisk-HOWTO/cd-roms.html

Microsoft Support Services "How to Create an El Torito Bootable CD-ROM". August 10, 2001
http://support.microsoft.com/support/kb/articles/Q167/6/85.asp

Cohen, Fred. "Managing Network Security: Bootable CDs" August 2001.
http://www.all.net/journal/netsec/2001-08.html

Willer, Lori. "Computer Forensics". May 4, 2001
http://www.sans.org/infosecFAQ/incident/comp_forensics2.htm

Wagner, Mike. "The Coroner's Toolkit: A handy Suite of Utilities". December 13, 2001
http://www.sans.org/infosecFAQ/threats/coroners_toolkit.htm

Danielle, Lora. "Introduction to dsniff". June 1, 2001
http://www.sans.org/infosecFAQ/audit/dsniff.htm

Trumper, Winfried. "CD-Writing HOWTO".
The Linux Documentation Project
http://www.linuxdoc.org/HOWTO/CD-Writing-HOWTO.html

Knopper, Klaus. "Building a Self-Contained Auto-Configuring Linux System on an ISO9660 Filesystem".
http://www.knopper.net/knoppix/knoppix-als2000-paper-html

The SANS Institute. "Incident Handling Step by Step". Version 1.5. May 1998

Resources

PLAC – http://sourceforge.net/projects/plac
MkCDrec – http://mkcdrec.sourceforge.net
Busybox – http://busybox.lineo.com
ISOLINUX – http://syslinux.zytor.com/iso.php
LNX-BBC – http://www.lnx-bbc.org

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

SuSE Linux Firewall on a CD – http://www.suse.com/us/products/suse_business/firewall
Linuxcare Bootable Toolbox – http://lbt.linuxcare.com
Partition Image – http://www.partimage.org
Gpart – http://www.stud.uni-hannover.de/user/76201/gpart
Chkrootkit -- http://www.chkrootkit.org
Ext2resize – http://ext2resize.sourceforge.net
Parted – http://www.gnu.org/software/parted/parted.html
Memtest86 – http://www.memtest86.com

© SANS Institute 2001, Author retains full rights

Last Updated: May 25th, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Malaysia @ MCMC 2013	Cyberjaya, MY	Jun 03, 2013 - Jun 08, 2013	Live Event
SANS Pen Test Berlin 2013	Berlin, DE	Jun 03, 2013 - Jun 08, 2013	Live Event
Industial Control Systems Security Training - Houston	Houston, TXUS	Jun 10, 2013 - Jun 15, 2013	Live Event
Security Impact of IPv6 Summit 2013	Washington, DCUS	Jun 14, 2013 - Jun 16, 2013	Live Event
SANSFIRE 2013	Washington, DCUS	Jun 14, 2013 - Jun 22, 2013	Live Event
SANS Canberra 2013	Canberra, AU	Jul 01, 2013 - Jul 13, 2013	Live Event
Digital Forensics & Incident Response Summit 2013	Austin, TXUS	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS London Summer 2013	London, GB	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS Rocky Mountain 2013	Denver, COUS	Jul 14, 2013 - Jul 20, 2013	Live Event
SANS Mumbai 2013	Mumbai, IN	Jul 22, 2013 - Jul 27, 2013	Live Event
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	Washington, DCUS	Jul 22, 2013 - Jul 26, 2013	Live Event
SANS San Francisco 2013	San Francisco, CAUS	Jul 29, 2013 - Aug 03, 2013	Live Event
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	Bangalore, IN	Aug 05, 2013 - Aug 10, 2013	Live Event
SANS Boston 2013	Boston, MAUS	Aug 05, 2013 - Aug 10, 2013	Live Event
Critical Security Controls Summit	Washington, DCUS	Aug 12, 2013 - Aug 18, 2013	Live Event
Industrial Control Systems Security Training - DC	Washington, DCUS	Aug 12, 2013 - Aug 16, 2013	Live Event
SANS Thailand 2013	Bangkok, TH	Aug 19, 2013 - Aug 31, 2013	Live Event
SANS Virginia Beach 2013	Virginia Beach, VAUS	Aug 19, 2013 - Aug 30, 2013	Live Event
Mobile Device Security Summit 2013	OnlineCAUS	May 30, 2013 - Jun 06, 2013	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced