Global Information Assurance Certification Paper

Biatchux: A New Tool for Incident Response

SANS GSEC Practical Assignment
Joe Lofshult
Version 1.3
Submitted April 11, 2002

Abstract

The system administrator at another company notifies you that computers at your site may have been compromised. In order to investigate what is happening, you need a pre-made toolkit you can pull out of your desk drawer and start using right away. Biatchux is such a tool. It is a new bootable Linux distribution created specifically for incident response, forensic analysis, and penetration testing. This paper describes Biatchux and analyzes its usefulness for responding to security incidents and performing forensic analyses.

The version of Biatchux reviewed for this paper is still a beta release (0.1.0.6b). While in this release it has some shortcomings, overall it's a very useful tool for performing an initial analysis of incidents on Windows 2000/NT, Linux, and Solaris systems. It also provides tools for performing in-depth forensic analyses of Linux and Solaris systems.

Biatchux: A New Tool for Incident Response

Introduction

It's Monday morning after a nice relaxing weekend. You walk into the office, sit down with a nice hot cup of coffee, and start checking your e-mail. You peruse a few system reports generated over the weekend, scan a few messages from your favorite e-mail lists, and then...what's this? An e-mail from a system administrator at another company claiming that over the weekend his network intrusion detection system has logged numerous attempted scans of his system on port 111, and the scans seem to be originating from systems on your network. You're suddenly wide-awake, but what do you do now?

Obviously, something is going on, but what? You quickly log in to one of the systems identified in the e-mail message, a PC running Linux, to have a look around. You check the running processes, but there's nothing unusual there. You check the network connections using netstat, but again nothing unusual. But still, you suspect there is something wrong. Next, you log in to another of the systems identified, this time a Solaris system, but again you see nothing unusual.

Then it hits you - maybe there are rootkits installed. After all, that is one of the first steps an intruder will take after a system break-in to maintain access. In its simplest form, a rootkit is just a collection of utilities that replace the standard system versions. A rootkit such as LRK5 (Linux Rootkit 5) includes trojan versions of chfn, chsh, crontab, du, find, ifconfig, inetd, killall, login, ls, netstat, passwd, pidof, ps, rshd, syslogd, tcpd, and top, along with other programs to cover an intruder's tracks. These binaries allow an intruder to work unnoticed by preventing a user from seeing certain processes or network connections.

So if a rootkit is installed, how are you going to see what is going on? One way is to just pull the plug and perform a forensic analysis of the system. You'll want to do that too, but first you would like to get as much information as possible from the live systems about what is happening. However, if a rootkit is installed you can't trust the binaries on the systems. This is when you need an incident response toolkit with a collection of trusted, static binaries you can rely on. This is where Biatchux comes in. And once you're done with the live analysis you can continue to use Biatchux to perform a forensic analysis of the systems, if you like.

This paper will describe Biatchux and analyze its usefulness as a tool for incident response and forensic analysis. It will also compare Biatchux with Trinux and PLAC, two other Linux security toolkits.

Biatchux Overview

Biatchux is a new bootable CD-ROM Linux distribution that, according to its developers, was designed "with the goal of providing an immediate environment to perform forensic analysis, incident response, data recovery, virus scanning and vulnerability assessment."

(Salusky and Zendzian) It is distributed as an ISO image that, in the current release, version 0.1.0.6b, is 117 MB when uncompressed. After downloading the compressed ISO image to a Linux system and uncompressing it, you can take a look at its contents before burning it onto a CD-R disk by mounting the image using a loopback interface with the following command:

```
# mount -o ro,loop biatchux-v.0.1.0.6b.iso /mnt/image
```

The contents of the image are as follows:

```
-r-xr-xr-x    1 root     root           58 Feb 25 03:07 autorun.inf
-r-xr-xr-x    1 root     root         3640 Mar 12 19:25 Biatchux-Features.rtf
-r-xr-xr-x    1 root     root         1168 Feb 28 05:45 CHANGES
-r-xr-xr-x    1 root     root         6631 Mar 12 19:03 Documentation.rtf
dr-xr-xr-x    2 root     root         2048 Mar 12 19:29 images
-r-xr-xr-x    1 root     root          182 Mar 12 19:04 README.rtf
dr-xr-xr-x    5 root     root         2048 Feb 18 20:45 statbins
-r--r--r--    1 root     root         1900 Mar 12 19:36 v0.1.0.6b-Changes
-r--r--r--    1 root     root            0 Feb 28 01:26 v0.1.0.6b.txt
dr-xr-xr-x   13 root     root         4096 Mar 12 17:14 win32
```

The images directory contains the bootable Linux distribution. The statbins directory contains static binaries for Linux 2.2 x86 and Solaris 2.7 from incident-response.org, and Windows NT/2000 binaries from Cygwin. Finally, the win32 directory contains various security applications that can be run on Windows NT and 2000 systems.

Booting Biatchux

The next step is to burn the image onto a CD-R and attempt to boot from it. The first thing you are presented with when booting from the Biatchux CD-ROM is a custom LILO boot menu that contains three options:

- biatchux
- biatchux-serial
- Memtest86

The biatchux-serial option provides support for a serial console, terminal server, or modem. Memtest86 is a utility to run diagnostics on the memory in an x86 PC. The default option is biatchux (without serial console support).

Biatchux uses a cramfs filesystem for /lib and /usr to minimize the amount of disk space required on the CD-ROM, and it loads them into a ramdisk at boot time. It does not run completely in RAM, though, as some libraries are accessed from a .tgz file on the CD-ROM as they are required. Therefore, the CD-ROM cannot be removed from the drive after the system boots.

When the boot completes, Biatchux displays a "Welcome to Biatchux" screen (Figure 1). Biatchux provides a menu with a number of options for performing setup tasks and

forensic operations, and the Welcome screen describes where all output from these operations will be placed.

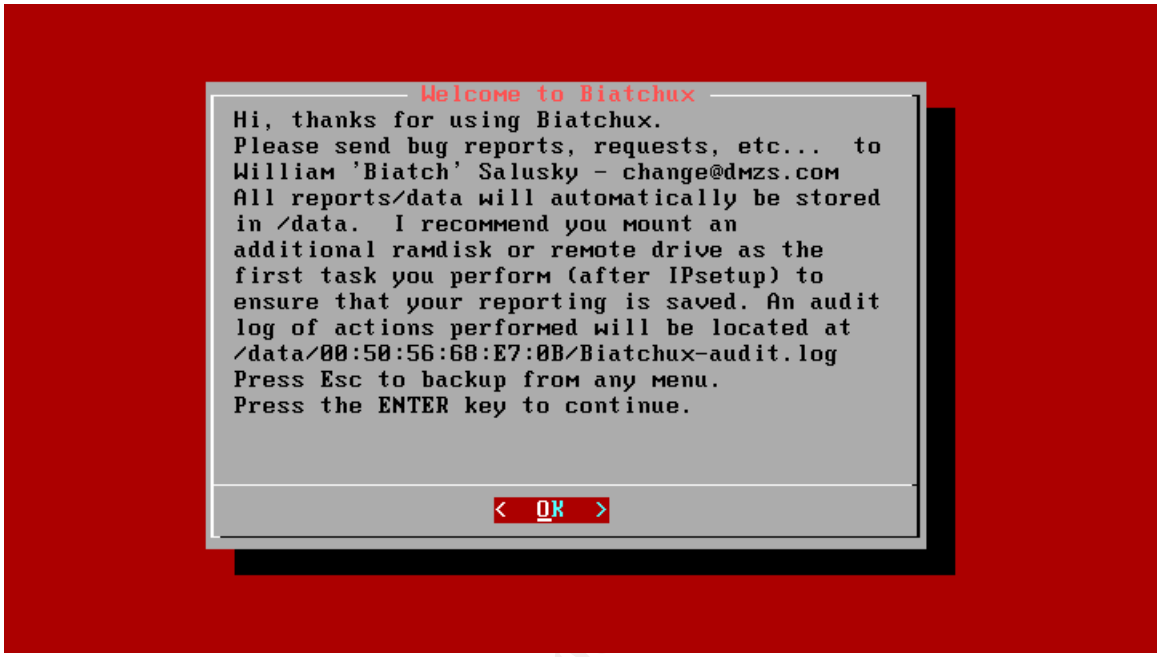

Figure 1

Once you press Enter to acknowledge the Welcome screen, you are presented with a menu with four options:

- Start-Here
- Forensics
- Virus-Scan
- PenTesting

In most cases, the first thing you'll want to do is select Start-Here, which takes you to the Getting Started Menu (Figure 2). From that menu, you can configure a static IP address or configure the IP via DHCP. You can also start a VNC server to allow remote access to the workstation. This would be useful in a situation where an operator could be given basic procedures on booting from CD-ROM, configuring the IP, and starting the VNC server so an investigator could analyze the system without actually being on-site.

Figure 2

Selecting the MountDataDrv option presents you with the Drive Mount Menu (Figure 3). This menu gives you the option to add more ramdisk for additional storage, or as better options, mount remote storage via NFS or SMB for permanent data storage. There are also menu options for mounting a USB or Firewire drive, although the menu options are just placeholders for the moment. You can, however, mount these devices from a command line, according to the messages displayed when trying these menu options.

If none of these options are available to you (i.e. no external storage is accessible), you could choose to copy all your data from the ramdisk to another system over the network using netcat, ncftp, or scp, all of which are included in the distribution. For example, to use netcat to copy the /data directory, you could start up a listening process on your analysis workstation as follows:

```
$ nc -l -p 2020 > data.tar
```

From a Biatchux command line you could then send the data directory to the target system using something like

```
# cd /data
# tar cf - . | nc -nv 192.168.1.100 2020
```

The important thing to remember is that unless you save the /data directory to a remote storage location, a local floppy, or some other peripheral, you'll lose all the information collected during your session since it is only stored in RAM.

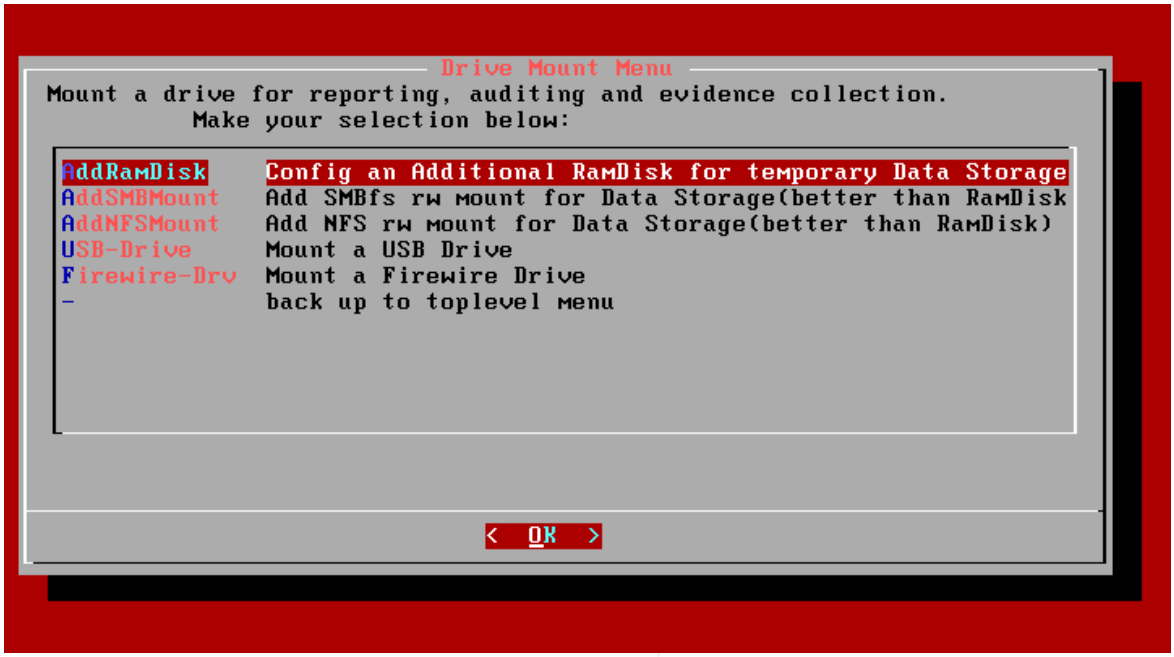

Figure 3

Finally, from the Start-Here menu you can also add virtual terminals so you can perform tasks from a command line. And in the current release, this is a requirement if you want to perform any serious work. You have the option of adding terminals with or without keystroke logging. If you choose the option to log keystrokes, the keystroke logs will be written to the /data directory, and a separate file will be created for each virtual terminal. To switch terminals, you can use the Alt- → and Alt- ← key combinations or, alternatively you can use Alt-F1, Alt-F2,..., Alt-F7. The first virtual terminal (Alt-F1) will always be the menu screen.

Biatchux Menus

The most useful options in the Forensics menu (Figure 4) that are currently implemented are the ability to mount all local hard drives read-only, and the ability to run the mac-robbers tool against the mounted drives and write the output to the /data directory. The menu also has options for searching for and grabbing Win32 registries and Unix password files; running chkrootkit to look for evidence of installed rootkits; searching for image files and running them through StegDetect to look for data hidden with steganography; creating a backup image of the drive being analyzed; and setting up autopsy, although not all of options are currently implemented.

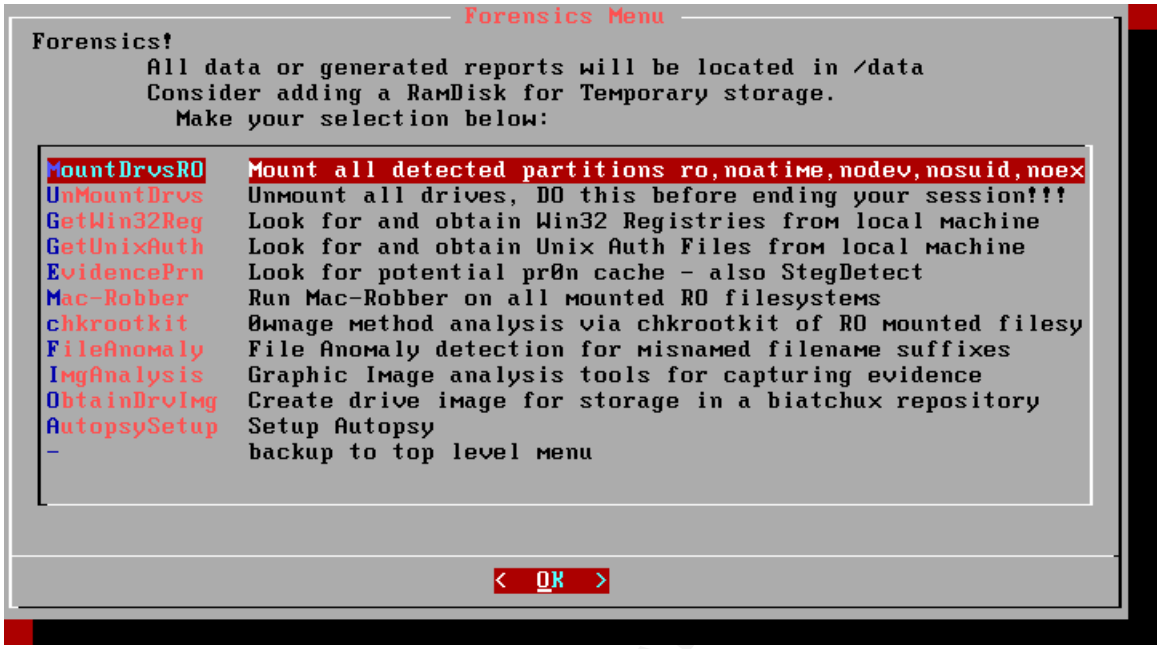

Figure 4

The Virus-Scan menu option is implemented and will run the F-Prot for Linux virus scanner from Frisk against the mounted file systems. F-Prot will detect DOS, Window, and Linux viruses and trojans. The menu also provides the option for loading updated signature files, either from the Internet or from a floppy disk. Neither update option will work, however, unless you have mounted additional disk space since the updated signatures cannot be written to the read-only cramfs filesystem. Also, if you are going to attempt to update signatures from the Internet, make sure you have configured your network interface, set up a default route, and set a name server.

Incident Response

Now that we've had a quick tour of Biatchux, let's see how it might be used to respond to a real incident. As an example, let's return to the scenario from the Introduction. You know something strange is occurring on some of your Linux and Solaris systems, but you've looked around and you can't find anything unusual. Since you suspect there might be a rootkit installed on these machines, you need some tools you can trust. So you put in the Biatchux CD-ROM, with its collection of static binaries, mount it, and start to look around.

Some of the included tools you'll want to use to see if you can determine what is happening on your system are lsof, netstat, ls, and mac-robber (Linux only). Assuming the intruder has not installed a LKM rootkit, these tools will let you see what processes are running, what files are in use, which files have been created, accessed, or modified recently, which ports are open, and any existing network connections. Other useful tools

include netcat and dd for copying data to a remote system, and md5 for determining if a suspected binary had been altered. The latter utility is particularly useful for Solaris systems since you can take the md5 output and use it as input to the Solaris Fingerprint Database. One final note about the included Solaris binaries is that the incident-response.org site, from which these binaries were taken, states that lsof and netcat for Solaris are not statically linked. Therefore, you should be somewhat skeptical of the results from these commands.

Finally, let's examine a scenario in which a Windows NT or 2000 system has been compromised, and you want to see if you can gather any evidence from the live system before shutting it down. In this scenario, you could put in the Biatchux CD-ROM and use the tools it provides, both the Cygwin binaries and the incident response tools included in the distribution. If the system has AutoRun enabled, Biatchux will automatically run biatchux.exe. If not, you could execute it from the CD-ROM manually to start the menu system shown in Figure 5, or you could run cmdenv.bat to start a trusted command shell.

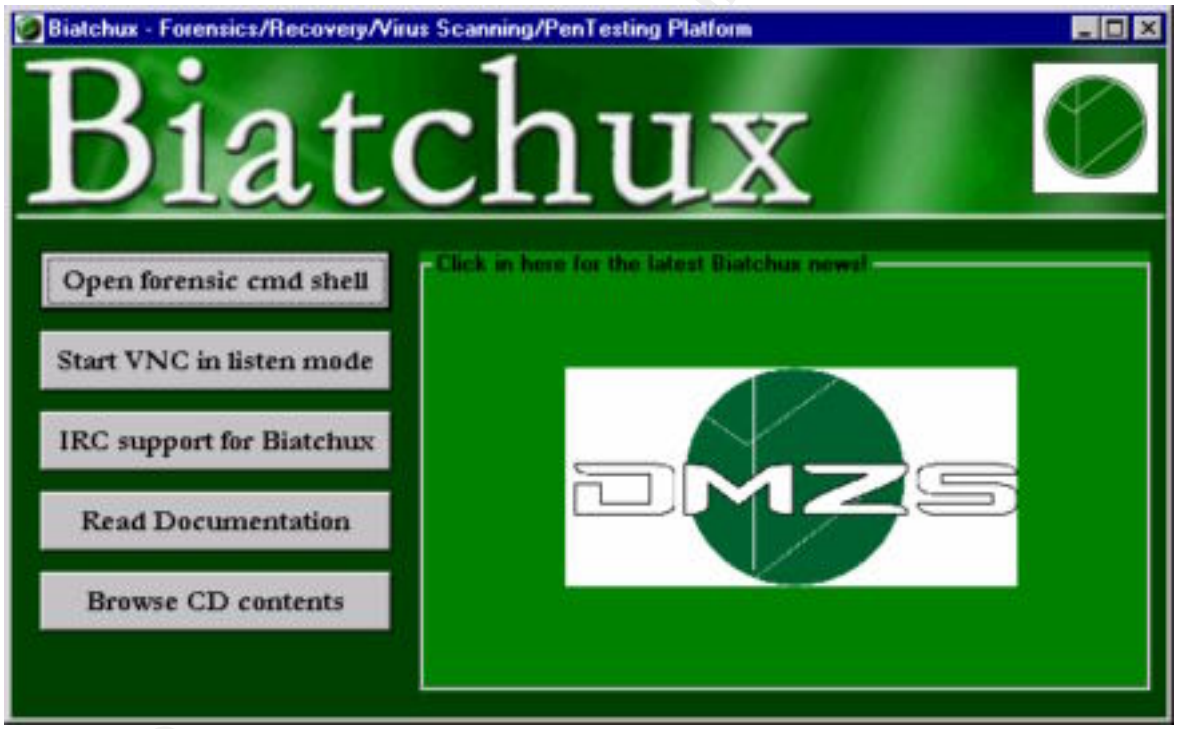

Figure 5

The forensic command shell option runs a batch file (cmdenv.bat) that sets the PATH variable to search the directories on the CD-ROM before looking in the normal locations, and then executes the cmd.exe that is also on the CD-ROM. The resulting command shell is shown in Figure 6. The IRC support is provided via a browser based IRC client that connects to an IRC server at dmzs.com. And, just like when booting from Biatchux into Linux, you can start a VNC server to allow remote access for analysis of the system.

Once you have opened a command shell, some of the useful tools available to you for analyzing your system are the:

- Cygwin binaries (Unix utilities for Win32 systems) including:
  - cat.exe, cksum.exe, cmp.exe, dd.exe, diff3.exe, diff.exe, find.exe, gawk.exe, grep.exe, head.exe, less.exe, ls.exe, nc.exe, tail.exe, tar.exe, wget.exe, xargs.exe
- tools in the win32 directory
  - listmodules.exe - a tool from ntsecurity.nu to list the modules (EXE's and DLL's) that are loaded into a process (Vidstrom)
  - strace.zip - an strace program for Win NT, 2000 to track system calls
  - winrelay - a TCP/UDP forwarder/redirector from ntsecurity.nu. (Vidstrom)
  - cmos-bios directory – contains a CMOS/BIOS password recovery tool
  - foundstone directory - contains various free tools from Foundstone
    - BOping – a scanner for installations of Back Orifice
    - DDosPing – a scanner for detecting DDoS programs
    - BinText – utility to search for strings in files
    - NTLast - a tool to analyze Windows event logs to identify who has accessed the system
    - Fport – a tool to report all open TCP and UDP ports and map them to an application
    - afind – a tool to list files by their last access times
    - sfind – a tool to scan the disk for hidden data streams and list the last access times
    - hfind – a tool to scan a disk for hidden files. It will find files that have either the hidden attribute set or NT's way of hiding things by using the directory/system attribute combination.
  - getif directory – contains tools for querying SNMP MIB variables (From WTCS)

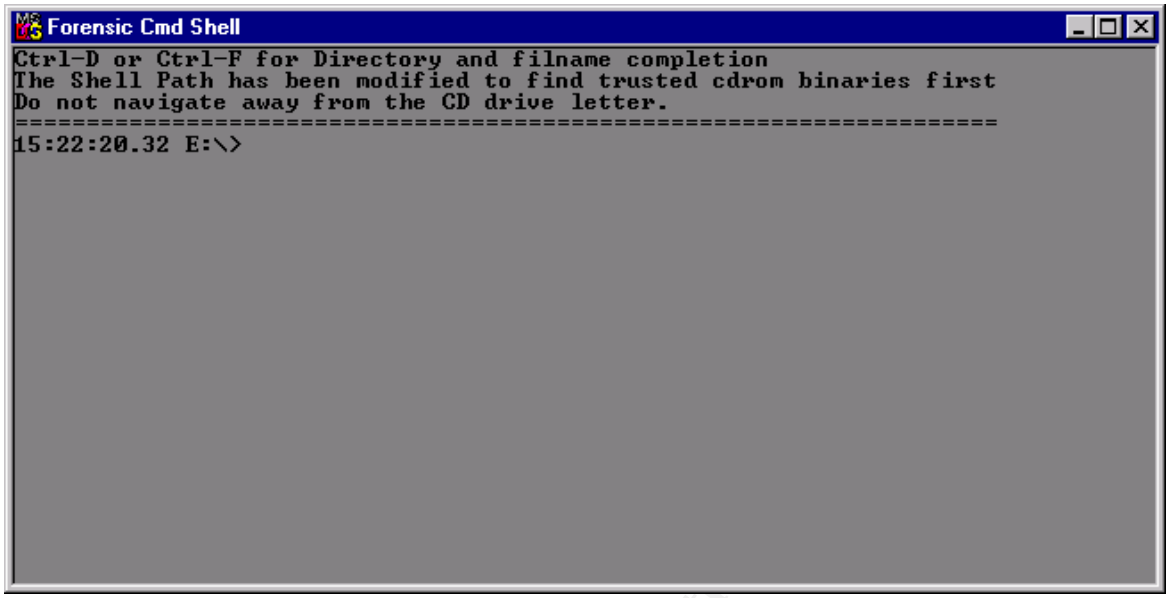

Figure 6

Forensic Analysis

Once you've completed your live analysis and you want to move on to a forensic examination of your systems, Biatchux might be useful as well. If you are in a situation in which you can't remove the hard drive(s) from the system in question for analysis, Biatchux has tools that can help with the analysis. The following steps work on both Linux and Windows systems.

The first step in a situation like this is to ensure the CMOS is set so the system will boot from CD-ROM before booting from the hard drive. This should prevent the system from writing to the hard drive during the boot process. At that point you can proceed to boot from the Biatchux CD-ROM.

The next step after booting from the CD-ROM should always be to make a bit-stream copy of the drive being examined. Prior to performing this step, though, you'll first need to configure a network interface. You can either do this through the main Biatchux menu or you can add virtual terminals and perform the configuration steps at the command line. At a command line, something similar to the following command should be sufficient to prepare to make a backup image:

```
# ifconfig eth0 192.168.1.111 netmask 255.255.255.0
# route add -net default gw 192.168.1.1
```

Next, you'll need to identify the partitions on the drive to copy. You can use the fdisk utility to find this out. Finally, before making the image backups for each partition you

should start up a netcat process listening on the target system:

```
# nc -l -p 2020 > victim_hda1.img
```

Then you can execute the backup command on the compromised system

```
# dd if=/dev/hda1 | nc -nv 192.168.1.110 2020
```

Repeat these two steps for each partition. There is an option on the forensics menu to create a backup copy like this, but it is not implemented in this release.

Finally, you should verify the backup is correct by calculating checksums of both the original partition and the backup image. You can use md5 or md5sum for this task.

```
# md5sum /dev/hda1
6c62d16dfa2ea7813e5b233e67ab7203   /dev/hda1
# md5sum victim_hda1.img
6c62d16dfa2ea7813e5b233e67ab7203   victim_hda1.img
```

Now, if you are going to follow proper forensic procedures, you should shut down the system again and analyze the backup image. Whether you continue to examine the original drive or boot Biatchux on an analysis machine containing the backup images, the analysis phase is where Biatchux's collection of tools comes in handy.

In addition to the standard Unix commands such as find and grep, Biatchux comes with a number of specialty tools for forensic analysis of Unix systems, including:

- chkrootkit - a tool to check for signs of a rootkit
- The Coroner's Toolkit (TCT)- a collection of tools for performing forensic analyses of Unix systems
- tctutils - additional tools that can be used with TCT
- Autopsy - a graphical interface to the tools in The Coroner's Toolkit and tctutils
- mac-robber - a tool for collecting the Modified, Accessed, Created (MAC) times from files. mac-robber outputs the MAC times in the same format as the output from "grave-robber -m", a tool from The Coroner's Toolkit. This output can then be used by mactimes, another tool from TCT, to establish a timeline of when files were modified, accessed, or created (@Stake).
- StegDetect - a tool for detecting steganographic content in image files.
- hexedit - A hex editor that can be used to search through files and disk images.
- LDE - Linux Disk Editor - a tool that allows you to view disk blocks, view directory entries, and view formatted inodes

Other Uses

Biatchux has other uses beyond incident response and forensics. These uses include (along with a condensed list of tools available):

- Vulnerability assessment (nmap, whisker, hping, firewalk, fragrouter, John-the-Ripper, nbtscan, nemesis, screamingCobra, onesixtyone, isnprober, hunt, p0f, THC-Hydra)
- Network administration and security (ethereal, tcpdump, dig, dsniff, netcat, hunt, ncftp, ngrep, p0f, arena)
- Load testing (hammerhead, apachebench)
- Disk/file recovery (hexedit, LDE)
- Intrusion Detection (snort)
- Firewall (ipchains)

Other Bootable Security Toolkits

PLAC, the Portable Linux Auditing CD, is an open-source Linux distribution that was developed by Fred Cohen and Associates. It was designed to be small enough to fit onto a business-card sized CD-R, which limits its size to less than 50 MB. Fred Cohen and Associates also offer a commercial version of PLAC, called the White Glove CD, which adds X11 and more utilities.

PLAC has support for a number of peripherals built in to its kernel, including SCSI disks, tape drives, and PCMCIA cards. It uses a 30 MB ramdisk for its root filesystem and a cloop filesystem for /usr. When PLAC boots it automatically searches all IDE and SCSI drives for any partitions with recognizable filesystems and mounts them read-only. (Bajusz).

Trinux is a very small Linux distribution that is bootable from floppy or CD-ROM, and resides completely in RAM. The basic boot image includes the BusyBox tools, just like Biatchux does, but there isn't much else included. There are many additional packages available for Trinux, though, that can be downloaded from http://trinux.sourceforge.net/pkg/. At boot time the additional packages can be loaded either from additional floppy disks, a local IDE drive, or from the network.

One major difference between Biatchux and both of these toolkits is the menu system in Biatchux. While it is not finished at this point, one of the goals of the developers is to have a simple to use menu that will walk a user through the proper procedure for a forensic analysis or incident response. This contrasts with Trinux and PLAC, in which the tools to perform the tasks may be offered by both, but the user has to have more knowledge to perform the analysis.

Another difference between Biatchux (and PLAC) and Trinux is that a user must build

his/her own toolkit from the Trinux packages that are currently available, while Biatchux and PLAC provide all the tools in one package.

An advantage that Trinux has over both PLAC and Biatchux is that some older PCs do not have BIOS support for booting from CD-ROM or do not have CD-ROM drives capable of reading CD-R disks, but all PCs support booting from floppy disk.

Finally, Trinux and PLAC do not contain any tools for live response to security incidents, while Biatchux includes tools for response to incidents on Solaris, Linux, and Win32 systems.

Table 1 contains a comparison of the three products as incident response and forensic toolkits.

Conclusions

While one of the stated design goals for Biatchux is to build menus that can lead anyone through an incident response or forensic analysis, the current menu system is still very basic and not fully functional. Many of the options on the menu are just placeholders to be implemented in a later version.

In addition to improving the menu system, I would also suggest the following:

- Add cryptcat to the static binaries and to the tools available in the boot distribution. Cryptcat is a version of netcat with Twofish encryption added. (Mandia and Prosise, p. 232)
- Include additional NT response tools
    - loggedon, pslist, listdlls, and filemon from Sysinternals (Mandia and Prosise, p. 227)
- Include a static binary version of mac-robber for Solaris.

Even with the shortcomings listed, Biatchux is a handy toolkit for a system administrator. It has an abundance of security tools included, and is especially useful for incident response given the static binaries and specialty tools included. It's also a useful toolkit for performing forensic analyses of systems. Given that the distribution is still fairly new, and seeing the major improvements that were made between versions 0.1.0.5b and 0.1.0.6b, I have a great deal of confidence that the Biatchux distribution will continue to evolve and grow to its full potential.

	Trinux v. 0.80rc2	PLAC v. 2.9.5	Biatchux v. 0.1.0.6b
Bootable from CD-ROM	X	X	X
Bootable from floppy	X		
Distribution size	1.44 MB*	47 MB	117 MB
Can remove boot media from system after boot	X	X**	
Automatically searches and mounts all partitions read-only at boot time		X	
Menu driven operation			X
Unix incident response and forensic tools included or available			
TCT	X***	X	X
tctutils	X***		X
Autopsy browser			X
Ethereal	X		X
tcpdump	X	X	X
mac-robber			X
chkrootkit		X	X
LDE	X	X	X
hexedit			X
md5sum	X	X	X
netcat	X	X	X
StegDetect			X
Trusted static binaries			
Windows			X
Linux x86			X
Solaris Sparc			X
Windows incident response and forensic tools			X

Table 1 – Comparison of features 1

* Basic kernel only. Most tools must be loaded separately.
** If one of the diskless boot options is used.
*** Non-Perl tools only.

References

@Stake. @stake Research Labs – Tools. <http://www.atstake.com/research/tools/index.html#forensic>.

Bajusz, Richard. Security Applications of Bootable Linux CD-ROMs. <http://rr.sans.org/linux/sec_apps.php>.

Dittrich, David. Basic Steps in Forensic Analysis of Unix Systems. <http://staff.washington.edu/dittrich/misc/forensics/>.

Dittrich, David. "Root Kits" and hiding files/directories/processes after a break-in. January 5, 2002. <http://staff.washington.edu/dittrich/misc/faqs/rootkits.faq>.

Foundstone - Free Tools. <http://www.foundstone.com/knowledge/free_tools.html>.

Franz, Matthew. Trinux homepage. <http://trinux.sourceforge.net/>.

Lee, Rob. Incident-Response homepage. <http://incident-response.org/>.

Mandia, Kevin and Chris Prosise. Incident Response: Investigating Computer Crime. Berkeley: Osborne/McGraw Hill, 2001.

Project: Portable Linux Auditing CD. <http://sourceforge.net/projects/plac>.

Salusky, William and David Zendzian. Biatchux. <http://biatchux.dmzs.com/>.

Showalter, Brad. Trinux – A Digital Tool Belt. October 10, 2001. <http://rr.sans.org/unix/trinux.php>.

Somer, Lord. Linux Rootkit. <http://online.securityfocus.com/tools/1489>.

Vidstrom, Arne. Security Toolbox. <http://ntsecurity.nu/toolbox>.