Infosec LiveDistros: Must-haves for the information security practitioner

By Russ McRee

Every information security professional should have a jump bag. Be it for incident response, forensic discovery or penetration testing, there are some tools your personal kit should not be without.

LiveDistros, also known as Live CDs, allow you the portability of a complete and highly functional operating system you can boot from external media on practically any hardware that supports the media. According to Wikipedia[1], a LiveDistro is:

> *an operating system distribution that is executed upon boot, without installation on a hard drive. Typically, it is stored on bootable media such as a CD-ROM (Live CD), DVD (Live DVD), USB Flash Drive, among others. The term "live" derives from the fact that it does not reside on a hard drive. Rather, it is "brought to life" upon boot without having to be physically installed onto a hard drive. A LiveDistro does not alter the current operating system or files unless the user specifically requests it. The system returns to its previous state when the LiveDistro is ejected and the computer is rebooted.*

Ultimately, this methodology contributes to great power at your immediate disposal, without having to deploy or carry full systems on dedicated hardware.

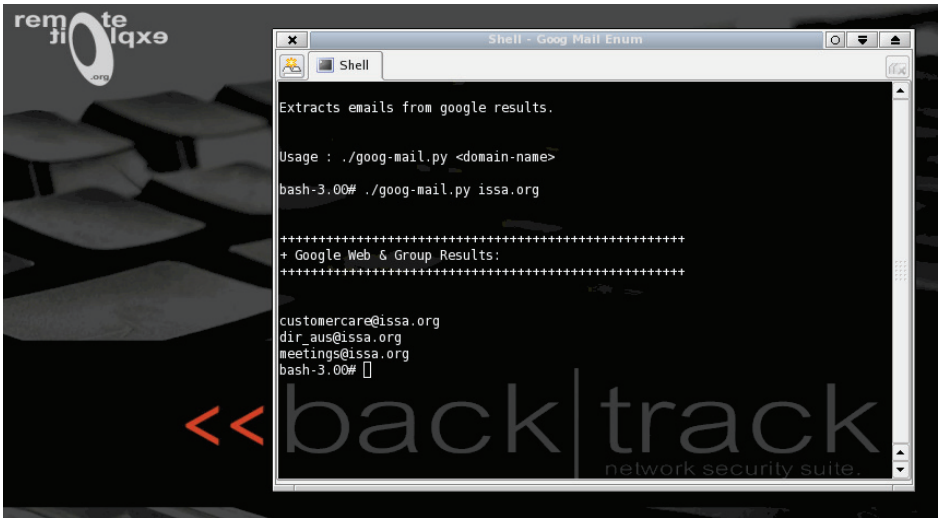

Figure 1: BackTrack and goog-mail at work

Let's review a couple of excellent LiveDistros I believe you'll find quite useful. These two distributions offer excellent Linux ISOs for purposes specific to the security professional's cause. LinuxISO.org defines a Linux ISO as "a file containing a cdrom disk image of a Linux distribution"[2]. The LiveDistros we will consider here are specifically Linux ISOs, geared toward a particular purpose. A caveat: Linux skills are definitely recommended for use of these LiveDistros.

BackTrack

BackTrack (remote-exploit.org) is the convergence of the Whax and Auditor projects and is an unquestionable must-have. Described as an "analysis platform," this LiveDistro includes a massive laundry list of tools. You'll find a variety of enumerators (tools for exploratory reconnaissance) including those for the WWW, Google, DNS, SMB, SNMP, SMTP, and LDAP. One of my favorites is the Google email enumerator goog-mail (see Figure 1).

Also included are the Metasploit Framework and the milw0rm and SecurityFocus archives. Nessus, Nikto, nmap, amap, and others are all there for your vulnerability and port scanning. Password tools like THC-Hydra and RainbowCrack are available, as well as three cross-platform fuzzers to "test the boundaries" of most anything that might touch a network. Where a software developer might refer to such activity as "stress testing," a vulnerability researcher will call it "fuzzing".[3] Refer to *Gray Hat Hacking: The Ethical Hacker's Handbook* for more information on fuzzing and debugging tools. Sniffers, Cisco tools, database and wireless analysis, forensic tools, and even a VMware player are at the ready.

As described, BackTrack is indeed a "network security suite." As always, the standard cautions apply here. Don't fire up BackTrack and let fly in your production environment, as you'll likely trigger any number of possible alerts, potentially leading to large men in black suits arriving at your cube or office.

All the same tools the bad guys use are here at your disposal: Be careful!

Download the BackTrack ISO here: http://www.remote-exploit.org/index.php/BackTrack_Downloads.

1 http://en.wikipedia.org/wiki/LiveDistro

2 http://linuxiso.org/viewdoc.php/isofaq.html#whatisiso

3 *Gray Hat Hacking: The Ethical Hacker's Handbook,* Harris, Harper, Eagle, Ness, Lester, McGraw-Hill, 2004, pg. 351

Helix 1.7

Dedicated to incident response and forensics, this distribution is a forensic powerhouse. When booted from the CD as a Linux OS, Helix (e-fense.com/helix/) is built to not touch the host computer in any way, thus maintaining forensically sound investigations. It also includes a Windows "side" for live investigation. SANS, among others, uses Helix for incident response and forensic training. Consider all the tools available. You'll find sleuthkit and autopsy for forensics. For slack space discovery there's bmap. As the authors of *Incident Response: Investigating Computer Crime* put it, "Slack space occurs when data is written to a storage medium in chunks that fail to fill the minimum block size defined by the operating system"[4]. Even after files are deleted, file system residue may remain in slack space, and can be quite useful in investigations.

Concern over rootkits has grown exponentially in the last few years, and will soon likely top all lists as the foremost security challenge. A rootkit is defined by Eric Cole in *Hackers Beware* as a tool enabling an attacker to get back into a system as root, super user, or administrator after the actual hack has occurred[5]. Call it a covert backdoor for use so the attacker may return unnoticed. Helix offers chkrootkit and rkhunter for use in detecting rootkits.

One of my favorite tools is AIR. As of the most recent Helix release, AIR 1.2.8, the Automated Image & Restore interface (see Figure 2), makes safe copying of media a breeze. This is, of course, essential. You would never want to investigate your original media, as doing so would greatly damage your legal standing.

The e-fense.com documents pages include some excellent papers on preserving digital evidence, first responder's procedures, and Helix for beginners. All are recommended reading. Also see http://www.forinsect.de/forensics/forensics-tools.html for links to all the forensics information and resources you might ever need.

Download the Helix 1.7 ISO here: http://www.e-fense.com/helix/downloads.php.

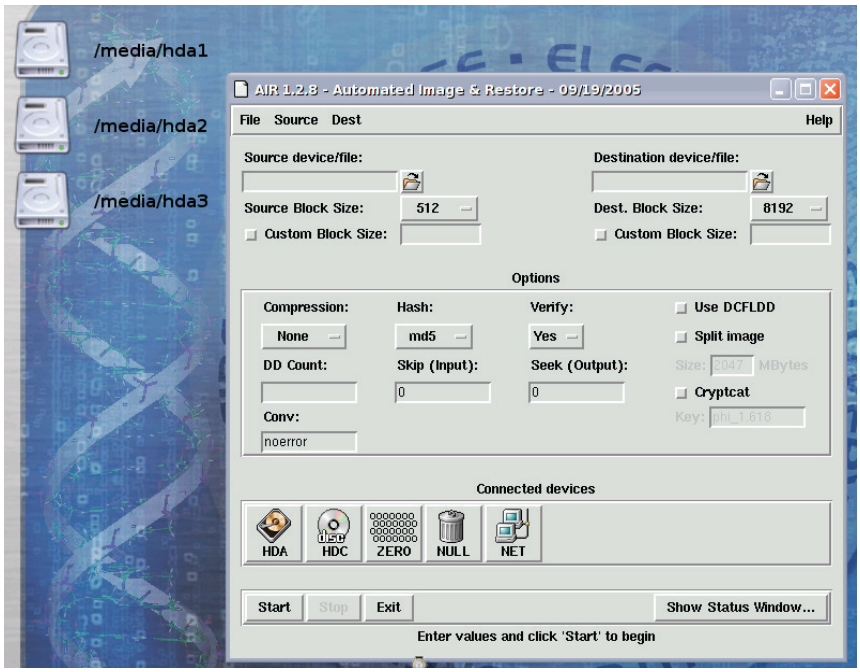

Figure 2: Helix and the Automated Image & Restore tool

Real-world uses for Helix and BackTrack

Helix

Let's start with Helix, and what might be a typical incident where it would serve well.

First, I must recommend reading *Helix 1.7 for Beginners,* by BJ Gleason and Drew Fahey, in advance of beginning your first audit. As always, there's no harm in testing Helix on your PC or in a lab as a precursor. The document is available on the e-fense.com website. You can use Helix "as a standard Windows application used to collect information from a 'live' (still turned on and logged in) Windows system"[6], but remember you are disturbing the state of the live system and potentially harming your investigation. However, you may have no choice, as with a server that can't go down or evidence that may be in memory, so this may be your only option.

More preferable is booting the CD at startup. "When Helix boots, it runs entirely off the CD, and only mounts the hard drives in read-only mode, so they can not be modified"[7].

The scenario: you've been contacted by HR and a developer's manager over concerns regarding theft of intellectual property. You've been approved to audit the developer's PC but not to seize it or to duplicate the drive. Obviously this can be a challenge, in that chain of custody standards must be preserved. Again, one key advantage of Helix is the ability to use it without altering the original file system.

We'll make some assumptions. Your organization has not been monitoring outbound traffic, so there are no logs or signatures available to legitimize the suspicion that the developer has been emailing code via Webmail to a competitor and spending a great deal of time browsing their Website.

Helix 1.7 includes Retriever 2.0, which allows hunting for specific documents, graphics, video, and Web-based email like Yahoo! Mail and Hotmail. Open the Helix menu, choose Forensics, and then choose Retriever. In the search path, remove the Knoppix reference and add `/media/hda1`, which should be the read-only mounted hard drive in the PC you're auditing. Finally, select Email, then Find.

Once the search is complete, you'll hopefully find references to ShowFolder or ShowLetter. Highlight ShowLetter and select View. The File Manager will open and offer you files to screen-capture, including `ShowLetter.htm`. Clicking it will open the file in Firefox. You may well have to hunt for specific content regarding the intellectual property in question, but you will find it with Retriever.

Once the content is identified, take a screenshot by going to the Helix menu, then System Tools, then Screenshot Utility. I typically save screenshots to the Desktop, then email them off to myself for an

4 *Incident Response: Investigating Computer Crime*, Kevin Mandia and Chris Prosise, McGraw-Hill, 2001, pg. 121

5 *Hackers Beware*, Eric Cole, New Riders, 2002, p. 548

6 *Helix 1.7 for Beginners,* BJ Gleason and Drew Fahey, http://www.e-fense.com/helix/docs.php

7 *Helix 1.7 for Beginners*, BJ Gleason and Drew Fahey, http://www.e-fense.com/helix/docs.php

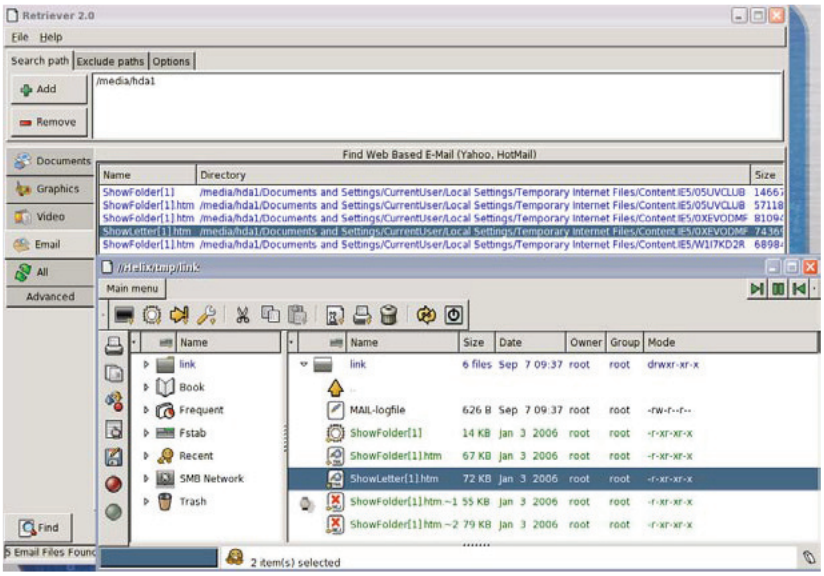

Figure 3: Retriever 2.0 finding Hotmail

investigation summary and evidence collection. Remember, you won't be able to, nor should you want to, write to the local hard drive.

Our developer has also been spending a lot of time browsing the competitor's Website. Again, we've booted to the LiveDistro and we want to review Internet Explorer activity. The Linux side offers pasco, from Foundstone, for this very cause.

I'll start by opening the root terminal, available right on the Helix menu bar. Type `updatedb` to bring the slocate database to a current state, then type `cd ~`, which will make your current path the root directory. Type `locate index.dat`. This will return all copies of index.dat, the IE tell-all, which can then be opened by pasco (Latin for browse). You'll likely see a number of `index.dat` files to choose from.

Zero in on `/media/hda1/Documents and Settings/Developer/Cookies/index.dat`.

Your command should read like this:

```
pasco /media/hda1/Documents and Settings/Developer/Cookies/index.dat > index.txt.
```

This will parse the contents of the `index.dat` file to `index.txt`, readable from the root directory. This, again, I typically email off to myself.

The important take-away from using Helix as a live Linux CD is that you leave no trail or damage on the Windows file system. This is critical. You might later need to seize the PC for more advanced investigation, and you want to ensure no damage to the case or the evidence. And remember, don't conduct investigations of this nature without the express written permission of your HR department!

BackTrack

The scenario: You've been asked to quickly do some database analysis in the hopes of preventing the DBA from going live with typical MS SQL security lapses. You have written permission – this is a must. Your goal is to convince management that it would not be in their best interest to go live until better security practices have been implemented. Your testing tools are unavailable, as the system that hosts them has had a hardware failure.

BackTrack to the rescue. BackTrack includes excellent database testing tools, amongst them SQLdict.

Boot the BackTrack CD, login as root, execute startx to start the GUI, and open the menu. First choose Internet, then Set IP Address. Once on the network, select Backtrack, then Database Tools, then MS-Sql, then SQLdict. You'll need a Password File for this effort. A great place to look if you don't already have one is here: ftp://ftp.ox.ac.uk/pub/wordlists/.

Load the password file of your choosing, enter the IP and account for the target server, and click Start. If the account has been given a weak password, you should have it in no time.

Worse and more of it, you know the server to be ill-maintained and likely at risk to certain MS SQL vulnerabilities. BackTrack offers the Metasploit Framework, which is handy for a quick and easy account installation. As an example, you're certain that the database can be exploited via the MSSQL 2000/MSDE Resolution Overflow because the installation is pre-SP3. On the BackTrack menu choose Exploit Archives, Metasploit Framework, then MsfWeb followed by Metasploit Web 2.6 Web-Gui. Scroll down to "MSSQL 2000/MSDE Resolution Overflow" when the browser opens, click it, choose the default choice for Select Target (there's only one), choose

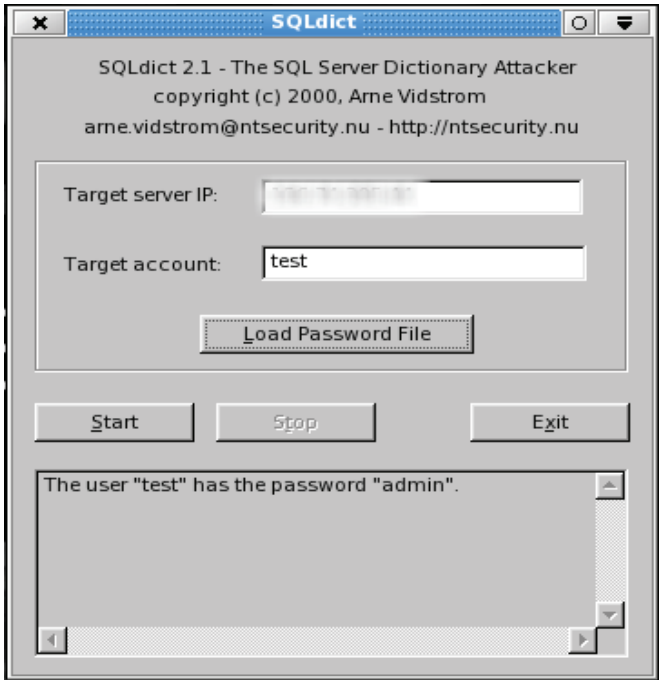

Figure 4: SQLdict

win32 – adduser, enter the target server IP under RHOST, for fun enter "flintstone" for the password and "fred" for the user. Accept all other defaults and click Exploit.

If you are successful, a message indicating such will be returned to your browser: point-and-click pen tests, on the fly, no pre-configuration required. When you can show the DBA and the management team that, not only can you tell them the passwords for poorly passworded accounts, but you could also add an account with little effort, perhaps they'll stop, review, and remediate before deploying.

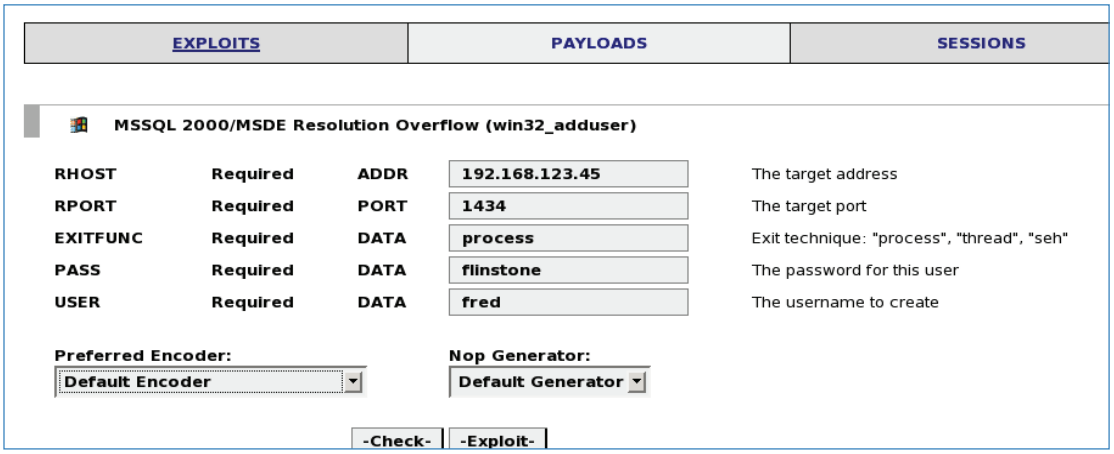

Figure 5: Metasploit and MS SQL

Again, before using these tools, please protect yourself and ensure that you have the appropriate permission to conduct audits or pen tests.

Regardless of which existing tools you may utilize, keep these LiveDistros especially handy, as I am certain, at some point, they will serve you well.

Summary

The two distributions described here are by no means the only ISOs available. I've used others like Knoppix STD, LAS, and NST. You can explore these and many others for yourself at http://www.securitydistro.com/.

About the Author

Russ McRee, GCIH, is a security analyst working in the Seattle area. He is a member of ISSA, Pacciso, InfraGard, and CCSA (Cyber Conflict Studies Association). Russ maintains holisticinfosec.org. Contact him at russ@holisticinfosec.org.

ISSA's "1+1" Membership Program

Ernest E. Zernial, Jr., MBA, CISSP, CISM – ISSA Vice President of Membership. He may be reached via e-mail at vp_membersez@issa.org.

The ISSA Business Plan for July 1, 2005 - December 31, 2007 has as its top two organizational priorities to increase worldwide paid General Membership to 12,000 members by December 31, 2006 and 16,000 members by December 31, 2007. Of these increases, the non-US paid membership goal is to 4,000 members by December 31, 2007. The ISSA needs your assistance to reach these goals so we may create a unified voice for security professionals around the world that can influence public opinion, government regulations, the media, and other important audiences.

We are encouraging each chapter member to remain an active ISSA member and participate in growing our membership by recruiting just one member a year for the next two years. We are calling this the ISSA "1+1" Membership Program." The "1+1" program will replace the current rewards program where each annual or two-year renewing member gets an ISSA promotional item. The new "1+1" recruiting and retention incentive is an all-expense paid trip to an ISSA Chief Information Security Officer (CISO) Executive Forum or an information security symposium/conference of your choice.

The final CISO Forum of 2006 will be held in Orlando, Florida, USA. Locations for the 2007 CISO Forums are under consideration and will include Vancouver, British Columbia, Canada. Specific trip incentives include:

- Round-trip airfare
- Hotel accommodations
- Conference fees
- $300 for expenses
- Dinner with the ISSA Board of Directors (if attending a CISO Executive Forum)
- Picture and interview for The ISSA Journal

The ISSA member recruiting the new general members and the new member will both be eligible to attend their choice of any CISO Forums or information security conference or symposium within one year of being selected. A pair of winners will be selected for every 1,000 new paid general memberships that are referred by a current ISSA general member and who have completed a new ISSA general membership application between 1 January 2006 and 31 December 2007.

Details of this program are posted on the ISSA Website at http://issa.org/1plus1.html, along with a PowerPoint presentation for each chapter to use. We know that ISSA can count on you to be an ambassador for ISSA and help qualified individuals who support the goals of ISSA become members. This issue of The ISSA Journal has a full-page general membership application. Keep this copy with you. If you wish to use our Web site and help the new member to register online, go to https://www.issa.org/join.taf?_function=form Remember to include your name in the space on the printed or electronic application after the statement, "If you were referred by a member, please enter their name."

We seek your feedback both now and through the "1+1" Membership Drive, so please send your comments and questions to vp_membersez@issa.org.

Notes

1. Current ISSA general members who drop their general membership after 1 October 2005 will not be eligible as a new general member for incentives under this promotional program.
2. A new general member is defined as an individual eligible for ISSA general membership who was not an ISSA general member or trial member prior to 31 December 2005.
3. An ISSA member is defined as an individual who has a current paid ISSA general membership as of 1 January 2006 or thereafter a new paid general member recruited after 1 January 2006