Multi-Tool DVD Sets: An important addition to the Incident Handler/ Pen Tester's toolkit

Jamal Bandukwala

Multi-Tool DVD Sets: An important addition to the Incident Handler/ Pen Tester's toolkit

GCIH Gold Certification

Author: Jamal Bandukwala, abanduk@rogers.com

Adviser: Joey Niem

Accepted: May 29th 2007

© SANS Institute 2007, Author retains full rights.

Table of Contents

Multi-Tool DVD Sets: An important addition to the Incident Handler/ Pen Tester's toolkit

Abstract:

My paper will deal with the software tools used in Incident Handling, forensics and pen testing. There are many tools out there and while there is a tool for every situation, it can be quite a challenge to catalogue and carry several different CDs filled with tools that may not be used in a given situation. While Linux based Live CDs do exist, they may not contain all the tools one needs and an incident handler may still need to carry several CDs to the site; it can take time to make sure you have the right tools for the job, and to maintain the appropriate versions of the tools.

This paper will aid the incident handling and security community by explaining and demonstrating forensically sound processes to create a powerful multi session DVD. This can be customized to contain several of the most popular Linux live CDs and a second DVD/CD that contains other tools that may not be contained on the live multi session DVD.

The paper will explain the criteria used to select the tools, examine the advantages, limitations and weaknesses of the multi DVD approach and most importantly will contain a detailed walk through of the process to make a multi boot DVD. Anyone from experienced to novice incident handlers, can follow the framework in this document to create customized multi-session DVDs useful to their organizations, irrespective of whether these are huge corporations with specialized security teams, specialized security companies or smaller groups that may lack a full time security force.

The most basic tools that should be in your software toolkit:

All incident handling jump-bags have a variety of hardware and software utilities. In order to customize and build a personalized multi boot live DVD set one first needs to examine some of the software needed, as part of their toolkit. The DVD set needs to have a good mix of trusted windows and UNIX/Linux tools (Mandia, Prosise & Pepe, 2003). Once the handler selects their tools, one also needs to make sure that their selections will not alter the host computer in any way. In addition to this, the analyst must verify that the tools being run on the computer under analysis are trusted, as in many cases the attacker may have their own copies of these tools on the target system (Mandia, et al. 2003). Mandia et al summarize the importance of preparation by the following, “a live investigation is not the time to create or test your toolkit for the first time” (Mandia, et al. 2003). Preparing one’s toolkit in advance and knowing exactly how it works and its limitations is crucial, because one cannot assume that the critical commands and services on an impacted system have not been compromised. Mandia et al raise an important point, when they note that many UNIX variants for instance Solaris 2.8 are not backwards or forwards compatible. This can complicate recovery efforts as programs compiled with one UNIX or Linux distribution may not be compatible with another variant of the same software (Mandia, et al. 2003). A good list of trusted basic UNIX commands and basic windows tools that one should have their own reliable copies of can be found in Appendix A. It is important to note that if one wants to build a

Solaris based live CD, it is possible to do this, but may require greater customization. The user will have to port over the tools needed, as there do not appear to be many security/pen-test based live Solaris distributions, while there are plenty of security based live Linux CD's. The best place to find information for re-mastering and creating Solaris live CD's appears to be the OpenSolaris live media site: http://www.opensolaris.org/os/project/livemedia/, while the most well known and actively maintained Solaris live CD distribution is genunix, this can be found at the following site: http://www.genunix.org/distributions/belenix_site/.

Semper Paratus (Always prepared): Preparation a key step in Incident Handling

The only way to handle the challenge of attackers using the same tools as incident handlers is for one to know the systems they will have to deal with and customize one's live DVD toolset to address these needs. One of the advantages of using a Live CD is that the user has access to a full scale Linux system, whose commands the user can trust. There may be times however, where one cannot use a Live CD for whatever reason (either due to lack of trust or hardware failure),in this case the analyst may need to put certain trusted Linux commands on to a CD, disk or some other portable device. In Mariusz Burdach's paper on Forensic analysis of a live Linux system, he assembles a list of Linux commands one should have as part of their Forensic toolkit (these are aimed towards Linux Live Incident Response)(Burdach, 2004) and the reader may wish to add a few more commands to their toolkit depending on

their needs. It is important to point out that most Linux Live CD's and the Live CD's mentioned in this paper already include the trusted commands listed in Burdach's list. Burdach also describes how to use these tools on a CD or disk for live response without negatively impacting the computer being investigated; this is essential for readers assembling various Linux commands (rather than using a live CD) and for any investigator who may not be familiar with carrying out analysis on a Live Linux system (Burdach, 2004). Mandia et al. recommends choosing the specific tools the reader wants and then customizing a live CD that meets their needs. While this may be sufficient for some readers, it can pose a problem for some incident handlers and investigators. There is a slight possibility that an incident handler can arrive at a site and find that they are missing a tool they wish they had downloaded or installed (but did not due to lack of space on a Linux live CD).

One has to keep in mind, that when dealing with volatile data on any live Unix/ Linux or windows systems information is changing all the time and when responding to an incident one wants to get all the volatile data they can as unobtrusively as possible. While it is possible for a first responder to manually run tools for this from trusted media, it is a lot more advisable to run these tools through a script (this may need to be customized for the first responder's organization and setup). A script reduces the room for error, and also has the potential to speed up the data gathering process (Kornblum, 2002).

One of the biggest challenges CSIRT teams and first responders may face when assembling the tools and commands

not included as part of the multi session DVD, can be assembling trusted commands and dependencies for proprietary Linux or UNIX systems. Jones and Rose point out that some commercial UNIX systems may lack facilities to statically compile certain tools (even if the source code is available); in such cases one may have to identify the dependencies or shared libraries of the program they wish to copy, and then copy these to their live CD (Jones, Bejtlich & Rose, 2006). It is necessary for one to understand the commands for the systems unique to their environment; the lsof command will usually work for most Linux/ UNIX systems, but some operating systems may have slightly differently named commands that execute the same functionality (Jones et al. 2006).

How I chose the Live CD's that I picked:

When deciding which distributions are going to be part of one's multi-os DVD, a number of factors need to be examined. These factors include ease of use, collection of tools, stability, distribution focus and capabilities, and distribution maintenance possibilities. The possibilities under investigation include Anonyom.os, Helix, Backtrack 1, Backtrack 2 and FCCU Linux (The Belgium Federal Police Force Linux distribution). I will briefly discuss the advantages and disadvantages of the distributions mentioned here, to whom they are focused towards and my reasons for wanting to include them as part of multi-boot DVD set.

The CDs I have chosen were mostly based on the knoppix/live CD distribution core; knoppix itself is based on the debian core. This is significant because it means that these CD's that are based on the debian core will all

use similar if not identical commands when it comes to updating the toolsets. I have also chosen distributions based on other cores, such as backtrack which is based on the slackware distribution. One major advantage of using slackware to build your live CD is its modularity; this makes it much easier to add and remove components as needed. It is important to point out that while all the distributions being examined can be used for Incident Handling and Penetration testing some are better suited to one task over another. Distributions like FCCU and HELIX are more focused towards Forensics and Incident Handling, while Backtrack has a very strong toolset with a more offensive attack focus better suited to pen testing.

Anonyom.os:

Anonyom.os is an Open BSD 3.8 based live CD; this distribution does not have any forensics or pen testing type tools on it. What makes Anonyom.os special is its ability to hide the user in plain sight; if a machine running this CD is probed, the probe believes that the machine is a WIN XP SP1 based box. This allows a penetration tester/ attacker or someone planning to carry out reconnaissance to carry out their task without drawing unwanted attention. The group that created this live distribution has provided an excellent technical guide to re-mastering and customizing one's own copy of this distribution, which can be found at http://kaos.to/cms/, called "How to Build an Open BSD Live CD from Scratch". As one can imagine, some of the basic steps are going to be slightly different from re-mastering Linux distributions. In this case the base operating system will have to be the

OpenBSD operating system, preferably the latest version available for download (Fade, 2006). Once a user sets up their workstation, the steps can be adapted to fit the template at the end of this paper. The user is then going to have plenty of options to make this a more effective attack or response CD (Fade, 2006). It is important to point out that as all the live distributions listed here are Linux or UNIX based many of the commands (while they may differ among different distributions) will still be recognizable or familiar to the user, with only minor adjustments necessary as needed.

Helix:

Helix is a live CD distribution based on Knoppix, aimed at incident handlers and forensics analysts. It has a significant collection of both Linux and windows based tools. One rather unique aspect of this particular distribution is that it is not limited to use as a Live CD; in fact it can be used for Windows based live response as well. This distribution is a very useful toolset for incident handling and forensics, but is not likely to be very helpful in a pen testing capacity.

The latest version of the Helix CD (version 1.9), which was released on July 13 2007 includes a significant amount of updates for both Linux and Windows tools. Helix is a debian based CD, and updating or adding new materials to a knoppix based live CD can get slightly complex, however once the handler/tester has understood the procedure the same basic process can be used to customize any knoppix or debian based live CDs.

Backtrack 1 and 2:

Backtrack is a slackware based distribution, which came about by the joining of two other security/ pen test distributions, Auditor and Whax. One of the advantages of using a slackware based distribution like backtrack, is its modularity, this makes it very easy to add, remove or update modules if one needs to customize the CD. In fact, the user does not even have to install a copy of their slackware based distribution to a hard-drive or a virtual machine. A tool called MySlaxCreator simplifies the process and allows the user to add or delete modules directly from the ISO; interestingly enough this tool is currently only available for windows.

One major advantage of this approach is that MySlaxCreator makes it a lot easier for both the advanced investigator and a newcomer to the industry to quickly put together a customized toolkit. As one can imagine however, if one's primary system runs Linux or anything other than windows, this wouldn't be the ideal tool, and one would have to re-master the CD in a manner similar to Helix and other Knoppix based distributions.

FCCU Linux (The Belgium Federal Police Force Linux):

FCCU Linux is similar to Helix in the sense that it is aimed primarily towards investigators, incident handlers and Forensic analysts. One of the biggest advantages of this distribution is that it is quite lightweight and as a result can be run on older hardware, with smaller amounts of RAM more easily than some of the other Linux distributions mentioned here. In addition to this, the distribution is actually used by the Belgium Federal Police

Force; this is significant because it can help with the tools proven in court question. While the FCCU Linux CD is extremely useful, it does have some limitations; one of its biggest limitations as opposed to Helix is that it does not have a section for Windows Live Incident Response. This maybe in part as it was designed for the police force and it may have been assumed that it would be safe to reboot or shut down the suspect's computer if needed and make a Forensic copy of the suspect's hard drive.

The FCCU Linux CD is also based on Knoppix and is under active development; this is useful because it means that re-mastering or customizing it requires the same procedure as most of the other knoppix based distributions. As one can imagine, while there is some overlap between the forensic tools on this distribution and other CDs listed earlier, the FCCU Linux also has some very interesting tools on it that are not found on the other CDs. A good example of this is pipebench, a tool that allows a forensic examiner or incident handler to see the speed at which information is coming through. This distribution and a list of the tools available can be found at the following website http://www.lnx4n6.be/index.php?sec=Documentation&page=bootcdcontent#video%20tools.

Reasons for not making the tools and distributions listed in the paper available as a download from me:

I had initially considered packaging the Linux distributions and other tools listed in this paper and making them available for download, but chose not do so. I decided against doing this for a few reasons, one of the

most important reasons being that it would be going against good/best practices by packaging these together and distributing them. This is because, it would make a lot more sense to indicate where these tools are located and allow the readers to decide whether they wish to download and use them. It is smarter for a user (especially in this context, as security researcher, incident handler, security team etc), to get the tools and distributions from the original sources if possible; unless of course, they know that the location or provider they are getting these distributions and tools from are trustworthy, and satisfy their needs, research or other purposes. In addition to this, specific tools have different licenses and licensing requirements and while most of the tools mentioned here are free, there are some tools which have limited free licenses; for instance the Windows Forensic Toolkit, is free for personal use but requires a onetime fee for commercial use. This is significant because if the software used in one's investigations is not properly licensed, there is a strong possibility that evidence gathered this way may be rejected if the case were ever to go to court. In addition to this it is significant to point out, that by getting these tools from trustworthy and/ or known sources it makes things easier for the Investigator/ Analyst to satisfy corporate audit requirements if need be and also has the added benefit of increasing the probability of evidence gathered being admissible in court as needed. If a reader decides to use some of the distributions and tools mentioned here, it would be more beneficial for them to choose the ones they require and then package them in a sound manner, by using

the template included in this paper. In addition to this, the tools I have recommended here are what I consider useful and appropriate for me, but depending on one's requirements tools may vary.

Examining the other tools that have been picked but are not part of the Multi-Session Live DVD:

While there are many very useful utilities on this live DVD, there were some that could not be included as part of one of these distributions, either due to lack of support for a distribution, or perhaps because it was a windows only tool, or lastly due to lack of space on a given live CD. It is important to point out that a multi boot DVD will not replace all Live CD's, but will cut down on the number of Live CD's and tools one needs to carry around. This is because depending on one's work environment there maybe various computers and systems that do not have DVD drives, but in most cases have at least a CD Rom; as mentioned the specifics of one's toolkit and the second CD/DVD or Disk depends on the analyst's specific environment and needs.

One of the tool-sets I would strongly recommend is the sysinternals suite from Microsoft, these small highly capable utilities include a number of very useful command line and gui based windows programs that can help a researcher determine the relationships between different programs, troubleshoot various situations and stop certain processes (this of course depends on the situation). The tools are available as a free download from the following link:
http://www.microsoft.com/technet/sysinternals/utilities/sys

internalssuite.mspx. The programs here are highly trusted and well known within the security community. It is interesting to point out that they were recently part of the 100 top security tools listing on the sectools.org website (this is a popular security tool listing maintained by Fydor, the author of the Nmap scanning tool). While some may choose to only download a couple of the tools from the Microsoft-Sysinternals site, I recommend downloading the full kit and making it a part of your DVD set, by both adding it to one of the Live CD's on your DVD, such as Helix, which has its own section of Windows Live Response tools, and on your second CD as a backup as well. The entire tool set is fairly small and rather than having to download just the tools you may need, or not being able to download or find a specific tool as you need it, you now have access to the full set and can have them at hand as and when you need them. There are a number of very useful utilities that make up this toolset; some of the most useful utilities are process explorer, PS Tools, Autoruns, TCPView and Rootkit Revealer. These tools are very useful to Incident Handlers and investigators, as they can provide significant data about an affected computers' system state and can safely be run from trusted media, without impacting the system being investigated.

I also recommend downloading a copy of the Windows Forensic Toolkit (WFT), the toolkit is essentially a very powerful batch script that can run forensic live response commands and utilities swiftly. Additionally, in terms of windows live response tools, I would also add memparser to this list. This tool which was the winner of the Digital Forensic Research Workshop 2005 Forensic challenge allows

an investigator to examine running memory and other volatile memory data (Betz, 2005). The ability to examine hidden processes and items in memory can be very useful when conducting an investigation , as some processes and surprises like rootkits can be well hidden, or only exist in memory.

It is also highly advisable to assemble a list of Linux live response tools and trusted commands specific to one's environment. It is important to point out that some of the distributions come with existing scripts customized for the toolset included, (the FCCU Toolkit comes with several scripts that can be run from the CD). This is significant because there is a high probability that the incident handler will have proprietary or unique Linux/Unix systems or home-grown utilities that they wish to keep on a forensics oriented distribution and on a backup piece of media as well. In circumstances like this it is advisable to have a live response script for your second CD/DVD (the alternate media) and also to edit the existing scripts on your live distributions as needed. Jones and Rose provide a good example of a working script that can be used with the Unix live response tools and commands they recommend (Jones et al. 2006); this script can act as an example and basis for building one's own or customizing this to better suit their environment. One may also want to consider the LINReS (Linux Incident Response Script), which can be found at the following site, http://www.niiconsulting.com/innovation/linres.html. LINRes is a Linux live response script that gathers a large amount of variable and non variable data from a suspect computer; one of its biggest strengths is that like the

Windows Forensic Toolkit, it helps automate most commands, reducing the likelihood of a first responder inadvertently damaging volatile system data. The script is available for free, but has been designed with Red Hat Enterprise Linux in mind, so there will be some work involved in customizing it to suit a reader's toolkit.

I choose to put these tools on the second DVD/ CD, but would also consider carrying the most critical tools (depending on your specific environment, for instance windows live response tools) on a usb key and write protecting the key. A paper describing how to write protect usb devices under Windows XP can be found at the following site http://www.accessdata.com/media/en_US/print/papers/wp.USB_Write_Protect.en_us.pdf. I found this to be very helpful; because write protecting the usb device means that I had taken reasonable steps to ensure that the device would not be written to and I can verify that I am dealing with my trusted tools and not the attacker's packages, if I need to use it in an investigation (this would be a just in case scenario). One of the biggest disadvantages that comes with using a usb key, is that it alters the Windows Registry settings on the PC it is plugged into. One has to keep in mind however that this does not mean, that such an attack on the windows registry key which could un-write block the usb key and destroy the integrity of the tools is impossible; it means that I have taken all reasonable and possible steps to ensure that my device and tools are secure from such an attack; there is always a remote possibility of an unknown or zero day attack that may be able to manipulate the windows registry key to carry out

said attack. In addition to this, as the device is a usb key it consequently gets treated as a drive and not the same way as a DVD or a CD does; this is important because it means the investigator/ analyst has greater flexibility when choosing what software to install on the key. I would strongly recommend keeping these tools on a usb key as a backup/ disaster scenario; if the first responders other tools fail, this allows the responder to still safely collect the volatile data.

Law and the need for process:

One has to realize that tools are not enough, while you follow technical steps to create your toolset; everything needs to be done in a process oriented manner. It is essential that you know your tools and are able to prove that you have used them in a forensically sound manner; if you are unable to prove this your evidence can be thrown out of court.

In their paper on the legal aspects of digital forensics, Ryan and Shpantzer raise some very interesting scenarios and points, which highlight the need for a process proving and highlighting that evidence gathered and tools used are done so in a forensically sound manner. One interesting scenario deals with an insider led targeted attack where several emails and messages disparaging executives are sent to various committees responsible for overseeing executives and senior management (using the names of random members of said organization). This of course creates a great deal of confusion, embarrassment and negative publicity about the same. The Security team has implemented a new Intrusion Detection System, which

generates significant information and the sysop/ analyst investigating this incident is able to trace the attack to what appears to be two insiders. This information is turned over to law enforcement and the company is able to issue a statement dealing with this (Ryan & Shpantzer, 2002). This may lead one to believe that this is the end of the situation, and the problem is solved. In this case as the IDS is a new system, the alleged attacker's lawyer could take advantage of this and argue that this was untried technology, hence the data gathered by it, should be dismissed as it is not trustworthy and is unreliable (Ryan & Shpantzer, 2002). In addition to this the lawyer also argues that the data is not gathered, stored, or even analyzed properly. To make matters worse, the evidence is dismissed at a pretrial and the alleged attackers counter-sue the organization for millions of dollars, stating that their reputation is damaged and jobs were negatively affected because of the false allegations against them. Ryan and Shpantzer point out that if this scenario seems realistic; it is because something quite similar to this actually affected George Mason University (Ryan & Shpantzer, 2002).

As an incident handler, investigator or analyst, one has an important responsibility to gather volatile data and evidence in the least invasive and most forensically sound manner possible. When researching the issue of multi OS DVD's, I noticed that while the technical steps to create a multi boot DVD were not the simplest, they were not the most complicated either and there was significant documentation explaining how to do this. At the same time however, I also realized that there was a lack of

documentation providing a process or guide and explaining how to develop your new tool or toolset in a sound manner explaining what one needed to do along the way.

This is significant because as tools are developed, they do not remain stagnant; they are constantly changing, new features are added and new bug fixes and stability enhancements are routinely released. Evidence gathered by a new tool can be challenged this way, by not only attacking the credibility of the software and the analyst involved, but also theoretically by attacking the manner in which the tool was developed.

There have been a few major cases in the USA that have greatly influenced how digital evidence is accepted and viewed in court; two of the most influential cases have been the Frye and the Daubert cases; prior to 1993, the rules on what was admissible as evidence was based on the Frye ruling; after 1993, the Daubert ruling with its new rules began to influence the admissibility of evidence (Ryan & Shpantzer, 2002). This is important because, as Multi-OS DVD sets are not widely deployed they too can be challenged as being new and unproven, unless it can be demonstrated otherwise.

In order to deal with scenarios such as those raised, by Ryan and Shpantzer a forensic analyst/ and incident handler needs to prepare for these sorts of situations prior to actually participating in any investigation. In order to make an incident handler’s job easier and increase the likelihood of evidence gathered being admitted in court, I have developed some templates; these templates can be used by any organization, no matter what its size and customized to suit their needs; Appendix B, deals with the

issue of new tools, and at the end of the paper there is a template/ walkthrough that deals with building a multi-DVD toolset in a forensically sound manner.

Advantages and disadvantages of building a Multi-Session DVD system and how this may affect an Organizations' incident response process:

While most modern computers have a DVD drive, some older computers you may encounter may only have a CD rom. This can pose a unique challenge as even if you carry a portable DVD drive, and the appropriate cables and materials you may still encounter a situation, where not all operating systems (i.e. older versions of windows) may recognize said drive unless you update the operating system's drivers (Kornblum, 2002). At the same time, you need to have an external hard drive as part of your jump bag to make forensic copies of the necessary evidence. If you are simply carrying out a pen test and updating the drivers or the Operating System is permitted, then this will probably not cause a problem; however, if you are on site actually carrying out an investigation or responding to an incident, doing so may damage the evidence and put your investigation at risk. In these cases a live CD is still necessary, however you do not need to carry several CD's with different tools on them, you can simply choose a small distribution, or build one of your own that only has some basic tools necessary for a forensics investigation or incident handling toolset. As we go through the walk through section of the paper, the reader will notice a step when I recommend that the user/ reader burn an ISO of each of the customized live distributions they are working with

prior to making the multi-session DVD. One of these verified CD's can easily work as the live CD distribution the handler carries with them, as a backup just in case the system does not have a DVD drive or the DVD does not work. If the reader/ user will be carrying out an incident response investigation, I strongly recommend carrying the reader's customized version of Helix (on CD). It is important to point out that the Helix CD contains both Windows only live Response tools and other Linux based incident handling tools as well.

While downloading the latest build of a preferred Linux live CD is always an option, there can be times an incident handler may want to add a customized tool not included as part of the standard toolset. While examining a suspect computer one or two DVD's containing all the tools the handler requires, can make it easier for him/ her to get access to the tools necessary and focus on the job at hand. Furthermore using the walk through process below and building a customized solution allows an organization to build and maintain a standard base image which can be used by all their security team members, even those specialists who are only called in when their expertise is required. A major advantage of having a standardized base is that it allows the team lead, manager or coordinator to ensure that all new members joining the team can get familiar with the specific security tools required by an organization (while many tools maybe freely available, organizations may have their own custom written in house tools, or specific versions of tools they may want their handlers to use or become familiar with). As one can imagine a standardized base can also lead to lower costs in

terms of training, and education for a given CSIRT or pen test team.

Organizations with just one person handling all their security, incident handling and tech support solutions will get a great deal of value from a multi DVD toolset, as that one person now has all the tools they need for multiple functions, in one or two DVD's, or CD's. In addition to this organizations with a small IT staff, or those that have a very tight IT and Forensics budget can take advantage of the free Forensics software included on these distributions. One very interesting opportunity that many organizations large and small can make use of is using the multi DVD distribution to create a forensic workstation, their only real costs being the hardware.

It is vital that a first responder or incident handler understands their tools and how they may impact the systems they are dealing with. The tools one uses from a live CD when carrying out an investigation can impact a systems state and in some cases change volatile system information; it is therefore crucial that the investigator knows their tools and can document this data to prevent it from hampering or weakening the investigation. Ricky D. Smith provides an excellent analysis of various live CD's and how they affect as this volatile data in his paper "Pros and Cons of using Linux and Windows Live CD's in Incident Handling and Forensics" (Smith, 2007).

Anti Forensics and Attacks on Forensic Tools: Why you need to keep your software up to date.

At the Blackhat Conferences in 2007, a very interesting paper was introduced which talked about attacks on forensics tools themselves. These developments are very serious because not keeping your toolkit up to date, especially when there are attacks that can potentially damage the integrity of your tools can harm the integrity of your investigations. Exploitable bugs in forensics software can seriously hamper a forensics investigation, by causing the software to crash prior to the investigator getting the data they require. In addition to this there is also a possibility of buffer overflow or stack overflow bugs allowing malicious code execution on the forensic examiners machine itself (Newsham, Palmer, Stamos & Burns, 2007). This is extremely dangerous as it has the potential to allow the attacker to corrupt the forensic image, hide or even destroy crucial evidence. Newsham points to an exotic theoretical scenario; in this case the forensic software under attack, simply ignores the evidence and hides whatever the attacker wants to cover up; in such a case there is no obvious evidence that an attack has even taken place (Newsham et al. 2007).

It is very important for the investigator to keep up with and understand how an attacker can take advantage of their tools and to have a backup tool available with them if need be. If the Encase utility has a vulnerability that can be taken advantage of, it would be advisable to have access to the Forensic Toolkit and the open source Sleuthkit, should they be required. The Timestomp utility from Metasploit.com's Metasploit Anti-Forensic

Investigation Arsenal (MAFIA), is a very powerful piece of software that an attacker can use to slowdown an investigation, by changing the four NTFS system timestamps (Gupta, 2006). This utility helps demonstrate the importance of understanding your tools, and being aware of what is taking place in terms of research in the security/ attacker communities. One has to keep in mind however that simply downloading the latest version of a given tool, (even if it fixes some important bugs) and deciding to use this instead of the existing version in their arsenal is not enough. It makes more sense to use a tool that one understands (even if it has bugs), rather than getting a version that is brand new and may have its own problems, unless the new tool has been thoroughly tested and proven to work by the investigator.

Building your own customized Multi Tool DVD system (Hardware requirements and notes):

Customizing and building one's own multi DVD set or even customizing a live CD requires a large amount of hard drive space and a significant amount of RAM. In order to give the reader a better understanding of the type of power needed for carrying out these exercises, I have decided to give a brief look at the sort of setup I am currently using. My machine has a core 2 duo 6600 processor, 2 GIG RAM, a DVD burner and a 500GB hard drive. I have WIN XP SP2 Pro as my base Operating System and run my various builds under VMware Workstation 5.5. I choose to run my builds on separate virtual machines because this allows me to revert to a prior clean state should something go wrong while I am remastering or installing an item on a system or

DVD. In addition to this, using virtual machines also allows me to continue accessing the internet, to check various items should my internet configuration not work as expected. It also allows me to run tests in other virtual machines with different configurations.

While some may argue that it is easier to simply roll one's own Knoppix based Forensics distribution suited for a team/ company, the live CD distributions mentioned here have already done a lot of that work for you, and distributions like Helix have already been re-mastered and fine tuned for various roles (in this case incident handling and forensics). The e-fense website for instance points out that the Helix Live distribution has been customized to be forensically sound and that it will not "touch the host computer in any way" (e-fence, 2007). Consequently, choosing a series of distributions and updating the tools on them to levels you trust and your organization is comfortable with is probably the wisest and easiest course of action. It is best to carry out one's updates using a process that documents all the steps taken to prove that the tool has been updated appropriately.

Customizing and building your own Multi-session DVD Set: A Walkthrough

Brief: How the Walkthrough will be organized

The walkthrough will start by going through the steps needed prior to actually updating and customizing the live CD's such as verifying the integrity of your tools and setting up the environment. Once the CD customization walk through has been completed the guide will move to taking the reader through the steps necessary to put all the newly created ISO's together into a multi session DVD.

Step 1: Choose your Live CD's

There are a large number of live CD distributions currently available, some are better known and are actively maintained while others have been abandoned but have a good setup and collection of tools and happen to also be the reader's favourites. I would strongly recommend the analyst examine the various live CD's available, look at what each one has to offer, examine their own needs and decide on which distributions, they want to include as part of their toolkit. I would also strongly recommend the analyst or tester get completely familiar with the tools and how they affect a system prior to using them in any investigation, or production/ real environment.

Step 2: Download your ISO's and other tools

Once the reader decides which live distributions to include in their toolkit it is time to download them; it is best to obtain the distributions from the original sources and then verify that these are indeed the legitimate

downloads by verifying these against the original's md5 check if available.

Step 3: Setting up your workspace

Making sure one's workspace is setup correctly will increase the likelihood of success, and reduce the number of failed attempts when trying to re-master a live CD, or multi-os DVD. In order to successfully customize your live CD, you first need to install a Linux operating system. While almost any of the major Linux distributions would do, one may want to consider installing a Debian based system, whether Debian itself, Ubuntu or a Knoppix build (especially if one plans to work with largely debian or knoppix based distributions). This is well documented and may make it easier to re-master a live CD as necessary, additionally as the CD's being remastered have a Debian base, most of the commands will also be fairly similar. It is important to point out, that I choose to use VMware, as it makes it easier for me to test out and experiment with different settings as needed, this is certainly not a requirement and you may wish to use real hardware, if you have this at your disposal.

The First thing one must do is create a new VMware machine and configure it to load from an ISO. Once this is complete, start the machine, and install a Linux distribution as your base image, make sure to give it plenty of RAM and swap space. The following website provides an excellent walkthrough on using cfdisk, setting up your machine and installing Linux in VMware (http://www.securityexplained.net/topics/virtEnv/index2.html). One must keep in mind that while most of the commands

here will be identical, the partitions may differ based on your machines setup.

While some may argue that this is unnecessary and most people installing or setting up Linux should already know how to do this, there may be some readers, or members of the incident handling team who may not have installed Linux before or simply do not install Linux that often. This process will allow anyone whether it is a new member to the incident handling team or an experienced member who simply needs a refresher to quickly follow the guide and begin preparing their workstation for base operating system installation.

In this case I chose to install Ubuntu 6.06 LTS as my base operating system. I chose this distribution/ operating system over others for several reasons. One feature I really liked about this distribution was its ease of use and hardware detection, it was fairly easy to install this version of Ubuntu and my hardware was detected without a problem. In addition to this, I also liked the 'clean' interface, as this made it more enjoyable to use and as it is based on Debian I knew that most of the commands would work effectively for the distributions I was re-mastering.

It is important to point out that simply installing Linux on your workstation is not enough, while some distributions may install all the tools one needs' to start re-mastering and developing the distributions, the Ubuntu distribution I chose did not have all the utilities I needed installed by default. One can add the necessary tools by executing the following command using the bash shell:

'sudo apt-get install cloop-utils mkisofs squashfs-tools qemu'

If one is unable to find the packages they need using this method, they may also wish to use the GUI based synaptic package manger which lists most of the packages available. In my case in addition to the packages mentioned above I also needed to install the pbuilder and debpkg packages. Once the user has downloaded the packages they require, some of the packages will need to be setup. A guide to installing and setting up the chroot environment for Ubuntu 6.06 can be found at the following site https://help.ubuntu.com/6.06/ubuntu/packagingguide/C/appendix-chroot.html. If the user needs to find a package and has been unable to find it this way, they may wish to search ubuntu's package repositories for the utility they are looking for. These packages include utilities to setup the chroot environment and build and edit packages and also include file systems one might need. It is important to point out that different live CD's (even if based on debian) can use different file systems. If one is re-mastering an ubuntu live CD they would need the squashfs-tools file system, while knoppix based live CD's generally use the cloop-utils package.

Step 4: Copy the cd content over into your virtual workstation

This step depends on the distributions one is working with, different Linux and UNIX distributions may require slightly different steps to execute this. It is strongly

recommended that the analyst search for documentation relating to the distribution they wish to work with, as commands between distributions may differ and furthermore some distributions and versions may have steps or commands unique to them.

In this case I had burnt the ISO's of the live CD's I was planning to work with to DVD, prior to entering my Ubuntu workstation. I started by copying the ISO I planned to work with to my desktop and then moved the ISO to a working directory by using the following commands at the bash prompt:

'mkdir ~/live'
'cd /home/user/Desktop/helix'
'mv Helix_v1.9-07-13-2007.iso ~/live'

Once the ISO has been copied, it is time to extract the CD contents; in this case I did this using the following commands at the bash prompt (Ubuntu, 2007):

'mkdir mnt'
'sudo mount-o loop Helix_v1.9-07-13-2007.iso mnt'
'mkdir extract-cd'
'rsync –exclude=/usr/local/sbin/extract_compressed_fs –a mnt/ extract-cd'

Step 5: Update the content for your live CD

In order to update the CD without negatively affecting the host system it is best to work in the chroot environment (Granneman, 2006). Once the user has entered the chroot environment, they can use the apt-get (Debian)

system to modify the components they wish to update. The user can enter the chroot system using the following command sequence:

'sudo chroot extract-cd'

At this point one can start using the apt-get command sequence to update the files they wish to. I would not recommend updating all the files available, and would only update the applications you need to. When remastering a specific distribution it is best to check for any notes or comments made by the author of that distribution. This is because some live CD's may have customized kernels', modules or special libraries setup to work with the different tools on the CD. If one just attempts to update everything on a live CD, there is a risk that the customized CD may not work as intended.

In order to update the CD using the apt-get system, one can use the following sequence of commands:

'sudo apt-get remove Mozilla-firefox' (note: this removes the current version of firefox)
'sudo apt-get install Mozilla-firefox' (note: this will download and install the latest version of firefox)

When this is complete, it is time for the analyst to clean up and exit the chroot environment. The cleanup routine can be done by executing the first of the following commands, when this is complete it is time to compress the

file system, this can be executed using the second command sequence listed below (Granneman, 2006).

'sudo apt-get clean'

'sudo mkisofs -iso-level 4 -R -U -V "Helix Custom" -hide-rr-moved -cache-inodes -no-bak -pad /usr/local/sbin/extract-cd | nice -5 create_compressed_fs - 65536 > /usr/local/sbin/extract-cd'

Step 6: Create your new ISO and burn it to CD

Step 7: Calculate the new md5 hash value and record it

After you have burnt the ISO, calculate the new md5 hash value and record it. This helps you make sure that the next time you burn a copy of your customized distribution; it has not been compromised or gone corrupt.

Step 8: Test your new customized live CD

Having burnt the ISO and calculated the new md5 hash value, it is time to test out your new live CD on both virtual and real hardware if possible. This is to ensure that it works as designed and verify you can see or access the tools you have added, removed or customized.

Step 9: Record the md5 values for the CD's you will be packaging.

Once you have completed step 8, burn all the distributions you will be packaging on separate CD's and record the md5 sum values and Release/ Distribution version information for all of these. In case something fails or a

distribution on your DVD is called into question or challenged, this demonstrates that you have a list of known good checksums and can test or prove that the version on your multi-os DVD matches this.

Step 10: Burn the distributions on to a DVD

When you have completed step 9, start your re-mastering Linux station and follow the steps outlined in Anindya Roy's creating a multi-boot DVD document, found at the following site: http://pcquest.ciol.com/content/enterprise/2005/105070101.asp.

Step 11: TEST

After you have completed step 10, and the DVD has been successfully burnt, test in on multiple configurations (this depends on one's specific environment and needs; verify that everything is working as designed on both virtual and real hardware. If this is successful and you are satisfied with your new tool, calculate the new md5 value for the Multi-OS DVD and record this along with your other Md5 sums.

Congratulations! You now have a powerful tool, with plenty of documentation and a strong process which can be analyzed, criticized and adapted as needed by your organization. In addition to this, the commands used to build the CD can be modified and possibly scripted to suit one's environment, resulting in the automation of a part of the build process.

Final Thoughts/ Conclusion:

It is important to keep in mind that while a Multi Distribution Live DVD set, makes a very important addition to your software toolkit, it may not replace the other tools you have as part of your existing software toolkit. This is because (depending on your environment) not all computers may have DVD drives, but most machines if not all will have CD Rom's. In addition to this some older hardware may not have a very large amount of RAM, and could take longer to run some of the more memory intensive distributions; in these cases you may wish to keep a less memory intensive security and forensics distribution available on CD as well. The reader may wish to keep a tested working copy of HELIX, or the FCCU Linux live CD available as individual CD's on hand in addition to their multi session live DVD. One has to remember that simply having a well engineered live CD or DVD is not enough. A process documenting what was done by the reader and the steps they carried out when developing their new toolset is crucial. This is especially important because while creating a Multi Session/OS DVD is not the most complicated issue, following a process to build this in a forensically sound manner is not the easiest. It is also important to point out that while Multi-OS DVD's are not new in themselves, they have not been widely deployed(if at all) as part of an Incident Handler's toolkit in the past; hence this may be treated as a new tool/ toolset by some in the information security and legal communities.

If one is not careful when building a new tool, or assembling one's toolset there is always a slight

possibility that crucial data can be lost, or get corrupted. In addition to this, even if the analyst knows that the data gathered with a new tool or toolset is untainted, others do not. The analyst may need to prove that the tool does what it says. A well designed process, customized to one's organizations environment and specific needs can help demonstrate that a tool or toolset was designed in a forensically sound manner, thus increasing the acceptability of a new tool or item and the data gathered by it in corporate, court environments and by the security community in general.

In conclusion a Multi-OS DVD set while a bit of a new concept, should become a crucial part of the Pen Tester/ Incident Handler's toolkit. This can lower training costs, and allows the analyst to carry their library of tools in a more accessible fashion. This does however require some work, it requires the analyst to understand their tools, and follow a process to ensure things are being done in a sound manner. The ultimate result is a very powerful tool and process customized to one's environment that can allow a security team to carry out their functions more effectively.

Appendix A

UNIX and Windows Live Response Tools one must have as part of their Multi Session DVD toolkit and Second CD/DVD.

The tools mentioned here can be used to gather volatile data for almost any Windows or UNIX/ Linux System; some of these trusted commands can be found in the Forensics oriented distributions mentioned earlier like HELIX or FCCU Linux. One may also wish to include these trusted commands and tools on both the Multi OS DVD and the CD, in case a DVD Drive is not available and as a backup, in case something ever goes wrong and an alternative piece of media is required (Mandia et al. 2003).

The List:

Linux/UNIX commands:

Ls	dd	bash	last	vi	cryptcat	datecat
netstat	icat	des	modinfo	w	strace	Hunter.o
strings	pcat	lsof	file	lsmod	cat	insmod
More	truss	perl	md5sum	pkginfo	rm	NetstatArproute
script	gzip	df	ps	netcat	ifconfig	dmesg
kstat	dcfldd	dd_rescue	ned	ldd		

LINres (Linux Incident Response Script)

Windows Forensic Toolchest

Memparser

Sysinternals Suite

Note:

This group of commands and tools is based on the list of useful Linux commands found in Mandia's book, Incident Response & Computer Forensics (Mandia et al. 2003)and Burdach's paper on Live forensic analysis of a Linux System (Burdach, 2004).

In terms of UNIX/ Linux Live Response, if a system has been compromised by a Kernel Level Rootkit like knak for instance, there are a number of ways for an attacker to hide the rootkit from regular system commands, and even if you do find the rootkit, you can never be absolutely sure that the compromised system is completely clean (Jones, Bejtlich et al. 2006). In such a scenario, the safest thing that can be done, is rebuilding the system from scratch.

Appendix B

Introducing a brand new or unknown (newly developed) tool to the security community: Process Template: A Walkthrough

This template can be used as a process document and checklist, to make sure your tool or toolset has been developed in a forensically sound manner. This can be especially useful when introducing a newly developed tool to the security community in general and can also help demonstrate due diligence and that you have taken all reasonable steps to ensure that your tool or toolset is sound and this may increase the likelihood of data gathered with your newly developed tool being accepted in court when needed. Analysts or readers should use this template as a starting point; while the information in this template might be enough to satisfy some organizations needs, each organization is unique and may wish to customize the template (while retaining the process and its essence)to better suit their specific requirements.

A. Document everything about the tool possible.

- How does it work?
- What are its dependencies?
- What is its purpose?
- Are there other tools that are widely used that do the same sort of thing?

B. Test the tool under various configurations.

- As an example if this is a windows only tool, have you tested this with multiple windows versions (or if the tool is only meant to support a single version of windows, have you tested your tools several times under identical conditions)?
- Is your data and are your results consistent?
- If there are other tools that do the same sort of thing as this tool, is the data generated similar across these tools, or is it radically different?

C. How does this tool affect the system being examined?

- Does the tool make minor changes to the system processes or modules or Windows Registry, and if so are these specific and consistent over different versions of the Operating system being examined? In addition to this has this been examined with different Service Packs and common enhancements?

D. Has this tool been examined or used by others (Colleagues/ friends or other experts) within the security community?

- Do others who examine the data generated by this tool view and interpret it the same way as you, or are their interpretations and understanding of the data generated different? If other experts interpret the data differently, can you provide an explanation for this? (Hailey, 2007).

E. Have you gone through the above Checklist?

- If you have made updates and revisions, have you created a change-document, listing what has changed between different versions?
- Have you made backups of all your necessary documentation and data?
- Has your documentation been prepared in a professional manner, one that is likely to be accepted by your peers and others in the security community and one you are prepared to exhibit in court if called upon or need be?

Multi-Tool DVD Sets: An important addition to the Incident Handler/ Pen Tester's toolkit

Bibliography:

Beckers, J. F. (2006). lnx4n6.be The Belgian Computer Forensic Website. Retrieved October 30, 2007, from Linux4n6 Web site: http://www.lnx4n6.be/index.php?sec=Documentation&page=bootcdcontent#video%20tools

BeleniX: The OpenSolaris Live CD. Retrieved October 30, 2007, from BeleniX Web site: http://www.genunix.org/distributions/belenix_site/

Betz, Chris (2005). Memparser Analysis Tool. *(Digital Forensics Workshop) DFRWS 2005 Forensics Challenge*, Retrieved October 29, 2007, from https://www.dfrws.org/2005/challenge/memparser.shtml

Burdach, M (2004-03-22). Forensic Analysis of a Live Linux System, Pt. 1. Retrieved October 29, 2007, from SecurityFocus Web site: http://www.securityfocus.com/infocus/1769

Burdach, M (2004-04-12). Forensic Analysis of a Live Linux System, Pt. 2. Retrieved October 29, 2007, from SecurityFocus Web site: http://www.securityfocus.com/infocus/1773

e-fense, The Helix Live CD page. Retrieved October 30, 2007, from Helix Incident Response and Forensics Web site: http://www.e-fense.com/helix/

Multi-Tool DVD Sets: An important addition to the Incident Handler/ Pen Tester's toolkit

Fade, (2006). How to build an Open-BSD Live-CD from Scratch. Retrieved October 29, 2007, from http://kaos.to/cms/component/option,com_docman/Itemid,34/task,cat_view/gid,24/

Granneman, S. (2006). *Hacking Knoppix*. Indianapolis, Indiana: John Wiley & Sons.

Gupta, C. (2006-06-22). Timestomp.exe. *Checkmate*, Retrieved October 29, 2007, from http://www.niiconsulting.com/checkmate/2006/06/timestompexe/#more-16

Hailey, S. (2007). Customize the Ubuntu Live CD. Retrieved October 30, 2007, from The Ethical Hacker Network: The Tools Proven in court question Web site: http://www.ethicalhacker.net/content/view/61/2/

Hurlbut, D AccessData: Write Protect USB Devices. Retrieved October 30, 2007, from AccessData: Write Protect USB Devices Web site: http://www.accessdata.com/media/en_US/print/papers/wp.USB_Write_Protect.en_us.pdf

Jones, Keith J. & Bejtlich, Richard & Rose, Curtis W. (2006). Real Digital Forensics: Computer Security & Incident Response. Chelmsford, Massachusetts: Addison-Wesley/Pearson Education, Inc.

Kornblum, J. (2002-08-08). Preservation of Fragile Evidence by First Responders. Retrieved October 29, 2007, from http://www.e-fense.com Web site: http://www.e-fense.com/helix/Docs/Jesse_Kornblum.pdf

Mandia, Kevin & Prosise, Chris & Pepe, Matt (2003). Incident Response & Computer Forensics: Second edition. Emeryville, California: McGraw-Hill/Osborne.

NII Consulting, (2007). LINReS. Retrieved October 30, 2007, from LINReS Web site: http://www.niiconsulting.com/innovation/linres.html

OpenSolaris Project: Live Media: Technologies for distributions running from CD and other media. Retrieved October 30, 2007, from OpenSolaris Project Web site: http://www.opensolaris.org/os/project/livemedia/

Roy, A. (2005). Creating a Multi-boot DVD. Retrieved October 30, 2007, from PCQuest: Enterprise: Creating a Multi-Boot DVD Web site: http://pcquest.ciol.com/content/enterprise/2005/105070101.asp

Russinovich, M (2007). Sysinternals Suite. Retrieved October 30, 2007, from Microsoft Technet: Sysinternals Suite Web site: http://www.microsoft.com/technet/sysinternals/utilities/sysinternalssuite.mspx

Multi-Tool DVD Sets: An important addition to the Incident Handler/ Pen Tester's toolkit

Newsham, T. & Palmer, C. & Stamos, A. & Burns, J. (2007-08-01). Breaking Forensics Software:Weaknesses in Critical Evidence Collection. *iSEC Partners*, Retrieved October 29, 2007, from http://www.isecpartners.com

Ryan, D. & Shpantzer, G. (2002). Legal Aspects of Digital Forensics. Retrieved October 29, 2007, from www.danjryan.com/Legal%20Issues.doc

Smith, R.D. (2007). Pros and Cons of using Linux and Windows Live CDs in Incident Handling and Forensics. *SANS Reading Room*, Retrieved October 29, 2007, from https://www2.sans.org/reading_room/whitepapers/honors/1706.php

Van Spyk, R. Chroot Environment. Retrieved October 30, 2007, from Security Explained: Installing Linux in a virtual environment Web site: http://www.securityexplained.net/topics/virtEnv/index2.html6/ubuntu/packagingguide/C/appendix-chroot.html

Ubuntu, Chroot Environment. Retrieved October 30, 2007, from Ubuntu Documentation: Chroot Environment Web site: https://help.ubuntu.com/6.06/ubuntu/packagingguide/C/appendix-chroot.html

Community, Ubuntu (2007). Customize the Ubuntu Live CD. Retrieved October 30, 2007, from LiveCDCustomization, Community Ubuntu Documentation Web site: https://help.ubuntu.com/community/LiveCDCustomization?action=show&redirect=LiveCDCustomization%2F6.06#head-93c6e5fbc9eb7fdb6e531354850474c781a92eb9