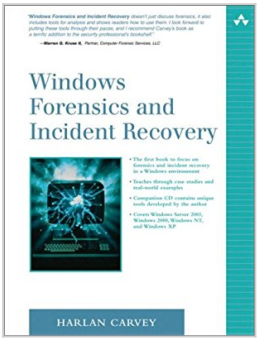

Windows Forensics and Incident Recovery

By Harlan Carvey

Windows Forensics and Incident Recovery By Harlan Carvey

Provides a 'command-line centric' view of Microsoft and non-Microsoft tools that can be very helpful to folks responsible for security and system administration on the Windows platform. This book focuses on forensics and incident recovery in a Windows environment. It teaches through case studies and real world-examples.

Windows Forensics and Incident Recovery

By Harlan Carvey

Windows Forensics and Incident Recovery By Harlan Carvey

Provides a 'command-line centric' view of Microsoft and non-Microsoft tools that can be very helpful to folks responsible for security and system administration on the Windows platform. This book focuses on forensics and incident recovery in a Windows environment. It teaches through case studies and real world-examples.

Windows Forensics and Incident Recovery By Harlan Carvey Bibliography

- Rank: #1708893 in Books
- Published on: 2004-07-31
- Original language: English
- Number of items: 1
- Dimensions: 9.10" h x 1.10" w x 7.00" l, 2.09 pounds
- Binding: Paperback
- 480 pages

Preface

As long as networks of Microsoft Windows systems aremanaged, administered, and used by people, security incidents will occur.Regardless of whether we√ïre talking about hundreds of corporate Windowsworkstations and servers or home user systems running Windows XP on broadbandconnections to the Internet, Windows systems will be attacked, compromised, andused for malicious purposes. This is not to say that only Windows systems willbe attacked; rather, Windows systems are highly pervasive throughout the entirecomputing infrastructure, from home and school systems to high-end e-commercesites. In contrast to this pervasiveness, information regarding conductingeffective incident response and forensic audit activities on Windows systems islimited, to say the least. Attacks may come from insiders who have legitimatephysical access to systems and are authorized to use them or from facelessindividuals hiding in the shapeless ether of the Internet. Knowing this, anyonewho manages or administers Windows systems (including the home user) needs toknow how to react when he suspects that an incident has occurred.

When it comes to investigating and resolving computer securityincidents, Windows systems lag well behind Linux and * nix systems. This gapcan be attributed to a variety of reasons. One reason is a lack of detailedtechnical knowledge regarding Windows systems themselves on the part ofadministrators. This lack of understanding may be due at least in part toMicrosoft√ïs use of graphical user interfaces (GUIs) to control everything fromthe installation process to all aspects of system administration. Attackers andmalicious users take steps to ensure that their activities remain hidden fromview, particularly from the system√ïs GUI tools such as the Event Viewer and theTask Manager. For example, enabling an audit policy requires that the systemadministrator navigate through multiple layers of the GUI, while an attackercan easily disable (and then reenable, if necessary) that audit policy with asingle command line tool (which, incidentally, is provided for free fromMicrosoft).

Other reasons for the "incident response gap" include a lack ofunderstanding regarding how to use available native and third-party tools toretrieve data and how to interpret the data that is collected from potentiallyinfected or compromised systems. Many useful and powerful tools that mirror thefunctionality used on Linux systems are not available through either theMicrosoft operating system distributions or the Resource Kits. Sites that makethese tools available are scattered across the Internet, with no centrallocation cataloguing them. This book was written to aid anyone investigatingincidents that occur on Windows systems by providing information regarding thetools and techniques used to respond to incidents and conduct forensic audits.

This book arose out of a need that I, and I am sure others, haveseen in the Microsoft Windows system administration community. Microsoft√ïsnetwork

operating systems, beginning with Windows NT, are designed to be easyto use and manage. These systems come with some very powerful tools. As usefulas these tools are to the administrator, they are also very useful to anattacker or to a malicious user. Most system administrators and owners spendtheir time dealing with Windows operating systems through the GUI, and in doingso, miss many of the important aspects of the operating system that go on"under the hood." For example, the Task Manager does not show the complete pathto the executable image for each process, nor does it display the command lineused to launch each process. This information is available using third-partytools, which most folks who work with Windows systems may not be familiar with.Therefore, it may be relatively simple to hide an errant process, such as anetwork backdoor, by renaming the file "svchost.exe" or something similarlyinnocuous.

Several years ago, I developed a hands-on course for teachingsystem administrators how to respond to security incidents on Windows 2000systems. While teaching the course to system administrators at variousorganizations, I saw the same things that I saw on listservs and on forums onthe Internet. During the first break on the first day of the course, I would goaround the room and "infect" all of the systems with a "Trojan." This "Trojan"was netcat, renamed to "inetinfo.exe," listening on port 80. When the attendeesreturned to the room, I√ïd tell them that I "infected" their systems andchallenged them to find it. The purpose of this exercise was not to find outwho could find the "Trojan" first but to look at the steps that the attendeeswould go through in their incident response activities, to look at their"methodology." Invariably, every attendee would examine the contents of theEvent Log, comb through the Task Manager, and maybe run `netstat √êan` from acommand prompt. All of the systems were connected to the Internet, and the onlyinstructions I would give to the class was that they could not use any of thetools from the course CD that I√ïd put together. As the course progressedthrough the rest of the two days, the attendees became familiar with the toolsand techniques they could use to retrieve valuable data about a system, as wellas how to interpret that data.

I√ïve assembled a good deal of unique content for this book,information that I√ïve developed because I haven√ït been able to locate it anyplace else and therefore had to do my own research. For example, when I firstbegan researching NTFS alternate data streams, there wasn√ït much informationavailable. Over time, research has revealed additional information, which isincluded in this book. I√ïve included tools that I√ïve developed (written inPerl) and information, results, and insights from my own research. This bookalso includes information from a variety of sources put together in a singlelocation so that it can be easily referenced.

Unlike other books about incident response, this book is specificto Windows systems. Other books on the subject will present a great deal ofinformation regarding Linux and Unix systems, and in some cases, leave it up tothe reader to extrapolate the information to Windows. All of the tools andtechniques presented in this book are specific to Windows (NT, 2000, XP, and2003) systems.

The book is organized so that the reader progresses through anunderstanding of incidents, what they are and how they can (and do) occur. Fromthere, the reader is guided through developing an understanding of what isrequired to prevent incidents and how to prepare for them, and then where tolook for data and how to analyze that data, should an incident occur. Datahiding and tools used

in incident response and live forensic audits are coveredat great length, and all of the information presented is specific to Windowsoperating systems, file systems (i.e., NTFS), and applications (i.e., MS Word,etc.). This information is presented in a progression, each chapter taking thecontent of the previous chapter further. However, each chapter can also stand onits own, as a reference that the reader can return to time and time again.

The main premise of this book is really very simple. Whenincidents occur, an entire spectrum of incident response activities can beperformed. The lower end of the spectrum involves...well...nothing. Noactivity. Basically, the incident goes completely unrecognized or is simplyignored. The opposite end of the spectrum consists of those activities thatpurists think of when they hear the word "forensics": the system is shut down ina forensically sound manner and a bit-level image of the drive is made. Allinvestigative activities are then conducted against that copy. This is usuallyaccompanied by law enforcement involvement and may even lead to prosecution.However, many organizations do not wish to involve law enforcement when anincident occurs and generally conduct non-litigious investigations because theyjust want to get systems back online and in use. In other cases, potentiallycompromised systems may be part of an e-commerce infrastructure, in whichdowntime is measured in hundreds of dollars per minute. In such cases, aninvestigation will occur, but it will not involve law enforcement or legalprosecution, as the goal is determining what, if anything, happened. These stepsmay be required to gather information and facts in order to justify furtheraction, such as taking the system down.

In addition, a great deal of extremely valuable informationregarding the state of the system is lost when the system is shut down. This informationis referred to as "volatile" information, and it includes such things asprocess information, network connections, clipboard contents, etc. Thisinformation can be retrieved, parsed, and analyzed in order to determine firstwhether an incident has even occurred, and then the extent of the incident. Insome cases, enough information may have been collected to show that theincident is manageable, and the system does not have to be taken out of serviceto be "cleaned." More importantly, the investigator will want to understand how the system was infectedor compromised so that shortfalls in security policies can be rectified andother systems protected.

The Perl programming language is used to programmaticallydemonstrate many of the concepts addressed throughout the book. The underlyingpremise of the book is to get the reader "under the hood" within the Windowssystem, that is, to show the reader how to move beyond the simple GUI toolsprovided with the operating system in order to collect information about thestate of the system. Many third-party tools are discussed, and several Perlscripts are provided in order to support this premise. Perl scripts are alsoused in this book to provide for customization and automation. Bycustomization, we mean that Perl is used to correlate and "massage" the outputof various third-party tools in order to present a more complete picture of thedata. By automation, we mean that Perl is used in this book to implement amethodology so that the investigator does not have to perform the steps byhand, thereby avoiding mistakes and making the overall process more efficient.

This book guides the reader through information, tools, andtechniques that are required to conduct incident response and live forensicaudit activities. By providing the necessary background for understanding howincidents occur and

how data can be hidden on compromised systems, the readerwill have a better understanding of the "why√ïs" and "how√ïs" of incidentresponse and forensic audit activities.

Read Windows Forensics and Incident Recovery By Harlan Carvey for online ebook

Windows Forensics and Incident Recovery By Harlan Carvey Free PDF d0wnl0ad, audio books, books to read, good books to read, cheap books, good books, online books, books online, book reviews epub, read books online, books to read online, online library, greatbooks to read, PDF best books to read, top books to read Windows Forensics and Incident Recovery By Harlan Carvey books to read online.

Online Windows Forensics and Incident Recovery By Harlan Carvey ebook PDF download

Windows Forensics and Incident Recovery By Harlan Carvey Doc

Windows Forensics and Incident Recovery By Harlan Carvey Mobipocket

Windows Forensics and Incident Recovery By Harlan Carvey EPub