Case Studies

This book will utilize five main scenarios so that you may follow along with the explanation of the techniques, tools, and processes presented throughout the text. You can follow along with every technique presented because all of the data collected is stored on the DVD, which is included with this book. (Please refer to “How to Use the DVD” in the Preface to access the evidence.) This section will introduce you to the players in each scenario along with the type of data that was collected during the response.

JBR Bank’s Intrusion

You are a law enforcement officer who specializes in computer crime. As you sit down at your desk, wishing you were outside in the sunshine instead of staring at a computer screen, you receive an exciting phone call from the director of IT at JBR Bank. JBR Bank is a large, well-respected financial institution, and many of your colleagues use their services. JBR has a Web site so that customers can check account activity, pay bills electronically, and execute other financial tasks. For the bank’s help desk to properly troubleshoot customer complaints, JBR has built a pool of machines it uses when investigating bugs in its online software. After asking a few key questions, you find out that these machines are not protected by a firewall. The IT staff keeps these customer desktop simulation systems in an “open environment” to mirror the setup that a customer might operate on his dial-up or broadband connection. The pool of machines contains everything from Linux to FreeBSD, Apple OS X, Windows 2000, Windows XP, and more. Each machine has various programs installed to emulate all of the different ways a customer's computer may be configured when he experiences a bug and calls the help desk requesting assistance.

JBR's director of IT tells you that on October 1, 2003, one of the help desk employees found an odd file on one of the customer desktop simulation systems. He accessed the Windows 2000 workstation (at IP address `103.98.91.41`) and noticed an `update.exe` file located in C:\ that was zero bytes long. This file was not placed on the machine during normal business practice, so the help desk employee called corporate security. The bank's incident response policy states that the machine must be investigated using a Live Response Process, which collects the volatile data that may be lost if the computer is powered down. The responder's IP address during the live response was `103.98.91.200`. After the live response had been completed, the JBR Bank's incident response team acquired a forensic duplication using the `dd` utility. The help desk was performing network troubleshooting during the suspected time of the intrusion and may have collected network traffic of interest.

JBR's director of IT would like you, acting as a law enforcement agent, to investigate the data his incident response team has collected. JBR Bank wants to know what violations of confidentiality or integrity may have occurred. The bank is concerned about new SEC guidelines, which encourage banks to report possible compromise of customer information. As the law enforcement agent, you must help JBR Bank understand the methods used by any intruder and the scope of the intrusion, if indeed the system was compromised.

The data for this scenario is found in the `JBR_Bank` directory on the DVD.

BRJ SOFTWARE'S INTRUSION

BRJ Software is a small software engineering company that writes applications supporting financial institutions. You work in BRJ's IT department and administer several servers. Your company's software developers create the source code for your company's products on the servers you control. You are also responsible for maintaining your company's domain name, so your e-mail address is listed within the publicly accessible WHOIS contact information. On September 8, 2003, the user known as `richard` came to you and said he discovered someone else logging into his account when he issued the `w` command.

You discover that the IP address Richard reported, `102.60.21.3`, is indeed a Linux machine that your developers occasionally use to test their software. After you realize that you must not have applied the latest security patches, you break out in a cold sweat. Your boss is going to be upset!

You immediately decide to write all of the network traffic you have captured for the past couple of months to CD-R media. After that, you run a Live Response Process on the victim machine to collect the volatile data. The responder's IP address is 102.60.21.149. Because the machine is not used heavily, you are able to take it offline and perform a forensic duplication to preserve the evidence that may contain deleted files. You begin a chain of custody for all of the evidence you collect in case you decide to hand it over to authorities.

The data for this scenario is found in the BRJ_Software *directory on the DVD.*

KERICU'S SEC VIOLATION

As a forensic examiner for a law enforcement entity's computer crime forensic lab, you see a lot of cases come and go. You've spent time reporting violations, where high-level executives alter financial documents to make their company look better in the eyes of their stockholders. One such company, Kericu, Inc., is a well-known telecommunications hardware developer. Its executives seem to have caught the "alteration bug." Kericu's CEO, Rodger Lewis, is well known for his computer skills, and he may have put those skills to evil use. The Department of Justice recently indicted Lewis for altering quarterly statements to boost his company's earnings. Because Lewis is renowned for having computer "sk1llz" ("skills" as known by the computer underground), you expect he has cleaned his tracks. Very little computer evidence may be available. In your experience, most medium to advanced users are aware of evidence elimination software, which makes your job difficult.

Fortunately, the executive vice president of finance, Aiden Paluchi, negotiated a deal with the Department of Justice. If Paluchi testifies against the CEO, he will receive immunity from any additional charges related to this case. Paluchi supplied the DOJ with the document he says Lewis altered. Paluchi also says this document was sent to the whole executive staff through e-mail. He supplies you with a copy of this e-mail, listed here:

```
To: executives@kericu.com
From: aiden.paluchi@kericu.com
Date: Thursday July 3, 2003 15:33:02 (EDT)
Subject: Q2 Earnings Spreadsheet
Attachments: earnings.xls

Gentlemen,

This document is ready for your approval. Please e-mail back any changes that I may
```

```
have missed. Hopefully next quarter will be better than this one.

Sincerely,
Aiden Paluchi

Executive VP of Finance
Kericu, Inc.
```

You travel to Kericu headquarters and begin your analysis. You begin by acquiring a forensic duplication of Lewis's laptop hard drive using `dd`. You quickly review the image for a "smoking gun." As you expected, you did not see `earnings.xls` anywhere on Lewis's hard drive. Your job just became much harder than you thought because you will have to do a deeper analysis. Just then, an agent runs into your office and slaps down a USB memory device that was found in Lewis's home. Hopefully, after you acquire a forensic duplication of the device, you may find additional evidence of Lewis's crime.

The data for this scenario is found in the `Kericu` *directory on the DVD.*

BLASTMAX'S THEFT OF INTELLECTUAL PROPERTY CASE

Karen Jenkins was an unhappy employee at BlastMax, Inc., a leading video card engineering firm. She had always complained that she was underpaid and would start looking for a new job as soon as the market rebounded. On October 21, 2003, she did just that and went to a competitor of BlastMax. As an administrator in the IT department, it is your responsibility to collect the computer resources allocated to Jenkins when her employment was terminated. You examine the hard drive in her laptop and notice that the system initialization CDs were used to restore the laptop to the same state as when it was purchased. Therefore, there is no evidence of wrongdoing.

On October 28, 2003, your company is due to launch a new chip for a video card that will revolutionize the gaming industry. Just as your company is going to announce the product on its Web site, a sudden denial of service attack hits your network. Potential customers cannot review the new product. Ignoring the wailing and moaning of your sales and marketing staff, you spring into action. You immediately activate your network monitoring station and begin analyzing data. Then one of your friends calls you out of the blue to tell you that your Web site went down. He was very excited to see the new product but now doubts your company's commitment to its business line. He also states that a new company just introduced a similar product this morning. After he tells you the name of the company, your head begins to hurt. It is the company that recently employed Jenkins.

As you rummage through the laptop bag returned by Jenkins, you notice a personal Palm Pilot she left behind. Since your company policy states that you commingle company data on personal devices at the employee's risk, you decide to acquire a forensic duplication. Your plan now is to analyze this evidence to prove that Jenkins was a conspirator for the theft of intellectual property.

Unfortunately, we were restricted from distributing PDA forensic images. This scenario will include detailed screenshots and instructions when it is discussed.

DRAFT COMPLETE'S ATTEMPTED THEFT

Draft Complete, Inc. is a small business specializing in the artistic development of high-end jewelry. Due to the expensive inventory at Draft Complete's headquarters, every employee is thoroughly searched when leaving the building. Bruce Armiter, an employee at Draft Complete, was recently leaving work, and a security guard discovered a Compact Flash memory card in his belongings. Specifically, Armiter hid the CF card under an athletic insert in his shoe.

The security guard turned over the card to you, a local police officer, because of a "gut feeling" he had. The guard believed Armiter was smuggling data such as pictures of new products and the HQ building schematics. The guard also believed Armiter was selling them to the highest bidder. Plans of the building layout would be very valuable to thieves. A burglar would have an easy time planning the best attack to obtain some of Draft Complete's precious inventory. Your job is to prove or disprove the claims of the security guard.

The data for this scenario is found in the `DraftComplete` *directory on the DVD.*

FORENSIC TOOL ANALYSIS—ANALYZING FILES OF UNKNOWN ORIGIN

During the course of a computer intrusion investigation you will inevitably come across an executable with an unknown purpose, so we have included three chapters that will introduce you to the methods, techniques, and tools to perform forensic tool analysis of unknown executable binaries to determine their function. These chapters are not specifically tied to any of the above five main scenarios. The two forensic tool analysis scenarios include the following:

- You're working in a forensic analysis shop and you're one of the few who know anything about Linux. Analysis of a recent computer intrusion involving a Linux system was performed. Utilizing EnCase, a timeline of the intrusion was performed and the details fully documented; one critical question, however, remains: What is the file `aio` that was discovered on the victim system and what does it do? Examination of the unknown binary with the built-in hexadecimal viewer in EnCase reveals almost no human-readable text strings. As is so often the case, you are not provided with any additional details regarding the case; you are simple provided the file to be analyzed. Your job is to determine the functions and capabilities of `aio`.

- Several Windows systems in your organization were recently compromised. The incident response teams took the necessary steps to respond and safeguard the network. During the initial incident response, forensic images were obtained, and the file `sak.exe` was found on several systems. Your objective is to determine all that you can about this executable.

The data for this scenario is found in the `ToolAnalysis` *directory on the DVD.*