AUERBACH

Cyber Crime Investigator's Field Guide

BRUCE MIDDLETON

Cyber Crime Investigator's Field Guide

BRUCE MIDDLETON

AUERBACH PUBLICATIONS

A CRC Press Company

Boca Raton London New York Washington, D.C.

Cover art courtesy of Greg Kipper.

Library of Congress Cataloging-in-Publication Data

Middleton, Bruce.
Cyber crime investigator's field guide / Bruce Middleton.
p. cm.
Includes index.
ISBN 0-8493-1192-6 (alk. paper)
1. Computer crimes—Investigation—Handbooks, manuals, etc. I. Title.

HV8079.C65 M53 2001
363.25'968—dc21 2001037869
CIP

Visit the Auerbach Publications Web site at www.auerbach-publications.com

Auerbach is an imprint of CRC Press LLC

No claim to original U.S. Government works
International Standard Book Number 0-8493-1192-6
Library of Congress Card Number 2001037869
Printed in the United States of America 1 2 3 4 5 6 7 8 9 0
Printed on acid-free paper

OTHER AUERBACH PUBLICATIONS

ABCs of IP Addressing
Gilbert Held
ISBN: 0-8493-1144-6

Application Servers for E-Business
Lisa M. Lindgren
ISBN: 0-8493-0827-5

Architectures for E-Business Systems
Sanjiv Purba, Editor
ISBN: 0-8493-1161-6

A Technical Guide to IPSec Virtual Private Networks
James S. Tiller
ISBN: 0-8493-0876-3

Building an Information Security Awareness Program
Mark B. Desman
ISBN: 0-8493-0116-5

Computer Telephony Integration
William Yarberry, Jr.
ISBN: 0-8493-9995-5

Cyber Crime Investigator's Field Guide
Bruce Middleton
ISBN: 0-8493-1192-6

Cyber Forensics:
A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes
Albert J. Marcella and Robert S. Greenfield, Editors
ISBN: 0-8493-0955-7

Information Security Architecture
Jan Killmeyer Tudor
ISBN: 0-8493-9988-2

Information Security Management Handbook, 4th Edition, Volume 1
Harold F. Tipton and Micki Krause, Editors
ISBN: 0-8493-9829-0

Information Security Management Handbook, 4th Edition, Volume 2
Harold F. Tipton and Micki Krause, Editors
ISBN: 0-8493-0800-3

Information Security Management Handbook, 4th Edition, Volume 3
Harold F. Tipton and Micki Krause, Editors
ISBN: 0-8493-1127-6

Information Security Policies, Procedures, and Standards: Guidelines for Effective Information Security Management
Thomas Peltier
ISBN: 0-8493-1137-3

Information Security Risk Analysis
Thomas Peltier
ISBN: 0-8493-0880-1

Information Technology Control and Audit
Frederick Gallegos, Sandra Allen-Senft, and Daniel P. Manson
ISBN: 0-8493-9994-7

New Directions in Internet Management
Sanjiv Purba, Editor
ISBN: 0-8493-1160-8

New Directions in Project Management
Paul C. Tinnirello, Editor
ISBN: 0-8493-1190-X

A Practical Guide to Security Engineering and Information Assurance
Debra Herrmann
ISBN: 0-8493-1163-2

The Privacy Papers:
Managing Technology and Consumers, Employee, and Legislative Action
Rebecca Herold
ISBN: 0-8493-1248-5

Secure Internet Practices:
Best Practices for Securing Systems in the Internet and e-Business Age
Patrick McBride, Joday Patilla, Craig Robinson, Peter Thermos, and Edward P. Moser
ISBN: 0-8493-1239-6

Securing and Controlling Cisco Routers
Peter T. Davis
ISBN: 0-8493-1290-6

Securing E-Business Applications and Communications
Jonathan S. Held and John R. Bowers
ISBN: 0-8493-0963-8

Securing Windows NT/2000:
From Policies to Firewalls
Michael A. Simonyi
ISBN: 0-8493-1261-2

TCP/IP Professional Reference Guide
Gilbert Held
ISBN: 0-8493-0824-0

AUERBACH PUBLICATIONS
www.auerbach-publications.com
To Order Call: 1-800-272-7737 • Fax: 1-800-374-3401
E-mail: orders@crcpress.com

Preface

In the past 30 years, there has been phenomenal growth in the area of data communications, to say the least. During the Vietnam War, one of my duty stations was on an island in the China Sea. I was part of a Signal Intelligence group, intercepting and decoding wartime communications traffic. We did our best to decode and analyze the information we intercepted, but there were many times when the help of a high-end (at that time) mainframe computer system was required. Did we have a communication network in place to just upload the data to the mainframe, let the mainframe do the processing, and then download the data back to us? Not a chance! We had to take the large magnetic tapes and give them to pilots on an SR-71 Blackbird, who flew the tapes to the United States for processing on a mainframe computer system. Once the results were obtained, we would receive a telephone call informing us of any critical information that had been found. It is hard to believe now that 30 years ago that was the way things were done.

Fast forward to today. There are data networks in place now that allow us to transmit information to and from virtually any location on Earth (and even in outer space to a degree) in a timely and efficient manner. But what has this tremendous enhancement in communications technology brought us? — another opportunity for criminal activity to take place. Who are the criminals in CyberSpace? One group to start with is organized crime ... such as the Mafia and others. What is their major focus? Financial activity, of course. They have found a new way to "mismanage" the financial resources (among other things) of others. Persons involved in foreign espionage activities also make use of our enhanced communication systems. They routinely break into government, military, and commercial computer networked systems and steal trade secrets, new designs, new formulas, etc. Even the data on your personal home computer is not safe. If you bring work home or handle your finances on your home computer system, both your personal data and your employer's data could easily be at risk. I could go on, but I am sure you get the picture.

Why does this happen? We cannot make these communication systems fully secure. Why? Think about it. Banks and homes and businesses have been in existence for as long as we can remember. Despite all the security precautions put in place for banks, homes, aircraft, and businesses, we have not been able to fully secure them. There are still bank robberies, aircraft hijackings, and businesses and homes being broken into. Almost nothing in the physical world is really secure. If someone wants to focus on or target something, more than likely they will obtain what they want — if they have the time, patience, and other sufficient resources behind them. We should not expect CyberSpace to be any different. Just like in the physical world, where we have to be constantly alert and on guard against attacks on our government, military, corporations, and homes, we have to be even more alert in cyberspace. Why? Because people can now come into your home, your business, or secured government and military bases without being physically seen. They can wreak havoc, changing your formulas, changing your designs, altering your financial data, and obtaining copies of documents, all without you ever knowing they had been there.

So where does this bring us? — to the fact that we need to keep doing the same things we have been doing for many years in the realm of physical security. Do not let your guard down. But it also means that we must continue to enhance our security in the cyber realm. Many excellent products (hardware and software) have been developed to protect our data communication systems. These products must be enhanced even more. There are also many new and enhanced laws in the past 15 years that provide law enforcement with more teeth to take a bite out of cyber crime. What is also needed all the more are those who know how to investigate computer network security incidents — those who have both investigative talents and a technical knowledge of how cyberspace really works. That is what this book is about, to provide the investigative framework that should be followed, along with a knowledge of how cyberspace works and the tools available to investigate cyber crime — the tools to tell the who, where, what, when, why, and how.

Contents

Chapter 1

The Initial Contact

When you are first contacted by a client, whether it be in person, over the telephone, or via e-mail, before you plunge headlong into the new case, there are some specific questions requiring answers up front. The answers to these questions will help you to be much better prepared when you actually arrive at the client's site to collect evidence and interview personnel. Also remember that the cases you may be involved with vary tremendously. A short listing of case types would be:

- Web page defacement
- Hospital patient databases maliciously altered
- Engineering design databases maliciously altered
- Murder
- Alibis
- Sabotage
- Trade secret theft
- Stolen corporate marketing plans
- Computer network being used as a jump-off point to attack other networks
- Computer-controlled building environmental controls maliciously modified
- Stolen corporate bid and proposal information
- Military weapons systems altered
- Satellite communication system takeover

Since there are so many different types of cases, review the questions listed below and choose those that apply to your situation. Ignore those that do not apply. Also, depending on your situation, think about the order in which you ask the questions. Note that your client may or may not know the answers to certain questions. Even if the client does not know the answers, these questions begin the thinking process for both you and the client. Add additional questions as you see fit, but keep in mind that this should be a short

discussion: its purpose is to help you be better prepared when you arrive at the client's site, not to have the answers to every question you can think of at this time. Questions you should ask will follow. Ensure that the communication medium you are using is secure regarding the client and the information you are collecting, i.e., should you use encrypted e-mail? Should you use a STU III telephone, etc.?

- Do you have an IDS (Intrusion Detection System) in place? If so, which vendor?
- Who first noticed the incident?
- Is the attacker still online?
- Are there any suspects?
- Are security policy/procedures in place?
- Have there been any contacts with ISPs, LEO (law enforcement organizations)?
- Why do you think there was a break-in?
- How old is the equipment?
- Can you quickly provide me with an electronic copy of your network architecture over a secure medium?
- What operating systems are utilized at your facility?
- If these are NT systems, are the drives FAT or NTFS?
- What type of hardware platforms are utilized at your facility (Intel, Sparc, RISC, etc.)?
- Do the compromised systems have CD-ROM drives, diskette drives, etc.?
- Are these systems classified or is the area I will be in classified? What level? Where do I fax my clearance?
- What size are the hard drives on the compromised systems?
- Will the System Administrator be available, at my disposal, when I arrive, along with any other experts you may have for the compromised system (platform level, operating system level, critical applications running on the system)?
- What type of information did the compromised system hold? Is this information crucial to your business?
- Will one of your network infrastructure experts be at my disposal when I arrive on-site (personnel who know the organization's network: routers, hubs, switches, firewalls, etc.)?
- Have your Physical Security personnel secured the area surrounding the compromised systems so that no one enters the area? If not, please do so.
- Does the crime scene area forbid or preclude the use of electronic communication devices such as cellular telephones, pagers, etc.?
- Please have a copy of the system backup tapes available for me for the past 30 days.
- Please put together a list of all the personnel involved with the compromised system and any projects the system is involved with.
- Please check your system logs. Have a listing when I arrive that shows who accessed the compromised system in the past 24 hours.

- Do the compromised systems have SCSI or parallel ports (or both)?
- Tell the client not to touch anything. Do not turn off any systems or power, etc.
- What is the name of hotels close by where I can stay?
- It will be supper time when I arrive. Will you have food available to me while I am working?
- Provide the client with your expected arrival time.
- Tell the client not to mention the incident to anyone who does not absolutely need to know.

Chapter 2

Client Site Arrival

On the way to the client's site (whether by car, train, or aircraft), do not waste time. Focus on reviewing the answers the client gave to the questions in Chapter 1. If you were able to obtain it, review the network topology diagram that was sent to you. Discuss with your team members (if you are operating as part of a team) various approaches to the problem at hand. Know what your plan of attack is going to be by the time you arrive on-site at the client's premises. If you are part of a team, remember that there is only one person in charge. Everyone on the team must completely support the team leader at the client site.

The first thing to do at the client's site is to go through a pre-briefing. This is about a 15-minute period (do not spend much time here ... begin the evidence collection process as quickly as possible) in which you interface with the client and the personnel he has gathered to help in your investigation, giving you the opportunity to ask some additional questions, meet key personnel you will be working with (Managers, System Administrators, key project personnel that used the compromised system, security personnel, etc.), and obtain an update on the situation (something new might have occurred while you were en route).

Once again, there are a variety of questions. Depending on the case, you will choose to ask some of the questions and ignore others. Again, also consider the order of the questions. These questions should also help generate some other questions. When the questions refer to "personnel," the reference is to those who (in some way, shape, or form) had access to the compromised system(s). Some of the questions can be asked to the entire pre-briefing group, whereas others may need to be asked privately. Use discretion and tact. Again, remember that you can ask questions now, but someone may have to go find the answers and report back to you.

- Was it normal for these persons to have been on the system during the past 24 hours?
- Who was the last person on the system?
- Does this person normally work these hours?
- Do any of your personnel have a habit of working on weekends, arriving very early, or staying very late?
- What are the work patterns of these personnel?
- At what time(s) did the incident occur?
- What was on the computer screen?
- When was the system last backed up?
- How long have these persons been with the organization?
- Have any of these persons behaved in a strange manner? Do any have unusual habits or an adverse relationship with other employees?
- Have there been any other unusual network occurrences during the past 30 days?
- Can you provide me with an overview of what has happened here?
- What programs/contracts were the compromised systems involved with? What personnel work on these programs/contracts?
- Is there anything different about the area where the systems reside? Does anything look out of place?
- What level of access (clearance) does each of the individuals have for the compromised system and the area where it resides?
- Are any of the personnel associated with the systems not United States citizens?
- Are any cameras or microphones in the area that could track personnel movements at or near the compromised system area?
- Are there access logs into/out of the building and area?
- Do people share passwords or user IDs?
- Does the organization have any financial problems or critical schedule slippages?
- Have any personnel taken extended vacations, had unexplained absences, or visited foreign countries for business/pleasure during the past 90 days?
- Have any personnel been reprimanded in the past for system abuse or any other issues?
- Are any personnel having financial or marital hardships? Are any having intimate relations with any fellow employee or contractor?
- Are any personnel contractors/part-time or not full-time employees?
- Who else had access to the area that was compromised?
- What are the educational levels and computer expertise levels of each of the personnel involved with the system?
- What type of work is this organization involved with (current and past)?
- Who first noticed the incident? Who first reported the incident? When?
- Did the person who noticed the incident touch anything besides the telephone?
- Does anyone else in the company know of this?
- Based on records from Physical Security, what time did each of the personnel arrive in the building today?

- Based on records from Physical Security, if any personnel arrived early, was anyone else already in the building? Was this normal for them?
- For the past 30 days, provide me with a listing of everyone who was on the compromised system, along with their dates/times of access.
- What was the purpose of that specific system?
- Has the employment of anyone in the organization been terminated during the past 90 days?
- Can you give me a copy of the organization's security policy/procedures.
- Why do you think there was a break-in? (Try to get people to talk.)
- Obtain any records available for the compromised system, such as purchasing records (see original configuration of box) and service records (modifications, problems the box had, etc.).
- Obtain a diagram of the network architecture (if you have not already obtained one).
- Verify that any experts associated with the system are present. Obtain their names and contact information.
- Briefly spell out the evidence collection procedure you will be following to those in the pre-briefing.
- Have you received the backup tape requested for the compromised system? If not, are backups done on a regularly scheduled basis?
- Was the system serviced recently? By whom?
- Were any new applications recently added to the compromised systems?
- Were any patches or operating system upgrades recently done on the compromised system?
- Were any suspicious personnel in the area of the compromised systems during the past 30 days?
- Were any abnormal access rights given to any personnel in the past 90 days who are not normally associated with the system?
- Are there any known disgruntled employees, contractors, etc.?
- Were any new contractors, employees, etc. hired in the past month?
- Are there any human resources, union, or specific organizational policies or regulations that I need to abide by while conducting this investigation?