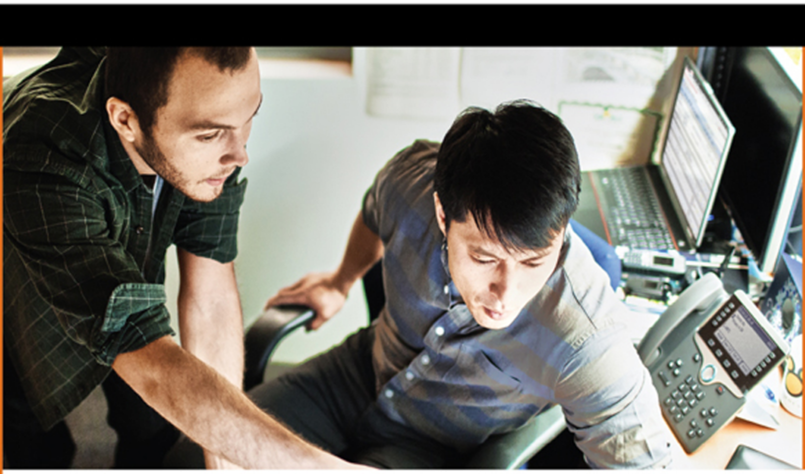

SECURITY

Investigating the Cyber Breach

The Digital Forensics Guide for the Network Engineer

Joseph Muniz
Aamir Lakhani

ciscopress.com

Investigating the Cyber Breach

The Digital Forensics Guide for the Network Engineer

Joseph Muniz, Aamir Lakhani

Cisco Press

800 East 96th Street

Indianapolis, Indiana 46240 USA

Investigating the Cyber Breach: The Digital Forensics Guide for the Network Engineer

Table of Contents

Cover

Title Page

Copyright Page

About the Authors

Dedications

Contents

Introduction

Chapter 1 Digital Forensics

- Defining Digital Forensics
- Engaging Forensics Services
- Reporting Crime
- Search Warrant and Law
- Forensic Roles
- Forensic Job Market
- Forensic Training
- Summary
- References

Chapter 2 Cybercrime and Defenses

- Crime in a Digital Age
- Exploitation

Pearson

Table of Contents

- Adversaries
- Cyber Law
- Summary
- Reference

Chapter 3 Building a Digital Forensics Lab

- Desktop Virtualization
  - VMware Fusion
  - VirtualBox
- Installing Kali Linux
- Attack Virtual Machines
- Cuckoo Sandbox
  - Virtualization Software for Cuckoo
  - Installing TCPdump
  - Creating a User on VirtualBox for Cuckoo
- Binwalk
- The Sleuth Kit
- Cisco Snort
- Windows Tools
- Physical Access Controls
- Storing Your Forensics Evidence
  - Network Access Controls
- Jump Bag
- Summary
- References

Chapter 4 Responding to a Breach

- Why Organizations Fail at Incident Response
- Preparing for a Cyber Incident

Table of Contents

Defining Incident Response

Incident Response Plan

Assembling Your Incident Response Team

When to Engage the Incident Response Team

Outstanding Items that Often Get Missed with Incident Response

Phone Tree and Contact List

Facilities

Responding to an Incident

Assessing Incident Severity

Following Notification Procedures

Employing Post-Incident Actions and Procedures

Identifying Software Used to Assist in Responding to a Breach

Trend Analysis Software

Security Analytics Reference Architectures

Other Software Categories

Summary

References

Chapter 5 Investigations

Pre-Investigation

Opening a Case

First Responder

Device Power State

Search and Seizure

Chain of Custody

Network Investigations

Forensic Reports

Case Summary

Table of Contents

    - Example
    - Acquisition and Exam Preparation
    - Example
    - Findings
    - Example
    - Conclusion
    - Example
    - List of Authors
    - Example
    - Closing the Case
  - Critiquing the Case
  - Summary
  - References
- Chapter 6 Collecting and Preserving Evidence
  - First Responder
  - Evidence
    - Autopsy
    - Authorization
  - Hard Drives
    - Connections and Devices
    - RAID
  - Volatile Data
    - DumpIt
    - LiME
    - Volatility
  - Duplication
    - dd
    - dcfldd

Table of Contents

ddrescue

Netcat

Guymager

Compression and Splitting

Hashing

MD5 and SHA Hashing

Hashing Challenges

Data Preservation

Summary

References

Chapter 7 Endpoint Forensics

File Systems

Locating Data

Unknown Files

Windows Registry

Deleted Files

Windows Recycle Bin

Shortcuts

Printer Spools

Slack Space and Corrupt Clusters

Alternate Data Streams

Mac OS X

OS X Artifacts

Log Analysis

IoT Forensics

Summary

References

Chapter 8 Network Forensics

Table of Contents

Network Protocols

Security Tools

- Firewall
- Intrusion Detection and Prevention System
- Content Filter
- Network Access Control
- Packet Capturing
- NetFlow
- Sandbox
- Honeypot
- Security Information and Event Manager (SIEM)
- Threat Analytics and Feeds
- Security Tool Summary

Security Logs

Network Baselines

Symptoms of Threats

- Reconnaissance
- Exploitation
- Malicious Behavior
- Beaconing
- Brute Force
- Exfiltration
- Other Indicators

Summary

References

Chapter 9 Mobile Forensics

Mobile Devices

- Investigation Challenges

iOS Architecture

Table of Contents

iTunes Forensics

iOS Snapshots

How to Jailbreak the iPhone

Android

PIN Bypass

How to Brute Force Passcodes on the Lock Screen

Forensics with Commercial Tools

Call Logs and SMS Spoofing

Voicemail Bypass

How to Find Burner Phones

SIM Card Cloning

Summary

Reference

Chapter 10 Email and Social Media

A Message in a Bottle

Email Header

Social Media

People Search

Google Search

Facebook Search

Summary

References

Chapter 11 Cisco Forensic Capabilities

Cisco Security Architecture

Cisco Open Source

Cisco Firepower

Table of Contents

Cisco Advanced Malware Protection (AMP)

Cisco Threat Grid

Cisco Web Security Appliance

Cisco CTA

Meraki

Email Security Appliance

Cisco Identity Services Engine

Cisco Stealthwatch

Cisco Tetration

Cisco Umbrella

Cisco Cloudlock

Cisco Network Technology

Summary

Reference

Chapter 12 Forensic Case Studies

Scenario 1: Investigating Network Communication

Pre-engagement

Investigation Strategy for Network Data

Investigation

Closing the Investigation

Scenario 2: Using Endpoint Forensics

Pre-engagement

Investigation Strategy for Endpoints

Investigation

Potential Steps to Take

Closing the Investigation

Scenario 3: Investigating Malware

Table of Contents

- Pre-engagement
- Investigation Strategy for Rogue Files
- Investigation
- Closing the Investigation

Scenario 4: Investigating Volatile Data

- Pre-engagement
- Investigation Strategy for Volatile Data
- Investigation
- Closing the Investigation

Scenario 5: Acting as First Responder

- Pre-engagement
- First Responder Strategy
- Closing the Investigation

Summary

References

Chapter 13 Forensic Tools

Tools

- Slowloris DDOS Tool: Chapter 2
- Low Orbit Ion Cannon
- VMware Fusion: Chapter 3
- VirtualBox: Chapter 3
- Metasploit: Chapter 3
- Cuckoo Sandbox: Chapter 3
- Cisco Snort: Chapter 3
- FTK Imager: Chapters 3, 9
- FireEye Redline: Chapter 3
- P2 eXplorer: Chapter 3
- PlainSight: Chapter 3
- Sysmon: Chapter 3

Table of Contents

WebUtil: Chapter 3

ProDiscover Basics: Chapter 3

Solarwinds Trend Analysis Module: Chapter 4

Splunk: Chapter 4

RSA Security Analytics: Chapter 4

IBMs QRadar: Chapter 4

HawkeyeAP: Chapter 4

WinHex: Chapters 6, 7

OSForensics: Chapter 6

Mount Image Pro: Chapter 6

DumpIt: Chapter 6

LiME: Chapter 6

TrIDENT: Chapter 7

PEiD: Chapter 7

Lnkanalyser: Chapter 7

Windows File Analyzer: Chapter 7

LECmd: Chapter 7

SplViewer: Chapter 7

PhotoRec: Chapter 7

Windows Event Log: Chapter 7

Log Parser Studio: Chapter 7

LogRhythm: Chapter 8

Mobile Devices

Elcomsoft: Chapter 9

Cellebrite: Chapter 9

iPhone Backup Extractor: Chapter 9

iPhone Backup Browser: Chapter 9

Pangu: Chapter 9

KingoRoot Application: Chapter 9

Table of Contents

Kali Linux Tools

Fierce: Chapter 8

TCPdump: Chapter 3

Autopsy and Autopsy with the Sleuth Kit: Chapters 3, 6

Wireshark: Chapter 8

Exiftool: Chapter 7

DD: Chapter 6

Dcfldd: Chapter 6

Ddrescue: Chapter 6

Netcat: Chapter 6

Volatility: Chapter 6

Cisco Tools

Cisco AMP

Stealthwatch: Chapter 8

Cisco WebEx: Chapter 4

Snort: Chapter 11

ClamAV: Chapter 10

Razorback: Chapter 10

Daemonlogger: Chapter 10

Moflow Framework: Chapter 10

Firepower: Chapter 10

Threat Grid: Chapter 10

WSA: Chapter 10

Meraki: Chapter 10

Email Security: Chapter 10

ISE: Chapter 10

Cisco Tetration: Chapter 10

Umbrella: Chapter 10

Norton ConnectSafe: No Chapter

Table of Contents

Cloudlock: Chapter 10

Forensic Software Packages

FTK Toolkit: Chapter 3

X-Ways Forensics: Chapter 3

OSforensics: Chapter 6

EnCase: Chapter 7

Digital Forensics Framework (DFF): Chapter 7

Useful Websites

Shodan: Chapter 1

Wayback Machine: Chapter 3

Robot.txt files: Chapter 2

Hidden Wiki: Chapter 2

NIST: Chapter 4

CVE: Chapter 4

Exploit-DB: Chapter 4

Pastebin: Chapters 4, 10

University of Pennsylvania Chain of Custody Form: Chapter 6

List of File Signatures: Chapter 9

Windows Registry Forensics Wiki: Chapter 7

Mac OS Forensics Wiki: Chapter 7

Miscellaneous Sites

Searchable FCC ID Database

Service Name and Transport Protocol Port Number Registry

NetFlow Version 9 Flow-Record Format

NMAP

Pwnable

Embedded Security CTF

CTF Learn

Reversing.Kr

Table of Contents

Hax Tor

W3Challs

RingZer0 Team Online CTF

Hellbound Hackers

Over the Wire

Hack This Site

VulnHub

Application Security Challenge

iOS Technology Overview

Summary

Index

Pearson