THE EXPERT'S VOICE® IN CYBERSECURITY

Cyber Operations

Building, Defending, and Attacking Modern Computer Networks

Mike O'Leary

Apress®

Cyber Operations

Building, Defending, and Attacking Modern Computer Networks

Mike O'Leary

Apress®

Cyber Operations: Building, Defending, and Attacking Modern Computer Networks

Mike O'Leary
Department of Mathematics, Towson University
Towson, MD, US

ISBN-13 (pbk): 978-1-4842-0458-0 ISBN-13 (electronic): 978-1-4842-0457-3
DOI 10.1007/978-1-4842-0457-3

Library of Congress Control Number: 2015950198

Managing Director: Welmoed Spahr
Acquisitions Editor: Robert Hutchinson
Developmental Editor: Matthew Moodie
Technical Reviewer: Jesse Varsalone
Editorial Board: Steve Anglin, Mark Beckner, Gary Cornell, Louise Corrigan, James DeWolf, Jonathan Gennick, Robert Hutchinson, Michelle Lowman, James Markham, Susan McDermott, Matthew Moodie, Jeffrey Pepper, Douglas Pundick, Ben Renow-Clarke, Gwenan Spearing, Matt Wade, Steve Weiss
Coordinating Editor: Rita Fernando
Copy Editor: Karen Jameson
Compositor: SPi Global
Indexer: SPi Global

Distributed to the book trade worldwide by Springer Science+Business Media New York, 233 Spring Street, 6th Floor, New York, NY 10013. Phone 1-800-SPRINGER, fax (201) 348-4505, e-mail orders-ny@springer-sbm.com, or visit www.springeronline.com. Apress Media, LLC is a California LLC and the sole member (owner) is Springer Science + Business Media Finance Inc (SSBM Finance Inc). SSBM Finance Inc is a Delaware corporation.

For information on translations, please e-mail rights@apress.com, or visit www.apress.com.

Apress and friends of ED books may be purchased in bulk for academic, corporate, or promotional use. eBook versions and licenses are also available for most titles. For more information, reference our Special Bulk Sales–eBook Licensing web page at www.apress.com/bulk-sales.

Any source code or other supplementary material referenced by the author in this text is available to readers at www.apress.com. For additional information about how to locate and download your book's source code, go to www.apress.com/source-code/.

Printed on acid-free paper

To all my students over the years; when I said "it is in the notes," these are the notes.

Contents at a Glance

About the Author xix

About the Technical Reviewer xxi

Acknowledgments xxiii

Introduction xxv

■ Chapter 1: System Setup 1

■ Chapter 2: Basic Offense 49

■ Chapter 3: Operational Awareness 95

■ Chapter 4: DNS and BIND 139

■ Chapter 5: Scanning the Network 177

■ Chapter 6: Active Directory 195

■ Chapter 7: Attacking the Domain 237

■ Chapter 8: Logging 283

■ Chapter 9: Network Services 311

■ Chapter 10: Malware and Persistence 367

■ Chapter 11: Apache and ModSecurity 411

■ Chapter 12: IIS and ModSecurity 457

■ Chapter 13: Web Attacks 485

■ Chapter 14: Firewalls 521

Chapter 15: MySQL and MariaDB 565

Chapter 16: Snort 605

Chapter 17: PHP 643

Chapter 18: Web Applications 679

Index 739

Contents

About the Author xix

About the Technical Reviewer xxi

Acknowledgments xxiii

Introduction xxv

Chapter 1: System Setup 1

Introduction 1

Virtualization Tools 1

VMWare Workstation 2

VirtualBox 5

Building Linux Systems 9

Configuring Software Repositories 10

Virtualization Support 15

Networking and Basic Configuration 17

Browser Software 30

Windows Systems 36

Virtualization Support 36

Windows SIDs 36

Networking and Basic Configuration 37

Notes and References 43

Introduction 43

Virtualization Tools 47

Building Linux Systems 47

Building Windows Systems 48

Chapter 2: Basic Offense 49

Introduction 49

Ethics 49

Metasploit 50

Vulnerabilities 50

Metasploit: Attacking the Browser 51

Metasploit Modules for Internet Explorer 51

Attack: MS13-055 CAnchorElement 53

Metasploit Modules for Firefox 59

Attack: Firefox XCS Code Execution 60

Metasploit: Attacking Flash 64

Attack: Adobe Flash Player Shader Buffer Overflow 65

Metasploit: Attacking Java 69

Attack: Java JAX-WS Remote Code Execution 70

Attack: Java Applet ProviderSkeleton Insecure Invoke Method 74

Metasploit and Meterpreter Commands 77

Meterpreter 82

Armitage 87

Notes and References 91

Introduction 91

Metasploit: Attacking the Browser 91

Metasploit: Attacking Flash 93

Armitage 93

References 94

Chapter 3: Operational Awareness 95

Introduction 95

Linux Tools 95

Detect: Java JAX-WS Remote Code Execution 102

Detect: Firefox XCS Code Execution 107

Windows Tools 110
Detect: MS13-055 CAnchorElement 119
Detect: Adobe Flash Player Shader Buffer Overflow 123
Network Tools 126
Detect: Java JAX-WS Remote Code Execution 130
Notes and References 134
Linux Tools 134
Windows Tools 136
Network Tools 137
References 137
Chapter 4: DNS and BIND 139
Introduction 139
Namespaces 139
Installing BIND 140
Basic Master Configuration 143
Configuring BIND 143
Forward Zone 144
Reverse Zone 146
Loopbacks 149
Root Hints 150
Controlling the Nameserver 150
Running BIND 151
Basic Slave Configuration 154
Querying DNS 157
Advanced Configuration 164
Recursion and DNS Amplification Attacks 168
Forwarders 171
Notes and References 173
References 175

Chapter 5: Scanning the Network 177
Introduction 177
NMap 177
Network Scanning and Metasploit 186
Metasploit Scanning Modules 188
Notes and References 192
Chapter 6: Active Directory 195
Introduction 195
Installation 195
Windows 2012 195
Windows 2008 198
Windows DNS 199
Scripting Windows DNS 202
DNS Configuration 204
Managing a Domain 208
Adding Systems 209
Adding Users 213
Running Commands Remotely 219
Organizing a Domain 223
Groups and Delegation 225
Remote Administration 227
Group Policy 228
Adding a Second Domain Controller 232
Notes and References 235
Installing Active Directory 235
DNS 235
Managing a Domain 235
Organizing a Domain 236

Chapter 7: Attacking the Domain 237
Introduction 237
Windows Reconnaissance 237
Windows Local Privilege Escalation 242
Bypassing Enhanced Protected Mode 243
Windows Privilege Escalation to SYSTEM 246
Privileged Attacks on a Windows System 254
Windows Domain Attacks 256
Windows Password Attacks 262
Windows Cached Credentials 264
Windows Hash Gathering 266
Windows Direct Attacks 268
Linux Privilege Escalation 270
Linux Privilege Escalation with Metasploit 271
Linux Direct Privilege Escalation 272
Linux Password Attacks 278
Notes and References 280
Windows Local Privilege Escalation 280
Windows Domain Attacks 280
Windows Password Attacks 280
Linux Privilege Escalation 281
Chapter 8: Logging 283
Introduction 283
Logging in Linux 283
Spoofing Log Messages 288
Remote Logging 289
Log Rotation 292

Logging in Windows 293
Rotating Windows Logs 301
Remote Windows Logs 302
Integrating Windows and Linux Logs 306
Notes and References 308
Chapter 9: Network Services 311
Introduction 311
SSH 311
Installing OpenSSH Server on Linux 313
Configuring OpenSSH Server on Linux 316
OpenSSH Clients on Windows 323
Man in the Middle Attack against SSHv1 326
Brute Force Attacks against SSH 331
Securing SSH 334
FTP Servers 338
Connecting to FTP Servers 340
Windows File Sharing 341
Windows Server 2012 342
Windows Server 2008 346
Accessing Windows File Shares 348
Individual File Shares 350
Samba Servers 353
Remote Desktop 357
Notes and References 362
OpenSSH Server 362
FTP Servers 363
Windows File Shares 364

Chapter 10: Malware and Persistence 367
Introduction 367
Document-Based Malware 367
Creating Malware 371
Persistence 379
Kerberos Golden Tickets 380
Sticky Keys 386
Persistence on Linux Systems 389
Malware Analysis 391
Detecting Persistence 401
Mandiant Redline 405
Notes and References 408
Malware Defense 409
Chapter 11: Apache and ModSecurity 411
Introduction 411
Apache Installation 411
Apache Configuration 414
Enabling Apache Status 416
Enabling Individual User Directories 418
Directory Aliases 420
CGI Scripts 421
Logs and Logging 423
Virtual Hosts 426
SSL and TLS 430
Signing Certificates 435
Redirection 438
Basic Authentication 438

ModSecurity 442
Installing ModSecurity 442
Starting ModSecurity 443
ModSecurity Rules 447
Notes and References 451
Chapter 12: IIS and ModSecurity 457
Introduction 457
Installation 457
IIS Configuration 458
Web Sites 460
Basic Settings 462
Command-Line Tools 463
Access Control 465
SSL/TLS 468
Redirection 473
Logging 474
ModSecurity 477
Notes and References 480
Chapter 13: Web Attacks 485
Introduction 485
Pillaging the Browser 485
Man in the Middle 490
Password Attacks 497
Burp Suite Web Proxy 497
Burp Suite Brute Force Password Attacks 499
Custom Password Attacks 503
Defending Against Password Attacks 505
Server Reconnaissance 506
Slowloris 510

Heartbleed 515
Notes and References 520
Chapter 14: Firewalls 521
Introduction 521
Network Firewalls 521
Virtual Networking 522
IPFire 523
Installing IPFire 523
IPFire Initial Configuration 525
Network Traffic Rules 527
Configuring the Network 528
Egress Filters and Proxies 534
IPFire Features 537
Attacks through a Network Firewall 538
Attacks from the DMZ 538
Attacking the Internal Network 541
Reconnaissance of the Internal Network 549
Bypassing the Firewall 555
Notes and References 562
Chapter 15: MySQL and MariaDB 565
Introduction 565
Installation 565
Using MySQL 576
Users and Privileges 578
The mysql Database 585
Managing MySQL 589
Configuration 590
Attacking MySQL 591
Notes and References 602

Chapter 16: Snort 605
Introduction 605
Installation 605
Snort as a Packet Sniffer 607
Snort as an Intrusion Detection System 610
Tuning Snort 619
Barnyard2 629
Configuring the Database 630
Configuring the Sensor 632
Starting Barnyard Automatically 635
Querying the Database 639
Notes and References 641
Chapter 17: PHP 643
Introduction 643
Installation 643
XAMPP 650
PHP on IIS 659
PHP Applications, Configuration, and Security 660
Register Globals 660
Include Vulnerabilities 663
Configuring PHP 670
Attacking PHP 671
Notes and References 677
Chapter 18: Web Applications 679
Introduction 679
Snort Report 679
BASE 684

phpMyAdmin 688
Installing phpMyAdmin 688
Attacking phpMyAdmin 694
Defending phpMyAdmin 699
Joomla 700
Installing Joomla 701
Attacking Joomla 706
Defending Joomla 710
WordPress 712
Installing WordPress 712
Attacking WordPress 719
Defending WordPress 726
Zen Cart 726
Installing Zen Cart 726
Attacking Zen Cart 734
Notes and References 736

Index 739

About the Author

Mike O'Leary is a professor at Towson University and the founding director of the School of Emerging Technologies. He developed and teaches hands-on capstone courses in computer security for both undergraduate and graduate students. He has coached the Towson University Cyber Defense team to the finals of the National Collegiate Cyber Defense Competition in 2010, 2012, and 2014.

About the Technical Reviewer

Jesse Varsalone has been teaching for 20+ years. Jesse has taught at undergraduate and graduate level at a number of colleges and universities including the Community College of Baltimore County, Champlain College, Coppin State University, Johns Hopkins University, Towson University, Stevenson University, University of Maryland Baltimore County, and University of Maryland University College. He also taught for 5 years at the Defense Cyber Investigations Training Academy (DCITA), where he was a member of the network intrusions track. Jesse holds a number of certifications in the IT field, including A+, Net+, iNet+, Server+, Linux+, CTT+, CISSP, MSCE, CCNA, and CCNA Security. Jesse has spoken at several conferences including many of the DoD Cyber Crime Conferences. He was a member of the Red Team for several years on the Mid-Atlantic College Cyber Defense Competition, where he originally met Dr. O'Leary. Jesse lives with his son Mason and daughter Kayla in Hanover, Maryland.

Acknowledgments

I would like to thank all of the students who have gone through my class over the years and provided suggestions on how to improve the course. I am especially grateful to the 2015 class and the Towson University 2015 Collegiate Cyber Defense team who have provided feedback on various drafts of these notes.

Let me thank Jesse Varsalone for his time and effort as technical reviewer, as well as the three anonymous amigos who provided valuable assistance looking over the first few chapters of the book.

I would also like to thank the members of the Apress team, including Rita Fernando and Robert Hutchinson who have provided wonderful assistance over the year it has taken to write this book.

I can't thank my family enough for giving me the time and the support to write this.

Introduction

How do you set up, defend, and attack computer networks? This book is a gentle introduction to cyber operations for a reader with a working knowledge of Windows and Linux operating systems and basic TCP/IP networking. It is the result of more than 10 years of teaching a university capstone course in hands-on cyber security.

It begins by showing how to build a range of Windows and Linux workstations, including CentOS, Mint, OpenSuSE, and Ubuntu systems. These can be physical or virtual systems built with VMWare Workstation or VirtualBox. Kali Linux is introduced and Metasploit is used to attack the browsers on these systems. A range of attacks are demonstrated, including attacks against Internet Explorer, Firefox, Java, and Adobe Flash Player. These attacks all leave traces on the target and the network that can be found by a savvy defender, and these methods are demonstrated.

This interplay between set up, attack, and defense forms the core of the book. It continues through the process of setting up realistic networks with DNS servers and Windows Active Directory. These networks are then attacked, and techniques to escalate privileges from local user to domain user to domain administrator are developed. These attacks leave tracks in the system logs that can be traced by defenders familiar with Windows and Linux logs. Of course, networks are built to provide services to users, so the book continues with an introduction to common services, including SSH, FTP, Windows file sharing, and Remote Desktop. An attacker that has gained access to a system wants to retain that access, so persistence mechanisms and malware are introduced, then defensive techniques and methods to detect, analyze, and remove Metasploit persistence scripts.

Next are web servers, both IIS and Apache. These are configured, including using signed SSL/TLS certificates, attacked via a range of techniques, and defended with tools such as ModSecurity. Real networks do not use a flat network topology, so network firewalls based on IPFire are introduced to separate the network into components and filter traffic in and out of the network. Databases are included in the network, and intrusion detection systems used to defend the network. The book concludes with an introduction to PHP- and PHP-based web applications including WordPress, Joomla, and Zen Cart.

How to Read This Book

This book is designed for readers who are comfortable with Windows, Linux, and networking who want to learn more about the operational side of cyber security. It is meant to be read hand in hand with systems; indeed the only way to learn cyber operations is to lay hands on a keyboard and work. Set up the various systems described in the book, try out the attacks, and look for the traces left by the attacks. Initially you may want to follow the text closely, but as you gain proficiency it is better to use the text only as a guide and starting place for your own explorations.

About the Systems

The book covers systems as they were used between 2008 and 2013. These systems should be patched now, so showing how to attack them today poses little risk to currently deployed systems. Back in the day though, these systems were vulnerable to these exploits even though they were fully patched at the time. The defensive techniques discussed throughout the book retain their value and can be used to defend even current systems from new attacks.

This book makes extensive use of Metasploit, and it is important to respect the fact that Metasploit is a cutting-edge tool that remains under active development. The various modules that are used in the examples in the text may be have been modified since this book was written, and some examples may work differently or not at all. Even during the year it has taken me to write this book, some Metasploit modules were modified. Note also that some Metasploit modules can be, well, finicky. For example, while I was working with one exploit module, I discovered that it would fail on some Kali systems and succeed on an essentially identical Kali system. After some experimenting and digging through Wireshark captures, I discovered that the exploit worked for some IP addresses and failed for others. Apparently the exploit encoded the callback address incorrectly but only in some cases. As another example, in June 2015, an update to Kali prevented Metasploit from starting; it took about a week before the issue was resolved.[1] However, these types of issues are normal and expected.

How This Book Is Structured

The book is divided into 18 chapters. When I use this material in my university capstone course, my students cover roughly one chapter each week. This book has more material than can be covered in a single semester course; I pick and choose the topics covered in class.

- Chapter 1, "System Setup," describes the process of setting up a testing environment using either VMWare Workstation or VirtualBox, including configuring private and protected networking. Instructions on how to install systems from 2008–2013, including Linux (CentOS, Kali, Mint, OpenSuSE, and Ubuntu) and Windows (Windows 7, Windows 8, Windows Server 2008, 2008 R2, 2012, and 2012 R2) are provided. The installation includes a complete ecosystem with Firefox, Java, and Flash Player.
- Chapter 2, "Basic Offense," covers the use of Metasploit on Kali to attack systems through the browser. This includes direct attacks against Internet Explorer and Firefox, as well as attacks against Java and Adobe Flash Player. Both Windows and Linux systems are targeted. Basic Metasploit and Meterpreter command are shown, and Armitage is introduced.
- Chapter 3, "Operational Awareness," covers the use of Windows and Linux tools and examines users, processes, and network connections on a system; this is supplemented by the use of network sniffing tools such as tcpdump, Wireshark, and Network Miner. Together, these tools are then applied to detect the signs left by the attacks from Chapter 2.

[1]See https://github.com/rapid7/metasploit-framework/issues/5553 or https://community.rapid7.com/thread/7388.

- Chapter 4, "DNS and BIND," introduces the setup and configuration of BIND DNS servers on both Windows and Linux systems. A simple DNS environment is built, with master and slave servers; the chapter includes advanced topics like forwarders and recursion. Common tools to query DNS servers like nslookup and dig are presented. DNS amplification attacks are a kind of distributed denial of service attack; these are demonstrated as well as methods to prevent a server from being used in such an attack.
- Chapter 5, "Scanning the Network," describes NMap, and how it can be used for host detection and network scanning. NMap can also be used from within Metasploit, and can store scan results in the Metasploit database.
- Chapter 6, "Active Directory," covers the process of configuring a Windows domain using Windows servers (2008, 2008 R2, 2012, and 2012 R2). Test domains are built with both Windows systems and Linux workstations using PowerBroker Open. Domain members are managed using a range of tools including PowerShell, psexec and Group Policy.
- Chapter 7, "Attacking the Domain," demonstrates how to move from a local unprivileged account on a domain member to gain SYSTEM access, then to an account on a domain controller, then to a domain administrator account. John the Ripper is used to attack password hashes, and Mimikatz is demonstrated. Privilege escalation in Linux systems is also demonstrated.
- Chapter 8, "Logging," describes the logging systems on Linux and Windows. The traces left in the logs by the privilege escalation attacks in Chapter 7 are identified. Remote logging servers are created that integrate logs from multiple systems.
- Chapter 9, "Network Services," begins with SSH and covers its installation, key generation, secure configuration, and use on Windows and Linux. A Man in the Middle attack against SSH protocol 1 is demonstrated. Methods to share files via FTP servers, Windows file shares, and Linux Samba file shares are shown. Remote Desktop on Windows is introduced.
- Chapter 10, "Malware and Persistence," covers the creation of malware, including document-based and stand-alone malware. Persistence mechanisms, including Kerberos golden tickets and sticky keys attacks are demonstrated. Malware is analyzed with a range of tools, including Bokken and ProcDot. Techniques for detecting and removing Metasploit persistence scripts are demonstrated.
- Chapter 11, "Apache and ModSecurity," covers the installation and configuration of Apache and ModSecurity on both Linux and Windows systems. A range of features are presented, including the use of per-user directories, directory aliases, CGI scripts, virtual hosts, and basic authentication. Servers are configured to use SSL/TLS, including self-signed certificates as well as the creation of a separate signing server.
- Chapter 12, "IIS and ModSecurity," covers the installation and configuration of IIS and ModSecurity on Windows Servers, including SSL/TLS and access control mechanisms.
- Chapter 13, "Web Attacks," begins by showing how to extract saved credentials from browsers. Man in the Middle attacks against SSL/TLS protected sites using Ettercap are demonstrated, including the use of sslstrip to prevent certificate warnings. Attacks against password protected web sites using Burp Suite and using custom tools are demonstrated, as well as defenses against these attacks. Common attacks against web servers, including Slowloris and Heartbleed are shown, along with appropriate countermeasures.

- Chapter 14, "Firewalls," introduces network firewalls based on the IPFire distribution. These can be used in a real or a virtual network to create internal networks and a DMZ. Egress filtering and web proxies can make a network much more resistant to attack. Attacks through the firewall are presented, including the use of SSH proxies, proxychains, and Metasploit pivots as ways to route traffic to protected assets. Shellshock is used to attack the IPFire system itself.
- Chapter 15, "MySQL and MariaDB," shows how to install and configure MySQL and MariaDB on both Windows and Linux. Common attacks are presented.
- Chapter 16, "Snort," introduces the intrusion detection system Snort, including the use of Barnyard2 to store the resulting alerts in a MySQL/MariaDB database.
- Chapter 17, "PHP," discusses PHP, including its installation on Linux and Windows; it also covers XAMPP. Attacks on PHP applications through common vectors like globally registered variables and remote include vulnerabilities are described and countermeasures discussed.
- Chapter 18, "Web Applications," covers Snort Report, BASE, phpMyAdmin, Joomla, WordPress, and Zen Cart. Each application is installed, common attacks discussed, and defensive countermeasures described.

Contacting the Author

You can reach Mike O'Leary at `moleary@towson.edu`. If you are a student or a faculty member participating at a Collegiate Cyber Defense exercise and you find this book helpful, I would love to hear from you.

CHAPTER 1

System Setup

Introduction

Cyber operations is about the configuration, defense, and attack of real systems. Publicly known vulnerabilities in deployed systems are patched, though perhaps not as rapidly as the security might hope. Any publicly known vulnerabilities that might be exploited in currently deployed systems are necessarily 0-days. In contrast, older systems can be attacked using a range of exploits that are known today, but were unknown when the systems were deployed. Thus, this book focuses on systems that were deployed between 2008 and 2013.

To configure, attack, and defend systems, a testing laboratory is required. Such a laboratory must not only allow systems to be built and run, but must provide a way to segregate them from the wider Internet; after all, older systems are known to be vulnerable to public exploits. One excellent solution is virtualization. A range of virtualization solutions exist; two commonly deployed solutions are VMWare and VirtualBox. This chapter begins with a review of these virtualization solutions.

The Notes and References lists the major Windows desktop and server operating systems released between 2008 and 2013; it also includes major releases from the CentOS, OpenSuSE, Ubuntu, and Mint Linux distributions. The section provides download locations for the various Linux distributions. This chapter shows how to build virtual machines running these operating systems.

A functioning computer system is more than just its operating system though; its entire ecosystem of installed applications must be considered. Desktop systems generally include a browser as well as plug-ins for various kinds of active web content. This chapter shows how to install three commonly used programs: Firefox, Java, and Adobe Flash Player on Windows and Linux workstations. These tools have been released in different versions and patch levels; the Notes and References lists release dates and download locations for these tools.

One advantage of modern operating systems and many major software packages is that they automatically download and install the latest security patches, often without user interaction. In almost every circumstance this is a good thing. To keep these test systems at a preferred patch level, this functionality must be disabled.

When this chapter is complete, the reader will have set up and configured a fully functional testing laboratory that can be used to run Windows and Linux virtual machines as they were deployed on a selected date between 2008 and 2013.

Virtualization Tools

A good testing laboratory needs a wide range of systems. Rather than use dedicated hardware for each system, it is much simpler to build systems using virtualization. Two of the most common tools for operating system virtualization are VMWare Workstation 10.0 and VirtualBox, while other choices include Hyper-V, Parallels, QEMU, and Xen. This section focuses solely on the first two of these. VMWare Workstation is

M. O'Leary, *Cyber Operations*, DOI 10.1007/978-1-4842-0457-3_1