



Cyber Operations

Building, Defending, and Attacking
Modern Computer Networks

—
Second Edition

—
Mike O’Leary

Apress®

Cyber Operations

**Building, Defending, and Attacking
Modern Computer Networks**

Second Edition

Mike O'Leary

Apress®

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

Mike O'Leary
Towson, MD, USA

ISBN-13 (pbk): 978-1-4842-4293-3
<https://doi.org/10.1007/978-1-4842-4294-0>

ISBN-13 (electronic): 978-1-4842-4294-0

Library of Congress Control Number: 2019933305

Copyright © 2019 by Mike O'Leary

This work is subject to copyright. All rights are reserved by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.

Trademarked names, logos, and images may appear in this book. Rather than use a trademark symbol with every occurrence of a trademarked name, logo, or image we use the names, logos, and images only in an editorial fashion and to the benefit of the trademark owner, with no intention of infringement of the trademark.

The use in this publication of trade names, trademarks, service marks, and similar terms, even if they are not identified as such, is not to be taken as an expression of opinion as to whether or not they are subject to proprietary rights.

While the advice and information in this book are believed to be true and accurate at the date of publication, neither the authors nor the editors nor the publisher can accept any legal responsibility for any errors or omissions that may be made. The publisher makes no warranty, express or implied, with respect to the material contained herein.

Managing Director, Apress Media LLC: Welmoed Spahr
Acquisitions Editor: Susan McDermott
Development Editor: Laura Berendson
Coordinating Editor: Rita Fernando

Cover designed by eStudioCalamar

Cover image designed by Freepik (www.freepik.com)

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 <http://www.apress.com/rights-permissions>.

Apress titles 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 Print and eBook Bulk Sales web page at <http://www.apress.com/bulk-sales>.

Any source code or other supplementary material referenced by the author in this book is available to readers on GitHub via the book's product page, located at www.apress.com/9781484242933. For more detailed information, please visit <http://www.apress.com/source-code>.

Printed on acid-free paper

*Dedicated to all of the security professionals
who volunteer their time to work with students.*

Table of Contents

About the Author	xxi
About the Technical Reviewer	xxiii
Acknowledgments	xxv
Introduction	xxvii
Chapter 1: System Setup	1
Introduction.....	1
Virtualization Tools	1
VMWare Workstation	2
VirtualBox	6
Building Linux Systems.....	11
Networking	11
Configuring Software Repositories.....	18
Services.....	24
Virtualization Support	25
Browser Software.....	28
Building Windows Systems.....	36
Installation.....	37
Virtualization Support	40
Networking on Windows.....	40
Browsers on Windows	43
Notes and References.....	45
Virtualization Tools.....	46
Building Linux Systems	46
Building Windows Systems	47

TABLE OF CONTENTS

- Chapter 2: Basic Offense 51**
 - Introduction..... 51
 - Ethics..... 51
 - Metasploit..... 52
 - Vulnerabilities..... 52
 - Metasploit: EternalBlue..... 53
 - Attack: EternalBlue on Windows 7 SP1 53
 - Metasploit: Attacking the Browser 62
 - Metasploit Modules for Internet Explorer 62
 - Attack: MS13-055 CAnchorElement 65
 - Metasploit Modules for Firefox..... 71
 - Attack: Firefox Proxy Prototype Privileged Javascript Injection 72
 - Metasploit: Attacking Flash..... 77
 - Metasploit Modules for Adobe Flash Player 77
 - Attack: Adobe Flash Player UncompressViaZlibVariant Uninitialized Memory..... 82
 - Metasploit: Attacking Java 86
 - Metasploit Modules for Java 86
 - Attack: Java JAX-WS Remote Code Execution 88
 - Attack: Java Applet ProviderSkeleton Insecure Invoke Method..... 93
 - Malware 96
 - Malware Attack: Windows Executable 96
 - Malware Attack: Linux ELF 100
 - Metasploit and Meterpreter Commands 101
 - Metasploit..... 101
 - Meterpreter 104
 - Armitage 115
 - Notes and References..... 117
 - References 119
- Chapter 3: Operational Awareness 121**
 - Introduction..... 121
 - Linux Tools 121
 - Determining Users Logged On to the System..... 121

Determining User Activity	124
Determining the State of the System	126
Detect: Java JAX-WS Remote Code Execution	131
Detect: Firefox XCS Code Execution	137
Windows Tools	141
Determining Users Logged On to the System.....	141
Determining the State of the System	144
Detect: MS13-055 CAnchorElement	151
Detect: Adobe Flash Player Shader Buffer Overflow.....	154
Network Tools	157
Tcpcmdump.....	157
Wireshark	157
Detect: Java JAX-WS Remote Code Execution	160
Notes and References.....	163
Chapter 4: DNS and BIND	165
Introduction.....	165
Namespaces.....	165
Installing BIND	166
Configuring BIND.....	168
Building a Master	168
Controlling the Nameserver.....	177
Starting BIND on Linux	178
Starting BIND on Windows.....	181
Completing the Installation.....	183
Building a Slave.....	184
Querying DNS.....	187
Nslookup.....	187
Dig	189
Advanced Configuration	194
Controlling Zone Transfers.....	194
Rncd: Updating Configuration.....	195

TABLE OF CONTENTS

- Rndc: Updating Zone Data 195
- Rndc: Server Control and Statistics..... 196
- Rndc: Logging DNS Queries..... 197
- BIND Version Reporting 198
- Forwarders 199
- Attacking BIND 201
 - Denial of Service Attacks Against BIND 201
 - Recursion and DNS Amplification Attacks 205
- Notes and References..... 208
- Chapter 5: Scanning the Network..... 213**
 - Introduction..... 213
 - NMap..... 213
 - NMap: Basic Usage..... 213
 - Zenmap..... 226
 - Network Scanning and Metasploit..... 227
 - Metasploit Database..... 228
 - Metasploit Scanning Modules 230
 - Custom Metasploit Modules 232
 - Notes and References..... 234
- Chapter 6: Active Directory 235**
 - Introduction..... 235
 - Installation 235
 - Installation on Windows Server 2012 and Later 235
 - Installation on Windows Server 2008 R2..... 239
 - Windows DNS..... 240
 - Scripting Windows DNS..... 242
 - DNS Configuration 244
 - Managing a Windows Domain..... 250
 - Adding Systems..... 250
 - Adding Users 257

Organizing a Domain.....	262
Groups and Delegation	265
Remote Server Administration Tools.....	266
Group Policy.....	267
Adding a Second Domain Controller.....	272
Notes and References.....	273
Installing Active Directory.....	274
DNS.....	274
Managing a Domain.....	274
Organizing a Domain	275
Chapter 7: Remote Windows Management.....	277
Introduction.....	277
Managing Systems Remotely.....	277
Server Message Block (SMB)	278
Remote Procedure Calls (RPC)	284
Sysinternals Tools.....	287
Windows Remote Management (WinRM)	290
Windows Management Instrumentation (WMI).....	293
WMI Structure.....	293
Using WinRM to Query WMI	296
Creating a WMI Namespace and Class	303
WMI Events.....	306
Using wmic to Interact with WMI.....	314
Using PowerShell to Interact with WMI	317
Using Other Languages to Interact with WMI	320
Using Linux to Interact with WMI.....	321
Windows Server Without a GUI	322
Installation Without a GUI	322
Managing the Firewall.....	326
Server Manager.....	331

TABLE OF CONTENTS

- Notes and References 334
 - Useful WMI Classes 335
 - Useful WMI Events 342
 - Useful WMI Subscription Classes 343
 - References 344
- Chapter 8: Attacking the Windows Domain 347**
 - Introduction 347
 - Windows Reconnaissance 347
 - Metasploit Tools 348
 - Native Windows Tools 353
 - Windows Local Privilege Escalation 356
 - Bypassing UAC 356
 - Windows Privilege Escalation to SYSTEM 364
 - Exploiting Insecure Configuration 371
 - Obtaining Domain Credentials 378
 - Network Attacks 378
 - Unprivileged Local Attacks 391
 - Privileged Local Attacks 395
 - Cracking Hashes with John the Ripper 404
 - Exploiting the Domain 407
 - Using Credentials Locally 407
 - Lateral Movement Across the Domain 409
 - Dumping Domain Hashes 414
 - Local Accounts 416
 - Notes and References 416
- Chapter 9: Privilege Escalation in Linux 419**
 - Introduction 419
 - Linux Reconnaissance 419
 - Metasploit Tools 419
 - Native Tools 421

Linux Privilege Escalation with Metasploit	422
Example: Ubuntu 14.04 and Overlayfs Privilege Escalation	422
Linux Direct Privilege Escalation.....	425
Example: Ubuntu 15.04 Apport CVE-2015-1325 Local Privilege Escalation Vulnerability....	427
Example: CentOS 6.3 and semtex.c.....	431
Dirty COW	434
Using Dirty COW	435
Linux Configuration Attacks	441
cron	441
SUID Programs	447
Linux Password Attacks	449
Cracking Linux Password Hashes with John the Ripper	451
Notes and References.....	451
Metasploit Attacks.....	452
Dirty COW	452
Chapter 10: Logging	455
Introduction.....	455
Logging in Linux.....	455
Syslog.....	456
Systemd-journald	460
Spoofing Log Messages	465
auditd	466
Remote Logging	472
Log Rotation	475
Logging in Windows.....	477
Viewing Windows Logs.....	481
Clearing Logs.....	486
Creating Logs	487
Auditing File Access	487

TABLE OF CONTENTS

- Rotating Windows Logs 490
- Remote Windows Logs 490
- Sysmon..... 493
- Integrating Windows and Linux Logs 501
- Notes and References..... 502
- Chapter 11: Malware and Persistence..... 507**
- Introduction..... 507
- Creating Malware..... 507
 - Msfnvenom 507
 - Veil-Evasion 517
- Windows Persistence..... 522
 - Persistence Using the Windows Startup Folder..... 522
 - Persistence Using the Registry..... 523
 - Scheduled Tasks..... 530
 - DLL Hijacking..... 533
 - Custom Services for Windows Persistence 534
 - WMI Persistence..... 536
 - Kerberos Golden Tickets..... 546
- Persistence on Linux Systems 552
 - Persistence Using Linux Startup Scripts 552
 - Persistence Using Cron Jobs..... 557
 - Custom Services for Linux Persistence 559
 - Other Approaches 563
- Notes and References 564
 - Malware..... 564
 - Windows Persistence 564
 - Registry 565
 - Scheduled Tasks..... 565
 - WMI Persistence..... 565
 - Golden Tickets 566

Chapter 12: Defending the Windows Domain	567
Introduction.....	567
Applications	568
Application Whitelisting via Software Restriction Policies	568
PowerShell	575
Detecting and Blocking Persistence	584
Startup Persistence	584
Registry Persistence.....	589
Scheduled Tasks.....	596
Service Persistence.....	600
WMI Persistence.....	604
Credentials.....	608
Passwords and Hashes	608
Mimikatz.....	611
Local Administrator Accounts.....	618
Domain Administrator Accounts	624
Manage the Network.....	624
Watching the Network	624
Network Autodiscovery.....	625
Controlling Lateral Movement	632
Notes and References.....	645
Software Restriction Policies.....	645
PowerShell	645
Persistence.....	646
WMI	646
Mimikatz.....	647
Local Administrator Accounts.....	647
Networking	647
Detecting Lateral Movement	648

Chapter 13: Network Services 649

- Introduction..... 649
- SSH 649
 - Linux Client Programs 649
 - Installing OpenSSH Server on Linux..... 652
 - Configuring OpenSSH Server on Linux 656
 - SSH Clients on Windows..... 665
 - Attacks Against SSH 668
 - Securing OpenSSH 675
 - TCP Wrappers..... 676
 - SSHGuard 676
- FTP Servers..... 684
 - Connecting to FTP Servers 686
- SMB File Sharing 687
 - Creating a SMB File Share..... 687
 - Creating a File Server on Windows..... 689
 - Accessing SMB File Shares 693
 - Creating Individual SMB File Shares on a Windows File Server 695
 - Samba Servers 698
 - Attacking SMB File Servers 704
- Remote Desktop..... 713
 - Persistence via Remote Desktop and Sticky Keys..... 715
- Notes and References..... 718

Chapter 14: Apache and ModSecurity 721

- Introduction..... 721
- Apache Installation 721
 - Installing Apache on CentOS..... 722
 - Installing Apache on OpenSuSE..... 723
 - Installing Apache on Ubuntu and Mint..... 724
 - Installing Apache on Windows..... 725
 - Version and Module Structure of Apache 725

Basic Apache Configuration	726
Configuring Apache on CentOS.....	726
Configuring Apache on OpenSuSE.....	727
Configuring Apache on Ubuntu and Mint.....	728
Apache Modules.....	729
Apache Modules: Apache Status	729
Apache Modules: Individual User Directories	737
Apache Modules: Aliases	742
Apache Modules: CGI Scripts.....	743
Logs and Logging.....	747
Error Log.....	748
Access Log	748
Virtual Hosts.....	752
Configuring a Virtual Host.....	752
SSL and TLS	756
Apache Modules: ssl_module.....	756
SSL/TLS Configuration.....	757
Signing Certificates	764
Redirection	767
Testing the Server.....	768
Testing HTTP Connections	768
Testing HTTPS Connections.....	769
Basic Authentication	772
htpasswd.....	772
Configuring Basic Authentication	774
ModSecurity.....	776
Installing ModSecurity.....	776
Configuring ModSecurity.....	778
ModSecurity Rules.....	781
ModSecurity Core Rule Set (CRS).....	783
Notes and References.....	785
Configuring EPEL.....	787

TABLE OF CONTENTS

- Chapter 15: IIS and ModSecurity 789**
 - Introduction..... 789
 - Installation 789
 - IIS Manager..... 790
 - Managing Multiple Web Servers from IIS Manager 791
 - Web Sites..... 793
 - Adding a Second Web Site..... 794
 - Default Documents 797
 - Directory Requests 797
 - Error Messages 797
 - Virtual Directories..... 798
 - Command-Line Tools 799
 - Access Control..... 801
 - Request Filtering 803
 - Authentication 804
 - SSL and TLS 805
 - Managing Web Server Certificates 805
 - Creating a Self-Signed Certificate 806
 - Windows System Certificates..... 806
 - Trusting a Signing Server 807
 - Creating a Signed Certificate..... 807
 - Managing Remote Servers 807
 - Choosing SSL/TLS Protocols and Ciphers 810
 - Redirection 811
 - Logs and Logging..... 812
 - ModSecurity..... 815
 - Notes and References..... 818
- Chapter 16: Web Attacks 821**
 - Introduction..... 821
 - Pillaging the Browser..... 821
 - Extracting Credentials from Internet Explorer 821
 - Extracting Credentials from Firefox..... 823

Man in the Middle	827
Ettercap	827
SSLStrip.....	833
Password Attacks.....	834
Burp Suite.....	835
Custom Password Attacks	842
Blocking Password Attacks with mod_evasive	843
Blocking Password Attacks on IIS	846
Heartbleed.....	846
ShellShock	850
Notes and References.....	856
Chapter 17: Firewalls	857
Introduction.....	857
Network Firewalls	857
Virtual Networking.....	859
IPFire.....	859
Installing IPFire.....	860
IPFire Initial Configuration	861
Network Traffic Rules	863
Configuring the Network	864
Web Proxies.....	870
Egress Filtering.....	872
IPFire Features	874
Attacks Through a Network Firewall.....	875
Impact of Egress Filters.....	875
Reconnaissance Beyond the Firewall.....	876
Pivots	882
SSH SOCKS5 Proxy	882
Using Metasploit Routes as Pivots	886
Mapping Egress Filter Rules.....	889

TABLE OF CONTENTS

- Attacking the Firewall 891
 - Obtaining IPFire Administrative Credentials 891
 - Pivoting to IPFire 892
 - Attacking IPFire 893
- Notes and References..... 895
- Chapter 18: MySQL and MariaDB..... 897**
 - Introduction..... 897
 - Installation 897
 - Installing MySQL and MariaDB on Linux..... 898
 - Starting MySQL and MariaDB on Linux..... 899
 - MySQL and MariaDB on Windows 899
 - The mysql Client..... 904
 - HeidiSQL 907
 - Users and Privileges 908
 - Initially Connecting to MySQL or MariaDB..... 908
 - Authenticating to MySQL 912
 - Privileges..... 923
 - Managing MySQL/MariaDB 930
 - Securing the Initial Installation..... 930
 - MySQL Configuration Files 931
 - Networking on Mint and Ubuntu..... 933
 - MySQLAdmin 933
 - Attacking MySQL..... 934
 - The MySQL History 934
 - Network Scanning for MySQL/MariaDB..... 935
 - Identifying MySQL Users 937
 - Brute Force Password Attacks Against MySQL and MariaDB..... 938
 - CVE 2012-2122 User Login Vulnerability 940
 - Cracking MySQL/MariaDB Hashes..... 941
 - CVE 2012-5613 Windows FILE Privilege Attack..... 942
 - Notes and References..... 945

Chapter 19: Snort	947
Introduction.....	947
Installing Snort.....	947
Installing Snort on Linux.....	947
Installing Snort on Windows	951
Snort as a Packet Sniffer	951
Snort as an Intrusion Detection System.....	956
Rule Installation.....	956
Starting Snort as an Intrusion Detection System	957
Testing Snort	961
Running Snort as a Service	964
Snort Variables and Preprocessors.....	971
Snort Output	977
Snort Rules	979
Snort and EternalBlue.....	980
Notes and References	981
Chapter 20: PHP.....	983
Introduction.....	983
Installing PHP on Linux	983
PHP on CentOS	984
PHP on OpenSuSE	988
PHP on Mint or Ubuntu	993
XAMPP.....	998
XAMPP Installation	998
Securing XAMPP	1001
PHP on IIS.....	1006
Installing PHP on Windows	1007
PHP Security	1013
Register Globals	1013
Include Vulnerabilities	1016
Remote Include Vulnerabilities	1019

TABLE OF CONTENTS

- Configuring PHP 1024
- Attacking PHP 1025
- PHP Persistence 1030
- Notes and References 1036
- Chapter 21: Web Applications 1039**
- Introduction 1039
- phpMyAdmin 1039
 - phpMyAdmin on CentOS via yum 1039
 - phpMyAdmin on OpenSuSE via zypper 1043
 - phpMyAdmin on Mint/Ubuntu via apt 1046
 - phpMyAdmin on Windows with XAMPP 1051
 - phpMyAdmin on Windows with IIS 1052
 - phpMyAdmin Feature Storage 1054
 - Attacking phpMyAdmin 1056
- Joomla! 1064
 - Installing Joomla! 1064
 - Using Joomla! 1072
 - Attacking Joomla! 1073
- WordPress 1084
 - Installing WordPress 1084
 - Using WordPress 1092
 - Attacking WordPress 1093
- Notes and References 1101
- Index 1103**

About the Author



Mike O'Leary is a professor at Towson University and was 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



Dr. Jacob G. Oakley spent over seven years in the U.S. Marines and was one of the founding members of the operational arm of Marine Corps Forces Cyberspace Command at NSA, Ft. Meade, Maryland, leaving that unit as the senior Marine Corps operator and a division technical lead. After his enlistment, he wrote and taught an advanced computer operations course, eventually returning back to mission support at Ft. Meade. He later left government contracting to do threat emulation and red teaming at a private company for commercial clients, serving as principal penetration tester and director of penetration testing and cyber operations. He is currently working as a Cyber SME for a government customer. He completed his doctorate in IT at Towson University researching and developing offensive cyber security methods and is the author of *Professional Red Teaming: Conducting Successful Cybersecurity Engagements* (Apress, 2019).

Acknowledgments

I would like to thank the students who have gone through my class over the years - this book would not exist without you. I hope to see you back!

Special thanks go to Jacob Oakley for his time and insight as technical reviewer.

I would also like to thank the members of the Apress team, including Rita Fernando and Susan McDermott, who have provided wonderful assistance over the two years 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 these systems, including EternalBlue and 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 setup, 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. Windows systems can be managed remotely using SMB, RPC, and WinRM; WMI is introduced, including the use of WMI to monitor systems. The Windows domain is then attacked, and techniques to escalate privileges from local user to domain user to domain administrator are developed. Tools like Mimikatz, Responder, and John the Ripper are used to obtain credentials, and hashes are passed across the domain. Linux systems are attacked next, and Dirty COW is demonstrated. To detect these attacks, a defender can turn to system logs; the reader will learn how logs are stored on Windows and Linux and how they can be made to interoperate. Sysmon is introduced and PowerShell used to query these logs.

An attacker with access to a system generally wants to maintain access to that system; this can be done using malware. Common vectors for persistence are demonstrated, including the registry, WMI persistence, and Kerberos golden tickets. A defender aware of these techniques can block or detect these attacks. An administrator can use PowerShell to search the domain to detect persistence mechanisms, firewall rules can be deployed to reduce lateral movement, and LAPS can be deployed to protect local accounts.

INTRODUCTION

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. 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 like 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 phpMyAdmin.

About the Systems

The book covers systems as they were used between 2011 and 2017. 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 current systems even from new attacks.

About the Book

This book is designed for readers who are comfortable with Windows, Linux, and networking who want to learn 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.

I have taught a university capstone course in cyber security since 2004, and this book evolved from that course. It provides the reader a comprehensive introduction to hands-on cyber operations. It contains more material than can be comfortably covered in a semester, and yet, despite its size, it is far from exhaustive.

The book includes online supplementary material at <https://www.apress.com/us/book/9781484242933>. There you can find additional notes for each chapter, along with exercises that can be used either by an intrepid individual reader or by someone teaching a course.

Formatting

One problem with writing a book that includes computer output is that sometimes the screen output is wider than the page. Wherever possible, the text reproduces exactly what appears as the output from a command. However, when the output of a line is longer than the line on a page, I have taken the liberty of editing and formatting the result to make it easier for the reader. As an example, the raw output might look like the following.

```
msf exploit(ms17_010_eternalblue) > show payloads
```

```
Compatible Payloads
```

```
=====
```

Name	Disclosure Date	Rank	Description
----	-----	----	-----
generic/custom		normal	Custom Payload
generic/shell_bind_tcp		normal	Generic
Command Shell, Bind TCP Inline			
generic/shell_reverse_tcp		normal	Generic
Command Shell, Reverse TCP Inline			
windows/x64/exec		normal	Windows x64
Execute Command			
windows/x64/loadlibrary		normal	Windows x64
LoadLibrary Path			

```
...Output Deleted ...
```

windows/x64/meterpreter/reverse_http		normal	Windows
Meterpreter (Reflective Injection x64), Windows x64 Reverse HTTP Stager (wininet)			

INTRODUCTION

```
windows/x64/meterpreter/reverse_https          normal  Windows
Meterpreter (Reflective Injection x64), Windows x64 Reverse HTTP Stager
(wininet)
windows/x64/meterpreter/reverse_tcp          normal  Windows
Meterpreter (Reflective Injection x64), Windows x64 Reverse TCP Stager
```

...Output Deleted ...

Instead, the text reads like the following.

```
msf exploit(ms17_010_eternalblue) > show payloads
```

Compatible Payloads

=====

Name	Rank	Description
----	----	-----
generic/custom	normal	Custom Payload
generic/shell_bind_tcp	normal	Generic Command Shell, Bind TCP Inline
generic/shell_reverse_tcp	normal	Generic Command Shell, Reverse TCP Inline
windows/x64/exec	normal	Windows x64 Execute Command
windows/x64/loadlibrary	normal	Windows x64 LoadLibrary Path

...Output Deleted ...

windows/x64/meterpreter /reverse_http	normal	Windows Meterpreter (Reflective Injection x64), Windows x64 Reverse HTTP Stager (wininet)
windows/x64/meterpreter /reverse_https	normal	Windows Meterpreter (Reflective Injection x64), Windows x64 Reverse HTTP Stager (wininet)
windows/x64/meterpreter /reverse_tcp	normal	Windows Meterpreter (Reflective Injection x64), Windows x64 Reverse TCP Stager

... Output Deleted ...

I hope you agree that the latter is more readable.

xxx

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. This text focuses on systems that were deployed between 2011 and 2017.

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 exists; two commonly deployed solutions are VMWare and VirtualBox. This chapter begins with an introduction to these virtualization solutions.

The chapter describes the major Windows desktop and server operating systems released between 2011 and 2017; it also includes major releases from the CentOS, OpenSuSE, Ubuntu, and Mint Linux distributions. The Notes and References 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 plugins 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. The Notes and References lists 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 test systems at a preferred patch level, this functionality must be controlled or 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 2011 and 2017.

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 and VirtualBox, while other

choices include ProxMox, Hyper-V, Parallels, QEMU, and Xen. This book focuses solely on the first two of these. VMWare Workstation is a long-standing, solid commercial product that runs on Windows and Linux; it has a free version called VMWare Player with reduced functionality. VirtualBox is a free, open source alternative; it runs on Windows Linux, Macintosh, and Solaris. In its current version, it is comparable to VMWare Workstation in functionality.

VMWare Workstation

The simplest way to learn about VMWare Workstation is to dive right in by installing and running a guest operating system.

Installing a VMWare Guest

Grab the install disc for a Linux distribution or a Windows system, and save that `.iso` file in some convenient location.¹ Launch VMWare Workstation. If the home tab appears, select “Create a New Virtual Machine”; if it does not, then the same option is available from the File menu.

VMWare Workstation begins the process of creating a new virtual machine by presenting the user with the “New Virtual Machine Wizard.” The “Typical” configuration is usually sufficient. The first question is the location of the install media; provide the location of the saved `.iso` file for the “Installer disc image file (iso).” In most, though not all cases, VMWare Workstation recognizes the operating system on the disc image. When VMWare Workstation moves to install a recognized operating system, it uses “Easy Install” and makes several choices for the user. This automated process is often convenient, however it precludes the user from choosing some things, like the system partition table or the precise collection of installed software; this can occasionally cause difficulty later.

When VMWare Workstation is installing a Windows system, it provides a dialog box that allows the user to enter the Windows product key, the precise version of Windows (e.g., Windows 8 Professional), and the new system’s user and password. When a Linux system like CentOS is being installed, VMWare instead asks for information about a system user: the user’s full name, the username, and the password for that user. The same password for the user is also used for the root account on the system. In either case, VMWare Workstation then asks for both the name of the virtual machine and the location in which it will be stored. The VMWare Workstation name is separate and distinct from any host name of the system; it is used solely by VMWare Workstation to generate the names of the files that comprise the virtual machine and will appear as the machine’s title within VMWare Workstation. When selecting the location of those files, note that there are many files for each virtual machine, so it is a very good idea to store each system in its own separate directory.

¹The Notes and References section at the end of the chapter provides links to locations containing installation discs for CentOS, Kali, Mint, Ubuntu, and OpenSuSE as well as to evaluation copies of Microsoft operating systems.