

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
Tcpdump.....	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
Rndc: 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 Appport 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
Msfvenom.....	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

TABLE OF CONTENTS

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
 - SSHGard 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