

Coding for Penetration Testers

Building Better Tools

Jason Andress

Ryan Linn



ELSEVIER

AMSTERDAM • BOSTON • HEIDELBERG • LONDON
NEW YORK • OXFORD • PARIS • SAN DIEGO
SAN FRANCISCO • SINGAPORE • SYDNEY • TOKYO

Syngress is an imprint of Elsevier

SYNGRESS

Contents

Foreword	xi
About the Authors	xiii
About the Technical Editor	xv
Acknowledgments.....	xvii
Chapter 0: Introduction	xix

CHAPTER 1	Introduction to command shell scripting	1
	On Shell Scripting	1
	What is a shell?	2
	What is a script?	3
	Shell scripts.....	3
	Where shell scripting is useful	4
	UNIX, Linux, and OS X shell scripting	5
	Shell availability and choices.....	5
	Working with shells	7
	Bash basics	8
	Hello World	8
	Variables.....	10
	Arguments.....	10
	Control statements	11
	Putting it all together with bash.....	15
	Adding /dev/tcp/ support to bash	15
	Building a port scanner with bash.....	16
	Improving the script	18
	Windows scripting.....	18
	Shell availability and choices.....	18
	Command.com and CMD.exe	18
	PowerShell	19
	Cygwin.....	20
	Other shells	21
	PowerShell basics	21
	Hello World	22
	Variables.....	23
	Arguments.....	25
	Control statements	26
	Conditionals	27
	Looping.....	28
	Putting it all together with PowerShell.....	29
	Building a port scanner with PowerShell	30
	Improving the script	32
	Summary.....	32
	Endnotes	33

CHAPTER 2	Introduction to Python	35
	What is Python?	35
	Where do we get Python?	36
	Where is Python useful?	36
	Multiplatform scripting.....	36
	Network scripting	36
	Extensive modules	37
	Reusable code that is easy to create	37
	Python basics	38
	Getting started.....	38
	Variables.....	39
	Modules.....	40
	Arguments.....	41
	Lists.....	44
	Dictionaries	46
	Control statements	51
	Functions.....	52
	File manipulation.....	54
	Exception handling	55
	Network communications.....	57
	Client communications.....	57
	Server communications	59
	Scapy.....	62
	Summary.....	68
	Endnotes	68
CHAPTER 3	Introduction to Perl	69
	Where Perl is useful	69
	Handling text	70
	Gluing applications together	70
	Working with Perl	71
	Editing tools.....	71
	Extending Perl scripts.....	72
	GUIs in Perl.....	73
	Perl basics.....	73
	Hello World	73
	Variables.....	75
	Shell commands.....	76
	Arguments.....	79
	Control statements	79
	Regular expressions	85
	File input and output	87
	Putting it all together.....	91

	Building an SNMP scanner with Perl	91
	Improving the script	97
	Summary	97
	Endnotes	98
CHAPTER 4	Introduction to Ruby	99
	Where Ruby is useful	99
	Ruby basics	100
	Variables	102
	Arrays and hashes	103
	Control statements	106
	Functions	109
	Building classes with Ruby	112
	Building a class	112
	Extending a class	114
	Accessing class data	115
	File manipulation	117
	Database basics	118
	Using DBI	119
	Using Active Record	121
	Network operations	124
	Client communications	124
	Server communications	126
	Putting it all together	129
	Summary	134
	Endnotes	135
CHAPTER 5	Introduction to Web scripting with PHP	137
	Where Web scripting is useful	137
	Getting started with PHP	138
	Scope	138
	PHP basics	138
	Functions	145
	Handling forms with PHP	147
	File handling and command execution	150
	File handling	150
	Command execution	154
	Putting it all together	156
	Summary	159
CHAPTER 6	Manipulating Windows with PowerShell	161
	Dealing with execution policies in PowerShell	161

	Execution policies.....	161
	Bypassing the policies	162
	Getting in	165
	Penetration testing uses for PowerShell.....	166
	Controlling processes and services	166
	Interfacing with the event logs.....	168
	Getting and sending files over the network	169
	Interfacing with the Registry.....	171
	PowerShell and Metasploit.....	176
	PowerShell-oriented Metasploit modules	177
	PowerDump	177
	Windows gather PowerShell environment setting enumeration	178
	Making use of the modules	178
	Summary.....	179
	Endnotes	180
CHAPTER 7	Scanner scripting.....	181
	Working with scanning tools.....	181
	Netcat.....	181
	Nmap.....	182
	Nessus/OpenVAS.....	182
	Netcat.....	183
	Implementations of Netcat	183
	Simple Netcat usage	184
	Building a Web server with Netcat.....	185
	Transferring files with Netcat.....	187
	Nmap.....	191
	Working with service probes in Nmap	191
	The Nmap scripting engine	194
	Building Nmap NSE files	194
	Nessus/OpenVAS.....	196
	NASL in Nessus and OpenVAS	196
	Nessus attack scripting language (NASL)	196
	Summary.....	199
	Endnotes	200
CHAPTER 8	Information gathering.....	201
	Information gathering for penetration testing.....	201
	Sources of information	202
	Patterns in information	202
	Metadata.....	203

What can we do with the information?.....	204
Talking to Google.....	205
Google hacking.....	205
Advanced operators	206
Automating Google discovery.....	207
Web automation with Perl.....	209
Pulling information from Web sites	209
Working with metadata	212
Finding metadata	212
Document metadata	214
Metadata in media files	214
Putting it all together.....	219
Summary.....	221
Endnotes	221
CHAPTER 9 Exploitation scripting	223
Building exploits with Python.....	223
Getting software	223
Setting up debugging.....	224
Causing our first crash.....	225
Using pattern_offset.....	228
Controlling EIP.....	230
Adding shellcode	232
Getting our shell	236
Creating Metasploit Exploits.....	237
Starting a template.....	237
Porting the exploit code.....	239
Executing the exploit.....	240
Exploiting PHP scripts	242
Remote File Inclusion	242
Command execution vulnerabilities	246
Cross-Site Scripting.....	248
What is XSS?.....	248
Exploiting XSS	249
Summary.....	253
CHAPTER 10 Post-exploitation scripting.....	255
Why post-exploitation is important	255
Windows shell commands.....	255
User management.....	256
Gathering network information.....	259
Windows network information gathering	260

Linux network information gathering.....	261
Scripting Metasploit Meterpreter	262
Getting a shell	262
Building a basic script.....	264
Executing the script.....	269
Database post-exploitation	270
What is SQL injection?.....	270
MySQL	271
SQL injection on Microsoft SQL Server	278
Summary.....	280
Appendix.....	283
Index	285