

# Nmap Network Exploration and Security Auditing Cookbook

*Third Edition*

Network discovery and security scanning  
at your fingertips

**Paulino Calderon**

**Packt>**

BIRMINGHAM—MUMBAI

# Nmap Network Exploration and Security Auditing Cookbook

## *Third Edition*

Copyright © 2021 Packt Publishing

*All rights reserved.* No part of this book may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, without the prior written permission of the publisher, except in the case of brief quotations embedded in critical articles or reviews.

Every effort has been made in the preparation of this book to ensure the accuracy of the information presented. However, the information contained in this book is sold without warranty, either express or implied. Neither the author(s), nor Packt Publishing or its dealers and distributors, will be held liable for any damages caused or alleged to have been caused directly or indirectly by this book.

Packt Publishing has endeavored to provide trademark information about all of the companies and products mentioned in this book by the appropriate use of capitals. However, Packt Publishing cannot guarantee the accuracy of this information.

**Group Product Manager:** Wilson D'souza

**Publishing Product Manager:** Rahul Nair

**Senior Editor:** Arun Nadar

**Content Development Editor:** Mrudgandha Kulkarni

**Technical Editor:** Shruthi Shetty

**Copy Editor:** Safis Editing

**Project Coordinator:** Ajesh Devavaram

**Proofreader:** Safis Editing

**Indexer:** Rekha Nair

**Production Designer:** Vijay Kamble

First published: November 2012

Second edition: May 2017

Third edition: August 2021

Production reference: 1200721

Published by Packt Publishing Ltd.

Livery Place

35 Livery Street

Birmingham

B3 2PB, UK.

ISBN 978-1-83864-935-7

[www.packt.com](http://www.packt.com)

*Special thanks to Fyodor for mentoring me back in the first GSoC program  
and to all the dev team, from whom I have learned a lot and who I now  
have the pleasure of knowing personally.*

*Omar and Yael, for always supporting me and not only being my hermanos  
but also my brothers.*

*Martha, for helping me be the best version of myself.*

*Nothing but love to all my friends. It is impossible to list all of you,  
but know that I appreciate all your love and support.*

# Contributors

## About the author

**Paulino Calderon** (@calderpwn on Twitter) is a published author and international speaker with over 10 years of professional experience in network and application security. He cofounded Websec in 2011, a consulting firm securing applications, networks, and digital assets operating in North America. When he isn't traveling to security conferences or consulting for Fortune 500 companies with Websec, he spends peaceful days enjoying the beach in Cozumel, Mexico. His contributions have reached millions of users through Nmap, Metasploit, OWASP Mobile Security Testing Guide (MSTG), OWASP Juice Shop, and OWASP IoT Goat.

*To my father, Dr. Paulino Calderon Medina, who taught me that our only limitations are the ones we set up in our minds, and my mother, Edith Pale Perez, who supported me unconditionally and always believed in me.*

## About the reviewer

**Nikhil Kumar** has more than 7 years of experience in cyber security with national and multinational companies. His core expertise and passions are information security, vulnerability assessment, penetration testing on network/infrastructure, and DAST/SAST/IAST on web and mobile applications.

He is an avid blogger and regular speaker on cyber-related topics at many colleges and private and government firms.

To reach his blogs or LinkedIn, visit the following sites:

<https://www.linkedin.com/in/nikhil-kumar-bb7a0590>

<https://blogs4all2017.blogspot.com>

<https://iot4all2017.blogspot.com>

He is a postgraduate in computer science and holds numerous cyber certifications, including Certified Ethical Hacker from the EC Council, ISO 27001 Lead Auditor from the IRCA, Certified 365 Security Administrator from Microsoft, Certified Azure Security Engineer Associate from Microsoft, Cyber Crime Intervention Officer from ISAC India, and Network Security Expert from FORTINET.

*I would like to thank my family, who have always motivated me to grow in my life and career. I would like to thank my friends and employers, who have always stood by me. My friends, Aphin Alexander, Rajdeep Gogoi, Prafull Kurekar, and Kanchan Jhangiani, have always been there for me. I would also like to thank Anubhav Kumar Lal and Ravali Vangala for giving me a reason to continue learning and growing.*

This page intentionally left blank

# Table of Contents

## Preface

---

## 1

### Nmap Fundamentals

---

Technical requirements	2	Using NSE scripts	
Building Nmap's source code	3	against a target host	22
Getting ready	3	How to do it...	23
How to do it...	4	How it works...	23
How it works...	5	There's more...	24
There's more...	5	Scanning random	
Finding online hosts	6	targets on the internet	28
How to do it...	6	How to do it...	28
How it works...	8	How it works...	29
There's more...	8	There's more...	29
Listing open ports on a target	10	Collecting signatures	
How to do it...	10	of web servers	30
How it works...	11	How to do it...	30
There's more...	12	How it works...	31
		There's more...	31
Fingerprinting OSes and		Scanning with Rainmap Lite	32
services running on a target	16	Getting ready	32
How to do it...	16	How to do it...	33
How it works...	18	How it works...	33
There's more...	19	There's more...	34

## 2

### Getting Familiar with Nmap's Family

---

<b>Monitoring servers remotely with Nmap and Ndiff</b>	<b>36</b>	How it works...	45
		There's more...	45
Getting ready	36		
How to do it...	36		
How it works...	38		
There's more...	39		
<b>Crafting ICMP echo replies with Nping</b>	<b>39</b>	Discovering systems with weak passwords with Ncrack	45
How to do it...	40	Getting ready	46
How it works...	40	How to do it...	46
There's more...	41	How it works...	46
		There's more...	47
<b>Managing multiple scanning profiles with Zenmap</b>	<b>41</b>	Using Ncat to diagnose a network client	48
How to do it...	41	How to do it...	48
How it works...	43	How it works...	50
There's more...	43	There is more...	50
<b>Running Lua scripts against a network connection with Ncat</b>	<b>44</b>	Defending against Nmap service detection scans	50
How to do it...	44	How to do it...	51
		How it works...	51
		There's more...	51

## 3

### Network Scanning

---

<b>Discovering hosts with TCP SYN ping scans</b>	<b>54</b>	There's more...	58
How to do it...	54		
How it works...	55	<b>Discovering hosts with UDP ping scans</b>	<b>58</b>
There's more...	56	How to do it...	59
		How it works...	59
<b>Discovering hosts with TCP ACK ping scans</b>	<b>57</b>	There's more...	59
How to do it...	57	Selecting ports in UDP ping scans	59
How it works...	58	<b>Discovering hosts with ICMP ping scans</b>	<b>60</b>



How to do it...	60	There's more...	71
How it works...	60		
There's more...	60		
<b>Discovering hosts with SCTP INIT ping scans</b>	<b>61</b>	<b>Discovering hosts with broadcast ping scans</b>	<b>72</b>
How to do it...	61	How to do it...	72
How it works...	62	How it works...	72
There's more...	63	There's more...	73
<b>Discovering hosts with IP protocol ping scans</b>	<b>63</b>	<b>Scanning IPv6 addresses</b>	<b>74</b>
How to do it...	63	How to do it...	75
How it works...	64	How it works...	75
There's more...	65	There's more...	75
<b>Discovering hosts with ARP ping scans</b>	<b>66</b>	<b>Spoofing the origin IP of a scan</b>	<b>77</b>
How to do it...	66	Getting ready	78
How it works...	67	How to do it...	78
There's more...	68	How it works...	79
<b>Discovering hosts with ARP ping scans</b>	<b>66</b>	There's more...	79
How to do it...	66		
How it works...	67	<b>Using port scanning for host discovery</b>	<b>80</b>
There's more...	68	How to do it...	80
<b>Performing advanced ping scans</b>	<b>70</b>	How it works...	81
How to do it...	70	There's more...	82
How it works...	71		

## 4

### Reconnaissance Tasks

<b>Performing IP address geolocation</b>	<b>84</b>	There's more...	89
Getting ready	85	<b>Obtaining traceroute geolocation information</b>	<b>90</b>
How to do it...	85	How to do it...	90
How it works...	86	How it works...	91
There's more...	86	There's more...	91
<b>Getting information from WHOIS records</b>	<b>87</b>	<b>Querying Shodan to obtain target information</b>	<b>92</b>
How to do it...	87	Getting ready	93
How it works...	89		

How to do it...	93	How it works...	97
How it works...	93	There's more...	97
There's more...	94		
<b>Collecting valid email accounts and IP addresses from web servers</b>	<b>94</b>	<b>Discovering hostnames by brute-forcing DNS records</b>	<b>98</b>
How to do it...	94	How to do it...	98
How it works...	95	How it works...	99
There's more...	95	There's more...	99
<b>Discovering hostnames pointing to the same IP address</b>	<b>96</b>	<b>Matching services with public vulnerability advisories and picking the low-hanging fruit</b>	<b>100</b>
How to do it...	96	How to do it...	100
		How it works...	101
		There's more...	102

## 5

### Scanning Web Servers

---

<b>Listing supported HTTP methods</b>	<b>104</b>	How it works...	112
How to do it...	104	There's more...	112
How it works...	105		
There's more...	105	<b>Detecting web application firewalls</b>	<b>114</b>
<b>Discovering interesting files and folders on web servers</b>	<b>107</b>	How to do it...	114
How to do it...	108	How it works...	115
How it works...	108	There's more...	115
There's more...	108	<b>Detecting possible XST vulnerabilities</b>	<b>117</b>
<b>Brute forcing HTTP authentication</b>	<b>109</b>	How to do it...	117
How to do it...	110	How it works...	118
How it works...	110	There's more...	118
There's more...	110	<b>Detecting XSS vulnerabilities</b>	<b>119</b>
<b>Brute forcing web applications</b>	<b>111</b>	How to do it...	119
How to do it...	112	How it works...	121
		There's more...	121

<b>Finding SQL injection vulnerabilities</b>	<b>122</b>	How to do it...	126
		How it works...	127
How to do it...	122	There's more...	127
How it works...	123		
There's more...	123	<b>Detecting exposed source code control systems</b>	<b>128</b>
<b>Finding web applications with default credentials</b>	<b>123</b>	How to do it...	128
How to do it...	123	How it works...	128
How it works...	124	There's more...	129
There's more...	125	<b>Auditing the strength of cipher suites in SSL servers</b>	<b>130</b>
<b>Detecting insecure cross-domain policies</b>	<b>126</b>	How to do it...	130
		How it works...	131
		There's more...	131

## 6

### Scanning Databases

<b>Listing MySQL databases</b>	<b>134</b>	<b>Finding root accounts with an empty password in MySQL servers</b>	<b>140</b>
How to do it...	135	How to do it...	140
How it works...	135	How it works...	140
There's more...	135	There's more...	141
<b>Listing MySQL users</b>	<b>136</b>	<b>Detecting insecure configurations in MySQL servers</b>	<b>141</b>
How to do it...	136	How to do it...	141
How it works...	137	How it works...	143
There's more...	137	There's more...	143
<b>Listing MySQL variables</b>	<b>137</b>	<b>Brute forcing Oracle passwords</b>	<b>144</b>
How to do it...	137	How to do it...	144
How it works...	138	How it works...	144
There's more...	138	There's more...	145
<b>Brute forcing MySQL passwords</b>	<b>139</b>		
How to do it...	139		
How it works...	139		
There's more...	140		

<b>Brute forcing Oracle SID names</b>	<b>145</b>	There's more...	157
How to do it...	145	<b>Retrieving MongoDB server information</b>	<b>157</b>
How it works...	146	How to do it...	157
There's more...	146	How it works...	158
<b>Retrieving information from MS SQL servers</b>	<b>146</b>	There's more...	158
How to do it...	146	<b>Detecting MongoDB instances with no authentication enabled</b>	<b>158</b>
How it works...	147	How to do it...	159
There's more...	147	How it works...	159
<b>Brute forcing MS SQL passwords</b>	<b>148</b>	There's more...	159
How to do it...	148	<b>Listing MongoDB databases</b>	<b>159</b>
How it works...	149	How to do it...	159
There's more...	149	How it works...	160
<b>Dumping password hashes of MS SQL servers</b>	<b>150</b>	There's more...	160
How to do it...	150	<b>Listing CouchDB databases</b>	<b>161</b>
How it works...	151	How to do it...	161
There's more...	151	How it works...	161
<b>Running commands through xp_cmdshell in MS SQL servers</b>	<b>152</b>	There's more...	161
How to do it...	152	<b>Retrieving CouchDB database statistics</b>	<b>162</b>
How it works...	153	How to do it...	162
There's more...	153	How it works...	163
<b>Finding system administrator accounts with empty passwords in MS SQL servers</b>	<b>154</b>	There's more...	163
How to do it...	154	<b>Detecting Cassandra databases with no authentication enabled</b>	<b>164</b>
How it works...	155	How to do it...	164
There's more...	155	How it works...	164
<b>Obtaining information from MS SQL servers with NTLM enabled</b>	<b>156</b>	There's more...	164
How to do it...	156	<b>Brute forcing Redis passwords</b>	<b>165</b>
How it works...	157	How to do it...	165
		How it works...	165
		There's more...	165

## 7

### Scanning Mail Servers

---

<b>Detecting SMTP open relays</b>	<b>168</b>	<b>There's more...</b>	<b>176</b>
How to do it...	168	<b>Retrieving the capabilities of an IMAP server</b>	<b>176</b>
How it works...	168	How to do it...	176
There's more...	169	How it works...	177
<b>Brute-forcing SMTP passwords</b>	<b>169</b>	There's more...	177
How to do it...	170	<b>Brute-forcing POP3 passwords</b>	<b>177</b>
How it works...	170	How to do it...	177
There's more...	170	How it works...	178
<b>Detecting suspicious SMTP servers</b>	<b>171</b>	There's more...	178
How to do it...	171	<b>Retrieving the capabilities of a POP3 server</b>	<b>178</b>
How it works...	171	How to do it...	179
There's more...	172	How it works...	179
<b>Enumerating SMTP usernames</b>	<b>173</b>	There's more...	179
How to do it...	173	<b>Retrieving information from SMTP servers with NTLM authentication</b>	<b>179</b>
How it works...	174	How to do it...	180
There's more...	174	How it works...	180
<b>Brute-forcing IMAP passwords</b>	<b>175</b>	There's more...	180
How to do it...	175		
How it works...	176		

## 8

### Scanning Windows Systems

---

<b>Obtaining system information from SMB</b>	<b>182</b>	<b>Detecting Windows clients with SMB signing disabled</b>	<b>184</b>
How to do it...	182	How to do it...	184
How it works...	183	How it works...	185
There's more...	184	There's more...	185

<b>Detecting IIS web servers that disclose Windows 8.3 names</b>	<b>186</b>	How it works...	199
		There's more...	199
How to do it...	186	<b>Finding domain controllers</b>	<b>200</b>
How it works...	187	How to do it...	200
There's more...	188	How it works...	200
		There's more...	201
<b>Detecting Windows hosts vulnerable to MS08-067 and MS17-010</b>	<b>188</b>	<b>Detecting the Shadow Brokers' DOUBLEPULSAR SMB implants</b>	<b>202</b>
How to do it...	189	How to do it...	202
How it works...	189	How it works...	203
There's more...	191	There's more...	204
<b>Retrieving the NetBIOS name and MAC address of a host</b>	<b>191</b>	<b>Listing supported SMB protocols</b>	<b>204</b>
How to do it...	192	How to do it...	204
How it works...	192	How it works...	204
There's more...	192	There's more...	205
<b>Enumerating user accounts of Windows targets</b>	<b>194</b>	<b>Detecting vulnerabilities using the SMB2/3 boot-time field</b>	<b>205</b>
How to do it...	194	How to do it...	205
How it works...	194	How it works...	206
There's more...	195	There's more...	206
<b>Enumerating shared folders</b>	<b>196</b>	<b>Detecting whether encryption is enforced in SMB servers</b>	<b>207</b>
How to do it...	196	How to do it...	207
How it works...	197	How it works...	207
There's more...	198	There's more...	207
<b>Enumerating SMB sessions</b>	<b>198</b>		
How to do it...	198		

## 9

### Scanning ICS/SCADA Systems

---

<b>Finding common ports used in ICS/SCADA systems</b>	<b>211</b>	There's more...	212
How to do it...	211	<b>Finding HMI systems</b>	<b>214</b>
How it works...	211	How to do it...	214

How it works...	215	There's more...	221
There's more...	215		
<b>Enumerating Siemens SIMATIC S7 PLCs</b>	<b>215</b>	<b>Enumerating Niagara Fox devices</b>	<b>221</b>
How to do it...	216	How to do it...	221
How it works...	216	How it works...	222
There's more...	216	There's more...	222
<b>Enumerating Modbus devices</b>	<b>216</b>	<b>Enumerating ProConOS devices</b>	<b>222</b>
How to do it...	217	How to do it...	223
How it works...	217	How it works...	223
There's more...	218	There's more...	223
<b>Enumerating BACnet devices</b>	<b>218</b>	<b>Enumerating Omrom PLC devices</b>	<b>223</b>
How to do it...	218	How to do it...	224
How it works...	219	How it works...	224
There's more...	219	There's more...	224
<b>Enumerating Ethernet/IP devices</b>	<b>220</b>	<b>Enumerating PCWorx devices</b>	<b>225</b>
How to do it...	220	How to do it...	225
How it works...	220	How it works...	225

## 10

### Scanning Mainframes

<b>Listing CICS transaction IDs in IBM mainframes</b>	<b>228</b>	<b>Brute-forcing z/OS JES NJE node names</b>	<b>230</b>
How to do it...	228	How to do it...	231
How it works...	228	How it works...	231
There's more...	229	There's more...	231
<b>Enumerating CICS user IDs for the CESL/CESN login screen</b>	<b>229</b>	<b>Enumerating z/OS TSO user IDs</b>	<b>232</b>
How to do it...	229	How to do it...	232
How it works...	230	How it works...	232
There's more...	230	There's more...	233

<b>Brute-forcing z/OS TSO accounts</b>	<b>233</b>	<b>Listing VTAM application screens</b>	<b>235</b>
How to do it...	233	How to do it...	235
How it works...	234	How it works...	235
There's more...	234	There's more...	236

# 11

## Optimizing Scans

---

<b>Skipping phases to speed up scans</b>	<b>238</b>	<b>parameters</b>	<b>249</b>
How to do it...	238	How to do it...	249
How it works...	239	How it works...	250
There's more...	244	There's more...	251
<b>Selecting the correct timing template</b>	<b>244</b>	<b>Adjusting scan groups</b>	<b>251</b>
How to do it...	245	How to do it...	251
How it works...	245	There's more...	252
There's more...	247	<b>Distributing a scan among several clients using dnmap</b>	<b>252</b>
<b>Adjusting timing parameters</b>	<b>247</b>	Getting ready	253
How to do it...	247	How to do it...	253
There's more...	248	How it works...	254
		There's more...	255

Adjusting performance

# 12

## Generating Scan Reports

---

<b>Saving scan results in a normal format</b>	<b>258</b>	How it works...	261
How to do it...	258	There's more...	262
How it works...	259	<b>Saving scan results to a SQLite database</b>	<b>263</b>
There's more...	259	Getting ready	263
<b>Saving scan results in an XML format</b>	<b>260</b>	How to do it...	263
How to do it...	260	How it works...	264
		There's more...	265



<b>Saving scan results in a greppable format</b>	<b>266</b>	How it works...	273
		There's more...	273
How to do it...	266	<b>Generating PDF reports with fop</b>	<b>273</b>
How it works...	267	Getting ready	274
There's more...	268	How to do it...	274
<b>Generating a network topology graph with Zenmap</b>	<b>268</b>	How it works...	274
How to do it...	268	There's more...	274
How it works...	269	<b>Saving NSE reports in Elasticsearch</b>	<b>275</b>
There's more...	270	Getting ready	275
<b>Generating HTML scan reports</b>	<b>270</b>	How to do it...	275
Getting ready	270	How it works...	277
How to do it...	270	There's more...	277
How it works...	271	<b>Visualizing Nmap scan results with IVRE</b>	<b>277</b>
There's more...	272	Getting ready	278
<b>Reporting vulnerability checks</b>	<b>272</b>	How to do it...	279
How to do it...	272	How it works...	280
		There's more...	281

## 13

### Writing Your Own NSE Scripts

<b>Making HTTP requests to identify vulnerable Supermicro IPMI/BMC controllers</b>	<b>286</b>	<b>Generating vulnerability reports in NSE scripts</b>	<b>296</b>
How to do it...	286	How to do it...	296
How it works...	287	How it works...	297
There's more...	289	There's more...	299
<b>Sending UDP payloads using NSE sockets</b>	<b>291</b>	<b>Exploiting an SMB vulnerability</b>	<b>300</b>
How to do it...	291	How to do it...	300
How it works...	293	How it works...	305
There's more...	294	There's more...	306
		<b>Writing brute-force password auditing scripts</b>	<b>306</b>

---

How to do it...	306	Writing a new NSE	
How it works...	310	library in Lua	321
There's more...	311	How to do it...	322
		How it works...	322
<b>Crawling web servers</b>		There's more...	323
<b>to detect vulnerabilities</b>	<b>311</b>		
How to do it...	312	<b>Writing a new NSE library</b>	
How it works...	317	<b>in C/C++</b>	<b>323</b>
There's more...	318	How to do it...	323
		How it works...	325
<b>Working with NSE threads,</b>		There's more...	326
<b>condition variables, and</b>			
<b>mutexes in NSE</b>	<b>319</b>	<b>Getting your scripts ready</b>	
How to do it...	319	<b>for submission</b>	<b>326</b>
How it works...	320	How to do it...	326
There's more...	321	How it works...	327
		There's more...	327

# 14

## Exploiting Vulnerabilities with the Nmap Scripting Engine

---

<b>Generating vulnerability</b>		<b>Crawling web servers</b>	
<b>reports in NSE scripts</b>	<b>330</b>	<b>to detect vulnerabilities</b>	<b>340</b>
How to do it...	330	How to do it...	340
How it works...	332	How it works...	345
There's more...	333	There's more...	347
<b>Writing brute-force</b>		<b>Exploiting SMB vulnerabilities</b>	<b>348</b>
<b>password auditing scripts</b>	<b>334</b>	How to do it...	348
How to do it...	335	How it works...	352
How it works...	338	There's more...	353
There's more...	339		

# Appendix A

## - HTTP, HTTP Pipelining, and Web Crawling Configuration Options

---

HTTP user agent	356	Configuring the NSE	
HTTP pipelining	356	httpspider library	356

## Appendix B

### – Brute-Force Password Auditing Options

---

Brute modes	360
-------------	-----

## Appendix C

### – NSE Debugging

---

Debugging NSE scripts	363	Exception handling	363
-----------------------	-----	--------------------	-----

## Appendix D

### – Additional Output Options

---

Saving output in all formats	365	Including the reason	
Appending Nmap output logs	366	for a port or host state	366
Including debugging		OS detection in	
information in output logs	366	verbose mode	367

## Appendix E

### – Introduction to Lua

---

<b>Flow control structures</b>	<b>369</b>	String repetition	377
Conditional statements – if,		String length	377
then, elseif	369	Formatting strings	377
Loops – while	370	Splitting and joining strings	377
Loops – repeat	370	<b>Common data structures</b>	<b>378</b>
Loops – for	370	Tables	378
<b>Data types</b>	<b>372</b>	Arrays	379
<b>String handling</b>	<b>372</b>	Linked lists	380
Character classes	372	Sets	380
Magic characters	373	Queues	381
Patterns	374	Custom data structures	382
Captures	375	<b>I/O operations</b>	<b>382</b>
Repetition operators	375	Modes	382
Concatenation	375	Opening a file	382
Finding substrings	376		

Reading a file	383	Arithmetic metamethods	387
Writing a file	383	Relational metamethods	387
Closing a file	383		
<b>Coroutines</b>	<b>384</b>	<b>Things to remember</b>	
Creating a coroutine	384	<b>when working with Lua</b>	<b>388</b>
Executing a coroutine	384	Comments	388
Determining the current coroutine	385	Dummy assignments	388
Getting the status of a coroutine	385	Indexes	388
Yielding a coroutine	386	Semantics	389
		Coercion	389
<b>Metatables</b>	<b>387</b>	Safe language	389
		Booleans	390

# Appendix F

## - References and Additional Reading

---

### Other Books You May Enjoy

---

### Index

---