

Hack The World with OSINT

Chris Kubecka

This is an excerpt of the book
ISBN-13: 978-0995687592
ISBN-10: 0995687595

Hack the World with OSINT

Published by Chris Kubecka & HypaSec

HypaSec is a registered entity in the Netherlands Commercial Registration:
63945517

Printed in the Netherlands

First Printing

ISBN: 978-0-9956875-9-2

Publisher: HypaSec, Netherlands

Graphics: Chris Kubecka

Technical Editor: E. Martinez II

Indexer: Chris Kubecka

The information contained in the book is distributed “as-is”. Although every effort has been taken for accuracy. Web sites, configurations, ISPs and other variables can affect results. The author assumes no liability for any errors or omissions, or any usage of the information contained herein.

The publisher, author, editor or contributors re not, to the fullest extent of the law under any assumption of liability for any injury and/or damage to persons or property as a matter of any products including liability, negligence or any use or operation of the information contained therein.

All rights reserved. No part of this work should or may be reproduced or transmitted without written permission. Author, publisher and editors are not responsible for any criminal misuse of the information contained in this book. Remember: Make memes not malware.

British Library Cataloguing-in-Publication Data

This book is written in British International English not US English

Application Submitted

Copyright © 2019 Chris Kubecka

All rights reserved.

Why a IT/IOT/ICS hacking book?

Nice people don't connect exploitable systems to the internet.

- Random Twitter User

Censys has been an invaluable tool in my OSINT toolbox. As such, I chose to share the knowledge, prompting me to write down the ins and outs of how to use the free tool with examples and case studies. Censys was very useful in the creation of a penetration course I wrote and taught at BSides Las Vegas in 2017. Although I love Shodan, Censys pulled me in with a different type of searching and discovery of interesting or weak systems. Shodan, becoming more and more my device OSINT side chick so to speak.



Table of Contents

| | |
|---|-------------|
| FORWARD | VI |
| LIST OF FIGURES..... | XVI |
| LIST OF TABLES | XXIV |
| INTRODUCTION..... | 1 |
| 0.1 Introduction | 1 |
| 0.2 Target Audience..... | 1 |
| 0.3 Conventions | 1 |
| 0.4 Other Resources..... | 1 |
| 0.5 Request for Comments..... | 2 |
| 0.6 Acknowledgements | 2 |
| 0.7 Technology and tools to create the book | 2 |
| 0.8 Protocol References | 3 |
| 0.9 Organization of the book | 4 |
| 1 WHAT IS CENSYS..... | 7 |
| 1.1 Introduction to Censys | 7 |
| 1.2 Censys Protocols | 9 |
| 1.3 Censys Query Syntax..... | 10 |
| 1.4 Censys Web Query examples | 13 |
| 2 HOW TO SETUP YOUR OSINT LAB..... | 15 |

| | |
|---|-----------|
| 2.1 Lab requirements | 16 |
| 2.2 OSINT Kali Distribution Information..... | 16 |
| 2.3 OSINT Kali64 in WM Player/Workstation/Fusion 14 | 17 |
| 2.4 OSINT Kali64 OVF in VM Player/Workstation 14 | 17 |
| 2.4 Installing and updating tools..... | 18 |
| 2.5 Installing Maltego on Windows..... | 18 |
| 2.6 Email Account Helper Tool 10-Minute Email..... | 19 |
| 2.7 Obtaining API Keys..... | 19 |
| 2.8 Configuring Maltego and API Keys..... | 20 |
| 3 REMOTE MANAGEMENT | 23 |
| 3.1 Introduction to Censys Remote Management Protocols..... | 23 |
| 3.2 Exploring FTP services | 25 |
| 3.3 Finding FTP servers busy status | 27 |
| 3.4 Finding FTP servers with user already logged in..... | 28 |
| 3.6 Finding FTP ThinServer..... | 29 |
| 3.7 Finding FTP MikroTik..... | 30 |
| 3.8 Finding FTP syntax error | 32 |
| 3.10 Exploring SSH services..... | 33 |
| 3.11 Survey of SSH server metadata | 35 |
| 3.12 Exploring Telnet services..... | 36 |
| 3.13 Discovering vulnerable Telnet service banners and settings | 38 |
| CASE STUDY: Trump Towers Toronto..... | 40 |

| | |
|---|-----------|
| 4 EMAIL | 43 |
| 4.1 Introduction to Censys Email Protocols | 43 |
| 4.2 Exploring SMTP | 44 |
| 4.3 Discovering SMTP Metadata..... | 51 |
| 4.4 Discovering SMTP Start TLS configuration | 54 |
| 4.4.1 SSL-Tools.net | 54 |
| 4.4.2 Netcraft.com..... | 55 |
| 4.5 Systems with TLS failures caused by misconfigurations | 56 |
| 4.6 TLS not available email systems..... | 57 |
| 4.7 Email servers with insufficient disk space or network congestion | 58 |
| 4.8 Censys search results for range of SMTP extended codes | 59 |
| CASE STUDY: Strip Start-TLS and EU GDPR..... | 60 |
| 5 HTTP & HTTPS | 69 |
| 5.1 Introduction to Censys HTTP/S Protocols | 69 |
| 5.2 Exploring HTTP..... | 70 |
| 5.3 Find H?cked webpages..... | 78 |
| 5.4 Find Teapots..... | 79 |
| 5.4 Exploring HTTPS..... | 79 |
| 5.5 Finding IIS server usage in the Top Million websites | 81 |
| 5.5 Find Heartbleed vulnerable systems in the Ukraine..... | 82 |
| 5.6 HTTPS Tags..... | 82 |
| 5.7 Finding Hacked Let's Encrypt certificates..... | 86 |
| 5.8 Find HTTPS using a known private key | 87 |

| | |
|--|------------|
| 5.9 Find weak encryption cipher protocols used by HTTP/S & SSH | 88 |
| 5.11 Discovering expired NSA.gov certificates | 90 |
| 5.12 Discovering weak Kingdom of Saudi Arabia MOFA servers | 92 |
| CASE STUDY: Responsible disclosure to the NSA..... | 94 |
| 6 DORKING WITH CENSYS..... | 97 |
| 6.1 Introduction to Censys Dorking | 98 |
| 6.2 Converting Dorks into Censys Dorks | 98 |
| 6.3 Discovering Porn websites | 99 |
| 6.4 Find Websites with Shells..... | 101 |
| 6.5 Discover WannaCry infected systems..... | 102 |
| 6.6 Find Power Meters..... | 104 |
| 6.7 Find Procon LED Modbus controllers..... | 105 |
| 6.8 Find Samsung Web Viewer for DVR and Security Cameras | 106 |
| 6.9 Dorking to find Anonymous FTP login services | 107 |
| 6.7 Using Dorking to discover Siemens systems..... | 108 |
| 6.10 Find weak random number generator java.util.Random | 108 |
| CASE STUDY: Making Ministers WannaCry..... | 111 |
| 7 ICS & SCADA..... | 117 |
| 7.1 Introduction to Censys ICS & SCADA Protocols | 117 |
| 7.3 Exploring Modbus | 119 |
| 7.4 Exploring DNP3..... | 123 |
| 7.5 Exploring S7 | 124 |
| 7.5 General Siemens S7 Censys search | 124 |

| | |
|--|------------|
| 7.6 General Siemens systems Censys search using certificates | 126 |
| 7.6 Exploring BACnet..... | 128 |
| 7.7 Find Siemens BACnet devices with web services | 129 |
| 7.8 Find OpenADR Management Interfaces..... | 129 |
| CASE STUDY: Critical Infrastructure love ♥ | 132 |
| 8 BUILDING CONTROL SYSTEMS & IOT..... | 135 |
| 8.1 Introduction to Censys Building Control Systems & IoT | 136 |
| 8.3 Find Fire Alarms | 137 |
| 8.5 Find Cinemas | 140 |
| 8.6 Find Solar Panel Systems | 140 |
| 8.7 Find Digital Video Recorders | 142 |
| 8.8 Find Miele washing machines & home appliances | 143 |
| 8.9 Find IoT Car Washing machines | 146 |
| 8.10 How to Hack a Smart Home..... | 147 |
| 9 OTHER PROTOCOLS..... | 149 |
| 9.1 Other Censys Protocols | 150 |
| 9.2 Exploring DNS | 150 |
| 9.3 Survey Chinese DNS systems | 152 |
| 9.4 Exploring SMB | 154 |
| 9.5 Discover SMB version 1 systems..... | 155 |
| 10 TAGS..... | 157 |
| 10.1 ZMap Project Tags | 157 |

| | |
|--|------------|
| 10.2 Alarm systems | 163 |
| 10.3 Discovering Known -private-keys | 166 |
| 10.3 Heartbleed vulnerable systems | 171 |
| 10.4 Find Russian FTP servers with databases | 173 |
| CASE STUDY: Riding the Printer Pwnie..... | 174 |
| 11 CENSYS REPORTS | 185 |
| 11.1 Censys Reporting..... | 185 |
| 11.2 Find Vulnerable IIS servers in an unconventional way | 186 |
| 11.3 SMTP Ciphers | 188 |
| 11.4 Build a report for the Top 10 Modbus Web Servers..... | 189 |
| 11.5 Discovering vulnerable SSH servers..... | 191 |
| 11.6 What is running in Iran | 193 |
| 11.7 North Korea has the internet? | 195 |
| 11.8 Discovering SMTP Start TLS Configurations | 199 |
| 11.9 Discovering SMTP servers with Command implementation errors..... | 203 |
| 11.10 Discovering DNS Open Resolvers..... | 209 |
| 11.11 Discovering vulnerable Telnet service banners and settings | 217 |
| 11.12 Find hacked websites..... | 219 |
| 12 CENSYS WITH TOOLS | 227 |
| 12.1 Censys API with tools..... | 227 |
| 12.2 Metasploit..... | 228 |
| 12.3 Metasploit Censys FBI certificate search..... | 229 |

| | |
|--|------------|
| 12.4 Recon NG | 230 |
| 12.4.1 Configure Recon-NG | 230 |
| 12.4.2 Import Additional Censys modules into Recon NG..... | 234 |
| 12.5 Spiderfoot..... | 234 |
| | |
| 13 REST API | 235 |
| | |
| 13.1 The Censys API | 236 |
| | |
| 13.2 Search | 236 |
| | |
| 13.3 View | 237 |
| | |
| 13.4 Create Report..... | 238 |
| | |
| 13.5 Report Query | 239 |
| 13.5.1 Get Job Status..... | 239 |
| 13.5.2 Get Job Results | 240 |
| 13.5.3 Get Series | 240 |
| 13.6.4 Get Series Details..... | 241 |
| | |
| 13.6 Report Export | 241 |
| 13.6.1 Start Export Job | 241 |
| 13.6.2 Export Get Job Status..... | 242 |
| | |
| 13.7 Data | 242 |
| 13.7.1 Data Get Series..... | 242 |
| 13.7.2 Data View Series | 243 |
| 13.7.3 Data View Results..... | 243 |
| | |
| RESOURCES | 245 |
| Further reading..... | 246 |
| | |
| BIBLIOGRAPHY | 283 |
| | |
| INDEX | 289 |
| | |
| ABOUT THE AUTHOR | 291 |

Where was that figure?

| | |
|--|----|
| Figure 1 10-Minute temporary email account | 19 |
| Figure 2 Maltego Transform options..... | 20 |
| Figure 3 Maltego Transform seed settings..... | 21 |
| Figure 4 FTP Code 120 Search..... | 27 |
| Figure 5 Details of a system with FTP Code 230 | 28 |
| Figure 6 Details of a system with FTP Code 220 | 29 |
| Figure 7 Details of a system with FTP Code 332 | 30 |
| Figure 8 Details of a system with FTP Code 452 | 31 |
| Figure 9 Details of a system with FTP Code 500 | 32 |
| Figure 10 Censys OVH systems possibly hacked | 35 |
| Figure 11 Censys 1st three OVH FR Hacked results..... | 36 |
| Figure 12 Censys search of Telnet excluding encryption options | 39 |
| Figure 13 Trump Towers Toronto FileZilla beta version 3/2018 | 40 |
| Figure 14 Censys SMTP protocol Metadata | 52 |
| Figure 15 SSL-Tools.net Start TLS Configuration Tester | 55 |
| Figure 16 Netcraft.com What's that site running? domain tool | 55 |
| Figure 17 Netcraft.com Results for DOD.gov | 56 |
| Figure 18 Summary of DOD.gov SPF & DMARC settings via Netcraft.com..... | 56 |
| Figure 19 Censys SMTP Unable to start code..... | 57 |
| Figure 20 Censys SMTP TLS not available code | 58 |
| Figure 21 Censys SMTP Insufficient disk space | 59 |
| Figure 22 Censys web search using a range of SMTP extended codes | 59 |
| Figure 23 Highlighted list of NSA subdomains listing Prism July 2017 | 61 |
| Figure 24 Censys.io Strip Start-TLS global scan 10 November 2017 | 62 |
| Figure 25 Censys.io Strip Start-TLS top country report 10 November 2017 | 63 |
| Figure 26 Censys.io Strip Start-TLS European scan 10 November | |

| | |
|---|----|
| 2017 | 63 |
| Figure 27 Censys.io Strip Start-TLS top European country report 10 November 2017..... | 64 |
| Figure 28 Censys.io Strip Start-TLS top UK network providers report 10 November 2017 | 64 |
| Figure 29 Censys.io Strip Start TLS UK BT owned systems 15 November 2017..... | 65 |
| Figure 30 Censys.io Strip Start-TLS Thailand government telecommunications systems 15 November 2017 | 65 |
| Figure 31 Censys.io Strip Start-TLS top NL network providers report 10 November 2017 | 66 |
| Figure 32 Censys.io Strip Start TLS NL KPN Static owned systems 15 November 2017 | 66 |
| Figure 33 80.http.get.status_code: 495..... | 78 |
| Figure 34 Censys web search “H?cked” using ? to replace a letter.... | 79 |
| Figure 35 Censys web search “HTTP 418 I'm a teapot” | 79 |
| Figure 36 Censys Ukrainian Heartbleed vulnerable search result..... | 82 |
| Figure 37 Censys Hacked certificate search | 86 |
| Figure 38 (Hacked) AND parsed.issuer.organization.raw: "Let's Encrypt"..... | 87 |
| Figure 39 Censys HTTPS & known private keys..... | 87 |
| Figure 40 Censys weak encryption protocols search | 88 |
| Figure 41 Censys weak encryption protocols search Country Breakdown | 89 |
| Figure 42 Censys search results weak Chinese encryption..... | 89 |
| Figure 43 NSA.gov certificates (nsa.gov) AND tags.raw: "expired". | 90 |
| Figure 44 Censys NSA.gov certificate names Metadata | 90 |
| Figure 45 Censys Metadata Country Breakdown of certificates with alternate DNS names containing NSA.gov | 91 |
| Figure 46 Censys Metadata Network Breakdown of certificates with alternate DNS names containing NSA.gov | 91 |
| Figure 47 Censys Metadata Common Tags of certificates with alternate DNS names containing NSA.gov | 92 |
| Figure 48 Censys KSA MOFA intelligence services search results ... | 92 |
| Figure 49 Weak Saudi intelligence services email server | 93 |

| | |
|--|-----|
| Figure 50 Crypto Log Jam Check positive vulnerability | 94 |
| Figure 51 Honest NSA Meme from LibertyManiacs.com | 95 |
| Figure 52 Censys keyword Porn Dorking..... | 99 |
| Figure 53 Censys HTTPS certificate DNS for PornHub.com | 99 |
| Figure 54 Censys web search result for PornHub.com DNS names in certificates | 100 |
| Figure 55 Censys web search result *.PornHub.com SSH services. | 100 |
| Figure 56 Censys PornHub.com associated system SSH details | 101 |
| Figure 57 CVEDetails result for OpenSSH version 7.4 vulnerabilities | 101 |
| Figure 58 Censys search for reverse shells..... | 102 |
| <i>Figure 59 Censys search results for WannaCry infected hosts using Dorking..</i> | 103 |
| Figure 60 Example Censys HTTP Body field WannaCry infected host | 103 |
| Figure 61 Censys Meternet power meter IoT login..... | 104 |
| Figure 62 Meternet Pro system..... | 104 |
| Figure 63 Meternet Pro access to picture files listed in HTML source code no authentication..... | 105 |
| Figure 64 Polish to English translated website for F&F Meternet Pro | 105 |
| Figure 65 80 HTTP Modbus to BACnet Configurator | 106 |
| Figure 66 Censys FTP anonymous FTP search | 108 |
| Figure 67 Siemens Simatic link in HTML..... | 108 |
| Figure 68 Censys weak java.util.Random search..... | 109 |
| Figure 69 Censys 80/HTTP system details with java.util.Random.. | 110 |
| Figure 70 Censys html body using java.util.Random | 110 |
| Figure 71 Weak Chinese encryption backdoors..... | 111 |
| Figure 72 Weak water infrastructure..... | 112 |
| Figure 73 Shodan Modbus map exposed in the UK..... | 112 |
| Figure 74 Exposed electric infrastructure | 113 |
| Figure 75 Exposed BlackEnergy vulnerable Siemens system | 113 |
| Figure 76 WanaCry vulnerable systems still unpatched..... | 114 |
| Figure 77 ABN AMRO bank part Dutch gov owned hacked with a RAT | 114 |
| Figure 78 S7 Censys metadata results | 125 |

| | |
|--|-----|
| Figure 79 Censys S7 dorking for Siemens | 126 |
| Figure 80 Censys certificate Siemens s7 with OR | 126 |
| Figure 81 Censys certificate tags for Siemens | 127 |
| Figure 82 Censys Siemens untrusted certificates | 128 |
| Figure 83 Hydroelectric OpenADR exposed to the internet | 131 |
| Figure 84 Censys Tag Fire Alarm web search result | 138 |
| Figure 85 Censys Tag Fire Alarm web search result detail | 138 |
| Figure 86 Censys web search fire alarm details page | 139 |
| Figure 87 Fire alarm basic information details..... | 139 |
| Figure 88 Censys certificate OU containing Notifier | 139 |
| Figure 89 Censys certificate OU containing Notifier metadata | 140 |
| Figure 90 Censys web cinema search | 140 |
| Figure 91 Censys cinema country breakdown | 140 |
| Figure 92 Censys solar panel device type search | 141 |
| Figure 93 Censys solar panel device type Tags | 142 |
| Figure 94 Censys Web Search for DVR Components Download... | 143 |
| Figure 95 Censys Miele@Home detail..... | 144 |
| Figure 96 Censys Miele gateway HTTP Body details | 145 |
| Figure 97 Miele gateway home screen..... | 145 |
| Figure 98 Miele Gateway Login xgw3000 is hardcoded as the user name | 146 |
| Figure 99 Unitec IoT automated car washers | 146 |
| Figure 100 Unitec web server details..... | 147 |
| Figure 101 Lexone Smart House Login | 148 |
| Figure 102 AIBot Motivational statement..... | 149 |
| Figure 103 General DNS Censys web search | 153 |
| Figure 104 Censys DNS China Metadata | 153 |
| Figure 105 Chinese DNS Answers A Common Tags Metadata | 154 |
| Figure 106 Censys search SMB v1systems | 156 |
| Figure 107 SMB version 1 support is True | 156 |
| Figure 108 Censys Alarm System Metadata overview | 164 |
| Figure 109 Censys Alarm System Country Breakdown..... | 165 |
| Figure 110 Censys Alarm System Common Tags | 166 |
| Figure 111 Censys.io scan known-public-key tag results 15 November 15, 2017..... | 166 |

| | |
|---|-----|
| Figure 112 Censys.io scan known-public-key tag Protocol Summary | 167 |
| Figure 113 Censys.io scan known-public-key tag and DSL/Cable Modem | 168 |
| Figure 114 Censys.io scan known-public-key tag and DSL/Cable Modem Metadata | 168 |
| Figure 115 Censys.io scan known-public-key tag and DSL/Cable Modem Country Breakdown | 169 |
| Figure 116 Censys.io scan known-public-key tag and DSL/Cable Modem Common Tags..... | 170 |
| Figure 117 Censys Heartbleed vulnerable search results | 171 |
| Figure 118 Censys Heartbleed vulnerable Country Breakdown..... | 171 |
| Figure 119 Censys Heartbleed vulnerable Network Breakdown..... | 172 |
| Figure 120 Censys Heartbleed vulnerable Common Tags | 172 |
| Figure 121 Censys Russian FTP database servers | 173 |
| Figure 122 Printers, a perfect attack pivot on your network | 174 |
| Figure 123 Censys Dork to find Brother printers with no password configured..... | 175 |
| Figure 124 Over three thousand printers with model :) | 176 |
| Figure 125 Even tells you the status, sweet | 177 |
| Figure 126 Abundance of compatible printers with admin tool..... | 177 |
| Figure 127 Think of all the evil things you can do | 178 |
| Figure 128 You can make your own PRN file | 178 |
| Figure 129 Parameter = loginurl happy hacker joy joy | 179 |
| Figure 130 Input | 179 |
| Figure 131 Accepts field submission | 180 |
| Figure 132 You can call me Mr. <script>alert(1)</script> ;-) | 180 |
| Figure 133 Yummy | 181 |
| Figure 134 Hope one of these isn't exposing something important, like a hospital network..... | 182 |
| Figure 135 CVE Details.com Microsoft IIS Vulnerabilities..... | 186 |
| Figure 136 Censys Report Top Ten 80.http.get.headers.server graph | 187 |
| Figure 137 Censys report result for email in IIS banner..... | 188 |
| Figure 138 Chinese vulnerable modems | 189 |

| | |
|---|-----|
| Figure 139 Censys Top 10 web servers graph on Modbus devices | 190 |
| Figure 140 CVEDetails listing IIS 7.5 vulnerabilities | 191 |
| Figure 141 Censys Top Ten report 22.ssh.v2.banner.version | 192 |
| Figure 142 Metasploit SSH version 1.5 exploit module | 193 |
| Figure 143 Iranian Country Metadata | 194 |
| Figure 144 Major networks in Iran | 194 |
| Figure 145 Censys Iran metadata report Common Tags | 195 |
| Figure 146 Censys search results for location.country North Korea | 196 |
| Figure 147 Censys Metadata report North Korea Network Breakdown | 196 |
| Figure 148 Censys STAR Ryugyong-dong KP network DPRK search results | 197 |
| Figure 149 Censys mail.silibank.net.kp details | 198 |
| Figure 150 Censys mail.silibank.net.kp Whois details..... | 199 |
| Figure 151 Censys SMTP Start TLS code 502 5.5.1 error code..... | 203 |
| Figure 152 Censys SMTP Start TLS code 552 5.5.1 Metadata.manufacturer.raw graph | 204 |
| Figure 153 Censys DNS Open Resolver is False | 209 |
| Figure 154 Censys report DNS open resolvers vs.. non November 2017 | 210 |
| Figure 155 DNS Open Resolver Metadata..... | 210 |
| Figure 156 Censys report DNS open resolvers vs.. non March 2018 | 211 |
| Figure 157 Censys DNS Lookup Errors on a DOD DNS server...212 | |
| Figure 158 Censys DNS Open Resolver search results..... | 215 |
| Figure 159 Censys Bulgarian DNS Open Resolver example | 216 |
| Figure 160 Censys DNS Open Resolver Country Breakdown | 217 |
| Figure 161 Censys Top Ten report telnet banners..... | 218 |
| Figure 162 Censys.io (hacked) AND metadata.os: "Windows" search result..... | 220 |
| Figure 163 Censys general keyword "hacked" search AND operating system..... | 221 |
| Figure 164 Metasploit setting Censys API information | 229 |
| Figure 165 Metasploit showing Censys module options..... | 229 |

| | |
|--|-----|
| Figure 166 How to open Recon -NG..... | 231 |
| Figure 167 Recon-NG loaded after red errors | 231 |
| Figure 168 Additional Censys Recon NG modules | 234 |
| Figure 169 HTTP Honeywell certificate organisation | 237 |

Where was that table?

| | |
|--|----|
| Table 1 Zmap and Censys.io protocols..... | 3 |
| Table 2 Common Social Engineering competition points/flags | 8 |
| Table 3 Censys.io and ZMap Protocols | 9 |
| Table 4 Censys.io query syntax examples | 11 |
| Table 5 Censys Example Web Search Queries | 13 |
| Table 6 Tool URL reference..... | 21 |
| Table 7 Censys Remote management protocols..... | 24 |
| Table 8 Censys Remote management tags..... | 24 |
| Table 9 Important FTP Censys fields & examples..... | 25 |
| Table 10 FTP 1st digit server return codes..... | 25 |
| Table 11 FTP 2nd digit codes..... | 26 |
| Table 12 FTP 100 Series Codes | 26 |
| Table 13 FTP 200 Series Codes | 27 |
| Table 14 FTP 300 Series Codes | 29 |
| Table 15 FTP 400 Series Codes | 30 |
| Table 16 FTP 500 Series Codes | 31 |
| Table 17 FTP 600 Series Codes | 32 |
| Table 18 FTP 10000 Series Codes | 32 |
| Table 19 Important SSH Censys fields & examples..... | 33 |
| Table 20 Important Censys Telnet field examples | 37 |
| Table 21 Telnet fields..... | 37 |
| Table 22 Censys 15/11/17 Host Report POP3/S & IMAP/S | 44 |
| Table 23 Important Censys SMTP fields & examples | 45 |
| Table 24 SMTP Protocol Codes | 45 |
| Table 25 SMTP Extended codes ESMTP | 48 |
| Table 26 Censys SMTP Metadata Country Breakdown | 52 |
| Table 27 Censys SMTP Metadata Network Breakdown | 53 |
| Table 28 Censys SMTP Metadata Common Tags..... | 54 |
| Table 29 Censys 15/11/17 Host Report HTTP and HTTPS .. | 70 |

| | |
|--|-----|
| Table 30 Important HTTP Censys fields & examples..... | 71 |
| Table 31 HTTP Information Codes..... | 72 |
| Table 32 HTTP Success Codes..... | 72 |
| Table 33 HTTP Redirection Codes..... | 73 |
| Table 34 HTTP Client Error Codes..... | 73 |
| Table 35 HTTP Server Error Codes | 75 |
| Table 36 HTTP Unofficial Codes..... | 76 |
| Table 37 Microsoft Internet Information Services HTTP Codes | 77 |
| Table 38 NGINX HTTP Error Codes..... | 77 |
| Table 39 HTTP 500 error codes..... | 78 |
| Table 40 Important HTTPS Censys fields & examples | 80 |
| Table 41 Censys HTTPS HTTP certificate Tags | 82 |
| Table 42 Censys HTTPS certificate fields | 83 |
| Table 43 Censys HTTPS Parsed certificate fields | 85 |
| Table 44 Censys 15/11/17 Host Report ICS and SCADA protocols..... | 118 |
| Table 45 ICS and SCADA Censys Tags | 118 |
| Table 46 Important MODBUS Censys fields & examples | 120 |
| Table 47 Basic MODBUS function names and codes..... | 120 |
| Table 48 MODBUS Exception codes..... | 121 |
| Table 49 ZMap Modbus object mapping | 122 |
| Table 50 Important DNP3 Censys fields | 123 |
| Table 51 Important Siemens S7 Censys fields & examples | 124 |
| Table 52 Important BACnet Censys fields & examples..... | 128 |
| Table 53 Censys 15/11/17 Host Report Building Control and IoT protocols..... | 136 |
| Table 54 Censys 15/11/17 Host Report other protocols scanned | 150 |
| Table 55 Censys Important DNS fields & examples | 150 |
| Table 56 Censys DNS Additionals fields..... | 151 |
| Table 57 Censys DNS Answers fields..... | 151 |
| Table 58 Censys DNS Authorities fields | 151 |
| Table 59 Censys DNS Questions fields..... | 152 |
| Table 60 Censys DNS Lookup fields..... | 152 |

| | |
|---|-----|
| Table 61 Important SMB Censys fields & examples..... | 155 |
| Table 62 Censys.io Tags | 158 |
| Table 63 Censys Report Top Ten 80.http.get.headers.server.187 | |
| Table 64 Censys Top 10 web server Host Report on Modbus devices..... | 190 |
| Table 65 Censys Top 10 report 22.ssh.v2.banner.version..... | 192 |
| Table 66 Censys SMTP Start TLS Configuration..... | 200 |
| Table 67 Censys SMTP Start TLS code 552 5.5.1 | |
| Metadata.manufacturer.raw report..... | 204 |
| Table 68 Censys Top 10 report 23.telnet.banner.banner | 218 |
| Table 69 Censys report Hacked and count by operating system 17 November 2017..... | 221 |
| Table 70 Filtered Top Ten report keyword Hacked by Windows OS | 222 |
| Table 71 POST Search Rest API URL Parameters & examples | 236 |
| Table 72 POST Search Rest API Data Parameters..... | 236 |
| Table 73 POST Search Rest API Response codes | 237 |
| Table 74 View Rest API GET URL Parameters | 237 |
| Table 75 View Rest API GET Response codes | 238 |
| Table 76 Rest API Report URL Parameters | 238 |
| Table 77 Rest API Report Index URL Parameter..... | 238 |
| Table 78 Rest API Report Data Parameters..... | 238 |
| Table 79 Rest API Report Response codes..... | 239 |
| Table 80 Rest API Report Query Data Parameter..... | 239 |
| Table 81 Rest API Report Query response codes..... | 239 |
| Table 82 Rest API Get Job Status URL Parameter..... | 240 |
| Table 83 Rest API Get Job Status response codes..... | 240 |
| Table 84 Rest API Get Job Results URL Parameter | 240 |
| Table 85 Rest API Get Job Results response codes | 240 |
| Table 86 Rest API Get Series response code..... | 241 |
| Table 87 Rest API Get Series Details URL Parameter..... | 241 |
| Table 88 Rest API Get Series Details response codes..... | 241 |
| Table 89 Rest API Export Get Job Status URL Parameter.... | 242 |
| Table 90 Rest API Export Get Job Status response codes.... | 242 |

| | |
|--|-----|
| Table 91 Rest API Data Get Series response codes | 243 |
| Table 92 Rest API Data View Results URL Parameters..... | 243 |
| Table 93 Rest API Data View Results response codes..... | 243 |
| Table 94 Additional Tools | 246 |
| Table 95 Censys Basic Parsed Certificate fields..... | 246 |
| Table 96 Censys Parsed Fingerprint fields | 247 |
| Table 97 Censys Apple Certificate Validation fields | 247 |
| Table 98 Censys NSS Firefox Validation Certificate fields.... | 248 |
| Table 99 Censys Google Certificate Transparency Validation fields | 248 |
| Table 100 Censys Parsed Validity fields..... | 248 |
| Table 101 Censys Parsed Subject fields | 249 |
| Table 102 Censys Parsed Issuer fields..... | 250 |
| Table 103 Censys Parsed Certificate Public Key fields..... | 251 |
| Table 104 Censys Parsed Certificate Miscellaneous fields | 252 |
| Table 105 Censys Parsed Certificate SAN fields | 252 |
| Table 106 Censys Parsed Certificate Basic Constraints fields | 254 |
| Table 107 Censys Parsed Key Usage fields | 255 |
| Table 108 Censys Parsed Certificate Extended Key Usage field | 255 |
| Table 109 Censys Parsed Certificate SKID field..... | 255 |
| Table 110 Censys Parsed Certificate AKID field | 256 |
| Table 111 Censys Parsed Certificate AIA field..... | 256 |
| Table 112 Censys Certificate Policy fields | 256 |
| Table 113Censys Parsed Certificate Control fields | 257 |
| Table 114 Censys Parsed Certificate Transparency Poison fields | 257 |
| Table 115 Censys Parsed Certificate Name Constraints fields | 257 |
| Table 116 Censys Parsed Certificate Unknown fields | 261 |
| Table 117 Censys Parsed Signature fields..... | 262 |
| Table 118 Censys Certificate Metadata fields..... | 262 |
| Table 119 Censys CCADB Audit fields..... | 262 |
| Table 120 ZLint..... | 269 |

Why Censys rocks!

0.1 Introduction

Open source intelligence gathering (OSINT) and web-based reconnaissance is an integral part of penetration testing and proactive defence. The more connected we are, the more information is held about everything. Yummy, juicy information for both a penetration tester or a malicious actor. Learning what sources of are available to start your search is an essential first step in learning about reconnaissance and how the information could be utilised or resold. Both issues you or your client need to know. All of the tools and techniques in this book can be ninjafied with Python, SQL, SDK or PowerShell.

0.2 Target Audience

Penetration testers, security and network analysis or anyone curious about open source intelligence gathering. Defenders and exploiters alike.

0.3 Conventions

Sensitive information may be removed from the examples, or modified.

0.4 Other Resources

Tools which can use all or part of Censys.io and ZMap

| Tool name | URL |
|-------------------|--|
| Python | www.python.org/downloads/ |
| Censys web search | Censys.io |

| | |
|--------------|---|
| ZMap & tools | github.com/zmap/zmap |
| Recon NG | bitbucket.org/LaNMaSteR53/recon-ng |
| Maltego | www.paterva.com/web7/ |
| Spiderfoot | www.spiderfoot.net/ |
| Metasploit | www.metasploit.com/ |
| NMap | nmap.org/ |
| PowerShell | docs.microsoft.com/en-us/powershell/scripting/powershell-scripting?view=powershell-6 |

0.5 Request for Comments

Bugs@hypasec.com

0.6 Acknowledgements

My significant other, who was patient and supportive through my grumbles, gripes and cursing at Word whilst writing this book. Friends Colonel JC Vega, LanaSec my sane lady rock, M. Blackmeer, @Marmusha chemical mayhem, stage shy former military intelligence, Commander Tosh, Jeff Man, David Z & Olga, Dr. Anita D'Amico & CodeDx, Joe Gray, Security BSides Amsterdam, London and LV crew, Caroline Wong, OWASP OC, Jack Rhysider Darknet Diaries, Austrian EU Presidency and Energy CERT, Dr./Lawyer/Diplomat Lucy, APPG AI, IoActive & Jennifer Sunshine, NSA, FBI Dr. WiFi, Andy Yen/ Proton Mail, evil gamemaster brother from another mother Stefan, Drew J and all the happy hackers out there who helped support me during the research and writing of this book.

0.7 Technology and tools to create the book

- VMWare Workstation Pro 12 and 14
- Two Asus ROG laptops, sadly one broke writing this book, the other is called Zombie
- Python & PowerShell

- Kali Penetration Testing Operating System
- (I hate) Word
- Mc Frontalot & YT Cracker's music

0.8 Protocol References

Censys is based on the ZMap project. ZMap is capable of multiple protocols; however, its capable of NTP but does not utilize the protocol fully.

Table 1 Zmap and Censys.io protocols

| Protocol name | Default port |
|--------------------|--------------|
| BACnet | 47808 |
| CWMP | 7547 |
| DNP3 | 20000 |
| DNS | 53 |
| FTP | 21 |
| HTTP | 80 |
| HTTPS | 443 |
| IMAP | 143 |
| IMAPS | 993 |
| MODBUS | 502 |
| NTP | 123 |
| Niagara Fox | 1911 |
| POP3 | 25 |
| POP3S | 995 |

| | |
|-------------------|------|
| Siemens S7 | 102 |
| SMTP | 25 |
| SMTPS | 465 |
| SSH | 22 |
| UPnP | 1900 |

0.9 Organization of the book

The book is divided by major protocol and service. Examples for each service and risk importance in a penetration and security researcher perspective.

Chapter 1: The Censys.io and ZMap.io Project

Information about the two projects and usefulness

Chapter 2: Setting up your OSINT lab

Get your virtual machine, lab and tools prepared. with API keys.

Chapter 3: Remote Management

FTP, SSH and Telnet protocols.

Chapter 4: Email

SMTP, SMTPS, IMAP, IMAPS, POP3 and POP3S

Chapter 5: HTTP & HTTPS

Web services over HTTP and HTTPS

Chapter 6: Dorking with Censys

Search engines are your friend: they want to help you find juicy files and vulnerable systems.

Chapter 7: ICS & Scada

BACnet, Fox, DNP3, MODBUS and Siemens S7

Chapter 8: Building Control Systems & IoT

Search engines are your friend: they want to help you find building

control systems and the Internet of Sh*t vulnerable systems.

Chapter 9: Other Protocols

DNS, UPnP, SMB

Chapter 10: Tags

How to leverage labelling performed by Censys called Tags.

Chapter 11: Reports

Detailed reports, pinpointing vulnerable or hacked systems and more.

Chapter 12: Censys with Tools

Combine the Censys API with some of your favourite hacking tools like Metasploit and Recon NG.

Chapter 13: Rest API

Using Censys to its fullest extent is the Rest API.

Companion Website

The companion website for the book is at, at

<https://tools.hypasec.com/>. Here you will find downloads, URL links, tips and tricks and any errata.



The middle section is missing because the remainder of the book is under copyright and available for sale. If you are a university and would like a copy, please email:
everything@hypasec.com

Sale link on Amazon:

<https://www.amazon.com/Hack-World-OSINT-Hackers-Gonna/dp/0995687595>

ISBN: ISBN-13: 978-0995687592

ISBN-10: 0995687595

Citations & works used

Bibliography

AgnesSmedley. 2017. *Spy*. 18 February.

<https://www.brainyquote.com/quotes/keywords/spy.html>.

Atkins, Christopher. 2016. *Hacking SCADA/Industrial Control Systems*. Lexington.

Bisson, David. 2017. *Second Wave of Shamoon 2: Disttrack Can Now Wipe Organizations' VDI Snapshots*. 12 1.
<https://www.tripwire.com/state-of-security/security-data-protection/cyber-security/second-wave-shamoon-2-disttrack-can-now-wipe-organizations-vdi-snapshots/>.

Bloomberg. 2016. *Editor's Picks*. 2016 September.
http://www.chicagobusiness.com/article/20160923/N_EWS07/160929874/trump-hotels-to-pay-50-000-fine-over-data-breaches.

Chipkin, Peter. 2009. *Bacnet for Field Technicians*. Vanvouver:
Chipkin Automation.

—. 2010. *Modbus for Field Technicians*. Vancouver: Chipkin Automation.

CVE Details. 2016. *CVE Details The ultimate security vulnerability datasource*. 02 April.
https://www.cvedetails.com/vulnerability-list/vendor_id-26/product_id-3436/version_id-92758/Microsoft-IIS-7.5.html.

2016. *CVE Details The ultimate security vulnerability datasource*. 2016 April. <https://www.cvedetails.com/>.
- David E. Sanfer, Eric Schmitt. 2016. *Spy Agency Consensus Grows That Russia Hacked D.N.C.* 26 July. http://www.nytimes.com/2016/07/27/us/politics/spy-agency-consensus-grows-that-russia-hacked-dnc.html?_r=0.
- Drupal. 2016. *Drupal Core - Highly Critical - Public Service announcement - PSA-2014-003*. 02 April. <https://www.drupal.org/PSA-2014-003>.
- DuckDuckGo.com. n.d. *Say hello to bangs*. Accessed June 26, 2017. <https://duckduckgo.com/bang>.
- Durumeric, David Adrian and Karthikeyan Bhargavan and Zakir. 2015. “Imperfect Forward Secrecy: {H}ow {D}iffie-{H}ellman Fails.” *22nd ACM Conference on Computer and Communications*, October.
- Freifeld, Karen. 2016. *Trump Hotels settles with N.Y. Attorney General over data breaches*. 23 September. <http://www.reuters.com/article/us-trumphotels-nyattorneygeneral-settlem-idUSKCN11T2KR>.
2016. https://censys.io/ipv4/*. 18 September. https://censys.io/ipv4/*.
- Hunt, Troy. 2012. *Shhh... don't let your response headers talk too loudly*. 28 February. Accessed November 2017, 5. <https://www.troyhunt.com/shhh-dont-let-your-response-headers/>.
- ICIJ Database. n.d. *ICIJ Database*. Accessed December 20, 2016. <https://offshoreleaks.icij.org/>.
- n.d. *ILOVEYOU*. Accessed November 2017, 17. <https://en.wikipedia.org/wiki/ILOVEYOU>.

- Knapp, Eric D, and Joel Thomas Langill. 2015. *Industrial Network Security, Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems*. Waltham: Syngress.
- Kubecka, Chrstina. n.d. “DefCon 22 Social Engineering CTF.” HypaSec. *DefCon 22 Social Engineering CTF*. Las Vegas.
- Matherly, John. 2016. https://www.shodan.io/search?query=*>. 3 March. 2016.
- Mehnle, Julian. 2016. *SPF Record Status*. 14 8. http://www.openspf.org/SPF_Record_Syntax.
2017. *Microsoft IIS*. 5 November. Accessed November 5, 2017. http://www.cvedetails.com/product/3436/Microsoft-IIS.html?vendor_id=26.
- MITRE. 2016. *CVE Common Vulnerabilities and Exposures The Standard for Infromation Security Vulnerabilitiy Names*. 02 April . 2016.
- National Institute of Standards and Technology. 2016. *Apache 2.2 vulneability search results*. 02 April. https://web.nvd.nist.gov/view/vuln/search-results?query=apache+2.2&search_type=all&cves=on.
- Netcraft UK. 2016. *Site Report*. 2 April. <https://www.netcraft.com>.
- NMap. n.d. *Home page*. Accessed May 1, 2016. Grabbing banners and naming services.
- Offensive Security. 2016. *Offensive Security's Exploit Database Archive*. 02 April. <https://www.exploit-db.com/>.
- OWASP. 2017. *Testing for Weak Encryption (OTG-CRYPST-004)*. 17 July. Accessed August 22, 2018. https://www.owasp.org/index.php/Testing_for_Weak

Encryption(OTG-CRYPST-004).

- Paganini, Pierluigi. 2017. *A Second variant of Shamoon 2 targets virtualization products*. 10 1.
<http://securityaffairs.co/wordpress/55235/malware/shamoon-2-virtualizations.html>.
- Rapid 7. 2016. *Rapid 7 Vulnerability & Exploit Database*. 02 April.
<https://www.rapid7.com/db/>.
- Rhysider, Jack. 2018. *Ep 13: Carna Botnet*. February 15. Accessed August 8, 2018.
<https://darknetdiaries.com/episode/13/>.
- Roa, Ub Narasinga. 1994. “A Handbook of Kannada Proverbs, with English Equivalents.” In *A Handbook of Kannada Proverbs, with English Equivalents*, by Ub Narasinga Roa, 5. New Delhi: Asian Educational Series.
- Robtex.com. 2016. *Website Review*. 02 April.
<https://www.robtex.com>.
- Ruwhof, Sijmen. 2017. *How to hack the upcoming Dutch Elections*. 2 February. <https://sijmen.ruwhof.net/weblog/1166-how-to-hack-the-upcoming-dutch-elections>.
- . 2017. *How to Hack the Upcoming Dutch Elections*. 28 January.
<https://sijmen.ruwhof.net/weblog/1166-how-to-hack-the-upcoming-dutch-elections>.
- Spiderfoot. 2016. *SpiderFoot Documentation*. 20 September.
<http://www.spiderfoot.net/documentation/>.
- Time. 2016. *belgium-isis-nuclear-power-station-brussels*. 26 March.
<http://time.com/4271854/belgium-isis-nuclear-power-station-brussels/>.
- Tīvārī, Gajendra. 1996. “Amana Prakāśana.” In *Ranja lidara ko bahuta hai*, by Gajendra Tīvārī, 1. University of

California.

- n.d. *View a List of HTTP Response Headers (IIS 7)*. Accessed November 2017, 17.
[https://technet.microsoft.com/en-us/library/cc753686\(v=ws.10\).aspx](https://technet.microsoft.com/en-us/library/cc753686(v=ws.10).aspx).
13. *Weak Diffie-Hellman and the Logjam Attack*. 2015 October. Accessed June 2017, 7. <https://weakdh.org>.
- Wikipedia. 2018. *ILOVEYOU*. 12 January. Accessed Februrary 20, 2018. *ILOVEYOU*.
- . 2017. *List of HTTP Status Codes*. 22 January . Accessed January 26, 2018.
https://en.wikipedia.org/wiki/List_of_HTTP_status_codes#Unofficial_codes.
- . 2016. *Nmap*. 04 April.
<https://en.wikipedia.org/wiki/Nmap>.
- . n.d. *NMap*. Accessed May 1, 2016.
<https://en.wikipedia.org/wiki/Nmap>.
- . 2017. *Republican Party (United States)*. 30 January.
[https://en.wikipedia.org/wiki/Republican_Party_\(United_States\)](https://en.wikipedia.org/wiki/Republican_Party_(United_States)) .
2017. *Wikipedia Saudi Aramco Cyber Attack*. 16 5.
https://en.wikipedia.org/wiki/Saudi_Aramco#Cyber_Attack.
2017. *Wikipedia Saudi Aramco Cyber Attack*. 17 5.
https://en.wikipedia.org/wiki/Saudi_Aramco#Cyber_Attack.
- Wikipedia. 2016. *Wikipedia*. 19 September.
[https://en.wikipedia.org/wiki/Democratic_Party_\(United_States\)](https://en.wikipedia.org/wiki/Democratic_Party_(United_States)).

- . 2016. *Wikipedia*. 13 March.
https://en.wikipedia.org/wiki/Panama_Papers.
 - . 2017. *Wikipedia*. 1 January.
https://en.wikipedia.org/wiki/Campaigning_in_the_United_Kingdom_European_Union_membership_referendum,_2016#Grassroots_Out.
 - . 2016. *Wikipedia*. 2 January.
[https://en.wikipedia.org/wiki/Fitna_\(film\)](https://en.wikipedia.org/wiki/Fitna_(film)).
- Youtube.com. 2016. *Apache 2.2.15 exploit Youtube.com search results*. 02 April.
<https://www.youtube.com/results?q=apache+2.2.15+exploit>.
- Zakir Durumeric, David Adrian, Ariana Mirian, Michael Bailey,
J. Alex Halderman. 2015. *A Search Engine Backed by Internet-Wide Scanning*. Detriot: Proceedings of the 22nd ACM Conference on Computer and Communications Security.

Index

- 10-Minute Email, 19
- BACnet, 128
 - Important Censys fields & examples, 128
- DNP3, 123
 - Important Censys fields, 123
- DNS, 150
 - Important Censys fields & examples, 150
- EU GDPR
 - HTTP Code 451, 75
- FTP, 25
 - 100 Series codes, 26
 - 10000 Series codes, 32
 - 1st digit server return codes, 25
 - 200 Series codes, 27
 - 2nd digit codes, 26
 - 300 Series Codes, 29
 - 400 Series codes, 30
 - 500 Series codes, 31
 - 600 Series codes, 32
 - Important Censys fields & examples, 25
- MikroTik discovery, 30
- Servers with busy status, 27
- Servers with logged in users, 28
- Syntax Errors, 32
- ThinServer discovery, 29
- Heartbleed, 82
- HTTP
 - Censys fields & examples, 71
 - Client Error Codes, 73
 - Important Censys fields & examples, 80
 - Important Censys HTTP properties, 70
 - Information Codes, 72
 - Microsoft Internet Information Services Codes, 77
 - NGINX Error codes, 77
 - Redirection Codes, 73
 - Server Error Codes, 75
 - Success Codes, 72
 - Unofficial Codes, 76
- HTTPS
 - Censys certificate fields, 83
 - Censys parsed certificate fields, 85
 - Certificate Tags, 82
 - Important Censys HTTPS properties, 79
- Hyper Text Transport Protocol, 70
- iCondom. *See* I must appreciate my SO more, dating is scary
- Internet of Things
 - Digital Video Recorder, 142
- Kali
 - Download, 21
- Maltego, 185
 - Configure API Keys, 20

Download URL, 21
MODBUS, 119
Basic function names,
120
Censys fields &
examples, 120
Exception Codes, 121
ZMap object mapping,
122
NSA
Prism, 68
OSINT-Kali
Credentials, 17, 18
OSINT-Kali Distribution,
16
Download URL, 21
Open OVF format, 17
Open VM Format, 17
OWASP
Test OTG-CRYPST, 88
Recon NG, 230
Rest API, 235
Create Report, 238
Report Data Parameters,
238
Report Export, 241
Report Index URL
Parameter, 238
Report Query, 239
Report Response codes,
239
Report URL Parameters,
238
Search, 236
Search Data Parameters,
236
Search Parameters &
examples, 236
Search Response codes,
237
View, 237
View Response codes,
238
View URL Parameters,
237
Shodan
API Key, 19
Siemens S7, 124
SMB, 154
Important Censys fields
& examples, 155
SMTP, 44
Important Censys fields
& examples, 45
Metadata, 51
SSH, 33
Censys banner report,
192
Important Censys fields
& examples, 33
Vulnerable server
discovery, 35, 191
Tags, 157
ICS & SCADA, 118
Telenet
Vulnerable system
discovery, 38, 217
Telnet, 36
Censys Top 10 banner
report, 218
Important Censys fields
& examples, 37

Who wrote this?

About the Author

Chris Kubecka, Security Researcher and CEO of HypaSec. HypaSec offers expert advice in cyber warfare, incident response management, lecturing, training in IT and ICS security, penetration testing, privacy and vulnerability scanning and writing services in security. HypaSec also build hands-on penetration and intelligence courses, such as a HypaSec hands-on version of the GIAC GPEN. Formerly, establishing several security groups for Saudi Aramco's international affiliates after the Shamon 1 attacks and headed the Information Protection Group for Aramco Overseas, Netherlands. Implementing and leading the Security Operations Centre, Network Operation Centre and Joint International Intelligence Group & the EU/UK Privacy Group for Aramco Overseas Company. With continuous professional experience in the field, her career includes the US Air Force, Space Command, private and public sector.

A conference presenter at Black Hat, OWASP, Security BSides, European Union Presidency for fintech and energy cyber security, CCC Chaos Computer Congress, Cyber Senate on ICS Security, Nuclear Cyber Security, European Council on Foreign Relations, OpenFest, Last H.O.P.E on water system insecurities and censorship, advises and lectures as an expert for several markets and governments. Chris has been featured in the media with Viceland News' Cyber Warfare series, Hacking the Infrastructure on HBO, Sky News, CNN, Fox News, Asian and European news outlets. Podcasts DarkNet Diaries and Security Weekly. MIT Technology Review "How to Implement Security after a Cyber Security Meltdown" March/April 2016 issue. Writing for 2600, Hackernoon, Free Code Camp, Peerlyst, several Bit Coin and defence related media.