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

British Library Cataloguing-in-Publication Data

This book is written in British International English not US English

Application Submitted

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 chic so to speak.

Table of Contents

Where was that figure?

Where was that table?

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/NEWS07/160929874/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 Consesnus 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/.

Tivārī, Gajendra. 1996. "Amana Prakāśana." In *Rañja līḍara ko bahuta hai*, by Gajendra Tivārī, 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.

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) .

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).

—. 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).

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 {I}nternet-Wide Scanning*. Detriot: Proceedings of the 22nd ACM Conference on Computer and Communications Security.

Index

Chris Kubecka

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.