PenTest
magazine

PENTESTER'S GUIDE 101

Shell Scripting
For Bug Bounty Hunters and Pentesters

Three Scary Tools
That Use the Shodan Search Engine

Starting a Cybersecurity Startup

AWS: Offensive and Defensive Cloud Security

06/2021 ISSN 2084-1117

PenTest magazine

EDITORIAL Team

Managing Editor

Bartłomiej Adach

bartek.adach@pentestmag.com

Proofreaders & Betatesters

Lee McKenzie, Bernhard Waldecker, Avi Benchimol, Girshel Chokhonelidze, Kevin Goosie, Paul Mellen, Robert Fling, Craig Thornton, Da Co, Tom Updegrove, Aditya Srivastava

Special thanks to the Proofreaders & Betatesters who helped with this issue. Without their assistance there would not be a PenTest Magazine.

Senior Consultant/Publisher

Paweł Marciniak

CEO

Joanna Kretowicz

joanna.kretowicz@pentestmag.com

DTP

Bartłomiej Adach

bartek.adach@pentestmag.com

COVER DESIGN

Hiep Nguyen Duc

PUBLISHER

Hakin9 Media Sp. z o.o.
02-511 Warszawa
ul. Bielawska 6/19
Phone: 1 917 338 3631
www.pentestmag.com

The techniques described in our articles may only be used in private, local networks. The editors hold no responsibility for misuse of the presented techniques or consequent data loss.

PenTest magazine

Dear PenTest Readers,

Summer is a perfect time to start a journey with something new, isn't it? That's why this month we decided to prepare an issue dedicated to all of you who are keen on getting into cybersecurity, but are still waiting to take the very first practical steps. Our contributors present you with various aspects of pentesting that are pillars of every cybersecurity expert to-be!

You'll learn about the basics of AWS security, Shell Scripting for your very first tools, and IoT. What's more, you are going to learn about interesting tools that use the Shodan search engine - it is a must for your OSINT practice at the reconnaissance stage before your pentests :)

For those of you who are already more advanced in pentesting, we also have a lot of interesting reads! We highly recommend the article on starting your cybersecurity start-up, if you're thinking about getting your own business ready. Moreover, in this edition, you will find articles on advanced ethical hacking techniques. You'll read about two ways to gain access to a domain controller in situations where there is no way to attack the lsass process, and a super interesting case of threat hunting for Remote Desktop Protocol (RDP) discovery.

To sum up, something cool for everyone, as usual :)

Enjoy,

PenTest Magazine's Editorial Team

Contents

Three Scary Tools That Use the Shodan Search Engine

Naqwada

Shodan is a search engine very different from the classic search engines that we are used to. Indeed, when Google or Yahoo! crawl only for ports 80 (HTTP) and 443 (HTTPS) open and accessible on the world wild web, Shodan, crawls all the open ports from 1 to 65535. This means that Shodan, unlike any normal search engine, does not focus on searching for web pages but on collecting banners of services (server response to a request). These services include HTTP, HTTPS, FTP, SSH, Telnet, SNMP and SIP protocols.

What can I find on Shodan?

Well, almost everything that requires an internet connection! This is one of the reasons why most people call Shodan "the most dangerous search engine in the world". With Shodan you can find IoT devices such as mobile phones, a connected fridge, security camera systems, crypto bot servers, any kind of servers located in North Korea, maritime satellites or even traffic lights... In short, Shodan will crawl and list anything that is connected to the internet with an open port.

Today I'm going to introduce you three scary tools that take advantage of Shodan to get sensitive information, access to unprotected Raspberry Pi servers and even access to security surveillance cameras anywhere in the world.

Scary, right? Let's start!

SHODAN QUEST

If Shodan can be seen as a huge cave containing an infinite number of things that can be explored, then Shodan Quest is the tool that will make you the explorer.

Shodan Quest is an open source tool coded in Python that can be used to search for sensitive devices/services on Shodan. The implemented collection of Shodan dorks can reveal sensitive personal and/or organizational information such as vulnerable internet routers or servers, access to some services like security cameras, maritime satellites, traffic light systems, prison pay phones, etc. This list is supposed to be useful for assessing security and performing pen-testing of systems.

For example, let's say I want to get a list of Android devices.

No problem! The implemented associated dork is "Android Debug Bridge" "Device" port:5555. With this dork, Shodan will find in his database all devices that have Android Debug Bridge open.

Better than words, this video shows us how to access an Android device in less than one minute using the Shodan Quest tool.

< https://webmshare.com/play/DemYQ >

Scary, isn't it? And this is just a small example of the wealth of information that can be found using Shodan dorks.

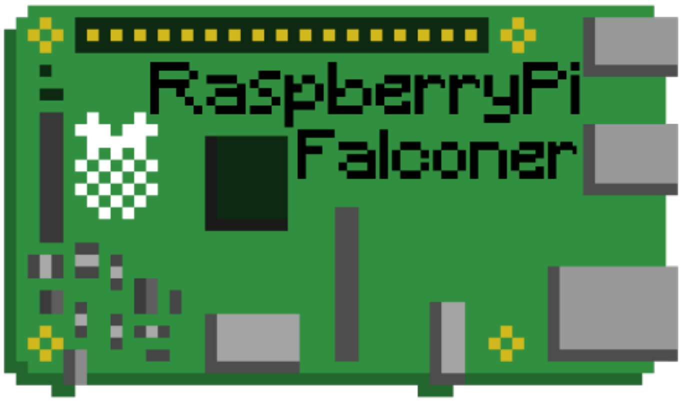
Shodan Quest tool and the complete list of dorks (more than 100 in total) is available on the following GitHub repository: https://github.com/Naqwada/Shodan-Quest

One dork, one quest, what will be yours?

Raspberry Pi Falconer

Raspberry Pi, Raspberry Pi… They're small, they're green, they're cheap, but above all they're very useful, especially when you consider how many unlimited projects you can do with. Whether you're a novice or an experienced pro, we've all tried at least one. The problem is that when we usually follow a tutorial online to do something with our Raspberry Pi, we are not often faced with the security aspect. And this how we end up with our Raspberry Pi and the SSH port open using the default credentials to the world without knowing it... And this is where another of our scary tools comes in, Raspberry Pi Falconer.

If we compare a Raspberry Pi to little green worms, then Raspberry Pi Falconer is the eagle that will eat them.



Indeed, Raspberry Pi Falconer is a useful tool that can be used to find unprotected Raspberry Pis with an open SSH port all over the world. To find them, the tool uses the Shodan search engine with its API, and with the help of Shodan dorks to target only Raspberry Pi devices. But not only that, once a target is detected, Raspberry Pi Falconer will try to initialize a connection with the Raspberry using the famous default credentials "pi" for the username and "raspberry" for the password and trying to get access into it.

Here is a tutorial that shows how to use Raspberry Pi Falconer.

< https://webmshare.com/play/WqJMK >

It can take some time to find a vulnerable Raspberry Pi but you don’t need to do anything else except wait to get positive results since everything is done automatically. Easy, isn't it?

This tool is open source and can be found on the following GitHub repository: https://github.com/Naqwada/RaspberryPi-Falconer

How many worms would you eat?

BiG Brother

Nowadays, surveillance cameras are everywhere, in the street, in restaurants and cafes, in offices, hotels and schools... It becomes difficult to find a place on this Earth where you’re not being filmed. And who ever thought if someone was watching us behind this camera, we probably think nobody. Maybe to reassure us a bit...

A major problem that often happens when we want to secure a place, is that we don't really know what type of surveillance camera will be best suited to our needs. So, we tend to turn to professionals in the industry that will advise us and offer custom packages. They take care of everything (installation, configuration ...) and you save time, it's a good deal, right?

Well, not so fast. At the time of writing this article one camera out of five is using default credentials. Why? It's difficult to find a proper reason, but it may be due to a lack of qualifications from the camera companies, or perhaps a certain pressure on the employees to push them to quickly install cameras in order to move on to the next client for more and more profits, but what do I know?

And this is where our third scary tool comes in games, his name, BiG Brother.

BiG Brother is another powerful Python tool that can be used to find video surveillance cameras with open ports worldwide. To find this, the tool also uses Shodan API. And with the help of the Shodan dorks, targets only specific video surveillance camera brands of our choice. Once a camera is detected, BiG Brother will attempt to initialize a connection to it using associated default credentials. It is also possible to target cameras in a specific country.

Here is a demo:

< https://webmshare.com/play/ZoXRO >

For the moment, it seems that three models of camera are supported, Canon, Panasonic and Sony, but other models are planned to be added.

As we can see, it took less than a few seconds to find available cameras in the country of our choice.

This tool is also open source and can be found on the following GitHub repository: https://github.com/Naqwada/BiG-Brother

Another problem that I won't talk about in this article is that, generally, the web interfaces of security surveillance cameras contain vulnerabilities and it is sometimes possible to bypass the authentication, or even in some cases take control of the server by remote execution.

Through these three examples, we have seen an overview of what can be done with Shodan and where the nickname of the "scariest search engine" comes from. Good things or bad things, the responsibility is ours. But what we can be sure of is that security is not yet perfected in our world. How long will it take? Good question...

By the way, as you probably saw in the tutorial videos, each tool required a Shodan API key in order to use their search service. For PenTest Magazine readers, I offer a free key, so you can test the different tools by yourself, cautiously, if you wish.

API KEY: Z7cRqljCHEczyRZQbuG3djUxikmDW6sT

Thank you for reading this article! Which of these three tools scared you the most? Let me know in the comment section below!