Scanning the Internet for Vulnerable Devices

Anna Sim and Sean Wang

ABSTRACT

We scan the internet for vulernable devices, focusing on select vulerabilities, using Shodan. Then, we analyze the data to see what the detected machines have in common. Additionally, we create our own scanner to scan the internet for machines vulernable to the same vulnerabilities and compare the results to those of Shodan's scan.

1. INTRODUCTION

With the growth and popularization of the intnert more and more devices are becoming connected to each other through the internet. This allows many devices to now have the convenience and accessibility of being connected to other devices through the internet, such as printing to a shared printer connected to the internet or controlling security cameras remotely.

However, a key problem that comes hand in hand with these advantages is that any any vulnerabilities could allow unwanted and unauthorized guests to control the device remotely. Devices without proper security can be attacked and the attackers can then control the devices and gain access to any information the device might have. In some cases, attackers can utilize the connection and control they have over the device to then attack the other devices connected to the same network. For example, Shodan is a tool that allows users to search for devices connected to the internet and can give potentially useful information for attackers. Currently, there are many computer systems, including traffic lights, security camers, or industrial control systems, that have little to no security, leaving them vulnerable to attackers[2].

The approach taken in this paper is to determine some Common Vulnerabilities and Exposures (CVEs) that can be detected remotely and then utilize Shodan to see how many machines have those vulnerabilities and what similarities the machines have. Then, since one approach to defense against this type of detection is to just prevent detection by Shodan, a custom scanning tool will be used to see if it has similar results.

Overall, the setup is simple and is mostly data analysis and comparison. The data returned by Shodan's search will be divided by the CVE that the machine is vulnerable to, but will also need to have the flexibility to pick a machine and see what CVEs Shodan determined it to be vulnerable to.

The methods for a custom scanner for specific CVEs will depend on the specific CVEs chosen. In this case, we plan to look at CVE-2014-2256, CVE-2019-0708, and CVE-2018-0101.

The main contributions of this paper are as follows:

- We explore more about the vulernabilities being searched for and provide more detail on how these can be exploited for some specific systems.
- We show how these vulernabilities can be detected using Shodan and what information can be gathered from these scans. We analyze this information and discuss how this could be used maliciously.
- We create our own scanner and compare its results to Shodan to get insight on how information of specific systems is exposed to the internet.

2. MOTIVATION

For this project, the works that we will build on most are the "Evaluation of the ability of the Shodan search engine to identify Internet-facing industrial control devices", "Impact of the Shodan Computer Search Engine on Internet-facing Industrial Control System Devices," and "Contactless Vulnerability Analysis using Google and Shodan."

All of the above mentioned works cover the Shodan search engine which will be helpful in starting this project and knowing what we can do to perform our own form of vulnerability analysis. The second report explains in more detail compared to the other two about the Shodan program itself, such as its functionality and device identification, indexing, as well as its setup and deployment. Together, these reports in addition to previous labs involving internet scanning will help us achieve our goal in discovering vulnerable machines found by our script.

The CVEs listed previously were chosen due to their commonality, since this would mean that there would be more information to work with. Additionally, that gives the custom scanner more opportunities in the situation that it does not perform as well as Shodan, so that a better comparison can be made between the two scanning methods.

3. OUR ARCHITECTURE

4. EXPERIMENTAL RESULTS

5. RELATED WORK

In "Impact of the Shodan Computer Search Engine on Internet-facing Industrial Control System Devices"[2], they discuss metrics on whether or not Shodan has been and is being used to target industrial control system devices. This addresses the concern of whether this method and channel of attack are widely used when targetting a specific set of devices.

In another paper, "Evaluation of the ability of the Shodan search engine to identify Internet-facing industrial control devices"[1], they analyze Shodan's detection ability on a specific programmable logic controller and suggests a potential solution to mitigate its visibility to Shodan.

In "Shodan Visualized"[3], the paper discusses how Shodan actually scans the internet.

In "Contactless Vulnerability Analysis using Google and Shodan"[4], the paper discusses combining Google searches and Shodan searches to determine the vulnerability of systems in large scale networks.

6. CONCLUSIONS

We expect that Shodan can detect these vulnerabilities and that not all machines with these vulnerabilities have been patched, since it may be harder to patch on certain machines than others. Additionally, we expect that the results of our own scanner to be similar to Shodan's scan, but with less results.

7. REFERENCES

[1] R. Bodenheim, J. Butts, S. Dunlap, and B. Mullins. Evaluation of the ability of the shodan search engine to identify internet-facing industrial control devices. Technical report, Air Force Institute of Technology, Jan. 2014.

[2] R. C. Bodenheim. Impact of the shodan computer search engine on internet-facing industrial control system devices. Technical report, Air Force Institute of Technology, Mar. 2014.

[3] V. J. Ercolani, M. W. Patton, and H. Chen. Shodan visualized. 2016.

[4] K. Simon, C. Moucha, and J. Keller. Contactless vulnerability analysis using google and shodan. 2017.