This is the Title
And This is Some More

ABSTRACT

asdf

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[1].

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. Additionally, the number of CVEs may need to be controlled so that there is not too much data to sift through.

The methods for a custom scanner for specific CVEs will depend on the specific CVEs chosen.

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.

3. OUR ARCHITECTURE

4. EXPERIMENTAL RESULTS

5. RELATED WORK

Point out other important approaches in the problem area. For example, if you are proposing an architecture, maybe OS or PL approaches to this problem.

The following paragraph included just for a figure. The caption of a figure is very important – I try to tell the entire

story in the figures and captions alone, just in case that is all the reader sees.

The general problem of determining whether information flows in a program from variable x to variable y is undecidable, as "any procedure purported to decide it could be applied to the statement **if** $f(x)$ halts **then** $y := 0$ and thus provide a solution to the halting problem for arbitrary recursive function" [2].

6. CONCLUSIONS

7. REFERENCES

[1] 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.

[2] D. E. Denning and P. J. Denning. Certification of programs for secure information flow. *Commun. ACM*, 20(7):504–513, 1977.