Chris Cohen

April 2, 2020

CS422 Final Project Proposal

Creation, Development, and Analysis of HoneyPots

1 Problem Definition

A honeypot is a term used in computer security to describe a network entity that purposefully lures attackers. It is particularly useful for frustrating and distracting attackers, since it is usually a dead end with no access to the desired part of the network. Attackers are constantly scanning the internet for vulnerabilities, and can wreak havoc if they are able to exploit any. A honeypot is an extra layer of security for a network, and even though it may not capture every attacker, it can take a good portion of malicious traffic away. One common use case for a honeypot is to set some sort of monitoring up, and collect information on the attackers. Analyzing this information can be valuable to help improve network security in other places that need it.

2 Motivation

I am majoring in Computer Science with emphasis on cybersecurity. This project is a great opportunity to gain cybersecurity experience, which I have very little of at this point. This subject piqued my interest, since it seemed like such a simple, but effective concept. Reading articles on this subject, people talk about the instant results they get after deploying the honeypot, which intrigues me. I find it hard to believe that attackers would try to invade my own home network, so I want to see it firsthand.

3 Related Work

3.1 HoneyHTTPD

One particular project that inspired me is HoneyHTTPD (https://github.com/bocajspear1/honeyhttpd). The idea of this project is that it makes it easy to set up fake web servers and record requests. It's also in Python, which will make it an invaluable resource to look at when I'm not sure where to go. There is functionality to deploy multiple honeypot servers at once, each listening for attackers. I will base my work off of this general idea, but will add blacklisting functionality, and a way to graph output after receiving it, making data easier and quicker to read.

3.2 StackHoneyPot

Another project that I found interesting is called StackHoneyPot (https://github.com/CHH/stack-honeypot). This is a honeypot that is created specifically for detection and trapping of spam bots. It detects if a field in a response form has been altered. Since this field isn't used by the website, it will be obvious that the client is a bot. If detected, it sends the bot to a dead end blank page. I plan to implement a similar idea with dynamic blacklists, where IPs that connect multiple times are blocked.

4 Proposed work

I plan to implement a honeypot using Python 3.7. One form of the honeypot will serve client requests using my HTTP web server that I created in Lab 1, and record said requests. Since my Lab 1 HTTP web server isn't perfect, I also plan to make a simple HTTPS server using built-in Python libraries to test. Each honeypot that I create will record every connection/request made, and log it in a readable file for later analysis. In addition, I plan to create a simple blacklist that is editable by the user, and a dynamic blacklist that blocks IPs who connect multiple times. I plan to leave the honeypot running for a couple of days, gather data, and create a graph that summarizes

the data gathered. It is worth noting that, seeing as I have done limited research on honeypots, I expect to implement more than just these features.

5 Schedule

I plan to start slow, researching, and exploring repositories on GitHub for existing honeypots. I don't underestimate what it may take to complete this, so I will start early. I aim to have the initial phase of the honeypot completed by the halfway mark, so that I can improve and polish the final product. Ideally, I have a week to test my honeypot at my own apartment, so that I can gather sufficient data. This is mostly for the dynamic blacklist (detecting and blocking IPs that connect multiple times), since it would not work well just running in a short period.

6 Team Members

For this project, I am deciding to work by myself. I made this decision so that I could complete a personal project and potentially stand out to recruiters in the future. Also, a team project during quarantine could complicate things.