My Safe Space

Project Proposal

[redacted]

Table of Contents

Abstract

Security has always been a necessity in life since the beginning of mankind. It can take the form of bodyguards, locks, walls, message encryption, and body armor. Ever since the creation of the internet, a new form of security was brought into the world, cybersecurity. When the internet was new many people didn't really understand how it worked and left themselves vulnerable to attacks unknowingly, but as time went on professionals discovered how to prevent these issues. However, like every other form of security, someone always figures a way around and breaks the security; because of this, a large portion of the population is left unaware of how to stay protected. This paper proposes the creation of software that can be used to help the average person stay protected by providing: useful information to know where their vulnerabilities may lie, easy methods to harden their system, and a variety of services to improve their system. This paper will give an outline of the issue at hand, the different objectives of the project, the resources used to shape the project, and a timeline for accomplishing the goals of the project.

1.0 Introduction

1.1 Background

As time goes on in the new age of technology everyone's life is becoming more integrated with cyberspace. Sadly, most people see technology as magic and don't quite understand how it works, therefore, this leads to a large group of people who stay vulnerable to cyberattacks without even knowing it. If there was an easy way to help teach people what kind of vulnerabilities may exist in their devices and what actions can be taken to prevent such vulnerabilities cybercrimes wouldn't happen as much.

Our first and most paramount issue at hand is keeping people safe. The primary objective of this project is to provide an application to the user that will keep them protected from various methods of exploits that can be used on the average individual or company. The next issue is making the information needed to understand cybersecurity easy to comprehend. This project will accomplish this by giving a variety of tools needed to stay safe and a thorough description of how each tool can be used to defend against vulnerabilities and exploits. The last issue is that most people don't have the motivation or desire to learn about cybersecurity due to various reasons. A remedy for this issue is devising a plan that gives the knowledge one needs with little effort from the user. The last objective of this application will be to provide the necessary resources to the user so they can quickly learn what kind of vulnerabilities and exploits exist and when new ones come out.

1.2 Motivation

My motivations for working on this project are my passions for security, keeping people safe from threats, and teaching others important information that will benefit them later in life. I used to think my methods for security were effective enough, but as I began learning more about cybersecurity I realized how little I truly knew and how ineffective my methods for security really were. Most people I know have similar practices as myself or less and thought it would be beneficial to many if I was able to pass on my knowledge to the general public in an easily digestible way that also gives all the necessary tools to stay safe.

1.3 Related Work

Windows and Linux Security Audit; Sergiu Miclea, Journal of Applied Business Information Systems, 2012

A Systematic Literature Review Of Security Software-Defined Network: Research Trends, Threat, Attack, Detect, Mitigate, And Countermeasure; Mochamad Teguh Kurniawan & Setiadi Yazid, ResearchGate, 2019

Linux Hardening in Hostile Networks: Server Security from TLS to TOR; Kyle Rankin, Addison-Wesley Professional, 2017

2.0 Problem Statement

As the population uses technology more in everyday life the need for security becomes more apparent each day. If people still fall victim to simple attacks like spam and phishing how many people are open to being attacked by more incognito methods. The average person does not have to worry too much about being sought out for attacks as companies would, but most people still prefer to have their privacy. Now with the complexity of technology, the amount of information one needs to know to understand all the ins and outs of cybersecurity can become overwhelming to the average person who is not in the computer science field.

With that being said, there needs to be an effective way to inform the populace how to protect themselves from cybercriminals without the requirements of monthly company training. The objective of this project is to solve this problem that exists in the world and hopefully one day a larger portion of people will understand cybersecurity and the knowledge will be as intuitive as putting a lock on your front door.

3.0 Proposed Project & Significance

3.1 Proposed Project

For this project, I am proposing an application that can be used to help individuals and companies harden their computers. This will be done in three parts. The first part is with securing and hardening the system directly; this will be done by having simple and in-depth options for changing core settings in your system to improve hardening. The second part is having a variety of services provided in one hub for the user to use that will benefit the user in keeping information safe, tracking network activity, and automatic hardening. The third part would be providing resources and information for the user that would help them learn more about cybersecurity beyond what the application can explain. It will also provide extra tools that aren't included in this application and give recommendations of other applications that would be useful.

3.2 Significance

Most people don't understand cybersecurity beyond knowing that they need some sort of anti-virus software on their computer. The significance of this project is to remedy this issue by providing a hardening application that shows the user exactly what is being changed, why it's being changed, and how the user can take further actions to ensure they are properly protected. It does not help the user out much to simply wave a wand and say you are now protected, it would be widely beneficial to explain to the customer what is being done.

4.0 Objectives

4.1 Project Objectives

4.1.1 Project Objective 1

Develop an application platform to perform all the functions that this project will consist of. This objective will take around 1-2 weeks.

4.1.2 Project Objective 2

Write sound code that properly secures a computer from threats and ensures no exploits exist. This will be an ongoing objective throughout the creation of the project.

4.1.3 Project Objective 3

Create a paper documenting everything over the course of this project and noting any issues that arise or functionalities that were not implemented.

4.2 Functional Objectives

4.2.1 Function Objective 1

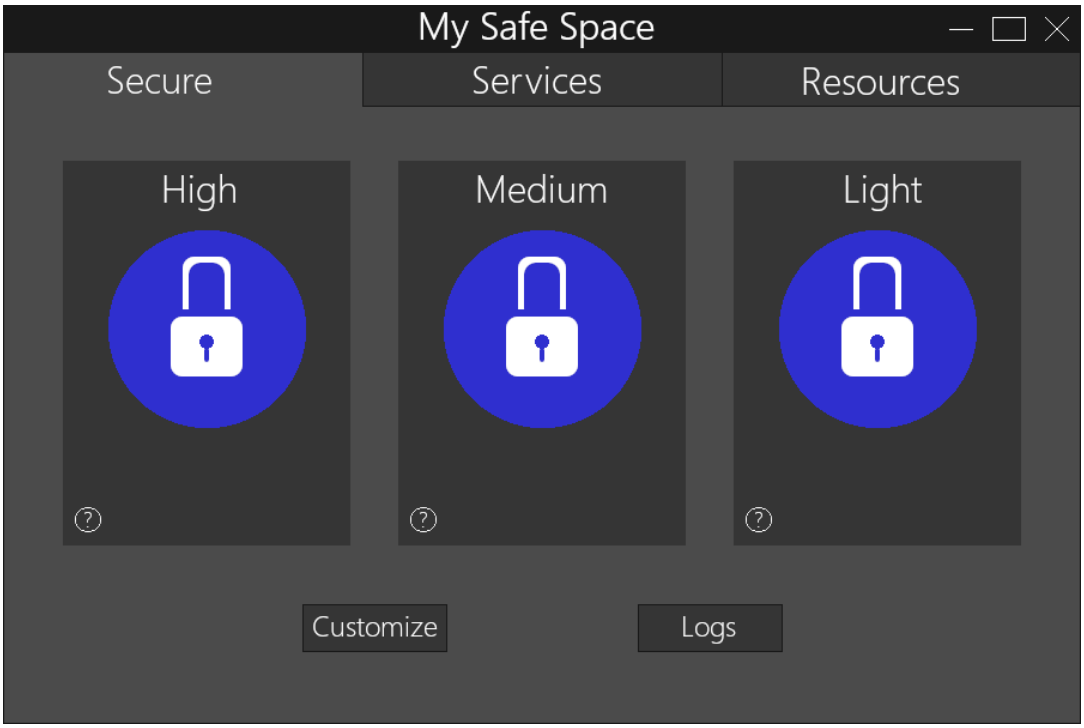

Figure 4.1: Secure tab

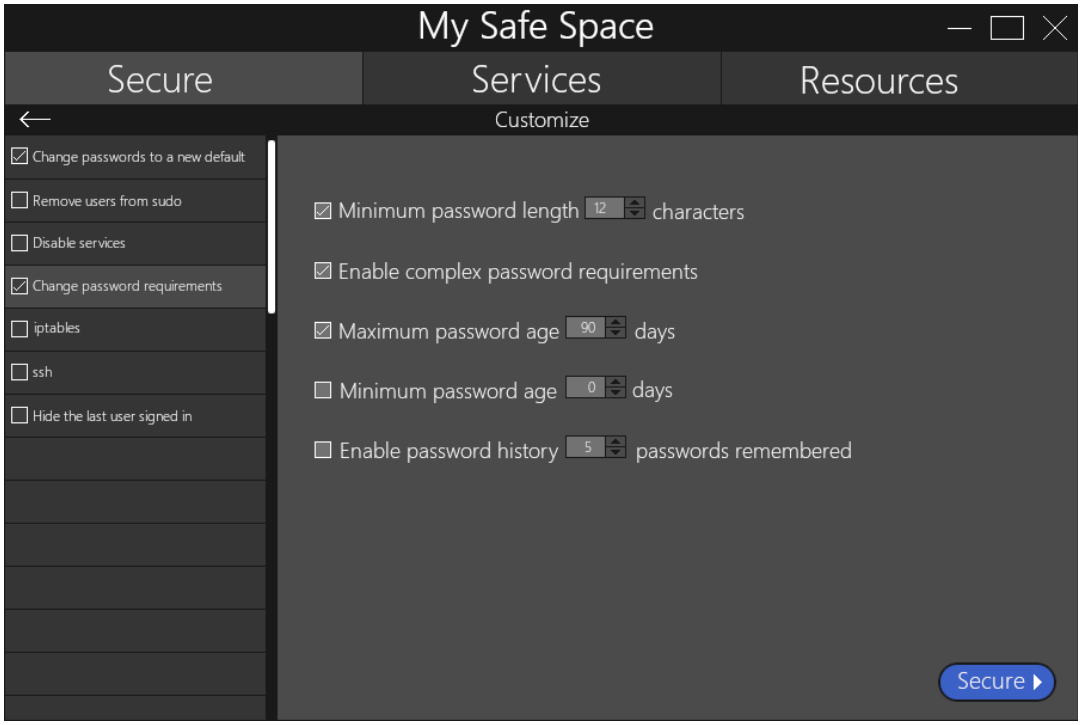

Figure 4.2: Customize options

Create default settings to harden a computer (figure 4.1) and implement custom options (figure 4.2) to give the user freedom to personalize how their computer is secured.

4.2.2 Function Objective 2

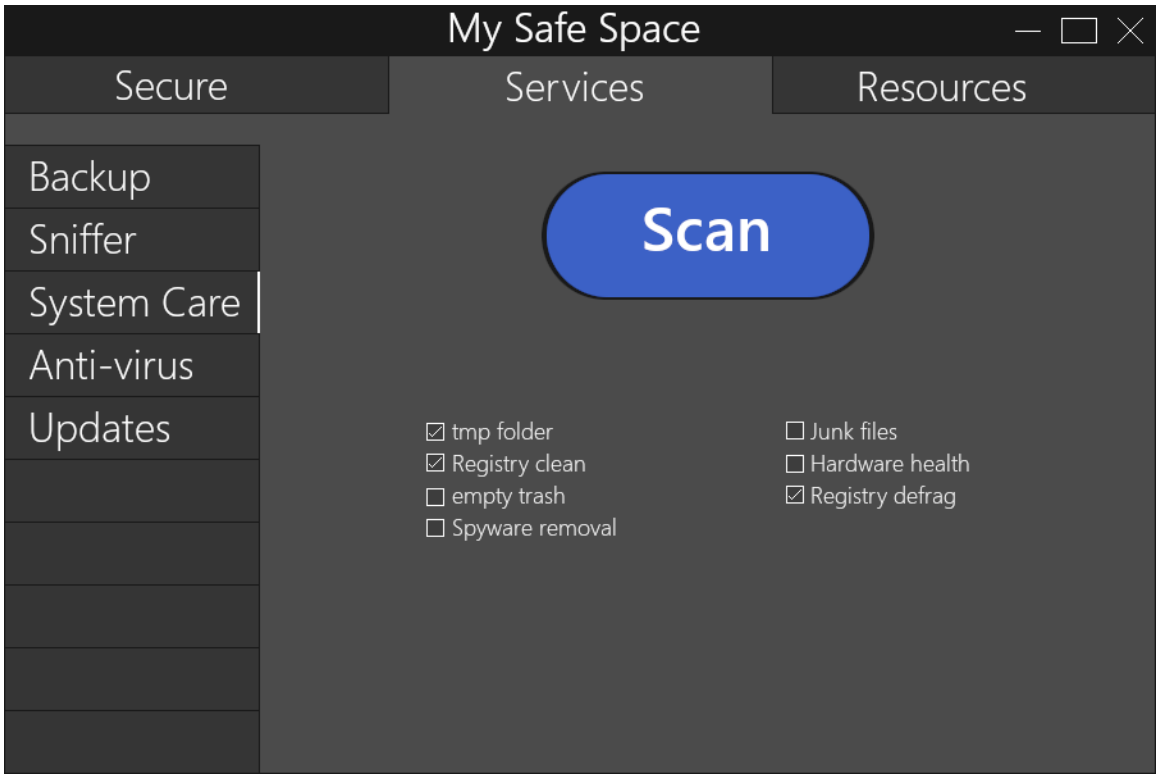

Figure 4.3: Services tab

Provide a variety of services: automatic backups, a sniffer, automatic updater, and anti-virus (figure 4.3). Services are subject to change depending on the available time to implement them.

4.2.3 Function Objective 3

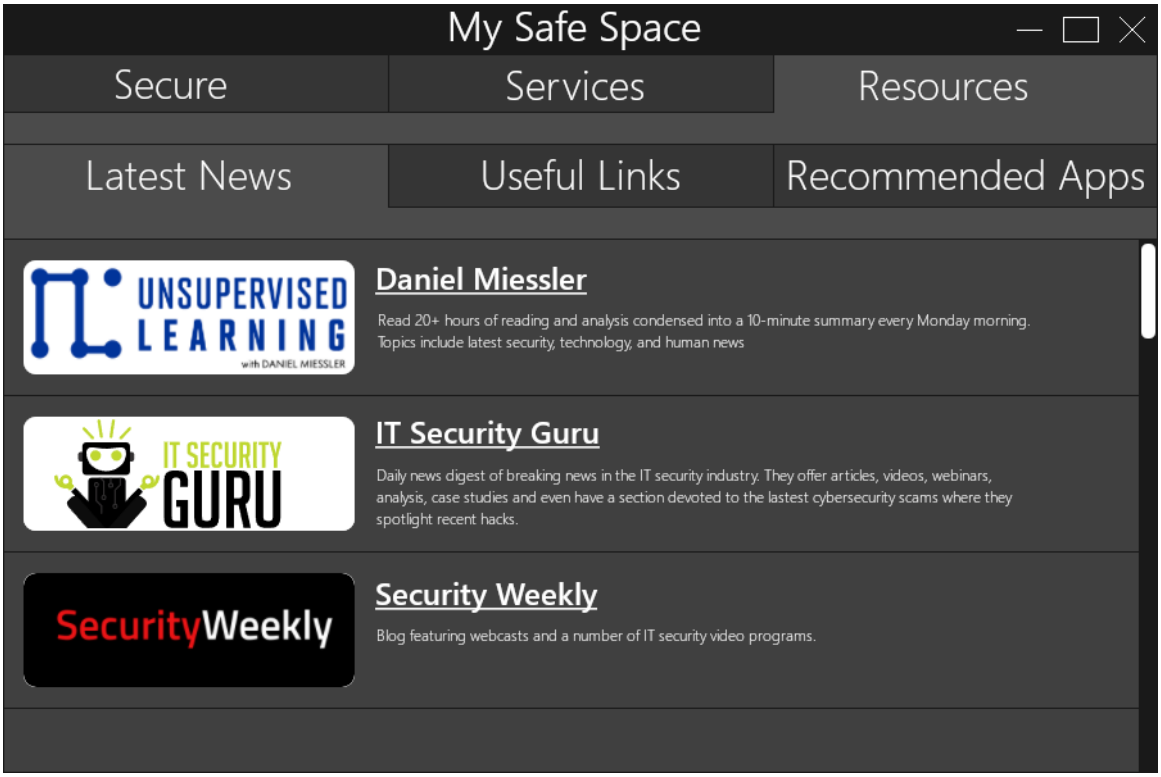

Figure 4.4: Resources tab

Provide resources for the user so they can stay informed about what kind of threats exist out there and how to protect themselves from them. These resources will include news outlets, websites that provide helpful functions, and other third-party applications that help with securing a computer (figure 4.4).

5.0 Activities

5.1 Phases

Phase 1: Research, Modeling, and Outlining

- Do research on what common vulnerabilities exist in companies and personal computers.
- Investigate other security applications to get a concrete idea of what this project's model and code should look like.
- Outline the foundation code for the key functions of this project.
- Model a basic structure of how the application would work; first through CLI to enable remote users without using the GUI and then build a structure for the GUI.

Phase 2: Development

- Test the application on VMs that are designed to have known vulnerabilities and see how they withstand attacks after hardening.
- Develop important secondary functions (services) and conduct tests to ensure they are working as intended.
- Create the resource section of the application.

Phase 3: Documentation

- Write out documentation of the implementations; discoveries found during research; performance and efficiency compared to existing applications; and the compatible platforms.

Phase 4: Additional Features

- Reserve additional time at the end of the project to allow for the addition of other features that go above and beyond the scope of the project but still have importance to the overall goals of the project.

6.0 Development Environment

The majority of the code used for this application will be python and will be using bash to fill in any gaps that can not be completed with python. PyQT5 framework will be used to implement a GUI interface on local Linux and Windows. The development of the whole project will be conducted in a VS Code environment.

7.0 Reports and Products

The end goal of this project is to create an application that can easily be downloaded (locally and remotely) on Linux and Windows to perform quick and easy hardening procedures for personal and corporate use. It will be an ideal way to set up a new server or computer that has default settings that may not be secure enough and can be customized depending on the level of security the user wants. In addition to the practical goals, another object of this project is to help educate the users in cybersecurity so they can stay protected and understand why certain methods are being used to secure their operating system, opposed to most applications that do all the technical work without the explanation of how and why things were done to secure their system. The source code for this application will also remain open source to allow others to add on and improve the application as cybersecurity is a never-ending battle that is always evolving and requires input from everyone for ultimate performance.

8.0 Schedule

	August				September				October					November				December				Totals
Research	8	6	6	6	4																	30
Modeling		4	6	6	6	6																28
Development					2	6	10	10	10	10	10	8	8									74
Testing							2	2	2	2	2	4	4	2	2							22
Modification														10	10	2						22
Final Report																10	10					20
Demonstration																		8	8			16
Hours	9	12	15	16	13	14	15	16	13	14	15	16	17	13	14	15	14	9	10	3	4	212

9.0 References

Windows and Linux Security Audit; Sergiu Miclea, Journal of Applied Business Information Systems, 2012

A Systematic Literature Review Of Security Software-Defined Network: Research Trends, Threat, Attack, Detect, Mitigate, And Countermeasure; Mochamad Teguh Kurniawan & Setiadi Yazid, ResearchGate, 2019

Linux Hardening in Hostile Networks: Server Security from TLS to TOR; Kyle Rankin, Addison-Wesley Professional, 2017