**Problem**

It is becoming all too common to see that hackers have once again broken into a company’s servers and stolen or encrypted their data, demanding ransom or some horrible consequences shall be unleashed upon the entity unlucky enough to have been the target of these nefarious acts. As software designers, we need to be aware of the vulnerabilities that can occur through poor code implementation and how to avoid them. One of the best ways to learn how to safeguard a system is to learn how to break into it. Once you know where the vulnerabilities lie, you can then take preventative measures to ensure that any weak points are protected. Know how software can become vulnerable will also help programmers code in such a way that their product is less susceptible to exploits.

Additionally, there is a career field for hackers that try and break into a company’s system at the request of the company itself. If a hacker can break into the system, they then disclose that information to the company so that vulnerabilities can be eliminated. This line of work is called penetration testing and is usually performed by people who refer to themselves as white hat hackers. People who are not trying to hack for their own personal gain, but to help better protect a system against other would-be intruders.

**Goals and Outcomes**

|  |  |
| --- | --- |
| Goal | Desired Outcome |
| 1. Develop a capture the flag application that is targeted at a younger age group than most of the CTF applications currently available. | User’s will be become proficient in hacking through the use of challenges. These challenges will vary in scope depending on the desired area the user would like to train in. As a user advances in a specific focus, the problems become more difficult. Eventually culminating in challenges that require knowledge from multiple areas. |
| 1. Use the concept of gamification when implementing our capture the flag project. | Users will be more likely to continue using the application when it is perceived as a game or has game-like aspects. Examples would be scoring points for solving challenges which are then used to determine your ranking. Being one of the first users to finish a new challenge will award bonus points or some other type of reward system. |
| 1. Use Kubernetes to keep user sessions isolated. We refer to these isolated instances as scenario pods. | Users will be unable to affect other user’s session and progress. This will also allow us to spin up a personalized learning environment for each user on demand. |

**Related Work**

The following is a list of CTF style applications that we will be using as a source of inspiration for our project:

* Hackthebox – A website that provides hacking challenges in a very CTF fashion. Aimed at more advanced users and with less gamification than some other options[1].
* SANS holiday hack – A competition during the winter holidays where hackers are set to solve a series of security related problems. Finding hidden messages in odd places and using those messages to earn points for the competition. These challenges are a great way to learn new techniques and test your hacking skills against others and there are opportunities for prizes[2].
* cyberfire - Another capture the flag style website. There are challenges that the user can attempt and if they retrieve the secret code word, can enter it for points[3].
* Overthewire– a gamified CTF website that starts with the very basics of hacking and helps you work your way up[4].
* PicoCTF (Carnegie Mellon University) - Another CTF platform aimed at a younger age group. Designed primarily as a game that is built on a CTF framework[5].

Concepts people will need to learn and understand to start hacking[6]:

* HTML/PHP
* a scripting language like JavaScript
* data xfer language like XML or JSON
* TCP/IP
* basic programming skills
* pen and paper cryptography

During a phone interview conducted on February 2nd, 2021 with Nicholas Leggett, NCOIC of Cyberspace Warfare Operations Training at Fairchild Air Force Base, the following were suggested as possible topics to start with:

* SQL injection
* time of check/time of use
* buffer overflow
* bounds-checking
* directory traversal
* phishing
* pen and paper cryptography

**References Sited**

[1] H. T. Box, “Hack The Box :: Penetration Testing Labs,” *Hack The Box*. https://www.hackthebox.eu (accessed Feb. 13, 2021).

[2] “The 2020 SANS Holiday Hack Challenge.” https://holidayhackchallenge.com/2020/ (accessed Feb. 13, 2021).

[3] “MOTH.” https://puzzles.cyberfire.training/ (accessed Feb. 13, 2021).

[4] “OverTheWire: Wargames.” https://overthewire.org/wargames/ (accessed Feb. 13, 2021).

[5] “picoCTF - CMU Cybersecurity Competition.” / (accessed Feb. 13, 2021).

[6] “Importance of Ethical Hacking in Today’s World,” *Edureka*, Aug. 07, 2019. https://www.edureka.co/blog/importance-of-ethical-hacking/ (accessed Feb. 11, 2021).