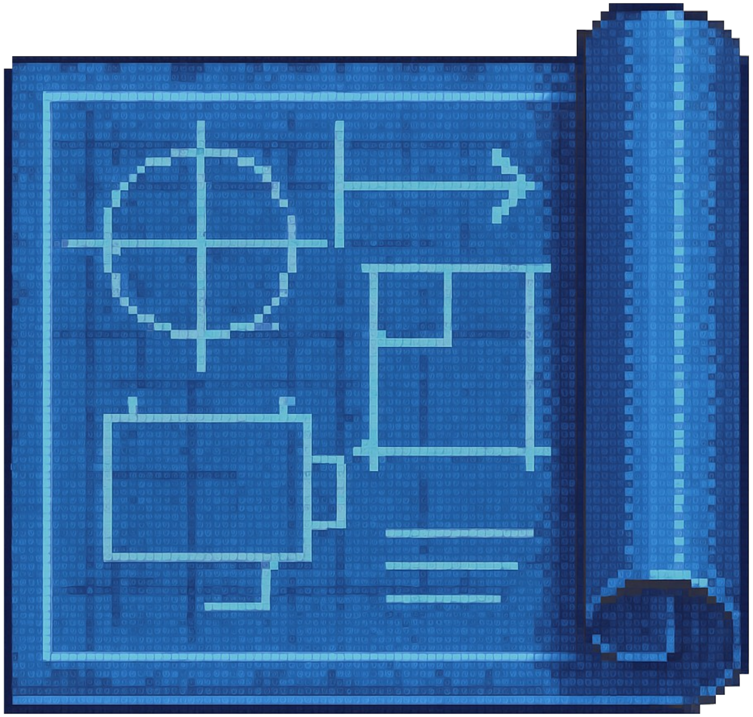
HackerFrogs Afterschool
Python Reverse Engineering

Class:
Reverse Engineering

Workshop Number:
AS-REV-00

Document Version:
1.0

Special Requirements:
Registered account at picoctf.org



Welcome to HackerFrogs Afterschool!

HackerFrogs Afterschool is a cybersecurity program for learning beginner cybersecurity skill across a wide variety of subjects.

This workshop is the intro class to Reverse Engineering.

What is Reverse Engineering?

According to Wikipedia, reverse engineering is a process or method through which one attempts to understand through deductive reasoning how a previously-made--

What is Reverse Engineering?

device, process, system, or piece of software accomplishes a task with very little (if any) insight into exactly how it does so.

What is Reverse Engineering?

Practical applications of reverse engineering in cybersecurity include malware analysis, and binary exploit / malware development

What is Reverse Engineering?

In our course, we'll be focusing on software reverse engineering, and in the realm of software reverse engineering, we'll look at C-compiled x86 programs

C Programming

C is a low-level coding language which is very commonly encountered in reverse engineering and binary hacking challenges

C Programming

We will only be learning enough C coding to read and write some very basic programs so we can better understand reverse engineering

ASM Instructions

Along with C, we'll also be learning the basics of x86 Assembly, since assembly languages are the closest human-readable language to binary machine code--

ASM Instructions

And all reverse engineering tools display x86 program instructions into x86 assembly language

What are CTFs?

HackerFrogs Afterschool classes prefer to incorporate CTF games into classes for a more interactive experience, but what are CTFs?

What are CTFs?

Cybersecurity Capture The Flag (CTF) games are training exercises where the goal of the exercise is to “capture the flag” through use of cybersecurity skills.

What are CTFs?

In this context, “capture” means to gain access to a file or other resource, and “flag” refers to a secret phrase or password.

Pico CTF

The CTF game we will be playing to learn basic digital forensics is called Pico CTF, which is one of the most well-known and well-respected CTF games, and is affiliated with Carnegie Mellon University.

Pico CTF

The Pico CTF game is made up of many challenges across different categories and difficulty levels. For this course well be looking at challenges in the reverse engineering category

What's Next?

In the next HackerFrogs Afterschool Reverse Engineering workshop, we'll continue begin our journey learning C, x86 assembly, and reverse engineering through PicoCTF

Until Next Time, HackerFrogs!