Assignment 3

Due Date: October 27th, 2024

This assignment is based on capture the flag (CTF) type contests. CTF contests are similar to hack-to-hire contests and are widely used for hiring good cyber security engineers by companies. CTF contests are more like treasure hunt games but conducted in cyber space. By solving a series of smaller tasks, you would eventually reach the top of the hill to capture the flag and hence the name. Skills needed are familiarity with using UNIX like systems, especially command line tools. You do not need familiarity with cryptographic algorithms (at least for basic CTF contests). In real world your job would be to simply do reconnaissance on enemy cyber space and capture as much intel (i.e. digital data) from the enemy cyber space. The digital gathered in case encrypted would be decrypted by a different set of experts. The following three platforms have a controlled environment where you can test your UNIX knowledge.

In this assignment you can choose to work in one of the following three environments.

1. Rensselaer Polytechnic Institute (RPI):

This is not a CTF but nevertheless gives you a hands-on expertise from the perspective of reverse engineering and system security. Setting of working environment and necessary tools (refer to Lab 3 email) has already been shared by you through email. You will have to complete **the 1st 4 labs** on this platform. The following link provides more info on the assignments and installation instructions.

- GitHub - RPISEC/MBE: Course materials for Modern Binary Exploitation by RPISEC
- To get help on lab 1 refer to RPISEC/MBE: writeup lab01 (Reverse Engineering) – devel0pment.de

As proof of work done, you will have to take appropriate screen shots to justify that you have indeed worked on your computer.

2. Carnegie Mellon University (CMU)

This is a classic CTF environment that is run as a course by CMU. They provide free access to all students across the globe. Please refer to the following link for more info on account creation and using the environment.

The CTF Primer (picoctf.com)

Complete all the assignments given in the above link. The link provides step by step guidance. However, you will have to practice the same on your own laptops and hence take screenshots (from time to time) to show that you have completed them on your own and on your laptop. This is a self-learning task.

NOTE: While not required for this assignment, if you want to officially take part in upcoming events in cyber security hosted by CMU please refer to picoCTF - CMU Cybersecurity Competition for more info.

3. Bandit War Game

You task is to complete until Level 15 (Max level is 23) of the bandit war game. The link to tasks is OverTheWire: Bandit. Once again document appropriately to prove that you have worked on the solution on your own.

NOTE: To keep you motivated, the solutions for the 1st 5 levels are at the following link. Getting Started with OverTheWire Bandit Security Games (tannerdolby.com)

Try to work on your own before you refer to the solution.