CSE 494: Artificial Intelligence for Cyber Security: Spring 2019

Lab 6: IOC files

Objectives of the lab:

- Introduce the students into IOC files.
- Show the students Redline software.
- Get malware information from the IOC files.

In the first part of this lab, we will use Redline to examine a bunch of IOC files and see what the output of these files is. (15-20 min).

1. We will learn how to use readline to get information about the system.
2. We will learn how to create a collector.
3. We will use the MD5 hashes in the IOC file to extract useful information about the virus or malware.
    a. Use a Json parser here again.
    b. Use VirusTotal API to extract the information.