**Password Forensics Scanner (PFS)**

**Project goals:** create a program/tool that scans through all files on a hard drive and returns any unsecured passwords. For example, employees at a company that type their passwords into a word document or text file. This tool would help companies increase security by neutralizing any unsecured passwords on their machines.

**Scope:** possibly related capabilities that may be achieved by PFS are finding other vulnerabilities on a machine’s hard drive(s), such as company specific files or data that should only be kept in a secured & encrypted area. Other capabilities could be to build a database that tracks the results after every time the tool is used on a machine. This would allow the tool to become smarter and better know where to search for vulnerabilities.

**Deliverables:** to create the PFS tool, the plan is to write a program using Python. The program will search all files and folders on a given machine’s hard drive(s) and return any unsecured passwords found. Documents that I intend to create are a Python script to actually search through the files and folders, a text file that serves as a library for specific file extensions and keywords to search for (i.e. .pwd, .pw, password, pass, etc.), as well as a document to neatly store any unsecured passwords/vulnerabilities found.