Отчет по основному заданию 1

Был проведен анализ предоставленного приложения онлайн библиотеки pyShelf и на основе это выбраны наиболее вероятные сценарии атак:

T1586.002 - Email Accounts

T1566.001 – Spearphishing Attachment

T1566.002 – Spearphishing Link

T1566.003 – Spearphishing via Service

T1566.004 - Spearphishing Voice

T1650 – Acquire Access

T1595.001 - Scanning IP Blocks

T1110.001 - Password Guessing

T1110.002 - Password Cracking

T1110.003 - Password Spraying

T1110.004 - Credential Stuffing

T1059.004 - Unix Shell

T1059.005 - Visual Basic

T1059.006 - Python

T1059.007 - JavaScript

T1037.004 - RC Scripts

T1560.003 - Archive via Custom Method

T1531 - Account Access Removal

- Наиболее возможная атака

- Есть возможность применения

- Возможность применения осень мала

Все сопутствующие файлы находятся в архиве task_1.7z