Personal Specialization Project

Hristo Kolew

Table of Contents

Introduction

During this project I will be working on a topic that I have chosen due to we have the freedom to choose whatever we want as long as it is connected to Cyber Security. I chose to work on two topics. First of them is to create a malware script that allows me to execute commands on a victim's computer. The second topic is to create a password manager. This will be an app that will store all your passwords and will keep them safe. I think both ideas are quite interesting and I think I have enough time to research and develop the topics.

Research Questions

Main Question:

How to create malware script to infiltrate a victim's computer?

Sub questions:

1. Which programming language is the best for malware and why?
2. How to establish connection between server and client?
3. What things I want to execute in victim's computer?

Main Question:

How to create a valid password manager?

Sub questions:

1. Which programming language is the best for password manager and why?
2. How to keep the passwords safe?
3. What previous knowledge should I have to create a valid password manager?

Research Questions	Strategies	Methods	Outcome
Which programming language is the best for malware and why?	Library, Field	Literature study, Community research, Problem analysis	Identification of programming languages commonly used for malware, analysis of their features, and reasons behind their effectiveness.
How to establish connection between server and client?	Library, Field	Literature study, Community research, Problem analysis	Understanding of various networking protocols and techniques for establishing client-server connections, identification of libraries or frameworks that facilitate connection establishment.
What things I want to execute in victim's computer	Library, Field, Showroom	Literature study, Problem analysis, Ethical check	Identification of potential actions or payloads to execute on a victim's computer, considering ethical implications and legality of such actions.
Which programming language is the best for password manager and why?	Library, Filed	Literature study, Community research, Problem analysis	Evaluation of programming languages suitable for developing secure password managers, considering factors such as encryption capabilities, cross-platform support, and community adoption.
How to keep the passwords safe?	Library, Field	Literature study, Problem analysis, Bad good and bad practices.	Understanding of best practices for password security, identification of encryption techniques, password storage methods, and potential vulnerabilities to mitigate.
What previous knowledge should I have to create a valid password manager?	Library	Literature study	Identification of key concepts related to password management, including encryption algorithms, secure storage mechanisms, and user authentication methods.

Planning

Sprint1- Researching	16.05.2023-28.05.2023
Sprint2- Technical exercise	29.05.2023-17.06.2023

This phase is probably the most important for me because I like to have a plan in my head so I can divide my work and make the separate tasks easier for me. After choosing both assignments, I started working on the planning. The first week and half I spend on researching about the topics and go in details about everything connected to them. During the researching phase I also start working on the documentation for the project which included introduction, planning and research question. After these almost two weeks I started working on the technical part. I spend two and half weeks to develop the password manager and two weeks on the malware, which in my opinion was enough time to finish and test it. When everything was done, the only thing that left was finishing the documentation, that I did during these tree weeks.

Preparation

Malware(python)

My preparation for the malware was I quite long due to the need to install and setup 1 Virtual machine with Linux, python with it's needed packages and PyCharm. I needed a local virtual machine because my local laptop will be used as a client and the Virtual machine as a server. After setting everything up I needed to install the following packages;

- Sys
- Socket
- OS - provides functions for interacting with the operating system and a portable way of using operating system-dependent functionality
- Zipfile - provides tools to create, read, write, append, and list a ZIP file.
- Pyautogui - allows for the running script to control mouse and keyboard, providing input much like how a user on the system would, allowing for interactions between applications on the system.
- Glob

Password Manager

My preparation for creating this application also was quite long due to installing python, cryptography with all the needed packages and a python compiler. After I installed the python language, I had to install compiler. First, I decided to go with Visual Studio Code because a lot of my friends and tutorials used it, but I was disappointed because when I get an error, I did not have any message or warning. Also, this compiler did not support the latest python version. These are the reason to change to PyCharm and I also had to repeat the process of installing the cryptography package and apply the needed updates.

Description and general overview

Malware

My malware is written on python language and all the presented packages in the preparation paragraph allowed me to complete the functionality. I have server and client side, in my scenario my Virtual Machine is the server and my local laptop is the client, who is connecting to the server. I have written files in both sides, which allows them to establish connection and execute commands. First, I start the server and then the client to establish the connection.

{picture of the connection}

After the successful connection, in the server side it appears option menu from which I could execute commands. These are the available possibilities:

- Running system commands
- Upload files

- Download files
- Change Directory
- Capture Screenshot

```
Connection established with: 192.168.178.189 on port: 51370
[+] Handle connection



        [1] Run Command on victim OS
        [2] Upload files to the victim machine
        [3] Download files from he victim machine
        [4] Change Dir
        [5] Capture Screenshot
        [99] Exit
[+] Select your options
```

When I choose the first option, I can execute command on the victim's machine.

```
>> systeminfo
[+] Getting Command Result

Host Name:                 N1IGHTMARE
OS Name:                   Microsoft Windows 11 Home
OS Version:                10.0.22621 N/A Build 22621
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Standalone Workstation
OS Build Type:             Multiprocessor Free
Registered Owner:          N/A
Registered Organization:   N/A
Product ID:                00325-81349-92615-AAOEM
Original Install Date:     4/15/2023, 1:23:25 PM
System Boot Time:          6/9/2023, 7:56:38 PM
System Manufacturer:       Acer
System Model:              Nitro AN515-57
System Type:               x64-based PC
Processor(s):              1 Processor(s) Installed.
                           [01]: Intel64 Family 6 Model 141 Stepping 1 GenuineIntel ~2304 Mhz
BIOS Version:              Insyde Corp. V1.18, 6/22/2022
Windows Directory:         C:\WINDOWS
System Directory:          C:\WINDOWS\system32
Boot Device:               \Device\HarddiskVolume1
System Locale:             en-us;English (United States)
Input Locale:              en-us;English (United States)
Time Zone:                 (UTC+01:00) Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna
```

When I select the second command, I can upload files into the victim's machine. After selecting this option, I could see what are the available files that I can upload. Whatever file is uploaded to victim's machine, it is received as a Zip file.

```
        [1] Run Command on victim OS
        [2] Upload files to the victim machine
        [3] Download files from he victim machine
        [4] Change Dir
        [5] Capture Screenshot
        [99] Exit
[+] Select your options2
[+] Uploading file
[+] Upload Files
         0   connection.zip
         1   Project Plan.pdf.zip
         2   screenshot.zip
         3   venv
         4   server.py
         5   connection
         6   main.py
[+] Select file : 2
[+] Selected File:  screenshot.zip
[+] Sending file
```

The third option is for downloading files/folder from the victim's machine. After choosing it I can see the available files/folders for download. I receive them as a Zip file. Almost same steps as the previous step.

```
      [1] Run Command on victim OS
      [2] Upload files to the victim machine
      [3] Download files from he victim machine
      [4] Change Dir
      [5] Capture Screenshot
      [99] Exit
] Select your optionsJ
] Download files
] Receeive Files/Folders
       0   client.py
       1   connection
       2   main.py
       3   Project Plan.pdf
       4   test
       5   venv
] Select the file/ folderJ
] User selected;  Project Plan.pdf
] Received zipped file
] Received name:  Project Plan.pdf.zip
] Receiving zipped file/folder
] File/Folder is Downloaded Successfully
```

The last option is to take screenshot of the victim's desktop and then receive them on the server side. Again, I receive the photo as a Zip file.

```
        [1] Run Command on victim OS
        [2] Upload files to the victim machine
        [3] Download files from he victim machine
        [4] Change Dir
        [5] Capture Screenshot
        [99] Exit
[+] Select your options5
[+] Capture Screenshot
[+] Receiving zipped file/folder
[+] File/Folder is Downloaded Successfully
```

Password Manager

My password manager is also written on python language and its packages, which allows me to complete the functionalities. It is an option-based application, made with simple menu, so it will be easier for me to navigate through the functionalities. These are the available options:

- Create key
- Load key
- Load file
- Add password
- Show passwords
- Exit

```
C:\Users\hrist\OneDrive\Desktop\PassManager\venv\Scri
 What do you want to do?
         1 Create a new key
         2 Load an existing key
         3 Load a Password file
         4 Add a new password
         5 Show the passwords
         q Quit

Enter your choice: 2
```

The first option is creating the needed cryptography key to lock and unlock the password file and store it in premade file.

The second option is loading this key to the system

```
Enter your choice: 2
[+] The key is loaded
b'aixfL3l0lM5IxIwGy9ydIwu5-m2D3eUBp40xRfPU2gY='
```

The third option is pretty similar to the previous option, it loads to the system the password file.

```
Enter your choice: 3
Site: test123, Username: username, Password: passwords
```

One of the last options is to add password to the file. After filling all the needed information, it will be added to the file

```
Enter your choice: 4
Enter Site: facebook
Enter Username: neshto
Enter Password: parolata
Enter your choice:
```

Conclusion, Reflection & Findings

During this project I managed to explore a new programming language regarding the application that I created. I manage to build a fully functional application with a lot of research and hard work. I managed to complete my main goal for the application, which was to add passwords to an existing file, display them, encrypt and decrypt the file with the use of cryptography key. I was able to learn the basics of python programming and to understand how the cryptography is working.

Talking about the assignment regarding the malware, there are I also managed to reach my goals, which I planned. Got better understating of what is actually malware and some things that you could possibly do with it. My main goals for functionality were to run command, upload, download, capture pictures and to add registry keys to startup programs in the victim's machine. It was quite fun and exciting to work on both assignments, which allowed to gain more experience and understanding.

To be honest, I believe my overall project was on a decent level with different types of things. I managed to create and to follow my planning and also did some good researching in order to be able to hold the correct path. Another thing that I improved was my organization skills, which allowed to finish everything in the right time. Also, I am proud of this project and how much hours I managed to put in it. The main key that I was able to do was separate the tasks, which included planning, researching, preparation and testing. I was very interested in doing this kind of project, where my responsibility was to choose topic and go in full details about it. I was able to develop my research skills even more and also to be more patient. This whole project was quite a challenge for me, but I like challenging myself and I truly believe this project learnt different skills and things, which will be useful for my future projects.