Computer Science Department
University of Crete

CS-455: Internet Attacks
Spring 2022 - 2023

Assignment 5
Reversing

Uploaded: 26/04/2023
Deadline: 10/05/2023

Introduction

In this assignment you will learn the basics of reverse engineering.

Notes

- You are allowed to use either IDA (https://hex-rays.com/ida-free/) or Ghidra (https://ghidra-sre.org/) for this assignment. Although IDA is recommended.
- It is required to provide screenshots and analytical reports of the reversed programs to prove your work. Please include this information in a single pdf file.

Questions

1. **[30%] Password Manager**

   Bob created his own password manager thinking that executables can't be reversed. He has a few hardcoded account credentials (username and password combinations) stored in the executable. You want to reverse his program and prove to him that this is not a secure way to implement a password manager. You are assigned to do the following:

   - Decompile the given executable using IDA (or Ghidra).
   - Identify the section where Bob's Email & eLearn hardcoded usernames and passwords are located, provide a screenshot of that.
   - What type of hash function does the program use to store the master password?
   - Try to identify the master password from the given hash (Bob is known to use weak single-word passwords).

- After identifying the master password, make use of the password manager and add a new account into it with your CSD ID as username and a (fake) password. Then provide a screenshot of the password manager's print option.

2. **[70%] Reversing WannabeCry**

Bob executed the WannabeCry virus and now all his files are encrypted. He asked you to help him break the virus and decrypt his files.

A few notes about the virus/environment you are given:

- You are given a directory in which the WannabeCry virus has already been executed.
- For safety reasons, the virus doesn't encrypt the whole disk, but only the virus_folder directory that exists in the same folder as the virus. The encrypted files that you are asked to decrypt can be found in this folder.
- To check how the encryption of the virus works, you can follow these steps:
  - Create a new empty directory.
  - Copy the WannabeCry executable in this directory.
  - Create a new virus_folder in this directory and place a few files that the virus will encrypt.
  - Execute the WannabeCry and notice its behavior.
  - These steps will help you get an understanding of how the virus was first executed. However, now you need to work on the directory you are given in order to decrypt Bob's files.

You are assigned to do the following:

- Decompile WannabeCry using IDA (or Ghidra) and play around with it to get a better understanding of what the virus does.
- Your goal is to break the virus and finally decrypt the files that exist in the virus_folder directory. Provide screenshots of the decrypted file contents.
- You will notice that upon execution the virus generates a KEY.txt file. What is the purpose of this file? What does it contain? How is it generated?
- Provide an analytical report of what the virus does – try to explain in your own words the algorithm of the virus, with as much detail as you can. The goal is to prove that you successfully reversed and understood what the program does.
- Provide screenshots of the top 3 most crucial parts (in your opinion) from the decompiled code and explain why they are crucial.

Resources and further reading

Beginner

- Short video tutorials for Ghidra
  - https://www.youtube.com/watch?v=K-NOg5z930o&list=PLKwUZp9HwWoB6kWyA_Nr3nWIMJLxpt5UC&index=1
- EVERYONE in Cyber Security Should Understand Reversing (it's EASY)
  - https://youtu.be/gh2RXE9BIN8
- Ghidra quickstart & tutorial: Solving a simple crackme
  - https://youtu.be/fTGTnrgjuGA
- GHIDRA for Reverse Engineering (PicoCTF 2022 #42 'bbbloat')
  - https://www.youtube.com/watch?v=oTD_ki86c9I

Advanced (game hacking)

- Windows Game Hacking with Ghidra and Cheat Engine
  - https://youtu.be/Pst-4NwY2is
- Reverse Engineering/Game Patching Tutorial: Full Res Roller Coaster Tycoon with Ghidra+x64dbg+Python
  - https://youtu.be/cwBoUuy4nGc

Channels

- LiveOverflow binary exploitation & reverse engineering playlist:
  - https://www.youtube.com/watch?v=iyAyN3GFM7A&list=PLhixgUqwRTjxglIswKp9mpkfPNfHkzyeN
- OALabs: Malware analysis tools, techniques, and tutorials
  - https://www.youtube.com/@OALABS

Submission

- Submit a pdf document including all the information requested above.
- Submissions will be done through eLearn.
- This assignment is an individual creative process and students must submit their own work. You are not allowed, under any circumstances, to copy another person's work. You must also ensure that your work won't be accessible to others.
- You are encouraged to post any questions you may have in the eLearn forum. If, however you believe that your question contains part of the solution or spoilers for the other students you can communicate directly with the course staff at hy455@csd.uoc.gr.

Disclaimer

It is **ILLEGAL** to attempt any type of attack against a target (individual, network, public/private entity, etc.) without authorization / explicit permission. Such actions are **prohibited and punished by law and university policies**.