BLG460E - Secure Programming

Assignment 3 : Reverse Engineering

Due Date: 19 April, 2022, 23:00 PM

This assignment aims to provide hands-on experience on reverse engineering ELF files. You can use the Linux virtual machine from the first assignment. In the assignment, there are 10 executable files you should analyze. You are required to obtain as much information as possible and prepare a report that contains your interpretations on the information you gathered from the files. The files are zipped in a file. The password is **21574** for the zip file.

Part 1: ELF file structure

Study on Executable and Linkable Format (ELF) file structures. Provide the parts of an ELF file in the report (headers, sections, etc.) in general and make comment on each part. Note that you are not expected to mention all fields in the parts, only big parts will be enough. Do not copy-paste from the internet. Try to use your own words.

Part 2: Analyze the given files

The zip file includes ten files. Analyze these ten files and answer the following questions separately for each file.

- Is the file malicious or benign? Explain how you come to that conclusion.
- What is the entropy of the file? What can you say about the files when you compare their entropies?
- What are the basic information about the file (file type, architecture, etc.)? Is the file executable? How did you obtain these information?
- Does the file contain any debugging information or not? How did you find out this information?
- Can you disassemble the file? Explain why you cannot or how you can.
- When you inspect the strings in the binary file what information could you say about the file? Here are some examples:
  - The file may gather information from /proc/ folder.
  - The file may make HTTP requests.
  - The file may run a shell command.
  - The file may contain an IP address.
  - The file may manipulate the processes.
  - The file may make some file operations.

  Explain how did you conclude your answers.
- After taking precautions, try to run the file in an isolated environment. Were you be able to run the file? If it worked, what happened? If it did not work, why?

- Is the file packed or not? Explain how did you find out whether it is packed or not. If it is packed try to unpack the file and answer all the questions above again for the unpacked file. Compare the results. Make comment on the differences.
- Considering the answers for the questions above, what is the purpose of the file? What does it do?

Hints

- You can use any program to examine the files. Here are some programs that can help you with that: **ent, nm, radare2, ltrace, strace, file, strings, gdb, objdump, hexdump, readelf.**
- **Hint for file5:** NO DEBUGGING! Try to run the file directly on Linux. Then, run it using `gdb`. What are the results?

  Try to find a way to inspect the content of the file. When you understand the problem, run the file properly. Explain what the program does and how did you solve the problems.

  Which functions are used in the file? What are the strings in the binary file? Can you disassemble the file?
- **Hint for file6:** The file seems broken. Try to find the problem and fix it. Then, run the file again. Explain the reason of the problem and what the program does.

Important Notes:

- Date and the time of the submission will not be changed. Please be aware of the deadline.
- Interactions among individuals are prohibited.
- Send an email to **sayinays@itu.edu.tr** for your questions.