You should see a zip file called gc.exe. This is a Windows XP executable. For this Grand Challenge. You will need to reverse engineer it to determine what it does. Unfortunately, the person who wrote it didn’t provide source code or instructions on safe handling of the executable.

If you execute it, you may find that it will do some damage to your machine. **BEFORE YOU START, make sure you have snapshots to revert back to in case the malware destroys your working VM image.**  The primary tool you should use, but are not limited to using, to perform this task is IDAPro.

You should provide me with two things:

* A description of what the program does, or potentially does. The best form of response to this requirement is to simply provide a documented source code version of the executable. C is a perfect language for this, but you may provide in any other language (except assembly) you wish.
* An annotated IDAPro database file, or whatever tool you decide to use, showing where you identified key components of the executable, and renamed functions, variables, parameters, etc. to meaningful names as a means of recording the purposes of each module.

Hint: use Ghidra as an additional tool.

When analyzing the malware, I was able to take a closer look at the functions, variables, etc. as well as how the executable works. I was able to use the applications used in previous labs as part of this analysis, with mostly using IdaPro. Originally when opening the malware given it is just a black executable window. After taking a deeper look in IdaPro I was able to see how the executable works. Initially looking at the strings of the file I was able to find out that the executable was initially a login application, i.e., the application/executable, *gc.exe* is a keylogger for the login. Within the exe being a keylogger, it is not a traditional keylogger. After opening the exe and typing anything, it gives a error message of encountering a problem but under “Mircrosoft.” Being able to close this application it gives the exe file the opportunity to save itself on the computer system under another service as *smdmfu.exe*. I was able to find this information using ProcessExplorer application, with finding this information through ProcessExplorer it was able to give the Administrator information under the malware, which can be viewed by the given screenshots at the end of this document. All the privileges are disabled other than the admin that created the malware, so that there is not a way to cancel or change anything of the keylogger. When attempting to kill or cancel the process running of the malware it gives the message, “Error opening process: Access is denied.” When analyzing in IdaPro, I was able to change variables, and functions within the application. For example, there were many more functions under d word dd , this was used to make it harder to read how the exe file works when analyzing. I was able to change the many jumps to jump 1, jump 2, etc. Also, when changing many more that can be seen in given screenshots, and IdaPro database file that was given. The main 2 keylogger paths that were used were *C:/crossdev/src/mingw-w64-v4-git/mingw-w64-crt/stdio* and *C:/crossdev/src/mingw-w64-v4-git/mingw-w64-crt/math, as well as having a packer of UPX.*

Graphical user interface, application, Word

Description automatically generatedGraphical user interface, table

Description automatically generatedTable

Description automatically generatedTable

Description automatically generatedGraphical user interface, text, application

Description automatically generatedGraphical user interface, text, application

Description automatically generatedGraphical user interface, text, application

Description automatically generatedGraphical user interface, application, table

Description automatically generatedText

Description automatically generatedText

Description automatically generated with medium confidenceGraphical user interface, application

Description automatically generatedGraphical user interface, application

Description automatically generatedGraphical user interface, text, application

Description automatically generatedGraphical user interface, application

Description automatically generatedGraphical user interface, text, application

Description automatically generatedGraphical user interface, text, application

Description automatically generatedText

Description automatically generatedGraphical user interface

Description automatically generated with medium confidence