

Forum:[Hack Forums](#)

Thread: [How can I encrypt and decrypt a binary file?](#)

SIM-4449385 - *October 29, 2019, 6:33 am*

Hey I want to get into white hat hacking and starting with trying to learn through some past CTFs that happened. Came across one that I think I know how can I get the flag, but I need to decrypt a file from binary to read it. How can I do it?

P.S. If you have a better option to learn than trying to solve CTFs and searching online on how to do certain things, feel free to offer me.

Bunnyslippers69 - *October 30, 2019, 2:09 am*

[LMGTFY](#)

CyberStrike - *October 30, 2019, 10:01 am*

Well generally when we are talking encryption the password would be included in the binary itself, I am talking encryption like what you would find in malware. Upon execution if we are to have a debugger say X64/X32 (debug) or WinDBG upon the file being loaded to memory you will start to see the MZ header, you can dump the file now from memory and rebuild IAT. Setting up breakpoints is up to you on where but often `ntcreateprocess` or something similar is a good idea. Fully expect you may have to run the file multiple times. (Of course I am assuming Windows if Linux then adjust accordingly in terms of the breakpoint)

Now many cft's also have another type of binary which will contain a password and upon execution which once again a debugger is used and once again creating breakpoints is on you. I would suggest getting familiar with the program in question perhaps using IDA/Ghidra/Cutter either way you would be looking for a comparative function. This is often referred to as "crackme" type challenges.

Edit: If this is malware please do all this in a VM and disable all sharing.