Reverse Engineering — Hacking Tools

The term reverse engineering, refers to the disassembling of an object, following a thorough examination of its composition/construction so to understand how it works to duplicate or upgrade the object.

Taken by older industries, the practice of reverse engineering is now widely used in the software engineering sector. In this digital-information age, reverse engineering has become a tool that can be used as a way to create compatible products that are cheaper than the existing ones or even free in some cases, uniquely modify the software, and exchange knowledge as a result into making better, more reliable and secure products.

Can be applied to various aspects of both software, and hardware development to understand how they behave under various conditions, to retrieve the source code that was lost, fix issues, to adapt existing software programs with new hardware, etc.

The use of reverse engineering is also greatly exercised to identify malicious content in the source code of a software, such as viruses, or to expose security flaws(backdoors, virus, misconfigurations) and address possible privacy issues.

Researchers can also use this technique to reverse engineer malware to understand how it works to nullify its properties, identify the potential owner, and use the knowledge gained to update their virus databases and prepare mitigation measures for future malware attacks.

Reverse engineering, the process of taking a software program's binary code and recreating it so as to trace it back to the original source code, is being widely used in computer hardware and software to enhance product features or fix certain bugs. For example, the programmer writes the code in a high-level language such as C, C++ etc. as computers do not speak these languages, the code written in these programming languages needs to be assembled in a format that is machine specific. In short, the code written in high level language needs to be interpreted into low level or machine language.

The process of converting the code written in high level language into a low level language without changing the original program is known as reverse engineering. It's similar to disassembling the parts of a vehicle to understand the basic functioning of the machine and internal parts etc. and thereafter making appropriate adjustments to give rise to a better performing or superior vehicle.

Where is Reverse Engineering Used?

- In software design, reverse engineering enables the developer or programmer to add new features to the existing software with or without knowing the source code. Different techniques are used to incorporate new features into the existing software.
- Reverse engineering is also very beneficial in software testing, as most of the virus programmers don't leave behind instructions on how they wrote the code, what they have set out to accomplish etc. Reverse engineering helps the testers to study the virus and other malware code. The field of software testing, while very extensive, is also interesting and requires vast experience to study and analyze virus code.
- The third category where reverse engineering is widely used is in software security. Reverse engineering techniques are used to make sure that the system does not have any major vulnerabilities and security flaws. The main purpose of reverse engineering is to make the system robust so as to protect it from spywares and hackers. Infact, this can be taken a step forward to Ethical hacking, whereby you try to hack your own system to identify vulnerabilities.

While one needs a vast amount of knowledge to become a successful reverse engineer, he or she can definitely have a lucrative career in this field by starting off with the basics. It is highly suggested that you first become familiar with assembly level language and gain significant amount of practical knowledge in the field of software designing and testing to become a successful software engineer.

Reverse Engineering Tools

As mentioned above, reverse engineering is the process of analyzing the software to determine its components and their relationships. The process of reverse engineering is accomplished by making use of some tools that are categorized into debuggers or disassemblers, hex editors, monitoring and decompile tools:

1. **Disassemblers** – A disassembler is used to convert binary code into assembly code and also used to extract strings, imported and exported functions, libraries etc. The disassemblers convert the machine language into a user-friendly format. There are different dissemblers that specialize in certain things.

2. **Debuggers** – This tool expands the functionality of a disassembler by supporting the CPU registers, the hex duping of the program, view of stack etc. Using debuggers, the programmers can set breakpoints and edit the assembly code at run time. Debuggers analyse the binary in a similar way as the disassemblers and allow the reverser to step through the code by running one line at a time to investigate the results.
3. **Hex Editors** – These editors allow the binary to be viewed in the editor and change it as per the requirements of the software. There are different types of hex editors available that are used for different functions.

4. **PE and Resource Viewer** – The binary code is designed to run on a windows based machine and has a very specific data which tells how to set up and initialize a program. All the programs that run on windows should have a portable executable that supports the DLLs the program needs to borrow from.

Reverse engineering has developed significantly and taken a positive approach to creating descriptive data set of the original object. Today, there are numerous legitimate applications of reverse engineering. Due to the development of numerous digitizing devices, reverse engineering software enables programmers to manipulate the data into a useful form. The kind of applications in which reverse engineering is used ranges from mechanical to digital, each with its own advantages and applications. Reverse engineering is also beneficial for business owners as they can incorporate advanced features into their software to meet the demands of the growing markets.