L8SF Exploit Development | Zero Day's and Zero Click Exploits

L8SF & Osamu-KJ

Contact

Author of the posts: L8SF | His Patreon

Publisher and rewriter of the document: Kevin Jerebica AKA Osamu-KJ | His website

Introduction

In case you are wondering why you still haven't made any money hacking..

Once again; i've had this discussion several times.. Film != Reality.

You can't just download a tool and start exploit development right away.

YOU need to start with the basics first which in this case is assembly language and low level development.

We all know it's a tough programming language and that SHOULDN'T stop you from learning it! If you need some motivation, go get yourself some motivational videos, talk to someone about it, share knowledge just make sure not to give up!

To learn and understand the essence of hacking, it is essential to understand programming itself. If you want to build up an effective skillset then you look at the C programming language and try to program it yourself (the language of course). Without externals, you make your own little programming language in assembly utilizing the syscalltable. Then and only then you start with real hacking. Which is finding weak spots in a program that you then exploit.

Also watching videos on youtube without touching your keyboard won't help. That is not considered learning and never will. Until you write your first compiler without a youtube video that wasnt you writing it. What will get you further on the other hand is self-studying and PRACTICE, a lot of it. Failing is a part of the life and you cannot avoid it. You will always have those 'no more motivation' times I call them and you should know that everyone is having them. And still.. that SHOULDN'T stop you from continuing to learn and PRACTICE!

Why learn assembly?

Learning assembly will teach you way more things than any other language can. By building a Compiler for the C language for example as your first project you'll learn the C's Syntax and Assembly simontaniously. Of course the more you work with assembly and create projects like your own compiler the more Assembly will become a second nature, which will enable you to read Assembly fast & like code. From my observations the problem is that people get used to the objective programming language too much and thus do not learn to look at the underlying imperative system, which makes it extremely difficult for a beginner to get into exploiting at its essence.

For example:

```
mov [brain], 1          ; move 1 into ram with adress brain
mov rax, 2              ; move 2 into register rax
mov [rax], [brain]      ; move value of ram:brain into ram:rax
```

An individual that started programming first will not understand that a register and a memory adress are two seperate things, because he learned to think in variables and object calls. He will most likely think that rax is an object that is either callable by address or as direct reference which are two totally different things inside the world of Assembly.

The best move would definitely be learning Assembly and C at the same time. (check the resources at the end of the document to learn about Assembly and C)

Moving onto Exploit Development

Now after immerging yourself into the world of Assembly and C it is time for you to start some real Exploit Development. For that we have the LiveOverFlow's Binary Exploitation Playlist, The CTF101 Guide to Binary Exploitation. Meanwhile learning from these two resources you should search up the internet for some Binary Exploitation CTF's or Challenges. As we've said.. Practice! Always! What I recommend is this amazing Github Repo → CTF Workshop.

For debugging you should use GDB of course → again check the resources to learn more about gdb.

Resources

NASM Assembly Language Tutorials – asmtutor.com

TutorialsPoint – NASM Assembly Lessons

Youtube Basic Tutorials – Made by Kupala

x86_64 Syscall Table

Github Assembly Language Topic Page

LiveOverFlow's Binary Exploitation Playlist

The CTF101 Guide to Binary Exploitation

CTF Workshop

GDB Tutorial – A walkthrough with Examples

GDB Youtube Guide Playlist – By Sidafa Conde