Vulnerability analysis and exploitation

Hossen Karim (karim.hossen@imag.fr)*
Feist Josselin (josselin.feist@imag.fr)*

Abstract: We present a series of practical works that we give to the master students of Grenoble university. They are divided in two parts, the first part is focused on the vulnerabilities discovery and analysis and the second part on the exploitation and post-exploitation using the Metasploit framework.

Keywords: practical, software security, vulnerability, exploitation, metasploit

1 Subject

For the second year of the master SAFE and SCCI of Grenoble, we give two practicals related to software security. The students already have a knowledge and experience on hardware architecture and software development but, most of the time, security aspects are only introduced in a therotical manner.

The practicals are splitted into two sessions of 3 hours each. During the first session, students trigger a crash by providing different inputs to a real application, e.g., mp3 players. Then, using a debugger, they learn exactly what a buffer overflow is and what its impact on the execution can be. After crafting an input to redirect the execution flow, students construct a real exploit and change the behavior of the program by executing a arbitrary code, called shellcode, which is able to execute commands. Following the progression, students can also try to bypass a real protection mechanisms like non-executable stack or address randomization.

The second session introduces to the students the metasploit framework. Students create a metasploit module to exploit the vulnerability found in the first session. By using more complex shellcode, e.g., meterpreter, students understand how to compromised the machine by installing a backdoor. Finally, students have seen all the steps of an attack, from the study of a crash to the creation of an exploit.

2 Contribution to student

By practicing on real vulnerabilities from the discovery to the exploitation, we believe that theses praticals help to develop student's awareness of security problems which are criticals for the users. In addition, it helps the students to build more secure softwares.

References

[703] Rapid 7. The metasploit framework, 2003. http://www.metasploit.com/.

* Laboratoire Verimag, 2 Avenue de Vignate, 38610 Gières, France