The Heartbleed Vulnerability

An unseen theft of protected information

Francesca Ponzetta

Lucas Norman Jonsson

Group 26

Background:

Heartbleed is a vulnerability that affects the OpenSSL cryptographic library. The exploitation of this vulnerability allows an attacker to steal information from the TLS server involved in the current TLS connection. In particular, the attacker may steal not only the secret key used by the TLS protocol in order to secure the communication but also users credentials and other sensitive information stored on the server. As the TLS protocol is used to secure communications and users data, this vulnerability should be patched in order to prevent its exploitation.

The goal of the project:

To further investigate the reasons behind the vulnerability, perform a successful attack abusing the heartbleed vulnerability and explore different countermeasure solutions.

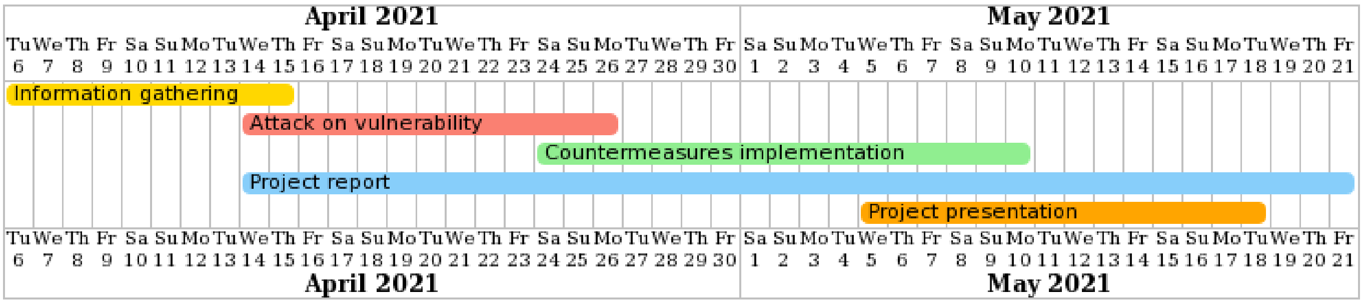
Relevance to language-based security:

The heartbleed vulnerability is a security bug in the OpenSSL software library, so it can be seen as an exploit taking place at the software level of the system. A way to fix this vulnerability is by modifying the existing code on the software level, that's why this issue is relevant to language-based security.

Overview of the planned work:

The main idea is to collect information about the heartbleed bug and how it is used in order to perform an attack. Then we will try to exploit it by performing attacks against a server on a virtual machine. We will also try to find software countermeasures to prevent the attack and after having applied these countermeasures we will try to perform again the attack in order to check their effectiveness.

Schedule:



Target grade: 5

The topic of the project is very relevant: we will explore the theory behind the vulnerability, perform attacks exploiting the vulnerability and also find and test different countermeasures while comparing and demonstrating their effectiveness.