**Deliverable #2: Topic Selection**

|  |
| --- |
| Group 7 Students |
| Khai Phan - 100901164 |
| Marco Rico - 111708178 |
| Andriy Yevseytsev - 131845158 |
| Carlianz Pura - 104375168 |

There are two topic options:

1. Exploit in Action

Document a particular vulnerability or exploit of a host system. Describe the method used to attack the vulnerability/exploit, and explain the security policy process that would be used to deal with such an attack. You may need to set up a testing lab to demonstrate your exploit. It does not matter whether the exploit was successful; if your exploit failed, you need to document why (you may need to surmise what prevented the attack from working)

2. Exploit in Code

Analyze a previous web-based program you wrote from a security perspective. Critically access your source code and use the Fortify Source Code Analysis Tool, or other testing tools, to find threats. Demonstrate how the existing code can be exploited by an attacker. Identify what changes would you make, and rewrite the code to improve program security and demonstrate that it is now secure.

NB: If your code has minor or no security threats, select a different program.

***Our team select topic 1 - Exploit in Action***

Why have we chosen this topic?

This topic is interesting for us and we know that DoS is still among one of the popular methods hackers usually use. This is specifically important to understand how it works because, in order to be a professional you not only need to create the system, you need to understand how the system can be protected from the security standpoint and moreover how to protect it. There are direct and indirect (spoofing) methods and the indirect method seems to be more interesting because there will be lots of types to take into consideration.