# Semester Project Proposal

**Proposal**: Testing and analyzing Zeus Botnet based on Reversed Engineering technique that we have learned in CYBR 4450 – Host-Based Vulnerability course

**Objective**: This project aims to demonstrate the behavior of the Zeus malware in a controlled virtual environment using VMware and Windows 7. The project aims to examine the malware's behavior in real-time using a debugger tool, such as OllyDbg or Immunity Debugger, to understand how it works and its potential impact on a vulnerable system.

**Team Members**: Trung Phan, Redmond Reed, Nora Almagthawi and Graham Bezanson

**Required Resources**: The following resources will be required for this project:

* Windows OS virtual machines, preferred older version like Windows 7 (Attack host and victim host)
* Vulnerable software, such as an older version of Adobe Reader or Java
* Zeus malware (obtained from a legitimate source for research and educational purposes)
* Debugger tool: OllyDbg, Immunity, IdaPro, Ghidra, Hex editor like PEBrowse

**Project Plan**:

* Set up the Windows 7 virtual machine on VMware and install vulnerable software.
* Obtain a copy of the Zeus malware from a legitimate source for research and educational purposes.
* Conducting static analysis.
* Conducting dynamic analysis using debugging tools to examine the malware's behavior in real-time, including how it infects the system, communicates with the command-and-control server, and steals sensitive information.
* Document the findings and present them in a clear and concise manner.
* Reflect on the project and discuss the potential impact of malware on vulnerable systems and the importance of cybersecurity measures.

**Conclusion**:

The demonstration of the Zeus malware in a virtual environment using a debugger tool provides an opportunity to understand the behavior of malware and its potential impact on vulnerable systems. The project aims to promote awareness of the importance of cybersecurity measures and how they can be used to detect and prevent malware attacks. No special or extra VM is required for this project.