Exploit Analysis

Problem Statement: For this project, you will choose an exploit from the open-source Metasploit Framework to reverse-engineer and analyze to determine its capabilities. Using the Metasploit framework, you will develop a payload to deploy via the exploit and test it against the vulnerable software package. Specifically, your task will be to answer the following set of questions:

Key Research Questions:

- What is the vulnerability in the target system that the exploit takes advantage of?
- When was the vulnerability first discovered and for which operating system/application and patch level?
- When was a patch introduced for the vulnerability? Are subsequent versions of the operating system/application still vulnerable to the exploit?
- What information do you need to acquire about a target system to successfully utilize the exploit (e.g. port scanning, OS fingerprinting, etc.)?
- How can you verify that the exploit successfully compromised the target system?
- What privilege level does the exploit provide on the target system? Does this privilege level allow you to perform any function on the target system?
- Does the exploit and subsequent deployed payload(s) evade detection of Personal Security Products (PSPs), such as Anti-Virus, Intrusion Detection System (IDS), etc.? If so, why?
- Do you need to choose an encoding technique to encode the payload so that an IDS or antivirus application will not catch the payload as it traverses a network in cleartext?
- Please describe the tools and techniques you used to perform your analysis.

Project Outline:

- Select and obtain approval to evaluate an exploit from the Metasploit framework. Document your analysis methodology for identifying intrinsic properties of the exploit.
- Develop a payload (shellcode, executable, etc.) to perform some functionality of your choosing on target. The shellcode/executable can be generated in C, Ruby, Javascript, Visual Basic, etc. Does your payload get detected by PSP products? Does your shellcode require encoding because it contains null characters, that when interpreted by many programs signify the end of a string and cause termination before completion? Please document your methods and any tools used.

Resources:

- David Kennedy; Jim O'Gorman; Deven Kearns; Mati Aharoni, "Metasploit", No Starch Press, 2011.
- Shakeel Ali; Tedi Heriyanto, "BackTrack 4: Assuring Security by Penetration Testing", Packt Publishing, 2011.