CIS 432: Ethical Hacking

Spring 2019

Lab #4: Client-Side Exploitations

Instructor: Yi Yang Lab #4 due: April 10th, 2019 before class begins

Total score is 100 points.

Please setup your Kali Linux VM and Windows XP VM and complete the following tasks:

1. Install an old version of Adobe Reader 8.1.2 in your Windows XP VM. Create a **PDF Embedded Executable** under Kali Linux. From Windows target, try to access this PDF. Once you click Open in the PDF warning, the payload will run and you will receive a meterpreter session in Metasploit framework under Kali Linux VM.
2. Install Java version 7 update 6 in your Windows XP VM. Java vulnerabilities are a prevalent client-side attack vector. Exploit **Java vulnerability** in Kali Linux VM and receive a meterpreter session from the Windows target.
3. Exploit the **browser\_autopwn** module in Kali Linux VM and count how many meterpreter sessions that you can create from the Windows XP target.
4. Install Winamp version 5.55 in Windows target VM. Exploit the **Winamp** malicious skin configuration file and receive a meterpreter session from Windows XP target.

This is an individual lab assignment. Please finish all the above tasks under Kali Linux virtual machine and submit a report describing how you achieved every task step by step. Please insert screenshots and short descriptions into your lab report as needed.