# Systems Security Homework #3 Due: 1pm on 3/25/2019

In this homework you will pick a metasploit module and demonstrate how to use it to gain access to your WinXP VM instance. You should use the ONL topology for this homework.

In class, we used the ms\_03\_026\_dcom module; you **must choose a different one** for this homework. Similarly, the Metasploit Unleashed tutorial uses ms08\_067\_netapi; so that one **cannot be used either**. Other than these constraints, you are free to choose any module so long as you are able to demonstrate that it can be used to (at a minimum) open a meterpreter session on your WinXP VM instance.

For your write-up and turn-in document, make a copy of this document, rename it to hw3-notes, and move it into your CSE 523 Google Docs collection. Use this document to complete the homework, using the space provided below.

**You are to complete this homework on your own. Do not ask (or answer) questions of other students; do not discuss any aspect of this homework with any other student. Direct all questions to the TAs or me.**

Your complete homework should include the following.

* An annotated transcript illustrating how to use your module of choice; include at least one screenshot at the end to demonstrate that it worked. Your transcript should be clear and easy for someone to reproduce; you can assume that a reader has the same Ubuntu/WinXP setup that you do. Your annotated transcript should be as easy to follow as exploring-msploit-notes. (You do not need to include gates.)
* Identify and briefly describe the vulnerability that is being exploited with this module. Add links to the appropriate CVE and MS bulletins.
* Find the ruby [source code](https://github.com/rapid7/metasploit-framework) for the exploit module. Include both the URL to the source file at github and a copy of the ruby source code in your write-up.
* Your writeup should be organized and well-written, with proper grammar and spelling.

*Do not change anything above this line. Add your homework write-up below it.*