CMSC 414
Lab 3 – Attack at Dawn
11/18/11

DUE 11:59 PM 12/05/11

Lab 3 will test your ability to scan, exploit and recon a system. DO NOT procrastinate. This lab will take you longer than you expect!

Background
You will be given a Windows XP SP2 virtual machine located here
http://www.cs.umd.edu/~waa/414-F11/Lab3.tgz

The machine is vulnerable to a number of well-known exploits. Find them, and exploit them!

Grading
The exact number of vulnerabilities is unknown. You will gain one point for each vulnerability identified and successfully exploited. If you identify and exploit ALL of the vulnerabilities that well known open source tools can exploit – you will earn 80%. You'll gain additional points (90%) if you identify and exploit vulnerabilities not found by the common open source tools.

Finally, I've placed malware on the host. Find the malware and identify the name, and explain how it works for an additional 10%.

Submission
You must submit the following for all vulnerabilities identified and exploited by well-known open source tools:

1. The CVE number for the vulnerability.
2. The Method of exploitation, e.g. the encoder, shell code etc.

For vulnerabilities not found by common tools, explain the method of how you found the vulnerability and exploited it.

For the malware, identify the malware and explain how the malware works.

Good luck!