Homework 1: System Security.
Due at 11:59PM on February 12, 2013 as a PDF via websubmit.

February 5, 2013

Quick questions.

Exercise 1. Explain how return oriented programming circumvents the "Data Execution Prevention" mitigation.

Exercise 2. One mitigation for return-to-libc attacks was to remove "dangerous" instructions from libc. Explain how return oriented programming circumvents this.

Exercise 3. Can heap spraying can be used to get around an ASLR mitigation? Why or why not?

Exercise 4. You are given a unix timestamp that was computed sometime between Jan 1, 2013 and Jan 4, 2013, but you don't know when. How many bits are in the timestamp? How many bits of Shannon entropy are in the timestamp?

Repeat the above for a timestamp computed from the .NET `DateTime.Ticks` property.
`http://msdn.microsoft.com/en-us/library/system.datetime.ticks.aspx`

Longer question.

Exercise 5. Search online for an article or presentation that outlines an exploit that gets around one of the mitigations described in David's Tuesday lecture on "Vulnerabilities and Mitigations"; the exploit should not have been mentioned in David's lecture. Explain the exploit that you found: how it works, what sort of attacker can perform it (*e.g.,* an attacker that learns the boot time of the machine, *etc.*), how often it works (*i.e.,* always, 50% of the time, *etc.*). Finally, indicate what year the exploit was found and whether or not (and how) the expliot has been mitigated. Don't forget to properly cite the article or presentation you found.

Your answer should be no longer than 400 words.

Submission policy.

Every submitted assignment MUST include the following information:

1. List of collaborators
2. List of references used (online material, course nodes, textbooks, wikipedia, etc.)
3. Number of late days used on this assignment
4. Total number of late days used thus far in the entire semester

If any of this information is missing, at least 20% of the points for the assignment will automatically be deducted from your assignment. See also discussion on plagiarism below.