CS363 Information Assurance and Security

-- Midterm Exam Study Guide

***(I reserve the right to interpret if a question is covered by this guide. Still, only about 90% of questions are covered by this guide****. )*

**Overview**:

1. CIA.

* Can rephrase it.
* Can give application examples.

**Buffer overflow**:

1. Can explain what it is, the cause of it, how to implement it
2. Know stack-based, heap-based, and in other segments
3. Can identify buffer overflow in the source code

**Shellcoding**:

1. Can explain how to use shellcode to exploit buffer overflow attacks
2. Know the process to write shellcode

**Format string**:

1. Know how to use format string to exploit buffer overflow attacks
2. Can identify format string security issues in the source code

**Countermeasures**:

1. Know defenses and countermeasures: canary, shadow stack, non-executable bit, ISR, ASR
2. Can use defenses and countermeasures to analyze scenarios.