Exam 2 Preparation

CS4630 Spring 2016
Goal & Coverage

• Again, the goal is to let you review the knowledge required to be a computer security expert
• Coverage: The lectures after the first exam
• Materials to review: slides, code examples and assignments
• Do not forget to get the latest slides from the syllabus
Exam Questions

- Two type of questions:
  - Conceptual questions
  - Problems (most of the exam are problems)
Conceptual Questions

- General information about vulnerabilities
- Stack smashing exploits
- Return-oriented programming
Problems

• Four problems from:
  - Stack smashing, arc-injection and code-injection
    • Review the code examples and slides
    • Review the buffer overflow assignment
  - Off-by-one vulnerability
    • Review the code example and the example in slides
  - Format string vulnerability
    • Review the code examples and slides
    • Review the format string assignment
  - Return-oriented programming
    • Review the code example and slides
  - The problems will be similar as the assignment questions
  - basic GDB commands and outputs
    • Review the slides on gdb
    • Review the buffer overflow assignment
Example Questions

- The conceptual questions are in the same format as in Exam 1
- Example problem:
  - Consider the following code.

```c
int bar(){
    char buff[8];

    gets(buff);
    return 0;
}
```
Example Question cont'd

- Example problem cont'd
  - If the stack of bar before *gets* is called is

<table>
<thead>
<tr>
<th>Address</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x12345678</td>
<td>Some data</td>
</tr>
<tr>
<td>0x084055e0</td>
<td>Return Address</td>
</tr>
<tr>
<td>0xbfffffd45</td>
<td>Saved EBP</td>
</tr>
</tbody>
</table>

buff
Example Question cont'd

• Example problem cont'd
  – If the attack string is
    “AAAABBBB\x45\xfd\xff\xbf\x45\x60\x44\x08”
  – Given in the values on the stack after the attack string is copied to buff by gets
  – What is the new saved EBP and new return address after the attack string is copied?
Example Question cont'd

- Example problem cont'd
  - Answer
    | Some data (0x12345600) |
    | Return Address (0x08446045) |
    | Saved EBP (0xbffffd45) |
    | "BBBBB" |
    | "AAAAA" |

- New EBP: 0xbffffd45, new return address: 0x08445045
- Pay attention to the details. Really problems in the exam may be easier or harder than this example.