Course Syllabus

Fall 2021, CS 6265-001/OCY

Information Security Lab: Reverse Engineering and Exploitation Labs

Professor: Dr. Taesoo Kim

Course Description
This course covers advanced techniques for writing exploits and patching vulnerabilities, taught through an intense, hands-on security laboratory. A significant part of this course involves solving Capture-The-Flag (CTF) and discussing strategies for solving such problems. This course covers a variety of topics including (but not limited to) reverse engineering, exploitation, binary analysis, and web.

Prerequisite
- Operating systems or equivalent (e.g., CS 3210 at GT).

Class Meetings
- Online course
- Online recitation (EST time, TBD)
  - Monday 12-1PM (TA)
  - Tuesday 9-10PM (TA)
  - Thursday 5-6PM (TA)
  - Friday 10-11AM (TA)

Course Goals
- Learn classes of security vulnerabilities
- Learn how to exploit security vulnerabilities
- Learn how to defend or mitigate security vulnerabilities

Grading Policy
- 100% Lab.
- If you didn’t turn in a single (full) lab, you will get an F.
  - In other words, you have to submit AT LEAST one flag per lab. Solving the tutorial counts, so if you solve all tutorials in all labs, you will not get an F.
- No midterm or final exams.
• 40%: A, 30-40%: B, 30-20%: C and below (in each group).
  o A: Five or more challenges per lab, AND all the tutorials
  o B: Four challenges per lab, AND all the tutorials
  o C: Up to three challenges per lab, AND all the tutorials
• Three groups: undergraduate, masters and PhD students
• We provide a week of a grace period (50% points after due date)
• See Game Rules for detailed information.

Class website
• Visit https://tc.gts3.org/cs6265/2021 to find tutorials and reference materials.

Homework and Quizzes Due Dates
• All labs will be due at the times in the table at the end of this syllabus.
• These times are subject to change so please check back often.

Timing Policy
• The Modules follow a logical sequence
• Assignments should be completed by their due dates.
• You will have access to the course content for the scheduled duration of the course.

Plagiarism Policy
• Plagiarism is considered a serious offense. You are not allowed to copy and paste or submit materials created or published by others, as if you created the materials. All materials submitted and posted must be your own.
• We strictly follow the cheating policy (read GT’s Academic Misconduct Policy).
• Do not publish or post your work online (e.g., GitHub). Any violation of these rules would result in F in your grade.

Student Honor Code
• All degree students should abide by the Georgia Tech Student Honor Code
• Review the Georgia Tech Student Honor Code: www.honor.gatech.edu.
• Any OMS Analytics degree student suspected of behavior in violation of the Georgia Tech Honor Code will be referred to Georgia Tech’s Office of Student Integrity.

Communication
• Please contact your instructor, teaching assistants, and fellow learners via the Piazza discussion forums.
• Often, discussions with fellow learners are the sources of key pieces of learning.
Online discussion is strongly encouraged, and it will help you a lot in solving lab problems. Please join Piazza and post your questions, ideas and thoughts.

Netiquette

Netiquette refers to etiquette that is used when communicating on the Internet. Review the Core Rules of Netiquette. When you are communicating via email, discussion forums or synchronously (real-time), please use correct spelling, punctuation and grammar consistent with the academic environment and scholarship\(^1\).


Course Topics and Release Dates

The table below contains a course topic outline and assignment due dates.

<table>
<thead>
<tr>
<th>Weeks</th>
<th>Course Topics</th>
<th>Release Dates (Eastern Time)</th>
</tr>
</thead>
</table>
| Week 1        | Introduction
Lesson 1 Introduction Tools and x86 | Aug 27, 2021 at 8:00 a.m.                     |
|               | Lab 1                           | Aug 27 at 8:00 a.m. - Sep 2, 2021 at 11:59 p.m.|
| Week 2        | Lesson 2                        |                                                 |
|               | Lab 2                           |                                                 |
| Week 3 & 4    | Lesson 3                        |                                                 |
|               | Lab 3                           |                                                 |
| Week 5        | Lesson 4                        |                                                 |
|               | Lab 4                           |                                                 |
| Week 6        | Lesson 5                        |                                                 |

1. Introduction
2. Tools and x86
3. Bomb Lab1
4. Shellcode and x86_64
5. Bomb Lab2 / Shellcode
6. Stack Overflow
7. Stack Overflow
8. Bypassing Stack Protections
9. Bypassing Stack Protections
10. Bypassing DEP and ASLR
11. Oct 1, 2021 at 8:00 a.m.
<table>
<thead>
<tr>
<th>Lab</th>
<th>Activity</th>
<th>Dates</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>Bypass DEP/ASLR</td>
<td>Oct 1 at 8:00 a.m. - Oct 7, 2021 at 11:59 p.m.</td>
</tr>
<tr>
<td></td>
<td><strong>Week 7 &amp; 8</strong></td>
<td><strong>Lesson 6</strong> Remote-oriented Programming</td>
</tr>
<tr>
<td>6</td>
<td>Return-oriented Programming</td>
<td>Oct 8 at 8:00 a.m. - Oct 21, 2021 at 11:59 p.m.</td>
</tr>
<tr>
<td></td>
<td><strong>Week 9 &amp; 10</strong></td>
<td><strong>Lesson 7</strong> Remote Exploitation</td>
</tr>
<tr>
<td>7</td>
<td>Remote Attacks</td>
<td>Oct 22 at 8:00 a.m. - Nov 4, 2021 at 11:59 p.m.</td>
</tr>
<tr>
<td></td>
<td><strong>Week 11</strong></td>
<td><strong>Lesson 8</strong> Miscellaneous Topics</td>
</tr>
<tr>
<td>8</td>
<td>Miscellaneous Topics</td>
<td>Nov 5 at 8:00 a.m. - Nov 11, 2021 at 11:59 p.m.</td>
</tr>
<tr>
<td></td>
<td><strong>Week 12 &amp; 13</strong></td>
<td><strong>Lesson 9</strong> Heap Exploitation</td>
</tr>
<tr>
<td>9</td>
<td>Exploiting Heap Bugs</td>
<td>Nov 12 at 8:00 a.m. - Nov 25, 2021 at 11:59 p.m.</td>
</tr>
<tr>
<td></td>
<td><strong>Week 14</strong></td>
<td><strong>Lesson 10</strong> Online In-class CTF</td>
</tr>
<tr>
<td>10</td>
<td>NSA Codebreaker Challenge</td>
<td>Dec 3, 2021 at 11:59 p.m.</td>
</tr>
<tr>
<td></td>
<td><strong>Final exam week</strong></td>
<td>NO FINAL</td>
</tr>
</tbody>
</table>

**Course Materials**

- All content and course materials can be accessed online
- There is no required textbook for this course
- Optional materials:
  
  - **Books & Manuals**
    
    - Phrack Magazine
    - The Shellcoder’s Handbook: Discovering and Exploiting Security Holes
    - Intel Architecture Software Developer Manuals
Staff/TA

- Seulbae Kim, Mingyi Liu
- Feel free to send us an email for support (6265-staff@cc.gatech.edu)

Technology/Software Requirements

- Internet connection (DSL, LAN, or cable connection desirable)
- Adobe Acrobat PDF reader (free download; see https://get.adobe.com/reader/)