Course Syllabus

CS 6265

Information Security Lab: Reverse Engineering and Exploitation Labs

Summer 2020

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).

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.
  o 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
• See Game Rules.
Class website
  • Visit https://tc.gts3.org/cs6265/2020-summer 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.

Attendance Policy
  • This is a fully online course.
  • Login on a regular basis to complete your work, so that you do not have to spend a lot of time reviewing and refreshing yourself regarding the content.

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.

Student Honor Code
  • All degree students should abide by the Georgia Tech Student Honor Code
  • Review the Georgia Tech Student Honor Code: http://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.
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.

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 | May 15, 2020 at 8:00 a.m. |
<p>|            | Lab 1                          | Bomb Lab1                    | May 15 at 8:00 a.m. - May 24, 2020 at 11:59 p.m. |
| Week 2     | Lesson 2                       | Shellcode and x86_64         | May 22, 2020 at 8:00 a.m. |
|            | Lab 2                          | Bomb Lab2 / Shellcode        | May 22 at 8:00 a.m. - May 31, 2020 at 11:59 p.m. |
| Week 3 &amp; 4 | Lesson 3                       | Stack Overflow               | May 29, 2020 at 8:00 a.m. |
|            | Lab 3                          | Stack Overflow               | May 29, 2020 at 8:00 a.m. - Jun 14, 2020 at 11:59 p.m. |
| Week 5     | Lesson 4                       | Bypassing Stack Protections  | Jun 12, 2020 at 8:00 a.m. |
|            | Lab 4                          | Bypassing Stack Protections  | Jun 12 at 8:00 a.m. - Jun 21, 2020 at 11:59 p.m. |
| Week 6     | Lesson 5                       | Bypassing DEP and ASLR       | Jun 19, 2020 at 8:00 a.m. |
|            | Lab 5                          | Bypassing DEP/ASLR           | Jun 19 at 8:00 a.m. - Jun 28, 2020 at 11:59 p.m. |
| Week 7 &amp; 8 | Lesson 6                       | Return-oriented Programming   | Jun 26, 2020 at 8:00 a.m. |</p>
<table>
<thead>
<tr>
<th>Week 9 &amp; 10</th>
<th>Lesson 7</th>
<th>Lab 6</th>
<th>Remote-oriented Programming</th>
<th>Return-oriented Programming</th>
<th>Jun 26 at 8:00 a.m. - Jul 12, 2020 at 11:59 p.m.</th>
<th>Jul 10, 2020 at 8:00 a.m.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lab 7</td>
<td>Lesson 7</td>
<td>Remote Exploitation</td>
<td>Remote Exploitation</td>
<td>Lab 7</td>
<td>Jul 10 at 8:00 a.m. - Jul 26, 2020 at 11:59 p.m.</td>
<td>Jul 10, 2020 at 8:00 a.m.</td>
</tr>
<tr>
<td>Final exam week</td>
<td>NO FINAL</td>
<td>NO FINAL</td>
<td>NO FINAL</td>
<td>Final exam week</td>
<td>NO FINAL</td>
<td>Jul 23 – Jul 30, 2020</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

**Technology/Software Requirements**

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