Western University
Faculty of Engineering
Department of Electrical and Computer Engineering

ECE 9609 / ECE 9069 – Introduction to Hacking: Exploitation and Protection of Systems and Software

Course Outline 2024

Description: Sometimes it seems like every time you read the news there's a story about a new security vulnerability. Have you ever wondered how these vulnerabilities come about, and how they are discovered and exploited? This course will introduce you to basic concepts and techniques used in the exploitation of systems and software (i.e., *hacking*). From activists to cyber criminals to national security agencies, hackers are an inescapable reality of the information age. The goal of this course is, as the saying goes, to know your enemy so that you might defend yourself against them.

Contact Hours: 3 lecture hours, 0.5 course.

Prerequisites: There are no formal prerequisites, however some background in Linux/UNIX, programming, and network protocols is assumed. A previous course in information security and cryptography is recommended (e.g., SE 4472 Information Security or CS 4434A/CS 9636A Network Security).

Course Reference Materials:

This course draws on many resources from around the internet. There is no formal textbook for the course. However, the following titles are a useful reference:

1. Mark Stamp. "Information Security: Principles and Practice." 2/e, John Wiley & Sons. 2011, ISBN: 978-0-470-62639-9
2. Jon Erickson. "Hacking: The Art of Exploitation." 2/e, No Starch Press. 2008, ISBN: 978-1593271442
3. Allen Harper. "Gray Hat Hacking: The Ethical Hacker's Handbook." 3/e, McGraw-Hill Osborne Media. 2011, ISBN: 978-00717425

Learning Objectives:

This course will study software and network vulnerabilities and how they are exploited. We will examine some well-known cases and ask you to share others with us via presentations and the course project. Specific objectives of the course are to:

- Enhance and expand your awareness of cyber threats,
- Develop analytical reasoning to identify behavioural and technological vulnerabilities,
- Stimulate critical thinking about practices and technologies that can lower exposure risk,
- Cultivate a design mentality making systems robust against known and unknown threats.

Lecture Topics:

Roughly the first half of course will be a mixture of formal lectures (see topics below) and case studies of recent hacks. The second half will consist of student presentations.

1. **Hacking Background.** Course introduction, core network and computing concepts (Networking, Command line utilities, File permissions, Programming languages, Web technologies. Capture the Flag challenge.
2. **Cyber Ethics and Vulnerability Scoring**. Ethical and unethical hackers, vulnerability disclosure, vulnerability reporting.
3. **Web security**. Cross site scripting (XSS), SQL injection
4. **Network security**. Network scanning/reconnaissance. Remote exploitation. Software vulnerability and exploit demonstration.
5. **Hacking Systems**. File and OS permissions. Identity, access and privilege. Password hashing.
6. **Hacking software**. Program flow, stacks, buffer overflows, return-oriented programming, shellcode

Evaluation:

<table>
<tr><th rowspan="2">Course Component</th><th rowspan="2">Weight</th><th colspan="2">Mark Breakdown</th></tr>
<tr><th>Component</th><th>Weight</th></tr>
<tr><td rowspan="4">Assignments</td><td rowspan="4">40%</td><td>Assignment 1</td><td>10%</td></tr>
<tr><td>Assignment 2</td><td>10%</td></tr>
<tr><td>Assignment 3</td><td>10%</td></tr>
<tr><td>Assignment 4</td><td>10%</td></tr>
<tr><td rowspan="2">Presentation</td><td rowspan="2">20%</td><td>Research paper seminar series
(ECE 9609 – Research/thesis students only)</td><td>20%</td></tr>
<tr><td>Cyber Tool/Method presentations
(ECE 9069—Course-based masters only)</td><td>20%</td></tr>
<tr><td>CVE Report</td><td>10%</td><td></td><td>10%</td></tr>
<tr><td>Final exam (in-person)</td><td>30%</td><td></td><td>30%</td></tr>
</table>

Collaboration and attribution requirements

- **Assignments**. Students may communicate with each other on ideas and approaches, but solutions must be written in the student's own words.

- **Reports and Presentations**. Students may collaborate and submit jointly authored documents within their group. Reports must be written in the group's own words. Any and all text taken from other sources must be clearly attributed/cited. It is your responsibility to draw a clear distinction between your words and diagrams, and the works of others. Be sure to refer to the section on Cheating and Plagiarism below**.**
- **Use of generative AI.** The use of generative AI (e.g., Chat-GPT) is permitted, however students are expected to author reports in their own words and clearly attribute/cite any use of generative AI. Significant portions of text reasonably suspected of being written by an unattributed generative AI source will be subject to follow-up questions, interviews or additional presentations by the course instructor.

Late Submission Policy: Assignments are due at 11:59pm (Eastern time) on their respective due dates. Assignments will be accepted up to 48 hours late without penalty, however course personnel will not provide assistance with assignments after their respective due dates. Assignments submitted more than 48-hours past its due date will receive a **grade of zero**.

It is your responsibility (a) to know the course due dates, (b) to understand the course late submission policy, and (c) to manage your time appropriately, including building resilience in your schedule against unforeseen delays.

Assignment and Project Submission: Assignments will be submitted on-line via OWL.

***Use of English:** In accordance with Senate and Faculty Policy, students may be penalized up to 10% of the marks on all assignments, tests, and examinations for improper use of English. Additionally, poorly written work with the exception of the final examination may be returned without grading. If resubmission of the work is permitted, it may be graded with marks deducted for poor English and/or late submission.

Class Participation and Attendance: Students are expected to come to class prepared to participate in class discussion about the readings. Any student who, in the opinion of the instructor, is absent too frequently from class, laboratory, or tutorial periods will be reported to the Dean (after due warning has been given). On the recommendation of the department, and with the permission of the Dean, the student will be debarred from submitting the final project in the course.

Absence Due to Illness or Other Circumstances: Students should immediately consult with the instructor or department Chair if they have any problems that could affect their performance in the course. Where appropriate, the problems should be documented (see the attached "Instructions for Students Unable to Write Tests or Examinations or Submit Assignments as Scheduled"). The student should seek advice from the instructor or department Chair regarding how best to deal with the problem. Failure to notify the instructor or department Chair immediately (or as soon as possible thereafter) will have a negative effect on any appeal.

For more information concerning medical accommodations, see the relevant section of the Academic Handbook:

http://www.uwo.ca/univsec/pdf/academic_policies/appeals/accommodation_medical.pdf

For more information concerning accommodations for religious holidays, see the relevant section of the Academic Handbook:
http://www.uwo.ca/univsec/pdf/academic_policies/appeals/accommodation_religious.pdf

Cheating and Plagiarism: Students must write solutions to assignments and exams **in their own words**. Whenever students take an idea or a passage from another author, they must acknowledge their debt both by using quotation marks where appropriate and by proper referencing such as footnotes or citations. University policy states that cheating, including plagiarism, is a scholastic offence. The commission of a scholastic offence is attended by academic penalties, which might include expulsion from the program. If you are caught cheating, there will be no second warning.

All required papers may be subject to submission for textual similarity review to commercial plagiarism-detection software under license to the University for the detection of plagiarism. All papers submitted will be included as source documents on the reference database for the purpose of detecting plagiarism of papers subsequently submitted to the system. Use of the service is subject to the licensing agreement, currently between the University of Western Ontario and Turnitin.com (http://www.turnitin.com).

Scholastic offences are taken seriously, and students are directed to read the appropriate policy, specifically, the definition of what constitutes a Scholastic Offence, in the relevant section of the Academic Handbook:
http://www.uwo.ca/univsec/pdf/academic_policies/appeals/scholastic_discipline_undergrad.pdf

Internet and Electronic Mail: Students are responsible for regularly checking their Western e-mail and the course web site: https://whisperlab.org/hacking and making themselves aware of any information that is posted about the course.

Accessibility: Please contact the course instructor if you require material in an alternate format or if any other arrangements can make this course more accessible to you. You may also wish to contact Services for Students with Disabilities (SSD) at 519-661-2111 ext. 82147 for any specific question regarding an accommodation.

Support Services: Office of the Registrar, http://www.registrar.uwo.ca/
Student Development Centre, http://www.sdc.uwo.ca/
Engineering Undergraduate Services, http://www.eng.uwo.ca/undergraduate/
USC Student Support Services, http://westernusc.ca/services/
Students who are in emotional/mental distress should refer to Mental Health @ Western, http://www.health.uwo.ca/mental_health/, for a complete list of options about how to obtain help.