# Offensive Security & Reverse Engineering (OSRE)

**Your Instructor**

|  |  |
| --- | --- |
| Name | Ali Hadi |
| Website | [www.ashemery.com](https://www.ashemery.com) / @[Champlain.edu](https://www.champlain.edu/academics/our-faculty/hadi-ali) |
|  | |

**Textbook**

None, but you can find below a list of useful books and resources:

* [Introduction To Software Exploits](http://opensecuritytraining.info/Exploits1.html)
* [Exploits 2: Exploitation in the Windows Environment](http://opensecuritytraining.info/Exploits2.html)
* [Hacking Techniques](http://opensecuritytraining.info/HTID.html)
* [Corelan Team Tutorials](https://www.corelan.be/index.php/articles/)
* [Mastering Metasploit, 3rd Edition](https://learning.oreilly.com/library/view/mastering-metasploit-/9781788990615/)
* [The Ghidra Book](https://learning.oreilly.com/library/view/the-ghidra-book/9781098125684/)
* [Reversing: Secrets of Reverse Engineering](https://learning.oreilly.com/library/view/reversing-secrets-of/9780764574818/)
* [Gray Hat Hacking The Ethical Hacker's Handbook, 5th Edition](https://learning.oreilly.com/library/view/gray-hat-hacking/9781260108422/)
* [Penetration Testing with Shellcode](https://learning.oreilly.com/library/view/penetration-testing-with/9781788473736/)
* [Hands-On Penetration Testing on Windows](https://learning.oreilly.com/library/view/hands-on-penetration-testing/9781788295666/)
* [Hacking: The Art of Exploitation, 2nd Edition](https://learning.oreilly.com/library/view/hacking-the-art/9781593271442/)

**Course Description**

This course is about offensive security and applying Red Teaming tactics and techniques. The goal is to exploit software and guide normal program execution to suit offensive needs. If you are interested in exploiting software, controlling operations, and leveraging such footholds within an enterprise’s network, then this course will help you learn that. Sample of topics covered: Windows PE File Format, Fuzzing, Memory Corruption (Server + Client), Limited Buffers and Shellcode Splitting, DLL Injections, Post-Exploitation including Pivoting to Lateral Movement.

**Course Objectives**

1. Understand the basics of Windows PE file format, DLLs, and how functions work
2. Understand reverse engineering and how to reverse software
3. Understand what memory corruption is and how to abuse normal execution flow
4. Learn the basics of Bug Hunting and Fuzzing
5. Understanding the different software Mitigation techniques you might encounter
6. Learn how to use a debugger for software exploitation
7. Learn how to use Metasploit for software exploitation and security testing in general
8. Gain hands-on skills to exploit vulnerable software: Stack, SEH, DEP, etc
9. Learn how to deal with limited buffers that will not fit your shellcode
10. Understand the importance of post-exploitation
11. How to perform tunneling to exploit hidden networks
12. Learn how to create backdoors using manual shell injection

# Course Calendar and outline

The table below outlines the topics covered by the class during the semester. This is a rough course outline and is subject to change. For the latest updated information students should log onto CANVAS. Also, the course is divided into modules not weeks or sessions. Essentially, what this means is we do not have to cover each topic in one session, as some might require less, while others require more than one session (e.g. reverse engineering).

|  |  |
| --- | --- |
| Module | Topic |
| 1 | The Basics (PE Format, DLLs, etc) |
| 2 | Reverse Engineering |
| 3 | Bug Hunting, Memory, How Functions Work, etc |
| 4 | Intro. to Memory Corruption (e.g. Buffer Overflows) |
| 5 | Metasploit “Crash Course” |
| 6 | Mitigation Techniques |
| 7 | SEH and Jumping Strategies |
| 7 | Egg Hunting |
| 8 | Return Oriented Programming (ROP) |
| 9 | Post-Exploitation & Tunneling |
| 10 | Manual Code Injection |
| 11 | **Final Project - CTF** |