|  |  |
| --- | --- |
| Instructor Information | Wade MackeyWade.mackey@temple.edu |
| Office Information | Alter Hall 602 |  |
| Office Hours | By Appointment |
| CRN | 25374 | Section | 1 | Location | Alter 602 | Time | Wednesday 5:30 – 8:00 |

# Course Objectives

In this course you will improve understanding of the process and tools used in Ethical Hacking and Penetration Testing.

The Key subject areas that are covered in the course are:

1. Utilization of the MetaSploit Framework in penetration testing
2. Web Application Hacking with Intercepting Proxies and the WebGoat application
3. Wireless Security and techniques to break wireless security

# Grading

|  |  |
| --- | --- |
| Item | Percentage ofTotal Points |
| Participation | 20% |
| Reports | 30% (15% per report) |
| Test 1 | 15% |
| Test 2 | 15% |
| Test 3 | 20% |
| Total | 100% |

# Participation

Much of your learning will occur as you prepare for and participate in discussions about the course material. The assignments, analysis, and readings have been carefully chosen to bring the real world into class discussion while also illustrating fundamental concepts.

To encourage participation, 20% of the course grade is earned by preparing before class and discussing the topics between and in class. Evaluation is based on you consistently demonstrating your engagement with the material. Assessment is based on what you contribute, not simply what you know.

1. Preparation before class – To facilitate active participation in the class I request that you do the following before noon on the day of the class:

Briefly address and summarize:

* 1. One key point you took from each assigned reading. (One or two sentences per reading)
	2. One question that you would ask your fellow classmates that facilitates discussion.

I will also require that you identify, and are prepared to discuss, an article about a current event in the Ethical Hacking and Penetration Testing arena each week. Each student is expected to contribute a link to an article to the online class discussion each week. An ideal article would be tied thematically to the topic of the week.

However, any article you find interesting and would like to share is welcome. The deadline for posting is noon on the day of class.

1. Participation during class – We will typically start each session with “opening” questions about the assigned readings and analyses. I may ask for volunteers, or I may call on you. Students called on to answer should be able to summarize the key issues, opportunities, and challenges in the analyses. All students should be prepared to answer these questions.

Another important aspect of in-class participation is completion of in-class assignments and contribution to any break out activities.

1. Participation between classes – To facilitate ongoing learning of the course material, we will also discuss course material on the class blog in between class.

You will post analyses to the course website.

The criteria for participation includes attendance, punctuality, level of preparation, professionalism, answering questions, discussing readings, discussing case studies, contributing to group activities, and contributing to a positive learning environment. Recognizing that students sometimes have unavoidable conflicts, the baseline for expected participation is assessed on one less week than the number of assigned weekly write-ups.

# Exercise Analysis

You will officially prepare three analyses reports that are assigned during the semester. For each assignment students are to break into groups and work together to prepare a one to two page report and a presentation of no more than four slides for presentation in the following class. Your analysis should not exceed one single-spaced page using 11 point Times New Roman font with one-inch margins. Do not prepare a separate cover page, instead put your name, the class section number (MIS5212.001), and the analysis in the top-left corner of the header.

To submit your analysis, you must post it on the class blog no later than **Tuesday at 8:00 AM** of the week it is due. Please copy your analysis in clear text onto the blog.

**Late submissions for this deadline will result in no credit earned for this assignment.**

There is no one particular style for a good analysis. But, there are some common elements to excellent submissions (additional, grade-specific criteria are provided at the end of this syllabus):

• The opening of the analysis makes it immediately clear which assignment and what question is being addressed.

• You have cited specific details regarding key facts and issues of the case. Instead of general observations about information technology or organizations that apply to any problem, draw details from the assignment itself. Analyses, observations, and suggestions should be tied directly to those key facts and issues. You can also draw on the other readings in the course to inform and support your arguments.

• After analyzing the details of the analysis, discuss how its specific issues have broader application. In other words, use your analysis to provide some advice to managerial decision-makers that can be applied to other situations beyond this case.

• Provide a balanced perspective. For example, when making a recommendation explain the pros and cons, providing both the rationale (the why) as well as its feasibility (the how). Well-considered recommendations include discussion of potential issues with your solution and conditions that should be in place for your recommendation to be successful.

# Exams

We will have 3 multiple choice question exams. The first one will cover MetaSploit and will comprise 15% of your final grade. The second exam will cover Web Application Hacking Techniques and will comprise 15% of your final grade. The third exam will cover wireless security and include some comprehensive questions from earlier tests and is weighted 20% of your final grade.

|  |
| --- |
| **Readings** |
| 2 | <http://www.offensive-security.com/metasploit-unleashed/Main_Page>Review Fundamentals, Information Gathering, and Vulnerability ScanningRead Exploit Development, Web App Exploit Development, Client Side Attacks and Auxiliary Module Reference |
| 3 | <http://www.offensive-security.com/metasploit-unleashed/Main_Page>Read MSF Post Exploitation, Meterpreter Scripting, Maintaining Access |
| 4 | <http://www.offensive-security.com/metasploit-unleashed/Main_Page>Read MSF Extended Usage and Metasploit GUIs |
| 5 | No Reading Assignment |
| 6 | <http://cdn.ttgtmedia.com/rms/pdf/SearchSecurity.in_Burp_%20Suite_tutorial_Part_01.pdf><http://cdn.ttgtmedia.com/rms/pdf/SearchSecurity.in_Burp_%20Suite_tutorial_Part_02.pdf><http://cdn.ttgtmedia.com/rms/pdf/SearchSecurity.in_Burp_%20Suite_tutorial_Part_03.pdf>We will only use the functionality discussed in the first paper.<http://www.sans.org/reading-room/whitepapers/application/web-application-injection-vulnerabilities-web-app-039-s-security-nemesis-34247><http://www.sans.org/reading-room/whitepapers/application/web-application-security-for-managers-27> |
| 7 | <http://sec4app.com/download/SQL_Injection_Tutorial.pdf> |
| 8 | No Reading Assignment |
| 9 | <https://www.wireshark.org/docs/wsug_html_chunked/ChapterIntroduction.html#ChIntroWhatIs><https://www.wireshark.org/docs/wsug_html_chunked/ChapterUsing.html> (Look through chapter so you are familiar with what you can find) |
| 10 | No Reading Assignment |
| 11 | <http://en.wikipedia.org/wiki/IEEE_802.11>[https://technet.microsoft.com/en-us/library/cc757419(v=ws.10).aspx](https://technet.microsoft.com/en-us/library/cc757419%28v%3Dws.10%29.aspx) |
| 12 | <http://aircrack-ng.org/doku.php?id=getting_started> |
| 13 | No Reading Assignment |

The SANS (System Administration, Networking, and Security) Institute articles are available from the SANS Reading Room at the following link:

<http://www.sans.org/reading_room/>

## Schedule

Date Topic Assignments

|  |  |  |
| --- | --- | --- |
| 1 | Course Introduction, Introduction to the Metasploit Framework including Basics, Intelligence Gathering, Vulnerability Scanning, and Exploitation |  |
| 2 | Meterpreter, Avoiding Detection, Client Side Attacks, and Auxiliary Modules |  |
| 3 | Social Engineering Toolkit, SQL Injection, Karmetasploit, Building Modules in Metasploit, and Creating Exploits |  |
| 4 | Porting Exploits, Scripting, and Simulating Penetration TestingEttercap |  |
| 5 | Test 1, Introduction to OWASP’s WebGoat application |  |
| 6 | Unvalidated Parameters, Broken Access Control, and Broken Authentication | Analysis Report: Learnings from Metasploit run against a publically available VM the student chooses |
| 7 | Cross Site Scripting, Injection Flaws, Error Handling, and Insecure Storage |  |
| 8 | Denial of Service, Configuration Management, and Web Services |  |
| 9 | Ajax Security and an Introduction to the WebGoat ChallengeWireshark |  |
| 10 | Test 2, Introduction to Wireless Security |  |
| 11 | Wireless Recon, WEP, and WPA2 | Analysis Report: Learnings from the WebGoat Challenge |
| 12 | WPA2 Enterprise, Wireless beyond WiFi |  |
| 13 | Cain and Able |  |
| 14 | Test 3 |  |