Special Topics: Network Penetration Testing
CSC 5991 Section 002
Winter 2017
0211 State Hall (STAT)
Saturday 10:00am – 3:00pm
January 14th – March 4th

Faculty Contact Information
Name: Jacob Brabbs
Office Location: N/A
Office Hours: by appointment
Phone: (734) 408-1998
Email: jacob.brabbs@wayne.edu or gi4872@wayne.edu

Course Description
This course is the introductory training in the line of penetration testing courses and certifications. The course helps students gain a valuable skill set in penetration testing by understand the importance of vulnerability assessments and ethical hacking.

The course enables students to understand the importance of vulnerability in Penetration Testing assessments by providing industry knowledge and skills in Penetration Testing. In doing so, the student is able to understand how malware and destructive viruses function. In addition, the course helps students learn how to attack and assess different types of systems and networks.

The course provides in-depth labs that focus on both open source and commercial based tools with industry best practices. These hands on labs emulate real world hacking scenarios and equip the candidate to assess your company’s security posture, help implement controls to better secure your company’s network infrastructure and how to combat against hackers and/or viruses, etc.

The goal of this course is to prepare the student to successfully pass the CPTE exam. In order to do so, the student is expected to be actively engaged in all aspects of the class. The class materials require thorough student review and the labs require substantial hands on time with the software tools presented

Credit Hours
Three (3) Credit Hours
Prerequisite(s)
CSC2200 and CSC2201, both with a grade of “C” or better, or
Graduate standing, or
Instructor approval.

Co-requisite(s)
None

Text Book
Mile2 C)PTE Workbook and materials will be provided to students.

Other Materials
Labs will be conducted using a virtual lab environment provided by Merit and the Michigan CyberRange. Each student will be issued a Merit account. The account information will be emailed to the student after they have registered for the Personal Labs VM environment.

Instructions for registering for the Personal Lab. To connect to the lab environment on the Merit/ Michigan CyberRange, the student will need to use the VMware Horizon Client. It is suggested that each student download the VMware Horizon Client to his or her laptop, so that the student can work with the labs between classes.

Merit specifies these laptop hardware requirements for connecting to the Merit/ Michigan CyberRange:
- x86- or x64-compatible 1.5 GHz CPU Minimum or higher
- DVD Drive (not a CD drive)
- 2 GigaByte RAM minimum with 4 GB or higher recommended
- Ethernet adapter (A wired connection is recommended in class. If your laptop supports only wireless, please make sure to bring an Ethernet adapter with you.)
- 5 GigaByte available hard drive space
- Windows 7 or above is recommended, but most any modern operating system will work fine.
- IE 7 or above, Firefox (most recent version recommended) installed

If you have additional questions about the laptop specifications, please contact the instructor.

Computer Programs
VMware Horizon Client
https://my.vmware.com/en/web/vmware/info/slug/desktop_end_user_computing/vmware_horizon_clients/4_0
Course Contents

This course is closely aligned with the C)PTE exam objectives. The course will cover the following topic areas (dates are tentative and subject to change):

Jan 14th  Review Syllabus and Class Policies
   Module 1 – Business & Technical Logistics of Penetration Testing
   Module 2 – Linux Fundamentals
   Module 3 – Information Gathering – Reconnaissance-Passive
   Appendix 1 - Economics and Law
   Labs Module 3 – Information Gathering: Footprinting and Reconnaissance
   Module 4 - Detecting Live Systems – Reconnaissance-Active

Jan 21st  Module 5 – Enumeration – Reconnaissance-Active
   Module 6 – Automated Vulnerability Assessment
   Labs Module 4 – Detecting Live Systems – Scanning Techniques
   Labs Module 5 - Enumeration

Jan 28th  Module 7 – Malware – Software Goes Undercover
   Module 8 – Assessing and Hacking Windows
   Labs Module 6 – Vulnerability Assessments
   Labs Module 7 – Software Goes Undercover
   Labs Module 8 – System Hacking – Windows Hacking

Feb 4th  Module 9 – Assessing and Hacking UNIX/Linux
   Module 10 – Advanced Assessment & Exploit Techniques
   MidTerm Exam

Feb 11th  Module 11 – Penetration Testing Wireless Networks
   Module 12 – Networks, Sniffing and IDS
   Labs Module 9 – System Hacking – UNIX/Linux
   Labs Module 10 – Advanced Vulnerability & Exploitation Techniques
   In Class Hands On Wireless Hacking Lab
   PenTest Report Project Introduction

Feb 18th  Module 13 – Assessing and Hacking Databases
   Module 14 – Assessing and Hacking Web Technologies
   Module 15 – Report Writing Basics
   In Class Hands On Network Sniffing/ IDS Lab
   Labs Module 13 – Attacking Databases & SQL Injection

Feb 25th  NO CLASS Work on PenTest Report Project

Mar 4th  PenTest Report Project Due
   Module/Lab 16 – Getting Started with PowerShell
   Module/Lab 17 – Using Advanced PowerShell Techniques
   Final Exam
Course Learning Objectives:

The course learning objectives are skills and abilities students should have acquired by the end of the course. Upon successful completion of this class, the student will be able to:

<table>
<thead>
<tr>
<th>#</th>
<th>CSC 5991-1701 Course Learning Objectives</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>describe the importance and benefits of Penetration Testing assessments</td>
</tr>
<tr>
<td>2</td>
<td>describe ethical guidelines and industry best practices for performing Penetration Testing assessments</td>
</tr>
<tr>
<td>3</td>
<td>describe how malware and destructive viruses function</td>
</tr>
<tr>
<td>4</td>
<td>demonstrate familiarity with both open source and commercial based tools used to perform Penetration Testing assessments</td>
</tr>
<tr>
<td>5</td>
<td>demonstrate the knowledge to perform a Penetration Testing assessments</td>
</tr>
<tr>
<td>6</td>
<td>recommend controls to implement to detect and respond to network breaches found in a Penetration Testing assessments</td>
</tr>
<tr>
<td>7</td>
<td>demonstrate the knowledge to prepare a Penetration Test report for senior management</td>
</tr>
</tbody>
</table>

Assessment:

PenTest Report Project 10%
Participation/Attendance: 30%
Midterm Exam: 30%
Final Exam: 30%

Grading Scale:

A: 93-100
A-: 90-92
B+: 85-89
B: 80-84
B-: 75-79
C+: 70-74
C: 65-69
C-: 60-64
F: 0-60
Grading Policies:
Students are expected to not only attend the class sessions, but discuss and analyze the topics presented in class and in the labs.

- Students that attend all sessions and regularly contribute to the course will receive full participation scores.
- Tests for each set of topics will be posted in Blackboard after each class session. Tests will consist of multiple-choice, selection, and essay questions regarding the concepts of the prior session. Unless otherwise noted, tests can be completed at any time up until 11:59 pm the Thursday following the class session.
- The final lab report shall be a vulnerability assessment report to senior management. The vulnerabilities discovered during the lab exercises shall provide the findings of the report. The student shall also include recommendations for mitigating the vulnerabilities.
- The final exam will cover all material in the course, and will be held on the last scheduled day of class. While tailored towards the course content, the final exam is a good indication of the knowledge and details also covered in the C)PTE certification exam.

Final grades may be modified at the instructor’s discretion based on the actual difficulty of the course material.

Religious Holidays:
Because of the extraordinary variety of religious affiliations of the University student body and staff, the Academic Calendar makes no provisions for religious holidays. However, it is University policy to respect the faith and religious obligations of the individual. Students with classes or examinations that conflict with their religious observances are expected to notify their instructors well in advance so that mutually agreeable alternatives may be worked out.

Student Disabilities Services:
- If you have a documented disability that requires accommodations, you will need to register with Student Disability Services for coordination of your academic accommodations. The Student Disability Services (SDS) office is located in the Adamany Undergraduate Library. The SDS telephone number is 313-577-1851 or 313-202-4216 (Videophone use only). Once your accommodation is in place, someone can meet with you privately to discuss your special needs. Student Disability Services' mission is to assist the university in creating an accessible community where students with disabilities have an equal opportunity to fully participate in their educational experience at Wayne State University.
- Students who are registered with Student Disability Services and who are eligible for alternate testing accommodations such as extended test time and/or a distraction-reduced environment should present the required test permit to the professor at least one week in advance of the
exam. Federal law requires that a student registered with SDS is entitled to the reasonable accommodations specified in the student’s accommodation letter, which might include allowing the student to take the final exam on a day different than the rest of the class.

Academic Dishonesty

Academic dishonesty means any activity that tends to compromise the academic integrity of the institution or subvert the education process. All forms of academic misbehavior are prohibited at Wayne State University, as outlined in the Student Code of Conduct (http://www.doso.wayne.edu/student-conduct-services.html). Students who commit or assist in committing dishonest acts are subject to downgrading (to a failing grade for the test, paper, or other course-related activity in question, or for the entire course) and/or additional sanctions as described in the Student Code of Conduct.

- **Cheating**: Intentionally using or attempting to use, or intentionally providing or attempting to provide, unauthorized materials, information or assistance in any academic exercise. Examples include:
  - copying from another student’s test paper;
  - allowing another student to copy from a test paper;
  - using unauthorized material such as a “cheat sheet” during an exam.
- **Fabrication**: Intentional and unauthorized falsification of any information or citation. Examples include:
  - citation of information not taken from the source indicated;
  - listing sources in a bibliography not used in a research paper.
- **Plagiarism**: To take and use another’s words or ideas as one’s own. Examples include:
  - failure to use appropriate referencing when using the words or ideas of other persons;
  - altering the language, paraphrasing, omitting, rearranging, or forming new combinations of words in an attempt to make the thoughts of another appear as your own.
- **Other forms of academic misbehavior include, but are not limited to**: unauthorized use of resources, or any attempt to limit another student’s access to educational resources, or any attempt to alter equipment so as to lead to an incorrect answer for subsequent users;
  - enlisting the assistance of a substitute in the taking of examinations;
  - violating course rules as defined in the course syllabus or other written information provided to the student;
  - selling, buying or stealing all or part of an un-administered test or answers to the test;
  - changing or altering a grade on a test or other academic grade records.

Course Drops and Withdrawals:

In the first two weeks of the (full) term, students can drop this class and receive 100% tuition and course fee cancellation. After the end of the second week there is no tuition or fee cancellation. Students who wish to withdraw from the class can initiate a withdrawal request on Pipeline. You
will receive a transcript notation of WP (passing), WF (failing), or WN (no graded work) at the time of withdrawal. No withdrawals can be initiated after the end of the tenth week. Students enrolled in the 10th week and beyond will receive a grade. Because withdrawing from courses may have negative academic and financial consequences, students considering course withdrawal should make sure they fully understand all the consequences before taking this step. More information on this can be found at http://reg.wayne.edu/pdf-policies/students.pdf.

Student Services:

- The Academic Success Center (1600 Undergraduate Library) assists students with content in select courses and in strengthening study skills. Visit www.success.wayne.edu for schedules and information on study skills workshops, tutoring and supplemental instruction (primarily in 1000 and 2000 level courses).
- The Writing Center is located on the 2nd floor of the Undergraduate Library and provides individual tutoring consultations free of charge. Visit http://clasweb.clas.wayne.edu/writing to obtain information on tutors, appointments, and the type of help they can provide.

Restriction on Recording Class Presentations:

Students need prior written permission from the instructor before recording any portion of this class. If permission is granted, the audio and/or video recording is to be used only for the student’s personal instructional use. Such recordings are not intended for a wider public audience, such as postings to the internet or sharing with others. Students registered with Student Disabilities Services (SDS) who wish to record class materials must present their specific accommodation to the instructor, who will subsequently comply with the request unless there is some specific reason why s/he cannot, such as discussion of confidential or protected information.