Course Catalog Description: This course will address theoretical concepts of operating system security, security architectures of current operating systems, and details of security implementation using best practices to configure operating systems to industry security standards. Server configuration, system-level firewalls, file system security, logging, anti-virus and anti-spyware measures and other operating system security strategies will be examined.

Prerequisites: ITMO456

Credit: 2-2-3 Semester Hours

Lecture/Lab Day, Time & Place: Wednesday 5:30pm – 9:30pm, Rice Campus room RC-244

Schedule of Topics/Readings: All readings should be done prior to class.

<table>
<thead>
<tr>
<th>Class Session</th>
<th>Date</th>
<th>Topic/Lab</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>January 14</td>
<td>Overview</td>
</tr>
<tr>
<td>2</td>
<td>January 21</td>
<td>Malicious Software</td>
</tr>
<tr>
<td>3</td>
<td>January 28</td>
<td>Malicious Attacks</td>
</tr>
<tr>
<td>4</td>
<td>February 4</td>
<td>User Authentication &amp; Access Control</td>
</tr>
<tr>
<td>5</td>
<td>February 11</td>
<td>Cryptographic Tools</td>
</tr>
<tr>
<td>6</td>
<td>February 18*</td>
<td>Host Based Intrusion Detection – Part 1</td>
</tr>
<tr>
<td>7</td>
<td>February 25*</td>
<td>Host Based Intrusion Detection – Part 2</td>
</tr>
<tr>
<td>8</td>
<td>March 4</td>
<td>Midterm Exam</td>
</tr>
<tr>
<td>9</td>
<td>March 11</td>
<td>System Firewalls</td>
</tr>
<tr>
<td>10</td>
<td>March 18</td>
<td>NO CLASS – Spring Break</td>
</tr>
<tr>
<td>11</td>
<td>March 25</td>
<td>OS agnostic hardening</td>
</tr>
<tr>
<td>12</td>
<td>April 1</td>
<td>Linux Hardening</td>
</tr>
<tr>
<td>13</td>
<td>April 8</td>
<td>Windows Hardening</td>
</tr>
<tr>
<td>14</td>
<td>April 15</td>
<td>Secure Communication</td>
</tr>
<tr>
<td>15</td>
<td>April 22</td>
<td>Post OS Hardening Testing</td>
</tr>
<tr>
<td>16</td>
<td>April 29</td>
<td>Review and Lab Time</td>
</tr>
<tr>
<td>17</td>
<td>May 6</td>
<td>Final Exam</td>
</tr>
</tbody>
</table>

* Out of town for work – lectures supplemented via pre-recorded video

Course Materials:
- Windows 8.1 system
- Ubuntu Linux
- Miscellaneous Bootable Linux Distributions
- VMware Workstation/Fusion (available on Microsoft Dreamspark [http://www.itm.iit.edu/dreamspark/](http://www.itm.iit.edu/dreamspark/)) or Oracle VirtualBox ([https://www.virtualbox.org/](https://www.virtualbox.org/))

Course Objectives:
Each successful student will be able to describe the different types of malicious threats targeted to an operating system. The student will be able to explain ways to mitigate these threats, correct vulnerable configurations, and use best practices to harden systems. This course and the concepts described in the class cover topics included on the Certified Information Systems Security Professional (CISSP). The GIAC Security Essentials (GSEC) certification is another recognized security certification that covers the concepts the student will learn throughout this course.
Graduate Plagiarism Academic Honesty:

Examination:

Undergraduate Research Paper:

Late Assignments:

Labs:

Spring 2015 Syllabus

Course Notes: Copies of the course lecture notes in the form of a PDF of the PowerPoint presentation accompanying each lecture will be provided for each student on Blackboard. This should be useful if you must miss a class. You should be aware that note taking is encouraged and should help your understanding of the material.

Readings: Readings for the class will be assigned in the form of online reading and provided lectures. All readings should be done before coming to class on the assigned date, and are mandatory and expected. Generally if you do the readings you will excel in the course, as the lectures serve as a clarification and explanation of material you should already be familiar with. Completion of reading may be verified by quizzes. Specific readings are assigned by topic above.

Attendance: As this is a live laboratory class and demonstrations of operating system security and functions are a key part of the class, attendance is critical. If you will not be able to attend class, please notify the instructor via email prior to class time. It is possible to arrange for absences in advance but they must be arranged by discussion with the instructor in advance.

Security Topic: Each student is required to find a current topic related to system security and submit the finding to blackboard under the discussion section for that week. The topic can be a new exploit or vulnerability or security solution. At the beginning of class, it is expected that you will talk about the topic. The discussion should be anywhere from 3-5 minutes in length. Duplicate topics not permitted, so look in the discussion area on blackboard before committing to a topic.

Labs: Each lab may include questions to ensure that the necessary skills have been mastered. There will be a lab with each lesson; all labs must be completed to receive full credit. Lab reports will be submitted via the Blackboard assignments page. Lab reports will contain answers to any questions and screenshots and will be due at the second class following the assignment.

Late Assignments: Late submissions are at my discretion and must be requested via email or in person. Any late assignments that are not approved by me will result in a 0 for that assignment.

Research Paper:

Graduate: A research paper addressing a topic in operating system security. The paper can be a solution to a problem related to operating system security, a business, or management issue resulting from or relating to system security, a discussion of system security management strategy, or a case study. The paper will be 15-20 pages, double spaced using 12 point font. Please reference http://www.itm.iit.edu/resources/paperguidelines.php for some guidelines and content of the paper

Undergraduate: A research paper addressing a topic in operating system security. The paper can be a solution to a problem related to operating system security, a business, or management issue resulting from or relating to system security, a discussion of system security management strategy, or a case study. The paper will be 5-10 pages, double spaced using 12 point font. Please reference http://www.itm.iit.edu/resources/paperguidelines.php for some guidelines and content of the paper

Examination: The midterm and final examination will consist of multiple choice, fill-in-the-blank, short answer, and short essay questions to demonstrate mastery of the material covered and to reflect preparation to pass a certification exam on this material. Questions will be based on the learning objectives for each topic. For the final exam only, you may have 1 page of notes front and back.

Academic Honesty:

Plagiarism: All work you submit in this course must be your own. You must fully attribute all material directly quoted in papers and you must document all sources used in the preparation of the paper using complete, APA-style bibliographic entries. Including directly quoted material in an assignment without attribution is always plagiarism and will always be treated as such by me. No more than thirty-three percent of material included in any paper may be direct quotes. If you submit plagiarized material you WILL receive a grade of ZERO for the assignment, an Academic Honesty Violation Report will be filed, and it may result in your expulsion from the course with a failing grade as per the IIT and ITM academic honesty policies. There is no excuse for not understanding this policy and if you do not understand it please let me know and I will be happy to discuss it with you until you do.

Collaboration: Students may only collaborate on assignments or projects that are explicitly designated as group assignments or projects. Students submitting work that is identical or in some cases even substantively the same will be asked to discuss the assignment with me. If one student admits to having copied the work, or if there is clear evidence who is guilty, the guilty student will be assigned a grade of zero. If no one admits to the offense or a reasonable determination of guilt cannot be made, each student...
involved will be assigned a grade of zero. In either case, an Academic Honesty Violation Report will be filed, and it may result in your expulsion from the course with a failing grade as per the IIT and ITM academic honesty policies.

Disabilities: Reasonable accommodations will be made for students with documented disabilities. In order to receive accommodations, students must obtain a letter of accommodation from the Center for Disability Resources and make an appointment to speak with me as soon as possible. My office hours are listed on the first page of the syllabus. The Center for Disability Resources (CDR) is located in 3424 S. State St., room 1C3-2 (on the first floor), telephone 312.567.5744 or disabilities@iit.edu.

Grading: Grading criteria for ITMS 458/558 students will be as follows:

- **A**
  - Outstanding work reflecting substantial effort ................................................................. 90-100%
- **B**
  - Undergraduate/IT Students: Excellent work reflecting good effort ......................... 80-89.99%
  - Graduate Students: Satisfactory work fully meeting expectations ......................... 80-89.99%
- **C**
  - Undergraduate/IT Students: Satisfactory work meeting minimum expectations ....... 70-79.99%
  - Graduate Students: Substandard work not meeting expectations ............................. 65-79.99%
- **D**
  - Undergraduate/IT Students: Substandard work not meeting expectations .......... 60-69.99%
  - Graduate Students: Graduate students may not be assigned a D grade ....................... N/A
- **E**
  - Undergraduate/IT Students: Unsatisfactory work ..................................................... 0-59.99%
  - Graduate Students: Unsatisfactory work ................................................................. 0-64.99%

The final grade for the class will be calculated as follows:

- Labs ........................................................................................................................................ 45%
- Research Paper ......................................................................................................................... 15%
- Midterm Exam ............................................................................................................................. 15%
- Final Exam .................................................................................................................................. 15%
- Class Participation/Security Topic ............................................................................................... 10%

Other Class Resources: Online readings and other class resources are on http://blackboard.iit.edu.

Our Contract: This syllabus is my contract with you as to what I will deliver and what I expect from you. If I change the syllabus, I will issue a revised version of the syllabus; the latest version will always be available on Blackboard. Areas with changes will be indicated by a black bar in the right-hand margin of the page.

Computer Labs: Class will be held in room RC-244 at IIT's Rice Campus, a lab administered by the IIT School of Applied Technology Technical Services. Each student will be assigned to a particular PC and will use the same system for the duration of the course. Your operating system will be on a removable hard drive which may be available for checkout from the instructor for lab use outside of class meeting times.

PC Shutdowns: Please turn off the monitor and properly shut down the computer at the end of each class.

Computer Use Policies: Please ensure that you have read and understand the IIT and ITM Network and Computer Use Policies found at http://www.itm.iit.edu/data/ITMComputerUsePolicies.pdf.