Syllabus for CYB 750
Offensive Security & Threat Management

NOTE: This syllabus document contains the basic information of this course. The most current syllabus is available in the full course.

Course Description
This course includes active defenses such as penetration testing, log management, hacking, threat management and system posturing. Students completing this course will have an understanding of, and the ability to preemptively secure computer and network resources by utilizing information about threats, actors and attack vectors and the ethics behind using this data.

Prerequisite(s)
CYB 700: Fundamentals of Cybersecurity
CYB 703: Network Security

Course Outcomes
Upon completing this course, you will be able to do the following:
• Evaluate offensive security processes
• Discuss the strengths and weaknesses of an offensive security program
• Evaluate the ethics of offensive security choices
• Create reporting and documentation that identifies actionable security concerns
• Create red team exercises

Course Requirements/Components
Case Study Discussions
There are two discussions in this course. In these discussions you will share views and interpretations of extensive, real-world cybersecurity incidents.

Assignments
There are six assignments in this course. These assignments will provide you with the opportunity to practice working with customers, including threat modeling, scoping, and determining rules of engagement for red team exercises.

Penetration Testing Labs
There are six labs in this course. Hone your technical skills by completing red team exercises in the virtual lab.
Documentation Projects
There are three projects in this course. Practice and refine your documentation skills by developing various industry-standard documents.

Course Outline
Module 01:
  • Current cyber threat landscape
Module 02:
  • Emulating attacker tactics and techniques
Module 03:
  • Rules of engagement
Module 04:
  • Scoping
Module 05:
  • Report writing
Module 06:
  • Report writing, part 2
Module 07:
  • Recon and scanning
Module 08:
  • Initial access
Module 09:
  • Initial access via exploitation
Module 10:
  • Maintain and elevate
Module 11:
  • Lateral movement and action on objective
Module 12:
  • Ethical hacking
Module 13:
  • Beyond servers and workstations
Module 14:
  • Niche offensive security skills
Module 15:
  • Further application and continuing education
Grading
The following grading scale will be used to evaluate all course requirements and to determine your final grade:

<table>
<thead>
<tr>
<th>Grade</th>
<th>Percentage Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>90% or greater</td>
</tr>
<tr>
<td>A-</td>
<td>87% - &lt; 90%</td>
</tr>
<tr>
<td>B+</td>
<td>83% - &lt; 87%</td>
</tr>
<tr>
<td>B</td>
<td>80% - &lt; 83%</td>
</tr>
<tr>
<td>B-</td>
<td>77% - &lt; 80%</td>
</tr>
<tr>
<td>C+</td>
<td>73% - &lt; 77%</td>
</tr>
<tr>
<td>C</td>
<td>70% - &lt; 73%</td>
</tr>
<tr>
<td>C-</td>
<td>65% - &lt; 70%</td>
</tr>
<tr>
<td>F</td>
<td>0 - &lt; 65%</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Assignment</th>
<th>Points</th>
</tr>
</thead>
<tbody>
<tr>
<td>Discussions: 2, 20 points each</td>
<td>40</td>
</tr>
<tr>
<td>Assignments: 6, 20 points each</td>
<td>120</td>
</tr>
<tr>
<td>Labs: 6, 100 points each</td>
<td>600</td>
</tr>
<tr>
<td>Projects: 3, 100 points each</td>
<td>300</td>
</tr>
<tr>
<td>Total Points</td>
<td>1060</td>
</tr>
</tbody>
</table>