ISM 326: Ethical Hacking
Fall 2019
Instructor: Dr. Hamid R. Nemati
Office: 425 Bryan Building
Voice Mail: 334-4993
E-Mail: nemati@uncg.edu

CATALOG DESCRIPTION:
Ethical hacking is presented as a process of intentionally attempting to hack a computer system to understand potential vulnerabilities that a malicious hacker could exploit and find ways to mitigate them.

COURSE OBJECTIVES:
This course prepares students to work as computer security professional by teaching the fundamentals of ethical hacking. It prepares students to pass the EC-Council Certified Ethical Hacker (CEH) certification exam.

STUDENT LEARNING OUTCOMES (SLOs):
Upon successful completion of this course, students should be able to define, describe, identify, and protect systems from threats involving:
- Footprints and scanning
- Enumeration and system hacking
- Malware
- Sniffers, session hijacking, and denial of service
- Web server hacking, web application attacks, and database attacks
- Wireless security attacks
- IDS, firewalls, and honeypots
- Physical security and social engineering
- Cryptographic attacks and defenses
- Cloud computing and botnets

PREREQUISITES: ISM 280 and ISM 201

REQUIRED COURSE MATERIALS:
ISBN 10: 0-7897-5691-9
You need to purchase e-version of the book and the learning environment:
https://www.ucertify.com/cart/?order=0185A&ref=&add_order=1

METHOD OF INSTRUCTION:
This class includes lecture and class discussion, demonstrations, and hands-on practice. Student participation is encouraged and mandatory in required assignments and practical demonstrations, including both individual and group tasks.
**ESTIMATED TIME PER FOR ONLINE TASKS**
- 15 minutes per pre-chapter quiz
- 60 – 120 minutes per chapter (reading)
- 30 to 60 minutes per exercise or lab
- 30 minutes per end-of-chapter-quizzes review questions set

**GRADING SYSTEM:**

<table>
<thead>
<tr>
<th>Graded Element</th>
<th>Maximum Points</th>
</tr>
</thead>
<tbody>
<tr>
<td>End of Chapter Quizzes</td>
<td>300 (30%)</td>
</tr>
<tr>
<td>Labs</td>
<td>300 (30%)</td>
</tr>
<tr>
<td>Exams</td>
<td>200 (20%)</td>
</tr>
<tr>
<td>Final Project</td>
<td>200 (20%)</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>1000</strong></td>
</tr>
</tbody>
</table>

The course will be letter graded. Letter Grades and Points are based on the following:


**COURSE DELIVERABLES:**
Details about course deliverables, including EOC quizzes, Labs, and Exams due dates are found online. All such deliverables submitted after the due date may not be accepted unless extenuating circumstances can be documented. In such cases, they are subject to a grading penalty of a minimum of 20% reduction for each day late.

**POLICY ON SERVER UNAVAILABILITY OR OTHER TECHNICAL DIFFICULTIES:**
The university is committed to providing a reliable online course system to all users. However, in the event of any unexpected server outage or any unusual technical difficulty which prevents students from completing a time sensitive assessment activity, the instructor will extend the time windows and provide

**ELECTRONIC MAIL AND ACCOUNTS:**
You should check your UNCG email and Canvas Course link regularly as I may send email updates or add new info on Canvas on an ongoing basis. You will be responsible for any information or announcements contained in the email messages or updates on Canvas.

**ACADEMIC INTEGRITY, ETHICAL ISSUES AND THE HONOR CODE POLICIES:**
Students are responsible for becoming familiar with the UNCG’s Academic Integrity Policies that are strictly enforced in this class. You may UNCG’s Academic Integrity Policies at this web site at http://academicintegrity.uncg.edu.
**Weekly Course Outline**

<table>
<thead>
<tr>
<th>Week</th>
<th>Topics</th>
<th>Reading and Questions</th>
</tr>
</thead>
</table>
| 1    | Chapter 1: *Introduction to Ethical Hacking*  
  • Security fundamentals  
  • Security testing  
  • Hacker and cracker descriptions  
  • Ethical hackers  
  • Test plans  
  • Ethics and legality  | Read pp. 2-35  
  Review questions 1-20, pp. 37-42 |
|      | VirtualBox  
  Kali Linux  | Read VirtualBox User Manual  
  Read Kali Linux Tutorial and Kali Linux Tools Description |
| 3    | Chapter 2: *Technical Foundations of Hacking*  
  • The attacker’s process  
  • The ethical hacker’s process  
  • Security and the stack  | Read pp. 44-76  
  Review questions 1-20, pp. 80-84 |
| 4 & 5| Chapter 3: *Footprinting and Scanning*  
  • The 7-step information-gathering process  
  • Identifying active machines  
  • OS fingerprinting  
  • Mapping the network attack surface  | Read pp. 86-137  
  Review questions 1-20 pp. 142-146 |
| 6    | Chapter 4: *Enumeration and System Hacking*  
  • Enumeration  
  • System hacking  | Read pp. 148-186  
  Review questions 1-20, pp. 189-193 |
| 7 & 8| Chapter 5: *Malware Threats*  
  • Viruses and worms  
  • Trojans  
  • Covert communication  
  • Keystroke logging and spyware  
  • Malware countermeasures  | Read pp. 194-239  
  Review questions 1-20, pp. 270-272 |
| 9 & 10| Chapter 6: *Sniffers, Session Hijacking, and Denial of Service*  
  • Sniffers  
  • Session hijacking  | Read pp. 248-290  
  Review questions 1-20, pp. 293-297 |

---

1 This schedule is tentative, and changes may be required during the semester.
<table>
<thead>
<tr>
<th>Chapter</th>
<th>Title</th>
<th>Topics</th>
<th>Additional Information</th>
</tr>
</thead>
</table>
| 11      | Chapter 7: **Web Server Hacking, Web Applications, and database Attacks** |  - Denial of service  
          - Distributed denial of service  | Read pp. 298-345  
                                            Review questions 1-20, pp 347-352 |
| 12 & 13 | Chapter 10: **Physical Security and Social Engineering** |  - Web server hacking  
          - Web application hacking  
          - Database hacking  | Read pp. 440-473  
                                            Review questions 1-15, pp. 475-478 |
| 14      | Chapters 8: **Wireless Technologies, Mobile Security, and Attacks** |  - Wireless technologies  
          - Mobile security  
          - Wireless LANs  | Read pp. 354-390  
                                            Review questions 1-15, pp. 391-394 |