

Course Number	CS 409	Course Title	Ethical Hacking				
Semester Hours	3	Course Coordinator	Henry Hexmoor				
Catalog Description	This course will explore the various means that an intruder has available to gain access to computer resources. We will investigate weaknesses by discussing the theoretical background, and whenever possible, actually performing the attack. We will then discuss methods to prevent/reduce the vulnerabilities. This course is targeted specifically for Certified Ethical Hacking (CEH) exam candidates, matching the CEH exam objectives with the effective and popular Cert Guide method of study.						
Textbooks							
Certified Ethical Hacker (CEH) Cert Guide Network Defense, Michael Gregg. Pearson IT Certification. ISBN-10: 0789751275 • ISBN-13: 9780789751270							
References							
Course Learning Outcomes							
<ul style="list-style-type: none"> Analyze security vulnerabilities of a network and develop a set of solutions for specific networking scenarios. Identify security tools including, but not limited to intrusion detection and firewall software. Exhibit an understanding of the threats posed by viruses to networks through the development of appropriate protection plans. Find and utilize available online resources as they pertain to developing a secure system. Develop comprehensive plans for network security using a full range of available tools. Prepare students for Ethical Hacking Certification (CEH) exam. 							
Assessment of the Contribution to Student Outcomes							
Outcome →	1	2	3	4	5	6	
Assessed →	X	X	X	X	X	X	
Prerequisites by Topic							
CS 202 or equivalent							

Major Topics Covered in the Course

1. Ethical hacking basics (5 lectures)
2. Technical foundations of hacking (2 lectures)
3. Footprinting and scanning (2 lectures)
4. Enumeration and system hacking (3 lectures)
5. Linux distros and automated assessment tool (2 lectures)
6. Trojans and backdoors (1 lecture)
7. Sniffers, session hijacking, and denial of service (3 lectures)
8. Web server hacking, web applications, and database attacks (2 lectures)
9. Wireless technologies, mobile security, and mobile attacks (3 lectures)
10. IDS, firewalls, and honeypots (2 lectures)
11. Buffer overflows, viruses, and worms (2 lectures)
12. Cryptographic attacks and defenses (8 lectures)
13. Physical security and social engineering (5 lectures)