COMP-4723 Course Syllabus

1 Course Information

Course Name	COMP-4723: Ethical Hacking
Prerequisites	COMP-4006
Required Textbook	No textbook required

2 Course Description

This course introduces students to the adversarial mindset essential for modern cybersecurity practitioners. By approaching security from the attacker's point of view, students learn how real-world intrusions occur and how to defend against them. The course covers foundational security principles, ethical considerations in hacking, reconnaissance and vulnerability discovery methods, exploitation techniques, network and application-layer attacks, wireless intrusions, and defensive strategies. Through hands-on practice with standard tools and platforms, students develop both offensive and defensive skills necessary for navigating today's complex cybersecurity landscape.

- Fundamentals of computer security (CIA, etc.)
- Ethical hacking: what makes it ethical?
- Networking overview and the steps involved in the hacking process
- Information gathering: target identification, network discovery
- Reconnaissance and network scanning, tools and techniques (DNS scanning and enumeration, port scanners, public information databases)
- Fingerprinting and vulnerability discovery/vulnerability analysis
- Vulnerability exploitation, gaining a foothold
- Tools and techniques for exploiting vulnerabilities (known exploits, new exploits, vulnerability databases, CWE/CVE, MITRE, NIST)
- Metasploit, Kali: open source vulnerability discovery and exploitation
- Manual exploitation, buffer overflow to RCE, ROPs and gadgets

- Automated vulnerability discovery, OpenVAS (Greenbone) for defense and low-hanging fruit
- Kali tools to assist in automating vulnerability discovery and analysis
- Honing your skills: vulnhub, hackthebox, etc.
- Network hacking (ARP spoofing, evil DHCP, WiFi spoofing, MAC attacks)
- Application layer attacks (injection attacks, web vulnerability, file inclusion, request forgery, etc.)
- Persistence: gaining and maintaining access (reverse shells, malware, RATs, process hiding and injection, etc.)
- Wireless attacks (cracking wireless networks)
- Defense and research: firewalls, intrusion detection systems, honeypots

3 Textbook and Materials

No textbook is required for this course. The course follows the progression of a number of ethical hacking certifications, including the Certified Ethical Hacker (CeH) and the Offensive Security series on Kali penetration testing. Neither of those certificates are the focus of this class, but purchasing materials related to these certifications can be used as a reference for the material covered in this course.

You will need a good internet connection and a laptop that meets DU specifications. (See `https://www.du.edu/it/support/how-to/students/laptops`). For technical support in using Canvas, please go to `http://otl.du.edu/knowledgebase/canvas`

3.1 Other Stuff

- Reliable access to a computer and the Internet. If you are online you can turn your homework in from wherever in the world you are!
- Wireshark, which is freely available. You will need to install this and make sure it's working on your computer.
- Basic virtualization: we'll be installing and using multiple layers of virtualization (primarily VMWare based) in this course. We will walk you through it, but if you don't know what virtualization is, look it up.
- AI usage: the purpose of this course is to provide you fundamental knowledge of security/networking/ethical hacking. While AI use is allowed, knowledge will be tested using in-person questions, paper-based quizzes and paper-based exams. These make up a significant portion of your grade, so you are going to need to *understand* the basics.

4 Course Learning Objectives

This course provides an in-depth understanding of how to protect computers and networks by first studying how adversaries think and operate. Students learn ethical hacking methodologies, hands-on penetration testing tools, and the legal and ethical frameworks that govern responsible security work. The class explores the role of ethical hackers in safeguarding organizations and governments, examines major vulnerability resources, and highlights federal and state computer crime laws. By engaging with both offensive and defensive security concepts, students gain the skills necessary to analyze vulnerabilities, understand emerging threats, and responsibly apply cybersecurity techniques in real-world environments.

- Know the basics of networking and network security
- Recognize the difference between ethical/legal hacking and unauthorized/illegal hacking, and to never perform hacking without permission
- Have a firm basis upon which to consider attaining a penetration testing certificate (e.g., CEH or PEN-200)
- Be able to build a system for ethical hacking/penetration testing, and understand the tools and resources for doing so
- Know how to perform network discovery, enumeration, and fingerprinting of a target
- Understand the tools and techniques used by ethical and unethical hackers for white hat or defense
- Possess the skills to perform vulnerability analysis of a target, in automated or manual fashion
- Have a level of understanding to start participating in CTF events for ethical hacking practice
- Be able to analyze and triage a vulnerability scan, as well as identify its potential weaknesses
- Know how and where to stay up to date on the latest in security updates, vulnerabilities, and breaches

5 Course Outcomes

The high level objectives of this course are as follows:

1. Analyze networked systems to **gather, identify and interpret** reconnaissance data, including enumeration results and vulnerability indicators.
2. Evaluate the **severity, relevance, and potential impact** of vulnerabilities using both automated scanning tools and manual assessment techniques.

3. Apply ethical hacking methodologies to safely execute controlled exploitation exercises within an authorized lab environment.

4. Create and configure a functional penetration-testing environment using industry-standard tools and document the methodology.

5. Distinguish between *legal, ethical, and unauthorized* hacking activities by referencing applicable federal and state regulations, and modern ethical considerations.

6. Synthesize information from major security intelligence sources (e.g., CVE, NVD, MITRE ATT&CK) to stay informed on emerging vulnerabilities and threats.

7. Produce clear, professional reporting that communicates assessment findings, exploitation steps, and prioritized remediation strategies.

6 Program Level Goals

Courses in the cyber security MS program, including this one, should contribute to overall program level outcomes for students. This course contributes to the following program level goals:

1. **Demonstrate a *basic* understanding of networking and network security.**

2. **Understand how modern operating systems work (with a leaning towards Unix style OSes).**

3. **Provide a *basic* understanding of core computer security concepts (CIA triad).**

4. **Explain the legal and ethical ramifications of malicious cyber activities, and have an awareness of their responsibilities when working in this field.**

5. **Take on the role of an attacker (with respect to penetration testing/red teaming) and be familiar with the tools used by ethical hackers in ascertaining the security of a system or network of systems.**

7 Knowledge Units

This course covers the following NSA cybersecurity Knowledge Units:

1. IT Systems Components (ISC, Foundational CDE)

2. Basic Networking (BNW, Core Technical CDE)

3. Network Defense (NDF, Core Technical CDE)

4. Advanced Network Technology and Protocols (ANT, Optional KU)

5. Systems Programming (SPG, Optional KU)

8 Attendance Policy

Regular attendance is expected. Students are responsible for all material covered in class, including announcements and handouts.

9 Academic Integrity

All work submitted for this course must be the student's own original work. Any instance of plagiarism or cheating will be dealt with according to the university's academic integrity policy. Refer to the Student Rights and Responsiblities, as well as the University of Denver Student Honor code, here: `https://studentaffairs.du.edu/student-rights-responsibilities`

10 Disability Services

If you have a disability that may affect your ability to complete the work for this course, please contact the Disability Services office at: `https://studentaffairs.du.edu/disability-services-progr`