DRAFT CSCE 5653 Network Security

**Catalog Description**

This course will be focused on understanding and applying foundational principles in security to real computer networks. We will study and implement several real attacks and take advantage of several recreated vulnerable systems in order to understand the modern landscape of network security. Other than implementing our own attacks, we will also be looking at various case studies of attacks and defense strategies, including known exploit proofs-of-concept, published papers, and documents from security agencies and cyber-security research firms.

**Prerequisites**

* It is assumed that the students are familiar with some programming languages, such as C, C++, Java, or Python.
* It is recommended that the students have a reasonably good background in computer networks.

**Textbook**

There is no required textbook. We suggest several texts.

* Computer & Internet Security: A Hands-on Approach, Second Edition, Wenliang Du,   
  ISBN: 978-1733003926 (hardcover) and 978-1733003933 (paperback)
* PoC||GTFO   
  <https://www.oreilly.com/library/view/pocgtfo/9781492067528/>
* MIT’s list on Computer Systems Security <http://css.csail.mit.edu/6.858/2019/reference.html>
* Security Engineering: A Guide to Building Dependable Distributed System, Ross J. Anderson  
  <https://www.cl.cam.ac.uk/~rja14/book.html>
* Hands-On Ethical Hacking and Network Defense, Michael T. Simpson, Nicholas Antill, 3rd Edition, 2016, Cengage Learning, ISBN: 987-1-285-45467-2

**Student Learning Outcomes**

By the end of this course, students will be able to:

* Gain a deep understanding of issues, concepts, threats, operational challenges as well as solutions in securing systems and networks
* Explore a range of existing problems and tensions in modern network security
* Use offensive cybersecurity tools to attack computer and network systems to understand how to defend against attacks
* Evaluate the threats to a computer or network system
* Learn real-world security principles through hands-on practices and tools to assess, defend, and investigate systems and networks

**Topics covered**

The course is organized into multiple cycles and each cycle will focus on one topic in network security from theory to practice. We will first study the theory behind various attack vectors as well as countermeasures, and then gain deep insights through hands-on construction and experimentation with real-world implementations.

* Network basics and security introduction (1 week)
* Network attacks (2.5 weeks)
* Unwanted traffic (e.g., DoS, spam, malware) (1.5 weeks)
* Web security (1.5 weeks)
* Network defense (1.5 weeks)

**Grading (tentative)**

Course grades will be determined by these weights:

Participation: 10%

Lab assignment: 45%

Quiz: 20%

Exam: 25%

**Academic Dishonesty Policy**

As a core part of its mission, the University of Arkansas provides students with the opportunity to further their educational goals through programs of study and research in an environment that promotes freedom of inquiry and academic responsibility. Accomplishing this mission is only possible when intellectual honesty and individual integrity prevail. Each University of Arkansas student is required to be familiar with and abide by the university’s ‘Academic Integrity Policy' at honesty.uark.edu/policy. Students with questions about how these policies apply to a particular course or assignment should immediately contact their instructor.

**Ethics and Responsibilities**

In this class, we will apply both offensive and defensive security techniques to non-production hardware/software systems. Every student must act responsibly adhering to the University of Arkansas Code of Computing Practices and the Computer and Network Security Policy.

**Prepared by**: Kevin Jin **Date**: 2/1/2021