1. **CS 444, Introduction to Cybersecurity**

2. **3 Credits:** Lecture 1 hour 15 min 2x/week.

3. **Instructor:** Ian Burres

4. **Textbook**: *Computer Security: Art and Science*, Matt Bishop, 2002. *Gray Hat Hacking, 2nd ed: The Ethical Hacker's Handbook,* Shon Harris, Allen Harper, Chris Eagle, and Jonathan Ness, 2007

5. **Course Description:** This class will focus on concepts and procedures relevant to the field of cybersecurity. Special emphasis will be placed on policies, risk management, attack vectors, and mitigation techniques. Students will also be exposed to ethical hacking techniques involving hands-on lab projects and quizzes. Though helpful, a background in computer programming is not a prerequisite for the course since the instructor will provide the necessary instruction to complete any programming related assignments (which will mostly consist of small scripts written to help automate certain cybersecurity procedures. Grades will be based on class participation, quizzes and exams, and hands-on lab activities.

Prerequisites or co-requisites: None.
Required, elective, or selected elective: Elective Course

6. **Specific outcomes of instruction:** At the completion of this course students will be able to:

Understand how abstractions and concepts of computer and network security and privacy apply to specific contemporary problems. Understand how to create and interpret security policies, baselines, and standards. Be familiar with the NIST Special Publication (SP) 800 series. Understand risk management principles and security governance frameworks. Understand basic networking fundamentals, to include OSI, TCP/IP, and OPsec. Understand attack vectors and known mitigation techniques. Become familiar with tools (like Kali Linux) used by cybersecurity personnel and specific job titles associated with the profession (ie. Ethical hacker, penetration tester, etc.). Understand the basic principles of programming and how to apply said understanding in the development of scripts. Understand cryptographic mechanisms and how to effectively apply them. Students will also have some exposure to intel x86/x64 assembly language, C, and Python.

7. **Assessed outcomes:** Basic understanding of network structures and protocols. Detailed understanding of security policies, ethics and laws, and risk management. Detailed understanding of potential attack vectors, threats, vulnerabilities, and mitigation techniques. Basic familiarity with security tools and scripting.

8. **Assignments:**

- (**4**) Exams approximately every 3 weeks
- (**8**) quizzes approximately 1-per week, except when taking exams
- (**4**) Hands-on labs to help reinforce content
- (**4**) short scripting/programming assignments)

A note on labs and scripting assignments: You will be able to complete the labs remotely, but you will be required to take snapshots of your results. The programming assignments will be easy enough for someone with little to no programming experience to complete. I promise they will be fun and enlightening.

Exams will only cover the content associated with the previous three weeks of instruction. If you do well on the quizzes, you should have no problems with the exams.

9. **Grading Rubric:**

Category	**Percent of Grade**
Participation	**10%**
Quizzes	**20%**
Exams	**30%**
Hands-on Projects (Labs)	**30%**
Scripting/basic programming assignments	**10%**

Enabled outcomes: B, C, I.

10. **Brief list of topics to be covered:**

- Ethics, legal issues, and human factors
- Policies (Bell-LaPadula, Biba, Chinese Wall, etc.)
- Mechanisms (access controls, capabilities, mandatory vs. discretionary access control)
- Security mechanism flaws, including concurrency issues
- Vulnerability classifications
- Static information flow model
- Dynamic information flow models
- Covert channels, timing channels, and inference channels
- Cryptography and trust relationships
- Privacy and Internet censorship
- Theory of security (game theory, network theory, etc.)
- Exposure to tools, programming concepts, and scripting