COURSE INTRO

CS-5156/CS-6056: SECURITY VULNERABILITY ASSESSMENT (SPRING 2025)
LECTURE 1

About this Course

- Legal issues associated with disclosure of security vulnerabilities
- Software and Operating System vulnerability
- Software and Operating System design and implementation
- Language (mainly C) design issues
- Network and protocol vulnerabilities
- Network attacks
- Intrusion and anomaly detection and prevention
- Hardware and architecture vulnerabilities and attacks
- Configuration vulnerabilities
- User interfaces and human factors
- Application security and detection of malfeasance

Textbook

- Recommended
  - Computer & Internet Security: A Hands-on Approach, 3rd Edition. By Wenliang Du. ISBN-13: 978-17330039-4-0, 2022
- Reference
  - Analyzing Computer Security: A Threat/Vulnerability/ Countermeasure Approach, 1st edition. By Charles P. Pfleeger and Shari Lawrence Pfleeger. ISBN-10: 0132789469, 2011

Course Components

- Lectures
- Article Reviews
- Labs
- Group Presentation

Lectures

- Concepts
- Demos
- Lab conceptual and technical walkthroughs
- Discussion of certain articles
- Group Presentation (subset of students)

During Lecture

- **Laptop use is allowed**
  - No GAMING please :) !!!

- **Please no electronic communications**
  - No email, instant messaging, cell phone calls, etc

- **Be Present**
  - Attendance will not be taken but is very **strongly encouraged**!!!

- **Please NO recordings or taking pictures of ANY KIND**

Article Reviews

- Shorter Article Reviews
  - Individual
  - Pick a recent article or news item of your choice in certain area(s) the instructor decides on (it is OK if choices overlap).
  - **Submit** a summary on Canvas in **PDF** under **by due date**.
    - You can submit anytime prior to the due date.
    - 0.5 – 1 page (Make sure you **include** the **link** to your article)
  - May dedicate a lecture or two for randomly selected students to discuss their article in class.
    - Be ready regardless: understand the article very well and research for related resources/articles to help you better present if selected
    - Discussion time per student: **MAX 5 minutes.**
    - Selected students should present the article to the rest of the class and encourage a very quick discussion (**Q/A**, opinions, etc…)
      - **Please** keep the **discussion** technical and **professional**.

Article Reviews

- Longer Article Reviews
  - Individual
  - Pick a recent article or news item of your choice in certain area(s) the instructor decides on (it is OK if choices overlap).
  - **Submit** an extended review on Canvas in **PDF** under "**Article Review 2" by due date**. You may submit your second review **anytime** during the semester as long as it is before the deadline.
    - 1.5 – 2 pages
    - Should include
      - A brief summary of the article
      - Your thoughts, and additional discussions of other related online resources
    - Make sure you **include** the **links** to your article as well as the additional resources
  - **No presenting in-class necessary**

Labs

- Individual assignments
- ~6-8 lab assignments (**could change**)
  - Risk Assessment
  - OS Vulnerabilities
  - Software Vulnerabilities
    - Buffer Overflow
    - String Format
    - Etc.
  - Hardware Vulnerabilities
  - Possible Others: Web and/or network vulnerabilities / IDSes

Group Presentation

- Teamwork (3 students per team)
- Topic of your choice
  - Please briefly discuss the topic choice with me before you start
  - **Important**: Cannot choose same topic you covered in other courses.
  - Possible topic choices
    - Tools (i.e. Snort, Metasploit, Tripwire, ELK, Security Onion, etc…)
      - If we cover the tool in class, you can still choose it as a topic BUT **you must present new advanced features** of the tool that we did not cover in class. Failure to do so may jeopardize your presentation grade.
    - Major Events / Data Breaches (requires possible technical coverage, more details will be given later in the semester)
    - Any other topic that relates to network security, cryptography, or cybersecurity in general that we DID NOT cover in class.
      - A modern encryption algorithm (e.g., Elliptic Curve Cryptography, A Quantum Cryptographic Algorithm)
      - Network Attacks and Defenses (E.g., TCP SYN Flood/Cookies, etc.)
      - Social Engineering (Tools, Tactics)
      - Wireless Network Attacks and Defenses (e.g., Jamming, etc.)
      - Mobile Attacks and Defenses (e.g., Android attacks, iOS attacks, etc.)
      - Security Visualization / SEIMs
      - Etc…

Group Presentation

- If we have time in the semester, some class time will be reserved for presentations
    - Roughly **12 minutes for each group** and 3 **minutes for Q/A**.
    - All students present on last 2 or 3 weeks of semester
- If no time, you will be asked as a group to record a video and submit on canvas prior to due date
- Assessment
    - Presentation skills
    - Clarity of presentation
    - Format / Content / Use of own visuals
    - Q/A performance (if in-person presentation)
    - Etc…