CYBR 4810: Cyber Defense

3 Credit Hours

Prerequisite: (CYBR 4220 and CYBR 4200), and Cybersecurity Major.

This course is a semester-long simulation using the virtual systems, software, practices, and procedures necessary for the protection of computer systems and networks. Students learn how to protect networks and systems as deployed in a typical organization. Course topics include policy and practice associated with the protection of communication resources, intrusion detection systems, firewalls, and use of various tools for system and network protection.

CYBR 4833: Wireless Security

3 Credit Hours

Prerequisite: (CYBR 3200 and CYBR 4323), and Cybersecurity Major.

This course explores the theory and practice of securing wireless networks from threats and attacks. Topics include Cryptography, Network Security Protocols, Security and Layered Architecture, Voice-Oriented Wireless Networks, Data-Oriented Wireless Networks, Security in Traditional Wireless Networks, Security in Wireless LAN, and Security in Wireless Ad Hoc Networks.

CYBR 4843: Ethical Hacking for Effective Defense

3 Credit Hours

Prerequisite: (CYBR 3200 and CYBR 4323) and Cybersecurity Major.

This course explores the identification and validation of network and system vulnerabilities by taking an adversarial approach to network, system, and data access. Topics include network attacks and defenses, Operating System and application vulnerabilities, social engineering attacks, and malware. Ethical, legal implications of network attacks are also discussed.

CYBR 4853: Computer Forensics

3 Credit Hours

Prerequisite: (CYBR 3210 and CYBR 3423), and Cybersecurity Major.

This course is an exploration of the tools and techniques used to conduct digital investigations. It will include digital evidence collection, recovery, and analysis. Topics are Legal issues relating to digital evidence, recovery of deleted files and discovery of hidden information, reconstruction of user activity from e-mail, temporary Internet files and cached data, assessment of the integrity of system memory and process architecture to reveal malicious code.