Cyber Security Courses (CYBR) - Online Undergraduate

CYBR 201 Fundamentals of Computer Networking 3 Cr.
This course is the study of the core theories and protocols that are the foundation of computer networking. The Open Systems Interconnection (OSI) model and the Transmission Control Protocol/Internet Protocol (TCP/IP), protocol suite are discussed in detail. This course provides a detailed overview of networking terminology, while examining the different networking topologies and architectures. Pre-requisites: none.

CYBR 210 Computer Programming with a High Level Language 3 Cr.
This course covers the fundamental concepts of computer programming, using a high level scripted programming language. The course emphasizes design and implementation standards. This course is designed to provide the skills necessary to become an effective cyber security practitioner. Prerequisite: None.

CYBR 215 Computer Programming with a Low Level Language 3 Cr.
This course covers the fundamental concepts of computer programming, using a low-level scripted programming language. This course is designed to provide the skills necessary to understand basic computer architecture, allowing the cyber security specialist to better identify, understand and remove security threats at the machine level. Pre-requisites: none.

CYBR 220 Windows Server Administration 3 Cr.
This course provides students with the skills necessary to design, implement, manage and protect a Microsoft Windows Server Active Directory Domain. Students apply the lessons learned in this course by implementing an Active Directory Domain in a virtual environment. Pre-requisites: none.

CYBR 225 Linux Administration 3 Cr.
This course provides students with the necessary knowledge and skills to install, configure, upgrade and manage a Linux operating system in an enterprise network. Additionally, students learn to perform normal business operations using the Linux Operating system. Pre-requisites: none.

CYBR 230 Relational Databases with SQL 3 Cr.
This course covers the fundamental concepts of relational databases and the scripted Structure Query Language (SQL) language used to manage them. Students learn how to design functional relational databases that conform to industry standards. Prerequisite: none.

CYBR 320 Vulnerability Testing I 3 Cr.
This course is the first of a two-part introduction to Penetration Testing and Vulnerability Assessment. This course presents the concepts, tools, and techniques used for penetration testing, vulnerability exploitation, assessment, reporting, and forensics; teaches multiple attack vectors as well as the defensive measures protecting against such attacks; focuses heavily on post-attack forensics allowing for a complete picture of the attack process. The course introduces several open- source tools such as the Metasploit framework, Nmap, Nessus, Wireshark and Kali Linux. This course includes hands-on lab exercises using a virtual computer environment. Prerequisite: permission of program manager.

CYBR 330 Forensic Accounting and Fraud Investigtions 3 Cr.
This course explores how Forensic accounting methodologies are used to uncover evidence of criminal activity. Students will develop an understanding of white-collar crime schemes, fraud in businesses, the circumstances in which it arises, techniques for identifying, assessing and preventing fraud, and the skills needed to aid in the prosecution of exposed frauds. This course examines individuals that carry out fraudulent activities, the indicators to look for, and what countermeasures can be adopted to mitigate their impact. Pre-req: none. Offered: Fall, Spring, Summer.

CYBR 370 Introduction to Information Warfare 3 Cr.
This course introduces students to the overall concept of Information Warfare (IW) and Information Operations (IO), particularly with regard to the US Federal government and the Department of Defense. Introduction to IW / IO surveys the development of Information Warfare (IW) and Information Operations (IO) as these elements of power have become more important for the United States Department of Defense (DoD) and Federal Government as a whole. The course assumes only a rudimentary familiarity with the basic concepts and terminology of modern Internet usage and computing and is not a technology-focused course. Pre-requisites: none.

CYBR 380 Offensive Information Warfare 3 Cr.
Students learn how Offensive Information Warfare is executed at the technical level and the defensive measures cybersecurity professionals use to prevent them. The following principles from the National Security Agency and Department of Homeland Security Information Assurance/Cyber Defense Knowledge Units are examined: Cyber, Defense, Cyber Threats, IA Fundamentals, Policy, Legal, Ethics, and Compliance, Network Defense and Networking Technology and Protocols. Prereqs: CYBR 370 or Program Manager permission.

CYBR 382 Defensive Information Warfare 3 Cr.
This course introduces students to the overall concept of Defensive Information Operations (D-IO), which are conducted across the range of military operations at every level of war to achieve mission objectives. Combatant commanders and mission owners must carefully consider their defensive posture and strategy in order to deter and defeat adversary intrusion while providing mission assurance. Upon completion of this course, students develop a defensive strategy by analyzing risk, cyberspace terrain, mission priorities, and utilizing threat intelligence. Pre-requisite CYBR 370 or Permission of Instructor.

CYBR 400 Cyber Capstone 6 Cr.
This is the final course of the program in which students analyze and synthesize program learning by examining a chosen organization's network infrastructure and security posture. Students present an in-depth analysis paper as their final deliverable. Pre-requisites: Completion of CJ442, DF311, DF312, DF411, CYBR320 & CYBR420 for the Computer Forensics and Vulnerability Management concentration or completion of CYBR370, CYBR380, CYBR382, CS407, POLS302 & CYBR410 c or permission of the Program Manager. This course may not be satisfied by transfer credit.

CYBR 410 Systems Assurance 3 Cr.
This course focuses on the design considerations involved with the security of site design. The course will also provide and understanding of the Levels of Trust and system accreditation/certificate processes. Life cycle management of software, hardware, and physical plant, from planning through destruction will be examined and reinforced using case studies. Additionally, understanding of the variety of security systems involving computers and networks and an ability to evaluate vulnerabilities will be discussed. Note: This course is under development and will be reviewed by the University Curriculum Committee.

CYBR 420 Vulnerability Testing II 3 Cr.
This course is the second of a two-part introduction to Penetration Testing and Vulnerability Assessment. This course presents the concepts, tools, and techniques used for penetration testing, vulnerability exploitation, assessment, reporting, and forensics; teaches multiple attack vectors as well as the defensive measures protecting against such attacks; focuses heavily on post-attack forensics allowing for a complete picture of the attack process. The course introduces several open-source tools such as the Metasploit framework, Nmap, Nessus, Wireshark, Vistumbler, BurpSuite, Nikto, Cain and Abel, Aircrack-ng Suite, John the Ripper, Social Engineer Toolkit and Kali Linux. This course includes hands-on lab exercises using a virtual computer environment. Pre-requisite: CYBR320 or permission of program manager.

CYBR XXX Cyber Security Elective 100 Cr.