This course, socket programming is also introduced. (Sp)

networking APIs (sockets). Protocols in all layers will be introduced. In multicast/broadcast, connectionless vs. connection-oriented), and network protocols, communication paradigms (point-to-point vs. multicast/broadcast, connectionless vs. connection-oriented), and networking APIs (sockets). Protocols in all layers will be introduced. In this course, socket programming is also introduced. (Sp)

This course provides an introduction to the UNIX operating system. Topics include files and directories, electronic mail, security, advanced file systems, network utilities, network file sharing, text utilities, shell programming, regular expressions, UNIX internals, UNIX system administration, UNIX variations, and systems programming. Programming assignments involve the UNIX shell script language. (F)

This course introduces cybersecurity, principles, and technologies. It deals with security issues related to systems and software. Topics include cyber threats and vulnerabilities, information security frameworks and policies, cryptography, penetration testing, and in-depth defense. The goal is to develop a foundation for further study in cybersecurity. (F)

This course introduces ethical frameworks applicable to cybersecurity, sources of applicable law and regulation. Second unit introduces issues relating to cybercrime: intellectual property, user privacy, information assurance, and harmful online content. Third unit introduces issues with IT in government operations. (Sp)

This course focuses on hardware (HW) security and covers security and trust from the HW perspective. It introduces students to HW components, including SoC and PCB, and examines security and trust issues in such HW components. Topics include digital lock, circuit theory, ASICs and FPGAs, HW security threats, malware, and attacks, along with specific countermeasures against HW attacks. (F)

This course introduces students to cyber forensics and cyber-crime scene analysis fundamentals. The various laws and regulations dealing with computer forensic analysis are discussed. Students are introduced to the emerging international standards for cyber forensic analysis and a formal methodology for conducting computer forensic investigations. (Sp)

Introduces the fundamentals of computer networks, including network architectures, network topologies, network protocols, layering concepts (for example, ISO/OSI, TCP/IP reference models), wired and wireless network protocols, communication paradigms (point-to-point vs. multicast/broadcast, connectionless vs. connection-oriented), and networking APIs (sockets). Protocols in all layers will be introduced. In this course, socket programming is also introduced. (Sp)

This course covers topics at the intersection of security and software engineering. This course introduces software engineering processes and standards for building secure software applications. It discusses secure software life cycle development principles to include security in every phase. It also explores security issues and vulnerabilities in software applications due to a lack of secure software engineering processes. (F)

This course provides a comprehensive introduction to system administration. Topics include virtualization, authentication and authorization, directory services, system management, and system security and to set up modern compute and storage clouds, networking systems, file systems, logging and analysis, and networking. Includes topics related to scripting for all administrative functions. Emphasis is placed on enterprise-level systems. (F, Sp)

This course covers concepts related to ethical hacking and penetration testing methods to assess, exploit, and report security vulnerabilities on systems and their resources. The course will emphasize the ethical application of penetration testing methods and hacking tools. (F, Sp)

This course provides a comprehensive introduction to operating systems. Class covers topics such as memory management, process management, information management, and computer security. Principles of performance evaluation. Class projects require the design and implementation of software systems. A UNIX family operating system will be used. (Sp)

This course covers topics related to ethical hacking and penetration testing methods to assess, exploit, and report security vulnerabilities on systems and their resources. The course will emphasize the ethical application of penetration testing methods and hacking tools. (F, Sp)

This course introduces cybersecurity, principles, and technologies. It deals with security issues related to systems and software. Topics include cyber threats and vulnerabilities, information security frameworks and policies, cryptography, penetration testing, and in-depth defense. The goal is to develop a foundation for further study in cybersecurity. (F)

This course introduces cybersecurity, principles, and technologies. It deals with security issues related to systems and software. Topics include cyber threats and vulnerabilities, information security frameworks and policies, cryptography, penetration testing, and in-depth defense. The goal is to develop a foundation for further study in cybersecurity. (F)

This course introduces software engineering processes and standards for building secure software applications. It discusses secure software life cycle development principles to include security in every phase. It also explores security issues and vulnerabilities in software applications due to a lack of secure software engineering processes. (F)

This course covers topics related to ethical hacking and penetration testing methods to assess, exploit, and report security vulnerabilities on systems and their resources. The course will emphasize the ethical application of penetration testing methods and hacking tools. (F, Sp)

This course covers concepts related to ethical hacking and penetration testing methods to assess, exploit, and report security vulnerabilities on systems and their resources. The course will emphasize the ethical application of penetration testing methods and hacking tools. (F, Sp)
CYBS 4333 Incidence Response Management 3 Credit Hours
Prerequisite: CYBS 3123. This course provides a comprehensive treatment of cyber incidents and how to manage them, including understanding attacker motivation, attack methods, and the anatomy of the attacks. Additionally, topics related to incidence readiness, remote triage tools, memory analysis, malware analysis, disk forensics, network intrusion detection tools, and others will be discussed. (F, Sp)

CYBS 4473 Network Security 3 Credit Hours
Prerequisite: CYBS 3113. The course deals with understanding all aspects of cybersecurity that involve the network. Topics will include network transport-level security, wireless network security, electronic mail security, IP security, firewalls, VPNs, Secure HTTP, person-in-the-middle attack scenarios, and SSL/TLS and SSH (SP). Learn about various tools for analyzing network data at various levels of the TCP/IP stack and operating security operations centers. (F)

CYBS 4583 Machine Learning for Cybersecurity 3 Credit Hours
Prerequisite: CYBS 3213 and ISE 3293. Various machine learning concepts, deep learning, time-series analysis, data mining, and other machine-learning concepts. Tools and libraries to analyze data sets, build predictive models, and evaluate the fit of the models. Common learning algorithms, including dimensionality reduction, classification, principal-component analysis, k-NN, k-means clustering, gradient descent, regression, logistic regression, regularization, multiclass data, algorithms, boosting and decision trees. Applies concepts to problems. (F, Sp)

CYBS 4883 Cryptography Fundamentals 3 Credit Hours
Prerequisite: CYBS 3213. This course introduces cryptography and its related tools. Specifically, in this course, cryptographic algorithms, protocols, and techniques will be introduced. The course will also introduce students to public key encryption, key exchange protocols, digital signatures, hashing-based encryption, and Data Encryption Standards. This course will also introduce cryptographic implementation in software and web application programming. (F)

CYBS 4953 Operating and Maintaining Cyber Ranges 3 Credit Hours
Prerequisite: CYBS 4473. Students will learn to use and build a cyber range for various assessments of threats and exploits. They will learn to build configurations for different business operations and the formation of red and blue team exercises. Students will have real-world experiences in handling situations without the real-world risk associated with practicing on live production equipment and systems. (Sp)

CYBS 4963 Cybersecurity Capstone 3 Credit Hours
Prerequisite: CYBS 4103 and Senior Standing. Provides the students with an experience to exhibit their knowledge and skills in all areas of cybersecurity. Students will work in small groups to identify and scope a cybersecurity problem and/or challenges. Required to write a proposal about their project and asked to create a work plan to develop solution to solve the problem/challenge. Create a final report and presentation. (Sp)