CYBERSECURITY (CYS)

CYS 0500 Ethical Hacking (0 Credits)
This course will immerse students through an interactive environment to be shown how to scan, test, hack and secure their own systems. This lab intensive approach will provide each student with in-depth knowledge and practical experience using the current essential security systems. Students will begin by learning how perimeter defenses work and then be led into scanning and attacking their own networks (no real network is harmed during the process). Students will then learn how intruders escalate privileges and what steps can be taken to secure a system. Students will also learn about Intrusion Detection, Policy Creation, Social Engineering, DDoS Attacks, Buffer Overflows and Virus Creation. Students will leave program with hands-on understanding and experience in Ethical Hacking. This course will prepare students for the ECC-Council ANSI accredited Certified Ethical Hacker exam 312-50.

CYS 0501 Certified Information Systems Security Professional(CISSP) (0 Credits)
This course is intended for experienced IT security-related practitioners, auditors, consultants, investigators, or instructors, including network or security analysts and engineers, network administrators, information security specialists, and risk management professionals. Analyze the ten domains required to pass the CISSP exam: information systems access control security architecture and design network security systems and telecommunications information security management goals information security classification and program development risk management criteria and ethical codes of conduct; software development security cryptography characteristics and elements physical security and operations security. Apply Business Continuity and Disaster Recovery Plans and identify legal issues, regulations, compliance standards, and investigation practices relating to information systems security. Required electronic curriculum is includes in the cost of the course. Prerequisite: It is highly recommended that students have certifications in Network + or Security+, or possess equivalent professional experience upon entering CISSP training. It will be beneficial if students have one or more of the following security-related or technology-related certifications or equivalent industry experience: MCSE, MCTS, MCITP, SCNP, CCNP, RHCE, LCE, CNE, SSCP®, GIAC, CISA™, or CISM®.

CYS 0502 CompTIA Security+ Certification (0 Credits)
The Security+ Certification is an internationally recognized validation of the technical knowledge required of foundation-level security practitioners. A Security+ certified individual has successfully demonstrated a foundation level of skill and knowledge in General Security Concepts, Communication Security, Infrastructure Security, Basics of Cryptography, and Operational / Organizational Security. The goal of this course is to provide students with the knowledge and skills required to install and configure systems to secure applications, networks, and devices; perform threat analysis and respond with appropriate mitigation techniques; participate in risk mitigation activities; and operate with an awareness of applicable policies, laws, and regulations and to be able to perform these tasks to support the principles of confidentiality, integrity, and availability.

CYS 0503 CompTIA Cybersecurity Analyst (CySA+) (0 Credits)
CompTIA Cybersecurity Analyst (CySA+) is a premier industry certification designed for cybersecurity professionals responsible for incident detection, prevention, and response through security monitoring.
Additional fees may apply