

CYBERSECURITY (CYBR)

CYBR 3101. Intro to Cybersecurity. (3 Credits)

Prerequisites: None **Credit Hours:** (3-0-3) This introductory course provides students with a foundational understanding of cybersecurity principles, practices, and technologies. Topics include the history and evolution of cybersecurity, threat landscapes, basic security concepts, risk management, cryptography, network security, and ethical/legal considerations. Students will explore real-world scenarios and gain practical insights into protecting digital assets in personal, academic, and professional environments. No prior technical experience is required, making this course ideal for students from all disciplines interested in cybersecurity awareness and career pathways.

CYBR 3200. Network Security Fundamentals. (3 Credits)

This course is an intensive, hands-on training program designed to prepare IT professionals to protect, detect, and respond to network security threats. Developed by EC-Council, this course focuses on the practical aspects of network defense, emphasizing real-world scenarios and security strategies. Participants will gain a deep understanding of network security technologies, including firewalls, VPNs, IDS/IPS systems, and endpoint protection, while learning how to analyze network traffic, identify vulnerabilities, and implement effective countermeasures. The course also covers risk management, incident response, and business continuity planning, making it ideal for network administrators, security analysts, and IT professionals seeking to strengthen their defensive capabilities. Upon completion, students will be prepared to take the EC-Council CND certification exam, validating their expertise in network defense and enhancing their career prospects in cybersecurity.

CYBR 3400. Operating Systems & Admin. (3 Credits)

This course offers a deep examination of modern operating systems (OS), specifically focusing on security configuration, administration, and hardening techniques for both Linux (e.g., Ubuntu, Red Hat) and Windows (e.g., Windows Server, Windows 10/11). Students will learn the inner workings of an OS from a security perspective, including user and access controls, file system permission, process management, kernel components, system auditing, and vulnerability mitigation strategies necessary to maintain a secure computational environment. This course is delivered online only and is structured for intensive learning over an eight-week term, emphasizing practical application of hardening techniques.

CYBR 4101. Ethical Hacking & Pentesting I. (3 Credits)

The course is an advanced, hands-on training program designed to teach students how to think and act like ethical hackers. This course provides in-depth knowledge of the tools, techniques, and methodologies used by cybersecurity professionals to assess and strengthen the security posture of networks, systems, and applications. Students will learn how to identify vulnerabilities, exploit weaknesses in a controlled environment, and apply countermeasures to prevent real-world attacks. Topics include footprinting, scanning, enumeration, system hacking, web application attacks, wireless security, and social engineering. The course emphasizes practical labs and real-world scenarios to prepare students for careers in ethical hacking, penetration testing, and cybersecurity analysis. Upon completion, students will be prepared to pursue industry-recognized certifications and contribute effectively to organizational security efforts.

CYBR 4102. Ethical Hacking& Pentesting II. (3 Credits)

The course is an advanced, hands-on training program designed to teach students how to think and act like ethical hackers. This course provides in-depth knowledge of the tools, techniques, and methodologies used by cybersecurity professionals to assess and strengthen the security posture of networks, systems, and applications. Students will learn how to identify vulnerabilities, exploit weaknesses in a controlled environment, and apply countermeasures to prevent real-world attacks. Topics include footprinting, scanning, enumeration, system hacking, web application attacks, wireless security, and social engineering. The course emphasizes practical labs and real-world scenarios to prepare students for careers in ethical hacking, penetration testing, and cybersecurity analysis. Upon completion, students will be prepared to pursue industry-recognized certifications and contribute effectively to organizational security efforts.

CYBR 4300. Cloud Computing & Security. (3 Credits)

This course provides a comprehensive exploration of security architectures and best practices necessary to secure modern cloud environments. It focuses on the principles, technologies, and compliance requirements across major cloud service providers (CSPs) including Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP). Key areas of study include the Shared Responsibility Model, data security, identity and access management (IAM), network security configuration, and continuous compliance monitoring in multi-cloud environments. The course is delivered online only and is structured for intensive learning over an eight-week term, emphasizing practical application through hands-on labs and case studies.