EC-Council | University

MASTER OF SECURITY SCIENCE

COURSE DESCRIPTION

EC-Council |University

Course Title: ECU 500 Managing Secure Network Systems

Purpose: This class is designed to provide the fundamental skills needed to analyze the internal and external security threats against a network, and to implement security mechanisms to protect an organization's information. The course helps to evaluate network and Internet security issues and provides security solutions such as the designing a security policy, troubleshooting networks, and digital signatures.

Course Title: ECU 501 Ethical Hacking & Countermeasures

Purpose: This class is designed to provide students an insight of current security scenario and increasing hacking attempts on various information systems. The goal of the ethical hacking and countermeasures is to help the organizations take preemptive measures against malicious attacks by attacking the system themselves staying within legal limits.

Course Title: ECU 502 Investigating Network Intrusions and Computer Forensics

Purpose: This class is designed to equip students with necessary skills required to identify computer crime; gather and preserve digital evidence by following set of standards and procedures that hold good in the court of law; assist the attorney in legal proceedings to prosecute criminals involved in cases where one/many computers were used as part of the crime.

Course Title: ECU 503 Security Analysis and Vulnerability Assessment

Purpose: Through groundbreaking penetration testing methods and techniques, Security Analysis and Vulnerability Assessment class helps students perform the intensive assessments required to effectively identify and mitigate risks to the security of the infrastructure.

Course Title: ECU 506 Conducting Penetration and Security Tests

Purpose: This course focuses on the mastery of the international standard for penetration testing. Topics include customers and legal agreements, penetration testing planning and scheduling, information gathering, external and internal network penetration testing, router penetration testing, firewalls penetration testing, intrusion detection system penetration testing, wireless networks penetration testing; password cracking penetration testing, social engineering penetration testing, PDA and cell phone penetration testing, and penetration testing report and documentation writing.

Course Title: ECU 507 Linux Networking and Security

Purpose: This course focuses on configuring a secure Linux network using command line and graphical utilities. Emphasis is placed on file sharing technologies such as the Network File System, NetWare's NCP file sharing, and File Transfer Protocol. Additional topics include making data secure, user security, file security, and network intrusion detection. Students will be required to take on the role of problem solvers and apply the concepts presented to situations that might occur in a work environment.

Course Title: ECU 509 Securing Wireless Networks

This course focuses on the various methods of securing wireless networks including authentication, authorization and encryption. Topics include radio frequency communications, infrared, Bluetooth, low-speed wireless local area networks, high-speed WLANs and WLAN Security, digital cellular telephone, fixed wireless, and wireless communications in business.

Course Title: ECU 510 Secure Programming

This class is designed to provide students an insight of current security scenario and increasing hacking attempts on various information systems. The goal of the ethical hacking and countermeasures is to help the organizations take preemptive measures against malicious attacks by attacking the system themselves staying within legal limits.

EC-Council |University

Course Title: ECU 513 Disaster Recovery

Purpose: This course is designed to provide fundamental skills needed to understand the methods in identifying vulnerabilities and taking appropriate countermeasures to prevent and mitigate failure or risks for an organization. It also provides the networking professional with a foundation in disaster recovery principles, including preparation of a disaster recovery plan, assessment of risks in the enterprise, development of policies, procedures, understanding of the roles and relationships of various members of an organization, implementation of the plan, disaster recovery and virtualization techniques. This course takes an enterprise-wide approach to develop a disaster recovery plan. Students will learn how to create a secure network by putting policies and procedures in place, and how to restore a network in the event of a disaster. Students are also exposed to various virtualization tools and techniques that form an important part while charting the disaster recovery solution.

Course Title: ECU 515 Project Management in IT Security

Purpose: This class is designed to provide students with the knowledge of how to manage IT security projects in order to enhance the success rate for both organizations as well as IT managers. It acts as an operational framework for users who design their own IT security project plan. The goal of PMITS is to help the students implement their IT project management skills by providing a roadmap for implementing the IT security in their organizations. It standardizes the knowledge base for business professionals by incorporating the best practices and legal standards related to corporate IT security.