

Course Syllabus Ethical Hacking Course



Dr. Kamal Alieyan
kamal@esu.ac.ae

Cybersecurity Law, Policy and Ethics

This course designed to help students to establish and govern minimum standards for credentialing entry-level information security specialists in ethical hacking measures, inform the public that credentialed individuals meet or exceed the minimum standards, and reinforce ethical hacking as a unique and self-regulating profession.

Required Textbook:

Topics:

- Module 01 – Information Security Fundamentals
- Module 02 – Ethical Hacking Fundamentals
- Module 03 – Information Security Threats and Vulnerability Assessment
- **Module 04 – Password Cracking Techniques and Countermeasures**
- **Module 05 – Social Engineering Techniques and Countermeasures**
- Module 06 – Network Level Attacks and Countermeasures
- Module 07 - Web Application Attacks and Countermeasures
- Module 08 – Wireless Attacks and Countermeasures
- Module 09 – Mobile Attacks and Countermeasures
- Module 10 – IoT and OT Attacks and Countermeasures
- **Module 11 – Cloud Computing Threats and Countermeasures**
- **Module 12 – Penetration Testing Fundamentals**

Learning Outcomes:

Upon successful completion of this course, students should be able to:

- Discuss the key issues plaguing the information security world and review various information security laws and regulations.
- Comprehend Cyber Kill Chain Methodology, hacking and ethical hacking concepts, hacker classes, different phases of a hacking cycle, and assess essential ethical hacking tools.
- Examine various information security threats and vulnerabilities, identify different types of malwares and perform vulnerability assessments.
- Explain and use different password cracking, social engineering, insider threats, and identity theft techniques, and discuss their countermeasures.
- Examine various network-level attacks, including sniffing, denial-of-service, and session hijacking, and discuss their countermeasures.
- Examine various application-level attacks, including webserver exploitation, OWASP top-10 attacks, and SQL injection, and discuss their countermeasures.
- Discuss different types of wireless encryption, examine wireless threats and attacks, and suggest countermeasures.
- Describe various mobile platform attack vectors, mobile device management, mobile security guidelines, and identify essential mobile security tools.
- Discuss IoT and OT concepts, examine various IoT and OT threats and attacks, and suggest countermeasures.
- Describe various Cloud computing technologies, examine cloud computing threats and attacks, and identify security techniques.
- Discuss fundamentals of penetration testing, its benefits, strategies, and phases, and examine guidelines for penetration testing.