

## Course Specification Document

<b>Title</b>	Ethical Hacking
--------------	-----------------

<b>Credits</b>	3 ECTS
----------------	--------

<b>Aims</b>	This course aims to introduce the student to the fundamental principles of ethical hacking, methods for analyzing and evaluating vulnerabilities, and techniques for addressing them. It enables the student to use modern methods and tools in penetration testing and ethical hacking of information and communication systems, including web servers, applications, operating systems, and wireless networks.
-------------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

### Intended learning outcomes

On successful completion of this course, the student will be able to:

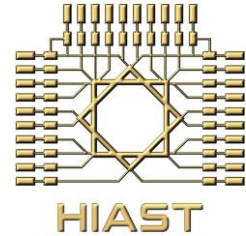
- Understand the fundamental concepts of information gathering processes and system penetration.
- Grasp the principles and methods of vulnerability analysis for information systems.
- Understand the principles of network penetration and data exchange penetration.
- Familiarize himself with the basic principles of web penetration and its applications.
- Learn the techniques for security testing of wireless networks and address resulting vulnerabilities.
- Conduct penetration tests for network systems.
- Implement and conduct vulnerability analysis and generate reports.
- Take the necessary measures to protect against penetration.

### Syllabus

- **Lab setup and tools preparation:** Equipping the lab computers and student computers with the necessary tools for remote work.
- **Information gathering:** Footprinting through search engines, footprinting via web services, footprinting through social media platforms, footprinting websites, conducting scanning, conducting enumeration.
- **Vulnerability analysis:** Analysis mechanisms and methods, OpenVAS, Nessus, GFI LanGuard, Nikto.
- **System penetration:** Accessing systems, modifying permissions, remote access and malware concealment, log scanning and digital evidence deletion.
- **Malware:** Using Trojans, Using viruses, conducting malware program analysis.
- **Social engineering:** Password acquisition, phishing, detecting phishing.

## Syrian Arab Republic

Higher Institute for Applied Sciences and Technology



- **Denial of service:** SYN flooding, hping3, DDOS, denial of service detection.
- **Network attacks:** Active sniffing, network sniffing, detecting sniffing, session hijacking.
- **Firewall evasion:** Intruder detection, malicious traffic detection, firewall evasion.
- **Web attacks:** Enumeration and scanning of web servers, FTP password cracking, Brute-force attack, XSS, CSRF, SQL injection, Web intrusion detection.
- **Wireless network attacks:** Analyzing local wireless network traffic, finding hidden networks, breaking WEP, breaking WPA, Android system penetration, protecting Android systems.
- **Encryption analysis:** Calculating hash functions, file and text message encryption, Email protection, disk encryption, encryption analysis.