Ethical Hacking

1. **Course number and name**: 020PIRES5 Ethical Hacking

2. **Credits and contact hours**: 4 ECTS credits, 35 contact hours (lectures + lab sessions)

3. **Instructor's or course coordinator's name**: Maroun Chamoun

4. **Text book**:
    a. **Other supplemental materials**:
    Handouts posted on the Web.

5. **Specific course information**
    a. **Catalog description**:
    Introduction to Ethical Hacking: Information Security, Hacking phases, Ethical Hacking Concepts and Scope – Footprinting and Reconnaissance - Scanning: Check for Live Systems, Check for Open Ports, Banner Grabbing, Scan for Vulnerability, Draw Network Diagrams - Enumeration – Cracking Passwords System Hacking: Gaining Access, Escalating Privileges, Executing Applications, Hiding Files, Covering Tracks – Network Hacking: DoS Attack, Sniffing, Spoofing, Session Hijacking – Web hacking: SQL Injection Attacks, Cross-Site Scripting (XSS) Attacks, Cross-Site Request Forgery (CSRF) Attack, Session Fixation Attack - Social Engineering.

    b. **Prerequisites:**

    c. **Required**: Elective for CCE students

6. **Specific goals for the course**
    The overall goal of this course is to understand penetration testing and determine how to better defend systems by learning to identify and exploit system weaknesses.

    a. **Specific outcomes of instruction:**
    - Learn about how system vulnerabilities manifest themselves and why hackers continue to enjoy success breaking into systems, despite increasing attention paid to cyber defense.
    - Gain experience with a systematic hacking methodology.
    - Learn about and experiment with hacking tools that can be applied at different stages of the hacking process.
    - Hands-on experience with Reconnaissance, Scanning tools, password hacking tools, system and network hacking, Metasploit and exploitation framework, Web exploitation, Social Engineering.

b. KPI addressed by the course:

KPI	a2	e3	f1	g1	h1	k2	k3
Covered	x	x	x		x	x	x
Assessed	x	x		x		x	

7. Topics and approximate lecture hours:

- Introduction to Ethical Hacking: “Information Security Threats and Attack Vectors”, “Hacking Concepts, Types, and Phases”, Ethical Hacking Concepts and Scope. Quiz on Ethical Hacking (2 lectures)
- Footprinting and Reconnaissance: Footprinting Concepts, Footprinting Methodology, Footprinting through Search Engines, Footprinting using Advanced Google Hacking Techniques, Footprinting through Social Networking Sites, Website Footprinting, Email Footprinting, WHOIS Footprinting, DNS Footprinting, Footprinting Countermeasures (3 lectures)
- Lab: Footpring using Passive Recon add-on, online tools and Advanced Google Hacking Techniques (1 lecture)
- Scanning Networks: Check for Live Systems, Check for Open Ports, Banner Grabbing, Scan for Vulnerability, Draw Network Diagrams. Quiz on Footprinting and Scanning. (3 lectures)
- Lab: Anonymity using proxychains and TOR (1 lecture)
- Lab: Check for Live Systems and Check for Open Ports and services with nmap (1 lecture)
- Lab: Vulnerability scan with nmap and nessus (1 lecture)
- Enumeration: NetBIOS Enumeration, SNMP Enumeration, LDAP Enumeration, SMTP Enumeration, Enumeration Countermeasures (1 lecture)
- Cracking Passwords: Microsoft Authentication, How Hash Passwords Are Stored, Password Salting, Default Passwords, Types of Password Attacks, Password Cracking Tools, How to Defend against Password Cracking (1 lecture)
- Lab: cracking Windows and Linux password (1 lecture)
- System Hacking: Goals of system hacking, Types of Attacks on a System, System Attack Tool:Metasploit, Gaining Access, Escalating Privileges, Executing Applications, Hiding Files, Covering Tracks. Quiz on Enumeration, Cracking password and System Hacking (3 lectures)
- Lab: System enumeration and hacking using metasploit (1 lecture)
- Lab: Installing Malware (Keylogger and backdoor) With Metasploit (1 lecture)
- Network Hacking: DoS Attack, Sniffing, Spoofing, Session Hijacking (2 lectures)
- Lab: Active Sniffing, DNS spoofing and ARP poisoning using DSNIFF (1 lecture)
- Web hacking: Web App Concepts, Web App Threats, SQL Injection Attacks, Cross-Site Scripting (XSS) Attacks, Cross-Site Request Forgery (CSRF) Attack, Session Fixation Attack, Improper Error Handling, Insecure Cryptographic Storage, Unvalidated Redirects and Forwards, Web Application Attack Countermeasures. Quiz on Network Hacking (4 lectures)
- Lab: Using SQL injection, XSS and commands injection to hack a demo website (www.karsana.com) (2:30 lab hours)

- Social Engineering: Behaviors Vulnerable to Attacks, Why Is Social Engineering Effective?, Phases in a Social Engineering Attack, Social Engineering Techniques, Identity Theft, Social Engineering Countermeasures. Quiz on Web Hacking and Social Engineering (2 lectures)
- Homework: Penetration testing: Non-Disclosure Agreement (NDA), Footprinting, scanning and Social Engineering (12 hours of mini-project)