

Course Name : Data Security							
Course Code	Course Type	Regular Semester	Lecture (hours/week)	Seminar (hours/week)	Lab. (hours/week)	Credits	ECTS
CMP 312	B	Spring	2.00	0.00	2.00	3.00	6.00
Lecturer		Elton Kaziu, Msc					
Assistant							
Course language		Albanian					
Course level		Bachelor					
Description		The objectives of this course are to familiarize students with: basic security threats on networks connected to the Internet basic tools to provide user and system security, and security resources available on the Internet. Topics include security framework overview, footprinting, scanning, enumeration, hacking framework, backdoor servers and Trojans, rootkits, Windows (7, 8, 10) and Linux vulnerabilities, dialup, VPN and network devices vulnerabilities, firewalls, Intrusion Detection System (IDS), Denial of Service (DoS) and DDoS, buffer overflows, spyware, phishing, social engineering and protecting the Web end-user. This is a project-oriented course using a restricted access UB Lab to practice the use of hacking and security tools.					
Objectives							
Core Concepts		Topics include security framework overview, footprinting, scanning, enumeration, hacking framework, backdoor servers and Trojans, rootkits, Windows (7, 8, 10) and Linux vulnerabilities, dialup, VPN and network devices vulnerabilities, firewalls, Intrusion Detection System (IDS), Denial of Service (DoS) and DDoS, buffer overflows, spyware, phishing, social engineering and protecting the Web end-user.					
Course Outline							
Week	Topic						
1	Introduction to Computer Security						
2	Networks and the Internet						
3	Cyber Stalking, Fraud, and Abuse						
4	Denial of Service Attacks						
5	Malware						
6	Techniques Used by Hackers						
7	Industrial Espionage in Cyberspace						
8	Encryption						
9	Computer Security Software						
10	Security Policies						
11	Network Scanning and Vulnerability Scanning						
12	Cyber Terrorism and Information Warfare						
13	Cyber Detective						
14	Introduction to Forensics						
15	Review						

16	Final Exam		
Prerequisites		The student must attend the course at a minimum rate of 75%.	
Literature		• Computer Security Fundamentals 5th Edition	
References		•	
Course Outcome			
1	The topics include an overview of the security framework, trace tracking, scanning, counting, piracy frameworks, backdoor servers and Trojans, rootkits, vulnerabilities in Windows (7, 8, 10) and Linux, vulnerabilities in mobile devices, VPNs and network devices, firewalls, Intrusion Detection Systems (IDS), Denial of Service (DoS) and Distributed Denial of Service (DDoS), buffer overflow, spyware, phishing, social engineering, and end-user web protection. This is a project-oriented course utilizing a restricted access lab environment to practice the use of hacking and security tools.		
Course Evaluation			
In-term Studies		Quantity	Percentage
Midterms		1	30
Quizzes		0	0
Projects		0	0
Term Projects		1	20
Laboratory		0	0
Class Participation		1	10
Total in-term evaluation percent			60
Final exam percent			40
Total			100
ECTS Workload (Based on Student Workload)			
Activities	Quantity	Duration (hours)	Total (hours)
Course duration (Including the exam week: 16x Total hours of the course)	16	4	64
Study hours outside the classroom (Preparation, Practice, etc.)	14	5	70
Duties	1	0	0
Midterms	1	8	8
Final Exam	1	8	8
Other	0	0	0
Total Work Load			150
Total Work Load / 25 (hours)			6.00
ECTS			6.00