

Cyber Security					
Credit Hours:	2	Course Code:	COSC-4112	Prerequisites:	None
Course Learning Outcomes (CLOs):					
At the end of the course, the students will be able to:				Domain	BT Level*
1. To be able to identify computer system threats				C	1
2. To be able to identify Malware attacks, and understand thestages of attack and payloads.				C	2
3. Implement various cryptographic techniques and simulate attack scenarios				C	3
* BT= Bloom’s Taxonomy, C=Cognitive Domain, P=Psychomotor Domain, A=Affective Domain					
#	SDG	Relevant CLOs			
1	SDG 4: Quality Education	CLO 1: To be able to identify Malware attacks, and understand thestages of attack and payloads. CLO 3: Implement various cryptographic techniques and simulate attack scenarios			
Course Contents:					
Introduction to Cyber security; Networks and the Internet; cyber threat landscape; understanding security; information security Principles (Confidentiality, Integrity, Availability); Information Security Terminology; Malware, types of malware; Malware Attack Lifecycle: Stages of Attack; Social engineering attacks; types of payload; Industrial Espionage in Cyberspace; Basic cryptography; Web application attacks; Database security; Cyber kill chain; Privacy and anonymity; Network security; Software security; Mobile device security; Mobile app security; Cyber Terrorism and Information Warfare; Introduction to Digital Forensics; Digital Forensics Categories.					
Teaching Methodology:					
Lectures, Written Assignments, Practical labs, Semester Project, Presentations.					
Course Assessment:					
Mid Term Exams, Final Term Exams, Assignments, Quizzes, Project, Presentations, Practical Exam					
Text Books:					
1. Computer Security Fundamentals by Chuck Easttom, 4th edition or latest 2. Security+ Guide to Network Security Fundamentals, by Mark Ciampa, 5th Edition 3. Security in Computing by C.P. Pfleeger, Prentice-Hall, 4th Edition or Latest					
Reference Material:					
1. Computer Security Fundamentals by Chuck Easttom, 4th edition or latest 2. Security+ Guide to Network Security Fundamentals, by Mark Ciampa, 5th Edition 3. Security in Computing by C.P. Pfleeger, Prentice-Hall, 4th Edition or Latest					
Cyber Security - Lab					
Credit Hours:	1	Course Code:	COSC-4212	Prerequisites:	None

Course Learning Outcomes (CLOs):		
At the end of the course, the students will be able to:		BT Level*
1. To be able to identify computer system threats	C	1
2. To be able to identify Malware attacks, and understand the stages of attack and payloads.	C	2
3. Implement various cryptographic techniques and simulate attack scenarios	C	3
* BT= Bloom's Taxonomy, C=Cognitive Domain, P=Psychomotor Domain, A=Affective Domain		
#	SDG	Relevant CLOs
1	SDG 4: Quality Education	<i>CLO 1:</i> To be able to identify Malware attacks, and understand the stages of attack and payloads. <i>CLO 3:</i> Implement various cryptographic techniques and simulate attack scenarios
Course Contents:		
Study of packet sniffer tools like Wireshark, tcpdump etc. Download and install VMware, Download and install, Kali Linux, Linux Terminal Commands, Retrieving Passwords from the Browser, Steganography, Using the Social Engineer Toolkit, Injection - SQL Injection, John the Ripper, The Hydra, Exploring VirusTotal, Study of different types of vulnerabilities for hacking a website / Web Applications., Installing a Honeypot, Study of the features of firewall in providing network security and to set Firewall Security in Windows, Steps to ensure Security of any one web browser (Mozilla/Firefox/Google Chrome)		
Teaching Methodology:		
Lectures, Written Assignments, Practical labs, Semester Project, Presentations.		
Course Assessment:		
Mid Term Exams, Final Term Exams, Assignments, Quizzes, Project, Presentations, Practical Exam		
Text Books:		
1. Computer Security Fundamentals by Chuck Easttom, 4th edition or latest 2. Security+ Guide to Network Security Fundamentals, by Mark Ciampa, 5th Edition 3. Security in Computing by C.P. Pfleeger, Prentice-Hall, 4th Edition or Latest		
Reference Material:		
1. Computer Security Fundamentals by Chuck Easttom, 4th edition or latest 2. Security+ Guide to Network Security Fundamentals, by Mark Ciampa, 5th Edition 3. Security in Computing by C.P. Pfleeger, Prentice-Hall, 4th Edition or Latest		