

Cyber Security – Lab					
Credit Hours:	1	Course Code:	CSEC-1202	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 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		CLO 1: To be able to identify Malware attacks, and understand the stages of attack and payloads. CLO 3: Implement various cryptographic techniques and simulate attack scenarios		
Course Contents:					
Course Contents (16 Labs)					
Lab No.	Lab Title		Topics Covered		
1	Lab Orientation and Cyber Security Environment		Lab safety, cybersecurity ethics, virtualization concepts, introduction to VirtualBox/VMware, installation of Windows and Linux virtual machines.		
2	Linux Fundamentals for Cyber Security		Linux file system, terminal commands, user management, file permissions, package management, and shell navigation.		
3	Windows Security Fundamentals		Windows Security Center, Microsoft Defender, Windows Firewall, User Account Control (UAC), local security policies, and event logs.		
4	Basic Networking and IP Configuration		IP addressing, subnetting basics, TCP/IP configuration, network troubleshooting using ipconfig, ifconfig, ping, tracert, and netstat.		
5	Network Traffic Analysis using Wireshark		Capturing network packets, protocol identification, packet filtering, and basic traffic analysis.		
6	Network Discovery using Nmap		Host discovery, port scanning, service detection, operating system detection, and interpreting scan results.		
7	Malware Awareness and Safe Analysis		Malware categories, indicators of compromise (IOCs), safe analysis using VirusTotal, Hybrid Analysis (demonstration), and Windows Sandbox.		
8	Password Security and		Password strength testing, password managers, multi-factor		

9	Authentication Cryptography Fundamentals		authentication (MFA), and secure authentication practices. Hashing (SHA-256), file integrity verification, symmetric and asymmetric encryption using OpenSSL or GPG.
10	Web Fundamentals	Security	Introduction to HTTP/HTTPS, browser developer tools, SSL/TLS certificates, secure browsing, and basic web vulnerabilities (demonstration).
11	Firewall Configuration		Configuring Windows Firewall and UFW (Linux), creating inbound and outbound rules, and basic network access control.
12	Secure Configuration	System	User and group management, software updates, secure configuration practices, backup, and recovery techniques.
13	Digital Forensics Basics		Introduction to digital evidence, metadata analysis, file hashing, chain of custody, and basic forensic tools (e.g., Autopsy demonstration).
14	Security Monitoring and Log Analysis		Windows Event Viewer, Linux system logs, introduction to SIEM concepts, and basic log analysis.
15	Cloud and Mobile Security Demonstration		Cloud security concepts, secure cloud storage, mobile device security settings, application permissions, and data privacy.
16	Mini Practical Assessment / Lab Project		Practical assessment involving network analysis, system hardening, basic vulnerability identification, documentation, and presentation.
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			