

Introduction to Cyber Security					
Credit Hours:	2+1	Course Code:	CSEC-1102	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:					
1. Introduction to Cyber Security - Evolution of Cyber Security - Cyber Security Domains - CIA Triad, AAA, Risk, Threat, Vulnerability, Exploit, Attack Surface 2. Cyberspace, Networks and the Internet - Internet Architecture - Network Models - Internet Services - Digital Ecosystem 3. Cyber Threat Landscape - Threat Actors - Nation-State Attacks - Organized Cybercrime - Insider Threats - Hactivism - Emerging Threats 4. Information Security Principles - Confidentiality - Integrity - Availability - Authentication - Authorization - Accountability - Non-Repudiation 5. Cyber Attacks and Malware - Malware Types - Ransomware - Spyware - Rootkits - Botnets					

- Fileless Malware
- Malware Life Cycle
- 6. **Social Engineering and Human Factors**
 - Phishing
 - Spear Phishing
 - Business Email Compromise
 - Vishing
 - Smishing
 - Pretexting
 - Insider Threats
- 7. **Cyber Kill Chain and MITRE ATT&CK Framework**
 - Attack Lifecycle
 - Reconnaissance
 - Initial Access
 - Persistence
 - Lateral Movement
 - Defense Strategies
- 8. **Fundamentals of Cryptography**
 - Symmetric Encryption
 - Asymmetric Encryption
 - Hash Functions
 - Digital Signatures
 - Public Key Infrastructure
 - Certificates
- 9. **Network Security Fundamentals**
 - Firewalls
 - IDS/IPS
 - VPN
 - Network Segmentation
 - Secure Network Architecture
- 10. **Application and Software Security**
 - Secure Software Development
 - OWASP Top 10
 - Web Application Security
 - API Security
 - Secure Coding Principles
- 11. **Cloud, Mobile and IoT Security**
 - Cloud Security Concepts
 - Shared Responsibility Model
 - Mobile Device Security
 - Mobile Application Security
 - IoT Security Challenges
- 12. **Identity and Access Management**
 - Authentication
 - Multi-Factor Authentication (MFA)
 - Single Sign-On (SSO)
 - Privileged Access Management
 - Password Security

13. Privacy, Ethics and Cyber Law

- Privacy Principles
- Data Protection
- Cyber Ethics
- Digital Rights
- Introduction to Cyber Laws
- Electronic Crimes

14. Digital Forensics and Incident Response

- Introduction to Digital Forensics
- Evidence Collection
- Chain of Custody
- Incident Response Process
- Security Operations Center (SOC)

15. Emerging Trends in Cyber Security

- Artificial Intelligence in Cyber Security
- Machine Learning for Security
- Zero Trust Architecture
- Cyber Threat Intelligence
- Blockchain Security
- Quantum Computing Threats

16. Cyber Security Careers and Future Directions

- Cyber Security Certifications
- Ethical and Professional Responsibilities
- National Cyber Security Frameworks
- Cyber Security Research
- Future Challenges
- Course Review

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