COURSE STRUCTURE AND SYLLABI

M.Sc. Cyber Security and Digital Forensics

2024-25 Batch

Centurion
UNIVERSITY

Shaping Lives...
Empowering Communities...

SCHOOL OF FORENSIC SCIENCES
CENTURION UNIVERSITY OF TECHNOLOGY & MANAGEMENT
Odisha-761211, India

Web Site: - www.cutm.ac.in

CENTURION UNIVERSITY OF TECHNOLOGY AND MANAGEMENT, ODISHA

CERTIFICATE

Centurion
UNIVERSITY
Shaping Lives...
Empowering Communities...

This is to certify that the syllabus of the Programmes M.Sc. Cyber Security and Digital Forensic of the School of Forensic Sciences is approved in the 14th Academic Council Meeting held on 22nd November 2024.

Pro-Vice Chancellor
CUTM, Odisha

Centurion
UNIVERSITY
Shaping Lives...
Empowering Communities...

TITLE OF THE PROGRAMME

A. Post Graduate Diploma in Cyber Security and Digital Forensics

B. Master of Science in Cyber Security and Digital Forensics (2 years)

C. Master of Science in Cyber Security and Digital Forensics (1 year)

SYLLABUS

Effective from 2024

AS PER NEP 2020

SCHOOL OF FORENSIC SCIENCES

CENTURION UNIVERSITY OF TECHNOLOGY AND MANAGEMENT, ODISHA

TABLE OF CONTENTS

CENTURION UNIVERSITY OF TECHNOLOGY AND MANAGEMENT

Centurion University is duly recognized as a pioneer is 'Skill Integrated Higher Education". Its unique model lays specific emphasis on creating sustainable livelihoods on a national scale in challenging geographies through education that results in employability and sparks entrepreneurship. This model has been recognized by multiple Governments (Central and State), International Organizations such as UNESCO and the World Bank as well as Policy think tanks such as the Niti Ayog.

The founders, faculty, and staff are fully committed to its credo: Shaping Lives. Empowering Communities.

This credo is underpinned by a value system of Inclusivity, Integrity, Equity, Respect, and Sustainability in everything we do.

Since its inception in 2005 and subsequent establishment as a University in 2010 (vide Odisha Act 4 of 2010), Centurion has created a unique environment that ensures a tailored learning and employability path for youth in some of the poorest and underserved geographies in Odisha and Andhra Pradesh

SCHOOL OF FORENSIC SCIENCES

Centurion University established the School of Forensic Sciences in the year 2017 with M.Sc. Forensic Science Programme and Gujarat Forensic Science University (GFSU) as a Knowledge partner.

VISION:

To be an inclusive centre for education, training, and research in Forensic Science and allied professions to create sustainable livelihoods.

MISSION

- To create much-required forensic experts in the field of investigative science.
- Developing a robust platform for students to interact with experts and develop problem-solving approaches.
- Sensitize students to harness their potential for the application of various scientific technologies in investigative Science.
- Be a potential support to strengthen the justice delivery system leading towards equality, integrity, and peace.

PREAMBLE

The M.Sc. programme in Cyber Security and Digital Forensics at Centurion University of Technology and Management (CUTM) is meticulously designed to equip students with advanced knowledge and practical skills in the ever-evolving fields of cybersecurity and digital forensics. As we navigate through an era marked by rapid technological advancements and an increasing reliance on digital platforms, the importance of securing digital information and investigating cyber crimes has never been more critical.

Our curriculum is a comprehensive blend of theoretical foundations and hands-on experiences, ensuring that our graduates are well-prepared to tackle contemporary challenges in cybersecurity and digital forensics. The program covers a wide range of topics including network security, cryptography, ethical hacking, cyber law, and forensic analysis, providing a robust framework for understanding and combating cyber threats.

At CUTM, we emphasize a multidisciplinary approach, integrating principles from computer science, law, and criminology. This holistic perspective enables our students to develop a well-rounded understanding of the complexities of cyber threats and the legal and ethical implications of digital investigations.

The faculty at CUTM comprises experienced professionals and researchers who bring knowledge and expertise to the classroom. Through interactive lectures, practical labs, and real-world case studies, students gain valuable insights and develop critical thinking and problem-solving skills. Additionally, our state-of-the-art laboratories and partnerships with industry leaders provide students access to cutting-edge tools and technologies, fostering an environment of innovation and continuous learning.

Upon completion of the program, graduates will be equipped to pursue a wide range of careers in cybersecurity, digital forensics, risk management, and related fields. They will be capable of securing digital infrastructures, investigating cybercrimes, and contributing to developing policies and strategies to protect against future threats.

Centurion University of Technology and Management is committed to nurturing the next generation of cybersecurity and digital forensics professionals who will safeguard our digital future. We invite you to embark on this challenging and rewarding journey with us and become a vital part of the global effort to secure our digital world.

COURSE STRUCTURE

Title of the Programme

A. **Post Graduate Diploma in Cyber Security and Digital Forensics**
B. **Master of Science in Cyber Security and Digital Forensics (2 years)**
C. **Master of Science in Cyber Security and Digital Forensics (1 year)**

S. No.	Qualifications	Level	Credits	Credit Points
1	P.G. Diploma	6	46 (32 DSC + 8 DEC + 4 SFS +2 MiP)	
2	1-Year PG after a 4-year UG	6.5	44 (12 DSC + 4 DEC + 4 SFS + 4 SI + 4 RM +16 RP)	
3	2-Year PG after a 3-year UG	7	90 (46 + 44)	

Credit distribution basket-wise

S. No.	Basket	Course	Credits	Total Credit per basket
1	I	Discipline Specific Core Courses (DSC)	16+16+12	44
2	II	Discipline Specific Elective Courses (DEC)	04+04+04	12
3	III	Summer Internship (SI) + Minor Project	04 + 02	06
4	IV	Research Project (RP) + Research Methodology	04 + 16	20
5	V	Skill for Success (SFS)	04	08
		Total		90

Credit distribution structure for two years / one-year PG Diploma with Multiple Entry and Exit Options

Year/ Level	**Semester**	**Major Subject Discipline-Specific**		**Research Methodology**	**Skill for Success**	**Minor Project / Internship**	**Research Project**	**Credits**	**Degree**
		Core Courses	Elective Courses						
1st Yr 6.0	I	4*4 = 16	4	-	4		-	24	PG Diploma After 3 years UG
	II	4*4 =16	4	-	-	2	-	22	
Cumulative Cr. 1st year		32	8	-	4	2	-	46	
EXIT: *Post Graduate Diploma: 40 credits with one 4 credit Skill Enhancement Course and/ or 2 credit Minor Project*									
2nd Yr 6.5 /7	III	4*3= 12	4	4	4	-	-	24	1/ 2 yr PG After 3 / 4 years UG Degree
	IV	-	-	-	-	4	16	20	
Cumulative Cr.		12	4	4	4	4	16	44	
Cumulative Cr.		44	12	4	8	6	16	90	
EXIT: *Postgraduate Degree: 80 credits with two 4-credit Skill Enhancement Courses and/ or Internship* *2 years i.e. 4 Semester (88 credits) after three years UG or 1 year i.e. 2 Semesters (44 credits) after four years UG Degree*									

PROGRAM EDUCATIONAL OBJECTIVES (PEOS) FOR M.SC. CYBER SECURITY AND DIGITAL FORENSICS

The M.Sc. program in Cyber Security and Digital Forensics at Centurion University of Technology and Management aims to produce graduates who will:

1. **Professional Expertise**: Develop deep technical expertise and practical skills in cybersecurity and digital forensics, enabling them to secure digital infrastructures, investigate cybercrimes, and provide solutions to mitigate cybersecurity threats.
2. **Leadership and Innovation**: Become leaders and innovators in the field, capable of managing and leading cybersecurity and forensic projects, driving technological advancements, and implementing effective security strategies in diverse organizational settings.
3. **Lifelong Learning**: Engage in continuous professional development and lifelong learning to stay abreast of evolving technologies, emerging threats, and best practices in cybersecurity and digital forensics.
4. **Ethical Responsibility**: Uphold high ethical standards and demonstrate a strong sense of responsibility in their professional conduct, ensuring compliance with legal frameworks and promoting ethical practices in cybersecurity and digital forensics.
5. **Multidisciplinary Integration**: Integrate knowledge from various disciplines, including computer science, law, and criminology, to develop holistic solutions to complex cybersecurity challenges and forensic investigations.
6. **Effective Communication**: Exhibit excellent communication skills, capable of articulating complex technical concepts to diverse audiences, including technical teams, management, and non-technical stakeholders.
7. **Research and Development**: Contribute to the body of knowledge in cybersecurity and digital forensics through independent research, innovation, and development of new tools, techniques, and methodologies.
8. **Global Perspective**: Understand and address global cybersecurity challenges, considering the cultural, legal, and ethical differences that influence cybersecurity practices and policies worldwide.

9. **Collaboration and Teamwork**: Work effectively in multidisciplinary and multicultural teams, demonstrating strong collaboration skills to achieve common goals in cybersecurity and digital forensic projects.
10. **Adaptability and Problem-Solving**: Develop the ability to adapt to rapidly changing technological landscapes and solve complex cybersecurity problems through creative and analytical approaches.

PROGRAMME OUTCOMES FOR M.SC. CYBER SECURITY AND DIGITAL FORENSICS

Upon successful completion of the M.Sc. in Cyber Security and Digital Forensics at Centurion University of Technology and Management, graduates will be able to:

1. **Advanced Knowledge of Cybersecurity**: Demonstrate a comprehensive understanding of cybersecurity principles, including network security, cryptography, and information assurance, to protect digital assets against cyber threats.
2. **Digital Forensic Expertise**: Apply digital forensic techniques to investigate and analyze cybercrimes, recovering and preserving digital evidence in a manner that is admissible in legal proceedings.
3. **Risk Assessment and Management**: Conduct thorough risk assessments, identifying vulnerabilities and implementing effective mitigation strategies to safeguard information systems.
4. **Implementation of Security Policies and Controls**: Design and implement effective security policies and access controls within organizational networks. Graduates will have the expertise to configure role-based access controls, enforce password policies, deploy IDS/IPS systems, and secure IoT devices, ensuring comprehensive protection against a wide range of cyber threats.
5. **Operating Systems Proficiency**: Explain various operating systems, their roles, and how they manage computer hardware, software, and subsystems. Describe memory allocation schemes and paging, enhancing the ability to secure and manage diverse operating environments.
6. **Forensic Investigative Strategies**: Utilize forensic investigative strategies and tools to locate and retrieve electronic data and history on networks and digital devices. Retrieve volatile and non-volatile information, deleted files, and partition data to support comprehensive digital investigations.

7. **Legal and Ethical Understanding**: Demonstrate a strong understanding of cyber laws, regulations, and ethical considerations, ensuring compliance with legal standards and promoting ethical practices in cybersecurity and digital forensics.
8. **Critical Thinking and Problem-Solving**: Utilize critical thinking and problem-solving skills to analyze complex cybersecurity issues, developing innovative solutions to address emerging threats and challenges.
9. **Communication Skills**: Communicate effectively with diverse stakeholders, including technical and non-technical audiences, through written reports, presentations, and collaborative discussions.
10. **Research and Innovation**: Engage in independent research and contribute to the body of knowledge in cybersecurity and digital forensics, fostering innovation and advancements in the field.
11. **Teamwork and Leadership**: Work collaboratively in multidisciplinary teams, demonstrating leadership and project management skills to complete cybersecurity and forensic investigations.
12. **Lifelong Learning and Professional Development**: Commit to continuous learning and professional development, staying abreast of the latest trends, technologies, and best practices in cybersecurity and digital forensics.

PROGRAM SPECIFIC OUTCOMES (PSOS) FOR M.SC. CYBER SECURITY AND DIGITAL FORENSICS

Upon successful completion of the M.Sc. program in Cyber Security and Digital Forensics at Centurion University of Technology and Management, graduates will be able to:

1. **Professional Careers in Cybersecurity and Forensics**: Secure employment in various cybersecurity and digital forensic roles such as Security Analyst, Forensic Investigator, Penetration Tester, and Incident Responder. Graduates will possess the practical skills and theoretical knowledge required to excel in these positions, addressing real-world cybersecurity challenges and contributing to the protection of digital assets.
2. **Entrepreneurship and Innovation**: Leverage their expertise to start and manage their cybersecurity firms or consultancy services. Graduates will be equipped with the knowledge to develop innovative cybersecurity solutions, create new forensic tools, and provide specialized services such as threat analysis, vulnerability assessments, and security audits, fostering entrepreneurship in the cybersecurity domain.
3. **Professionalism and Ethical Conduct**: Exhibit high standards of professionalism and ethical behavior in all aspects of their work. Graduates will understand and adhere to legal, ethical, and regulatory requirements in cybersecurity and digital forensics, ensuring responsible and ethical practices in their professional careers. They will also demonstrate effective communication, teamwork, and leadership skills, contributing positively to their organizations and the broader cybersecurity community.
4. **Continuous Learning and Development**: Engage in lifelong learning and professional development to stay current with the rapidly evolving cybersecurity landscape. Graduates will pursue advanced certifications, attend industry conferences, participate in workshops, and engage in research activities to continuously enhance their knowledge and skills, ensuring they remain at the forefront of the field

ELIGIBILITY

B.E. / B. Tech. in Engineering / Technology branches OR B.Sc. (Information Technology (IT) /Computer Science (CS/Electronics)) OR Bachelor of Computer Applications (BCA) OR B.Sc. Forensic Science in cyber forensic/ digital forensic/ computer forensic OR Equivalent qualification from a recognized University with a minimum 55% (50% for SC/ST/ PwD candidates in the qualifying examination.

TEACHING METHODOLOGY:

- **Lectures**: In-depth theoretical discussions on each topic.
- **Case Studies**: Analysis of real-world cyber security incidents.
- **Group Discussions**: Encouraging student interaction and exchange of ideas.
- **Hands-on Exercises**: Practical exercises to apply theoretical concepts.
- **Guest Lectures**: Industry experts sharing their experiences and insights.

ASSESSMENT SCHEME

1. Evaluation for Theory papers (T, TP & TPP)

1.1. End semester theory examinations (50% weightage):

- Duration – 3 hours
- Full Mark – 100. During result processing, it will be proportionately added.
- Distribution of marks (should cover all COs)

a. 10 short questions x 2 marks = 20 marks

b. 5 long questions x 12 marks = 60 marks

c. 4 short notes x 5 marks = 20 marks

1.2. Continuous assessments: Details are as indicated in the table below:

SL No	Continuous Assessment	Score
	Individual / Group Presentation The rubric is as under: ● Content & creativity – 05 ● Presentation & Discussion – 05	10
	Mid-semester (Written Examination) Mark Distribution: ● 5 short questions x 1 marks = 5 marks ● 2 long questions x 5 marks = 10 marks ● 2 short notes x 2.5 marks = 5 marks	20
	Assignment (2 assignments x 5 marks each)	10
	Learning Record (Based on the parameters indicated in the learning record format, course faculty to evaluate and award score)	10
	TOTAL	50

2. Evaluation of Practice/ Laboratory Components: The evaluation of the practice component will be carried out 50% by the concerned faculty and 50% by the external examiner and will be conducted as per the present policy. Details are as under:

	Internal	**Score**
A	Concept	10
B	Planning & Execution/ Practical/ Simulation/ Programming	10
C	Result and Interpretation	10
D	Record/ Report	10
E	Viva	10
	Total	50
	External	
A	Execution & Result	20
B	Record of Applied and Action Learning	10
C	Viva	20
	Total	50

3. Evaluation of Project Component: The evaluation of the project component will be completed 50% by the concerned faculty and 50% by the external examiner and will be conducted as per the present policy. The following guidelines may be referred to during the evaluation of internal and external components:

	INTERNAL	
A	Understanding the relevance, scope, and dimension of the project	10
B	Methodology	10
C	Quality of Analysis and Results	10
D	Interpretations and Conclusions	10
E	Report	10
	Total	50
	EXTERNAL	
A	Understanding the relevance, scope, and dimension of the project	10

B	Report	20
C	Viva	20
	Total	50

PASS CRITERIA

A. **Theory papers:** students must secure a minimum of **30% in individual components** (both continuous assessment & end-semester theory) **along with 40% in aggregate**

B. **Theory & practice papers:**

a. Theory component: minimum of 30% in individual components (both continuous assessment & end-semester theory) along with 40% in aggregate

b. Practice component: minimum of 50% marks both in internal & external

C. **Theory & project type papers:**

a. Theory component: minimum of 30% in individual components (both continuous assessment & end-semester theory) along with 40% in aggregate

b. Project component: minimum of 50% marks both in internal & external

D. **Theory, practice & project type papers:**

a. Theory component: minimum of 30% in individual components (both continuous assessment & end-semester theory) along with 40% in aggregate

b. Practice component: minimum of 50% marks both in internal & external

c. Project component: minimum of 50% marks both in internal & external

E. **Practice & project type papers:**

a. Practice component: minimum of 50% marks both in internal & external

b. Project component: minimum of 50% marks both in internal & external

F. **Workshop or Internship type papers:** 50% in aggregate

TEACHING SCHEME

COURSE CODE	COURSE NAME	HOURS PER WEEK	CREDITS				CREDITS PER SEMESTER
			T	P	Pj	PER	
SEMESTER I							
CUFS1056	Introduction to Cyber Security	4	4	0	0	4	24
CUFS1057	Network Security	5	3	1	0	4	
CUFS1058	Digital Forensics Fundamentals	5	3	1	0	4	
CUFS1059	Programming for Cyber-Security	5	3	1	0	4	
	Elective I	5	4	0	0	4	
	Skill for Success I	8	0	2	2	4	
SEMESTER II							
CUFS1060	Advanced Cryptography	5	3	1	0	4	22
CUFS1061	Incident Response and Management	5	3	1	0	4	
CUFS1062	Malware Analysis and Reverse Engineering	5	3	1	0	4	
CUFS1063	Ethical Hacking and Penetration Testing	5	3	1	0	4	
	Elective II	5	3	1	0	4	
CUFS1064	Minor Project / Summer Training	4	0	0	2	2	
SEMESTER III							
CUFS1066	Advanced Digital Forensics	5	3	1	0	4	24
CUFS1067	Cyber Security Policy and Management	4	4	0	0	4	
CUFS1068	Data Privacy and Protection	4	4	0	0	4	
CUFS1069	Research Methodology in Cyber Security	5	3	0	1	4	
	Elective III	5	3	1	0	4	
	Skill for Success I	8	0	2	2	4	
SEMESTER IV							
CUFS1070	Capstone Project and Thesis	32	0	0	16	16	20
CUFS1071	Internship	16	0	0	04	4	
							90

T: Theory; P: Practice; Pj: Project [1 Credit= 1 hour Theory; 1 credit = 2 Hours Practice / Project]

BASKET

BASKET 1: DISCIPLINE-SPECIFIC CORE COURSES

SI. No.	COURSE CODE	NAME OF THE CORE COURSES	CREDITS	TEACHING HOURS / WEEK
1	CUFS1056	Introduction to Cyber Security	4+0+0	4
2	CUFS1057	Network Security	3+1+0	5
3	CUFS1058	Digital Forensics Fundamentals	3+1+0	5
4	CUFS1059	Programming for Cyber-Security	3+1+0	5
5	CUFS1060	Advanced Cryptography	3+1+0	5
6	CUFS1061	Incident Response and Management	3+1+0	5
7	CUFS1062	Malware Analysis and Reverse Engineering	3+1+0	5
8	CUFS1063	Ethical Hacking and Penetration Testing	3+1+0	5
9	CUFS1066	Advanced Digital Forensics	3+1+0	5
10	CUFS1067	Cyber Security Policy and Management	3+1+0	5
11	CUFS1068	Data Privacy and Protection	4+0+0	4
12	CUFS1069	Research Methodology	3+0+1	5

BASKET 2: DISCIPLINE-SPECIFIC ELECTIVE COURSES

SI. No.	COURSE CODE	NAME OF THE ELECTIVE COURSES	CREDITS	TEACHING HOURS / WEEK
1	CUFS1072	Cyber Law and Ethics	4+0+0	4
2	CUFS1073	Cyber Threat Intelligence	3+1+0	5
3	CUFS1074	Secure Software Development	3+1+0	5
4	CUFS1075	Mobile Device Forensics	3+1+0	5
5	CUFS1076	Cyber-Physical Systems Security	3+1+0	5
6	CUFS1077	Artificial Intelligence in Cyber Security	3+1+0	5
7	CUFS1078	Cloud Security	3+1+0	5
8	CUFS1079	Machine Learning for Cyber Security	3+1+0	5

BASKET 3: MINOR PROJECT AND INTERNSHIP

SI. No.	COURSE CODE	NAME OF THE COURSES	CREDITS	TEACHING HOURS / WEEK
1	CUFS1064	Minor Project	0+0+2	4
2	CUFS1065	Summer Internship	0+0+2	4
3	CUFS1071	Internship	0+0+4	8

BASKET 4: RESEARCH

SI. No.	COURSE CODE	NAME OF THE COURSES	CREDITS	TEACHING HOURS / WEEK
1	CUFS1069	Research Methodology	3+0+1	5
2	CUFS1070	Capstone Project and Thesis	0+0+16	32

BASKET 5: SKILL FOR SUCCESS (PREFERRED FROM CUTM BASKET OF 120+ COURSES)

SI. No.	NAME OF THE ELECTIVE COURSES	CREDITS	TEACHING HOURS / WEEK
1	Internet of things	0+2+2	8
2	Introduction to Blockchain Technology	0+2+2	8
3	Introduction to NLP	0+2+2	8
4	Introduction to Quantum Computing	0+2+2	8
5	Job Readiness Programme	0+0+4	8

BASKET I: DISCIPLINE-SPECIFIC CORE COURSES

CUFS1056: INTRODUCTION TO CYBER SECURITY

Credits: 04 (4+0+0)

Duration: 40 hrs

Course Description:

This course offers a foundational overview of cybersecurity, providing essential knowledge to protect information systems and data. It covers basic concepts, terminologies, and the critical importance of cybersecurity in today's digital world. Students will explore various cyber threats and vulnerabilities, along with methods used by cyber attackers. The course includes basic security measures like firewalls, encryption, and secure communication protocols. Through both theoretical insights and practical applications, students will be prepared for advanced study and careers in cybersecurity.

Course Objectives

1. To understand and articulate fundamental cybersecurity concepts and terminologies, recognizing the critical importance of cybersecurity in the digital age.
2. To learn to Identify and evaluate various cyber threats and vulnerabilities, understanding the techniques used by cyber attackers and methods for mitigating these risks.
3. To learn to implement basic security measures and basics of cryptography.

Course Outcomes:

By the end of this course, students will:

1. Understand the fundamental concepts and importance of cyber security.
2. Identify and describe various types of cyber threats and attacks.
3. Develop and implement security policies and procedures to protect information assets.
4. Perform risk assessments and develop strategies to manage cyber risks.
5. Apply basic cryptographic techniques to secure information.

Course Content:

Module 1: Overview of Cyber Security

Introduction to Cyber Security: Key concepts, historical development, role in protecting assets.; Cyber Security Objectives: Overview of the CIA Triad, and the concepts of authentication, authorization, and non-repudiation.; Cyber Security Domains: Brief introduction to information, network, application, and physical security.; Cyber Security Frameworks and Standards: Overview of NIST Cybersecurity Framework, ISO/IEC 27001, CIS Controls.

Module 2: Cyber Threats and Attacks

Types of Cyber Threats: Focus on major threats like malware, phishing, insider threats, and APTs.; Cyber Attack Vectors: Overview of network-based, web-based, endpoint, and cloud-based attacks.; Case Studies of Major Cyber Attacks: Brief analysis of high-profile incidents.; Attack Methodologies: Summary of reconnaissance, scanning, gaining access, maintaining access, and covering tracks.

Module 3: Security Policies and Procedures

Introduction to Security Policies: Purpose and importance, with examples of common policies.; Security Policy Development: Key steps, roles, and responsibilities in creating policies.; Security Procedures: Overview of incident response, change management, and access control.; Security Policy Implementation: Focus on training, awareness, monitoring, and regular updates.

Module 4: Risk Management

Introduction to Risk Management: Importance and key frameworks.; Risk Assessment: Brief on identifying assets, threats, vulnerabilities, and evaluating risks.; Risk Mitigation Strategies: Overview of avoidance, transference, mitigation, and acceptance.; Risk Monitoring and Review: Continuous assessment and adjustment based on evolving threats.

Module 5: Cryptography Basics

Introduction to Cryptography: Overview and historical context.; Symmetric & Asymmetric Encryption: Principles and common algorithms.; Cryptographic Hash Functions: Key concepts and applications in digital signatures and data integrity.; Digital Signatures and Certificates: Basics of PKI, role of CAs, and usage of digital certificates.

Practice Component:

1. Setting up and configuring firewalls.
2. Implementing basic encryption techniques.
3. Performing vulnerability assessments using basic tools.
4. Simulating cyber-attack scenarios and response measures.

Suggested Reading and Resources:

1. "Cybersecurity for Beginners" by Raef Meeuwisse.
2. "Introduction to Cyber Security: Stay Safe Online" by Ravi Das and Preston de Guise.
3. "Computer Security: Principles and Practice" by William Stallings and Lawrie Brown.
4. "Cybersecurity Essentials" by Charles J. Brooks, Christopher Grow, Philip Craig, and Donald Short.
5. "Introduction to Cyber Security" by David White.
6. NIST Cyber Security Framework.
7. ISO/IEC 27001 standard documentation.
8. Online resources and research papers on recent cyber security incidents and best practices.

CUFS1057: NETWORK SECURITY

Credits: 04 (3+1+0)

Duration: 50 hrs

Course Description:

This course provides an in-depth understanding of network security principles, practices, and technologies. It covers various aspects of securing network infrastructures, including threat analysis, mitigation strategies, and the implementation of security protocols. The course also explores current trends and emerging threats in network security.

Course Objectives:

1. To understand the fundamental principles of network security.
2. To implement and manage network security measures and protocols.
3. To gain practical experience with network security tools and technologies.

Course Outcomes:

1. Explain fundamental concepts of network security.
2. Identify and analyze various network threats and vulnerabilities.
3. Implement network security measures and protocols to mitigate threats.
4. Utilize cryptographic techniques to secure network communications.
5. Use network security tools to monitor, detect, and respond to security incidents.

Course Content:

Module 1: Introduction to Network Security

Overview of Network Security, Security Goals: Confidentiality, Integrity, Availability; Types of Attacks: Passive and Active Attacks; Threats, Vulnerabilities, and Risks; Security Policies and Models

Module 2: Network Security Protocols

Secure Socket Layer (SSL) and Transport Layer Security (TLS); Internet Protocol Security (IPSec); Secure Shell (SSH); Virtual Private Networks (VPNs); Wireless Security Protocols (WPA, WPA2, WPA3)

Module 3: Network Threats and Defense Mechanisms

Malware: Viruses, Worms, Trojans, Ransomware; Denial of Service (DoS) and Distributed Denial of Service (DDoS) Attacks; Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS); Firewalls and Packet Filtering; Anti-malware Tools and Techniques

Module 4: Network Security Management

Network Security Policies and Procedures; Network Security Architectures; Security Information and Event Management (SIEM); Incident Response and Management; Security Auditing and Compliance

Module 5: Emerging Trends and Technologies in Network Security

Cloud Security; Internet of Things (IoT) Security; Blockchain and Network Security; Artificial Intelligence and Machine Learning in Network Security; Zero Trust Security Models

Practice Component

1. Configuration and management of firewalls and IDS/IPS
2. Implementation of VPNs and secure communication protocols
3. Practical exercises with cryptographic tools and techniques
4. Network traffic analysis using tools like Wireshark
5. Simulation of network attacks and defense mechanisms

Suggested Reading:

1. Network Security Essentials: Applications and Standards by William Stallings
2. Cryptography and Network Security: Principles and Practice by William Stallings
3. Computer Security: Principles and Practice by William Stallings and Lawrie Brown
4. The Web Application Hacker's Handbook by Dafydd Stuttard and Marcus Pinto
5. Practical Network Security: Tools and Techniques for Securing Your Network by Bastian Ballmann
6. Research papers and articles from IEEE Xplore, ACM Digital Library, and other reputable sources.

CUFS1058: DIGITAL FORENSICS FUNDAMENTALS

Credits: 04 (3+1+0)

Duration: 50 hrs

Course Description:

This course introduces the principles and practices of digital forensics, focusing on the techniques used to investigate cybercrimes. Students will learn how to recover and analyze digital evidence from various types of devices and systems, ensuring that it is admissible in legal proceedings. The course also covers the ethical and legal considerations involved in digital forensic investigations.

Course Objectives:

1. Understand the fundamental principles and concepts of digital forensics.
2. Learn techniques for recovering and analyzing digital evidence.
3. Develop an understanding of the ethical and legal aspects of digital forensics.

Course Outcomes:

1. Explain fundamental principles of digital forensics.
2. Recover and analyze digital evidence from different devices.
3. Ensure the integrity and admissibility of digital evidence.
4. Understand and adhere to ethical and legal standards in digital forensics.
5. Apply forensic techniques to practical scenarios in cybercrime investigations.

Course Content:

Module 1: Introduction to Digital Forensics

Definition and Scope: Understanding digital forensics, its significance, and its role in cybersecurity; History and Evolution: Development of digital forensics over time; Types of Digital Forensics: Computer forensics, mobile device forensics, network forensics, etc.; Legal and Ethical Issues: Understanding the legal framework and ethical considerations in digital forensic investigations.

Module 2: Digital Evidence and Crime Scene Management

Digital Evidence: Definition, types, and characteristics. Identification and Collection: Procedures for identifying and collecting digital evidence. Preservation of Evidence: Techniques for preserving the integrity of digital evidence. Chain of Custody: Maintaining and documenting the chain of custody.

Module 3: Forensic Investigation Process

Investigation Framework: Steps involved in digital forensic investigations. Imaging and Cloning: Techniques for creating forensic copies of digital media. Data Recovery: Methods for recovering deleted, hidden, or encrypted data. Analysis Techniques: Basic techniques for analyzing digital evidence.

Module 4: Introduction to Forensic Tools and Software

Forensic Tools: Overview of commonly used tools in digital forensics (e.g., FTK, EnCase, Autopsy). Open-source vs. Commercial Tools: Comparison and selection of tools based on the investigation. Hands-on Practice: Practical sessions using forensic tools to analyze sample data.

Module 5: Reporting and Presenting Digital Evidence

Documentation: Importance of documentation in digital forensic investigations. Report Writing: Structure and content of forensic reports. Presentation of Evidence: Techniques for presenting digital evidence in court. Expert Testimony: Role of a digital forensic expert in legal proceedings.

Practice Component:

1. Recovering deleted files and partition data.
2. Performing forensic analysis of digital devices.
3. Using forensic tools such as EnCase and FTK.
4. Simulating digital forensic investigations.

Suggested Reading:

1. Digital Forensics and Incident Response: Incident response techniques and procedures to respond to modern cyber threats by Gerard Johansen.

2. Guide to Computer Forensics and Investigations by Bill Nelson, Amelia Phillips, and Christopher Steuart.
3. "Computer Forensics: Cybercriminals, Laws, and Evidence" by Marjie T. Britz.

CUFS1059: PROGRAMMING FOR CYBER-SECURITY

Credits: 04 (3+1+0)

Duration: 50 hrs

Course Description:

This course provides an introduction to programming concepts and techniques relevant to cybersecurity. Students will learn to write scripts and programs to automate security tasks, analyze malware, and develop security tools. The course emphasizes practical programming skills that can be applied to various cybersecurity domains.

Course Objectives:

1. Introduce programming concepts and techniques relevant to cybersecurity.
2. Develop skills in writing scripts and programs for security tasks.
3. Enable students to create and use security tools for various cybersecurity applications.

Course Outcomes:

On successful completion of this course, students will be able to:

1. Understand basic programming concepts and techniques.
2. Write scripts to automate cybersecurity tasks.
3. Develop programs for malware analysis and security tool development soulmates.
4. Apply programming skills to practical cybersecurity scenarios.
5. Utilize programming knowledge to enhance cybersecurity measures and strategies.

Course Content:

Module 1: Programming Languages (Python, C++)

Introduction to Python and C++ for cybersecurity applications; Basic syntax, data types, and control structures; Writing functions, handling files, and error handling; Object-oriented programming concepts relevant to cybersecurity

Module 2: Scripting for Security

Writing and executing security scripts using Python and Bash; Automating network scanning, log analysis, and incident response tasks; Integrating scripts with security tools (e.g., Nmap, Wireshark); Parsing and analyzing security data using scripting

Module 3: Secure Coding Practices

Importance of secure coding in preventing vulnerabilities; Common security vulnerabilities: SQL injection, buffer overflows, cross-site scripting (XSS); Techniques for writing secure code: input validation, error handling, and encryption; Code review processes and secure coding standards (e.g., OWASP)

Module 4: Vulnerability Identification and Patching

Identifying vulnerabilities in code and applications; Static and dynamic analysis tools for vulnerability detection; Techniques for patching code to eliminate vulnerabilities; Case studies of real-world vulnerabilities and their patches

Module 5: Automation of Security Tasks

Automating routine security tasks: scanning, monitoring, and reporting; Scripting for automated patch management and updates; Using automation tools (e.g., Ansible, Puppet) in security operations; Best practices for maintaining automation scripts

Practice Component:

1. Writing scripts for network scanning and vulnerability assessment.
2. Developing simple malware analysis tools.
3. Automating security tasks using programming languages like Python.
4. Creating and testing custom security tools.

Suggested Readings:

1. Python for Cybersecurity: Using Python for Cyber Offense and Defense" by Howard E. Poston III
2. Black Hat Python: Python Programming for Hackers and Pentesters" by Justin Seitz.
3. Violent Python: A Cookbook for Hackers, Forensic Analysts, Penetration Testers, and Security Engineers" by TJ O'Connor.

4. "Automate the Boring Stuff with Python: Practical Programming for Total Beginners" by Al Sweigart."Hacking: The Art of Exploitation" by Jon Erickson
5. "The CERT® C Coding Standard: 98 Rules for Developing Safe, Reliable, and Secure Systems" by Robert C. Seacord
6. "Automate the Boring Stuff with Python" by Al Sweigart

CUFS1060: ADVANCED CRYPTOGRAPHY

Credits: 04 (3+1+0)

Duration: 50 hrs

Course Description:

This course offers an in-depth exploration of advanced cryptographic techniques and their applications in cybersecurity. Students will learn about modern encryption algorithms, cryptographic protocols, and key management practices. The course also covers the theoretical foundations of cryptography and its practical implementations.

Course Objectives:

1. Provide a deep understanding of advanced cryptographic techniques and algorithms.
2. Explore the applications of cryptographic protocols in securing communications and public key infrastructure.
3. Develop skills in implementing and managing cryptographic solutions.

Course Outcomes:

1. Explain advanced cryptographic techniques and their theoretical foundations.
2. Implement modern encryption algorithms and protocols.
3. Manage cryptographic keys and secure key distribution.
4. Analyze the security of cryptographic systems.
5. Apply cryptographic techniques to practical cybersecurity problems.

Course Content:

Module 1: Symmetric and Asymmetric Encryption

Symmetric Encryption: Advanced Techniques: Modes of operation (ECB, CBC, CFB, OFB, CTR), Stream ciphers vs. block ciphers, Key distribution and management; Algorithms: Advanced Encryption Standard (AES), Triple DES (3DES), Blowfish, Twofish, RC4;- Asymmetric Encryption: Fundamental Principles: Public key vs. private key, Key pairs and key management; Algorithms: RSA (Rivest-Shamir-Adleman), Elliptic Curve Cryptography (ECC), Diffie-Hellman Key Exchange;- Applications: Secure communication (SSL/TLS), Digital signatures, Data encryption and decryption

Module 2: Cryptographic Protocols

Design Principles: Security goals (confidentiality, integrity, authentication, non-repudiation), Protocol components and structure, Threat models and adversary capabilities; Key Protocols: Secure Sockets Layer (SSL) and Transport Layer Security (TLS), Secure/Multipurpose Internet Mail Extensions (S/MIME), Kerberos authentication protocol, Pretty Good Privacy (PGP); Analysis Techniques: Formal methods and models, Protocol verification and validation, Security proofs and analysis tools; Applications: Secure email communication, Secure file transfer, Secure online transactions (e-commerce)

Module 3: Public Key Infrastructure (PKI)

PKI Components: Public and private keys, Certificates and certificate authorities, Registration Authorities (RAs) and end entities; Certificates: X.509 certificate standard, Certificate lifecycle (issuance, renewal, revocation), Certificate Revocation Lists (CRLs) and Online Certificate Status Protocol (OCSP); Key Management: Key generation and distribution, Key storage and protection, Key usage policies and practices; Applications: Digital signatures and authentication, Secure web browsing (HTTPS), Email encryption and signing

Module 4: Digital Signatures and Certificates

Digital Signature Algorithms: RSA digital signatures, Digital Signature Algorithm (DSA), Elliptic Curve Digital Signature Algorithm (ECDSA). Certificate Authorities (CAs): Role and responsibilities, Trust models and hierarchies, Cross-certification and web of trust. Certificates: Certificate creation and validation, Using certificates for secure communication, Trust anchor management. Applications: Code signing, Document signing, Secure software distribution

Module 5: Cryptanalysis

Cryptanalytic Techniques: Brute force attacks, Differential and linear cryptanalysis, Side-channel attacks (timing attacks, power analysis), Algebraic attacks. Breaking Cryptographic Systems: Case studies of historical cryptanalysis (Enigma, DES), Modern cryptanalytic methods, Quantum cryptanalysis. Attack Simulations: Practical exercises in cryptographic attacks, Tools and software for cryptanalysis, Analyzing vulnerabilities in cryptographic implementations;- Defensive Measures: Strengthening algorithms against attacks, Best practices for secure implementation, Continuous assessment and improvement of cryptographic systems.

Practice Component:

1. Implementing encryption algorithms in programming languages / Implementing and testing encryption algorithms (AES, RSA, ECC).
2. Designing and analyzing cryptographic protocols using tools like ProVerif.
3. Configuring and managing PKI systems/ Setting up a PKI environment and managing digital certificates.
4. Creating and verifying digital signatures using PGP and X.509 certificates.
5. Performing cryptographic attacks and defenses./ Conducting cryptographic attack simulations and analyzing their effectiveness.
6. Analyzing the security of cryptographic protocols.

Suggested Reading:

1. Bruce Schneier, "Applied Cryptography: Protocols, Algorithms, and Source Code in C."
2. Alfred J. Menezes, Paul C. van Oorschot, and Scott A. Vanstone, "Handbook of Applied Cryptography."
3. Niels Ferguson, Bruce Schneier, and Tadayoshi Kohno, "Cryptography Engineering: Design Principles and Practical Applications."
4. William Stallings, "Cryptography and Network Security: Principles and Practice."
5. Christof Paar and Jan Pelzl, "Understanding Cryptography: A Textbook for Students and Practitioners."

CUFS1061: INCIDENT RESPONSE AND MANAGEMENT

Credits: 04 (3+1+0)

Duration: 50 hrs

Course Description:

This course covers the principles and practices of incident response and management in cybersecurity. Students will learn how to develop and implement effective incident response plans, manage security incidents, and recover from cyber attacks. The course also explores the roles and responsibilities of incident response teams.

Course Objectives:

1. Understand the principles of incident response and management in cybersecurity.
2. Develop and implement effective incident response plans.
3. Learn to manage and recover from security incidents and cyber attacks.

Course Outcomes:

On sucessful completion of the course, the student will be able to:

1. Explain the principles and importance of incident response in cybersecurity.
2. Develop comprehensive incident response plans.
3. Manage and coordinate incident response efforts effectively.
4. Perform post-incident analysis and recovery.
5. Evaluate and improve incident response strategies and practices.

Course Content:

Module 1: Incident Response Lifecycle

Overview of the Incident Response Lifecycle; Preparation: Developing an Incident Response Plan (IRP); Identification: Detecting and recognizing incidents; Importance of an organized approach to managing incidents

Module 2: Incident Detection and Analysis

Techniques for detecting cybersecurity incidents; Tools and methodologies for incident analysis; Correlation of events and threat intelligence; Incident classification and prioritization;

Module 3: Containment, Eradication, and Recovery

Strategies for containing cybersecurity incidents to limit damage; Techniques for eradicating threats from systems; Recovery processes to restore normal operations; Ensuring data integrity and system security during recovery

Module 4: Post-Incident Activities

Documentation and reporting of incidents; Lessons learned and continuous improvement, Reviewing and updating the Incident Response Plan; Communication with stakeholders and regulatory bodies;

Module 5: Forensic Readiness

Importance of forensic readiness in incident response; ; Preparing systems and processes for forensic investigation; Ensuring evidence is legally admissible;Integration of forensic readiness into the incident response plan;

Practice Component:

1. Creating and testing incident response plans.
2. Simulating security incidents and response actions.
3. Conducting post-incident analysis and reporting.
4. Coordinating incident response team activities.

Suggested Reading:

1. "Incident Response & Computer Forensics" by Jason T. Luttgens, Matthew Pepe, and Kevin Mandia.
2. "The Art of Incident Response: Detecting and Responding to Cyberattacks" by Sandy Bacik.
3. "Blue Team Handbook: Incident Response Edition" by Don Murdoch.

CUFS1062: MALWARE ANALYSIS AND REVERSE ENGINEERING

Credits: 04 (3+1+0)

Duration: 50 hrs

Course Description:

This course provides an in-depth study of malware analysis and reverse engineering techniques. Students will learn how to analyze malicious software, understand its behavior, and develop strategies to mitigate its impact. The course covers both static and dynamic analysis methods, as well as reverse engineering tools and techniques.

Course Objectives:

1. Understand the principles and techniques of malware analysis.
2. Develop skills in static and dynamic analysis of malicious software.
3. Learn to use reverse engineering tools and techniques to analyze malware behavior.

Course Outcomes:

On the successful completion of this course, students will be able to:

1. Explain the principles and techniques of malware analysis and reverse engineering.
2. Perform static analysis to understand malware structure and code.
3. Conduct dynamic analysis to observe malware behavior in a controlled environment.
4. Utilize reverse engineering tools to analyze and dissect malicious software.
5. Develop strategies to mitigate and defend against malware threats.

Course Content:

Module 1: Malware Types and Behaviors

Introduction to Malware: Definition, types, and characteristics of malware.; Common Malware Types: Viruses, worms, Trojans, ransomware, spyware, adware, rootkits, and botnets.; Malware Behaviors: Persistence mechanisms, propagation methods, evasion techniques, and payload delivery.; Case Studies: Analysis of notable malware incidents and their impacts.

Module 2: Static and Dynamic Analysis

Introduction to Static Analysis: Analyzing malware without execution; file fingerprinting, metadata analysis, and binary code inspection; Introduction to Dynamic Analysis: Executing malware in a controlled environment; monitoring file system, network activity, and memory usage. ;Tools for Static Analysis: Strings, PEiD, IDA Pro.; Tools for Dynamic Analysis: Sandbox environments (e.g., Cuckoo Sandbox), Process Monitor, Wireshark.; Case Studies: Practical examples of static and dynamic analysis.

Module 3: Reverse Engineering Tools

Introduction to Reverse Engineering: Understanding the process of reverse engineering malware.; Key Tools: IDA Pro, Ghidra, OllyDbg, Radare2, Binary Ninja.; Reverse Engineering Techniques: Disassembly, decompilation, debugging.; Tool Integration: Combining multiple tools for comprehensive analysis. ; Case Studies: Demonstrations of reverse engineering using these tools.

Module 4: Deobfuscation Techniques

Introduction to Obfuscation: Understanding why and how malware is obfuscatet; Common Obfuscation Techniques: Packing, encryption, polymorphism, metamorphism.; Deobfuscation Strategies: Unpacking, code normalization, string decryption, control flow analysis.; Tools for Deobfuscation: Unpackers, debuggers, emulators.; Case Studies: Real-world examples of deobfuscating malware.

Module 5: Malware Defense Strategies

Introduction to Malware Defense: Principles of protecting systems from malware. Preventative Measures: Antivirus software, intrusion detection systems, network segmentation.; Detection Techniques: Signature-based, behavior-based, heuristic analysis.; Response and Mitigation: Incident response planning, malware removal, recovery procedures.; Case Studies: Implementing defense strategies in real-world scenarios.

Practice Component:

1. Identify and classify malware samples based on their characteristics.
2. Perform a static analysis of a given malware sample to extract relevant information.
3. Execute a malware sample in a sandbox environment and analyze its behavior.

4. Use IDA Pro to reverse engineer a piece of malware and understand its functionality / Using reverse engineering tools like IDA Pro and OllyDbg.
5. Apply deobfuscation techniques to unravel an obfuscated malware sample / Developing mitigation strategies for malware threats (Simulating malware infection and response scenarios).

Suggested Readings:

1. Sikorski, M., & Honig, A. (2012). Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software. No Starch Press.
2. Egele, M., Scholte, T., Kirda, E., & Kruegel, C. (2012). A Survey on Automated Dynamic Malware-Analysis Techniques and Tools. ACM Computing Surveys.
3. Ligh, M. H., Adair, S., Hartstein, B., & Richard, M. (2010). Malware Analyst's Cookbook and DVD: Tools and Techniques for Fighting Malicious Code. Wiley.
4. Zeltser, L. (2014). Malware Analysis for Incident Responders. SANS Institute.
5. Egele, M., Kruegel, C., Kirda, E., & Vigna, G. (2012). Symantec's Guide to Reverse Engineering. Symantec Press.

CUFS1063: ETHICAL HACKING AND PENETRATION TESTING

Credits: 04 (3+1+0)

Duration: 50 hrs

Course Descriptor:

This course introduces the fundamental concepts and techniques of ethical hacking and penetration testing. Students will learn how to identify, exploit, and mitigate vulnerabilities in systems while adhering to ethical and legal standards. The course emphasizes practical skills in penetration testing methodologies, reconnaissance, exploitation, and reporting.

Course Objectives:

1. To provide students with a comprehensive understanding of penetration testing methodologies and tools.
2. To develop the skills necessary for conducting ethical hacking, including reconnaissance, scanning, exploitation, and post-exploitation.
3. To emphasize the importance of ethical and legal considerations in penetration testing practices.

Course Outcomes:

On the completion of this course, students will be able to:

1. Understand and apply various penetration testing methodologies to assess the security of information systems.
2. Perform reconnaissance and scanning techniques to gather intelligence on target systems.
3. Execute exploitation and post-exploitation techniques to identify and exploit system vulnerabilities.
4. Prepare detailed reports and recommend mitigation strategies based on penetration testing findings.
5. Recognize and adhere to ethical and legal responsibilities in ethical hacking and penetration testing activities.

Course Content:

Module 1: Penetration Testing Methodologies

Introduction to Penetration Testing: Definition, purpose, and scope.; Types of Penetration Testing: Black-box, white-box, and gray-box testing.; Phases of Penetration Testing: Planning, reconnaissance, exploitation, reporting.; Tools and Frameworks: Overview of popular penetration testing tools and frameworks (e.g., Metasploit, Nmap, Burp Suite). **Case Studies**: Examples of real-world penetration tests and their outcomes.

Module 2: Reconnaissance and Scanning

Introduction to Reconnaissance: Passive and active reconnaissance techniques.; Information Gathering: WHOIS lookup, DNS enumeration, social engineering, OSINT.; Scanning Techniques: Network scanning, port scanning, vulnerability scanning.; Tools for Reconnaissance and Scanning: Nmap, Nessus, Wireshark.; Case Studies: Practical examples of reconnaissance and scanning in penetration testing.

Module 3: Exploitation and Post-Exploitation

Introduction to Exploitation: Exploiting vulnerabilities in systems and applications.; Types of Exploits: Buffer overflows, privilege escalation, web application exploits.; Post-Exploitation Techniques: Maintaining access, data exfiltration, pivoting.; Tools for Exploitation: Metasploit, SQLmap, John the Ripper.; Case Studies: Analysis of successful exploitation and post-exploitation scenarios.

Module 4: Reporting and Mitigation

Importance of Reporting: Key elements of a penetration testing report.; Report Writing Techniques: Structuring reports, documenting findings, and recommendations.; Mitigation Strategies: Remediation planning, patch management, configuration changes.; Tools for Reporting: Report generation tools, vulnerability management platforms.; Case Studies: Reviewing and analyzing penetration testing reports.

Module 5: Ethical and Legal Issues

Introduction to Ethics in Hacking: The role of ethics in penetration testing. Legal Frameworks: Laws and regulations governing ethical hacking (e.g., Computer Fraud and Abuse Act, GDPR). Contracts and Agreements: Non-disclosure agreements (NDAs), statements of work (SOW). Certification and Professionalism: Relevant certifications (e.g., CEH, OSCP) and professional conduct. Case Studies: Ethical dilemmas and legal issues in penetration testing.

Practice Component:

1. Reconnaissance and Scanning: Conduct a full reconnaissance and scanning exercise on a simulated target network.
2. Exploitation: Exploit a vulnerable web application using SQL injection and gain unauthorized access.
3. Post-Exploitation: Perform post-exploitation tasks such as privilege escalation and data exfiltration.
4. Report Writing: Create a detailed penetration testing report based on the findings from practical exercises.
5. Ethical Decision-Making: Analyze a case study involving an ethical dilemma in penetration testing and propose a solution.

Suggested Readings:

1. Erickson, J. (2008). Hacking: The Art of Exploitation (2nd ed.). No Starch Press.
2. Engebretson, P. (2013). The Basics of Hacking and Penetration Testing (2nd ed.). Syngress.
3. McClure, S., Scambray, J., & Kurtz, G. (2012). Hacking Exposed 7: Network Security Secrets & Solutions. McGraw-Hill Education.
4. Harris, S. (2019). Gray Hat Hacking: The Ethical Hacker's Handbook (5th ed.). McGraw-Hill Education.
5. Andress, J. (2014). The Basics of Information Security (2nd ed.). Syngress.

CUFS1066: ADVANCED DIGITAL FORENSICS

Credits: 04 (3+1+0)

Duration: 50 hrs

Course Description:

This advanced course delves deeper into the specialized areas of digital forensics, focusing on complex investigation techniques, emerging challenges, and the application of forensic analysis in various digital environments.

Course Objectives:

1. To deepen understanding of advanced forensic techniques and methodologies.
2. To explore emerging trends and challenges in digital forensics.
3. To develop proficiency in analyzing complex digital evidence.
4. To enhance skills in reporting and presenting complex forensic findings.

Course Outcomes:

1. Students will gain advanced knowledge and skills in digital forensics.
2. Students will be able to conduct complex forensic investigations.
3. Students will understand and address emerging challenges in digital forensics.
4. Students will be able to produce and present detailed forensic reports.

Course Content:

Module 1: Advanced Forensic Techniques and Methodologies

Advanced Imaging and Cloning: Techniques for handling large-scale data and complex storage systems; Memory Forensics: Techniques for analyzing volatile memory (RAM) for forensic evidence.; Live Forensics: Conducting forensic investigations on live systems without shutting them down.; Advanced Data Recovery: Recovering data from damaged, encrypted, or sophisticated storage devices.

Module 2: Network Forensics

Introduction to Network Forensics: Overview of network forensic concepts and methodologies.; Traffic Analysis: Techniques for capturing and analyzing network traffic.; Intrusion Detection and Analysis: Identifying and analyzing network intrusions. Log Analysis: Investigating and interpreting logs from various network devices.

Module 3: Mobile Device Forensics

Mobile Forensic Challenges: Understanding the complexities of mobile device forensics.; Acquisition Techniques: Methods for acquiring data from mobile devices (e.g., logical, physical, and file system acquisition); Analysis Tools: Tools and techniques for analyzing mobile data (e.g., Cellebrite, Oxygen Forensics); App Analysis: Investigating data from mobile applications and cloud synchronization.

Module 4: Cloud and IoT Forensics

Cloud Forensics: Challenges and methodologies for conducting forensic investigations in cloud environments.; IoT Forensics: Understanding the forensic implications of Internet of Things devices.; Data Acquisition in Cloud/IoT: Techniques for acquiring data from cloud services and IoT devices. ; Case Studies: Real-world examples of cloud and IoT forensic investigations.

Module 5: Legal and Ethical Challenges in Advanced Forensics

Legal Framework: Understanding the legal challenges in advanced digital forensic investigations. Ethical Considerations: Navigating the ethical dilemmas in handling complex digital evidence. Cross-border Investigations: Addressing the challenges of international digital forensic investigations. Expert Testimony: Preparing and delivering expert testimony in complex cases.

Suggested Readings:

1. Casey, E. (2019). Handbook of Digital Forensics and Investigation. Academic Press.
2. Altheide, C., & Carvey, H. (2011). Digital Forensics with Open Source Tools. Syngress.
3. Quick, D., & Choo, K-K. R. (2018). Cloud Storage Forensics. Syngress.
4. Ademu, I., Imafidon, C., & Preston, D. (2011). Advanced Techniques in Computer Forensics. Springer.

CUFS1067: CYBER SECURITY POLICY AND MANAGEMENT

Credits: 04 (3+1+0)

Duration: 50 hrs

Course Descriptor:

This course provides a comprehensive understanding of the policies and management strategies required to protect information systems in organizations. It emphasizes the governance, frameworks, risk management, business continuity planning, and compliance auditing necessary to establish and maintain robust cyber security practices.

Course Objectives:

1. To introduce students to the principles and best practices in cyber security governance and management.
2. To enable students to assess risks and implement appropriate security frameworks and standards.
3. To prepare students to develop and manage business continuity plans and ensure compliance with security policies and regulations.

Course Outcomes:

By the end of this course, students will be able to:

1. Understand and apply the principles of cyber security governance in organizational settings.
2. Analyze and implement security frameworks and standards to enhance cyber security.
3. Conduct thorough risk assessments and develop effective risk management strategies.
4. Design and manage business continuity plans to ensure organizational resilience.
5. Perform compliance audits and understand regulatory requirements in cyber security.

Course Content:

Module 1: Cyber Security Governance

Introduction to Cyber Security Governance: Definition, importance, and key principles.; Roles and Responsibilities: Stakeholders in cyber security governance.; Cyber Security Policies: Development, implementation, and enforcement.; Governance Models: Centralized vs. decentralized governance.; Case Studies: Analysis of governance failures and successes.

Module 2: Security Frameworks and Standards

Overview of Security Frameworks: NIST Cybersecurity Framework, ISO/IEC 27001.; Implementation of Frameworks: Best practices and challenges.; Security Standards: Understanding and applying relevant standards (e.g., CIS Controls).; Aligning Frameworks with Organizational Goals: Customizing frameworks to fit specific needs.; Case Studies: Application of frameworks in different industries.

Module 3: Risk Assessment and Management

Risk Assessment Fundamentals: Identifying assets, threats, vulnerabilities, and impacts.; Risk Management Strategies: Avoidance, transference, mitigation, and acceptance.; Risk Mitigation Techniques: Implementing controls and monitoring effectiveness.; Continuous Risk Monitoring: Adjusting strategies based on evolving threats.; Case Studies: Real-world examples of risk management practices.

Module 4: Business Continuity Planning

Introduction to Business Continuity Planning (BCP): Importance and objectives.; Developing a BCP: Identifying critical processes and resources.; Disaster Recovery Planning (DRP): Developing and testing recovery strategies.; Crisis Management: Roles and responsibilities during a cyber incident.; Case Studies: Lessons learned from past incidents and disruptions.

Module 5: Compliance and Auditing

Introduction to Compliance: Understanding legal and regulatory requirements.; Compliance Management: Implementing and monitoring compliance programs.; Auditing Processes: Planning, conducting, and reporting security audits.; Common Compliance Challenges: Addressing issues such as data protection and privacy.; Case Studies: Audit findings and their impact on organizational security.

Practice Components:

1. Governance Policy Development: Create a cyber security governance policy for a fictitious organization.
2. Framework Implementation Workshop: Apply the NIST Cybersecurity Framework to a case study.
3. Risk Assessment Exercise: Conduct a risk assessment for a given scenario and propose mitigation strategies.
4. BCP Simulation: Develop and test a business continuity plan for a cyber incident.
5. Compliance Audit Simulation: Perform a mock compliance audit based on a set of given regulations.

Suggested Readings:

1. Whitman, M. E., & Mattord, H. J. (2018). Principles of Information Security (6th ed.). Cengage Learning.
2. Tipton, H. F., & Krause, M. (2007). Information Security Management Handbook (6th ed.). Auerbach Publications.
3. Stallings, W., & Brown, L. (2018). Computer Security: Principles and Practice (4th ed.). Pearson.
4. von Solms, R., & van Niekerk, J. (2013). Information Security Governance. Springer.
5. Ross, R., & McEvilley, M. (2020). Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems. NIST.

CUFS1068: DATA PRIVACY AND PROTECTION

Credits: 04 (4+0+0)

Duration: 40 hrs

Course Descriptor:

This course provides an in-depth exploration of data privacy and protection, focusing on the principles, laws, and technologies essential to safeguarding sensitive information. Students will learn to navigate privacy regulations, respond to data breaches, apply anonymization techniques, and leverage privacy-enhancing technologies.

Course Objectives:

1. To introduce students to the core principles of data protection and the legal frameworks governing data privacy.
2. To equip students with the skills needed to effectively respond to data breaches and protect sensitive information.
3. To familiarize students with advanced techniques in data anonymization and privacy-enhancing technologies.

Course Outcomes:

On the successful completion of this course, students will be able to:

1. Understand and apply fundamental data protection principles to ensure the privacy and security of information.
2. Navigate and comply with global and regional privacy laws and regulations.
3. Develop and implement effective data breach response strategies.
4. Apply data anonymization techniques to protect privacy while maintaining data utility.
5. Utilize privacy-enhancing technologies to strengthen data security in various contexts.

Course Content:

Module 1: Data Protection Principles

Introduction to Data Protection: Importance and fundamental concepts.; Key Data Protection Principles: Lawfulness, fairness, transparency, data minimization, accuracy, storage limitation, integrity, and confidentiality.; Data Lifecycle Management: Collection, storage, processing, sharing, and deletion of data.; Roles and Responsibilities: Data controllers, data processors, and data subjects.; Case Studies: Analysis of data protection failures and successes.

Module 2: Privacy Laws and Regulations

Overview of Privacy Laws: GDPR, CCPA, HIPAA, and other relevant global regulations.; Comparative Analysis: Differences and similarities between various privacy laws.; Compliance Requirements: Understanding and implementing regulatory obligations.; Cross-Border Data Transfers: Challenges and legal considerations.; Case Studies: Legal cases related to privacy violations and their outcomes.

Module 3: Data Breach Response

Introduction to Data Breaches: Types, causes, and consequences.; Data Breach Response Plan: Key components and steps to take during a breach.;Incident Detection and Reporting: Techniques for identifying and reporting breaches.; Notification Requirements: Legal obligations for breach disclosure.; Case Studies: Examination of high-profile data breaches and organizational responses.

Module 4: Data Anonymization Techniques

Introduction to Data Anonymization: Importance and challenges. Anonymization Techniques: K-anonymity, differential privacy, and pseudonymization.;Balancing Privacy and Utility: Techniques to maintain data utility while ensuring privacy.; Re-identification Risks: Understanding and mitigating the risks of re-identification.; Case Studies: Practical applications of anonymization techniques in various industries.

Module 5: Privacy-Enhancing Technologies

Introduction to Privacy-Enhancing Technologies (PETs): Overview and significance.; Types of PETs: Encryption, secure multi-party computation, homomorphic encryption, zero-knowledge proofs.; Implementing PETs: Strategies and best practices for deployment.; Challenges and Limitations: Technical, legal, and ethical considerations.; Case Studies: Real-world examples of PETs in action.

Suggested Readings:

1. Solove, D. J., Schwartz, P. M., & Hartzog, W. (2018). Information Privacy Law (6th ed.). Wolters Kluwer.
2. Tene, O., & Polonetsky, J. (2012). Privacy in the Age of Big Data: A Time for Big Decisions. Stanford Law Review Online.
3. Regan, P. M. (2015). Privacy and Technology: The Emerging Regulation of Algorithms and Artificial Intelligence. Cambridge University Press.
4. Carey, P. (2018). Data Protection: A Practical Guide to UK and EU Law (5th ed.). Oxford University Press.
5. Roessler, B., & Mokrosinska, D. (Eds.). (2015). Social Dimensions of Privacy: Interdisciplinary Perspectives. Cambridge University Press.

BASKET II: DISCIPLINE-SPECIFIC ELECTIVE COURSES

CUFS1072: CYBER LAW AND ETHICS

Credits: 04 (4+0+0)

Course Duration: 40 hours

Course Description:

This course is designed to provide M.Sc. Cyber Security and Digital Forensics students with a comprehensive understanding of the legal and ethical frameworks governing cyberspace. It covers key aspects of cyber law, including IT Act provisions, data protection, intellectual property rights, and cybercrime regulations. The course also delves into the ethical considerations essential for professionals in the field of cyber security and digital forensics.

Course Objectives:

1. To provide a thorough understanding of the legal frameworks and regulations that govern cyberspace.
2. To explore the ethical issues and dilemmas faced by professionals in cyber security and digital forensics.
3. To equip students with the knowledge to navigate and apply cyber laws in professional practice, ensuring compliance and ethical integrity.

Course Outcomes:

Upon successful completion of the course, students will be able to:

1. Understand and interpret the key provisions of the Information Technology Act and other relevant cyber laws.
2. Analyze and apply legal principles to real-world cyber security and digital forensic cases.
3. Identify and address ethical challenges in cyber security and digital forensics.
4. Evaluate the legal implications of cybercrimes and the role of law enforcement agencies.
5. Develop strategies to ensure legal compliance and uphold ethical standards in professional practice.

Course Content:

Module 1: Introduction to Cyber Law

Overview of Cyber Law: Definition, Scope, and Importance. The Information Technology Act, 2000: Objectives, Key Provisions, and Amendments. Jurisdictional Issues in Cyberspace. Legal Recognition of Electronic Records and Digital Signatures. Cyber Law in International Context: Comparative Analysis of Cyber Laws in Different Countries.

Module 2: Cyber Crimes and Legal Responses

Classification of Cyber Crimes: Hacking, Phishing, Identity Theft, Cyberstalking, Cyberbullying, etc. Legal Provisions for Cyber Crimes: Sections 43, 66, 67, and other relevant provisions of IT Act. Role of Law Enforcement Agencies in Combating Cyber Crimes. Case Studies: Landmark Judgments in Cyber Crime Cases. Challenges in Cyber Crime Investigation and Prosecution.

Module 3: Data Protection and Privacy Laws

Data Protection Laws: Overview and Key Principles. The General Data Protection Regulation (GDPR) and its Global Impact. Indian Data Protection Framework: Personal Data Protection Bill. Privacy Rights in the Digital Age. Legal Implications of Data Breaches and Unauthorized Data Access.

Module 4: Intellectual Property Rights in Cyberspace

Introduction to Intellectual Property Rights (IPR) in Cyberspace. Copyright, Trademark, and Patent Issues in Digital Media. Software Piracy, Digital Rights Management (DRM), and Legal Protection. Legal Challenges in Protecting IPR in the Online Environment. Case Studies: Infringement of IPR in Cyberspace and Legal Remedies.

Module 5: Ethics in Cyber Security and Digital Forensics

Introduction to Ethics in Cyber Security. Ethical Hacking: Concepts, Techniques, and Legal Boundaries. Professional Ethics in Digital Forensics: Code of Conduct and Best Practices. Ethical Dilemmas in Cyber Security and Forensic Investigations. Case Studies: Ethical Issues and Resolutions in Cyber Security.

Suggested Readings:

1. Nandan Kamath, "Law Relating to Computers, Internet and E-commerce: A Guide to Cyberlaws and the Information Technology Act, 2000," Universal Law Publishing, 2012.
2. Sunit Belapure and Nina Godbole, "Cyber Security: Understanding Cyber Crimes, Computer Forensics and Legal Perspectives," Wiley India Pvt. Ltd., 2011.
3. Pavan Duggal, "Cyber Law: The Indian Perspective," Saakshar Law Publications, 2020.
4. Jonathan Rosenoer, "CyberLaw: The Law of the Internet," Springer, 1997.
5. Michael E. Whitman and Herbert J. Mattord, "Principles of Information Security," Vikas Publishing House, New Delhi, 2003.
6. Richard A. Spinello, "CyberEthics: Morality and Law in Cyberspace," Jones & Bartlett Learning, 2013.

CUFS1073: CYBER THREAT INTELLIGENCE

Credits: 04 (3+1+0)

Course Duration: 50 hours

Course Description:

This course is designed to provide M.Sc. Cyber Security and Digital Forensics students with an in-depth understanding of Cyber Threat Intelligence (CTI). It covers the processes and methodologies involved in gathering, analyzing, and applying threat intelligence to protect and defend organizational assets. Students will learn how to identify, assess, and mitigate cyber threats using both strategic and tactical intelligence. The course also explores the role of CTI in incident response, threat hunting, and risk management.

Course Objectives:

1. To equip students with the knowledge and skills to collect, analyze, and utilize cyber threat intelligence effectively.
2. To provide an understanding of the various types of cyber threats and the intelligence lifecycle.
3. To enable students to integrate CTI into cyber security strategies and incident response efforts.

Course Outcomes:

Upon successful completion of the course, students will be able to:

1. Understand the key concepts, types, and importance of Cyber Threat Intelligence in cyber security.
2. Analyze and evaluate different sources of threat intelligence and apply them to real-world scenarios.
3. Develop strategies to incorporate threat intelligence into cyber security operations and risk management.
4. Conduct threat intelligence analysis to support incident response and threat hunting activities.

5. Utilize tools and platforms for collecting, analyzing, and sharing threat intelligence.

Course Content:

Module 1: Introduction to Cyber Threat Intelligence

Overview of Cyber Threat Intelligence: Definition, Purpose, and Benefits. The Intelligence Cycle: Collection, Processing, Analysis, Dissemination, and Feedback. Types of Threat Intelligence: Strategic, Tactical, Operational, and Technical. Threat Intelligence vs. Threat Data: Differences and Interrelations. Role of CTI in Cyber Security Operations and Risk Management.

Module 2: Threat Intelligence Collection and Sources

Data Collection Methods: Open Source Intelligence (OSINT), Human Intelligence (HUMINT), Signals Intelligence (SIGINT), and Technical Intelligence (TECHINT).; Sources of Threat Intelligence: Internal Logs, External Feeds, Dark Web Monitoring, Social Media, etc.; Threat Intelligence Platforms (TIPs) and Tools: Overview and Usage.; Challenges in Threat Intelligence Collection: Data Overload, False Positives, and Privacy Concerns.; Legal and Ethical Considerations in Threat Intelligence Gathering.

Module 3: Threat Intelligence Analysis and Reporting

Analysis Techniques: Indicator of Compromise (IOC) Analysis, Threat Actor Profiling, Attack Patterns, and Tactics, Techniques, and Procedures (TTPs).; Tools for Threat Intelligence Analysis: SIEM, STIX, TAXII, YARA, etc.; Developing Threat Intelligence Reports: Structure, Content, and Key Elements. Communicating Threat Intelligence to Stakeholders: Tailoring Reports for Different Audiences. Case Studies: Analysis of Real-World Threat Intelligence Reports.

Module 4: Integrating Threat Intelligence into Cyber Security Operations

Incorporating CTI into Security Operations Centers (SOCs). Role of CTI in Incident Response and Threat Hunting. Enhancing Cyber Defense through Proactive Threat Intelligence. Risk Management and Threat Intelligence: Identifying, Assessing, and Mitigating Risks. Case Studies: Successful Integration of CTI in Organizations.

Module 5: Advanced Topics in Cyber Threat Intelligence

Threat Intelligence Sharing: Collaboration and Information Exchange (ISACs, CERTs). Emerging Threats and Trends: APTs, Zero-Day Exploits, Supply Chain Attacks, etc. Automation and AI in Threat Intelligence: Benefits and Challenges. Building a Threat Intelligence Program: Best Practices and Frameworks. Future of Cyber Threat Intelligence: Evolving Threat Landscapes and Intelligence Techniques.

Practice Component:

1. Hands-on exercises in gathering threat intelligence using OSINT tools and techniques.
2. Practical analysis of IOCs, TTPs, and threat actor profiles using industry-standard tools.
3. Students will develop and present a threat intelligence report based on a simulated attack scenario.
4. Role-playing exercises simulating incident response activities enhanced by threat intelligence.
5. Using a Threat Intelligence Platform (TIP) to collect, analyze, and visualize threat data.

Suggested Readings:

1. Henry Dalziel, “How to Define and Build an Effective Cyber Threat Intelligence Capability,” Syngress, 2014.
2. Chris Sanders, “Practical Packet Analysis: Using Wireshark to Solve Real-World Network Problems,” No Starch Press, 2017.
3. Robert M. Lee and Rob Lee, “The Practice of Network Security Monitoring: Understanding Incident Detection and Response,” No Starch Press, 2013.
4. J. O. Garrison, “Cyber Threat Intelligence: Strategies and Methods,” CreateSpace Independent Publishing Platform, 2016.
5. Scott J. Roberts and Rebekah Brown, “Intelligence-Driven Incident Response: Outwitting the Adversary,” O’Reilly Media, 2017.
6. Mike Chapple and David Seidl, “CompTIA CySA+ Study Guide: Exam CS0-002,” Sybex, 2020.

CUFS1074: SECURE SOFTWARE DEVELOPMENT

Credits: 04 (3+1+0)

Course Duration: **50** hours

Course Description:

This course aims to provide M.Sc. Cyber Security and Digital Forensics students with a comprehensive understanding of secure software development practices. The course covers the principles, methodologies, and tools required to design, develop, and maintain secure software systems. Students will learn to identify and mitigate security vulnerabilities, apply secure coding practices, and integrate security throughout the software development lifecycle (SDLC). The practical component emphasizes hands-on experience in secure coding, threat modeling, and code review.

Course Objectives:

1. To provide an understanding of secure software development principles and practices.
2. To equip students with the skills to identify, assess, and mitigate security vulnerabilities in software applications.
3. To enable students to integrate security into the software development lifecycle, ensuring robust and secure software systems.

Course Outcomes:

Upon successful completion of the course, students will be able to:

1. Understand the importance of security in software development and the impact of insecure coding practices.
2. Identify common security vulnerabilities in software applications and apply secure coding practices to mitigate them.
3. Integrate security into the software development lifecycle, including design, implementation, testing, and deployment phases.

4. Conduct threat modeling, code reviews, and security testing to identify and address security issues in software.
5. Utilize industry-standard tools and methodologies to develop secure software systems and maintain their security post-deployment.

Course Content:

Module 1: Introduction to Secure Software Development

Overview of Secure Software Development: Importance and Challenges. Secure Software Development Lifecycle (SSDLC): Phases and Key Activities. Common Software Vulnerabilities: OWASP Top 10, CWE/SANS Top 25. Principles of Secure Software Design: Least Privilege, Defense in Depth, Fail-Secure Defaults, etc. Legal and Regulatory Requirements for Software Security: GDPR, PCI-DSS, HIPAA, etc.

Module 2: Secure Coding Practices

Secure Coding Standards and Guidelines: OWASP Secure Coding Practices, CERT Secure Coding Standards. Common Coding Vulnerabilities: SQL Injection, Cross-Site Scripting (XSS), Buffer Overflows, etc. Input Validation and Output Encoding: Techniques and Best Practices. Authentication, Authorization, and Session Management: Secure Implementation. Error Handling and Logging: Avoiding Information Leakage and Secure Logging Practices.

Module 3: Security in the Software Development Lifecycle

Threat Modeling: Identifying Threats, Attack Vectors, and Mitigation Strategies. Secure Design and Architecture: Design Patterns, Security Design Reviews. Security Testing: Static and Dynamic Analysis, Penetration Testing, Fuzz Testing. Secure Deployment: Configuration Management, Secure Build Processes, Continuous Integration/Continuous Deployment (CI/CD) Security. Post-Deployment Security: Monitoring, Incident Response, Patching, and Maintenance.

Module 4: Advanced Topics in Secure Software Development

Cryptography in Software Development: Encryption, Hashing, Digital Signatures, and Key Management. Secure API Development: Best Practices for RESTful and SOAP APIs. Secure Mobile Application Development: Platform-Specific Security Considerations (iOS, Android).

DevSecOps: Integrating Security into DevOps Practices. Case Studies: Analysis of High-Profile Software Security Breaches and Lessons Learned.

Module 5: Secure Software Development Tools and Frameworks

Overview of Secure Development Tools: Static and Dynamic Code Analyzers, Dependency Checkers. Secure Development Frameworks: Overview and Application (e.g., Spring Security, OWASP ASVS). Code Review and Peer Review Processes: Best Practices for Security. Secure Version Control Practices: Secure Git Workflows, Secrets Management. Continuous Security Testing and Automation: Integrating Security into CI/CD Pipelines.

Practice Component:

1. Hands-on implementation of secure coding practices in real-world programming scenarios.
2. Developing threat models for different types of software applications and proposing mitigation strategies.
3. Conducting static and dynamic analysis of code, identifying vulnerabilities, and applying fixes.
4. Participating in peer reviews with a focus on security, identifying potential issues, and proposing solutions.
5. Developing secure APIs and conducting security tests to ensure robust implementation.

Suggested Readings:

1. Gary McGraw, “Software Security: Building Security In,” Addison-Wesley Professional, 2006.
2. Michael Howard and Steve Lipner, “The Security Development Lifecycle,” Microsoft Press, 2006.
3. Mark Graff and Kenneth van Wyk, “Secure Coding: Principles and Practices,” O’Reilly Media, 2003.

4. OWASP Foundation, "OWASP Secure Coding Practices - Quick Reference Guide," OWASP, 2010.
5. Jim Manico and August Detlefsen, "Iron-Clad Java: Building Secure Web Applications," McGraw-Hill Education, 2014.
6. Julie JCH Ryan and Daniel J. Ryan, "The Introduction to Secure Software Development," Cengage Learning, 2016.

CUFS1075: MOBILE DEVICE FORENSICS

Credits: 04 (3+1+0)

Course Duration: 50 hours

Course Description:

This course provides an in-depth exploration of mobile device forensics, focusing on the methodologies, tools, and techniques used to investigate mobile devices in digital forensic investigations. Students will gain knowledge about the architecture of mobile devices, the challenges of mobile forensics, and the legal considerations involved. The course also covers data acquisition, analysis, and the extraction of evidence from various mobile operating systems. The practical component offers hands-on experience with mobile forensic tools and techniques.

Course Objectives:

1. To provide students with a comprehensive understanding of mobile device forensics and its importance in digital investigations.
2. To equip students with the skills to acquire, analyze, and preserve digital evidence from mobile devices.
3. To familiarize students with the legal and ethical considerations in mobile device forensics and the challenges posed by emerging mobile technologies.

Course Outcomes:

Upon successful completion of the course, students will be able to:

1. Understand the architecture and operating systems of mobile devices and their implications for forensic investigations.
2. Identify and utilize appropriate tools and techniques for the acquisition and analysis of data from mobile devices.
3. Analyze digital evidence from various mobile platforms, including Android, iOS, and Windows Mobile.

4. Apply forensic principles to extract and interpret data from mobile devices while maintaining the integrity of the evidence.
5. Navigate the legal and ethical challenges associated with mobile device forensics and present findings clearly and concisely.

Course Content:

Module 1: Introduction to Mobile Device Forensics

Overview of Mobile Device Forensics: Definition, Importance, and Challenges. Mobile Device Architecture: Hardware and Software Components. Mobile Operating Systems: Android, iOS, Windows Mobile, and Others. Legal and Ethical Considerations in Mobile Forensics: Privacy Issues, Search and Seizure Laws, Admissibility of Evidence. Introduction to Mobile Device Evidence Types: Call Logs, SMS, Emails, Photos, Videos, Location Data, and Apps.

Module 2: Mobile Device Acquisition

Principles of Mobile Device Evidence Acquisition: Preservation, Chain of Custody, Documentation. Data Acquisition Techniques: Manual, Logical, Physical, and File System Acquisition. Challenges in Data Acquisition: Encryption, Passwords, and Anti-Forensic Techniques. Tools for Mobile Device Acquisition: UFED, XRY, Oxygen Forensic Suite, and Others. Best Practices for Handling Mobile Devices in Forensic Investigations.

Module 3: Analysis of Mobile Device Data

Data Parsing and Analysis: Extracting and Interpreting Evidence from Call Logs, Messages, Contacts, Media Files, and Apps. Analyzing Mobile Applications: Social Media, Instant Messaging, Browsers, and GPS Data. Reverse Engineering Mobile Apps: Understanding the Forensic Implications. Malware Analysis on Mobile Devices: Identifying and Analyzing Malicious Software. Reporting and Presenting Mobile Device Forensic Findings.

Module 4: Advanced Mobile Device Forensics

Mobile Device Cloud Forensics: Acquiring Data from Cloud Services Linked to Mobile Devices. Forensic Analysis of Emerging Mobile Technologies: Wearable Devices, IoT Devices, and Smart Home Systems. Bypass Techniques for Locked or Encrypted Mobile Devices: Legal and Ethical

Considerations. Advanced Techniques for Extracting Deleted Data: Recovering Deleted SMS, Photos, and Other Data. Case Studies: High-Profile Mobile Device Forensic Investigations.

Module 5: Mobile Device Forensic Tools and Frameworks

Overview of Mobile Device Forensic Tools: Open Source and Commercial. In-Depth Study of Key Tools: Cellebrite UFED, XRY, Oxygen Forensic Suite, MOBILedit Forensic, and Magnet AXIOM. Validation and Testing of Mobile Forensic Tools: Ensuring Accuracy and Reliability. Challenges in Using Mobile Forensic Tools: Tool Limitations, Tool Selection, and Cross-Platform Issues.Future Trends in Mobile Device Forensics: Artificial Intelligence, Machine Learning, and Automation.

Practice Component:

1. Hands-on practice with various acquisition techniques (manual, logical, physical).
2. Use forensic tools to analyze call logs, SMS, emails, and other data types.
3. Investigate and analyze data from social media apps, messaging apps, and browser history.
4. Acquire and analyze data from cloud services linked to mobile devices.
5. Validate and compare different mobile forensic tools for accuracy and reliability.

Suggested Readings:

1. Andrew Hoog, “Mobile Forensics: Investigating Data and Image Files on Mobile Devices,” Syngress, 2011.
2. Heather Mahalik, “Practical Mobile Forensics,” Packt Publishing, 2016.
3. Eoghan Casey, “Handbook of Digital Forensics and Investigation,” Academic Press, 2009.
4. Clint P. Garrison, “Digital Forensics for Handheld Devices,” Auerbach Publications, 2010.
5. Lee Reiber, “Mobile Forensics: Advanced Investigative Strategies,” McGraw-Hill Education, 2016.

CUFS1076: CYBER-PHYSICAL SYSTEMS SECURITY

Credits: 04 (3+1+0)

Course Duration: **50** hours

Course Description:

This course delves into the security challenges and solutions associated with Cyber-Physical Systems (CPS), which integrate computing, networking, and physical processes. Students will explore the vulnerabilities, threats, and security measures essential for protecting CPS, including Industrial Control Systems (ICS), the Internet of Things (IoT), and smart grids. The course combines theoretical knowledge with practical applications, enabling students to develop and implement security strategies in real-world CPS environments.

Course Objectives:

1. To provide an understanding of the fundamental concepts and architecture of Cyber-Physical Systems and their security challenges.
2. To equip students with the skills to identify, analyze, and mitigate security threats in CPS, including Industrial Control Systems and IoT.
3. To enable students to design and implement security solutions tailored to the unique requirements of CPS, considering both cyber and physical components.

Course Outcomes:

Upon successful completion of the course, students will be able to:

1. Comprehend the architecture and components of Cyber-Physical Systems and identify potential security vulnerabilities.
2. Assess and analyze security risks associated with CPS, including those related to Industrial Control Systems and IoT.
3. Design and implement security measures to protect CPS against various threats, including cyber-attacks and physical intrusions.
4. Integrate security practices into the development and maintenance of CPS, ensuring resilience and reliability.

5. Apply theoretical knowledge in practical scenarios, securing CPS in industries such as energy, transportation, healthcare, and manufacturing.

Course Content:

Module 1: Introduction to Cyber-Physical Systems (CPS) Security

Overview of Cyber-Physical Systems: Definition, Importance, and Applications. CPS Architecture and Components: Sensors, Actuators, Controllers, Networks, and Physical Processes. Security Challenges in CPS: Threat Landscape, Attack Vectors, and VulnerabilitiesCase Studies: Security Incidents in CPS (e.g., Stuxnet, Ukraine Power Grid Attack). Introduction to Standards and Regulations for CPS Security.

Module 2: Industrial Control Systems (ICS) Security

Overview of Industrial Control Systems: SCADA, DCS, PLCs, and RTUs. Security Challenges in ICS: Threats, Vulnerabilities, and Attack Scenarios. Risk Assessment and Management in ICS: Identifying Critical Assets, Assessing Risks, and Implementing Controls. ICS Security Solutions: Network Segmentation, Intrusion Detection Systems (IDS), and Secure Communication Protocols. Incident Response and Recovery in ICS: Best Practices and Case Studies.

Module 3: Internet of Things (IoT) Security in CPS

IoT in Cyber-Physical Systems: Applications and Security Challenges. IoT Architecture and Protocols: Communication, Data Storage, and Processing. Security Threats in IoT: Device Exploits, Data Breaches, and Botnets IoT Security Solutions: Authentication, Encryption, and Access Control. Securing IoT Devices and Networks: Best Practices and Emerging Trends.

Module 4: Security in Smart Grids and Critical Infrastructures

Introduction to Smart Grids: Components, Functionality, and Security Challenges. Threats to Smart Grid Security: Cyber-Attacks, Physical Attacks, and Insider Threats. Security Solutions for Smart Grids: Encryption, Secure Communication, and Resilience Strategies. Critical Infrastructure Protection: Security Strategies for Energy, Transportation, and Healthcare Systems. Case Studies: Security Breaches in Critical Infrastructures and Lessons Learned.

Module 5: Advanced Topics in CPS Security and Future Trends

Emerging Threats in CPS: AI and Machine Learning-Based Attacks, Quantum Computing. Security for Autonomous Systems: Drones, Autonomous Vehicles, and Robotics. Privacy and Ethics in CPS: Data Protection, Compliance, and Ethical Considerations.Future Trends in CPS Security: Advances in Secure Architectures, AI for CPS Security. Research Directions and Challenges in CPS Security.

Practice Component:

1. Risk Assessment and Threat Modeling: Conduct risk assessments for CPS and develop threat models.
2. ICS Security Lab: Hands-on experience with securing Industrial Control Systems using network segmentation and IDS.
3. IoT Security Lab: Implement security measures for IoT devices, including encryption and access control.
4. Smart Grid Simulation: Analyze and secure a simulated smart grid environment against cyber-attacks.
5. Incident Response Simulation: Practice responding to and recovering from a cyber-attack on a CPS environment.

Suggested Readings:

1. Edward J. M. Colbert and Alexander Kott, “Cyber-Security of SCADA and Other Industrial Control Systems,” Springer, 2016.
2. David W. P. King, “Security in Cyber-Physical Systems: Foundations, Principles, and Applications,” Wiley, 2017.
3. Fei-Yue Wang, “Cyber-Physical Systems: A Computational Perspective,” CRC Press, 2015.
4. Sujeet Shenoi, “Critical Infrastructure Protection,” Springer, 2019.
5. Dieter Gollmann, “Computer Security,” Wiley, 2011.

CUFS1077: ARTIFICIAL INTELLIGENCE IN CYBER SECURITY

Credits: 04 (3+1+0)

Duration: 50 hours

Course Descriptor:

This course explores the integration of Artificial Intelligence (AI) within the field of Cyber Security. It covers the fundamental principles and applications of AI techniques such as machine learning, deep learning, and neural networks in detecting, preventing, and responding to cyber threats. Students will gain practical experience through hands-on labs, developing skills in applying AI to real-world cybersecurity challenges.

Course Objectives:

1. To provide a deep understanding of how AI can be leveraged to enhance cybersecurity measures and address emerging cyber threats.
2. To equip students with the knowledge of various AI techniques and their applications in detecting and mitigating cyber-attacks.
3. To develop practical skills in implementing AI-based solutions to improve the effectiveness and efficiency of cybersecurity operations.

Course Outcomes:

Upon successful completion of this course, students will be able to:

1. Analyze and evaluate the role of AI in enhancing cybersecurity practices.
2. Implement AI algorithms to detect and respond to cyber threats in real-time.
3. Design AI-driven systems for automated threat intelligence and incident response.
4. Assess the ethical considerations and potential risks associated with the use of AI in cybersecurity.
5. Apply advanced AI techniques such as machine learning and deep learning to solve complex cybersecurity challenges.

Course Content:

Module 1: Introduction to AI in CyberSecurity

Overview of AI and its relevance in Cybersecurity. Types of AI: Machine Learning, Deep Learning, Neural Networks. Role of AI in enhancing cybersecurity defense mechanisms Challenges and limitations of AI in cybersecurity

Module 2: Machine Learning for Cyber Threat Detection

Introduction to machine learning algorithms: supervised, unsupervised, and reinforcement learning. Application of machine learning in threat detection and anomaly detectionBuilding and training machine learning models for cybersecurity. Case studies on machine learning in cybersecurity

Module 3: Deep Learning and Neural Networks in Cyber Security

Fundamentals of deep learning and neural networks. Application of deep learning in intrusion detection systems (IDS). Implementing neural networks for malware detection and classification. Real-world examples of deep learning in cybersecurity

Module 4: AI for Automated Threat Intelligence and Incident Response

Overview of threat intelligence and its importance in cybersecurity. Role of AI in automating threat intelligence gathering and analysis. AI-driven incident response: from detection to mitigation. Tools and platforms for AI-based threat intelligence and response

Module 5: Ethical Considerations and Future Trends in AI-Driven Cyber Security

Ethical concerns in AI and cybersecurity: privacy, bias, and accountability. AI in offensive cybersecurity: the dual-use dilemma. Future trends: AI for proactive defense and prediction of cyber threats. Emerging technologies: AI in blockchain security, IoT security, and quantum computing

Practice Component:

1. Implementing machine learning algorithms for anomaly detection in network traffic.
2. Developing a neural network-based model for malware detection.
3. Building and training a deep learning model for intrusion detection.
4. Automating threat intelligence using AI tools and platforms.
5. Case study analysis: AI in real-world cybersecurity scenarios.

Suggested Readings:

1. "Artificial Intelligence in Cybersecurity" by Leslie F. Sikos
2. "Machine Learning and Security: Protecting Systems with Data and Algorithms" by Clarence Chio and David Freeman
3. "Deep Learning for Cybersecurity" by Nandhini Abirami R and Amit Kumar Singh
4. "AI in Cybersecurity" by Reza Montasari and Richard Hill
5. "Hands-On Machine Learning for Cybersecurity: Safeguard your system by making your machines intelligent using the Python ecosystem" by Soma Halder and Sinan Ozdemir

CUFS1078: CLOUD SECURITY

Credits: 04 (3+1+0)

Duration: 50 hours

Course Descriptor:

This course explores the principles and practices of securing cloud computing environments. It covers essential cloud security concepts, technologies, and strategies to protect data, applications, and infrastructure in cloud-based environments. Students will gain practical experience through hands-on labs, focusing on implementing and managing security measures in cloud platforms.

Course Objectives:

1. To provide an in-depth understanding of cloud computing models, architectures, and their associated security challenges.
2. To equip students with the knowledge and skills to implement and manage security measures in various cloud environments.
3. To develop the ability to analyze and address security risks and compliance requirements in cloud computing.

Course Outcomes:

Upon successful completion of this course, students will be able to:

1. Explain the fundamental concepts and models of cloud computing and their security implications.
2. Implement security measures and best practices for different cloud service models (IaaS, PaaS, SaaS).
3. Identify and mitigate common security threats and vulnerabilities in cloud environments.
4. Evaluate and ensure compliance with security standards and regulations relevant to cloud computing.
5. Apply practical skills to secure cloud-based applications and data through hands-on labs and projects.

Course Content:

Module 1: Introduction to Cloud Computing and Security

Overview of cloud computing: models (IaaS, PaaS, SaaS), and architectures; Cloud service providers and deployment models (public, private, hybrid); Cloud security challenges and considerations; Fundamental security principles for cloud environments

Module 2: Cloud Security Technologies and Practices

Identity and Access Management (IAM) in cloud environments; Encryption techniques: data at rest, data in transit; Network security: firewalls, intrusion detection and prevention systems (IDPS); Secure configuration and management of cloud resources

Module 3: Risk Management and Compliance in Cloud Security

Risk assessment and management in cloud environments; Compliance requirements: GDPR, HIPAA, and other regulations; Cloud security standards and frameworks (ISO/IEC 27001, NIST, CSA); Implementing and managing compliance controls in the cloud

Module 4: Securing Cloud-Based Applications

Security considerations for cloud-based application development; Secure software development lifecycle (SDLC) in the cloud; Application security testing and vulnerability assessment; Case studies on securing cloud applications

Module 5: Incident Response and Disaster Recovery in the Cloud

Cloud-specific incident response strategies and procedures; Developing and implementing cloud disaster recovery plans; Backup and data recovery solutions for cloud environments Best practices and tools for cloud incident management

Practice Component:

1. Configuring and managing Identity and Access Management (IAM) in a cloud environment.
2. Implementing encryption for data at rest and data in transit using cloud services.
3. Setting up and securing network resources in a cloud environment (firewalls, IDPS).
4. Conducting a risk assessment and compliance audit for a cloud-based application.
5. Developing a disaster recovery plan and conducting a backup and recovery simulation.

Suggested Readings:

1. Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance by Tim Mather, Subra Kumaraswamy, and Shahed Latif
2. Cloud Security: A Comprehensive Guide to Secure Cloud Computing by Ronald Krutz and Russell Dean Vines
3. Cloud Security for Dummies by Joe Weinman
4. Securing the Cloud: Cloud Computer Security Techniques and Tactics" by Curtis Franklin Jr.
5. Cloud Security and Compliance: A Practical Guide by Ben Potter and Scott Ward

CUFS1079: MACHINE LEARNING IN CYBER SECURITY

Credits: 04 (3+1+0)

Duration: 50 hours

Course Descriptor:

This course delves into the application of machine learning techniques within the realm of cybersecurity. It covers foundational concepts, methodologies, and tools of machine learning as they pertain to various cybersecurity challenges. Students will learn to develop and implement machine learning models for detecting, preventing, and responding to cyber threats through practical, hands-on experience.

Course Objectives:

1. To provide a comprehensive understanding of machine learning techniques and their applications in cybersecurity.
2. To equip students with practical skills in designing, implementing, and evaluating machine learning models for various cybersecurity tasks.
3. To develop the ability to analyze and address the challenges and limitations of applying machine learning in real-world cybersecurity scenarios.

Course Outcomes:

Upon successful completion of this course, students will be able to:

1. Understand and explain key machine learning concepts and algorithms relevant to cybersecurity.
2. Develop and apply machine learning models for detecting and classifying cyber threats.
3. Implement machine learning-based solutions to enhance cybersecurity defenses and incident response.
4. Evaluate the performance and effectiveness of machine learning models in cybersecurity applications.
5. Address and mitigate challenges and limitations associated with machine learning in cybersecurity.

Course Content:

Module 1: Introduction to Machine Learning in CyberSecurity

Overview of machine learning and its relevance to cybersecurity. Types of machine learning: supervised, unsupervised, and reinforcement learning. Key algorithms: decision trees, SVM, clustering, neural networks. Introduction to cybersecurity threats and challenges addressed by machine learning

Module 2: Data Preparation and Feature Engineering

Data collection and preprocessing for cybersecurity applications. Feature selection and extraction techniques. Handling imbalanced data and dealing with noisy data. Case studies on data preparation in cybersecurity contexts

Module 3: Machine Learning Models for Threat Detection

Supervised learning models for malware detection: logistic regression, SVM, random forests. Unsupervised learning models for anomaly detection: clustering, autoencoders. Model training, validation, and evaluation techniques. Practical examples and case studies

Module 4: Advanced Machine Learning Techniques in Cyber Security

Deep learning models for complex cybersecurity problems: CNNs, RNNs. Applying reinforcement learning to adaptive security measures. Ensemble methods and model stacking for improved performance. Real-world applications and challenges

Module 5: Practical Considerations and Ethical Implications

Practical challenges in deploying machine learning models in production environments. Ethical considerations: privacy, fairness, and accountability. Future trends and emerging technologies in machine learning and cybersecurity. Case studies on ethical dilemmas and practical issues

Practice Component:

1. Building and evaluating a supervised learning model for malware classification.
2. Implementing an unsupervised learning model for detecting anomalies in network traffic.
3. Applying deep learning techniques to identify and classify cyber threats.

4. Data preparation and feature engineering for a cybersecurity machine learning project.
5. Evaluating and addressing the performance and ethical issues of machine learning models.

Suggested Readings:

1. Machine Learning for Cybersecurity: Principles, Techniques, and Applications by Raffael Marty
2. Machine Learning and Security: Protecting Systems with Data and Algorithms by Clarence Chio and David Freeman
3. Hands-On Machine Learning for Cybersecurity by Soma Halder and Sinan Ozdemir
4. Machine Learning for Cybersecurity Cookbook: Over 50 recipes to detect and prevent cyber threats using machine learning by Emmanuel Tsukerman
5. Applied Machine Learning for Cyber Security: Real-time Threat Detection and Response by Josh Corman and Andrew Ginter

BASKET III: INTERNSHIP IN CYBER SECURITY AND DIGITAL FORENSICS

A. CUTM1065 Summer Internship / **Credits: 02**
CUTM1066 Minor Project **Duration:** 02-04 weeks

B. CUTM 1071 Internship in 2nd year: **Credits: 04**
Duration: 04-08 weeks

Course Description:

The Internship offers students practical experience in a professional setting, applying their theoretical knowledge to real-world challenges. Students will work with industry professionals on projects related to cybersecurity and digital forensics, gaining hands-on experience in various aspects such as threat analysis, incident response, forensic investigation, and security management. This course aims to bridge the gap between academic learning and practical application, preparing students for careers in the field.

Course Objectives:

1. To provide students with real-world experience in applying cybersecurity and digital forensics concepts and techniques.
2. To develop professional skills and competencies relevant to the cybersecurity and digital forensics industry.
3. To facilitate the application of academic knowledge to practical scenarios, fostering a deeper understanding of real-world challenges and solution**s.**

Course Outcomes:

Upon successful completion of the internship, students will be able to:

1. Apply theoretical knowledge of cybersecurity and digital forensics to practical, real-world problems and projects.
2. Develop and implement effective strategies for threat analysis, incident response, and forensic investigations in a professional setting.

3. Gain practical experience in professional environments, improving their technical and soft skills, such as communication, teamwork, and project management.
4. Evaluate and contribute to the development of security and forensic policies, procedures, and best practices within the organization.
5. Demonstrate professional growth and readiness for a career in cybersecurity and digital forensics through reflective practice and feedback from industry mentors.

BASKET IV: RESEARCH

CUFS1069: RESEARCH METHODOLOGY

Credits: 04 (3+0+1)

Course duration: 50 hrs

Course Description:

This course provides comprehensive coverage of the principles and practices of research methodology. It aims to equip students with the necessary skills to conduct independent research, including literature review, research planning, data collection and analysis, and effective communication of research findings. The course also addresses ethical issues, intellectual property rights, and the components essential for writing research papers and theses.

Course Objectives:

1. To understand the various types of research and methodologies involved in conducting effective and reliable research.
2. To develop the skills required to collect, analyze, and interpret data accurately and effectively.
3. To learn the essential components and best practices for writing research papers and theses, as well as understanding ethical issues and intellectual property rights.

Course Outcomes:

On successful completion of this course, students will be able to:

1. Conduct comprehensive literature reviews to inform and support research.
2. Develop and execute detailed research plans and designs.
3. Apply appropriate data collection methods and analyze data using statistical tools.
4. Write structured and well-documented research papers and theses.
5. Understand and address ethical issues, intellectual property rights, and copyright in research.

Course Content:

Module 1: Basics of Research

Objectives and types of research: Descriptive vs. Analytical, Applied vs. Fundamental, Quantitative vs. Qualitative, and Conceptual vs. Empirical; Research Formulation: Literature review and development of hypothesis; Research design and methods: Developing a research plan - Exploration, Description, Diagnosis, and Experimentation; Determining experimental and sample designs

Module 2: Data Analysis Methods

Data Collection and Analysis: Methods of data collection – Sampling methods and data processing; Data Analysis: Types of data, Basic concept of frequency distribution, Measure of central values – Mean, median, and mode, Measure of dispersion, Range, mean deviation and standard deviation, Probability theory and classical definition of probability, Bayes theorem of probability, Conditional probability and coincidence probability; Statistical Analysis: Chi-square test, ANOVA, SPSS; Types of Errors and Interpretation of Findings

Module 3: Scientific Reports and Thesis Writing

Reporting and thesis writing: Structure and components of scientific reports and thesis; Significance and different steps in the preparation; Illustrations, Bibliography; Presentations: Oral and Poster; Importance of effective communication in scientific research

Module 4: Ethical Issues and Intellectual Property Rights

Basics of ethical issues in research; Understanding intellectual property rights and copyright; Ethical standards and practices in research; Plagiarism and how to avoid it; Legal aspects of research and intellectual property

Module 5: Advanced Research Techniques and Tools

Advanced research methodologies and their applications; Use of software tools in research: SPSS, R, NVivo; Multivariate analysis techniques; Meta-analysis and systematic reviews; Emerging trends and future directions in research methodology

Project Component:

1. Calculation of mean, median, and mode, standard deviation, variance, perform chi-square test and T-test and student’s T-test on a set of values from Minor Project

2. Write a review article

Suggested Readings:

1. Research Methodology: Methods and Techniques by C.R. Kothari, Gaurav Garg, New Age International Publishers.
2. Research Design: Qualitative, Quantitative, and Mixed Methods Approaches by John W. Creswell, J. David Creswell, SAGE Publications.
3. The Craft of Research by Wayne C. Booth, Gregory G. Colomb, Joseph M. Williams, University of Chicago Press.
4. Practical Research: Planning and Design by Paul D. Leedy, Jeanne Ellis Ormrod, Pearson.
5. Publication Manual of the American Psychological Association by American Psychological Association.
6. Research Methodology, by Sinha, S.C. and Dhiman, A.K., 2002. EssEss Publications.
7. Research Methods: the concise knowledge base by Trochim, W.M.K., 2005; Atomic Dog Publishing. 270p.
8. Research Methods: A Process of Inquiry, Allyn and Bacon by Anthony, M., Graziano, A.M. and Raulin, M.L., 2009.

CUFS1070: CAPSTONE PROJECT AND THESIS

Credits: 16

Duration: 4 months (approximately 300 hours)

Course Description:

The Capstone Project and Thesis course is the culmination of the M.Sc. Cyber Security and Digital Forensics program, designed to integrate and apply the knowledge and skills acquired throughout the coursework. Students will undertake a comprehensive research project or a practical, industry-relevant project that addresses a significant problem or challenge within the field. This course emphasizes independent research, critical analysis, and practical application, culminating in a formal thesis and project presentation. The Capstone Project and Thesis aim to demonstrate the student's ability to conduct high-quality research, solve complex problems, and contribute to the field of cybersecurity and digital forensics.

Course Objectives:

1. To enable students to apply advanced research methods and problem-solving techniques to a significant project or thesis topic in cybersecurity or digital forensics.
2. To develop students' ability to conduct independent research, including data collection, analysis, and interpretation, culminating in a well-documented thesis.
3. To enhance students' skills in presenting and communicating their research findings and project outcomes effectively to both academic and professional audiences.

Course Outcomes:

Upon successful completion of the Capstone Project and Thesis course, students will be able to:

1. Demonstrate proficiency in conducting independent, original research or practical projects that address significant problems in cybersecurity or digital forensics.
2. Apply advanced analytical and methodological skills to develop and execute a research plan or project strategy.

3. Produce a high-quality thesis that adheres to academic standards and showcases the ability to critically evaluate and synthesize research findings.
4. Effectively communicate research findings and project results through a formal thesis and oral presentation.
5. Demonstrate the ability to manage and complete a substantial research or project task within a set timeframe, exhibiting project management and organizational skills.

Centurion
UNIVERSITY
Shaping Lives...
Empowering Communities...

Centurion University of Technology and Management, Odisha

CAMPUSES:

Paralakhemundi Campus
Village Alluri Nagar
P.O. – R Sitapur, Via- Uppalada
Paralakhemundi, Dist.- Gajapati
Odisha, India. PIN– 761211

Bhubaneswar Campus
Ramchandrapur
P.O. – Jatni, Bhubaneswar
Dist.- Khurda, Odisha,
India, PIN– 752050

Balangir Campus
Behind BSNL Office
IDCO land, Rajib Nagar
Dist.- Balangir, Odisha
India, PIN-767001

Rayagada Campus
IDCO Industrial Area
Pitamahal, Rayagada
Dist.-Rayagada, Odisha
India, PIN-765001

Balasore Campus
Gopalpur,
P.O.-Balasore
Dist.-Balasore, Odisha
India, PIN-756044

Chatrapur Campus
Ramchandrapur,
Kaliabali Chhak,
P.O-Chatrapur, Dist.-Ganjam
Odisha, India, PIN-761020