PG Diploma in Cyber Security

Course Structure

w.e.f. 2022-23

Department of Computer Engineering

Gujarat Power Engineering and Research Institute, Mevad

Constituent College of Gujarat Technological University
Nr. Toll Booth, Mehsana –Ahmedabad Expressway, Mehsana

PG Diploma in Cyber Security

Course Structure, Teaching Scheme

w.e.f. 2022-23

Rationale of the Program:

Post Graduate Diploma in Cyber Security program (PGDCS) of One Year duration is offered at the Gujarat Power Engineering and Research Institute (GPERI), a Constituent College of GTU which is located at Mehsana, North Gujarat region campus.

It is a unique program designed to impart the essential skills to cater to the fastest-growing trends in the industry. Cyber security is the application of technologies, processes, and controls to protect systems, networks, programs, devices and data from cyber-attacks. It aims to reduce the risk of cyber-attacks and protect against the unauthorized exploitation of systems, networks and technologies. Cyber security is a critical business issue for every organization. It addresses people, processes, and technology. PGDCS program prepares fresh graduates and mid-career professionals to take up various cyber security career opportunities in different geographies of the world.

The contribution of Cyber Security in protecting business networks is immense. With the increase in cyber security risks, it has become one of the most important international agendas for almost every organization. Hacking and other security failures, which might endanger the global economy, have made it imperative for businesses across the globe to recruit professionals who are capable of filling major skill gaps in cyber security.

Program Outcome

- **Knowledge in Mathematics and Computer Science:** Understand the basic concepts, fundamental principles and scientific theories related to Data Science.
- **Abstract thinking:** Ability to absorb and understand the abstract concepts that lead to various advanced theories in Mathematics, Statistics, and Computer science.
- **Modelling and solving:** Ability in modelling and solving problems by identifying and employing the appropriate existing theories and methods.
- **Advanced theories and methods:** Understand advanced theories and methods to design solutions for complex data science problems.
- **Applications in Sciences:** Understand the role of mathematical sciences and apply the same to solve real-life problems in fields of data science.
- **Modern software tool usage:** Acquire the skills in handling scientific tools towards problem-solving and solution analysis.
- **Environment and sustainability:** Understand the significance of preserving the environment towards sustainable development.

- **Ethics:** Imbibe ethical, moral and social values in personal and social life leading to a highly cultured and civilized personality. Continue to enhance the knowledge and skills in mathematics and computer science for constructive activities, and demonstrate the highest standards of professional ethics.

- **Individual and teamwork:** Function effectively as an individual, and as a member or leader in diverse teams, and in multidisciplinary settings.

- **Communication:** Develop various communication skills such as reading, listening, and speaking which will help in expressing ideas and views clearly and effectively.

- **Project management and Research:** Demonstrate knowledge, understand the scientific and management principles and apply these to one's own work, as a member/ leader in a team to manage projects and multidisciplinary research environments. Also, use the research-based knowledge to analyse and solve advanced problems in data science.

- **Life-long learning:** Recognize the need for, and have the preparation and ability to engage in independent and life-long learning in the broadest context of technological change.

Course Details:

Sr. No.	Name of Course and Specialization	Department	Intake (As per AICTE)	Duration of Course (Year)	Proposed Fee (Rs.)
1.	**Post Graduate Diploma (Cyber Security)**	Computer Engineering, GPERI	30	01 (No. Of semesters - 02)	Rs. 12,500 /- per Semester

Admission Eligibility:

Bachelor's or Master's Degree in Engineering (Computer Egg./CSE/IT/ICT/EC)
OR
Bachelor or Master in Science (with Computer Science / IT/Computer Application)
OR
Bachelor or Master (IT/Computer Application) from any recognized University approved by UGC AIU

Permission may be granted to start the PG diploma in Cyber Security at GPERI.

PG Diploma in Cyber Security

Course Structure, Teaching Scheme
w.e.f. 2022-23

(Proposed Tentative) Course Structure & Syllabus

Semester-I										
	Courses	**L**	**T**	**P**	**Cr**	**E**	**M**	**I**	**V**	**Total**
	Principles of Cyber Security	4	0	2	5	70	30	20	30	150
	Fundamental of Computer Networking and Security	4	0	2	5	70	30	20	30	150
	Cyber Security Techniques	4	0	2	5	70	30	20	30	150
	Computational Number Theory and Cryptography	4	0	2	5	70	30	20	30	150
					20					

Semester-II										
	Courses	**L**	**T**	**P**	**Cr**	**E**	**M**	**I**	**V**	**Total**
	Artificial Intelligence in Cyber Security	3	0	2	4	70	30	20	30	150
	Cloud Computing and Security	3	0	0	3	70	30	20	30	150
	Advanced Cryptography	3	0	2	4	70	30	20	30	150
	Ethical Hacking Practices	2	0	2	3	70	30	20	30	150
	Defensive Programming (Elective-I)	3	0	2	4	70	30	20	30	150
	Operating System and Host Security (Elective-I)	3	0	2	4	70	30	20	30	150
	Mini Project	0	0	4	2	-	-	30	70	100
					20					

PG Diploma in Cyber Security

Course Structure, Teaching Scheme
w.e.f. 2022-23

SEMESTER-I

Course Name: Principles of Cyber Security
Subject Code:

Teaching and Examination Scheme:

Teaching Scheme			Credits	Examination Marks				Total Marks
L	T	P	C	Theory Marks		Practical Marks		
				ESE(E)	PA (M)	PA (V)	PA (I)	
4	0	2	5	70	30	20	30	150

Content:

Sr. No.	Content	Teaching Hours	Module Weightage (%)
1.	Systems Vulnerability Scanning Overview of vulnerability scanning, Open Port / Service Identification, Banner / Version Check, Traffic Probe, Vulnerability Probe, Vulnerability Examples, OpenVAS, Metasploit. Networks Vulnerability Scanning - Netcat, Socat, understanding Port and Services tools - Datapipe, Fpipe, WinRelay, Network Reconnaissance – Nmap, THC-Amap and System tools. Network Sniffers and Injection tools – Tcpdump and Windump, Wireshark, Ettercap, Hping Kismet	12	25
2.	Network Defense tools Firewalls and Packet Filters: Firewall Basics, Packet Filter Vs Firewall, Packet Characteristic to Filter, Stateless Vs Stateful Firewalls, Network Address Translation (NAT) and Port Forwarding, Snort: Introduction Detection System	9	25
3.	Web Application Tools Scanning for web vulnerabilities tools: Nikto, W3af, HTTP utilities - Curl, OpenSSL and Stunnel, Application Inspection tools – Zed Attack Proxy, Sqlmap. DVWA, Webgoat, Password Cracking and Brute-Force Tools – John the Ripper, L0htcrack, Pwdump, HTC-Hydra	9	25
4.	Introduction to Cyber Crime and law Cyber Crimes, Types of Cybercrime, Hacking, Attack vectors, Cyberspace and Criminal Behavior, Clarification of Terms, Traditional Problems Associated with Computer Crime, Introduction to Incident Response, Digital Forensics, Realms of the Cyber world, Recognizing and Defining Computer Crime, Contemporary Crimes, Contaminants and Destruction of Data, Indian IT ACT 2000.	6	10
5.	Introduction to Cyber Crime Investigation Keyloggers and Spyware, Virus and Warms, Trojan and backdoors,	9	15

	Steganography, DOS and DDOS attack, SQL injection, BufferOverflow, Attack on wireless Networks.		

Reference Books:

1. Cyber Security Understanding Cyber Crimes, Computer Forensics and Legal Perspectives by Nina Godbole and Sunit Belpure, Publication Wiley
2. Cyber Security and Cyber Laws Paperback – 2018 by Alfred Basta, Nadine Basta , Mary Brown , Ravinder Kumar, publication Cengage 3.
3. Anti-Hacker Tool Kit (Indian Edition) by Mike Shema, Publication Mc Graw Hill.
4. Cyber security and laws – An Introduction, Madhumita Chaterjee, Sangita Chaudhary, Gaurav Sharma, Staredu Solutions

Course Outcome:

1: Describe system and web vulnerability.

2: Evaluate network defence tools.

3: Understand the cyber laws

4: Investigate a cybercrime, prepare report and apply laws for the case

PG Diploma in Cyber Security

Course Structure, Teaching Scheme

w.e.f. 2022-23

SEMESTER-I

Course Name: Fundamental of Computer Networking and Security
Subject Code:

Teaching and Examination Scheme:

Teaching Scheme			Credits	Examination Marks				Total Marks
				Theory Marks		Practical Marks		
L	T	P	C	ESE(E)	PA (M)	PA (V)	PA (I)	
4	0	2	5	70	30	20	30	150

Content:

Sr. No.	Content	Teaching Hours	Module Weightage (%)
1.	Unit I: Computers and Cyber Security Introduction to Computers, Computer History, Software, Hardware, Classification, Computer Input-Output Devices, Windows, DOS Prompt Commands, Linux/Mac Terminal and Commands, Basic Computer Terminology, Computer Security models, Computer Security Terms, Computer Ethics, Business and Professional Ethics, Need for cyber security; Cyber Frauds and crimes, Digital Payments, Various Search Engines, Introduction to Auditing, Deep Web, VAPT, Smartphone Operating systems, introduction to compliances ,Globalization and border less world.	8	20
2.	Unit II: Python Scripting and PHP Basics Python Basics, Variables and Types, Lists, Basic Operators, String Formatting, Basic String Operations, Conditions, Loops, Functions, Classes and Objects, Dictionaries, Modules and Packages.	6	15
3.	Unit III: Cyber Laws Need for Cyber Regulations; Scope and Significance of Cyber laws : Information Technology Act 2000; Network and Network Security, Access and Unauthorised Access, Data Security, E Contracts and E Forms. Penal Provisions for Phishing, Spam, Virus, Worms, Malware, Hacking, Trespass and Stalking; Human rights in cyberspace, International Co-operation in investigating cybercrimes.	8	20
4.	Unit IV: Encoding Encoding: Charset, ASCII, UNICODE, URL Encoding, Base64, Illustration: ISBN/ QR Code/ Barcode, Binary hamming codes and Binary Reedmuller codes.	6	15
5.	Unit V: Web Application Architecture HTML Basics, XAMPP	6	15

	Server Setup, Hosting Websites Linux, Apache, Virtualisation, Server Configurations, Web Application Firewalls..		

Reference Books: Suggested Readings:

1. Langtangen, H.P. (2012). Python Scripting for Computational Science (4th Ed.). Springer
2. Behrouz A. Forouzan (2004). Data communication and Networking. Tata McGraw-Hill.
3. Kurose, James F. & Ross, Keith W. (2003). Computer Networking: A Top-Down Approach Featuring the Internet (3rd Ed.). Pearson Education.
4. Shklar, L. & Rosen, R. (2009). Web Application Architecture: Principles, Protocols and Practices (2nd Ed.). John Wiley & Sons.
5. Craig, B. (2012). Cyber Law: The Law of the Internet and Information Technology. Pearson.

Course Outcome:

1. Understand the fundamentals of computer networks and protocols.

2. Differentiate the different layers of issues, solutions and working

3.Apply the defending approach against network security threats.

4.Apply cryptographic algorithms to achieve security goals.

5.Assess the security protocols to provide a secure communication network.

PG Diploma in Cyber Security

Course Structure, Teaching Scheme

w.e.f. 2022-23

SEMESTER-I

Course Name: Cyber Security Techniques
Subject Code:

Type of course: PG diploma

Teaching and Examination Scheme:

Teaching Scheme			Credits	Examination Marks				Total Marks
L	T	P	C	Theory Marks		Practical Marks		
				ESE(E)	PA (M)	PA (V)	PA (I)	
4	2	0	5	70	30	20	10	150

Content:

Sr. No.	Content	Teaching Hours	Module Weightage (%)
1	Introduction Security services, security services, security mechanisms Finite fields – group, ring, fields, modular arithmetic, The Euclidean algorithm. Symmetric Cipher Model, Cryptography, Cryptanalysis and Attacks; Substitution and Transposition techniques	7	15%
2	Stream ciphers and block ciphers, Block Cipher structure, Data Encryption standard (DES) with example, strength of DES, Design principles of block cipher, AES with structure, its transformation functions, key expansion, example and implementation	5	10%
3	Multiple encryption and triple DES, Electronic Code Book, Cipher Block Chaining Mode, Cipher Feedback mode, Output Feedback mode, Counter mode	4	5%
4	Public Key Cryptosystems with Applications, Requirements and Cryptanalysis, RSA algorithm, its computational aspects and security, Diffie-Hillman Key Exchange algorithm, Man-in-Middle attack	7	15%
5	Cryptographic Hash Functions, their applications, Simple hash functions, its requirements and security, Hash functions based on Cipher Block Chaining, Secure Hash Algorithm (SHA)	5	10%
6	Message Authentication Codes, its requirements and security, MACs based on Hash Functions, Macs based on Block Ciphers	5	10%
7	Digital Signature, its properties, requirements and security, various digital signature schemes (Elgamal and Schnorr), NIST digital Signature algorithm	4	8%
8	Key management and distribution, symmetric key distribution using	4	7%

	symmetric and asymmetric encryptions, distribution of public keys, X.509 certificates, Public key infrastructure		
9	Remote user authentication with symmetric and asymmetric encryption, Kerberos	3	5%
10	Web Security threats and approaches, SSL architecture and protocol, Transport layer security, HTTPS and SSH	6	10%

Reference Books:

1. Cryptography And Network Security, Principles And Practice Sixth Edition, William Stallings, Pearson
2. Information Security Principles and Practice By Mark Stamp, Willy India Edition
3. Cryptography & Network Security, Forouzan, Mukhopadhyay, McGrawHill
4. Cryptography and Network Security Atul Kahate, TMH
5. Cryptography and Security, C K Shyamala, N Harini, T R Padmanabhan, Wiley-India
6. Information Systems Security, Godbole, Wiley-India
7. Information Security Principles and Practice, Deven Shah, Wiley-India
8. Security in Computing by Pfleeger and Pfleeger, PHI
9. Build Your Own Security Lab : A Field Guide for network testing, Michael Gregg, Wiley India

Course Outcome:

Students will be able to

Sr. No.	CO statement
CO-1	Define terms related to cryptography, hashing, message authentication code, digital signature.
CO-2	Describe and discuss symmetric key cryptography algorithms, public key cryptography algorithms, hashing algorithms, Message authentication code generation algorithms, digital signature algorithms, key generation and key management, issues in web security and solution, issues in Transport layer security and solution.
CO-3	Demonstrate the generation of keys and execution of symmetric and public key algorithms from given data.
CO-4	Implement cryptography solution for given security problem by identifying strength and weaknesses of algorithms based on cryptanalytic and brute force attack

PG Diploma in Cyber Security

Course Structure, Teaching Scheme
w.e.f. 2022-23

SEMESTER-I

Course Name: Computational Number Theory and Cryptography
Subject Code:

Type of course: PG diploma

Prerequisite: Basic knowledge of Computer Networks and Basic mathematics

Rationale: The course focuses on mathematical foundation. It highlights the basics of number theory like, GCD, Divisibility, Prime number etc. This course includes algebraic structure for Groups, Discrete logarithms and Classification. Probability theory is important to understand the concept of probability and conditional probability. Coding theory is important for liner code, hamming code and syndrome decoding. Pseudorandom number is used for Next bit predictor and Blum-Blum-Shub Generator. All mathematical concepts are highly important for the mathematical foundation and calculation of Cyber Security.

Teaching and Examination Scheme:

Teaching Scheme			Credits	Examination Marks				Total Marks
L	T	P	C	Theory Marks		Practical Marks		
				ESE(E)	PA (M)	PA (V)	PA (I)	
4	2	0	5	70	30	20	10	150

Content:

Sr. No.	Content	Teaching Hours	Module Weightage (%)
1	**Introduction to Number Theory** Introduction-Divisibility - Greatest common divisor – Primes- Prime numbers – Cardinality of Primes, Fundamental theorem of arithmetic - Mersenne primes - Fermat numbers, Fermat's and Euler's Theorem, Testing for Primality, Factorization, The Chinese Reminder Theorem, Quadratic Congruence, Exponentiation and Logarithms, Discrete Logarithms	**10**	**20**
2	**Pseudorandom Number Generation and Stream Ciphers** Principles of Pseudorandom Number Generation, Principles of Pseudorandom Number Generation using a Block Cipher, Stream Ciphers, RC4 , True Random Number Generators	**08**	**15**
3	**Discrete Mathematics for Cryptography** Cryptography and Modular Arithmetic, Inverses & GCDs, The RSA Cryptosystems, Mathematical Induction, Recursion, Recurrences and Induction, Recurrences and Selection	**05**	**10**

4	**Coding Theory** Introduction - Basic concepts: codes, minimum distance, equivalence of codes, Linear codes - Generator matrices and parity-check matrices - Syndrome decoding – Hamming codes - Hadamard Code - Goppa codes	**08**	**15**
5	**Cryptographic Hash Functions** Application of Cryptographic Hash Functions, Two Simple Hash Functions, Requirements and Security, Hash Functions Based on Cipher Block Chaining, Secure Hash Functions (SHA), SHA-512	**05**	**10**
6	**Probability Theory** Introduction – Concepts of Probability - Conditional Probability - Baye's Theorem - Random Variables – discrete and continuous- central Limit Theorem-Stochastic Process- Markov Chain.	**07**	**15**
7	**Algebraic Structures and Finite Fields** Groups – Cyclic groups, Co sets, Modulo groups - Primitive roots – Discrete logarithms The Euclidean Algorithm, Modular Arithmetic, Algebraic Structures-Groups, Rings and Fields, Future Fields of the Form GF(2"), Polynomial Arithmetic, Finite Fields of the Form GF(2^n)	**07**	**15**

Reference Books:

1. Sheldon M Ross, "Introduction to Probability Models", Academic Press, 2003.
2. Joseph A. Gallian, ''Contemporary Abstract Algebra', Narosa, 1998.
3. Cryptography and Network Security by William Stallings 5th Edition Pearson Education
4. Ivan Niven, Herbert S. Zuckerman, and Hugh L. Montgomery, 'An introduction to the theory of numbers', John Wiley and Sons 2004.
5. C.L. Liu, 'Elements of Discrete mathematics', McGraw Hill, 2008.
6. Cryptography and Network Security by Behrouz A. Forouzan TMH Publication

Course Outcome:

After learning the course the students should be able to:

1. To learn about Number theory including Divisibility, Greatest common divisor and Prime numbers.
2. To understand and apply Euclidean algorithm, Fermat's theorem and Euler's theorem.
3. To calculate probability for discrete random variables and continuous random variables.
4. To apply the concept of Coding.
5. To use Pseudorandom number generation for Next Bit Predictors and Blum-Blum-Shub Generator.

SEMESTER-II

Course Name: Artificial Intelligence in Cyber Security
Subject Code:

Teaching and Examination Scheme:

Teaching Scheme			Credits	Examination Marks				Total Marks
L	T	P	C	Theory Marks		Practical Marks		
				ESE(E)	PA (M)	PA (V)	PA (I)	
3	0	2	4	70	30	30	20	150

Content:

Sr. No.	Content	Teaching Hours	Module Weightage (%)
1.	Unit 1: Artificial Intelligence Core Concepts and Tools Evolution of AI: from expert systems to data mining, Types of machine learning, Algorithm training and optimization, AI in the context of cyber security, Setting up AI for cyber security arsenal, Python for AI and cyber security	6	25
2.	Unit 2: Detecting Cyber Security Threats with AI Detecting spam with perceptron, Spam detection with SVMs, Phishing detection with logistic regression and decision trees, Spam detection with Naïve Bayes, Malware analysis at glance, Decision tree malware detectors, detecting metamorphic malware with HMMs, Advanced malware detection with deep learning, Network Anomaly detection techniques, Network attack classification, Detecting botnet topology, Different ML algorithms for botnet detection	10	25
3.	Unit 3: Protecting Sensitive Information and Assets Authentication abuse prevention, account reputation scoring, User authentication with keystroke recognition, Biometric authentication with facial recognition, introducing fraud detection algorithm, Predictive analytics for credit card fraud detection, Evaluating the quality of predictions	10	25
4.	Unit 4: Evaluating and Testing AI Arsenal Best practising for featuring engineering, evaluating a detector's performance with ROC, using cross-validation for algorithms, Evading ML detectors, Challenging ML anomaly detection, Testing for data and model quality, Ensuring securing and reliability	10	25

Reference Books:

1. Hands-On Artificial Intelligence for Cybersecurity by Alessandro Parisi Packt Publishing
2. AI in Cybersecurity by Leslie F. Sikos Springer International Publishing

Course Outcome:

Sr. no.	Course Outcomes
1.	Understand the core concepts and practical aspects of artificial intelligence in the context of cyber security.
2.	Apply the artificial intelligence-based methods for detecting cyber security threats.
3.	Apply the artificial intelligence-based methods for providing secure authentication mechanisms.
4.	Analyse the artificial intelligence-based detection and prevention methods for cyber security.
5.	Analyse the artificial intelligence-based detection and prevention methods for cyber security.

PG Diploma in Cyber Security

Course Structure, Teaching Scheme

w.e.f. 2022-23

SEMESTER-II

Course Name: Cloud Computing and Security
Subject Code:

Teaching and Examination Scheme:

Teaching Scheme			Credits	Examination Marks				Total Marks
L	T	P	C	Theory Marks		Practical Marks		
				ESE(E)	PA (M)	PA (V)	PA (I)	
3	0	0	3	70	30	30	20	150

Content:

Sr. No.	Content	Teaching Hours	Module Weightage (%)
1.	**Introduction to Cloud Computing:** The Evolution of Cloud Computing, What is Cloud computing? , SPI framework of Cloud Computing, Traditional Software Model, Cloud Service Delivery model, Cloud Deployment Models, Key Drivers to Adopting the Cloud, The Impact of Cloud Computing on Users, Governance in the Cloud, Barriers to Cloud Computing Adoption in the Enterprise.	5	15%
2.	**Security Fundamentals and Risk Issues in the Cloud:** Cloud Information Security Objectives, Cloud Security Services, Cloud Security Design Principles, Secure Cloud Software Requirements, Security Policy Implementation and decomposition, Cloud Computing and Business Continuity/Disaster Recovery, CIA triad,Privacy and compliance risk.	5	15%
3.	**Infrastructure Security:** Infrastructure Security: The Network Level, Infrastructure Security: The Host Level, Infrastructure Security: The Application Level	6	15%
4.	**Data Security and Storage:** Aspects of Data Security, Data Security Mitigation, Provider Data and Its Security	4	10%
5.	**Identity and Access Management:** Trust Boundaries and IAM, Why IAM? , IAM Challenges, IAM Definitions, IAM Architecture and Practice, Getting Ready for the Cloud, Relevant IAM Standards and Protocols for Cloud Services, IAM Practices in the Cloud. Cloud Authorization Management, Cloud	10	25%

	Service Provider IAM Practice		
6	**Security Management in the Cloud:** Security Management Standards, Security Management in the Cloud, Availability Management, SaaS Availability Management, PaaS Availability Management, IaaS Availability Management, Access Control, Security Vulnerability, Patch, and Configuration Management	7	20%

Reference Books:

1. Tim Mather, Subra Kumaraswamy, and Shahed Latif, Cloud Security and Privacy, O'Reilly.

2. Raghu Yeluri and Enrique Castro-Leon, Building the Infrastructure for Cloud Security A Solutions view, Apress open.

3. Ronald L. Krutz and Russell Dean Vines, Cloud Security A Comprehensive Guide to Secure Cloud Computing, Wiley

Course Outcome:

After successful completion of the course, student will be able to

1. Evaluate the various layers of cloud infrastructure
2. Integrate encryption and identity management services in a cloud environment
3. Perform vulnerability assessments in a cloud environment
4. Develop a cloud disaster recovery and business continuity plan

PG Diploma in Cyber Security

Course Structure, Teaching Scheme

w.e.f. 2022-23

SEMESTER-II

Course Name: Advanced Cryptography
Subject Code:

Teaching and Examination Scheme:

Teaching Scheme			Credits	Examination Marks				Total Marks
				Theory Marks		Practical Marks		
L	T	P	C	ESE(E)	PA (M)	PA (V)	PA (I)	
3	0	2	4	70	30	20	30	150

Content:

Sr. No.	Content	Teaching Hours	Module Weightage (%)
1.	UNIT-I: Introduction to Key Management and Distribution Symmetric Key Distribution Using Symmetric Encryption, Symmetric Key Distribution Using Asymmetric Encryption, Distribution of Public Keys.	08	20
2.	UNIT-II: User Authentication Remote User-Authentication Principles , Remote User-Authentication Using Symmetric Encryption, Kerberos, Remote User Authentication Using Asymmetric Encryption, Federated Identity Management, Personal Identity Verification.	08	20
3.	UNIT-III: Cryptanalysis Classic techniques of cryptanalysis, Modern methods, Rainbow tables, The birthday paradox, Other methods for breaching cryptography.	06	15
4.	UNIT-IV: Cryptographic Backdoors General concepts of cryptographic backdoors, Specific examples of cryptographic backdoors, Prevalence of cryptographic backdoors, Countermeasures.	06	15
5.	UNIT-V: Steganography Steganography basics, The history of steganography, Modern methods and algorithms, Tools for steganography, Steganalysis, Distributed steganography.	06	15
6	UNIT-VI: The Future of Cryptography Cryptography and the cloud, Homomorphic cryptography, The anatomy of ransomeware attack, Modern Hardware Design Practices, Quantum cryptography.	06	15

Reference Books:

1. Cryptography and Network Security, Principles and Practice Sixth Edition, William Stallings, Pearson
2. Modern Cryptography: Applied Mathematics for Encryption and Information Security, Chuck Easttom, McGraw-Hill Education
3. Cryptography & Network Security, Forouzan, Mukhopadhyay, McGraw-Hill
4. Cryptography and Network Security Atul Kahate, TMH
5. Cryptography and Security, C K Shyamala, N Harini, T R Padmanabhan, Wiley-India

Course Outcome:

After completion of the Course, Students will be able to:

No	Course Outcomes
01	Understand the basic Key Management and distribution concepts with their various types.
02	Differentiate between authentication using symmetric encryption and authentication using asymmetric encryption.
03	Apply classic and modern techniques for cryptanalysis.
04	Analyze various cryptographic backdoors for their merits and demerits.
05	Evaluate various algorithms and tools for steganography with their applications.

PG Diploma in Cyber Security

Course Structure, Teaching Scheme

w.e.f. 2022-23

SEMESTER-II

Course Name: Ethical Hacking Practices
Subject Code:

Teaching and Examination Scheme:

Teaching Scheme			Credits	Examination Marks				Total Marks
L	T	P	C	Theory Marks		Practical Marks		
				ESE(E)	PA (M)	PA (V)	PA (I)	
2	0	2	3	70	30	20	30	150

Content:

Sr. No.	Content	Teaching Hours	Module Weightage (%)
1.	Unit-I: An Introduction to Ethical Hacking: Security Fundamental, Security testing, Hacker and Cracker, Descriptions, Test Plans-keeping It legal, MITRE ATT&CK framework.	02	8
2.	Unit-II: The Technical Foundations of Hacking: The Attacker's Process, The Ethical Hacker's Process, Security and the Stack	04	12
3.	Unit-III: Footprinting and scanning: Information Gathering, Determining the Network Range, Identifying Active Machines, Finding Open Ports and Access Points, OS Fingerprinting Services, Mapping the Network Attack Surface	05	15
4.	Unit-IV: Enumeration, System Hacking and Malware Threats: Enumeration, System Hacking, Viruses and Worms, Trojans, Covert Communication, Keystroke Logging and Spyware, Malware Countermeasures	05	15
5.	Unit-V: Web Server attacks and its Security Sniffers, Session Hijacking, Denial of Service, Distributed Denial of Service, Web Server Hacking, Web Application Hacking, Database Hacking, Web Server Countermeasures	06	20
6	Unit-IV: Network Security, Wireless Technologies, Mobile Security and Attacks Intrusion Detection Systems, Firewalls, Honeypots, Wireless Technologies, Mobile Device Operation and Security, Wireless LANs, Physical Security, Social Engineering	06	20
7	Unit-VII: Current Trends The latest technology attacks with AI and its countermeasures.	03	10

Reference Books:

1. Certified Ethical Hacker, Version 9, Second Edition, Michael Gregg, Pearson IT Certification
2. Hacking the Hacker, Roger Grimes, Wiley
3. The Unofficial Guide to Ethical Hacking, Ankit Fadia, Premier Press

Course Outcome:

After completion of the Course, Students will be able to:

No	Course Outcomes
01	To outline the Indicator of Compromise for the system.
02	To develop the attack plan which covers planning, organize and performing penetration testing on a simple network.
03	Analyze different models & techniques for securing the systems.
04	Differentiate the tools to conduct ethical hacking as per the CEH modules.
05	Critiquing how the red team and blue team process in terms to compromise the system and defending the system as per IOC

PG Diploma in Cyber Security

Course Structure, Teaching Scheme

w.e.f. 2022-23

SEMESTER-II

Course Name: Defensive Programming (Elective-I)
Subject Code:

Teaching and Examination Scheme:

Teaching Scheme			Credits	Examination Marks				Total Marks
L	T	P	C	Theory Marks		Practical Marks		
				ESE(E)	PA (M)	PA (V)	PA (I)	
3	0	2	4	70	30	30	20	150

Content:

Sr. No.	Content	Teaching Hours	Module Weightage (%)
1.	UNIT 1: Introduction: A Penetration Test with Python, Setting Up Development Environment, Python language basics	07	19
2.	UNIT 2: Secure Coding: Secure Code Review, Methodology, Secure Code Review Technical Reference, Code Review Checklist, Threat Modeling Examples, HTML5	07	19
3.	UNIT 3: Network Programming Basics: Networking: Basics of Networking, Networking and Multithreading Programming – sockets, Threads and processes, Chat Application	03	07
4.	UNIT 4: Penetration Testing: Build port scanner, Build SSH botnet, FTP Scanner, Regular Expression	05	12
5.	UNIT 5: Forensic Investigation with Python: Analysis of wireless access point in the Registry, Recover deleted items in recycle bin, Parse PDF metadata, Investigating application artifacts with python	06	16
6	UNIT 6: Network Traffic Analysis with Python: Introduction of PyGeoIP, Analyse LOIC traffic, Pentagon's Dilemma, Intrusion Detection System using Scapy	04	10
7	UNIT 7: Wireless mayhem with python: Introduction of Wireless Security, Setting of Wireless attack environment, Listen wireless secret, Firesheep Detection	05	12

8	UNIT 8: Web recon with python: Introduction of Social Engineering, Mass Social Engineering	02	05

Reference Books:

Reference Book:

1. David Beazley and Brian K. Jones, Recipes for Mastering Python3 Cookbook, 3rd Edition, O'Reilly, 2013.
2. Mark Summerfield, Programming in Python 3, 2nd Edition, Pearson Education, 2010.
3. Violent Python – A Cookbook for Hackers, Forensic Analysts, Penetration Testers and Security Engineer by TJ O'Connor
4. Penetration Testing: A Hands-On Introduction to Hacking 1st Edition by Georgia Weidman
5. Larry Conklin and Gary Robinson, OWASP Code Review Guide 2.0 by OWASP Foundation, 2017.

Course Outcome:

1. Understand the fundamentals of python programming and fundamentals of penetration testing methodology for web applications.
2. Execute the secure code review practice for defensive programming.
3. Implement web applications and web services using python programming.
4. Analyze the digital investigation process through hands-on exercises.
5. Detect the network intrusions through network traffic analysis and web recon with python

PG Diploma in Cyber Security

Course Structure, Teaching Scheme

w.e.f. 2022-23

SEMESTER-II

Course Name: Operating System and Host Security (Elective-I)
Subject Code:

Teaching and Examination Scheme:

Teaching Scheme			Credits	Examination Marks				Total Marks
L	T	P	C	Theory Marks		Practical Marks		
				ESE(E)	PA (M)	PA (V)	PA (I)	
3	0	2	4	70	30	20	30	150

Content:

Sr. No.	Content	Teaching Hours	Module Weightage (%)
Part-I Operating System			
1.	OS Processes, Synchronization, Memory Management, File Systems	2	5
2.	Trusted Operating Systems, Assurance in Trusted Operating Systems, Virtualization Techniques.	3	6
3.	Secure operating systems, Security goals, Trust model, Threat model	4	9
4.	Access Control Fundamentals – Protection system – Lampson's Access Matrix, Mandatory protection systems, Reference monitor.	4	9
5.	Multics – Multics system, Multics security, Multics vulnerability analysis	3	6
6.	Security in Ordinary OS – Unix, Windows	3	6
7.	Verifiable security goals – Information flow, Denning's Lattice model, Bell-Lapadula model, Biba integrity model, Covert channels.	4	9
8.	Security Kernels – Secure Communications processor, Securing Commercial OS	3	6
9.	Secure Capability Systems – Fundamentals, Security, Challenges Secure Virtual Machine Systems	3	6
10.	Case study – Windows, Linux kernel, Android, DVL, Solaris Trusted Extensions	4	8
Part-I I Host Security			
1.	Introduction of BIOS and identification of trusted platform	1	2
2.	Techniques for Recording Platform State	1	2

3.	Can We Use Platform Information Locally?	2	4
4.	Can We Use Platform Information Remotely?	2	4
5.	How Do We Make Sense of Platform State?	2	4
6.	Roots of Trust	2	4
7.	Challenges in Bootstrapping Trust in Secure Hardware.	2	4
8.	Validating the Process, Implementing Trust Bootstrapping: Open Source Tools	2	4
9.	Human Factors & Usability	1	2

Reference Books:

1. Trent Jaeger, Operating System Security, Morgan & Claypool Publishers, 2008.
2. Bryan Parno, Jonathan M. McCune, Adrian Perrig, Bootstrapping Trust in Modern Computers, Springer Science & Business Media, 2011.
3. BRAGG, Network Security: The Complete Reference, McGraw Hill Professional, 2012.

Course Outcome:

1. Understand the concept of secure operating system
2. Learn to design a secure operating systems
3. Understand introductory concepts of BIOS UEFI/EFI boot process.
4. Understand the System Management Mode (SMM), chip-set architecture
5. Understand how the BIOS interacts with the Trusted Platform Module (TPM) and the measured boot process

SEMESTER-II

Course Name: Mini Project
Subject Code:

Teaching and Examination Scheme:

Teaching Scheme			Credits	Examination Marks				Total Marks
L	T	P	C	Theory Marks		Practical Marks		
				ESE(E)	PA (M)	PA (V)	PA (I)	
0	0	4	2	-	-	70	30	100

OBJECTIVES:

- To develop their own innovative prototype of ideas and design a project.
- To train the students in preparing mini project reports and examination.

The students in a group of 3 to 4 work on a topic approved by the faculty members of the department and prepares a comprehensive mini project report after completing the work to their satisfaction. The progress of the project is evaluated based on a minimum of two reviews. The review committee may be constituted by the Head of the Department. A mini project report is required at the end of the semester. The mini-project work is evaluated based on oral presentation and the mini-project report jointly by internal examiners constituted by the Head of the Department and an external examiner appointed by GTU.