Dr. B. C. Roy Engineering College, Durgapur

Department of CSE(CS)

Field	Details
Course Name	Quantum Cryptography
Course Code	CY-601
Semester	6
Course Category	Open Elective Courses
Credits	3
Hours per Week	3L:0T:0P

1. Prerequisites

- Fundamental programming skills (e.g., Python or Java) and basic data structures

- Discrete mathematics including modular arithmetic, probability, and basic graph theory

- Introductory computer security/cryptography concepts (confidentiality, integrity, symmetric encryption basics)

2. Course Learning Objectives

- This course introduces students to fundamental concepts and applications of the subject

- Students will learn theoretical foundations and practical skills relevant to the field

3. Teaching Methodology

- Lectures and Presentations

- Interactive Discussions and Case Studies

- Lab Sessions

• Guest Lectures

4. Evaluation System

Activities	**Class Test Full marks**	**Assignment Full marks**	**Attendance Full marks**	**Total Marks**
CIA-1	25	10	5	40
CIA-2	25	10	5	40
End Semester Examination (ESE)	_	_	_	60
Total				100

5. Course Modules

Module	**Topics**	**Hours**
1	**Fundamentals of Classical Cryptography & Security** - Security goals (confidentiality, integrity, authenticity, non-repudiation) - Threat model: active, passive and brute-force attacks - Symmetric cipher basics - substitution & transposition techniques - One-Time Pad (Vernam cipher) and perfect secrecy - Secret-key distribution problem & basic key-exchange ideas - Principles of cryptographic design (Kerckhoffs's principle, defence-in-depth) - Overview of modern block ciphers (DES -> AES) - conceptual view - Introduction to hash functions and Message Authentication Codes (MACs) - Brief overview of public-key cryptography (RSA concept) - Steganography - hiding information in non-	6

	cryptographic media	
2	**Symmetric & Asymmetric Key Cryptography** - Feistel network structure and its role in block ciphers - Simplified DES -> DES -> AES - key schedule and round function ideas - Symmetric encryption modes (ECB, CBC, CTR) and their security properties - Public-key cryptography principles (key pairs, hardness assumptions) - RSA algorithm - key generation, encryption, decryption (high-level math only) - Diffie-Hellman key exchange - basic protocol and security intuition - ElGamal encryption - concept and relation to DH - Discrete Logarithm Problem - intuitive difficulty - Random Oracle Model - purpose in security proofs (conceptual) - Classical bits vs. quantum bits - why quantum topics follow	7
3	**Fundamental Quantum Mechanics & Quantum Computing** - Qubit representation & Bloch-sphere visualization - Superposition and measurement - the two golden rules - No-cloning theorem and its security implications - Quantum uncertainty principle - intuitive view - Compatible vs. incompatible measurement bases - Quantum entanglement (Bell states) and basic teleportation idea - Tensor product notion - building multi-qubit states (qualitative) - Quantum gates (X, H, CNOT, Pauli) and circuit model - Simple quantum error-detection (parity check) concepts - Quantum parallelism & Deutsch-Jozsa algorithm (high-level) - Grover's search - quadratic speed-up intuition - Overview of quantum algorithms - Shor's algorithm (conceptual impact only)	8
4	**Quantum Cryptography & Quantum Key Distribution (QKD)** - Why quantum cryptography is needed (future-proof security) - Quantum communication basics - single-photon encoding, polarization - BB84 protocol - detailed steps, basis choice,	8

	sifting - Other prepare-and-measure protocols (B92, six-state) - key differences - Entanglement-based QKD (Ekert91) - basic idea and security test - Classical post-processing: basis reconciliation, error estimation, privacy amplification - Security analysis: intercept-resend, photon-number-splitting attacks, error-rate thresholds - Practical implementation: photon sources (weak laser, quantum dots), detectors (SNSPD, APD), transmission media (fiber, free-space) - Alternative encoding schemes (time-bin, phase encoding) - Error-correction overview - Cascade and modern LDPC approaches - Authentication of the classical channel - unconditional methods	
5	**Post-Quantum Cryptography & Quantum-Resistant Primitives** - Effect of quantum algorithms (Shor) on RSA, ECC and DH - NIST PQC landscape - families and representative candidates * Lattice-based (Kyber, Dilithium) - intuitive LWE/SIS ideas * Code-based (Classic McEliece) - basic coding-theory view * Hash-based signatures (SPHINCS+, XMSS) - Merkle-tree construction * Multivariate schemes (Rainbow) - high-level concept - Security considerations for PQC - parameter selection, side-channel resistance - Post-quantum key-exchange and digital-signature protocols - Migration pathways - integrating PQC into existing PKI and TLS stacks - Quantum-resistant fully homomorphic encryption - conceptual overview - Use-case scenarios (cloud security, IoT, critical infrastructure)	7
6	**Quantum Cryptographic Systems, Networks & Trust Models** - Architecture of a QKD system - hardware (sources, detectors, modulators) and software stack - QKD network topologies: point-to-point, trusted-node, and emerging quantum-repeater designs - QKD network protocols - Q3P framework,	6

	SECOQC architecture, routing basics - Trust models - Ring of Trust, Point-of-Trust, and real-world case study (medical data exchange) - Implementation attacks on QKD - side-channel, detector blinding, Trojan-horse - Standardization & certification - ETSI, ISO/IEC 23889, and emerging compliance frameworks - Future directions - satellite QKD, integration with classical networks, quantum-safe authentication - Ethical, legal and regulatory aspects of deploying quantum-secure infrastructure	

6. References

Textbooks:

1. Kollmitzer C., Pivk M. (Eds.), Applied Quantum Cryptography, Lect. Notes Phys. 797 (Springer, Berlin Heidelberg 2010

2. P. Kaye, R. Laflamme, and M. Mosca: An Introduction to Quantum Computing, Oxford University Press, New York

3. William Stallings, Cryptography and Network Security Principles and Practice Fourth Edition, Pearson Education, 2019.

Reference Books:

1. Thomas Vidick and Stephanie Wehner, "Introduction to Quantum Cryptography", Cambridge University Press, 2023.

2. Bellare, Mihir, and Shafi Goldwasser. "Lecture notes on cryptography." (2008).

3. Quantum Cryptography by Donald J. Barrett.

7. Course Outcomes

ID	Statement	Action Verb	Knowledge Level
CY-601.1	Recall and list the four fundamental security goals (confidentiality, integrity, authenticity, non-repudiation) and identify at least three classical cryptographic techniques	Recall	Remember

	(substitution cipher, one-time pad, DES) covered in the course.		
CY-601.2	Explain the operating principles of symmetric block ciphers (Feistel networks, key schedule) and asymmetric schemes (RSA, Diffie-Hellman), and illustrate how each achieves confidentiality or secure key exchange.	Explain	Understand
CY-601.3	Apply quantum-mechanical concepts such as superposition, measurement, and entanglement to construct simple quantum circuits (e.g., Hadamard and CNOT) and predict their output states for given inputs.	Apply	Apply
CY-601.4	Analyze the BB84 quantum key distribution protocol by simulating basis selection, sifting, and error estimation, and identify at least two potential attacks (intercept-resend, photon-number-splitting) with their effect on security thresholds.	Analyze	Analyze
CY-601.5	Evaluate three NIST post-quantum cryptography candidates (Kyber, Dilithium, SPHINCS+) against criteria of security level, performance, and implementation considerations, and recommend a migration pathway for integrating them into an existing TLS infrastructure.	Evaluate	Evaluate
CY-601.6	Design a comprehensive quantum-resistant communication architecture that combines QKD (including trusted-node topology) with post-quantum cryptographic primitives, addresses authentication of the classical channel, and complies with relevant standards (ETSI, ISO/IEC 23889).	Design	Create

8. CO-PO Mapping

CO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
CO1	3	2	1	1	-	1	-	1	-	1	-	2

CO2	3	2	2	2	2	1	-	1	-	2	-	2
CO3	3	2	2	2	3	1	-	1	2	2	-	3
CO4	3	3	2	3	2	2	1	2	2	2	2	3
CO5	3	2	3	2	3	2	1	2	2	3	3	3
CO6	3	3	3	3	3	3	2	3	3	3	3	3

9. CO-PSO Mapping

CO	PSO1	PSO2	PSO3
CO1	3	2	1
CO2	3	2	1
CO3	2	1	1
CO4	3	2	1
CO5	3	3	2
CO6	3	3	2

Dr. B. C. Roy Engineering College, Durgapur

Department of CSE(CS)

Field	Details
Course Name	Internet of Things
Course Code	CY-602
Semester	6
Course Category	Open Elective Courses
Credits	3
Hours per Week	3L:0T:0P

1. Prerequisites

- Fundamental programming skills (Python and/or C) with basic control structures and data handling

- Introductory computer networking concepts (IP addressing, subnetting, OSI/TCP-IP model)

- Basic electronics and microcontroller fundamentals (digital I/O, sensors/actuators, Arduino/Raspberry Pi basics)

2. Course Learning Objectives

- This course introduces students to fundamental concepts and applications of the subject

- Students will learn theoretical foundations and practical skills relevant to the field

3. Teaching Methodology

- Lectures and Presentations

- Interactive Discussions and Case Studies

• Lab Sessions

• Guest Lectures

4. Evaluation System

Activities	Class Test Full marks	Assignment Full marks	Attendance Full marks	Total Marks
CIA-1	25	10	5	40
CIA-2	25	10	5	40
End Semester Examination (ESE)	–	–	–	60
Total				100

5. Course Modules

Module	Topics	Hours
1	**Foundations of the Internet of Things** - Introduction to IoT: definitions, key characteristics and recent adoption trends - Historical evolution of IoT and emerging market drivers - IoT functional stack & core functional blocks (sensing, actuation, connectivity, data, services) - Physical and logical design of IoT systems (device, gateway, cloud layers) - Reference architectures (IoT-WF, simplified 3-tier model) and standardization bodies - Enabling technologies overview: cloud, fog, edge, AI/ML basics (conceptual only) - Identifier schemes for "things": UID, URI, IPv6 addressing, EUI-64 - IoT vs. Machine-to-Machine (M2M): concepts, differences and convergence - Introductory security concepts for IoT: threat landscape, confidentiality, integrity, availability	5

	- Overview of regulatory and standards landscape (ISO/IEC 27001, NIST 800-53, GDPR, IEC 62443)	
2	**Sensors, Actuators & Embedded Hardware Platforms** - Sensor fundamentals: types, working principles, key performance metrics and classification - Actuator fundamentals: types, operating principles and selection criteria - Role of sensing & actuation in end-to-end IoT solutions - Development board families: Arduino UNO, Raspberry Pi, ESP32/NodeMCU and brief comparison - Arduino ecosystem: IDE, board architecture, GPIO, PWM, serial/UART - Raspberry Pi basics: Linux OS, GPIO, I^{2}C, SPI, UART interfaces - Introductory C programming for embedded systems (structures, pointers, arrays) - lab focus - Introductory Python for IoT (data types, control flow, functions, modules, file I/O, OOP) - lab focus - Interfacing common peripherals (LEDs, relays, DC motor, ultrasonic sensor, DHT22, LDR, keypad, gas sensor) to Arduino/Raspberry Pi - Firmware lifecycle basics and OTA update concepts (security-aware)	6
3	**IoT Networking, Protocols & Security Foundations** - Fundamentals of networking: IP vs. MAC addressing, subnetting basics - IEEE 802 family overview (802.3 Ethernet, 802.11 Wi-Fi, 802.15.4, 802.11ah) and their IoT use-cases - WPAN technologies: ZigBee, BLE, NFC, Z-Wave, HART, BACnet, Modbus - LPWAN technologies: LoRaWAN, Sigfox - characteristics and deployment scenarios - IP-based IoT protocols: IPv6, 6LoWPAN, RPL, CoAP, MQTT, AMQP, REST/HTTP, HTTPS - Application-layer protocols (optional overview): SCADA, XMPP - Network management protocols: SNMP, NETCONF/YANG - practical relevance - Secure communication mechanisms: TLS/DTLS, PSK, certificate-based authentication - Network segmentation, firewall basics and IoT-specific DMZ design - Security considerations for IEEE 802.15.4, 802.11ah and LPWAN (encryption, key	7

	management)	
4	**IoT Software Development, Platforms & Cloud Integration** - IoT system development lifecycle and design methodology (requirements -> deployment) - Logical design using Python - case study: weather-monitoring system - Core Python packages for IoT (paho-mqtt, requests, pandas, gpiozero, json, datetime) - Device integration patterns, data acquisition, preprocessing and local storage - Open-source IoT platforms: Node-RED, ThingsBoard, Eclipse Kura - hands-on overview - Commercial cloud services snapshot: AWS IoT Core, Azure IoT Hub, Google Cloud IoT Core - Cloud dashboards & visualization tools: Blynk, ThingSpeak, Grafana - Identity & access management for devices (OAuth 2.0, JWT, X.509 certificates, device provisioning) - Secure OTA firmware update workflow and version control - Intro to containerised edge runtimes (Docker) and CI/CD pipelines for IoT	8
5	**Data Analytics, Big Data & Edge/Fog Computing for IoT** - Big-data characteristics for IoT (volume, velocity, variety, veracity) - End-to-end data pipeline: acquisition -> storage -> processing -> analytics - Fundamentals of distributed storage (HDFS overview) and batch processing (MapReduce concept only) - Real-time processing frameworks: Apache Spark Structured Streaming, Apache Storm - conceptual view - Stream processing of MQTT/CoAP data streams (windowing, aggregation) - Time-series databases for IoT (InfluxDB, TimescaleDB) and query basics - Fog and edge computing concepts: placement of analytics, latency trade-offs - Lightweight ML/AI techniques for IoT (rule-based anomaly detection, simple predictive models) - no heavy mathematics - Service models (IaaS, PaaS, SaaS, DaaS) and selecting appropriate cloud/edge services for IoT workloads - Security-aware analytics: data integrity verification	8

	and privacy-preserving aggregation	
6	**IoT Applications, Case Studies & Laboratory Projects** - Domain-specific case studies: Smart Home, Smart Cities, Precision Agriculture, Healthcare, Industrial Automation, Smart Grid, Supply-Chain & Logistics - Legal, ethical, privacy and environmental considerations in IoT deployments - Security-by-design checklist for each domain (threat modeling, data protection, secure onboarding) - Comprehensive lab suite (selected experiments): * LED & relay control, PWM dimming * Traffic-light simulation with state machine logic * Ultrasonic-based intrusion detection & water-level monitoring * Smart street-light with LDR and ambient-light adaptation * DC-motor speed control via PWM * Moisture-sensor driven waste-classification prototype (DHT22) * pH sensing, gas-leak detection, weather-station data collection * UART communication, keypad logging, secure data transmission - Capstone project: design-implement-evaluate an end-to-end IoT solution that integrates sensors, edge processing, cloud analytics, a visual dashboard and incorporates security best practices (authentication, encryption, OTA updates)	8

6. References

Textbooks:

1. IoT Fundamentals: Networking Technologies, Protocols and Use Cases for Internet of Things, David Hanes, Gonzalo Salgueiro, Patrick Grossetete, Rob Barton and Jerome Henry, Cisco Press, 2017

2. Arshdeep Bahga, Vijay Madisetti, " Internet of Things- A Hands On Approach", Universities press, 2014.

3. Adrian Mcewen, Hakin Cassimally, "Designing The Internet of Things", First Edition, Wiley, 2014.

4. Hakima Chaouchi, ― "The Internet of Things Connecting Objects to the Web" ISBN : 978-1-84821-140-7, Wiley Publications

Reference Books:

1. Daniel Minoli, **—** "Building the Internet of Things with IPv6 and MIPv6: The Evolving World of M2M Communications", ISBN: 978-1-118-47347-4, Willy Publications

2. Raj Kamal , " Internet of Things: Architecture and Design", McGraw Hill.2nd edition June 2022

3. David Hanes, Gonzalo Salgueiro, Patrick Grossetete, Robert Barton, Jerome Henry,"IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Things", 1 stEdition, Pearson Education (Cisco Press Indian Reprint). (ISBN: 978-9386873743)

4. The Internet of Things - Key applications and Protocols, Olivier Hersent, David Boswarthick, Omar Elloumi and Wiley, 2012 (for Unit2).

7. Course Outcomes

ID	Statement	Action Verb	Knowledge Level
CY-601.1	Course Outcome 1	Understand	Understand
CY-601.2	Course Outcome 2	Understand	Understand
CY-601.3	Course Outcome 3	Understand	Understand
CY-601.4	Course Outcome 4	Understand	Understand
CY-601.5	Course Outcome 5	Understand	Understand
CY-601.6	Course Outcome 6	Understand	Understand

8. CO-PO Mapping

CO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
CO1	3	2	1	1	1	1	1	-	1	1	1	2
CO2	3	2	1	1	1	1	1	-	1	1	1	2
CO3	2	3	1	2	1	1	1	-	1	1	1	2
CO4	2	1	3	1	2	2	1	-	1	1	1	2
CO5	2	1	2	2	3	1	1	-	1	1	1	2
CO6	1	1	1	1	1	1	1	-	2	2	2	3

9. CO-PSO Mapping

CO	PSO1	PSO2	PSO3
CO1	3	2	1
CO2	3	2	1
CO3	3	2	1
CO4	2	3	1

CO5	2	3	1
CO6	1	2	3

DR. B.C. ROY SOCIETY
ENGINEERING
AN AUTONOMOUS INSTITUTE

Dr. B. C. Roy Engineering College, Durgapur

Department of CSE(CS)

Field	Details
Course Name	Cyber Threat Intelligence and Incident Response
Course Code	CY-603
Semester	6
Course Category	Professional Elective Courses
Credits	3
Hours per Week	3L:0T:0P

1. Prerequisites

• Fundamental understanding of computer networks and protocols (e.g., TCP/IP, OSI model)

• Basic knowledge of operating systems and command-line usage (Windows and Linux)

• Introductory cybersecurity concepts, including the CIA triad, common threat types, and basic risk assessment

2. Course Learning Objectives

• This course introduces students to fundamental concepts and applications of the subject

• Students will learn theoretical foundations and practical skills relevant to the field

3. Teaching Methodology

• Lectures and Presentations

• Interactive Discussions and Case Studies

• Lab Sessions

- Guest Lectures

4. Evaluation System

Activities	**Class Test Full marks**	**Assignment Full marks**	**Attendance Full marks**	**Total Marks**
CIA-1	25	10	5	40
CIA-2	25	10	5	40
End Semester Examination (ESE)	_	_	_	60
Total				100

5. Course Modules

Module	Topics	Hours
1	**Fundamentals of Cyber Incidents & Threat Intelligence** - Cyber-incident fundamentals and recent statistics - Information as a business asset & data-classification basics - Core CIA triad and basic risk concepts (confidentiality, integrity, availability) - Vulnerability, threat, and attack taxonomy - Common types and examples of security incidents - Incident categorisation (low, medium, high) and impact basics - Introduction to Cyber Threat Intelligence (CTI): purpose, consumers and key characteristics - CTI lifecycle overview (collection -> processing -> analysis -> dissemination -> feedback) - Basic threat-modeling concepts (ATT&CK, STRIDE) and their relevance to CTI - Overview of industry frameworks (NIST CSF, ISO/IEC 27001) and legal context (GDPR, HIPAA) for incident handling	8
2	**Incident Prioritization, Planning & Preparation**	7

	- Risk-scoring and prioritisation methods (CVSS, DREAD) - Goals, objectives and measurable KPIs for incident response - Incident-response policy, plan and procedure components * Policy elements * Plan elements * Procedure elements - Incident-response team structure, roles (IR lead, analyst, forensics, communications) and SOC integration - Selecting a response model (centralised, distributed, hybrid) - Preparation check-lists, asset inventory and baseline security controls - Detection fundamentals: attack vectors, indicators, precursors - Reporting obligations and coordination with national CERTs / ISACs - Cost estimation techniques and basic impact assessment	
3	**Incident Handling Lifecycle & Forensic Operations** - End-to-end incident handling process (Identification -> Containment -> Eradication -> Recovery -> Lessons-learned) - Incident recording, classification, communication and status reporting - Containment strategies (network, host, logical isolation) - Evidence collection, preservation and chain-of-custody procedures * Windows, Linux, mobile, network devices, cloud services * Imaging tools, hash verification, write-blockers - Legal admissibility of digital evidence and courtroom preparation basics - Eradication techniques and secure system recovery - Post-incident activities: root-cause analysis, lessons learned, policy improvement - Forensic analysis methodologies and common toolsets (Volatility, Autopsy, FTK) - Use of honeypots and sandbox environments for evidence gathering	7
4	**Malware Analysis and Reverse Engineering** - Malware fundamentals: types, life-cycle and terminology (virus, worm, Trojan, ransomware,	6

	etc.) - Core malware components (replicator, concealer, payload) and trigger mechanisms - Static analysis techniques (file-header inspection, strings, hash comparison) - Dynamic analysis workflow * Baseline sandbox preparation * System & network monitoring, API/registry/file-system tracing * Capture of execution artefacts and post-run data analysis - Automated analysis frameworks and cloud-based sandboxes - Defeating obfuscation, packing and polymorphism - Malware taxonomy, phylogeny and digital virology concepts - Mapping malicious behaviour to ATT&CK techniques - Case studies (Conflicted C-Worm, Companion virus, logical bomb)	
5	**Cyber Threat Intelligence Processes, Models & Tools** - Detailed CTI lifecycle (collection -> processing -> analysis -> dissemination -> feedback) - Indicators of Compromise (IoCs) and threat-data feeds - Threat-intel models: Cyber Kill Chain, Diamond Model, Hunting Maturity Model - Structured exchange formats and protocols: STIX, TAXII, CybOX, OpenIOC, IODEF, VERIS, TLP - Open-source CTI platforms (OTX, CIF, MISP) and tooling basics - Threat-intel sharing frameworks, legal and privacy considerations - Proactive intelligence gathering: dark-web monitoring, underground forums, threat-actor profiling - Building CTI requirements: asset prioritisation, adversary profiling, consumer needs - Integration of CTI with ATT&CK and threat-hunting playbooks - Metrics for CTI effectiveness and reporting best practices	6
6	**Advanced Operational Topics: Threat Hunting, DevSecOps & Cloud Incident Response** - Threat-hunting readiness assessment and maturity model - Leveraging CTI for hypothesis-driven hunting (tactics, techniques, procedures)	8

	- DevSecOps principles and secure CI/CD pipeline design - Cloud-security fundamentals (CSA CCM, CIS Benchmarks) and incident response in virtualised environments - Use of virtualization and containerisation for containment and analysis - Advanced IR tools and platforms: SIEM, EDR, SOAR, XDR - Incident response in hybrid and multi-cloud architectures - Legal, regulatory and compliance implications (e.g., GDPR breach notification, industry-specific mandates) - Emerging trends: AI-assisted analysis, automated remediation, collaborative defence ecosystems	

6. References

Textbooks:

1. Luttgens Jason, Pepe Matthew, and Mandia Kevin, 2014, ―Incident Response & Computer Forensics‖, Third Edition, McGraw-Hill Education, ISBN: 978- 0071798686.

2. Friedman, J., & Bouchard, M. (2015). Definitive Guide to Cyber Threat Intelligence: Using Knowledge about Adversaries to Win the War against Targeted Attacks. CyberEdge Group.

3. Dalziel, H. (2014). How to define and build an effective cyber threat intelligence capability. Syngress.

Reference Books:

1. Robertson, J., Diab, A., Marin, E., Nunes, E., Paliath, V., Shakarian, J., & Shakarian, P. (2017). Darkweb cyber threat intelligence mining. Cambridge University Press.

2. Murdoch Don, 2016, ―Blue Team Handbook: Incident Response Edition: A condensed field guide for the Cyber Security Incident Responder‖, CreateSpace Independent Publishing Platform, 2.2 Edition , ISBN: 978-1500734756

3. Gourley Bob, 2014, ―The Cyber Threat‖, Create space Independent Pub.

7. Course Outcomes

ID	Statement	Action Verb	Knowledge Level
CY-603.1	Recall and list the fundamental concepts of cyber incidents, including the CIA triad, vulnerability-threat-attack taxonomy, common incident types, and the principal industry frameworks (NIST CSF, ISO/IEC 27001, GDPR, HIPAA).	Recall	Remember
CY-603.2	Explain the complete Cyber Threat Intelligence (CTI) lifecycle, the purpose of each phase, and how models such as ATT&CK, STRIDE, the Cyber Kill Chain and the Diamond Model support threat-intel production and sharing.	Explain	Understand
CY-603.3	Apply risk-scoring methods (e.g., CVSS, DREAD) to prioritize incidents, and develop a documented incident-response policy, plan and checklist that align with organisational KPIs and reporting obligations.	Apply	Apply
CY-603.4	Analyze a malware sample by performing static and dynamic analysis, identify its components, behaviours, and associated ATT&CK techniques, and produce a concise technical report of findings.	Analyze	Analyze
CY-603.5	Evaluate forensic evidence-collection procedures (imaging, hashing, chain-of-custody) across Windows, Linux, mobile, and cloud environments for legal admissibility, and critique the adequacy of incident-handling documentation and lessons-learned processes.	Evaluate	Evaluate
CY-603.6	Design and implement an automated threat-hunting or cloud-incident-response workflow that integrates CTI feeds (STIX/TAXII), DevSecOps controls, and orchestration tools (SIEM, EDR, SOAR), and justify its effectiveness using appropriate metrics.	Design	Create

8. CO-PO Mapping

CO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
CO1	2	2	1	1	1	2	-	2	-	-	1	2
CO2	3	3	2	2	2	2	-	2	2	2	2	3
CO3	3	3	3	3	2	3	-	2	2	3	3	2
CO4	3	3	1	3	3	2	-	2	2	3	1	3
CO5	3	3	2	3	3	3	-	3	2	3	2	3
CO6	3	3	3	3	3	2	-	2	3	2	3	3

9. CO-PSO Mapping

CO	PSO1	PSO2	PSO3
CO1	3	2	2
CO2	2	3	1
CO3	2	2	3
CO4	2	3	1
CO5	2	2	3
CO6	2	3	2

Dr. B. C. Roy Engineering College, Durgapur

Department of CSE(CS)

Field	Details
Course Name	Malware Analysis
Course Code	CY-604
Semester	6
Course Category	Professional Elective Courses
Credits	3
Hours per Week	3L:0T:0P

1. Prerequisites

• Fundamentals of operating systems and Windows internals (process isolation, memory management, system calls)

• Basic understanding of computer architecture and assembly language (x86/x86-64 instruction set, calling conventions, binary formats)

• Introductory networking concepts (TCP/IP, ports, protocols, packet capture)

2. Course Learning Objectives

• This course introduces students to fundamental concepts and applications of the subject

• Students will learn theoretical foundations and practical skills relevant to the field

3. Teaching Methodology

• Lectures and Presentations

• Interactive Discussions and Case Studies

- Lab Sessions
- Guest Lectures

4. Evaluation System

Activities	**Class Test Full marks**	**Assignment Full marks**	**Attendance Full marks**	**Total Marks**
CIA-1	25	10	5	40
CIA-2	25	10	5	40
End Semester Examination (ESE)	–	–	–	60
Total				100

5. Course Modules

Module	**Topics**	**Hours**
1	**Foundations of Malware & Threat Landscape** - Evolution of malware: historic milestones and modern trends - Malware taxonomy (virus, worm, trojan, rootkit, bot, spyware, ad-ware, ransomware, logic bomb) - Malware lifecycle & attack phases (recon, delivery, exploitation, installation, command-and-control, actions on objective) - Common vulnerability classes (buffer overflow, injection, privilege escalation, insecure deserialization) - Core OS security concepts (process isolation, memory protection, ASLR, DEP, sandboxing) - Rationale for malware analysis and overview of analysis types (static, dynamic, hybrid, reverse-engineering) - Basic threat-modeling and risk-assessment terminology relevant to malware - Legal, ethical, and compliance considerations for	5

	malware research	
2	**Secure Analysis Environment & Toolchain Setup** - Designing a forensically sound, isolated analysis lab (air-gap, network segmentation) - Virtualization fundamentals, VM hardening, snapshot strategy, anti-VM countermeasures - Installing and configuring core tooling: Sysinternals suite, Wireshark, Process Monitor, hash/YARA utilities, sandbox platforms - Evidence handling, chain-of-custody, and documentation best practices for analysis workflows - Safety procedures: safe handling of live samples, network traffic redirection, and containment - Automation basics: scripting common setup tasks and batch processing of samples	6
3	**Static Malware Analysis Techniques** - Portable Executable (PE) format deep-dive: headers, sections, import/export tables - File identification, fingerprinting, hash verification, and use of public hash databases - String extraction, resource analysis, and creation of YARA signatures - Detecting packing, obfuscation, metamorphism, and polymorphism (entropy analysis, packer identification) - x86/x86-64 architecture basics: instruction set, registers, calling conventions, stack layout, endianness - Hands-on with static tools: PEiD, Dependency Walker, Resource Hacker, BinText, FileAlyzer - Counter-measures used by malware to thwart static analysis and how to bypass them	8
4	**Dynamic Malware Analysis & Behavioral Monitoring** - Goals of dynamic analysis and when to apply it - Configuring VMs for dynamic work: network isolation, simulated services, and sandbox automation - System-level monitoring: process creation, file-system activity, registry changes, and Windows event logs - Network monitoring with Wireshark and PCAP analysis for C2 traffic - Debugging fundamentals: breakpoints, step execution, exception handling, kernel vs. user mode debugging	8

	- Dynamic analysis toolset: ProcMon, Process Explorer, x64dbg, IDA Pro (dynamic), VirusTotal, automated sandbox solutions - Extracting Indicators of Compromise (IOCs) and building behavioral profiles - Anti-dynamic analysis techniques (anti-VM, sleep/timeout evasion) and mitigation strategies	
5	**Reverse Engineering, Malware Functionality & Anti-Analysis** - Structured reverse-engineering workflow: from binary to high-level understanding - Disassembly and debugging with IDA Pro, x64dbg, and OllyDbg (source- vs. assembly-level view) - API call tracing, import reconstruction, and call-reference analysis - Core malware capabilities: downloader, dropper, loader, keylogger, backdoor, credential stealer, persistence mechanisms (registry, scheduled tasks, services, startup folder, IFEO, AppInit_DLLs, DLL hijacking) - Code-injection techniques: process injection, APC, detours, reflective DLL loading - Shellcode analysis and 64-bit malware considerations - Anti-reverse-engineering tactics: anti-disassembly, anti-debugging, anti-forensic tricks, packer/unpacker strategies - Practical unpacking and de-obfuscation methods	7
6	**Specialized Domains, Detection Strategies & Capstone** - Mobile malware analysis fundamentals for Android (APK structure, Dalvik bytecode) and iOS (IPA, sandbox bypass) - Malicious document analysis: PDF, Office (Word/Excel) and RTF file formats, macro-based exploits - Introductory machine-learning concepts for malware detection (feature extraction, model types: SVM, Random Forest, Decision Trees, Naïve Bayes) - focus on practical implementation, no heavy mathematics - Emerging trends: file-less attacks, supply-chain threats, ransomware evolution, AI-generated malware - Reporting standards and templates (STIX/TAXII, MITRE ATT&CK mapping), OSINT integration, and effective communication of findings - Capstone project: end-to-end malware analysis	8

	using an automated sandbox, generation of YARA rules, and delivery of a written report plus oral presentation	

6. References

Textbooks:

1. Abhijit Mohanta, Anoop Saldanha, Malware Analysis and Detection Engineering a Comprehensive Approach to Detect and Analyze Modern Malware, 2020, 1 edition, Apress (ISBN 978-1-4842-6192-7), United States.

2. M. Sikorski and A. Honig, Practical Malware Analysis: The Hands-on Guide to Dissecting Malicious Software. 2012, 1 edition, No Starch Press San Francisco, CA. (ISBN No.: 9781593272906), United States.

3. Practical malware analysis The Hands-On Guide to Dissecting Malicious Software by Michael Sikorski and Andrew Honig ISBN-10: 159327-290-1, ISBN-13: 978-1-59327-290-6, 2012 2

Reference Books:

1. Computer viruses: from theory to applications by Filiol, Eric Springer Science & Business Media, 2006

2. Monnappa K A, Learning Malware Analysis- Explore the concepts, tools, and techniques to analyze and investigate Windows malware, 2018, 1 edition, Packt Publishing, (ISBN 978-1-78839-250-1), United Kingdom.

3. Hacking exposed™ malware & rootkits: malware & rootkits security secrets & Solutions by Michael Davis, Sean Bodmer, Aaron Lemasters, McGraw-Hill, ISBN: 978-0-07-159119-5, 2010

7. Course Outcomes

ID	Statement	Action Verb	Knowledge Level
CY-602.1	Course Outcome 1	Understand	Understand
CY-602.2	Course Outcome 2	Understand	Understand
CY-602.3	Course Outcome 3	Understand	Understand
CY-602.4	Course Outcome 4	Understand	Understand
CY-602.5	Course Outcome 5	Understand	Understand
CY-602.6	Course Outcome 6	Understand	Understand

8. CO-PO Mapping

CO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
CO1	3	2	1	1	1	1	1	-	1	1	-	2
CO2	3	2	1	1	1	1	1	-	1	1	-	2
CO3	2	3	1	1	1	1	1	-	1	1	-	2
CO4	1	1	1	1	1	3	2	1	1	1	-	2
CO5	1	1	1	1	1	2	3	2	1	1	-	2
CO6	1	1	1	1	1	2	2	3	2	2	1	2

9. CO-PSO Mapping

CO	PSO1	PSO2	PSO3
CO1	3	2	1
CO2	2	3	1
CO3	1	1	3
CO4	2	2	2
CO5	1	2	3
CO6	3	2	2

Dr. B. C. Roy Engineering College, Durgapur

Department of CSE(CS)

Field	Details
Course Name	Principles of Cyber Law & Ethics
Course Code	CY-605
Semester	6
Course Category	Program Core Courses
Credits	3
Hours per Week	3L:0T:0P

1. Prerequisites

- Fundamental understanding of computer systems and basic networking concepts

- Introductory knowledge of legal principles, contracts, and basic Indian law

- Basic awareness of information security concepts and elementary cryptography (e.g., public-key and symmetric encryption)

2. Course Learning Objectives

- Guide students to develop a comprehensive understanding of the legal, regulatory, and ethical foundations that govern cyberspace, both within India and in the international context.

- Enable students to critically analyze and apply Indian cyber-law statutes (IT Act, PDPA draft, etc.) and relevant global frameworks to real-world scenarios involving e-commerce, data protection, and cyber-crimes.

- Equip students with the ability to evaluate cyber-security governance, risk-management, and compliance mechanisms, including standards, policies, and incident-response procedures, and to articulate their legal implications.

• Foster the capacity to assess emerging technologies (AI, blockchain, biometric systems, deep-fakes) through a multidisciplinary lens that integrates legal obligations, professional codes of conduct, and ethical considerations.

• Prepare students to communicate effectively about cyber-law and cyber-ethics issues to diverse stakeholders, and to formulate informed recommendations for policy, litigation, or organizational practice.

3. Teaching Methodology

• Lectures and Presentations

• Interactive Discussions and Case Studies

• Lab Sessions

• Guest Lectures

4. Evaluation System

Activities	**Class Test Full Marks**	**Assignment Full Marks**	**Attendance Full Marks**	**Total Marks**
CIA-1	25	10	05	40
CIA-2	25	10	05	40
End Semester Examination (ESE)	-	-	-	60
Total				100 Marks

5. Course Modules

Module	**Topics**	**Hours**
1	**Foundations of Cyberspace & Cyber Law** - Evolution of computer technology and emergence of cyberspace - Need for cyber law: societal and economic drivers - Foundations of cyber jurisprudence - Doctrinal, consensual and real approaches - Core cyber ethics and professional code of conduct - Cyber jurisdiction - Hierarchy of courts in India	7

	- Civil vs. criminal jurisdiction in cyberspace - International instruments shaping cyber sovereignty (Budapest Convention, Council of Europe recommendations) - Principles of state responsibility and territoriality in cyberspace	
2	**Legal Framework - Indian IT Act & International Perspectives** - Overview of the Indian Information Technology Act, 2000 - Key amendments (2008) and current limitations - Legal recognition of electronic records and e-signatures - Conceptual basics of public-key and symmetric cryptography (no deep mathematics) - Digital signatures: concepts, legal status and Certifying Authorities - Electronic Governance provisions and statutory duties of government agencies - Liability of Network Service Providers and Intermediaries - Role, powers and procedures of the Cyber Regulations Appellate Tribunal - Rights and remedies for users in the digital age (Section 43A, privacy provisions) - Comparative snapshot of IT/ cyber laws in the US, EU (GDPR) and other major jurisdictions - Emerging Indian legislation: Personal Data Protection Bill (draft) and its implications	8
3	**Cyber Crimes, Investigation & Forensics** - Definition and taxonomy of cybercrime (hacking, identity theft, cyber-stalking, etc.) - Cyber-terrorism and cyber-warfare basics - Cyber defamation, pornography and obscenity offences - Financial cyber-frauds and related offences - Fundamentals of cyber-crime investigation - Handling of digital/electronic evidence and chain-of-custody principles - Incident-response lifecycle and evidence preservation - Core forensic techniques and widely used tools (e.g., FTK, Autopsy, Wireshark) - Legislative framework: relevant IPC sections, Evidence Act provisions, banking and privacy statutes - admissibility standards for electronic evidence in Indian courts	7

4	**E-Commerce, Intellectual Property & Liability** - Overview of e-commerce models and the digital marketplace - Legal issues specific to e-commerce (consumer protection, cross-border transactions) - Formation, validity and enforcement of electronic contracts - Contractual and non-contractual liability in the information society - Legal framework for electronic transactions (Electronic Transactions Ordinance & related statutes) - Intellectual Property Rights in cyberspace - Copyright in digital content - Trademarks, domain names and cybersquatting - Defamation on digital platforms - Intermediary liability, safe-harbor provisions and recent judicial trends - Regulation of digital payments and fintech services	6
5	**Privacy, Data Protection & Security Governance** - Information security fundamentals and privacy concepts in cyberspace - Data-protection challenges in electronic communication and cloud services - Security policies, standards and regulatory landscape (ISO 27001, NIST CSF, Indian cyber-security policy) - Legal developments in cyber-security (recent amendments, sector-specific rules) - Security considerations for e-transactions and digital wallets - Governance, risk management and compliance (GRC) frameworks - Conducting information-security risk assessments - Data-breach notification requirements and incident-response planning - National and organizational cyber-security policies and their ethical linkages - Introductory view of cyber-insurance as a risk-mitigation tool	8
6	**Cyber Ethics, Professional Codes & Emerging Issues** - Importance of cyber law and ethics for professionals - Ethical foundations in the information society - Professional and organisational codes of ethics for	6

	cyber-security practitioners - Risk-management ethics and responsible disclosure practices - Artificial Intelligence ethics: core principles, bias, accountability and emerging regulations - Blockchain and distributed-ledger ethics: legal developments and security implications - Ethical considerations for biometric data and digital identity - Responsibilities of users, developers and managers in cyber-security - Emerging ethical challenges: deep-fakes, misinformation, AI-generated content, and societal impact - Guidelines for ethical hacking and penetration-testing standards	

6. References

Textbooks:

1. Pavan Duggal - "Cyber Law: An Exhaustive Section-Wise Commentary on the Information Technology Act, 2000"

2. Jyoti Rattan - "Cyber Laws, Information Technology and Artificial Intelligence" (EBC)

Reference Books:

1. Pavan Duggal - "Information Technology Law and Practice: Cyber Laws & E-Commerce, Data Privacy, Social Media & E-Governance" (LexisNexis)

2. "Ethics and Cyber Law" (compiled text / monograph)

7. Course Outcomes

ID	Statement	Action Verb	Knowledge Level
CY-605.1	Recall and list the key historical milestones of computer technology, the evolution of cyberspace, and the fundamental concepts of cyber jurisdiction, cyber law doctrines, and international instruments governing cyberspace.	Recall	Remember

CY-605.2	Explain the core principles of cyber ethics, professional codes of conduct, and the major provisions of the Indian IT Act (including amendments), GDPR, and other comparative cyber-law frameworks, distinguishing between civil and criminal liability.	Explain	Understand
CY-605.3	Apply the legal requirements for electronic records, digital signatures, and e-commerce contracts to evaluate the compliance of a given online transaction against the Indian IT Act, the Electronic Transactions Ordinance, and relevant consumer-protection statutes.	Apply	Apply
CY-605.4	Analyze a simulated cyber-crime incident by identifying applicable IPC sections, Evidence Act provisions, and chain-of-custody rules; select appropriate forensic tools (e.g., FTK, Autopsy, Wireshark) and justify their use in preserving admissible electronic evidence.	Analyze	Analyze
CY-605.5	Evaluate the effectiveness of privacy, data-protection, and security-governance frameworks (ISO 27001, NIST CSF, Indian cyber-security policy) for a mid-size organization, and recommend risk-mitigation and breach-notification measures that satisfy legal and ethical obligations.	Evaluate	Evaluate
CY-605.6	Design a comprehensive cyber-security policy and incident-response plan that integrates legal compliance (IT Act, PDP Bill draft, AI-ethics guidelines), ethical hacking standards, and technical controls (encryption, access management, cyber-insurance) for a hypothetical enterprise.	Design	Create

8. CO-PO Mapping

CO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
CO1	3	1	1	1	-	2	-	1	-	1	-	1
CO2	3	2	1	2	-	3	1	3	1	2	-	2
CO3	3	3	2	2	1	3	-	2	1	2	1	2
CO4	3	3	1	3	3	3	-	2	2	2	1	2
CO5	3	3	3	2	2	3	1	3	2	3	2	2
CO6	3	3	3	2	2	3	1	3	3	3	3	2

9. CO-PSO Mapping

CO	PSO1	PSO2	PSO3
CO1	2	1	3
CO2	2	1	3
CO3	2	1	3
CO4	1	3	2
CO5	3	1	3
CO6	3	2	3

DR. B.C. ROY SOCIETY
ENGINEERING
AN AUTONOMOUS INSTITUTE

Dr. B. C. Roy Engineering College, Durgapur

Department of CSE(CS)

Field	Details
Course Name	Vulnerability Assessment & Penetration Testing
Course Code	CY-606
Semester	6
Course Category	Program Core Courses
Credits	3
Hours per Week	3L:0T:4P

1. Prerequisites

- Fundamental networking concepts (TCP/IP model, IP addressing, common protocols and ports)
- Basic Linux/Unix command-line proficiency and operating-system fundamentals
- Introductory programming/scripting skills (e.g., Python or Bash)

2. Course Learning Objectives

- This course introduces students to fundamental concepts and applications of the subject
- Students will learn theoretical foundations and practical skills relevant to the field

3. Teaching Methodology

- Lectures and Presentations
- Interactive Discussions and Case Studies
- Lab Sessions

• Guest Lectures

4. Evaluation System

Activities	**Class Test Full marks**	**Assignment Full marks**	**Attendance Full marks**	**Total Marks**
CIA-1	25	10	5	40
CIA-2	25	10	5	40
End Semester Examination (ESE)	_	_	_	60
Total				100

5. Course Modules

Module	Topics	Hours
1	**Foundations of Ethical Hacking & Linux Environment** - Core security concepts (CIA triad, risk management, security controls) - Ethical-hacking terminology, hacker classifications & hacktivism - Legal, regulatory and professional ethics (laws, codes of conduct, compliance frameworks - ISO 27001, NIST) - Penetration-testing lifecycle (recon -> reporting) and test types (network, web, physical, social) - Fundamentals of cryptography for security professionals (symmetric, asymmetric, hashing, key management) - Introduction to Linux for security work * Linux architecture & why it is preferred for security tools * Installing Linux in a virtual machine (VMware/VirtualBox) * File-system layout and basic command-line skills (ls, cd, cp, mv, chmod, chown)	6

	* Text editors (vi, nano) and text-processing utilities (grep, awk, cut, sort) * Package management with apt (search, install, update, remove) - Overview of Kali Linux (purpose, download, installation, network configuration, updating and tool selection) - Basic networking refresher (TCP/IP model, IPv4/IPv6 addressing, common ports & protocols)	
2	**Reconnaissance, Scanning & Social Engineering** - Defining scope, rules of engagement and documentation of the engagement plan - Open-source intelligence (OSINT) techniques: search engines, social media, DNS, WHOIS, Shodan - Network discovery and scanning with Nmap (host discovery, port & service enumeration, version detection) - Service-specific enumeration (SMB, NFS, SMTP, LDAP, RDP) using native tools and scripts - Packet capture and analysis fundamentals with Wireshark (filters, protocol decoding) - Vulnerability-scanning overview * Types of scans (credentialed, unauthenticated, web, network) * Installing, configuring and running Nessus/OpenVAS * Mapping findings to assets and risk rating - Social-engineering fundamentals * Human-psychology models, attack vectors, phishing, pre-texting, baiting * Hands-on lab with the Social-Engineering Toolkit (SET) and password-profile tools - Conducting a basic phishing simulation and reporting the results	7
3	**Exploitation & Privilege Escalation** - Exploit research workflow (identifying CVEs, using Exploit-DB, selecting Metasploit modules) - Introduction to the Metasploit Framework (console, module types, payloads, basic Meterpreter commands) - Linux exploitation basics * Stack concepts and simple buffer-overflow demonstration (no advanced memory-model math) * Writing a minimal proof-of-concept exploit and testing in a controlled VM - Privilege-escalation techniques * Linux vectors (SUID mis-configurations, kernel module exploits, weak sudo settings) * Windows vectors (token impersonation,	8

	unquoted service paths, insecure registry settings) - Credential-access methods * Password-dumping tools (lsass, sam, hashdump), offline cracking basics (hashcat, John the Ripper) * Brute-force and password-spraying considerations - Network sniffing and spoofing * tcpdump basics, ARP spoofing with ettercap, MITM concepts - Post-exploit automation (simple scripting with msfconsole, basic persistence techniques)	
4	**Web Application & Client-Side Security** - Web-server fundamentals and common hardening practices - OWASP Top 10 overview and mapping to testing activities - Injection attacks * SQL injection (in-band, out-of-band, blind) - detection and exploitation * Command/OS injection and unsafe deserialization - Cross-Site Scripting (XSS) - reflected, stored, DOM-based - Cross-Site Request Forgery (CSRF) and insecure authentication mechanisms - Session management weaknesses (session fixation, hijacking) - Web-application testing tools * Nikto for server fingerprinting * Burp Suite (proxy, scanner, intruder, repeater) - hands-on lab - Client-side security basics * Browser security models, same-origin policy, clickjacking * Simple client-side script injection and mitigation techniques - Defensive coding guidelines and secure development lifecycle (SDLC) basics	7
5	**Post-Exploitation, Maintaining Access & Reporting** - Persistence mechanisms (backdoors, scheduled tasks, startup scripts, rootkits) and safe removal - Tunneling and proxy techniques (SSH tunnels, SOCKS proxies, VPN pivoting) - Clean-up procedures and evidence handling after a test - Documentation standards (evidence collection, chain of custody, log keeping) - Penetration-test reporting formats	6

	* Technical report (findings, evidence, remediation steps) * Executive summary (risk language, business impact) * Remediation roadmap and validation testing - Effective presentation skills for technical and non-technical stakeholders - Communication during an engagement (status updates, escalation, incident handling) - Mapping findings to risk frameworks (CVSS scoring, NIST CSF, ISO 27001 controls)	
6	**Advanced & Specialized Topics** - Physical security testing * Threat modeling for facilities, entry techniques, tailgating, lock-picking basics * Counter-measures and insider-threat considerations - Wireless security assessment * Wi-Fi standards (WEP, WPA/WPA2/WPA3), authentication methods * Rogue AP attacks, deauthentication, WPA/WPA2-PSK cracking with Aircrack-ng - Malware analysis fundamentals (no deep reverse-engineering math) * Sample collection, static analysis (strings, PE/ELF headers), dynamic sandboxing basics * Introduction to honeypots and threat-intel sharing - Advanced Windows exploitation (practical SEH abuse, bypassing DEP/ASLR using known techniques) - Advanced social-engineering vectors * Vishing, smishing, deep-fake phishing, physical pre-texting * Building a security-awareness program - Emerging trends * Cloud-service security testing (IAM misconfigurations, container security) * IoT device assessment basics * Security automation & scripting (Python for scanning, API integration) - Review of career pathways, certifications (OSCP, CEH, GPEN) and professional development	8

6. References

Textbooks:

1. Gray Hat Hacking-The Ethical Hackers Handbook", Allen Harper, Stephen Sims, Michael Baucom, 3rd Edition, Tata Mc Graw-Hill.

2. The Web Application Hacker's Handbook-Discovering and Exploiting Security flaws", Dafydd Suttard, Marcus pinto, 1st Edition, Wiley Publishing.

3. Kimberly Graves, "CEH: Official Certified Ethical Hacker Review Guide", Wiley Publishing Inc. 2007.

4. TediHeriyanto, Shakeel Ali, "Backtrack 4: Assuring Security byPenetration Testing", Shroff/Packt Publishing.

Reference Books:

1. Patrick Engebretson, "The Basics of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made Easy", Syngress.

2. Ronald L. Krutz and Russell Dean Vines, "The CEH Prep Guide: The Comprehensive Guide to Certified Ethical Hacking", Wiley.

3. PenetrationTesting:Hands-onIntroductiontoHacking",GeorgiaWeidman,1stEdition,NoStarchPress.

4. The Pen Tester Blueprint - Starting a Career as an Ethical Hacker, L. Wylie, Kim Crawly,1st Edition, Wiley Publications.

7. Course Outcomes

ID	Statement	Action Verb	Knowledge Level
CY-604.1	Recall and list at least ten core security concepts, Linux command-line utilities, and basic TCP/IP networking components required for penetration-testing activities.	Recall	Remember
CY-604.2	Explain the ethical-hacking lifecycle, relevant legal/regulatory frameworks (e.g., ISO 27001, NIST), and OSINT techniques, and differentiate between the various hacker classifications and test types.	Explain	Understand
CY-604.3	Demonstrate the ability to configure and operate reconnaissance and scanning tools (Nmap, Nessus/OpenVAS, Wireshark, SET) to discover	Demonstrate	Apply

	assets, enumerate services, and conduct a basic phishing simulation in a controlled lab environment.		
CY-604.4	Analyze vulnerability data and exploit results to perform privilege-escalation attacks on Linux and Windows targets, execute web-application attacks (SQLi, XSS, CSRF), and map findings to CVSS scores and relevant control frameworks.	Analyze	Analyze
CY-604.5	Evaluate the effectiveness of discovered security weaknesses, propose appropriate mitigation strategies, and justify remediation recommendations using NIST CSF and ISO 27001 control mappings.	Evaluate	Evaluate
CY-604.6	Create a complete penetration-testing deliverable--including technical findings, executive summary, remediation roadmap, and a short presentation--while also developing a reusable Python script that automates at least one scanning or reporting task.	Create	Create

8. CO-PO Mapping

CO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
CO1	3	2	1	1	1	1	-	-	-	-	-	2
CO2	3	2	1	2	1	3	-	3	1	2	1	2
CO3	2	2	2	3	3	1	-	1	1	1	1	2
CO4	2	3	2	3	2	2	-	2	1	1	1	2
CO5	2	2	3	2	1	3	1	3	1	3	2	2
CO6	2	2	3	2	3	2	1	2	2	3	3	2

9. CO-PSO Mapping

CO	PSO1	PSO2	PSO3
CO1	3	2	1
CO2	2	1	3
CO3	2	3	1
CO4	1	3	2
CO5	1	2	3

CO6	2	3	1