Chhattisgarh Swami Vivekananda Technical University, Bhilai (C.G.)

Program/Semester: B.Tech. (VII Sem)	**Branch: Cyber Security**
Subject: Quantum Cryptography	**Course Code: D131711(022)**
Total/Minimum-Pass Marks (End Semester Exam):100/35	**L:2 T:1 P:0 Credits: 3**
Class Tests & Assignments to be conducted : 2 each	**Duration (End Semester Exam): 03 Hours**

Course Objectives:

1. To analyze quantum mechanics relevance to computing and cryptography.
2. To evaluate the mechanics and security of various Quantum Key Distribution (QKD) protocols.
3. To appraise quantum security's theoretical foundations against classical models.
4. To assess quantum computing's cryptographic threat and formulate PQC solutions.
5. To investigate challenges and solutions in quantum-safe communication deployment.

UNIT- I: Foundations of Quantum Mechanics for Computing
Quantum States and Qubits: Superposition principle, Bloch Sphere representation, mathematical modeling of qubits**, Principle of Superposition:**Parallel computation analogy, measurement collapse, Hadamard gate application, **Quantum Entanglement:**Spooky action at a distance, EPR paradox, Bell states, eavesdropping detection, **Quantum Gates and Circuits:**Single-qubit gates (X, Y, Z, H), multi-qubit gates (CNOT, SWAP), circuit composition

UNIT- II: Quantum Key Distribution (QKD) Protocols
BB84 Protocol: Polarization encoding, basis reconciliation, sifting process, error rate analysis, **B92 Protocol:**Two-state system, non-orthogonal states, efficiency trade-offs, simplified implementation, **E91 Protocol:** Entanglement-based security, Bell test verification, device-independent security

UNIT-III: Principles of Quantum Security
Quantum Eavesdropping: Intercept-resend attacks, photon-number splitting, basis mismatch exploits, **No-Cloning Theorem:** Quantum state copying impossibility, security foundation, mathematical proof, **Information-Theoretic Security:** Computational vs unconditional security, future-proof guarantees

UNIT- IV: Post-Quantum Cryptography (PQC)
Quantum Threat: Shor's algorithm impact, RSA/ECC vulnerability, Grover's algorithm implications, **PQC Definition:** Classical algorithms resistant to quantum attacks, NIST standardization process, **PQC Families:**Lattice-based, code-based, multivariate, hash-based, isogeny-based cryptography, **Standardization Status:** CRYSTALS-Kyber, CRYSTALS-Dilithium, Falcon, SPHINCS+ implementations

UNIT-V: Practical Aspects & Future
QKD Implementation: Fiber optic limitations, free-space challenges, detector vulnerabilities, **Hybrid Cryptography:**Transitional strategies, parallel algorithm deployment, crypto-agility, **Quantum Internet:**Entanglement distribution, quantum repeaters, secure cloud computing, **Societal Impact:** Cryptographic migration costs, national security implications, long-term planning

TextBooks:

1. Nielsen, M. A., & Chuang, I. L. (2010). Quantum Computation and Quantum Information: 10th Anniversary Edition. Cambridge University Press.

ReferenceBooks:

1. Gisin, N., et al. (2002). Quantum Cryptography. Reviews of Modern Physics
2. Bernstein, D. J., & Lange, T. (2017). Post-Quantum Cryptography. Springer
3. Yanofsky, N. S., &Mannucci, M. A. (2008). Quantum Computing for Computer Scientists

Course Outcomes

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

1. Explain quantum mechanics core concepts and illustrate their mathematical representations.
2. Compare QKD protocols (BB84, B92, E91) and simulate their operational steps.
3. Analyze quantum eavesdropping and justify information-theoretic security via the no-cloning theorem.
4. Evaluate classical cryptosystem vulnerabilities to quantum algorithms and categorize PQC families.
5. Discuss practical challenges in quantum-safe solutions and propose quantum internet applications.

Chhattisgarh Swami Vivekananda Technical University, Bhilai (C.G.)

Program/Semester: B.Tech. (VII Sem)	Branch: Cyber Security
Subject: Quantum Cryptography (Lab)	Course Code: D131721(022)
Total/Minimum-Pass Marks(End Semester Exam): 40/20	L:0 T:0 P:2 Credits: 1

Course Objectives

1. Apply foundational quantum principles by building simulated quantum circuits.
2. Implement and debug simulated QKD protocols (BB84, B92).
3. Evaluate QKD security by simulating and analyzing eavesdropping.
4. Utilize PQC libraries for basic cryptographic operations.
5. Analyze and compare quantum protocols or attack scenarios via simulation.

Suggested list of experiments (but should not be limited to)
The lab component is designed to be completed using a quantum simulation framework such as **IBM's Qiskit or Microsoft's Quantum Development Kit**.

1. **Familiarize with the quantum simulation environment:**Define a quantum register and a classical register. Create a simple circuit to initialize a qubit, apply a Pauli-X gate (quantum NOT), and measure the outcome. Execute the simulation and analyze the results.
2. **Understand and create superposition states:** Apply the Hadamard gate to a qubit to put it into a superposition of |0⟩ and |1⟩ Run the simulation multiple times to observe the probabilistic nature of measurement (approximately 50% 0s and 50% 1s).
3. **Creating Quantum Entanglement:**Generate and verify an entangled state (Bell state). Create a two-qubit circuit. Apply a Hadamard gate to the first qubit and a CNOT gate to both qubits. Measure both qubits and run the simulation. Verify that the outcomes are perfectly correlated (only 00 and 11 appear).
4. **Simulating the BB84 Protocol:**Implement a simplified version of the BB84 protocol.

a) Simulate Alice generating a random sequence of bits and bases to polarize photons (prepare qubit states). Simulate Bob measuring these qubits with his own random sequence of bases.

b) Implement the "sifting" process where Alice and Bob publicly compare bases and discard measurements where their bases did not match. Generate the final sifted key.

5. **Simulating an Eavesdropper on BB84:** Demonstrate how an eavesdropper is detected.Introduce a third party (Eve) into the BB84 simulation from Lab 4/5. Eve will implement an intercept-resend attack. Compare Alice and Bob's final sifted keys and calculate the Quantum Bit Error Rate (QBER). Show that Eve's presence introduces a significant number of errors.
6. **Simulating the B92 Protocol:** Implement the simpler B92 QKD protocol. Create a simulation where Alice sends qubits in one of two non-orthogonal states. Simulate Bob's measurement process, where some outcomes are conclusive and others are discarded. Generate a shared key and compare the efficiency to the BB84 simulation.
7. **Advanced Eavesdropping:** Simulate a more sophisticated attack on BB84 (e.g., photon-number splitting if feasible, or basis mismatch attack).
8. **Protocol Efficiency Analysis:** Conduct a comparative performance analysis of BB84 and B92 under simulated noisy conditions.
9. **E91 Simulation:** Implement a basic simulation of the E91 protocol by generating entangled pairs and simulating measurements on different bases to check for Bell's inequality violation.
10. **Exploring a Post-Quantum Cryptography Library:** Get acquainted with libraries implementing PQC algorithms and understand their basic usage.Using a high-level library (e.g., a Python library like pqcrypto if available, or a conceptual walkthrough of usage examples with provided code snippets), implement basic operations like key generation, encryption/decryption, or signing/verification for a selected PQC algorithm (e.g., a lattice-based scheme). Analyze and compare key sizes and performance (e.g., encryption/decryption time) with classical counterparts if tools allow.

TextBooks:

1. Nielsen, M. A., & Chuang, I. L. (2010). Quantum Computation and Quantum Information: 10th Anniversary Edition. Cambridge University Press.

ReferenceBooks:

1. Bernstein, D. J., & Lange, T. (2017). Post-Quantum Cryptography. Springer
2. Yanofsky, N. S., &Mannucci, M. A. (2008). Quantum Computing for Computer Scientists

Course Outcomes:

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

1. Construct circuits demonstrating superposition and entanglement.
2. Implement and verify QKD protocols (BB84, B92) through simulation.
3. Detect and quantify eavesdropping impact on QKD via analysis.
4. Experiment with PQC libraries for cryptographic operations.
5. Assess quantum protocol efficiency/security via comparative analysis or advanced simulations.

Chhattisgarh Swami Vivekananda Technical University, Bhilai (C.G.)

Program/Semester: B.Tech. (VII Sem)	**Branch: Cyber Security**
Subject: Cloud Security	**Course Code: D131712(022)**
Total/Minimum-Pass Marks (End Semester Exam): 100/35	**L:2 T:1 P:0 Credits: 3**
Class Tests & Assignments to be conducted : 2each	**Duration(End Semester Exam): 03 Hours**

Course Objectives

1. Describe cloud computing models, core components and the specific security challenges of cloud environments.
2. Explain virtualization, containerization, and architectural security controls used in public/private/hybrid clouds.
3. Apply identity, access management and cryptographic controls to protect cloud-hosted data and services.
4. Analyze cloud network, storage and application security issues and perform basic threat assessment.
5. Evaluate governance, compliance and incident response practices for cloud deployments and propose simple secure architectures.

UNIT-I: Foundations of Quantum Mechanics for Computing
Quantum States and Qubits: Superposition principle, Bloch Sphere representation, mathematical modeling of qubits, Principle of Superposition: Parallel computation analogy, measurement collapse, Hadamard gate application, Quantum Entanglement: Spooky action at a distance, EPR paradox, Bell states, eavesdropping detection, Quantum Gates and Circuits: Single-qubit gates (X, Y, Z, H), multi-qubit gates (CNOT, SWAP), circuit composition

UNIT-II: Foundations: Cloud models, service & deployment models, threat landscape
Definitions: IaaS, PaaS, SaaS, public/private/hybrid clouds, shared-responsibility model, Cloud enabling tech: virtualization, multi-tenancy, elasticity, provisioning, Cloud threat taxonomy (data breaches, misconfiguration, insecure APIs, insider threats), Introduction to cloud security standards and guidance (NIST, CSA)

UNIT-III: Virtualization, Hypervisors, Containers & Identity & Access Management (IAM)
Virtualization concepts, hypervisor types, VM isolation issues, Containerization basics (Docker, Kubernetes): attack surface and security considerations, IAM concepts: authentication vs authorization, federation (SAML, OAuth2, OpenID Connect), roles & policies, least privilege, Identity in the cloud (single sign-on, AD/IdP integration)

UNIT-IV: Data protection, cryptography & key management
Data classification in cloud, data lifecycle (in-transit, at-rest, in-use), Symmetric/asymmetric crypto basics applied to cloud (TLS, disk/envelope encryption), Key Management Service (KMS) concepts, HSMs, secrets management (Vault), Client-side vs server-side encryption tradeoffs, tokenization, secure backups

UNIT-V: Network, platform & application security in cloud
Virtual networks, VPCs, subnets, security groups, firewalls, Network segmentation, micro-segmentation, Zero Trust basics for cloud, Secure API design, WAFs, DDoS basics, load-balancer security, Logging, monitoring, auditing, SIEM basics in cloud (CloudWatch, Stackdriver etc.)

UNIT-V: Governance, compliance, incident response & secure cloud design patterns
Governance: cloud policies, shared responsibility, vendor risk management, SLA/contract basics, Compliance & privacy (GDPR basics, Indian data protection considerations), Incident response, forensics in the cloud, business continuity & disaster recovery (backup strategies), Secure architecture review: reference architectures, hardening checklists, case studies (AWS/Azure/GCP basic examples)

TextBooks:

1. Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance - Tim Mather, Subra Kumaraswamy, Shahed Latif (O'Reilly).
2. Cloud Computing: Concepts, Technology & Architecture Thomas Erl (Pearson).

ReferenceBooks:

1. Cloud Security: A Comprehensive Guide to Secure Cloud Computing - Ronald L. Krutz& Russell Dean Vines (Wiley).
2. Practical Cloud Security: A Guide for Secure Design and Deployment - Chris Dotson (O'Reilly).
3. NIST Special Publication 800-144: Guidelines on Security and Privacy in Public Cloud Computing.
4. Cloud Security Alliance - Security Guidance (v5)

Course Outcomes

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

1. Explain cloud models and identify security threats unique to cloud deployments.
2. Demonstrate understanding of virtualization/containers and configure basic IAM policies.
3. Implement basic encryption and key management techniques to protect cloud data.
4. Design and test basic network and application security controls in a cloud environment.
5. Create a simple compliance-aware incident response and secure-deployment plan for a sample cloud system.

Chhattisgarh Swami Vivekananda Technical University, Bhilai (C.G.)

Program/Semester: B.Tech. (VII Sem)	Branch: Cyber Security
Subject: Cloud Security (Lab)	Course Code: D131722(022)
Total/Minimum-Pass Marks(End Semester Exam):40/20	L:0 T:0 P:2 Credits:1

Course Objectives

1. Provide hands-on experience in configuring and securing cloud resources using IAM, encryption, network, and container security controls.
2. Develop proficiency in utilizing open-source and cloud-native tools for scanning, monitoring, and hardening cloud environments.
3. Cultivate the ability to design, execute, and document incident-response procedures for simulated cloud security breaches.
4. Enable application of compliance frameworks and security guidelines (CSA, NIST) in evaluating and improving cloud deployments.
5. Integrate theoretical knowledge into a secure cloud-based mini-project, demonstrating end-to-end implementation of best practices.

Suggested list of experiments (but should not be limited to)

1. Explore AWS/GCP free tier; create account, understand console & shared-responsibility model; deploy a sample VM.
2. Launch VMs, inspect hypervisor/container differences; run a Docker container and map ports; introduce Kubernetes (Minikube).
3. Configure IAM: create users, groups, roles; write and test a least-privilege policy; experiment with OAuth2 / OpenID Connect sample flow.
4. Use OpenSSL to create keys and certificates; enable TLS for a simple web app; use cloud KMS to encrypt/decrypt an object.
5. Implement server-side vs client-side encryption: encrypt a file locally and upload; use KMS/HSM simulation.
6. Configure VPC/subnet/security groups/firewall rules; verify connectivity; simulate misconfiguration and remediation.
7. Deploy a sample web app, scan with OWASP ZAP, apply WAF rules; run basic DDoS simulation in safe lab environment (rate-limiting).
8. Use monitoring/logging: enable CloudWatch/Stackdriver/Cloud Audit Logs; create alerts and simple dashboards.
9. Create an incident response playbook for a simulated breach (data-leak scenario), collect logs, perform basic forensic steps (snapshot VM, preserve evidence).
10. Compliance checklist & vendor assessment exercise: map cloud controls to CSA/NIST guidance; perform policy gap analysis.
11. Mini-project - Secure-deploy a simple 3-tier application on cloud (or local minikube), implement IAM, encryption, network controls, logging; produce report with risk assessment and incident-response plan.

Tools & Platforms

1. **Cloud platforms:** AWS / Azure / GCP (free tiers or edu credits) or local Minikube/VirtualBox.
2. **Tools:** Docker, Kubernetes (kubectl), OpenSSL, Wireshark, OWASP ZAP, HashiCorp Vault, Terraform (optional), Cloud provider CLIs (awscli/gcloud/az).
3. **Monitoring & SIEM basics:** CloudWatch, Stackdriver, or open-source (ELK stack basic demo).

TextBooks:

1. Practical Cloud Security: A Guide for Secure Design and Deployment – Chris Dotson, O'Reilly.

ReferenceBooks:

1. Docker and Kubernetes for Beginners – Arun Gupta & Michael Hausenblas, O'Reilly.
2. AWS Certified Security – Specialty Exam Guide – Stuart Scott, Packt Publishing.

Course Outcomes:

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

1. Configure and deploy cloud resources while applying identity, access, and encryption controls.
2. Implement virtualization and container security measures in public, private, or hybrid cloud environments.
3. Apply network segmentation, firewall rules, and monitoring tools to secure cloud-hosted applications.
4. Perform basic threat detection, incident-response, and forensic analysis in simulated cloud scenarios.
5. Evaluate cloud deployments for compliance and security gaps, proposing improvements through a documented mini-project.

Chhattisgarh Swami Vivekananda Technical University, Bhilai (C.G.)

Program/Semester: B.Tech. (VII Sem)	**Branch: Cyber Security**
Subject: Database Security	**Course Code: D131713(022)**
Total/Minimum-Pass Marks (End Semester Exam): 100/35	**L:3 T:1 P:0 Credits: 4**
Class Tests & Assignments to be conducted: 2each	**Duration (End Semester Exam): 03Hours**

Course Objectives

1. Introduce fundamental concepts, threats, and vulnerabilities related to database security.
2. Provide an understanding of authentication, authorization, encryption, and access control mechanisms.
3. Enable students to detect and mitigate database security threats, including SQL injection.
4. Familiarize students with database auditing, compliance regulations, and disaster recovery planning.
5. Equip students with skills to design secure database systems.

UNIT-I: Introduction to Database Security
Security goals: Confidentiality, Integrity, Availability (CIA), Threats and vulnerabilities in databases, Security models: DAC, MAC, RBAC, Overview of SQL security features.

UNIT-II: Authentication and Access Control
User identification and password policies, Grant, Revoke, and role management in SQL, Multi-factor authentication concepts, Access control in MySQL, PostgreSQL,Oracle.

UNIT-III:: Encryption and Data Privacy
Data-at-rest and data-in-transit encryption, Symmetric and asymmetric encryption, Transparent Data Encryption (TDE), Data masking and tokenization, Hands-on with DBMS-based encryption functions.

UNIT-IV: Database Threats and Mitigation
SQL injection: types, detection, prevention, Insider threats and privilege abuse, Secure coding practices for stored procedures, Database firewalls and intrusion detection.

UNIT-V: Auditing, Compliance, and Disaster Recovery
Database auditing and logging, Compliance standards: GDPR, HIPAA, PCI DSS basics, Backup and recovery models, Incident response and breach handling, Designing secure database schemas and security policies

TextBooks:

1. Alfred Basta and Melissa Zgola, Database Security, Cengage Learning, 2011.

ReferenceBooks:

1. Michael Gertz & Sushil Jajodia, Handbook of Database Security, Springer, 2008.
2. Silberschatz, Korth& Sudarshan, Database System Concepts, McGraw Hill (Security Chapters).
3. Bertino, E., & Sandhu, R., "Database Security – Concepts, Approaches, and Challenges," IEEE Transactions on Dependable and Secure Computing, 2005.

Course Outcomes

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

1. Define and explain the fundamental concepts, models, and goals of database security.
2. Apply authentication, authorization, and access control techniques in SQL-based environments.
3. Implement encryption and data masking techniques to protect sensitive information.
4. Analyze common database threats and evaluate countermeasures to mitigate risks.
5. Design secure database schemas, auditing policies, and disaster recovery plans.

Chhattisgarh Swami Vivekananda Technical University, Bhilai (C.G.)

Program/Semester: B.Tech. (VII Sem)	**Branch: Cyber Security**
Subject: Cyber and Digital Forensics (Professional Elective)	**Course Code: D131731(022)**
Total/Minimum-Pass Marks (End Semester Exam): 100/35	**L:1 T:1 P:0 Credits: 2**
Class Tests & Assignments to be conducted : 2 each	**Duration(End Semester Exam): 03 Hours**

Course Objectives

1. Introduce core concepts, processes and terminology of digital forensics and cyber investigations.
2. Teach standard forensic procedures for evidence identification, acquisition, preservation and chain-of-custody.
3. Provide hands-on experience with common forensic tools and techniques for disk, memory and network data.
4. Cover the legal, ethical and reporting aspects of forensic investigations in the Indian context.
5. Develop students' ability to perform basic forensic analysis and present findings in a clear, reproducible report.

UNIT-I: Fundamentals of Cyber & Digital Forensics
Definitions, scope, types of forensics (computer, mobile, network, cloud), Forensic process model: identification, collection, preservation, analysis, reporting, Role of first responder, incident response basics, Evidence concept: admissibility, integrity, reproducibility.

UNIT-II: Forensic Acquisition & Evidence Handling
Imaging: logical vs physical vs live memory (RAM) acquisition, Write-blockers, hardware & software tools for imaging, Hashing and integrity verification; chain-of-custody documentation, Storage fundamentals (FAT, NTFS, ext*, partition tables) relevant to evidence retrieval.

UNIT-III: File System, Data Recovery & Artifact Analysis
File metadata, timestamps, slack space, deleted file recovery, file carving, Registry basics (Windows registry artifacts) and common artifacts (user activity, recently used files, browser artifacts), Timeline analysis and correlation across artifacts.

UNIT-IV: Memory, Mobile & Network Forensics
Volatile memory forensics: acquisition (FTK Imager, LiME), basics of memory analysis (strings, Volatility), Mobile device forensics basics (Android/iOS artifacts, backups, limitations), SIM/SD card considerations, Network forensics: packet capture basics, analysingpcap with Wireshark, basic intrusion evidence (suspicious flows, data exfiltration indicators).

UNIT-V: Legal, Ethical, Reporting & Case Studies
Legal framework and evidence admissibility (Indian Evidence Act basics, search & seizure principles, privacy considerations) — conceptual (refer to local counsel for specifics), Ethics, privacy, and professional responsibilities, Forensic reporting best practices; writing clear, reproducible reports; presenting evidence in court (expert witness basics), Mini case-studies: common scenarios and walkthroughs (insider data theft, basic malware incident reconstruction).

TextBooks:

1. Nelson, B., Phillips, A., Enfinger, F., &Steuart, C. - Guide to Computer Forensics and Investigations (latest edition).

ReferenceBooks:

1. Casey, E. - Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet (Elsevier).
2. Britz, M. T. - Computer Forensics and Cyber Crime: An Introduction (or similarly titled edition).

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

1. Define and explain fundamental digital forensics concepts, terminologies and workflows.
2. Prepare and demonstrate proper evidence acquisition and preservation.
3. Perform basic forensic analysis on storage and volatile memory using open-source tools.
4. Analyze simple network logs and capture files to detect and reconstruct basic incidents.
5. Produce a concise, structured forensic report having oral briefing with findings, limitations and recommendations.

Chhattisgarh Swami Vivekananda Technical University, Bhilai (C.G.)

Program/Semester: B.Tech. (VII Sem)	**Branch: Cyber Security**
Subject: Information Security (Professional Elective)	**Course Code: D131733(022)**
Total/Minimum-Pass Marks (End Semester Exam): 100/35	**L:1 T:1 P:0 Credits: 2**
Class Tests & Assignments to be conducted : 2 each	**Duration (End Semester Exam): 03 Hrs**

Course Objectives

1. Introduce fundamental principles, concepts, and terminology of information security.
2. Familiarize students with common threats, vulnerabilities, and attack methods targeting computer systems and networks.
3. Develop skills for implementing basic security mechanisms like authentication, encryption, and access control.
4. Provide hands-on exposure to security tools for monitoring, detection, and prevention.
5. Enhance awareness of legal, ethical, and organizational aspects of information security.

UNIT-I: Introduction to Information Security
Fundamentals: CIA triad, security services, security mechanisms, Security models: Bell–LaPadula, Biba, Clark–Wilson, Threats, vulnerabilities, risks, and attacks (passive vs active), Security policies and standards (ISO/IEC 27001 overview).

UNIT-II: Cryptography Fundamentals
Symmetric encryption: DES, AES, Asymmetric encryption: RSA, Diffie–Hellman, Hash functions: SHA family, message authentication codes (MACs), Digital signatures and certificates (PKI basics), Secure key management practices.

UNIT-III: Authentication, Access Control, and Security Protocols
Authentication methods: passwords, OTP, biometrics, multi-factor, Access control models: DAC, MAC, RBAC, Network security protocols: SSL/TLS, IPSec, HTTPS, Kerberos, Secure email protocols: PGP, S/MIME.

UNIT-IV: Network & System Security
Firewalls: packet filtering, stateful inspection, application proxies, IDS/IPS: Snort basics, signature-based and anomaly-based detection, Securing operating systems and network devices, Malware: viruses, worms, ransomware, spyware — detection and prevention, Security in wireless networks (WPA2/WPA3).

UNIT-V: Security Management, Laws & Incident Handling
Security governance and risk management basics, Incident response process: preparation, detection, containment, eradication, recovery, lessons learned, Business continuity and disaster recovery planning, Indian IT Act 2000 & amendments, CERT-IN guidelines, Ethical and professional responsibilities

Text Books:

1. William Stallings - Cryptography and Network Security: Principles and Practice (latest edition)

ReferenceBooks:

1. Behrouz A. Forouzan&Debdeep Mukhopadhyay - Cryptography and Network Security (McGraw-Hill)
2. Mark Stamp - Information Security: Principles and Practice (Wiley)

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

1. Define and explain core information security concepts, goals, and models.
2. Identify and classify threats, vulnerabilities, and attacks on systems and networks.
3. Apply cryptographic algorithms and authentication mechanisms to secure data and communications.
4. Implement and configure basic security controls such as firewalls, IDS/IPS, and access control lists.
5. Analyze security incidents and recommend suitable mitigation measures

Chhattisgarh Swami Vivekananda Technical University, Bhilai (C.G.)

Program/Semester: B.Tech. (VII Sem)	**Branch: Cyber Security**
Subject: Vulnerability Assessment and Penetration Testing (Professional Elective)	**Course Code: D131732(022)**
Total/Minimum-Pass Marks (End Semester Exam): 100/35	**L:1 T:1 P:0 Credits: 2**
Class Tests & Assignments to be conducted : 2 each	**Duration(End Semester Exam): 03 Hours**

Course Objectives

1. Introduce concepts, methodologies, and tools used in vulnerability assessment and penetration testing.
2. Develop skills for identifying, analyzing, and mitigating security vulnerabilities in networks, applications, and systems.
3. Provide hands-on exposure to common penetration testing frameworks and reporting methods.
4. Enhance understanding of legal, ethical, and compliance considerations in security testing.
5. Prepare students to plan, execute, and document a basic penetration test in a controlled environment.

UNIT-I: Introduction to Vulnerability Assessment & Penetration Testing
Information security fundamentals review, Difference between vulnerability assessment and penetration testing, Scope definition, rules of engagement, and pre-engagement interactions, Types of testing: black-box, white-box, grey-box, VAPT methodology and phases (Reconnaissance, Scanning, Exploitation, Reporting), Ethics and legal considerations in India (IT Act 2000, CERT-IN guidelines).

UNIT-II: Reconnaissance & Information Gathering
Passive vs. active reconnaissance, WHOIS, DNS enumeration, Google dorking, metadata analysis, Network mapping (Nmap basics, service discovery, OS detection), Web application reconnaissance (robots.txt, sitemap, headers), Social engineering overview (limited, theory only for ethics).

UNIT-III: Vulnerability Assessment Techniques
Automated vulnerability scanning (Nessus, OpenVAS), Web vulnerability scanning (OWASP ZAP, Nikto), Manual verification of vulnerabilities, Common vulnerability types (OWASP Top 10, CVEs), Analyzing scanner output and reducing false positives.

UNIT-IV: Penetration Testing Methods
Exploitation fundamentals and payload delivery, Exploiting network services (SSH, SMB, FTP vulnerabilities), Web exploitation basics (SQL injection, XSS, file upload flaws), Password attacks (brute force, dictionary, hash cracking), Post-exploitation activities (privilege escalation, persistence), Metasploit Framework basics.

UNIT-V: Reporting, Mitigation & Best Practices
Report structure: executive summary, methodology, findings, recommendations, appendices, Evidence documentation (screenshots, logs, proof of concept), Risk rating methodologies (CVSS basics), Patch management and secure configuration, Best practices for secure system design, Final project: Conduct a mini VAPT on a controlled lab environment and submit a report.

Text Books:

1. Dafydd Stuttard & Marcus Pinto - The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws (2nd ed.)

ReferenceBooks:

1. Georgia Weidman - Penetration Testing: A Hands-On Introduction to Hacking (No Starch Press).
2. Patrick Engebretson - The Basics of Hacking and Penetration Testing (Elsevier/Syngress).

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

1. Explain the concepts, scope, and phases of VAPT.
2. Apply vulnerability scanning techniques and analyze scan reports.
3. Perform basic penetration testing on networks, systems, and web applications using appropriate tools.
4. Evaluate security risks and propose mitigation measures based on testing results.
5. Prepare professional VAPT reports that include findings, evidence, and recommendations.