Syllabus for PGDM with Cybersecurity as a specialisation (Duration: 2 years)

General Timeline Assumptions: 1 semester comprises 17-18 weeks of study; the PGDM course is to be completed in 4 semesters (spanning 2 years)

The unique pedagogical approach followed in this program ensures that students get 80% practical hands-on training for skill development along with theoretical knowledge for real-world understanding and application.

Assessments would be conducted after each module and will contribute towards the overall score. Semester exams would be conducted at the end of each semester. Finally, the cumulative scores would be taken into consideration to award the Diploma.

To pass the course and become eligible for the guaranteed employment program, students would need to score marks above 85% in their overall assessment that includes theory and practical exams.

The detailed syllabus for the **PGDM- Cybersecurity** program is given below.

	Course Modules Offered:		
Course	Theory (+ Skill Development)	**Credits**	
Semester 1			
PGDMG101	Management Functions and Organization Behaviour	4 -1	Core
PGDMG102	Business Communication	2	Core
PGDMG103	Financial And Management Accounting	4	Core
PGDMG104	Introduction To Information Technology + Fundamentals of Cybersecurity	2 + 2	Change
PGDMG105	Managerial Economics	3	Core
PGDMG106	Quantitative Techniques for Managers	4 -1	Core
PGDMG107	Marketing Management	4 -1	Core
PGDMG108	Business Law and Corporate Governance (+ Legal and ethical issues in cybersecurity)	3 + 1	Change
PGDMG109	International Business (replace with Cyber risk and compliance management)	3	Change
PGDMG110	Supply Chain Management (replace with Project Management for Cybersecurity)	3	Change
PGDMG111	Foreign Language- German/ French	2	Core
		Total 34	

Semester 2			
PGDMG201	Entrepreneurship management Replace	4	Change
PGDMG202	Strategic Management and Security Leadership)	4	Change
PGDMG203	International Business	3	Core
PGDMG204	Research Methodology	4	Core
PGDMG205	Management Accounting	4	Core
PGDMG206	Economic Environment for Business	3	Core
PGDMG207	Corporate Communication & Cybersecurity business Communication	2	Core
PGDMG208	Service Management (+ Incidence Response and service management)	3	Change
PGDMG209	Logistics and Transportation (replace with Programming for Cybersecurity)	3	Change
PGDMG210	Foreign Language - German/ French	2	Core
PGDMG211	Project and viva report	2	
		Total 34	
Semester 3			
PGDM301	**Infrastructure Security and Penetration Testing**	4	
PGDM302	**Web Application Security**	4	
PGDM303	**Mobile Application Security**	4	
PGDM304	**Attack Surface Management**	4	
PGDM305	Internships + Project and Viva Report	3	
		Total 27	
Semester 4			
PGDM401	**Cloud Security**	4	
PGDM402	**DevSecOps**	4	
PGDM403	**Advanced Web Application Security**	4	
PGDM404	**Advanced Infrastructure Security and Penetration Testing**	4	
PGDM405	Internships + Project and Viva Report	3	
		Total 27	

Detailed Syllabus: Course Overview, Learning Outcomes and Recommended Reading List

For Semesters 1 and 2, details of core retained modules of the PGDM program already exist with RMS. The details of the added Cybersecurity specific modules are provided below.

PGDMG101	Management Functions and Organization Behaviour

PGDMG102	Business Communication
PGDMG103	Financial And Management Accounting
PGDMG104	Introduction To Information Technology + Fundamentals of Cybersecurity

Fundamentals of Cybersecurity

Course Introduction and Objectives

This course provides a strong foundation in cybersecurity, equipping students with essential knowledge in information security principles, networking fundamentals, and operating system security. Designed for both technical and non-technical students, it introduces core cybersecurity concepts and their real-world applications. Learners will explore critical areas such as cyber threats, network security, risk management, and system protection strategies. The course blends theoretical learning with hands-on practice, ensuring students develop both conceptual understanding and practical skills required for a successful cybersecurity career.

Course Outcomes

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

- Understand the fundamental principles of information security, including confidentiality, integrity, and availability (CIA Triad).
- Identify common cyber threats, attack vectors, and risk mitigation strategies.
- Demonstrate knowledge of networking fundamentals, including communication models (OSI/TCP-IP) and key protocols.
- Analyze network security threats and implement protective measures such as firewalls, IDS/IPS, and VPNs.

- Gain proficiency in Windows and Linux operating systems, focusing on security configurations, access control, and system hardening.
- Apply security best practices in real-world IT environments and understand the role of compliance frameworks.

Course Content

Unit 1: Introduction to Information Security

This unit introduces the fundamental concepts of information security, including the CIA Triad (Confidentiality, Integrity, and Availability), which forms the foundation of cybersecurity practices. Students will explore various cyber threats, such as malware, phishing, ransomware, and social engineering attacks, and examine strategies to mitigate these risks. The module will also cover risk management principles, security policies, and key compliance frameworks such as GDPR, NIST, and ISO 27001, helping students understand the regulatory aspects of cybersecurity.

Unit 2: Networking Fundamentals

A solid understanding of networking is crucial for cybersecurity professionals. This unit covers the basics of computer networks, including different network types such as LAN, WAN, and VPN. Students will explore communication models (OSI and TCP/IP) and understand how data flows through networks. Key networking protocols, such as HTTP/S, FTP, DNS, SSH, and TLS/SSL, will be examined in detail. Additionally, students will learn about IP addressing, subnetting, and network topologies, building a strong foundation for understanding network security in later modules.

Unit 3: Network Security Essentials

This unit focuses on protecting networks against cyber threats by implementing defensive security measures. Students will learn about firewalls, Intrusion Detection and Prevention Systems (IDS/IPS), and Virtual Private Networks (VPNs), which help safeguard networks from unauthorized access. The course will also cover encryption methods, secure communication protocols, and network security frameworks. Advanced topics such as Man-in-the-Middle (MITM) attacks, Distributed Denial of Service (DDoS) attacks, and DNS spoofing will be explored, providing insight into modern attack techniques and defense mechanisms.

Unit 4: Operating Systems & Security

Understanding operating systems is essential for securing IT environments. This unit introduces students to Windows and Linux security fundamentals, covering user

account management, file permissions, system hardening techniques, and secure configurations. Students will explore Windows security features such as NTFS permissions, Group Policy settings, and access control mechanisms, as well as Linux security measures, including file system permissions, user roles, and system auditing tools. The importance of patch management, security updates, and endpoint protection will also be emphasized to ensure secure operating system configurations.

Recommended Books

Latest & Industry-Relevant Books

1. "Cybersecurity All-in-One For Dummies" – Joseph Steinberg (2023)
    - A beginner-friendly book covering cybersecurity principles, security tools, and best practices.
2. "Practical Cybersecurity Architecture" – Ed Moyle & Diana Kelley (2023)
    - A deep dive into designing secure systems, risk assessment, and compliance strategies.
3. "Zero Trust Security: An Enterprise Guide" – Jason Garbis & Jerry W. Chapman (2022)
    - Essential reading for understanding Zero Trust security and modern network defense.
4. "CompTIA Security+ Guide to Network Security Fundamentals" – Mark Ciampa (2022, 7th Edition)
    - Covers core security concepts, risk mitigation, and foundational cybersecurity skills.

This course ensures that students develop a strong cybersecurity foundation, enabling them to understand, analyze, and defend against cyber threats while applying industry best practices. The combination of conceptual learning, hands-on exercises, and case studies prepares students for further specialization in cybersecurity.

PGDMG105	Managerial Economics
PGDMG106	Quantitative Techniques for Managers
PGDMG107	Marketing Management
PGDMG108	Business Law and Corporate Governance (+ Legal and ethical issues in cybersecurity)

Legal and Ethical Issues in Cybersecurity

Course Introduction and Objectives

This module explores the legal frameworks, ethical dilemmas, and compliance requirements in the field of cybersecurity. It covers international and national cybersecurity laws, ethical hacking principles, data protection regulations, and the legal consequences of cybercrimes. Students will gain a deep understanding of cyber laws, ethical responsibilities, and best practices for ensuring compliance while conducting security operations.

Course Outcomes

By the end of this module, students will:

- Understand global and regional cybersecurity laws, including GDPR, CCPA, and India's IT Act.
- Examine legal responsibilities related to cybersecurity, data breaches, and digital forensics.
- Explore intellectual property rights (IPR) and cybersecurity-related legal frameworks.
- Analyze ethical considerations in ethical hacking, penetration testing, and cyber defense strategies.
- Learn about privacy regulations, surveillance laws, and user data protection.
- Understand the legal consequences of cybercrimes such as hacking, phishing, and identity theft.
- Study corporate cybersecurity policies and compliance frameworks like ISO 27001, NIST, and HIPAA.
- Evaluate real-world case studies on cybercrime investigations and legal proceedings.

Course Content

Unit 1: Cybersecurity Laws and Regulations

Covers international and national cyber laws, including GDPR (General Data Protection Regulation), CCPA (California Consumer Privacy Act), India's IT Act, and Computer Fraud and Abuse Act (CFAA). Explores data privacy regulations, digital evidence handling, and compliance obligations for businesses.

Unit 2: Cybercrime and Legal Consequences

Examines different types of cybercrimes, their legal implications, and law enforcement procedures. Discusses hacking, identity theft, phishing, ransomware, and insider threats. Explores legal frameworks for digital forensics, cyber investigations, and prosecution of cybercriminals.

Unit 3: Ethical Considerations in Cybersecurity

Focuses on ethics in hacking, penetration testing, and responsible disclosure of vulnerabilities. Covers ethical hacking guidelines, cyber warfare ethics, and corporate cybersecurity policies. Discusses privacy concerns in AI-driven cybersecurity and ethical dilemmas in digital surveillance.

Unit 4: Compliance and Corporate Cybersecurity Policies

Explores industry standards and best practices for cybersecurity governance. Covers ISO 27001, NIST Cybersecurity Framework, HIPAA (Health Insurance Portability and Accountability Act), and PCI DSS (Payment Card Industry Data Security Standard). Discusses corporate security policies, incident response protocols, and risk management strategies.

Recommended Books & Resources

1. "Cybersecurity Law" – Jeff Kosseff
2. "The Ethics of Cybersecurity" – Markus Christen, Bert Gordijn, Michele Loi
3. "Cybercrime and Digital Forensics: An Introduction" – Thomas J. Holt, Adam M. Bossler, Kathryn C. Seigfried-Spellar
4. GDPR, HIPAA, and ISO 27001 Compliance Guidelines (Latest Editions)

This module provides a solid legal and ethical foundation for cybersecurity professionals, enabling them to navigate complex legal landscapes and uphold ethical standards in digital security operations.

PGDMG109	International Business (replace with Cyber risk and compliance management)

Cyber Risk and Compliance Management

Course Introduction and Objectives

This module focuses on identifying, assessing, and mitigating cybersecurity risks while ensuring compliance with industry regulations and standards. It covers risk management frameworks, governance models, regulatory requirements, and compliance best practices to help organizations maintain security integrity and legal adherence.

Course Outcomes

By the end of this module, students will:

- Understand cyber risk management principles and frameworks like NIST, ISO 27001, CIS Controls, and FAIR.
- Learn to identify, assess, and mitigate cybersecurity risks using structured methodologies.
- Gain knowledge of legal and regulatory frameworks (GDPR, HIPAA, PCI-DSS, SOX, etc.).
- Explore cyber governance, risk, and compliance (GRC) models for managing organizational security posture.
- Develop skills in threat modeling, vulnerability assessments, and risk impact analysis.
- Learn to design and implement security policies, controls, and compliance programs.
- Understand audit procedures, incident reporting, and regulatory compliance audits.
- Gain hands-on experience in cyber risk assessment tools and compliance automation.

Course Content

Unit 1: Fundamentals of Cyber Risk Management

Covers cyber risk identification, classification, and assessment methodologies. Introduces risk management models, including quantitative vs. qualitative risk analysis and risk treatment options.

Unit 2: Regulatory and Compliance Frameworks

Explores major cybersecurity regulations and compliance requirements. Discusses ISO 27001, NIST CSF, PCI-DSS, GDPR, HIPAA, SOX, and other global security standards.

Unit 3: Governance, Risk, and Compliance (GRC) Implementation

Introduces GRC models and strategies for integrating risk management with business objectives. Covers compliance program development, policy creation, and security governance structures.

Unit 4: Auditing, Incident Reporting, and Compliance Monitoring

Focuses on cyber risk assessment tools, security audits, continuous monitoring strategies, and incident reporting procedures. Discusses third-party risk management and compliance automation.

Recommended Books & Resources

1. "Cybersecurity Risk Management" – Cynthia Brumfield
2. "NIST Cybersecurity Framework: A Guide for Policy Makers" – National Institute of Standards and Technology (NIST)
3. "The Security Risk Assessment Handbook" – Douglas Landoll
4. "Cybersecurity and Privacy Law Handbook" – Melissa Lukings, Richard Jochelson
5. ISO 27001 and NIST CSF Compliance Guides

This module provides a comprehensive understanding of cyber risk and compliance management, equipping students with practical skills to navigate cybersecurity governance, compliance audits, and risk mitigation strategies.

PGDMG110	Supply Chain Management (replace with Project Management for Cybersecurity)

Project Management for Cybersecurity

Course Introduction and Objectives

This module focuses on project management methodologies, frameworks, and best practices specific to cybersecurity initiatives. It covers risk management, resource allocation, budgeting, compliance, and execution of cybersecurity projects. Students will learn how to plan, implement, monitor, and close cybersecurity projects efficiently, ensuring security objectives are met while managing constraints like cost, time, and scope.

Course Outcomes

By the end of this module, students will:

- Understand project management principles and how they apply to cybersecurity.
- Learn agile, waterfall, and hybrid methodologies for cybersecurity project execution.
- Develop risk management strategies to mitigate security threats during project implementation.
- Explore budgeting, cost estimation, and resource allocation for cybersecurity projects.
- Understand compliance requirements and regulatory considerations in security project planning.
- Implement incident response and business continuity planning as part of cybersecurity projects.
- Utilize project management tools like Jira, Trello, and Microsoft Project for efficient tracking.
- Learn to manage stakeholder expectations and team collaboration in security projects.

Course Content

Unit 1: Fundamentals of Cybersecurity Project Management

Covers core project management principles, including scope, timeline, budget, and stakeholder management. Introduces cybersecurity project frameworks and governance models.

Unit 2: Risk Management and Compliance

Focuses on risk identification, assessment, and mitigation within cybersecurity projects. Covers regulatory compliance requirements (ISO 27001, NIST, GDPR, HIPAA) and legal considerations for security initiatives.

Unit 3: Execution and Monitoring of Cybersecurity Projects

Explores agile and waterfall methodologies in cybersecurity project execution. Introduces key performance indicators (KPIs), security metrics, and monitoring tools to track project progress. Discusses team collaboration and stakeholder communication strategies.

Unit 4: Incident Response and Business Continuity Planning

Covers developing and implementing cybersecurity incident response plans, including disaster recovery, business continuity, and crisis management. Explores case studies on real-world cybersecurity project failures and successes.

Recommended Books & Resources

1. "Cybersecurity Program Development for Business" – Chris Moschovitis
2. "Project Management for the Unofficial Project Manager" – Kory Kogon, Suzette Blakemore, James Wood
3. "Managing Cybersecurity Risk: Cases Studies and Solutions" – Jonathan Reuvid
4. PMBOK Guide (Project Management Body of Knowledge) – PMI (Project Management Institute)
5. ISO 27001 Implementation Guides

This module equips students with the knowledge and tools needed to manage cybersecurity projects effectively, ensuring security, compliance, and risk mitigation while delivering successful outcomes.

PGDMG111	Foreign Language- German/ French

Semester 2

PGDMG201	Entrepreneurship management Replace
PGDMG202	Strategic Management and Security Leadership)

Security Leadership and Communication – Course Introduction and Objectives

This module focuses on developing effective leadership skills, strategic decision-making, and communication techniques in the field of cybersecurity. Security leaders must align cybersecurity initiatives with business objectives, influence stakeholders, and foster a security-conscious culture within organizations. The module emphasizes crisis management, executive communication, stakeholder engagement, and security governance.

Course Outcomes

By the end of this module, students will:

- Develop leadership skills for managing cybersecurity teams and initiatives.
- Learn strategic decision-making in security risk assessment and incident response.
- Master communication techniques for technical and non-technical stakeholders.
- Understand how to build a cybersecurity-aware organizational culture.
- Gain expertise in policy advocacy, crisis management, and incident communication.
- Learn how to influence executive leadership and board-level discussions.
- Develop skills in public speaking, stakeholder engagement, and negotiation.
- Understand ethics and governance in cybersecurity leadership.

Course Content

Unit 1: Cybersecurity Leadership Principles

Explores the core attributes of security leadership, including strategic vision, decision-making, risk management, and organizational security culture development.

Unit 2: Effective Security Communication

Focuses on translating complex cybersecurity concepts into business language. Covers technical writing, executive briefings, security awareness training, and boardroom communication.

Unit 3: Crisis Management and Incident Communication

Teaches effective crisis response strategies, incident reporting frameworks, and coordinating internal and external communication during security incidents. Discusses media handling and public relations in cybersecurity crises.

Unit 4: Governance, Ethics, and Stakeholder Engagement

Covers security governance frameworks, regulatory compliance, and ethical leadership in cybersecurity. Explores stakeholder management and cross-functional collaboration.

Recommended Books & Resources

1. "Cybersecurity Leadership: Powering the Modern CISO" – Mansur Hasib
2. "Security Metrics, A Beginner's Guide" – Caroline Wong
3. "The Art of Cybersecurity Leadership" – Dan Blum
4. "Communicating the UX Vision: 13 Anti-Patterns That Block Good Security Decisions" – Martina Hodges-Schell
5. NIST Cybersecurity Leadership Guidelines

This module equips professionals with leadership and communication expertise essential for driving cybersecurity initiatives, engaging stakeholders, and managing crisis situations effectively.

PGDMG203	International Business
PGDMG204	Research Methodology
PGDMG205	Management Accounting
PGDMG206	Economic Environment for Business
PGDMG207	Corporate Communication & Cybersecurity business Communication
PGDMG208	Service Management (+ Incidence Response and service management)

Incident Response and Service Management

Course Introduction and Objectives

This module provides a comprehensive framework for handling cybersecurity incidents, minimizing damage, and ensuring quick recovery. It also covers service management best practices, including incident prioritization, escalation, and post-incident review. The course follows industry-standard frameworks such as NIST, ISO 27035, and ITIL for structured incident handling and service management.

Course Outcomes

By the end of this module, learners will:

- Understand the incident response lifecycle, from detection to recovery.
- Develop structured response plans for cybersecurity incidents.
- Learn threat intelligence techniques to proactively detect and prevent attacks.
- Master forensic investigation methods to analyze security breaches.
- Apply service management best practices for IT security operations.
- Learn the importance of communication and coordination in incident response.
- Understand compliance requirements related to incident handling.
- Gain hands-on experience in handling real-world security incidents.

Course Content

Unit 1: Fundamentals of Incident Response

- Understanding the incident response lifecycle (NIST, SANS)
- Key incident response roles and responsibilities
- Incident classification, escalation, and containment strategies

Unit 2: Threat Intelligence and Detection

- Leveraging threat intelligence for early detection
- Using SIEM (Security Information & Event Management) and log analysis
- Identifying Indicators of Compromise (IoCs)

Unit 3: Digital Forensics and Investigation

- Collecting and analyzing digital evidence

- Memory and disk forensics techniques
- Root cause analysis of cybersecurity incidents

Unit 4: Service Management and Compliance

- ITIL best practices for service management
- Incident reporting and documentation
- Compliance standards (ISO 27035, GDPR, NIST 800-61)
- Post-incident reviews and continuous improvement

Recommended Books & Resources

1. "Incident Response & Computer Forensics" – Jason T. Luttgens, Matthew Pepe
2. "The Cybersecurity Incident Management Guide" – Matthew Wallace
3. "ITIL Foundation: IT Service Management" – Axelos
4. "NIST Special Publication 800-61: Computer Security Incident Handling Guide"
5. "Cybersecurity Operations and Service Management" – John W. Rittinghouse

---

This module provides a structured approach to managing cybersecurity incidents, ensuring organizations can respond effectively, reduce impact, and improve their security posture over time.

PGDMG209	Logistics and Transportation (replace with Programming for Cybersecurity)

Programming for Cybersecurity – Course Introduction and Objectives

This course introduces students to fundamental programming concepts with a strong focus on cybersecurity applications. Students will explore essential programming languages such as Python and C, which are widely used in security-related tasks. The course covers core programming constructs, hands-on exercises, and techniques for identifying and mitigating security vulnerabilities in code. By developing and securing vulnerable applications, students will gain practical experience in both offensive and defensive programming. The curriculum also introduces students to industry-standard tools and techniques for reviewing and

securing code, equipping them with critical problem-solving skills for cybersecurity challenges.

Course Outcomes

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

- Understand the core concepts of programming and their applications in cybersecurity.
- Write programs using Python, C, and other relevant languages to perform security-related tasks.
- Apply fundamental programming constructs, including variables, loops, conditionals, and functions.
- Develop and analyze vulnerable applications to understand security flaws.
- Identify and mitigate security vulnerabilities in code through static analysis and penetration testing.
- Utilize industry-standard tools for code review, debugging, and security testing.

Course Content

Unit 1: Introduction to Programming for Cybersecurity

This unit provides an overview of fundamental programming languages used in cybersecurity, focusing on Python and C. Students will explore the significance of these languages in security-related tasks such as penetration testing, automation, and system-level programming. The unit introduces secure coding principles and best practices to ensure code reliability and protection against vulnerabilities.

Unit 2: Programming Constructs and Logic

Students will gain hands-on experience with basic programming constructs, including variables, loops, conditionals, and functions. This unit focuses on logic-building skills and debugging techniques. It also highlights the importance of secure coding practices to prevent common vulnerabilities such as buffer overflows and improper error handling.

Unit 3: Identifying and Fixing Security Vulnerabilities

This unit introduces students to common security vulnerabilities in code, such as SQL injection, command injection, and insecure authentication mechanisms. Students will analyze real-world examples of security flaws, use automated tools for static code analysis, and apply best practices for mitigating risks through secure coding techniques.

Unit 4: Developing and Securing Vulnerable Applications

Students will develop intentionally vulnerable applications to understand how attackers exploit weaknesses. By working through real-world attack vectors, they will learn how to implement security patches, use penetration testing tools, and apply secure coding methodologies to protect applications from cyber threats.

Recommended Books

1. **"Python for Cybersecurity: Using Python for Cyber Offense and Defense"** – Howard E. Poston III (2022)
2. **"The Art of Secure Software Development"** – Mark S. Merkow (2023)
3. **"Hacking APIs: Breaking Web Application Programming Interfaces"** – Corey J. Ball (2022)
4. **"Secure Coding in C and C++"** – Robert C. Seacord (2022, 2nd Edition)

This streamlined course provides a **strong foundation in programming for cybersecurity**, ensuring students develop **both offensive and defensive coding skills** essential for the field.

PGDMG210	Foreign Language - German/ French
PGDMG211	Project and viva report

Semester 3

PGDM301	**Infrastructure Security and Penetration Testing**

Infrastructure Security & Penetration Testing – Course Introduction and Objectives

This module provides an in-depth understanding of **network security principles, penetration testing methodologies, and offensive security techniques**. Students will gain hands-on experience with essential tools for **network discovery, security auditing, penetration testing, and exploitation**. The course covers **network architecture analysis, port scanning, packet manipulation, vulnerability assessment, and advanced exploitation techniques** using Metasploit and PowerShell. Additionally, students will explore **Wi-Fi security** and best practices for securing wireless networks. This module is designed to equip students with both **defensive and offensive security skills**, making them adept at securing IT infrastructures against cyber threats.

Course Outcomes

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

- Understand the principles and methodologies for securing networks and IT infrastructure.
- Use networking tools effectively for **network discovery, auditing, and penetration testing**.
- Conduct **port scanning, vulnerability assessments, and attack simulations** on network services.
- Review network architecture and recommend security improvements.
- Craft and manipulate network packets for security analysis and penetration testing.
- Perform **exploitation techniques using Metasploit** and **offensive PowerShell scripting**.
- Assess **Wi-Fi security risks** and apply best practices to secure wireless networks.

Course Content

Unit 1: Network Security Fundamentals & Tools

This unit covers the **core principles of securing networks**, including firewall configurations, access control, and encryption. Students will explore essential tools used in networking and penetration testing, such as **Nmap, Wireshark, and Netcat**, to conduct **network discovery and auditing**.

Unit 2: Penetration Testing Methodologies & Exploitation

Students will learn how to conduct **penetration testing on network services** by identifying vulnerabilities and exploiting them. Topics include **port scanning, vulnerability assessment, and attack execution**. The unit provides hands-on experience with **Metasploit**, teaching students how to craft exploits and analyze system weaknesses.

Unit 3: Advanced Network Attacks & Packet Manipulation

This unit focuses on **advanced network exploitation**, including **packet crafting, packet sniffing, and MITM (Man-in-the-Middle) attacks**. Students will use tools like **Scapy and Ettercap** to manipulate network traffic and perform security analysis.

Unit 4: Wi-Fi Security & Offensive PowerShell

The final unit explores **Wi-Fi security risks, attack vectors, and best practices**. Students will engage in **wireless penetration testing**, covering topics like **WPA/WPA2 cracking and rogue access points**. Additionally, this unit introduces **offensive PowerShell**,

demonstrating how attackers leverage scripting for security operations and how defenders can mitigate such threats.

Recommended Books

1. **"Network Security Assessment: Know Your Network"** – Chris McNab (2023)
2. **"The Art of Network Penetration Testing"** – Royce Davis (2020)
3. **"Practical Network Penetration Testing"** – Gilbert Owusu (2023)
4. **"Metasploit: The Penetration Tester's Guide"** – David Kennedy, Jim O'Gorman, Devon Kearns, and Mati Aharoni (2022, 2nd Edition)

This module provides **hands-on, real-world experience** in **infrastructure security and penetration testing**, equipping students with both **defensive and offensive cybersecurity expertise**.

PGDM302	**Web Application Security**

Web Application Security

Course Introduction and Objectives

This module provides a **comprehensive understanding of web application security threats, vulnerabilities, and secure coding practices**. Students will explore the most **critical web security risks**, including **injection attacks, authentication flaws, broken access control, and security misconfigurations**. The course emphasizes **hands-on learning**, equipping students with the skills to **identify, exploit, and remediate vulnerabilities** in web applications. By integrating **secure development practices**, **logging mechanisms**, and **security headers**, this module ensures students are prepared to defend against real-world web application attacks.

Course Outcomes

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

- Identify and analyze **common web application security threats** and their impact.
- Implement **secure coding best practices** to prevent vulnerabilities.
- Understand and mitigate **SQL, NoSQL, OS, and LDAP injection attacks**.
- Strengthen authentication mechanisms to prevent **broken authentication attacks**.

- Secure web applications against **sensitive data exposure** and improper access control.
- Detect and remediate **cross-site scripting (XSS), XML external entity (XXE), and insecure deserialization vulnerabilities**.
- Improve **logging, monitoring, and security configurations** for enhanced incident response.
- Apply **content security policies (CSP) and security headers** for additional protection.

Course Content

Unit 1: Introduction to Web Application Security

Students will explore **common web security threats**, including **the OWASP Top 10 vulnerabilities**, and understand **the significance of secure coding practices**. This unit introduces **secure web development methodologies** and the **importance of input validation and sanitization** to prevent attacks.

Unit 2: Exploiting and Mitigating Web Application Vulnerabilities

This unit focuses on **in-depth analysis of common vulnerabilities**, including **injection attacks (SQL, NoSQL, OS, and LDAP), broken authentication, sensitive data exposure, and XML external entity (XXE) attacks**. Students will **analyze real-world attack scenarios** and learn how to **apply remediation techniques**.

Unit 3: Advanced Security Risks & Secure Coding Practices

Students will investigate **advanced web security risks**, such as **insecure deserialization, broken access control, and security misconfigurations**. This unit also introduces **secure session management techniques, error handling strategies, and logging best practices** to enhance **web application resilience**.

Unit 4: Defensive Strategies & Web Security Enhancements

The final unit focuses on **security hardening techniques**, such as **applying security headers (CSP, HSTS, X-Frame-Options), managing third-party components, and implementing secure development pipelines**. Students will **conduct security assessments**, use **automated security tools**, and **apply best practices for logging, monitoring, and incident response**.

Recommended Books

1. **"The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws"** – Dafydd Stuttard & Marcus Pinto (2023, 3rd Edition)
2. **"Web Security for Developers: Real Threats, Practical Defense"** – Malcolm McDonald (2022)
3. **"Practical Web Penetration Testing"** – Joseph Muniz (2023)
4. **"OWASP Top 10 for Web Application Security"** – OWASP (Latest Edition)

This module ensures students develop **both offensive and defensive web security skills**, making them proficient in **identifying, exploiting, and mitigating security threats** in modern web applications.

PGDM303	**Mobile Application Security**

Mobile Application Security

Course Introduction and Objectives

This module provides a **detailed understanding of mobile application security**, equipping students with **essential knowledge and hands-on experience** in securing mobile applications. The course covers **threat landscapes, platform security architectures, secure coding practices, and vulnerability assessment techniques** for both **Android and iOS**. Students will explore **OWASP Mobile Top 10 vulnerabilities, secure authentication methods, cryptography, secure communication, and mobile device management**. Advanced topics include **code tampering, reverse engineering, UI-based attacks, and device exploitation**. By the end of this course, students will be able to **analyze, exploit, and secure mobile applications against sophisticated threats**.

Course Outcomes

By the end of this course, students will:

- Understand **iOS and Android security architectures** and their security models.
- Identify and mitigate **common mobile application security vulnerabilities**.
- Apply **OWASP Mobile Top 10** security principles.
- Implement **secure data storage, secure authentication, and encryption mechanisms**.
- Detect and prevent **code tampering, reverse engineering, and extraneous functionality risks**.
- Secure mobile applications against **MitM attacks, side-channel leaks, and UI-based threats**.
- Utilize **mobile device management (MDM) strategies** for enterprise security.
- Perform **comprehensive security assessments** and improve **client-side security**.

Course Content

Unit **1: Introduction to Mobile Security & Threat Landscape**

This unit provides an overview of **mobile application security threats** and the importance of securing mobile apps. Students will explore **Android and iOS security architectures**, mobile attack vectors, and secure coding best practices to **minimize security risks**.

Unit **2: OWASP Mobile Top 10 & Secure Mobile Development**

Students will study **OWASP's Mobile Top 10 vulnerabilities**, such as **improper platform usage, insecure data storage, weak authentication, insecure authorization, and cryptographic weaknesses**. Practical labs will focus on **exploiting and mitigating these vulnerabilities** through secure development practices.

Unit **3: Advanced Mobile Security Threats & Mitigation**

This unit delves into **advanced security threats**, including **code tampering, reverse engineering, and extraneous functionalities**. Students will explore **attack vectors like MitM attacks, UI-based attacks, and side-channel data leaks**. Hands-on exercises will reinforce **security controls and risk mitigation**.

Unit **4: Mobile Application Security Testing & Secure Deployment**

Students will learn **penetration testing techniques** for mobile apps, using tools like **static code analysis, dynamic testing, and reverse engineering tools**. The unit also covers **secure deployment best practices, mobile security policies, and compliance frameworks**.

Recommended Books

1. **"Android Hacker's Handbook"** – Joshua J. Drake, Zach Lanier, Collin Mulliner, Pau Oliva, Stephen A. Ridley, and Georg Wicherski (2023, Updated Edition)
2. **"iOS Application Security"** – David Thiel (2022)
3. **"The Mobile Application Hacker's Handbook"** – Dominic Chell, Tyrone Erasmus, Shaun Colley, and Ollie Whitehouse (2023, Updated Edition)
4. **"OWASP Mobile Security Testing Guide"** – OWASP (Latest Edition)

This module prepares students to **analyze, exploit, and secure mobile applications**, ensuring they gain **comprehensive expertise in mobile security testing and secure development practices**.

PGDM304	**Attack Surface Management**

Attack Surface Management – Course Introduction and Objectives

This module provides a **comprehensive understanding of Attack Surface Management (ASM)**, focusing on identifying, analyzing, and mitigating security risks across an organization's digital infrastructure. Students will learn **how attackers discover and exploit vulnerabilities** through various means such as **data breaches, credential leaks, exposed services, and misconfigured assets**. The course emphasizes **proactive security measures, continuous monitoring, threat intelligence, and vulnerability management**. Hands-on exercises and attack scenario simulations will equip students with **real-world expertise in identifying, managing, and reducing the attack surface effectively**.

Course Outcomes

By the end of this course, students will:

- Understand **attack surface fundamentals** and how digital assets contribute to security risks.
- Learn techniques for **data breach detection, credential leak prevention, and code vulnerability identification**.
- Gain hands-on experience in **domain and subdomain discovery and risk management**.
- Utilize **service discovery methods** to detect potential security exposures.
- Detect and mitigate **phishing attacks and fake applications**.
- Implement **configuration hardening** and **vulnerability management** strategies.
- Leverage **threat intelligence and continuous monitoring** for proactive attack surface defense.
- Conduct **simulated attack scenarios** to understand real-world security threats.

Course Content

Unit **1: Introduction to Attack Surface Management**

Students will explore **the fundamentals of attack surfaces**, including **how security exposures emerge in modern IT environments**. Key topics include **digital footprints, assets at risk, and the importance of proactive security measures**.

Unit **2: Identifying and Analyzing Security Exposures**

This unit covers **data breach detection techniques, credential leakage prevention, and code leaks identification**. Students will engage in **hands-on exercises to analyze and mitigate real-world security exposures**.

Unit **3: Securing Digital Assets & Reducing Attack Surface**

Students will focus on **securing domains, subdomains, and exposed services**. The module covers **service discovery techniques, phishing detection, fake application identification, and best practices for configuration hardening**.

Unit **4: Threat Intelligence, Monitoring & Attack Simulation**

The final unit emphasizes **threat intelligence integration, continuous monitoring strategies, and vulnerability management**. Students will engage in **real-world attack scenario simulations**, applying their knowledge to **detect, analyze, and mitigate attack surface threats**.

Recommended Books

1. **"The Art of Attack: Attacker Mindset for Security Professionals"** – Maxie Reynolds (2021)
2. **"Practical Cyber Intelligence: How Action-Based Intelligence Can Be an Effective Response to Incidents"** – Wilson Bautista Jr. (2020)
3. **"Threat Modeling: Designing for Security"** – Adam Shostack (2021)
4. **"The Cybersecurity Playbook: How Every Leader and Employee Can Contribute to a Culture of Security"** – Allison Cerra (2020)

This module equips students with **essential skills to proactively manage and reduce an organization's attack surface**, ensuring **better threat visibility, risk mitigation, and overall cybersecurity resilience**.

PGDM305	Internships + Project and Viva Report

Semester 4

PGDM401	**Cloud Security**

Cloud Security – Course Introduction and Objectives

Cloud Security is a critical aspect of modern cybersecurity, focusing on protecting data, applications, and infrastructures hosted in cloud environments. This module provides a **comprehensive understanding of cloud computing**, including **virtualization, deployment models, cloud service providers, security best practices, and real-world case studies**. Students will learn to **identify vulnerabilities, implement security controls, and defend against cloud-based threats**. Through **hands-on exercises and cloud hacking demonstrations**, learners will develop **practical expertise in securing cloud environments** and ensuring the confidentiality, integrity, and availability of cloud-based assets.

Course Outcomes

By the end of this course, students will:

- Understand **virtualization fundamentals** and different types of **virtualization and cloud containers**.
- Gain insights into **cloud computing models** (IaaS, PaaS, SaaS) and compare major cloud service providers (AWS, Google Cloud, Microsoft Azure).
- Learn **cloud security best practices**, including securing sensitive data and preventing document cloning.
- Explore **cloud migration strategies** and key drivers for cloud adoption.
- Analyze **real-world cloud security case studies** to understand risks and mitigation strategies.
- Participate in **hands-on cloud security exercises**, implementing security measures in cloud environments.
- Observe **cloud hacking demonstrations** to understand attack techniques and defensive strategies.

Course Content

Unit **1: Fundamentals of Cloud Computing and Virtualization**

Students will explore **the basics of cloud computing**, including **virtualization technologies, cloud computing components, and deployment models (IaaS, PaaS, SaaS)**. This unit also covers **various virtualization techniques and cloud container technologies** used in securing cloud environments.

Unit **2: Cloud Security and Risk Management**

This unit focuses on **identifying key cloud security risks, implementing security controls, and securing sensitive business data**. Students will learn about **document cloning prevention, serverless security, and best practices for securing cloud infrastructures**.

Unit **3: Threats and Vulnerabilities in Cloud Environments**

Students will analyze **real-world cloud security breaches**, learning how to **identify, assess, and mitigate cloud vulnerabilities**. The unit also includes **cloud hacking demonstrations**, providing insights into **attack techniques and defense mechanisms**.

Unit **4: Practical Cloud Security & Hands-On Exercises**

The final unit emphasizes **hands-on security implementation**, including **securing cloud storage, encrypting data, configuring security policies, and using cloud security tools**. Students will also explore **cloud migration strategies and secure cloud architecture design**.

Recommended Books

1. **"Cloud Security Handbook: A Practical Guide to Securing Cloud Environments"** – Eyal Estrin (2022)
2. **"Zero Trust and Cloud Security: Principles, Practices, and Patterns for Secure Cloud Architectures"** – Aravind Narayanan (2023)
3. **"Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance"** – Tim Mather, Subra Kumaraswamy, Shahed Latif (2022)
4. **"Practical Cloud Security: A Guide for Secure Design and Deployment"** – Chris Dotson (2021)

This module prepares students to become **proficient in cloud security**, equipping them with the skills to **secure cloud infrastructures, detect vulnerabilities, and implement advanced security measures** for cloud-based applications.

PGDM402	**DevSecOps**

DevSecOps

Course Introduction and Objectives

DevSecOps integrates security into the **software development lifecycle (SDLC)**, ensuring that security is not an afterthought but a continuous process throughout development and

deployment. This module provides an **in-depth understanding of secure coding practices, automated security testing, supply chain security, and CI/CD security**. Students will explore **policy as code, infrastructure as code (IaC), and threat modeling techniques** to enhance security posture in modern development environments. The course combines **theoretical knowledge with hands-on implementations** to equip learners with **practical DevSecOps skills for securing applications and infrastructure**.

Course Outcomes

By the end of this course, students will:

- Understand **DevSecOps principles** and the significance of embedding security into **software development and operations**.
- Implement **secure coding best practices** and **CI/CD security measures** to mitigate software vulnerabilities.
- Integrate **automated security testing** into **CI/CD pipelines** for continuous vulnerability detection.
- Apply **the Shift-Left Security approach**, emphasizing security at the early stages of development.
- Utilize **Policy as Code and Infrastructure as Code (IaC)** to automate security enforcement.
- Assess and mitigate **software supply chain risks** using **Software Composition Analysis (SCA)** tools.
- Conduct **threat modeling** and **risk assessment** to identify and mitigate security threats.
- Gain **hands-on experience** in implementing DevSecOps strategies through practical exercises.

Course Modules & Descriptions

Unit **1: Foundations of DevSecOps and Secure Software Development**

This unit introduces **DevSecOps principles**, exploring how security is integrated into the **Software Development Lifecycle (SDLC)**. Students will learn about **secure coding practices and risk mitigation strategies**.

Unit **2: CI/CD Security and Automated Testing**

Students will implement **security best practices in Continuous Integration and Continuous Deployment (CI/CD) pipelines**. The unit covers **automated security testing, vulnerability scanning, and shift-left security principles**.

Unit **3: Supply Chain Security and Infrastructure as Code (IaC)**

This unit focuses on **securing the software supply chain**, ensuring the integrity of **dependencies, third-party components, and open-source software**. Students will explore **Policy as Code and Infrastructure as Code (IaC)** for enforcing security policies automatically.

Unit **4: Threat Modeling, Risk Mitigation & Hands-On Implementations**

The final unit emphasizes **threat modeling, risk assessment, and real-world security implementations**. Students will participate in **hands-on exercises** to apply DevSecOps practices in securing applications and infrastructure.

Recommended Books

1. **"Accelerating DevSecOps: A Practical Guide"** – Sean D. Mack (2022)
2. **"Security as Code: DevSecOps Patterns for Secure Software Development"** – BK Sarthak (2023)
3. **"Practical DevSecOps: Secure Software Development with CI/CD Pipelines"** – Imran Mohammed (2022)
4. **"Cloud Native DevOps with Kubernetes"** – John Arundel & Justin Domingus (2021)

This module equips students with **practical DevSecOps expertise**, enabling them to **secure applications, automate security processes, and mitigate risks throughout the software development lifecycle**.

PGDM403	**Advanced Web Application Security**

Advanced Web Application Security – Course Introduction and Objectives

This module delves into **sophisticated attack vectors targeting modern web applications**, equipping students with the **skills to identify, exploit, and mitigate advanced security threats**. It focuses on **second-order injections, Out-of-Band (OOB) exploitations, Single Sign-On (SSO) vulnerabilities, encryption-related attacks, and emerging research-based security breaches**. Through **hands-on exercises**, students will apply cutting-edge techniques to **analyze, defend, and strengthen web applications** against evolving cyber threats.

Course Outcomes

By the end of this course, students will:

- Understand and exploit **Second-Order Injection attacks** and develop **countermeasures**.
- Identify and mitigate **Out-of-Band (OOB) vulnerabilities** leveraging **external interaction techniques**.
- Analyze and address **security issues in Single Sign-On (SSO) implementations**.
- Explore **encryption-related attacks**, including **breaking cryptographic mechanisms**.
- Learn **crypto techniques** and how attackers **bypass encryption defenses**.
- Examine **advanced, research-based application security breaches** and **emerging attack techniques**.
- Gain **hands-on experience** in **cutting-edge web application security methodologies**.

Course Content

Unit **1: Advanced Injection Techniques**

Explores **second-order injections**, their impact, and mitigation strategies. Covers **SQL, NoSQL, and OS-level injection persistence techniques**.

Unit **2: Out-of-Band (OOB) Exploitations & SSO Vulnerabilities**

Introduces **Out-of-Band attack methods**, leveraging **DNS and HTTP interactions for exploitation**. Examines **SSO security flaws and best practices for securing authentication flows**.

Unit **3: Cryptographic Attacks & Defense Strategies**

Focuses on **encryption-related vulnerabilities, crypto-breaking techniques, and cryptanalysis methodologies**. Covers **weak cipher attacks, padding oracle exploits, and real-world cryptographic breaches**.

Unit **4: Research-Based Exploits & Hands-on Attack Simulations**

Analyzes **recent, research-based application security breaches** and latest exploitation techniques. Students will conduct **practical exercises, simulated attacks, and vulnerability analysis in real-world web applications**.

Recommended Books & Resources

1. **"The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws"** – Dafydd Stuttard & Marcus Pinto
2. **"Real-World Bug Hunting: A Field Guide to Web Hacking"** – Peter Yaworski
3. **"Black Hat Python: Python Programming for Hackers and Pentesters"** – Justin Seitz
4. **OWASP Web Security Testing Guide** (Latest Version)

This module prepares students to **tackle the most advanced web security challenges**, making them proficient in **detecting, exploiting, and securing web applications from cutting-edge cyber threats**.

PGDM404	**Advanced Infrastructure Security and Penetration Testing**

Advanced Infrastructure Security and Penetration Testing – Course Overview

This module focuses on **advanced methodologies and techniques for securing IT infrastructure** and conducting **comprehensive penetration testing** to identify and mitigate vulnerabilities. Learners will gain hands-on experience in **network security, attack simulations, exploitation techniques, and defensive strategies** while using industry-standard tools such as **Metasploit, Nmap, Wireshark, Burp Suite, and PowerShell for security operations**.

Learning Outcomes

By the end of this module, learners will:

- **Understand advanced network security concepts** and their applications.
- **Perform in-depth penetration testing** on various infrastructure components.
- **Identify vulnerabilities and exploitation techniques** used by attackers.
- **Secure network services, protocols, and architectures** against threats.
- **Conduct packet analysis and traffic manipulation** for security testing.
- **Utilize offensive security tools** for ethical hacking and penetration testing.
- **Apply best practices in defensive security measures** and hardening techniques.

Course Content

Unit 1: Advanced Network Security and Threat Modeling

- **In-depth understanding of network security architectures** and defense mechanisms.
- **Network reconnaissance techniques** (active and passive) using Nmap and Wireshark.
- **Threat modeling and risk assessment** for enterprise networks.
- **Defensive strategies** against real-world cyber threats.

Unit 2: Infrastructure Penetration Testing Techniques

- **Advanced port scanning and network mapping** using automated tools.
- **Exploit development and vulnerability assessment** in enterprise environments.
- **Manipulating network packets** for testing security controls.
- **Attacking network services** and common infrastructure vulnerabilities.

Unit 3: Red Teaming & Offensive Security

- **Metasploit Framework for advanced exploitation** and privilege escalation.
- **PowerShell for penetration testing** and post-exploitation techniques.
- **Bypassing firewalls and intrusion detection systems (IDS/IPS).**
- **Simulating real-world attack scenarios** using adversary emulation tactics.

Unit 4: Defensive Strategies & Secure Network Hardening

- **Incident detection and response** to infrastructure attacks.
- **Mitigating vulnerabilities** with security patches and configuration hardening.
- **Best practices for securing cloud, hybrid, and on-premises infrastructures.**
- **Hands-on case studies** with penetration testing reports and remediation plans.

Recommended Books & Resources

1. **"The Art of Network Penetration Testing"** – Royce Davis
2. **"Metasploit: The Penetration Tester's Guide"** – David Kennedy
3. **"Practical Network Security"** – Allan Liska
4. **"Hands-On Penetration Testing with Python"** – Furqan Khan
5. **"Offensive Security Certified Professional (OSCP) Study Guide"**

This module provides **advanced practical skills in infrastructure security and penetration testing**, preparing professionals for **real-world cybersecurity challenges** in enterprise environments.

PGDM405	Internships + Project and Viva Report