ST JOSEPH'S UNIVERSITY BANGALORE

A Public –Private-Partnership University under RUSA 2.0 of MHRD(Government of India), established by the Karnataka Govt. Act No. 24 of 2021

SCHOOL OF INFORMATION TECHNOLOGY

DEPARTMENT OF ADVANCED COMPUTING

SYLLABUS FOR

POSTGRADUATE DIPLOMA

IN

AI ENHANCED CYBER SECURITY

PROGRAM OVERVIEW

This postgraduate diploma bridges the gap between traditional offensive/defensive security and the emerging paradigm of Artificial Intelligence. It moves beyond static defense mechanisms to explore predictive threat intelligence, automated incident response, and adversarial machine learning.

SUMMARY OF CREDITS

SEM	Code	Title	Hrs/Week	Total Hrs	Credits	Max. Marks
I	PGACS 1126	Introduction to Ethical Hacking and AI Security	3	45	3	50
I	PGACS 1226	Intelligent Scanning and Penetration Techniques	3	45	3	50
I	PGACS 1326	Report Writing and Predictive Mitigation	3	45	3	50
I	PGACS 1426	Governance, Risk, Compliance and AI Regulations	3	45	3	50
I	PGACS 1P126	AI and Cyber Security Lab	2	30	1	25
I	PGACS 1P226	Mini Project	4	60	2	25
II	PGACS 2P126	Internship / Capstone Project	50	800	25	50
Total					**40**	

SYLLABUS DETAILS

Semester	I
Paper Code	PGDCS 1126
Paper Title	INTRODUCTION TO ETHICAL HACKING AND AI SECURITY
Number of teaching hrs per week	3 Hrs
Total number of teaching hrs per semester	45
Number of credits	3

UNIT I: INTRODUCTION TO ETHICAL HACKING AND AI (5 hrs)

Core ethics principles, privacy and consent, legal boundaries, responsible data handling, real-world dilemmas, professional codes of conduct, standards of responsible disclosure and data evidence handling using open-source privacy checklists (Secure Privacy Checklist).

UNIT II: INTRODUCTION TO ETHICAL HACKING AND AI (17 hrs)

Ethical Hacking concepts and essential terminology including the impact of Artificial Intelligence on modern security. Different phases involved in an exploit by a Hacker and the role of AI in accelerating the cyber kill chain. Overview of Attacks and Identification of Exploit Categories, including specific AI-driven threats like Deepfakes, synthetic media, and automated social engineering via LLM vulnerability scanners (Garak). Legal implications of Hacking, AI ethics, Law, and Punishment.

UNIT III: ETHICAL HACKING PHASES AND ADVERSARIAL TACTICS (18 hrs)

Essential terms like Hacker, Hacking, Cracker, Ethical Hacker, Threat, Vulnerability, Target of Evaluation, Attacks, and Exploits. Introduction to Adversarial Machine Learning and how attackers use data poisoning to deceive security systems. Elements of Security and how Hacking impacts these elements in an AI-driven landscape using the (IBM Adversarial Robustness Toolbox) for defense.

SELF STUDY (5 hrs)

SUGGESTED BOOK:

1. Krutz, Ronald L., & Vines, Russell Dean. The CEH Prep Guide: The Comprehensive Guide to Certified Ethical Hacking. Wiley Publications, 2007.
2. Chio, C., Freeman, D. (2018). Machine Learning and Security: Protecting Systems with Data and

Algorithms. O'Reilly Media.
3. Vorobeychik, Y., & Kantarcioglu, M. (2018). Adversarial Machine Learning. Morgan and Claypool Publishers.

Semester	I
Paper Code	PGDCS 1226
Paper Title	INTELLIGENT SCANNING AND PENETRATION TECHNIQUES
Number of teaching hrs per week	3 Hrs
Total number of teaching hrs per semester	45
Number of credits	3

UNIT I: SCANNING & ENUMERATION (19 hrs)

Scanning as a part of the pre-attack phase. Use of dialers, port scanners, network mapping, sweeping, and vulnerability scanners, with a focus on reducing false positives through automated verification. Usage of Open-source tools like OpenVAS, Recon-ng, Nmap with NSE AI scripts for scanning and behavioral profiling to detect anomalies beyond static signatures.

UNIT II: PENETRATION TECHNIQUES AND TOOLS (20 hrs)

Gaining Access phase of the attack including how the attack occurs using both manual techniques and AI-driven password cracking tools. Maintaining access phase where the hacker tries to retain ownership of the system using obfuscated malware. Techniques & tools used by hackers to maintain access. Covering tracks Phase of the hacking activity including removal of evidence and defeating AI-based forensic analysis using PentestGPT - Community Edition & Wazuh.

SELF STUDY (6 hrs)

SUGGESTED BOOK:

1. Seitz, J., & Arnold, T. (2021). Black Hat Python: Python Programming for Hackers and Pentesters (2nd Edition). No Starch Press.
2. Saxe, J., & Sanders, H. (2018). Malware Data Science: Attack Detection and Attribution. No Starch Press.

Semester	I
Paper Code	PGDCS 1326
Paper Title	REPORT WRITING AND PREDICTIVE MITIGATION
Number of teaching hrs per week	3 Hrs
Total number of teaching hrs per semester	45
Number of credits	3

UNIT I: REPORT WRITING AND MITIGATION (22 hrs)

Introduction to Report Writing & Mitigation, requirements for low level reporting & high-level reporting of Penetration testing results. Utilization of Large Language Models (LLMs) for assisting in executive summary generation and automated documentation (ChatGPT & Google Gemini Flash).

UNIT II: DEMONSTRATION OF VULNERABILITIES AND MITIGATION (17 hrs)

Demonstration of vulnerabilities and Mitigation of issues identified including tracking. Introduction to predictive mitigation strategies and Security Orchestration, Automation, and Response (SOAR) concepts to streamline defense mechanisms (Shuffle SOAR).

SELF STUDY (6 hrs)

SUGGESTED BOOK:

1. Roberts, S. J., & Brown, R. (2023). Intelligence-Driven Incident Response: Outwitting the Adversary (2nd Edition). O'Reilly Media.

Semester	I
Paper Code	PGDCS 1426
Paper Title	GOVERNANCE, RISK, COMPLIANCE & AI REGULATIONS
Number of teaching hrs per week	3 Hrs
Total number of teaching hrs per semester	45
Number of credits	3

UNIT I: GOVERNANCE RISK AND COMPLIANCE (19 hrs)

Introduction to GRC. Detailed explanations along with case studies. Designing IT policies, Security policies, procedures, and systems. Governance of "Shadow AI" and developing policies for the ethical and secure use of Generative AI within the enterprise (NIST AI RMF Playbook).

UNIT II: COMPLIANCE AND CERTIFICATIONS TYPES (20 hrs)

All compliance and certifications like ISO 27001:2013, PCI-DSS, SOC 2 Type 2, GDPR, Sox, Fisma, HIPAA, ITIL, COBIT. Overview of emerging AI-specific frameworks including the NIST AI Risk Management Framework (AI RMF) and the EU AI Act (LLM Guard & Hugging Face).

SELF STUDY (6 hrs)

SUGGESTED BOOK:

1. Ammanath, Beena. Trustworthy AI: Implementing Trust and Managing Risk. Wiley Publications, 2022.
2. Kumar, Ram Shankar Siva, & Anderson, Hyrum. Not with a Bug, But with a Sticker: Attacks on Machine Learning Systems. Wiley Publications, 2019.

Semester	I
Paper Code	PGDCS 1P126
Paper Title	AI & CYBER SECURITY LAB
Number of teaching hrs per week	3 Hrs
Total number of teaching hrs per semester	45
Number of credits	3

List of Lab Experiments using Python, ChatGPT, OpenVAS, Wazuh, Scikit-learn.

1. Internal Network scanning using Lan Scanner tool
2. External Network scanning using Superscan tool
3. Data Enumeration by Nmap
4. Port and Service Enumeration
5. Privilege escalation attack
6. Internal vulnerability assessment and External vulnerability assessment
7. Website vulnerability assessment
8. SQL injection attack and Cross Site Scripting attack
9. Phishing Detection using Machine Learning
10. Automated Vulnerability Scanning and Report Generation.