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

ST. JOSEPH’S INSTITUTE OF INFORMATION TECHNOLOGY

DEPARTMENT OF ADVANCED COMPUTING

SYLLABUS FOR POSTGRADUATE DIPLOMA IN CYBER SECURITY

SUMMARY OF CREDITS IN PG DIPLOMA IN CYBER SECURITY

Total hrs in the semester	Credit	Number of hrs per week	Title	Code number
Semester -I				
45	3	3	Introduction to Ethical Hacking	PGDCS 1123
45	3	3	Scanning, Enumeration and Penetration Techniques	PGDCS 1223
45	3	3	Report Writing and Mitigation	PGDCS 1323
45	3	3	Governance Risk and Compliance	PGDCS 1423
PRACTICALS				
30	1	2	Cyber Security Lab	PGDCS1P1
60	2	4	Mini Project	PGDCS1P2
Total Credits 15				
Semester –II				
800	25	50	Internship/project	PGDCS2P1
Total Credits for the course 40				

SYLLABUS DETAILS

CODE NUMBER: PGDCS 1123
TITLE OF THE PAPER : INTRODUCTION TO ETHICAL HACKING

UNIT I: INTRODUCTION TO ETHICAL HACKING (19 hrs)

Ethical Hacking concepts and essential terminology. Different phases involved in an exploit by a Hacker. Overview of Attacks and Identification of Exploit Categories. Legal implications of Hacking. Hacking, Law and Punishment

UNIT II: ETHICAL HACKING PHASES (20 hrs)

Essential terms like Hacker, Hacking, Cracker, Ethical Hacker, Threat, Vulnerability, Target of Evaluation, Attacks and Exploits. Elements of Security and how Hacking impacts these elements.

SELF STUDY (6 hrs)

SUGGESTED BOOK:

No specific book

CODE NUMBER: PGDCS 1223

TITLE OF THE PAPER :SCANNING, ENUMERATION AND PENETRATION TECHNIQUES

UNIT I: SCANNING & ENUMERATION (19 hrs)

Scanning as a part of the pre-attack phase. Use of dialers, port scanners, network mapping, sweeping, vulnerability scanners etc. Usage of Open source tools for scanning. Gaining Access phase of the attack including how the attack occurs

UNIT II: PENETRATION TECHNIQUES AND TOOLS (20 hrs)

Maintaining access phase where the hacker tries to retain ownership of the system. Techniques & tools used by hackers to maintain access. Covering tracks Phase of the hacking activity including removal of evidence of hacking to avoid forensics & legal action.

SELF STUDY (6 hrs)

SUGGESTED BOOK:

No specific book

CODE NUMBER: PGDCS 1323

TITLE OF THE PAPER : REPORT WRITING AND MITIGATION

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.

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

Demonstration of vulnerabilities and Mitigation of issues identified including tracking

SELF STUDY (6 hrs)

SUGGESTED BOOK:

No specific book

CODE NUMBER : PGDCS 1423
TITLE OF THE PAPER : GOVERNANCE RISK AND COMPLIANCE

UNIT I: GOVERNANCE RISK AND COMPLIANCE (19 hrs)
Introduction to GRC. Detailed explanations along with case studies. Designing IT policies, Security policies, procedures, systems.

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

SELF STUDY (6 hrs)

SUGGESTED BOOK:

- The CEH Prep Guide: The Comprehensive Guide to Certified Ethical Hacking, by Ronald L. Krutz (Author), Russell Dean Vines, Wiley Publications

LABORATORY

CODE NUMBER: PGDCS1P1

TITLE OF THE PAPER: CYBER SECURITY LAB

List of Lab Experiments:

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
7. External vulnerability assessment
8. Website vulnerability assessment
9. SQL injection attack
10. Cross Site Scripting attack

11. Web exploitation:

- HTTP basics
- The protocol
- Verbs
- Error codes
- Cookie security
- Session fixation
- Cross-site request forgery
- Same Origin Policy
- Cross domain Request Policy
- Enumerating Comments
- Cross-site scripting
- Reflected
- Stored
- DOM
- Detection, exploitation, and mitigation
- Clickjacking
- Directory traversal
- Authorization bypasses and forced browsing
- Command injection
- SQL injection
- Detection, exploitation, and mitigation
- Exploiting blind SQL
- Insecure Direct Object Reference
- Secure password storage
- File inclusion vulnerabilities
- File upload vulnerabilities
- Null termination vulnerabilities
- Unchecked redirects

- Server-side request forgery
- Server Side Includes
- HTTP Parameter pollution