SEMESTER S6

FUNDAMENTALS OF CYBER SECURITY

Course Code	PBCST604	CIE Marks	60
Teaching Hours/Week (L: T:P: R)	3:0:0:1	ESE Marks	40
Credits	4	Exam Hours	2 Hrs 30 Min.
Prerequisites (if any)	None	Course Type	Theory

Course Objectives:

1. To teach the security terminologies along with familiarization of web-based attacks and the vulnerability assessment tools for real time practices
2. To help learners to perform network analysis and learns the measures to handle security bleaches at the system level

SYLLABUS

Module No.	Syllabus Description	Contact Hours
1	**Information Security** Introduction, Threats to Information Systems, Cyber Security and Security risk analysis, Information Gathering- Reconnaissance, Reco-ng, Software Vulnerabilities- Buffer Overflow, Stack Overflow, Format String, Vulnerability Assessment and Penetration Testing- Burpsuite, Metasploit.	10
2	**Web Security** Web Attacks- SQL Injection Attacks, Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF), Domain Name System- Security Issues with DNS, DNS attacks, DNSSEC, OWASP ZAP, WebGoat, Damn Vulnerable Web Application (DVWA), Website Mirroring, HTTRACK, Email Security- Email risks, Protocols, Operating safely when using email.	12
3	**Network Security:** Network Security Terminologies, DoS, DDoS, ARP Spoofing and Session	12

	Hijacking, Capturing the Network Traffic- Promiscuous Mode, Flooding, DHCP Redirection, Redirection and Interception with ICMP. Port Scanning- TCP and UDP, Port Scanning Tools- Nmap, SuperScan, Wireshark- Analysing and Filtering Traffic	
4	**System Security:** Windows Security: Attacks against windows system, Installing applications, Authentication and access control, Upgrades and Patches, Operating Windows safely, Windows Defender Firewall. Linux Security- Attacks in Linux system, Physical security, Controlling the configuration, Authentication and access control, Upgrades and Patches, Operating Linux safely, SELinux.	**10**

Suggestion on Project Topics

Network Traffic Monitoring and Analysis using Wireshark:

- Development: Capture network traffic in a controlled environment using Wireshark.
- Security Analysis & Fixing: Analyze captured traffic to identify potential vulnerabilities (e.g., plaintext passwords) and recommend security enhancements.

OWASP ZAP (Zed Attack Proxy) Security Testing Framework:

- Development: Create a web application with some common vulnerabilities.
- Security Analysis & Fixing: Use OWASP ZAP to perform security testing on the application, identify vulnerabilities, and then fix these issues by implementing secure coding practices.

Web Application Vulnerability Identification Using Burp Suite:

- Development: Develop a simple web application with common security flaws, such as SQL injection, XSS, and broken authentication mechanisms.
- Security Analysis & Fixing: Use Burp Suite to scan the application, identify vulnerabilities, and analyze the attack surface. Afterward, secure the application by fixing these vulnerabilities and re-running the scan to verify the fixes.

Penetration Testing Framework Using Metasploit:

- Development: Set up a vulnerable virtual environment using tools like Metasploitable or create your own vulnerable system or network services.
- Security Analysis & Fixing: Use Metasploit to exploit the system, demonstrate various attacks like privilege escalation, and then apply patches, configuration changes, and security best practices to mitigate the discovered vulnerabilities.

Course Assessment Method

(CIE: 60 marks, ESE: 40 marks)

Continuous Internal Evaluation Marks (CIE):

Attendance	Project	Internal Ex-1	Internal Ex-2	Total
5	30	12.5	12.5	60

End Semester Examination Marks (ESE)

In Part A, all questions need to be answered and in Part B, each student can choose any one full question out of two questions

Part A	Part B	Total
• 2 Questions from each module. • Total of 8 Questions, each carrying 2 marks **(8x2 =16 marks)**	2 questions will be given from each module, out of which 1 question should be answered. Each question can have a maximum of 2 subdivisions. Each question carries 6 marks. **(4x6 = 24 marks)**	**40**

Course Outcomes (COs)

At the end of the course students should be able to:

Course Outcome		Bloom's Knowledge Level (KL)
CO1	Use assessment tools for vulnerability testing	**K3**
CO2	Use various security tools to study web based attacks	**K3**
CO3	Identify the network based attacks using network monitoring tools	**K3**
CO4	Illustrate the system security measures used for windows and Linux operating systems	**K2**

Note*: K1- Remember, K2- Understand, K3- Apply, K4- Analyse, K5- Evaluate, K6- Create*

CO-PO Mapping Table:

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

Text Books				
Sl. No	**Title of the Book**	**Name of the Author/s**	**Name of the Publisher**	**Edition and Year**
1	Build Your Own Security Lab	Michael Gregg	Wiley	1/e, 2008
2	Network security and Cryptography	B. Menezes	Cengage	1/e, 2010
3	Shellcoder's Handbook: Discovering and Exploiting Security Holes	Chris Anley, John Heasman, Felix Lindner, Gerardo Richarte	Wiley	2/e,2007
4	Network Security Bible	Eric Cole, Ronald Krutz, James W Conley	Wiley	1/e, 2010

Reference Books				
Sl. No	**Title of the Book**	**Name of the Author/s**	**Name of the Publisher**	**Edition and Year**
1	Cryptography and Network Security	Behrouz A Forouzan	Tata McGraw-Hill.	3/e,2015
2	The Complete Reference: Information Security	Mark Rhodes-Ousley	McGraw-Hill	2/e,2012

Video Links (NPTEL, SWAYAM…)	
Module No.	**Link ID**
1	https://onlinecourses.nptel.ac.in/noc23_cs127/preview
2	https://onlinecourses.nptel.ac.in/noc24_cs85/preview
3	https://onlinecourses.swayam2.ac.in/nou19_cs08/preview
4	

PBL Course Elements

L: Lecture (3 Hrs.)	**R: Project (1 Hr.), 2 Faculty Members**		
	Tutorial	**Practical**	**Presentation**
Lecture delivery	Project identification	Simulation/ Laboratory Work/ Workshops	Presentation (Progress and Final Presentations)
Group discussion	Project Analysis	Data Collection	Evaluation
Question answer Sessions/ Brainstorming Sessions	Analytical thinking and self-learning	Testing	Project Milestone Reviews, Feedback, Project reformation (If required)
Guest Speakers (Industry Experts)	Case Study/ Field Survey Report	Prototyping	Poster Presentation/ Video Presentation: Students present their results in a 2 to 5 minutes video

Assessment and Evaluation for Project Activity

Sl. No	Evaluation for	Allotted Marks
1	Project Planning and Proposal	5
2	Contribution in Progress Presentations and Question Answer Sessions	4
3	Involvement in the project work and Team Work	3
4	Execution and Implementation	10
5	Final Presentations	5
6	Project Quality, Innovation and Creativity	3
Total		**30**

1. **Project Planning and Proposal (5 Marks)**

    - Clarity and feasibility of the project plan
    - Research and background understanding
    - Defined objectives and methodology

2. **Contribution in Progress Presentation and Question Answer Sessions (4 Marks)**

    - Individual contribution to the presentation
    - Effectiveness in answering questions and handling feedback

3. **Involvement in the Project Work and Team Work (3 Marks)**

    - Active participation and individual contribution
    - Teamwork and collaboration

4. **Execution and Implementation (10 Marks)**

    - Adherence to the project timeline and milestones
    - Application of theoretical knowledge and problem-solving
    - Final Result

5. **Final Presentation (5 Marks)**

    - Quality and clarity of the overall presentation
    - Individual contribution to the presentation
    - Effectiveness in answering questions

6. **Project Quality, Innovation, and Creativity (3 Marks)**

    - Overall quality and technical excellence of the project
    - Innovation and originality in the project

Creativity in solutions and approaches