1	**Dates**	• 8,9,11,12,14,15,16,17,19,21,22,23,24,25,26,28 April 2025
2	**End Module Assessment**	9-May-2025
3	**Lab Assessment**	Before 9-May-2025
4	**Evaluation Details**	**T - Theory** **L - Lab** **A - Assignments / Mid module Evaluations**

Centre for Development of Advanced Computing Software Training and Development Centre (Kochi & Thiruvananthapuram)					
PG - DCSF Feb 2025					
WEEK	**MODULE NAME**	**DURATION** (120 Hours)			**EVALUATION DETAILS**
		THEORY	**LAB**	**REVISION**	
	Pentesting and Incident Response	56 Hours	60 Hours	4 Hours	60 Marks (20 T + 20 L + 20 A)
SCHEDULE					
Date	Theory Session (09:30 AM to 01: 00 PM)		Lab Session (02:00 PM to 06:00 PM)		

	Session 1:
	Topic: Penetration Testing Process
	
	Lecture:
	• Pre-engagement
	  ○ Rules of Engagement
	  ○ Liabilities and Responsibilities
	• Methodologies
	  ○ PTES
	  ○ OWASP Testing Guide
	• Reporting
	  ○ What do clients want?
	  ○ Report Structure
	  ○ Report templates and guides
		• Discussion about latest cyber attacks like Ransomware etc
		• Analysis of sample pentesting reports	

	Session 2: **Topic: OSINT** **Lecture:** • OSINT process - Setting Up an OSINT Platform, Sock Puppets, Data Analysis, • Core OSINT Skills - Leveraging Search Engines, Harvesting Web Data, File Metadata Analysis, Reverse Image Searching, Image Analysis • People investigations – email addresses, usernames, address and phone numbers, image searching, people search engines, social media, geo locations • Website, Domain and IP investigations -	• Conduct professional OSINT investigations to obtain information about a person or company	

	Website Investigations ○ Understanding how to use third-party data to explore website content ○ Active discovery of website data ○ Analysis of the infrastructure that runs a website ○ WHOIS - What is WHOIS and how can WHOIS data be used in OSINT work? ○ DNS- What is DNS and how can understanding DNS records help OSINT investigations? ○ IP Addresses - How to research and geolocate IP addresses ○ Discovering and analyzing Internet-facing hosts ○ Wireless OSINT		
	Session 3: **Topic** : **Social Engineering Penetration Testing** **Lecture** • Social Engineering Attacks • Social Engineering Test • Methods Used To Perform Social Engineering Attacks • Steps To Performing A Social Engineering	• Familiarizing social engineering attacks • Tools – SET, Sherlock, OSINT	

	Penetration Test – ○ Step 1: Test Planning And Scoping ○ Step 2: Attack Vector Identification ○ Step 3: Penetration Attempts ○ Step 4: Reporting Lab		
	Session 4: **Topic : Network Penetration Testing** **Lecture** • Network Penetration Test • Benefits Of Performing A Network Penetration Test • Steps In Network Penetration Testing ○ Step 1: Information Gathering And Client Expectations ○ Step 2: Reconnaissance And Discovery ○ Step 3: Performing The Network Penetration Test ○ Step 4: Reporting, Recommendations, And Remediation Analysis	Tools - Nessus, Nmap, NetCat, Hydra, Wireshark, Nikto, Metasploit, PRET, Burpsuite	
	Session 5&6: **Topic: Introduction to Web Applications** **Lecture:** • HTTP/S Protocol Basics • Encoding • Same Origin • Cookies • Sessions • Web Application Proxies	• Analyze cookie,session details by intercepting requests using Burp Proxy	

	Session 7:
	Topic: Reconnaissance and Enumeration for Pen Testers
	
	Lecture:
	• Passive Information Gathering
	• Active Information Gathering
	  ○ NMAP
	  ○ Port Scanning
	  ○ Enumeration
	• Scanning and Vulnerability Enumeration
	• Fingerprinting the web server
	• Enumerating subdomains
	• Crawling the website
	• Finding hidden file
		• Gather information using Whois
		• Find target ISP
		• Fingerprint the Webserver using Netcat, WhatWeb
		• Explore Burp target crawler	

	Session 8:
	Topic: Cross-Site Scripting
	Lecture:
	• Basics
	• Anatomy of an XSS Exploitation
	• The three types of XSS
	• Finding XSS
	• XSS Exploitation
	• Mitigation techniques
	  ○ Input Validation
	  ○ Context-Aware Output Encoding
	  ○ Never trust user input
		• Access Cookie, LocalStorage
		• Remove Alerts,Script
		• Regular Expression Filtering
		• XSS on HTML Entities
		• Heartbleed Exploitation
		• Insecure Deserialization
		• Reflected and Persistent XSS Attacks
		• DOM-Based XSS Attacks
		• Spidering and Forced Browsing
		• File Inclusion
		• HTML Injection	

	Session 9 & 10: **Topic: Authentication and Authorization**	• Analyze Single-factor, Two-	

	Lecture: • Authentication vs. Authorization • Authentication factors • Credentials over unencrypted channel • Inadequate password policy • User enumeration • Default or easily-guessable user accounts • The remember me functionality • Password reset feature • Logout weaknesses • Insecure direct object references • Missing function level access control • Parameter modification • Incorrect redirection • SessionID prediction	factor authentications in various applications • Crack the passwords using Dictionary/Brute force attacks • Analyze cache data in browser • Analyze cookies	
	Session 11: **Topic: Session Security** **Lecture:** • Weaknesses of the session identifier • Session hijacking • Session Fixation • Cross-Site Request Forgeries	• Exploit session hijacking • Prevent session hijacking • Session Hijacking via Packet sniffing	
	Session 12: **Topic: File and Resource Attacks, Clickjacking** **Lecture:** • Path conversion • Encoding • Best defensive techniques • Local File Inclusion (LFI) • Remote File Inclusion (RFI) • Unrestricted File Upload • Clickjacking	• Upload a vulnerable file to server • Defend the file upload based on file content • Analyze web page to check the possibility of Clickjacking	

	• Using HTTP header X-Frame-Options • Feasibility study on possibility of Clickjacking • HTTP Response Splitting		

	Session 13:
	Topic: Web Services
	
	Lecture:
	• Introduction
	• Web Services Implementations
	  ○ XML-RPC
	  ○ JSON-RPC
	  ○ SOAP
	  ○ RESTful
	• The WSDL Language
	  ○ Interaction between client and server
	  ○ Objects in the WSDL
	  ○ SOAP in action
	• Attacks
	  ○ WSDL Disclosure
	  ○ WSDL Scanning
	  ○ SOAPAction Spoofing
	  ○ SQLi through SOAP messages
		•	

	Session 14 & 15: **Topic: Penetration Testing on MYSQL** **Lecture:** • Introduction to MySQL-Server • DML,DDL,DCL queries • Penetration testing on MySQL	• Scan for MySQL database and connect • MySQL Brute-Force Attack • Run SQL queries without Login into Mysql • Extract Mysql-Schemadump Information • Extracting Login from	

		Mysql-server • Explore Writable Directories • Enumerate File • Port Transferring	

	Session 16 & 17 & 18:
	Topic: Incident Handling and Response Process
	
	Lecture:
	• Events and Incidents
	• Need for Incident Response
	• Incident Response Policy,Plan and Procedure
	• NIST Incident Response Framework
	• CERT-in
	• Incident Response Process Methodology: The OODA Loop
	• Incident Response Team Structure
	  ○ Team Models
	  ○ Team Model Selection
	  ○ IR Personnel
	  ○ Dependencies within Organizations
	  ○ IR Team Services
	• 6 Phases in the Incident Response Plan and Handling an Incident
	  ○ Preparation
	  ○ Detection and Analysis
	  ○ Containment,Eradication and Recovery
	  ○ Post-Incident Activity
	• Incident Handling Checklist
	• Incident Response Myth Busting for Executives
	• Information Sharing Techniques
		• Discuss about Incidents Handling Scenarios, Incident-Related Data Elements	

	Session 19:
	Topic: Handling and Responding to Web Application Security Incidents
	
	Lecture:
	• Web Fundamentals and Secure Configuration
	  ○ How Do Web Applications Work?
	  ○ Why are web applications so vulnerable to attacks?
	• Web Application Attacks
	• Front-End Security
	• APIs and Microservices
	• DevSecOps and Defending the Flag
		• Scan the web applications using website security scanners and find out vulnerabilities.
		• HTTP traffic inspection and spoofing, SSRF and credential-stealing, SQL Injection, Cross Site Request Forgery, Cross Site Scripting, Authentication vulnerabilities and defense, Multifactor authentication, Session vulnerabilities and testing, Authorization vulnerabilities and defense, SSL vulnerabilities, WSDL enumerations, Front End Features and CSP (Content Security Policy), Clickjacking, Deserialization and DNS rebinding, GraphQL, API gateways and JSON, SRI and Log review	

	Session 20: **Topic: Handling and Responding to Insider Threats** **Lecture:** • Insider Threats • Anatomy of an Insider Attack • Insider Risk Matrix • Insider Threats Detection and Response Plan • Guidelines for Detecting and Preventing Insider Threats	• Employee Monitoring Tools - Activity Monitor, Net Spy Pro, Spector Pro, SpyAgent, Handy Keylogger, Anti Keylogger, Actual Spy, SpyBuddy, SoftActivity Keylogger, Elite Keylogger, Spy Sweeper	
	Session 21: **Topic: Information Security Management** **Lecture:** • Information Security Management Standards like ISO/IEC 27001		