Course Code	Course Title	L	T	P	C
OLMCA623	Penetration Testing	3	1	0	4
Pre-requisite	NIL	Syllabus Version			
		1.0			

Course Objectives

1. Understand penetration testing methodologies for identifying vulnerabilities.
2. Develop skills to plan, execute, and manage security assessments.
3. Learn attack techniques, defenses, and reporting best practices.

Course Outcomes

On successful completion of this course, the student will be able to:

1. Explain the fundamentals of penetration testing, its phases, strategies, and the role of red and purple teaming operations.
2. Develop, schedule, and coordinate penetration tests by setting test goals, following IEEE standards, and preparing detailed test deliverables.
3. Perform tasks such as firewall testing, password cracking, social engineering, and exploit vulnerabilities in Linux and Windows systems.
4. Apply sniffing, SQL injection, ARP poisoning, and session hijacking, and understand countermeasures for these attacks.
5. Generate comprehensive penetration testing reports, prioritize actionable insights, develop remediation plans, and apply best practices for security improvement.

Module:1 Introduction to Info Sec& Pen Testing

Need of InfoSec - CIA Triad - Incident Response – Threats – Phishing - Dark web. Pen Testing: Introduction - Testing Techniques - Process -Types, Strategies- Operational strategies for security testing - Identifying benefits - Prioritizing the systems - Phases of penetration testing – Popular PenTest tools.

Module:2 Business of Hacking

Pen Tester Ethos - Taxonomy-The Future of Hacking- Know the Tech-Pen Tester Training - Knowledge Transfer- Pen Tester Tradecraft -Personal Liability-Being the Trusted Advisor-Managing a Pen Test. Teaming operations: Red and purple - objectives and operations.

Module:3 PenTest Plan & Bug Bounty Programs

Duties of a Licensed Penetration Tester - Penetration Testing Planning and Scheduling : Purpose, Building a Plan, Setting Up a Test Goal, IEEE Standards, Test-Plan Identifier, Test Deliverables, Penetration Test Planning Phases.
Bug Bounty Programs : Types – Incentives -Controversy -Popular Bug Bounty Program Facilitators

Module:4 Exploiting Systems

Introduction to Pre–Penetration Testing: Checklist, Pre-penetration Testing Steps, , Firewall penetration testing - social engineering penetration testing - Password cracking penetration testing. Exploitation: Getting shells without exploit-capturing password hashes –Using Winexe and WMI – Basic Linux and Windows Exploits.

Module:5 Sniffing

Sniffers & SQL Injection Active and passive sniffing- ARP Poisoning- Session Hijacking- DNS Spoofing- Conduct SQL Injection attack – Counter measures. Cracking techniques - Key loggers - Escalating privileges- Hiding Files- Steganography technologies- Countermeasures.

Module:6	**Post PenTest**			
External Penetration Testing: Internal Testing, Steps for Conducting External Penetration Testing, Recommendations for Internal Network Penetration Testing.				
Module:7	**Reporting**			
Penetration Testing Report, Summary of Test Execution, Results and Analysis -Post Actions: Prioritize Recommendations, Develop an Action Plan, Process creation, Apply Updates and Patches, Capture Lessons Learned and Best Practices, Create Security Policies, Conduct Training, Conduct a Social Engineering Class, Destroy the Penetration Testing Report.				
	Total Hours of Study:			**120 hours**
Text Book(s)				
1.	Gray Hat Hacking, “The Ethical Hackers Handbook, Allen Harper, Stephen Sims, Michael Baucom, 5th Edition, Tata McGraw-Hill, 2020.			
2.	Phillip L. Wylie, Kim Crawley, “The Pentester BluePrint: Starting a Career as an Ethical Hacker”, 2020, Wiley, United States.			
3.	Sabih, Zaid, “Learn Ethical Hacking from Scratch: Your stepping stone to penetration testing”, 2018 Packt Publishing Ltd, United Kingdom.			
Reference Books				
1.	Mike Chapple , “CompTIA PenTest+Study Guide” Sybex, 2nd Edition, 2021.			
2.	"The Penetration Testing Procedures and Methodologies", EC-Council, Cengage Learning, 2010.			
Mode of Evaluation: CAT, Digital assignments, Quiz, and FAT				
Recommended by Board of Studies		28-10-2024		
Approved by Academic Council		No. 76	Date	28-11-2024