



Pentesting Master Program (PTMP v2)



AI-Integrated
360° Pentesting



Microsoft 365
Integrated



Industry
Aligned



The Problem With Learning Pentesting Today



Learn Skills, Not Engagements

Learners often master tools and individual techniques through labs, but rarely experience how those skills fit into a structured, end-to-end pentest methodology.



Practice Without Professional Context

Most learning environments don't expose learners to scope, authorization, Rules of Engagement, client communication, evidence collection and professional reporting as part of the actual testing process.



Knowledge Without the Complete Picture

Learning is often divided into isolated domains or certification objectives, making it difficult to connect network, web, API, cloud, AD and other security skills into one complete assessment.



You may know how to exploit a vulnerability. But do you know how to conduct a professional penetration test from **start to finish**?



From Learning Pentesting to Understanding Complete Engagements

The Pentesting Master Program (PTMP v2) is designed to bridge the gap between learning individual security techniques and understanding how professional penetration testing engagements are planned, executed, documented, and delivered.



360° Pentesting Learning

Explore multiple security domains through a structured learning pathway, from foundations and core methodology to specialized testing areas.



Engagement-Oriented Practice

Understand scope, authorization, Rules of Engagement, testing workflows, evidence handling, and professional reporting.



Industry-Aligned Workflows

Build familiarity with the documentation, collaboration, and communication practices used in professional environments.



AI-Integrated Learning

Explore how AI can support pentesting workflows while developing the judgment needed to validate results and make informed decisions.

Multi Domain Pentesting

Build a broader understanding of how security weaknesses are discovered, validated, and assessed across different technology environments.

PTMP v2 introduces learners to multiple pentesting domains through a structured learning pathway, helping them connect individual techniques with the wider security assessment process.

Infrastructure & Enterprise Security

Network Penetration Testing, Active Directory Penetration Testing, Cloud & Container Security Testing

Application Security

Web Application Penetration Testing, API Penetration Testing, Mobile Application Security Testing, Source Code Review & Thick Client Testing

360°

Specialized & Embedded Security

Database Penetration Testing, Wireless & RF Security Testing, IoT & Firmware Security Testing

AI & Emerging Technologies Security

LLM/AI Application Penetration Testing



AI-Integrated Pentesting



AI-Assisted Reconnaissance

Explore how AI can help organize reconnaissance findings and identify areas for further investigation.



Scripting & Automation

Use AI assistance to understand scripts, automate repetitive tasks, and improve workflow efficiency.



Vulnerability Analysis

Support the analysis of potential weaknesses, technical findings, and remediation approaches.



LLM & AI Application Security

Explore security testing concepts relevant to applications powered by large language models and other AI systems.



Report Writing & Documentation

Use AI assistance to organize findings, improve clarity, and structure technical documentation, while validating every claim.

Microsoft 365 Integrated Learning Environment

PTMP v2 integrates Microsoft 365 into the learning experience, providing a structured digital workspace for technical assignments, documentation, collaboration, and professional communication.

From executing hands-on pentesting exercises to documenting findings and presenting reports, learners develop professional workflows that extend beyond the lab and prepare them for the corporate world, where Microsoft 365 is widely used for everyday collaboration and business operations.



Professional Identity
Email and communication



Structured Learning
Resources, notes, & tasks



Collaboration
Meetings & interactions



Professional Workflow
Technical Reports

According to LAND BASE, Top companies using Microsoft 365:



Industry-Aligned Learning

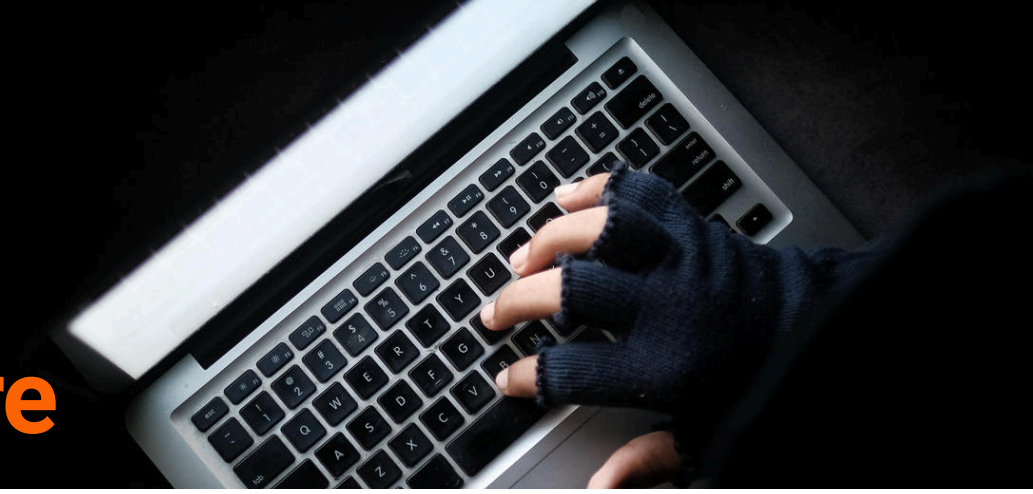
Corporate penetration testing is more than finding vulnerabilities. It requires a structured methodology, verifiable evidence, risk-based prioritization, and professional reporting.

PTMP v2 integrates relevant industry-recognized methodologies, frameworks, standards, and technical guidelines across its learning modules. This helps learners understand not only how to perform security tests, but also how to approach assessments in a structured and professionally responsible manner.

PTMP v2 MODULES ALIGN WITH:



Learning Architecture



01

FOUNDATIONS

Build essential technical knowledge



02

CORE PENTESTING WORKFLOW

Learn the end-to-end methodology



03

MULTI-DOMAIN PENTESTING

Explore different technology environments



04

ADVANCED & EMERGING PRACTICES

Explore AI and advanced security concepts



05

PROFESSIONAL PRACTICE & CAPSTONE

Bring the learning together

PTMP v2 Syllabus

1 FOUNDATIONS

Build the technical knowledge and practical skills required for penetration testing.

- » **Module 1:** Cybersecurity, Pentest Methodologies, Law & Lab Setup
- » **Module 2:** Networking Fundamentals for Security Professionals
- » **Module 3:** Linux for Pentesting
- » **Module 4:** Windows Internals & PowerShell for Pentesters
- » **Module 5:** Scripting & Automation for Pentesters

Tools Highlights:



2 CORE PENTEST WORKFLOW

Master the end-to-end methodology used to conduct structured penetration tests.

- » **Module 6:** Information Gathering & OSINT
- » **Module 7:** Scanning & Enumeration
- » **Module 8:** Vulnerability Assessment & Risk Rating
- » **Module 9:** Exploitation & Initial Access
- » **Module 10:** Privilege Escalation & Lateral Movement
- » **Module 11:** Post-Exploitation & Evidence Collection

» **Module 12:** Reporting Foundations

Tools Highlights:



3 **TARGET DOMAINS**

Apply core pentesting methodology across diverse technologies and attack surfaces.

- » **Module 13:** Network Penetration Testing
- » **Module 14:** Active Directory Penetration Testing
- » **Module 15:** Web Application Penetration Testing
- » **Module 16:** API Penetration Testing
- » **Module 17:** Database Penetration Testing
- » **Module 18:** Cloud & Container Security Testing
- » **Module 19:** Mobile Application Security Testing
- » **Module 20:** Wireless & RF Security Testing
- » **Module 21:** IoT & Firmware Security Testing
- » **Module 22:** Source Code Review & Thick Client Testing

Tools Highlights:



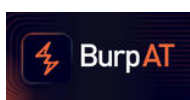
4

EMERGING TECH & HUMAN LAYER

Explore AI, LLM security and human-centric attack surfaces.

- » **Module 23:** AI-Augmented Pentesting Workflows
- » **Module 24:** LLM / AI Application Penetration Testing
- » **Module 25:** Social Engineering & Human-Layer Security

Tools Highlights:



many
more

5

Professional Practice & Capstone

Experience how real-world security engagements are planned, executed and delivered.

- » **Module 26:** Red Team Operations: C2 & Evasion
- » **Module 27:** Purple Teaming, Detection & Compliance
- » **Module 28:** Advanced Reporting & Client Communication
- » **Module 29:** VDP & Bug Bounty
- » **Module 30:** Final Capstone: Full-Scope Penetration Test

Tools Highlights:



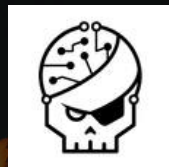
many
more

Beyond the Lab

CTF & Bug Bounty Aligned Learning

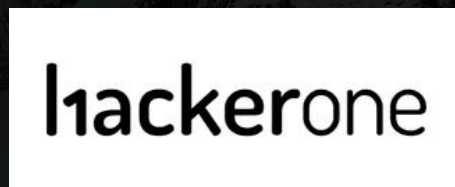
01 / Capture The Flag (CTF)

Apply your knowledge through structured security challenges that strengthen technical reasoning, investigative thinking, and hands-on problem-solving.



02 / Bug Bounty & VDP

Understand how security researchers identify, validate, document, and responsibly disclose vulnerabilities in real-world applications.



Career Support



Technical skills are just one part of getting hired. PTMP supports your career journey with practical guidance to help you present your skills, prepare for interviews, and navigate the cybersecurity job market.



Resume Building:

Build an ATS-friendly resume highlighting your skills, projects, and practical experience.



LinkedIn Optimization:

Enhance your LinkedIn profile to improve professional visibility and networking.



Job Search Strategy:

Learn to identify suitable roles, find opportunities, and plan effective job applications.



Mock Interviews:

Practice technical and HR interviews with feedback to improve your confidence and performance.

Certificate of Completion



CERTIFICATE

OF COMPLETION

This Certificate is given to :

PARTICIPANT NAME

for successfully completing the **Pentesting Master Program (PTMP V2)**.
Demonstrating commitment to practical learning in penetration testing, security assessment, and professional reporting.



COMPLETION DATE
[DD MMM YYYY]



CERTIFICATE ID
[PTMP2-XXXX]

sign

AUTHORIZED SIGNATORY
[Name & Signature]



Program Highlights

Program	Pentesting Master Program v2 (PTMP v2)
Offered By	Certifence Technologies Pvt. Ltd.
Duration	3 Months 85 hrs
Delivery	Online Live Weekdays 09-11 PM IST
Coverage	10+ Pentesting Domains
Projects	20+ Real-World Projects
Tools	100+ Cybersecurity Tools
AI Integration	AI-assisted Penetration Testing
Microsoft 365	MS 365 Integrated Learning Environment
Alignment	PTES, NIST, OWASP, MITRE, CIS, & More



NEXT
COHORT

FROM 19th OCT
09 - 11 PM IST

Cohort Details



19th OCT 2026
(3 Months)



09 - 11 PM IST
(Weekdays)



5,999 INR
(Incl. all taxes)

Eligibility Criteria:

Applicants must meet at least ONE of the following eligibility pathways:

- **Academic Pathway:** Candidates pursuing or holding a bachelor's degree or equivalent qualification in Computer Science, Information Technology, Cybersecurity, or a related discipline.
- **Professional Pathway:** IT or cybersecurity professionals with at least 2 years of relevant professional experience.
- **PTMP Progression Pathway:** Successful graduates of CERTIFENCE PTMP Specialist.

Admission Process



Apply

Fill out and submit the PTMP v2 Admission Form.



Review & Selection

Our admission panel reviews your application and evaluates your eligibility.



Offer & Onboarding

Selected candidates receive an Offer Letter and proceed with enrollment and program onboarding.



**Start Your
Application Now**

For Any Support



+91 8878843350
+91 8800124987

~~—We Teach Penetration Testing—~~

We Teach Real World Penetration Testing



www.certifence.com



info@certifence.com



+91 8800124987