SYLLABUS FOR BOARD OF STUDIES ADOPTION — generated from the live catalogue record

Ethical Hacking and Penetration Testing

S-05A · 5 days (configurable 1–5 days) · Informatics · Security · Years: 3rd, PG

CONTENTS

1. Overview 2
2. Hours and credit position 2
3. Course outcomes 2
4. Course content — modules 2
5. Assessment scheme (100 marks) 3
6. CO–PO mapping 3
7. Every participant receives 3
8. Fee 3
9. Designed by 3

Catalogue S-05A · version 2 · generated 2026-10-11

OVERVIEW

Reconnaissance, scanning, exploitation and reporting against a deliberately vulnerable lab environment.

Cybersecurity roles far outnumber qualified candidates; hands-on penetration testing against an authorised lab, with professional reporting, gives students a demonstrable security skill set.

HOURS AND CREDIT POSITION

Contact hours: 40 Guided project: 20 Self-study: 0 Notional total: 60

Credit claim: 2
60 notional hours ÷ 30 hours per credit (NSQF track, UGC Micro-credentials Guidelines §5.3.3) = 2 credits.

COURSE OUTCOMES

CO1. Describe the phases of a penetration test and the rules of engagement (K2)
CO2. Perform reconnaissance and scanning against an authorised lab target (K3)
CO3. Identify and exploit common vulnerability classes in a lab environment (K3)
CO4. Test a web application against the OWASP Top 10 (K3)
CO5. Produce a professional penetration-test report with remediation advice (K5)

COURSE CONTENT — MODULES

Hours shown are the recommended format; module time scales proportionally when the engagement runs 1–5 days.

Module 1 — Security foundations and ethics (5h recommended)
Theory: The CIA triad, legal scope, rules of engagement, authorisation
Lab: Draft rules of engagement for a lab test
Output: Rules-of-engagement document

Module 2 — Reconnaissance (5h recommended)
Theory: Passive and active information gathering
Lab: Gather information on an authorised lab target
Output: Reconnaissance notes

Module 3 — Scanning and enumeration (5h recommended)
Theory: Port scanning, service enumeration, vulnerability scanning
Lab: Scan and enumerate the lab target
Output: Scan report

Module 4 — Exploitation basics (5h recommended)
Theory: Common vulnerability classes, using an exploitation framework in the lab
Lab: Exploit a known vulnerability in the lab
Output: Exploitation log

Module 5 — Web application testing (5h recommended)
Theory: The OWASP Top 10, injection, broken access control
Lab: Test a lab web application against the OWASP Top 10
Output: Web-test findings

Module 6 — Post-exploitation and privilege escalation (5h recommended)
Theory: Within the authorised lab: privilege escalation, persistence concepts
Lab: Escalate privileges on the lab host
Output: Post-exploitation notes

Module 7 — Network and wireless testing (5h recommended)
Theory: Within the authorised lab: network and wireless assessment
Lab: Assess the lab network
Output: Network findings

Module 8 — Reporting capstone (5h recommended)
Theory: Professional reporting, risk rating, remediation advice
Lab: Write a professional penetration-test report
Output: Penetration-test report

ASSESSMENT SCHEME (100 MARKS)

Continuous lab exercises — 40 marks
Capstone project & demonstration — 40 marks
Quiz & viva voce — 20 marks

CO–PO MAPPING

CO1 !’ PO6 (strength 2)
Scope, authorisation and ethics are the professional responsibility of the role.

CO2 !’ PO4 (strength 2)
Reconnaissance and scanning are structured investigation.

CO3 !’ PO4 (strength 2)
Finding and confirming vulnerabilities is investigation.

CO4 !’ PO5 (strength 2)
Web testing uses the profession's modern tools.

CO5 !’ PO10 (strength 2)
The report is the professional communication deliverable.

EVERY PARTICIPANT RECEIVES

- Certificate of completion
- Course material
- LMS access
- Interview question bank
- Mock interview & viva practice
- Optional nasscom NSQF assessment (priced per candidate on your quotation)

FEE

¹1,500 per student, incl. GST
Excludes the optional nasscom assessment where offered. Final pricing on your college's quotation.

DESIGNED BY

Venkat Kurela — Founder & Director, Kurela Cognisive Private Limited