

Ethical Hacking & Penetration Testing

Learn ethical hacking through authorised, hands-on penetration testing of networks, web apps and APIs with professional reporting.



8 weeks

DURATION

81 hours

GUIDED LEARNING

2 projects

PORTFOLIO

ABOUT THE ACADEMY

Practical learning. Work you can demonstrate.

Brightnest AI Academy brings live instruction, guided practice and career preparation together for individuals and teams.

23

FOCUSED COURSES

6

FLAGSHIP PROGRAMMES

Noida

ACADEMY LOCATION

Our approach

1

Learn

Understand concepts through live instruction and current examples.

2

Build

Apply learning through labs, assignments and guided projects.

3

Explain

Document decisions, results, trade-offs and limitations.

4

Prepare

Connect completed work with CVs, interviews and workplace conversations.

PEOPLE BEHIND THE ACADEMY

Meet Ranjeet Kumar



ACADEMY ADVISER

Ranjeet Kumar

Innovation & Growth Leader

15+ years

Experience in data, artificial intelligence and machine learning leadership.

Areas of expertise

- Data science and machine learning solution leadership
- AI product strategy and scalable data platforms
- Technology team leadership and mentorship
- Practical AI and data adoption for business transformation

Education

Master of Information Systems, Anna University, Chennai
Bachelor of Computer Science Engineering

COURSE OVERVIEW

Build your next set of skills

Assess vulnerabilities and conduct authorised penetration testing using professional methodologies. Progress from Ethics, Scope and Penetration Testing Methodology to Penetration Testing Capstone through guided labs, assessed projects, and portfolio evidence.

Who this is for

Security learners and practitioners developing authorised offensive-security skills.

Before you begin

Learners should understand networking, Linux/Windows, and cybersecurity fundamentals. All lab testing is conducted only in authorised environments.

Ethical hacking requires explicit authorisation, controlled methodology, reproducible evidence, risk-based reporting, and verified remediation-not indiscriminate tool use.

LEARNING OUTCOMES

What you will be able to do

01

Create a professional rules-of-engagement and test plan for an authorised lab target.

02

Map the attack surface of a deliberately vulnerable lab environment.

03

Enumerate hosts/services and validate high-priority findings without destructive actions.

04

Exploit safe intentionally vulnerable hosts in a controlled lab and document remediation.

05

Test a deliberately vulnerable web app, reproduce issues and recommend fixes.

06

Complete an end-to-end exploit-to-remediation validation workflow in a lab.

07

Conduct a full authorised penetration test against a multi-service lab and present findings to a mock client.



CURRICULUM

Course curriculum

8 modules · 8 weeks · 81 hours of guided learning

01 Ethics, Scope and Penetration Testing Methodology

5 hours

TOPICS

Authorisation · Rules of engagement · Scope · Evidence · Reporting · Attack lifecycle · Legal/ethical boundaries · Lab safety

PRACTICAL WORK

Create a professional rules-of-engagement and test plan for an authorised lab target.

Tools: Kali Linux lab, Documentation templates

Assessment: Scope review

Portfolio evidence: Pen-test engagement plan

02 Reconnaissance and Attack Surface Mapping

8 hours

TOPICS

Passive/active recon · DNS · Subdomains · Technology fingerprinting · Exposed services · Metadata · OSINT principles · Asset inventory

PRACTICAL WORK

Map the attack surface of a deliberately vulnerable lab environment.

Tools: Nmap, Amass/Subfinder concepts, Browser tools

Assessment: Recon lab

Portfolio evidence: Attack-surface map



CURRICULUM

Course curriculum

8 modules · 8 weeks · 81 hours of guided learning

03 Scanning, Enumeration and Vulnerability Validation

10 hours

TOPICS

Port/service discovery · Version detection · Enumeration · Vulnerability scanning · False positives · Manual validation · Prioritization

PRACTICAL WORK

Enumerate hosts/services and validate high-priority findings without destructive actions.

Tools: Nmap, Lab vulnerability scanner

Assessment: Technical lab

Portfolio evidence: Validated vulnerability report

04 Network and Host Exploitation Concepts

10 hours

TOPICS

Authentication weaknesses · Insecure services · Misconfiguration · Privilege escalation concepts · Lateral movement concepts · Credential hygiene · Post-exploitation boundaries

PRACTICAL WORK

Exploit safe intentionally vulnerable hosts in a controlled lab and document remediation.

Tools: Metasploitable/HTB-style lab, Linux/Windows VMs

Assessment: Lab practical

Portfolio evidence: Host exploitation case report

CURRICULUM

Course curriculum

8 modules · 8 weeks · 81 hours of guided learning

05 Web Application Security and OWASP Risks

12 hours

TOPICS

HTTP · Sessions · Input validation · Injection · XSS · Access control · SSRF concepts · File handling · Business logic · Secure coding remediation

PRACTICAL WORK

Test a deliberately vulnerable web app, reproduce issues and recommend fixes.

Tools: Burp Suite Community/OWASP ZAP, Vulnerable web lab

Assessment: Web pentest report

Portfolio evidence: Web security findings portfolio

06 Authentication, API and Cloud-Native Attack Surface

10 hours

TOPICS

JWT/OAuth concepts · API authorisation · Rate limits · IDOR/BOLA · Secrets · Container/cloud misconfig concepts · API testing methodology

PRACTICAL WORK

Assess a vulnerable REST API for authorisation and input-validation issues.

Tools: Burp/ZAP, Postman/curl, API lab

Assessment: API security lab

Portfolio evidence: API penetration test report



CURRICULUM

Course curriculum

8 modules · 8 weeks · 81 hours of guided learning

07 Exploitation Workflow, Evidence and Remediation

8 hours

TOPICS

Exploit selection · Safe proof-of-concept · Shell hygiene · Data minimisation · Evidence capture · Cleanup · Risk rating · Remediation verification

PRACTICAL WORK

Complete an end-to-end exploit-to-remediation validation workflow in a lab.

Tools: Kali, Lab targets, Reporting tools

Assessment: Practical checkpoint

Portfolio evidence: Evidence-backed remediation package

08 Penetration Testing Capstone

18 hours

TOPICS

Scope · Recon · Enumeration · Web/API/network testing · Evidence · Risk rating · Executive summary · Technical remediation · Retest

PRACTICAL WORK

Conduct a full authorised penetration test against a multi-service lab and present findings to a mock client.

Tools: Kali, Nmap, Burp/ZAP, Lab environment

Assessment: Capstone report and presentation

Portfolio evidence: Professional penetration testing report

APPLIED PORTFOLIO

Projects you will build

Two portfolio projects supported by guided module work.

PORTFOLIO PROJECT 1

Authorised Multi-Service Penetration Test

Test a vulnerable network/web/API lab and produce a client-style report.

DELIVERABLES

Rules of engagement · Evidence · Findings · Remediation · Retest results

PORTFOLIO PROJECT 2

Web and API Security Assessment

Assess authentication, authorisation and input-handling weaknesses in a vulnerable application.

DELIVERABLES

Burp/ZAP evidence · Risk ratings · Developer remediation guidance

LEARNING EXPERIENCE

Learn, practise and present

- Live instructor-led sessions that connect concepts to real workplace decisions.
- Guided labs and workshops in every module.
- Assignments, checkpoints and practical feedback.
- Portfolio documentation, demonstrations and capstone review.
- Access to recordings and LMS resources according to the published batch policy.
- Career preparation based on completed work and target roles.

Tools you will work with

Kali Linux lab · Documentation templates · Nmap · Amass · Subfinder concepts · Browser tools · Lab vulnerability scanner · Metasploitable · HTB-style lab · Linux · Windows VMs · Burp Suite Community · OWASP ZAP · Vulnerable web lab · Burp · ZAP

CAREER PREPARATION

Build confidence for interviews

A structured process to connect your learning with your next career step.

01**Role clarity**

Identify roles that fit your background, interests and current skills.

02**Profile readiness**

Review your CV, LinkedIn, GitHub and project summaries.

03**Project proof**

Prepare to demonstrate completed work and explain your decisions.

04**Interview practice**

Practise technical questions, project walkthroughs and interviews.

05**Opportunity updates**

Receive relevant job openings and employer requirements, subject to availability and learner readiness.

Career support helps you prepare. Employment outcomes depend on experience, project quality, interview readiness and market conditions.

LEARNER JOURNEYS

Companies where our learners have been hired

Across the Brightnest AI Academy learner community



Learner employment history across the academy; not a placement guarantee for this course. Names and logos identify employers; they do not imply endorsement or a hiring partnership.

BEFORE YOU ENROL

Your questions, answered

Is the Ethical Hacking & Penetration Testing course suitable for beginners?

This course progresses from intermediate to advanced level. Learners should understand networking, Linux/Windows, and cybersecurity fundamentals. All lab testing is conducted only in authorised environments.

What will I build during the course?

You will complete guided labs in every module and build two portfolio projects: Authorised Multi-Service Penetration Test and Web and API Security Assessment. Deliverables include working files or code, documentation, testing or evaluation evidence, and a final presentation.

Which tools and platforms are covered?

Key tools include Kali Linux lab, documentation templates, Nmap, Amass, Subfinder concepts, browser tools, lab vulnerability scanner, and Metasploitable. Additional platforms are introduced in relevant modules through practical tasks, and the toolset may evolve as industry practice changes.

How long does the course take?

The course includes approximately 81 guided learning hours across 8 modules, delivered over 8 weeks.

Which career paths can this course support?

The curriculum supports the development of skills relevant to roles such as Penetration Tester, Ethical Hacker, and Vulnerability Assessment Analyst. Career outcomes depend on prior experience, project quality, interview readiness and market conditions; employment is not guaranteed.

BEFORE YOU ENROL

Your questions, continued

Will I receive mentor and career support?

The course includes live instruction, lab support, assignment feedback, project reviews and career preparation covering portfolio development, CV writing, LinkedIn profile improvement, and interview guidance.

FEES & ADMISSIONS

Plan your next step

COURSE FEE

INR 35,000 + GST

EMI and easy instalments available

Duration	8 weeks
Level	Intermediate-Advanced
Learning format	Live mentor-led learning
Batch starts	Expected Saturday / Sunday starts

Check the live Batches page for the next expected weekend. Confirm the exact date, class times and availability with admissions.

Book a free demo class >

+91 73030 11395

brightnestaiacademy.com/batches

A-56, Sector-64, Noida, Uttar Pradesh - 201301