BlueGuardia

Penetration Testing Bootcamp

14-Week Practitioner Programme · Online · Theory + Hands-On Labs

14	100%	Kali
WEEKS	ONLINE	HANDS-ON
Full Programme	Flexible Timing	Real Attack Labs

// THE OPPORTUNITY

Why Penetration Testing?

Every organisation is a target. Demand for skilled ethical hackers who can find vulnerabilities before real attackers do has never been higher — and it keeps growing.

> *"Offense informs defense.*
> *You cannot protect what you do not understand."*
>
> — Practitioner Principle

$130K

Avg. senior pentest salary (US)

Glassdoor 2024

3.5M

Unfilled cybersecurity roles

ISC2 2024

+35%

Growth in ethical hacking demand

BLS 2024

92%

Firms reported breaches last year

IBM Report 2024

ABOUT US

Forging Cyber Attackers

BlueGuardia is a cybersecurity training institute built by practitioners. Our mission: produce job-ready Penetration Testers and SOC Analysts through hands-on, real-world training — then grow into a full Managed Security Service Provider.

// OUR LONG GAME

From training institute to full-service MSSP.

- Penetration Testing across web, mobile & network
- 24/7 managed SOC services with detection engineering
- Vulnerability Assessment & AI Pen Testing
- OT Security Operations & GRC / Compliance

Practitioner-Built

Trainers are active pentesters — not academics.

Real Lab Environment

Kali Linux, real targets, real tools — not slides.

Job-Ready Outcomes

Resume, LinkedIn & interview prep built into the programme.

14 Weeks to Penetration Tester

Weeks 1–4
SECTION 1

Foundation & Theory

- Org context & cybersecurity landscape
- OS & networking fundamentals
- Cybersecurity concepts, CIA Triad, AAA
- Attack types, malware, phishing

Online · Flexible Scheduling

Weeks 5–12
SECTION 2

Core Pentesting Labs

- OWASP Top 10:2025 deep dive
- Recon · Scanning · Exploitation
- Post-Exploitation & Reporting
- Capstone: Full Pentest Simulation

Kali Linux Lab Environment

Weeks 13–14
SECTION 3

Job-Ready Profile

- LinkedIn profile optimisation
- Job-ready resume preparation
- Interview Q&A coaching
- Industry expert sessions

Active Pentesters as Trainers

// PENTESTER

Penetration Tester

Penetration Testers are the offensive force of cybersecurity. They think like attackers, probe for weaknesses, exploit them ethically, and report findings to harden defences.

Junior Pentester
Learning & tool-based testing

Mid-Level Pentester
Independent tester, full engagements

Senior / Lead
Leads engagements, reviews work

Red Team Lead
Adversary simulation & advanced attacks

Skills You Will Build

Reconnaissance

OSINT · Google Dorking · DNS enum · subdomain discovery

Scanning & Enumeration

Nmap · Nikto · Gobuster · ffuf · service fingerprinting

OWASP Top 10:2025

XSS · SQL Injection · IDOR · SSRF · Access Control flaws

Exploitation

Metasploit · OWASP ZAP · BeEF · SQLMap · command injection

Post-Exploitation

Privilege escalation · persistence · lateral movement · pivoting

Pentest Reporting

PoC evidence · risk rating · executive & technical reporting

What You Will Learn

Week 1

Basic Knowledge

- Org structure & cybersecurity roles
- Market trends
- Hardware & Internet basics

Week 2

Cyber Fundamentals

- CIA Triad · AAA · Attack types
- Malware · Phishing · Social Engineering
- Encryption & Hashing

Weeks 3–4

OS & Networking

- Windows & Linux basics · CLI
- TCP/IP · OSI · Subnetting
- Protocols · Firewalls · VPNs

Week 5

Pentest Intro

- What is penetration testing?
- Career paths & terminologies
- Kali Linux setup & CLI basics

Weeks 5–12

OWASP & Phases

- OWASP Top 10:2025
- Recon · Scanning · Exploitation
- Post-Exploitation & Reporting

Weeks 5–12 · LABS

- Vulnerability Assessment
- Web App Exploitation
- Post-Exploitation
- Capstone Pentest Sim
- Pentest Report Writing

Your Pentesting Arsenal

Reconnaissance

- Nmap · Nessus · Nikto
- Gobuster · ffuf · Dirb
- Sublist3r · Amass · dig
- Google Dorking · Hunter.io

Web App Testing

- OWASP ZAP · Burp Suite
- SQLMap · BeEF
- tplmap · jwt_tool
- Param Miner · Turbo Intruder

Exploitation

- Metasploit Framework
- Hydra · Medusa
- Authorize · Intruder
- Custom payloads & shells

Post-Exploitation

- Privilege escalation scripts
- Credential harvesting
- Persistence mechanisms
- Reverse & bind shells

Scanning & VA

- Nessus · OpenVAS
- OWASP ZAP · AppScan
- W3af · WebInspect
- SQLMap · RIPS

Reporting

- Documentation & PoC
- Risk rating framework
- Executive summaries
- Technical write-ups

// ADDITIONAL PERKS

More Than Just a Course

Capstone CTF Simulation
Full pentest on a lab environment — all phases

Completion Certificate
Recognised credential for your portfolio

LinkedIn Optimisation
Profile review & recruiter-ready guidance

Interview Preparation
Common questions bank + mock sessions

Industry Expert Sessions
Live Q&A with active pentesters

// WHAT YOU WALK OUT WITH

Your Outcomes

- Solid foundation in cybersecurity fundamentals
- Hands-on experience with real pentest tools
- OWASP Top 10:2025 exploitation skills
- Full pentest lifecycle: Recon → Report
- Professional LinkedIn profile for recruiters
- Interview preparation & common question bank
- Certificate of completion
- Access to a community of practitioners

Train the Talent.

Build the Firm.

Defend the Industry.

Join Cadre 1 and launch your career as a Penetration Tester. Limited seats. Real tools. Real outcomes.

Apply Now → blueguardia.com

blueguardia.com