



EDUBLENDS

Fuel Your Future.

Fuel your **Future**

Dive into Edublends Academy's world of opportunities with industry internships, specialized training, and globally recognized certifications



Track 6: Cyber Security Assistant → Ethical Hacker

Basic to Advanced · 270 Hours Total

At EduBlends, we don't just train—we create future industry leaders!

Program Summary

A progression from supervised monitoring to full-scope offensive assessment — Linux and IDS foundations through to VAPT and forensics.



Program Duration

270 hours across 3 levels
(approx. 20 weeks)



Weekly effort

12-15 hours a week



Learning Mode: Online and Offline
Classes, including Pre-Recorded
Videos, Live Sessions, and Interactive
Q&A Sessions.



Cyber Range & Cloud Lab access
with isolated attack and defence
environments



**Industry-Sponsored Internship
Facilitation**



Certificate Upon successful
completion of each level, participants
will be awarded a verified digital
certificate by EduBlends and Industry

A Progressive Learning Pathway Aligned to Your Graduation

At EduBlends Academy, we provide a structured learning pathway that allows students to build cybersecurity expertise across their graduation journey, with each level mapped to a semester window and a defined exit role.

1. **Basic Level (Sem 3) — Cyber Security Assistant:** Linux administration, IDS/IPS monitoring and traffic inspection. Exit role: Junior SOC Analyst.
2. **Intermediate Level (Sem 5) — Junior Cyber Security Associate:** Reconnaissance, web testing and forensic evidence collection. Exit role: Security Analyst L1.
3. **Advanced Level (Sem 6–7) — Ethical Hacking & Forensics:** Full-scope offensive assessment across networks, applications and endpoints. Exit role: Penetration Tester (VAPT).

By following this structured pathway, students complete the full track within their graduation period, emerging as industry-ready professionals with a portfolio of evidenced, lab-based security work.

Track 6 – Cyber Security Assistant → Ethical Hacker

Basic → Advanced · 270 hours total · 30 practical lab sessions and a panel-assessed capstone

Program Levels

Level	Title	Semester	Hours	Focus
Basic	Cyber Security Assistant	Sem 3	90 hrs	Linux administration, IDS/IPS monitoring and traffic inspection
Intermediate	Junior Cyber Security Associate	Sem 5	90 hrs	Reconnaissance, web testing and forensic evidence collection
Advanced	Ethical Hacking & Forensics	Sem 6–7	90 hrs	Full-scope offensive assessment across networks, applications and endpoints

Target Roles

Level	Semester	Role
Basic	Sem 3	Junior SOC Analyst — foundational awareness through hands-on Linux, IDS/IPS monitoring and traffic inspection
Intermediate	Sem 5	Security Analyst L1 — triaging alerts, conducting first-line investigations, and supporting senior analysts
Advanced	Sem 6–7	Penetration Tester (VAPT) — full-scope offensive assessments across networks, applications, and endpoints

Certification Alignment

Level	Certifications
Basic — Cyber Security Assistant	Microsoft SC-900 Security Fundamentals · Google Professional Cloud Security Engineer · Microsoft SC-200 · IBM Cybersecurity Analyst Professional · AWS Certified Security – Specialty
Intermediate — Junior Cyber Security Associate	CompTIA Security+ · Google Professional Cloud Security Engineer
Advanced — Ethical Hacking & Forensics	EC-Council CEH · EC-Council CHFI · Offensive Security OSCP · CompTIA CySA+

Vendor certification examinations are sat separately and are not included in programme fees. Preparation coverage is indicative and does not guarantee an examination pass.

Top Recruiters

TCS · Cognizant · Genpact · HCLTech

Recruiter names indicate the employers and sectors our graduates target; they do not constitute a placement guarantee or a formal hiring partnership.

Entry Requirements

The Basic level is open entry; no prior programming or security experience is assumed. The Intermediate level requires completion of the Basic level or equivalent networking and Linux competence. The Advanced level requires completion of the Intermediate level or demonstrable hands-on security experience.

Program Frameworks – Basic Level: Cyber Security Assistant

Sem 3 • 90 hours • Linux administration, IDS/IPS monitoring and traffic inspection • 10 practical lab sessions

M1 | Security Fundamentals & Threat Landscape 18 hrs

Module / Topic

- CIA triad, threat actors and motivations, attack lifecycle, security controls, governance basics

Practical Lab Sessions

Lab 1: Map a documented breach to the attack lifecycle and identify control failures.

Lab 2: Build a control matrix for a small organisation

M2 | Linux Administration for Security 22 hrs

Module / Topic

- Command line, filesystem and permissions, users and groups, services, package management, logging and auditing

Practical Lab Sessions

Lab 3: Build and harden a Linux host; configure auditing and log forwarding.

Lab 4: Investigate a simulated compromise using system logs alone

M3 | Network Traffic Inspection with Wireshark 20 hrs

Module / Topic

- Capture strategy, display filters, protocol decoding, session reconstruction, spotting anomalies

Practical Lab Sessions

Lab 5: Capture and decode traffic across four protocols in a live lab.

Lab 6: Identify malicious activity in a provided capture and evidence it

M4 | IDS/IPS Monitoring & Alert Handling 18 hrs

Module / Topic

- Sensor placement, signature and anomaly detection, rule interpretation, alert triage, tuning

Practical Lab Sessions

Lab 7: Deploy an IDS sensor and interpret the alerts it generates.

Lab 8: Tune the ruleset to reduce noise and document the coverage retained

M5 | Security Documentation & Escalation 12 hrs

Module / Topic

- Ticketing workflow, incident notes, escalation criteria, stakeholder communication, handover quality

Practical Lab Sessions

Lab 9: Write incident notes and an escalation summary for a live alert.

Lab 10: Complete a shift handover and have it peer-reviewed against a rubric

Program Frameworks – Intermediate Level: Junior Cyber Security Associate

Sem 5 · 90 hours · Reconnaissance, web testing and forensic evidence collection · 10 practical lab sessions

M1 | Reconnaissance & Enumeration with Nmap 20 hrs

Module / Topic

- Host discovery, port scanning, service and version detection, scripting engine, timing and stealth

Practical Lab Sessions

- Lab 1:** Enumerate a lab estate and produce a complete asset and service inventory.
- Lab 2:** Use the Nmap scripting engine to detect weak configurations at scale

M2 | Web Application Testing with Burp Suite 20 hrs

Module / Topic

- Proxy workflow, request manipulation, authentication testing, scanning, validating findings manually

Practical Lab Sessions

- Lab 3:** Test a web application for the OWASP Top 10 using Burp Suite.
- Lab 4:** Manually validate every automated finding and discard the false positives

M3 | Forensic Evidence Collection 18 hrs

Module / Topic

- Chain of custody, disk and memory acquisition with FTK Imager, verification hashing, documentation standards

Practical Lab Sessions

- Lab 5:** Acquire and verify a disk image and a memory capture.
- Lab 6:** Complete a full evidence log and chain-of-custody record

M4 | Alert Triage & First-Line Investigation 18 hrs

Module / Topic

- Triage frameworks, enrichment sources, investigation workflow, decision criteria, escalation quality

Practical Lab Sessions

- Lab 7:** Investigate three alerts end to end and reach an evidenced verdict on each.
- Lab 8:** Escalate one confirmed incident with a complete investigation package

M5 | Vulnerability Management Operations 14 hrs

Module / Topic

- Scan scheduling, asset criticality, risk prioritisation, remediation tracking, reporting to stakeholders

Practical Lab Sessions

- Lab 9:** Build a prioritised remediation backlog from a scan across the estate.
- Lab 10:** Produce a stakeholder report showing risk reduction over two cycles

Program Frameworks – Advanced Level: Ethical Hacking & Forensics

Sem 6–7 · 90 hours · Full-scope offensive assessment across networks, applications and endpoints · 10 practical lab sessions

M1 | Penetration Testing Methodology 18 hrs

Module / Topic

- Scoping and rules of engagement, standards and frameworks, phases of an assessment, evidence and legal boundaries

Practical Lab Sessions

Lab 1: Scope and plan a full-scope engagement with signed rules of engagement.

Lab 2: Build an evidence capture plan and test it in a dry run

M2 | Network Exploitation with Kali & Metasploit 22 hrs

Module / Topic

- Service exploitation, payloads and handlers, privilege escalation, persistence, pivoting between subnets

Practical Lab Sessions

Lab 3: Compromise a lab host, escalate privileges and establish persistence.

Lab 4: Pivot across subnets and document the complete kill chain

M3 | Web Exploitation with SQLmap 18 hrs

Module / Topic

- Injection discovery, automated exploitation, database extraction, WAF evasion, remediation guidance

Practical Lab Sessions

Lab 5: Discover and exploit injection points, extracting data with SQLmap.

Lab 6: Write remediation guidance and re-test to confirm the fix

M4 | Credential Attacks & Lateral Movement 18 hrs

Module / Topic

- Credential storage, Mimikatz techniques, pass-the-hash, Active Directory attack paths, detection opportunities

Practical Lab Sessions

Lab 7: Extract credentials with Mimikatz and move laterally in an AD lab.

Lab 8: Map the attack path and identify where detection should have triggered

M5 | Offensive Capstone & Forensic Reporting 14 hrs

Module / Topic

- Full engagement delivery, forensic-quality evidence, executive and technical reporting, panel defence

Capstone Lab

Lab 9: Deliver a full-scope offensive assessment with forensic-grade evidence.

Lab 10: Present the report, business impact and remediation roadmap to a panel

Track 6 Toolkit – Core Tools & Technologies

Every tool below is used in a defined lab session at the level shown.

Category	Tools / Platforms
Traffic Analysis	Wireshark
Detection	IDS / IPS
Operating System	Linux
Reconnaissance	Nmap
Web Testing	Burp Suite
Forensics	FTK Imager
Offensive OS	Kali Linux — the pen-tester's primary OS
Exploitation	Metasploit — exploit development and post-exploitation
Injection	SQLmap — automated SQL injection
Credential Attacks	Mimikatz — credential extraction and lateral movement

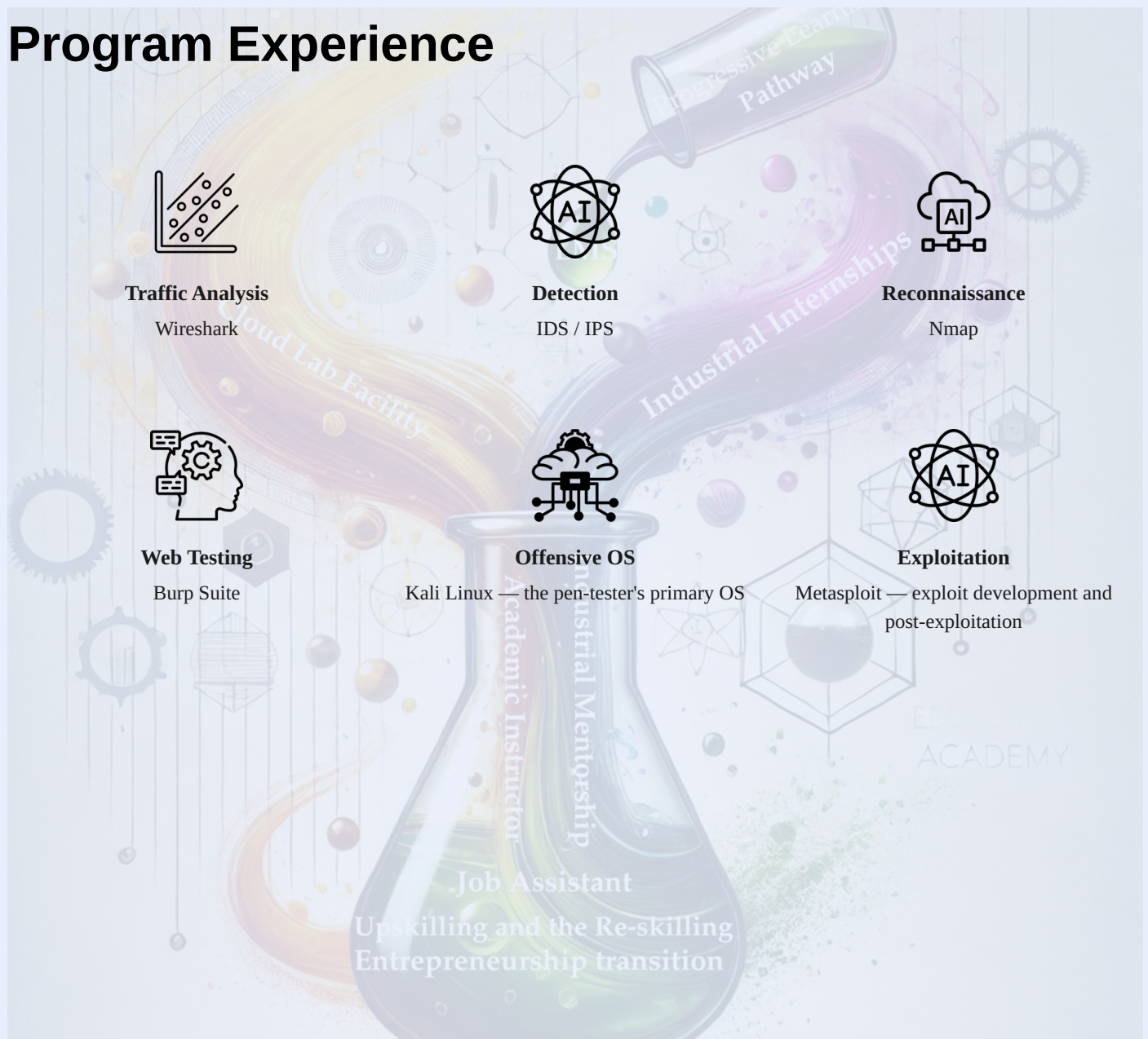
Tools by Level

Level	Toolset
Basic — Cyber Security Assistant	Wireshark · IDS / IPS · Linux
Intermediate — Junior Cyber Security Associate	Nmap · Burp Suite · FTK Imager
Advanced — Ethical Hacking & Forensics	Kali Linux — the pen-tester's primary OS · Metasploit — exploit development and post-exploitation · SQLmap — automated SQL injection · Mimikatz — credential extraction and lateral movement

Lab Environments

All practical sessions run in EduBlends cyber range and cloud lab environments. Offensive exercises are delivered on isolated, purpose-built ranges under defined rules of engagement, and forensic work uses write-blocked images and verified acquisition procedures.

Program Experience



The Cyber Security Assistant → Ethical Hacker track spans three levels and 270 hours, delivered through 30 structured lab sessions and a panel-assessed capstone. Learners progress from linux administration, ids/ips monitoring and traffic inspection at the Basic level, through reconnaissance, web testing and forensic evidence collection at Intermediate, to full-scope offensive assessment across networks, applications and endpoints at Advanced. Every topic is reinforced in isolated cyber range and cloud lab environments that mirror live industry workflows, so that graduates leave with evidenced, portfolio-grade security work.

Expected outcomes



Advanced Industrial Internship Certifications

Differentiate yourself from your peers by earning the industrially recognized Advanced industrial internship Certification



Students Blending Team

EduBlends blends the students for the industry-ready



For the Industrial, By the Industry

Learn and apply concepts on industry projects from industry, along with personalized industry mentorship



Industry Integration Layer

This program is designed with integrated industry collaboration, where enterprise partners contribute to curriculum alignment, real-world problem statements, and internship pathways.



Cyber Range & Cloud Lab Facilities

Isolated attack and defence ranges, forensic workstations and cloud sandboxes for real industrial problems



360 Degree Career Support — Entrepreneurial Program

Idea-to-Enterprise Catalyst by EduBlends Academy is a structured entrepreneurial program that guides innovators from ideation to execution, helping them build and scale tech-driven businesses such as security consultancies, managed services and SaaS solutions.



Personalized Mentorship

Get unparalleled personalized mentorship and doubt resolution from industrialists and academicians.

Sample Weekly Program Planner



4–5 hours

Live interaction with the programme learning facilitator



1–2 hours

Recorded video lecture with faculty



1 hour

Group discussion with industrial mentor and academic instructor



4–5 hours

Cyber range and cloud lab practice exercises



2 hours

Rigorous, graded assignments to apply and reinforce the material

12–15 hours

Total weekly effort

Who Is This Program For?

Career Launchers

The Basic level (Sem 3) is designed for students and early-career IT professionals with no prior security background who want a structured, hands-on entry into cybersecurity.

Career Builders

The Intermediate level (Sem 5) suits IT support staff, network engineers and system administrators who want to move into hands-on security engineering and analysis roles.

Career Switchers

The Intermediate level also serves mid-career professionals working outside security who want credible, evidenced capability before making a career change.

Specialists & Founders

The Advanced level (Sem 6–7) is for learners who have completed the earlier levels, or who bring equivalent experience, and want to move into specialist and consultant roles — or to launch a security venture through the entrepreneurial programme.

Progressive Learning Pathway: Our curriculum is structured to provide a seamless learning experience, from foundational security skills at the Basic level through to specialist practice at Advanced.

- **Basic — Cyber Security Assistant (Sem 3)** for students beginning their graduation, providing the core tools and foundations to start the journey
- **Intermediate — Junior Cyber Security Associate (Sem 5)** for students who have completed the Basic level, and for individuals looking to upskill into hands-on security roles
- **Advanced — Ethical Hacking & Forensics (Sem 6–7)** for students who have finished the earlier levels, and experienced individuals transitioning into specialist roles or entrepreneurship

Programs Key Features

Why Choose Our Courses?

Cyber Range & Cloud Lab: Gain hands-on experience in isolated attack and defence ranges with forensic workstations and cloud sandboxes, for real-world, industry-level security projects.

Industrial Internships & Expert Mentorship: Work on live industry projects, receive guidance from practising security professionals, and get the support you need for your career or entrepreneurial journey.

Personalized Instructor Support: Learn from experienced instructors committed to your growth, whether you are triaging your first alert or leading a full-scope engagement.

	Cyber Range Access	Industry-Integrated Internship	Live Mentorship by Industry Experts	Entrepreneurship Support
Coursera				
Udemy				
UpGrad Online				
Scaler Academy				
Simplilearn				
Unacademy				
EduBlends Academy	✓	✓	✓	✓

Comparison rows left intentionally blank pending verification. Competitor feature claims must be sourced, dated and evidenced before publication.